

Command™

The Command Filtering and Notification Component of iSecurity



User Manual

Version 1.1



Updated: 11/09/2012

Copyright Notice

© Copyright Raz-Lee Security Inc. All rights reserved.

This document is provided by Raz-Lee Security for information purposes only.

Raz-Lee Security© is a registered trademark of Raz-Lee Security Inc. Action, System Control, User Management, Assessment, Firewall, Screen, Password, Audit, Capture, View, Visualizer, FileScope, Anti-Virus, AP-Journal © are trademarks of Raz-Lee Security Inc. Other brand and product names are trademarks or registered trademarks of the respective holders. Microsoft Windows© is a registered trademark of the Microsoft Corporation. Adobe Acrobat© is a registered trademark of Adobe Systems Incorporated. Information in this document is subject to change without any prior notice.

The software described in this document is provided under Raz-Lee's license agreement.

This document may be used only in accordance with the terms of the license agreement. The software may be used only with accordance with the license agreement purchased by the user. No part of this document may be reproduced or retransmitted in any form or by any means, whether electronically or mechanically, including, but not limited to: photocopying, recording, or information recording and retrieval systems, without written permission given by Raz-Lee Security Inc.

Visit our website at <http://www.razlee.com> .

Record your Product Authorization Code Here:

Computer Model:	<input type="text"/>
Serial Number:	<input type="text"/>
Authorization Code	<input type="text"/>

Table of Contents

About This Manual	1
Product Documentation Overview	1
Printed Materials	1
Online Help	1
Typography Conventions	1
Other iSecurity Products	2
Chapter 1: Introducing Command	4
The Need for Command	5
Feature Overview	5
Benefits	5
System Requirements	6
Native OS/400 Text Based User Interface	6
Menus	6
Data Entry Screens	6
Chapter 2: Command Security	8
Work with Restricted Commands	8
Adding a New Command Restriction	9
Work with Command Rules	10
Work with a Command Rule	11
Filter Conditions	13
Message to Send	16
Adding a Command Alert	17
Edit Action Script	19
Replacement Variables	20
Conditional Branching	20
Replace Values	20
Copying a Command Rule	22
Adding a New Restricted Command	23
Deleting a Restricted Command	24
Chapter 3: Definitions, Analysis and Maintenance	25
Command General Definitions	26

About This Manual

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on AS400 systems. However, any user with basic knowledge of AS400 operations will be able to make full use of this product after reading this book.

Product Documentation Overview

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal AS400 experience. The documentation package includes a variety of materials help users become familiar with this software quickly and effectively.

Printed Materials

This user guide is the only printed documentation necessary for understanding this product. It is available in user-friendly PDF format and may be displayed or printed using Adobe Acrobat Reader version 4.0 or higher. Acrobat Reader is included on the product CD-ROM.

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

Online Help

AS400 context sensitive help is available at any time by pressing the **F1** key. A help window appears containing explanatory text that relates to the function or option currently in use. Online help will shortly be available in Windows help format for viewing on a PC with terminal emulation.

Typography Conventions

- Menu options, field names, and function key names are written in **Bold**.
- References to chapters or sections are written in *Italic*.
- OS/400 commands and system messages are written in ***Bold Italic***.
- Key combinations are separated by a dash, for example: Shift-Tab.
- Emphasis is written in **Times New Roman bold**.

Other iSecurity Products

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.

Other iSecurity products include:



Action

Action automatically intercepts and responds to security breaches, system activity events, QHST contents, and other message queues. Inquiring messages can be automatically answered. Alerts are sent by e-mail, SMS, pagers, or the message queues. Command scripts with replacement variables perform customized corrective actions, such as terminating a user session or disabling a user profile.



AP-Journal

AP-Journal automatically manages database changes by documenting and reporting exceptions made to the database journal.



Assessment

Assessment checks your ports, sign-on attributes, user privileges, passwords, terminals, and more. Results are instantly provided, with a score of your current network security status with its present policy compared to the network if iSecurity were in place.



