

Firewall™

The Network Security Solution of



User Manual

Version 15



Updated: 05/24/2011

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"/>

About This Manual

Who Should Read This Book

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on System i. However, any user with basic knowledge of System i 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 System i experience. The documentation package includes a variety of materials to familiarize the user with Firewall quickly and effectively.

Printed Materials

This user guide is the only printed documentation necessary for understanding **Firewall**. 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.

Firewall includes a single user guide that covers the following topics:

- Introduction
- Installation
- Start-up and Initial Configuration
- Using Firewall

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

System i context-sensitive help is available at any time through the **F1** key. A help window appears containing explanatory text relating 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 **Sans-Serif 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**.

Table of Contents

About This Manual	ii
<i>Who Should Read This Book</i>	<i>ii</i>
<i>Product Documentation Overview</i>	<i>ii</i>
<i>Printed Materials</i>	<i>ii</i>
<i>Online Help</i>	<i>ii</i>
<i>Typography Conventions.....</i>	<i>ii</i>
New Features in Firewall Versions.....	1
New Features for Firewall 15.6	1
New Features for Firewall 15.5	1
New Features for Firewall 15.0	1
Chapter 1: Introducing Firewall	2
What is Firewall?	2
Why is Firewall Necessary?	2
Feature Overview	3
<i>Top-Down Security Design.....</i>	<i>3</i>
<i>Multi Thread Support.....</i>	<i>4</i>
<i>Firewall Rules and the Best-Fit Algorithm.....</i>	<i>5</i>
<i>FYI Simulation Mode.....</i>	<i>5</i>
<i>Emergency Override.....</i>	<i>5</i>
<i>Rule Wizards</i>	<i>5</i>
<i>Log.....</i>	<i>5</i>
<i>Query Wizard</i>	<i>6</i>
The “User-Centric” Approach	6
<i>User Security.....</i>	<i>6</i>
<i>User Management</i>	<i>7</i>
<i>Intrusion Detection.....</i>	<i>7</i>
Native OS/400 Text Based User Interface	8
Other iSecurity Products	10
Chapter 2: First Steps	11
Initial Setup and Definition Overview	11
Starting Firewall for the First Time	12
Modifying Operators’ Authorities	12
FYI Simulation Mode.....	14
Enabling Protection for all Servers.....	16
Using the Rule Wizards	17
<i>Procedural Overview</i>	<i>18</i>
<i>Analyzing Historical Activity.....</i>	<i>19</i>
<i>Defining the Working Data Set.....</i>	<i>21</i>
<i>Working with the Plan Security Wizard Screens</i>	<i>21</i>
<i>Native OS/400 Objects Log</i>	<i>23</i>
<i>Update Rules</i>	<i>26</i>
User Groups	27
<i>OS/400 Group Profiles.....</i>	<i>27</i>
<i>Firewall Proprietary User Groups.....</i>	<i>27</i>
Time Groups	30
<i>Overview.....</i>	<i>30</i>
<i>Using Time Groups as Filter Criteria</i>	<i>31</i>
<i>Defining and/or Modifying Time Groups</i>	<i>31</i>
Application Groups	32

Overview.....	32
Defining and/or Modifying Application Groups.....	32
Location Groups.....	34
Overview.....	34
Chapter 3: Basic Security	37
About Servers & Exit Points	37
Working with Server Security Rules	38
Using the Global Server Security Settings Feature	42
FYI Simulation Mode – Global Setting	44
Using the Emergency Override Feature.....	44
Chapter 4: Dynamic Filtering Security	46
IP Address Firewall Rules	46
SSL Support:.....	49
Why Raz-Lee developed the SSL Solution	50
The Customer's Testing Methodology	50
SNA Firewall Rules	51
Chapter 5: User Security.....	53
Conceptual Framework	53
Verb Support	53
Rule Definition Procedure	54
Client Application Security	56
User Management	58
Work with Users.....	58
Reports	63
Disable Inactive Users.....	65
Restricting User Sign-on Times.....	66
User Absence Security.....	68
Password Control Tools.....	70
Analyze Default Passwords	70
Password Statistical Report	71
Chapter 6: Object Security.....	73
Procedural Overview	73
Native OS/400 Objects	74
Files.....	74
Libraries.....	77
Data Queues.....	79
Printer Files	81
Programs.....	83
Commands.....	85
Command Exceptions.....	87
Work with Pre-check Library Replacement.....	88
IFS Objects	91
Chapter 7: Logon Security.....	93
Procedural Overview	95
FTP/RExec (Incoming).....	96
Client FTP (Outgoing)	98
Telnet and Sign-on	100
Telnet Logon.....	100
SSL Control in Firewall	102
Sign-on	102

Internet (WSG)	106
Passthrough.....	109
Chapter 8: Queries, Reports and Logs	111
Query Wizard	111
Procedural Overview	112
Working with Queries.....	112
General Query Parameters (Add/Modify Screen)	113
Defining Output Fields.....	117
Sort Criteria	118
Running Queries.....	119
Print Query to Output File and Send Via Email.....	122
Working with the Activity Log.....	123
Statistics	127
Group Items for Selection.....	128
Using the Report Scheduler	131
Overview.....	131
The Definition Process	131
Working with Report Groups.....	132
Working with Individual Reports.....	136
Running Reports.....	136
Chapter 9: Advanced Security Features	138
DDM, DRDA Security.....	138
Pre-Check User Replacement.....	138
DRDA Post-Check User Replacement.....	140
DHCP Security	140
TCP/IP Port Restrictions.....	142
Work with TCP/IP Port Restrictions	142
License Management Security.....	143
License Management.....	143
Display License Management Log	145
Chapter 10: Configuration and Maintenance.....	146
System Configuration.....	146
General Definitions	146
Additional Settings	148
User Exit Programs.....	149
Transaction Post-Processing.....	151
Intrusion Detection.....	151
Password Exit Programs.....	152
Enable ACTION (CL Script + More)	153
SYSLOG.....	154
Log retention	155
Language Support	156
The Maintenance Menu	157
iSecurity Part 1 Global.....	158
Firewall Specifics.....	160
General.....	162
Purging all data of FIREWALL.....	163
*PRINT1-*PRINT9 Setup.....	163
Journal Product Definitions.....	164
iSecurity Central Administration	168
Appendix: List of Firewall Exit Points.....	172

New Features in Firewall Versions

New Features for Firewall 15.6

New feature “Client Application Security”, option 18

New Features for Firewall 15.5

- Inherit in-product IFS authorities from higher directory or file (81→2)
- Skip SQL parsing if accept/reject network access decision was taken at global, IP or user level (81→2)
- Web application server performance improvements (2→1→1→1 “Skip Checks” options) dramatically improve performance when a high volume of requests originate from a well secured IP that uses SSL.
- Streamline rules support for multiple libraries (21→61) by using “model libraries” to define security rules
- SQL long names (up to 128) are now support for Table (File) and for Collection/Schema (Library)
- SQL and Wizards performance improvements
- In Users and Groups security, for %Group the number of members appears and Group Profiles are signified by *GRPPRF

New Features for Firewall 15.0

Inherited Authority for IFS objects (optional)

- Optional change in IFS object authorization determination
- The Best Fit algorithm has new variations: If selected, the change allows getting authority from the preceding directories, or even from any level of a higher generic name
- Enables easier distribution of authorities by directories

Chapter 1: Introducing Firewall

What is Firewall?

Firewall is a truly comprehensive network security solution that completely secures your System i (AS/400) against all known external threats, and also controls what users are permitted to do **after** access is granted. **Firewall** is a robust, cost-effective security solution.

Firewall is the by far the most intuitive and easy-to-use security software product on the market today. Its top-down functional design and intuitive logic creates a work environment that even System i novices can master in minutes. **Firewall** features a user-friendly, Java-based GUI and a System i Navigator (OpsNav) plug-in, in addition to the traditional green-screen interface.

Why is Firewall Necessary?

Previously, the System i was used almost exclusively in a closed environment, with host systems connected to remote data terminals via proprietary technologies. Within this closed environment, the security features of the OS/400 operating system provided the strongest data and system security in the world. User profiles, menus and object level security provided all the tools necessary to control what users were allowed to see and do.

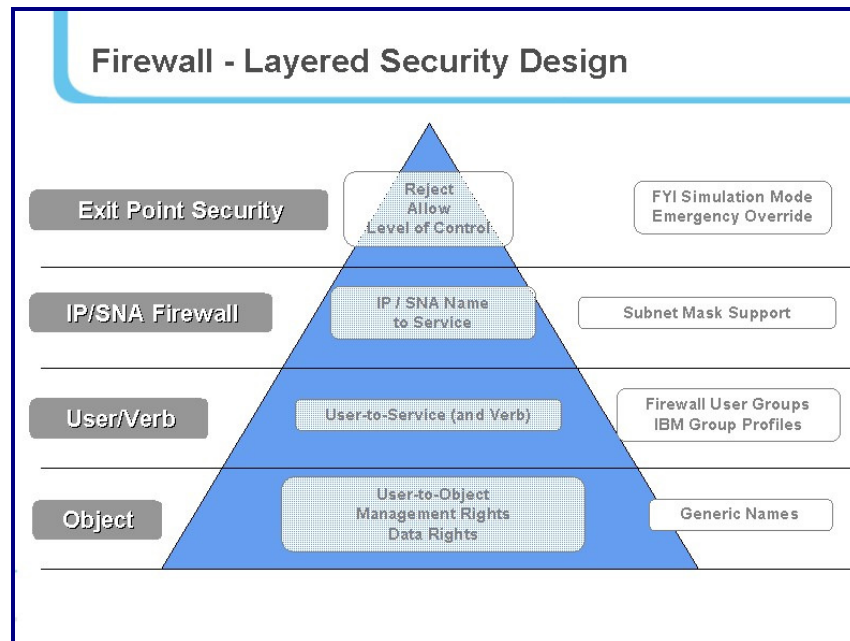
In today's world of enterprise networks, PCs, distributed databases, Internet and web technologies, closed computing environments are all but extinct. Technological advances compelled IBM to open up the System i and its OS/400 operating system to the rest of the world. This openness brought along many of the security risks inherent in distributed environments. System administrators need to equip themselves with a new generation of security tools to combat these evolving threats. **Firewall** is an advanced security tool which enhances native OS/400 by controlling access through all known external sources as well as controlling what users are permitted to do once access is granted.

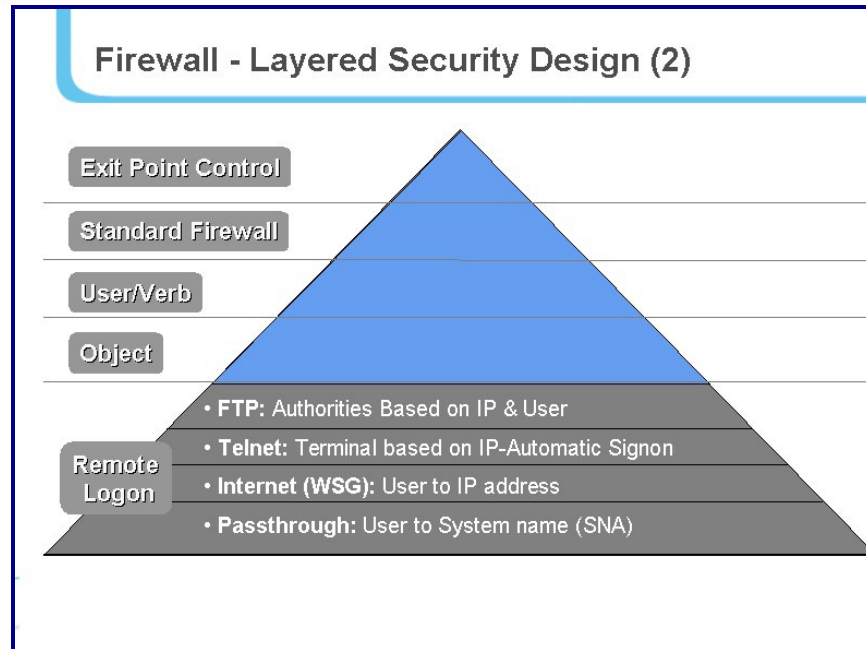
Feature Overview

Top-Down Security Design

Top-Down security design means that the process of designing and applying security rules follows the most efficient logical path possible. In other words, the user has to formulate a minimal number of rules in order to achieve maximum security and the System i has to process apply rules to far fewer transactions than many similar products. This saves planning and maintenance time as well as valuable system resources.

Top down security offers a simple hierarchy of rule types. When a higher level rule type fully meets a situation's security requirements, the user doesn't have to formulate any more rules for the said situation. The following drawing illustrates this concept.





System i security is based on five basic levels:

- Server/Exit Point Security
- TCP/IP Address Firewall Security
- User-to-Service Security
- Object Security
- Logon Security (provides additional security features once access has been granted)

Simply put, whenever a higher, less specific rule will suffice, you do not need any more specific rules. For example, if you do not need to use FTP, you simply reject all transactions at the FTP Server/Exit Point level. You do not need to define any rules that limit FTP access via specific IP addresses, by specific users, or to specific objects.

Multi Thread Support

Calling programs from a thread that is not the main one forces various limitations on the called programs. For example, the command Override with Data Base File (OVRDBF) cannot be used. This requires special programming in the called program.

Firewall secures network access by providing programs to be called by security related exit points. Firewall modules have been specifically treated to improve their capability to work in secondary threads. This support is not all-encompassing also because it is related to system API's abilities to function in such circumstances.

We recommend, when possible, working in single thread mode. Otherwise, perform a check, such as checking the log, in order to validate proper performance.

Firewall Rules and the Best-Fit Algorithm

Firewall is a rules-based security product. The user creates a wide variety of rules to cover many different situations and to counter different kinds of threats. Some rules will likely apply globally to all or most activity types while others will cover very specific situations.

The user can enable the FYI Simulation Mode globally for all activity regardless of server or user. The user can also enable FYI individually for specific function servers as a parameter in server security rules. In this manner, security rules can be tested for specific servers without affecting rules that apply to other servers.

FYI Simulation Mode

FYI Simulation Mode allows the user to simulate the application of security rules without physically rejecting any activity. All "rejected" transactions are recorded in the Activity Log as such but the activity is allowed to proceed without interruption. This feature allows you to test your rules under actual working conditions without adversely affecting user access.

The FYI Simulation Mode may be enabled globally for all activity or enabled for individual function servers. In this manner, one can test security rules for specific servers without affecting rules that apply to other servers.

Emergency Override

The Emergency Override feature allows the user to override all existing security rules temporarily by allowing or rejecting all activity. This feature is useful in order to respond quickly to emergencies such as critical transactions being rejected due to problems with **Firewall** security rules or a sudden security breach.

Rule Wizards

The unique Rule Wizards feature makes security rule definition a snap, even for non-technical system administrators. This user-friendly feature allows the user to view historical activity together with the security rule currently in effect on a single screen. One can even modify the existing rule or define a new rule without closing the wizard. The Rule Wizards are an invaluable tool for defining the initial set of rules after installing **Firewall** for the first time.

Log

The activity log provides complete details for every transaction captured as a result of a security rule. The user can select the activities to be included in the Activity Log and the conditions under which they are logged (average of 800 bytes per SQL statement). Users can display or print selected records from the Activity Log by entering the **Display Firewall Log (DSPFWLOG)** on any command line or from numerous locations on **Firewall** menus and data screens.

For REJECTS - The log entry shows the first level where the request is a violation to the Firewall rules.

For ALLOWED – The log entry shows the last test that was taken and found valid.

- QSECOFR as well as any other user CANNOT update or delete records from the file that contains the log. This is true even when using SQL, DFU, and CHGFC command and so on.

- Users that are authorized to option 82, 11 as Administrators can setup the number of days that data is kept online
- Users that are authorized to option 82, 11 as Administrators can use STRFW, 82, 51. Work with Collected Data and remove data of full days.
- QSECOFR as well as any other user who is authorized, can change the logging option in **Firewall** per service (exit point). Type: STRFW, 1, 1
- QSECOFR as well as any other user who is authorized can change the logging option per user in **Firewall**. Type STRFW, 1, 11

Query Wizard

The powerful Query Wizard allows users to design custom output reports that show exactly the necessary data without programming or technical knowledge. One can create query definitions by using a series of simple parameter definition screens. Output may be a printed report, a screen display or a text file saved on the System i.

Highly detailed filter criteria enables users to select only the necessary records by using Boolean operators and the ability to combine complex logical conditions. Firewall's flexibility enables users to specify the sort order according to multiple fields. All reports can run automatically and be e-mailed to the system administrator as HTML, PDF or CSV files.

The “User-Centric” Approach

Firewall has a “user-centric” approach set in the top-down model, which helps the security administrator to manage user security easily and efficiently and reduces the number of security rules.

Raz-Lee Security has created two new user groups in addition to the existing general Firewall group. Together they form three groups that enable organization of the users: General Groups, Application Groups, and Location Groups. See *Chapter 3: First Steps*.

User Security

Firewall offers optimized basic user security. Defining a single user security definition can be performed as described in the following table (see *Chapter 6: User-to-Service Security* for more detail).

Method	Description
%Groups	Assign a user to a user group (similar to the option of selecting members for each of the user groups).
Services	Same as the previous method of user-to-service definitions
IP	Same as the Location group rules, but only applicable to single users.
Device Names	Only for Telnet sign on. Same as Location group rules, but only applicable to single users

User Management

Originally an **Action** feature enabling user management abilities, User Management has been added to **Firewall**. It contains several powerful security tools that control access permissions. User Management enhances active system security by allowing users to perform the following tasks:

- View and modify security parameters in user profiles using a convenient wizard
- Automatically disable inactive users
- Restrict user sign-on to specific hours and days
- Prevent user sign-on during planned absences or following termination
- Analyze default passwords for effectiveness

See *Chapter 5: User-to-Service Security*.

Intrusion Detection

This feature enables **Firewall** to trigger proactive responses (similar to the ones available on the **Action** module but less flexible). Those responses, such as notification about intrusions to the admin by MSGQ and email are general, easy to use, yet important.

See *Chapter 10: Maintenance*.

Native OS/400 Text Based User Interface

Firewall is designed from the ground up to be a user-friendly product for auditors, managers, security personnel and system administrators. The user interface follows standard System i CUA 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 easy access to all features with a minimum number of clicks. 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.

Commands

Many **Firewall** features are accessible from any command line simply by typing the appropriate commands. Some of the most commonly used commands appear below.

- Display **Firewall** log (*DSPFWLOG*)
- Run a **Firewall** query (*RUNFWQRY*)
- Run a predefined group of reports (*RUNRPTGRP*)
- Print user profile information report (*PRTFWUSRP*)

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 filter with generic text support

The following table describes the various data entry screen options.

Desired Procedure	Required Steps
Entering data in a field	Type the desired text and then press Enter or Field Exit
Moving from one field to another without changing the contents	Press the Tab or Shift-Tab keys
Viewing options for a data field together with an explanation	Press F4
Accepting the data displayed on the screen and continue	Press Enter

Function Keys

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

Other iSecurity Products



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



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 triggers customized responses to threats via the integrated script processor contained in 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. Easy-to-use Rule Wizard helps define rules and actions.



Capture silently captures and documents user screens for tracking and monitoring – without any effects on system performance. Capture can run in playback mode and can be used to search within texts. It also preserves job logs for subsequent review. Screen captures can be according to user name, IP address, time of day, and more.



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 modification to existing applications.



Anti-Virus provides virus detection and prevention. Anti-Virus scans, validates, and checks IFS files as they are enrolled or modified, authenticates them, and erases/quarantines infected files. Includes an updateable database and a simple interface.



Screen protects unattended terminals and PC workstations from unauthorized use. It provides adjustable, terminal- and user-specific timeout capabilities. Screen locking and signoff periods may be defined according to variable criteria such as date, time of day or user profile.



Password is a general-purpose password management product that ensures user passwords cannot be easily guessed or cracked. Password allows the user to manage a variety of password security parameters and maintains a history log of attempts to create passwords. This log can easily be displayed or printed.



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



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

Chapter 2: First Steps

This chapter covers the steps necessary to begin using **Firewall** for the first time. Also covered in this chapter are the basic procedures for configuring the product for day-to-day use.

Initial Setup and Definition Overview

Firewall is easy to set up and use right out of the box. The factory default parameters are adequate for many installations. You will likely need to configure only a few parameters to meet the specific needs of your organization.

It should be noted that, by default, protection is disabled for all servers, users and objects following initial installation. You must enable protection and define your security rules in order to begin enjoying the benefits of **Firewall** protection.

As with any computer security product, careful consideration should be given to defining security rules that will maximize protection for your organization against intrusion and user abuse - without adversely affecting legitimate user access and/or system response time. Before beginning the steps below, the user should complete the process of identifying which specific servers and objects are to be protected and which users should be granted access rights thereto.

This section is intended to help you with the process of configuring **Firewall** and defining your first security rules according to your organization's security policies. The process entails the following steps, in sequential order:

1. Obtain and enter the authorization code (temporary or permanent) if you have not already done so.
2. Start **Firewall**.
3. Change the **iSecurity** product password.
4. Enable the **FYI Simulation Mode** on a global basis using the **System Configuration** option on the main menu.
5. Review the basic system configuration parameters and change those necessary to meet your organizational needs.
6. Enable protection and logging for all activity on all servers. Make certain that the security level is set to **1** (Allow All) for all servers.
7. After a suitable period of activity (several days or weeks), use the **Rule Wizards** to analyze the logged activity and to define security rules based upon your organizational security policies.
8. Use the **Activity Log** and the **Query Wizard** to analyze activities not covered by the Rule Wizards. Define appropriate rules based on this analysis.
9. Create User Groups and Time Groups according to your organizational requirements.
10. After a suitable period of further activity, use the **Rule Wizards**, **Activity Logs** and queries to ensure that your new rules are effectively blocking unauthorized access, while not preventing legitimate user access.

11. Disable the **FYI Simulation Mode**. From this point forward unauthorized user access will be blocked.

Starting Firewall for the First Time

In order to use this product, the user must have the ***SECOFR** special authority. To start **Firewall**, type the **STRFW** command at the command line. The main menu appears after a few moments.

An additional product password is also required to access most product features. The default product password is **QSECOFR**. We recommend that this password be changed as soon as possible, using the procedure described below.

```

GSFWPMNU                               Firewall                               iSecurity
                                                                              System:  S520

Basic Security                               Logon Control
 1. Activation and Server Setting           31. FTP/REXEC
 2. Dynamic Filtering (IP, System Names)    32. Telnet
                                           34. Passthrough

User Security                               Advanced Features and More
11. Users and Groups                       41. Rule Wizards
12. Applications                           42. Advanced Security Features
13. Locations                             43. Log, Reports, Queries
                                           45. User Management
18. Client Application Security            49. Time Groups

Object Security                             Maintenance
21. Native AS/400 Objects                  81. System Configuration
22. IFS (QDLS,NFS,QOpenSys...)             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

```

Firewall Main Menu

Modifying Operators' Authorities

The Operators authorities' management is now maintained from one place for the entire **iSecurity** on all its modules.

There are three default groups:

- ***AUD#SECAD**- All users with both ***AUDIT** and ***SECADM** special authorities. By default, this group has full access (Read and Write) to all **iSecurity** components.
- ***AUDIT** - All users with ***AUDIT** special authority. By default, this group has only Read authority to **Audit**.
- ***SECADM**- All users with ***SECADM** special authority- By default, this group has only Read authority to **Firewall**.

iSecurity related objects are secured automatically by product authorization lists (named security1P). This strengthens the internal security of the product. It is essential that **Work with**

Operators be used to define all users who have ***SECADM**, ***AUDIT** or ***AUD#SECAD** privileges, but don't have all object authority. **Work with Operators** screen has Ussr (user management) and Adm for all activities related to starting, stopping subsystems, jobs, import/export and so on. **iSecurity** automatically adds all users listed in **Work with Operators** to the appropriate product authorization list.

Users may add more operators, delete them, and give them authorities and passwords according to their own judgment. Users can even make the new operators' definitions apply to all their systems; therefore, upon import, they will work on every system.

Password = *BLANK for the default entries. Use **DSPPGM GSIPWDR** to verify.
The default for other user can be controlled as well.

If the organization wishes to have a the default to be *BLANK than they have to enter:
CRTDTAARA SMZTMPC/DFTPWD *char 10

NOTE: When installing **iSecurity** for the first time, certain user(s) might not have access according to the new authority method. Therefore, the first step you need to take after installing is to edit those authorities.

To modify operators' authorities, follow this procedure.

1. Select **82. Maintenance Menu** from the main menu. The **Maintenance Menu** appears.
2. Select **11. Work with Operators** from the **Maintenance Menu**. The **Work with Operators** screen appears.

Work with Operators												
Type options, press Enter.												
1=Select 4=Delete												
Authority level: 1=*USE, 9=*FULL												
Opt	User	System	FW	Scr	Pwd	AV	Aud	Act	Cpt	Jrn	Vw	Vsl
	*AUD#SECAD	S720	1	9	9	9	9	9	9	9	9	9
	*AUDIT	S720					9	9	9	9		9
	*SECADM	S720	9	9	9	9					9	9
	ELI	S720	9	9	9	9	9	9	9	9	9	9
	FER	S720	1	1	1	1	1	1	1	1	1	1
	FERNANDO	S720	1	1	1	1	1	1	1	1	1	1
	GS	S720	9	9	9	9	9	9	9	9	9	9
	IMA	S720	9	9	9	9	9	9	9	9	9	9
	JAVA1	S720	9	9	9	9	9	9	9	9	9	9
	NANDO	S720	9	9	9	9	9	9	9	9	9	9
More...												
FW =Firewall Pwd=Password Aud=Audit Cpt=Capture Vw =View												
Scr=Screen AV =AntiVirus Act=Action Jrn=Journal Vsl=Visualizer												
Usr=User Mgt. ADM=Admin.												
F3=Exit F6=Add new F8=Print F11=*SECADM/*AUDIT authority F12=Cancel												

Work with Operators

3. Type **1** next to the user to modify his authorities (or press **F6** to add a new user).
The **Modify Operator** screen appears.


```

                                Modify Operator

Type choices, press Enter.

Operator . . . . . QSECOFR
System . . . . . *ALL          *ALL, Name
Password . . . . . *SAME       Name, *SAME, *BLANK
Authorities by module:
Firewall . . . . . 9          1=*USE, 9=*FULL, 3=*QRY
Screen . . . . . 9          1=*USE, 9=*FULL
Password . . . . . 9          1=*USE, 9=*FULL
AntiVirus . . . . . 9        1=*USE, 9=*FULL
Audit . . . . . 9          1=*USE, 9=*FULL, 3=*QRY
Action . . . . . 9          1=*USE, 9=*FULL
Capture . . . . . 9         1=*USE, 9=*FULL
Journal . . . . . 9         1=*USE, 9=*FULL
View . . . . . 9           1=*USE, 9=*FULL
Visualizer . . . . . 9      1=*USE, 9=*FULL
User management . . . . . 9  1=*USE, 9=*FULL
Product Administrator . . . 9  1=*USE, 9=*FULL

F3=Exit   F12=Cancel
  
```

Modify Operator

Option	Description
Password	Name = Password Same = Same as previous password when edited Blank = No password
1 = *USE	Read authority only
9 = *FULL	Read and Write authority
3 = *QRY	Run Queries. For auditor use.

- Set authorities and press **Enter**. A message is prompted informing that the user being added/modified was added to the Authority list that secures the product's objects; the user carries Authority *CHANGE and will be granted Object operational authority. The Authority list is created in the installation/release upgrade process. The SECURITY_P user profile is granted Authority *ALL whilst the *PUBLIC is granted Authority *EXCLUDE. All objects in the libraries of the product (except some restricted special cases) are secured via the Authority list.

FYI Simulation Mode

The FYI Simulation Mode allows users to simulate the application of security rules without physically rejecting any activity. All "rejected" transactions are recorded in the Activity Log as such but the activity is allowed to proceed without interruption. This feature allows users to test your rules under actual working conditions without adversely affecting user access.

Users can enable the FYI Simulation Mode globally for all activity regardless of server or user. One can also enable FYI individually for specific function servers as a parameter in server security rules. In this manner, one can test security rules for specific servers without affecting rules that apply to other servers.

To enable **FYI** globally for all servers and users, perform the following steps:

1. Select **81. System Configuration** from the main menu. The **Global Parameters** screen appears.
2. Select **1** from the **Global Parameters** screen. The **General Definitions** screen appears.

```

Firewall General Definitions

Type options, press Enter.

Emergency override ALL Security setting . . . 0 0=Regular (no override)
                                                1=Allow      3=Reject
                                                2=Allow+Log  4=Reject+Log

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.

Check OS/400 Group and Supplemental profile Y Y, N

Enable Super Speed Processing . . . . . N Y, N
The functionality of the product is not affected by this setting.
Set this value to N, well before you plan a "Hot Upgrade" of the product.
This will enable temporary suspension of the activity during installation.
Hot upgrade is safe . . . . . Y (See manual)

F3=Exit F12=Previous

```

Firewall General Definitions

3. Emergency override ALL Security Setting option allow you to override all of the Firewall security settings. Type 0 for regular Firewall settings.

Option	Description
0=Regular	No override, regular Firewall security definitions. Default setting.
1=Allow	Allow all users/groups for all services. None of the exit points is locked.
2=Allow+Log	Allow all users/groups for all services and log the activities.
3=Reject	Reject all users/groups from all services. All of the exit points are locked.
4=Reject+Log	Reject all users/groups from all services and log the activities.

4. Type a 'Y' in the **Work in FYI (Simulation) Mode** field.

NOTE: You may leave the **Work in FYI (Simulation) Mode** field as '**N**', but configure certain servers to work in FYI (see *Modifying Server Security*).

5. Select '**Y**' at the **Check OS/400 Group and Supplemental profile** field to make sure both group profile and the supplemental groups' authorizations are checked. It is enough to have permission for a service in one of the groups.
6. Select '**Y**' at the **Enable Super Speed Processing** to leave programs in memory between system IPLs, which will allow fast performances.

NOTE: Before an upgrade, set **Enable Super Speed Processing** to '**N**' and perform an IPL.

7. Hot upgrade is safe: this option will allow performing an update which is performed without first terminating Firewall. When **Enable Super Speed Processing** is set to **Y**, this may leave programs in memory between system IPLs. Therefore, a Hot Upgrade should not be attempted if Hot Upgrade is Safe is set to **N**.
8. Press **Enter** twice to return to the main menu.

Enabling Protection for all Servers

In order to gather activity data for subsequent analysis, users should enable protection for all servers (if only temporarily) and enable logging of all transactions into the Activity Log. To accomplish this, perform the following steps in order:

1. Select **1. Activation and Server Setting** from the main menu and **1. Work with Servers**. The **Work with Server Security** screen appears.
2. Press **F22**. The **Global Server Security Settings** screen appears.
3. Make certain that ***ALL** appears in the **Exit point group** field.
4. Type '***YES**' in the **Secure** field.
5. Type '***YES**' in the **Log** field.
6. Press **Enter** twice to return to the main menu.
7. Make absolutely certain that the **FYI Simulation Mode** is enabled as described above.

```

Global Server Security Settings

Type choices, press Enter.

Exit point group . . . . . *ALL      *ALL, *IP, *SNA, *FILTR, *DBSRV,
                                     *PRT, *DTAQ, *CMD, *LICMT,
                                     *CNTSRV, *USRPRF, *RMTSGN

Secure . . . . . *YES      *YES, *NO
Check . . . . . *MAX      *ALLOW, *REJECT, *MAX
Filter IP/SNA . . . . . *NO      *YES, *NO
Log . . . . . *YES      *YES, *REJECTS, *NO
Allow Action to react . . . . *YES      *YES, *REJECTS, *NO
*FYI mode (server level) . . *NO      *YES, *NO
Skip "Other" exit points . . *YES      *YES, *NO
An "Other" exit point is one which an unidentified program is already assigned
to it. Such an entry is denoted by the word OTHER in the SECURE column.

A blank entry is equivalent to *SAME.

F3=Exit  F12=Cancel

```

Global Server Security Settings

NOTE: In some cases a restart of QSERVER is required for FULL implementation. This can be delayed until next IPL.

When QSERVER is restarted, NETSERVER will be restarted automatically if it was active.

Using the Rule Wizards

The unique Rule Wizards feature makes security rule definition a snap, even for non-technical system administrators. This user-friendly feature allows users to view historical activity together with the security rule currently in effect on a single screen. One can even modify the existing rule or define a new rule without closing the wizard. The Rule Wizards are an invaluable tool for defining the initial set of rules after installing **Firewall** for the first time.

Rule Wizards are available for the following types of rules:

- Servers usage
- Native OS/400 object security
- IFS Object security
- Incoming IP Address Firewalls
- Outgoing IP Address Firewalls
- User-to-Service Security

Procedural Overview

The basic procedure for working with the rule wizards is as follows:

1. Select **41** from the main menu. Several different types of rule wizards are available, but the basic procedure is the similar for all of them.

GSWZRMNU		Rule Wizards	Firewall
			System: S720
Wizards	Helps you to		
1. Servers	Check usage of servers. Recommended setting for unused servers is *REJECT. This is a query only.		
2. Incoming IP	For each IP range (for example company branch), specify permitted operations.		
21. Re-use	Restrict target where data is sent to by IP ranges defined.		
3. Outgoing IP	Specify the services which a User, Group Profile or Internal Group is permitted to use.		
31. Re-use	Specify who can use specific objects (FILES, COMMANDS, etc.) and how (Read, Write, Update, ...).		
4. Users	Specify who can use IFS Objects (folder/file*), and how (Read, Write, Update, ...)		
41. Re-use			
5. Native Objects			
51. Re-use			
6. IFS Objects			
61. Re-use			
99. Advanced Options			
Wizards summarize recent activity, compare it to current security setting, and enable creating/modifying rules. Enter new setting in R=Revised column.			
Selection or command			
===> █			
F3=Exit F4=Prompt F9=Retrieve F12=Cancel			
F13=Information Assistant F16=AS/400 main menu			

Rule Wizards main menu

2. Select a wizard from one of the **Rule Wizards** to view summarize recent activity log for that rule type.

Options 1-6 on this screen initiate IBM system commands. Enter new or updated settings in the R=Revised column.

Options **2. Incoming IP** and **3. Outgoing IP** on this screen offer a new value, ***FAST**, for the Wizard Type option. ***FAST** automatically brings up the following screen when the IBM command completes.

The Re-use options (21, 31, 41, 51, and 61) reuse the output of the IBM command initiated (by options 1-6) to save processing time.

