iSecurity

Firewall™

The Network Security Solution

Software Version: 17.32

Updated: December 11, 2016

RAZ-LEE™

The iSeries Security Experts

Copyright Notice

Visit our web site at www.razlee.com.

Record your product authorization code here.

Computer Model	
Serial Number	
Authorization Code	

Table of Contents

1 About This Manual

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

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 IBM i experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

Printed Materials

This user guide is the only printed documentation necessary for understanding this product. It is available in user-friendly PDF format and may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: http://www.adobe.com/.

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

Typography Conventions

The following conventions are used for ease in understanding the information types presented.

- IBM i commands system messages, menu options, field names, function key names are written in **Arial Bold**.
- References to chapters or sections and emphasis are written in ***Italic.***
- Key combinations are separated by a dash, for example: Shift-Tab.

iSecurity Product Suite

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the-box" security.

The iSecurity Product Suite includes:

Product	Description
Firewall (this product) 	Firewall protects and secures all types of access, to and from the System i, within or outside the organization, under all types of communication protocols. Firewall manages user profile status, secures entry via predefined entry points, and profiles activity by time. Its Best Fit algorithm determines the validity of any security-related action, hence significantly decreasing system burden while not compromising security.
Change Tracker - NEW 	Change Tracker automatically tracks modifications in the software and file structure within production libraries. Changes are tracked at both the object and source levels. It does not require any special actions by programmers.
DB-Gate - NEW 	**Direct IBM i Client-only Access to Non-DB2 Databases** DB-Gate empowers IBM i customers with exciting data access capabilities, based on Open Database Connectivity (ODBC), employing standard IBM i facilities to enable fully database-transparent access to remote systems.
COMMAND 	COMMAND monitors and filters commands and its parameters before they are run, enabling you to control each parameter, qualifier or element, in conjunction with the context in which it is about to run. Options include Allow, Allow with Changes and Reject. It includes a comprehensive log, proactive alerting and easily integrates with SIEM.
Authority On Demand 	Authority on Demand (AOD) provides an advanced solution for emergency access to critical application data and processes, which is one of the most common security slips in System i (IBM i) audits. Current manual approaches to such situations are not only error-prone, but do not comply with regulations and often-stringent auditor security requirements.

Product	Description
Capture 	Capture silently captures and documents user screens for tracking and monitoring, without any effects on system performance. It also preserves job logs for subsequent review. Capture can run in playback mode and can be used to search within texts.
AP-Journal 	AP-Journal automatically manages database changes by documenting and reporting exceptions made to the database journal.
Anti-Virus 	Anti-Virus is a dedicated iSeries-specific product engineered to provide full protection to the server, its file contents, and resident iSeries or System i dedicated software.
Visualizer 	Visualizer is an advanced DWH statistical tool with state-of-the-art technology. This solution provides security-related data analysis in GUI and operates on summarized files; hence, it gives immediate answers regardless of the amount of security data being accumulated.
Audit 	Audit is a security auditing solution that monitors System i events in real-time. It includes a powerful query generator plus a large number of predefined reports. Audit can also trigger customized responses to security threats by means of the integrated script processor contained in Action.

Product	Description
View 	View is a unique, patent-pending, field-level solution that hides sensitive fields and records from restricted users. This innovative solution hides credit card numbers, customer names, and so on. Restricted users see asterisks or zeros instead of real values. View requires no change in existing applications. It works for both SQL and traditional I/O.
Screen 	Screen protects unattended terminals and PC workstations from unauthorized use. It provides adjustable, terminal- and user-specific timeout capabilities.
Password 	Password provides a first-tier wall of defense for users by ensuring that user passwords cannot be easily cracked.
Assessment 	Assessment checks your ports, sign-on attributes, user privileges, passwords, terminals, and more. Results are instantly provided, with a score of your current network security status with its present policy compared to the network if iSecurity were in place.

New Features in Firewall Versions

Additions in Firewall 17.32

- The DBOPEN/SQL Exit Point Setting (**STRFW 1 > 2**) has been enhanced to include "Control by Exit-Point".
- A new option exists in **STRFW > 1 > 9. Work with Database SQL Server Jobs**.
- The DSPFWLOG option in **STRFW > 41 > 1 Additional Message Information** has new updates.
- **STRFW > 11** now includes a new SQL verb Merge record status.
- **DSPFWLOG TYPE(*TELNET)** provides Info. about Server IP.
- **STRFW 81 > 1/2 Export /Import Definitions** parameters moved to definitions screen.

Additions in Firewall 17.31

- The DBOPEN/SQL Exit Point Setting (**STRFW 81 > 10**) has been enhanced. While DB-OPEN has superiority over SQL exit point in performance and accuracy of analysis, SQL statements which do not involve OPEN of files cannot be recorded by its use. New features were added to enable simultaneous use of the two exit points to allow the full monitoring of activity and still preserve the advantages of each.

Options 7 and 8 were added, so the product now allows:

1=DBOPEN All files

2=DBOPEN Audited files

7= DBOPEN All files + the ability to monitor SQL statements that cause no OPEN

8= DBOPEN Audited files + the ability to monitor SQL statements that cause no OPEN

9=SQL

Selecting option 7 or 8, where both exit points are used, SQL setting can accept:

1=All operations

2=Non DBOPEN operations

Should be set to **2=Non DBOPEN operations**.

Note that it is possible to set DBOPEN to monitor only pre-selected files. This will dramatically reduce the number of time this exit point is being alerted by the operation system, providing a performance improvement.

1. To enable DBOPEN to monitor only pre-selected files, select option 2 or 8.
2. You must also pre-select files to be monitored by use of **STRFW 21 > 51** or by other methods which sets these file audit attribute to *CHANGE or *READ. Doing so does not mean that the Audit module should be set to include entries which may be generated as per this definition.

- Firewall as well as all iSecurity modules allow tracing of product definitions by use of DB-Journaling and the completely free use of the AP-Journal for this reporting.

To enable this option, follow:

1. Set definition files to be journaled (**STRFW 82 > 71**)
2. Set Global Installation (**STRFW 89 > 59**)
   - Auto jrn def files on install = Y

- Use AP-Journal to trace def chgs =Y

3. Trace changes (**STRFW 82 > 79**)

- A generic Base Support menu has been added in the product (**STRFW 89**). This screen integrates many functionalities which cross different modules of iSecurity.
- Email now contain an address book for names and lists of Emails (**STRFW 89 > 1**). Usage of names is allowed in all places where Email addresses can be entered. Definition of Email has been unified for most products (**STRFW 89 > 2**).
- The Email configuration screen (**STRFW > 89 > 2**) now supports **F10=Verify E-mail configuration**. Selecting this option will result in sending a mail to the Product-Admin Email that is defined in Global Installation Defaults (**STRFW > 89 > 59**).
- The ZIP parameter has been added to the report generator command. It can be secured by using a password. When using the Report Scheduler, it is possible to specify ZIP in the group definition. Doing so will ZIP all following report output to a single ZIP file.
- "No Data" notification added to Email subject of empty reports as security is based on exception identification, this addition saves time as there is no need to open empty reports.
- In Syslog definitions (**STRFW 81 > 32/33/34**), the SYSLOG message is now enabled for multiple SIEM messages and message structures using built-in as well as mixed variables and constants. The feature enables adjustable Port, Severity, Facility and Length while offering UDP, TCP and TLS (encrypted) support in CEF and LEEF and user editable modes, using filters for relevant fields.
- Processing of SIEM is done on a separate job per SIEM. A buffer exists to allow intermediate communication problems, or SIEM downtime. Once this buffer is full, the processing is not delayed. A message is then sent to QSYSOPR, and an attempt to reconstruct communication is made periodically and consistently. **Note**: Such problems might cause a loss of a number of messages.
- In Global Installation Defaults (**STRFW > 89 > 59**), a SYLOG source Port/IP field has been added (UDP only).
- LEEF - a standard used by IBM QRadar, as well as CEF - a standard used by HP ArcSight and others- are now supported. Both offer the sending of data in Field Mode by pairs of Field name and Field value.
- iSecurity supports all QAUDJRN messages and all Firewall (network security) messages. Formatting is by Audit Type and Sub type or by Firewall server. In this way, for audit types that represent different activities, e.g. Type OM with sub types: M-Move and R-Rename, only relevant fields will be sent.
- QHST, QSYSOPR and any other Message Queue are supported in LEEF and CEF field mode.
- Standard message support, i.e. message edited with its replacement values is preserved. This enables sending information in any free format as well as LEEF and CEF.
- The Work with Queries (**STRFW 41 > 1**) enables exporting selective queries. To do so select **X=Export** for one or many queries, in one or more instances. When **F3=Exit** is pressed, a screen is displayed allowing the user to specify the target system or systems group (Multi System must be available). Alternatively, *NONE can be entered. *NONE will display the name of the *SAVF that is created, and the Import command parameters that are required on the report system to load the exported reports. With *NONE it is the customer's responsibility to transfer the *SAVF to the target systems.
- A new function (**STRFW 82 > 93**) enables technicians to load a full set of reports (i.e. files AUSELQP and AUSELCP from SMZ4DTA) to a user defined library and select which reports to copy from it. Once selected, the user has to select the from and to libraries, and after pressing Enter, the list of reports in the From library is displayed. This option may be

important, for example, when some reports have been accidentally deleted, and there is a need to load them from a backup.

- The Query Generator has been enhanced to support in the area of sorting information and the layout of sorted data:
  - Break after change of a specified number of key fields will cause a subtitle to appear when a change is encountered. Fields that appear on the subtitle will be omitted from detail lines.
  - Sort order can be defined as A=Ascending D=Descending
  - Records to include can be 1=All 2=One record per key.
    (This existing item is mentioned for completeness purpose)
  - When a query is run on multiple systems, the System field containing the system name will be implicitly added to the printed fields, if it is not there.
- Firewall now present improved possibilities to report product definitions:
  - The standard Print Definition option has been enhanced to provide a single spool file to include all the different definitions.
  - The menu provides a separate entry for reporting Firewall Definition (**STRFW 42**)
  - A new query was added to the Firewall Definition Query Generator (which includes HTMP, PDF, Email) to include the Definitions of Firewall:
    - Z$9_FWDFN $9 Firewall definitions
- This option has been enhanced and reshaped. Among the enhancements:
  - Product-Admin Email
  - Add SYSTEM to query mail subject

Additions in Firewall 17.27

- In the Definitions of IFS Object Usage (**STRFW > 22 > 1)** defining a generic entry for the directory allows the directory subtree to inherit In-product IFS authorities, according to the definitions in the Additional Definitions screen (**STRFW > 81 > 2**).
- In the Syslog definitions (**STRFW > 81 > 71**), variable **&6** now represents the IP and not the Product ID.
- In the Native Object Security menu (**STRFW > 21**), in options **1 – 6**, when opening a new definition with **F6**, there is now no validation on the Library. Previously, you could not enter ***USRLIBL** as the Library.

Additions in Firewall 17.22

- When defining Users and Groups, you can now limit them to single IP address. From that IP address, they will be allowed to work with as many sessions as necessary.
- The process for running a second Network Security system in parallel to Firewall has been improved.

NOTE: Because this option involves running other vendor programs, it is provided as a service which carries no warranty for its consequences.

Additions in Firewall 17.17

- Firewall now supports using **TLS** (Transport Layer Security) to transport Syslog messages.

Additions in Firewall 17.15

- The Open Database Settings interface has been improved and renamed as the DBOPEN / SQL Exit Point Setting.
- In the Firewall **Additional Settings** screen, the **Skip all activity for users** parameter has been renamed to **Skip activities of user or grpprf**.
- In the Work with Operators screen, there is now an option to copy a definition from one user to another, enabling you to set up rules quickly for new users.
- In the definitions of both Server security settings and User security settings, the rules for DBOPEN now follow immediately after the rules for SQL.
- In the definitions of native object security, you can now add exception rules for commands.

Additions in Firewall 17.05

- Groups are now available in Wizards. See Using the Rule Wizards on page 27 and General Definitions on page 192 for further details.
- Group profiles are now available for TCP/IP port restrictions. See Work with TCP/IP Port Restrictions on page 186.
- DBOPEN SQL CLI verb is now supported.

Additions in Firewall 17.04

- The maximum number of days for log and journal retention has been increased from 98 to 9998 days. The *NOMAX value has been changed from 99 days to 9999 days. Upgrading the system will automatically change values of 99 to 9999. For more information, see Log Retention on page 205.
- The Firewall maintenance night job GS#MNT now checks automatically for authorization codes expiration. Where appropriate, a message is sent to the QSYSOPR message queue. For temporary or rental authorization codes, no code or permanent codes are not checked.

Additions in Firewall 17.03

- The Swap user profile mechanism when checking network accesses is now at the object level. Until now the support for check authority to objects was done by a different user inside Firewall as a logical replacement. With this enhancement, Firewall actually performs a real swap operation. That is, Firewall passes a different user profile name to the IBM i operating system; the user profile to which Firewall is swapping must be allowed access to the specific server and object within Firewall. For more information, see Create a Swap User Profile Rule on page 131.
- A new Query has been added to allow you to report on the Definitions of Native Object Security. When you define the new query, set the **Server ID** to **1K** and the **Description** to **FW-DFN Native Object Security**. For details about adding queries, see Query Wizard on page 84.

Additions in Firewall 17.00

- Support for IPv6
- Changes in menus to allow for more efficient working and to remove redundancies
- Support for Showcase version 9.0
- Crash bypass - If the job responsible for writing to the log fails for any reason, it will not crash; the log will automatically write directly to GSCALP

- The **Display Firewall Log** command (**DSPFWLOG**) (**11. Display Log** in the Reporting Menu), now uses standard SQL instead of IBM Query to build the log
- The Incoming IP Addresses option in the Dynamic Filtering menu (**STRFW --> 2 --> 1**) now supports incoming IP address *LCL

2 Introducing Firewall

What is Firewall?

Firewall is a comprehensive network security solution for the IBM i (AS/400) that completely secures your system against external threats initiated via the network, and also controls permitted user activities after access is granted. Firewall is a robust, cost-effective security solution.

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

Although Firewall was not designed to protect your command line usage. It will secure the STRSQL command line usage to various tables.

Why is Firewall Necessary?

Originally the IBM 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 IBM i 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, laptops, distributed databases, Internet and web technologies, closed computing environments are basically extinct. Technological advances compelled IBM to open up the IBM i and its 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 that solution!

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 formulates a minimal number of rules for achieving maximum security and the system applies these rules to transactions; the unique design behind Firewall leads to checking far fewer transactions than competitive 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 additional rules for the particular situation. The following drawing illustrates this concept.

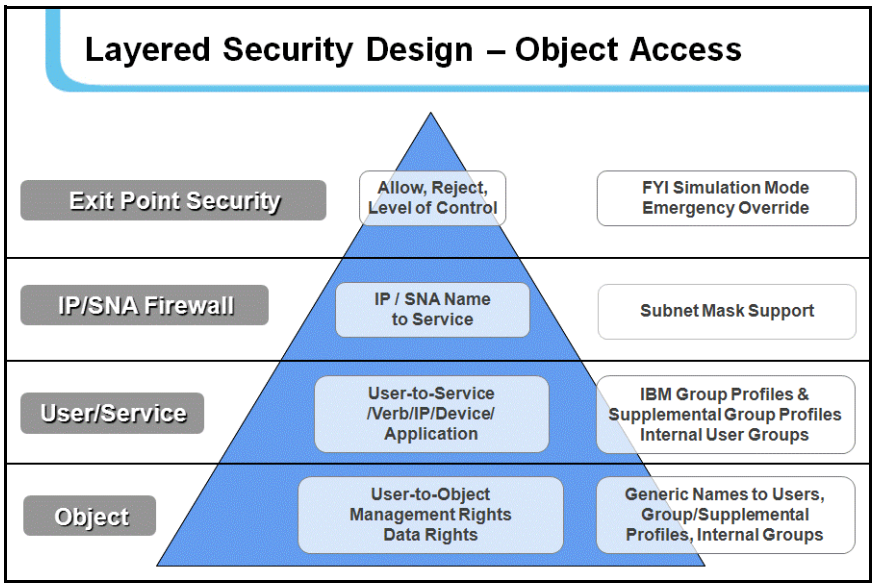


Figure 2-1. Layer Security Design - Object Access

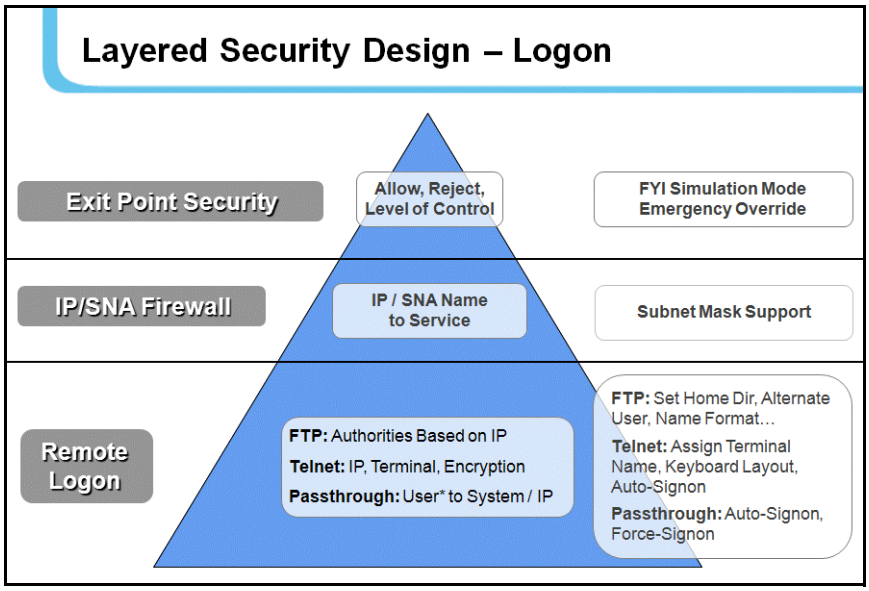


Figure 2-2. Layered Security Design - Logon

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, you 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. Users 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. Users 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 Getting Started on page 17.

User Security

Firewall offers optimized basic user security. Defining a single user security definition can be performed as described in the following table. See User Security on page 115 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

Method	Description
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

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 Configuration and Maintenance on page 191.

Native IBM i 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)
- Display Firewall user activity (DSPFWUSRA)

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**

3 Getting Started

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 Users, 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.

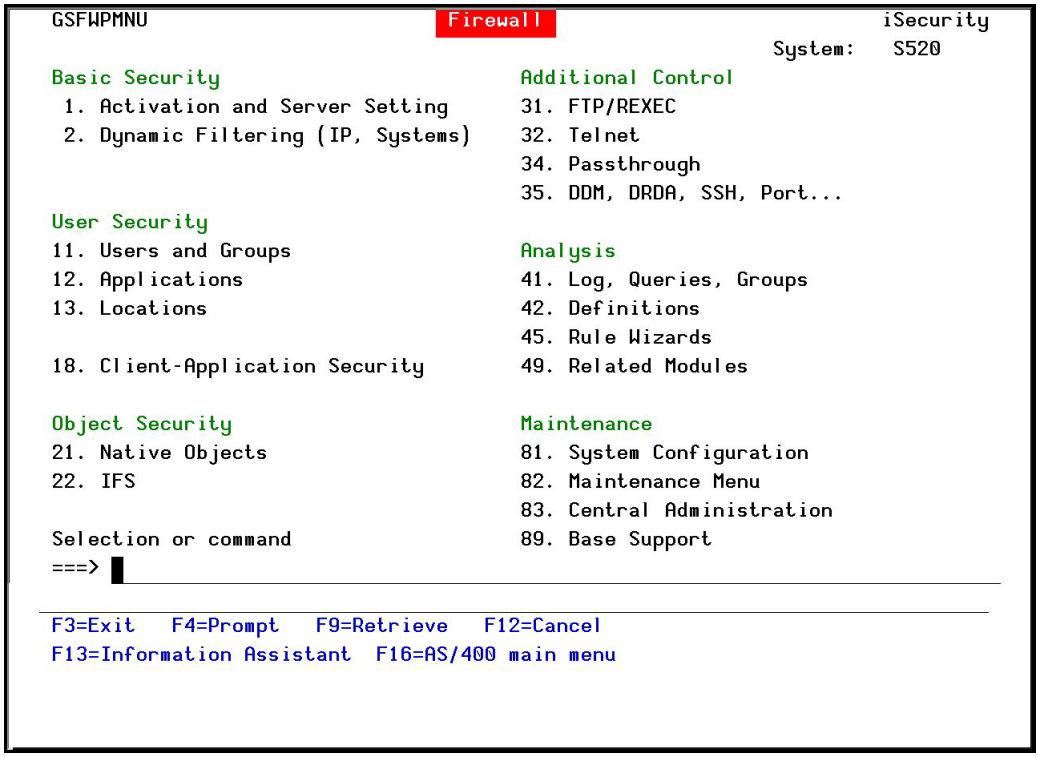


Figure 3-1. Firewall Main Menu

Managing Operators Authorities

The Operators authorities' management is now maintained from one place for the entire iSecurity product suite 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 do not have all object authority. the 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.

Modifying Operators Authorities

To modify operators' authorities:

1. Select **89 > 11. Work with Operators**. The **Work with Operators** screen appears.

```
                              Work with Operators

Type options, press Enter.
  1=Select   3=Copy    4=Delete
             Auth.level: 1=*USE, 3=*QRY(FW,AU,CT), 5=*DFN(CT,EN), 9=*FULL
   User       System  FW SC PW CM AV AU AC CP JR VW VS RP NO CT PR UM EN ADM
_  *AUD#SECAD S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9
_  *AUDIT     S520                 9  9  9  9  9     9
_  *SECADM    S520     9  9  9     9                 9  9                 9
_  ALEX       S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9     9
_  AU         S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9     9
_  AV         S520     9  9  9     9  9  9  9  9  9  9  9  9  9  9  9  9  9
_  EVGTST     S520     9  9  9     9  9  9  9  9  9  9  9  9        9  9  9
_  JAVA       S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9
_  JR         S520     9  9  9     9  9  9  9  9  9  9  9  9  9     9     9
_  LOWUSR     S520
_                                                                    More...
FW=Firewall    SC=Screen   PW=Password   CM=Command     AU=Audit      AC=Action
AV=Antivirus   CP=Capture  JR=Journal    VS=Visualizer  UM=User Mgt.  ADM=Admin
RP=Replication NO=Native Obj.Compliance  CT=Chg Tracker PR=Pwd Reset  VW=View
EN=Encryption/Tokenization

F3=Exit    F6=Add new    F8=Print   F11=*SECADM/*AUDIT authority   F12=Cancel
```

Figure 3-2. Work with Operators Screen

2. Open a Modify/Add New Operator screen by doing one of the following:

- To modify an existing operator, type **1** next to that operator and press **Enter**.
- To copy an existing operator, type **3** next to that operator and press **Enter**.
- To add a new operator press **F6**.

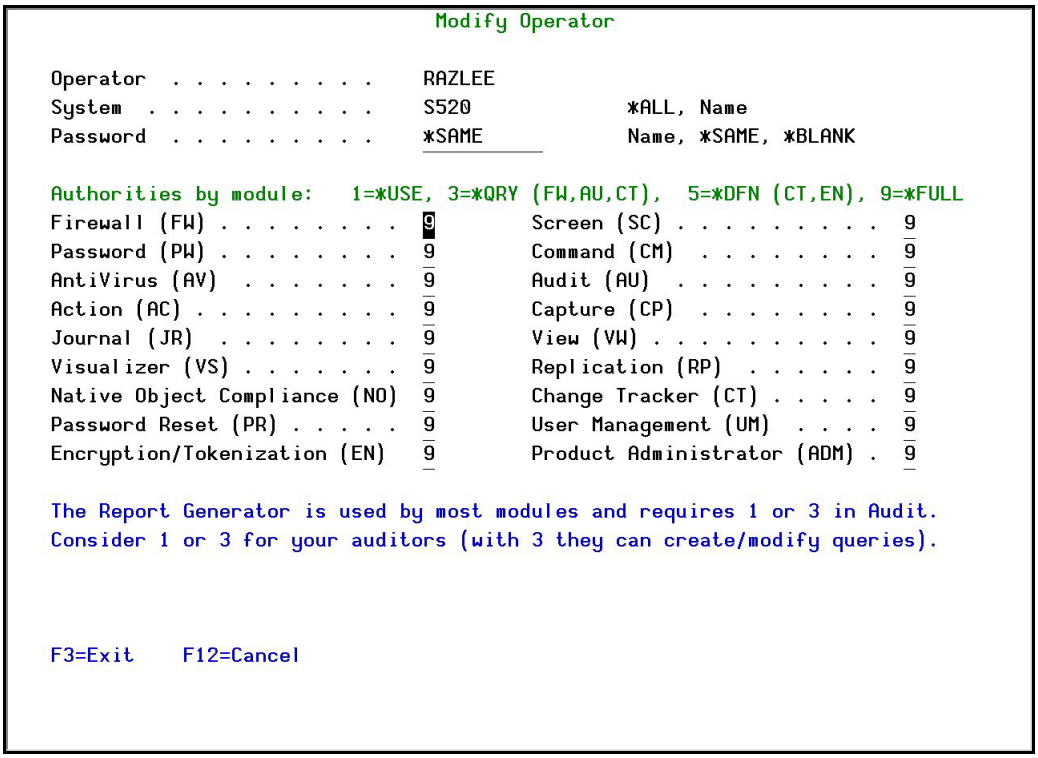


Figure 3-3. Modify Operator Screen

Field	Description / Options
Operator	Name of the operator
System	System the operator is using
Password	**Name** = Password **Same** = Same as previous password when edited <*blank*> = No password
FW	Firewall
SC	Screen
PW	Password
AV	Anti-virus
AU	Audit
AC	Action
CP	Capture
JR	Journal
VW	View
VS	Visualizer
UM	User Management
ADM	Admin

Field	Description / Options
RP	Replication
NO	Native Object Security
CT	Change Tracker
PR	Password Reset
EN	Encryption/Tokenization

Authorities	
1 = *USE	Read authority only.
9 = *FULL	Read and Write authority.
3 = *QRY	Run Queries. For auditor use.
5 = *DFN	Specific to the Firewall product.

Function Keys	
F6=Add new	
F8=Print	
F11=*SECADM/*AUDIT authority	

3. Set authorities and press **Enter**.

   The user being added/modified is 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** while 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.

NOTE: The SECURITY_P users are the owners of all product objects, where _ is replaced by the single character that is the appropriate library identifier (SMZ1, SMZ 2, and so on). Each library can contain several products.

A - Agent for Power-i
B - DB-Gate
T - Change Tracker
1 - Firewall, Screen, PWD
2 - Audit, Action
3 - View
4 - Journal
5 - AntiVirus
7 - Capture
8 - Authority on Demand

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. They can also enable FYI individually for specific function servers as a parameter in server security rules. In this manner, you 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 > 1. General Definitions**. The **General Definitions** screen appears.

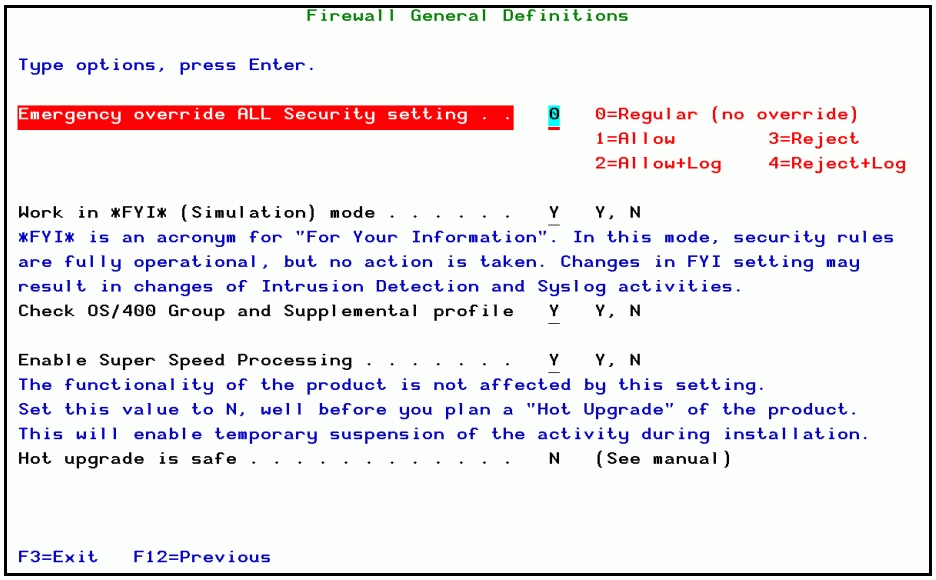


Figure 3-4. Firewall General Definitions Screen

Fields	Description
Emergency override ALL Security Setting	This option allows you to override all of the Firewall security settings.
Work in *FYI* (Simulation) mode	Security rules are fully operational, but no action is taken. Changes in FYI setting may result in changes of Intrusion Detection and Syslog activities.
Check OS/400 Group and Supplemental profile	Set to **Y** to ensure both group profile and the supplemental groups' authorizations are checked. It is sufficient to have permission for a service in one of the groups.
Enable Super Speed Processing	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.

Fields	Description
Hot upgrade is safe	Allows an update to be 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**.

Options	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.

2. Type **0** for regular Firewall settings.
3. Set **Work in FYI (Simulation) Mode** to **Y**.

NOTE: You may leave the **Work in FYI (Simulation) Mode** field as **N**, while configuring specific servers to work in FYI (see Working with Server Security Rules on page 53).

4. Set **Check OS/400 Group and Supplemental profile** to **Y** to ensure both group profile and the supplemental groups' authorizations are checked. It is sufficient to have permission for a service in one of the groups.
5. Set **Enable Super Speed Processing** to **Y** 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.

6. **Hot upgrade is safe:** A Hot Upgrade should not be attempted if Hot Upgrade is Safe is set to **N**.
7. Press **Enter** twice to return to the main menu.

Working with Server Security

In order to gather activity data for subsequent analysis, users should enable protection for all servers and enable logging of all transactions into the Activity Log.

To enable protection for all Servers:

1. Select **1 > 1. Work with Servers**. The **Work with Server Security** screen appears.

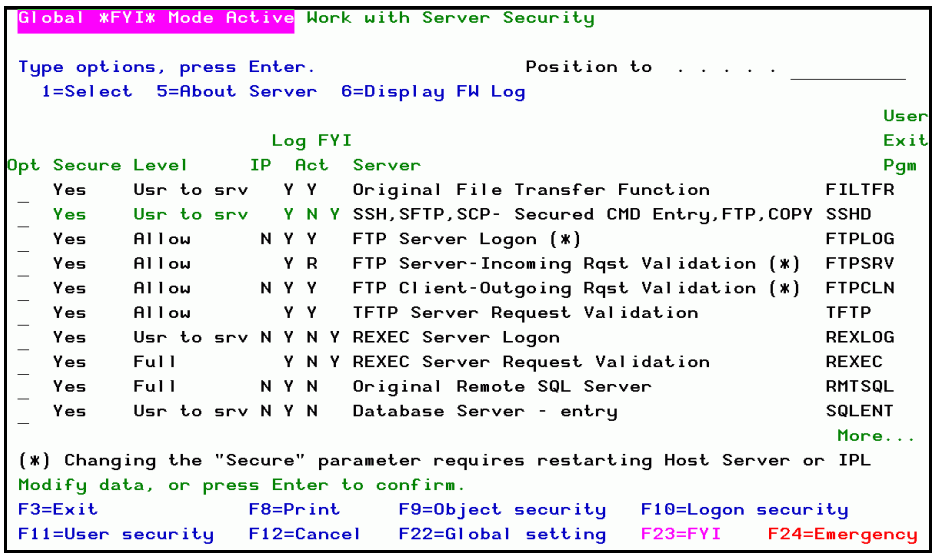


Figure 3-5. Work with Server Security Screen

2. Press **F22**. The Global Server Security Settings screen appears.

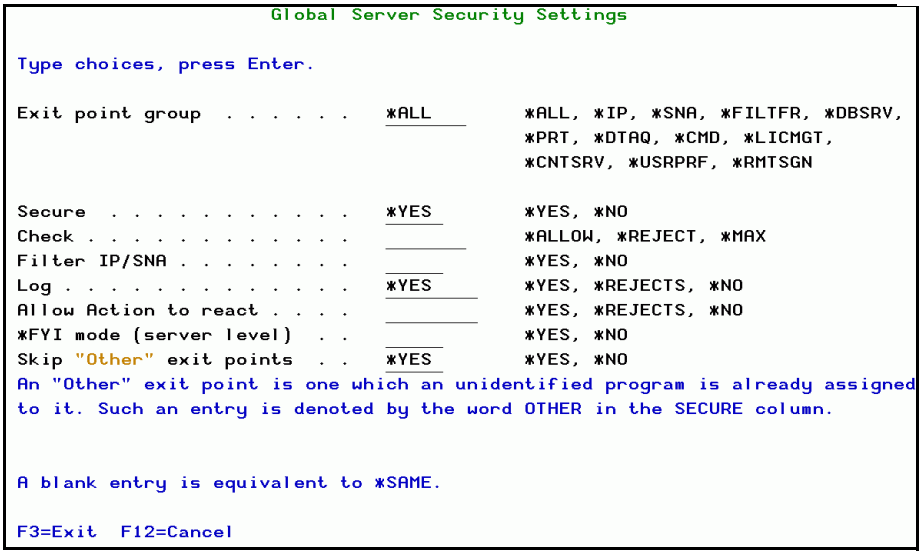


Figure 3-6. Global Server Security Settings

3. Make certain that ***ALL** appears in the Exit point group field.
4. Set **Secure** to ***YES**.
5. Set **Log** to ***YES**.
6. Press **Enter** twice to return to the main menu.
7. Make absolutely certain that the **FYI Simulation Mode** is enabled as described above.

Fields	Description / Options
Exit point group	***ALL, *IP, *SNA, *FILTFR, *DBSRV, *PRT, *DTAQ, *CMD, *LICMGT, *CNTSRV, *USRPRF, *RMTSGN**
Secure	***YES, *NO**
Check	***ALLOW, *REJECT, *MAX**
Filter IP/SNA	***YES, *NO**
Log	***YES, *REJECTS, *NO**
Allow Action to react	***YES, *REJECTS, *NO**
***FYI mode (server level)**	***YES, *NO**
Skip "Other" exit points	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.

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. Users 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 IBM i 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 **45. Rule Wizards** 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:    S520
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),
    21. Re-use             specify permitted operations.
 3. Outgoing IP            Restrict target where data is sent to by IP ranges
    31. Re-use             defined.
 4. Users                  Specify the services which a User, Group Profile or
    41. Re-use             Internal Group is permitted to use.
 5. Native Objects         Specify who can use specific objects (FILES, COMMANDS,
    51. Re-use             etc.) and how (Read, Write, Update, ...).
 6. IFS Objects            Specify who can use IFS Objects (folder/file*), and
    61. Re-use             how (Read, Write, Update, ...)
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
```

Figure 3-7. 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 2-6) to save processing time.
3. Select option **99. Advanced Options**, to customize the wizards' rules.

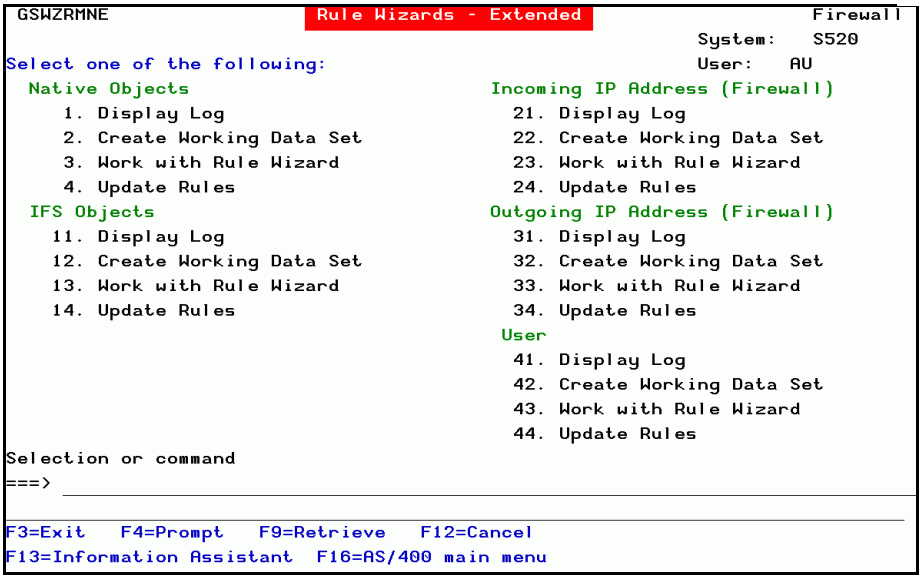


Figure 3-8. Rule Wizards - Advanced Options

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 also applicable to the other wizards.

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**:

1. Select **45 > 1. Servers**. The **Display User Activity** screen appears.

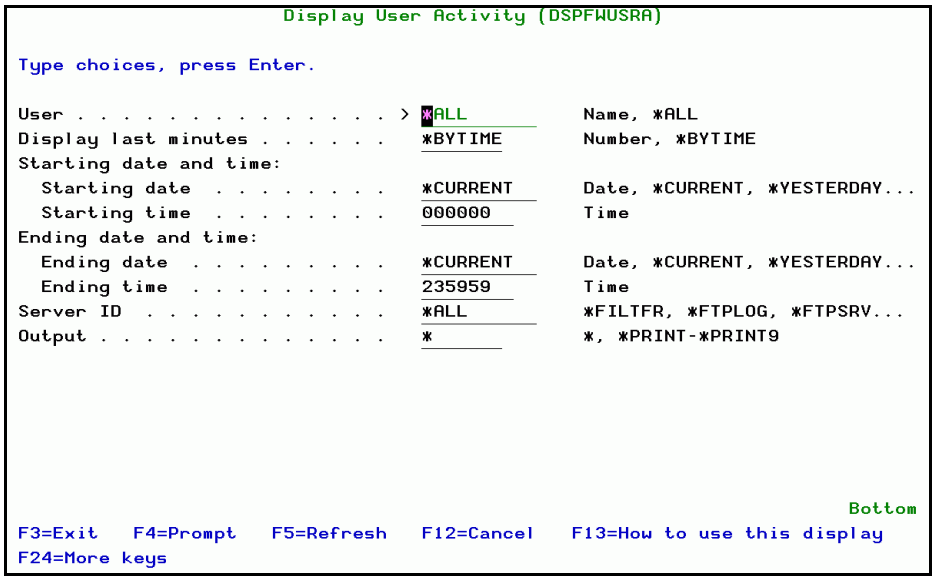


Figure 3-9. Display User Activity

Field	
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 to 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

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

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 also applicable to the other wizards.

To define the working data set:

1. Select **99 > 23. Work with Rule Wizard**. The **Incoming Objects Wizard** screen appears.

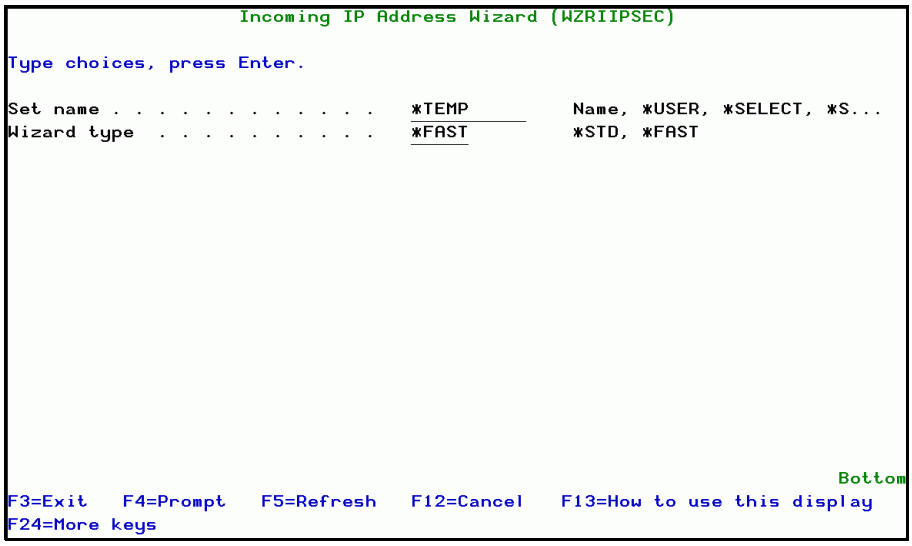


Figure 3-10. Incoming Objects Wizard

2. Choose a wizard type to work with and press **Enter** to return to the **Rule Wizards - Extended** menu.
3. Select **99 > 22. Create Working Data Set** for the **Incoming IP Address (Firewall)**. The **Summarize Incoming IP Address** screen appears as shown in Figure 3-11 on page 32.

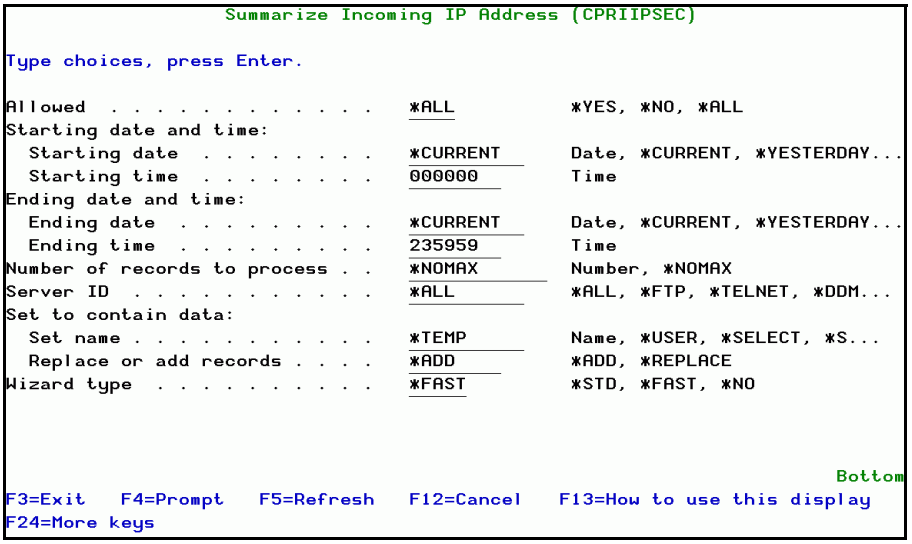


Figure 3-11. Summarize Incoming IP Address Screen

Field	Description
Allowed	***YES** = Allowed ***NO** = Rejected ***ALL** = All activity
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
Number of Records to Process	Maximum number of records to process (**Number**) ***NOMAX** = No maximum (Default)
Set to contain data	
Set name	Enter the name for the Set that you are creating: **Name** ***USER** ***SELECT** ***S...** ***TEMP**
Replace or add records	***ADD** - add the new records to the records already in the set. ***REPLACE** - replace the records already in the set with the new records.
Wizard type	***STD** ***FAST** - automatically brings up the following screen when the IBM command completes ***NO**

Function Keys	
F4=Prompt	Opens a prompt screen to specify field values.
F9=All parameters	Display all parameters.
F11=Keywords	Toggles to display list of parameters.
F15=Error messages	Display generated error messages.
F16=Command complete	Save and run security rules.

4. Press **Enter** to run the wizard. The security rule runs. Upon completion, the **Plan Incoming IP Security** screen appears as shown in Figure 3-12 on page 33.

Working with the Plan Security Wizard Screens

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.

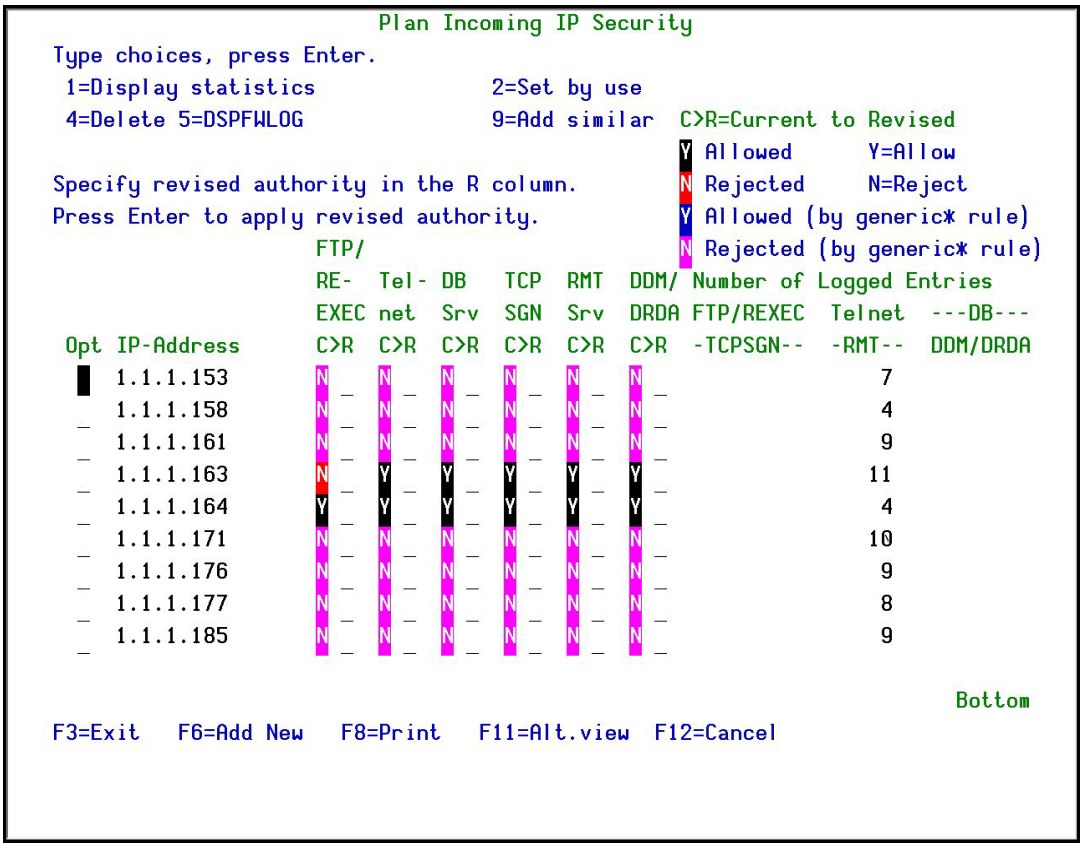


Figure 3-12. Plan Incoming IP Security Screen

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 an **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.

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

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.

Field	Description
'C' Columns	Display the rule currently in effect for each activity type (column). **Y** = allowed; **N** = rejected.
'R' Columns	Type 'Y' (Allow) or 'N' (Reject) to modify the rule currently in effect for each activity type.

Options	Description
1=Display statistics	Show statistics for a specific IP address
2=Set by use	
4=Delete	Delete this rule.
5=DSPFWLOG	Display the detailed Activity Log for this rule.
9=Add similar	Create a new rule based on an existing rule.

Function Keys	Description
F6=Add new	Create a new rule covering activity NOT shown on any line. For example, create a new rule for an IP address that does not appear on this screen.
F8=Print	Print all activity and rules shown in this wizard.
F11=Alt. view	Displays additional data for each line with fewer lines per screen.

Native OS/400 Objects Log

Options **4**, **5** and **6** on **Firewall Option 45** 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 **21. Native Objects** from the main menu. The **Native Object Security** opens.
2. Select **41. Create Working Data Set**. The **Summarize Native AS/400 Log (CPRNTVSEC)** screen appears as shown in Figure 3-13 on page 35.

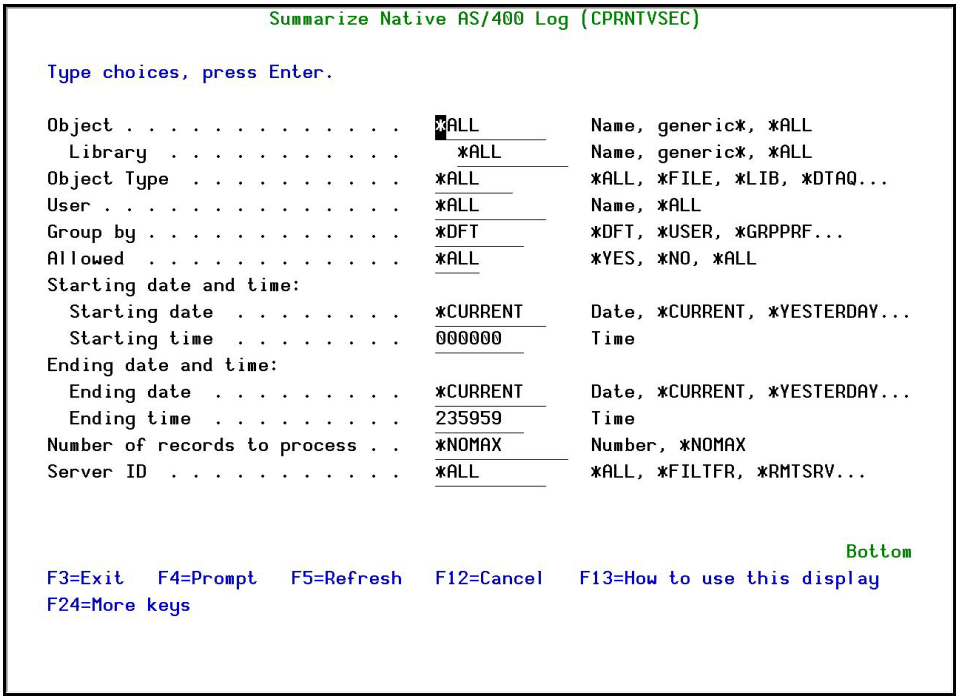


Figure 3-13. Summarize Native AS/400 Log

Field	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*)

Field	Description
Group by	Select a group from a list • ***DFT** - use the value in the **Wizard Group by** parameter in the Firewall General Definitions (see General Definitions on page 192). • 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.

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

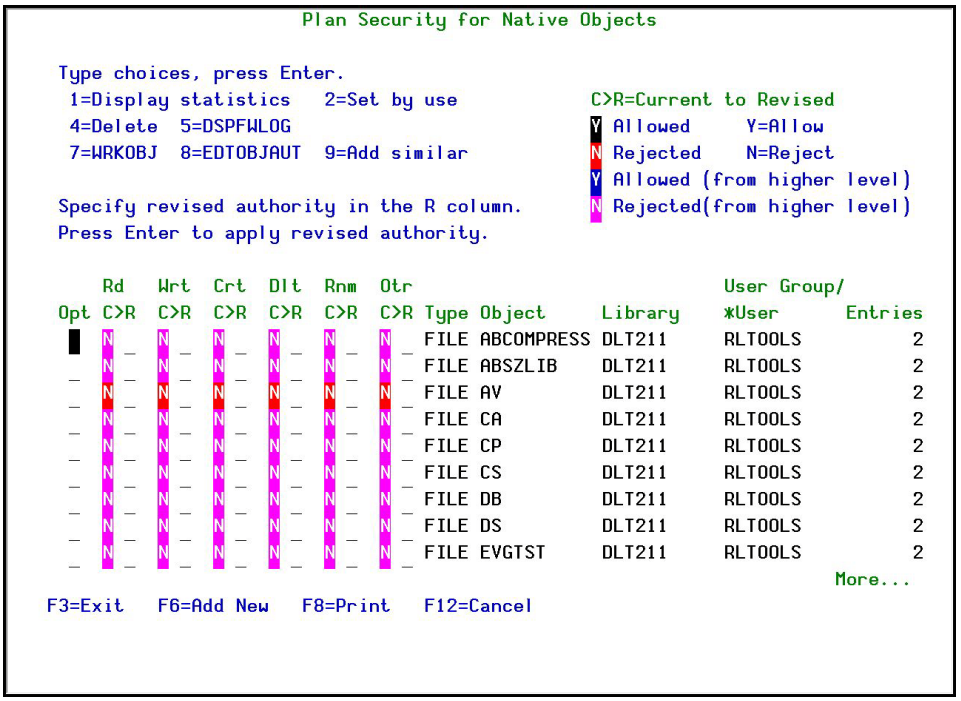


Figure 3-14. Plan Security for Native Objects

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, described below:

- IBM i Group Profiles
- Firewall Proprietary User Groups

IBM i Group Profiles

IBM i group profiles are useful for a variety of System i administration and security tasks. Use the **CRTUSRPRF** or **WRKUSRPRF** commands to create IBM i 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 IBM i 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 (For example, **%SALES)**. These user groups are defined within Firewall, and they may include both individual user profiles and IBM i group profiles.

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

Defining User Groups

To work with Firewall proprietary user groups

1. Select **11. Users and Groups** from the main menu. The **Work with User Security** screen opens.

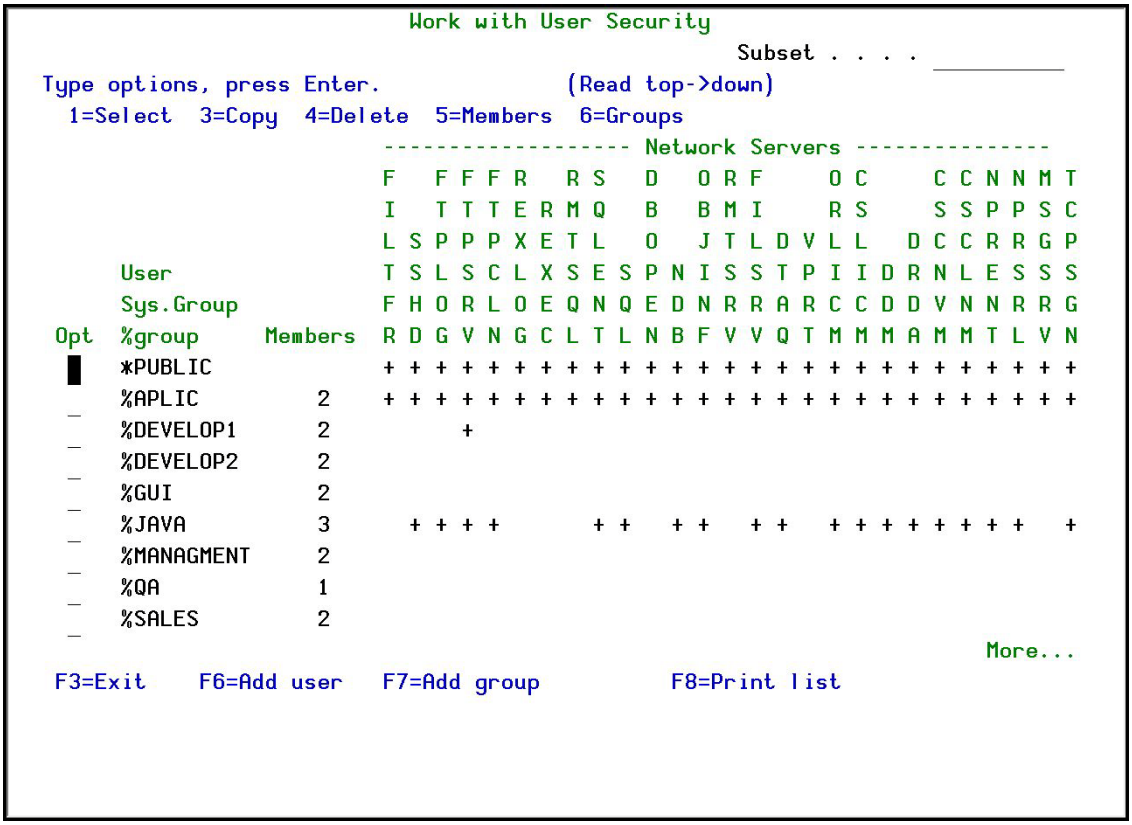


Figure 3-15. Work with User Security Screen

Field	Description
Network Servers	Vertically displays the network server names and its rule status for each user in the User Group Authorities column: **+** = User-to-service rule overrides the global server security rule. Allow a user the access to a server and check for object authorizations. **V** = User-to-service rule overrides with verb (command) support <*blank*> = Global server security rule governs activity for this server **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).
Members	The number of members within a **%** group or indicates the system user is a group profile

Options	
1=Select	Modify user or group profile or group. The Modify User Security screen appears.
3=Copy	Copy user profile or group definitions.
4=Delete	Delete user profile or group.
5=Members	Edit the group's members.
6=Groups	Groups (shows the association between the user and group profiles).

Function Keys	Description
F6=Add user	Add a new user. The **Add User Security** screen appears.
F7=Add group	Add a new group. The **Add User Group Security** screen appears.
F8=Print list	Print user group definitions.

2. Open the appropriate **User Security** screen (**Add** or **Modify**).
3. Edit the field values and press **Enter** to confirm.

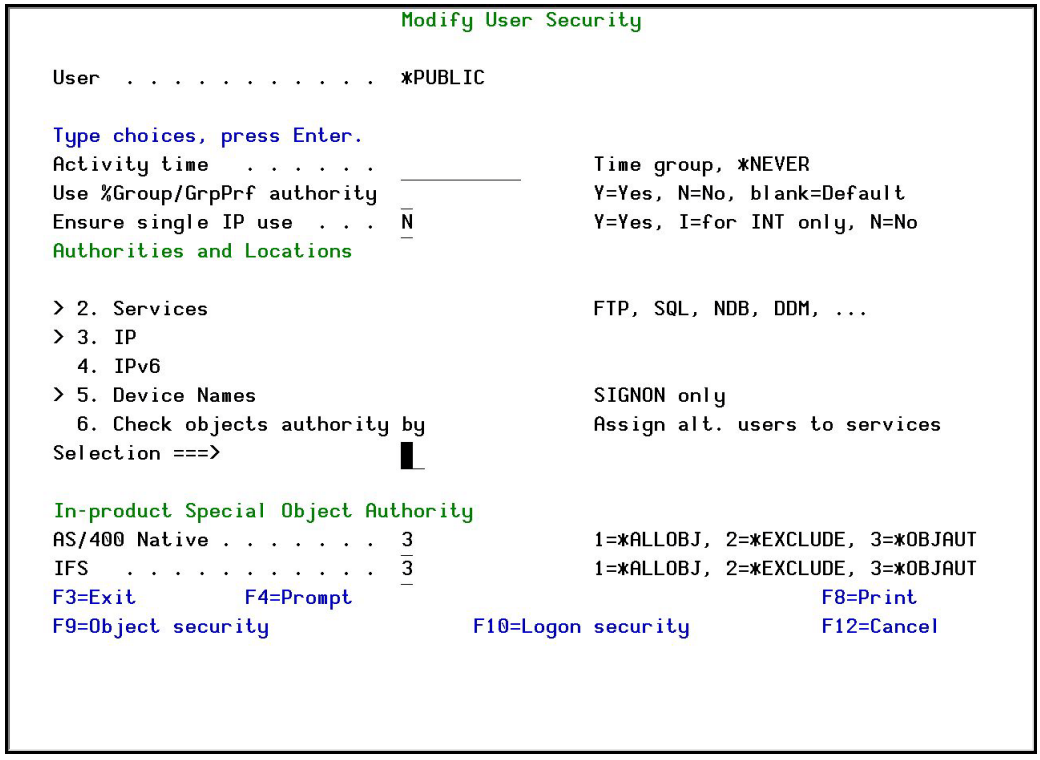


Figure 3-16. Modify User Security

Field	
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 =

Field	
Use %Group/GrpPrf Authorities	**Y** = use a specific group authorities **N** = don't use any specific group authorities
Ensure single IP use	Ensure that users can only access the system through a single IP address. Within that address, the user can access as many sessions as required. **Y** = Yes **I** = Interactive jobs only **N** = No If the user is a group profile, this parameter refers to all users in the group.
Authorities and Locations	**1. By %Groups** = specify authorities based on groups **2. Services** = specify authorities and location by Services name **3. IP** = specify authorities and location by IP address **4. IPv6** = specify authorities and location by IPv6 address **5. Device Names** = specify authorities and location by Device name **6 Check objects authority by** = specify different object authorities to be checked based upon the exit point being used. This user does not necessarily have to exist in the operating system. See Work with Alternative Users on page 98 for an explanation of this option. > Precedes every item that has already been defined
In-product Special Object Authority	Use this field to define object authority for the user/group for AS/400 Native and IFS objects. **1=*ALLOBJ** = All objects **2=*EXCLUDE** = Exclude from **3=*OBJAUT** = Object Authorities

Function Keys	
F8=Print	Print user-to-service security rules
F9=Object security	Work with object security rules
F10=Logon security	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 IBM i group profiles.

To add a user to a group:

1. Type **5** (Members) to add a member.
2. Type in the user profile name in one of the User fields, or press **F4** to select a user profile from a list window. 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.

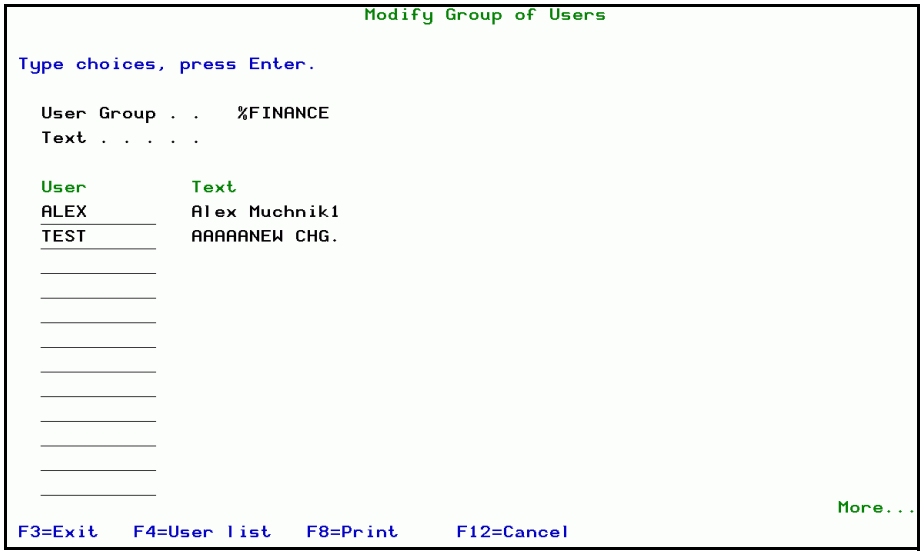


Figure 3-17. Modify Group of Users Screen

Function Keys	Description
F4=User list	Display the list of users.
F8=Print	Print user-to-service security rules.

Time Groups

Overview

Many of the Firewall rules and reporting features take advantage of the unique Time Group feature. Time groups allow users to apply predefined sets of time-based filters to different queries without having to define complex criteria for each query. Time groups also work with the report scheduler and the display Activity Log features.

For example, you 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, you 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 **41. Log, Queries, Groups** from the main menu. The **Reporting** menu appears.
2. Select **49. Time Groups** from the main menu. The **Define Time Groups** screen appears.

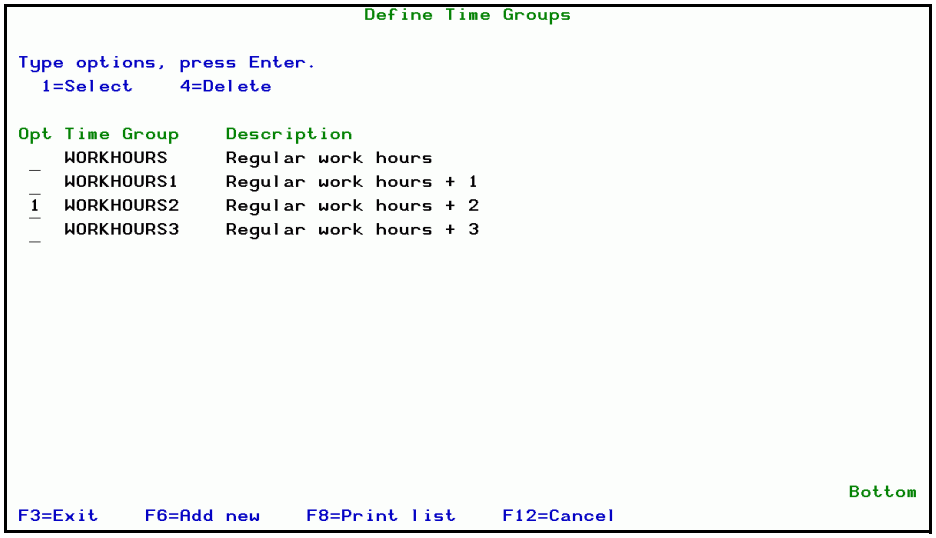


Figure 3-18. Define Time Groups

Option	Description
1=Select	Modify a time group.
4=Delete	Delete a time group.

Function Keys	Description
F6=Add new	Add a new time group
F8=Print list	Print list of time groups

3. Type **1** next to the time group you want to modify or press **F6** to add a new group. The **Change/Add Time Group** screen opens as shown in Figure 3-19 on page 45.

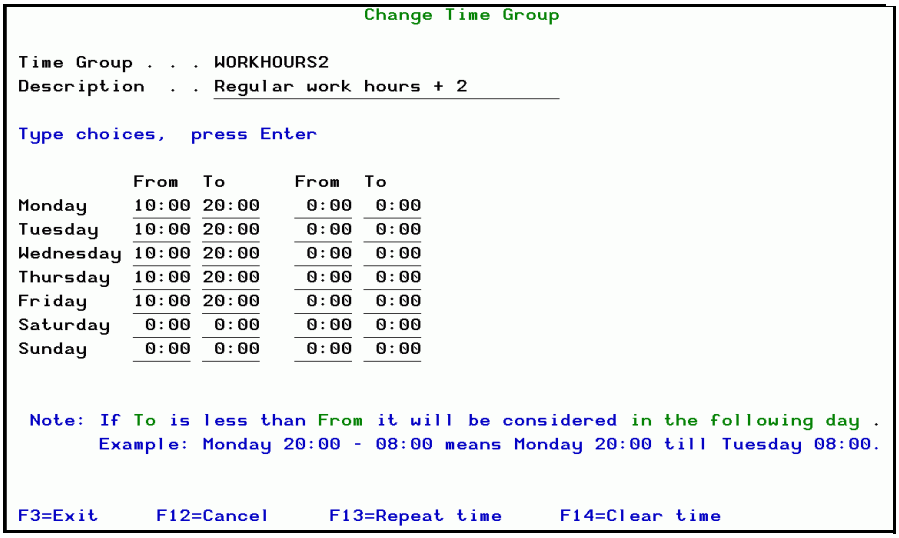


Figure 3-19. Change Time Group Screen

Field	Description
Time Group	Name of the Time Group
Description	Text description of the Time Group.

Function Keys	
F13=Repeat time	Repeats the time range of the above (previous) day.
F14=Clear time	Clears all time ranges for the remainder of the week from the day the cursor is on.

NOTE: If the **To** value is earlier than the **From** value, the **To** value will be considered in the following day. For example, Monday 20:00 - 08:00 means Monday 20:00 till Tuesday 08:00.

4. Define or modify the time group settings and press **Enter** to accept the definition and return to the **Define Time Groups** screen.

Application Groups

Overview

In some cases, a transaction logged by Firewall displays a local server name, for example ***LCL-SCSERVER**, instead of an exact IP address.

For these cases, the user can be added as an application member (an application does not require IP analysis), in addition to the rules and definitions the user already has in Users and Groups.

Application Groups consist of users whose access to certain applications is defined to be identical. The name of the group is the application itself (for example, **%#Excel**, **%#OPSNAV**, and so on). Define which servers are used by the application, and then select its members. Upcoming releases will include predefined application groups for widely used applications, such as OPSNAV and FILE-SERVER.

You can also define object level rules for application groups.

Limitations for Groups

You can define two access groups: a group for which access is allowed and a group for which access is denied. There can be no more than 256 users in the smaller of the two groups.

Defining and Modifying Application Groups

To define an application group:

1. Select **12. Applications** from the main menu. The **Work with Application Groups** screen appears.

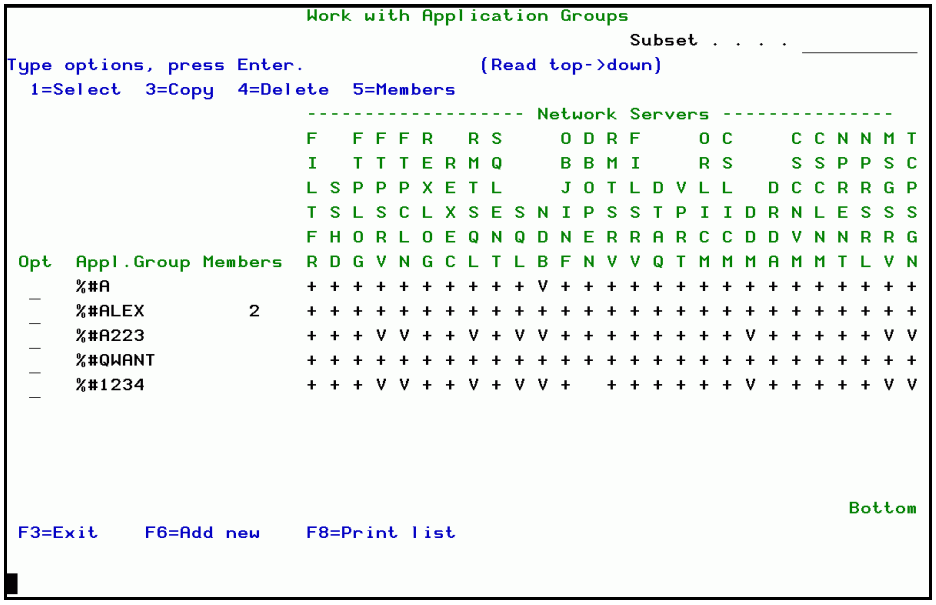


Figure 3-20. Work with Application Groups

Field	Description
Application	Name of application group

Options	Description
1=Select	Modify an application group.
3=Copy	Copy an existing application group.
4=Delete	Delete an application group.
5=Members	Edit the group members (OS400 Users and Group profiles).

Function Keys	Description
F6=Add new	Add a new application group.
F8=Print list	Print a list of application groups.

2. Select **1** to modify a group (as shown below) or press **F6** to create a new group. See Figure 3-21 on page 48.

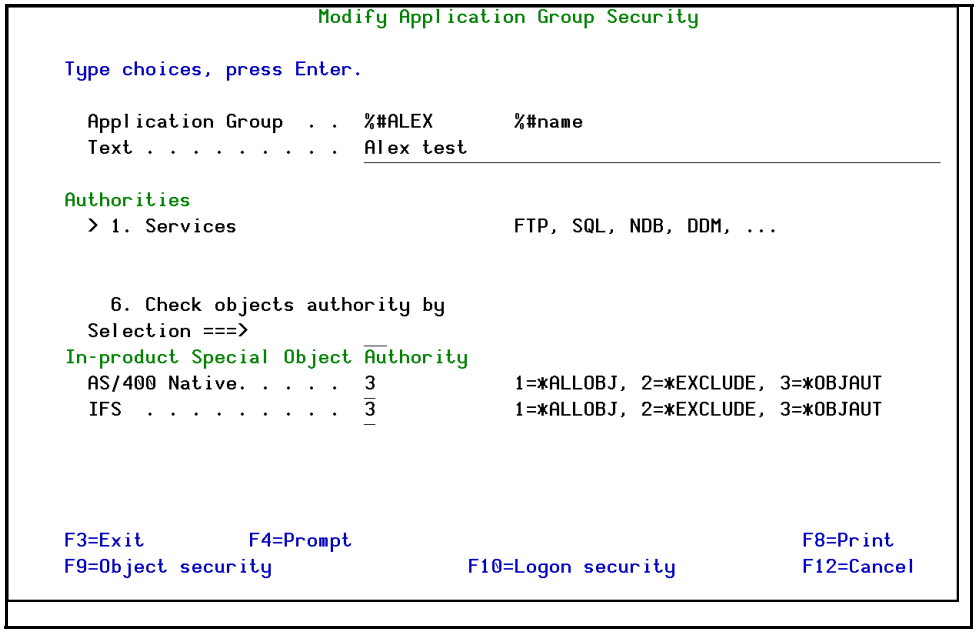


Figure 3-21. Modify Application Group Security Screen

Field	Description
Application Group	Name of application group
Text	Enter a description of the application group
Authorities	**1. Services** = choose server **6. Check objects authority by** = specify different object authorities to be checked based upon the exit point being used. This user does not necessarily have to exist in the operating system. See Work with Alternative Users on page 98 for an explanation of this option. > Precedes item that has already been defined
In-product Special Object Authority	This feature defines the level of authority for both: AS/400 Native and IFS objects. ***ALLOBJ** = Users are granted *ALLOBJ for IFS object ***EXCLUDE** = All object authority is denied for this user ***OBJAUT** = Object authority is subject to object security rules

Function Keys	Description
F9=Object security	Work with object security rules
F10=Logon security	work with logon security rules

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.

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

Defining and Modifying Location Groups

Perform the following steps to define location groups.

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