Audit

Audit is a security auditing solution that monitors System i events in real-time. It includes a powerful query generator plus a large number of predefined reports. Audit can also trigger customized responses to security threats by means of the integrated script processor contained in Action.



Capture

Capture silently captures and documents user screens for tracking and monitoring, without any effects on system performance. It also preserves job logs for subsequent review. Capture can run in playback mode and can be used to search within texts.



Change Tracker

Change Tracker automatically tracks modifications in production libraries, at both the object and source levels. It does not require any special actions by programmers, relying solely on the changes actually made to libraries as logged in QAUDJRN.



DB Gate

DB Gate lets users open concurrent and transparent SQL connections to numerous types of remote data sources and databases, on any IBM or non-IBM platform, using STRSQL and compile using CRTSQL for programs which refer to these databases.



Firewall

Firewall protects and secures all types of access, to and from the System i, within or outside the organization, under all types of communication protocols. Firewall manages user profile status, secures entry via pre-defined entry points, and profiles activity by time. Its Best Fit algorithm determines the validity of any security-related action, hence significantly decreasing system burden while not compromising security.



Password

Password provides a first-tier wall of defense for users by ensuring that user passwords cannot be easily cracked.



Screen

Screen protects unattended terminals and PC workstations from unauthorized use. It provides adjustable, terminal- and user-specific timeout capabilities.



View

View is a unique, patent-pending, field-level solution that hides sensitive fields and records from restricted users. This innovative solution hides credit card numbers, customer names, etc. Restricted users see asterisks or zeros instead of real values. View requires no change in existing applications. It works for both SQL and traditional I/O.



Visualizer

Visualizer is an advanced DWH statistical tool with state-of-the-art technology. This solution provides security-related data analysis in GUI and operates on summarized files; hence, it gives immediate answers regardless of the amount of security data being accumulated.

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.

NOTE: If 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

```
CMMENU                               Command                               iSecurity
                                     System:   S520

Command Security                      Analysis
  1. Work with commands                41 Work with Queries
                                       42. Command log

Definitions                            Maintenance
  31. Time Groups                      81. System Configuration
  32. General Groups                   82. Maintenance Menu
                                       83. Central Administration

Selection or command
===> █

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

Command MainScreen

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

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: 110MB
- **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**.



The following 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: 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 following 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.

```

Work with Restricted Commands
Type options, press Enter.                Subset . . . _____
  1=Select  4=Remove  7=Activate  8=Deactivate

Opt  Status  Command  Library
---
-    ---    ADDACC  QSYS    Add Access Code
-    ---    ADDCLUNODE  QSYS    Add Cluster Node Entry
-    ---    CHGUSRAUD  QSYS    Change User Auditing
-    ---    CHGUSRPRF  QSYS    Change User Profile
-    ---    CHKSLAUT  SMZ1    SL-Check Site License Authorization
-    ---    CPYF      QSYS    Copy File
█    Active  DSPAULOG  SMZ4    Display Audit Log
-    ---    DSPFSDTAQ  SMZ2    FST-Edit Data Q
-    Active  DSPSYSSTS  QSYS    Display System Status
-    ---    IBI       SMZ1    i Business Intelligence
-    ---    PWRDOWNSYS  QSYS    Power Down System
-    ---    TELNET    QSYS    Start TCP/IP TELNET
-    ---    WRKFSTRC  SMZ1    FS trace
-    ---    WRKSBSJOB  QSYS    Work with Subsystem Jobs
More...

F3=Exit  F6=Add New  F8=Print  F12=Cancel
  
```

Work with Restricted Commands Screen

Parameter	Description
Option 1	Select 1 to edit the selected command rule
Option 4	Displays the Remove Restricted Command screen. Press Enter to remove the selected command and return to the Work with Restricted Commands screen
Option 7	Activates the selected command

Parameter	Description
Option 8	Deactivates 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 following Add Restricted Command screen is displayed.

```

Add Restricted Command

Type choices, press Enter.