3. Select option **99. Advanced Options**, to customize the wizards' rules

```

GSWZRMNE                                     Rule Wizards - Extended                               Firewall
                                                                                               System:  S720

Select one of the following:

Native Objects
  1. Display Log
  2. Create Working Data Set
  3. Work with Rule Wizard
  4. Update Rules

IFS Objects
  11. Display Log
  12. Create Working Data Set
  13. Work with Rule Wizard
  14. Update Rules

Incoming IP Address (Firewall)
  21. Display Log
  22. Create Working Data Set
  23. Work with Rule Wizard
  24. Update Rules

Outgoing IP Address (Firewall)
  31. Display Log
  32. Create Working Data Set
  33. Work with Rule Wizard
  34. Update Rules

User
  41. Display Log
  42. Create Working Data Set
  43. Work with Rule Wizard
  44. Update Rules

Selection or command
===> █

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

Rule Wizards - Advanced Options

4. Select **Display Log** to view summarize recent activity log for that rule type.
5. Select **Create Working Data Set** to define the scope of the historical activity data to be examined by the wizard.
6. Select **Work with Rule Wizard** to display the **Plan Security** screen for the appropriate wizard. Use this screen to compare historical activity with the security rule currently in force and to revise this rule if appropriate.
7. Select **Update Security Rules** to apply the rule changes.

The example in the following procedure is taken from the **Servers** wizard, but is applicable to the other wizards as well.

Analyzing Historical Activity

The **Rule Wizard** enables the user to review the **Activity Log** as a first step in the process of analyzing activity. The **Activity Log** allows users to view details of historical activity. This step is optional and may be performed at any time during the wizard process.

To display the **Activity Log**, follow this procedure.

1. Select option **1. Servers** from the wizards menu. The **Display User Activity** screen appears.

```

Display User Activity (DSPFWUSRA)

Type choices, press Enter.

User . . . . . > *ALL      Name, *ALL
Display last minutes . . . . . *BYTIME    Number, *BYTIME
Starting date and time:
  Starting date . . . . . *CURRENT      Date, *CURRENT, *YESTERDAY...
  Starting time . . . . . 000000      Time
Ending date and time:
  Ending date . . . . . *CURRENT      Date, *CURRENT, *YESTERDAY...
  Ending time . . . . . 235959      Time
Server ID . . . . . *ALL      *FILTER, *FTPLOG, *FTPSRV...
Output . . . . . *      *, *PRINT-*PRINT9

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

Display User Activity

- Choose the records that you wish to examine from this screen and press **Enter** to continue.

The table on the following page describes the record selection and display options

Parameter or Option	Description
User	Filter records by user profile
Display Last n Minutes	Select only the records occurring within the previous number of minutes as specified by the user Number = Enter the number of minutes *BYTIME = According the starting and ending time specified below
Starting Date & Time Ending Date & Time	Select only the records occurring within the range specified by the starting and ending date/time combination. Date or Time = Enter the appropriate date or time *CURRENT = Today (Current Date) *YESTERDAY = Previous date *WEEKSTR/*PRVWEEKS = Current week/Previous week start *MONTHSTR/ *PRVMONTH = Current month/Previous month start *YEARSTR/ *PRVYEARS = Current year/ Previous year start *SUN -*SAT = Day of week
Server ID	Filter records by server ID or display the user's activity in ALL servers
Output	* = Display *Print = Printed report *PRINT1-*PRINT9 = select print option

Defining the Working Data Set

You can select the records from the Activity Log that will comprise the working data set that is summarized on the wizard screens.

The example in the following procedure is taken from the **Incoming IP Address** wizard, but is applicable to the other wizards as well.

1. To define the working data set, select **99. Advanced Options** -> choose a wizard type to work with and select **Create Working Data Set** from the wizard menu. The **Summarize** screen appears. Samples from two of the wizards are shown below. Refer to the table on the following page for an explanation of the required parameters.

```

Summarize Incoming IP Address (CPRIIPSEC)

Type choices, press Enter.

Allowed . . . . . *ALL          *YES, *NO, *ALL
Starting date and time:
  Starting date . . . . . *CURRENT    Date, *CURRENT, *YESTERDAY...
  Starting time . . . . . 000000      Time
Ending date and time:
  Ending date . . . . . *CURRENT    Date, *CURRENT, *YESTERDAY...
  Ending time . . . . . 235959      Time
Number of records to process . . *NOMAX    Number, *NOMAX
Server ID . . . . . *ALL          *ALL, *FTP, *TELNET, *DDM...
Set to contain data:
  Set name . . . . . *TEMP        Name, *USER, *SELECT, *S...
  Replace or add records . . . *ADD      *ADD, *REPLACE
Wizard type . . . . . *FAST       *STD, *FAST, *NO

                                           Bottom
F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys
  
```

Summarize Incoming IP Address

Working with the Plan Security Wizard Screens

The example described in this section refers to the outgoing IP address firewall activity type. The same principles apply to the other rule wizards.

The **Plan Incoming IP Security** screen displays activity statistics for the current working set together with currently defined rule settings (Column “**C**”) and a place to enter revised rule settings (Column “**R**”). Enter revised rule setting as desired and press **Enter** to continue.

Plan Incoming IP Security

Type choices, press Enter.
 Opt: 4=Delete 5=DSPFWLOG
 9=Create Security
 Specify revised authority in the R column.
 Press Enter to apply revised authority.

C>R=Current to Revised
 Y Allowed Y=Allow
 N Rejected N=Reject
 Y Allowed (by generic* rule)
 N Rejected (by generic* rule)

Opt	IP-Address	RE- EXEC C>R	Tel- net C>R	DB Srv C>R	TCP SGN C>R	RMT Srv C>R	DDM C>R	Number of Logged Entries FTP/REXEC Telnet --DB-- -TCP--SGN-- -RMT-- --DDM--
█	1.1.1.148	Y	Y	Y	Y	Y	Y	1
-	1.1.1.149	N	N	N	N	N	N	2
-	1.1.1.151	Y	Y	N	N	N	N	6
-	1.1.1.155	Y	Y	N	N	N	N	39 2
-	1.1.1.177	Y	Y	Y	Y	Y	Y	2 9
-	1.1.1.183	Y	Y	N	Y	Y	Y	3
-	1.1.1.196	Y	Y	N	Y	Y	N	2
-	81.191.64.89	N	Y	Y	Y	N	Y	33
-	192.168.1.1	N	N	N	N	N	N	1
-	192.168.1.3	Y	Y	Y	Y	Y	Y	2

More...

F3=Exit F6=Add New F8=Print F11=Alt.view F12=Cancel

Plan Incoming IP Security

Each line in this screen represents activity for a single IP address. The quantities represent the number of actual transactions for each activity type for this IP address. Press **F11** to display the statistics for the bottom row of activity types (NDB, RMT, REXEC and WSG).

The "C" column shows the rule currently in effect for activity type on a line. A 'Y' indicates that transactions will be allowed and a 'N' indicates that transactions will be rejected. The background color of each letter indicates whether the rule currently in effect is **specific** to this line (IP Address) or is "**generic**", meaning that the current rule applies to more than one line.

For example, the rules for the first line (1.1.1.53) are relevant **for this IP address only**. The second line (1.1.1.55) is covered by a "generic" rule that applies to several IP addresses. This generic rule could be a default rule that covers all IP addresses that are not covered by a specific rule or it could be single rule that covers multiple IP addresses via the use of the subnet mask.

Background Color	Rule Source
Green (Black at the white display) or Red	Specific rule
Cyan (Blue at the white display) or Pink	"Generic" rule

Use the "R" column to modify the rule in effect for that line. If the line is covered by a generic rule, an entry in the "R" column has the effect of creating a new rule specific to that line.

Option	Description
'C' Columns	Display the rule currently in effect for each activity type (column). Refer to the previous page for a more detailed explanation. 'Y' = allowed. 'N' = rejected.
'R' Columns	Type 'Y' (Allow) or 'N' (Reject) to modify the rule currently in effect for each activity type. Refer to the previous page for a more detailed explanation.
Opt	4 = Delete this rule 5 = Display the detailed Activity Log for this rule 9 = Create a new rule based on an existing one
F6	Create a new rule covering activity NOT shown on any line. For example, use F6 to create a new rule for an IP address that does not appear on this screen.
F8	Print all activity and rules shown in this wizard
F11	Displays additional data for each line with fewer lines per screen

Native OS/400 Objects Log

Options 4, 5 and 6 on **Firewall** Option 41 screen have a "Group by" parameter for summarizing log output data.

Value ***GRPPRF** summarizes by system group profiles plus all users not defined in group profiles.

Value ***USRGRP** summarizes by user groups and value ***GROUP** first causes the product to attempt to associate the user with a relevant user group and then to attempt to associate the user with a relevant group profile.

If both fail, the user profile name appears in the report.

1. To see the Summarize Native AS/400 Log, select option **1. Create Working Data Set** from the **Native OS/400 Object Security** menu.
2. The **Summarize Native AS/400 Log (CPRNTVSEC)** screen appears

Summarize Native AS/400 Log (CPRNTVSEC)

Type choices, press Enter.

Object	<u>*ALL</u>	Name, generic*, *ALL
Library	<u>*ALL</u>	Name, generic*, *ALL
Object Type	<u>*ALL</u>	*ALL, *FILE, *LIB, *DTAQ...
User	<u>*ALL</u>	Name, *ALL
Group by	<u>*GROUP</u>	*USER, *GRPPRF, *USRGRP...
Allowed	<u>*ALL</u>	*YES, *NO, *ALL
Starting date and time:		
Starting date	<u>*CURRENT</u>	Date, *CURRENT, *YESTERDAY...
Starting time	<u>000000</u>	Time
Ending date and time:		
Ending date	<u>*CURRENT</u>	Date, *CURRENT, *YESTERDAY...
Ending time	<u>235959</u>	Time
Number of records to process . .	<u>*NOMAX</u>	Number, *NOMAX
Server ID	<u>*ALL</u>	*ALL, *FILTER, *RMTSRV...

Bottom

F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

Summarize Native AS/400 Log

Option	Description
Object/Library	Object name and library path (Native object and User wizards only) Generic* = All objects/libraries beginning with the text string preceding the * *ALL = All objects/Libraries
Object Type	Object type (Native object and User wizards only) Press F4 to select the object type from a list
User	Enter a user profile or press F4 to select from a list (not on all wizards)
Group by	Select a group from a list Value *GRPPRF summarizes by system group profiles plus all users not defined in group profiles. Value *USRGRP summarizes by user groups and value *GROUP first causes the product to attempt to associate the user with a relevant user group and then to attempt to associate the user with a relevant group profile. If both fail, the user profile name appears in the report.
Allowed	*YES = Include allowed transactions only *NO = Include rejected transactions only *ALL = Include all transactions
Starting date & time Ending date & time	Selects only the events occurring within the range specified by the start and end date/time combination Date and time = Enter the date and time or one of the following constants: *CURRENT = Current day *YESTERDAY = Previous day *WEEKSTR/*PRVWEEKS = Current week/Previous week start *MONTHSTR/ *PRVMONTH = Current month/Previous month start *YEARSTR/ *PRVYEARS = Current year/ Previous year start *SUN -*SAT = Day of week
Server ID	Press F4 to select a server ID from a list window or type *ALL to include activity for all servers.
Set name	Enter a name for this data set or use one of the following constants: *USER = Use your user profile as the data set name *SELECT or *S = Select a data set from the pop-up list
Replace or add records	*ADD = Add records to an existing data set of one exists. *REPLACE = Replace an existing data set of the same name
Wizard type	*FAST (default) = which allows to initiate a rule wizard immediately by pressing Enter. *STD (standard) *NO

2. Enter the required parameters and press **Enter** to begin the selection process and return to the **Wizard** menu.

```

Plan Security for Native Objects

Type choices, press Enter.
  Opt: 4=Delete  5=DSPFWLOG          C>R=Current to Revised
        7=WRKOBJ  8=EDTOBJAUT  9=Create Security  Y=Allow  Y=Allow
Specify revised authority in the R column.  N=Rejected  N=Reject
Press Enter to apply revised authority.  Y=Allowed (from higher level)
                                          N=Rejected (from higher level)

  Rd  Wrt  Crt  Dlt  Rnm  Otr
Opt C>R C>R C>R C>R C>R C>R Type Object Library *User Entries
  V  -  -  -  -  -  -  CMD ADDLIB QSYS GLIORA 1
  N  -  -  -  -  -  -  CMD CALL QSYS CATEST 53
  N  -  -  -  -  -  -  CMD CALL QSYS INNA 19
  N  -  -  -  -  -  -  CMD CALL QSYS QSECOFR 5695
  N  -  -  -  -  -  -  CMD CHGAUT QSYS GILANITK 19
  N  -  -  -  -  -  -  CMD CHGAUT QSYS GLIORA 8
  N  -  -  -  -  -  -  CMD CHGAUT QSYS GHASSAB 2
  N  -  -  -  -  -  -  CMD CHGAUT QSYS GSHARONA 1
  N  -  -  -  -  -  -  CMD CHGAUT QSYS GYAFIT 1
                                          More...

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

Plan Security for Native Objects

Update Rules

The final step is to apply the new and revised security rules that were created via the wizards.

1. To update rules, select **Update Security Rules** from the wizard menu. The **Update** screen appears. Samples from two of the wizards are shown below. Refer to the table on the following page for an explanation of the required parameters.

```

Native AS/400 Objects Update (UPDNTVSEC)

Type choices, press Enter.

Set name . . . . . > *USER          Name, *USER, *SELECT, *S...
Object . . . . .                      Name
Library . . . . .                      Name
Object Type . . . . . *ALL           *ALL, *FILE, *CMD, *PGM...
User . . . . . *ALL                 Name, *ALL
Delete set after processing . . *YES  *YES, *NO

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

Native AS/400 Objects Update

2. Enter the required parameters and press **Enter** to begin the selection process and return to the **Wizard** menu.

User Groups

User groups allow you to apply security rules to predefined groups of users. User groups are also useful as filter criteria for queries and reports. The use of user groups greatly reduces the number of rules required to implement security policies as well as the time spent defining and maintaining rules.

Also note that User Groups are defined in **Firewall Option 11** and **Group Profiles** are defined in the system.

The benefit of this new feature is that instead of the report containing thousands of lines of user data, user groups, group profiles, and user profiles are listed.

Firewall supports the use of two types of user groups:

- OS/400 group profiles
- Firewall proprietary user groups

OS/400 Group Profiles

OS/400 group profiles are useful for a variety of System i administration and security tasks. Use the **CRTUSRPRF** or **WRKUSRPRF** commands to create OS/400 group profiles. To assign other user profiles to the group profile, simply enter the group profile name in the **Group Profile** field for each individual user profile that is a member of a group.

Firewall Proprietary User Groups

Overview

Firewall proprietary user groups offer greater flexibility when it comes to grouping users together for the purpose of minimizing security rules and query filtering. Since OS/400 group profiles are used for many other administrative tasks, they may not be as efficient for grouping users together for security purposes.

Firewall proprietary user groups are always identified by the '%' symbol as the first character (e.g. %SALES). These user groups are defined within **Firewall**, and they may include both individual user profiles and OS/400 group profiles.

The following section describes the procedures for defining **Firewall** user groups.

Defining User Groups

1. To work with **Firewall** proprietary user groups, select **11. Users and Groups** from the main menu. The **Work with User Security** screen appears.

```

Work with User Security
Subset . . . .
Type options, press Enter. (Read top->down) Servers securing
1=Select 3=Copy 4=Delete 5=Members 6=Groups User Level only
-----Network Servers-----
F F F F R R R F O O C C C N N M S O T
I T T T E R M M I R R S S P P S Q B C
L P P P X E T T L D D V L L D C C R R G L J P
T L S C L X S S N S S T T P I I D R N L E S S E I S
F O R L O E Q Q D R R A A R C C D D V N N P R N N G
R G V N G C L L B V V Q Q T M M M A M M T L V T F N
User
System Group
Opt %group Members
+-----+-----+-----+
+ *PUBLIC 9 +-----+-----+-----+
+ %AABBCC 8 +-----+-----+-----+
+ %AAVVV 8 +-----+-----+-----+
+ %AA7 8 +-----+-----+-----+
+ %ADMIN 8 +-----+-----+-----+
+ %DEMO 1 +-----+-----+-----+
+ %EVG 3 +-----+-----+-----+
+ %EVV 361 +-----+-----+-----+
+ %FWGRP +-----+-----+-----+
More...

F3=Exit F6=Add user F7=Add group F8=Print list

```

Work with User Security

Option	Description
Opt	<p>1 = Modify user profile or group. The Modify User Security screen appears.</p> <p>3 = Copy user profile or group definitions</p> <p>4 = Delete user profile or group</p> <p>5 = Edit the group's members</p>
Servers	<p>Displays the rule status for each server type:</p> <p>+ = User-to-service rule overrides the global server security rule. Allow a user the access to a server and check for object authorizations.</p> <p>V = User-to-service rule overrides with verb (command) support</p> <p>Blank = Global server security rule governs activity for this server</p> <p>S = Allow a user to access a server and skip the check for object authorizations. This simplifies the test for some users (normally for batch applications, which are playing the role of servers and the desire to save performance in such cases).</p>
F6	Add a new user. The Add User Security screen appears.
F7	Add a new group. The Add User Group Security screen appears.
F8	Print user group definitions
F3	Return to the main menu

1. To work with an existing rule, type **1** in the **Opt** field or press **F6** to create a new rule. Use the **PageUp** and **PageDown** keys to scroll through the list. Press **Enter** to continue.
2. Enter parameters on the **Add/Modify Parameters** screen and press **Enter** to confirm.

```

Modify User Security

User . . . . . *PUBLIC

Type choices, press Enter.
Activity Time . . . . . _____ Time group, *NEVER
Use Group Authority . . . . . Y=Yes, N=No, blank=Default
Enable Services based also on OS/400 and %USER Group profiles

Authorities and Locations

2. Services FTP, SQL, NDB, DDM, ...
3. IP
4. Device Names SIGNON only
Selection ==> █

In-product Special Object Authority
AS/400 Native. . . . . 3 1=*ALLOBJ, 2=*EXCLUDE, 3=*OBJAUT
IFS . . . . . 3 1=*ALLOBJ, 2=*EXCLUDE, 3=*OBJAUT

F3=Exit F4=Prompt F8=Print
F9=Object security F10=Logon security F12=Cancel

```

Modify User Security

Parameter or Option	Description
User	Displays the user profile or user group name
Activity Time	Time Group = type a time group name or press F4 to select from a list. *NEVER =
Use Group Authorities	Y = use a specific group authorities N = don't use any specific group authorities
Authorities and Locations	2. Services = specify authorities and location by Services name 3. IP = specify authorities and location by IP name 4. Device Names = specify authorities and location by Device name
In-product Special Object Authority	Use this field to define object authority for the user/group for AS/400 Native and IFS objects.
F8	Print user-to-service security rules
F9	Work with object security rules
F10	Work with Logon security rules

Add User profiles to a Group

The Create/Modify screen allows you to define the users belonging to the group. A user group may contain individual user profiles or OS/400 group profiles.

- ```

Modify Group of Users

Type choices, press Enter.

User Group . . %ADMIN
Text

User Text
AV Programmer of Anti Virus
QUSER Work Station User

More...

F3=Exit F4=User list F8=Print F12=Cancel

```

2. Press **Enter** to accept the profiles and return to the **Work with User Security** screen.

**NOTE:** A user can be in several **Firewall** user groups simultaneously.

## Overview

For example, one may be using a number of different queries and reports to audit the activities of certain employees during normal working hours and a different group of employees during nights and weekends. This can be accomplished with just one time group using the following guidelines:

1. Create a time group that defines normal working hours for each day of the week.
2. Use an inclusive time group filter (activities occurring during the time group periods) for each query or report covering activity during normal working hours.



3. Use an exclusive time group filter (activities **not** occurring during the time group periods) for each query or report covering activity outside of normal working hours.

## Using Time Groups as Filter Criteria

One common use of time groups is as filter criteria in security rules, queries and reports. For example, time groups can be used to restrict application of a rule to specific times and days of the week.

Time group filters can be either:

- **Inclusive** – Including all activities occurring during the time group periods
- **Exclusive** – Including all activities **not** occurring during the time group periods

Generally, an exclusive time group filter is indicated by placing an 'N' (NOT) in the field immediately preceding the time group name field on the rule definition or query definition screen.

For example, one can use an exclusive time group filter to apply a rule to any time occurring outside of days and hours specified in the time group.

## Defining and/or Modifying Time Groups

Perform these steps to define a time group.

1. Select **49. Time Groups** from the main menu. The **Define Time Groups** screen appears.

Define Time Groups

Type options, press Enter.  
1=Select    4=Delete

| Opt Time Group                            | Description                  |
|-------------------------------------------|------------------------------|
| <input checked="" type="checkbox"/> NIGTH | Night Shift time group       |
| <input type="checkbox"/> SUMMER           | The Work Hours During Summer |
| <input type="checkbox"/> WINTER           | Work Hours During Winter     |

Bottom

F3=Exit
F6=Add new
F8=Print list
F12=Cancel

### Define Time Groups

2. Select a time group to modify or press **F6** to add a new group.
3. Press **Enter** to accept the definition and return to the **Define Time Groups** screen.



| Option             | Description                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>         | <b>1</b> = Modify an application group.<br><b>3</b> = Copy an existing application group<br><b>4</b> = Delete an application group<br><b>5</b> = Edit the group members (OS400 Users and Group profiles) |
| <b>Application</b> | Name of application group                                                                                                                                                                                |
| <b>F3</b>          | Return to the main menu                                                                                                                                                                                  |
| <b>F6</b>          | Add a new application group.                                                                                                                                                                             |
| <b>F8</b>          | Print application group definitions                                                                                                                                                                      |

2. Select **1** to modify a group or press **F6** to create a new group (as shown below).

```

Add Application Group Security

Type choices, press Enter.

Application Group . . . █ %#name
Text

Authorities
 1. Services FTP, SQL, NDB, DDM, ...

Selection ==>

In-product Special Object Authority
AS/400 Native. 3 1=*ALLOBJ, 2=*EXCLUDE, 3=*OBJAUT
IFS 3 1=*ALLOBJ, 2=*EXCLUDE, 3=*OBJAUT

F3=Exit F4=Prompt F8=Print
F9=Object security F10=Logon security F12=Cancel

```

### Add Application Group Security

| Option                                     | Description                                                                                                                                                                                                                                                                                 |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Application Group</b>                   | Application group name                                                                                                                                                                                                                                                                      |
| <b>Text</b>                                | Enter a description of the application group                                                                                                                                                                                                                                                |
| <b>Authorities</b>                         | <b>Services</b> = choose server<br><b>Selections</b> = Enter your choice of service                                                                                                                                                                                                         |
| <b>In-product Special Object Authority</b> | This feature defines the level of authority for both native and IFS objects.<br><b>*OBJAUT</b> = Object authority is subject to object security rules<br><b>*EXCLUDE</b> = All object authority is denied for this user<br><b>*ALLOBJ</b> = Users are granted <b>*ALLOBJ</b> for IFS object |
| <b>F3</b>                                  | Return to the main menu                                                                                                                                                                                                                                                                     |

3. Press **Enter** to accept the definition.

## Location Groups

### Overview

Location Groups are collections of users whose access to certain location is defined by IP and device name(s). For example, create a Chicago group in which all users have access to the System i only from the Chicago branch IP range. The location group, which even supports each Telnet sign-on, may be used only from OS V4R5 and fully complies on all the servers from OS V5R1.

You can define object level rules in location groups as well.

Perform the following steps to define and/or modify location groups

### Defining and/or Modifying Location Groups

1. Select **13. Locations** from the main menu. The **Work with Location Groups** screen appears as below.

```

Headquarters Work with Location Groups

Type options, press Enter.
 1=Select 3=Copy 4=Delete 5=Members

Opt Location
 -- -----
 1 %@CHICAGO Chicago Office
 2 %@NEWYRK New York Office
 3 %@HEADQ Headquarters

F3=Exit F6=Add new F8=Print list

Bottom

```

### Work with Location Groups

| Option          | Description                                                                                                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>      | <b>1</b> = Modify a location group.<br><b>3</b> = Copy an existing location group<br><b>4</b> = Delete a location group<br><b>5</b> = Edit the group members (OS400 Users and Group profiles) |
| <b>Location</b> | Location name                                                                                                                                                                                 |
| <b>F3</b>       | Return to the main menu                                                                                                                                                                       |
| <b>F6</b>       | Add a new location group.                                                                                                                                                                     |
| <b>F8</b>       | Print location group definitions                                                                                                                                                              |

Up to two separate time periods can be defined per day. Please note that if the "To" time is earlier than the "From" time, it will be considered to roll over to the following day. This is illustrated in the following screenshot.

```

Modify Location Group Security

Type choices, press Enter.
Location Group %CHICAGO %@name
Text Chicago Office

Activity Time WINTER Time group, *NEVER

Locations
 1. IP
 2. Device Names SIGNON only

Selection ==> L

F3=Exit F4=Prompt F8=Print
F9=Object security F10=Logon security F12=Cancel

```

### Modify Location Group Security

| Parameter or Option   | Description                                                                                                                                                                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Location Group</b> | Name of location group                                                                                                                                                                                                                                   |
| <b>Text</b>           | Enter descriptive text                                                                                                                                                                                                                                   |
| <b>Activity Time</b>  | <b>Time Group</b> = Select a time group<br><b>*NEVER</b> = If this option is selected, members of this group are disabled and cannot log in                                                                                                              |
| <b>Locations</b>      | <b>IP</b> = The IPs that are allowed to be accessed by this Location group<br><b>Device names</b> = Device names which are allowed to be accessed to telnet sign-on<br><b>Selection</b> = Enter which of the above are being defined (IP or device name) |



## Chapter 3: Basic Security

Server security is the topmost level, and most basic level of security provided by **Firewall**. Server security rules determine how each server is to be protected and what level of access control is desired. Rules include the following parameters:

- Enabling or disabling protection for each server
- Specifying the level of access control (allow all activity, reject all activity or allow activity subject to more specific rules regarding users, objects, or logon parameters)
- Determining which transactions are to be recorded in the Activity Log
- Determining whether or not **Action** can respond automatically to specific events by sending messages to key personnel or running proactive command scripts to prevent security breaches
- Allowing custom user exit programs to perform specific actions
- Whether the FYI simulation mode is active for each server

**Firewall** server security rules control access to the servers on a global basis for all users. You can also define **User-to-Service** security rules to control access to the servers for specific users or groups of users. User-to-Service security rules are discussed in *Chapter 5: User-to-Service Security*.

### About Servers & Exit Points

**Exit Points** are components of the OS/400 API that manage the interface with various system resources. These **Exit Points** govern the interface between the System i and various external access protocols and methodologies, such as FTP, Telnet, ODBC database access, DRDA database access, etc.

OS/400 employs a variety of logical **Servers** (sometimes referred to as **Function Servers**) that control activity between applications and the exit points. Each server controls one or more specific exit points.

**Exit Programs** are scripts or programs that run automatically whenever activity occurs via a particular exit point. Customized exit programs can provide additional security or functionality for specific types of activity.



## Working with Server Security Rules

**Firewall** uses only one security rule for each server. Working with server security consists of modifying these rules. By default, protection is disabled for all servers and all activity is allowed.

To work with server security rules:

1. Select **1. Activation and Server Setting** from the main menu. Select option **1. Work with Servers**, the **Work with Server Security** screen appears.

The **Work with Server Security** screen lists the current rules for each server. The number of servers available is dependent on the version of OS/400 installed on the system. This screen displays the current status of each server security rule. One can select one or more rules for modification. The user can also view an explanation and display the Activity Log for each server directly from this screen.

2. Set rules according to the following table. To modify a rule, select **1**.
3. Press **Enter** to confirm and return to the **Work with Server Security** screen.

```

Global *FYI* Mode Active Work with Server Security

Type options, press Enter.
 1=Select 5=About Server 6=Display FW Log

 User
 Exit
 Pgm

Opt Secure Level Log FYI Server
█ No Original File Transfer Function FILTFR
- No FTP Server Logon (*) FTPLOG
- No FTP Server-Incoming Rqst Validation (*) FTSPSRV
- No FTP Client-Outgoing Rqst Validation (*) FTPCLN
- No TFTP Server Request Validation TFTP
- No REXEC Server Logon REXLOG
- No REXEC Server Request Validation REXEC
- No Original Remote SQL Server RMTSQL
- No Database Server - SQL access & Showcase SQL
- No Database Server - data base access NDB
- More...

(*) Changing the "Secure" parameter requires restarting Host Server or IPL
Modify data, or press Enter to confirm.
F3=Exit F8=Print F9=Object security F10=Logon security
F11=User security F12=Cancel F22=Global setting F23=FYI F24=Emergency

```

### Work with Server Security

**NOTE:** In some cases a restart of QSERVER is required for FULL implementation. This can be delayed until next IPL.

When QSERVER is restarted, NETSERVER will be restarted automatically if it was active.

| Option                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>                | <b>1</b> = Select a rule for modification. The <b>Modify Server Security</b> screen appears<br><b>5</b> = View a description of the server<br><b>6</b> = View the Activity Log for the server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Secure</b>             | <b>*YES</b> = Secured <b>*NO</b> = Not secured                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Level</b>              | This option is not available for exit points that deal with specific operations (such as Change User Profile and Pre-Power Down System)<br><b>1</b> = Allow all activity (available for all other exit points)<br><b>2</b> = Reject all activity (available for all other exit points)<br><b>3</b> = Allow activity subject to User-to-Service security rules (not available for exit points that are supported until the Logon level i.e. Telnet and Remote Sign-on)<br><b>9</b> = Full security – differs in <b>logon</b> and <b>user-to-object</b> .<br><b>Logon</b> activates the logon limitation rules (user to system name, IP and user name).<br><b>User-to-object</b> activates your user limitation rules. |
| <b>Log FYI FW, Action</b> | Shows if FYI mode is currently being logged for <b>Firewall</b> and <b>Action</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Server</b>             | Name/description of server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>User Exit Pgm</b>      | Name of custom user exit program for this server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>F8</b>                 | Print all server security rules                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>F9</b>                 | Work with object security rules                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>F10</b>                | Work with logon security rules                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>F11</b>                | Work with user-to-service security rules                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>F22</b>                | Define server security rules globally for predefined groups of servers <b>or</b> for all servers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>F23</b>                | Enable or disable the FYI simulation mode globally for all servers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>F24</b>                | Use the Emergency Override feature                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

```

Global *FYI* Mode Active Modify Server Security

Type choices, press Enter.

Server FILTER Original File Transfer Function
Secure 1 1=Yes, 2=No
Security level 9 1=Allow All
 2=Reject All
 3=User to Service
 9=Full (User+Object)

Information to log 4 1=None
 2=Rejects only
 4=All
Allow Action to react 3 1=No, 2=Rejects only, 3=All
Run Server-Specific User Exit Program. 1 1=Yes, 2=No, blank=Default
See example in SMZ8/GRSOURCE FWAUT#A.
Run in FYI Simulation mode 1=Yes, blank=Default

F3=Exit F9=Object security
F10=Logon Security F11=User security F12=Cancel

```

### Modify Server Security

| Parameter or Option                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Server</b>                                | Server name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Secure</b>                                | *YES = Secured<br>*NO = Not secured                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Security Level</b>                        | This option is not available for exit points that deal with specific operations (such as Change User Profile and Pre-Power Down System)<br>1 = Allow all activity (available for all other exit points)<br>2 = Reject all activity (available for all other exit points)<br>3 = Allow activity subject to User-to-Service security rules (not available for exit points that are supported until the Logon level i.e. Telnet and Remote Sign-on)<br>9 = Full security – differs in <b>logon</b> and <b>user-to-object</b> .<br><b>Logon</b> activates the logon limitation rules (user to system name, IP and user name).<br><b>User-to-object</b> activates your user limitation rules.                                                                               |
| <b>Information to Log</b>                    | 1 = Do not log any activity<br>2 = Log rejected transactions only<br>4 = Log all activity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Allow Action to React</b>                 | 1 =No (disables the <b>Firewall</b> real-time detection rules for this server)<br>2 = Rejects only (will activate <b>Firewall</b> real-time detection rules only on rejections from this server)<br>3 = All (will activate <b>Firewall</b> real-time detection rules for all accesses from this server)                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Run Server-Specific User Exit Program</b> | <b>Yes</b> =Run a specific exit program after passing <b>Firewall</b> rules for this server. The program <b>SMZTMPA/UPyyyyyy</b> will be called. (yyyyyy is the server short name). Write your own <b>SMZTMPA/UPyyyyyy</b> program according to the example in <b>SMZ8/GRSOURCE FWAUT#A</b> .<br><br>The program that initiates the call is <b>GRCLUER</b> . This program runs in USER authority and therefore the user (i.e. every user in the system) will have the authority to run the program <b>SMZTMPA/UPyyyyyy</b><br><br>If the program <b>SMZTMPA/UPyyyyyy</b> is not accessible, the regular security applies.<br><br><b>No</b> = If there is a general exit program configured, it will not be activated for this server.<br><b>Blank</b> = global setting |
| <b>Run in FYI Simulation Mode</b>            | 1 = Enable FYI Simulation mode for this server only<br><b>Blank</b> = Use global parameter for all servers (System Configuration)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Using the Global Server Security Settings Feature

The global server security settings feature is a real time-saver that allows users to modify server security rules quickly for all servers or for predefined server groups. Server groups include several related servers, enabling definition of rules for all on a single screen. The following table describes the members of the server groups.

| Server Group  | Description                                                                                                                                                                                                                                                                                           | Server Group   | Description                                                                                                                                     |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>*IP</b>    | FTP Server Logon<br>FTP Server-Incoming Rqst Validation<br>FTP Client-Outgoing Rqst Validation                                                                                                                                                                                                        | <b>*CMD</b>    | REXEC Server Request Validation<br>Remote Command/Program Call                                                                                  |
| <b>*SNA</b>   | DDM request access<br>DRDA Distributed Relational DB access<br>Remote sign-on (Passthrough)                                                                                                                                                                                                           | <b>*LICMGT</b> | Original License Mgmt Server<br>Central Server - license mgmt                                                                                   |
| <b>*FILTR</b> | Original File Transfer Function<br>FTP Server Logon (*)<br>FTP Server-Incoming Rqst Validation<br>FTP Client-Outgoing Rqst Validation<br>TFTP Server Request Validation<br>Original Remote SQL Server<br>Database Server - SQL access & Showcase<br>Database Server - data base access<br>File Server | <b>*CNTSRV</b> | Central Server - license mgmt<br>Central Server - conversion map<br>Central Server - client mgmt                                                |
| <b>*DBSRV</b> | Database Server – entry<br>Database Server - object information                                                                                                                                                                                                                                       | <b>*USRPRF</b> | Change User Profile<br>Create User Profile<br>Delete User Profile - after delete<br>Delete User Profile - before delete<br>Restore User Profile |
| <b>*PRT</b>   | Network Print Server - entry<br>Network Print Server - spool file<br>Database Server – entry<br>Database Server - object information                                                                                                                                                                  | <b>*RMTSGN</b> | Remote sign-on (Passthrough)                                                                                                                    |
| <b>*DTAQ</b>  | Original Data Queue Server<br>Data Queue Server                                                                                                                                                                                                                                                       |                |                                                                                                                                                 |

To work with server security rules globally:

1. Select **F22=Global setting** from the **Work with Server Security** screen. The **Global Server Security Settings** screen appears.
2. Press **Enter** to accept.

```

Global Server Security Settings

Type choices, press Enter.

Exit point group *ALL *ALL, *IP, *SNA, *FILTR, *DBSRV,
 *PRT, *DTAQ, *CMD, *LICMT,
 *CNTSRV, *USRPRF, *RMTSGN

Secure *YES *YES, *NO
Check *MAX *ALLOW, *REJECT, *MAX
Filter IP/SNA *NO *YES, *NO
Log *YES *YES, *REJECTS, *NO
Allow Action to react *YES, *REJECTS, *NO

Skip "Other" exit points . . *YES *YES, *NO
An "Other" exit point is one which an unidentified program is already assigned
to it. Such an entry is denoted by the word OTHER in the SECURED column.

A blank entry is equivalent to *SAME.

F3=Exit F12=Cancel

```

### Global Server Security Settings

| Parameter or Option             | Description                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Exit point group</b>         | Enter an exit point group from the list to the right                                                                                                                                                                                                                                                                                                                                  |
| <b>Secure</b>                   | *YES = Secured<br>*NO = Not secured                                                                                                                                                                                                                                                                                                                                                   |
| <b>Check</b>                    | *ALLOW = Allow all activity<br>*REJECT = Reject all activity<br>*MAX = Full security – allow activity subject to user-to-service, object and login security rules as appropriate                                                                                                                                                                                                      |
| <b>Filter IP/SNA</b>            | *YES = Secured<br>*NO = Not secured                                                                                                                                                                                                                                                                                                                                                   |
| <b>Log</b>                      | *YES = Log all activity<br>*REJECTS = Log rejected transactions only<br>*NO = Do not log any activity                                                                                                                                                                                                                                                                                 |
| <b>Allow Action to React</b>    | Allow <b>Action</b> to respond automatically to specific events by sending messages to key personnel or running proactive command scripts to prevent security breaches.<br>*YES = Allow <b>Action</b> to respond for this server only<br>*REJECTS = Allow <b>Action</b> to respond for rejected transactions only<br>*NO = Do not allow <b>Action</b> to respond for this server only |
| <b>Skip "other" exit points</b> | An “Other” exit point is one to which an unidentified program is already assigned. Such an entry is denoted by the word <b>OTHER</b> in the <b>SECURED</b> column.<br>*YES = skip<br>*NO = Do not skip<br><br><b>NOTE:</b> <i>iSecurity Firewall and other Network Security products can work in parallel. For more information please contact Support.</i>                           |

## FYI Simulation Mode – Global Setting

The FYI Simulation Mode may be enabled or disabled globally for all activity or enabled for individual function servers. In this manner, users can test security rules for specific servers without affecting rules that apply to other servers. In addition, administrators can selectively activate FYI mode for individual function servers.