```
                        Work with Location Groups

Type options, press Enter.
  1=Select  3=Copy  4=Delete  5=Members
                                                    Subset . . . . _________
Opt  Loc.Group   Members
_    %@ABC
_    %@ABC1
_    %@ALEX                 Alex TEST
_    %@FRONTDSK       1     Accounting Users at the Front Desk
_    %@NY                   NY
_    %@QWER
_    %@Q3
_    %@000
_    %@002                  Location Group %@002
_    %@007                  PCI Users
_    %@022                  Location Group %@022
_    %@033                  Location Group %@033
_

                                                                      Bottom
F3=Exit     F6=Add new     F8=Print list
```

Figure 3-22. Work with Location Groups Screen

Field	Description
Subset	Choose a subset of location groups

Options	Description
1=Select	Modify a location group.
3=Copy	Copy an existing location group
4=Delete	Delete a location group
5=Members	Edit the group members (OS400 Users and Group profiles).

Function Keys	Description
F6=Add new	Add a new location group.
F8=Print list	Print location group definitions.

2. Select **1** to modify a group (as shown below) or press **F6** to create a new group. See Figure 3-23 on page 50.

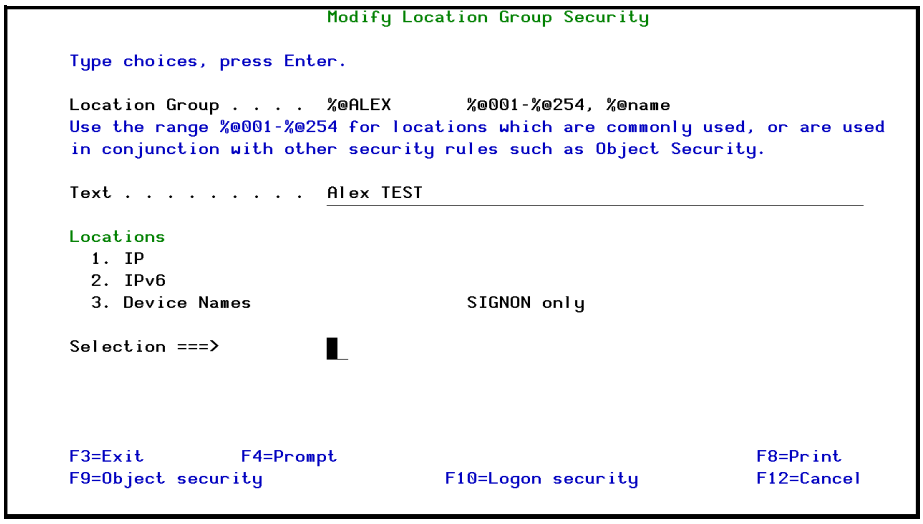


Figure 3-23. Modify Location Group Security

Field	
Location Group	Name of location group. To enable the specification of these groups as a simple number, the location groups named %@001-%@254 can be regarded in other places where applicable, only by the number. This is mainly in use for assigning objects that can be accessed by specific users only when the reference is being done from a specific location. This is a request which is being enforced by PCI/DSS auditors in some places.
Text	Type descriptive text
Locations	
1. IP	The IP addresses that are allowed to be accessed by this location group
2. IPv6	The IPv6 addresses that are allowed to be accessed by this location group
3. Device names	Device names which are allowed to be accessed to telnet sign-on
Selection	Enter one of the above locations.

Function Keys	
F4=Prompt	Opens a prompt screen that allows you to select **1** or more users or user groups.
F8=Print	Print the location group rules
F9=Object security	Work with object security rules
F10=Logon security	work with logon security rules

4

Server Settings and Activation

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 Working with Server Security Rules on page 53.

About Servers & Exit Points

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

IBM i 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.

For a list of the Exit Points that iSecurity Firewall works with, see Appendix: List of Firewall Exit Points on page 277.

Activation and Server Setting

To define activation and server settings:

1. Select **1. Activation and Server Setting**. The **Activation and Server Setting** screen appears.

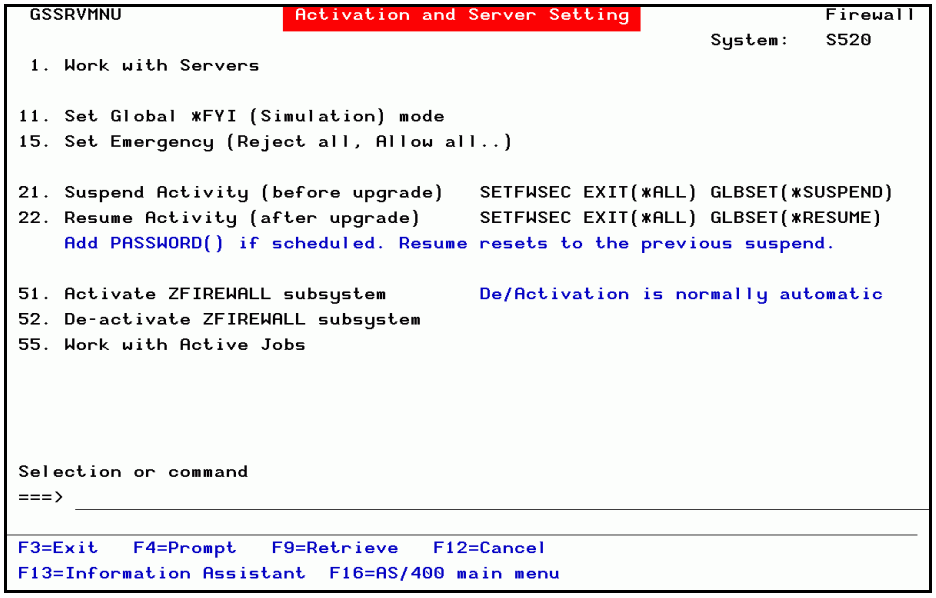


Figure 4-1. Activation and Server Setting

Option	Description
Work with Servers	Displays the current server security rules for each server, as described in the section below.
Set Global *FYI (Simulation) mode	Enables Firewall to simulate the application of rules without rejecting transactions. Activity is recorded in the log with the ***FYI*** designation.
Set Emergency	Enables emergency override of ALL Security settings.
Suspend Activity	It is strongly recommended before an upgrade to use this feature to suspend all Firewall activities.
Resume Activity	After an upgrade, you can use this feature to quickly enable all activities as they had been working previously.
Activate ZFIREWALL subsystem	Activation and deactivation is normally automatic. The Start Subsystem (STRSBS) command launches a ZFIREWALL subsystem using the subsystem description specified in the command.
De-activate ZFIREWALL subsystem	The End Subsystem (ENDSBS) command ends the specified ZFIREWALL subsystem and specifies what happens to active work being processed. No new jobs or routing steps are started in the subsystem after this command is run.
Work with Active Jobs	Shows the names and status information of jobs being processed by the ZFIREWALL subsystem.

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.

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

1. Select **1 > 1 Work with Servers**. The **Work with Server Security** screen appears as displayed in Figure 4-2 on page 53.
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.

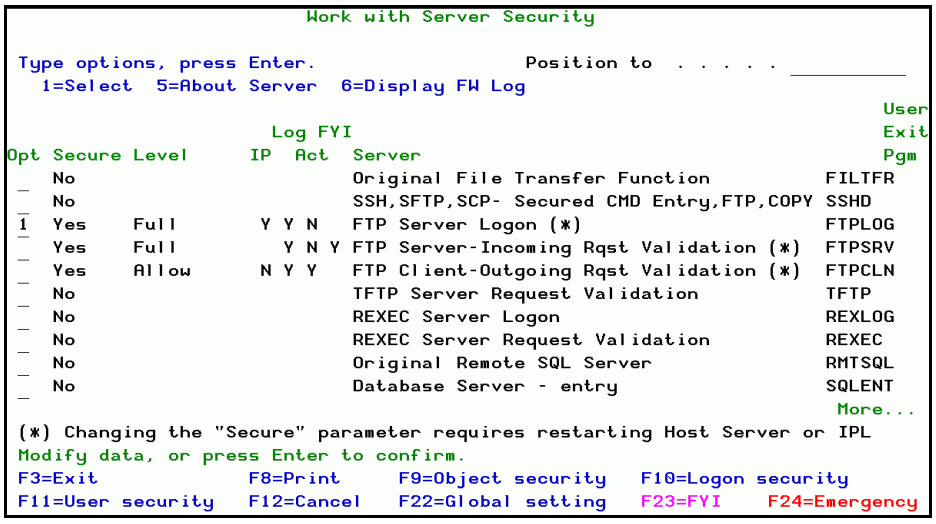


Figure 4-2. Work with Server Security

Field	Description
Opt	**1** = Select a rule for modification. The **Modify Server Security** screen appears **5** = View a description of the server **6** = View the Activity Log for the server
Secure	***YES** = Secured ***NO** = Not secured

Field	Description
Level	This option is not available for exit points that deal with specific operations (such as Change User Profile and Pre-Power Down System) **1** = Allow all activity (available for all other exit points) **2** = Reject all activity (available for all other exit points) **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 Signon) **9** = Full security - differs in logon and user-to-object. **Logon** activates the logon limitation rules (user to system name, IP and user name). **User-to-object** activates your user limitation rules.
Log FYI FW, Action	Shows if FYI mode is currently being logged for Firewall and Action
Server	Name/description of server
User Exit Pgm	Name of custom user exit program for this server

Function Keys	Description
F8=Print	Print all server security rules
F9=Object security	Work with object security rules
F10=Logon security	Work with logon security rules
F11=User security	Work with user-to-service security rules
F22=Global setting	Define server security rules globally for predefined groups of servers or for all servers
F23=FYI	Enable or disable the FYI simulation mode globally for all servers
F24=Emergency	Use the Emergency Override feature

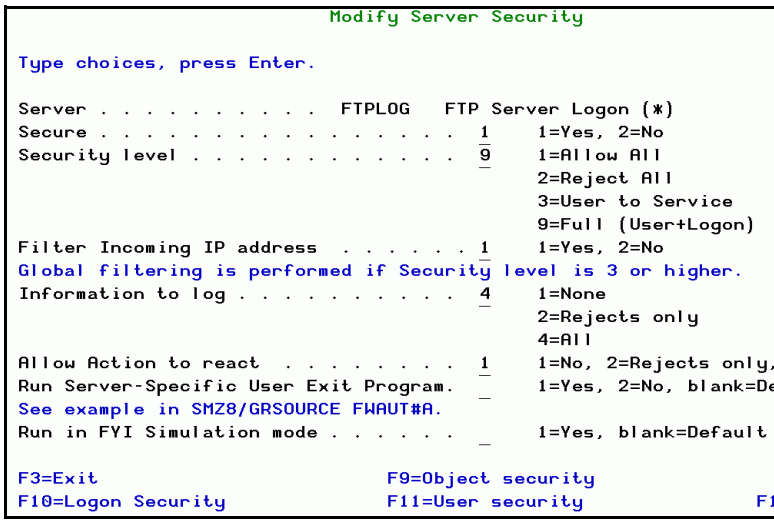


Figure 4-3. Modify Server Security

Field	Description / Options
Server	Server name
Secure	***YES** = Secured ***NO** = Not secured To register the Firewall program on the IBM i exit points, all Servers should be set to Secure = ***YES**. However, all servers marked with an asterisk (*)in the Work with Server Security Screen (Figure 4-2 on page 53) and also the SSHD and DBOPEN servers require either a restart or for an IPL to be performed. Only change these servers when you can perform these tasks.
Security Level	This option is not available for exit points that deal with specific operations (such as Change User Profile and Pre-Power Down System) **1** = Allow all activity (available for all other exit points) **2** = Reject all activity (available for all other exit points) **3** = Allow activity subject to User-to-Service security rules (not available for exit points that are supported until the Logon level such as Telnet and Remote Sign-on) **9** = Full security - differs in logon and user-to-object. Logon activates the logon limitation rules (user to system name, IP and user name). User-to-object activates your user limitation rules.
Filter Incoming IP Address	**1** = Yes **2** = No
Information to Log	**1** = Do not log any activity. **2** = Log rejected transactions only. **4** = Log all activity.
Allow Action to React	**1** = None. Disables the Firewall real-time detection rules for this server. **2** = Rejects only (will activate Firewall real-time detection rules only on rejections from this server). **3** = All (will activate Firewall real-time detection rules for all accesses from this server).

Field	Description / Options
Run Server-Specific User Exit	**1** = Yes. Run a specific exit program after passing Firewall rules for this server. The program SMZTMPA/UPyyyyyy will be called. (yyyyyy is the server short name). Write your own SMZTMPA/UPyyyyyy program according to the example in SMZ8/GRSOURCE FWAUT#A. The program that initiates the call is GRCLUER. This program runs in USER authority and therefore the user (every user in the system) will have the authority to run the program SMZTMPA/UPyyyyyy If the program SMZTMPA/UPyyyyyy is not accessible, the regular security applies. **2** = No. If there is a general exit program configured, it will not be activated for this server. <*blank*> = global setting
Run in FYI Simulation Mode	**1** = Yes. Enable FYI Simulation mode for this server only <*blank*> = Use global parameter for all servers (System Configuration) **Note:** If you are working in FYI mode, but still want **Firewall Actions** to be performed in the **Audit** module, you must ensure that the **Firewall & Screen (Action)** parameter is set to **A=Always**. This parameter is accessed as follows: 1. In the **Audit** main menu, select **81. System Configuration**. The **System Configuration** menu appears. 2. In the **System Configuration** menu, select **5. Auto start activities in ZAUDIT**. The **Auto Start Activities in ZAUDIT Subsystem** screen appears. See the **Configuration** chapter in the **Audit User Guide** for more details.

Function Keys	Description
F9=Object security	Work with object security rules
F10=Logon security	Work with logon security rules
F11=User security	Work with user-to-service security rules

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.

4. If you changed Servers that require either a restart or an IPL, a **Special Instructions** screen is displayed. Follow the instructions on that screen.

SSH Secure Shell (SSH, SFTP, SCP)

Secure Shell (SSH) is an open source protocol that allows users to establish a secure link for data traffic that otherwise flows in-the-clear over communication links.

Since V5R3, OpenSSH has been included as a standard part of the IBM i. Its advantage over other communication methods is that it allows one to use Public and Private keys (with an option to rely only on these encryption keys or include additional User/Password identification). Aside from providing a secured channel, it offers the following functions:

- **SSH daemon (sshd)** - a server program for SSH that enables an SSH client to log in and perform commands (AIX style)
- **SFTP (Secure FTP)** - a secured popular replacement of FTP
- **SCP (Secure Copy)** - a secured method to copy files.

Firewall Implementation for SSH

In the Global Server Setting, a service named SSHD can be controlled.

NOTE: Unlike other services, the ***FYI** (Simulation) mode is not applicable here.

NOTE: If your system administrator already uses SSH to manage which users allowed/denied to log in the system, you should not use Firewall for this purpose, as Firewall will overwrite the SSH definitions.
If you do decide to use Firewall, the original SSH definitions are saved in this IFS file: **/QOpenSys/QIBM/UserData/SC1/OpenSSH/openssh-$<*sshv*>/etc/sshd_config_saved.<*$$*>**, where ***sshv*** is the SSHD version number and **<*$$*>** is the QSHELL process number that performed the change.

Due to the nature of the implementation, SSHD has to be restarted whenever a setting is changed. This is true also when User Grouping is changed. This restart *does not* affect any running SSH session.

To apply changes:

1. Select **35. DDM, DRDA, SSH, Port...** . 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                           SSHD Security           SETFWSPC *SSHD
15. Display DHCP Security Log           51. Activate Current Setting
                                        55. Prepare Setting For Next Start
                                        Use after every change in SSHD securit
TCP/IP Port Restrictions                or in user profile grouping.
21. Work with TCP/IP Port Restrictions



Selection or command
===>
```

Figure 4-4. Work with Advanced Security

2. Select **51. Activate Current Setting**. The **Set Firewall Special Security (SETFWSPC)** screen appears.

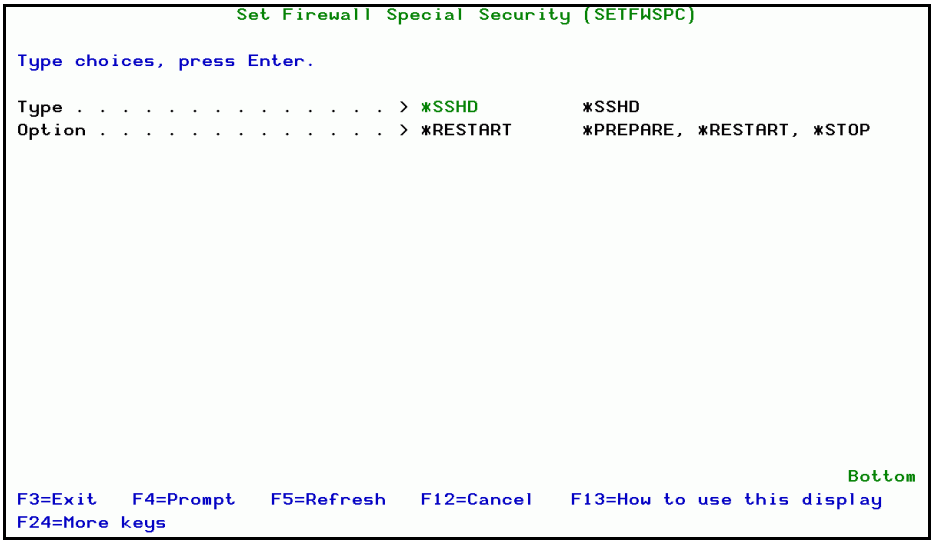


Figure 4-5. Activate SSH Current Settings

Limitations

- When you work with the SSH server there is no support for working in FYI mode.
- Activating the SSH server causes the server to restart.

Displaying SSH Activity log

Use the **DSPFWLOG TYPE (*SSHD)** command to display SSH activity.

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
***IP**	FTP Server Logon FTP Server-Incoming Rqst Validation FTP Client-Outgoing Rqst Validation
***SNA**	DDM request access DRDA Distributed Relational DB access Remote sign-on (Passthrough)
***FILTFR**	Original File Transfer Function FTP Server Logon (*) FTP Server-Incoming Rqst Validation FTP Client-Outgoing Rqst Validation TFTP Server Request Validation Original Remote SQL Server Database Server - SQL access & Showcase Database Server - data base access File Server
***DBSRV**	Database Server - entry Database Server - object information

Server Group	Description
***PRT**	Network Print Server - entry Network Print Server - spool file Database Server - entry Database Server - object information Original Data Queue Server Data Queue Server
***DTAQ**	Original Data Queue Server Data Queue Server
***CMD**	REXEC Server Request Validation Remote Command/Program Call
***LICMGT**	Original License Mgmt Server Central Server - license mgmt
***CNTSRV**	Central Server - license mgmt Central Server - conversion map Central Server - client mgmt
***USRPRF**	Change User Profile Create User Profile Delete User Profile - after delete Delete User Profile - before delete Restore User Profile
***RMTSGN**	Remote sign-on (Passthrough)

Options	
1=Select	Modify an existing PTF definition.
4=Delete	Delete a PTF definition.

Function Keys	
F4=Prompt	Opens a prompt screen to select 1 or more PTF definitions.

To work with server security rules globally:

1. Select **1 > 1. Work with Servers**. The **Work with Server Security** screen appears.

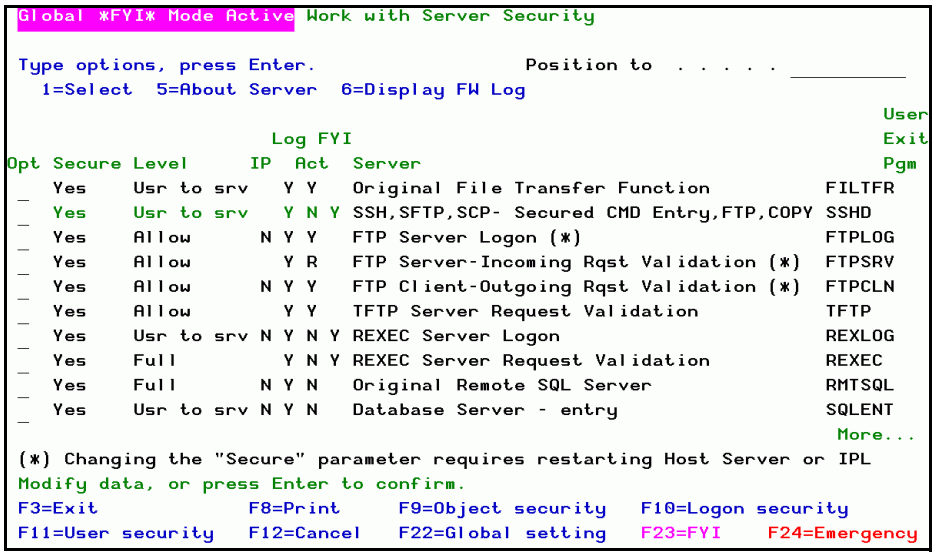


Figure 4-6. Work with Server Security Screen

2. Press **F22**. The **Global Server Security Settings** screen appears.

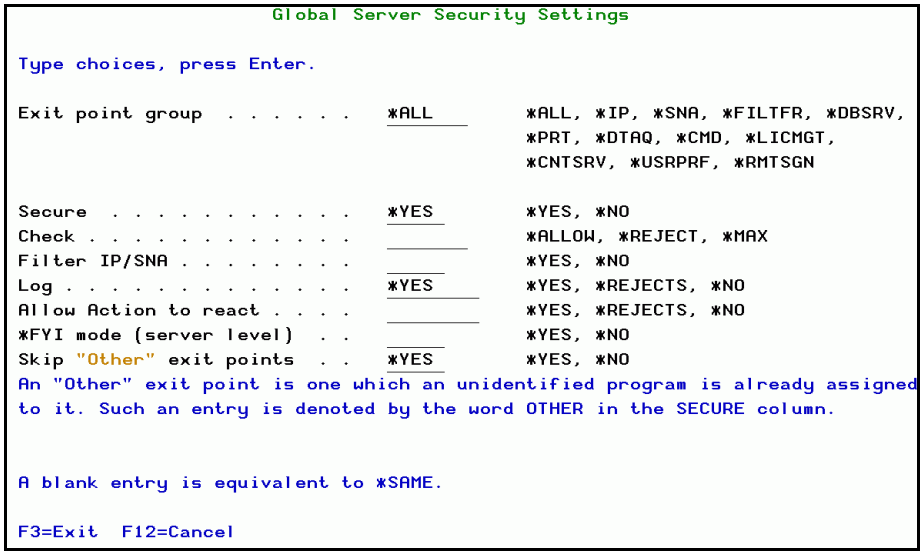


Figure 4-7. Global Server Security Settings

Fields	
Exit point group	Enter an exit point group from the list to the right. ***ALL, *IP, *SNA, *FILTFR, *DBSRV, *PRT, *DTAQ, *CMD, *LICMGT, *CNTSRV, *USRPRF, *RMTSGN**
Secure	***YES** = Secured ***NO** = Not secured To register the Firewall program on the IBM i exit points, all Servers should be set to Secure = ***YES**. However, all servers marked with an asterisk (*) in the **Work with Server Security Screen** (Figure 4-6 on page 60) and also the SSHD and DBOPEN servers require either a restart or for an IPL to be performed. Only change these servers when you can perform these tasks. If you cannot change them now with a global change, then you should change them individually as described in Working with Server Security Rules on page 53.
Check	***ALLOW** = Allow all activity ***REJECT** = Reject all activity ***MAX** = Full security - allow activity subject to user-to-service, object and login security rules as appropriate
Filter IP/SNA	***YES** = Secured ***NO** = Not secured
Log	***YES** = Log all activity ***REJECTS** = Log rejected transactions only ***NO** = Do not log any activity
Allow Action to React	Allow Action to respond automatically to specific events by sending messages to key personnel or running proactive command scripts to prevent security breaches. ***YES** = Allow Action to respond for this server only ***REJECTS** = Allow Action to respond for rejected transactions only ***NO** = Do not allow Action to respond for this server only
Skip "other" exit points	An "Other" exit point is one to which an unidentified program is already assigned. Such an entry is denoted by the word OTHER in the SECURED column. ***YES** = skip ***NO** = Do not skip NOTE: iSecurity Firewall and other Network Security products can work in parallel. For more information please contact Support.

3. Modify settings and needed. Press **Enter** to accept.

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. Select **1 > 1.** The **Work with Server Security** screen appears.
2. Press **F23**. The **Firewall *FYI* Simulation Mode** screen appears.
3. Type **Y** to enable FYI globally or type **N** to disable FYI. Press **Enter** to continue.

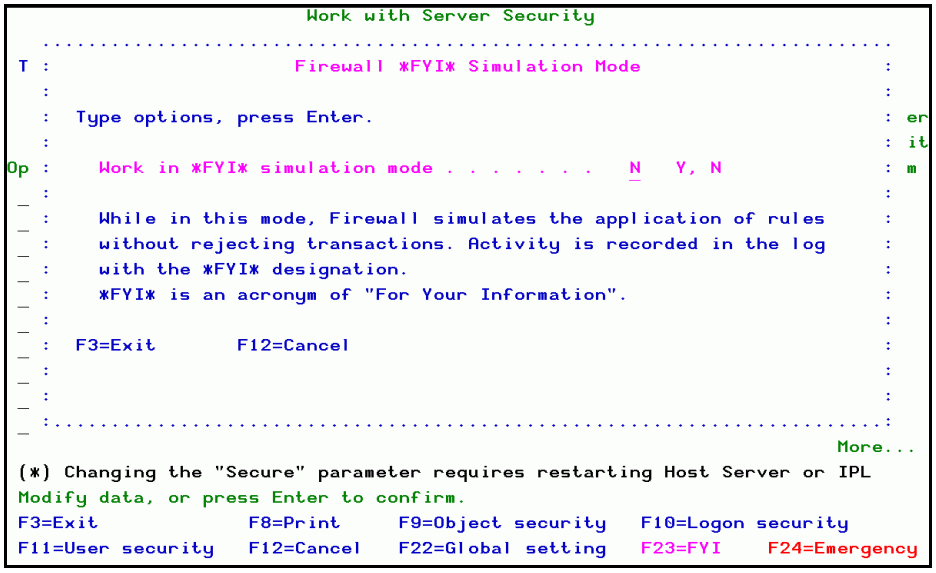


Figure 4-8. Work with Server Security: Firewall FYI* Simulation Mode Parameter

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:

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

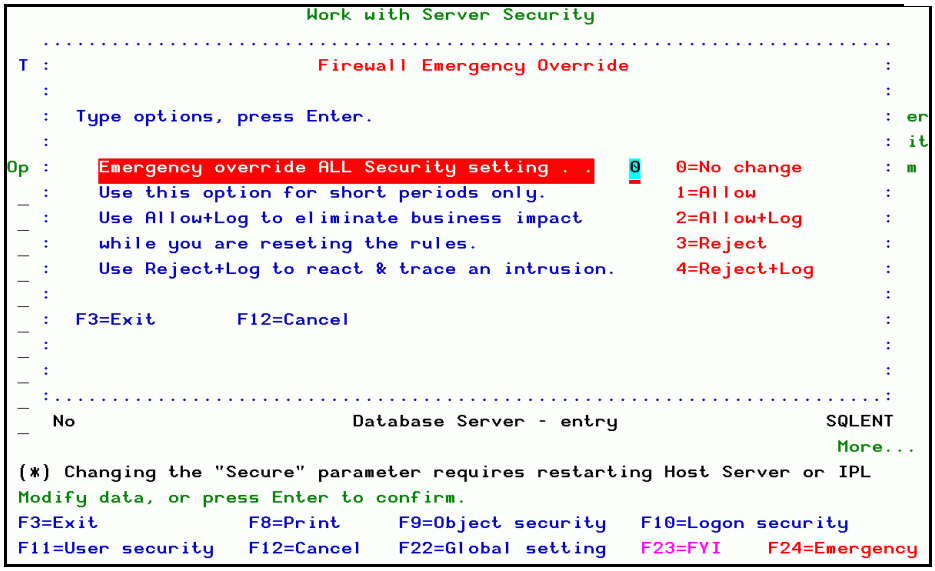


Figure 4-9. Work with Server Security: Firewall Emergency Parameter

Options	
0=No change	Disable emergency override - all rules function normally.
1=Allow	Allow all activity
2=Allow+Log	Allow and log all activity.
3=Reject	Reject all activity.
4=Reject+Log	Reject and log all activity.

5

Setting Up Dynamic Filtering

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 procedures 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 IPv4 addresses and standard prefixes for IPv6 addresses. For each address or range of addresses, you 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)

IPv4 Addresses

To create or modify IPv4 address firewall rules:

1. Select **2. Dynamic Filtering (IP, Systems)**. The **Work with Dynamic Filtering** screen appears.

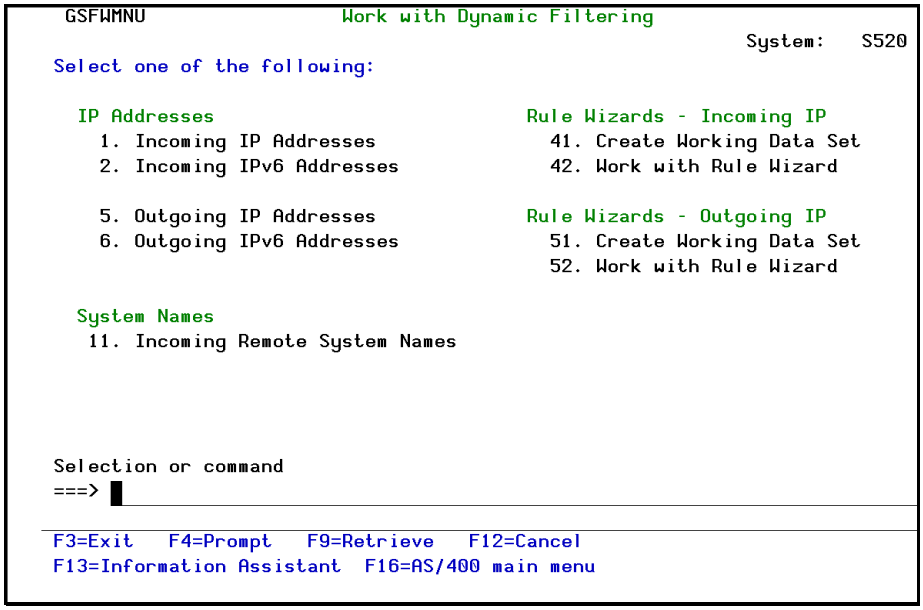


Figure 5-1. Work with Dynamic Filtering Screen

2. Select **1. Incoming IP Addresses** from the **Work with Dynamic Filtering** menu. To work with Outgoing activity, select **5** from the **Work with Dynamic Filtering** menu. In both cases, 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.

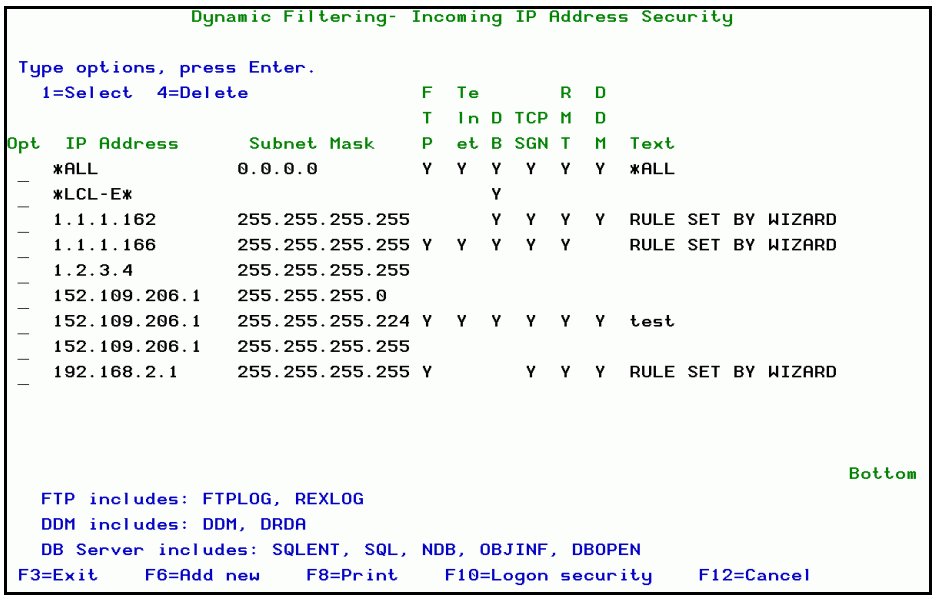


Figure 5-2. Work with Firewall - Incoming IP Address Security

Field	
Defaults	Specifies defaults assigned to changes made in this library.

Options	
1=Select	Modify an existing IP definition.
4=Delete	Delete an IP definition.

Function Keys	
F4=Prompt	Opens a prompt screen to select 1 or more PTF definitions.
F6=Add new	Opens a prompt screen to select 1 or more IPv6 definitions.
F8=Print	
F10=Logon security	

4. If you are creating or modifying a rule, the **Dynamic Filtering Incoming/Outgoing IP Address** screen appears.

```
                Dynamic Filtering- Modify Incoming IP Address

Type choices, press Enter.

IP Address  . . .   *ALL                          Address, *ALL
Subnet mask . . .   0.0.0.0                      F4 for list
Text  . . . . . .   *ALL

                  FTP/   Tel-  DB   TCP   Rmt
                  REXEC  net   Srv  SGN   Srv  DDM
Secure value. . .   _      _     _    _     _    _     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 statments 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
```

Figure 5-3. Modify Firewall Incoming IP Address Screen

Field	Description
IP Address	Enter an IP address using standard decimal format.
Subnet Mask	Enter the subnet mask using standard decimal format to define a range of IP addresses. Refer to the examples or press F4 to select an appropriate subnet mask range.

Field	Description
Text	Descriptive text
Secure value	**Y=Yes** = Type **Y** to allow activity or leave the field Blank to reject activity for each individual server. **S=SSL** = Type **S** to set SSL restrictions for the various types of access protocols. **A**=Allow always **B**=SSL+Skip checks **L**=Allow always and log **M**=SSL+Skip checks+Log Use of **B** and **L** 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.
Equivalent IP Range	Displays the range of IP addresses as defined by the subnet mask.

5. Enter your required definitions and press **Enter**.

IPv6 Addresses

To create or modify IPv6 address firewall rules:

1. Select **2. Dynamic Filtering (IP, Systems)**. The **Work with Dynamic Filtering** screen appears.

```
 GSFWMNU                  Work with Dynamic Filtering
                                                        System:   S520
Select one of the following:

  IP Addresses                          Rule Wizards - Incoming IP
    1. Incoming IP Addresses              41. Create Working Data Set
    2. Incoming IPv6 Addresses            42. Work with Rule Wizard

    5. Outgoing IP Addresses            Rule Wizards - Outgoing IP
    6. Outgoing IPv6 Addresses            51. Create Working Data Set
                                          52. Work with Rule Wizard

  System Names
   11. Incoming Remote System Names



Selection or command
===>

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

Figure 5-4. Work with Dynamic Filtering Screen

2. Select **2. Incoming IPv6 Addresses** from the **Work with Dynamic Filtering** menu. To work with Outgoing activity, select **6** 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.

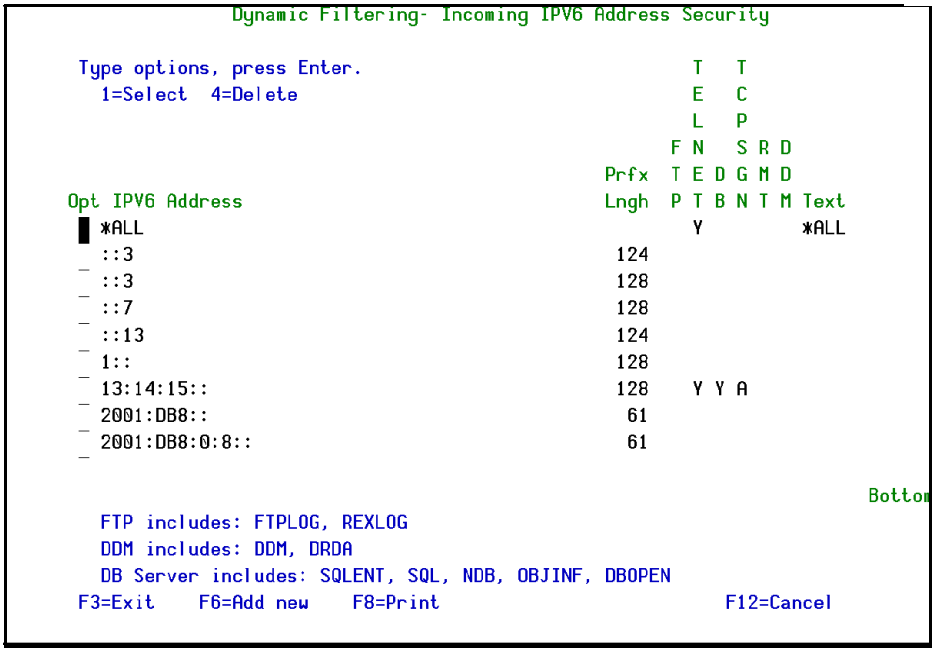


Figure 5-5. Work with Firewall - Incoming IPv6 Address Security

Field	
Defaults	Specifies defaults assigned to changes made in this library.

Options	
1=Select	Modify an existing IPv6 definition.
4=Delete	Delete an IPv6 definition.

Function Keys	
F4=Prompt	Opens a prompt screen to select 1 or more IPv6 definitions.
F6=Add new	Opens a prompt screen to select 1 or more IPv6 definitions.
F8=Print	
F10=Logon security	

3. Type **1** to select an existing rule or press **F6** to create a new rule.
4. If you are creating or modifying a rule, the **Dynamic Filtering Incoming/Outgoing IPv6 Address** screen appears.

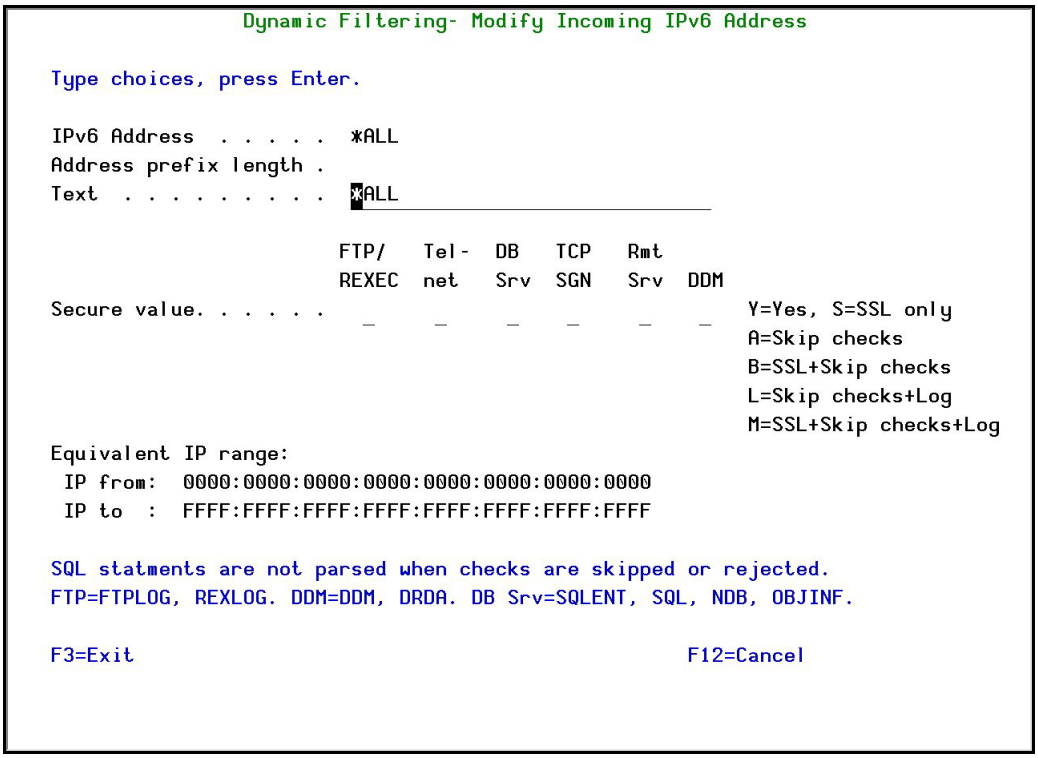


Figure 5-6. Modify Firewall Incoming IPv6 Address Screen

Field	Description
IPv6 Address	Enter an IPv6 address using the standard format.
Address prefix length	Enter the address prefix length
Text	Descriptive text
Secure value	**Y=Yes** = Type **Y** to allow activity or leave the field Blank to reject activity for each individual server. **S=SSL** = Type **S** to set SSL restrictions for the various types of access protocols. **A**=Allow always **B**=SSL+Skip checks **L**=Allow always and log **M**=SSL+Skip checks+Log Use of **B** and **L** 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.
Equivalent IP Range	Displays the range of IP addresses as defined by the address prefix

5. Enter your required definitions and press **Enter**.

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 include:

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

To set the security mode to SSL:

1. Select **2 > 1**, type **1**. The **Dynamic Filtering - Modify Incoming IP Address** screen appears.

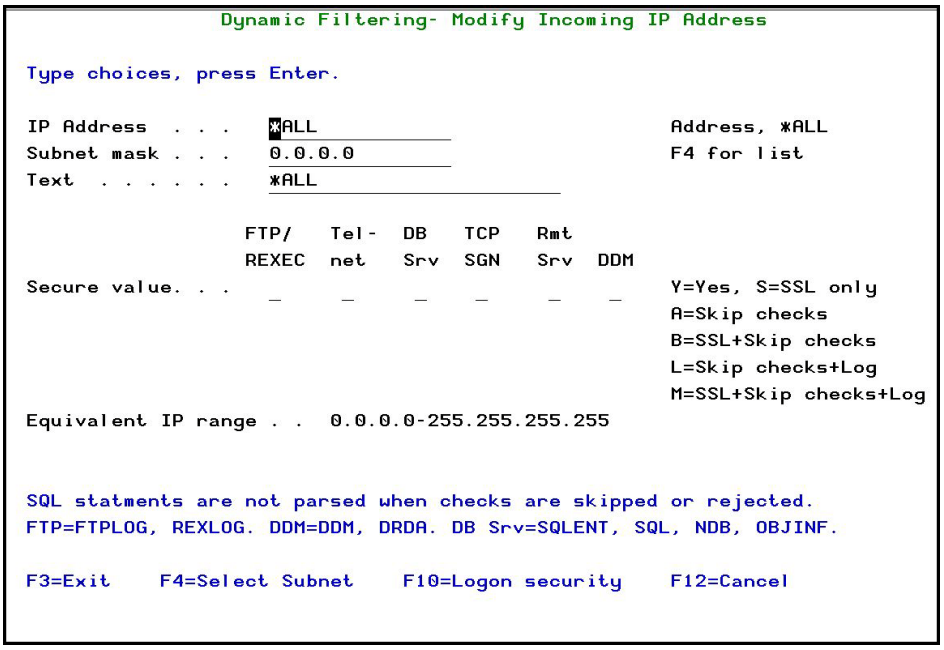


Figure 5-7. Dynamic Filtering- Modify Incoming IP Address

Field	Description
IP Address	Enter an IP address using the standard format.
Subnet mask	Enter the subnet mask or F4 for list
Text	Descriptive text

Field	Description
Secure value	**Y=Yes** = Type **Y** to allow activity or leave the field Blank to reject activity for each individual server. **S=SSL** = Type **S** to set SSL restrictions for the various types of access protocols. **A**=Allow always **B**=SSL+Skip checks **L**=Allow always and log **M**=SSL+Skip checks+Log Use of **B** and **L** 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.
Equivalent IP Range	Displays the range of IP addresses as defined by the address prefix

2. Press **Enter**.

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 IBM i 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. > 11. Incoming Remote System Names** from the **Work with Dynamic Filtering** menu. The **Dynamic Filtering- Incoming Remote System Names Security** screen appears. This screen lists all existing rules showing which communication protocols are allowed or rejected.