Command . . . . . CHGFC          Name
Library . . . . . *LIBL          Name, *LIBL

Activate definition . . . . . Y          Y=Yes  N=No

F3=Exit  F4=Prompt  F12=Cancel

Modify data, or press Enter to confirm.
  
```

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.

Parameter	Description
Library	Enter the name of the specific library where the command will run. If entering a command when *LIBL is displayed, Command will automatically insert the first library from the Library List that includes this command.
Activate Definition	Y=Yes N=No

Work with Command Rules

From the **Work with Restricted Commands** screen, choose **1. Select** to view a command's rules and edit them. The Work with Command Rules screen is displayed with each rule numbered according to the sequence in which it runs.

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.

```

Work with Command Rules
Command: QSYS/CHGUSRPRF          Change User Profile
Type option, press Enter.
  1=Select  3=Copy  4=Delete  6=Condition  7=Replace values  8=Message  9=Alert
          Allow
Opt  Seq  Run  Action
█    1.0  Y    *NONE    Only *ALLOBJ user can give *ALLOBJ +other limits
-    2.0  Y    AU155636MI  User profile *DISABLED
-          Y    *NONE    Default for: QSYS/CHGUSRPRF
          -

Bottom

F3=Exit  F6=Add New  F8=Print  F12=Cancel  F22=Renumber

Modify data, or press Enter to confirm.
  
```

Work with Command Rules Screen



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 description
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 (e.g., 2, 4, 5). Select option 22. Renumber to reset the first command rule in the sequence to 1, incrementing by +1 for each new row.

To edit a specific command rule row, choose **1. Select**. The Work with a Command Rule screen appears. When done, press Enter; press Enter again to confirm the update.

Work with a Command Rule

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 Command Rules screen.

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

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

```

Work with a Command Rule

Command: QSYS/PWRDWN SYS      Power Down System

Type choices, press Enter.

Sequence Id . . . . . 1.0
Description . . . . . Alert System Operator and Restart the System

Select options:
Work with conditions . . . . . > Y           Y=Yes
Alert by Action Id . . . . . *NONE          Name, *ADD, *NONE, F4=Prompt
Work with message text to send > Y         Y=Yes

Work with changes to apply
before running the command . > Y           Y=Yes

Allow the command to run . . . Y           Y=Yes (with/out changes)
                                           N=No (reject it)

> appears when definitions already exist.

F3=Exit  F4=Prompt  F12=Cancel

```

Work with a Command Rule Screen

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
Work with conditions	<p>Y=Yes (or empty)</p> <p>When updating the rule, if Yes is selected (i.e., there is a rule condition), displays the Filter Condition screen when cycling through the different rule screens.</p> <p>Note: For the actual command (i.e., final command rule row), this option is called Default and is empty.</p>
Alert by Action Id	<p>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</p> <p>Name = Name of an action</p> <p>*ADD (default) = Define a new action for this rule</p> <p>*NONE = no action is defined</p> <p>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.</p>



Parameter	Description
Work with message text to send	Y=Yes (or empty) When updating the rule, if Yes is selected (i.e., there is message text), displays the Message to Send screen when cycling through the different rule screens.
Work with changes to apply before running the command	Y=Yes When updating the rule, if Yes is selected (i.e., there is a replacement value), displays the Replace Values screen when cycling through the different rule screens.
Allow the command to run	Y=Yes (with/out changes) N=No (reject it)
>	This symbol appears when a definition already exists

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**.

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.

Group 1

Group 2

```

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
Or Parameter
User profile
A Status
O User profile
A User class
A Job description
- User profile
- User password
- Special authority...
- Set password to expired
- Status

Q/E
Id Test Value (use F4 for ITEM), *N=Missing
EQ QSECOFR
EQ *DISABLED
EQ MICHAEL
EQ SECOFR
Q 1 EQ LIBRARY

More...