To change the global setting for the FYI Simulation Mode:

1. Press **F23** from the **Work with Server Security** screen. The **Firewall \*FYI\* Parameter** pop-up window appears.
2. Type 'Y' to enable FYI globally or type 'N' to disable FYI. Press **Enter** to continue.

```

Work with Server Security
.....
T : Firewall *FYI* Simulation Mode :
: :
: Type options, press Enter. : er
: : it
Op: Work in *FYI* simulation mode Y Y, N : ■
: : Y
: :
: While in this mode, Firewall simulates the application of rules :
: without rejecting transactions. Activity is recorded in the log :
: with the *FYI* designation. :
: *FYI* is an acronym of "For Your Information". :
: :
: F3=Exit F12=Cancel :
: :
: :
: :
: :
: :
: :
More...
(*) Changing the "Secure" parameter requires restarting Host Server or IPL
Modify data, or press Enter to confirm.
F3=Exit F8=Print F9=Object security F10=Logon security
F11=User security F12=Cancel F22=Global setting F23=*FYI F24=Emergency

```

## Work with Server Security: Firewall FYI\* Parameter

## Using the Emergency Override Feature

The Emergency Override feature allows users to override all existing security rules temporarily by allowing or rejecting all activity. This feature is useful in order to respond quickly to emergencies such as critical transactions being rejected due to problems with **Firewall** security rules or a sudden security breach.

To work with emergency override, follow the following procedure:

1. Press **F24** from the **Work with Server Security** window. The **Firewall Emergency Parameter** pop-up window appears.
2. Type a setting according to the below table.
3. Press **Enter** to confirm and return to the **Work with Server Security** window.



```

Global *FYI* Mode Active Work with Server Security
.....
T : Firewall Emergency Override
:
: Type options, press Enter.
:
Op : Emergency override ALL Security setting . . 0 0=No change
: Use this option for short periods only. 1=Allow
: Use Allow+Log to eliminate business impact 2=Allow+Log
: while you are resetting the rules. 3=Reject
: Use Reject+Log to react & trace an intrusion. 4=Reject+Log
:
: F3=Exit F12=Cancel
:
:
:
:
: Yes Full Y Y Y Database Server - data base access NDB
: More...
(*) Changing the "Secure" parameter requires restarting Host Server or IPL
Modify data, or press Enter to confirm.
F3=Exit F8=Print F9=Object security F10=Logon security
F11=User security F12=Cancel F22=Global setting F23=FYI F24=Emergency

```

### Work with Server Security: Firewall Emergency Parameter

| Parameter or Option | Description                                                                                                                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Setting</b>      | <b>0</b> = Disable emergence override – all rules function normally<br><b>1</b> = Allow all activity<br><b>2</b> = Allow and log all activity<br><b>3</b> = Reject all activity<br><b>4</b> = Reject and log all activity |

## Chapter 4: Dynamic Filtering Security

**Firewall** rules control activity originating from or outbound to specific IP addresses. Inbound activity from specific SNA system names may likewise be controlled.

**Firewall** also supports SSL restrictions on access to FTP, Telnet, Data Base Server (including ODBC), Sign-on, Remote Access and DDM servers.

### IP Address Firewall Rules

IP address firewall rules can apply to outbound and inbound activity. The definition procedure and data screens are the same for both activity types.

Rules control activity for individual IP addresses or ranges of IP addresses using standard subnet mask notation. For each address or range of addresses, one can choose to allow or reject activity for any of the following servers:

- FTP/REXEC (includes: FTPLOG, REXLOG)
- Telnet
- Internet WSG
- DB Server (includes: SQLENT, SQL, NDB, OBJINF)
- TCP Sign-on Server
- Remote Command/Program Call (RMTSRV)
- DDM (includes: DDM, DRDA)

To create or modify IP address firewall rules,

1. Select **2** from the main menu. The **Work with Dynamic Filtering** menu appears.
2. Select **1. Incoming IP Addresses** from the **Work with Dynamic Filtering** menu. To work with Outgoing activity, select **2** from the **Work with Dynamic Filtering** menu. In either case, the **Dynamic Filtering** screen appears. This screen lists all existing rules showing which communication protocols are allowed or rejected.
3. Type **1** to select an existing rule or press **F6** to create a new rule.

```

Dynamic Filtering- Incoming IP Address Security

Type options, press Enter.
1=Select 4=Delete

F Te W R D
T In S D TCP M D
P et G B SGN T M Text

Opt IP Address Subnet Mask Y Y *ALL
1.1.1.1 255.255.255.128 Y
1.1.1.99 255.255.255.255 Y Y Y RULE SET BY WIZARD
1.1.1.161 255.255.255.255 Y Y Y RULE SET BY WIZARD
1.1.1.173 255.255.255.255 Y Y Y Y Y Y
1.1.1.196 255.255.255.255 Y S
1.2.3.4 255.255.255.255 Y Y S Y PP

FTP includes: FTPLOG, REXLOG
DDM includes: DDM, DRDA
DB Server includes: SQLENT, SQL, NDB, OBJINF
F3=Exit F6=Add new F8=Print F10=Logon security F12=Cancel

Bottom

```

### Work with Firewall – Incoming IP Address Security

| Parameter or Option | Description                                                |
|---------------------|------------------------------------------------------------|
| <b>F6</b>           | Create a new firewall rule                                 |
| <b>F8</b>           | Print list of firewall rules                               |
| <b>F10</b>          | Work with Logon security rules                             |
| <b>Opt</b>          | 1 = Modify an existing rule<br>4 = Delete an existing rule |

4. If you are creating or modifying a rule, the **Dynamic Filtering Incoming/Outgoing IP Address** screen appears. The table following the screen examples details the appropriate rule parameters.

```

Dynamic Filtering- Modify Incoming IP Address

Type choices, press Enter.

IP Address . . . *ALL
Subnet mask . . . 0.0.0.0
Text *ALL

FTP/ Tel- DB TCP Rmt
REXEC net Srv SGN Srv DDM
Secure value. . . - Y - - - - Y=Yes, S=SSL only
 A=Skip checks
 B=SSL+Skip checks
 L=Skip checks+Log
 M=SSL+Skip checks+Log

Equivalent IP range . . 0.0.0.0-255.255.255.255

SQL statements are not parsed when checks are skipped or rejected.
FTP=FTPLOG, REXLOG. DDM=DDM, DRDA. DB Srv=SQLENT, SQL, NDB, OBJINF.

F3=Exit F4=Select Subnet F10=Logon security F12=Cancel

```

### Modify Firewall Incoming IP Address

| Parameter or Option        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP Address</b>          | Enter an IP address using standard decimal format.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Subnet Mask</b>         | Enter the subnet mask using standard decimal format to define a range of IP addresses. Refer to the examples or press <b>F4</b> to select an appropriate subnet mask range.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Text</b>                | Descriptive text                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Secure value</b>        | <p><b>Y=Yes</b> = Type 'Y' to allow activity or leave the field <b>Blank</b> to reject activity for each individual server.</p> <p><b>S=SSL</b> = Type 'S' to set SSL restrictions for the various types of access protocols.</p> <p><b>A</b> = Allow always</p> <p><b>B</b> = SSL+Skip checks</p> <p><b>L</b> = Allow always and log</p> <p><b>M</b> = SSL+Skip checks+Log</p> <p>Use of <b>B</b> and <b>L</b> can dramatically improve performance for situations such as high volume of requests that come from an already "confident" (well secured) IP that uses SSL, which doesn't require checking of the requests. An example can be a server connected via SSL which issues many SQL (ODBC) and/or Program calls.</p> |
| <b>Equivalent IP Range</b> | Displays the range of IP addresses as defined by the subnet mask.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>F10</b>                 | Work with Logon security rules                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## SSL Support:

iSecurity Firewall now supports SSL restrictions on access to FTP, Telnet, Data Base Server (including ODBC), Sign-on, Remote Access and DDM servers.

This feature is unique and unequaled in the System i security network access market.

The benefits of this feature are:

1. Simple, easy to use interface for defining SSL restrictions for the various types of access protocols (see Figure 1 below).
2. Full integration with iSecurity Firewall's capabilities, providing a "one-stop" solution for all of your company's security network access requirements (see Figure 2 below).
3. The ability to test SSL connectivity before "live" implementation using FYI (for-your information) simulation mode (see Figure 3 below).

```

Dynamic Filtering- Modify Incoming IP Address

Type choices, press Enter.

IP Address 1.1.1.1 Address, *ALL
Subnet mask 255.255.255.128 F4 for list
Text

FTP/ Tel - DB TCP Rmt
RExec net WSG Srv SGN Srv DDM

Y=Yes, S=SSL only Y - - - - - -

Equivalent IP range 1.1.1.0-1.1.1.127

S=SSL requires that the connection is encrypted (Checked from V5R1)

FTP includes: FTPLOG, REXLOG
DDM includes: DDM, DRDA
DB Server includes: SQLENT, SQL, NDB, OBJINF

F3=Exit F4=Select Subnet F10=Logon security F12=Cancel

```

### Secure access protocols with SSL

```

: Firewall *FYI* Simulation Mode :
: :
: Type options, press Enter. :
: :
: Work in *FYI* simulation mode Y Y, N :
: :
: While in this mode, Firewall simulates the application of rules :
: without rejecting transactions. Activity is recorded in the log :
: with the *FYI* designation. :
: *FYI* is an acronym of "For Your Information". :
: :
: F3=Exit F12=Cancel :
: :

```

### Test SSL connectivity while using FYI mode

## Why Raz-Lee developed the SSL Solution

A Raz-Lee customer wished to implement "port restriction" (to separate unsecured and SSL- and ODBC accesses for a specific IP range).

The customer has subsidiaries with specific IP ranges, some of which are capable of communicating via SSL, while others are not. The customer wanted to allow normal port access for specific IP ranges for the subsidiaries which are not capable of using SSL, and wanted to use SSL ports only for the SSL-capable IP range. All other IP addresses should be restricted.

The required solution must be implemented at the IP level and not at the user level, and has to be implemented for ODBC.

In the future, when the entire customer's subsidiaries use SSL, they will want to fully block unsecured ODBC servers. In short, they are not able to restrict unsecured ODBC on the OS/400 level at this time.

## The Customer's Testing Methodology

In order to define their requirements, the company used iSeries Navigator and Microsoft Excel with the iSeries Navigator Data Access plug-in.

When Navigator was configured for non-SSL connections and data was imported via Excel, the customer saw the connections on the i5/OS with NETSTAT connections on ports 8470, 8471, and 8476. These are the normal (non-SSL) ports of host servers.

When Navigator was configured for SSL connections using the same data accessing method, connections were made on ports 9470, 9471, 9476. The customer understood these to be the secured ports of the host servers.

Based on these findings, the customer wanted to define IP address ranges that could access System i data only in secured mode.

## SNA Firewall Rules

SNA firewall rules govern incoming activity from other IBM systems conforming to the SNA system name protocol. Rules control incoming activity for individual system names. For each system name, you can choose to allow or reject activity for any of the following servers:

- DDM
- DRDA
- Passthrough

### To work with SNA firewall rules:

1. Select **2** from the main menu.
2. Select **11. Incoming Remote System Names** from the **Work with Dynamic Filtering** menu. The **Dynamic Filtering- Incoming Remote System Names Security** menu appears. This screen lists all existing rules showing which communication protocols are allowed or rejected.
3. Type **1** to select an existing rule or press **F6** to create a new rule.

```

Dynamic Filtering- Incoming Remote System Names Security

Type options, press Enter.
 1=Select 4=Delete

PASS-
Opt System* DDM DRDA THROUGH Text
 *ALL
 S4455778 Y Y Y my software house
 _

F3=Exit F6=Add new F8=Print F10=Logon security F12=Cancel

Bottom

```

### Work with Firewall – Incoming Remote System Names

| Parameter or Option | Description                                                              |
|---------------------|--------------------------------------------------------------------------|
| <b>F6</b>           | Create a new firewall rule                                               |
| <b>F8</b>           | Print list of firewall rules                                             |
| <b>F10</b>          | Work with Logon security rules                                           |
| <b>Opt</b>          | <b>1</b> = Modify an existing rule<br><b>4</b> = Delete an existing rule |



If you are creating or modifying a rule, the **Dynamic Filtering- Modify Incoming Remote System Name** screen appears. The table following the screen example details the appropriate rule parameters.

```

Dynamic Filtering- Modify Incoming Remote System Name

Type choices, press Enter.

System S4455778 Name, generic*, *ALL
Text my software house

Y=Yes DDM DRDA Passthrough
 Y Y Y

F3=Exit F10=Logon security F12=Cancel

```

### Modify Incoming Remote System Name

| Parameter or Option | Description                                                                                               |
|---------------------|-----------------------------------------------------------------------------------------------------------|
| <b>System</b>       | SNA system name                                                                                           |
| <b>Text</b>         | Description of the SNA system                                                                             |
| <b>Y=Yes</b>        | Type 'Y' to allow activity or leave the field <b>Blank</b> to reject activity for each individual server. |
| <b>F10</b>          | Work with Logon security rules                                                                            |

## Chapter 5: User Security

### Conceptual Framework

User-to-service security rules control the activity of specific users, profiles groups and **Firewall** user groups in individual servers. You can also use user-to-service rules to grant or deny users **\*ALLOBJ** (all objects security) for native OS/400 and IFS objects.

Server security rules, as described in Chapter 4, control activity for each server on a global basis for all users. User-to-Service security rules allow users to control activity via these servers for individual users or groups of users. Group-based rules may be defined for OS/400 group profiles or **Firewall** User Groups.

User-to-service rules override the global server security rules, providing that the **Security Level** parameter is set to **3** or above. For example, if the **Security Level** parameter in the server security rule for the FTP server is set to **3** (user-to-service), user-to-server rules may allow activity for certain users and reject access for others. The **\*PUBLIC** user profile serves (see screen example below) as a default user-to-server rule for all users not explicitly covered by a rule.

### Verb Support

User-to-server rules can also restrict activity on certain servers according to specific remote commands, known as **Verbs** in the System i world. This feature enables limiting user ability to execute specific remote commands. For example, members of the user group **%PGMR** are not permitted to execute the SQL delete command as shown in the following screen.

```

Modify User Security

Type choices, press Enter.
User *PUBLIC

>> Set: 1=Allow (+) 2=Reject 3=By Verb (V) 4=Allow+Skip object check (S)
Log: blank=No change 1=None 2=Rejects 4=All

General User Verb Short
Setting Setting Set Log Support Name
None Yes █ Original File Transfer Function FILTER
None Yes - FTP Server Logon FTPLOG
None Yes - Yes FTP Server-Incoming Rqst Validation FTPSRV
None Yes - Yes FTP Client-Outgoing Rqst Validation FTPCLN
None Yes - REXEC Server Logon REXLOG
None Yes - REXEC Server Request Validation REXEC
None Yes - Yes Original Remote SQL Server RMTSQL
None Yes - Yes Database Server - SQL access & Showcase SQL
None Yes - Yes Database Server - data base access NDB
More...

F3=Exit F4=Prompt F8=Print F9=Object security F10=Logon security
F11=Modify Set/Log F12=Cancel F23=Reject all

```

### Modify User Security

Verb (command) rule support is available for the FTP, SQL, and Database and DDM servers.

## Rule Definition Procedure

To work with user-to-service security, select **11. Users and Groups** from the main menu. The **Work with User Security** screen appears. This screen lists provide a quick glance at the user-to-service rules currently in effect.

- To work with an existing rule, type **1** in the **Opt** field or press **F6** to create a new rule. Use the **PageUp** and **PageDown** keys to scroll through the list. Press **Enter** to continue.

```

Work with User Security

Type options, press Enter. (Read top->down)
1=Select 3=Copy 4=Delete 5=Members

-----Network Servers-----
F F F F R R R F O O C C C N N M S O T
I T T T E R M M I R R S S S P P S Q B C
L P P P X E T T L D D V L L D C C R R G L J P
T L S C L X S S N S S T T P I I D R N L E S S E I S
F O R L O E Q Q D R R A A R C C D D V N N P R N N G
R G V N G C L L B V V Q Q T M M M A M M T L V T F N

User
System Group
Opt
 █ *PUBLIC
 - %FTP
 - %GGG
 - %JJJJ
 - EDI
 - ELIH
 - LEO
 - LUCAS
 - QSECOFR

 V +
 + V + + V V
 +
 +
 + V + + + + + + +
 +
 + V + V
 + + + V
 + V

More...

F3=Exit F6=Add user F7=Add group F8=Print list

```

### Work with User Security

The following table explains the options and information on **Work with User Security** screen.

| Parameter or Option | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>          | <b>1</b> = Select this rule for modification<br><b>3</b> = Copy this rule for another user/group<br><b>4</b> = Delete this rule<br><b>5</b> = Modify group members                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Servers</b>      | Displays the rule status for each server type:<br><b>+</b> = User-to-service rule overrides the global server security rule. Allow a user the access to a server and check for object authorizations.<br><b>V</b> = User-to-service rule overrides with verb (command) support<br><b>Blank</b> = Global server security rule governs activity for this server<br><b>S</b> = Allow a user to access a server and skip the check for object authorizations. This simplifies the test for some users (normally for batch applications, which are playing the role of servers and the desire to save performance in such cases). |

|           |                                      |
|-----------|--------------------------------------|
| <b>F6</b> | Create a rule for a new User         |
| <b>F7</b> | Create a rule for a new Group        |
| <b>F8</b> | Print user-to-service security rules |

4. Enter parameters on the **Add/Modify Parameters** screen and press **Enter** to confirm.

```

 Modify User Security

User *PUBLIC

Type choices, press Enter.
Activity Time _____ Time group, *NEVER
Use Group Authority Y=Yes, N=No, blank=Default
Enable Services based also on OS/400 and %USER Group profiles

Authorities and Locations

2. Services FTP, SQL, NDB, DDM, ...
3. IP
4. Device Names SIGNON only
Selection ==> L

In-product Special Object Authority
AS/400 Native. 3 1=*ALLOBJ, 2=*EXCLUDE, 3=*OBJAUT
IFS 3 1=*ALLOBJ, 2=*EXCLUDE, 3=*OBJAUT

F3=Exit F4=Prompt F8=Print
F9=Object security F10=Logon security F12=Cancel

```

### Modify User Security

| Parameter or Option                        | Description                                                                                                                                                                                                      |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User</b>                                | Displays the user profile or user group name                                                                                                                                                                     |
| <b>Activity Time</b>                       | <b>Time Group</b> = type a time group name or press <b>F4</b> to select from a list.                                                                                                                             |
| <b>Use Group Authorities</b>               | <b>Y</b> = use a specific group authorities<br><b>N</b> = don't use any specific group authorities                                                                                                               |
| <b>Authorities and Locations</b>           | <b>2. Services</b> = specify authorities and location by Services name<br><b>3. IP</b> = specify authorities and location by IP name<br><b>4. Device Names</b> = specify authorities and location by Device name |
| <b>In-product Special Object Authority</b> | Use this field to define object authority for the user/group for <b>AS/400 Native</b> and <b>IFS</b> objects.                                                                                                    |
| <b>F8</b>                                  | Print user-to-service security rules                                                                                                                                                                             |
| <b>F9</b>                                  | Work with object security rules                                                                                                                                                                                  |
| <b>F10</b>                                 | Work with Logon security rules                                                                                                                                                                                   |

## Client Application Security

Client Application Security is an alternative way to set network security.

Until now, most IBM i network access products focused on the Database being accesses, Commands and Program calls in order to determine if the access should be accepted or rejected.

Client Application Security provides the ability to allow a Client Application to be authorized as a whole rather than by the ways in which it accesses the Database, Commands and Program calls.

Once the application is verified for use by a specific user (including Group/Supplemental profiles), from a specific IP, within a specific time frame, etc., all the network access activities of this application will be considered "authorized", requiring no specific detailed authority to be defined.

Client Access Security is, indeed, a revolution in defining and benefiting from network access security.

In order to activate the **Client Application Security** feature, select option **81 → 3. User Exit Programs** and ensure that the **Enable Application Level Security** field is set to **\*STD**.

```

Firewall User Exit Programs

Type options, press Enter.

Allow/Reject request *NONE Name, *NONE
Library Name, *LIBL
This user program is called at the end of the authorization verification,
and may override the decision. See example in SMZ8/GRSOURCE FWAUT#A.

Enable Application Level Security *STD Name, *NONE, *STD
Library Name, *LIBL
GUI product identifies itself and continues without farther inspections.
For *STD value initial identification program SMZ8/GSASTDR should be
called by GUI with two parameters:
<Application name> - *CHAR 20, <Identification key> - *CHAR 50

Pre Power Down System *NONE Name, *NONE
Library Name, *LIBL
This user program is called before system is powered down.
No parameters are passed to this program.

F3=Exit F12=Previous

```

### Firewall User Exit Programs

1. To work with **Client Application Security** go to option **18. Client Application Security** from the main menu

```

Work with Client-Application Security
Subset . . .

Type options, press Enter.
1=Select 3=Copy 4=Delete

Opt Application Active
- JAVARAZLEE Y Definitions for Java
- AX Y
- DD Y nnxx
- EVG2 Y Test for EVG2
- RTY Y sdsdfsfs
- VBN Y frete

Bottom
Client-Application Security is an alternative to user/object security. See Help
F3=Exit F6=Add new F8=Print F12=Cancel

```

## Work with Client-Application Security

2. Press **F6** to add a new client-application

```

Add Client-Application Security

Type information, press Enter.

Application
Text
Active Y Y=Yes, N=No, A=Administrators only

Setting the "Active" for an application controls the level of service that
users can get from this application. While Active=N or Active=A, the product
will still identify the request as such which falls in the category of the
application, but will recognize that the application cannot be used.

F3=Exit F12=Cancel

```

## Add Client-Application Security

## User Management

This chapter presents several powerful security tools that **Firewall** shares with **Action**. These control the ability of users to sign-on to the system and enhance active system security by allowing users to perform the following tasks:

- View and modify security parameters in user profiles using a convenient wizard interface
- Automatically disable inactive users
- Restrict user sign-on to specific hours and days
- Prevent user sign-on during planned absences or following termination
- Analyze default passwords for effectiveness

To work with the user sign-on control tools, select **15. User Management** from the main menu. The **User Management Sign-on** menu appears. Select the desired function from this menu.

| AUUSRMN                                                                                    |  | User Management                | iSecurity/Action<br>System: S720 |
|--------------------------------------------------------------------------------------------|--|--------------------------------|----------------------------------|
| Select one of the following:                                                               |  |                                |                                  |
| <b>Active User</b>                                                                         |  | <b>Authorized Signon Times</b> |                                  |
| 1. Work with Users (WRKACUSR)                                                              |  | 21. Work with Schedule         |                                  |
|                                                                                            |  | 22. Display Schedule           |                                  |
| 5. Print Special Authorities                                                               |  |                                |                                  |
| 6. Print Environment Information                                                           |  | <b>User Absence Security</b>   |                                  |
|                                                                                            |  | 41. Work with Schedule         |                                  |
| <b>Disable Inactive Users</b>                                                              |  | 42. Display Schedule           |                                  |
| 11. Work with Auto-Disable                                                                 |  |                                |                                  |
| 15. Exceptions                                                                             |  | <b>Password Control</b>        |                                  |
|                                                                                            |  | 61. Analyze Default Passwords  |                                  |
|                                                                                            |  | 62. Password Report            |                                  |
| Selection or command<br>==> <input type="text"/>                                           |  |                                |                                  |
| F3=Exit F4=Prompt F9=Retrieve F12=Cancel<br>F13=Information Assistant F16=AS/400 main menu |  |                                |                                  |

### User Management

## Work with Users

The **Work with Users Wizard** enables viewing and modifying several security-related parameters in the user profile by using a user-friendly wizard interface. One can view and work with many different users at once and compare settings between different users.

The security officer can use this tool to review all users at-a-glance and immediately disable suspicious users. One-key access is provided to many of the other user sign-on tools.

To start the **Work with Users** wizard, follow this procedure.

1. Select **1** from the **User Management** menu. The **Action Work with Users** screen appears, offering you several options to display filtered subsets of users.



```

Action Work with Users (WRKACUSR)

Type choices, press Enter.

User *ALL Name, generic*, *ALL
User disabled *ALL *YES, *NO, *ALL
User has password *ALL *YES, *NO, *ALL
Days since last signon is GE . . *ALL Number, *ALL
Invalid signon attempts is GE . *ALL Number, *ALL

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

```

### Action Work with Users

| Parameter or Option                   | Description                                                                                                                                                                                                     |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User</b>                           | <p><b>*ALL</b> = Display all users</p> <p><b>Generic*</b> = Display all users beginning with text preceding the *</p> <p><b>Name</b> = Display a specific user profile</p>                                      |
| <b>User enabled</b>                   | <p><b>*YES</b> = Display enabled users, with passwords, who can sign-on</p> <p><b>*NO</b> = Display disabled users and those who cannot sign-on</p> <p><b>*ALL</b> = Display users irrespective of status</p>   |
| <b>User has password</b>              | <p><b>*YES</b> = Display only users whose password has expired</p> <p><b>*NO</b> = Display only users whose password has not expired</p> <p><b>*ALL</b> = Display users irrespective of password expiration</p> |
| <b>Days since last sign-on is GE</b>  | <p><b>*Number</b> = Display only users who have not signed on for at least the specified number of days</p> <p><b>*ALL</b> = Display users irrespective days since last sign-on</p>                             |
| <b>Invalid sign-on attempts is GE</b> | <p><b>*Number</b> = Display only users who have not signed on for at least the specified number of days</p> <p><b>*ALL</b> = Display users irrespective days since last sign-on</p>                             |

- The **Work with Users Wizard** consists of three screens – **Basic**, **Sign-on**, and **Password**. Each containing several related parameters. The same function key options are available on all screens. On each of these screens, users that cannot sign-on to the system are displayed in **pink**. Use **F11** to navigate between screens.

#### Screen 1: Work with User Status - Basic

This screen shows whether individual users can sign-on to the System i. In order to sign-on, users must be enabled and have a valid, non-expired password.

```

Work with User Status - Basic
iSecurity
Position to . . .

Type options, press Enter.
1=Select 3=Enable 4=Disable 6=Reset count 7=Expire 9=New password
Users displayed in pink are not eligible to sign on.

Opt User Disabled Password
 ILAN Yes IT Team
 ISAAC
 JAVA
 JAVA01 Yes Vajava for AS/400 Lab - Programmer
 JAVA3 Yes GUI Testing
 JOHN
 JR
 KIRK Yes Sales Team
 LENNY Yes Sales Team

F3=Exit F7=Subset F8=Print F11=Additional parameters F12=Cancel
F14=Absence Security F15=Auto-disable exceptions F16=Signon times

```

### Work with User Status - Basic

| Parameter or Option | Description                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>          | <b>1</b> = Display all parameters for the selected user profile (see below)<br><b>3</b> = Enable user profile<br><b>4</b> = Disable user profile<br><b>6</b> = Reset invalid sign-on attempt counter – prevents automatic disabling of this user due to excessive sign-on errors<br><b>7</b> = Set password to 'expired' – this user must change password at next sign-on |
| <b>Enabled</b>      | <b>Blank</b> = User profile is enabled<br><b>No</b> = User profile is disabled                                                                                                                                                                                                                                                                                            |
| <b>Password</b>     | <b>Blank</b> = User profile has a valid password and can sign-on<br><b>None</b> = No password is associated with this user profile and he cannot sign-on                                                                                                                                                                                                                  |
| <b>F7</b>           | Display a subset of user profiles filtered according to status parameters (available on all screens)                                                                                                                                                                                                                                                                      |
| <b>F11</b>          | Display the next of the three parameter screens for the currently displayed user profiles                                                                                                                                                                                                                                                                                 |
| <b>F14</b>          | Temporarily disable users during planned absences (e.g. vacation, sick, leave of absence), or permanently delete users leaving the organization                                                                                                                                                                                                                           |
| <b>F15</b>          | Specify users that should never be disabled automatically, even if they have not signed on for a long period of time (inactive user)                                                                                                                                                                                                                                      |
| <b>F16</b>          | Restrict user sign-on to predefined working hours                                                                                                                                                                                                                                                                                                                         |

In order to display all the parameters for a single user, type **1** in the **Opt** field to the left of the desired user. The following screen appears:

Work with User Status - Details

iSecurity

User . . . . .

JOHN  
John Smith - IT Team

Disabled . . . . .

Password . . . . .

Previous signon . . . . .

11/05/07      1:34

Days passed . . . . .

6

Planned action . . . . .

Invalid attempts . . . . .

Expiration interval . . .

Expiration date . . . . .

Days in use . . . . .

6

Days left . . . . .