```
          Dynamic Filtering- Incoming Remote System Names Security

Type options, press Enter.
  1=Select  4=Delete
                       PASS-
Opt System*  DDM DRDA THROUGH Text
_  *ALL       Y
_  LLLLLLLL
                                                                  Bottom
F3=Exit    F6=Add new    F8=Print    F10=Logon security    F12=Cancel
```

Figure 5-8. Dynamic Filtering- Incoming Remote System Names Security Screen

2. Type **1** to select an existing rule or press **F6** to create a new rule.

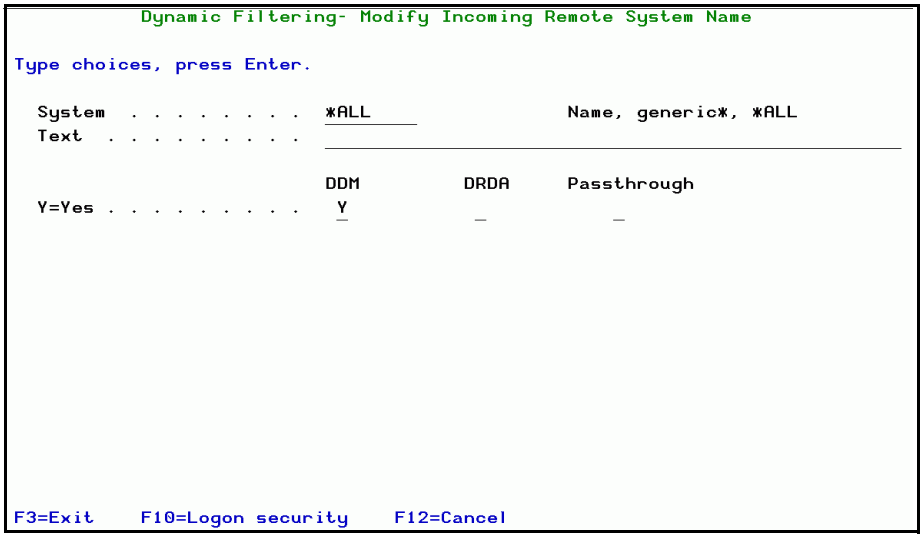


Figure 5-9. Work with Firewall - Modify Incoming Remote System Names Screen

Options	
1=Select	Modify an existing rule.
4=Delete	Delete an existing rule.

Function Keys	
F6=Add new	Create a new firewall rule.
F8=Print	Print list of firewall rules.
F10=Logon security	Work with Logon security rules.

6

Firewall Definitions

This chapter describes how to work with Firewall definitions.

To access this menu, select **42. Definitions** from the Firewall main menu.

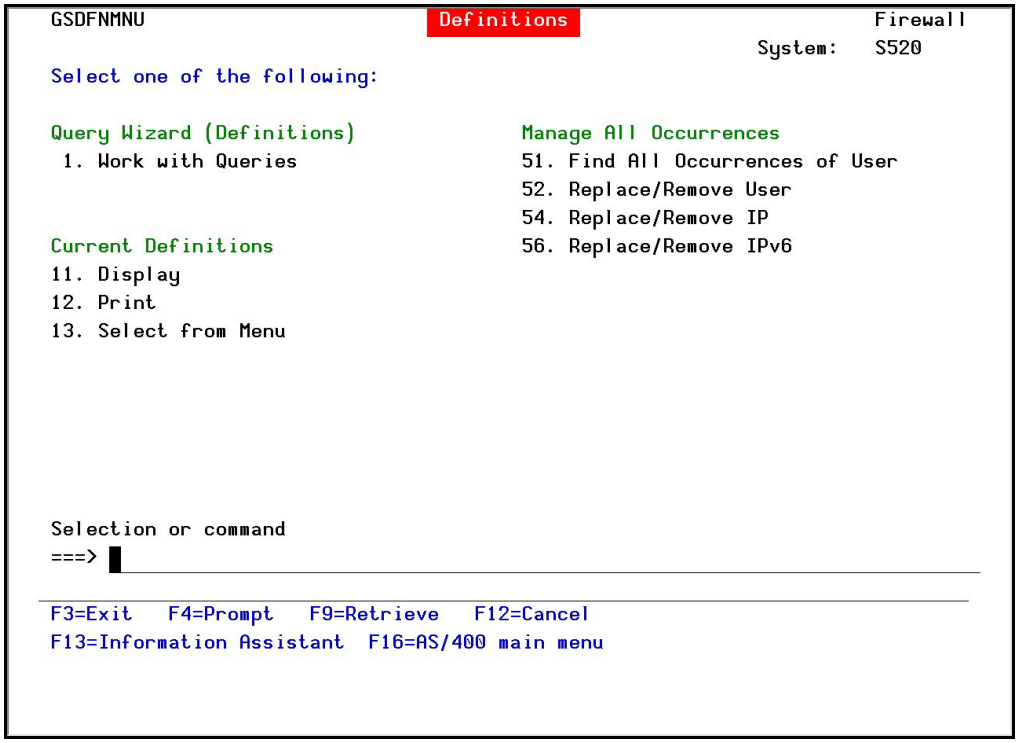


Figure 6-1. Definitions Menu

Query Wizard (Definitions)

The Query Wizard for Definitions allows you to work with predefined queries, to create new queries and to run one-time queries. For more information, see Query Wizard on page 84 in the Queries, Reports and Logs chapter.

The predefined queries available from the Definitions menu are a different set of queries to those available from the Reporting menu. The categories of reports available from the Definitions menu are shown in the table below.

Report category	Description
$9	Product definitions
1K	Native Object security

Report category	Description
1L	IFS Object security
1M	Command exceptions
1N	Users and groups

Current Settings

This feature allows you to display/print your Firewall definitions.

Display

1. To display your definitions, select **11. Display** from the **Definitions** menu. The **Display Security I Definitions** screen appears.
2. Enter a **Report type** to choose which definitions you want to display. Additional parameters appropriate to your choice appear that allow you to filter what will be displayed. The **Output** parameter is predefined as *****.
3. Enter your filter choices and press **Enter**. The report is displayed.

NOTE: Selecting ***ALL** for the Report Type only produces a single spool file, and not a separate spool file for each type of definition.

Print

The standard Print Definition option provides a single spool file to include all the different definitions.

1. To print your definitions, select **12. Print** from the **Definitions** menu. The **Display Security I Definitions** screen appears.
2. Enter a **Report type** to choose which definitions you want to print. Additional parameters appropriate to your choice appear that allow you to filter the report contents. The **Output** parameter is predefined as ***PRINT**.
3. Enter your filter choices and press **Enter**. The job is submitted.

NOTE: Selecting ***ALL** for the Report Type only produces a single spool file, and not a separate spool file for each type of definition.

Select from Menu

This option allows you to display/print your definitions from previously predefined queries.

1. Select **13. Select from Menu** from the **Definitions** menu. The **Definition Reporting - By Subject** menu appears.

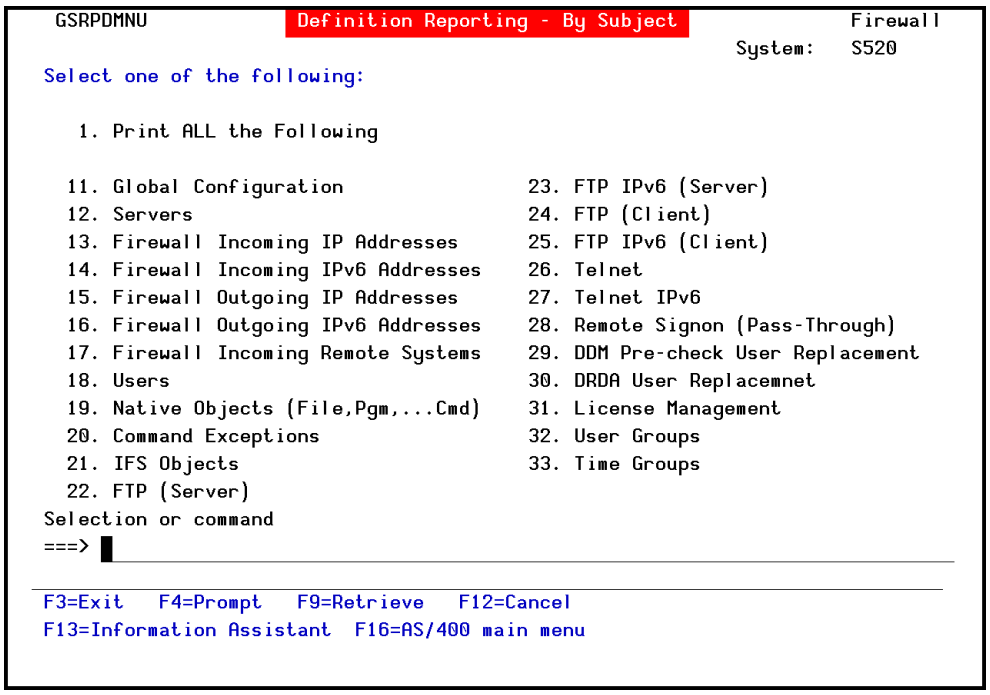


Figure 6-2. Definition Reporting - By Subject Menu

2. Select the definition type whose definitions you want to display/print.
3. If necessary, update the filter and output parameters.
4. Press **Enter**. The job is submitted.

Manage All Occurrences

This section enables you to perform global actions on all occurrences of definitions.

Find All Occurrences of User

This option allows you to print all the definitions of a specific User or of a %Group.

1. Select **51. Find All Occurrences of User** from the **Definitions** menu. The **Replace FW user** screen appears. The **Replace to user** field is predefined as ***PRINT** and cannot be changed.

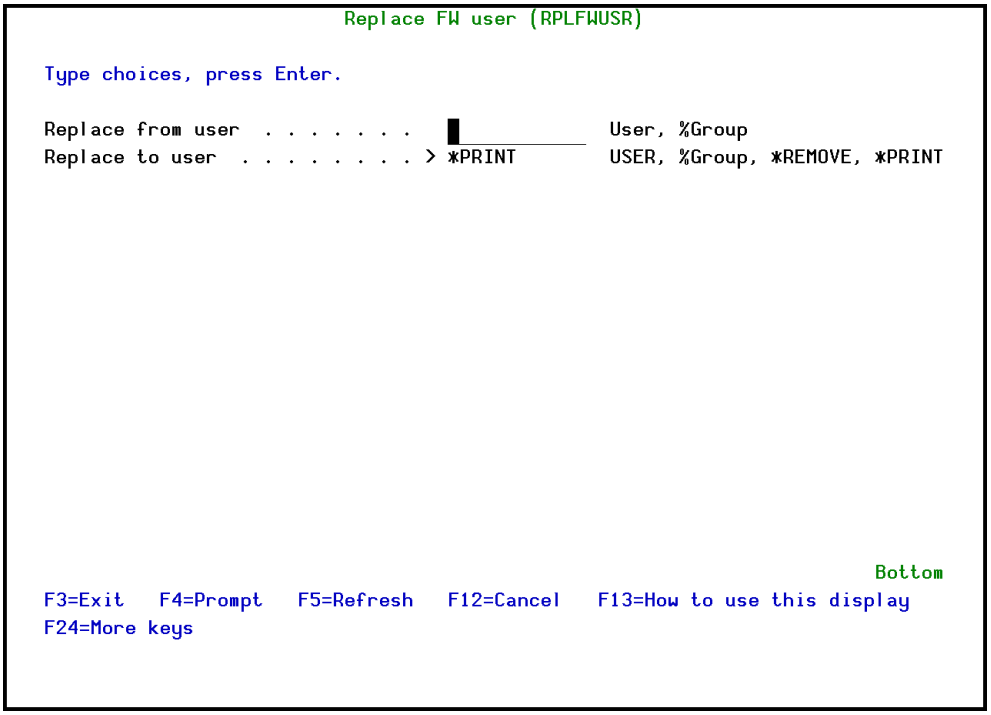


Figure 6-3. Print User Definitions Screen

2. Type the User or %Group you want to print in the **Replace from user** field.
3. Press **Enter**. The job is submitted.

Replace/Remove User

This option allows you to replace a specific User or %Group in all definitions with another User or %group. You can also remove or print all the definitions of a specific User or of a %group.

1. Select **52. Replace/Remove User** from the **Definitions** menu. The **Replace FW user** screen appears.

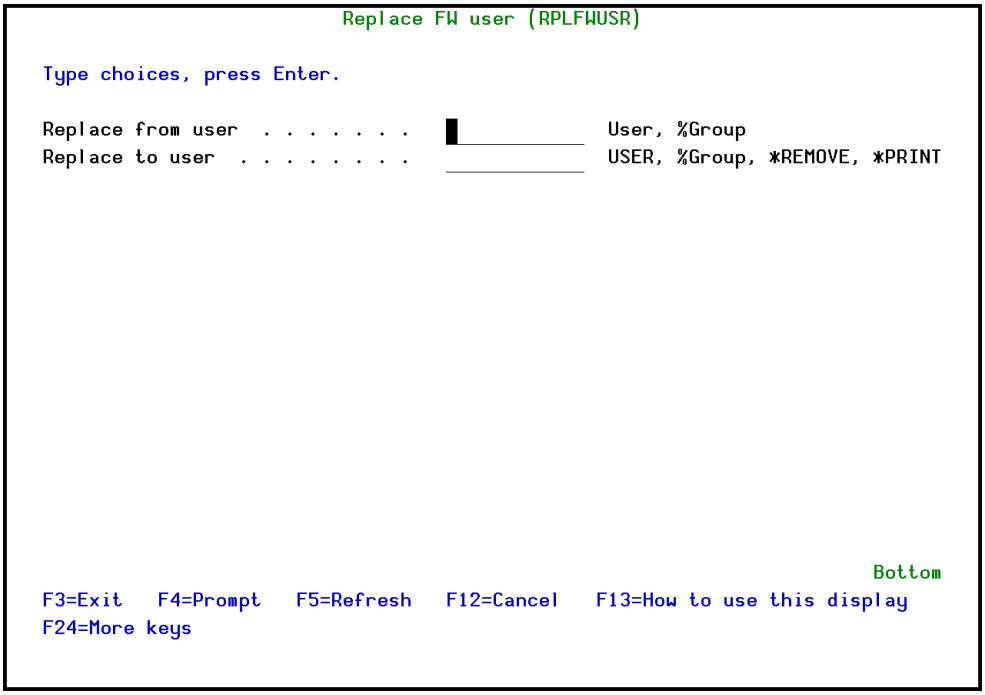


Figure 6-4. Replace/Remove User Definitions Screen

2. Type the parameters as shown in the table below.
3. Press **Enter**. The job is submitted.

Field	
Replace from user	The User or %Group to be replaced, removed or printed
Replace to user	**User** or **%Group** - the replacement User or %Group ***REMOVE** - remove all definitions for this User or %Group ***PRINT** - print all definitions for this User or %Group

Replace/Remove IP

This option allows you to replace a specific IP address in all definitions with another IP address. You can also remove or print all the definitions of a specific IP address.

1. Select **54. Replace/Remove IP** from the **Definitions** menu. The **Replace IP** screen appears.

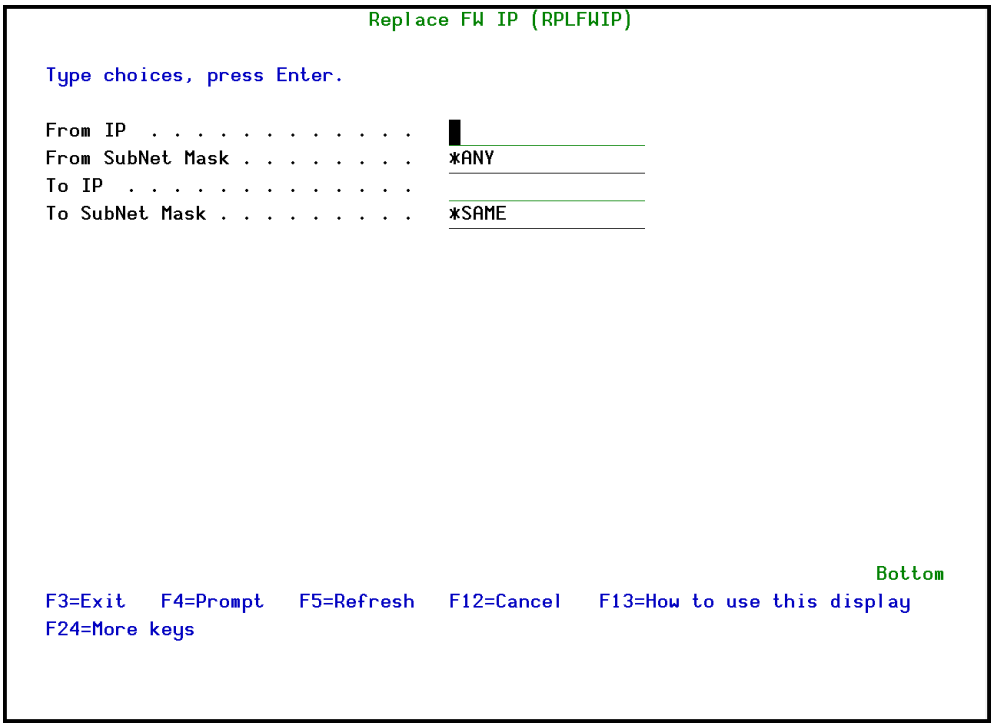


Figure 6-5. Replace/Remove IP Definitions Screen

2. Type the parameters as shown in the table below.
3. Press **Enter**. The job is submitted.

Field	
From IP	The IP address to be replaced, removed or printed Enter an IP address using standard decimal format.
From SubNet Mask	Enter a subnet mask using standard decimal format to define a range of IP addresses.
To IP	**IP address** - - the replacement IP address. Enter an IP address using standard decimal format. ***REMOVE** - remove all definitions for this IP address ***PRINT** - print all definitions for this IP address
To SubNet Mask	**Subnet Mask** - Enter a subnet mask using standard decimal format to define a range of IP addresses. ***SAME** - Use the same subnet mask as the **From SubNet Mask** field This field is not relevant if the **To IP** field is ***REMOVE** or ***PRINT**.

Replace/Remove IPv6

This option allows you to replace a specific IPv6 address in all definitions with another IPv6 address. You can also remove or print all the definitions of a specific IPv6 address.

1. Select **56. Replace/Remove IPv6** from the **Definitions** menu. The **Replace IPv6** screen appears.

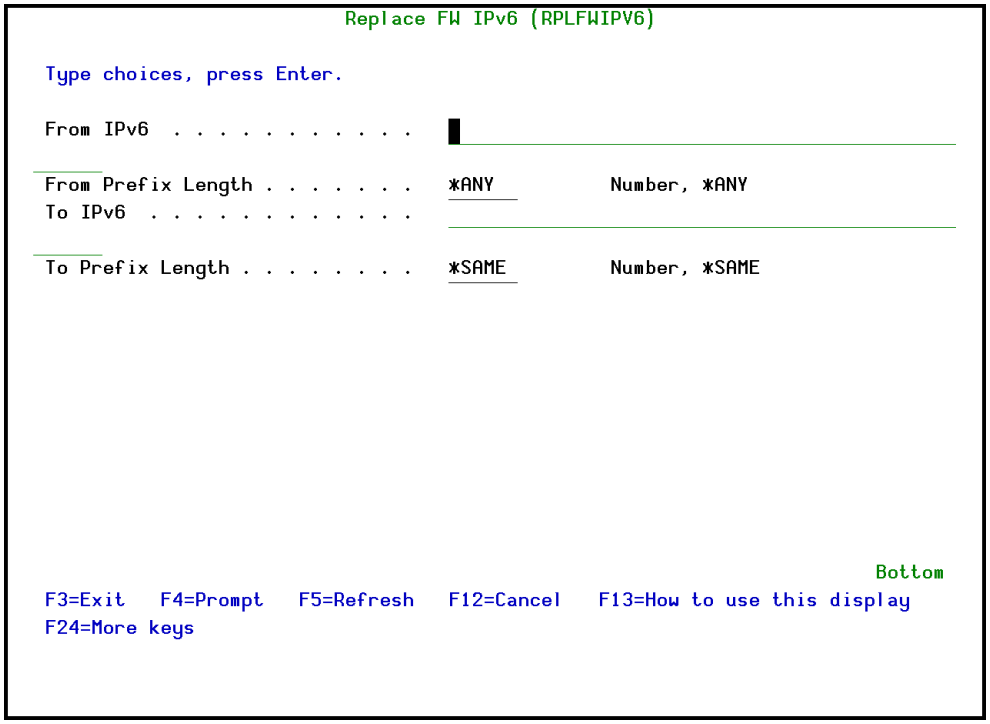


Figure 6-6. Replace/Remove IPv6 Definitions Screen

2. Type the parameters as shown in the table below.
3. Press **Enter**. The job is submitted.

Field	
From IPv6	The IPv6 address to be replaced, removed or printed Enter an IP address using the standard format.
From Prefix Length	Enter the address prefix length.
To IPv6	**IPv6 address** - - the replacement IPv6 address. Enter an IP address using standard decimal format. ***REMOVE** - remove all definitions for this IPv6 address ***PRINT** - print all definitions for this IPv6 address
To Prefix Length	**Prefix Length** - Enter the address prefix length. ***SAME** - Use the same prefix length as the **From Prefix Length** field This field is not relevant if the **To IPv6** field is ***REMOVE** or ***PRINT**.

7

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 more than one hundred 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 **41. Log, Queries, Groups** from the Firewall main menu.

```
 GSRPTMNU                          Reporting                          Firewall
                  (Including HTML, PDF, CSV, Outfile->GUI) System:    S520
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                              Network reporting SYSTEM()
41. Group Items for Selection               71. Network Description
48. Copy Time Group                         75. Current Job CntAdm Messages
49. Time Groups                             76. All Jobs CntAdm Messages

Selection or command
===>

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

Figure 7-1. Reporting Menu

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 **41 > 1. Work with Queries** 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, **X** to export or press **F6** to create a new query.
3. Press **Enter** to proceed to the definition screens.

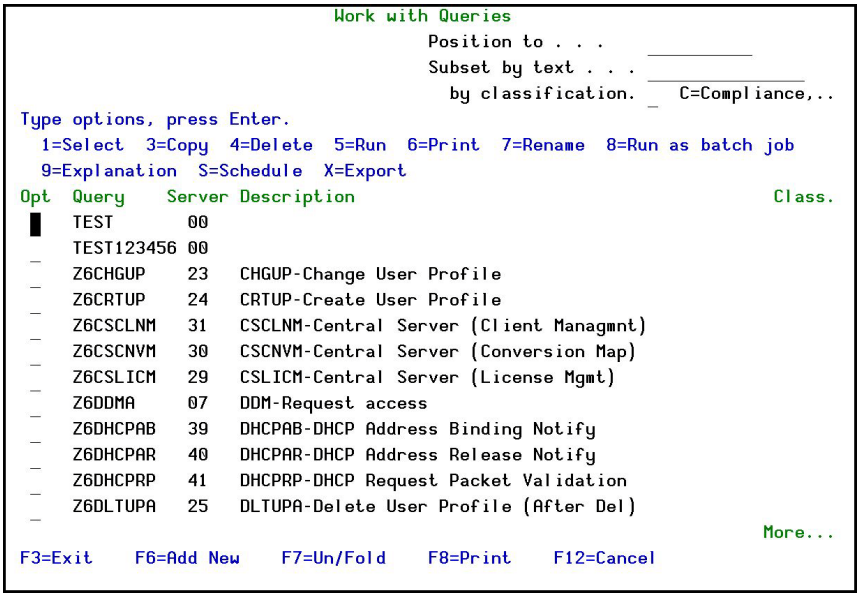


Figure 7-2. Work with Queries Screen

The following tables list the options available on this screen.

Field	
Position to	Position the cursor to this query name. This can save you having to page through a large number of queries.
Subset by text	Only display the queries that contain this text.
By classification	Only display the queries that contain this classification.

Options	
F6=Add New	Create a new query
1=Select	Select a query for modification.
3=Copy	Copy a query. Type the new query name and description in the pop-up window and press **Enter** to continue.
4=Delete	Delete the query. Press **Enter** to confirm deletion when the warning message appears.
5=Run	Run the selected query as an interactive job.
6=Print	Print the selected query to the standard output device and file type (*PDF, *HTML, *CSV …)
7=Rename	Rename the query. Type the new query name in the pop-up window and press **Enter**.
8=Run as batch job	Run the selected query as a batch job.
9=Explanation & Classification	Displays a popup window that defines the classification and explanation for the report. The explanation is added to the end of the report, enabling the recipient of the report (for example, an auditor) to receive it together with actual data.
S=Schedule	Add the report to a report group.
X=Export	Export one or many queries. When **F3=Exit** is pressed, a screen is displayed allowing the user to specify the target system or systems group (Multi System must be available). Alternatively, ***NONE** can be entered. ***NONE** will display the name of the ***SAVF** that is created, and the Import command parameters that are required on the report system to load the exported reports. With ***NONE** it is the customer's responsibility to transfer the ***SAVF** to the target systems.

NOTE: A Firewall query has been added **Z$9_FWDFN $9 Firewall definitions (Spool file format)** which enables you to run queries for Firewall and spool them to HTMP, PDF, and email.

Modifying Queries

This screen contains several basic query definition parameters.

1. To work with query parameters, enter the required parameters and press **Enter** to continue.

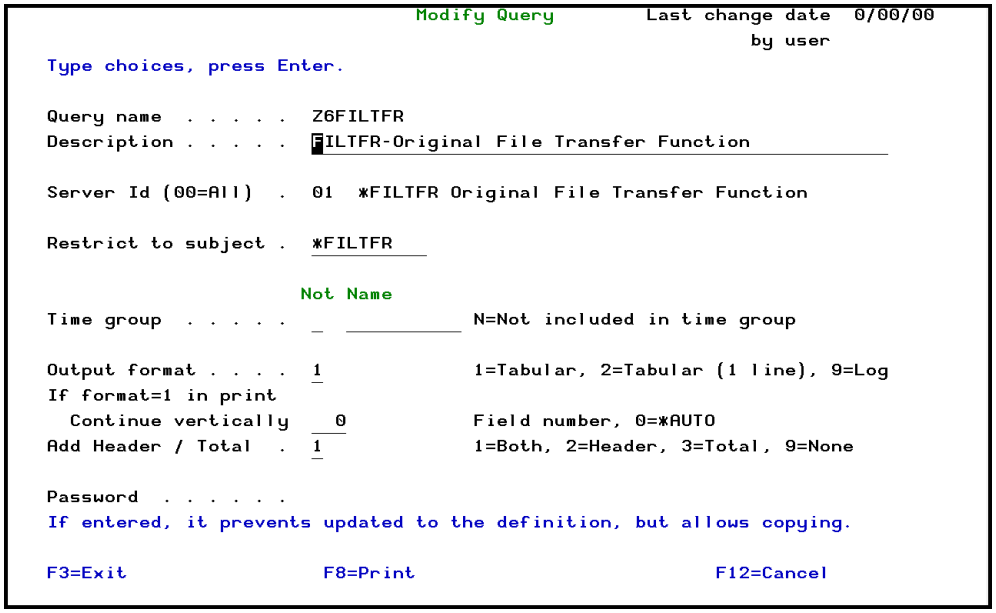


Figure 7-3. Modify Query Screen

Field	
Query Name	Name of the query
Description	Free text description of the query.
Server Id (00=All)	Type the server against which this query will run. Type 00 to run the query against all servers.
Restrict to subject	You can restrict the query to a specific type of activity. Press **F4** for a list of possible entries.
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
Continue Vertically	**Field number**, ***Auto** Only valid for Output Format = 1
Add Header / Total	**1** = Both **2** = Header **3** = Total **9** = None
Password	Enter a password to prevent updates to the query definition.

2. Press **Enter** from the **Modify Query** screen to continue to the **Filter Conditions** screen.

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.

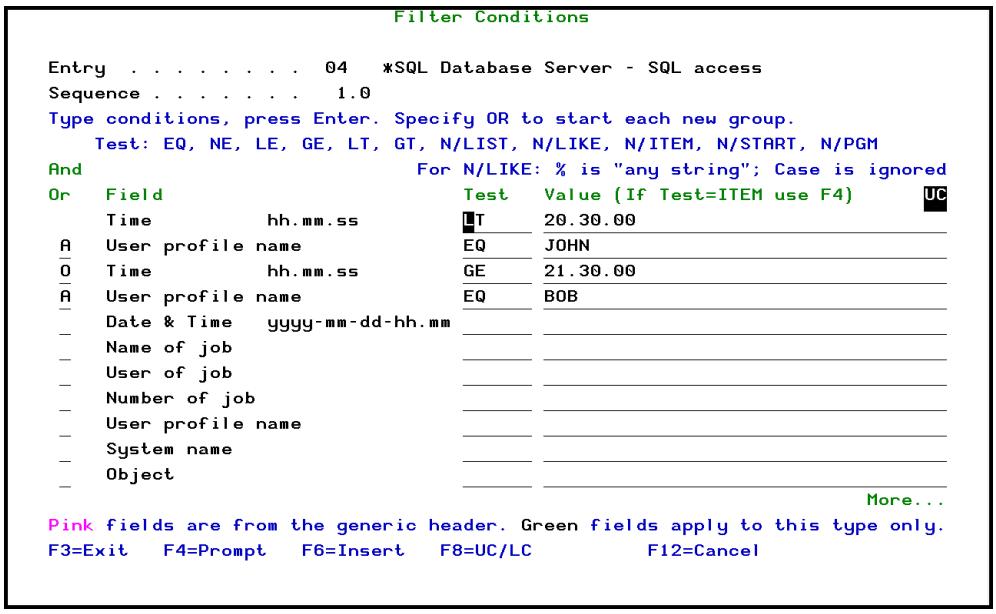


Figure 7-4. Filter Conditions Screen

Field	
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

Function Keys	
F4=Prompt	Opens a prompt screen.
F6=Insert	Insert a new condition.
F8=UC/LC	Toggle between case sensitive and not case sensitive for the N/LIKE comparison.

Comparison Test Operators

The following comparison test operators are available:

Test	Description	Value Field Data
EQ, NE	Equal to, Not equal to	Value

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

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 A **or** the conditions listed in Group B. Group B includes the **Or** condition and all of the **And** conditions that follow it.

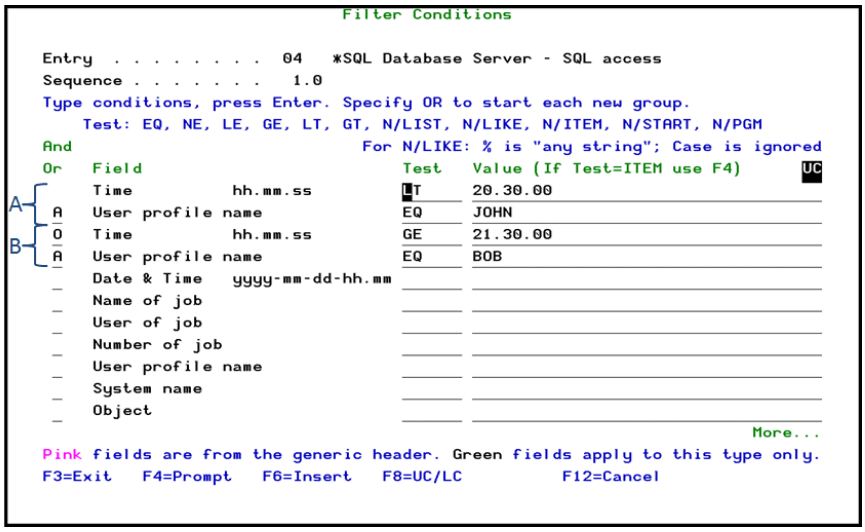


Figure 7-5. Filter Conditions Screen

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.

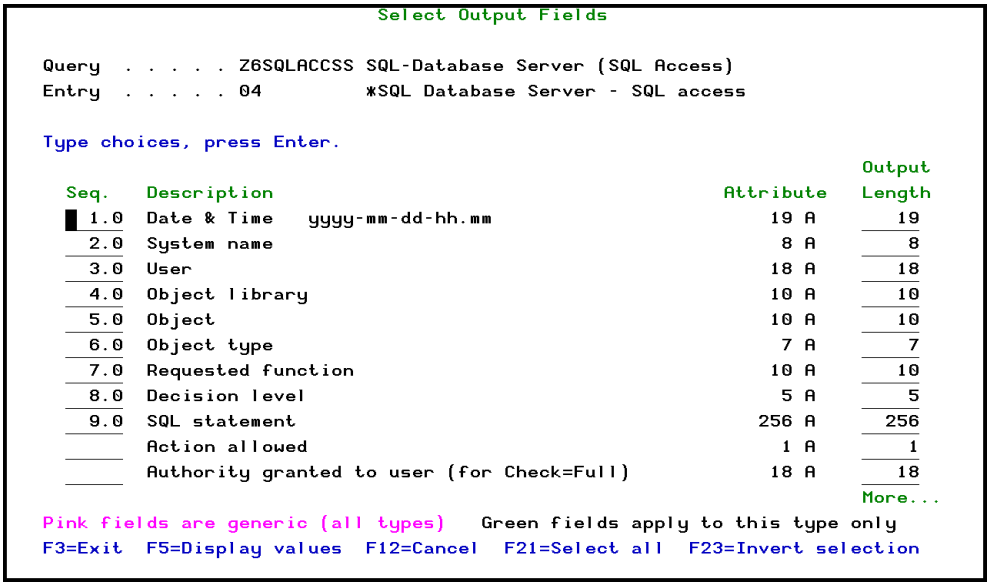


Figure 7-6. Select Output Fields Screen

Field	
Seq.	Enter the sequence in which you wish this field to appear in the query output. Lower numbers appear toward the left of the output and higher numbers appear toward the right.
Output Length	Number of characters of the field to print.

Function Keys	
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.

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.

When a query is run on multiple systems, the System field containing the system name will be implicitly added to the printed fields, if it is not there.

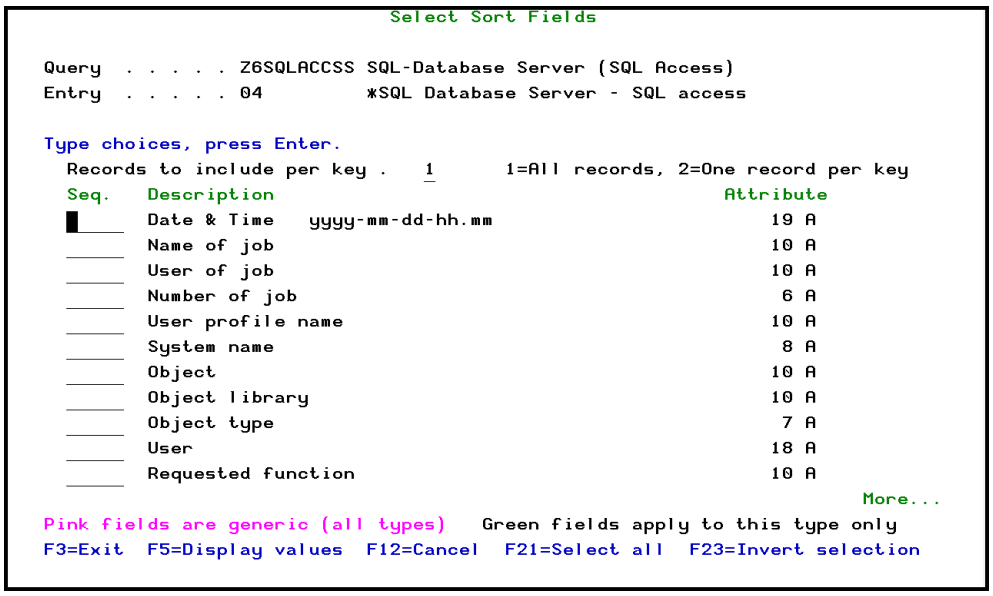


Figure 7-7. Select Sort Fields Screen

Field	
Records to include per key	**1** = All records Once the user selects a field with records to include per key, all records will appear in the report. **2** = One record per key This option displays only a single match to the field. For example, if multiple SQL fields would be returned using All Records, only a single one will be written in the report when using this option.
Seq.	Enter the sort sequence for the field. The lowest sequence number represents the primary sort field. The second lowest number represents the secondary sort field, and so on.
Description	Description of field to sort
Attribute	Sort order can be defined as **A**=Ascending **D**=Descending

Function Keys	
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.