F3=Exit F4=Prompt F6=Insert F7=Prompt CMD F8=CMD help F11=Text/Fld
F12=Cancel
    
```

Filter Conditions Screen

Parameter	Description
And/Or	<p>A or Blank = And</p> <p>O = Or</p> <p>Combine multiple filter conditions in one rule using Boolean AND/OR operators to create complex rules that produce precise results.</p> <p>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.</p> <p>'And' condition groups the 'Or' condition which was defined before it.</p> <p>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.</p>
Parameter	<p>Parameters</p> <p>"..." denotes a list of additional values</p> <p>Pink fields are part of the generic header common to all journal types</p> <p>Green fields represent data specific to this journal type</p>



Parameter	Description
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: <ul style="list-style-type: none"> • 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 grpprf3)
Test	Comparison test type (see table below for details)
Value	Comparison value text. Note: This field 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 as shown in the following table:

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 %



Test	Description	Value Field Data
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.	<p>*USER – Check that the value is a user in a %GROUP of users</p> <p>*GRPPRF – Check that the value is a user in an OS/400 Group Profile</p> <p>*USRGRP – USER and all user profiles which are members of same user groups as USER</p> <p>*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.</p> <p>*SPCAUT – Check that the value is in the users Special-Authority</p>
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.


```

Add Alert

Type choices, press Enter.

Action Name . . . . . GS110019QP
Description . . . . . Created by Action _____

Define alert message recipients
1=E-mail 2=Message Queue 3=User 4=Remote User 5=LAN user 6=SMS 7=Special
8=Syslog 9=SNMP T=Twitter
Type Recipient address, *USER, *DEV, *JOB, *SYSTEM
1 J@J.COM
2 QSYSOPR
3 QSECOFR
6 2019976520
8
9
T
More...

F3=Exit F12=Cancel

```

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, <i>Working with Message Queues</i> section.
User	User profile or AS/400 group profile
Remote User	Remote system user (<i>SNDNETMSG</i>)
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. System Configuration > 71. Syslog
SNMP	As defined in 81. System Configuration > 81. iSecurity/Base > 32. SNMP
Twitter	As defined in 81. System Configuration > 81. iSecurity/Base > 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.

Edit Action Script

Action . . GS094014QP

Type choices, press Enter.
 Note: Add quotes where needed. e.g. CALL PGM PARM('&PARM01' '&PARM02').

Order	Label	Command, GOTO label (unconditional)
1.00		CHGUSRPF USRPF (&ZRUSPF) PASSWORD() STATUS(*DISABLED)
2.00		On error, go to label . . ERROR1 ENDJOB JOB(&ZRJOB/&ZRUSER/&ZRNBR) OPTION(*IMMED)
3.00	ERROR1	On error, go to label . . _____
4.00		On error, go to label . . _____
		On error, go to label . . _____

More...

F3=Exit F4=Prompt F7=Replacement variables F8=Replacement job F12=Cancel

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, do the following:

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 following Replace Values screen appears. This screen also appears when cycling through the screens after the Work with Command Rule screen.

Replace Values

```

Cmd . QSYS/PWRDWNYSYS
Type conditions, press Enter.
Operations: DFTPRM, OMTPRM, DFTLST, OMTLST, SET, RPL
For RPL use %aaa%bb% to replace every aaa with bb.
Q/E=Qualifier/Element, enter its Id or leave blank. "... denotes List.
Parameter          Q/E Id Oper  Value
How to end                █
Controlled end delay time
Restart options          E  SET  *YES
IPL source
Image catalog
End subsystem option...
Timeout option
Confirm
Command name
Command library
    
```

Bottom

F3=Exit F7=Prompt CMD F8=CMD help F10=Long value F11=Text/FId F12=Cancel

Replace Values Screen

Parameters / Options	Description
Parameter	Parameters associated with the current command rule
Q/E	Qualifier or Element to replace
ID	ID of the Qualifier or Element
Oper	Action to take (as defined in the Operations line above) DFTPRM – Default Parameter OMTPRM – Omit Parameter DFTLST –Default List OMTLST – Omit List SET – Set Parameter RPL – Replace Parameter
Value	Replacement value
F7	Prompt CMD– to display the command parameters
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 following 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.

```

Copy a Command Rule

Command: QSYS/DSPSYSSTS      Display System Status

Type choices, press Enter.