F3=Exit   F7=Enable   F8=Disable   F9=Reset password count   F10=Expire password  
F12=Cancel

**Work with User Status – Details**

Use the function keys to modify parameters as shown at the following table:

| Parameter or Option | Description                                                                                                       |
|---------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>F7</b>           | Enable user profile                                                                                               |
| <b>F8</b>           | Disable user profile                                                                                              |
| <b>F9</b>           | Reset invalid sign-on attempt counter – prevents automatic disabling of this user due to excessive sign-on errors |
| <b>F10</b>          | Set password to ‘expired’ – user must change password at next sign-on                                             |

### **Screen 2: Work with User Status - Sign-on**

This screen displays recent sign-on statistics for each user profile. In addition, the scheduled date of any automatic actions (disable or delete) by the **Action** absence control feature is displayed.

| Work with User Status - Signon                                    |        |                 |             | iSecurity       |
|-------------------------------------------------------------------|--------|-----------------|-------------|-----------------|
| Type options, press Enter.                                        |        |                 |             | Position to . . |
| 1=Select 3=Enable 4=Disable 6=Reset count 7=Expire 9=New password |        |                 |             |                 |
| Opt                                                               | User   | Previous signon | Days passed | Planned action  |
| —                                                                 | ILAN   | 31/07/06 17:37  | 170         |                 |
| —                                                                 | ISAAC  | 7/01/07 14:27   | 10          |                 |
| —                                                                 | JAVA   |                 |             |                 |
| —                                                                 | JAVA01 | 24/01/06 19:59  | 358         |                 |
| —                                                                 | JAVA3  |                 |             |                 |
| —                                                                 | JOHN   | 17/01/07 10:19  |             |                 |
| —                                                                 | JR     | 22/09/06 16:06  | 847         |                 |
| —                                                                 | KIRK   | 17/01/07 19:29  |             |                 |
| —                                                                 | LENNY  |                 |             |                 |
| F3=Exit F7=Subset F8=Print F11=Additional parameters F12=Cancel   |        |                 |             |                 |
| F14=Absence Security F15=Auto-disable exceptions F16=Signon times |        |                 |             |                 |

### Work with User Status – Sign-on

| Parameter or Option     | Description                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>              | <b>1</b> = Display all parameters for selected user profile<br><b>3</b> = Enable user profile<br><b>4</b> = Disable user profile<br><b>6</b> = Reset invalid sign-on attempt counter – prevents automatic disabling of this user due to excessive sign-on errors<br><b>7</b> = Set password to ' <b>expired</b> ' – this user must change password at next sign-on |
| <b>Previous Sign-on</b> | Date and time of previous sign-on for this user profile                                                                                                                                                                                                                                                                                                            |
| <b>Days Passed</b>      | Days since previous sign-on for this user profile                                                                                                                                                                                                                                                                                                                  |
| <b>Planned Action</b>   | Displays the date of planned <b>absence control</b> actions (Delete or disable) for this user profile                                                                                                                                                                                                                                                              |

### Screen 3: Work with User Status - Password

This screen displays the number of invalid sign-on attempts and the expiration status of user passwords. This information makes it possible for the security officer to verify that users change their passwords in accordance with the security policy.

| Work with User Status - Password                                  |                  |                     |                 |             | iSecurity       |
|-------------------------------------------------------------------|------------------|---------------------|-----------------|-------------|-----------------|
| Type options, press Enter.                                        |                  |                     |                 |             | Position to . . |
| 1=Select                                                          | 3=Enable         | 4=Disable           | 6=Reset count   | 7=Expire    | 9=New password  |
|                                                                   | Invalid Attempts | Expiration Interval | Expiration Date | Days In use | Days Left       |
| Opt                                                               | User             |                     |                 |             |                 |
| █                                                                 | ILAN             |                     |                 | 170         |                 |
| —                                                                 | ISAAC            |                     |                 | 10          |                 |
| —                                                                 | JAVA             | *NOMAX              |                 | 10          |                 |
| —                                                                 | JAVA01           |                     |                 | 10          |                 |
| —                                                                 | JAVA3            |                     |                 | 10          |                 |
| —                                                                 | JOHN             |                     |                 | 286         |                 |
| —                                                                 | JR               |                     |                 | 847         |                 |
| —                                                                 | KIRK             | *NOMAX              |                 | 20          |                 |
| —                                                                 | LENNY            |                     |                 | 328         |                 |
| F3=Exit F7=Subset F8=Print F11=Additional parameters F12=Cancel   |                  |                     |                 |             |                 |
| F14=Absence Security F15=Auto-disable exceptions F16=Signon times |                  |                     |                 |             |                 |

### Work with User Status – Password

| Parameter or Option        | Description                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>                 | <b>1</b> = Display all parameters for selected user profile<br><b>3</b> = Enable user profile<br><b>4</b> = Disable user profile<br><b>6</b> = Reset invalid sign-on attempt counter – prevents automatic disabling of this user due to excessive sign-on errors<br><b>7</b> = Set password to 'expired' – this user must change password at next sign-on |
| <b>Invalid Attempts</b>    | <b>Blank</b> = User profile is enabled<br><b>No</b> = User profile is disabled                                                                                                                                                                                                                                                                            |
| <b>Expiration Interval</b> | Number of days between required password changes                                                                                                                                                                                                                                                                                                          |
| <b>Expiration Date</b>     | Next password expiration date                                                                                                                                                                                                                                                                                                                             |
| <b>Days in Use</b>         | Number of days the current password has been in use                                                                                                                                                                                                                                                                                                       |
| <b>Days Left</b>           | Number of days before the current password expires                                                                                                                                                                                                                                                                                                        |

## Reports

**User Management** offers two reports that show user profile information.

- Option **5. Print Special Authorities**: the **Special Authorities** report shows details of special authorities assigned to users individually or as part of a group authority. Another parameter that is displayed is a user's limited capabilities.

Display Spooled File

File : QPSECUSR  
Control :  
Find :  
\*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9...+

User Profile Information

5722SS1 V5R2M0 020719  
Report type : \*AUTINFO  
Select by : \*SPCAUT  
Special authorities : \*ALL

-----Special Authorities-----  
\*IO

| User Profile | Group Profiles | *ALL<br>OBJ | *AUD<br>IT | SYS<br>CFG | *JOB<br>CTL | *SAV<br>SYS | *SEC<br>ADM | *SER<br>VICE | *SPL<br>CTL | User Class | Owner   |
|--------------|----------------|-------------|------------|------------|-------------|-------------|-------------|--------------|-------------|------------|---------|
| AARRR        | *NONE          |             |            |            |             |             |             |              |             | *USER      | *USRPRF |
| ABA          | *NONE          |             |            |            |             |             |             |              |             | *USER      | *USRPRF |
| AHARALE      |                | X           | X          | X          | X           | X           | X           | X            | X           | *USER      | *GRPPRF |
|              | QSECOFR        | X           | X          | X          | X           | X           | X           | X            | X           |            |         |
|              | SALE           | X           | X          | X          | X           | X           | X           | X            | X           |            |         |
| AMY          | *NONE          |             |            |            |             |             |             |              |             | *USER      | *USRPRF |
| ANATHM       |                | X           | X          | X          | X           | X           | X           | X            | X           | *SECOFR    | *GRPPRF |
|              | QSECOFR        | X           | X          | X          | X           | X           | X           | X            | X           |            |         |
|              | SALE           | X           | X          | X          | X           | X           | X           | X            | X           |            |         |
|              | DMBANKALL      |             |            |            |             |             |             |              |             |            |         |

F3=Exit F12=Cancel F19=Left F20=Right F24=More keys

### User Profile Information (Special Authorities Report)

- Option 6. **Print Environment Information:** the **Environment Info** report shows environment details including the current library and various default libraries.

User Profile Information

Page 1

5769SS1 V4R1M0 970829 S44K1246 18/02/03 14:35:34

Report type : \*ENVINFO  
Select by : \*SPCAUT  
Special authorities : \*ALL

| User      | Current | Initial Menu/ | Initial Program/ | Job Description/ | Message Queue/ | Output Queue/ | Attention Program/ |
|-----------|---------|---------------|------------------|------------------|----------------|---------------|--------------------|
| Profile   | Library | Library       | Library          | Library          | Library        | Library       | Library            |
| ADVERTISE | *CRTDFT | MAIN          | *NONE            | QDFTJOB          | ADVERTISE      | *WRKSTN       | *SYSVAL            |
|           |         | *LIBL         |                  | QGPL             | QUSRSYS        |               |                    |
| AHARALE   | *CRTDFT | MAIN          | INLUSR           | QBATCH           | AHARALE        | *WRKSTN       | POPATN             |
|           |         | *LIBL         | SALE             | SALE             | QUSRSYS        |               | SMZP               |
| ALLOBJ    | *CRTDFT | MAIN          | *NONE            | QDFTJOB          | ALLOBJ         | *WRKSTN       | *SYSVAL            |
|           |         | *LIBL         |                  | QGPL             | QUSRSYS        |               |                    |
| ANGUS     | *CRTDFT | MAIN          | INLPGM           | QDFTJOB          | ANGUS          | *WRKSTN       | POPATN             |
|           |         | *LIBL         | DS               | QGPL             | QUSRSYS        |               | SMZP               |
| ANGUS2    | *CRTDFT | MAIN          | INLPGM           | QDFTJOB          | ANGUS2         | *WRKSTN       | POPATN             |
|           |         | *LIBL         | DS               | QGPL             | QUSRSYS        |               | SMZP               |
| ANONYMOUS | *CRTDFT | MAIN          | *NONE            | QDFTJOB          | ANONYMOUS      | *WRKSTN       | *SYSVAL            |

### User Profile Information (Environmental Info Report)

- To print these reports, select 5 or 6 from the **User Management** menu. Enter the report type and filter parameters as shown on the following screen.

```

Print User Profile (PRTAUUSRP)

Type choices, press Enter.

Type of information > *AUTINFO *ALL, *AUTINFO, *ENVINFO...
Select by *SPCAUT *SPCAUT, *USRCLS, *MISMATCH
Output *PRINT *PRINT, *PRINT1-*PRINT9
Job description QBATCH Name, *NONE
Library *PRODUCT Name, *PRODUCT, *LIBL...

Additional Parameters

Special authorities *ALL *ALL, *NONE, *ALLOBJ...
+ for more values
User class *ALL *ALL, *USER, *SYSOPR...
+ for more values

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

```

### Print User Profile

| Parameter or Option    | Description                                                                                                                                                                                                                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select by</b>       | <p><b>*SPCAUT</b> = User profiles are selected based on special authorities</p> <p><b>*USRCLS</b> = User profiles are selected based on user class</p> <p><b>*MISMATCH</b> = User profiles are selected based on the fact that their special authorities are not the default values assigned to their user class</p> |
| <b>Job description</b> | Date and time of previous sign-on for this user profile                                                                                                                                                                                                                                                              |

## Disable Inactive Users

The presence of valid but inactive user profiles can pose a potentially serious security threat. Hackers can exploit these profiles to gain access to critical data via FTP, ODBC connectivity or other methods even without knowing the password.

For this reason, it is always a good idea to periodically audit your system and disable any users who have not signed on recently. The Work with Users Wizard, discussed in the previous section, is an excellent tool for performing such a review and manually disabling inactive users.

**Action** includes the **Auto-Disable** feature, which allows for disabling of inactive user profiles automatically after a specified period. Automatic disabling applies to any user who has not signed on for the specified number of days. One can also designate specific users as exceptions, who cannot be disabled automatically. OS/400 system-generated profiles (prefixed by the letter 'Q') are never automatically disabled.

- To enable the Auto-Disable feature, select **11. Work with Auto-Disable** from the **User Management** menu. Set the **Auto-Disable inactive users** parameter to **\*YES** and specify the number of days of inactivity in the appropriate field.
- To disable this feature, set the **Auto-Disable inactive users** parameter to **\*NO**.



```

Auto-Disable Inactive Users

Type choices, press Enter.

Auto-Disable inactive users. . . ☒ NO *YES, *NO

Days of inactivity 0 1-366

Users who have not signed on for the specified period will be disabled
automatically by this feature.

Q* profiles, which are required for system activity, are never disabled.
Press F11 to prevent specific users from being disabled automatically.

F3=Exit F11=Auto-Disable exceptions F12=Cancel

```

### Auto-Disable Inactive Users

- To define exceptions from the Auto-Disable default, select **15. Exceptions** from the **User Management** menu. The **Auto-Disable Exceptions** screen appears. Press **F6** and type the user profile name(s) that should not be disabled automatically.
- To delete a user profile from this exception list, type **4** next to the name and press **Enter**.

## Restricting User Sign-on Times

Even valid user profiles have the potential for abuse. A common hacker trick is to obtain a user's password and use it to sign-on after the user has left work in order to access programs and data with that user's authorities. Using this method, a dishonest employee can bypass object level security and remain invisible to subsequent audit.

An effective defense against this scenario would be to restrict user sign-on to authorized working hours. **Action** includes a user-friendly tool for defining authorized sign-on periods for users, by time and day of the week.

1. To define authorized sign-on times for users, select **21. Work with Schedule** from the **User Management** menu. The following screen appears (a table of explanation follows).



```

Sorted by User Work with Signon Schedule

Type options, press Enter.
 1=Select 4=Delete Position to User . _____

 Opt User Group Enable Disable Days
 ─── ─── ─── ─── ─── ───
 1 ABBY 7:00 19:00 *FRI *THU *WED *TUE
 - AMY 8:00 16:00 *MON *TUE *WED *THU
 - ANNAM QSECOFR :00 :00 *ALL
 - AU 8:00 19:00 *TUE *WED *THU
 - AV QSECOFR :00 :00 *ALL
 - DANIEL SALE 8:00 10:00 *MON *TUE *WED *THU *FRI

 More...

F3=Exit F6=Add new F8=Print F11=Sort by User/Group F12=Cancel

```

### Work with Sign-on Schedule

| Parameter or Option | Description                                                                              |
|---------------------|------------------------------------------------------------------------------------------|
| <b>Opt</b>          | 1 = Select to modify<br>4 = Delete the selected user                                     |
| <b>Position to</b>  | Position the cursor at the first item beginning with the text string typed in this space |
| <b>F8</b>           | Print a report showing sign-on schedules for all users                                   |

**NOTE:** You can create only one sign-on schedule for each user profile.

2. Select a user from the list or press **F6** to define a new user schedule. The **Create Sign-on Schedule** screen appears.

```

Create Signon Schedule

Type choices, press Enter.

Enable 8:00 Time
Disable 19:00 Time

This rule is in effect:
Everyday Y
-or-
Only on specified days Mon Tue Wed Thr Fri Sat Sun

Apply schedule to ONE of the following:
All users in group profile
User profile(s) Name
Selecting the last option and pressing F4, enables you to apply the signon
schedule to more than one user at a time.

F3=Exit F4=Prompt F12=Cancel

```

### Create Sign-on Schedule

| Parameter or Option           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable/Disable</b>         | Time of day using a 24-hour format                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>This rule is in effect</b> | <b>Everyday</b> = Type "Y" to apply schedule to every day of the week<br><b>Specified days</b> = Type "Y" on the desired week days                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Apply Schedule to</b>      | <b>User profile</b> = Enter user profile name or a generic text string to create a schedule for all user profiles beginning with the text string preceding the "*" (i.e. <b>R*</b> applies to all users beginning with the letter <b>R</b> )<br><b>All users in group profile</b> = Enter a group profile name to create a schedule for all users contained in the group profile<br><b>Select users from list</b> = Enter a generic text string to select user profiles from a list of all user profiles beginning with the text string preceding the "*" (i.e. <b>R*</b> displays all users beginning with the letter <b>R</b> ). You may then select one or more of them |

## User Absence Security

Another common security risk occurs when an authorized user is away on temporary leave (e.g. vacation, sick leave, maternity leave, business trips, etc.) or leaves the organization. **Action** allows you make certain that nobody can sign on with specific user profiles during such scheduled absences by disabling or deleting user profiles automatically on a specific date.

To work with user absence security,

1. Select **41. Work with Schedule** from the **User Management** menu. The following screen appears.

```

Work with User Absence Schedule

Disable users on temporary leave (eg. vacation, sick, leave of absence), or
Permanently delete users leaving the organization.
Type options, press Enter.
 1=Select 4=Delete
Opt User Date Description
 a53 31/05/08
 a54 13/05/09
 fdsgg 14/06/06
 A38 11/08/08
 A54 9/05/13
 EVA 15/05/09
 QSECOFR 28/05/08 Security Officer big
 TEST1 8/12/12

Bottom
Users displayed in red are scheduled to be deleted. F11 for more details.
F3=Exit F6=Add New F8=Print list F11=Fold/Drop F12=Cancel

```

### Work with User Absence Schedule

2. Select a user from the list or press **F6** to add a new user. The **Modify User Absence Schedule** screen appears.

```

Modify User Absence Schedule

Type choices, press Enter.

User EVA
Date 15/05/09
Action 1
 1=Disable
 2=Delete

For scheduled *DELETE:
Owned object option
New owner (if *CHGOWN).

Primary group change option
New primary group
New primary group authority
 *NODLT, *DLT, *CHGOWN
 *NOCHG, *CHGPGP
 *OLDPGP, *PRIVATE, *CHANGE
 *USE, *EXCLUDE

F3=Exit F12=Cancel

```

### Modify User Absence Schedule

3. Enter the appropriate parameters as described in the following table.

| Parameter or Option | Description                            |
|---------------------|----------------------------------------|
| User                | User profile to be disabled or deleted |

| Parameter or Option                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Date</b>                                                       | Date on which the user profile will be disabled or deleted                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Action</b>                                                     | 1 = Disable user profile<br>2 = Delete user profile                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>The following parameters apply to scheduled deletions only</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Owned object action</b>                                        | Specify the action to be performed when a user profile scheduled for deletion owns one or more objects:<br><b>*NODLT</b> = If the user profile owns any objects, neither the user profile nor the objects are deleted<br><b>*DLT</b> = Both the user profile and any objects owned by it are deleted<br><b>*CHGOWN</b> = The user profile is deleted and ownership of all objects is transferred to the alternate user profile specified in the <b>New Owner</b> parameter                                                               |
| <b>New owner</b>                                                  | User profile name of the new owner when object ownership is transferred by the <b>*CHGOWN</b> parameter                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>New primary group</b>                                          | Name of the user profile that will become new the primary group                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>New primary group authority</b>                                | <b>*OLDPGP</b> = The new primary group inherits the same authority as the old primary group<br><b>*PRIVATE</b> = The new primary group inherits the same private authority as previously defined for all owned objects<br><b>*ALL</b> = The new primary group assumes the <b>*ALL</b> authority<br><b>*CHANGE</b> = The new primary group assumes the <b>*CHANGE</b> authority<br><b>*USE</b> = The new primary group assumes the <b>*USE</b> authority<br><b>*EXCLUDE</b> = The new primary group assumes the <b>*EXCLUDE</b> authority |

---

**NOTE:** Refer to IBM documentation for a complete discussion regarding the concepts of object ownership and primary groups.

---

## Password Control Tools

This section describes two tools that help you correct potential security risks caused by easy to guess passwords.

### Analyze Default Passwords

A profile is said to have a **default password** whenever the password is the same as the profile name. Obviously, this is dangerous because it is so easy to guess. This feature allows users to print a report of all the user profiles on the system that have a default password and optionally disable those profiles or expire their passwords.

To perform the analysis, select **61. Analyze Default Passwords** from the **User Management** menu. The **Analyze Action + Default Passwords** screen appears.

```

Analyze Action+ Dft Passwords (ANZAUDFTP)

Type choices, press Enter.

Action taken against profiles . *NONE *NONE, *DISABLE, *PWDEXP

Job description > QBATCH Name, *NONE
Library *PRODUCT Name, *PRODUCT, *LIBL...

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

```

### Analyze Default Passwords

The system prints the following report.

| User profiles with default passwords.           |           |        |            |                |
|-------------------------------------------------|-----------|--------|------------|----------------|
| 5769SS1 V4R1M0 970829                           |           |        |            | S44K1246 18/02 |
| Action taken against profiles . . . . . : *NONE |           |        |            |                |
| User                                            |           |        |            |                |
| Profile                                         | STATUS    | PWDEXP | Text       |                |
| AHARALE                                         | *ENABLED  | *YES   |            |                |
| ALLOBJ                                          | *ENABLED  | *NO    |            |                |
| ANGUS                                           | *DISABLED | *YES   |            |                |
| ANGUS2                                          | *DISABLED | *YES   |            |                |
| ANONYMOUS                                       | *DISABLED | *NO    |            |                |
| CPUSCOPE                                        | *DISABLED | *YES   | CpuScope   |                |
| DRDA                                            | *DISABLED | *YES   |            |                |
| ELIH                                            | *ENABLED  | *NO    | Eli Haleli |                |
| EMAIL                                           | *DISABLED | *YES   |            |                |
| GENIUS1                                         | *DISABLED | *YES   |            |                |
| GENIUS2                                         | *DISABLED | *YES   |            |                |
| GENIUS3                                         | *DISABLED | *YES   |            |                |
| GENIUS4                                         | *DISABLED | *YES   |            |                |
| GENIUS5                                         | *DISABLED | *YES   |            |                |

### User Profiles with Default Passwords

### Password Statistical Report

This feature allows users to print a report showing information similar to that displayed on the **Work with Users Wizard**.

```

Print User Profile (PRTAUUSRP)

Type choices, press Enter.

Type of information > *PWDINFO *ALL, *AUTINFO, *ENVINFO...
Select by *SPCAUT *SPCAUT, *USRCLS, *MISMATCH
Output *PRINT *PRINT, *PRINT1-*PRINT9
Job description > QBATCH Name, *NONE
Library *PRODUCT Name, *PRODUCT, *LIBL...

Additional Parameters

Special authorities *ALL *ALL, *NONE, *ALLOBJ...
+ for more values
User class *ALL *ALL, *USER, *SYSOPR...
+ for more values

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

```

### Print User Profile

| Parameter or Option        | Description                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select by</b>           | <p><b>*SPCAUT</b> = User profiles will be selected for the report based on special authorities</p> <p><b>*USRCLS</b> = User profiles will be selected for the report based on user class</p> <p><b>*MISMATCH</b> = User profiles will be selected for this report only if their special authorities are not the same as the default authorities assigned to their user class</p> |
| <b>Job description</b>     | Batch job subsystem and library                                                                                                                                                                                                                                                                                                                                                  |
| <b>Special authorities</b> | Filter according to one or more special authority types                                                                                                                                                                                                                                                                                                                          |
| <b>User class</b>          | Filter according to one or more user class types                                                                                                                                                                                                                                                                                                                                 |

## Chapter 6: Object Security

Object security controls access to objects originating from specific external sources such as FTP, ODBC, etc. The user can specify the operations an external user is allowed to perform on these objects. Rules may be defined for the following object types: files, libraries, data queues, printer files, programs, commands and IFS objects.

**Firewall** can restrict a user's ability to perform specific actions, such as read, write, create, delete, rename, and run, etc., on protected objects.

**Firewall** offers an efficient system in which the user needs to create only a small number of general rules restricting the use of commands for all or most users, and then creates a few exceptions to these rules. This feature is discussed later on in its own section.

### Procedural Overview

The basic procedure for defining any of the object security rules is similar. The following sections provide details and explanations regarding the specific parameters and definitions for each type of logon security rule.

1. Select **21** from the main menu. The **Native AS/400 Object Security** menu appears.
2. Choose the object type from the **Native AS/400 Object Security** menu.
  - a. Select **1** for files.
  - b. Select **2** for libraries.
  - c. Select **3** for data queues.
  - d. Select **4** print files.
  - e. Select **5** for programs.
  - f. Select **6** for commands.
  - g. Select **7** command exceptions.
3. The appropriate **Work with Object Security** screen appears. Refer to the appropriate rule type section for details regarding that screen.
4. Type **1** to select an existing rule for editing or press **F6** to create a new rule. The relevant **ADD/Modify** screen appears.
5. Enter or modify the parameters for the appropriate rule type. Refer to the appropriate rule type section for details and explanations regarding the screen and its parameters
6. Press **Enter** to confirm and return to the **Work with Object Security** screen.
7. Press **Enter** to confirm and return to the main menu.

## Native OS/400 Objects

This section describes the screens used to work with native OS/400 objects. Select **21. Native AS/400 Objects** from the main menu. The **Native AS/400 Object Security** menu appears.

|                                                |                                             |              |
|------------------------------------------------|---------------------------------------------|--------------|
| GSNTVMNU                                       | <b>Native AS/400 Object Security</b>        | Firewall     |
|                                                |                                             | System: S720 |
| Select one of the following:                   |                                             |              |
| <b>Definitions</b>                             | <b>Rule Wizard</b>                          |              |
| 1. Files                                       | 41. Create Working Data Set                 |              |
| 2. Libraries                                   | 42. Work with Rule Wizard                   |              |
| 3. Data Queues                                 |                                             |              |
| 4. Printer Files                               | <b>Pre-check Replacement for Validation</b> |              |
| 5. Programs                                    | 61. Pre-check Library Replacement           |              |
| 6. Commands                                    |                                             |              |
| 9. Command Exceptions                          |                                             |              |
| <b>Reporting</b>                               |                                             |              |
| 11. Display Native AS/400 Object Log           |                                             |              |
| Selection or command                           |                                             |              |
| ==> █                                          |                                             |              |
| F3=Exit F4=Prompt F9=Retrieve F12=Cancel       |                                             |              |
| F13=Information Assistant F16=AS/400 main menu |                                             |              |

### Native AS/400 Object Security

The specific details of each object type are discussed in the following sections.

## Files

- From the **Native AS/400 Object Security** screen, select **1. Files**. The **Work with Native AS/400 File Security** screen appears. This screen lists all the rules currently in effect.
- Type **1** to modify an existing rule or press **F6** to create a new rule.
- Press **Enter** to return to the **Native OS/400 Object Security** menu.



```

Work with Native AS/400 File Security

Type options, press Enter.
 1=Select 3=Copy 4=Delete Subset

```

| Opt | File    | Library | Users        |
|-----|---------|---------|--------------|
| █   | *ALL    | *ALL    | QSECOFR      |
| -   | AU      | DLT     | QSECOFR      |
| -   | *ALL    | QGPL    | QSECOFR      |
| -   | Q*      | QGPL    | %SECRP       |
| -   | QCLSRC  | QGPL    | *PUBLIC USER |
| -   | GSEPNTJ | QTEMP   | JAVA         |
| -   | GSCASP  | SMZTMPA | QUSER        |

```

F3=Exit F6=Add new F8=Print F12=Cancel

Bottom

```

### Work with Native AS/400 File Security

| Parameter or Option | Description                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>          | <b>1</b> = Select this rule for modification<br><b>3</b> = Copy this rule for another user<br><b>4</b> = Delete this rule |
| <b>F6</b>           | Add new rule                                                                                                              |
| <b>F8</b>           | Print rules                                                                                                               |
| <b>Subset</b>       | Search a file or library whose names contain the subset                                                                   |

## Add/Modify Native AS/400 File Security

```
Modify Native AS/400 File Security
```

Type information, press Enter.

File . . . . . SCUST  
Library . . . . SALE

Define user authority, press Enter.  
Y=Yes

| User*, %Group                             | DATA                  |                       | FILE MANAGEMENT       |                       |                       |                       |
|-------------------------------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Group profile                             | Read                  | Write                 | Create                | Delete                | Rename                | Other                 |
| *PUBLIC                                   | Y                     | Y                     | Y                     | Y                     | Y                     | Y                     |
| DAVID _____                               | Y                     | Y                     | Y                     | -                     | -                     | -                     |
| █_____                                    | -                     | -                     | -                     | -                     | -                     | -                     |
| _____<br>_____<br>_____<br>_____<br>_____ | -<br>-<br>-<br>-<br>- | -<br>-<br>-<br>-<br>- | -<br>-<br>-<br>-<br>- | -<br>-<br>-<br>-<br>- | -<br>-<br>-<br>-<br>- | -<br>-<br>-<br>-<br>- |

F3=Exit    F4=Prompt    F12=Cancel

More...

## Modify Native AS/400 File Security

In the **Modify Native AS/400 File Security** screen, define permissions for one user profile, profile group or **Firewall** user group on each line. Use the **PageUp** and **PageDown** keys to scroll through a long list.

For each activity type, **Y** = Activity allowed and **Blank** = Activity rejected. **\*Public** is the default rule for all users not explicitly covered by an object security rule.

**NOTE:** Always make certain that the **\*Public** rule contains sufficient permissions to allow access of ordinary users to objects.

| Parameter or Option | Description                                                                             |
|---------------------|-----------------------------------------------------------------------------------------|
| <b>File/Library</b> | File name and library path of the file(s) included in this rule.                        |
| <b>User, Group</b>  | Enter user profile or press <b>F4</b> to select a user profile or group name from list. |
| <b>Read</b>         | 'Y' = Users may read the specified file                                                 |
| <b>Write</b>        | 'Y' = Users may write, edit or update the specified file                                |
| <b>Create</b>       | 'Y' = Users may create a new file                                                       |
| <b>Delete</b>       | 'Y' = Users may delete the specified file                                               |
| <b>Rename</b>       | 'Y' = Users may rename the specified file                                               |
| <b>Other</b>        | 'Y' = Users may perform other actions on the specified file.                            |

Press **Enter** to return to the **Work with Native Object Security** screen.

## Libraries

1. From the **Native AS/400 Object Security** screen, select **2. Libraries**. The **Work with Native AS/400 Library Security** screen appears. This screen lists all the rules currently in effect.
2. Type **1** to modify an existing rule or press **F6** to create a new rule.
3. Press **Enter** to return to the **Native OS/400 Object Security** menu.

```

Work with Native AS/400 Library Security

Type options, press Enter.
1=Select 3=Copy 4=Delete Subset

Opt Library ----- Users -----
 *ALL
 SALE1 JOHN
 -

F3=Exit F6=Add new F8=Print F12=Cancel

Bottom

```

### Work with Native AS/400 Library Security

| Parameter or Option | Description                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>          | <b>1</b> = Select this rule for modification<br><b>3</b> = Copy this rule for another user<br><b>4</b> = Delete this rule |
| <b>F6</b>           | Add new rule                                                                                                              |
| <b>F8</b>           | Print rules                                                                                                               |
| <b>Subset</b>       | Search a file or library whose names contain the subset                                                                   |

## Add/Modify Native AS/400 Library Security

```

Modify Native AS/400 Library Security

Type information, press Enter.

Library SALE1

Define user authority, press Enter.
Y=Yes

User*, %Group
Group profile
*PUBLIC
CRAIG
JANE
█

LIBRARY MANAGEMENT
Create Delete Rename Other
Y Y - -
Y - - -
- - - -
- - - -
- - - -
- - - -
- - - -

More...

F3=Exit F4=Prompt F12=Cancel

```

### Modify Native AS/400 Library Security

In the **Modify Native AS/400 Library Security** screen, define permissions for one user profile, profile group or **Firewall** user group on each line. Use the **PageUp** and **PageDown** keys to scroll through a long list.

For each activity type, 'Y' = Activity allowed and **Blank** = Activity rejected. **\*Public** is the default rule for all users not explicitly covered by an object security rule. Always make certain that the **\*Public** rule contains sufficient permissions for ordinary users to access objects.

| Parameter or Option | Description                                                  |
|---------------------|--------------------------------------------------------------|
| <b>Library</b>      | Shows the libraries covered by the rule                      |
| <b>Create</b>       | 'Y' = Users may create a new file                            |
| <b>Delete</b>       | 'Y' = Users may delete the specified file                    |
| <b>Rename</b>       | 'Y' = Users may rename the specified file                    |
| <b>Other</b>        | 'Y' = Users may perform other actions on the specified file. |

Press **Enter** to return to the **Work with Native Object Security** screen.

## Data Queues

1. From the **Native AS/400 Object Security** screen, select **3. Data Queues**. The **Work with Native AS/400 Data Security** screen appears. This screen lists all the rules currently in effect.
2. Type **1** to modify an existing rule or press **F6** to create a new rule.
3. Press **Enter** to return to the **Native OS/400 Object Security** menu.

```

Work with Native AS/400 Data Queue Security

Type options, press Enter.
 1=Select 3=Copy 4=Delete Subset
Opt Data Queue Library ----- Users -----
 1 *ALL *ALL

F3=Exit F6=Add new F8=Print F12=Cancel

Bottom

```

### Work with Native AS/400 Data Queue Security

| Parameter or Option | Description                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>          | <b>1</b> = Select this rule for modification<br><b>3</b> = Copy this rule for another user<br><b>4</b> = Delete this rule |
| <b>F6</b>           | Add new rule                                                                                                              |
| <b>F8</b>           | Print rules                                                                                                               |
| <b>Subset</b>       | Search a data queue or library whose names contain the subset                                                             |

## Add/Modify Object Data Queue Security

```

 Modify Native AS/400 Data Queue Security

Type information, press Enter.

Data Queue . . *ALL
Library *ALL

Define user authority, press Enter.
Y=Yes

User*, %Group |----- DATA -----|-- DQ MANAGEMENT --|
Group profile |Read Write |Create Delete |
*PUBLIC |Y Y |Y Y |
%JAVA |Y Y |Y Y |
JIM |Y Y |— — |
DANNY |Y — |— — |
█ |— — |— — |
 |— — |— — |
 |— — |— — |
 |— — |— — |

```

More...

F3=Exit    F4=Prompt    F12=Cancel

## Modify Native AS/400 Data Queue Security

Define permissions for one user profile, profile group or **Firewall** user group on each line. Use the **PageUp** and **PageDown** keys to scroll through a long list.

For each activity type, **'Y'** = Activity allowed and **Blank** = Activity rejected. **\*Public** is the default rule for all users not explicitly covered by an object security rule. Always make certain that the **\*Public** rule contains sufficient permissions for ordinary users to access objects.

| Parameter or Option | Description                                                                             |
|---------------------|-----------------------------------------------------------------------------------------|
| <b>Data Queue</b>   | Shows the data queue(s) included in this rule.                                          |
| <b>User, Group</b>  | Enter user profile or press <b>F4</b> to select a user profile or group name from list. |
| <b>Read</b>         | 'Y' = Users may read the specified file                                                 |
| <b>Write</b>        | 'Y' = Users may write, edit or update the specified file                                |
| <b>Create</b>       | 'Y' = Users may create a new file                                                       |
| <b>Delete</b>       | 'Y' = Users may delete the specified file                                               |

Press **Enter** to return to the **Work with Native Object Security** screen.

## Printer Files

1. From the **Native AS/400 Object Security** screen, select **4. Printer Files**. The **Work with Native AS/400 Print File Security** screen appears. This screen lists all the rules currently in effect.
2. Type **1** to modify an existing rule or press **F6** to create a new rule.
3. Press **Enter** to return to the **Native OS/400 Object Security** menu.

```

Work with Native AS/400 Print File Security

Type options, press Enter.
 1=Select 3=Copy 4=Delete Subset
Opt Print File Library ----- Users -----
 █ *ALL *ALL

F3=Exit F6=Add new F8=Print F12=Cancel

Bottom

```

### Work with Native AS/400 Print File Security

| Parameter or Option | Description                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>          | <b>1</b> = Select this rule for modification<br><b>3</b> = Copy this rule for another user<br><b>4</b> = Delete this rule |
| <b>F6</b>           | Add new rule                                                                                                              |
| <b>F8</b>           | Print rules                                                                                                               |
| <b>Subset</b>       | Search a print file or library whose names contain the subset                                                             |

## Add/Modify Print File Security

```

Modify Native AS/400 Print File Security

Type information, press Enter.

Print File . . *ALL
Library *ALL

Define user authority, press Enter.
Y=Yes

User*, %Group Open Print
Group profile File
*PUBLIC Y
%G Y
%SALETEAM Y
FRED Y
KATE Y
█ -
 -
 -

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

### Modify Native AS/400 Print File Security

Define permissions for one user profile, profile group or **Firewall** user group on each line. Use the **PageUp** and **PageDown** keys to scroll through a long list.

For each activity type, 'Y' = Activity allowed and **Blank** = Activity rejected. **\*Public** is the default rule for all users not explicitly covered by an object security rule. You should always make certain that the **\*Public** rule contains sufficient permissions to allow access to objects by ordinary users.

| Parameter or Option       | Description                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------|
| <b>Print File/Library</b> | Shows the print file(s) and library path included in this rule                          |
| <b>User, Group</b>        | Enter user profile or press <b>F4</b> to select a user profile or group name from list. |
| <b>Open Print file</b>    | 'Y' = Users may use the specified file                                                  |

Press **Enter** to return to the **Work with Native Object Security** screen.



1. From the **Native AS/400 Object Security** screen, select **5. Programs**. The **Work with Native AS/400 Program Security** screen appears. This screen lists all the rules currently in effect.
2. Type **1** to modify an existing rule or press **F6** to create a new rule.
3. Press **Enter** to return to the **Native OS/400 Object Security** menu.

## Work with AS/400 Program Security

| Parameter or Option | Description                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>          | <b>1</b> = Select this rule for modification<br><b>3</b> = Copy this rule for another user<br><b>4</b> = Delete this rule |
| <b>F6</b>           | Add new rule                                                                                                              |
| <b>F8</b>           | Print rules                                                                                                               |
| <b>Subset</b>       | Search a program or library whose names contain the subset                                                                |

## Add/Modify Object Security Screen

```
Modify Native AS/400 Program Security
```

Type information, press Enter.