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 predefined schedule. This option is typically used for generating periodic audit reports.
- Query Menu - Select one of the following options from the Query menu:
- 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 *JOHNSMITH* and you enter run-time criteria for the user *BILLJONES*, 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 Firewall Query** screen.

```
                        Run Firewall Query (RUNFWQRY)

Type choices, press Enter.

Query  . . . . . . . . . . . . .  *SELECT       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, *PDF, *HTML..




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

Figure 7-8. Run Firewall Query Screen

Field	
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 to 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
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
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
Merge data to a single output	***YES**, ***NO** (When <System to run for> is not *CURRENT)
Place output on	***CURRENT**, ***SYSTEM** (When <System to run for> is not *CURRENT)
Print format	***SHORT**, ***FULL** (When Output = *PRINT)
Add column headings	***NO**, ***YES** (When Output = *CSV)
Add control fields	***NO**, ***YES**: if Output = *OUTFILE or *CSV, some fields (for example, user, type) are added to the record to enable easier programming manipulation
Job description	**Name**, ***NONE** to run interactively
Library	**Library** of the job description
Type	Filter records by audit type ***All** = All types as specified in the query definition ***QRY** = Select server type from a list **Server Type** = Enter the server type
Program Name	***ALL** or Filter records by the name of the program that created the journal record.
Job Name	***ALL** or Filter records by OS/400 job name.

Field	
Job Name - User	***ALL** or Filter records by OS/400 job name.
Job Name - Number	***ALL** or Filter records by OS/400 job name.
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
Filter by Time Group - Time Group	**Name** = Name of time group ***SELECT** = Select time group from list at run time
Original command sent from	**Internal use only**
Object	The IFS object name that is created. ***TEMP** = a temporary object is created and deleted after being attached ***QRY** = The name is the query name ***AUTO** = The name will be created automatically
Directory	**/iSecurity/report output/** ***DATE** = A new directory per date is created to keep all reports running during that date
User defined data	**Internal use only**

Function Keys	
F4=Prompt	Prompt for valid entries in the field where the cursor is located.
F5=Refresh	Restores the default definitions
F9=All Parameter	Display all parameters available for the command. Usually, the only parameters displayed are those that are relevant, depending on already entered parameters.
F10=Additional parameters	Display the relevant additional parameters that are relevant, depending on already entered parameters.
F11=Keywords/Choices	Toggle between displaying the keywords or the choices for each parameter.
F14=Command string	Display the full command string that will be run, on the basis of the current parameter choices.
F15=Error messages	Display any relevant error messages.
F16=Command complete	Run the command instantly.
F24=More keys	Display additional command keys.

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.

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

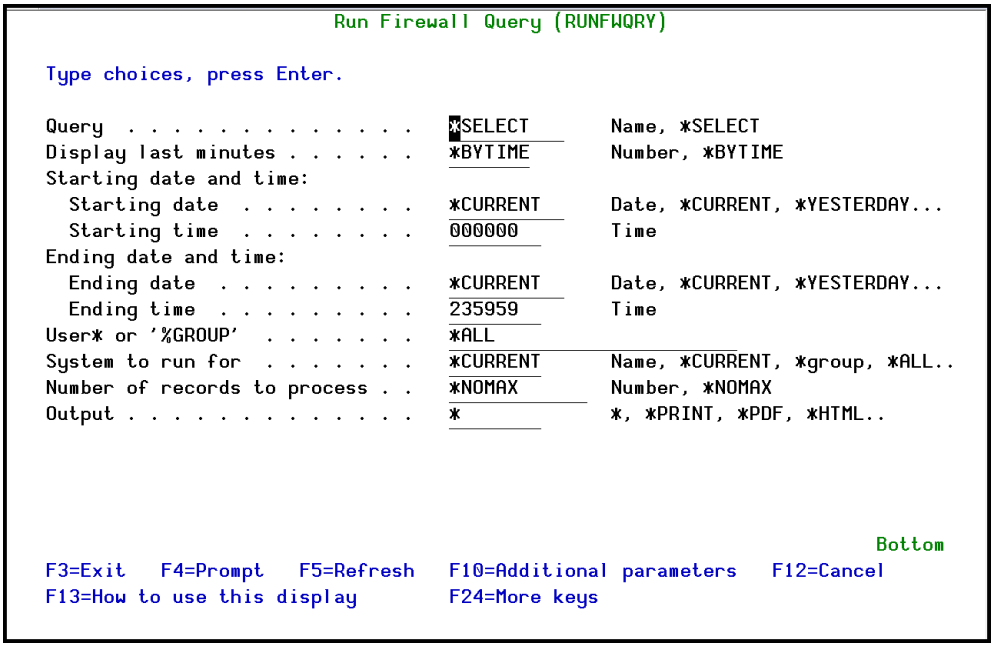


Figure 7-9. Run Firewall Query Screen

For Output field, the following options will open additional parameters: ***HTML**, ***PDF**, ***CSV**.

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 massages 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 **41. Log, Queries, Groups** from the main menu. The Reporting menu appears.
2. Select **19. Select from menu** and choose one of the many predefined 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.

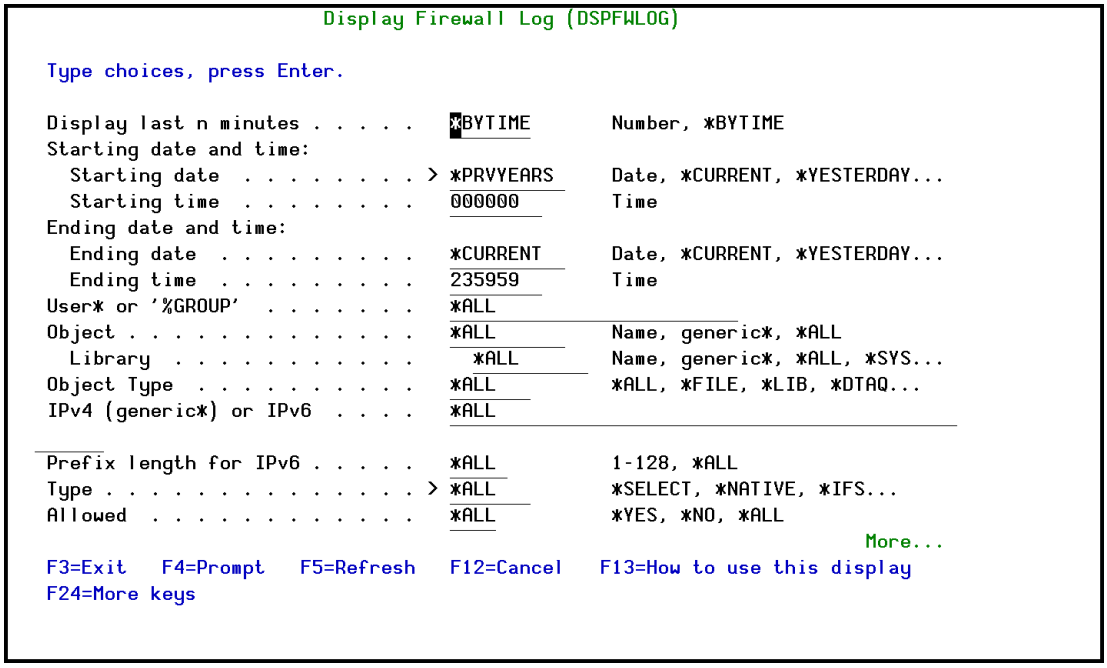


Figure 7-10. Display Firewall Log Screen

Field	
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 to 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
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

Field	
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
Merge data to a single output	***YES**, ***NO** (When <System to run for> is not *CURRENT)
Place output on	***CURRENT**, ***SYSTEM** (When <System to run for> is not *CURRENT)
Print format	***SHORT**, ***FULL** (When Output = *PRINT)
Add column headings	***NO**, ***YES** (When Output = *CSV)
Add control fields	***NO**, ***YES**: if Output = *OUTFILE or *CSV, some fields (for example, user, type) are added to the record to enable easier programming manipulation
Job description	**Name**, ***NONE** to run interactively
Library	**Library** of the job description
Type	Filter records by audit type ***All** = All types as specified in the query definition ***QRY** = Select server type from a list **Server Type** = Enter the server type
Program Name	***ALL** or Filter records by the name of the program that created the journal record.
Job Name	***ALL** or Filter records by OS/400 job name.
Job Name - User	***ALL** or Filter records by OS/400 job name.
Job Name - Number	***ALL** or Filter records by OS/400 job name.
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
Filter by Time Group - Time Group	**Name** = Name of time group ***SELECT** = Select time group from list at run time
Original command sent from	**Internal use only**
Object	The IFS object name that is created. ***TEMP** = a temporary object is created and deleted after being attached ***QRY** = The name is the query name ***AUTO** = The name will be created automatically
Directory	**/iSecurity/report output/** ***DATE** = A new directory per date is created to keep all reports running during that date
User defined data	**Internal use only**

Function Keys	
F4=Prompt	Prompt for valid entries in the field where the cursor is located.
F5=Refresh	Restores the default definitions
F9=All Parameter	Display all parameters available for the command. Usually, the only parameters displayed are those that are relevant, depending on already entered parameters.
F10=Additional parameters	Display the relevant additional parameters that are relevant, depending on already entered parameters.
F11=Keywords/Choices	Toggle between displaying the keywords or the choices for each parameter.
F14=Command string	Display the full command string that will be run, on the basis of the current parameter choices.
F15=Error messages	Display any relevant error messages.
F16=Command complete	Run the command instantly.
F24=More keys	Display additional command keys.

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. See Figure 7-12 on page 101 for an example of the audit log display.

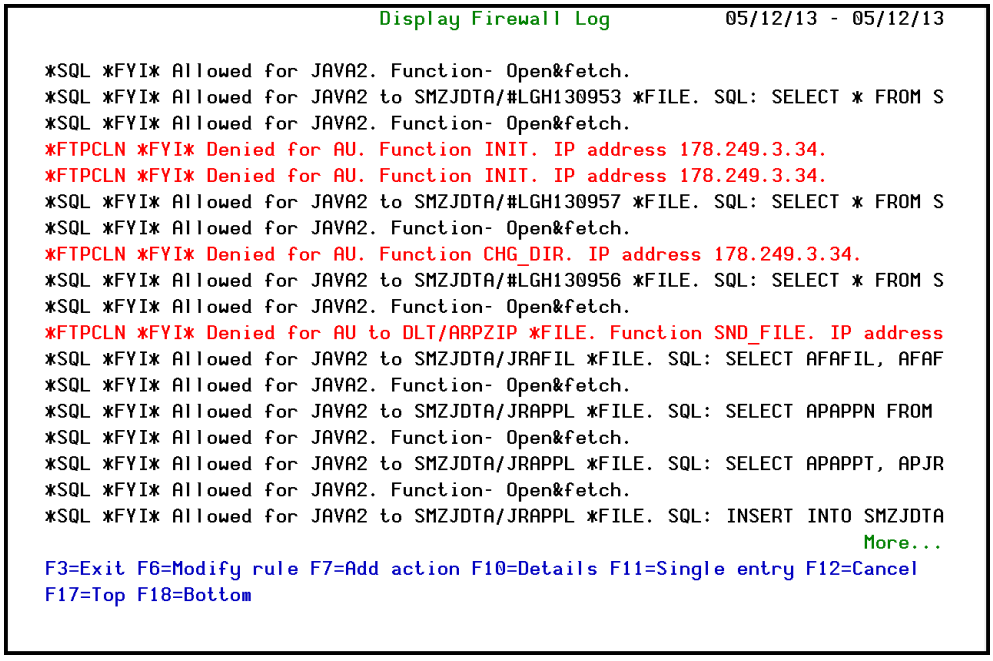


Figure 7-11. Display Firewall Log

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 pro-actively 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 F11 or Enter. Figure 7-12 on page 101 displays an example of an activity log.

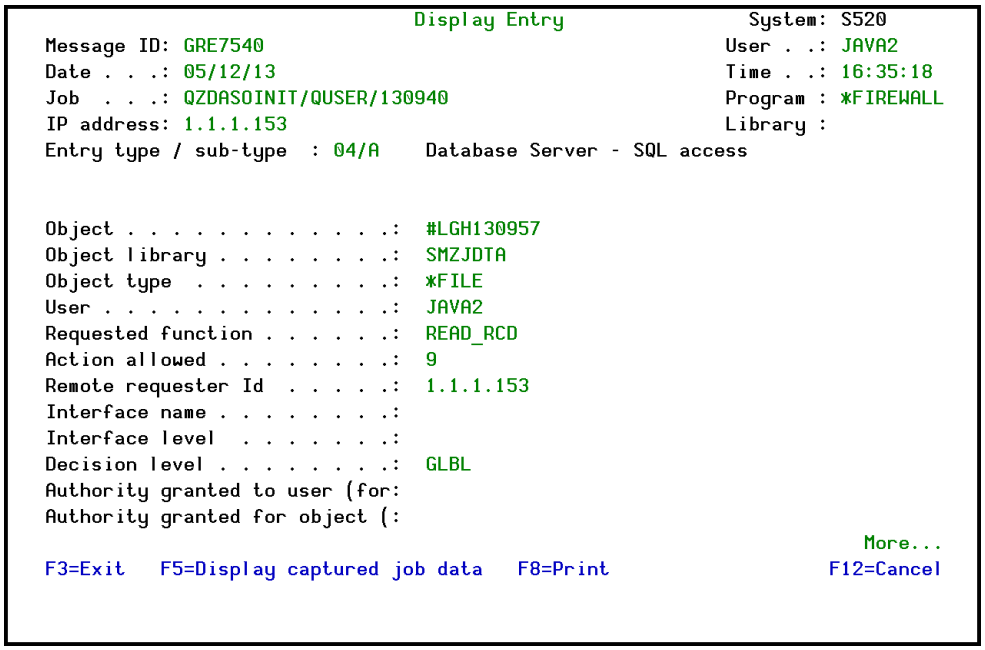


Figure 7-12. Individual Message Information

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.

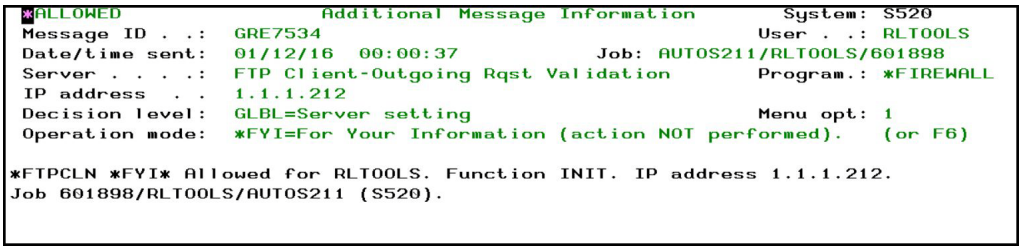


Figure 7-13. Additional Message Information

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.

1. To work with statistical information, select option **41. Log, Queries, Groups** from the main menu. The **Reporting** menu appears.
2. Select option **62. User Activity Statistics**. The **Display User Activity** screen appears.

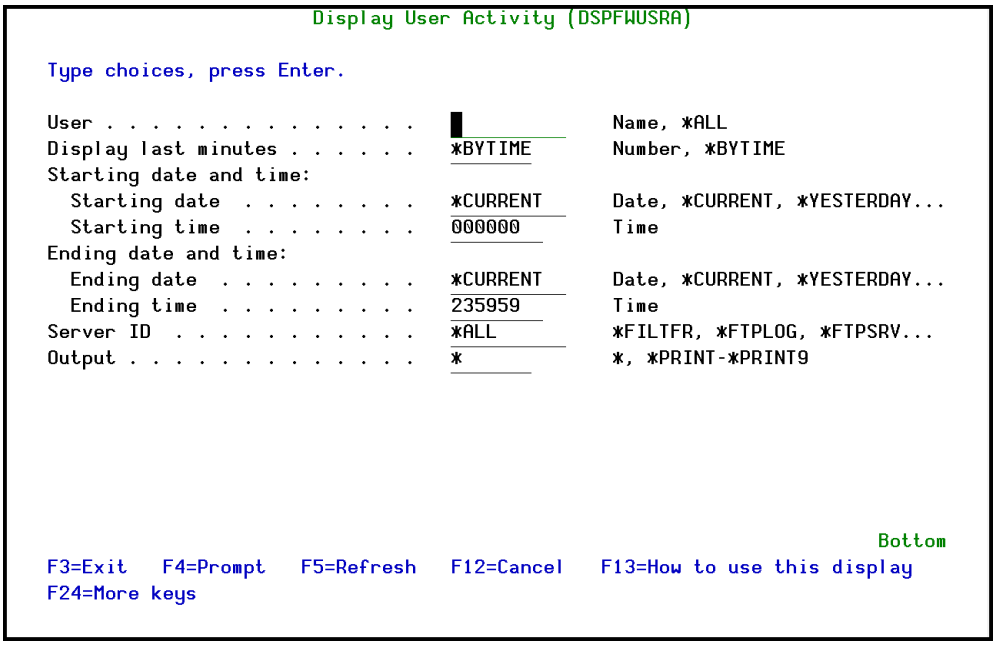


Figure 7-14. Display User Activity

Field	
User	
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 to 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

Field	
Server ID	Choose servers you want to examine. For all servers, enter ***ALL**.
Output	***PRINT** = Prints to the local printer ***PRINT1** = Prints to the remote printer ***PRINT2** = Prints to both remote and local printers

Group Items for Selection

Define assorted groups of reports to meet 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, and so on.

For each GROUP-TYPE, you can define an unlimited number of GROUPS and within the 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 might 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. Similarly, 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 and so on, which are the users who have this particular privilege defined in their special authority.

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

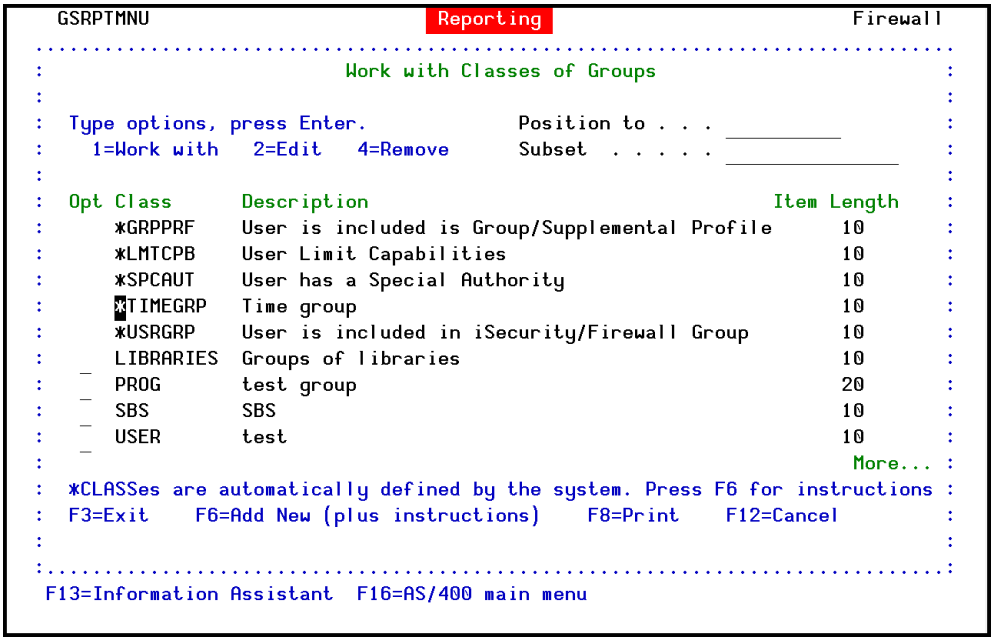


Figure 7-15. Work with Classes of Groups

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

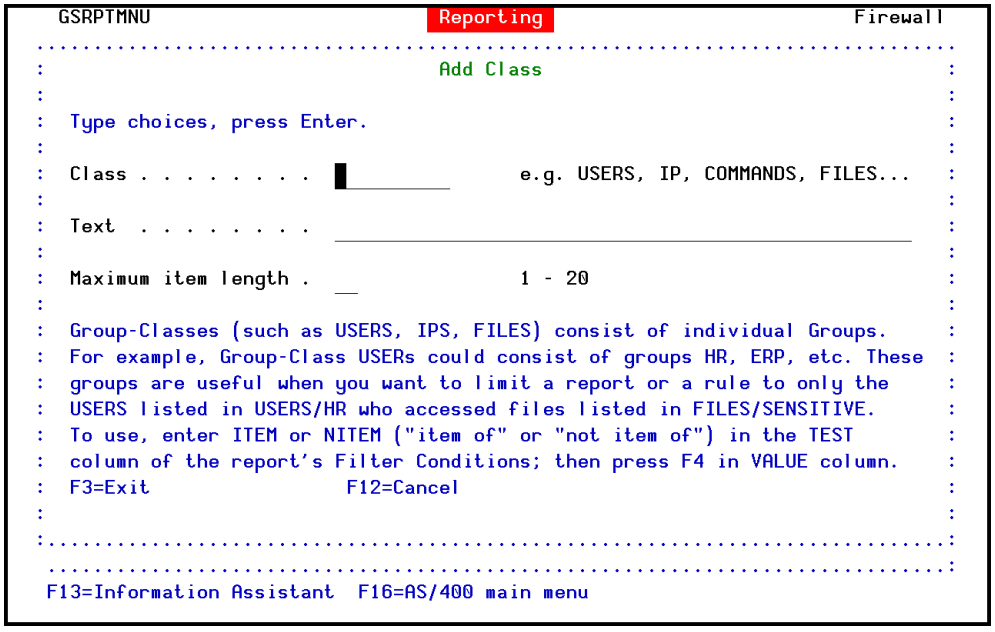


Figure 7-16. Add Class

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

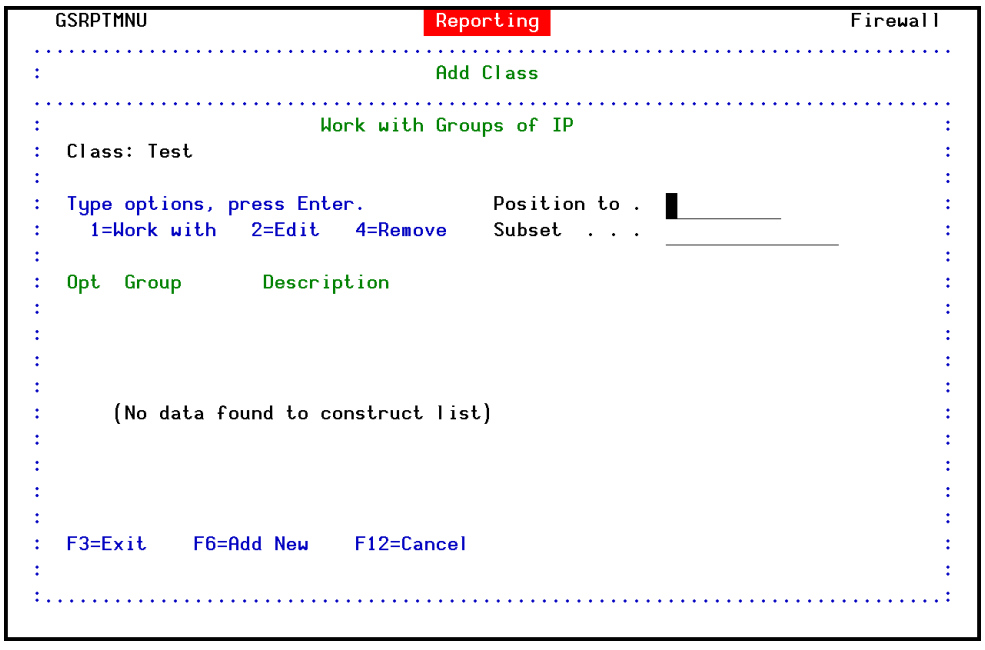


Figure 7-17. Work With Groups

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

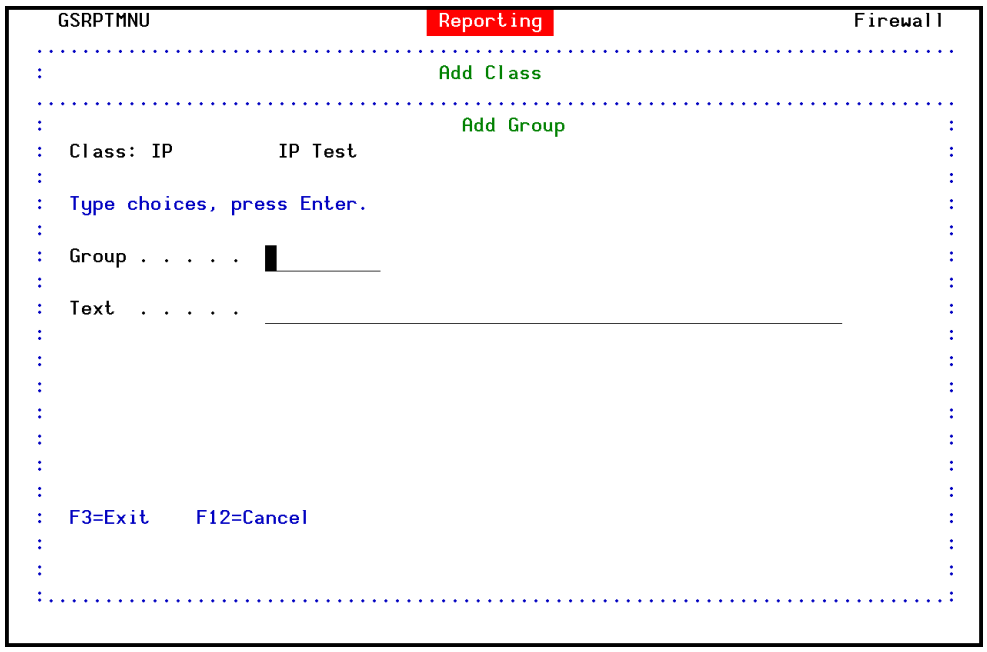


Figure 7-18. Add Group

The following TYPES are supported:

- *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 and provides instructions for its use.

Overview

The Report Scheduler allows you to run predefined "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:

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 **41 > 51. Work with Report Scheduler** from the **Log, Queries, Groups** menu. The **Work with Report Scheduler** screen appears.

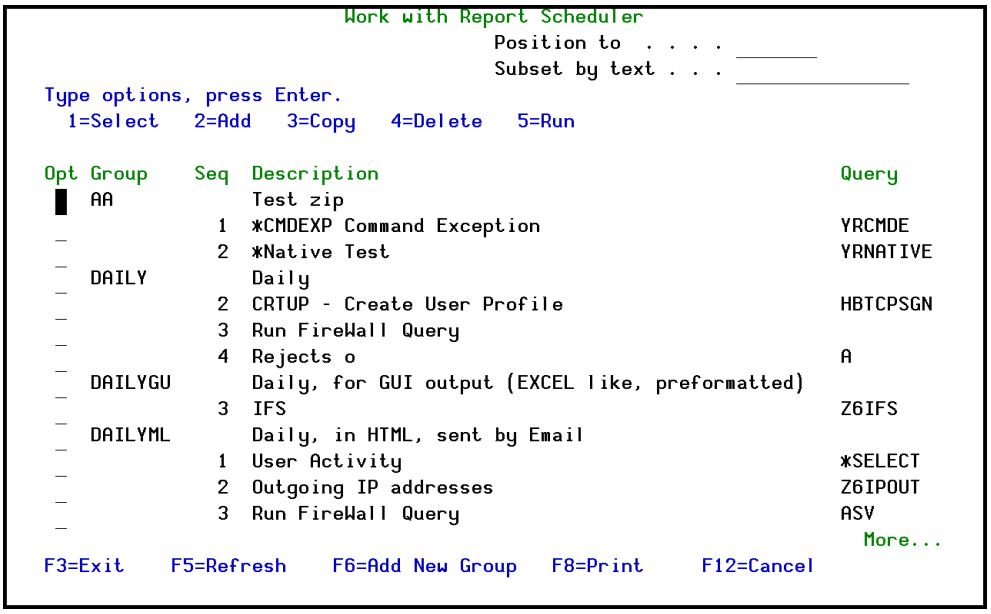


Figure 7-19. Work with Report Scheduler

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.

Field	
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

Function Keys	
F5=Refresh	Restores the default definitions
F6=Add New Group	Create a new report group.
F8=Print	Print the report groups.

2. Press **F6** to create a new report group or type **1** to select an existing group.
3. The **Modify Report Group** screen appears. Assign a name to the report group and enter a brief description.

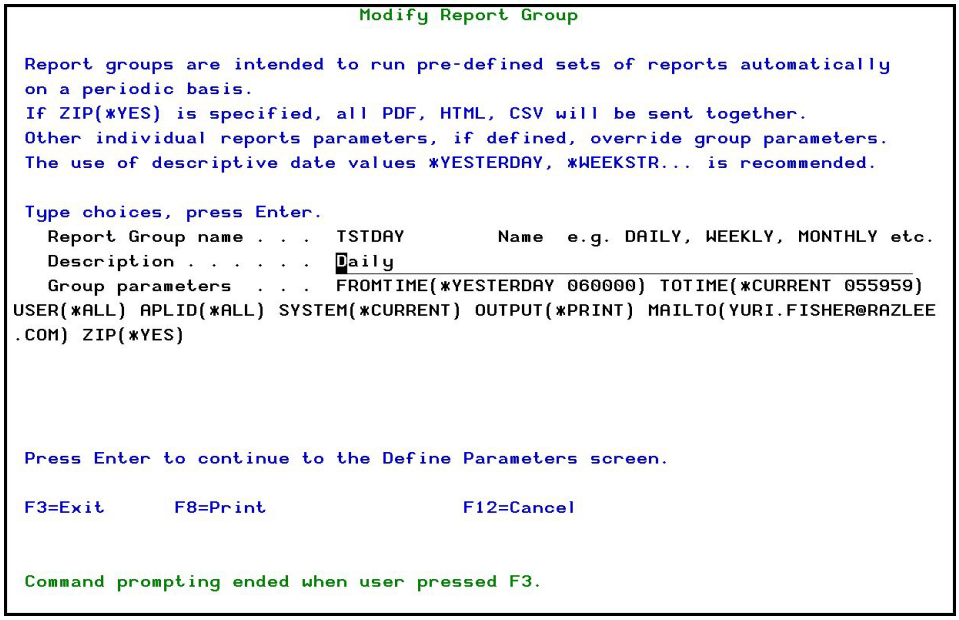


Figure 7-20. Modify Report Group

Field	
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: **FROMTIME (*YESTERDAY 060000)** = From time specified **TOTIME (*CURRENT 055959)** = To time specified **USER (*ALL)** = User/s in group **APLID (*ALL)** = Application ID in group **SYSTEM (*CURRENT)** = System in group **OUTPUT *(PRINT)** = Output type **MAILTO (<email>)** = Mail to member/s **ZIP (*YES)** = Zip and password protect

4. Select a Group parameter, and 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 (that is, it 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 ***BILL*** and you enter run-time criteria for the user ***JOHN***, no records will be displayed.

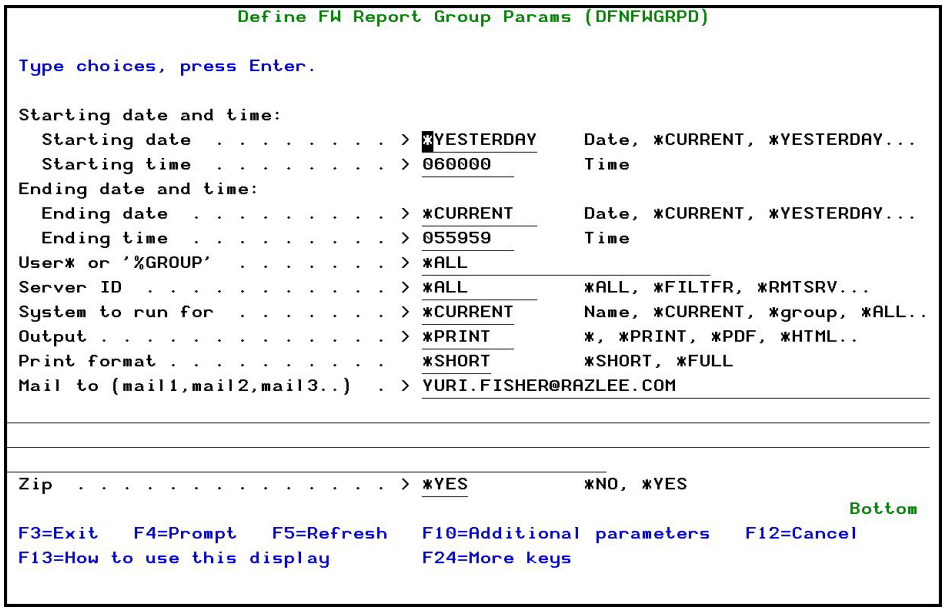


Figure 7-21. Define FW Report Group Details

Field	
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
Mail to (mail1, mail2, mail3...)	Mail recipients listed for receipt of group report email.

Field	
Zip	***YES** enables Group report to be zipped and password protected.

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

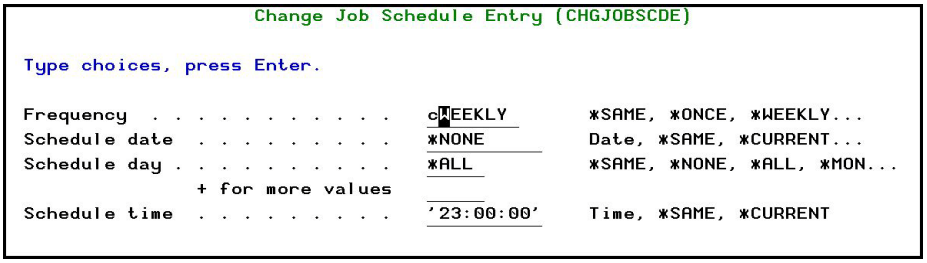


Figure 7-22. Change Job Schedule Entry

Field	
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) ***NONE** = Use day of week value in the Schedule Date field above. ***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 to an individual report to modify it. The **Add Report Definition** screen appears.

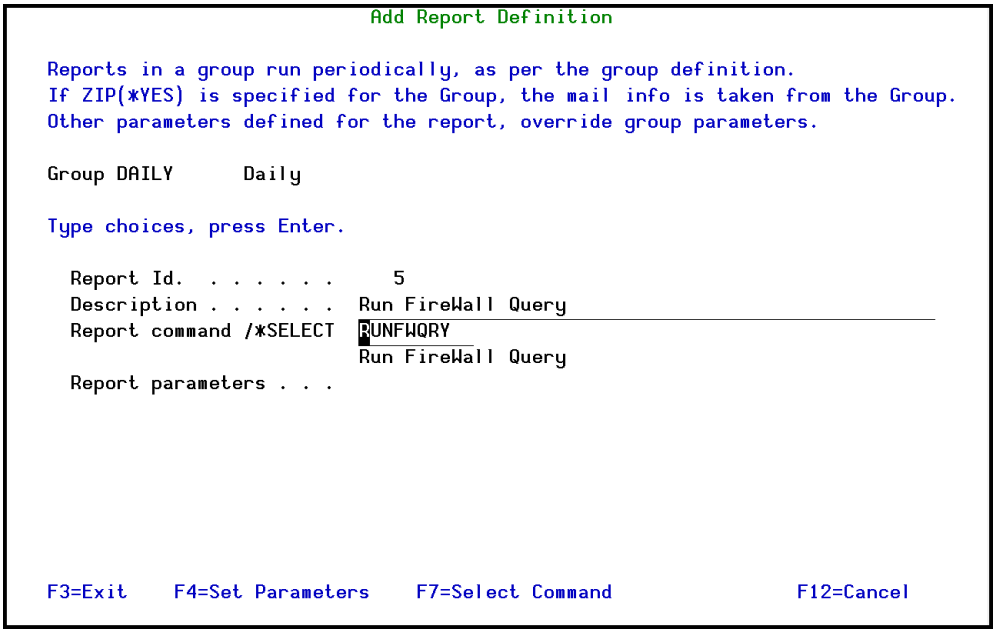


Figure 7-23. Add Report Definition

Field	
Report ID	Numeric identification automatically assigned by the Firewall
Description	Free text description of the report
Report Command (F4)	Press F4 to select the 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. Run a Report Group** from the **Log, Queries, Groups** menu. The **Run Report Group** screen appears.
2. Set your parameters according to the following table.

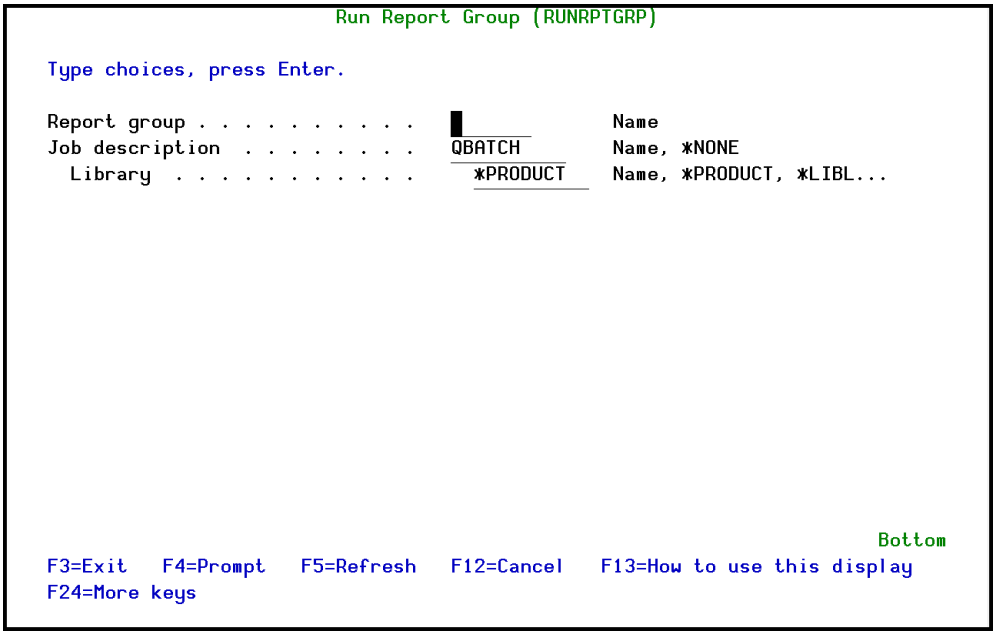


Figure 7-24. Run Report Group

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

8

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 IBM i and IFS objects.

Server security rules, as described in the Server Settings and Activation chapter, 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 IBM i 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, you can define that members of the user group **%PGMR** are not permitted to execute the SQL delete command.

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

Working with User Security

To work with user-to-service security:

1. 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.
2. To work with an existing rule, type **1** to select a rule or press **F6** to create a new rule.

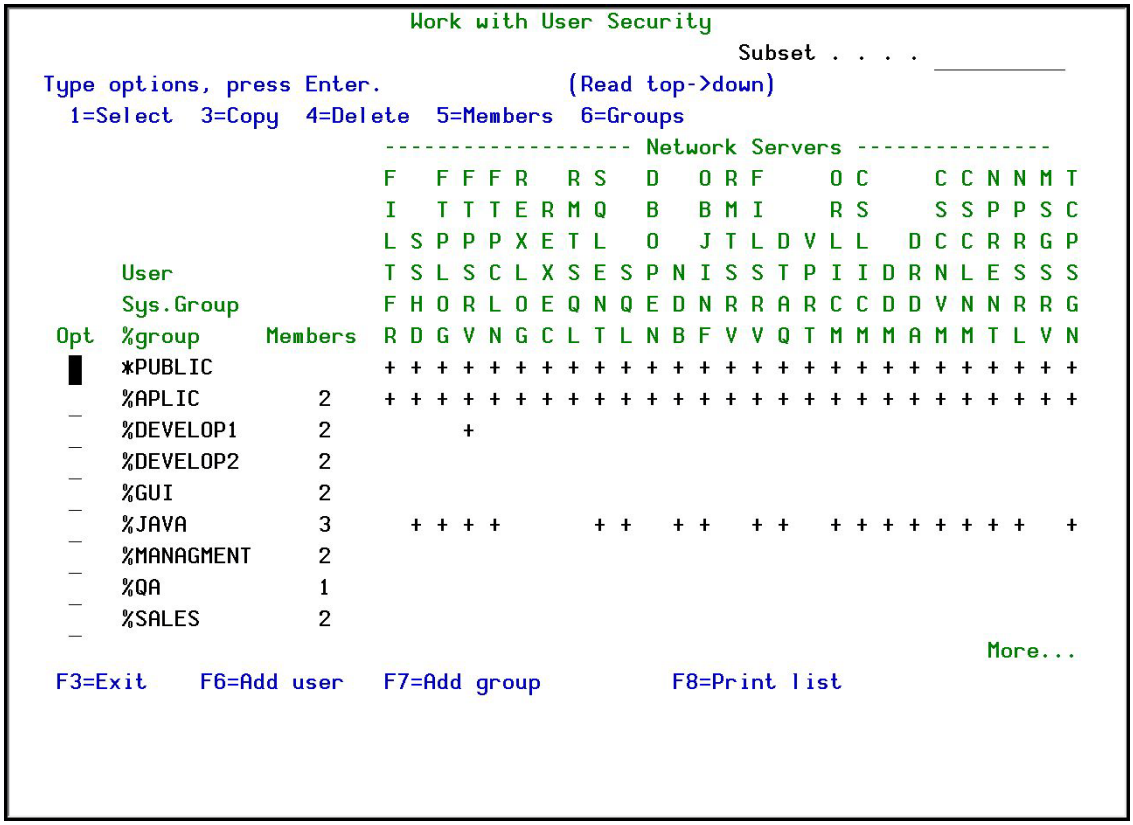


Figure 8-1. Work with User Security Screen

Field	Description
Servers	Displays the rule status for each server type: **+** = User-to-service rule overrides the global server security rule. Allow a user the access to a server and check for object authorizations. **V** = User-to-service rule overrides with verb (command) support **Blank** = Global server security rule governs activity for this server **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).
Members	The number of members within a %group or indicates the system user is a group profile

Options	
1=Select	Modify an existing rule.
3=Copy	Copy this rule for another user/group.
4=Delete	Delete an existing rule.
5=Members	Modify group members.
6=Groups	Show the association between the user and group profiles.

Function Keys	
F6=Add new	Create a rule for a new User.
F7=Add group	Create a rule for a new Group.
F8=Print list	Print user-to-service security rules

3. Enter parameters on the **Add/Modify User Security** screen and press **Enter** to confirm.

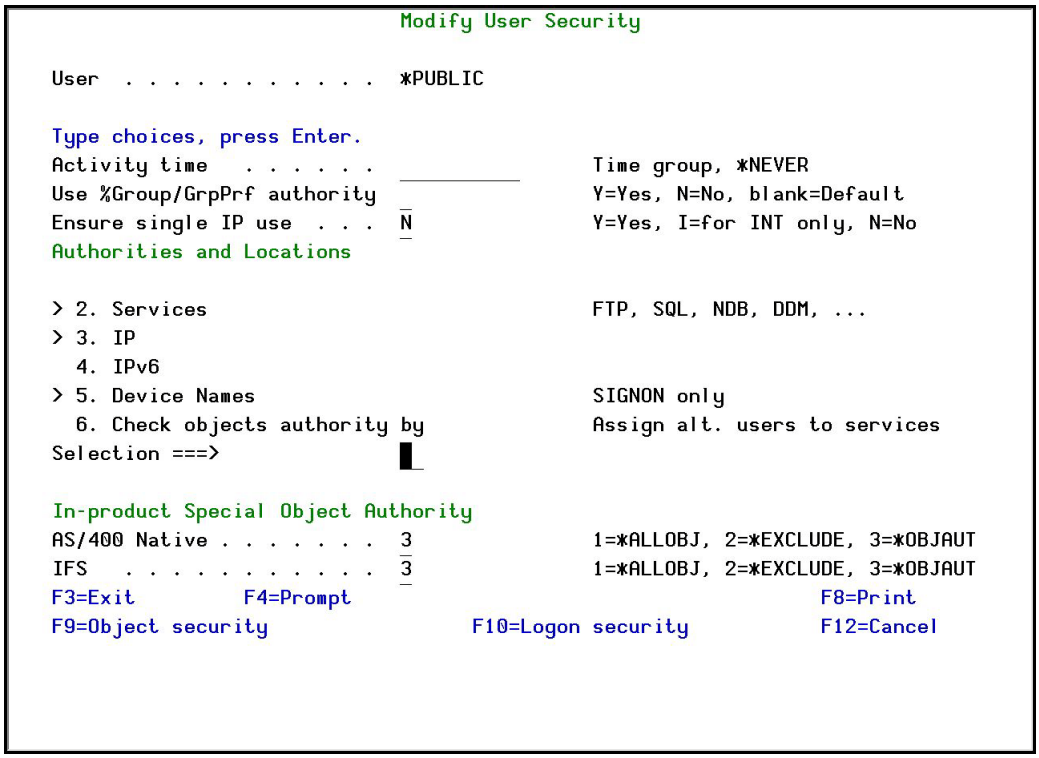


Figure 8-2. Modify User Security Screen

Field	
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** = The user cannot connect at any time.
Use %Group/GrpPrf Authorities	**Y** = use a specific group authorities **N** = don't use any specific group authorities
Ensure single IP use	Ensure that users can only access the system through a single IP address. Within that address, the user can access as many sessions as required. **Y** = Yes **I** = Interactive jobs only **N** = No If the user is a group profile, this parameter refers to all users in the group.

Field	
Authorities and Locations	**1. By %Groups** = specify authorities based on groups **2. Services** = specify authorities and location by Services name **3. IP** = specify authorities and location by IP address **4. IPv6** = specify authorities and location by IPv6 address **5. Device Names** = specify authorities and location by Device name **6 Check objects authority by** = specify different object authorities to be checked based upon the exit point being used. This user does not necessarily have to exist in the operating system. See Work with Alternative Users on page 98 for an explanation of this option. > Precedes every item that has already been defined
In-product Special Object Authority	Use this field to define object authority for the user/group for AS/400 Native and IFS objects. **1=*ALLOBJ** = All objects **2=*EXCLUDE** = Exclude from **3=*OBJAUT** = Object Authorities

Options	
1=Select	Modify an existing rule.
3=Copy	Copy this rule for another user/group
4=Delete	Delete an existing rule.
5=Members	Modify group members.
6=Groups	Show the association between the user and group profiles.

Function Keys	
F6=Add new	Create a rule for a new User
F7=Add group	Create a rule for a new Group
F8=Print list	Print user-to-service security rules

See Defining and Modifying Application Groups on page 47 and Defining and Modifying Location Groups on page 49.

Working with Client-Application Security

The capacity to secure client applications exists in the Client-Application Security module in **STRFW > 18**.

To work with client-application security:

1. Select **18. Client-Application Security** from the main menu. The **Work with Client-Application Security** screen appears.

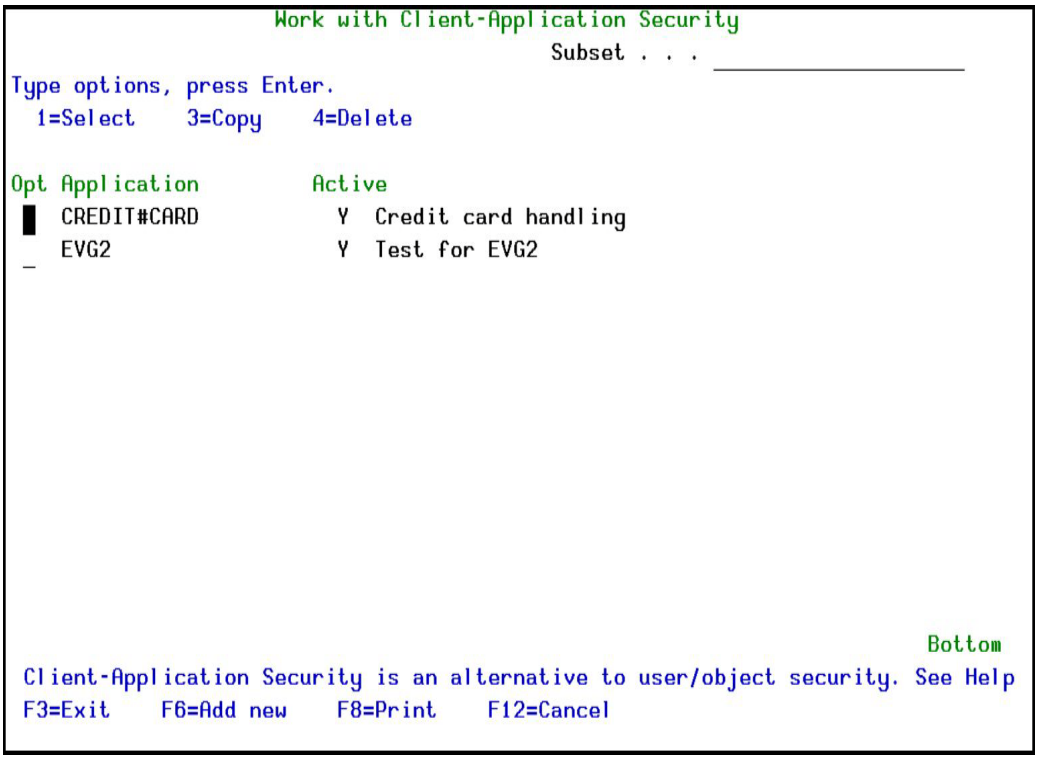


Figure 8-3. Work with Client-Application Security Screen

Options	
1=Select	Modify an existing rule.
3=Copy	Copy this rule for another user/group
4=Delete	Delete an existing rule.

Function Keys	Description
F6=Add new	Create a rule for a new User.
F8=Print	Print the list of client-application rules

2. Select **F6=Add New**. The **Add Client-Application Security** screen appears.

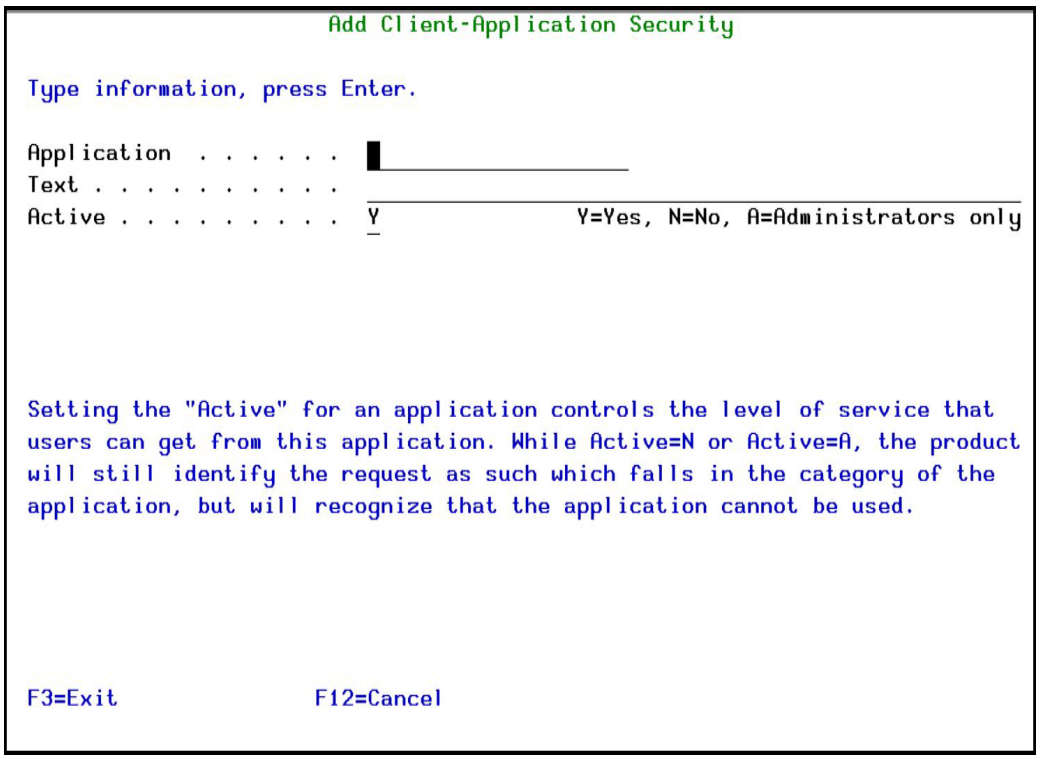


Figure 8-4. Add Client-Application Security Screen

Options	
Application	Type the Application name
Text	Type the Application description
Active	Select from the following options: **Y=Yes** **N=No** **A=Administrators only**

3. Press **Enter**. The General Features screen appears.

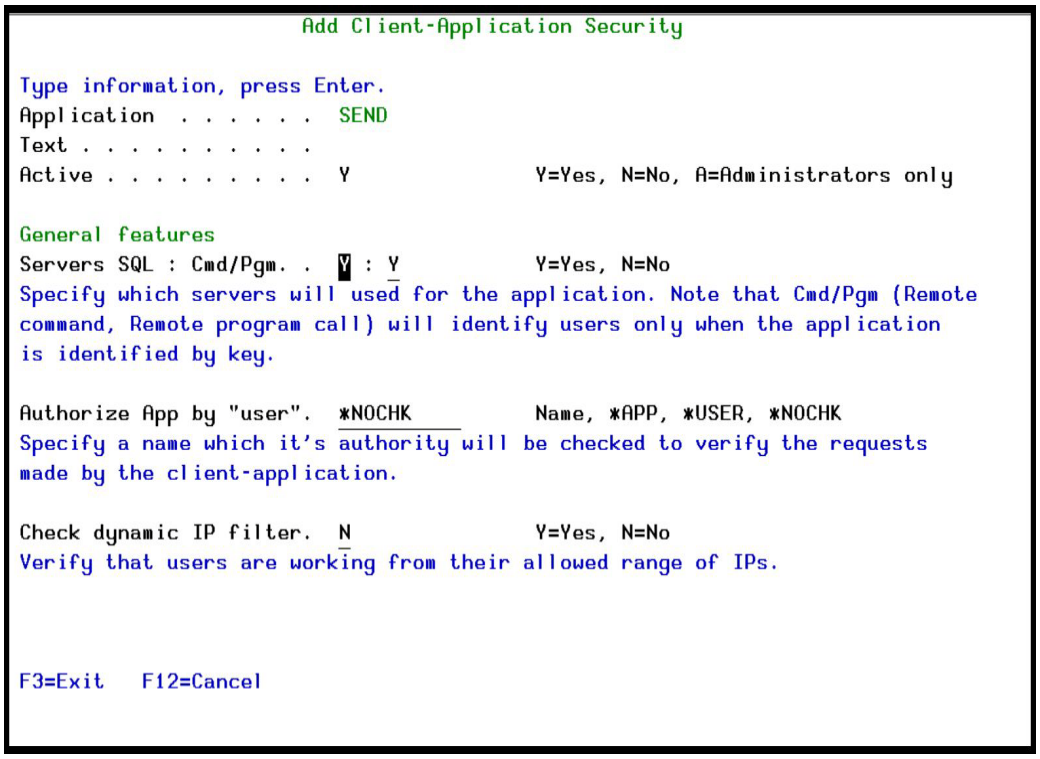


Figure 8-5. Add Client-Application Security Screen

Options	
Servers SQL : Cmd/Pgm	**Y**=Yes, **N**=No
Authorize App by "user"	**Name** = check by name of authorized user application ***APP** = check any authorized application ***USER** = check any authorized user ***NOCHK** = no check
Check dynamic IP filter	**Y**=Yes, **N**=No

4. Press **Enter**. The Identification features screen appears.

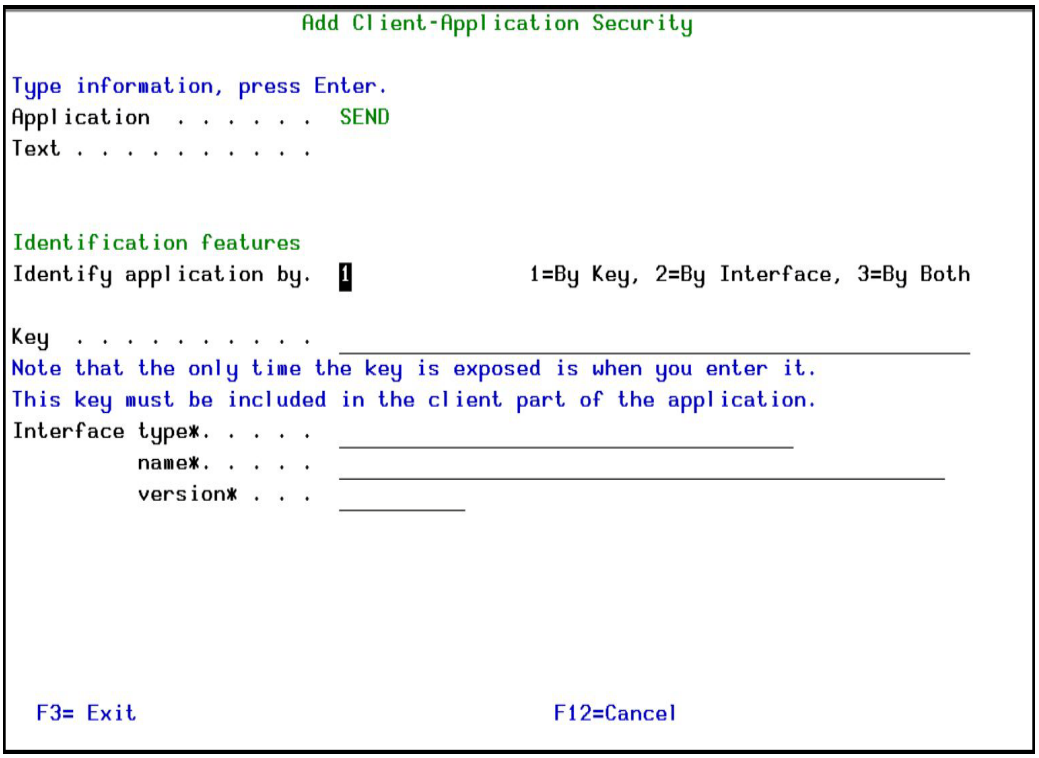


Figure 8-6. Add Client-Application Security Screen

Options	
1=By Key	Type in a Key to use as identification
2=By Interface	Selecting Interface will require the following credentials: type*... name*... version*...
3=By Both	Integrated identification means which include both Key and Interface credentials

5. Press **Enter**. The Group selection screen appears.

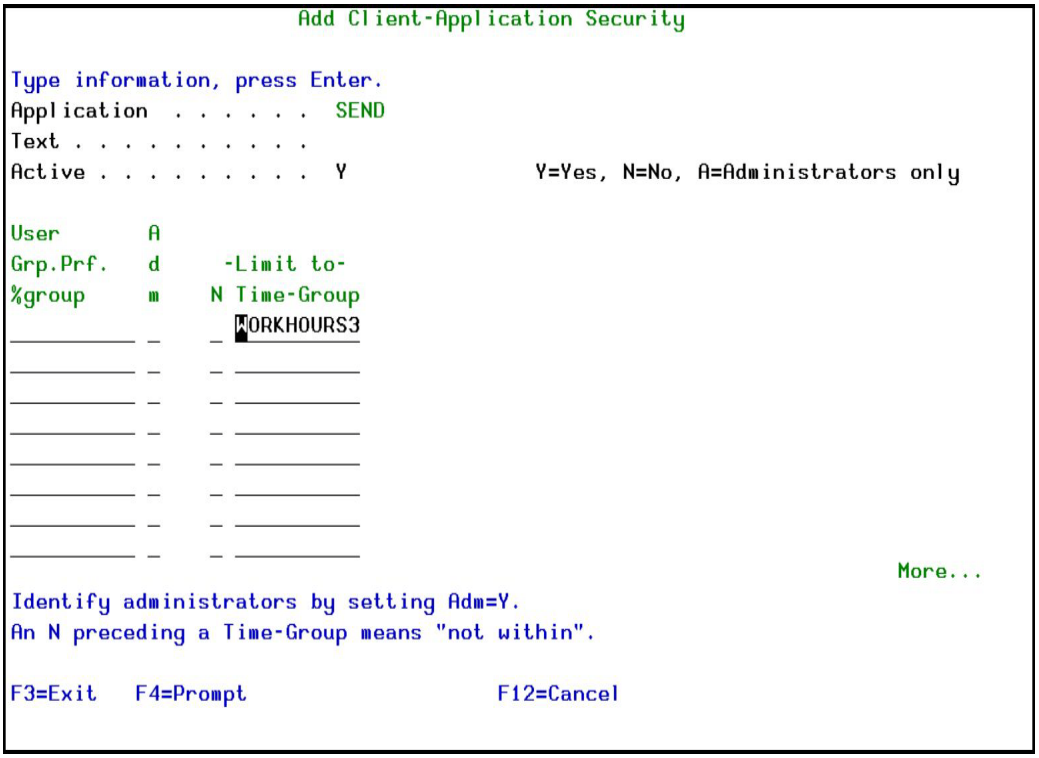


Figure 8-7. Add Client-Application Security Screen

Options	
User Grp. Prf. %group	Select user group preference - Raz-Lee groups
-Limit to- Time-Group	Limit the group to a specific time period. Selecting 'N' means 'not within'.

9

Object Security

Object security controls access to objects originating from specific external sources such as FTP, ODBC, and so on. 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, run, and so on, on protected objects. The Firewall log contains messages output by application of these rules. See the Queries, Reports and Logs chapter for a description of how to display the logs.

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.

NOTE: In Object Security when implementing i5/OS native object security, a user with no authority to reach an object will not be able to do so even if a Firewall rule enables it.
Despite this, users can implement Firewall to tighten objects security and reject allows by i5/OS native object security users (for example, user A is allowed to LIB/*ALL in i5/OS native object security; however, Firewall only allows LIB/A).

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. Native Objects** 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.
   - Select **1** for files.
   - Select **2** for libraries.
   - Select **3** for data queues.
   - Select **4** print files.
   - Select **5** for programs.
   - Select **6** for commands.
   - 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 IBM i objects.

Open the **Native [AS/400] Object Security** menu by selecting **21. Native Objects** from the main menu.

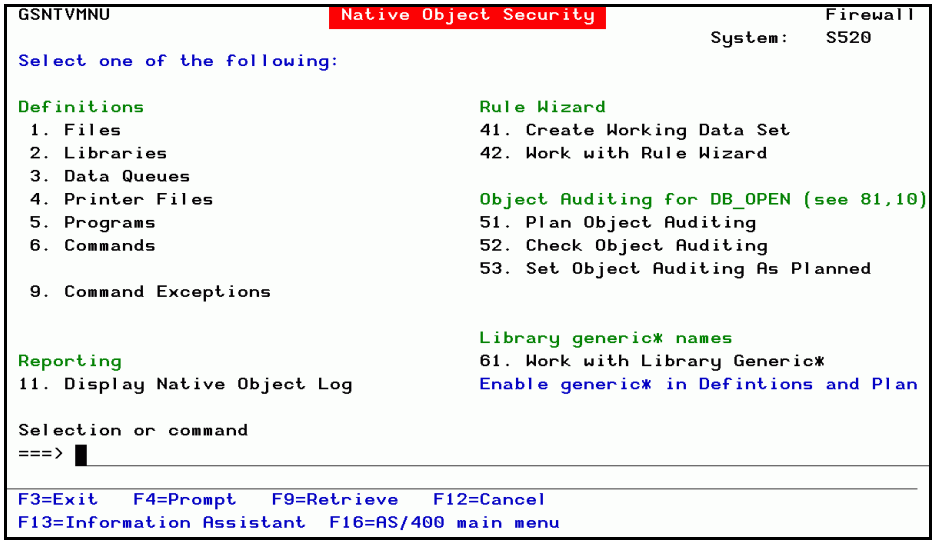


Figure 9-1. Native Object Security Screen

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

Files

1. In the **Native 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.
2. Type **1** to modify an existing rule or press **F6** to create a new rule.

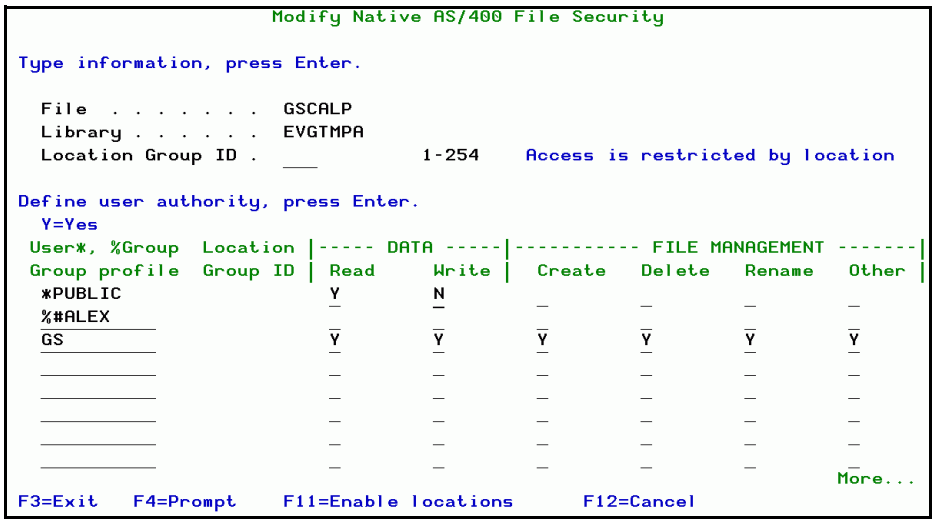


Figure 9-2. Modify Native AS/400 File Security Screen

Field	
File / Library	File name and library path of the file(s) included in this rule.
User, Group	Enter user profile or press F4 to select a user profile or group name from a list.
Location Group ID	To restrict by a specific location for each user, clear this parameter, press **F11**=Enable Locations, then, in the field which opens next to each user, specify the location for each user that is allowed to issue activity for the specified objects.
Read	**Y** = Users may read the specified file
Write	**Y** = Users may write, edit or update the specified file
Create	**Y** = Users may create a new file
Delete	**Y** = Users may delete the specified file
Rename	**Y** = Users may rename the specified file
Other	**Y** = Users may perform other actions on the specified file.

Function Keys	
F4=Prompt	When available, opens a prompt screen to select 1 or more definitions.

3. Edit the File Security settings. Then press **Enter** to return to the **Native OS/400 Object Security** menu.

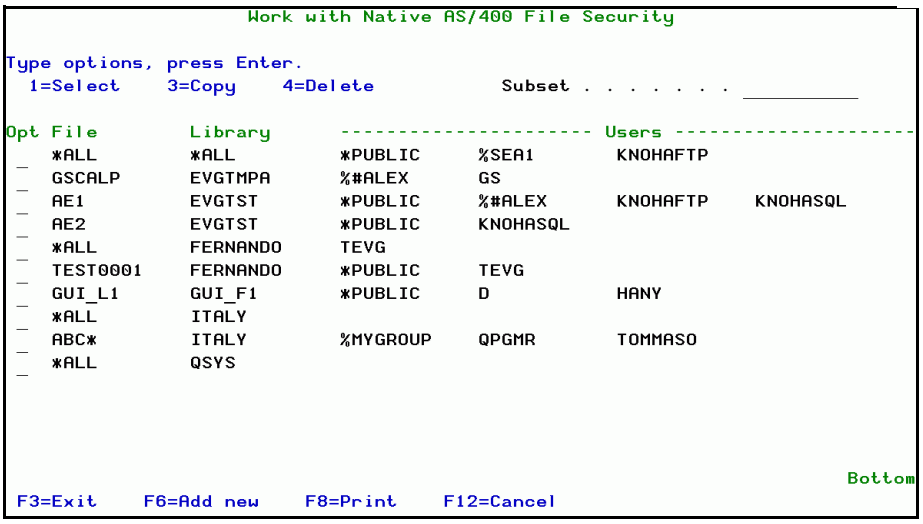


Figure 9-3. Work with Native AS/400 File Security Screen

Field	
Subset	Search a file or library whose names contain the subset.

Options	
1=Select	Modify this rule.
3=Copy	Copy this rule for another user.
4=Delete	Delete this rule.

Function Keys	
F6=Add new	Add new rule
F8=Print	Print rules

Add/Modify Native AS/400 File Security

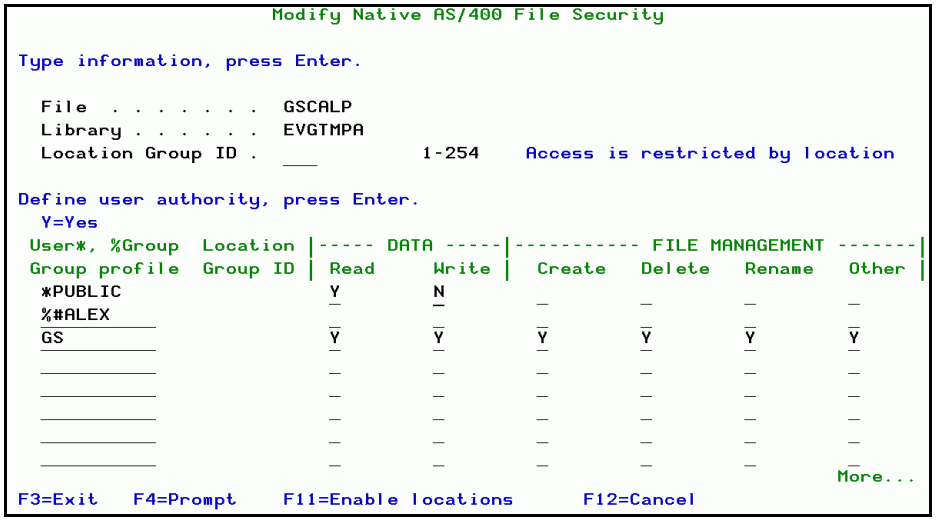


Figure 9-4. Modify Native AS/400 File Security Screen

Field	
File / Library	File name and library path of the file(s) included in this rule.
User, Group	Enter user profile or press F4 to select a user profile or group name from a list.
Location Group ID	To restrict by a specific location for each user, clear this parameter, press **F11**=Enable Locations, then, in the field which opens next to each user, specify the location for each user that is allowed to issue activity for the specified objects.
Read	**Y** = Users may read the specified file
Write	**Y** = Users may write, edit or update the specified file
Create	**Y** = Users may create a new file
Delete	**Y** = Users may delete the specified file
Rename	**Y** = Users may rename the specified file
Other	**Y** = Users may perform other actions on the specified file.

Function Keys	
F4=Prompt	Opens list to select 1 or more users/groups.

1. 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.
2. You can restrict access of all users or specific users by their location using the **Location Group ID**. If a location is specified at the top of the screen, all access to the objects will be restricted only for changes made from that location.
3. 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.

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

Create a Swap User Profile Rule

You can set up a rule that allows you use a different user profile than the current profile to determine access under specific conditions. The example below shows how to create a rule that when the User is JAVA2 and the Server is SQL, the access rules to be used are those of QPGMR.

For these rules to work, **Firewall** must be working in real mode, that is FYI is turned off, and Swap User must be allowed at abject level.

1. Create an NOS rule:
   a. Select **21. Native Objects** from the Main menu. The **Native Object Security** menu appears.
   b. Select **1. Files** from the **Native Object Security** menu. The **Work with Native AS/400 File Security** screen appears.

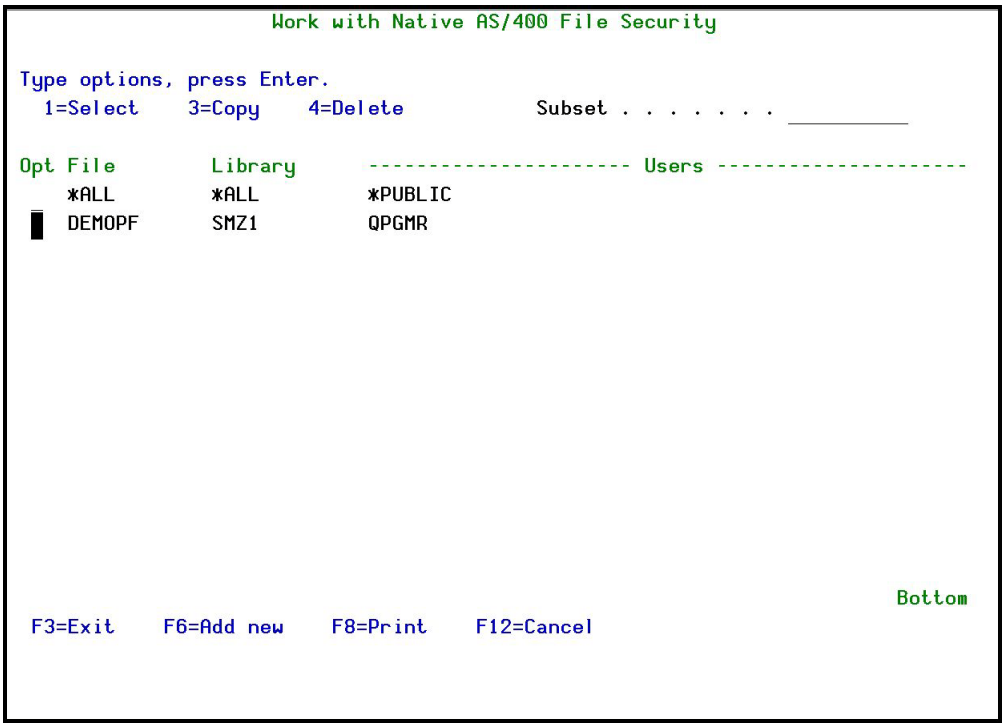


Figure 9-5. Work with Native AS/400 File Security

   c. Set **File *ALL**, **Library *ALL** to allow all users to use all files. Set file **DEMOPF** in library **SMZ1** to allow only QPGMR and reject all other users.

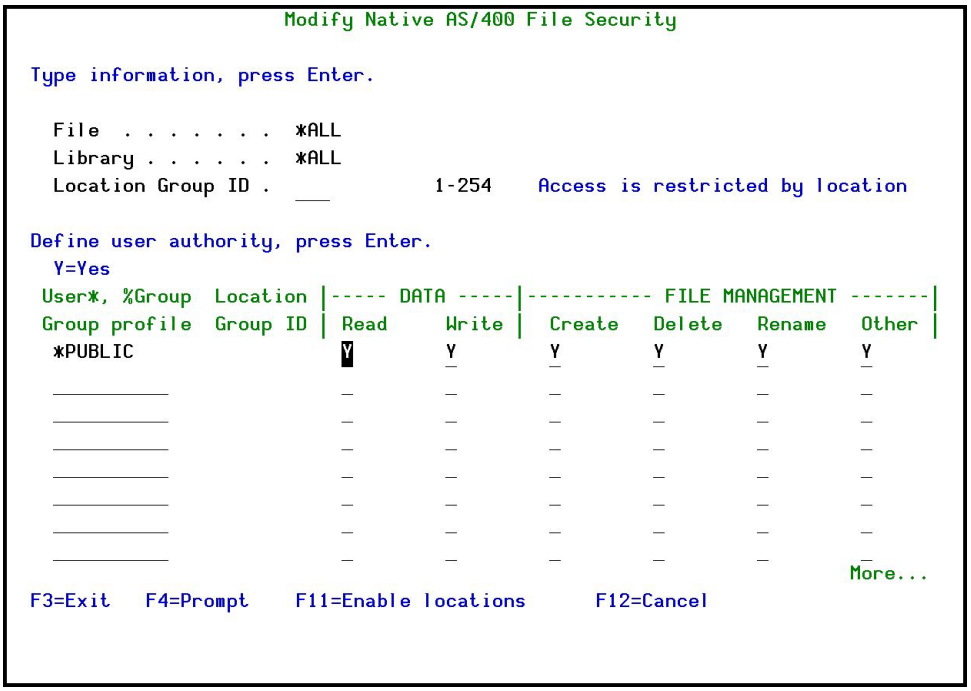


Figure 9-6. Modify Native AS/400 File Security

2. Create a user rule and a swap user profile.
   a. Select **11. Users and Groups** from the Main menu. The **Work with User Security** screen appears.

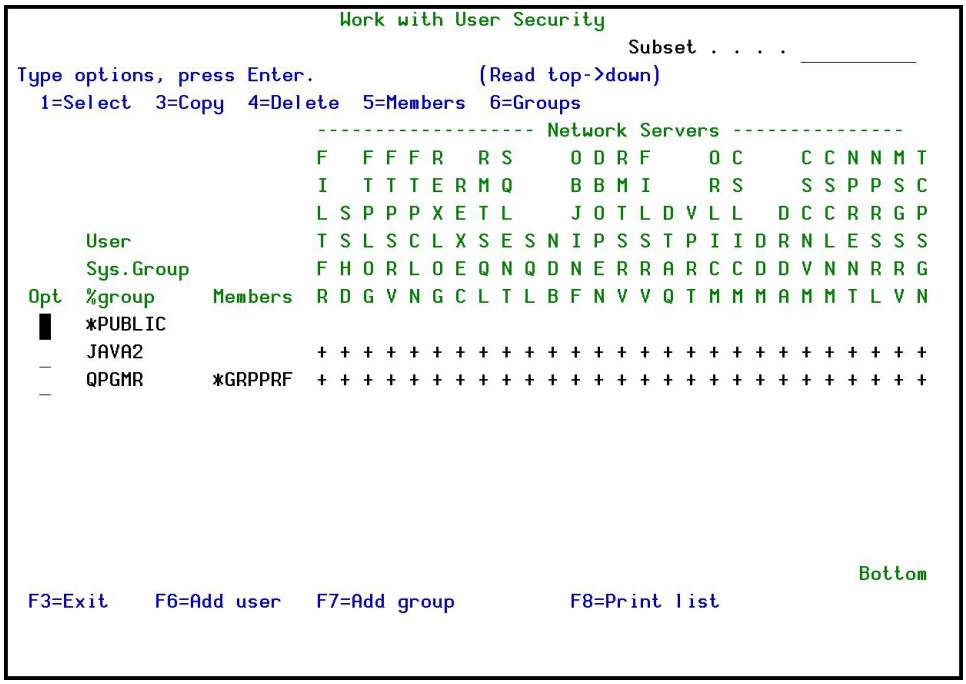


Figure 9-7. Work with User Security

   b. Select **JAVA2**. The **Modify User Security** screen appears.
   c. Select option **6 Check objects authority by**. The **Work with Alternative Users** screen appears.

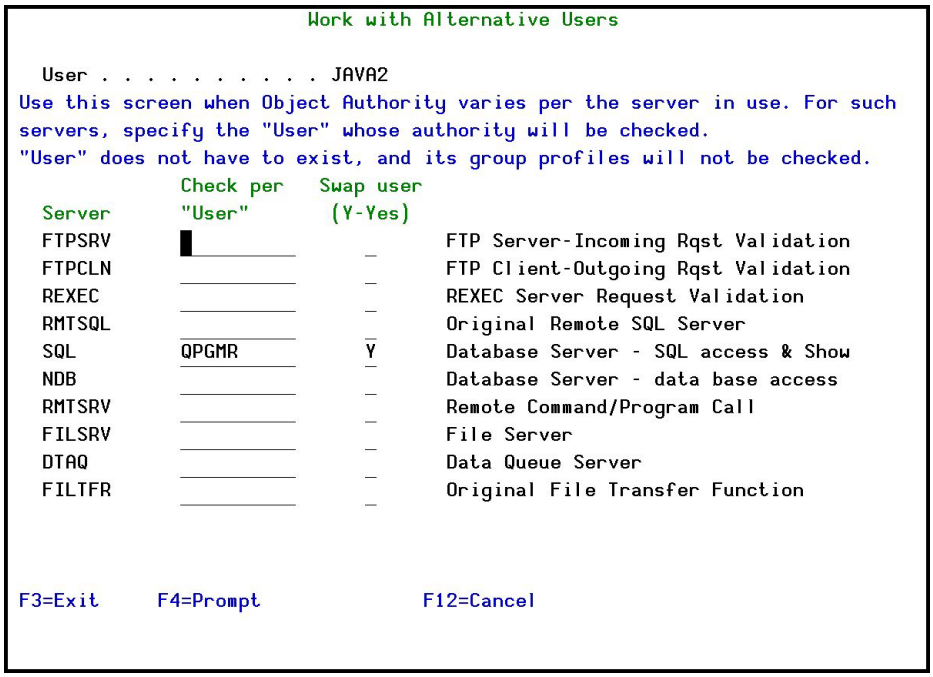


Figure 9-8. Work with Alternative Users

d. Set QPGMR as the alternative user for server SQL.

3. Set up FYI mode for all servers

a. Select **1. Activation and Server Setting** from the Main menu. The **Activation and Server Setting** menu appears.

b. Select **1. Work with Servers** from the **Activation and Server Setting** menu. The **Work with Server Security** screen appears.

c. Press **F22=Global setting**. The **Global Server Security Settings** screen appears. Ensure the settings are as shown below.

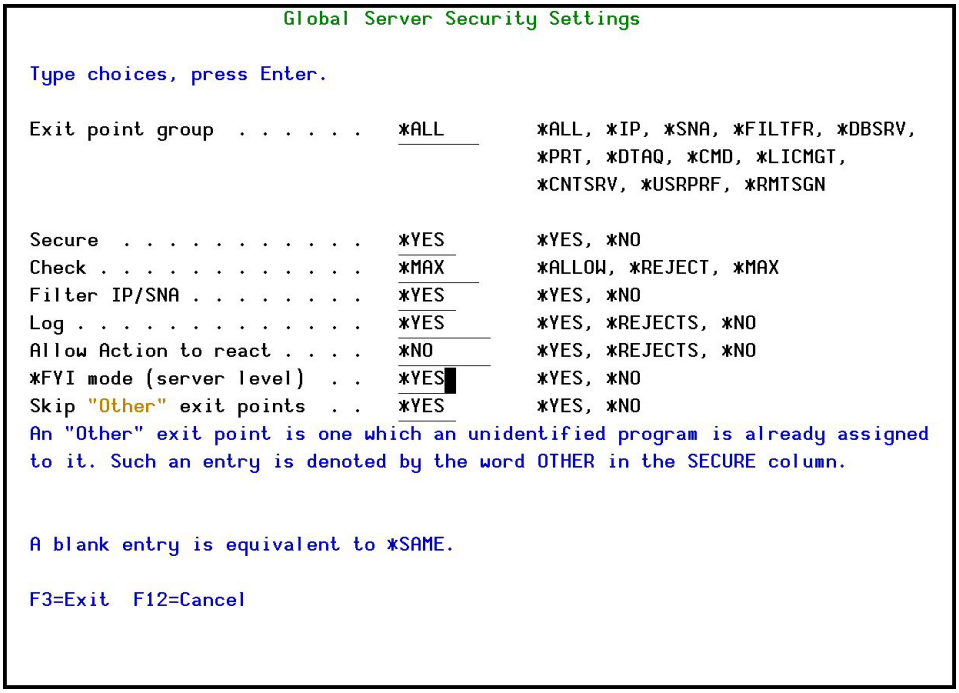


Figure 9-9. Global Server Security Settings

4. Ensure that the SQL server is set up to run in real mode.
   a. Select **1. Activation and Server Setting** from the Main menu. The **Activation and Server Setting** menu appears.
   b. Select **1. Work with Servers** from the **Activation and Server Setting** menu. The **Work with Server Security** screen appears.
   c. Select the **SQL** server. The **Modify Server Security** screen appears.

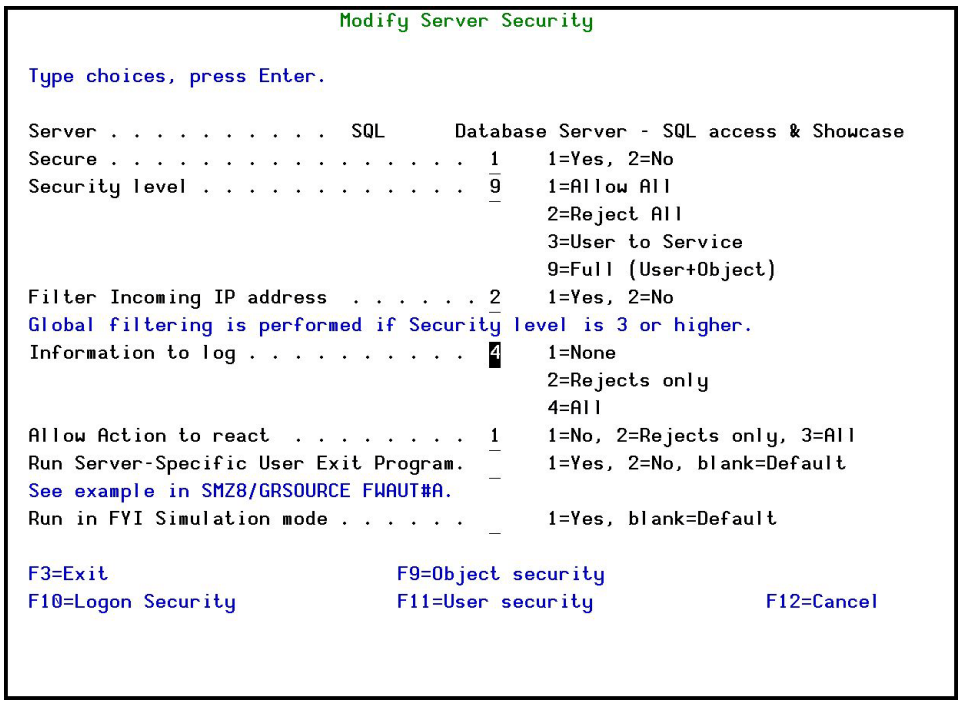


Figure 9-10. Modify Server Security

d. Ensure that **Run in FYI Simulation** mode is blank.

Your swap user profile rule is now ready.

Libraries

Add/Modify Native AS/400 Library Security

1. In 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.

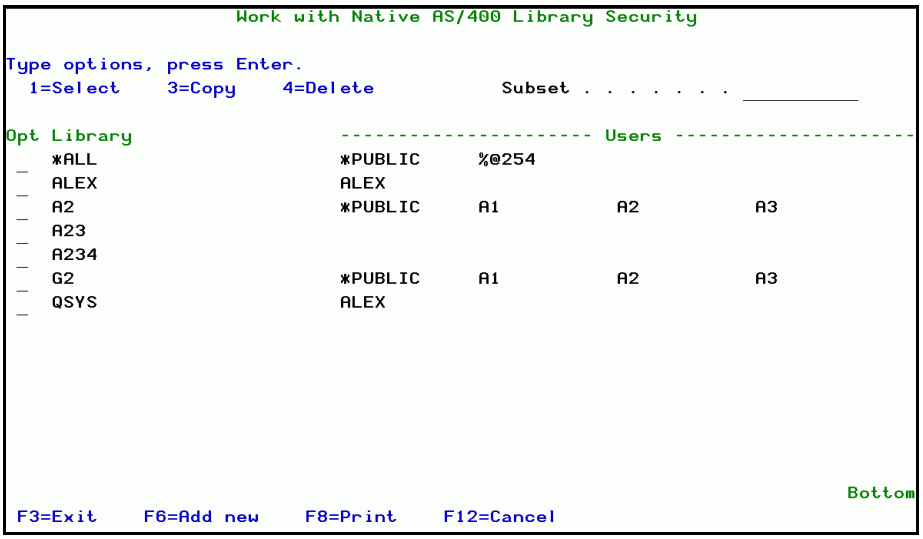


Figure 9-11. Work with Native AS/400 Library Security Screen

2. Type **1** to modify an existing rule or press **F6** to create a new rule.

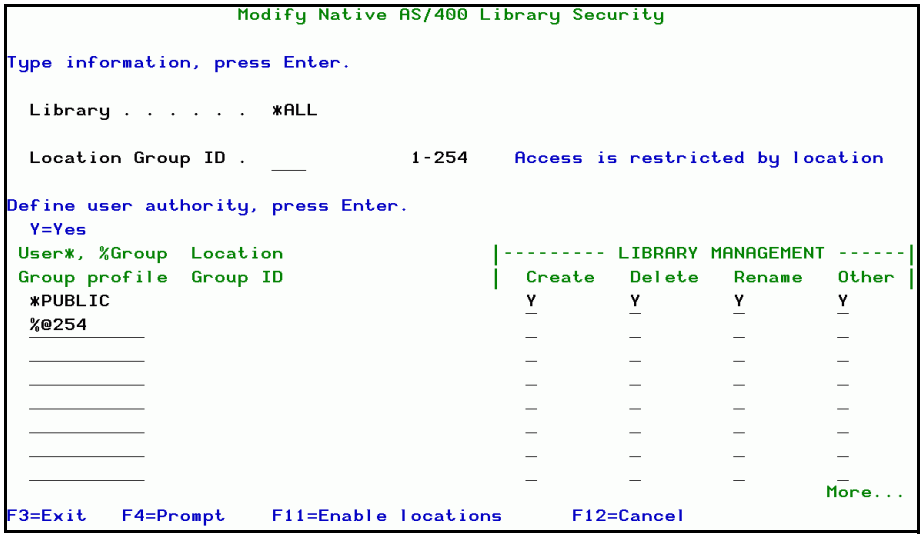


Figure 9-12. Modify Native Library Security Screen

Field	
Library	Shows the libraries covered by the rule.
Location Group ID	To restrict by a specific location for each user, clear this parameter, press **F11**=Enable Locations, then, in the field which opens next to each user, specify the location for each user that is allowed to issue activity for the specified objects.
Create	**Y** = Users may create a new file.
Delete	**Y** = Users may delete the specified file.
Rename	**Y** = Users may rename the specified file.
Other	**Y** = Users may perform other actions on the specified file.

Function Keys	
F4=Prompt	Opens list to select 1 or more users/groups.

3. Edit the Library Security settings:
   - 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.