Filter Id.
From . . . . . 1.0 TEST DSPSYSSTS
To . . . . . █ 1.0 TEST DSPSYSSTS

F3=Exit  F12=Cancel
    
```

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

Adding a New Restricted Command

To add a new restricted command, select **1. Work with Commands** from the main menu. When the Work with Restricted Commands appears, select **F6. Add New**. The following Add Restricted Command screen is displayed.

```

Add Restricted Command

Type choices, press Enter.

Command . . . . . █          Name
Library . . . . . *LIBL      Name, *LIBL

Activate definition . . . . . Y      Y=Yes  N=No

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

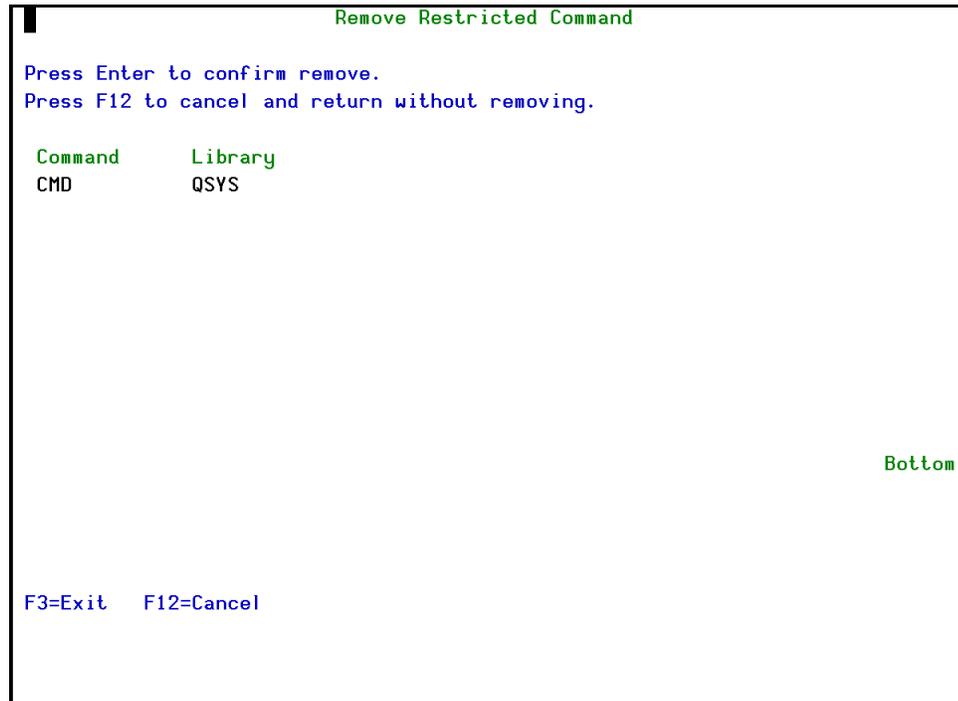
Add Restricted Command Screen

Parameter	Description
Command	Name = Enter the name of the command If a specific library has been defined, pressing F4 will display the Select Command popup. Choose a command from the list and enter 1. Select .
Library	Name = Enter the name of a specific library *LIBL = Associate the command with all libraries
Activate Definition	Y = Yes N = No



Deleting a Restricted Command

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



Remove Restricted Command Screen

Chapter 3: 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 referenced in the following table.

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 section below
	81. iSecurity/Base – see Audit User Manual
82. Maintenance Menu	Firewall User Manual
83. Central Administration	Audit User Manual

Command General Definitions

The 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**.

```

Command General Definitions

Type options, press Enter.

Secure (Check commands) . . . . . 1 1=Yes, 2=No

Information to log . . . . . 4 1=None
                               2=Rejects and changes
                               4=All

Work in *FYI* (Simulation) mode . . . . . N Y, N
*FYI* is an acronym for "For Your Information". In this mode,
security rules are fully operational, but no action is taken.

F3=Exit F12=Previous
    
```

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
Work in *FYI* (Simulation) mode	*FYI* is an acronym for "For Your Information". In this mode, command rules are fully operational, but no action is actually taken. This enables one to review the History Log for analysis, and thereby create valid security rules at a later time. Y= Enable FYI N = Do not enable FYI