```
Program CLRPFM
Library QSYS
```

Define user authority, press Enter.  
Y=Yes

| User*, %Group            | Run     |
|--------------------------|---------|
| Group profile            | Program |
| *PUBLIC                  | Y       |
| %JAVA                    | Y       |
| <input type="checkbox"/> | -       |
| <input type="checkbox"/> | -       |
| <input type="checkbox"/> | -       |
| <input type="checkbox"/> | -       |
| <input type="checkbox"/> | -       |
| <input type="checkbox"/> | -       |

F3=Exit    F4=Prompt    F12=Cancel

More...

## Modify Native AS/400 Program Security

Define permissions for one user profile, profile group or **Firewall** user group on each line. Use the **PgUp** and **PgDn** keys to scroll through a long list.

For each activity type, **'Y'** = Activity allowed and **Blank** = Activity rejected. **\*Public** is the default rule for all users not explicitly covered by an object security rule. You should always make certain that the **\*Public** rule contains sufficient permissions for ordinary users to access objects.

| Parameter or Option    | Description                                                                             |
|------------------------|-----------------------------------------------------------------------------------------|
| <b>Program/Library</b> | Name and library path of the program(s) included in this rule                           |
| <b>User, Group</b>     | Enter user profile or press <b>F4</b> to select a user profile or group name from list. |
| <b>Run Program</b>     | 'Y' = Users may run the specified program                                               |

Press **Enter** to return to the **Work with Native Object Security** screen.

## Commands

1. From the **Native AS/400 Object Security** screen, select **6. Commands**. The **Work with Native AS/400 Command Security** screen appears. This screen lists all the rules currently in effect.
2. Type **1** to modify an existing rule or press **F6** to create a new rule.
3. Press **Enter** to return to the **Native OS/400 Object Security** menu.

```

Work with Native AS/400 Command Security

Type options, press Enter.
 1=Select 3=Copy 4=Delete Subset

Opt Command Library Users -----
 1 *ALL *ALL
- DSPAULOG QGPL QSECOFR
- DSPFWLOG QGPL JAVA
- ADDLIBL QSYS GLIORA

F3=Exit F6=Add new F8=Print F12=Cancel

Bottom

```

### Work with Native AS/400 Command Security

| Parameter or Option | Description                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>          | <b>1</b> = Select this rule for modification<br><b>3</b> = Copy this rule for another user<br><b>4</b> = Delete this rule |
| <b>F6</b>           | Add new rule                                                                                                              |
| <b>F8</b>           | Print rules                                                                                                               |
| <b>Subset</b>       | Search a command or library whose names contain the subset                                                                |

## Add/Modify Command Security

```
Modify Native AS/400 Command Security
```

Type information, press Enter.

```
Command DSPFWLOG
Library QGPL
```

Define user authority, press Enter.  
Y=Yes

| User*, %Group | Run     |
|---------------|---------|
| Group profile | Command |
| *PUBLIC       |         |
| JAVA _____    | Y_____  |
| █_____        | -_____  |
| _____-        | -_____  |
| _____-        | -_____  |
| _____-        | -_____  |
| _____-        | -_____  |
| _____-        | -_____  |

F3=Exit    F4=Prompt    F12=Cancel

More...

## Modify Native AS/400 Command Security

Define permissions for one user profile, profile group or **Firewall** user group on each line. Use the **PageUp** and **PageDown** keys to scroll through a long list.

For each activity type, **'Y'** = Activity allowed and **Blank** = Activity rejected. **\*Public** is the default rule for all users not explicitly covered by an object security rule. Always make certain that the **\*Public** rule contains sufficient permissions to allow ordinary users to access objects.

| Parameter or Option     | Description                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------|
| <b>Command /Library</b> | Name and library path of the command(s) included in this rule                           |
| <b>User, Group</b>      | Enter user profile or press <b>F4</b> to select a user profile or group name from list. |
| <b>Run Command</b>      | 'Y' = Users may execute the specified command                                           |

Press **Enter** to return to the **Work with Native Object Security** screen.

## Command Exceptions

When working with command rules, it is easier to define restrictions globally for all users or for large groups of users. Unfortunately, there are usually only a few users who truly need permission to execute certain commands. **Firewall** provides the ability to create one rule that prevents all or most users from using certain commands and then to create a few exceptions to that rule for the select few who are authorized to use the relevant commands.

One can define exceptions that will permit commands to be executed via the command line, within programs, FTP, REXEC (Remote Command Execution), and/or DDM.

The procedure for working with exceptions is quite simple:

1. Define the global or general command security rules as described in the previous section.
2. Select **9** from the **Native AS/400 Object Security** menu. The following screen appears.
3. This screen lists all the rules currently in effect. Type **1** to work with an existing rule or press **F6** to create a new rule.

Work with Command Exceptions

Type options, press Enter.  
1=Select    3=Copy    4=Delete

| Opt | Command | Users     |
|-----|---------|-----------|
| █   | ROWR    | ...       |
| —   | RUNFTP  | %BANK ... |

Bottom █

F3=Exit    F6=Add new    F8=Print    F11=Un/Fold    F12=Cancel

### Work with Command Exceptions

| Parameter or Option | Description                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| Opt                 | <b>1</b> = Select this rule for modification<br><b>3</b> = Copy this rule for another user<br><b>4</b> = Delete this rule |

4. Press **Enter** to return to the **Native OS/400 Object Security** menu.

## Modify Command Exception

Modify Command Exception

Command . . . TEST

Define user authority, press Enter.  
Y=Yes

| User Group/<br>User* | Cmd | FTP /<br>RExec | DDM |
|----------------------|-----|----------------|-----|
| *PUBLIC              | Y   | Y              | -   |
| SPCLAUTH             | Y   | Y              | -   |
| RUNFTP               | -   | Y              | -   |
| █                    | -   | -              | -   |
|                      | -   | -              | -   |
|                      | -   | -              | -   |
|                      | -   | -              | -   |
|                      | -   | -              | -   |
|                      | -   | -              | -   |
|                      | -   | -              | -   |

More...

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

### Modify Command Exception

Define permissions for one user profile, profile group or **Firewall** user group on each line. Use the **PageUp** and **PageDown** keys to scroll through a long list.

For each activity type, 'Y' = Activity allowed and **Blank** = Activity rejected. **\*Public** is the default rule for all users not explicitly covered by an object security rule. You should always make certain that the **\*Public** rule contains sufficient permissions to allow access to objects by ordinary users.

| Parameter or Option     | Description                                                               |
|-------------------------|---------------------------------------------------------------------------|
| <b>Command /Library</b> | Name and library path of the command(s) included in this rule             |
| <b>User/User Group</b>  | Enter user profile or press <b>F4</b> to select a user profile from list. |
| <b>Command</b>          | 'Y' = Users may execute OS/400 commands                                   |
| <b>FTP/RExec</b>        | 'Y' = Users may execute commands via FTP or RExec                         |
| <b>DDM</b>              | 'Y' = Users may execute commands via DDM                                  |

Press **Enter** to return to the **Native OS/400 Object Security** screen.

## Work with Pre-check Library Replacement

In case there are many libraries that require the same authorities, select option 61 to create one library of authorization rules to be applied to the list of libraries.

### Work with Pre-check Library Replacement

Type options, press Enter.

1=Select 4=Delete

Subset . . . \_\_\_\_\_

| Opt | Source Library | Target Library |
|-----|----------------|----------------|
| █   | A*             | REUT           |
| —   | B*             | AV1            |
| —   | C*             | CV             |
| —   | CCCC           | CVTPFXLS       |
| —   | DD*            | DLT#AUGS       |
| —   | DDDDDD         | YYYYYY         |
| —   | FFF            | BBB            |
| —   | ZZZZZZ         | ZION           |

Bottom

Use this screen to eliminate repetitive rules in cases where there is a set of libraries which require similar Native Object rules.

For testing purposes only, the check will be conducted on the Target Library.

F3=Exit F6=Add new F8=Print F12=Cancel

### Work with Pre-check Library Replacement

Press F6 to add a new library of rules. This will be the “Target Library”

### Add Pre-check Library Replacement

Type choices, press Enter.

Source Library . . . . . █ \_\_\_\_\_ Name, \*generic

Target Library . . . . . \_\_\_\_\_ Name, F4=Prompt

F3=Exit F4=Prompt F12=Cancel

### Add a new Target Library

Enter the “Source Library” of the objects you wish to apply the authorization rule. Enter a “Target Library” that will contain a single set of rules to be applied.



In the specific object screen (option 1-9) define the original rules to be applied through the “Target Library”.

The message will appear in the Firewall log as follows:

```

Additional Message Information System: S720
Message ID . . : GRE6051 Transaction : *REJECTED
Date sent . . : 27/04/10 Time sent : 17:20:43
Server . . . : Remote Command/Program Call
Decision level: OBJCT=Object authority Menu opt: 21
Operation mode: *FYI=For Your Information (action NOT performed). (or F6)

*RMISRV *FYI* Denied for QSECOFR to TZION/GSEPHDR *PGM. IP address 1.1.1.164.
Source library before Pre-check SMZ4.
The examined security rule was for object TZION/*ALL user *PUBLIC operation RUN.

F3=Exit F6=Modify decision rule F7=Add action F12=Cancel

```

## IFS Objects

To work with IFS Object Security:

1. Select **22** from the main menu. The **IFS Security** menu appears.
2. Select **1** from the **IFS Security** menu. The **Work with IFS Security** screen appears.
3. This screen lists all the IFS rules currently in effect. Type **1** to work with an existing rule or press **F6** to create a new rule.
4. Press **Enter** to return to the **IFS Security** menu.

**NOTE:** File names for IFS objects may be entered with upper or lower case letters.

Work with IFS Security

Type options, press Enter.  
 1=Select    3=Copy    4=Delete                      Subset . . . . \_\_\_\_\_

| Opt                                 | File System/Root Dir | Directory/File name | Users       |
|-------------------------------------|----------------------|---------------------|-------------|
| <input checked="" type="checkbox"/> | *ALL                 | *ALL                |             |
| -                                   | /                    | CD*                 |             |
| -                                   | qibm                 | *ALL                | JAVA    ... |
| -                                   | rami                 | rami.csv            | JAVA        |

Bottom

F3=Exit    F6=Add new    F8=Print    F11=Un/Fold    F12=Cancel

### Work with IFS Security

| Parameter or Option | Description                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b>          | <b>1</b> = Select this rule for modification<br><b>3</b> = Copy this rule for another user<br><b>4</b> = Delete this rule |
| <b>F6</b>           | Add new rule                                                                                                              |
| <b>F8</b>           | Print rules                                                                                                               |
| <b>Subset</b>       | Search a print file or library whose names contain the subset                                                             |

## Add/Modify IFS Security

```

Modify IFS Security

File System/Root Dir rami
Directory/File name rami.csv

Define user authority, press Enter.
Y=Yes
User Group/
User* Read Write Rename Delete Move
*PUBLIC
JAVA Y Y - Y -
█ - - - - -
 - - - - -
 - - - - -
 - - - - -
 - - - - -
 - - - - -
 - - - - -
 - - - - -
 - - - - -
More...

F3=Exit F4=Prompt F8=Print F9=Print File System F12=Cancel

```

## Modify IFS Security

Define permissions for one user profile, profile group or **Firewall** user group on each line. Use the **PageUp** and **PageDown** keys to scroll through a long list.

For each activity type, **'Y'** = Activity allowed and **Blank** = Activity rejected. **\*Public** is the default rule for all users not explicitly covered by an object security rule. You should always make certain that the **\*Public** rule contains sufficient permissions to allow access to objects by ordinary users.

| Parameter or Option    | Description                                                               |
|------------------------|---------------------------------------------------------------------------|
| <b>File System</b>     | Shows the IFS file system to which this rule applies                      |
| <b>Directory/File</b>  | Shows the file name(s) and directory path(s) included in this rule        |
| <b>User/User Group</b> | Enter user profile or press <b>F4</b> to select a user profile from list. |
| <b>Read</b>            | 'Y' = Users may read the specified file                                   |
| <b>Write</b>           | 'Y' = Users may write, edit or update the specified file                  |
| <b>Delete</b>          | 'Y' = Users may delete the specified file                                 |
| <b>Rename</b>          | 'Y' = Users may rename the specified file                                 |
| <b>Other</b>           | 'Y' = Users may perform other actions on the specified file.              |

Press **Enter** to return to the **Work with IFS Object Security** screen.

## Chapter 7: Logon Security

Logon security rules define logon attributes for specific combinations of IP addresses (or SNA names) and user profiles. In addition, logon security rules can control what a user is permitted to do subsequent to logon. For example:

- Modify a logon request by automatically assigning an alternate user profile having different, presumably more restrictive, permissions and authorities
- Assign different initial menus, current libraries and initial auto-run programs than those specified in the user profile (Telnet only)
- Rename Telnet terminal names to (and thereby the system job name) in order to facilitate easy tracking of remote access requests, real time auditing and **Action** proactive responses.
- Overriding default system settings to force the appearance of the sign-on screen.

**Logon security rules are available for the following server types:**

- Incoming FTP requests
- Outgoing FTP requests
- REXEC (Remote Command Execution)
- Telnet
- Sign-on requests via the Internet (WSG)
- Passthrough

Subsequent sections discuss the options and parameters for each individual rule type.

---

**NOTE:** *The **Security Level** parameter in the server security rule must be set to '9' (full) in order to enable logon security for the appropriate servers. Refer to*

---

---

*Chapter 3: for details.*

---

## Procedural Overview

The basic procedure for defining any of the logon security rules is similar. The following sections provide details and explanations regarding the specific parameters and definitions for each type of logon security rule.

3. Choose the logon type from the main menu.
  - Select **31** for FTP and REXEC
  - Select **32** for Telnet and Sign-on
  - Select **33** for Internet logon (WSG)
  - Select **34** Passthrough
4. Set definitions.
  - Each **Logon Security** menu follows the same principles. Select the definition you want to set. For example, in the **FTP/RExec Logon Security** screen, choose **1** for Incoming FTP, and **2** for Outgoing FTP. The appropriate **Work with Logon Security** screen appears. Refer to the appropriate rule type section for details of the screen.
  - Type **1** to select an existing rule for editing or press **F6** to create a new rule. The **Add/Modify** screen appears. The screen parameters and options are the same.
  - Enter modify the parameters for the appropriate rule type. Refer to the appropriate rule type section or for details and explanations regarding the screen and its parameters
  - Press **Enter** to confirm and return to the **Work with Logon Security** screen.
5. Choose your desired reporting (logs) option by selecting options **11** (and optionally **12** and **13**) for display logs
6. Press **Enter** to confirm and return to the main menu.

Basic options for screens are given in the table below.

| Option     | Description                                                                                                                                                                                                                                                                                                                               |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Opt</b> | <b>1</b> = Select this rule for modification<br><b>3</b> = Copy this rule for another user<br><b>4</b> = Delete this rule<br><b>5</b> = IP Range (WSG Only)<br><b>F6</b> = Add new rule<br><b>F8</b> = Print rules<br><b>F9</b> = Add new rule<br><b>F11</b> = Alternate view (changes display by reducing the amount of lines on screen) |

## FTP/REXEC (Incoming)

This server is called when clients make requests to connect to the AS/400 by FTP or REXEC server.

1. To set Logon security rules for FTP/REXEC, select **31. FTP/REXEC** from the main menu.
2. From the FTP/REXEC Logon Security screen, select option **1**. The **Work with FTP/REXEC Logon Security** screen appears.
3. To add a new rule, press **F6**. The **Add FTP/REXEC Logon User** screen appears (screen and parameters are the same as Modify FTP/REXEC Logon User, seen on the following page).
4. Set parameters according to the following table and press **Enter**. FTP rules are according to user and IP.

```

Work with FTP/REXEC Logon Security

Type options, press Enter.
 1=Select 3=Copy 4=Delete Subset
Opt User Group/User* IP addresses and authorities
 1 *PUBLIC *ALL-2
- %@NEWYORK *ALL-1
- %@ROME *ALL-2
- JOHN *ALL-2, 1.1.1.100-1

F3=Exit F6=Add new F8=Print F12=Cancel

Bottom

```

### Work with FTP/REXEC Logon Security

| Parameter or Option     | Description                                                                                          |
|-------------------------|------------------------------------------------------------------------------------------------------|
| <b>Opt</b>              | 1 = Select this rule for modification<br>3 = Copy this rule for another user<br>4 = Delete this rule |
| <b>F6</b>               | Add new rule                                                                                         |
| <b>F8</b>               | Print rules                                                                                          |
| <b>Subset</b>           | Search a user group/user or IP addresses/authorities whose names contain the subset                  |
| <b>User Group/ User</b> | User and/or user group for whom the rules are set                                                    |

**IP addresses and authorities**

1 = Allowed  
2 = Rejected  
3 = Alternative Sign-on (see *Alternative Logon* in the following table for more details)

Modify FTP/RExec Logon User

Type information, press Enter.

User . . . . . \*PUBLIC

1=\*ALLOW  
2=\*REJECT  
3=\*ALTLOGON

| IP Address | Subnet Mask |   | Text |
|------------|-------------|---|------|
| *ALL       | 0.0.0.0     | 1 | TT   |
|            |             | - |      |
|            |             | - |      |
|            |             | - |      |
|            |             | - |      |

More...

For \*ALTLOGON (alternative logon):

|                         |         |                                |
|-------------------------|---------|--------------------------------|
| Validation password . . | *PGM    | Password, *NOCHK, *SYS, *PGM   |
| Alt User . . . . .      | *SAME   | Name, *SAME, F4 for list       |
| Alt Password . . . . .  | *PGM    | Password, *SAME, *BYPASS, *PGM |
| Alt Current library . . | *USRPRF | Library, *USRPRF               |

F3=Exit F4=Prompt F10=Additional parameters F11=Alt.view F12=Cancel

**Modify FTP/RExec Logon User**

| Parameter              | Description                                                                                                                                                                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User                   | Enter the user profile                                                                                                                                                                                                                                                                |
| IP Address/Subnet Mask | Enter IP address and subnet mask in decimal format. You must enter the IPs from which you allow this user to access or be denied FTP to your AS/400.<br><b>TIP:</b> Press <b>F4</b> and select the subnet mask from a list.                                                           |
| Logon                  | 1 = Allow logon request<br>2 = Reject logon request<br>3 = Sign-on automatically if permitted by System i configuration                                                                                                                                                               |
| Time group             | Enter time group name or press <b>F4</b> to select from list.                                                                                                                                                                                                                         |
| Text                   | Enter descriptive text                                                                                                                                                                                                                                                                |
| Alternative Logon      | The user can access FTP from this IP but without the usual authorities. He will be changed into an “alternative” (shadow) user with limited capabilities. This “alternative” user needs to be configured in advance ( <i>CRTUSRPRF</i> ). This is done without that user’s knowledge. |
| Validation Password    | This is the password used to validate the incoming user profile.<br><b>Password</b> = Type the password that is to be required for sign-on<br><b>*NOCHK</b> = password is not checked                                                                                                 |



|                            |                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | <p><b>*SYS</b> = Validation performed according to password in user profile</p> <p><b>*PGM</b> = Use password presented by calling program</p>                                                                                                                                                                                                                                          |
| <b>Alt User</b>            | Automatically sign-on with specified replacement user profile                                                                                                                                                                                                                                                                                                                           |
| <b>Alt Password</b>        | <p>This is the password to be assigned to the alternate user. Use the specified password for logon instead of that in the user profile</p> <p><b>*Same or Blank</b> = Do not replace password for alternate user</p> <p><b>*BYPASS</b> = Bypass password validation at sign-on for alternate user</p> <p><b>*PGM</b> = Use password presented by calling program for alternate user</p> |
| <b>Alt Current Library</b> | Automatically replace the default current library with specified library                                                                                                                                                                                                                                                                                                                |

## Client FTP (Outgoing)

This server is used when the AS/400 issues FTP (sub) commands as a client to another system.

1. To work with Client FTP Security, select **2. Client FTP (Outgoing)** from the **FTP/REXEC Logon Security** screen. The **Work with Client FTP Security** screen appears.
2. Set parameters according to the following table and press **Enter**. Select **F6** to add a new rule or option **1** to modify.

```

Work with Client FTP Security

Type options, press Enter.
 1=Select 3=Copy 4=Delete Subset
Opt User Group/User* Outgoing IP addresses and authorities
 █ *PUBLIC *ALL-2
 _ QSECOFR *ALL-2, 192.168.100.100-2

F3=Exit F6=Add new F8=Print F12=Cancel Bottom

```

### Work with Client FTP Security

```

 Modify FTP Client User

Type information, press Enter.
User *PUBLIC

Outgoing 1=Allow
IP Address Subnet Mask 2=Reject Text

ALL 0.0.0.0 1
1.1.1.1 255.255.255.255 1 Headquarters

More...

F3=Exit F4=Prompt F11=Alternate view F12=Cancel

```

| Parameter                       | Description                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User                            | Enter the user profile                                                                                                                                                                                                                |
| Outgoing IP Address/Subnet Mask | Enter the outside system IP address and subnet mask in decimal format. Enter which IPs this user can connect to and which are to be rejected from your AS/400.<br><b>TIP:</b> Press <b>F4</b> and select the subnet mask from a list. |
| Allow/Reject                    | <b>1</b> = Allow logon request<br><b>2</b> = Reject logon request                                                                                                                                                                     |
| Text                            | Enter descriptive text                                                                                                                                                                                                                |

## Telnet and Sign-on

This logon control manages two features

| Option                               | Description                                                                                                                                                                                                                              |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Telnet Logon (option 1)</b>       | Auto Sign-on configuration as well as IP address and password type restrictions. This entry is used only on the first time a device connects the system (for example, when PC emulation software starts).                                |
| <b>Sign-on Validation (option 5)</b> | Sign-on configurations per user with IP, terminal name, and number-of-sessions restrictions.<br>This entry is used for each time a user attempts Sign-On from the Telnet server (for example, when the "Enter Password" screen is used). |

## Telnet Logon

- To work with Telnet and Sign-on, select **32. Telnet** from the **Firewall Main** menu. The **Telnet Security** screen appears.

GSTELMNU
Telnet Security
Firewall  
System: S720

Select one of the following:

**Definitions**

1. Telnet Logon  
This entry is used only on the first time a device connects the system.  
For example, when a PC emulation software starts.  
To control the Sign On screen (which might be used several times during a single Telnet session), use Work with Users to specify allowed IPs and device names.

**Reporting**

11. Display Telnet Log  
12. Display Telnet Logon Log  
13. Display Telnet Termination Log

15. Display SIGNON Log

Selection or command  
==>

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

## Telnet Security

- Select **1. Telnet Logon** from the Telnet Security screen. The **Work with TELNET Logon Security** screen appears.

Work with TELNET Logon Security

Type options, press Enter.

1=Select 3=Copy 4=Delete 5=IP range

Subset . . .

| Opt | IP Address | Subnet Mask   | Incoming Terminal | Min pvd | Logon       | Assigned Terminal |
|-----|------------|---------------|-------------------|---------|-------------|-------------------|
| 1   | *ALL       | 0.0.0.0       | *ALL              | 0       | *ACCEPT     | *SAME             |
| 2   | 1.2.3.4    | 255.255.255.0 | *ALL              | 0       | *AUTOSIGNON | *SAME             |
| 3   | 1.2.5.6    | 128.0.0.0     | *ALL              | 0       | *AUTOSIGNON | *SAME             |
| 4   | 1.5.5.3    | 252.0.0.0     | *ALL              | 0       | *AUTOSIGNON | *SAME             |
| 5   | 1.5.6.3    | 240.0.0.0     | *ALL              | 0       | *REJECT     | *SAME             |
| 6   | 9.9.9.0    | 255.255.255.0 | *ALL              | 0       | *ACCEPT     | ITIP#*            |

Bottom

F3=Exit F5=Refresh F6=Add new F8=Print F12=Cancel

### Work with Telnet Logon Security

- Set parameters according to the following table and press **Enter**. Select **F6** to add a new rule or option **1** to modify.

Modify TELNET Logon Security setting

Type information, press Enter.

Selection criteria:

IP Address . . . . . \*ALL Address, F4 for list

Subnet mask . . . . . 0.0.0.0 F4 for list

Incoming terminal name \*ALL Name, generic\*, \*ALL, F4 for list

Minimum pvd validation 0 0=No password, 1=With password

Process:

Time group . . . . . 2=Encrypted pvd, 3=Connection SSL

Logon . . . . . 1 Name, F4 for list

For \*ACCEPT/\*AUTOSIGNON/\*FRCSIGNON Logon:

Assign terminal name . \*SAME 1=\*ACCEPT, 2=\*REJECT, 3=\*AUTOSIGNON

Set new Code page . . . 4=\*FRCSIGNON

Character set . . . Generic\*, \*SAME, \*SYSTEM, F4=List

Keyboard layout . . .

For \*AUTOSIGNON Logon:

Alt User . . . . . Name, \*SAME, F4 for list

Alt Current library . . Name, \*SAME

Alt Program to call . . Name, \*SAME

Alt Initial Menu . . . Name, \*SAME

F3=Exit F4=Prompt F12=Cancel

### Modify Telnet Logon Security Setting

| Parameter                     | Description                                                                                                                                                                                                                                                               |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP Address/Subnet Mask</b> | IP address and subnet mask in decimal format.<br><b>TIP:</b> Press <b>F4</b> and select the subnet mask from a list.                                                                                                                                                      |
| <b>Incoming Terminal Name</b> | Terminal name assigned by the System i or emulation software                                                                                                                                                                                                              |
| <b>Minimum Pwd Validation</b> | This is the method used to validate the incoming user profile.<br>Apply rule according to password validation level:<br><b>0</b> = No password validation<br><b>1</b> = Use password<br><b>2</b> = Use encrypted password<br><b>3</b> = Connection is using SSL           |
| <b>Time group</b>             | Enter time group name or press <b>F4</b> to select from list.                                                                                                                                                                                                             |
| <b>Logon</b>                  | <b>1</b> = Accept logon request<br><b>2</b> = Reject logon request<br><b>3</b> = Sign-on automatically if permitted by System i configuration<br><b>4</b> = Force sign-on even if System i is configured for automatic sign-on                                            |
| <b>Assigned terminal name</b> | Enter the name to optionally replace the incoming terminal name<br><b>Generic*</b> = Text before "*" plus sequentially assigned number<br><b>*SAME</b> or <b>Blank</b> = Do not replace the income terminal name<br><b>*SYSTEM</b> = Use terminal name assigned by OS/400 |
| <b>Set new</b>                | Define Code page, Character set and Keyboard layout                                                                                                                                                                                                                       |
| <b>Alt User</b>               | Automatically sign-on with specified replacement user profile                                                                                                                                                                                                             |
| <b>Alt Current Library</b>    | Automatically replace the default current library with specified library                                                                                                                                                                                                  |
| <b>Alt Program</b>            | Automatically replace the default program to be run at sign-on                                                                                                                                                                                                            |
| <b>Alt Initial menu</b>       | Automatically replace the default initial user menu at sign-on                                                                                                                                                                                                            |

## SSL Control in Firewall

**Firewall** can be set up to request SSL on Telnet and FTP session, based on the IP or User.

To set up SSL control in **Firewall**, follow this procedure.

1. Select **32. Telnet** from the **Firewall** main menu. The **Telnet Security** screen appears.
2. Select **1. Telnet Logon** to access the **Work with TELNET Logon Security** screen.
3. Press **F6** to access the **Add TELNET Logon Security Setting** screen.

## Sign-on

**Firewall** Telnet Sign-on feature enables limiting a user to sign-on from a specific IP or terminal name (for each sign-on), as well as limiting the number of sessions the user will be allowed to work in.

To work with sign-on security, select **15. Display SIGNON Log** from the **Telnet Security** screen.

1. Set the parameters and press **Enter**. The **Display Firewall Log** screen appears, with all the transactions that used the **Sign-On** server.

```

Display Firewall Log 22/01/07 - 22/01/07
█
*SIGNON *FYI* Denied for DAN from 192.168.1.6 in job 521311/DAN/QPADEV0002
*SIGNON *FYI* Denied for DAN from 192.168.1.6 in job 521312/DAN/QPADEV0002

Bottom
F3=Exit F6=Modify rule F7=Add action F10=Details F11=Single entry F12=Cancel
F17=Top F18=Bottom

```

### Display Firewall Log

2. Select **F10** for additional message information or **F6** to modify the rule.

```

Additional Message Information System: S720
█
Message ID : GRE6422 Transaction : *REJECTED
Date sent : 22/01/07 Time sent : 01:05:45
Server : Sign-On Completed
Decision taken on level: GSSGN=Signon logon
Operation mode : *FYI=For Your Information (action NOT performed)

*SIGNON *FYI* Denied for DAN from 192.168.1.6 in job 521311/DAN/QPADEV0002.
The rejection is based on security rule for IP Address.
The examined security rule was for user *PUBLIC IP *ALL subnet mask 0.0.0.0.

F3=Exit F6=Modify rule F7=Add action F12=Cancel

```

### Additional Message Information

```

Work with User Security

Type options, press Enter. (Read top->down)
1=Select 3=Copy 4=Delete 5=Members 6=Groups

-----Network Servers-----
F F F F R R R F O O C C C N N M S O T
I T T T E R M M I R R S S S P P S Q B C
L P P P X E T T L D D V L L D C C R R G L J P
T L S C L X S S N S S T T P I I D R N L E S S E I S
F O R L O E Q Q D R R A A R C C D D V N N P R N N G
R G V N G C L L B V V Q Q T M M M A M M T L V T F N

User
System Group
Opt %group
 *PUBLIC
 %FTP + V +
 %GGG +
 %JJJJ +
 %OOO +
 EDI + V +
 ELIH +
 LEO + V + V
 LUCAS + + + V +

More...

F3=Exit F6=Add user F7=Add group F8=Print list
*SIGNON Transaction for user DAN, IP 192.168.1.6 in job 521311/DAN/QPADE

```

### Work with User Security

3. Type **1=Select** to modify the rule

```

Modify User Security

User *PUBLIC

Type choices, press Enter.
Activity Time Time group, *NEVER
Use Group Authority . . . Y=Yes, N=No, blank=Default
Enable Services based also on OS/400 and %USER Group profiles

Authorities and Locations

2. Services FTP, SQL, NDB, DDM, ...
3. IP
4. Device Names SIGNON only
Selection ==>

In-product Special Object Authority
AS/400 Native. 3 1=*ALLOBJ, 2=*EXCLUDE, 3=*OBJAUT
IFS 3 1=*ALLOBJ, 2=*EXCLUDE, 3=*OBJAUT

F3=Exit F4=Prompt F8=Print
F9=Object security F10=Logon security F12=Cancel

```

### Modify User Security



## Work with Sign-on IP Validation

| Parameter               | Description                                                                                                          |
|-------------------------|----------------------------------------------------------------------------------------------------------------------|
| IP Address /Subnet Mask | IP address and subnet mask in decimal format.<br><b>TIP:</b> Press <b>F4</b> and select the subnet mask from a list. |
| Allow/Reject            | <b>1=ALLOW</b> = Allow logon request<br><b>2=REJECT</b> = Reject logon request                                       |
| Text                    | Descriptive text                                                                                                     |

- ## Chapter : Logon Security



```

Work with Sign-On Device Validation

User / Group *PUBLIC

Type information, press Enter.
Y=Yes

Device* Allow
*ALL █
_____ -
_____ -
_____ -
_____ -
_____ -
_____ -
_____ -
_____ -
_____ -
_____ -

F3=Exit F8=Print More...
F12=Cancel

*SIGNON Transaction for user DAN, IP 192.168.1.6 in job 521311/DAN/QPADE

```

### Work with Sign-on Device validation

#### Internet (WSG)

This server provides sign-on for client browser (such as Internet Explorer or Netscape Navigator) bypassing AS/400 sign-on panel.

1. To work with WSG logon security, select **33. Internet (WSG)** from the **Firewall Main** menu. The **Internet-WSG Logon Security** screen appears.
2. Select **1. Internet-WSG Logon**. The **Work with WSG Logon Security** screen appears.
3. Set parameters according to the following table and press **Enter**. Select **F6** to add a new rule or option **1** to modify.

Work with WSG Logon Security

Type options, press Enter.

1=Select    3=Copy    4=Delete    5=IP range

Subset . . . \_\_\_\_\_

To start a session from a Web browser specify:

1. On AS/400 - CHGWSGA DSPSGN(\*NO)

2. On Web browser - http://hostname:5061/WSG/QAPP0100

| Opt | IP Address | Subnet Mask | Logon User | AUTO-SIGNON PARAMETERS |      |         |
|-----|------------|-------------|------------|------------------------|------|---------|
|     |            |             |            | Program                | Menu | Library |
| █   | *ALL       | 0.0.0.0     |            |                        |      |         |

Bottom

F3=Exit    F5=Refresh    F6=Add new    F8=Print    F12=Cancel

### Work with WSG Logon Security

| Parameter or Option                                   | Description                                                                                                                                                                                             |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP Address and Subnet Mask</b>                     | IP address and subnet mask in decimal format.<br><b>TIP:</b> Press <b>F4</b> and select the subnet mask from a list.                                                                                    |
| <b>Logon</b>                                          | <b>Y</b> = Allow logon request and use auto-sign-on                                                                                                                                                     |
| <b>User</b>                                           | User profile                                                                                                                                                                                            |
| <b>Auto-Sign-on Parameters (only if Logon is yes)</b> | <b>Program</b> = initial program to be called upon sign-on<br><b>Menu</b> = menu to be called upon sign-on that will initialize the screen<br><b>Library</b> = first library to be checked upon sign-on |

```

Modify WSG Logon Security Setting

Type information, press Enter.