   - You can restrict access of all users or specific users by their location using the Location Group ID. If a location is specified at the top of the screen, all access to the objects will be restricted only for changes made from that location.
   - 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.
4. When finished, press **Enter** to return to the **Native OS/400 Object Security** menu.

Data Queues

This screen lets you define permissions for one user profile, profile group or Firewall user group on each line.

Add/Modify Object Data Queue Security

1. In 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.

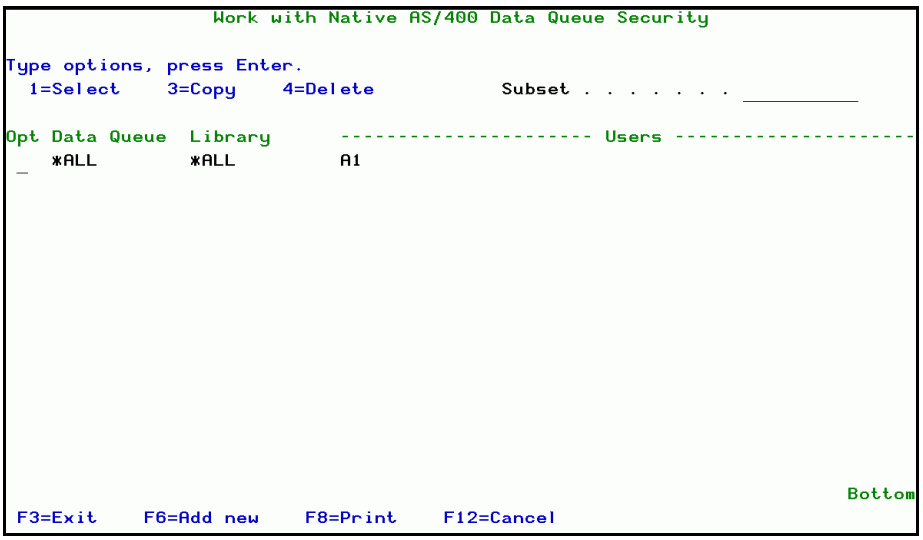


Figure 9-13. Work with Native AS/400 Data Queue Security Screen

Field	
Subset	Search a data queue or library whose names contain the subset.

Options	
1=Select	Modify this rule.
3=Copy	Copy this rule for another user.
4=Delete	Delete this rule.

Function Keys	
F6=Add new	Add new rule.
F8=Print	Print rules.

2. Type **1** to modify an existing rule or press **F6** to create a new rule.
3. Edit the Data Queue Security settings:
   - 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.
   - You can restrict access of all users or specific users by their location using the Location Group ID. If a location is specified at the top of the screen, all access to the objects will be restricted only for changes made from that location.
   - 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.

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

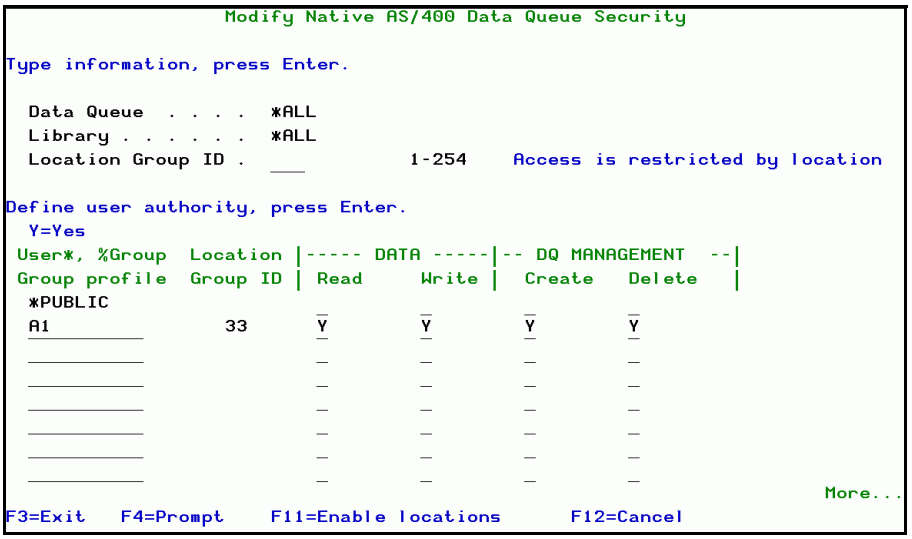


Figure 9-14. Modify Native AS/400 Data Queue Security Screen

Field	
Data Queue	Shows the data queue(s) included in this rule.
Library	Shows the libraries covered by the rule.
User, Group	Enter user profile or press **F4** to select a user profile or group name from a list.
Location Group ID	To restrict by a specific location for each user, clear this parameter, press **F11**=Enable Locations, then, in the field which opens next to each user, specify the location for each user that is allowed to issue activity for the specified objects.
Read	**Y** = Users may read the specified file.
Write	**Y** = Users may write, edit or update the specified file.
Create	**Y** = Users may create a new file.
Delete	**Y** = Users may delete the specified file.

Function Keys	
F4=Prompt	Opens list to select 1 or more users/groups.

Printer Files

Use this screen to Define permissions for one user profile, profile group or Firewall user group.

Add/Modify Print File Security

1. In 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.

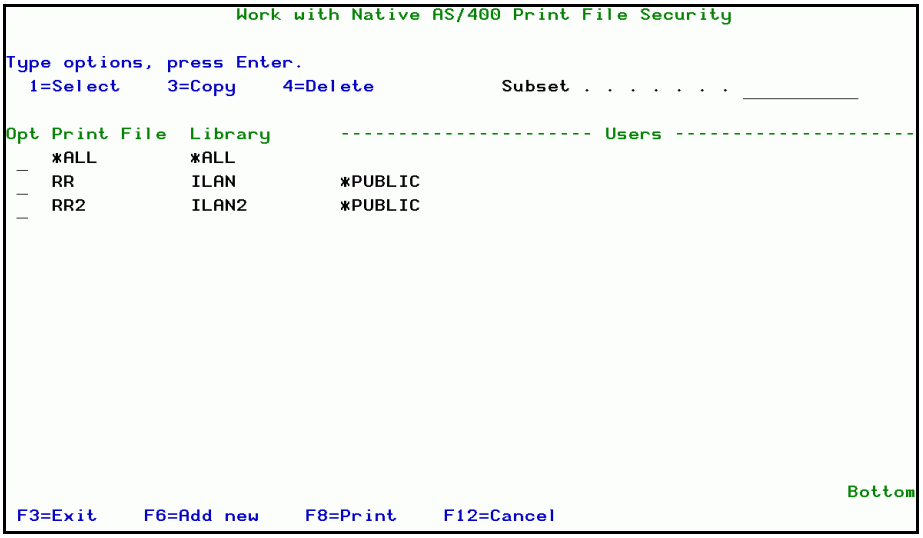


Figure 9-15. Work with Native AS/400 Print File Security Screen

2. Type **1** to modify an existing rule or press **F6** to create a new rule.
3. Edit the Data Queue Security settings:
   - 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.
   - You can restrict access of all users or specific users by their location using the Location Group ID. If a location is specified at the top of the screen, all access to the objects will be restricted only for changes made from that location.
   - 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.

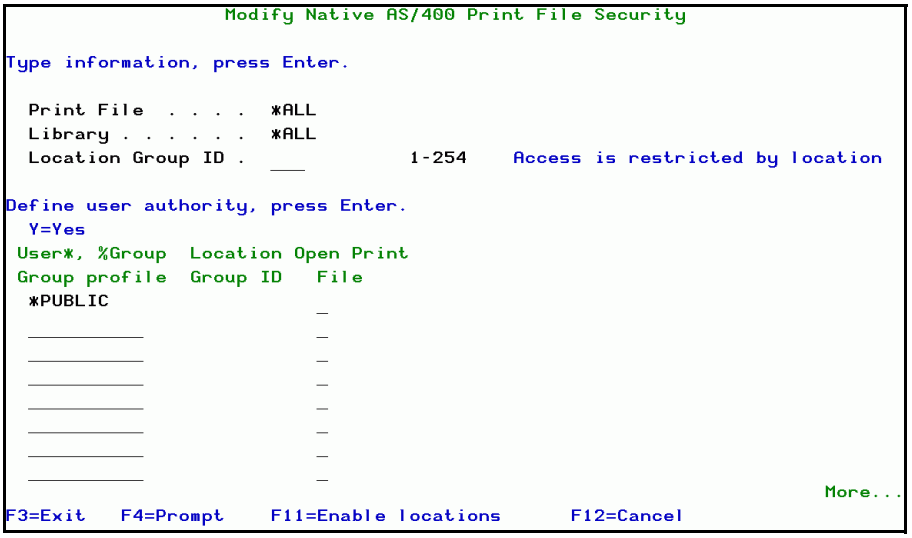


Figure 9-16. Modify Native AS/400 Print File Security Screen

Parameter/Option	Description
Print File	Shows the print file(s) path included in this rule.
Library	Shows the libraries covered by the rule.
Location Group ID	To restrict by a specific location for each user, clear this parameter, press **F11**=Enable Locations, then, in the field which opens next to each user, specify the location for each user that is allowed to issue activity for the specified objects.
User, Groups	Enter user profile or press **F4** to select a user profile or group name from a list.
Open Print File	**'Y'** = Users may use the specified file

4. When finished press **Enter** to return to the **Native OS/400 Object Security** menu.

Programs

1. In 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.

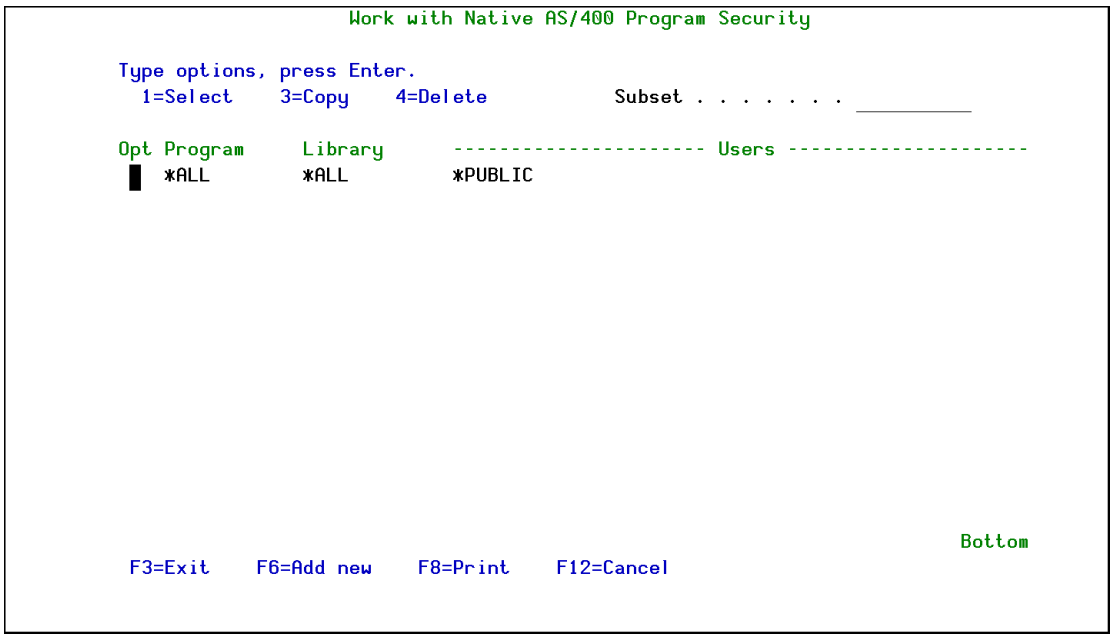


Figure 9-17. Work with Native AS/400 Program Security Screen

Field	
Opt	**1** = Select this rule for modification **3** = Copy this rule for another user **4** = Delete this rule
F6	Add new rule
F8	Print rules
Subset	Search only programs/libraries whose name contains the subset

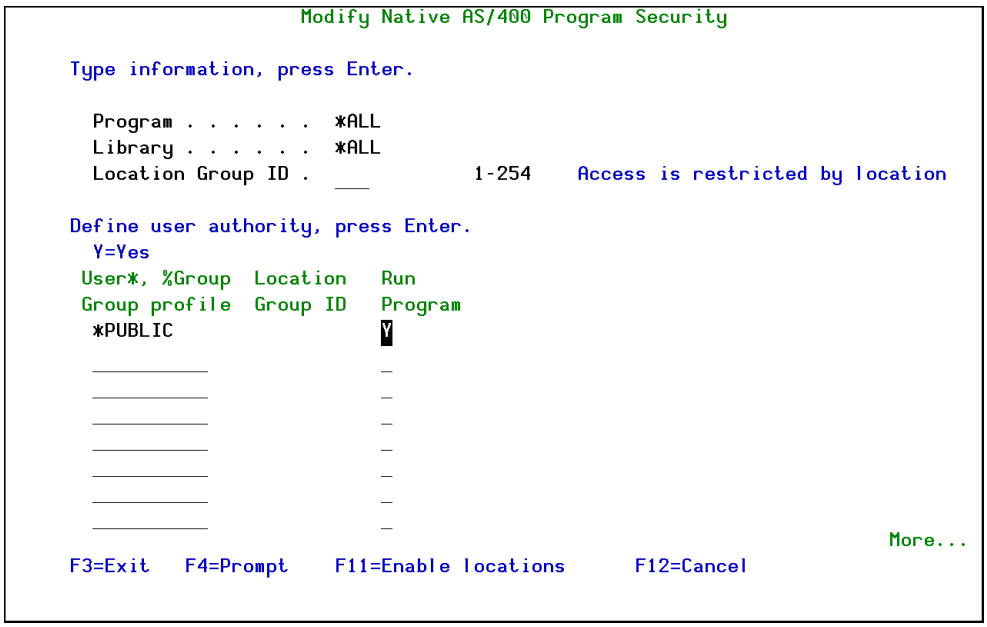


Figure 9-18. Add/Modify Native AS/400 Program Security Screen

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

You can restrict access of all users or specific users by their location using the Location Group ID. If a location is specified at the top of the screen, all access to the objects will be restricted only for changes made from that location.

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.

Field	
Program	Shows the program(s) included in this rule.
Library	Shows the libraries covered by the rule.
Location Group ID	To restrict by a specific location for each user, clear this parameter, press **F11**=Enable Locations, then, in the field which opens next to each user, specify the location for each user that is allowed to issue activity for the specified objects.
User, Group	Enter user profile or press **F4** to select a user profile or group name from a list.
Run Program	**Y** = Users may run the specified program

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

Commands

Firewall protects by the beginning of the command string. If you want more protection that analyzes commands and protects by every parameter value, origin of commands and so on, you should use the **Command** module.

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 work with an existing rule or press **F6** to create a new rule.
3. Press **Enter** to return to the **Native OS/400 Object Security** menu.

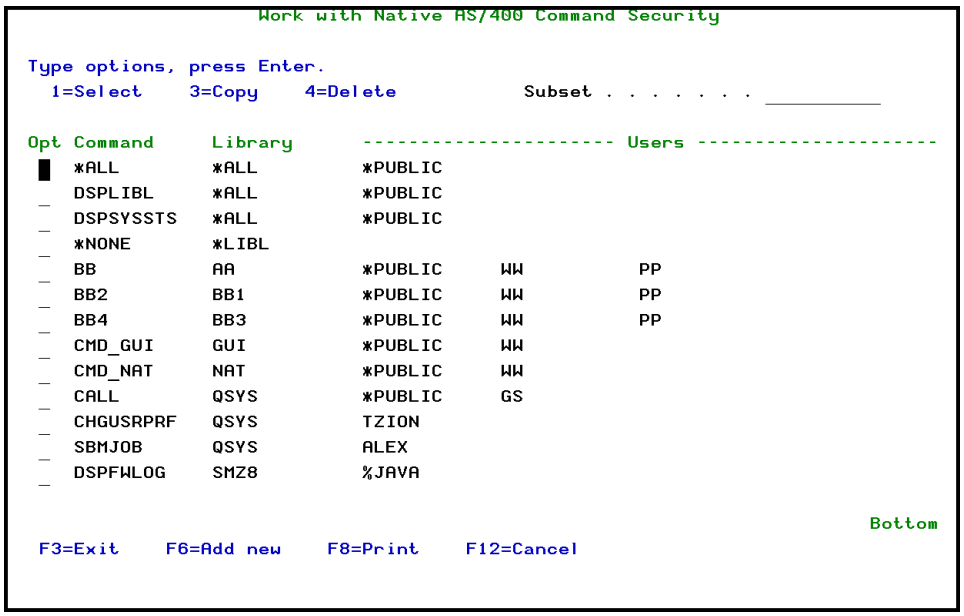


Figure 9-19. Work with Native AS/400 Command Security

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

Field	
Opt	**1** = Select this rule for modification **3** = Copy this rule for another user **4** = Delete this rule
F6	Add new rule
F8	Print rules
Subset	Search only commands whose name contains the subset

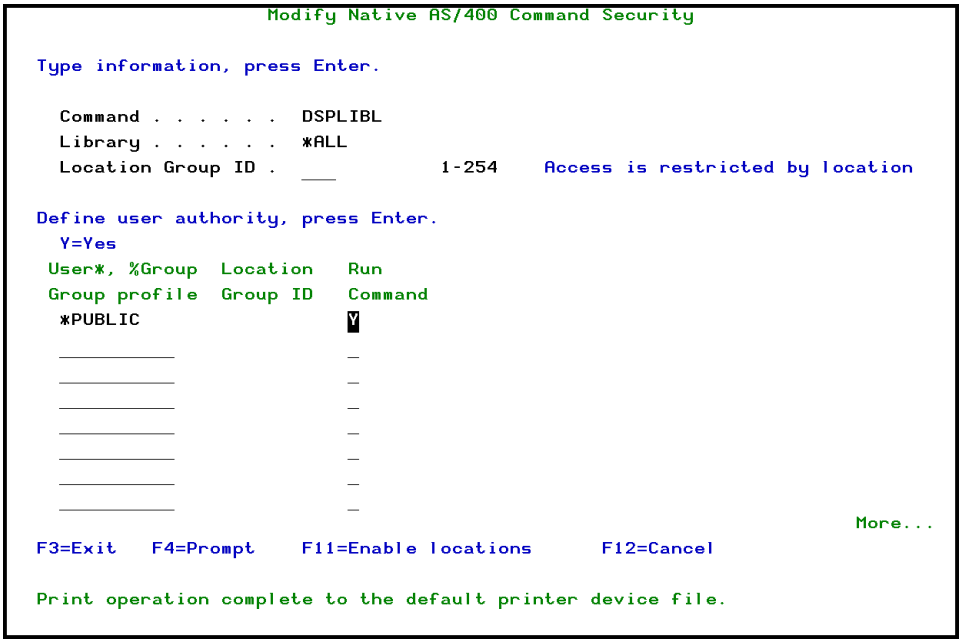


Figure 9-20. Modify Native AS/400 Command Screen

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.

You can restrict access of all users or specific users by their location using the Location Group ID. If a location is specified at the top of the screen, all access to the objects will be restricted only for changes made from that location.

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 ordinary users to access objects.

Field	
Command	Shows the command(s) included in this rule.
Library	Shows the libraries covered by the rule.
Location Group ID	To restrict by a specific location for each user, clear this parameter, press **F11**=Enable Locations, then, in the field which opens next to each user, specify the location for each user that is allowed to issue activity for the specified objects.
User, Group	Enter user profile or press **F4** to select a user profile or group name from a list.
Run Command	**Y** = Users may run the specified program

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.

You 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. This screen lists all the rules currently in effect.
3. Type **1=Select** to work with an existing rule or press **F6** to create a new rule.

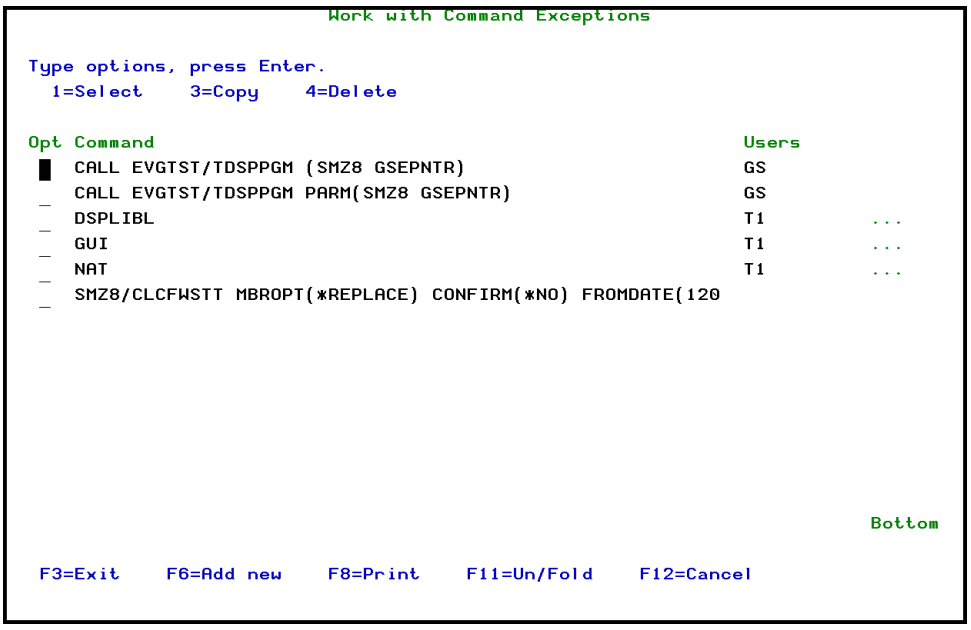


Figure 9-21. Work with Command Exceptions Screen

Field	
Opt	**1** = Select this rule for modification **3** = Copy this rule for another user **4** = Delete this rule
F6	Add new rule
F8	Print rules

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

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.

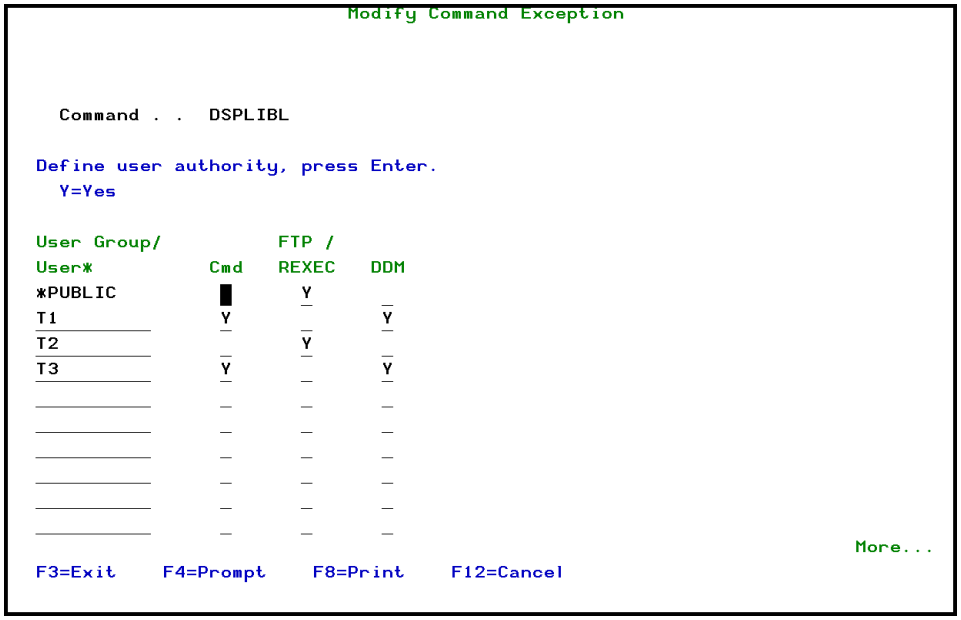


Figure 9-22. Modify Command Exception Screen

Field	
Command/Library	Name and library path of the command(s) included in this rule. You can include many commands by simply entering the generic beginning of the command. For example, to create a rule for the **CHGUSRAUD**, **CHGUSRPRF**, **CHGUSRPRTI**, and **CHGUSRTRC** commands, simply enter **CHGUSR**.
User/User Groups	Enter user profile or press **F4** to select a user profile or group name from a list.
Cmd	'**Y**' = Users may execute OS/400 commands
FTP/REXEC	'**Y**' = Users may execute commands via FTP or REXEC
DDM	'**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

If you have many libraries that require the same set of permissions and authorities, you can create a single library of authorization rules to be applied to a list of libraries.

1. Select **61. Work with Library Generic*** from the **Native AS/400 Object Security** menu. The **Work with Policy (generic*) Libraries** screen appears. This screen lists all the rules currently in effect.

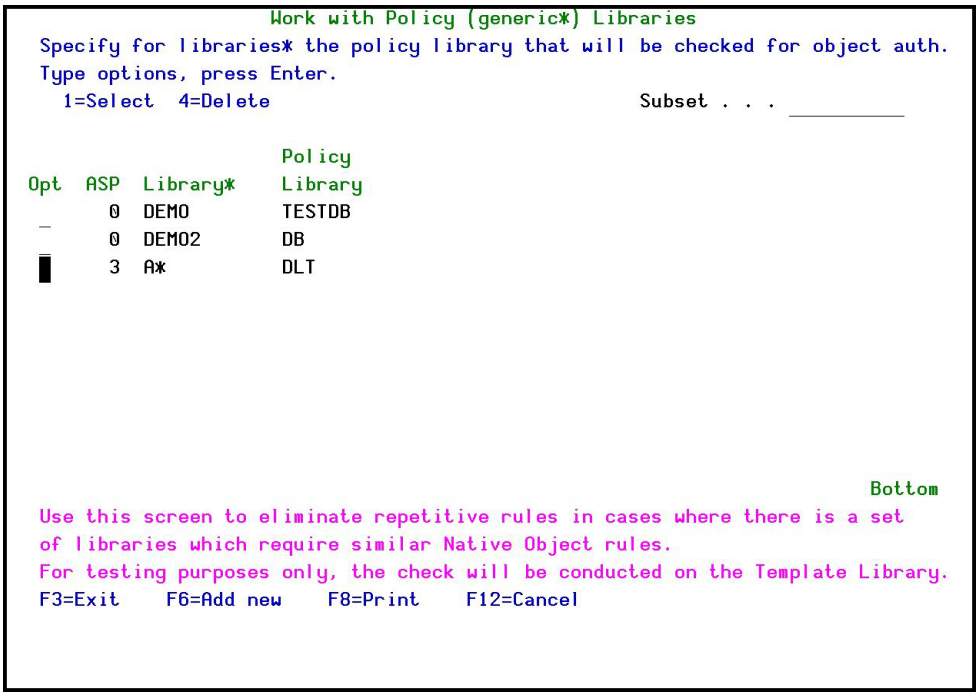


Figure 9-23. Work with Policy (generic*) Libraries

2. Type **1=Select** to work with an existing rule or press **F6** to create a new rule. The **Add Policy Library** screen appears.

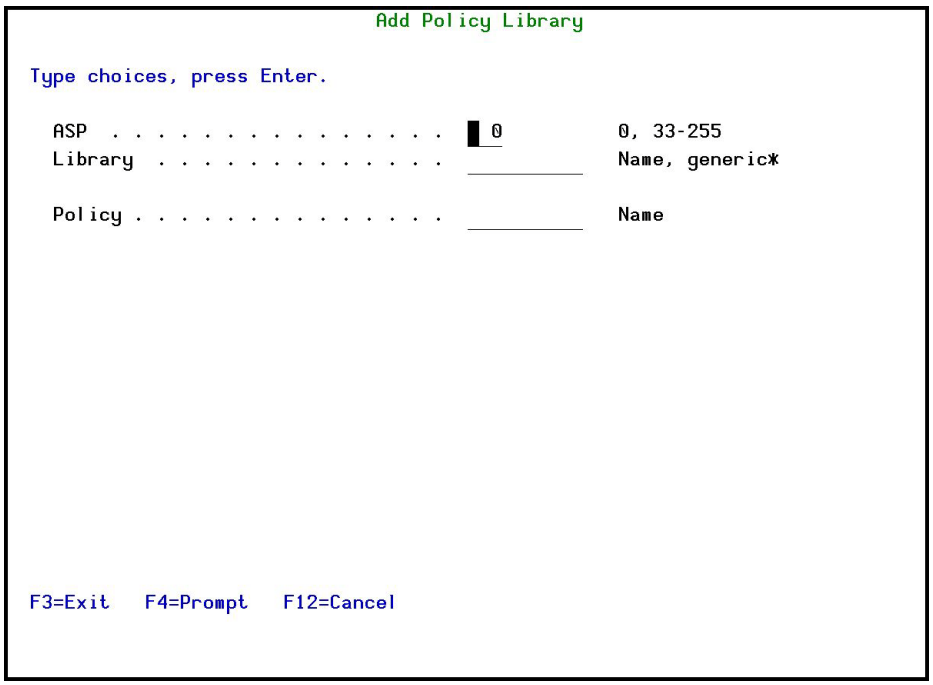


Figure 9-24. Add Policy Library Screen

3. If you are using auxiliary storage, enter the **ASP** number.
4. Enter the Library that contains the objects to which you wish to apply the authorization rules. You can also define a set of libraries by using a wild card. For example, type **ABC*** to apply the policy to all libraries whose name begins with **ABC**.
5. Enter the Policy that is the Library that contains those rules.

In the specific object screens (options 1-9, described above), define the original rules to be applied through the Policy Library.

IFS Objects

To work with IFS Object Security:

1. Select **22**. **IFS** from the main menu. The **IFS Security** menu appears.
2. Select **1. IFS Object Usage** from the **IFS Security** menu. The **Work with IFS Security** screen appears.

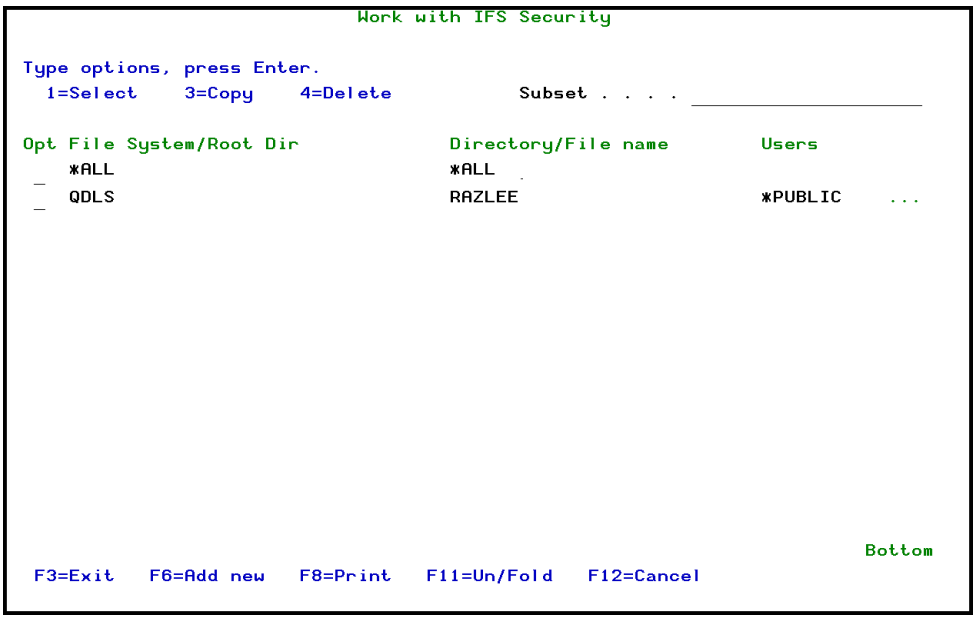


Figure 9-25. Work with IFS Security Screen

Field	
Opt	**1** = Select this rule for modification **3** = Copy this rule for another user **4** = Delete this rule
F6	Add new rule
F8	Print rules
Subset	Search only files/directories whose name contains the subset

Add/Modify IFS Security

1. Type **1** to work with an existing rule or press **F6** to create a new rule from the **Work with IFS Security** screen.

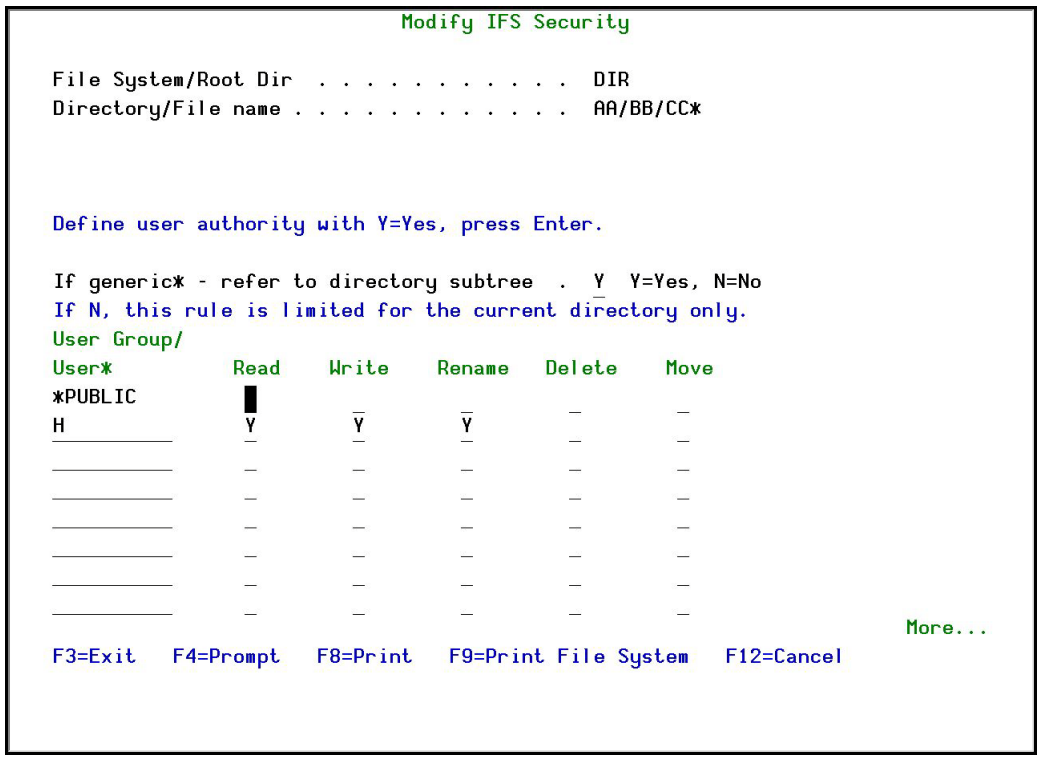


Figure 9-26. Modify IFS Security Screen

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. You should always make

certain that the ***Public** rule contains sufficient permissions to allow access to objects by ordinary users.

Field	
File System	Shows the IFS file system to which this rule apples
Directory/File	Shows the file name(s) and directory path(s) included in this rule
If generic* - refer to directory subtree	**Y** = Yes **N** = No This parameter depends on how you set the **Inherit In-product IFS authorities** parameter in the **Firewall Additional Settings** screen. See Additional Settings on page 194 for more details. See below for an example of how the two parameters work together.
User/User Group	Enter user profile or press **F4** to select a user profile from list.
Read	**Y** = Users may read the specified file
Write	**Y** = Users may write, edit or update the specified file
Delete	**Y** = Users may delete the specified file
Rename	**Y** = Users may rename the specified file
Other	**Y** = Users may perform other actions on the specified file.

2. Enter your required parameters and press **Enter** to return to the **Work with IFS Object Security** screen.

IFS Object Security Example

This example discusses how to use the IFS security parameters in conjunction with the **Inherit In-product IFS authorities** parameter in the **Firewall Additional Settings** screen. For this example, assume a file system called **TEST** which has two directories **AA** and **BB**. In each directory, there are three sub-directories: **AAA**, **BBB**, and **CCC**. This structure can be seen visually below.

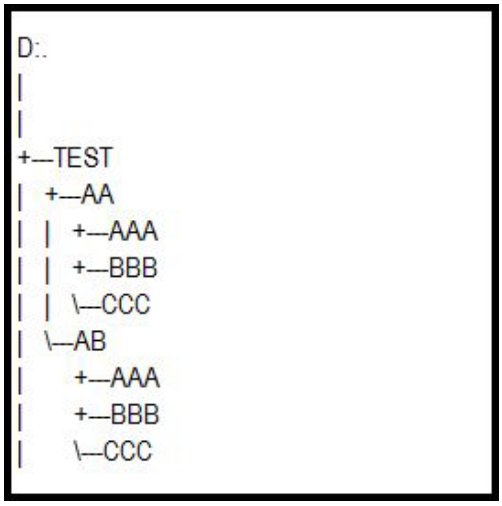


Figure 9-27. Modify IFS Security Screen

Example 1: the **Inherit In-product IFS authorities** parameter is set to **1**

- To limit authority to **TEST/AA**, set the following:
  - **File System/Root Dir** = TEST
  - **Directory/File Name** = AA/*
  - **If generic* - refer to directory subtree** = N

  The rules set for **TEST/AA/*** apply only to **TEST/AA**. They do not apply to **TEST/AA/AAA**, **TEST/AA/BBB**, **TEST/AA/CCC**, or to **TEST/AB** and its sub-directories.

- To limit authority to **TEST/AA** and **TEST/AB**, set the following:
  - **File System/Root Dir** = TEST
  - **Directory/File Name** = A*
  - **If generic* - refer to directory subtree** = N

  The rules set for TEST/A* apply only to **TEST/AA** and **TEST/AB**. They do not apply to **TEST/AA/AAA**, **TEST/AA/BBB**, **TEST/AA/CCC**, **TEST/AB/AAA**, **TEST/AB/BBB**, or **TEST/AB/CCC**.

- To not limit authority to **TEST/AA**, set the following:
  - **File System/Root Dir** = TEST
  - **Directory/File Name** = AA/*
  - **If generic* - refer to directory subtree** = Y

  The rules set for **TEST/AA/*** apply to **TEST/AA**, **TEST/AA/AAA**, **TEST/AA/BBB**, and **TEST/AA/CCC**.

- To not limit authority to **TEST/AA** and **TEST/AB**, set the following:
  - **File System/Root Dir** = TEST
  - **Directory/File Name** = A*
  - **If generic* - refer to directory subtree** = Y

  The rules set for **TEST/A*** apply to all possible paths from **TEST/A***.

Additional Control

The Additional Control section of the Firewall allows you to create Logon security rules that 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 and outgoing FTP requests
- REXEC (Remote Command Execution)
- Telnet
- 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 the Getting Started chapter 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.

1. In the Firewall Main menu, select one of the following secure communication protocols:

Select	For
31	FTP/REXEC
32	Telnet
34	Passthrough
35	DDM, DRDA, SSH, Port...(see Advanced Security Features on page 179)

2. Menus 31, 32, 34 follow the same principle. Each menu contains a Definitions and a Reporting section. Select the Definition or Report option to use and press **Enter**.

For Example:

- In the **FTP/REXEC Logon Security** menu, choose **1** for Incoming FTP, and **5** 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.

3. Choose the desired reporting (logs) option by selecting options **11** (and optionally **12, 13** and **15**) for display logs.
4. Press **Enter** to confirm and return to the main menu.

The basic options for screens are described in the table below.

Options	
1=Select	Select this rule for modification
3=Copy	Copy this rule for another user
4=Delete	Delete this rule
5=IP Range	Explains the selected IP Range (where relevant)

Function Keys	
F6=Add new rule	
F8=Print	
F10=Additional parameters	Displays additional parameters
F11=Alternative view	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 System i by FTP or REXEC server.

FTP/REXEC (Incoming) for IPv4 addresses

To set Logon security rules for FTP/REXEC for IPv4 addresses:

1. Select **31 > 1. FTP/REXEC Logon** from the **FTP/REXEC Logon Security** menu. The **Work with FTP/REXEC Logon Security** screen appears.

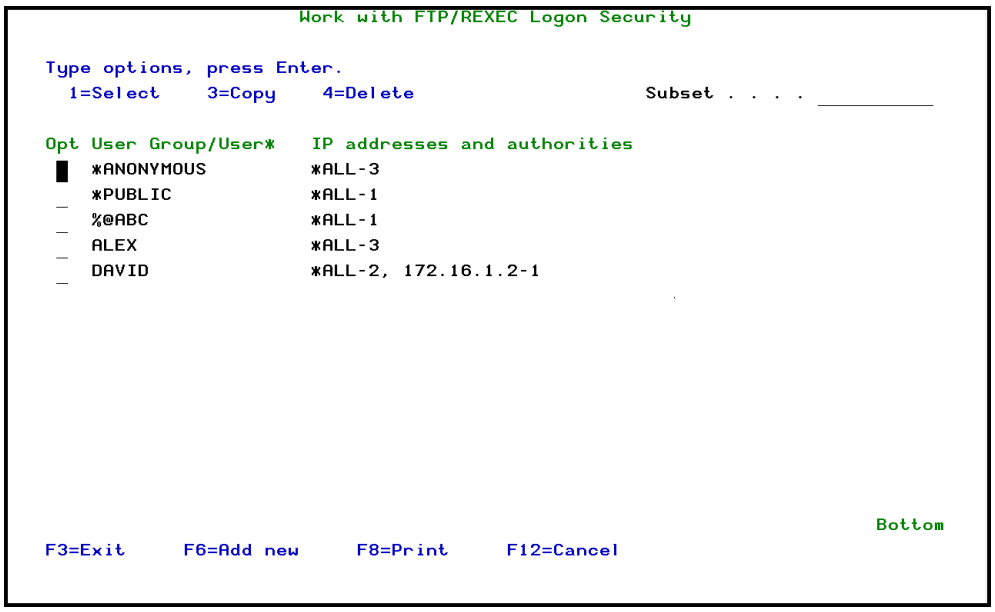


Figure 9-28. Work with FTP/REXEC Logon Security Screen

Field	
Subset	Search a user group/user or IP addresses/authorities whose names contain the subset.
User Group/ User	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)

Options	
1=Select	Modify this rule.
3=Copy	Copy this rule for another user.
4=Delete	Delete this rule.

Function Keys	
F6=Add new	Add new rule
F8=Print	Print rules

2. 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**).

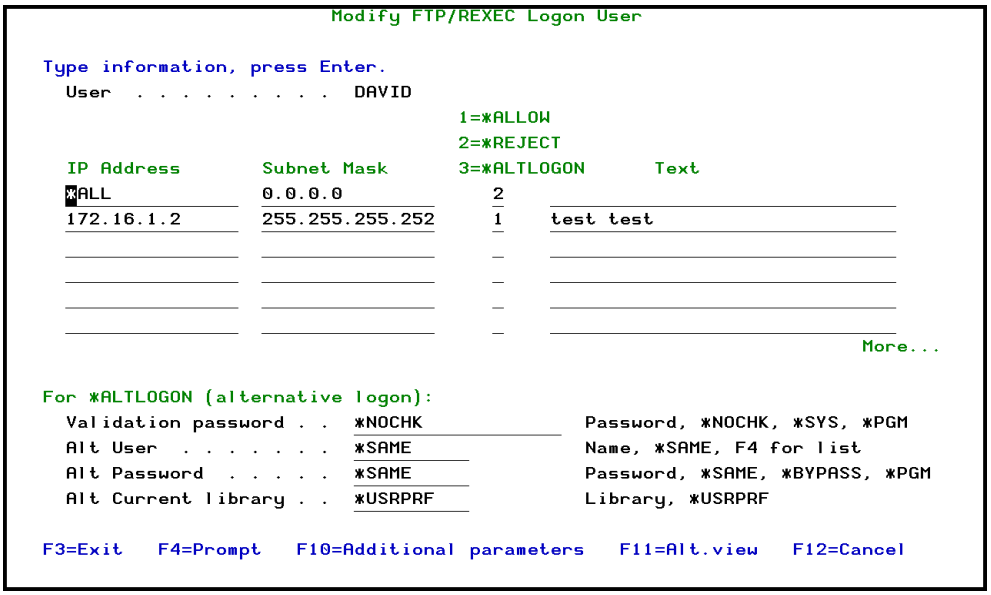


Figure 9-29. Modify FTP/REXEC Logon User Screen

Field	
User	Enter the user profile.
IP addresses	Enter an IP address using standard decimal format.
Subnet Mask	Enter the subnet mask using standard decimal format to define a range of IP addresses. Refer to the examples or press F4 to select an appropriate subnet mask range.
Logon	**1** = Allowed **2** = Rejected **3** = Alternative Sign-on (see Alternative Logon in the following table for more details)
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 (CRTUSRPRF). This is done without that user's knowledge.
Validation Password	This is the password used to validate the incoming user profile. **Password** = Type the password that is to be required for sign-on ***NOCHK** = password is not checked ***SYS** = Validation performed according to password in user profile ***PGM** = Use password presented by calling program
Alt User	Automatically sign-on with specified replacement user profile.

Field	
Alt Password	This is the password to be assigned to the alternate user. Use the specified password for logon instead of that in the user profile ***Same or Blank** = Do not replace password for alternate user ***BYPASS** = Bypass password validation at sign-on for alternate user ***PGM** = Use password presented by calling program for alternate user
Alt Current Library	Automatically replace the default current library with specified library.
Initial Home directory	The initial setting of the home directory to use for this session. When specified, this must be a valid absolute path name.
CCSID of initial home directory	The CCSID of the initial home directory.
CCSID of password	The CCSID of the alternate password
Name formal	***SAME** ***AS400** = Use the LIBRARY/FILE.MEMBER name format ***PC** = Use the path name format.
Current working directory	***SAME** ***CURRENT** = Use the current directory ***HOME** = Use the home directory
Data connection encryption option	Specifies whether FTP data connections for this FTP session are to be encrypted. ***SAME** ***NOTALLOW** = Encryption of FTP data connections is not allowed for this FTP session. ***ALLOW** = Encryption of FTP data connections is allowed (but not required) for this FTP session. ***REQUIRED** = Encryption of FTP data connections is required for this FTP session.

Function Keys	
F10=Additional parameters	Opens the continuation parameters screen.

3. Set the parameters according to the table and press **Enter**. FTP rules are according to user and IP.

The **Validation Password** is for the user specified in the FTP. Firewall compares the password entered in FTP to the one entered in this field. If this field contain ***SYS**, Firewall ensures that the password entered in FTP is the one defined on the system for the FTP user.

After the password is confirmed, the **Alt User**, the **Alt Password**, and the **Alt Current Library** are sent to the System i ensures that the **Alt User** and the **Alt Password** are a valid combination for FTP, and the user will see the message <*Alt-user*> logged on.

FTP/REXEC (Incoming) for IPv6 addresses

To set Logon security rules for FTP/REXEC for IPv6 addresses:

1. Select **31 > 2. FTP/REXEC Logon IPv6** from the **FTP/REXEC Logon Security** menu. The **Work with FTP/REXEC Logon Security** screen appears.

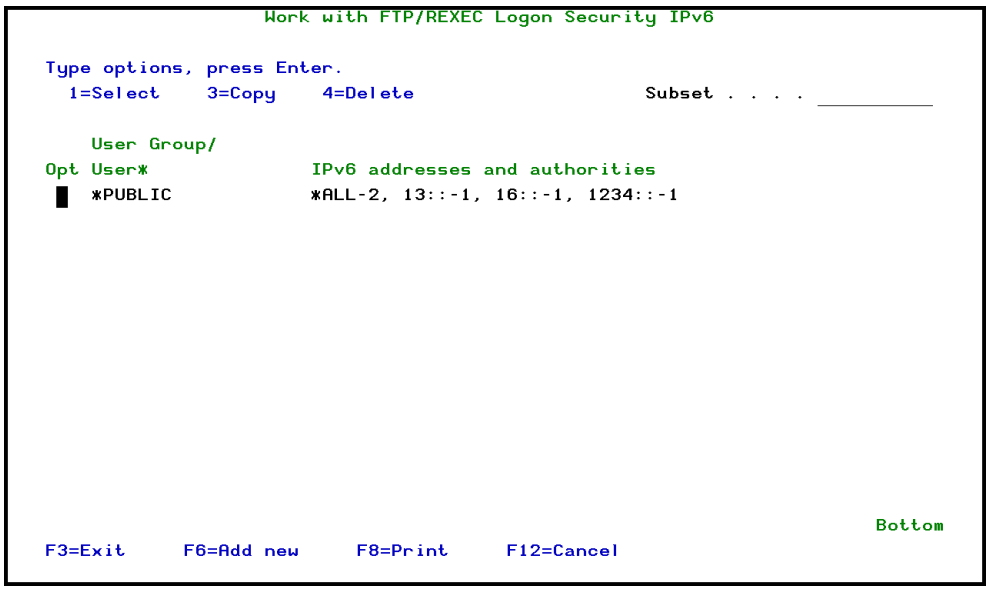


Figure 9-30. Work with FTP/REXEC Logon Security IPv6 Screen

Field	
Subset	Search a user group/user or IP addresses/authorities whose names contain the subset.
User Group/ User	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)

Options	
1=Select	Modify this rule.
3=Copy	Copy this rule for another user.
4=Delete	Delete this rule.

Function Keys	
F6=Add new	Add new rule
F8=Print	Print rules

2. To add a new rule, press **F6**. The **Add FTP/REXEC Logon User screen IPv6** appears (the screen and parameters are the same as the **Modify FTP/REXEC Logon User IPv6**, as shown in Figure 9-31 on page 161.

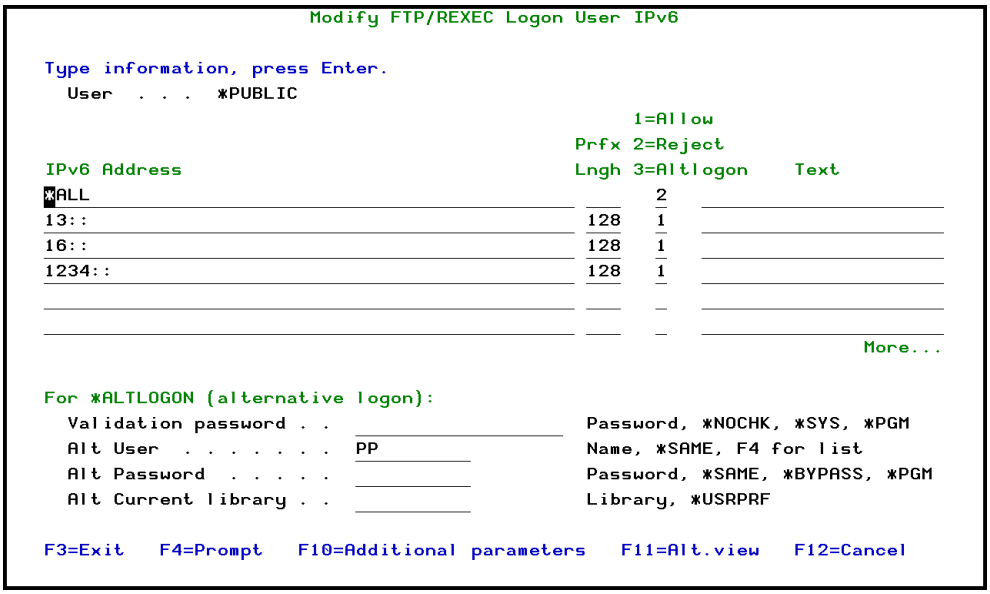


Figure 9-31. Modify FTP/REXEC Logon User IPv6 Screen

Field	
User	Enter the user profile.
IPv6 addresses	The IPv6 addresses for this user/user group.
Prfx Lngh	Prefix length for the IPv6 address
Logon	**1** = Allowed **2** = Rejected **3** = Alternative Sign-on (see Alternative Logon in the following table for more details)
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 (CRTUSRPRF). This is done without that user's knowledge.
Validation Password	This is the password used to validate the incoming user profile. **Password** = Type the password that is to be required for sign-on ***NOCHK** = password is not checked ***SYS** = Validation performed according to password in user profile ***PGM** = Use password presented by calling program
Alt User	Automatically sign-on with specified replacement user profile.

Field	
Alt Password	This is the password to be assigned to the alternate user. Use the specified password for logon instead of that in the user profile ***Same or Blank** = Do not replace password for alternate user ***BYPASS** = Bypass password validation at sign-on for alternate user ***PGM** = Use password presented by calling program for alternate user
Alt Current Library	Automatically replace the default current library with specified library.
Initial Home directory	The initial setting of the home directory to use for this session. When specified, this must be a valid absolute path name.
CCSID of initial home directory	The CCSID of the initial home directory.
CCSID of password	The CCSID of the alternate password
Name format	***SAME** ***AS400** = Use the LIBRARY/FILE.MEMBER name format ***PC** = Use the path name format.
Current working directory	***SAME** ***CURRENT** = Use the current directory ***HOME** = Use the home directory
Data connection encryption option	Specifies whether FTP data connections for this FTP session are to be encrypted. ***SAME** ***NOTALLOW** = Encryption of FTP data connections is not allowed for this FTP session. ***ALLOW** = Encryption of FTP data connections is allowed (but not required) for this FTP session. ***REQUIRED** = Encryption of FTP data connections is required for this FTP session.

Function Keys	
F10=Additional parameters	Opens the continuation parameters screen.

3. Set parameters according to the table and press **Enter**. FTP rules are according to user and IP.

The **Validation Password** is for the user specified in the FTP. Firewall compares the password entered in FTP to the one entered in this field. If this field contain ***SYS**, Firewall ensures that the password entered in FTP is the one defined on the system for the FTP user.

After the password is confirmed, the **Alt User**, the **Alt Password**, and the **Alt Current Library** are sent to the computer operating system.

The operating system ensures that the **Alt User** and the **Alt Password** are a proper combination for FTP, and the user will see the message <*Alt-user*> logged on.

Client FTP (Outgoing)

This server is used when the System i issues FTP (sub) commands as a client to another system.

Client FTP (Outgoing) for IPv4 addresses

1. To set Client FTP security rules for FTP/REXEC, select **31. FTP/REXEC** from the main menu. The **FTP/REXEC Logon Security** menu appears.
2. To work with Client FTP Security, select **5. Client FTP (Outgoing)** from the **FTP/REXEC Logon Security** menu. The **Work with Client FTP Security** screen appears.

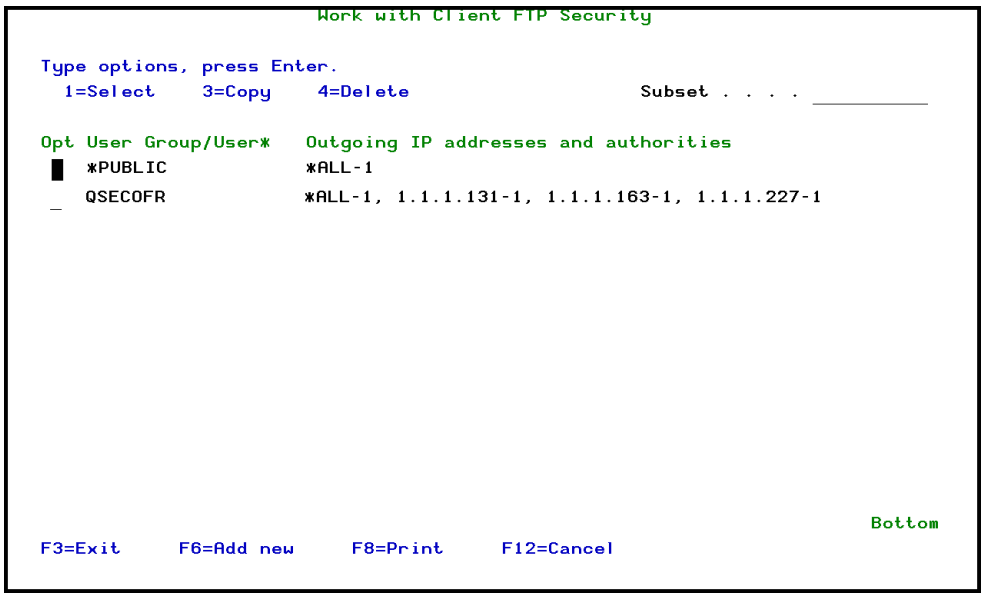


Figure 9-32. Work with Client FTP Security Screen

Field	
Subset	Search a user group/user or IP addresses/authorities whose names contain the subset.
User Group/ User	User and/or user group for whom the rules are set.
IP addresses and authorities	IP of the system to which the user wants to communicate from the System i. **1** = Allowed **2** = Rejected

Options	
1=Select	Modify this rule.
3=Copy	Copy this rule for another user.
4=Delete	Delete this rule.

Function Keys	
F6=Add new	Add new rule
F8=Print	Print rules

3. Select **F6** to add a new rule or option **1** to modify. The **Modify FTP Client User** screen.

appears.

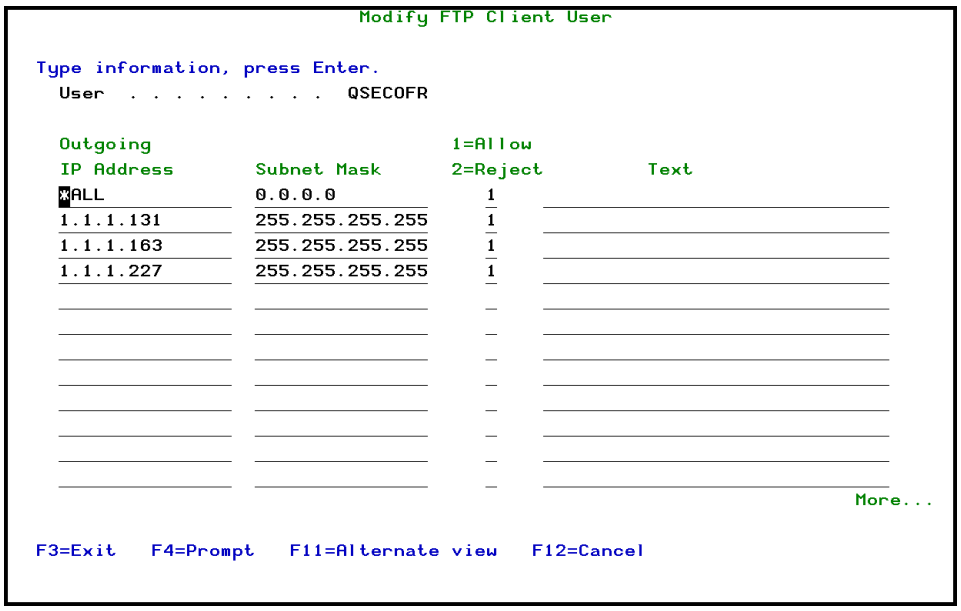


Figure 9-33. Modify FTP Client User Screen

Field	
User	Enter the user profile.
IP addresses	Enter an IP address using standard decimal format.
Subnet Mask	Enter the subnet mask using standard decimal format to define a range of IP addresses. Refer to the examples or press F4 to select an appropriate subnet mask range.
Logon	**1** = Allowed **2** = Rejected
Text	Enter descriptive text

4. Set parameters according to the table and press **Enter**.

Client FTP (Outgoing) for IPv6 addresses

1. To set Client FTP security rules for FTP/REXEC, select **31. FTP/REXEC** from the main menu. The **FTP/REXEC Logon Security** menu appears.
2. To work with Client FTP Security, select **6. Client FTP IPv6 (Outgoing)** from the **FTP/REXEC Logon Security** menu. The **Work with Client FTP Security** screen appears.

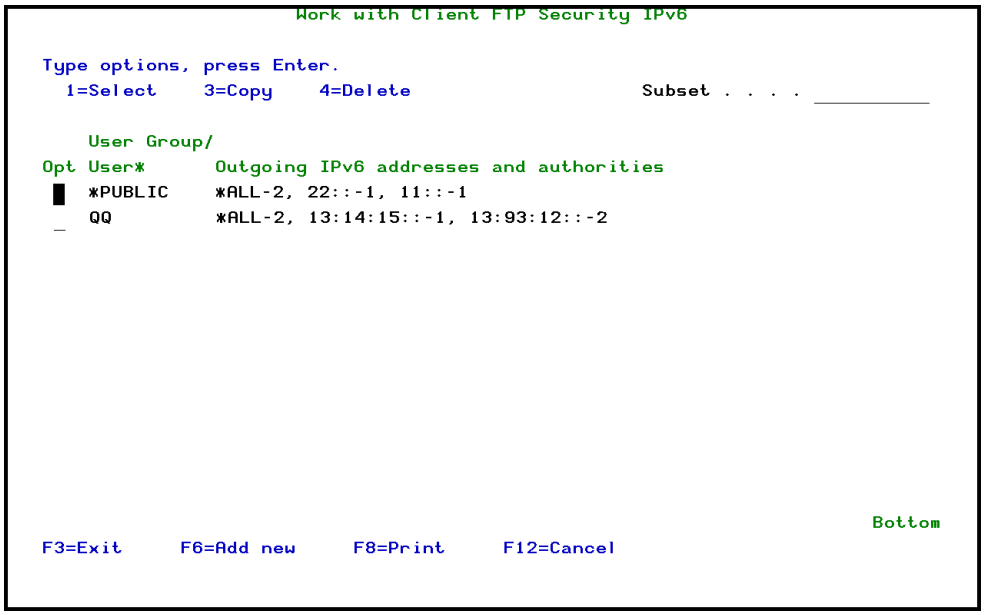


Figure 9-34. Work with Client FTP Security IPv6 Screen

Field	
Subset	Search a user group/user or IP addresses/authorities whose names contain the subset.
User Group/ User	User and/or user group for whom the rules are set.
IP addresses and authorities	IP of the system to which the user wants to communicate from the System i. **1** = Allowed **2** = Rejected

Options	
1=Select	Modify this rule.
3=Copy	Copy this rule for another user.
4=Delete	Delete this rule.

Function Keys	
F6=Add new	Add new rule
F8=Print	Print rules

3. Select **F6** to add a new rule or option **1** to modify. The **Modify FTP Client User IPv6** screen appears.

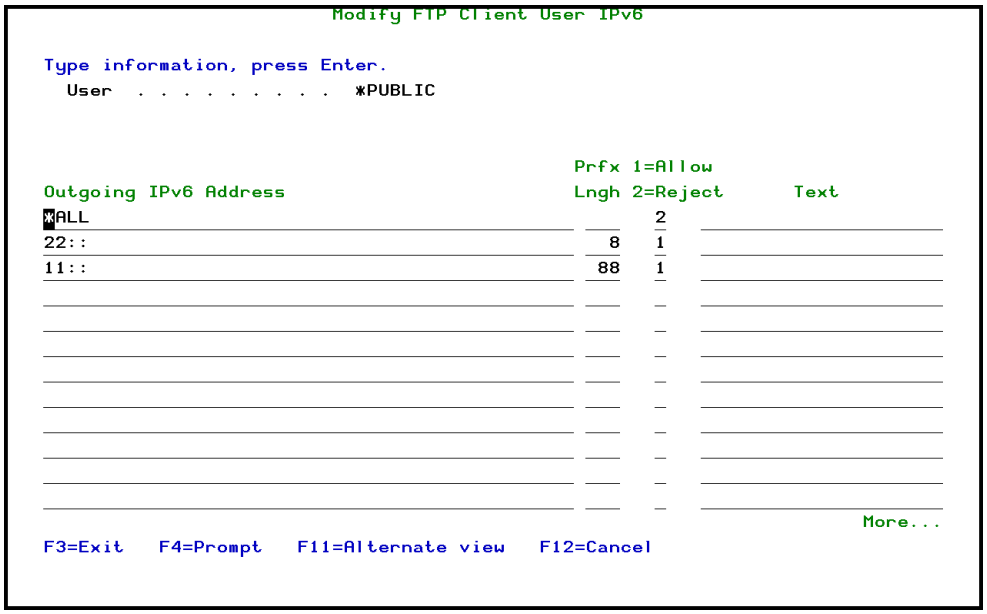


Figure 9-35. Modify FTP Client User IPv6 Screen

Field	
User	Enter the user profile.
IP addresses	Enter an IP address using standard decimal format.
Subnet Mask	Enter the subnet mask using standard decimal format to define a range of IP addresses. Refer to the examples or press F4 to select an appropriate subnet mask range.
Logon	**1** = Allowed **2** = Rejected
Text	Enter descriptive text

4. Set parameters according to the table and press **Enter**.

Telnet Security

You should define the Telnet Logon to control the first time a device connects to the system, for example when PC emulation software starts. Within the Telnet session, use Work with Users to specify permitted IP addresses and device names.

Telnet Logon

To work with Telnet and Sign-on

1. Select **32. Telnet** from the Firewall Main menu. The **Telnet Security** menu appears.
2. Select **1. Telnet Logon** from the **Telnet Security** menu. The **Work with TELNET Logon Security** screen appears.

```
                    Work with TELNET Logon Security

Type options, press Enter.                          Subset . . .
  1=Select  3=Copy  4=Delete  5=IP range          Min
                                      Incoming    pwd                 Assigned
Opt IP Address       Subset Mask      Terminal    vld  Logon          Terminal
 _  *ALL             0.0.0.0          *ALL         0   *ACCEPT        *SAME
 _  1.1.1.105        255.255.255.255  *ALL         0   *FRCSIGNON     QPADEV0005
 _  1.1.1.155        255.255.255.255  *ALL         0   *ACCEPT        *SAME
 _  1.1.1.160        255.255.255.255  *ALL         0   *REJECT
 _  1.1.1.184        255.255.255.255  *ALL         0   *AUTOSIGNON    QPADEV0005
 _  1.1.1.222        255.255.255.192  *ALL         0   *ACCEPT        *SAME
 _  1.1.1.200        255.255.255.255  *ALL         0   *FRCSIGNON     *SAME
 _  1.1.1.222        255.255.255.240  *ALL         0   *ACCEPTSIP     *SAME
 _  1.1.1.222        255.255.255.255  *ALL         0   *ACCEPTSIP     *SAME
 _  1.1.33.51        255.255.255.255  *ALL         1   *ACCEPT        *SAME
 _  2.24.46.68       255.255.255.255  *ALL         0   *ACCEPT        *SAME
 _  3.34.35.37       255.255.255.255  *ALL         0   *ACCEPT        *SAME
 _  4.44.45.47       255.255.255.255  *ALL         0   *ACCEPT        *SAME
 _  7.11.33.33       255.255.255.248  *ALL         0   *ACCEPT        *SAME
                                                                   More...
F3=Exit    F5=Refresh    F6=Add new    F8=Print                   F12=Cancel
```

Figure 9-36. Work with Telnet Logon Security Screen

Field	
Subset	Search a user group/user or IP addresses/authorities whose names contain the subset.

Options	
1=Select	Modify this rule.
3=Copy	Copy this rule for another user.
4=Delete	Delete this rule.
5=IP Range	Display the equivalent IP range for this rule

Function Keys	
F6=Add new	Add new rule
F8=Print	Print rules

3. Select **F6** to add a new rule or option **1** to modify.

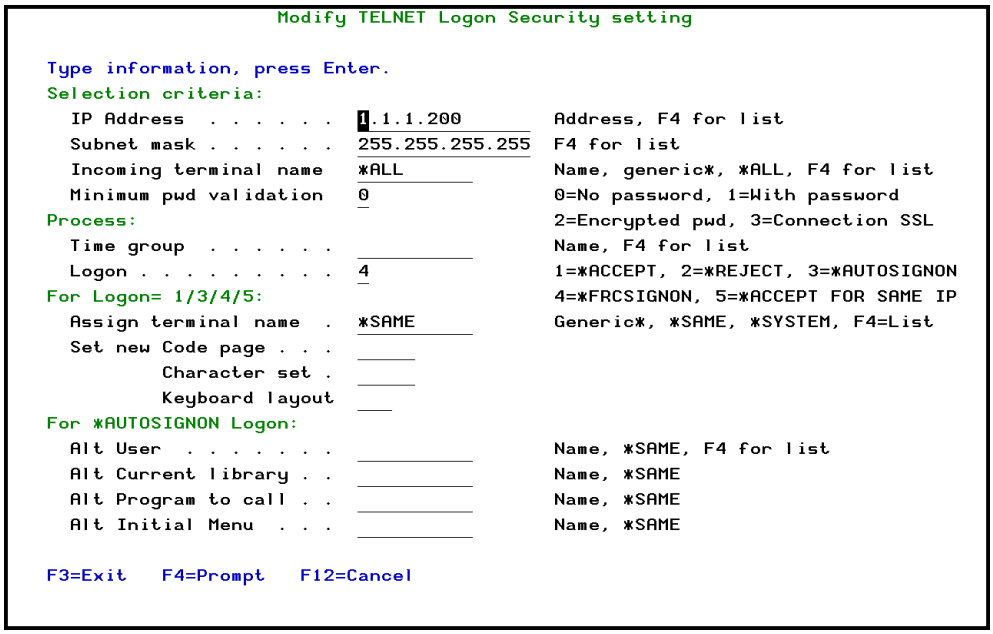


Figure 9-37. Modify Telnet Logon Security Setting Screen

Field	
Selection criteria:	
IP Address/Subnet Mask	IP address and subnet mask in decimal format. TIP: Press F4 and select the subnet mask from a list.
Incoming Terminal Name	Terminal name assigned by the System i or emulation software. **Generic*** ***ALL** ***BLANKS** F4 for a list of all available terminals.
Minimum Pwd Validation	This is the method used to validate the incoming user profile. Apply rule according to password validation level: **0** = No password validation **1** = Use password **2** = Use encrypted password **3** = Connection is using SSL
Process:	
Time group	Enter time group name or press **F4** to select from a list.
Logon	**1** = Accept logon request **2** = Reject logon request **3** = Sign-on automatically if permitted by System i configuration **4** = Force sign-on even if System i is configured for automatic sign-on **5** =Accept logon request for the same IP

Field	
Assign terminal name	Enter the name to optionally replace the incoming terminal name Generic* = Text before "*" plus sequentially assigned number *SAME or Blank = Do not replace the income terminal name *SYSTEM = Use terminal name assigned by IBM i
Set new	Define Code page, Character set and Keyboard layout
Alt User	Automatically sign-on with specified replacement user profile
Alt Current Library	Automatically replace the default current library with specified library
Alt Program	Automatically replace the default program to be run at sign-on
Alt Initial menu	Automatically replace the default initial user menu at sign-on

Function Keys	
F4=Prompt	Opens a prompt screen for the appropriate parameter.

4. Set parameters according to the table and press **Enter**.

Telnet Logon IPv6

1. To work with Telnet and Sign-on, select **32 > 2. Telnet Logon IPv6** from the Telnet Security screen. The **Work with TELNET Logon Security IPv6** screen appears.

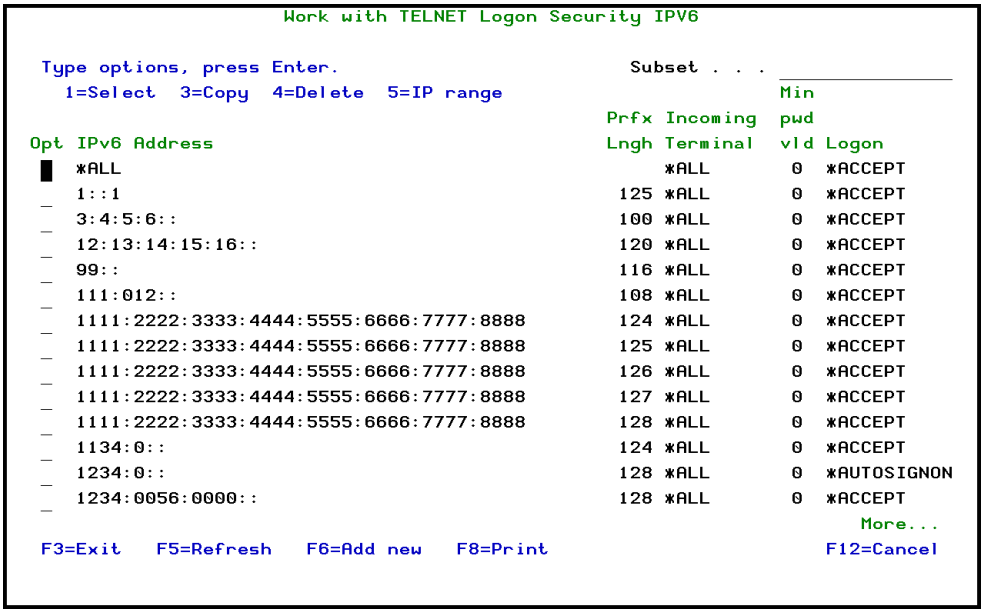


Figure 9-38. Work with Telnet Logon Security IPv6 Screen

Field	
Subset	Search a user group/user or IP addresses/authorities whose names contain the subset.

Options	
1=Select	Modify this rule.
3=Copy	Copy this rule for another user.
4=Delete	Delete this rule.
5=IP Range	Display the equivalent IP range for this rule

Function Keys	
F6=Add new	Add new rule
F8=Print	Print rules

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

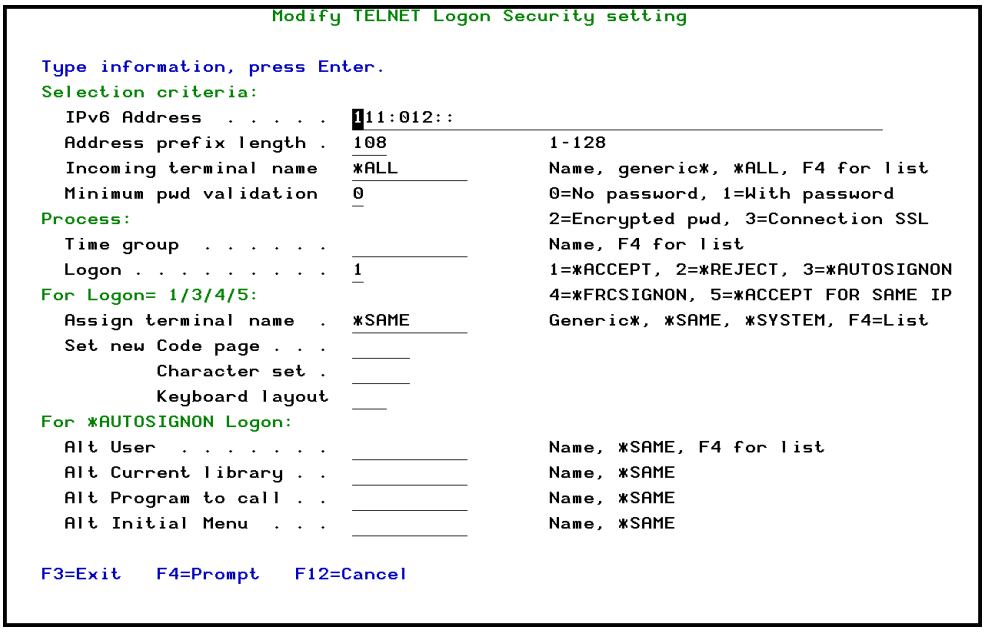


Figure 9-39. Modify Telnet Logon Security Setting IPv6 Screen

Field	
Selection criteria:	
IPv6 Address/Prefix Length	IPv6 address and prefix length.
Incoming Terminal Name	Terminal name assigned by the System i or emulation software. **Generic*** ***ALL** ***BLANKS** F4 for a list of all available terminals.
Minimum Pwd Validation	This is the method used to validate the incoming user profile. Apply rule according to password validation level: **0** = No password validation **1** = Use password **2** = Use encrypted password **3** = Connection is using SSL
Process:	
Time group	Enter time group name or press **F4** to select from a list.
Logon	**1** = Accept logon request **2** = Reject logon request **3** = Sign-on automatically if permitted by System i configuration **4** = Force sign-on even if System i is configured for automatic sign-on **5** =Accept logon request for the same IP

Field	
Assign terminal name	Enter the name to optionally replace the incoming terminal name Generic* = Text before "*" plus sequentially assigned number *SAME or Blank = Do not replace the income terminal name *SYSTEM = Use terminal name assigned by IBM i
Set new	Define Code page, Character set and Keyboard layout
Alt User	Automatically sign-on with specified replacement user profile
Alt Current Library	Automatically replace the default current library with specified library
Alt Program	Automatically replace the default program to be run at sign-on
Alt Initial menu	Automatically replace the default initial user menu at sign-on

Function Keys	
F4=Prompt	Opens a prompt screen for the appropriate parameter.

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 > 1. Telnet Logon** to access the **Work with TELNET Logon Security** screen.
2. Press **F6** to access the **Add TELNET Logon Security Setting** screen.
3. See Telnet Security on page 166 for details of the Telnet parameters.

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:

1. Select **32 > 15. Display SIGNON Log** from the **Telnet Security** screen.
2. Set the parameters and press **Enter**. The **Display Firewall Log** screen appears, with all the transactions that used the **Sign-On** server.

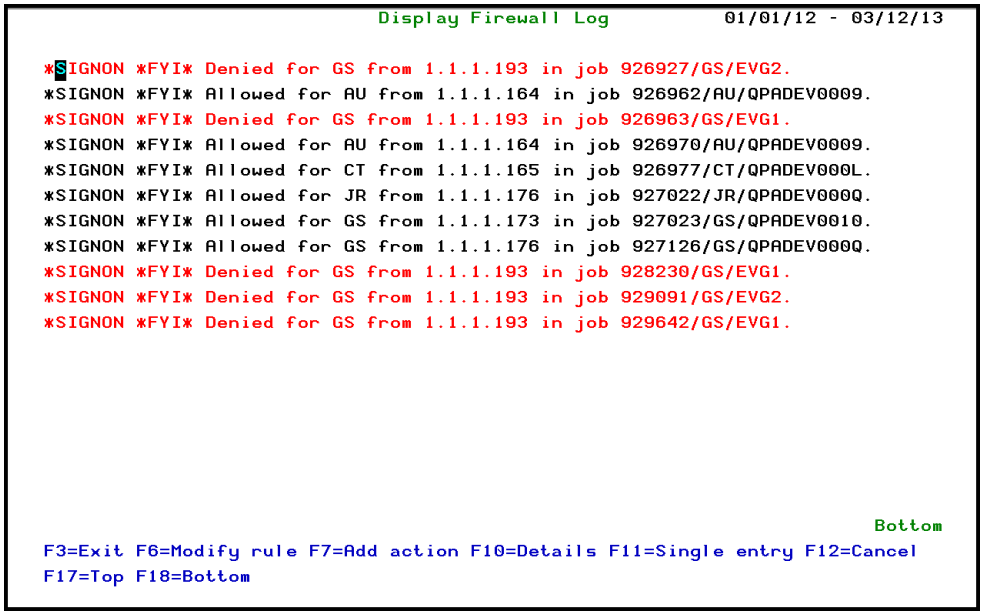


Figure 9-40. Display Firewall Log Screen

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

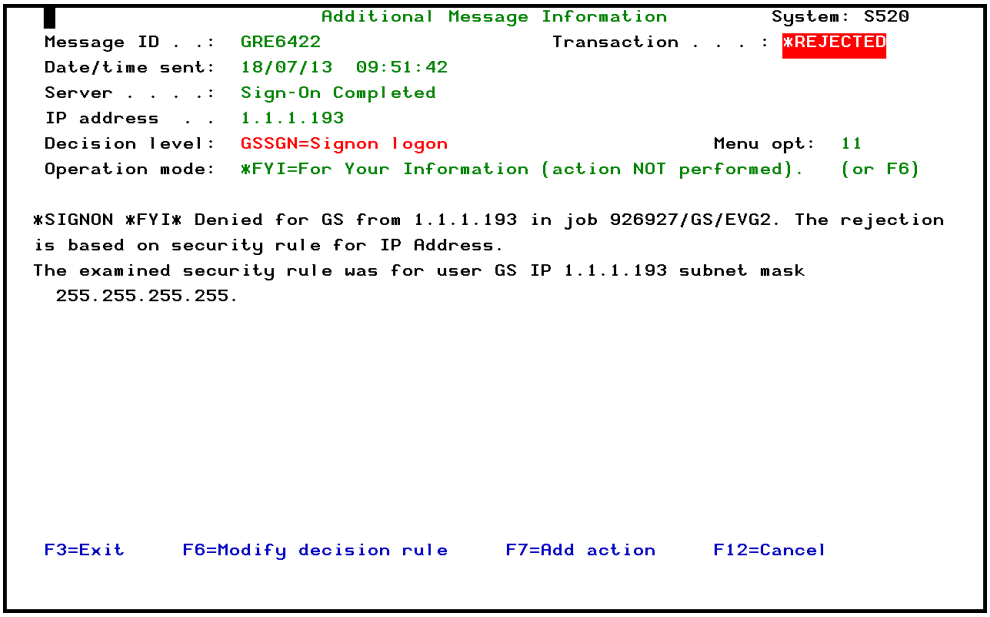


Figure 9-41. Additional Message Information

4. In the **Work with User Security** screen, select the user of sign-on transaction (example: GS) and type **1**.

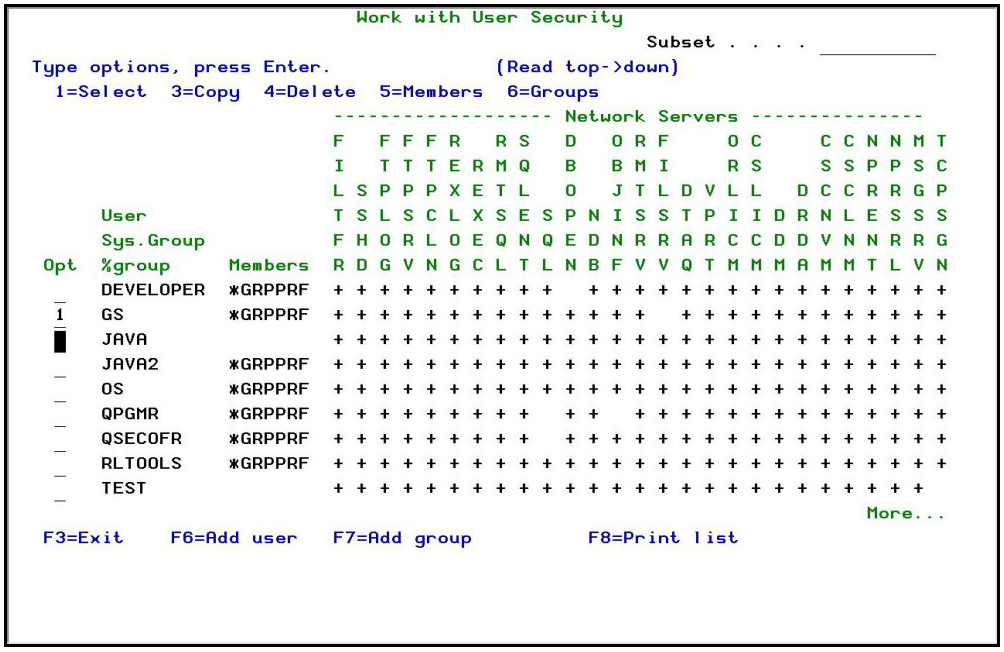


Figure 9-42. Work with User Security Screen

5. Select **5. Device Names** from the **Modify User Security** screen to add or modify sign-on device names.

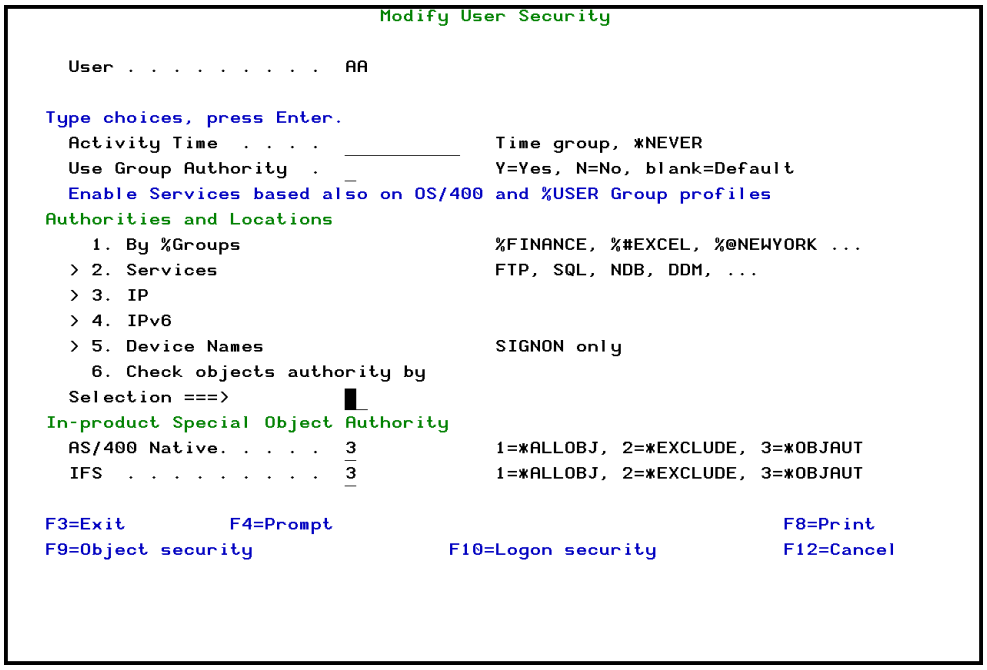


Figure 9-43. Modify User Security Screen

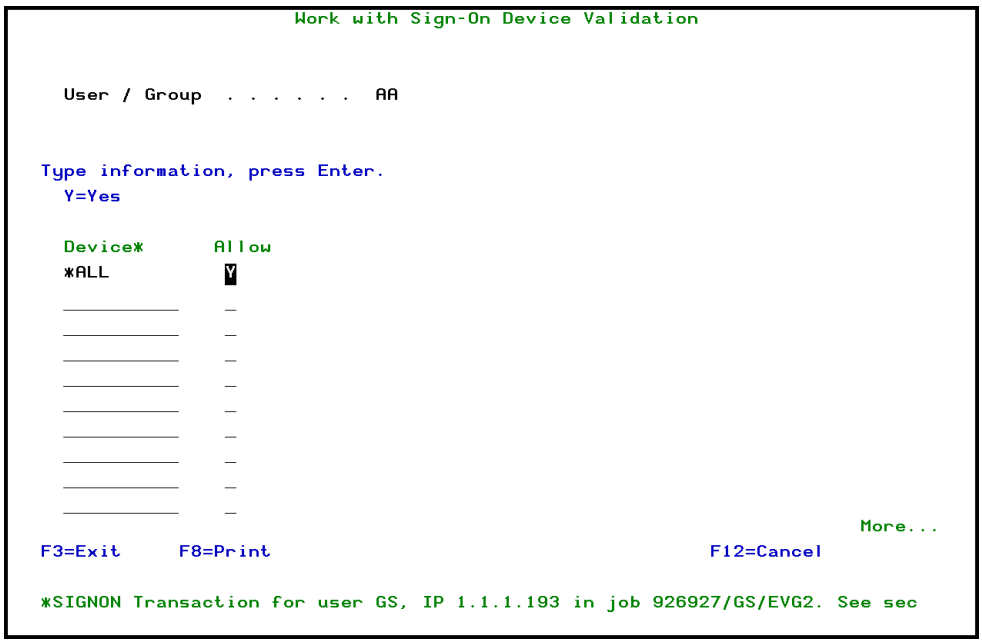


Figure 9-44. Work with Sign-on Device Validation Screen

Work with Alternative Users

When Object Authority varies according to the server in use, specify the User whose authority will be checked. The User does not have to exist, and its group profiles will not be checked.

To set the parameters, select **11. Users and Groups** from the main menu, then select a User System Group (but not a %group). When the **Modify User Security** screen is displayed, select Option **6. Check objects authority by**. The **Work with Alternative Users** screen appears, as displayed below.

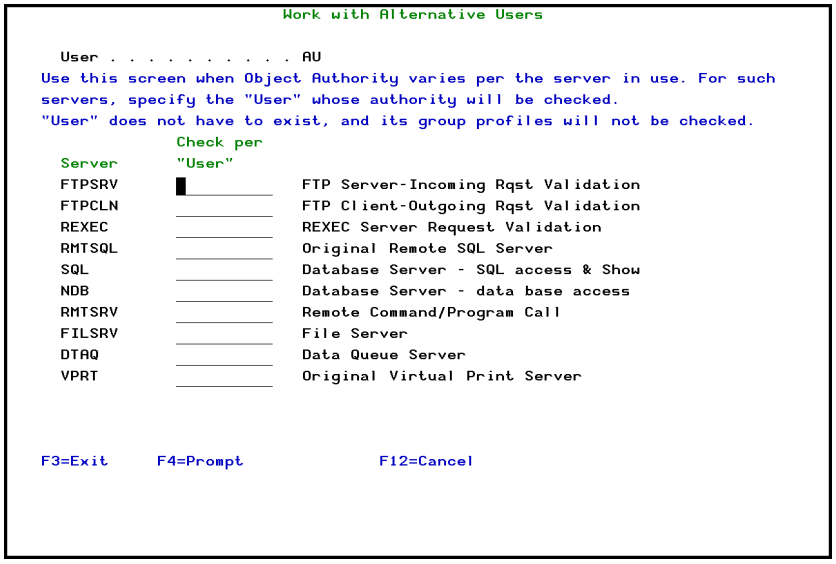


Figure 9-45. Work with Alternative Users Screen

Field	
User	The selected user for which you are selecting alternative users
Server	Server names
Check per "User"	Enter the name of the user whose authority will be checked.

Function Keys	
F4=Prompt	Opens a prompt screen to select 1 or more Users/User groups.

Passthrough Security

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.

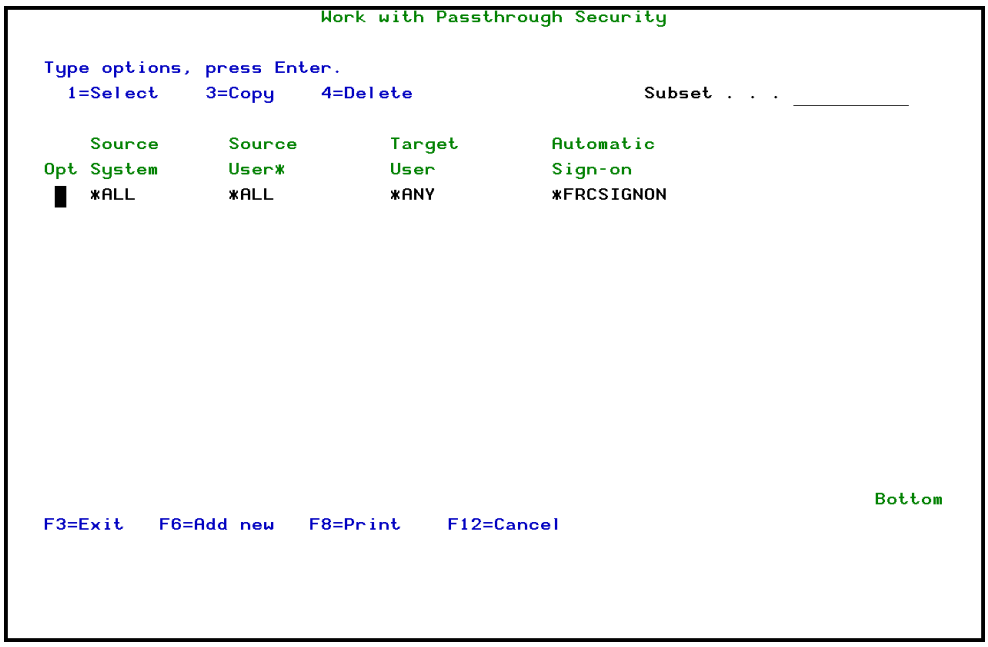


Figure 9-46. Work with Passthrough Security Screen

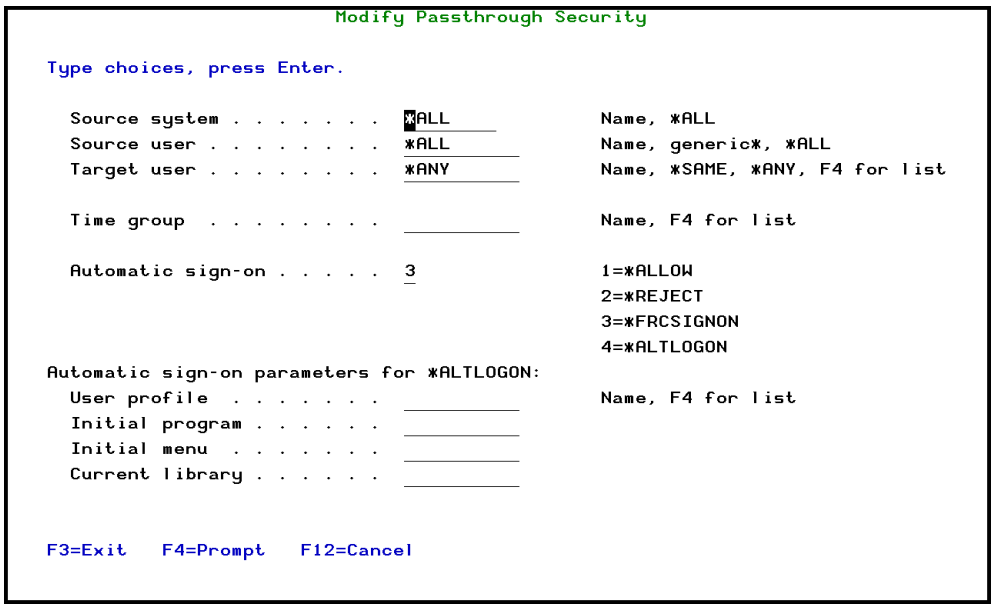


Figure 9-47. Modify Passthrough Security Screen

Field	
Source System	SNA system name of the source (incoming) computer.
Source User	User profile of the source system.
Target User	User profile for logon at the target system.
Automatic Sign-on	**1** = Accept logon request. **2** = Reject logon request. **3** = Force sign-on even if System i is configured for automatic sign-on **4** = Sign-on automatically with an alternate user profile.
User Profile	Automatically sign-on with specified replacement user profile
Initial Program	Automatically replace the default program to be run at sign-on
Initial menu	Automatically replace the default initial user menu at sign-on
Current Library	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.

For information about Working with Advanced Security, see Advanced Security Features on page 179.

10

Advanced Security Features

The **Work with Advanced Security** Screen enables the user to configure powerful security settings. To access these settings, select **35. DDM, DRDA, SSH, Port...** from the Firewall main menu. The **Work with Advanced Security** screen appears.

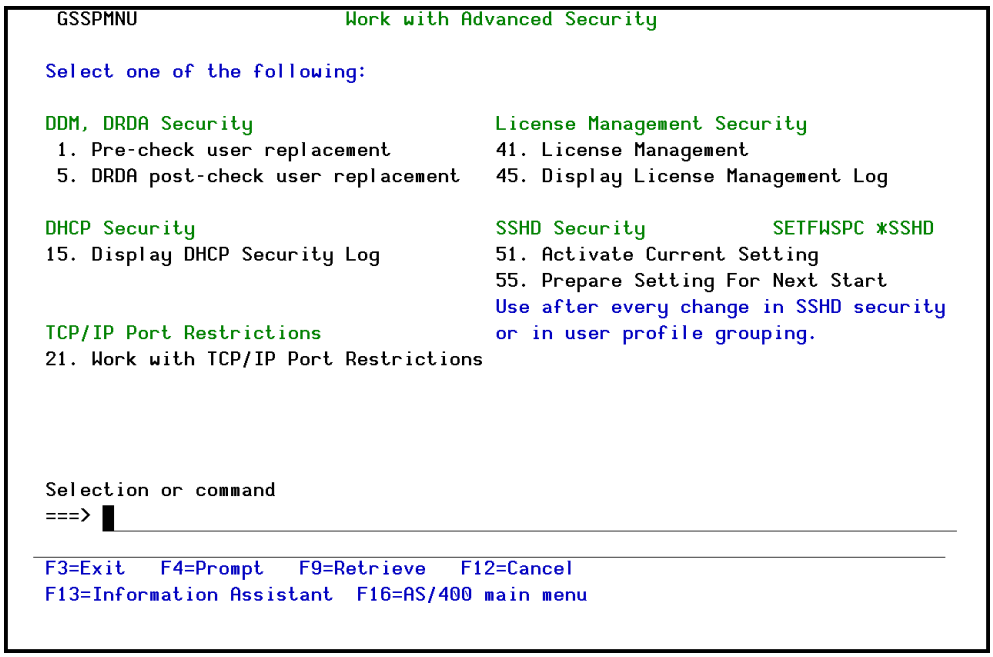


Figure 10-1. Work with Advanced Security Screen

DDM 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.

For example, to connect the PC and the AS400, Java makes internal use of DDM. This is done through a standard API. In addition, some of the features in iSecurity use DDM, amongst them are:

- Check iSecurity authority license
- Export/Import
- Replication
- Password Reset
- RLSNDPTF
- RUNXXQRY

DRDA Security

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: (i) the application requester function and (ii) 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**.

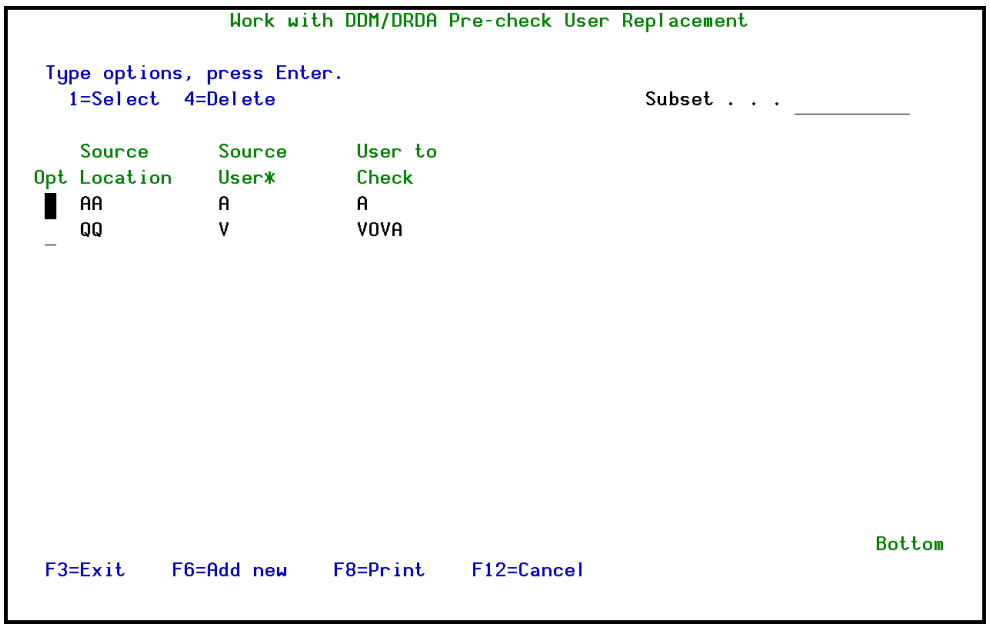


Figure 10-2. Work with DDM/DRDA Pre-check User Replacement Screen

Field	
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.

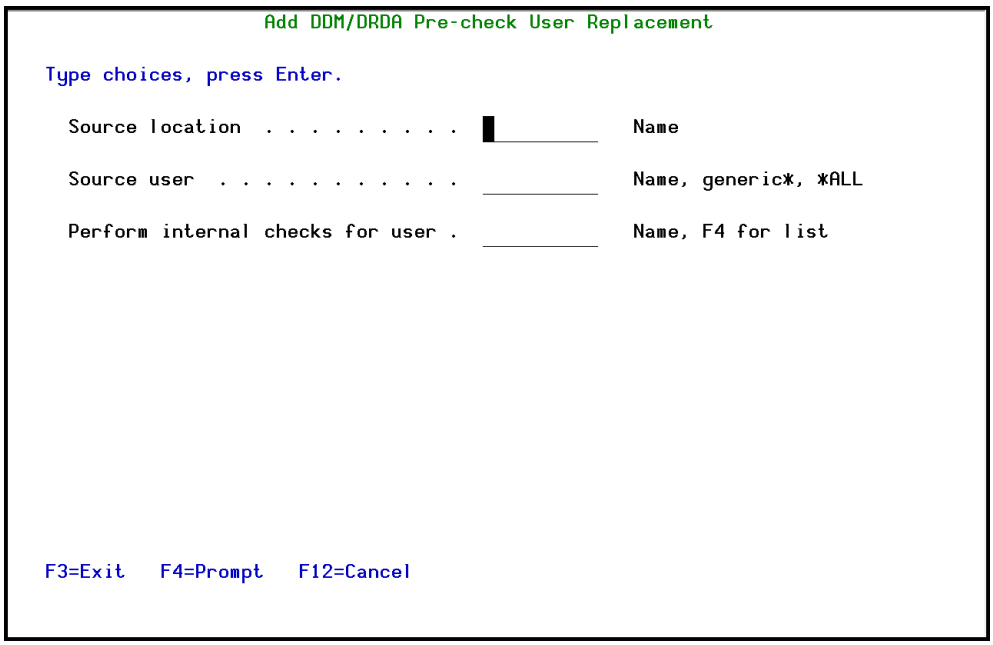


Figure 10-3. Add DDM/DRDA Pre-check User Replacement Screen

Field	
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.

1. 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.
2. Set your desired parameters and press Enter. To modify, select **1**. To add, select **F6**.

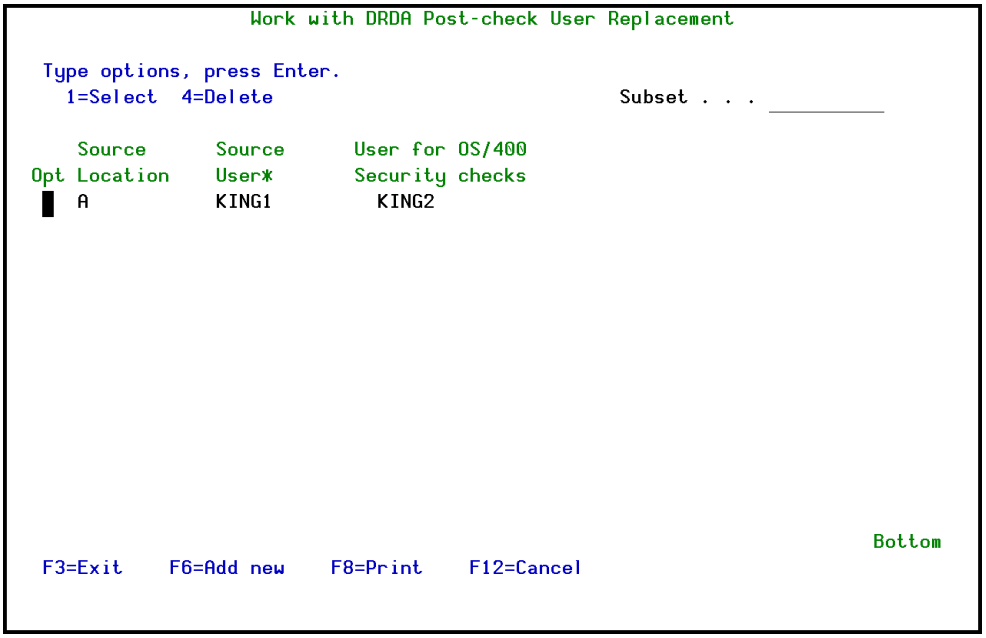


Figure 10-4. Work with DDM/DRDA Post-check User Replacements Screen

Field	
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 System i 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**.

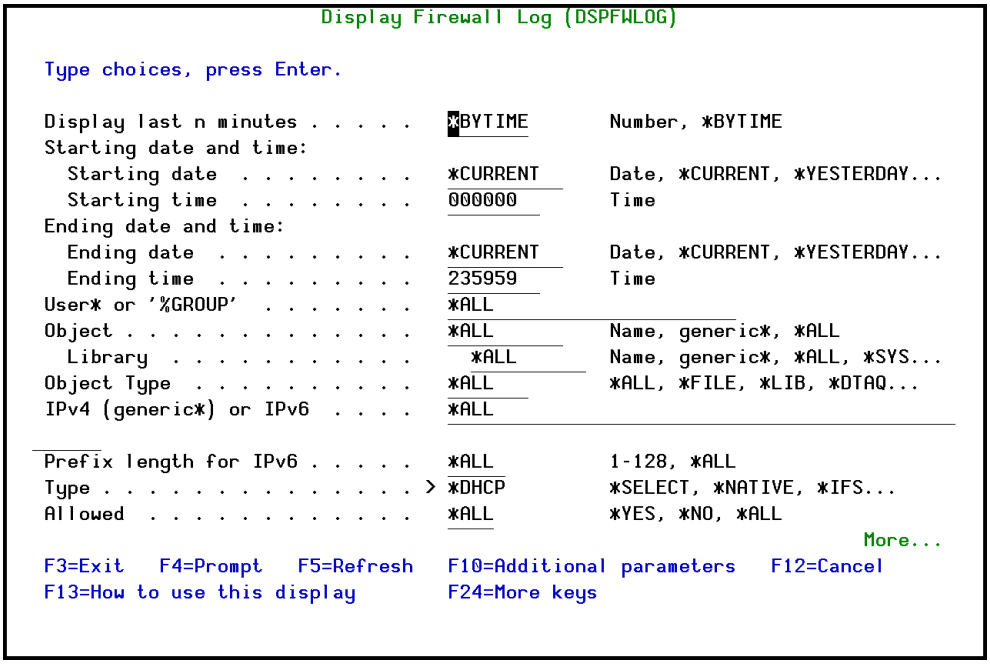


Figure 10-5. Display Firewall Log Screen

Field	
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 to 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
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

Field	
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
Merge data to a single output	***YES**, ***NO** (When <System to run for> is not *CURRENT)
Place output on	***CURRENT**, ***SYSTEM** (When <System to run for> is not *CURRENT)
Print format	***SHORT**, ***FULL** (When Output = *PRINT)
Add column headings	***NO**, ***YES** (When Output = *CSV)
Add control fields	***NO**, ***YES**: if Output = *OUTFILE or *CSV, some fields (for example, user, type) are added to the record to enable easier programming manipulation
Job description	**Name**, ***NONE** to run interactively
Library	**Library** of the job description
Type	Filter records by audit type ***All** = All types as specified in the query definition ***QRY** = Select server type from a list **Server Type** = Enter the server type
Program Name	***ALL** or Filter records by the name of the program that created the journal record.
Job Name	***ALL** or Filter records by OS/400 job name.
Job Name - User	***ALL** or Filter records by OS/400 job name.
Job Name - Number	***ALL** or Filter records by OS/400 job name.
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
Filter by Time Group - Time Group	**Name** = Name of time group ***SELECT** = Select time group from list at run time
Original command sent from	**Internal use only**
Object	The IFS object name that is created. ***TEMP** = a temporary object is created and deleted after being attached ***QRY** = The name is the query name ***AUTO** = The name will be created automatically
Directory	**/iSecurity/report output/** ***DATE** = A new directory per date is created to keep all reports running during that date
User defined data	**Internal use only**

Function Keys	
F4=Prompt	Prompt for valid entries in the field where the cursor is located.
F5=Refresh	Restores the default definitions
F9=All Parameter	Display all parameters available for the command. Usually, the only parameters displayed are those that are relevant, depending on already entered parameters.
F10=Additional parameters	Display the relevant additional parameters that are relevant, depending on already entered parameters.
F11=Keywords/Choices	Toggle between displaying the keywords or the choices for each parameter.
F14=Command string	Display the full command string that will be run, on the basis of the current parameter choices.
F15=Error messages	Display any relevant error messages.
F16=Command complete	Run the command instantly.
F24=More keys	Display additional command keys.

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.

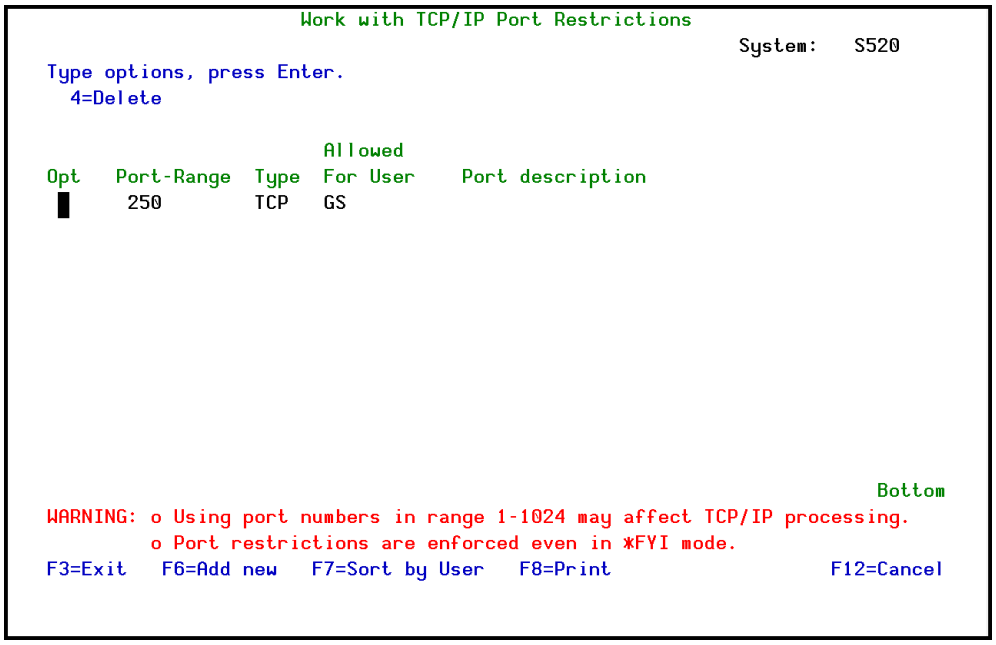


Figure 10-6. Work with TCP/IP Port Restrictions Screen

Field	
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.

2. Select **F6** to add a new rule. The **Add TCP/IP Port Restriction** screen appears.

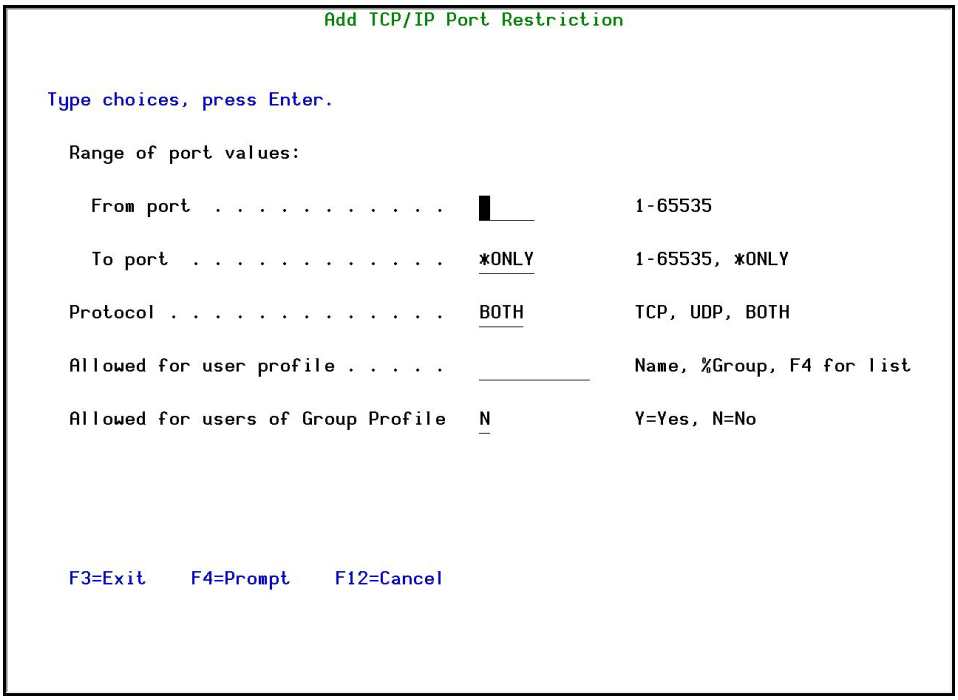


Figure 10-7. Add TCP/IP Port Restriction

Field	
From port	The port that is being restricted or the first port in the range that is being restricted.
To port	The last port in the range that is being restricted. If only one port is restricted, enter ***ONLY**.
Protocol	**TCP** **UDP** **BOTH**
Allowed for user profile	**Name** = The rule is added for the specific name **%Group** = The rule is added for all members of %Group
Allowed for users of Group Profile	**Y** = Yes, allows you to open a single rule for all members of a Group Profile. **N** = No (default value)

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.

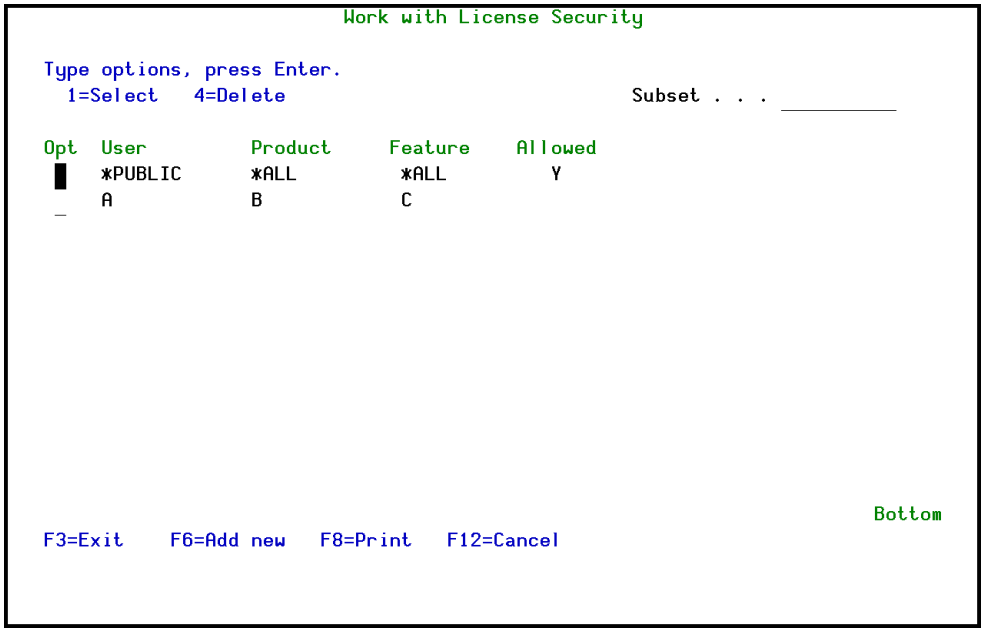


Figure 10-8. Work with License Security Screen

Field	
User	User working with particular software
Product	Software with which the user is working
Feature	The feature that the user has access to ***ALL** = all features
Allowed	Y = User is allowed to access this software

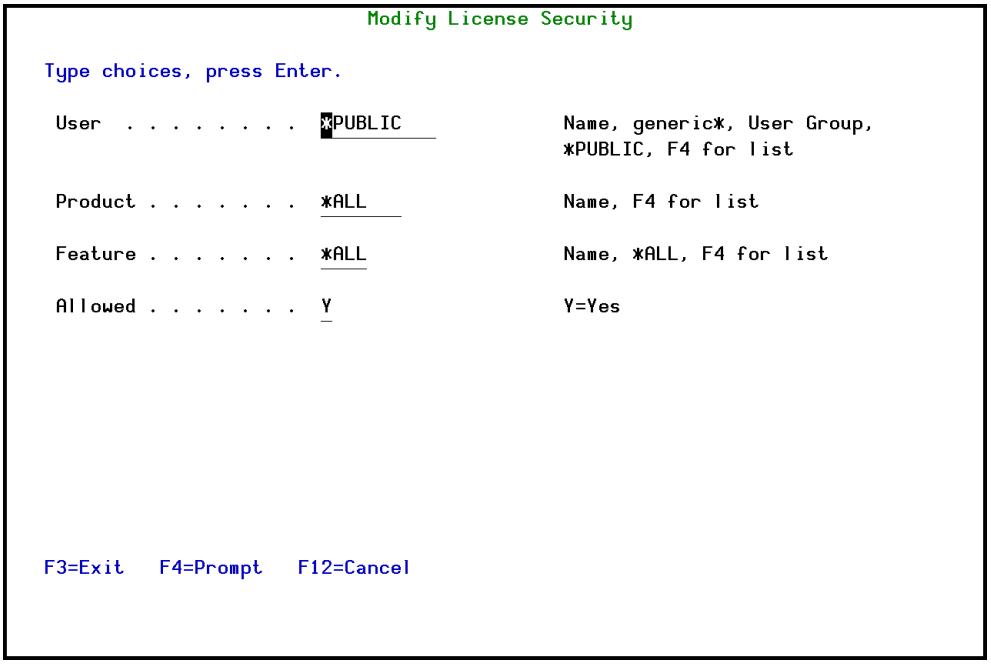


Figure 10-9. Modify License Security Screen

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 DHCP Security on page 183, and press **Enter.**

SSH Daemon Server Security, SETFWSPC *SSHD

After every change in SSHD security or in user profile grouping, click one to execute option **51. Activate Current Setting** and option **55. Prepare Setting For Next Start**.

Configuration and Maintenance

System Configuration

This section describes how to set the general configuration for Firewall.

To set general configurations:

1. Select **81. System Configuration** from the Main screen. The **iSecurity (part I) Global Parameters** screen appears.