IP Address 1.0.0.1 Address, F4 for list
Subnet mask 255.255.255.255 F4 for list

Time group _____ Name, F4 for list

Logon Y Y=Yes

Auto-signon parameters for Logon=Yes
User JOHN Name, F4 for list
Password ***** Password, *PGM
Program _____ Program
Menu _____ Menu
Current library _____ Library

F3=Exit F4=Prompt F12=Cancel

```

### Modify WSG Logon Security Setting

| Parameter                          | Description                                                                                                                                                                                                                        |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP Address/Subnet Mask</b>      | IP address and subnet mask in decimal format.                                                                                                                                                                                      |
| <b>Time group</b>                  | Enter time group name or press <b>F4</b> to select from list.                                                                                                                                                                      |
| <b>Logon</b>                       | <b>Y</b> = Allow logon request and use auto-sign-on<br><b>Blank</b> = Reject logon request                                                                                                                                         |
| <b>User (only if Logon is yes)</b> | Automatically performs sign-on with specified replacement user profile                                                                                                                                                             |
| <b>Password</b>                    | Requires the specified password for logon instead of the password in the user profile (This is the password to be assigned to the "alternate" user).<br><b>*PGM</b> = Use password presented by calling program for alternate user |
| <b>Program</b>                     | Automatically replace the default program to be run at sign-on                                                                                                                                                                     |
| <b>Initial menu</b>                | Automatically replace the default initial user menu at sign-on                                                                                                                                                                     |
| <b>Current Library</b>             | Automatically replace the default current library with specified library                                                                                                                                                           |

**NOTE:** To work with WSG security, select **11. Display WSG Logon Log** from the **Internet-WSG Logon Security** screen.

## Passthrough

This server specifies how the outside systems handle remote sign-on requests. It may alter sign-on information

1. To work with Passthrough security, select **34. Passthrough** from the **Firewall** main menu. The Passthrough Security screen appears.
2. Select **1. Passthrough Logon**. The **Work with Passthrough Security** screen appears.
3. Set parameters according to the following table and press **Enter**. Select **F6** to add a new rule or option **1** to modify.

```

Work with Passthrough Security

Type options, press Enter.
 1=Select 3=Copy 4=Delete

Source Source Target Automatic
Opt System User* User Sign-on
 █ *ALL *ALL *ANY *REJECT
 - *ALL *ALL *SAME *REJECT
 - *ALL *ALL JOHN *ALLOW

F3=Exit F6=Add new F8=Print F12=Cancel

Bottom

```

### Work with Passthrough Security

| Parameter or Option      | Description                                                                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source System</b>     | SNA system name of the source (incoming) computer                                                                                                                                                                      |
| <b>Source User</b>       | User profile of the source system                                                                                                                                                                                      |
| <b>Target User</b>       | User profile for logon at the target system                                                                                                                                                                            |
| <b>Automatic Sign-on</b> | <b>1</b> = Accept logon request<br><b>2</b> = Reject logon request<br><b>3</b> = Force sign-on even if System i is configured for automatic sign-on<br><b>4</b> = Sign-on automatically with an alternate user profile |

```

Modify Passthrough Security

Type choices, press Enter.

Source system *ALL Name, *ALL
Source user *ALL Name, generic*, *ALL
Target user JOHN Name, *SAME, *ANY, F4 for list

Time group Name, F4 for list

Automatic sign-on 1 1=*ALLOW
 2=*REJECT
 3=*FRCSIGNON
 4=*ALTLOGON

Automatic sign-on parameters for *ALTLOGON:
User profile Name, F4 for list
Initial program
Initial menu
Current library

F3=Exit F4=Prompt F12=Cancel

```

### Modify Passthrough Security

| Parameter                | Description                                                                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source System</b>     | SNA system name of the source (incoming) computer                                                                                                                                                                      |
| <b>Source User</b>       | User profile at the source system<br><b>Generic*</b> = Any user profile beginning with the text before the '*'<br><b>*ALL</b> = All users                                                                              |
| <b>Target user</b>       | User profile for logon at the target system<br><b>*SAME</b> = Use the source user profile<br><b>Generic*</b> = Any user profile beginning with the text before the '*'                                                 |
| <b>Time group</b>        | Enter time group name or press <b>F4</b> to select from list.                                                                                                                                                          |
| <b>Automatic Sign-on</b> | <b>1</b> = Accept logon request<br><b>2</b> = Reject logon request<br><b>3</b> = Force sign-on even if System i is configured for automatic sign-on<br><b>4</b> = Sign-on automatically with an alternate user profile |
| <b>User Profiler</b>     | Automatically sign-on with specified replacement user profile                                                                                                                                                          |
| <b>Initial Program</b>   | Automatically replace the default program to be run at sign-on                                                                                                                                                         |
| <b>Initial menu</b>      | Automatically replace the default initial user menu at sign-on                                                                                                                                                         |
| <b>Current Library</b>   | Automatically replace the default current library with specified library                                                                                                                                               |

**NOTE:** To work with Passthrough security, select **11. Display Passthrough Logon Log** from the **Passthrough Security** screen.

## Chapter 8: Queries, Reports and Logs

This chapter presents the reporting features that are built into **Firewall**. An effective security policy relies on queries and reports to provide traceability for system activity. All **Firewall** queries and reports work with data contained in the Activity Log.

**Firewall** offers several powerful, but user-friendly, tools that create output containing only relevant data, in a useful format. All of this can be accomplished without programming, with the following tools:

- **Query Wizard** - Selects the events that need to be audited using powerful filter criteria, and creates screen-based or printed reports that present the data in a customized format
- **Activity Log** - Displays or prints the contents of the **Firewall** Activity Log quickly and easily in a standard format using basic filter criteria
- **Report Scheduler** - Automatically runs queries and reports at user-specified times

In addition to these tools, **Firewall** contains with over 100 predefined reports and queries that are ready to run at any time. All reporting features are available via the **Reporting** menu. To access this menu, select **43. Log, Reports, Queries** from the main menu.

```

GSRPTMNU Reporting Firewall
 (Including HTML, PDF, CSV, Outfile->GUI) System: S720
Select one of the following:

Query Wizard Report Scheduler
 1. Work with Queries 51. Work with Report Scheduler
 2. Run a Query 52. Run a Report Group

Log Other reports
 11. Display Log 61. Activity Statistics
 19. Select from Menu 62. User Activity Statistics
 65. Product Settings

Reporting Aids System for Reporting
 41. Group Items for Selection 71. Change System for Reporting
 49. Time Groups 72. Systems Available in Real Time

Selection or command
===> █

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

```

### Reporting

In addition, the Activity Log display feature is available directly from several screens throughout **Firewall** as well as by using the **DSPFWLOG** command from any command line.

### Query Wizard

The powerful Query Wizard allows you to design custom output reports that show only the necessary data, without programming and with no requirement for technical knowledge.

Query definitions are created by using a series of simple parameter definition screens. Output can be a printed report, a screen display or a text file saved on the System i.

Highly detailed filter criteria enable selection of only the required records using Boolean operators, as well as the ability to combine logical conditions. You have full flexibility to specify the sort order according to multiple fields.

The wizard allows you to output only the relevant data fields and to specify the order in which they appear on the report. You can design tabular summary reports showing one line for each record or detail reports showing record data on multiple lines.

## Procedural Overview

The procedure for defining queries consists of the following steps:

1. Select an existing query to work with or create a new query.
2. Define general query parameters specifying the activity type(s) to be included and the output format.
3. Define the record selection (filter) criteria.
4. Select the data fields to be included in the report and the order in which they appear.
5. Define the record sort criteria according to one or more data fields.
6. Run the query with the option to specify additional run-time filter criteria.

## Working with Queries

1. To work with queries, select **1** from the **Reporting** menu. The **Work with Queries** screen appears.
2. Type the desired option next to a query. Type **1** to modify a query, **3** to copy or press **F6** to create a new query.
3. Press **Enter** to proceed to the definition screens.

Work with Queries

Position to . . . \_\_\_\_\_  
 Subset . . . . . \_\_\_\_\_

Type options, press Enter.

1=Select 3=Copy 4=Delete 5=Run 6=Print 7=Rename 8=Run as batch job

| Opt                                 | Query      | Server | Description                           |
|-------------------------------------|------------|--------|---------------------------------------|
| <input checked="" type="checkbox"/> | Z6IPOUT    | 00     | *Firewall* Outgoing IP addresses      |
| <input type="checkbox"/>            | Z6LICMGT   | 00     | *Firewall* License Management         |
| <input type="checkbox"/>            | Z6NATIVE   | 00     | *Firewall* Native                     |
| <input type="checkbox"/>            | Z6REJECTS  | 00     | *Firewall* Rejects                    |
| <input type="checkbox"/>            | Z6RTMSRV   | 00     | *Firewall* Remote Server              |
| <input type="checkbox"/>            | Z6SNA      | 00     | *Firewall* SNA                        |
| <input type="checkbox"/>            | Z6SQL      | 00     | *Firewall SQL*                        |
| <input type="checkbox"/>            | Z6SQLPIERR | 00     | *Firewall SQL*                        |
| <input type="checkbox"/>            | Z6USER     | 00     | *Firewall* User                       |
| <input type="checkbox"/>            | Z6USRACT   | 00     | *Firewall* User Activity              |
| <input type="checkbox"/>            | Z6USRPRF   | 00     | *Firewall* User Profile Modifications |

Bottom

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

### Work with Queries

| Option    | Description                                                                                                    |
|-----------|----------------------------------------------------------------------------------------------------------------|
| <b>F6</b> | Create a new query.                                                                                            |
| <b>1</b>  | Select a query for modification.                                                                               |
| <b>3</b>  | Copy a query. Type the new query name and description in the pop-up window and press <b>Enter</b> to continue. |
| <b>4</b>  | Delete a query. Press <b>Enter</b> to confirm deletion when the warning message appears.                       |
| <b>5</b>  | Run the selected query as an interactive job.                                                                  |
| <b>6</b>  | Print the selected query to the standard output device and file type ( <b>*PDF, *HTML, *CSV ...</b> )          |
| <b>7</b>  | Rename a query. Type the new query name in the pop-up window and press <b>Enter</b> .                          |
| <b>8</b>  | Run the selected query as a batch job.                                                                         |

This screen contains several basic query definition parameters.

- ```

Modify Query

Type choices, press Enter.

Query name . . . . . Z6IPOUT
Description . . . . . *Firewall* Outgoing IP addresses
_____
Query type . . . . . 1                1=All servers -or- Single server
                                           2=List of servers (selected later)
If query type=1
  Server Id (00=All) . 00 Generic entry type (00-99)

Restrict to subject . *IPOUT
                      _____
                      Not Name

Time group . . . . . _____ N=Not included in time group
Output format . . . . 1          1=Tabular, 2=Tabular (no fold), 9=Log
If format=1 in print
  Continue vertically 0          Field number, 0=*AUTO
Add Header / Total . 1          1=Both, 2=Header, 3=Total, 9=None
Sort . . . . . 1              1=By all fields, 2=By header, 3=No sort
_____

F3=Exit                F8=Print                F12=Cancel

```

Modify Query

| Parameter or Option | Description |
|----------------------|--|
| Query Name | Name of query |
| Description | Free text query description |
| Query Type | 1 = Single server type query or all servers
2 = Multiple server types to be selected on a subsequent screen.
(see below) |
| Not | N = Select records not included in the specified time group
(Exclusive)
Blank = Select records included in the specified time group
(Inclusive) |
| Time Group | Name = Enter the name of the time group to use as a filter
Blank = Do not use a time group |
| Output Format | 1 = Detailed tabular format with option for multi-line field display (Fold)
2 = Summary tabular format – one line per record
9 = Log display output format |
| Sort Options | 1 = Sort using all log record fields
2 = Sort using only generic fields
3 = No sorting (time sequence) |

- When defining a multiple server type query, it is necessary to select the server types and to define record selection criteria parameters separately for each server type. When the **Query Type** field is set to **2**, the following screen automatically appears, allowing you to add and work with server types.

NOTE: *In Multiple server type queries, you can only display the fields that are common to all server types. You must use a single server type query to display the fields which are specific to a particular server type.*

- Press **Enter** from the **Modify Query** screen to add a server type **or** select an existing filter type to modify. You may add the same server type more than once with different record selection criteria. The **Filter Conditions** screen appears immediately afterwards.

You may include multiple filter conditions in your definition. Each filter condition consists of a comparison test applied to one of the fields in the Activity Log record.

Define filter criteria and press **Enter**.

NOTE: *Filter conditions are optional. If no filter conditions are defined, your query will include all events for the specified audit type or types.*

Filter Conditions

Server 04 *SQL Database Server - SQL access

Sequence 1.0

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

Tests: EQ, NE, LE, GE, LT, GT, LIST, NLIST, LIKE, NLIKE, ITEM, NITEM, START

For LIKE, NLIKE use % as "any string".

| And | Or | Field | Test | Value |
|-----|----|-------------------|------------------|-------------|
| | | Date & Time | yyyy-mm-dd-hh.mm | |
| | | Time | hh.mm.ss | |
| | | Name of job | | |
| | | User of job | | |
| | | Number of job | | |
| | | User profile name | EQ | JOHN |
| | | System name | LIST | \$720 \$150 |
| | | Object | START | PAYROLL |
| | | Object library | | |
| | | Object type | | |
| | | User | | |

More...

F3=Exit F4=Prompt F6=Insert F12=Cancel

Filter Conditions

| Parameter or Option | Description |
|---------------------|--|
| And/Or | A or Blank = And O = Or |
| Field | Data field in the Activity Log |
| Test | Comparison test type – see table on following page for details |
| Value | Value to be used as the comparison test |
| 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 |

Comparison Test Operators

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 % |
| ITME, 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 | *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 |

| Test | Description | Value Field Data |
|--------------|-------------|---|
| | new types. | 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 | Starting characters of string |

And/Or Boolean Operators

You may combine multiple filter conditions in one query using Boolean AND/OR operators. This allows you to create complex queries that produce precise results.

When using ‘Or’ operators in your filter conditions, the order in which each condition appears in the list conditions is critical. The ‘Or’ operator allows you to group several conditions together because it includes all the ‘And’ conditions that follow it until the next ‘Or’ operator or until the end of the list.

The following example illustrates this principle. This query 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.

Filter Conditions

Server 04 *SQL Database Server - SQL access
 Sequence 1.0
 Type conditions, press Enter. Specify OR to start each new group.
 Tests: EQ, NE, LE, GE, LT, GT, LIST, NLIST, LIKE, NLIKE, ITEM, NITEM, START
 For LIKE, NLIKE use % as "any string".

| <p>Group 1</p> <p>Group 2</p> | <p>And</p> <p>Or</p> | <table border="0"> <tr> <th style="text-align: left;">Field</th> <th style="text-align: left;">Test</th> <th style="text-align: left;">Value</th> </tr> <tr> <td>Time hh.mm.ss</td> <td>LT</td> <td>20.30.00</td> </tr> <tr> <td>User profile name</td> <td>EQ</td> <td>JOHN</td> </tr> <tr> <td>System name</td> <td>LIST</td> <td>S720 S150</td> </tr> <tr> <td>Object</td> <td>START</td> <td>PAYROLL</td> </tr> <tr> <td>Date & Time yyyy-mm-dd-hh.mm</td> <td></td> <td></td> </tr> <tr> <td>Time hh.mm.ss</td> <td></td> <td></td> </tr> <tr> <td>Name of job</td> <td></td> <td></td> </tr> <tr> <td>User of job</td> <td></td> <td></td> </tr> <tr> <td>Number of job</td> <td></td> <td></td> </tr> <tr> <td>User profile name</td> <td></td> <td></td> </tr> <tr> <td>System name</td> <td></td> <td></td> </tr> </table> | Field | Test | Value | Time hh.mm.ss | LT | 20.30.00 | User profile name | EQ | JOHN | System name | LIST | S720 S150 | Object | START | PAYROLL | Date & Time yyyy-mm-dd-hh.mm | | | Time hh.mm.ss | | | Name of job | | | User of job | | | Number of job | | | User profile name | | | System name | | | <p>More...</p> |
|-------------------------------|----------------------|---|-------|------|-------|---------------|----|----------|-------------------|----|------|-------------|------|-----------|--------|-------|---------|------------------------------|--|--|---------------|--|--|-------------|--|--|-------------|--|--|---------------|--|--|-------------------|--|--|-------------|--|--|----------------|
| Field | Test | Value | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Time hh.mm.ss | LT | 20.30.00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| User profile name | EQ | JOHN | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System name | LIST | S720 S150 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Object | START | PAYROLL | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Date & Time yyyy-mm-dd-hh.mm | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Time hh.mm.ss | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Name of job | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| User of job | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Number of job | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| User profile name | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System name | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

F3=Exit F4=Prompt F6=Insert F12=Cancel

Filter Conditions

Defining Output Fields

The **Select Output Fields** screen allows selection of the fields from the Activity Log that will appear in the query output as well as the order in which they should appear from left to right. Fields appear in ascending order on the screen, with the top field corresponding to the left-hand field in the query report. The second field corresponds to the field located to the right of the left-hand field, and so on.

The user can change the order of the fields simply by modifying the sequence numbers. Any field can be deleted from the query report by deleting the sequence number. When pressing **Enter**, the new field sequence appears on the screen, with deleted (blank sequence number) fields appearing at the bottom.

You must select at least one field for output.

Fields shown in pink are part of the generic header and are common to the Activity Log record for all audit types. Fields shown in **green** (on the screen) are specific to the Activity Log record for the currently selected audit type only.

Select Output Fields

Query Z6LICMGT *Firewall* License Management
Type 00 Generic entry type (00-99)

Type choices, press Enter.

| Seq. | Description | Attribute |
|---|----------------------------------|-----------|
| <input checked="" type="checkbox"/> 1.0 | Allowed / Rejected | 1 A |
| <input type="checkbox"/> 2.0 | *FYI mode (simulation) | 1 A |
| <input type="checkbox"/> 3.0 | User profile name | 10 A |
| <input type="checkbox"/> 4.0 | Product Id (for license request) | 10 A |
| <input type="checkbox"/> 5.0 | Feature Id (for license request) | 10 A |
| <input type="checkbox"/> 6.0 | Function | 10 A |
| <input type="checkbox"/> 7.0 | Decision level | 5 A |
| <input type="checkbox"/> | Server name | 10 A |
| <input type="checkbox"/> | Name of job | 10 A |
| <input type="checkbox"/> | User of job | 10 A |
| <input type="checkbox"/> | Number of job | 6 A |

More...

F3=Exit F5=Display values F12=Cancel F21=Select all F23=Invert selection

Select Output Fields

| Option | Description |
|-------------|--|
| F5 | Displays field values |
| F21 | Selects all options |
| F23 | Invert selection – All selected items will be deselected and all items that are not selected will become selected
NOTE: You may wish to change the sequence numbers after using this command. |
| Seq. | Enter the sequence in which you wish this field to appear in the query output. Lower numbers appear toward the left and higher numbers appear toward the right. |

Sort Criteria

You may sort records in your query output according to any combination of fields in the Activity Log record. The lowest sequence number (normally 1.0) represents the primary sort field. The second lowest number (normally 2.0) represents the secondary sort field, and so on.

Fields shown in **pink** are part of the generic header and are common to the Activity Log record for all audit types. Fields appearing in **green** (on the screen) are specific to the Activity Log record for the currently selected audit type.

```

Select Sort Fields

Query . . . . . Z6LICMGT  *Firewall* License Management
Type  . . . . . 00       Generic entry type (00-99)

Type choices, press Enter.

Seq.  Description                                     Attribute
 1    Server name                                     10 A
 2    Function                                         10 A
 3    Allowed / Rejected                             1 A
 4    *FYI mode (simulation)                         1 A
 5    Decision level                                 5 A
 6    Name of job                                    10 A
 7    User of job                                    10 A
 8    Number of job                                  6 A
 9    User profile name                             10 A
10    Object                                           10 A
11    Object library                                 10 A
More...

F3=Exit  F5=Display values  F12=Cancel  F21=Select all  F23=Invert selection

```

Select Sort Fields

| Parameter or Option | Description |
|---------------------|--|
| F5 | Displays field values |
| F21 | Selects all options |
| F23 | Invert selection – All selected items will be deselected and all items that are not selected will become selected
NOTE: You may wish to change the sequence numbers after using this command. |
| Seq. | Enter a number representing the sort sequence |

Running Queries

The final screen in the definition procedure allows you to run your query immediately. If you do not wish to run your query at this time, press **F3** to exit. All query definition parameters will be preserved.

Firewall provides you with several different options for running queries:

- **During Query Definition** – You can run queries as the final step in the definition procedure. This is useful for testing and debugging queries.
- **Work with Queries Screen** – Run a query by typing **5** to the left of one or more queries in the list. This option is especially useful for running several queries sequentially.
- **Report Scheduler** – This powerful feature automatically runs queries according to a pre-defined schedule. This option is typically used for generating periodic audit reports.
- **Query Menu** – Select one of the following options from the **Query** menu:
 - **11. Display** – Display query results on the screen
 - **12. Print** – Print a hard copy of the query as an interactive job
 - **13. Submit as Batch Job** – Submit the query as a batch job. This is recommended for large, resource intensive queries.
- **Command Line** – Enter the Run Firewall Query command (**RUNFWQRY**) from any command line. This allows you to run a query at any time, even if you are working on other tasks.
- **Display Log** – Queries can also be used to filter data when viewing Activity Log data. This is useful for applying sophisticated filter criteria that are unavailable with the display log command.

You may specify **run-time filter criteria** that apply only to the current instance of the query. Run-time filter criteria allow you to display or print only a **subset** of the data extracted by the query definition. For example, if your query definition does not filter records according to user profile, you may specify run-time criteria that will display activity only for specific user.

However, run-time filter criteria will not return data that is excluded from the actual query definition. For example, if your query definition includes filter criteria only for the user profile **JOHNKERRY** and you enter run-time criteria for the user **GEORGEW**, no events will be displayed.

The procedure for running queries is virtually identical for all of the above options. Each method involves entering several run-time parameters on the **Run Audit Query** screen.

Run Firewall Query (RUNFWQRY)

Type choices, press Enter.

| | | |
|----------------------------------|----------|--------------------------------|
| Query | > Z6IFS | Name, *SELECT |
| Display last minutes | *BYTIME | Number, *BYTIME |
| Starting date and time: | | |
| Starting date | *CURRENT | Date, *CURRENT, *YESTERDAY... |
| Starting time | 000000 | Time |
| Ending date and time: | | |
| Ending date | *CURRENT | Date, *CURRENT, *YESTERDAY... |
| Ending time | 235959 | Time |
| User* or '%GROUP' | *ALL | |
| System to run for | *CURRENT | Name, *CURRENT, *group, *ALL.. |
| Number of records to process . . | *NOMAX | Number, *NOMAX |
| Output | > *PRINT | *, *PRINT, *PDF, *HTML.. |
| Print format | *SHORT | *SHORT, *FULL |

More...

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

Run Firewall Query

| Parameter or Option | Description |
|--|--|
| Query | Name = Name of Query
*SELECT = Select from list at run time |
| Display Last Minutes | Select only the records occurring within the previous number of minutes as specified by the user
Number = Enter the number of minutes
*BYTIME = According the starting and ending time specified below |
| Starting Date & Time
Ending Date & Time | Select only the records occurring within the range specified by the start and end date/time combination.
Date or Time = Enter the appropriate date or time
*CURRENT = Today (Current Date)
*YESTERDAY = Previous date
*WEEKSTR/*PRVWEEKS = Current week/Previous week start
*MONTHSTR/ *PRVMONTH = Current month/Previous month start
*YEARSTR/ *PRVYEARS = Current year/ Previous year start
*SUN -*SAT = Day of week |
| Type | Filter records by audit type
*All = All types as specified in the query definition
F4 = Select server type from a list |
| User* or '%Group' | Filter records by a user profile or group name |
| System to run for | The system to report information from
*CURRENT = the current system
*Name = a group of systems as defined in STRAUD, 83, 1
*ALL = all the systems defined in STRAUD, 83, 1 |
| Job Name - User | Filter records by OS/400 job name. |
| Job Name - Number | Filter records by OS/400 job number. |

| Parameter or Option | Description |
|--|---|
| Number of Records to Process | Maximum number of records to process
* NOMAX = No maximum (Default) |
| Output | * = Display
* Print = Printed report
* PDF = Print report to PDF outfile
* HTML = Print report to HTML outfile
* CSV = Print report to CSV outfile
* Outfile = Print report to view from the GUI |
| User Profile | Filter records by user |
| Filter by Time Group - Relationship | Filter records by time group
* IN = Include all records in time group
* OUT = Include all records not in time group
* NONE = Do not use time group, even if included in query definition
* QRY = Use time group as specified in query definition |
| Type | Filter records by audit type
* All = All types as specified in the query definition
F4 = Select server type from a list |
| Program Name | Filter records by the name of the program that created the journal record. |
| Filter by Time Group - Time Group | Name = Name of time group
* SELECT = Select time group from list at run time |

Press **Enter** to continue. You may press **F18** at any time during the data retrieval process to display a pop-up status window. This window continuously displays the number of records processed and selected. Press **Esc** at any time to halt retrieval and immediately display the query or log.

Print Query to Output File and Send Via Email

NOTE: To ensure you always receive iSecurity reports emails, please add DONOT@REPLY.COM and NOREPLY@ISECURITY.COM to your email contact list.

1. Select preferred **Output** file type (*PDF, *HTML, *CSV ...) and press **Enter**

```

Run Firewall Query (RUNFWQRY)

Type choices, press Enter.

Query . . . . . > Z6IFS      Name, *SELECT
Display last minutes . . . . . *BYTIME    Number, *BYTIME
Starting date and time:
  Starting date . . . . . *CURRENT    Date, *CURRENT, *YESTERDAY...
  Starting time . . . . . 000000      Time
Ending date and time:
  Ending date . . . . . *CURRENT    Date, *CURRENT, *YESTERDAY...
  Ending time . . . . . 235959      Time
User* or '%GROUP' . . . . . *ALL      Name, *CURRENT, *group, *ALL..
System to run for . . . . . *CURRENT    Number, *NOMAX
Number of records to process . . . . . *NOMAX
Output . . . . . > *PDF      *, *PRINT, *PDF, *HTML..
Object (*TEMP for attach only) *MAIL

More...

F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys
  
```

Run Firewall Query

2. Type ***MAIL** in the **Object** field, press **Page Down** and enter the email address you want the file to be sent to in the **Mail to** field.

```

Run Firewall Query (RUNFWQRY)

Type choices, press Enter.

Directory ('/dir/') . . . . . *DATE

Mail to (mail1,mail2,mail3..) . . . admin@razlee.com

Mail text . . . . .

+ for more values

Object size to allow attach . . . 4      Size in MB, *NO, *NOMAX
Delete if attached . . . . . *YES      *NO, *YES

Bottom

F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys
  
```

Run Firewall Query

3. Press **Enter** to run the print

Working with the Activity Log

You can use the **Display Firewall Log (DSPFWLOG)** command to display the contents of the Activity Log quickly and easily in a standard format using basic filter criteria. You can even use previously defined queries as filter criteria for the log display. This feature is best suited for investigating immediate problems such as program failures, errors or suspicious activity.

Firewall includes many ready-to-use log display sets. Just enter a few parameters on a simple data screen and the specified data appears in seconds. A hard copy of the Activity Log results can be printed as well.

The “Backward Glance” Feature

This unique feature lets the user view the last several minutes of activity without having to define specific time or date parameters. The user can specify a period (in minutes), press **Enter**, and transactions occurring that period of time quickly appear. Backward Glance really comes in handy when assisting users with error messages that pop up or verifying that a batch job has successfully been completed.

Using Time Groups

The Activity Log display makes full use of the convenient time group feature. This timesaving feature further enhances the ability to get to important data quickly.

Basic Procedure

A few simple steps are all that is necessary in order to view your data:

1. Select **43. Log, Reports, Queries** from the main menu. The **Reporting** menu appears.
2. Select **19. Select from menu** and choose one of the many pre-defined log display options. Examples of these selections are:
 - **1. Entire Log** – Display all entries in the Activity Log. This option is useful when examining all activities over a period of time, perhaps in conjunction with the Backward Glance feature.
 - **2. Rejects Only** – Display only activities that have been rejected
 - **5. Entire Log** – Display only occurrences from the last 5 minutes
3. Enter run-time filter and other parameters on the **Display Firewall Log** Entries screen.

Display Firewall Log (DSPFWLOG)

Type choices, press Enter.

| | | |
|----------------------------------|--------------------|-------------------------------|
| Display last n minutes | <u>*BYTIME</u> | Number, *BYTIME |
| Starting date and time: | | |
| Starting date | > <u>*PRVYEARS</u> | Date, *CURRENT, *YESTERDAY... |
| Starting time | <u>000000</u> | Time |
| Ending date and time: | | |
| Ending date | <u>*CURRENT</u> | Date, *CURRENT, *YESTERDAY... |
| Ending time | <u>235959</u> | Time |
| User* or '%GROUP' | <u>*ALL</u> | |
| Object | <u>*ALL</u> | Name, generic*, *ALL |
| Library | <u>*ALL</u> | Name, generic*, *ALL, *SYS... |
| Object Type | <u>*ALL</u> | *ALL, *FILE, *LIB, *DTAQ... |
| IP generic address | <u>*ALL</u> | |
| Type | <u>*ALL</u> | *SELECT, *NATIVE, *IFS... |
| Allowed | <u>*ALL</u> | *YES, *NO, *ALL |
| Number of records to process . . | <u>*NOMAX</u> | Number, *NOMAX |
| Output | > <u>*</u> | *, *PRINT-*PRINT9, *OUTFILE |

Bottom

F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

Display Firewall Log

| Parameter or Option | Description |
|--|--|
| Display last n minutes | Selects only the events occurring within the previous number of minutes as specified by the user
Number = Enter the desired number of minutes
*BYTIME = According to starting and ending times specified below |
| Starting date & time
Ending date & time | Selects only the events occurring within the range specified by the starting and ending date/time combination
Date and time = Enter the appropriate date or time
*CURRENT = Current day
*YESTERDAY = Previous day
*WEEKSTR/*PRVWEEKS = Current week/Previous week start
*MONTHSTR/ *PRVMONTH = Current month/Previous month start
*YEARSTR/ *PRVYEARS = Current year/ Previous year start
*SUN -*SAT = Day of week |
| Starting date & time
Ending date & time
(Continued) | |
| IP generic address | Filter by IP address |
| Type | Server type
*All = All server types
F4 = Select server type group from a list
*UP = lists all output operations over files: WRITE / CREATE / MOVE / DELETE / RENAME
*DOWN = lists all Read operations over files |
| Allowed | *YES = Allowed
*NO = Rejected
*ALL = All activity |
| Number of records to process | Maximum number of records to process
*NOMAX = No maximum (Default) |

| Parameter or Option | Description |
|--|--|
| Output | *PRINT = prints to local printer
*PRINT1 = prints to remote printer
*PRINT 2 = prints to both remote and local printers
*PRINT 3-9 = user modifiable |
| Filter by Time Group - Relationship | *IN = Include all records in time group (Inclusive)
*OUT = Include all records not in time group (Exclusive)
*NONE = Do not use time group, even if included in query definition |
| Filter by time group - Time group | Name = Name of time group
*SELECT = Select time group from list at run time |
| Filter using query rules | Use an existing query to filter Activity Log entries. This is useful for applying complex filter criteria.
Name = Name of an existing query
*None = Do not use query rules (Default) |

4. Press **Enter** to display the Activity Log.

- You may press **F18** at any time during the data retrieval process to display a pop-up status window. This window continuously displays the number of records processed and selected.
- Press **Esc** at any time to halt retrieval and immediately display the query or log. An example of the audit log display appears as follows.

```

Display Firewall Log          11/06/09 - 11/06/09

*TELOFF *FYI* Telnet session ended to device QPADEV000V.
*TELOFF *FYI* Telnet session ended to device QPADEV000R.
*TELNET Allowed 1.1.1.1.
*TELNET Allowed 1.1.1.1.
*TELNET Allowed 1.1.1.1.
*SIGNON *FYI* Allowed for JAVA1 from *LCL-QZSOSIGN in job // .
*SQL *FYI* Denied for JAVA1 to SMZODTA/ODPRVD *FILE. SQL: SELECT PRPRVD,PRTEXT
*SQL *FYI* Denied for JAVA1 to SMZODTA/ODPRVD *FILE. SQL: SELECT PRTEXT,PRINFM
*SQL *FYI* Denied for JAVA1 to SMZODTA/ODPRVD *FILE. SQL: SELECT PRPRVD,PRTEXT
*SQL *FYI* Denied for JAVA1 to SMZODTA/ODPRVD *FILE. SQL: UPDATE SMZODTA/ODPRV
*SQL *FYI* Denied for JAVA1 to SMZODTA/ODPRVD *FILE. SQL: SELECT PRPRVD,PRTEXT
*TELNET Denied 1.1.1.144.
*TELNET Denied 1.1.1.178.
*TELNET Denied 1.1.1.178.
*TELNET Denied 1.1.1.178.
*TELNET Denied 1.1.1.178.
*TELNET Denied 1.1.1.178.
*SQL *FYI* Denied for JAVA1 to SMZ8/PROCGSEPNT *PGM. SQL: CALL SMZ8/PROCGSEPNT
More...
F3=Exit F6=Modify rule F7=Add action F10=Details F11=Single entry F12=Cancel
F17=Top F18=Bottom

```

Display Firewall Log

5. Press **F6** to modify the applicable rule based on an entry in the log. The rule definition screen for the applicable rule type opens. This feature allows the user to respond proactively to a situation discovered while reviewing the log, and leads the user to the exact screen where modification is required.

6. To view the details of an individual entry, move the cursor to the desired line and press **Enter** or **F11**. An example of an activity log entry appears below.

| Display Entry | | System: S720 |
|--|------------------------|--------------------------------|
| Message ID | : GRE4083 | User profile : *NONE |
| Date | : 11/06/09 | Time : 07:13:41 |
| Job | : 412264/QTCP/QTDEVICE | Program : *FIREWALL |
| IP address | : | Library : |
| Entry type / sub-type | : 08/A | Telnet Device Initialization |
| | | |
| Action allowed | : 0 | |
| IP address | : 1.1.1.144 | |
| Auto-signon user | : | |
| Auto-signon current library | : | |
| Auto-signon initial program | : | |
| Menu (Alt Signon) | : | |
| Terminal name | : | |
| Min. password validation | : 0 | |
| Server Id | : 08 | |
| | | |
| F3=Exit F5=Display captured job data F8=Print F12=Cancel | | Bottom |

Additional Message Information

7. When pressing **F1** on a display log entry and viewing the **Additional Message Information** screen, displaying 'Decision Level' now informs you how to correct the problem, for example: Menu option: 2, 1 or 2 means enter 2 from the main menu, and then enter either option 1 or 2.

| Additional Message Information | | System: S720 |
|---|--------------------------------|-----------------------------------|
| Message ID . . . | : GRE4083 | Transaction : *REJECTED |
| Date sent . . . | : 11/06/09 | Time sent : 07:13:41 |
| Server | : Telnet Device Initialization | |
| Decision level: | : GSTEL=Telnet logon | Menu opt: 32->1 |
| Operation mode: | : *NORMAL | (or F6) |
| | | |
| *TELNET Denied 1.1.1.144. Min.password validation 0. Remote port 52105. | | |
| The examined security rule was for IP 1.2.3.4 subnet mask 252.0.0.0 incoming device *ALL password validation 0. | | |
| | | |
| F3=Exit F6=Modify decision rule F7=Add action F12=Cancel | | |

Additional Message Information

Statistics

This option provides statistics on access via a specific server or all servers, for all users.

Activity Summary is for groups of users and **User Activity Summary** is for a specific user.

The screens are the same.

Select option **62. User Activity Statistics**, the **Display User Activity** screen appears

```

Display User Activity (DSPFWUSRA)

Type choices, press Enter.