```
                    iSecurity (part I) Global Parameters     29/11/16 08:07:24

Firewall  *FYI*                              SIEM Support
 1. General Definitions                      70. Main Control-----> Active
 2. Additional Settings                      71. SIEM 1: syslog#1     Y
 3. User Exit Programs                       72. SIEM 2: Syslog#2     Y
 4. Transaction Post Processing              73. SIEM 3: Syslog#3     Y
 5. Intrusion Detection System               74. JSON                 N
 6. Password Exit Programs
 7. Enable ACTION (CL Script + more)         79. Setting Severity for Servers
 9. Log Retention


Other Products Definitions Active            General
11. Command                   Y              81. iSecurity/Base Configuration
21. Screen                    N              91. Language Support
31. Password                  N              99. Copyright Notice
41. 2FA

Selection ===>
Release ID . . . . . .  17.36 16-11-24    44DE466  520 7459   1
Authorization code . . . . . .  801612720413              1   S520
F3=Exit    F22=Enter authority code
```

Figure 11-1. iSecurity (part I) Global Parameters Screen

General Definitions

This option presents general definitions relating to emergency overrides, FYI (Simulation) mode, Firewall history log, IBM i Group and Supplemental profiles, and Super Speed processing. Follow this procedure:

1. Select **81 > 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**.

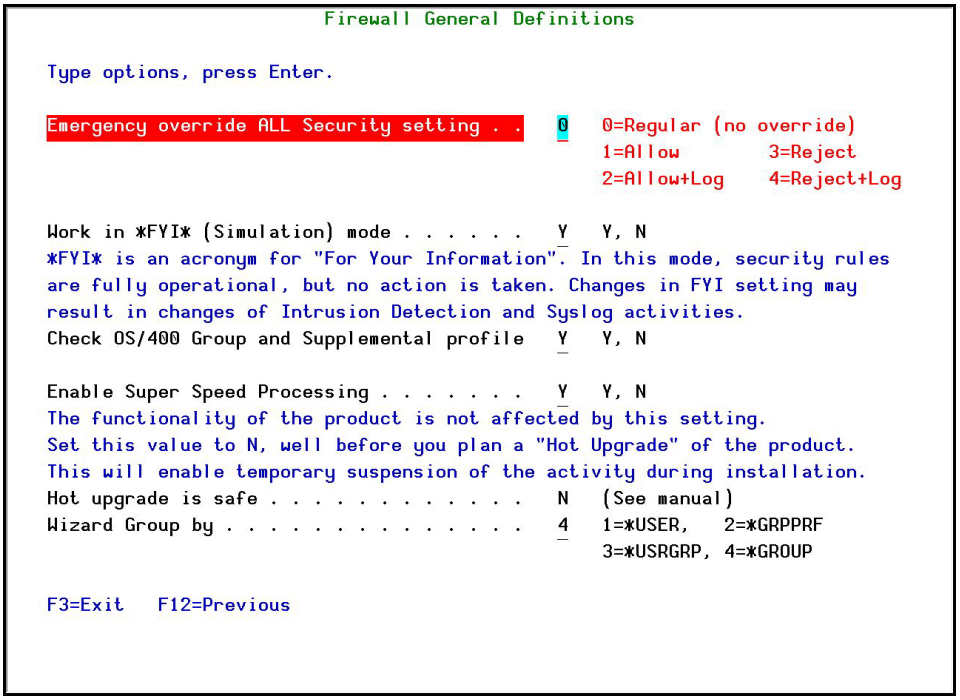


Figure 11-2. Firewall General Definitions Screen

Field	
Emergency override ALL Security setting	This option is explained in full detail in Using the Emergency Override Feature on page 62. **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 FYI Simulation Mode - Global Setting on page 61. **Y** = Enable FYI globally **N** = Do not enable FYI

Field	
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, to improve product performance. Disable this feature a week before an upgrade, in order to perform a "hot upgrade" - allowing you to upgrade the product without shutting down during the upgrade. **Y** = enable super speed processing **N** = disable super speed processing Note: After you change this parameter, you must perform an IPL for it to take affect.
Hot upgrade is safe	**Y**/**N**: shows when it is safe to perform a Hot Upgrade.
Wizard Group by	Set the option that will be used when ***DFT** is chosen as the parameter for **Group By** when working with Rule Wizards. **1=*USER** summarizes by user profile **2=*GRPPRF** summarizes by system group profiles plus all users not defined in group profiles. **3=USRGRP** summarizes by user groups and value **4=*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. This is the default value. See Using the Rule Wizards on page 27 for further details.

Additional Settings

To define additional settings:

1. Select **82 > 2. Additional Settings** from the **iSecurity (part I) Global Parameters** screen. The **Firewall Additional Settings** screen appears.

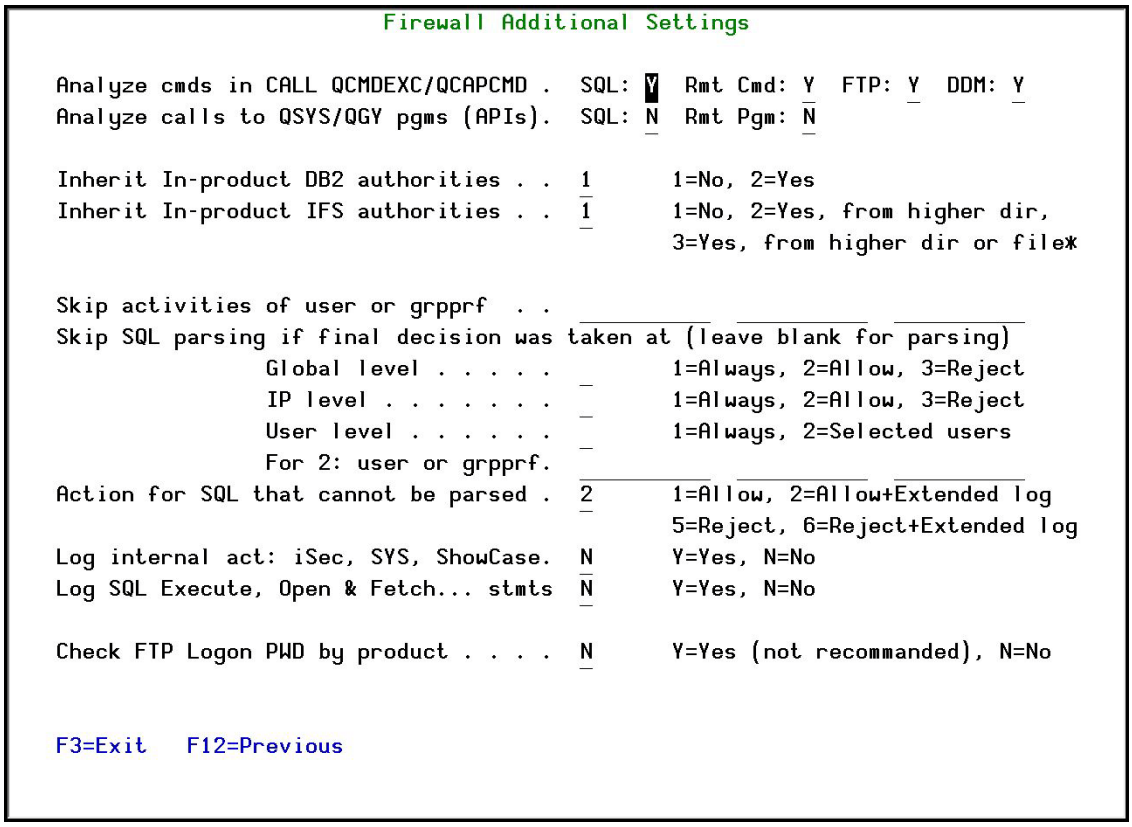


Figure 11-3. Firewall Additional Settings Screen

Field	
Analyze cmds in CALL QCMDEXC/QCAPCMD	**N**=No **Y**=Enables analysis of commands within the defined servers (SQL, Remote CMD, FTP, DDM) when these commands are called by QCMDEXC or QCAPCMD. This analysis will allow you to see calls to other programs/commands that are embedded within QCMDEXC or QCAPCMD. We recommend that you set all these options to **Y**.
Analyze calls to QSYS/QGY programs (APIs)	**N**=No **Y**=Enables analysis of the programs (for example, APIs) that reside in the QSYS library within the defined servers (SQL, Remote Pgm). Such calls are normally allowed calls to APIs and should not need analysis. We recommend that you set all these options to **N**.
Inherit In-product DB2 authorities	**1**=No (Default) **2**=Yes - Less generic authority takes preference over more generic authority concerning the object name in Native Object Security.

Field	
Inherit In-product IFS authorities	**1**=No (Default) **2**=Yes - Priority is given to the higher directory security rule over more specific security rules in lower directories **3**=Yes - Priority is given to the higher directory security rule or generic file over more specific security rules in lower directories or generic files For a full explanation of how this definition works, together with examples, see Add/Modify IFS Security on page 152.
Skip activities of user or grpprf	Define up to three user or group profiles for which no firewall checking will be done. These users/groups are authorized without being checked.
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 further review).
Action for SQL that cannot be parsed	Some SQL statements may not be parsed. The following options are possible: **1**=Allow transaction (Default) **2**=Allow transaction and write an unparsed SQL statement to the special extended log **5**=Reject transaction **6**=Reject transaction and write an unparsed SQL statement to the special extended log
Log iSecurity internal/GUI activity	**N**=No (Default) **Y**=Yes
Check FTP Logon PWD by product	**N**=No (Default) - The request might be rejected due to other reasons before ensuring that the password is valid **Y**=Yes (not recommended) - 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.

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 **82 > 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**.

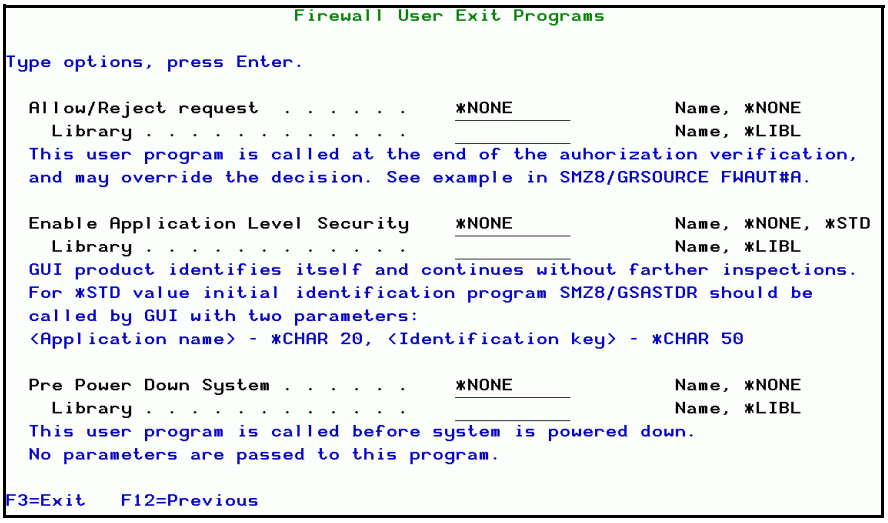


Figure 11-4. Firewall User Exit Programs Screen

Field	
Allow/Reject Request	After Firewall determines an action as legitimate or unauthorized, it can perform an additional check, which can override the first decision. **Name** = name of user exit program ***NONE***= do not call any program. (Use this option when there is no exit program) ***LIBL** = library where program is located
Enable Application Level Security	***STD** = application security will be checked by the standard iSecurity Firewall program SMZ8/GSASTDR. To activate the Application Security feature, ensure that this field has ***STD** definition **Name** = name of custom-made application security program ***NONE** = no application security check
Pre- Power Down System	If you want to call a program before "power down" (shutting down the System i), you must do it here. **Name** = name of user exit program ***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 Working with Server Security Rules on page 53).

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.

These Data Queues enable users to bind Firewall with external products such as pager systems. These Data Queues are formatted according to the log file SMZ8/GSCALP and should be created by means of the CRTDTAQ command with a length similar or greater than the log file SMZ8/GSCALP size.

1. To use Transaction Post Processing, select **82 > 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 formatted according to the log file SMZ8/GSCALP
    and should be created by means of the CRTDTAQ command with a length
    similar or greater than the log file SMZ8/GSCALP size.

F3=Exit    F12=Previous
```

Figure 11-5. Firewall Transaction Post-Processing Data Queues Screen

Field	
Post Processing Data Queues:	
Accepted Transactions	Name, Library
Rejected Transactions	Name, Library

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 **82 > 5. Intrusion Detection** from the **iSecurity (part I) Global Parameters** screen. The **Firewall Intrusion Detection** screen appears.
2. Set correct parameters and press **Enter**.

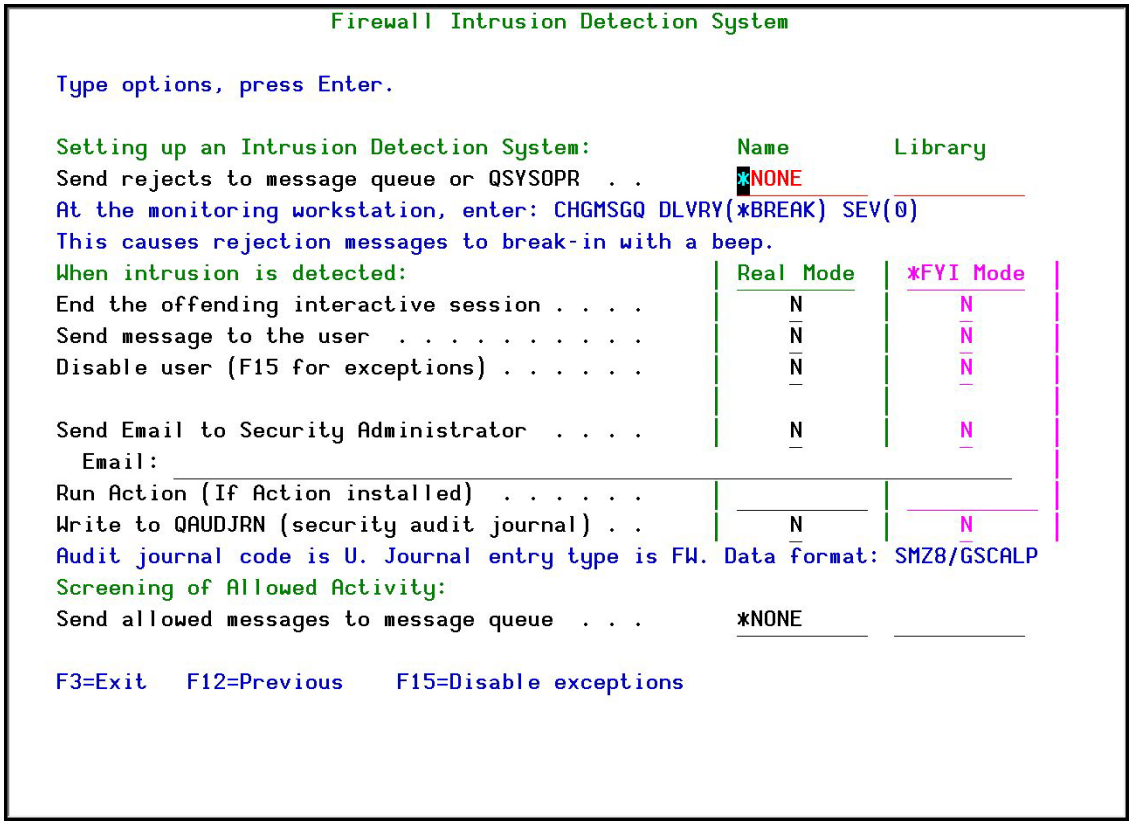


Figure 11-6. Firewall Intrusion Detection System Screen

Field	
Setting up an Intrusion Detection System:	
Send rejects to message queue or QSYSOPR	At the monitoring workstation, enter: CHGMSGQ DLVRY(*BREAK) SEV(0)This causes rejection messages to break-in with a beep.
Name	The name of the message queue to receive the intrusion messages
Library	The library for the message queue
When intrusion is detected:	For Real Mode and *FYI Mode
End the offending interactive session	**Y; N**
Send message to the user	**Y; N**
Disable user (F15 for exceptions)	**Y; N** If you enter **Y** for this parameter, you can press F15 to set up a list of users who should **NOT** be disabled
Send Email to Security Administrator	**Y,** then type Email**; N.**
Run Action (If Action installed)	**Y; N**

Field	
Write to QAUDJRN (security audit journal)	**Y; N** Audit journal code is U. Journal entry type is FW. Data format: SMZ8/GSCALP
Screening of Allowed Activity:	
Send allowed messages to message queue	Enter the name and library of the message queue to be screened.

Function Keys	
F15=Disable exceptions	Specify users that should never be disabled automatically, even if they have not signed on for a long period of time (inactive user).

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 **82 > 6. Password Exit Programs** from the **iSecurity (part I) Global Parameters** screen.
2. Set correct parameters and press **Enter**.

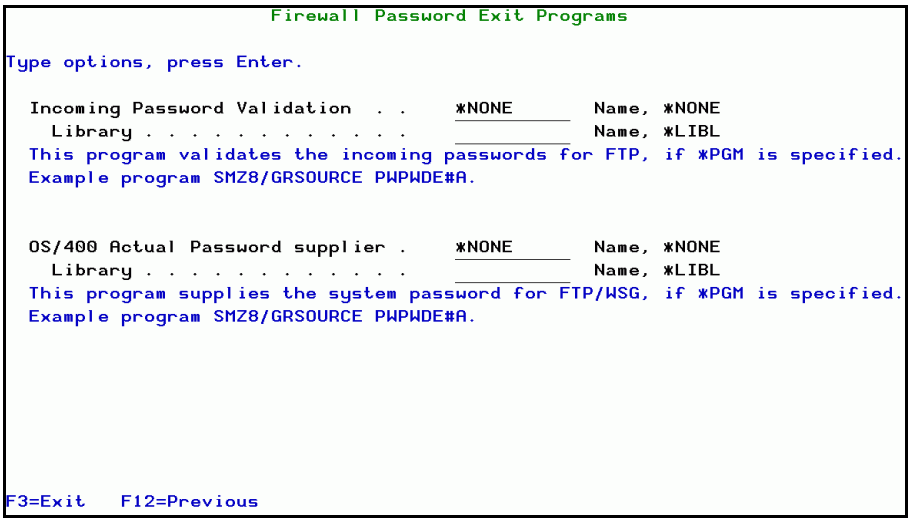


Figure 11-7. Firewall Password Exit Programs Screen

Enable ACTION (CL Script + More)

Real-time detection allows Action to react automatically to security events generated by Firewall and Screen. When enabled, these events are checked against predefined rules, which trigger alert messages and/or command scripts.

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 **82 > 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.

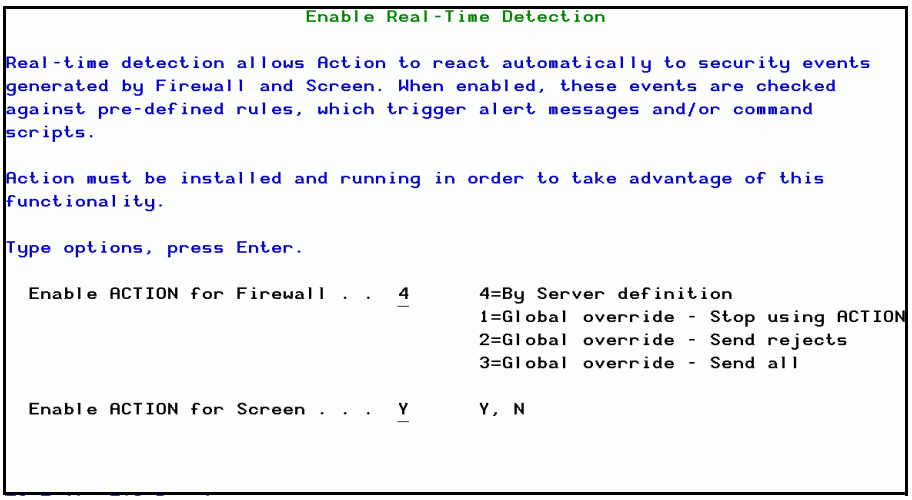


Figure 11-8. Enable Real-Time Detection Screen

Field	
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)

3. Select **1. Activation and Server Setting** from the Firewall main menu. The Activation and Server Setting menu opens.
4. Select **1. Work with Servers**.

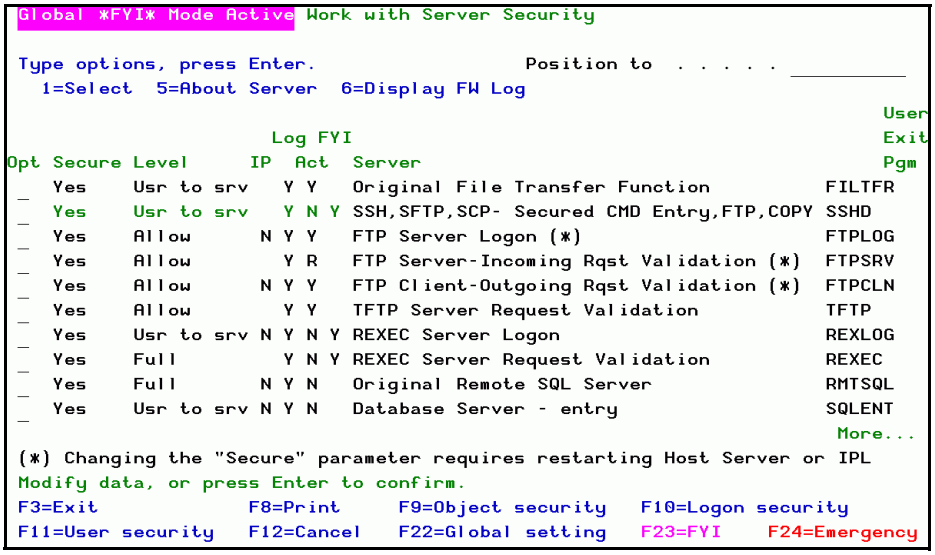


Figure 11-9. Work with Server Security Screen

Field	Description
Opt	**1** = Select a rule for modification. The **Modify Server Security** screen appears **5** = View a description of the server **6** = View the Activity Log for the server
Secure	***YES** = Secured ***NO** = Not secured
Level	This option is not available for exit points that deal with specific operations (such as Change User Profile and Pre-Power Down System) **1** = Allow all activity (available for all other exit points) **2** = Reject all activity (available for all other exit points) **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 Signon) **9** = Full security - differs in logon and user-to-object. **Logon** activates the logon limitation rules (user to system name, IP and user name). **User-to-object** activates your user limitation rules.
IP	Shows if the incoming IP address is being filtered,
Log FYI FW, Action	Shows if FYI mode is currently being logged for Firewall and Action
Server	Name/description of server
User Exit Pgm	Name of custom user exit program for this server

Function Keys	Description
F8=Print	Print all server security rules
F9=Object security	Work with object security rules
F10=Logon security	Work with logon security rules
F11=User security	Work with user-to-service security rules

Function Keys	Description
F22=Global setting	Define server security rules globally for predefined groups of servers or for all servers
F23=FYI	Enable or disable the FYI simulation mode globally for all servers
F24=Emergency	Use the Emergency Override feature

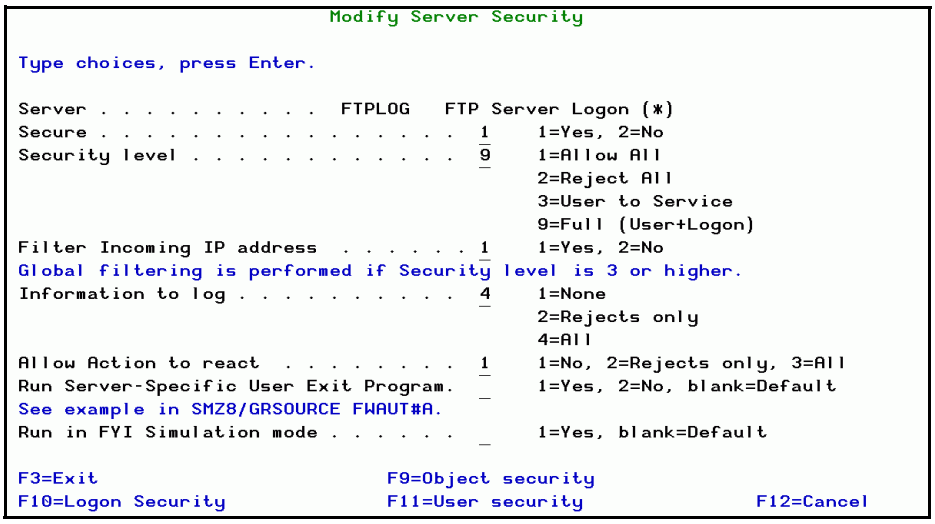


Figure 11-10. Modify Server Security Screen

Field	Description / Options
Server	Server name
Secure	***YES** = Secured ***NO** = Not secured
Security Level	This option is not available for exit points that deal with specific operations (such as Change User Profile and Pre-Power Down System) **1** = Allow all activity (available for all other exit points) **2** = Reject all activity (available for all other exit points) **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) **9** = Full security - differs in logon and user-to-object. Logon activates the logon limitation rules (user to system name, IP and user name). User-to-object activates your user limitation rules.
Information to Log	**1** = Do not log any activity **2** = Log rejected transactions only **4** = Log all activity
Allow Action to React	**1** = No (disables the Firewall real-time detection rules for this server **2** = Rejects only (will activate Firewall real-time detection rules only on rejections from this server) **3** = All (will activate Firewall real-time detection rules for all accesses from this server)

Field	Description / Options
Run Server-Specific User Exit	**1** = Yes. Run a specific exit program after passing Firewall rules for this server. The program **SMZTMPA/UP*yyyyyy*** will be called. (***yyyyyy*** is the server short name). Write your own **SMZTMPA/UP*yyyyyy*** program according to the example in SMZ8/GRSOURCE FWAUT#A. The program that initiates the call is GRCLUER. 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 SMZTMPA/UPyyyyyy If the program SMZTMPA/UPyyyyyy is not accessible, the regular security applies. **2** = No. If there is a general exit program configured, it will not be activated for this server. <*blank*> = global setting
Run in FYI Simulation Mode1	**1** = Enable FYI Simulation mode for this server only <<*blank*>> = Use global parameter for all servers (System Configuration)

Function Keys	
F8=Print	Print user-to-service security rules.
F9=Object security	Work with Object security rules.
F10=Logon security	Work with Logon security rules.
F11=User security	Work with User security rules.

5. Choose a server and select option **1** from the **Modify Server Security** screen.
6. Choose desired option from the **Allow Action to React** field and press **Enter**.

Log Retention

Log Retention allows you to define for how many days you want to keep the Firewall log and if you want to run a backup program before the logs are deleted A standard backup program is provided: SMZ8/ BRSOURCE GSLOGBKP.

The job **GS#MNT** is used to delete the logs after the number of retention days has been reached. The job is placed in the job scheduler and runs at a specific time.

To define log retention:

1. Select **81 > 9. Log Retention** from the **iSecurity (part I) Global Parameters** screen. The **Log & Journal Retention** screen appears.

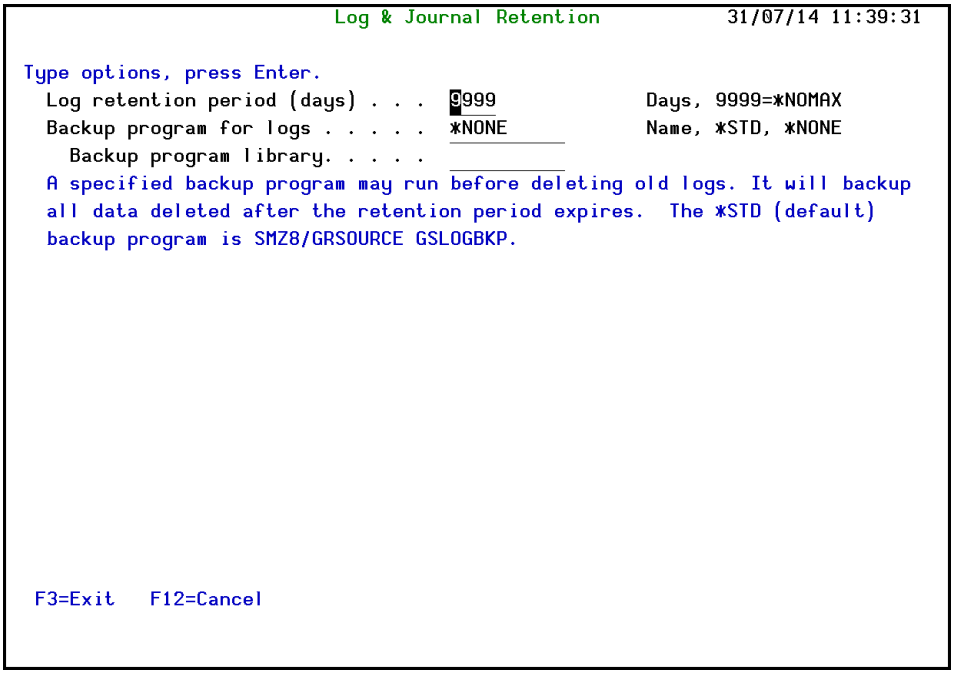


Figure 11-11. Log & Journal Retention Screen

2. Select the correct options according to the following table.

Field	Description / Options
Log retention period (days)	Days. 9999=*NOMAX
Backup program for logs	The backup program to be run before the logs are deleted
Backup program library	The library where the backup program is situated.

Exit Point Settings: DBOPEN and SQL

Raz-Lee Security's Firewall network access solution is a product that works on Exit Points. These exit points are part of the operating system, and receive control as part of the normal processing of network access operations. Business logic in the exit point decides whether to accept or reject these network access operations. At times, operating system settings provide the system with directives of how to treat FTP application messages.

The SQL exit point is one of the more than 55 exit points in the system. This exit point usually receives sentences from external references. Other exit points control network access via ODBC or JDBC which assist in accessing data-bases on other systems. When the SQL Exit Point is initiated, based upon pre-defined settings, Firewall decides whether or not to authorize the network access request. For this purpose we need to know if the function is a Create, Delete or Build function of an index or a Select function; we also need to investigate which table is required.

SQL statements normally include numerous tables and files. The challenge with SQL is to be able to isolate the names of the files by parsing the SQL statement. Because SQL syntax is very complicated, much CPU time is expended in parsing while resulting accuracy is at question. This, in spite of the use of formal languages of properties of data called BNF and of other application plug-ins that know how to parse these other applications, called Yak and Bison. Another consideration is the need to stay current with IBM's operating system versions.

Beginning in OS release 7.1, IBM added an Exit Point called DBOPEN that calls programs after IBM parsing. This means is that if someone sent an SQL statement containing a syntax error, the parser should detect the parsing error so that DBOPEN will not be called.

DBOPEN is different from the SQL exit point in many respects and works on all Open operations. It also parses the list of files as written in the SQL statement including the file name and the physical file name, by the IO name or table. DBOPEN works on both SQL Opens and on Traditional IO, those that are internal to the system and the external ones.

DBOPEN encompasses much more functionality than the SQL Exit Point and saves the extraneous parsing of the SQL Exit Point. On the other hand, SQL Exit Points detect numerous items that DBOPEN doesn't, such as Create Scheme/Library or Operations.

Using Firewall option **1 > 2** provides an extensive set of parameters to properly define DBOPEN and SQL Exit Points.

To define the exit point settings:

1. Select **1 > 2. Setting DB-OPEN and SQL** from the **Activation and Server Setting** menu. The **Setting DB-OPEN and SQL** screen appears.

NOTE: Recommended values appear in pink.

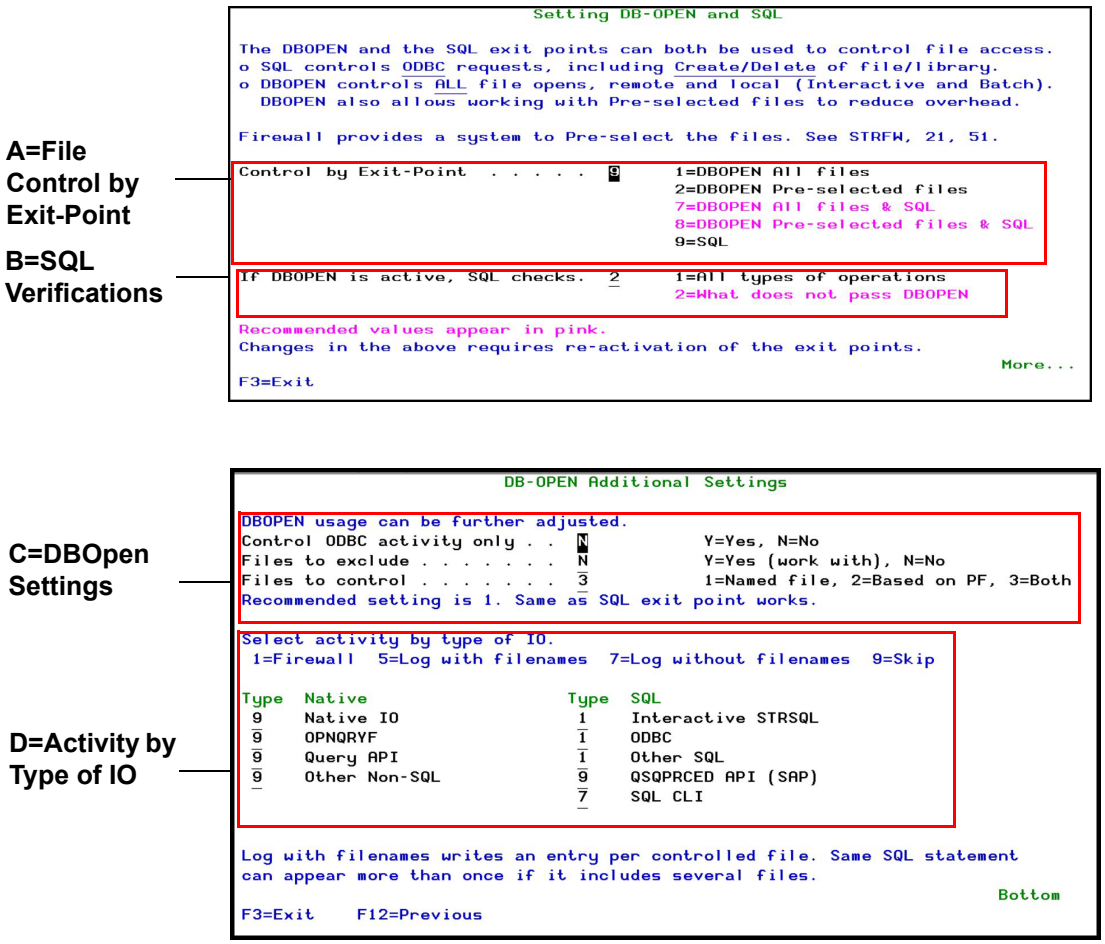


Figure 11-12. Firewall DBOPEN / SQL Exit Point Setting Screens

2. Select the correct options according to the following table:

Field	Description / Options
A=Control by Exit-Point	Firewall provides a system to Pre-select the files. See STRFW, 21, 51. **1=DBOPEN All files**. All files are indiscriminately parsed. **2=DBOPEN Pre-Selected files**. Only files that were marked will be audited; The markings are implemented by changing the Audit status from *NONE to *Read or *Change. Certain files are processed either SQL and/or DBOpen; **7= Both. DBOPEN All Files & SQL**. DBOpen for All files, plus SQL. Both exit points will be parsed. **8= Both. DBOPEN Pre-Selected files & SQL**. Only DBOpen marked files will be parsed. **9=SQL**; no DBOpen. **Important!** During activation of Servers, it is recommended to set security first to **N**, and then to secure **Y**. Remove the exit program and then reapply using: **STRFW > 1> 1 > Secure N > Secure Y.** **Note:** Please remember that setting SQL Server from Yes to No or visa versa, will require a restart for it to take effect.
B=SQL Verifications	If DBOpen is active, SQL checks. **1=All operations**; **2=Non DBOPEN operations**. If 7 or 8 were selected both Exit Points are selected. If 1 was selected, SQL will re-parse everything all over again (good for testing purposes), or if 2 was selected SQL will parse for operations that do not arrive at DBOpen, like, Creation of Library.
C=DBOpen Settings	**Control ODBC activity only..** **Y=Yes** **N=No** **Note: Limit to QZDASOINIT/QSQSRVR**. Should the DBOpen limit operations only for ODBC > if **Y**, the operation of DBOpen is limited only for these operations for SQL exit points. **Files to exclude....** Select specific files to exclude from the list. **Files to control.....** **1=Named file.** Can select file names to Control, in the views or tables in the sentences themselves **2=Based on PF** (on real physical tables) **3=Both**

Field	Description / Options
D=Activity by Type of IO	DBOpen works with nine (9) different IO types: Firewall enables marking each IO type with an Activity: **1=Firewall.** To filter in Firewall **5=Log with filenames.** Log of line for each file (DBOpen logs many names of files at once) **7=Log without filenames.** Log of line for each file (no file name is logged) **9=Skip**

Work with Files to Exclude in DB-OPEN

When selecting Files to Exclude Y=Yes, the Work with Files to Exclude in DB-OPEN window appears.

To define the Files to Exclude:

1. Select **1 > 2.**
2. Select Page Down.
3. In Files to Exclude, select **Y=Yes**, and press **Enter**.

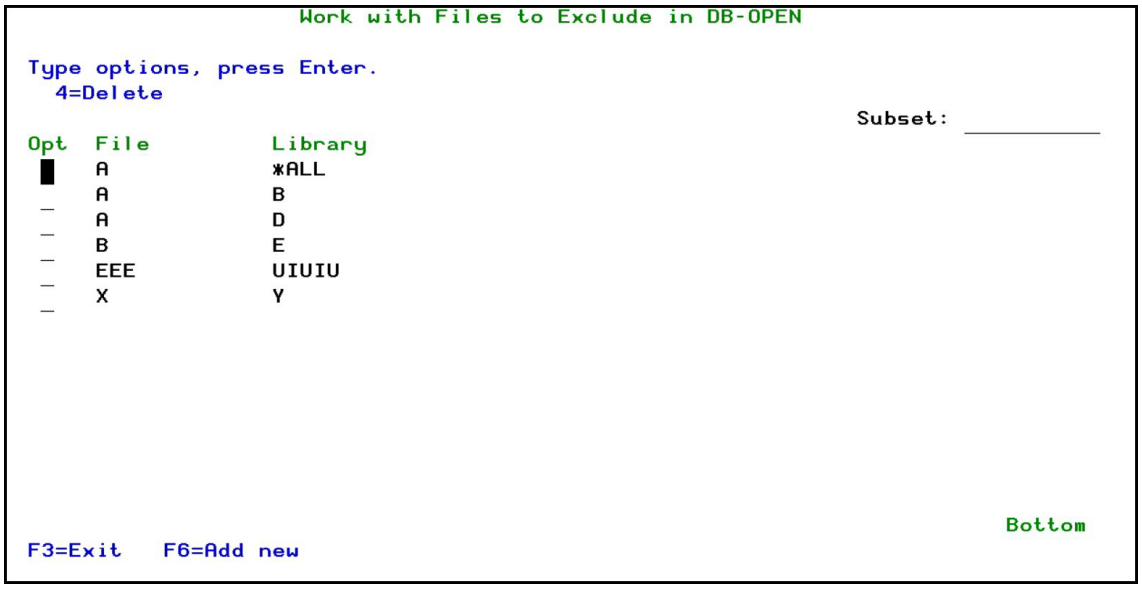


Figure 11-13. Work with Files to Exclude in DB-OPEN

Function Keys	
F3=Exit	Exit the Files to Exclude screen
F6=Add new	Add new Files to Exclude

4. Select **F6=Add New**. The Add New Files to Exclude screen appears.

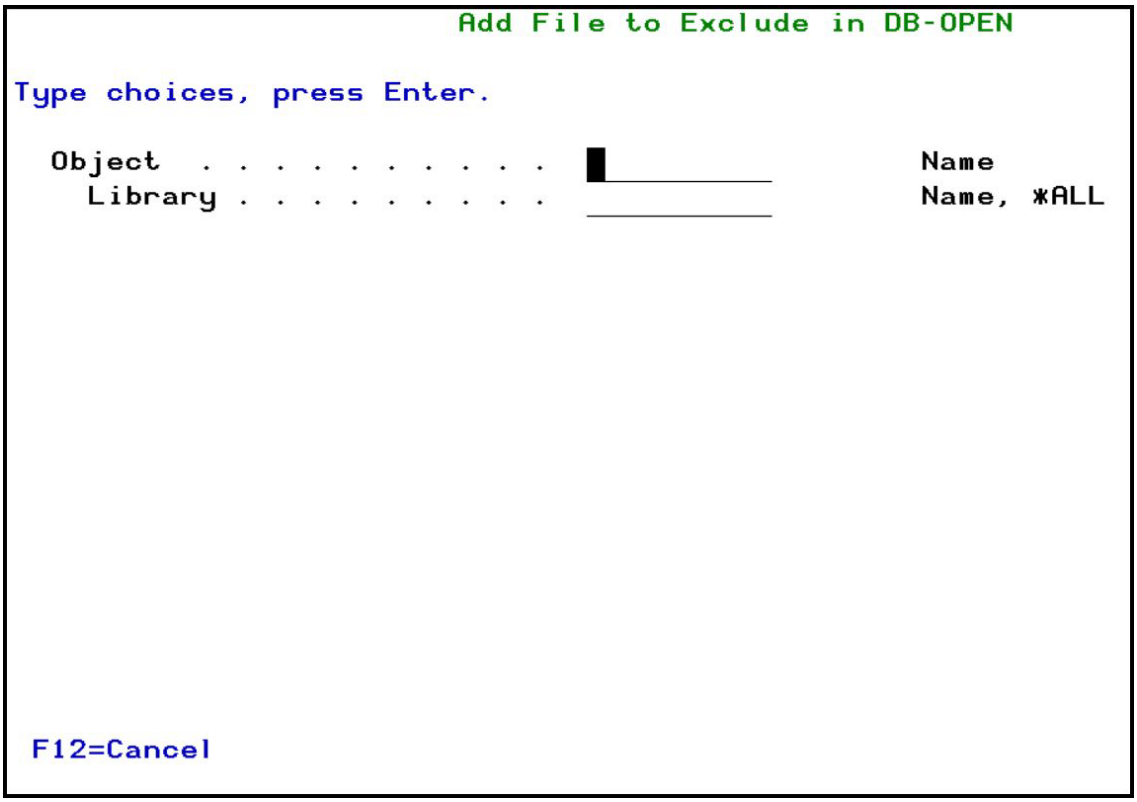


Figure 11-14. Add File to Exclude in DB-OPEN

Option	
Object	Give the name of the object to exclude
Library	Give the name of the library to exclude

Work with Database SQL Server Jobs

QZDASOINIT jobs are used to serve SQL to JDBC and ODBC client applications.