User . . . . . █ Name, *ALL
Display last minutes . . . . . *BYTIME Number, *BYTIME
Starting date and time:
  Starting date . . . . . *CURRENT Date, *CURRENT, *YESTERDAY...
  Starting time . . . . . 000000 Time
Ending date and time:
  Ending date . . . . . *CURRENT Date, *CURRENT, *YESTERDAY...
  Ending time . . . . . 235959 Time
Server ID . . . . . *ALL *FILTR, *FTPLG, *FTPSRV...
Output . . . . . * *, *PRINT-*PRINT9

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

Display User Activity

| Parameter or Option | Description |
|---|--|
| Display last minutes | Selects only the events occurring within the previous number of minutes as specified by the user
Number = Enter the desired number of minutes
*BYTIME = According to starting and ending times specified below |
| Starting date & time
Ending date & time | Selects only the events occurring within the range specified by the starting and ending date/time combination
Date and time = Enter the appropriate date or time
*CURRENT = Current day
*YESTERDAY = Previous day
*WEEKSTR/*PRVWEEKS = Current week/previous week start
*MONTHSTR/ *PRVMONTH = Current month/previous month start
*YEARSTR/ *PRVYEARS = Current year/ previous year start
*SUN -*SAT = Day of week |
| Starting date & time
Ending date & time
(Continued) | |
| Server ID | Choose servers you want to examine. To examine all servers, choose *ALL . |

| Parameter or Option | Description |
|---------------------|---|
| Output | <p>*PRINT = prints to local printer</p> <p>*PRINT1= prints to remote printer</p> <p>*PRINT2 = prints to both remote and local printers</p> <p>*PRINT3-9 = user modifiable</p> |

Group Items for Selection

Define assorted groups of reports in line with your requirements, to schedule a particular group of reports to run as one unit sometime in the future.

%GROUP is used for defining a group of user-profiles that all share the same authorities.

This solution enables defining GROUPS by GROUP-TYPES. These GROUP-TYPES can be any system entity such as files, libraries, applications, identification numbers, etc.

For each GROUP-TYPE, one can define an unlimited number of GROUPS and within GROUPS any number of items. For example, all identification numbers of the PCs in the organization can be defined as one group in the GROUP-TYPE defined as MACHINE_ADDRESS. Another group in MACHINE_ADDRESS may contain all identification numbers of the PCs in a sister organization.

In all comparison tables, for defining rules, for generating and selecting queries, or for defining the items in reports, the ITEM GROUP-TYPE/GROUP syntax can be used to include only those transactions which contain the GROUP-TYPE/GROUP specified. Likewise, NITEM GROUP-TYPE/GROUP can be used to include only those transactions which do not contain the GROUP-TYPE/GROUP defined.

In addition, special GROUPS such as groups of users already defined on the system, all of which have a common identifying characteristic. For example, the group profile of the system, group profiles defined in **Firewall**, and virtual groups of users named *SECADM, *SAVESYS etc. which are the users who have this particular privilege defined in their special authority.

1. To define Groups and Items, select option **43. Log, Reports, Queries** from the main menu, and option **41. Group Items for Selection** from the **Reporting** menu. The **Work with Classes of Groups** screen appears.

| GSRPTMNU | | Reporting | Firewall | |
|---|--------|-----------------------------------|----------|--------|
| Work with Classes of Groups | | | | |
| Type options, press Enter. | | | | |
| 1=Work with 2=Edit 4=Remove | | Position to . . . | | |
| | | Subset | | |
| Opt | Class | Description | Item | Length |
| * | GRPPRF | OS/400 Group profiles | 10 | |
| * | SPCAUT | Users by their Special Authority | 10 | |
| * | USRGRP | User groups in iSecurity/Firewall | 10 | |
| B | | hhhhhhhhh | 1 | |
| COMMANDS | | Commands of various types | 10 | |
| FFF | | | 5 | |
| III | | | 1 | |
| ILAN | | | 1 | |
| JJJ | | | 1 | |
| More... | | | | |
| *CLASsEs are automatically defined by the system. Press F6 for instructions : | | | | |
| F3=Exit F6=Add New (plus instructions) F12=Cancel : | | | | |
| F13=Information Assistant F16=AS/400 main menu | | | | |

Work with Classes of Groups

- Press **F6** to add a new class or type **1** to modify an existing class to your needs.

| GSRPTMNU | | Reporting | Firewall | |
|--|--|------------------------------------|----------|--|
| Add Class | | | | |
| Type choices, press Enter. | | | | |
| Class | | e.g. USERS, IP, COMMANDS, FILES... | | |
| Text | | | | |
| Maximum item length . | | 1 - 20 | | |
| Group-Classes (such as USERS, IPS, FILES) consist of individual Groups. | | | | |
| For example, Group-Class USERS could consist of groups HR, ERP, etc. These | | | | |
| groups are useful when you want to limit a report or a rule to only the | | | | |
| USERS listed in USERS/HR who accessed files listed in FILES/SENSITIVE. | | | | |
| To use, enter ITEM or NITEM ("item of" or "not item of") in the TEST | | | | |
| column of the report's Filter Conditions; then press F4 in VALUE column. | | | | |
| F3=Exit | | F12=Cancel | | |
| F13=Information Assistant F16=AS/400 main menu | | | | |

Add Class

- Press Enter. The **Work with Groups** screen appears.


```

GSRPTMNU                                Reporting                                Firewall
:
:                                     Add Class
:
:                                     Work with Groups of IP
:
: Class: IP Class
:
: Type options, press Enter.           Position to .  |
:   1=Work with  2=Edit  4=Remove     Subset . . .  |
:
: Opt Group      Description
:
:
: (No data found to construct list)
:
:
: F3=Exit      F6=Add New      F12=Cancel
:
:

```

Work with Groups

4. Press **F6** to add a new Group or **1** to modify items in existing group to your needs.

```

GSRPTMNU                                Reporting                                Firewall
:
:                                     Work with Classes of Groups
:
:                                     Work with Groups of COMMANDS
:
:                                     Work with Group Items
:
: Type : COMMANDS  Commands of various types
: Group: USRCOMMAND User commands
: Type information, press Enter.
:
: Item      Description
: CHGUSRPRF
: CRTUSRPRF
: DSPUSRPRF
: RTVUSRPRF
: WRKUSRPRF
:
:                                     More...
:
: F3=Exit      F12=Cancel
:
:

```

Work with Group Items

The supported TYPES are:

- *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 *USRGRPs

NOTE: *If the TYPE is missing, *USER or *USRGRP is assumed based on the appearance of the percentage symbol ("%") as the first character in the GROUP.*

Using the Report Scheduler

This section describes the Report Scheduler feature and provides step-by-step instructions for its use.

Overview

The Report Scheduler allows you to run pre-defined “report groups” automatically according to a fixed schedule. A **report group** is comprised of one or more individual queries, reports or Activity Log inquiries that are executed together at a designated time. Grouping reports in this manner is more efficient because the scheduling details and other run-time parameters need to be defined only once for the entire group.

The most common application of the Report Scheduler is automatically running periodic audit reports based on queries. A schedule can be set up to run reports on a daily, weekly or monthly basis. Additional schedule parameters are provided to enable the user to specify the day of the week, day of the month and time of day that your report will run.

The Report Scheduler can print several different types of reports, such as:

- Queries
- **Firewall** Activity Logs reports
- **Action** Activity Logs, which contain records of actions actually performed
- User Profile Reports

The Report Scheduler is based on the native OS/400 scheduling facility, but with added support for the report group feature and an improved user interface.

The Definition Process

The Report Scheduler incorporates a wizard-based interface to make the definition process simple and user friendly.

To define and schedule reports to run automatically, perform the following steps in order:

1. Create any queries to be included in the relevant report group.
2. Create or modify the report group as follows:
 - Assign a report group name and description.
 - Enter schedule data and run-time parameters for the group.
3. Create the individual reports to be included in the report group as follows:
 - Assign a report name and select the report type.
 - Define the run-time parameters for each the report.

4. Run the report group, if desired.

These steps are explained in detail in the following sections.

Working with Report Groups

The first step in the Report Scheduler definition process is to define the report group. The report group definition consists of a group name, description and several run time parameters that apply to each report in the group.

1. Select **51** from the **Log, Reports, Queries** menu. The **Work with Report Scheduler** screen appears.
2. Press **F6** to create a new report group or type **1** to select an existing group.

Work with Report Scheduler

Subset by name . . *ALL
 Position to . . .

Type options, press Enter.
 1=Select 2=Add 3=Copy 4=Delete 5=Run

| Opt | Group | Seq | Description |
|-----|---------|-----|----------------------------------|
| █ | DAILY | | Daily Scheduled Report |
| — | | 1 | Display Firewall Log |
| — | | 2 | Activity of the Security Officer |
| — | | 3 | Change User Profiles |
| — | | 4 | Payroll File Access Log |
| — | MONTHLY | | Monthly Scheduled Report |
| — | | 1 | Sales Library Access Log |
| — | WEEKLY | | Weekly Scheduled Report |
| — | | 1 | Run Firewall Log |
| — | | 2 | Payroll File Access Log |
| — | | 3 | *Firewall SQL* |

Bottom

F3=Exit
F5=Refresh
F6=Add New Group
F8=Print
F12=Cancel

Work with Report Scheduler

Report groups appear on the screen sorted in alphabetical order by the group name. The individual reports contained in each group appear directly below the group name arranged according to a user-modifiable sequence.

| Parameter or Option | Description |
|---------------------|--|
| F6 | Create new report group |
| Opt | 1 = Select group for modification
2 = Add a new report to the selected group
3 = Copy the group along with all its reports, or
Copy an individual report from one group to another
4 = Delete the group along with all of its reports, or
Delete an individual report |

3. The **Modify Report Group** screen appears. Assign a name to the report group and enter a brief description.

Modify Report Group

Report groups are intended to run pre-defined sets of reports automatically on a periodic basis. Each report group may include several individual reports. Parameters defined for Report Groups override those for individual reports. The use of descriptive date values, such as: *YESTERDAY, *WEEKSTR, *MONTHSTR, etc. is highly recommended.

Type choices, press Enter.

| | | |
|-------------------------|-------------------------|--------------------------------------|
| Report Group name . . . | WEEKLY | Name e.g. DAILY, WEEKLY, MONTHLY ... |
| Description | Weekly Scheduled Report | |
| Group parameters . . . | | |

Press Enter to continue to the Define Parameters screen.

F3=Exit F8=Print F12=Cancel

Modify Report Group

| Option | Description |
|--------------------------|---|
| Report Group Name | Enter a name with a maximum of 7 alphanumeric characters. The name must begin with a letter. |
| Description | Free text description of the report group |
| Group Parameters | Command string automatically generated by Firewall based on run-time parameters specified for the report group |

4. Press **Enter** to continue.

This screen allows the user to define **run-time filters** that apply to all reports in the group. Run-time filter criteria allow the user to display or print only a **subset** of the data extracted by the query definition. For example, if a query definition does not include filter criteria for a user profile (i.e. includes all user profiles), this screen can be used to print only activity associated with a specific user profile.

Run-time filter criteria will not extract data that is not included in the query definition itself. For example, if a query definition includes filter criteria only for the user profile **RICH** and one enters run-time criteria for the user **GEORGEW**, no records will be displayed.

```

Define FW Report Group Params (DFNFWGRPD)

Type choices, press Enter.

Starting date and time:
  Starting date . . . . . > *YESTERDAY   Date, *CURRENT, *YESTERDAY...
  Starting time . . . . . > 060000       Time
Ending date and time:
  Ending date . . . . . > *CURRENT       Date, *CURRENT, *YESTERDAY...
  Ending time . . . . . > 055959       Time
User* or '%GROUP' . . . . . *ALL
Server ID . . . . . *ALL               *ALL, *FILTR, *RMTSRV...
System to run for . . . . . *CURRENT    Name, *CURRENT, *group, *ALL..
Output . . . . . *PRINT                *, *PRINT, *PDF, *HTML..
Print format . . . . . *SHORT          *SHORT, *FULL

Additional Parameters

Job description. . . . . QBATCH        Name, *NONE
Library . . . . . *PRODUCT            Name, *PRODUCT, *LIBL...
More...

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

Define FW Report Group Details

| Option | Description |
|-----------------------------|--|
| Starting/Ending Date | Enter a fixed date or use one of the following constants:
*CURRENT = The current date (day the report runs)
*YESTERDAY = The day before the current date
*WEEKSTR = Beginning of the current week
*PRVWEEKS = Beginning of the previous week
*MONTHSTR = Beginning of the current month
*PRVMONTHS = Beginning of the previous month
*YEARSTR = Beginning of the current year
*PRVYEARS = Beginning of the previous year
*MON - *SUN = Day of the current (or previous) week
NOTE: All constants are relative to the day on which the report runs. |
| Starting/Ending Time | Time of day using the 24 hour clock (HH:MM:SS) |
| User* or '%GROUP' | User profile or Group name that instigated the event being audited |
| Server ID | Choose servers you want to examine. To examine all servers, choose *ALL . |
| System to run for | The system to report information from
*CURRENT = the current system
*Name = a group of systems as defined in STRAUD, 83, 1
*ALL = all the systems defined in STRAUD, 83, 1 |
| Output | *PRINT = prints to local printer
*PRINT1 = prints to remote printer
*PRINT2 = prints to both remote and local printers
*PRINT3-9 = user modifiable |
| Print Format | *SHORT = Short format
*FULL = Full report format |
| Results | *BOTH = display rejected and accepted transactions |

| Option | Description |
|-----------------------|--|
| | * REJECT = display rejected transactions
* ACCEPT = display accepted transactions |
| Object/Library | Object and library path |
| Object Type | One of the available objects types from option 21. Native AS/400 Objects (Firewall Main menu) |

5. Press **Enter** to continue to the **Change Job Schedule Entry** screen.

Change Job Schedule Entry (CHGJOBSCDE)

Type choices, press Enter.

| | | |
|-----------------------------|------------|-----------------------------|
| Frequency | *WEEKLY | *SAME, *ONCE, *WEEKLY... |
| Schedule date, or | *NONE | Date, *SAME, *CURRENT... |
| Schedule day | *ALL | *SAME, *NONE, *ALL, *MON... |
| + for more values | | |
| Schedule time | '23:00:00' | Time, *SAME, *CURRENT |

Bottom

F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

Change Job Schedule Entry

| Option | Description |
|----------------------|---|
| Frequency | * SAME = Value does not change
* ONCE = Run the report group once only
* WEEKLY = Run on the same day or days of each week
* MONTHLY = Run on the same day or days of each month |
| Schedule Date | Date = The specific day on which the report will run
* SAME = Value does not change
* CURRENT = The current date (day the report runs)
* MONTHSTR = First day of the next month
* MONTHEND = Last day of the current month
* NONE = Use day of week value in the Schedule Day field below |
| Schedule Day | * ALL = Run every day (Overrides frequency parameter)
* MON * TUE * WED * THU
* FRI * SAT * SUN
* NONE = Use day of week value in the Schedule Date field above. |
| Schedule Time | Time of day using the 24 hour clock (HH:MM:SS) |

The **Schedule Date** and **Schedule Day** fields are mutually exclusive. If one is used, the other must be set to the value ***NONE**. Other fields may appear on this screen, which is associated with the OS/400 **CHGJOBSCDE** command. These fields are not relevant under most circumstances.

6. Press **Enter** to complete the definition and return to the **Work with Report Scheduler** screen.

Working with Individual Reports

The next step in the definition process is to define the individual reports that are contained in the report group.

1. To add a new report to a group, type **2** next to the group name, or type **2** next an individual report to modify it. The **Modify Report Definition** screen appears.

Add Report Definition

Reports in a group run periodically, as per the group definition.
Parameters defined in the Group, override the same ones defined for reports.

Group DAILY Daily Scheduled Report

Type choices, press Enter.

Report Id. 5

Description Display User Activity

Report command /*SELECT DSPFWUSRA

Display User Activity

Report parameters . . . █

F3=Exit F4=Set Parameters F12=Cancel

Modify Report Definition

| Option | Description |
|----------------------------|--|
| Report ID | Numeric identification automatically assigned by the Firewall |
| Description | Free text description of the report |
| Report Command (F4) | Press F4 to select report type from a pop-up window |

2. Define run time parameters for this report. The actual parameters available are specific to the report type.
3. Press **Enter** to finish the definition and return to the **Work with Report Scheduler** screen.

Running Reports

The Report Scheduler submits all scheduled reports as batch jobs automatically on the day and time as specified in the definition. A report can be run manually at any time.

To run a report manually:

1. Select **52** from the **Log, Reports, Queries** menu. The **Run Report Group** screen appears.
2. Set parameters according to the following table.

```

Run Report Group (RUNRPTGRP)

Type choices, press Enter.

Report group . . . . . █      Name
Job description . . . . . QBATCH  Name, *NONE
Library . . . . . *PRODUCT  Name, *PRODUCT, *LIBL...

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

Run Report Group

| Parameters | Description |
|------------------------|---|
| Report Group | Enter the report group name |
| Job Description | Your batch job subsystem – normally <i>QBATCH</i> |
| Library | Name = Library name
*Product = <i>SMZ4</i> or the default product library
*LIBL = Current library list
*CURLIB = Current Library |

Chapter 9: Advanced Security Features

The Work with Advanced Security Screen enables the user to configure powerful security settings. To access these settings, select **42. Advanced Security Features** from the **Firewall** main menu. The **Work with Advanced Security** screen appears.

```

GSSPMNU                                Work with Advanced Security

Select one of the following:

DDM, DRDA Security                      License Management Security
  1. Pre-check user replacement          41. License Management
  5. DRDA post-check user replacement    45. Display License Management Log

DHCP Security
  15. Display DHCP Security Log

TCP/IP Port Restrictions
  21. Work with TCP/IP Port Restrictions

Selection or command
===> █

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

Work with Advanced Security

DDM, DRDA Security

Distributed Data Management (DDM) is a function of the operating system that allows an application program or user on one system to use database files stored on a remote system. The system must be connected by a communications network, and the remote system must also use DDM. The term also applies to the underlying communications architecture.

Distributed Relational Database Architecture^(TM) (DRDA^(R)) is the architecture that defines formats and protocols for providing transparent access to remote data. DRDA defines two types of functions: the application requester function and the application server function.

Both of these are integrated into the **Firewall** advanced security features.

Pre-Check User Replacement

This feature applies to both DDM and DRDA. **Firewall** performs a “pre-check” whenever a certain user enters from a certain location. **Firewall** “invents” an entity that does the checking.

To work with Pre-Check User Replacement:

1. Select **1. Pre-check user replacement** from the **Work with Advanced Security** screen. The Work with DDM/DRDA Pre-check User Replacement screen appears.
2. Set the correct parameters and press **Enter**.

```

Work with DDM/DRDA Pre-check User Replacement

Type options, press Enter.
1=Select 4=Delete

Source      Source      User to
Opt Location User*      Check
  ───────── ───────── ─────────
  *ALL      *ALL      QUSER
  S44K1246  MICHAEL  EVEGENY
  S44K1246  RICH    QSECOFR
  S44K1246  THEBOSS  QSECOFR

F3=Exit  F6=Add new  F8=Print  F12=Cancel

Bottom
  
```

Work with DDM/DRDA Pre-check User Replacement

| Parameters | Description |
|-----------------|--|
| Source Location | System name of remote server |
| Source User | User profile name of target DDM job |
| User to Check | User for which internal check is performed |

NOTE: Add DDM/DRDA Pre-check User Replacement and Modify DDM/DRDA Pre-check User Replacement share the same settings.

```

Modify DDM/DRDA Pre-check User Replacement

Type choices, press Enter.

Source location . . . . . DEVELOP      Name
Source user . . . . . *ALL             Name, generic*, *ALL
Perform internal checks for user . DEVELOPER      Name, F4 for list

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

Modify DDM/DRDA Pre-check User Replacement

| Parameters | Description |
|---|--|
| Source location | System name of remote server |
| Source user | User profile name of target DDM job |
| Perform internal checks for user | Name = name of user being checked
F4 for list =press this option to |

DRDA Post-Check User Replacement

This is a “post-check” only applicable for DRDA. In this option, **Firewall** replaces restricted users with someone who has the correct authority.

- To work with **DRDA Post-Check User Replacement**, select **5. DRDA post-check user replacement** from the **Work with Advanced Security** screen. The **Work with DRDA Post-check User Replacement** screen appears.
- Set your desired parameters and press **Enter**. To modify, select **1**. To add, select **F6**.

```

Work with DRDA Post-check User Replacement

Type options, press Enter.
1=Select 4=Delete

Source      Source      User for OS/400
Opt Location User*      Security checks
- - - - -
1 *ALL      *ALL      QUSER
- S44K1246  %ACCT     RICH
- S44K1246  %PRGMR    EVEGENY
- S44K1246  QSECOFR   QSECOFR
- S44K1246  THEBOSS   QSECOFR

F3=Exit  F6=Add new  F8=Print  F12=Cancel

Bottom

```

Work with DDM/DRDA Post-check User Replacement

| Parameters | Description |
|------------------------|--------------------------------------|
| Source location | System name of remote server |
| Source user | User profile name of target DRDA job |

DHCP Security

DHCP (Dynamic Host Configuration Protocol) is a communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network. DHCP is defined by the Internet Engineering Task Force (IETF).

The AS/400 may essentially play the role of a DHCP server. If so, it records the activities and transactions in a log. This option allows the user to view and inspect that log.

1. Select **15. Display DHCP Security Log** from the **Work with Advanced Security** screen. The **Display Firewall Log** screen appears.
2. Type options and press **Enter**.

```

Display Firewall Log (DSPFWLOG)

Type choices, press Enter.

Display last n minutes . . . . . *BYTIME      Number, *BYTIME
Starting date and time:
  Starting date . . . . . *CURRENT      Date, *CURRENT, *YESTERDAY...
  Starting time . . . . . 000000      Time
Ending date and time:
  Ending date . . . . . *CURRENT      Date, *CURRENT, *YESTERDAY...
  Ending time . . . . . 235959      Time
User* or + '%GROUP' . . . . . *ALL
Object . . . . . *ALL      Name, generic*, *ALL
Library . . . . . *ALL      Name, generic*, *ALL, *SYS...
Object Type . . . . . *ALL      *ALL, *FILE, *LIB, *DTAQ...
IP generic address . . . . . *ALL
Type . . . . . > *DHCP      *SELECT, *NATIVE, *IFS...
Allowed . . . . . *ALL      *YES, *NO, *ALL
Number of records to process . . *NOMAX      Number, *NOMAX
Output . . . . . *      *, *PRINT-*PRINT9, *OUTFILE
                                           More...

F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys
  
```

Display Firewall Log

| Parameter or Option | Description |
|--|---|
| Display last n minutes | Select only the events occurring within the previous number of minutes as specified by the user
Number = Enter the desired number of minutes
*BYTIME = According to starting and ending times specified below |
| Starting date & time
Ending date & time | Select only the events occurring within the range specified by the start and end date/time combination
Date and time = Enter the appropriate date or time
*CURRENT = Current day
*YESTERDAY = Previous day
*WEEKSTR/*PRVWEEKS = Current week/Previous week start
*MONTHSTR/ *PRVMONTH = Current month/Previous month start
*YEARSTR/ *PRVYEARS = Current year/ Previous year start
*SUN -*SAT = Day of week |
| Starting date & time
Ending date & time
(Continued) | |
| User* or '%Group' | Filter records by user profile or group |
| Object | Filter records by object
Name = Specific object by name
Generic* = All objects/libraries beginning with the text string preceding the *
*ALL = All types as specified in the query definition |

| Parameter or Option | Description |
|--|---|
| Object Type | Filter records by object type. |
| Type | Server type
* All = All server types
F4 = Select server type group from a list |
| Allowed | * YES = Allowed * NO = Rejected * ALL = All activity |
| Number of records to process | Maximum number of records to process
* NOMAX = No maximum (Default) |
| Output | * PRINT = prints to local printer
* PRINT1 = prints to remote printer
* PRINT2 = prints to both remote and local printers
* PRINT3-9 = user modifiable |
| Additional Parameters | |
| Filter by Time Group - Relationship | * IN = Include all records in time group (Inclusive)
* OUT = Include all records not in time group (Exclusive)
* NONE = Do not use time group, even if included in query definition |
| Filter by time group - Time group | Name = Name of time group
* SELECT = Select time group from list at run time |
| Filter using query rules | Use an existing query to filter Activity Log entries. This is useful for applying complex filter criteria.
Name = Name of an existing query
* None = Do not use query rules (Default) |

TCP/IP Port Restrictions

Work with TCP/IP Port Restrictions

Transmission Control Protocol/Internet Protocol is an industry-standard, non-proprietary set of communications protocols that provide reliable end-to-end connections between applications over interconnected networks of different types.

In the world of TCP/IP, an IP address is necessary in order to reach a destination. At the destination, a port, which serves as a virtual door or window, is required. In today's world, it is imperative to protect and guard the ports in your system. Thus, **Firewall** restricts certain users to certain ports by defining the port range accessible to them.

Port information consists of a list of the ports or port ranges, protocols, and the user profiles. You need to define port information only if you want to restrict the use of a port or range of ports to one or more users.

1. To add, display, remove, or print port restrictions, select **21. Work with TCP/IP Port Restrictions** from the **Work with Advanced Security** screen. The **Work with TCP/IP Port Restrictions** screen appears.
2. Enter the parameters according to the following table. To add, select **F6**.

```

Work with TCP/IP Port Restrictions
System: S720

Type options, press Enter.
4=Delete

Opt  Port-Range  Type  Allowed  Port description
  1  250        TCP   GS
  2  250        UDP   GS
  3  1500       TCP   JAVA
  4  1500       UDP   JAVA

Bottom
WARNING: Using port numbers in range 1-1024 may affect TCP/IP processing.
F3=Exit  F6=Add new  F7=Sort by User  F8=Print  F12=Cancel
  
```

Work with TCP/IP Port restrictions

| Parameters | Description |
|-------------------|---|
| Port Range | Specifies the port number or range of port numbers identifying the port or ports that are being restricted. Valid values range from 1 through 65 535.
NOTE: Ports 1 - 1024 are used by the system-supplied TCP/IP applications. If the user specifies ports 1 through 1024, this can affect the operation of those applications.
Lower = lower end of port range
Upper = *ONLY (Used to restrict only a single port)
User = The user profile that will use this port or range of ports. |
| Opt. | 4 = Delete (deletes the restrictions for a port)
F6 = Add: Use to add a port restriction by typing the port number into the input field at the top of the list. To add more restrictions, use the Add function again. |

License Management Security

Licensed programs can either be unlimited or limited to a group of users.

License Management

This option enables users to supervise, and therefore allow and restrict, the use of licensed copies of their software.

1. To work with License Security, select **41.License Management** from the **Work with Advanced Security** screen. The **Work with License Security** screen appears.
2. Set parameters according to the following table and press **Enter**. Select **F6** to add a new user or option **1** to modify.

```

Work with License Security

Type options, press Enter.
  1=Select  4=Delete

Opt  User      Product  Feature  Allowed
-
  █  *PUBLIC    *ALL    *ALL     Y
  -  %PGMR      5716PW1  5050     Y
  -  %PGMR      5769ST1  5050     Y
  -  %PRGMR      5716RG1  5050     Y
  -  A          B        C
  -  AA         B        C         Y
  -  QSYSOPR     5716PT1  5050     Y
  -  RICH       5769QU1  5050     Y
  -  THE*       5769XF1  *ALL     Y

F3=Exit  F6=Add new  F8=Print  F12=Cancel

Bottom
  
```

Work with License Security

| Parameters | Description |
|------------|---|
| User | User working with particular software |
| Product | Software in question |
| Feature | The feature that the user has access to
*ALL = all features |
| Allowed | Y = User is allowed to access this software |

```

Modify License Security

Type choices, press Enter.

User . . . . . █PUBLIC      Name, generic*, User Group,
                                *PUBLIC, F4 for list

Product . . . . . *ALL       Name, F4 for list

Feature . . . . . *ALL       Name, *ALL, F4 for list

Allowed . . . . . _         Y=Yes

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

Modify License Security

Display License Management Log

This feature provides information about every transaction generated by the License Management server.

1. To display the log, select **45. Display License Management Log** from the **Work with Advanced Security** screen. The **Display Firewall Log** screen appears.
2. Set parameters according to the table in the DHCP Security section earlier in this chapter, and press **Enter**.

Chapter 10: Configuration and Maintenance

System Configuration

This section reviews the process of setting general configuration for **Firewall**.

To reach this screen, select **81. System Configuration** from the main screen. The **iSecurity (part I) Global Parameters** screen appears.

```

*FYI* Mode Active      iSecurity (part I) Global Parameters

Select one of the following:

Firewall
  1. General Definitions
  2. Additional Settings
  3. User Exit Programs
  4. Transaction Post Processing
  5. Intrusion Detection System
  6. Password Exit Programs
  7. Enable ACTION (CL Script + more)
  8. SYSLOG
  9. Log Retention

Screen
  11. General Definitions
  12. Customize Messages

Password
  21. Password Dictionaries

System Configuration
  81. iSecurity/Base

General
  91. Language Support
  99. Copyright Notice

Selection ==> █

Release ID . . . . . 15.0  09-11-12   4465D5A  720 206A
Authorization code . . . . . _____ 0

F3=Exit   F22=Enter authority code
  
```

iSecurity (part I) Global Parameters

General Definitions

This option presents general definitions relating to emergency overrides, FYI (Simulation) mode, **Firewall** history log, OS/400 Group and Supplemental profiles, and Super Speed processing. Follow this procedure:

1. Select **1. General Definitions** from the **iSecurity (part I) Global Parameters** screen. The **Firewall General Definitions** screen appears.
2. Set parameters and definitions according to the following table and press **Enter**.

```

Firewall General Definitions

Type options, press Enter.

Emergency override ALL Security setting . . 0  0=Regular (no override)
                                           1=Allow    3=Reject
                                           2=Allow+Log 4=Reject+Log

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.

Check OS/400 Group and Supplemental profile  _  Y, N

Enable Super Speed Processing . . . . . N  Y, N
The functionality of the product is not affected by this setting.
Set this value to N, well before you plan a "Hot Upgrade" of the product.
This will enable temporary suspension of the activity during installation.
Hot upgrade is safe . . . . . Y  (See manual)

F3=Exit  F12=Previous

```

Firewall General Definitions

| Parameter or Option | Description |
|--|---|
| Emergency override ALL Security setting | This option is explained in full detail in Chapter 4, <i>Using the Emergency Override Feature</i> .
0 = Disable emergence override – all rules function normally
1 = Allow all activity
2 = Allow and log all activity
3 = Reject all activity
4 = Reject and log all activity |
| Work in FYI Simulation Mode | This option is explained in full detail in Chapter 4, <i>FYI Simulation Mode –Global Setting</i> .
Y = Enable FYI globally
N = Do not enable FYI |
| Check OS/400 Group and Supplemental profile | Firewall checks permissions the same way the system does. First, it checks the permissions of the user, and if there are none, it checks the group profile. If there are still no permissions, it checks its supplemental group profile. iSecurity follows IBM's method of requiring up to 17 checks to examine user permissions.
NOTE: The more checks Firewall performs, the lengthier the validation process. The unique algorithm upon which this product is based guarantees a highly rapid process. This option configures how you check users for access.
Y = Check user for access; if not allowed, check group/supplemental profile for access
N = Check user for access; if not allowed, reject access without checking group/supplemental profile |
| Enable Super Speed Processing | Super Speed Processing keeps the most useful commands in the Firewall CPU memory, therefore improving product |

| Parameter or Option | Description |
|---------------------|--|
| | performance. Disable this feature a week before upgrade, in order to perform a “hot upgrade” – allowing you to upgrade product without shutting down.
Y = enable super speed processing
N = disable super speed processing |

Additional Settings

Firewall can ensure that a proper password is entered even before performing any other checks, and before allowing the operating system to validate that password.

If the parameter is set to ‘N’ (recommended) at the **Check FTP Logon PWD by product** field, the request might be rejected due to other reasons before ensuring that the password is valid.

The field **Inherit In-product DB2 authorities** refers to optional Native Object Security inheritance

Skip SQL parsing if final decision was taken at... Eliminate SQL parsing when not needed. This option can be activated separately based on the level on which the decision was taken and the type of the decision.

For example: an organization wishes to eliminate parsing of an SQL which was rejected as it has been received from an unauthorized IP (The request can still be logged for farther review).

```

Firewall Additional Settings

Type options, press Enter.

      SQL Remote Cmd FTP DDM
Analyze cmds in CALL QCMDEXC/QCAPCMD . Y Y Y Y
      SQL Remote Pgm
Analyze calls to QSYS programs (APIs). Y Y

Inherit In-product DB2 authorities . . 1 1=No, 2=Yes
Inherit In-product IFS authorities . . 1 1=No, 2=Yes, from higher dir,
                                         3=Yes, from higher dir or file*

Skip SQL parsing if final decision was taken at (leave blank for parsing)
      Global level . . 1 1=Always, 2=Allow, 3=Reject
      IP level . . . 1 1=Always, 2=Allow, 3=Reject
      User level . . . 2 1=Always

Check FTP Logon PWD by product . . . . N Y=Yes (not recommended), N=No
Y provides messages about invalid password in Firewall log.

F3=Exit F12=Previous

```

Firewall Additional Settings

User Exit Programs

User Exit Programs are an option for the user to access a program *after* **Firewall** filters have rejected a particular authorization attempt.

1. To work with Firewall User Exit Programs, select **3. User Exit Programs** from the **iSecurity (part I) Global Parameters** screen. The **Firewall User Exit Programs** screen appears.
2. Set parameters and press **Enter**.

```

Firewall User Exit Programs

Type options, press Enter.

Allow/Reject request . . . . . *NONE          Name, *NONE
Library . . . . .                Name, *LIBL
This user program is called at the end of the authorization verification,
and may override the decision. See example in SMZ8/GRSOURCE FWAUT#A.

Enable Application Level Security *STD          Name, *NONE, *STD
Library . . . . .                Name, *LIBL
GUI product identifies itself and continues without farther inspections.
For *STD value initial identification program SMZ8/GSASTDR should be
called by GUI with two parameters:
<Application name> - *CHAR 20, <Identification key> - *CHAR 50

Pre Power Down System . . . . . *NONE          Name, *NONE
Library . . . . .                Name, *LIBL
This user program is called before system is powered down.
No parameters are passed to this program.

F3=Exit  F12=Previous
  
```

Firewall User Exit Programs

| Parameter or Option | Description |
|--|---|
| Allow/Reject Request | <p>After Firewall determines an action as legitimate or unauthorized, it can perform an additional check, which can override the first decision.</p> <p>Name = name of user exit program</p> <p>*NONE= do not call any program. (Use this option when there is no exit program)</p> <p>*LIBL = library where program is located</p> |
| Enable Application Level Security | <p>*STD = application security will be checked by the standard iSecurity Firewall program SMZ8/GSASTDR.</p> <p>To activate the Application Security feature, ensure that this field has *STD definition</p> <p>Name = name of custom-made application security program</p> <p>*NONE = no application security check</p> |
| Pre- Power Down System | <p>If you want to call a program before “power down” (shutting down the AS/400), you must do it here.</p> <p>Name = name of user exit program</p> |

| Parameter or Option | Description |
|---------------------|---|
| | *NONE* = do not call any program. (Use this option when there is no exit program.) |

NOTE: You may also set exit program “behavior” for each server (see *Modifying Server Security*).

Transaction Post-Processing

This option informs particular data queues of accepted/rejected transactions. The user can send all rejected transactions to one data queue, all accepted transactions to another, or send them both to the same message queue.

1. To use Transaction Post Processing, select **4. Transaction Post Processing** from the **iSecurity (part I) Global Parameters** screen. The **Firewall Transaction Post Processing Data Queues** screen appears.
2. Set correct parameters and press **Enter**.

Firewall Transaction Post Processing Data Queues

Type options, press Enter.

Post Processing Data Queues:

| | Name | Library |
|---------------------------------|-------|---------|
| Rejected Transactions | *NONE | _____ |
| Accepted Transactions | *NONE | _____ |

These Data Queues enable users to bind Firewall with external products such as pager systems. These Data Queues are created automatically. Entries are formatted according to the standard log file SMZ8/GSCALP.

F3=Exit F12=Previous

Firewall Transaction Post-Processing Data Queues

Intrusion Detection

This option is related to Transaction Post-Processing, but involves message queues instead of data queues. Intrusion Detection lets particular message queues know of accepted/rejected transactions. Users can send all rejected transactions to one message queue, all accepted transactions to another, or send them both to the same message queue.

1. To use Intrusion Detection, select **5. Intrusion Detection** from the **iSecurity (part I) Global Parameters** screen. The **Firewall Intrusion Detection** screen appears.
2. Set correct parameters and press **Enter**.

```

Firewall Intrusion Detection System

Type options, press Enter.

Setting up an Intrusion Detection System:
Enter a message queue name or QSYSOPR . . . . . QSYSOPR *LIBL
At the monitoring workstation, enter: CHGMSGQ DLVRY(*BREAK) SEV(0)
This causes rejection messages to break-in with a beep.
When intrusion is detected:
End the offending interactive session . . . . . N N
Send message to the user . . . . . N N
Disable user (F15 for exceptions) . . . . . N N
Send Email to the user . . . . . N N
Send Email to Security Administrator . . . . . N N
Email: udi@razlee.com
Run Action (If Action installed) . . . . . N N
Write to QAUDJRN (security audit journal) . . . . . N N
Audit journal code is U. Journal entry type is FW. Data format: SMZ8/GSCALP
Screening of Allowed Activity:
Enter a message queue name . . . . . *NONE

F3=Exit F12=Previous F15=Disable exceptions
  
```

Firewall Intrusion Detection System

| Parameter or Option | Description |
|---|--|
| Monitoring message queues | Name = name of user
Library = location of message queue |
| Write rejections to security audit journal | Select Y (Yes) or N (No) to send rejections to the Audit journal. |

Password Exit Programs

This option provides an additional check for FTP passwords. It is a security risk to code passwords which are kept for later use. Whenever a password has to be validated, and the ***PGM** is written as the validation parameter, the program mentioned here will be called to verify that the entered password is the correct one.

1. To work with Password Exit Programs, select **6. Password Exit Programs** from the **iSecurity (part I) Global Parameters** screen.
2. Set correct parameters and press **Enter**.


```

Firewall Password Exit Programs

Type options, press Enter.

Incoming Password Validation . .  *NONE      Name, *NONE
Library . . . . .                Name, *LIBL
This program validates the incoming passwords for FTP, if *PGM is specified.
Example program SMZ8/GRSOURCE PWPWDE#A.

OS/400 Actual Password supplier .  *NONE      Name, *NONE
Library . . . . .                Name, *LIBL
This program supplies the system password for FTP/WSG, if *PGM is specified.
Example program SMZ8/GRSOURCE PWPWDE#A.

F3=Exit  F12=Previous
    
```

Firewall Password Exit Programs

Enable ACTION (CL Script + More)

This feature enables **Action** to respond automatically to security events generated by **Firewall** and **Screen**. In order for this feature to work, the user must verify that **Action** is installed and functioning correctly.

To enable real-time detection:

1. Select **7. Enable ACTION (CL Script + more)** from the **iSecurity (part I) Global Parameters** screen. The **Enable Real-Time Detection** screen appears.
2. Select the correct options according to the following table.
3. Select **1. Work with Servers** from the **Firewall** main menu.
4. Choose a server and select option **1** from the **Modify Server Security** screen.
5. Choose desired option from the **Allow Action to React** field and press **Enter**.


```

Enable Real-Time Detection

Real-time detection allows Action to react automatically to security events
generated by Firewall and Screen. When enabled, these events are
checked against pre-defined rules, which trigger alert messages and/or
command scripts.

Action must be installed and running in order to take advantage of this
functionality.

Type options, press Enter.

Enable ACTION for Firewall . . 3      4=By Server definition
                                      1=Global override - Stop using ACTION
                                      2=Global override - Send rejects
                                      3=Global override - Send all

Enable ACTION for Screen . . . N      Y, N

F3=Exit  F12=Previous

```

Enable Real-Time Detection

| Option | Description |
|-----------------------------------|--|
| Enable Action for Firewall | 1 = Do not use Action
2 = Act only by rejects
3 = Act by all transactions
4 = Act by server. (default) |
| Enable Action for Screen | Y = Enable Screen protection
N = Do not enable Screen protection (default) |

SYSLOG

This feature sends security-related events from various IBM i facilities (such as logs and message systems) to a remote Syslog server according to range of severities like: emergency, alert, critical, error, warning and more.

By using **SYSLOG**, a user can decide whether he wants the SYSLOG to contain all of **Firewall** events (2=All), rejects only (1) or none (0).

SYSLOG

Send SYSLOG **2** 0=None, 1=Rejects, 2=All

Send *FYI (with *FYI in front) Y Y=Yes, N=No

Use option 81=iSecurity/Base from previous menu to define SYSLOG global parameters.

If you wish to send only certain events, either use the Action module with the SNDSYSLOG command, or specify a user filter program in the SYSLOG global parameters.

F3=Exit F12=Previous

SYSLOG

By using **Audit -> 81. System Configuration -> 21. Syslog Definitions**, a user can define when to send Syslog messages, to what IP address, from which facility (list of optional facilities below), in what range of severity (list below) and the format of the message.

Log retention

Determine how many days you want to keep the **Firewall** log.

The job GS#MNT is used to delete logs regarding the number of retention days. This job is placed as a job scheduler and is working at a specific time.

99 = *NOMAX (save and do not erase old history logs)

Log & Journal Retention

Type options, press Enter.

| | | |
|-----------------------------------|-------|-------------------|
| Log retention period (days) . . . | 99 | Days, 99=*NOMAX |
| Backup program for logs | *NONE | Name, *STD, *NONE |
| Backup program library. | | |

A specified backup program may run before deleting old logs. It will backup all data deleted after the retention period expires. The *STD (default) backup program is SMZ8/GRSOURCE GSLOGBKP.

F3=Exit F12=Cancel

Log & Journal Retention

Language Support

Double-Byte Character Set (DBCS) is a set of characters in which each character is represented by two bytes. These character sets are commonly used by national languages, such as Japanese and Chinese, which have more symbols than can be represented by a single byte.

There are two option: the default setting of 'N' (do not support DBCS), and 'Y' (support DBCS). Choose an option based on the relevant national language.

1. To work with iSecurity Language Support, select **91. Language Support** from the **iSecurity (part I) Global Parameters** screen. The **iSecurity Language Support** screen appears.
2. Set your desired parameter and press **Enter**.

```

iSecurity Language Support

Select one of the following:

DBCS system . . . . . N Y, N

F3=Exit  F12=Cancel
  
```

iSecurity Language Support

The Maintenance Menu

The Maintenance Menu enables the user to set and display global definitions for Security Part 1. To access the Maintenance Menu, select **82. Maintenance Menu** from the **Firewall** main menu.

```

GSMINTM                               Maintenance Menu                               iSecurity/Part 1
                                                                              System:  S520

Select one of the following:

iSecurity Part 1 Global                                Password Specific
 1. Export Definitions                                41. Copy Dictionary Language
 2. Import Definitions                                42. Import Dictionary Language
 5. Display Definitions                                General
Operators and Authority Codes                          51. Work with Collected Data
11. Work with Operators                                52. Check Locks
12. Work with Authority Codes                          53. Localize
                                                         59. *PRINT1-*PRINT9 Setup
Firewall Specific                                       Journal Files
21. Save Firewall Log                                  71. Add Journal
22. Set Firewall Defaults                              72. Remove Journal
25. Replace Firewall Users                             79. Display Journal
Screen Specific                                         Uninstall
31. Delete Activity Entries                            91. Uninstall Product
Selection or command                                   99. More ...

==> █

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

Maintenance Menu

iSecurity Part 1 Global

Export / Import Definitions

This option is useful in transferring configuration settings/definitions from one System i to another, when you need to distribute definitions between LPARs or different machines.

Firewall will export/import: IP addresses/ System names (SNA)/ Users/ Groups/ Applicant/ Locate/ Native & IFS/ Logon controls FTP-TELNET-Passthrough/ Prechecks DDM-DRDA/ Time groups and more.

```

Export iSecurity/Part 1 Defns. (EXPS1DFN)

Type choices, press Enter.

Collection type . . . . . █ *NEW, *ADD
Work library and SAVF in QGPL . *AUTO Name, *AUTO (S1 + System)
Firewall options . . . . . *SAME *ADD, *REPLACE, *BYSUBJECT...
Screen options . . . . . *SAME *ADD, *REPLACE, *BYSUBJECT...
General options . . . . . *SAME *ADD, *REPLACE, *BYSUBJECT...

Update remote systems:
  Systems to update . . . . . *NONE Name, *group, *ALL, *NONE
  Update type . . . . . *UPD *UPD, *REPLACE

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

Export iSec Part 1 Definitions (EXPS1DFN)

```

Import iSecurity/BASE Defns.  (IMPS1DFN)

Type choices, press Enter.

Input type . . . . . *SAVF      *LIB, *SAVF

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

Import iSec Part 1 Definitions (IMPS1DFN)

| Parameter or Option | Description |
|--------------------------------------|--|
| Work library and SAVF in QGPL | Destination of export library.
S1 (Security One) is default setting
Name= name of target library. |
| Firewall /Screen Options | Definitions pertaining to these two applications
*ADD = add to a previously imported/exported rule
*REPLACE = replace a previously imported/exported rule
*BYSUBJECT= import/export rules by subject (IP address, etc.) |
| Update remote systems | Systems to update= When exporting Firewall definitions, the user can choose to export and import at once by preparing the definitions in a SAVF and send it to a remote system or several remote systems, and automatically import them into it.
Update type
*UPD = add new records and replace existing
*REPLACE = clear the definition file and copy the new |
| Keep backup in library | Name= library where backup definitions are found |

Display Definitions

This feature enables the user to display and print iSecurity Part One definitions:

1. To display, select the desired report type from the **Display Security I Definitions** screen. After selecting report type, additional parameters appear.

2. Select choices and press **Enter**.

```

Display Security I Definitions (DSPS1DFN)

Type choices, press Enter.

Report type . . . . . █ *ALL, *CFG, *SRVR, *IPIN...

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

Display Security 1 Definitions

| Parameter or Option | Description |
|---------------------|--|
| Report type | *ALL = all general definitions
*CFG = per configuration
*SRVR = per server
*IPIN = per IP address |
| Format | *LIST = Short form
*DETAILS = full form |
| Output | Select correct print option. See *PRINT1- *PRINT9 Setup at the end of this chapter for details. |

Work with Operators

See *Modifying Operators'* **Chapter 2: First Steps** for a description of this feature.

Firewall Specifics

Save Firewall Log

Allows users to save the daily **Firewall** log in a SAVF format.

```

Save iSecurity Log (SAVLOGDAY)

Type choices, press Enter.

Save file . . . . . █      Name
Library . . . . .      *CURLIB  Name, *CURLIB
Date . . . . .      *CURRENT  Date, *CURRENT

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

Save Firewall Log

Replace Firewall Users

This option has 2 purposes:

1. Copy and delete the users' Firewall definitions and rules as defined in options 11, 12, 13, 21, 22, 31, 32, to another user profile.
2. Remove the user definitions and rules from the Firewall, using *REMOVE at the Replace to user field.

```

Replace FW user (RPLFWUSR)

Type choices, press Enter.

Replace from user . . . . . █      User, %Group
Replace to user . . . . .      USER, %Group, *REMOVE, *PRINT

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

Replace FW user (RPLFWUSR)

General

Work with Collected Data

Administrators can view summaries of **Audit**, **Firewall**, and **Action** journal contents by day, showing the number of entries for each day together with the amount of disk space occupied. Administrators can optionally delete individual days in order to conserve disk space.

1. To view summaries of audit journals, select **51. Work with Collected Data**. The **Work with Collected Data** screen appears.

Work with Collected Data

S720

Type options, press Enter.

Module █

1=Firewall
 2=Audit
 3=Action
 4=Capture

F3=Exit

Work with Collected data

2. Enter **1** (Firewall) and press **Enter**. The **Work with Collected Data – Firewall** screen appears.

| Work with Collected Data - Firewall | | | | | | S720 |
|-------------------------------------|----------------|---------|-----------|-----------|-----------|-----------------------|
| Type options, press Enter. | | | | | | Total Size (MB): 10.5 |
| 4=Delete | | | | | | |
| Opt | Collected Date | Records | Size (MB) | Save Date | Save Time | |
| █ | 13/11/08 | 20 | .0 | 15/12/08 | 20:28:16 | |
| — | 14/11/08 | 0 | .0 | 15/12/08 | 20:28:16 | |
| — | 15/11/08 | 0 | .0 | 15/12/08 | 20:28:16 | |
| — | 16/11/08 | 8 | .0 | 15/12/08 | 20:28:16 | |
| — | 17/11/08 | 171 | .1 | 15/12/08 | 20:28:16 | |
| — | 18/11/08 | 758 | .5 | 15/12/08 | 20:28:16 | |
| — | 19/11/08 | 964 | .7 | 15/12/08 | 20:28:16 | |
| — | 20/11/08 | 1,059 | .8 | 15/12/08 | 20:28:16 | |
| — | 21/11/08 | 16 | .0 | 15/12/08 | 20:28:16 | |
| — | 22/11/08 | 16 | .0 | 15/12/08 | 20:28:16 | |
| — | 23/11/08 | 537 | .4 | 15/12/08 | 20:28:16 | |
| — | 24/11/08 | 624 | .5 | 15/12/08 | 20:28:16 | |
| — | 25/11/08 | 682 | .5 | 15/12/08 | 20:28:16 | |
| — | 26/11/08 | 520 | .4 | 15/12/08 | 20:28:16 | |
| | | | | | | More... |
| F3=Exit F5=Refresh F12=Cancel | | | | | | |

Work with Collected Data - Firewall

3. Enter the correct options and press **Enter**.

Purging all data of FIREWALL

*RMVM SMZTMPA/GSCALP *ALL
CLRPFM SMZTMPA/GSSTTSP*

*PRINT1-*PRINT9 Setup

Firewall allows the user to define up to nine specific printers for printing output. These may be local or remote printers. ***PRINT1-*PRINT9** are special values which can be entered in the **OUTPUT** parameter of any commands or options that support printed output.

Output to any of the nine remote printers is directed to a special output queue specified on the ***PRINT1-*PRINT9 User Parameters** screen, which, in turn, directs the output to a print queue on the remote system. You use the **CHGOUTQ** command to specify the IP address of the designated remote location and the name of the remote output queue.

By default, two remote printers are pre-defined. ***PRINT1** is set to print at a remote location (such as the home office). ***PRINT2** is set to print at a remote location in addition to the local printer. In addition:

- ***PRINT3** creates an excel file.
- ***PRINT3-9** are user modifiable

To define remote printers, perform the following steps:

1. Select **82** from the main menu.

2. Select **59** from the **Maintenance** menu. The ***PRINT1-*PRINT9 User Parameters** screen appears.

Journal Product Definitions

Add Journal

Select option **71. Add Journal** to record the system physical files changes in the data library. The screen **Create Journal – Confirmation** appears. Press **Enter** to confirm.

```

GSMINTM                               Maintenance Menu                               iSecurity/Part 1
                                          System: S720
Select .....
: █                                     Create Journal - Confirmation :
iSecuri :                               :
  1. Ex : You are about to start journaling the product files.      : uage
  2. Im : The journal receivers will be created in library          : nguage
  5. Di : SMZ8JRND . If this library does not exist, it will        :
Operato : be automatically created.                                  : Data
  11. Wo :                                                           :
  12. Wo : If you wish to create the library in a specific ASP,      :
        : you should press F3=Exit, create this library, and        : p
Firewal : run again this option.                                     :
  21. Sa :                                                           :
  22. Se : Press Enter to start journaling, F3 to Exit.             :
Screen  :                                                           :
  31. De : F3=Exit                                                  :
        :                                                           :
Selecti :.....
==> 71

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

```

Create Journal – Confirmation

Remove Journal

Select option **72. Remove Journal** to end the journaling of changes in the system physical files. The **End Journal - Confirmation** screen appears. Press **Enter** to confirm.

```

GSMINTM                                     Maintenance Menu                               iSecurity/Part 1
                                                                 System:      S720

Select .....
: █                                     End Journal - Confirmation                               :
iSecuri :                                     :
1. Ex :   You are about to end journaling the product files.           : uage
2. Im :   The journaling will stop in library SMZ8JRND                 : nguage
5. Di :                                     :
Operato :   Press Enter to end journaling.                             : Data
11. Wo :                                     :
12. Wo :   F3=Exit                                                     :
:                                     : p
Firewal .....
21. Save Firewall Log                                           71. Add Journal
22. Set Firewall Defaults                                       72. Remove Journal
Screen Specific                                           79. Display Journal
31. Delete Activity Entries                               Uninstall
                                                                 91. Uninstall Product

Selection or command
==> 72

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
12 entries converted from journal SMZ8 in SMZTMPA.
  
```

End Journal - Confirmation

Display Journal

To view journalled files, select option **79. Display Journal**.

```

Display Journal Entries

Journal . . . . . : SMZ8          Library . . . . . : SMZTMPA

Type options, press Enter.
5=Display entire entry

Opt  Sequence  Code  Type  Object      Library      Job          Time
█      1      J    PR    AUACTIONP   SMZTMPA      QPADEV000V   13:48:01
-      2      D    JF    AUACTNPD   SMZTMPA      QPADEV000V   13:48:02
-      3      F    JM    AUACTNPD   SMZTMPA      QPADEV000V   13:48:02
-      4      D    JF    AULOGDJ    SMZTMPA      QPADEV000V   13:48:03
-      5      F    JM    AULOGDJ    SMZTMPA      QPADEV000V   13:48:03
-      6      D    JF    AULOGOUT   SMZTMPA      QPADEV000V   13:48:03
-      7      F    JM    AULOGOUT   SMZTMPA      QPADEV000V   13:48:03
-      8      D    JF    AUQSTN     SMZTMPA      QPADEV000V   13:48:03
-      9      F    JM    AUQSTN     SMZTMPA      QPADEV000V   13:48:03
-     10      D    JF    AUSELCP    SMZTMPA      QPADEV000V   13:48:03
-     11      F    JM    AUSELCP    SMZTMPA      QPADEV000V   13:48:03
-     12      D    JF    AUSELQPD   SMZTMPA      QPADEV000V   13:48:03
                                                                 More...

F3=Exit  F12=Cancel
  
```

Display Journal Entries

```

*PRINT1-*PRINT9 User Parameters

Type options, press Enter.
Using OUTPUT(*PRINTn) where n=1-9, provides extra control over prints.
Use this screen to specify parameters for this feature. This functionality can
be modified. For details see the original source SMZ8/GRSOURCE GSSPCPRT.

Press F14 for setup instructions

  OutQ      OutQ      Save
*PRINT  Name  Library  Hold  Description
  1  CONTROL  SMZTMPA  Y  N  OUTQ to print on the remote
  2  CONTROL  SMZTMPA  Y  N  Local+OUTQ that print on the remote
  3  _____  _____  -  -  _____
  4  _____  _____  -  -  _____
  5  _____  _____  -  -  _____
  6  _____  _____  -  -  _____
  7  _____  _____  -  -  _____
  8  _____  _____  -  -  _____
  9  _____  _____  -  -  _____

Bottom

F3=Exit  F8=Print  F12=Cancel  F14=Setup instructions

```

*PRINT1-*PRINT9 User Parameters

- Enter the name of the local output queue and library as shown in the above example. The user may optionally enter a description.

| Parameter | Description |
|--------------|--|
| * Print | Printer number |
| OutQ Name | Name of the local output queue |
| OutQ Library | Name of the local output queue's library |
| Save | Y= yes
N = no |
| Hold | Y= yes
N = no |
| Description | Optional text description |

- Enter the following command on any command line to direct output to the remote printer. This assumes that the designated output queue has already been defined.

```

CHGOUTQ OUTQ('local outq/library') RMTSYS(*INTNETADR)
+ RMTprtQ('outq on remote') AUTOSTRWTR(1) CNNTYPE(*IP) TRANSFORM(*NO)
+ INTNETADR('IP of remote')

```

| Parameter | Description |
|-------------|---------------------------------|
| QUTQ() | Name of the local output queue |
| RMTprtQ() | Name of the remote print queue |
| INTNETADR() | IP address of the remote system |

NOTE: Press **F14** for Setup instructions

If the desired output queue has not yet been defined use the **CRTOUTQ** command to create it. The command parameters remain the same.

For example, **PRINT1* in the above screen, the following command would send output to the output queue 'MYOUTQ' on a remote system with the IP address '1.1.1.100' as follows:

```
CHGOUTQ OUTQ(CONTROL/SMZTMPA) RMTSYS(*INTNETADR)
+ RMTPRTO(MYOUTQ) AUTOSTRWTR(1) CNNTYPE(*IP) TRANSFORM(*NO)
+ INTNETADR(1.1.1.100)
```

Uninstall

Choose **91. Uninstall Product** from the **Maintenance** Menu, and follow the directions on the screen.

```

Uninstall SECURITY1P

You are about to uninstall this product.
All program files, data and definitions will be deleted.
You are advised to print this screen for further reference.
Before proceeding, ensure that:
  o The product has been entirely de-activated
  o IPL was done
  o No user or batch job is working or intends to work with this product

To run uninstall procedure you should do the following:
  o Exit from the current session
  o Open a new session using QSECOFR or equivalent user profile
  o Enter: CALL SMZ8/GRRMVPRD

Once the uninstall is completed, enter: DLTLIB SMZ8
Backups of previous releases might exist under the name QGPL/P_SMZ*
To confirm proper uninstall, use DSPUSRPRF SECURITY1P TYPE(*OBJOWN)

F3=Exit
  
```

Uninstall SECURITY1P

iSecurity Central Administration

Option **83. Central Administration** allows running reports in 2 different ways:

```

GSCNTMN      iSecurity Central Administration - Firewall  iSecurity/CntAdm
                                                    System: S720

Select one of the following:

Definitions    Use SYSTEM() in the reporting menu to run reports on the network
1. Work with network definitions

Log Copy       Add a 3 character extension of your choice to data library name
11. Run Reports on a Copy of Remote System Log

Transfer Log Copy
21. Export Product Log
22. Import Product Log, Collect from Remote

Transfer Definitions
31. Export Definitions, Update Remote Systems
32. Import Definitions

Communication Log
71. Current Job CntAdm Messages
72. All Jobs CntAdm Messages

Selection or command
==> █

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

iSecurity Central Administration – Firewall

1. To get current information from existing report or query. Adjusting the system parameters only, to collect information from all the groups in the system to output file that can be sent via email, select option **1. Define Communication Attributes**. The **Work with Network Systems** screen appears.
2. Press **F6** to define a new network system to work with and press Enter to **confirm**.


```

Add Network System

Type choices, press Enter.

System . . . . . █      Name
Description . . . . .      *Name
Group where included . . .      *Name

Communication Details
Type . . . . . *IP      *SNA, *IP
IP or remote name . . . . .

Mode (for *SNA) . . . . . *NETATR      Name, *NETATR

F3=Exit      F12=Cancel

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

Add Network System

- To run the reports on a copy of data library of a remote system, select option 11. **Select a Copy, run Reports.** The **Running Locally on a Copy of a Remote System** screen appears displays the system's information and shows libraries which start with SMZ4DTA* or SMZTMPA*

```

Running Locally on a Copy of a Remote System      S720
iSecurity/Audit

Type options, press Enter.
1=Select

Opt  Ext  System  Text
>    005  S150    iSecurity/1: Firewall, Screen, PWD & WideScope A
█      SMZTMPA lib of S150

Bottom

This option allows you to run locally on a copy of the data of a remote system.
Alternatively, you may use the standard reporting system specifying SYSTEM(),
to report the current status of a single system or group of systems in either
a merged or non-merged report.
F3=Exit to *CURRENT system      F12=Cancel
  
```

Running Locally on a Copy of a Remote System

Note:

NOTE: Running on multiple systems with either of the following:

- Merge data to a single output . MRGDTA(*NO),
- Place output on OUTON(*SYSTEM)

valid for *, *PRINT-*PRINT9 only.

Selecting other output types such as *HTML, *PDF... may result in unexpected results.

- To create a distribution package of the definitions created (export) select options **21. Create a Distribution Package**. The **Export iSecurity/Part 1 Defns. (EXPS1DFN)** screen appears

Export iSecurity/Part 1 Defns. (EXPS1DFN)

Type choices, press Enter.

| | | |
|----------------------------|-----------------|-------------------------------|
| Target library: | | |
| Prefix | <u>S1</u> | Name |
| Name | <u>*SYSNAM</u> | Character value |
| Firewall options | <u>*REPLACE</u> | *ADD, *REPLACE, *BYSUBJECT... |
| Screen options | <u>*REPLACE</u> | *ADD, *REPLACE, *BYSUBJECT... |
| General options | <u>*REPLACE</u> | *ADD, *REPLACE, *BYSUBJECT... |

Bottom

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

F24=More keys

Export iSecurity/Part 1 Defns. (EXPS1DFN)

- To restore a distribution package of the definitions created (import) select options **22. Restore a Distribution Package**. The **Import iSecurity/Part 1 Defns. (IMPS1DFN)** screen appears

Import iSecurity/Part 1 Defns. (IMPS1DFN)

Type choices, press Enter.

| | | |
|----------------------------------|-----------------|-------------------------------|
| From library | <u>S1BACKUP</u> | Name |
| Keep backup in library | <u>*REPLACE</u> | Name, *NONE |
| Firewall options | <u>*REPLACE</u> | *ADD, *REPLACE, *BYSUBJECT... |
| Screen options | <u>*REPLACE</u> | *ADD, *REPLACE, *BYSUBJECT... |
| General options | <u>*REPLACE</u> | *ADD, *REPLACE, *BYSUBJECT... |

Bottom

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

Import iSecurityPart 1 Defns. (IMPS1DFN)

Appendix: List of Firewall Exit Points

- **iSecurity for System i** protects all the security-related exit points.
- In order to display all the exit points, use command WRKREGINF.
- Sign On: **iSecurity** is the **only** iSeries security solution that checks all green screen signons, both by IP address and by screen name.

Following is a list of the 53 security-related exit points covered by iSecurity.

Note that some exit points are interconnected.

| | |
|--------------------------|--|
| 1. QIBM_QTF_TRANSFER | Original File Transfer Function- TRAN0100 |
| 2. QIBM_QTMF_SVR_LOGON | FTP Server Logon- TCPL0100 |
| 3. QIBM_QTMF_SVR_LOGON | FTP Server Logon- TCPL0200 |
| 4. QIBM_QTMF_SVR_LOGON | FTP Server Logon- TCPL0300 |
| 5. QIBM_QTMF_SERVER_REQ | FTP Server Incoming Request Validation-VLRQ0100 |
| 6. QIBM_QTMF_CLIENT_REQ | FTP Client Outgoing Request Validation-VLRQ0100 |
| 7. QIBM_QTOD_SERVER_REQ | TFTP Server Request Validation-VLRQ0100 |
| 8. QIBM_QTMX_SVR_LOGON | REXEC Server Logon- TCPL0100 |
| 9. QIBM_QTMX_SVR_LOGON | REXEC Server Logon- TCPL0300 |
| 10. QIBM_QTMX_SERVER_REQ | REXEC Server Request Validation-VLRQ0100 |
| 11. QIBM_QRQ_SQL | Original Remote SQL Server- RSQL0100 |
| 12. QIBM_QZDA_SQL1 | Database Server- SQL Access & Showcase- ZDAQ0100 |
| 13. QIBM_QZDA_SQL2 | Database Server- SQL Access- ZDAQ0200 |
| 14. SC_QUERY_ROW_SEC | Database Showcase- SCRS0100 |
| 15. QIBM_QZDA_NDB1 | Database Server- data base access- ZDAD0100 |
| 16. QIBM_QZDA_NDB1 | Database Server- data base access- ZDAD0200 |
| 17. QIBM_QZRC_RMT | Remote Command/Program Call- CZRC0100 |
| 18. QIBM_QPWFS_FILE_SERV | File Server- PWFS0100 |
| 19. QIBM_QTG_DEVINIT | Telnet Device Initialization- INIT0100 |
| 20. QIBM_QTG_DEVTERM | Telnet Device Termination- TERM0100 |
| 21. QIBM_QWT_JOBNOTIFY | Sign-on Completed- NTFY0100 |
| 22. QIBM_QTMT_WSG | WSG Server Sign-On Validation- QAPP0100 |
| 23. QIBM_QHQ_DTAQ | Original Data Queue Server- DTAQ0100 |
| 24. QIBM_QZHQ_DATA_QUEUE | Data Queue Server- ZHQ00100 |
| 25. QIBM_QVP_PRINTERS | Original Virtual Printer Server- PRNT0100 |

| | |
|--------------------------|--|
| 26. QIBM_QLZP_LICENSE | Original License Mgmt. Server- LICM0100 |
| 27. QIBM_QZSC_LM | Central Server- License Mgmt.- ZSCL0100 |
| 28. DDM | Network Attribute- DDM Requested Access-DDMACC |
| 29. DRDA | Network Attribute- Display Requested Database Access- DDMACC |
| 30. QIBM_QZSC_NLS | Central Server- Conversion Map- ZSCN0100 |
| 31. QIBM_QZSC_SM | Central Server- Client Mgmt.- ZSCS0100 |
| 32. QIBM_QNPS_ENTRY | Network Printer Server- entry- ENTR0100 |
| 33. QIBM_QNPS_SPLF | Network Printer Server- spool file- SPLF0100 |
| 34. QIBM_QMF_MESSAGE | Original Message Server- MESS0100 |
| 35. QIBM_QZDA_INIT | Database Server- entry- ZDAI0100 |
| 36. QIBM_QZDA_ROI1 | Database Server- object information- ZDAR0100 |
| 37. QIBM_QZDA_ROI1 | Database Server- object information- ZDAR0200 |
| 38. QIBM_QSY_CHG_PROFILE | Change User Profile- CHGP0100 |
| 39. QIBM_QSY_CRT_PROFILE | Create User Profile- CRTP0100 |
| 40. QIBM_QSY_DLT_PROFILE | Delete User Profile- after Delete- DLTP0100 |
| 41. QIBM_QSY_DLT_PROFILE | Delete User Profile- before Delete- DLTP0200 |
| 42. QIBM_QSY_RST_PROFILE | Restore User Profile- RSTP0100 |
| 43. QIBM_QZSO_SIGNONSRV | TCP Signon Server- ZSOY0100 |
| 44. QIBM_QWC_PWRDWN SYS | Prepower Down System- PWRD0100 |
| 45. QIBM_QTOD_DHCP_ABND | DHCP Address Binding Notify- DHCA0100 |
| 46. QIBM_QTOD_DHCP_ARLS | DHCP Address Release Notify- DHCR0100 |
| 47. QIBM_QTOD_DHCP_REQ | DHCP Request Packet Validation- DHCV0100 |
| 48. QRMTSIGN | System Value- Remote Signon Control |
| 49. QPWDVLDPGM | System Value- Password Validation |
| 50. QIBM_QP0L_SCAN_OPEN | IFS Scan on Open- SCOP0100 |
| 51. QIBM_QP0L_SCAN_CLOSE | IFS Scan on Close- SCCL0100 |
| 52. QINACTITV | System Value- Inactive Job Timeout |
| 53. QINACTMSGQ | System Value- Inactive Job MessageQ |

Thank you for using iSecurity Firewall.

If you have any questions or problems, please contact:

Emails:

marketing@razlee.com

support@razlee.com

Raz-Lee New York

Tel: 1-888-RAZLEE-4

Tel: 1-888-RAZLEE-2

Raz-Lee Israel

Tel: +972-9-9588860