1. Select **9. Work with Database SQL Server Jobs (QZDASOINIT)** from the main menu. The Work with Database SQL Server Jobs screen appears.

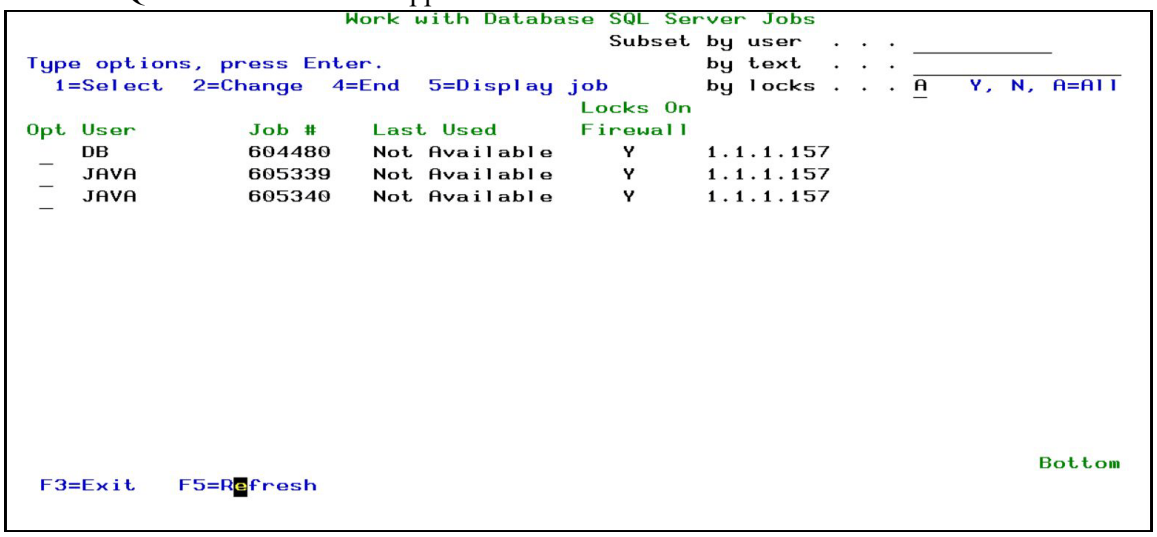


Figure 11-15. Work with Database SQL Server Jobs

Working with Screen

The **Screen** product is a complementary product to **Firewall**. The Screen options enable you to configure this product and the modes that the system can operate in, for example the amount of time between successive checks, or the number of attempts a user is allowed to correctly enter a password.

General Definitions

To configure **Screen**:

1. Select **81 > 11. General Definitions** from the **iSecurity (part I) Global Parameters** menu. The **Screen General Definitions** screen appears.

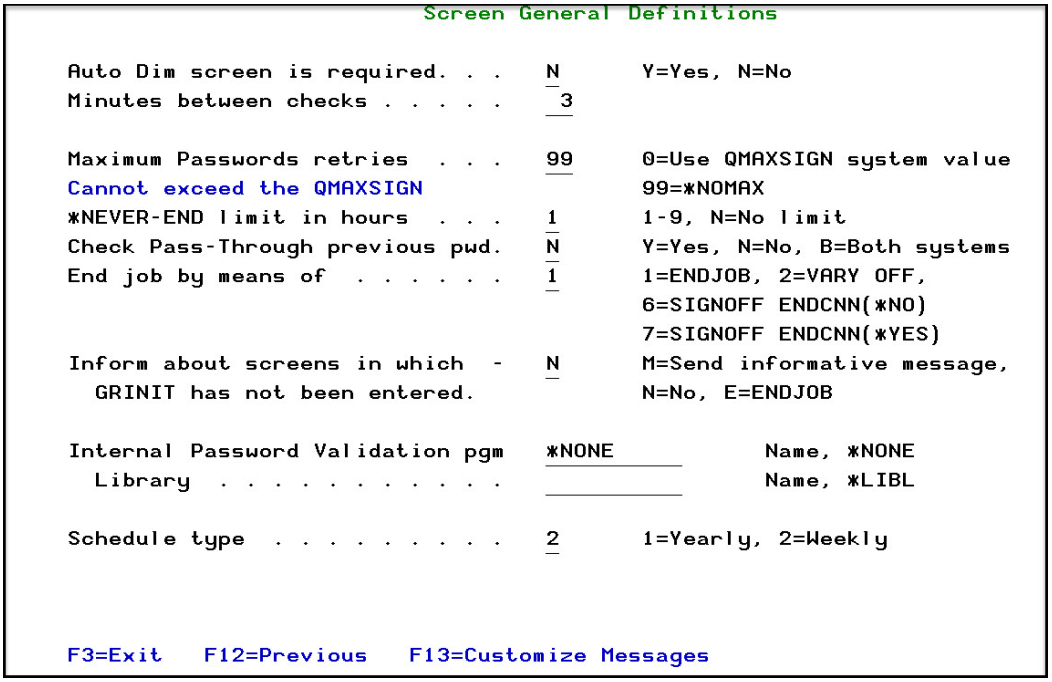


Figure 11-16. Screen General Definitions

Field	Description / Options
Automatic Dim Screen is required	**Yes** = Activate this feature **No** = Do not activate this feature If the same information is displayed on a screen for a long period of time, the characters become fixed on the screen and are visible even when the screen is not operated. The data will appear as a dark shadow even when something else is displayed on the screen. Therefore, the auto dimming option is important for workstations that do not have auto dim, such as PCs and older workstations. Workstations with auto dim, but do not use this option can also benefit from it.
Minutes between checks	Setting this option will define how many minutes will pass between successive checks. The default value is **3**.
Maximum Passwords retries	Enter the number of retries allowed before the terminal is locked. *0* = The number will be taken automatically from the system value (**QMAXSIGN**) that defines the number of trials for entering the operating system password. *99* =Unlimited number of trials (***NOMAX**) (but it cannot exceed the **QMAXSIGN** system value.

Field	Description / Options
Check Pass-Through previous pwd	Pass-Through terminals (Home to Target) are protected by **Screen** on the Target system. The following choices are available for this setting. **Y=Yes** - The lock state can be ended if the entered password corresponds to the SIGNON Home System. **N=No** - The lock state can be ended if the entered password corresponds to the SIGNON Target System **B=both systems** - The lock state can be ended if the entered password corresponds to either the SIGNON Target System or the SIGNON Home System.
End job by means of	Select the way you wish to extend the control of terminating a job. **1=ENDJOB** - End all active jobs (this is the default) **2=VARY OFF** - End all jobs then vary off terminal **3=JLDJOB** - Hold the active job. **6=SIGNOFF ENDCNN(*NO)** - Sign off and end the connection **7=SIGNOFF ENDCNN(*YES)** - Sign off without ending the connection
Inform about screens in which GRINIT has not been entered	**M=** send informative message **N=** No
Internal Password Validation pgm and Library	There are two passwords in Screen - entered by the user and entered from the product. If the user internal security program is enabled, it will replace the user password by its own password (10 characters) and the Screen password by a system password called ***GSPASSWORD***. If the contents of ***GSPASSWORD*** are identical to the **Screen** password, the user internal security program is run; otherwise an error will occur before the end of the run. ***NONE:** No user internal security **Name:** The name of the security program ***LIBL (Library)**: Enter the library name
Schedule type	Define how you will set up your schedule **1**=Yearly **2**=Weekly

Function Keys	
F13=Customize Messages	**Screen Translation** screen

2. Enter your required options and press **Enter**.

Customize Messages

You can translate all screen messages that users see.

To translate screen messages:

1. Select **81 > 11. General Definitions** from the **iSecurity (part I) Global Parameters** menu. The **Screen General Definitions** screen appears.
2. Select **F13=Customize Messages**. The **Screen Translation** screen appears.

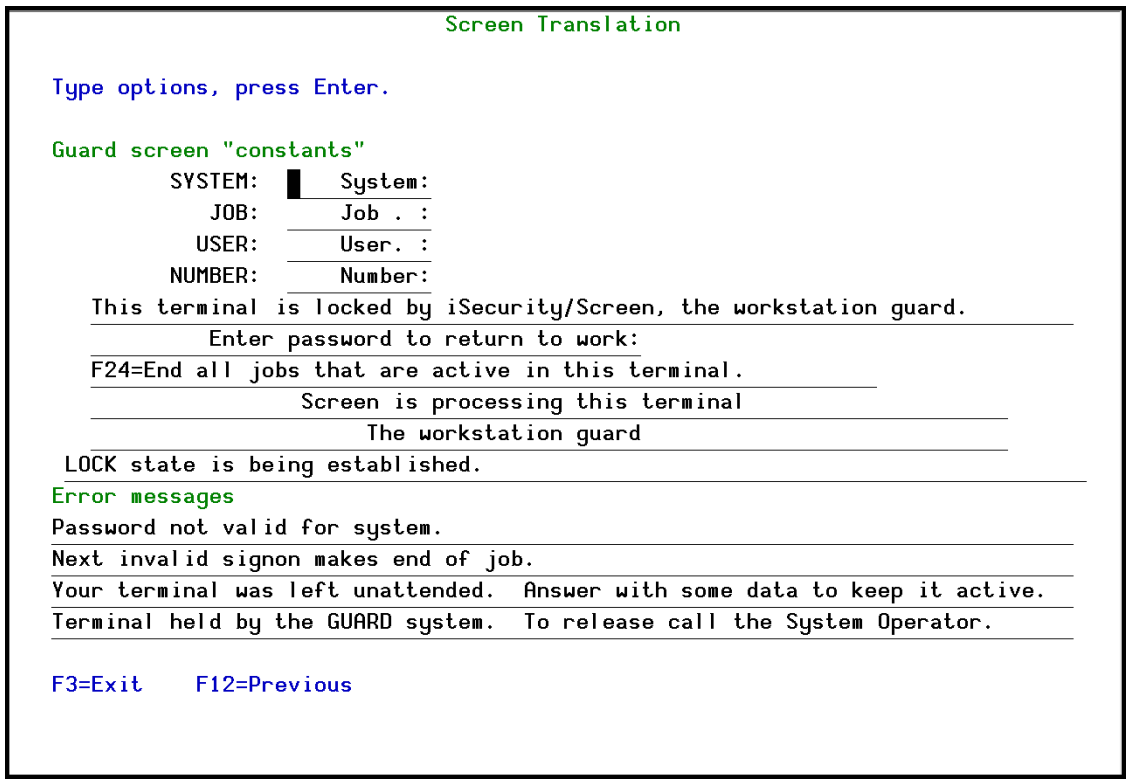


Figure 11-17. Screen Translation

3. All visible constants and messages are displayed. Overwrite them with your text, clear the field and press **Enter**.

To translate the help text, follow these procedures on the following page:

1. Create a new member in the ***GRSOURCE*** file in library ***SMZ8***.
2. Copy the original help text to the new member.
3. To translate as required without altering the control records identified by .PGM, .FMT, and so on, select *12* from the **System Configuration** menu and enter the name of the new member at the bottom of the translation panel.

Command General Definitions

This feature enables users to define the parameters for working with the **Command** product.

Command dynamically creates a custom security environment, letting users control exactly when and how individual users can execute specific commands and applications.

To define Command general definitions:

1. Select **81 > 31. General Definitions** from the **iSecurity (part I) Global Parameters** screen. The **Command General Definitions** screen appears.
2. Select options according to the following table.

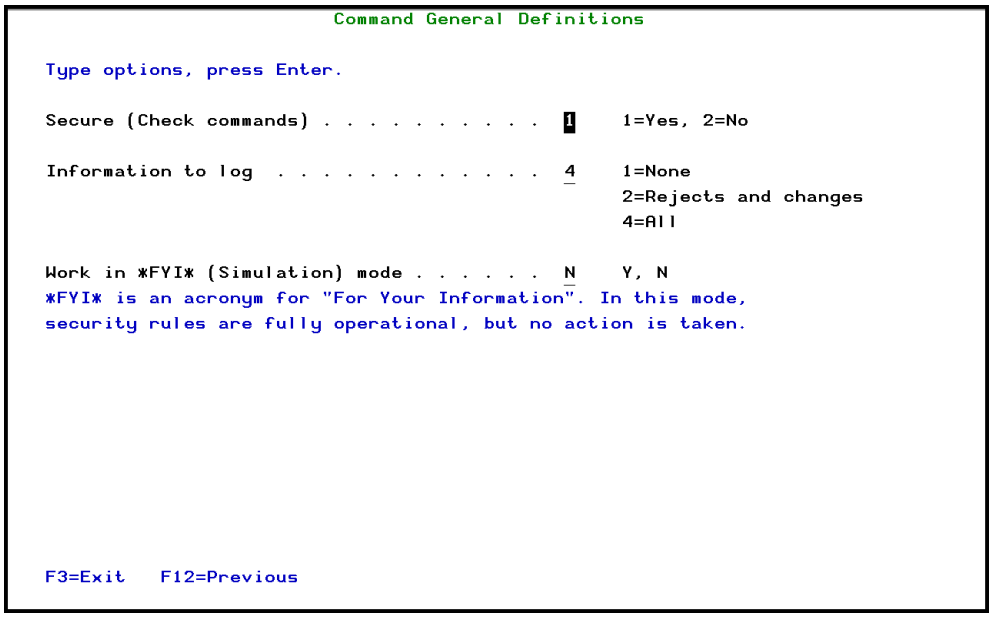


Figure 11-18. Command General Definitions Screen

Field	Description / Options
Secure (Check commands)	**1** = Yes **2** = No **9** =
Information to log	**1** = None **2** = Rejects and changes **4** = All
Work in *FYI* (Simulation) mode **In FYI mode, all security rules are checked, but no actions are taken if a breach of the rules occurs. You can use FYI mode to fine tune your rules.**	**Y**, **N**

SIEM Support

Numerous iSecurity products integrate with SEM/SIEM systems by sending security alerts instantaneously to these systems; web-based alerts are supported using Twitter www.twitter.com (can transmit up to 1000 lines per second). Message alerts contain detailed event information about application data changes, deletes or reads of objects and files, emergency changes in user authorities, IFS viruses detected, malicious network access to the Series i, and more.

Syslog Parameters

The syslog standards, LEEF and CEF send data in Field mode enabling pairs of data to be displayed, i.e. Field name and Field value. QHST, QSYSOPR and others in the message queue are supported in LEED and CEF field mode. UDP, TCP and TLS (encrypted) protocols are supported and once the settings are turned on, the SIEM can intercept the message and make it legible for the Syslog Admin. Standard message support for edited messages and replacement values exist, enabling sending information in any free format as well as LEEF and CEF.

To send syslog messages for SIEM:

1. Select **81 > 71. Main Control** in the **iSecurity/Base System Configuration** menu. The **Main Control for SIEM & DAM** screen is displayed.

```
                        Main Control for SIEM & DAM          9/05/16 10:31:11

 Send SYSLOG Messages to SIEM
 SIEM 1: syslog#1    . . . . . .     2          0=None, 1=Rejects, 2=All
 SIEM 2: Syslog#2    . . . . . .     0          0=None, 1=Rejects, 2=All
 SIEM 3: Syslog#3    . . . . . .     0          0=None, 1=Rejects, 2=All

 Send JSON messages (for DAM). .     0          0=None, 1=Rejects, 2=All
If you change the value to or from 0, you must restart the ZFIREWALL subsytem.
For this use Suspend Activity (opt. 1/21) and then Resume Activity (opt. 1/22).



 See STRAUD, 81, 39 for a stand-alone SYSLOG test (without any other system)









 Note: Re-activate subsystem after changes.
 F3=Exit    F12=Cancel
```

Figure 11-19. Main Control for SIEM & DAM

Parameter	Description
Run rules before sending	**Y** = Yes **N** = No
Send SYSLOG messages to SIEM	**Y** = Yes **N** = No **A** = Action only
Send JSON messages (for DAM)	**Y** = Yes **N** = No
As only operation	**Y** = Yes **N** = No

3. Enter the required parameters and press **Enter**.

Triple Syslog Definitions (#1-#3)

Events from IBMi, and different Audit entry types are sent to a remote SYSLOG server according to range of severities such as emergency, alert, critical, error, warning and more. When Send SYSLOG messages (for SIEM) is set to Yes in the Main Control for SIEM & DAM definitions, the product will automatically send all events according to the Severity range to auto send (list below) for the message structure selected, as described in the table below.

The option to use more than one SIEM is implemented on a separate job per SIEM. This is enabled by an intermediate buffer which assists SIEM to overcome communication problems or SIEM downtime, while sending a message to QSYSOPR when the buffer is full or processes are delayed. For this purpose Triple Syslog definitions are required, which are described in this section.

To configure SIEM message structure:

1. Select **72/73/74. SYSLOG** in the **Firewall** menu. The selected **SYSLOG Definitions** screen is displayed.

```
                          SYSLOG Definitions              9/05/16 10:34:13

SIEM 1 name . . . . . .   Syslog#1                              Port:   1468
SYSLOG type . . . . . .   2       1=UDP, 2=TCP, 3=TLS
Send if in FYI mode . .   Y       Y=Yes, N=No
Destination address . .   1.1.1.164

"Severity" range to auto send .   0 - 0  Emergency - EMERGENCY
"Facility" to use . . . . . .     22

Msg structure or *LEEF, *CEF  .   *CEF

*LEEF (IBM QRadar), *CEF (HP ArcSight) or mix variables and constants (ex & %):
&1=First level msg    &3=Msg Id.              &4=System               &5=Module
&6=IP                 &7=Service              &8=Host name            &9=User
&H=Hour               &M=Minute               &S=Second               &X=Time
&d=Day in month       &m=Month (mm)           &y=Year (yy)            &x=Date
&a/&A=Weekday (abbr/full)                     &b/&B=Month name (abbr/full)
Convert data to CCSID . . . . .       0  0=Default, 65535=No conversion
Maximum length  . . . . . .        1024  128-9800

Note: Re-activate subsystem after changes.
F3=Exit   F12=Cancel
```

Figure 11-20. SYSLOG Definitions Screen

Field	Description / Options
SIEM # name	The name of the Syslog
Port	The port the Syslog is listening to according to the SYSLOG type
SYSLOG type	**1**=UDP **2**=TCP **3**=TLS (Syslog over TLS uses port number 6514)
Send if in FYI mode	**Y** = Yes **N** = No
Destination address	Enter the destination IP address (without quotes)

Field	Description / Options
Severity range to auto send	Enter the severity range from which the SYSLOG message will be sent: **0-7 Emergency – DEBUG** Where: **0 =** EMERGENCY - EMERGENCY **1 =** EMERGENCY - ALERT **2 =** EMERGENCY - CRITICAL **3 =** EMERGENCY - ERROR **4 =** EMERGENCY - WARNING **5 =** EMERGENCY - NOTICE (SIGNIFICANT) **6 =** EMERGENCY - INFORMATIONAL **7 =** EMERGENCY - DEBUG
Facility to use	Enter the facility from which the SYSLOG message will be sent Where: **1** = USER-LEVEL MESSAGES **2** = MAIL SYSTEM **3** = SYSTEM DAEMONS **4** = SECURITY/AUTHORIZATION MESSAGES **5** = SYSLOGD INTERNAL **6** = LINE PRINTER SUBSYSTEM **7** = NETWORK NEWS SUBSYSTEM **8** = UUCP SUBSYSTEM **9** = CLOCK DAEMON **10** = SECURITY/AUTHORIZATION MESSAGES **11** = FTP DAEMON **12** = NTP SUBSYSTEM **13** = LOG AUDIT **14** = LOG ALERT **15** = CLOCK DAEMON **16** = LOCAL USE 0 (LOCAL0) **17** = LOCAL USE 1 (LOCAL1) **18** = LOCAL USE 2 (LOCAL2) **19** = LOCAL USE 3 (LOCAL3) **20** = LOCAL USE 4 (LOCAL4) **21** = LOCAL USE 5 (LOCAL5) **22** = LOCAL USE 6 (LOCAL6) **23** = LOCAL USE 7 (LOCAL7)
Message structure	Two built-in message structures are available: ***LEEF** = Log Event Extended Format ***CEF** = Common Event Format **-Or-** Use mixed variables and constants (ex & %) (see SIEM Support). A full description of the available variables is in the table below.
Convert data to CCSID	**0** = Default **65535** = No conversion
Maximum length	128 - 9800

Variable	Description
&a	Abbreviated name of the day of the week (Sun, Mon, and so on)
&A	Full name of the day of the week (Sunday, Monday, and so on)
&b	Abbreviated month name (Jan, Feb, and so on)
&B	Full month name (January, February, and so on)
&c	Date/Time in the format of the locale
&C	Century number [00-99], the year divided by 100 and truncated to an integer
&d	Day of the month [01-31]
&D	Date Format, same as &m/&d/&y
&e	Same as &d, except single digit is preceded by a space [1-31].
&g	2 digit year portion of ISO week date [00,99]
&G	4 digit year portion of ISO week date. Can be negative
&h	Same as &b
&H	Hour in 24-hour format [00-23]
&I	Hour in 12-hour format [01-12]
&j	Day of the year [001-366]
&L	Three digit milliseconds part of event time
&m	Month [01-12]
&M	Minute [00-59]
&n	Newline character
&O	UTC offset. Output is a string with format +HH:MM or –HH:MM, where + indicates east of GMT, - indicates west of GMT, HH indicates the number of hours from GMT, and MM indicates the number of minutes from GMT
&p	AM or PM string
&r	Time in AM/PM format of the locale. If not available in the locale time format, defaults to the POSIX time AM/PM format: &I:&M:&S &p
&R	24-hour time format without seconds, same as &H:&M
&S	Second [00-61]. The range for seconds allows for a leap second and a double leap second
&t	Tab character
&T	24-hour time format with seconds, same as &H:&M:&S
&u	Weekday [1,7]. Monday is 1 and Sunday is 7
&U	Week number of the year [00-53]. Sunday is the first day of the week
&V	ISO week number of the year [01-53]. Monday is the first day of the week. If the week containing January 1st has four or more days in the new year then it is considered week 1. Otherwise, it is the last week of the previous year, and the next year is week 1 of the new year
&w	Weekday [0,6], Sunday is 0
&W	Week number of the year [00-53]. Monday is the first day of the week

Variable	Description
&x	Date in the format of the locale
&X	Time in the format of the locale
&y	2 digit year [00,99]
&Y	4-digit year. Can be negative
&z	UTC offset. Output is a string with format +HHMM or -HHMM, where + indicates east of GMT, - indicates west of GMT, HH indicates the number of hours from GMT, and MM indicates the number of minutes from GMT
&Z	Time zone name
&1	The first level message
&3	The ID of the first level mess
&4	The name of the system where the event took place
&5	The two character RazLee product code
&6	Prod ID
&7	Service
&8	The IP address of the system where the event took place
&9	The user ID for the event

4. Enter the required parameters and press **Enter**.

SYSLFC - SYSLOG FACILITY:

1 = USER-LEVEL MESSAGES

2 = MAIL SYSTEM

3 = SYSTEM DAEMONS

4 = SECURITY/AUTHORIZATION MESSAGES

5 = SYSLOGD INTERNAL

6 = LINE PRINTER SUBSYSTEM

7 = NETWORK NEWS SUBSYSTEM

8 = UUCP SUBSYSTEM

9 = CLOCK DAEMON

10 = SECURITY/AUTHORIZATION MESSAGES

11 = FTP DAEMON

12 = NTP SUBSYSTEM

13 = LOG AUDIT

14 = LOG ALERT

15 = CLOCK DAEMON

16 = LOCAL USE 0 (LOCAL0)

17 = LOCAL USE 1 (LOCAL1)

18 = LOCAL USE 2 (LOCAL2)

19 = LOCAL USE 3 (LOCAL3)

20 = LOCAL USE 4 (LOCAL4)

21 = LOCAL USE 5 (LOCAL5)

22 = LOCAL USE 6 (LOCAL6)

23 = LOCAL USE 7 (LOCAL7)

**SYSLSV - SYSLOG SEVERITY:

0 = EMERGENCY - EMERGENCY

1 = EMERGENCY - ALERT

2 = EMERGENCY - CRITICAL

3 = EMERGENCY - ERROR

4 = EMERGENCY - WARNING

5 = EMERGENCY - NOTICE (SIGNIFICANT)

6 = EMERGENCY - INFORMATIONAL

7 = EMERGENCY - DEBUG

To prompt and receive alerts, define an **Alert Message** in **Action** **(STRACT → 31. Work with Actions).**

JSON Definitions

Use JSON to send events to the DB-OPEN exit point.

1. Select **81 > 75. JSON**. The **JSON Definitions** screen appears.

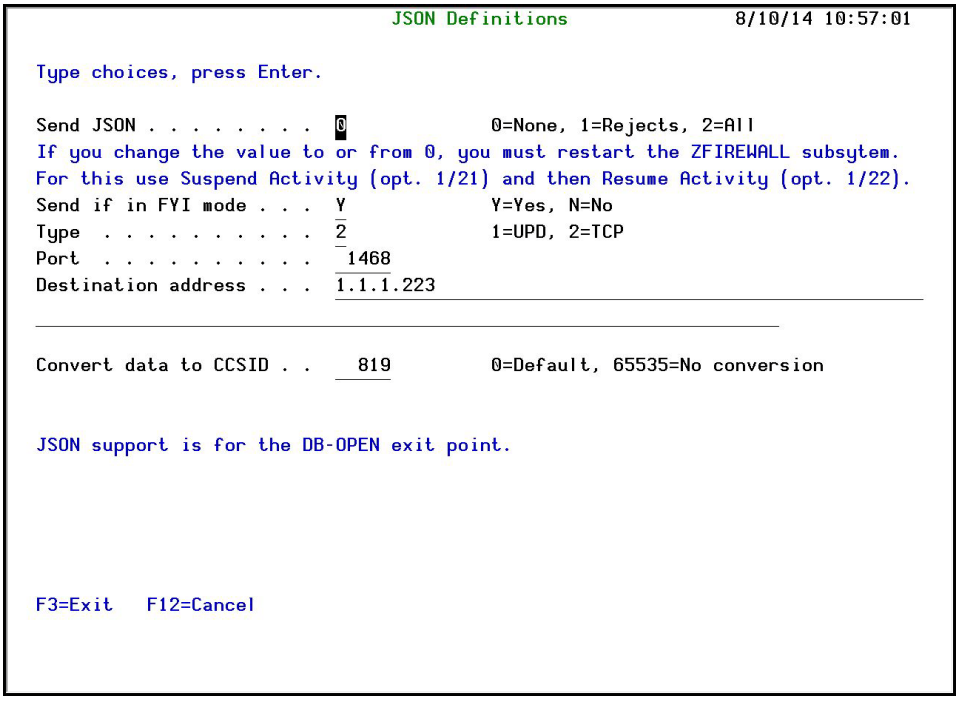


Figure 11-21. JSON Definitions Screen

Field	Description / Options
Send JSON	**0**=None **1**=Rejects **2**=All If you change the value to or from 0, you must restart the ZFIREWALL subsytem. To do this, use Suspend Activity (opt. 1/21) and then Resume Activity (opt. 1/22).
Send if in FYI mode	**Y**=Yes **N**=No
Type	**1**=UPD **2**=TCP
Port	Enter the JSON port
Destination address	Enter the destination IP address
Convert data to CCSID	**0** = Default **65535** = No conversion

2. Enter your required parameters and press **Enter**.

Language Support

The Double-Byte Character Set (DBCS) is a character 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 options: the default setting of **N** (do not support DBCS), and **Y** (support DBCS). Choose an option based on the relevant national language.

To work with iSecurity Language Support:

1. Select **81 > 91. Language Support**. The **iSecurity Language Support** screen is displayed.
2. Set your desired parameter and press **Enter**.

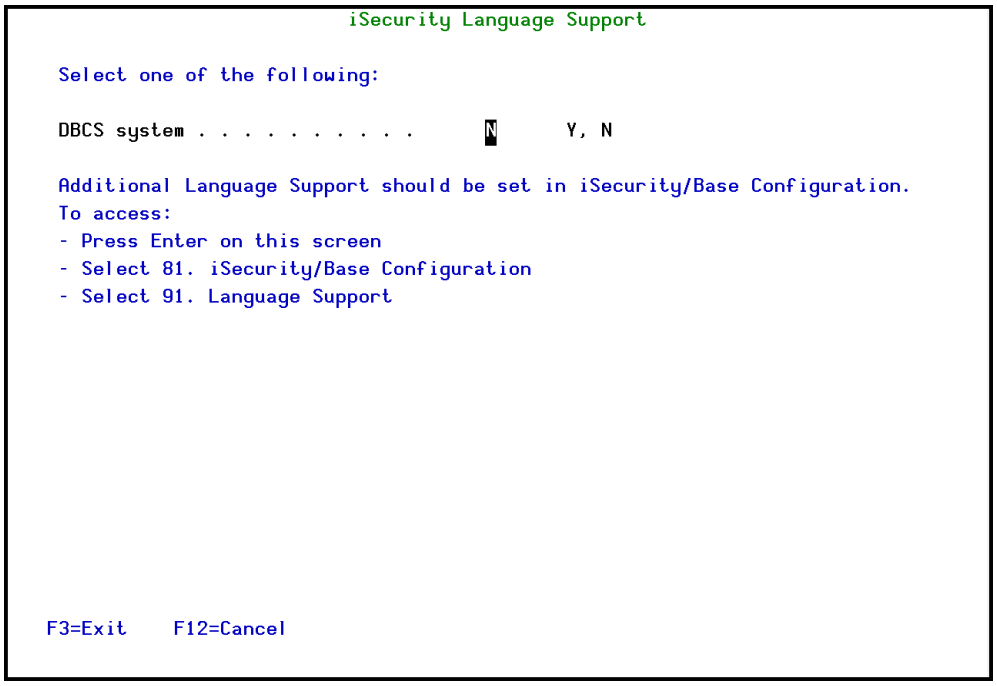
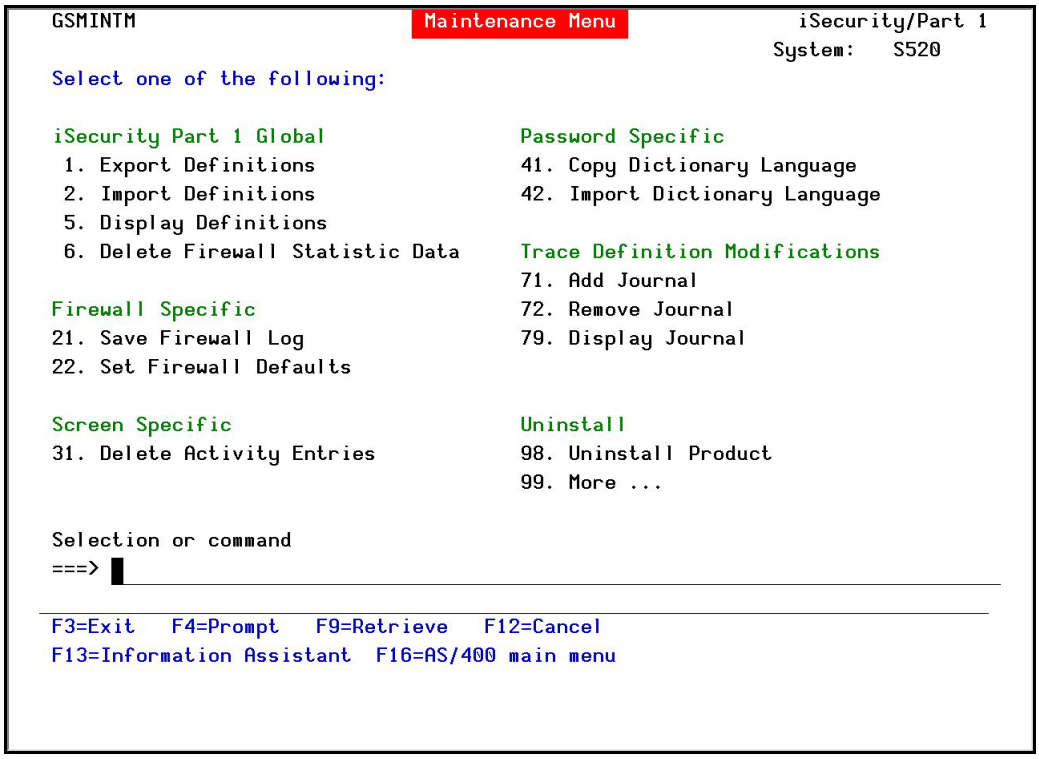


Figure 11-22. iSecurity Language Support Screen

For additional language support, use **81. iSecurity/Base Configuration** in the **iSecurity (part I) Global Parameters** screen.

System Maintenance

The **Maintenance Menu** enables the user to set and display global definitions for iSecurity Part 1. To access the **Maintenance** Menu, select **82. Maintenance Menu** from the Firewall main menu.



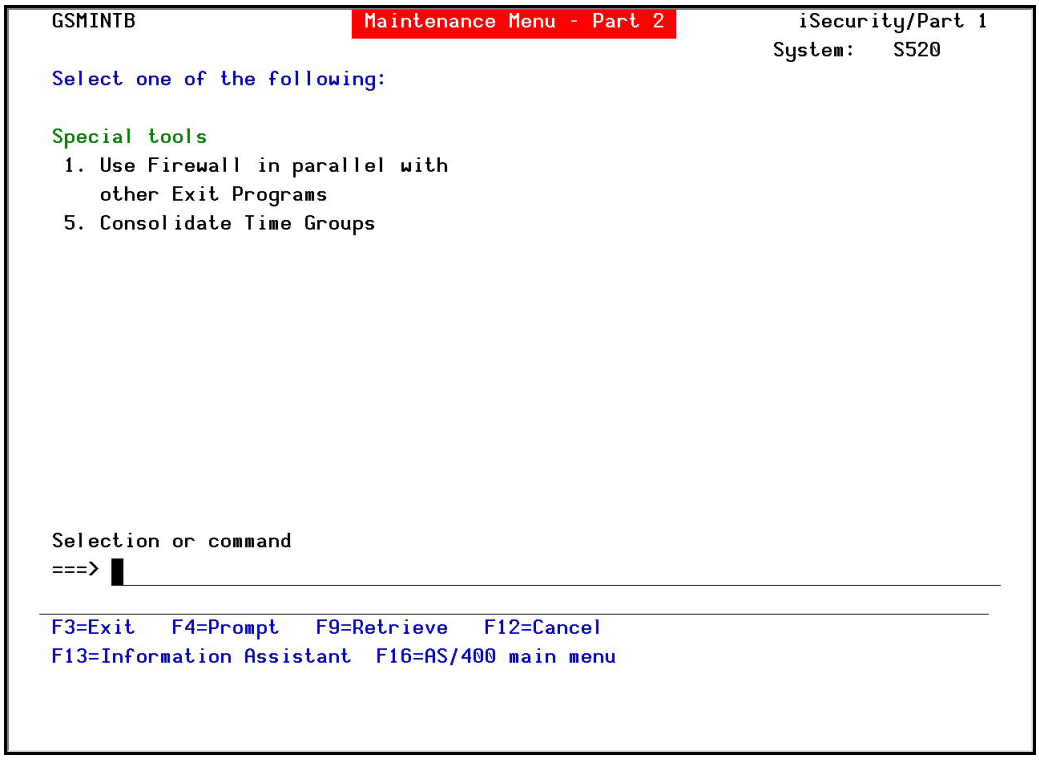


Figure 11-23. Maintenance Menus

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 can export/import: IP addresses, System names (SNA), Users, Groups, Applicant, Locate, Native and IFS, Logon controls for FTP-TELNET-Passthrough, Prechecks for DDM-DRDA, Time Groups and so on.

To configure for export:

1. Select **82 > 1. Export Definitions** from the **Maintenance** menu.

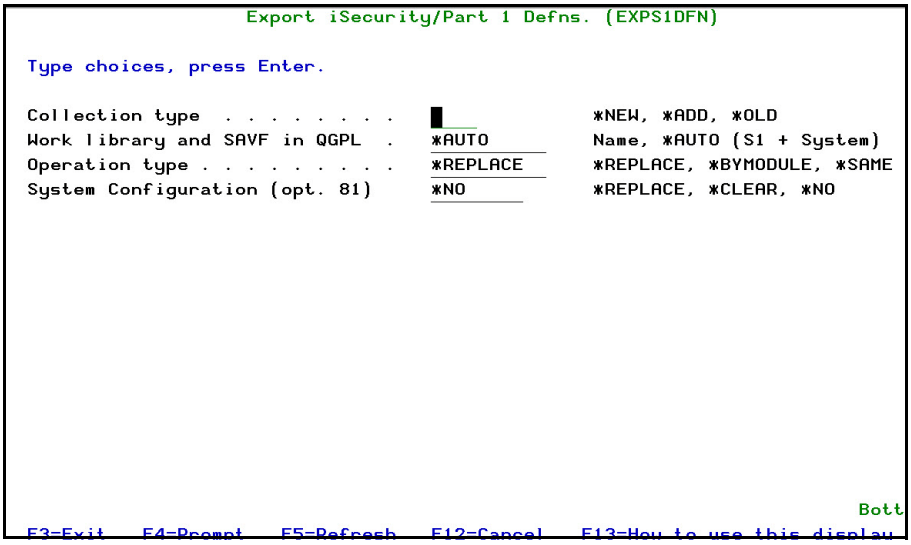


Figure 11-24. Export iSec Part 1 Definitions (EXPS1DFN)

To configure for import:

1. Select **82 > 2. Import Definitions** from the **Maintenance** menu.

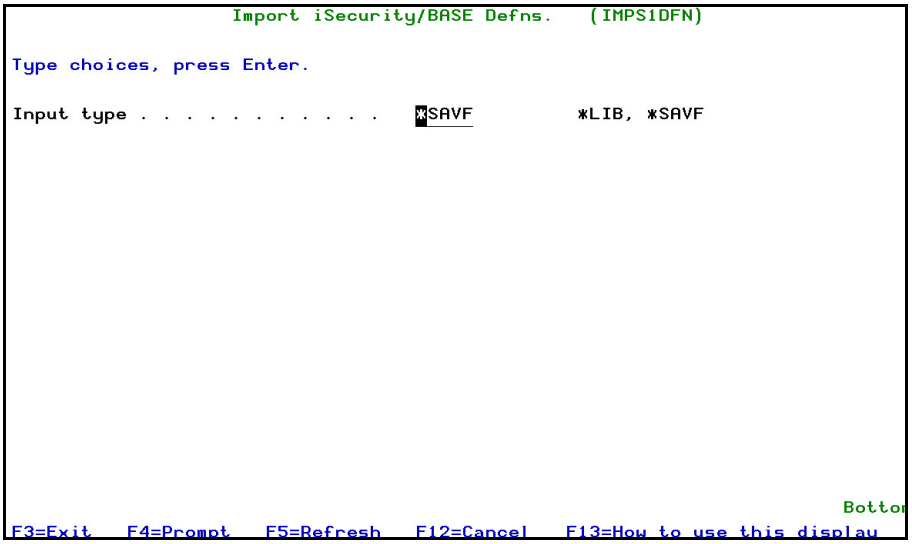


Figure 11-25. Import iSec Part 1 Definitions (IMPS1DFN)

Field	
Input type	***SAVF** or ***LIB**

Function Keys	
F4=Prompt	Opens a prompt screen to select 1 or more definitions.

Save Secure Status

This feature enables the user to save, suspend or resume initial global settings.

1. Select **82 > 4. Save Secure Status.** The **Save Secure Status** screen appears.

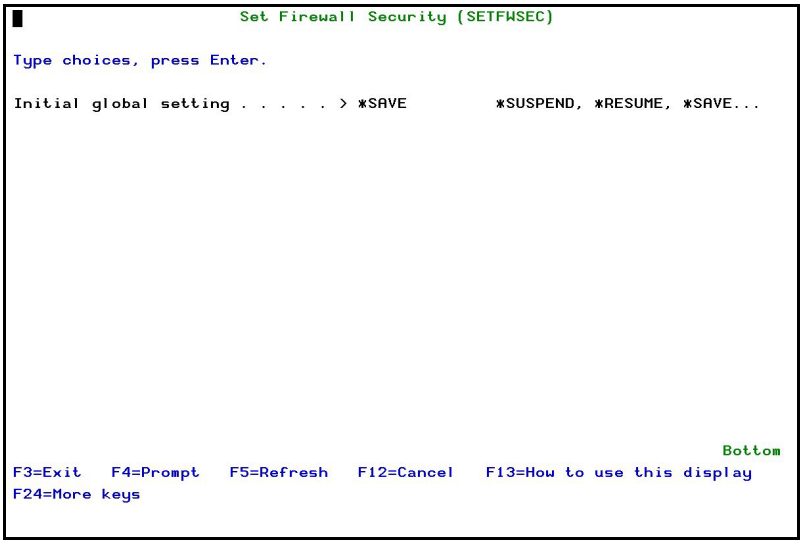


Figure 11-26. Save Secure Status Screen

Field	
Initial global setting	***SAVE** = save initial global setting for firewall ***SUSPEND** = suspend initial global setting for firewall ***RESUME** = resume initial global setting for firewall

Function Keys	
F24=More keys	Opens a prompt screen to select 1 or more definitions.
F9=All parameters	View all possible parameters on global settings screen.
F11=Keywords/Choices	View option keywords or toggle to view choices.
F14=Command string	Command line for global settings screen.
F15=Error messages	Lists pending messages
F16=Command complete	Return to Initial global settings.

2. Select the settings required and press **Enter.**

Display Definitions

This feature enables the user to display and print iSecurity Part One definitions:

1. Select **82 > 5. Display Definitions**. The **Display Security I Definitions** screen appears.

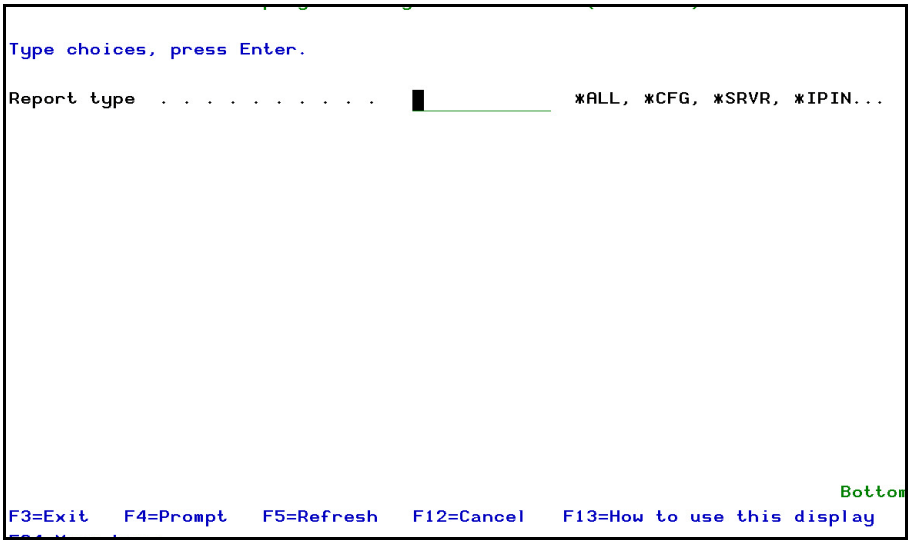


Figure 11-27. Display Security 1 Definitions Screen

Field	
Report type	***ALL** = all general definitions ***CFG** = per configuration ***SRVR** = per server ***IPIN** = per IP address

Function Keys	
F4=Prompt	Opens a prompt screen to select 1 or more definitions.

2. Select the desired report type from the **Display Security I Definitions** screen. After selecting report type, additional parameters appear.
3. Select choices and press **Enter**.

Delete Firewall Statistic Data

Statistical data that is no longer needed can be removed from the disk, saving valuable storage space. This also reduces the time taken to produce reports. However, you should ensure that this deletion is supported by a proper backup/restore policy.

1. Select **82 > 6. Delete Firewall Statistic Data** from the **Maintenance Menu**. The **Delete Firewall Statistic Data** screen appears.

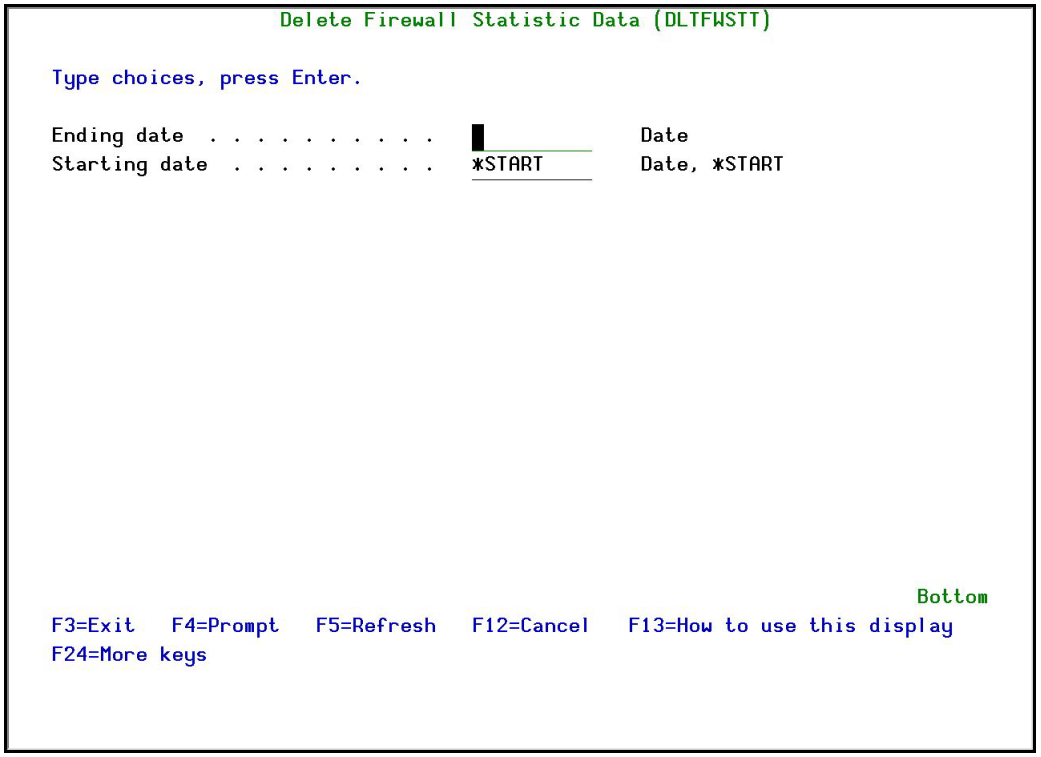


Figure 11-28. Delete Firewall Statistic Data

2. Enter the starting and ending dates of the date you want to delete and press **Enter**.

Firewall Specifics

Save Firewall Log

If you want to free up space, you can save the daily **Firewall** log in a SAVF format.

To save the Firewall log:

1. Select **82 > 21. Save Firewall Log** from the **Maintenance Menu**. The **Save iSecurity Log** screen appears.

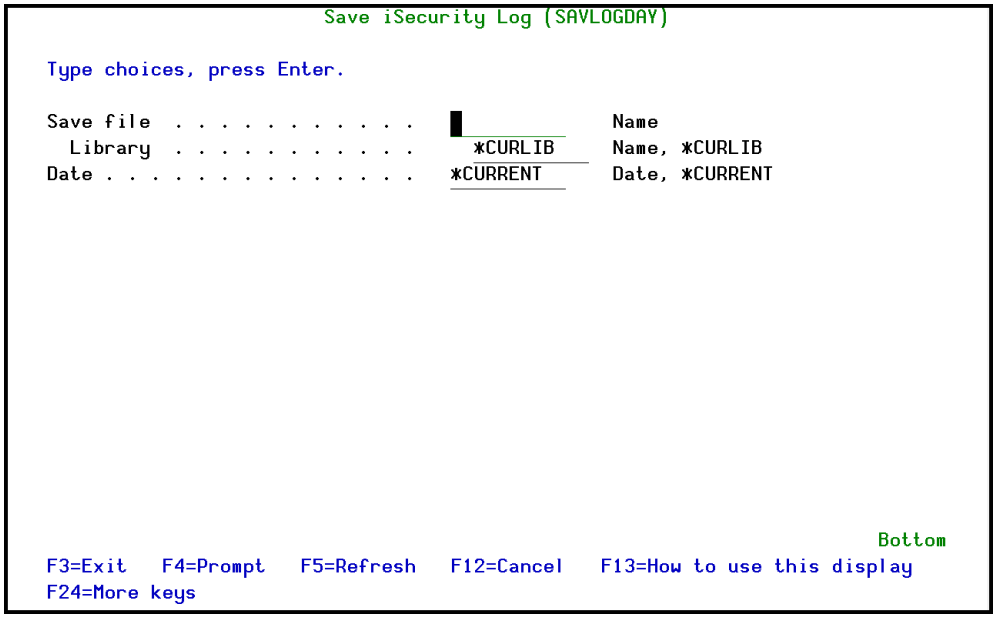


Figure 11-29. Save Firewall Log Screen

Field	
Save file	Give a meaningful name to the file
Library	Enter either a library name or ***CURLIB**
Date	Enter a specific date or enter ***CURRENT** for today's file.

Function Keys	
F4=Prompt	Opens a prompt screen to select 1 or more definitions.

2. Enter parameters as shown in the table before and press **Enter**.

Set Firewall Defaults

You can set default behavior for various Firewall parameters. The possible behaviors are described in the table below.

To set the Firewall defaults:

1. Select **82 > 22. Set Firewall Defaults** from the **Maintenance Menu**. The **Set Firewall Defaults** screen appears.
2. Enter parameters as shown in the table below and press **Enter**.

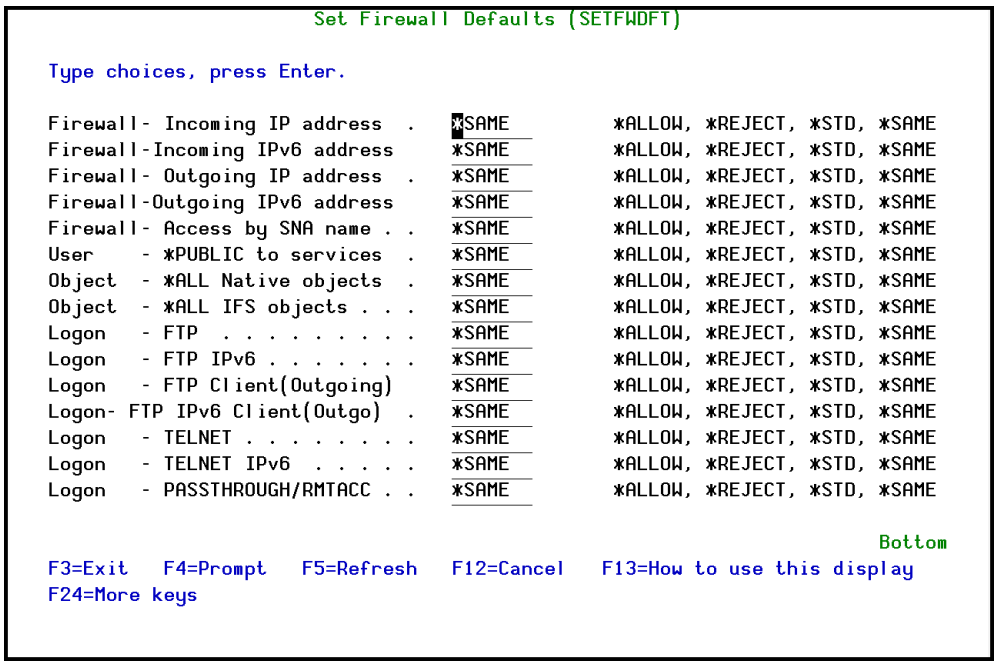


Figure 11-30. Set Firewall Defaults Screen

Field	
For each parameter, choose one of the options below	
***ALLOW**	Change this parameter so that all checks for this parameter will be allowed unless specifically defined to be rejected.
***REJECT**	Change this parameter so that all checks for this parameter will be rejected unless specifically defined to be allowed.
***SAME**	Do not change this parameter.
***STD**	Restore the behavior of this parameter to the initial installation behavior (factory defaults).

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 **89 > 51. Work with Collected Data** from the **Base Support** menu. The **Work with Collected Data** screen appears.

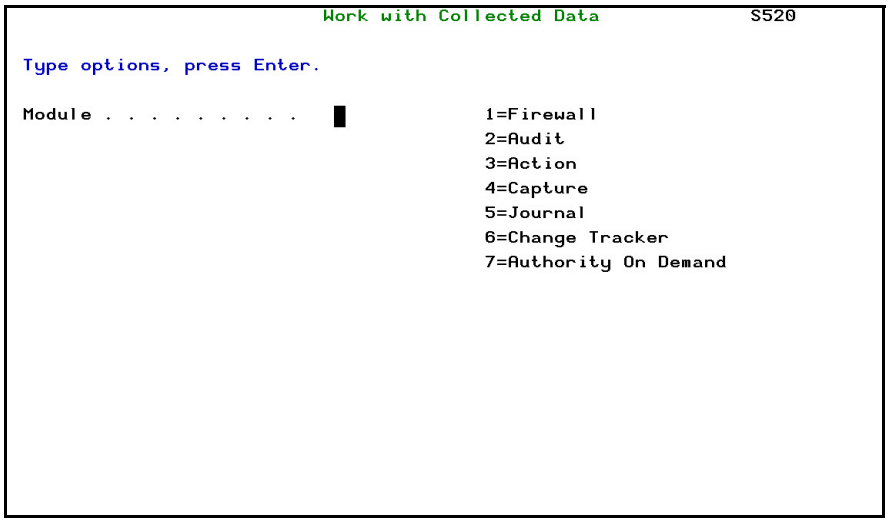


Figure 11-31. Work with Collected Data Screen

2. Enter **1** (**Firewall**) and press **Enter**. The **Work with Collected Data - Firewall** screen appears.

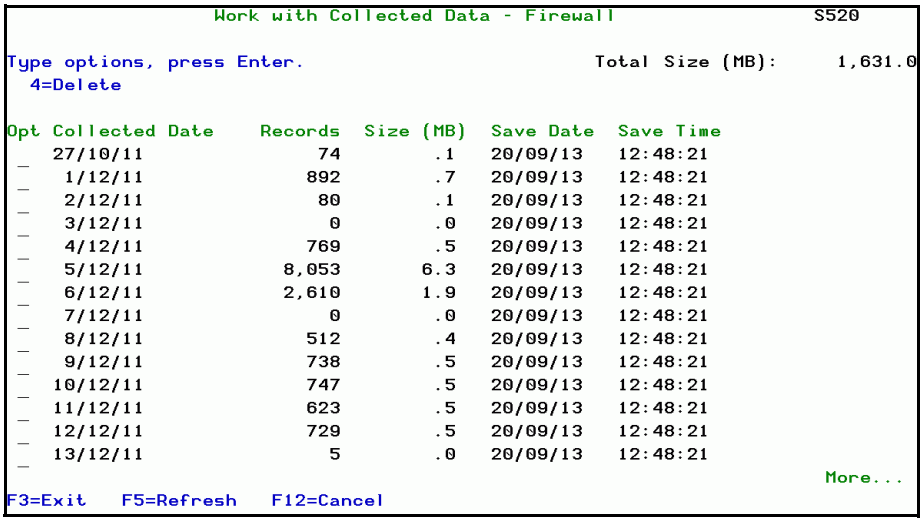


Figure 11-32. Work with Collected Data - Firewall Screen

3. Enter the correct options and press **Enter**.

*PRINT1-*PRINT9 and *PDF Setup

*PRINT1-*PRINT Setup

Firewall allows you to define up to nine specific printers for printing output. These can 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 predefined. ***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 **59. *PRINT1-*PRINT9, *PDF Setup** in the Maintenance Menu. The **Printer Files Setup** screen appears.
2. Type **1** and press **Enter**. The ***PRINT1 - *PRINT9** Setup screen appears.
3. Enter parameters as shown in the table below and press **Enter**.

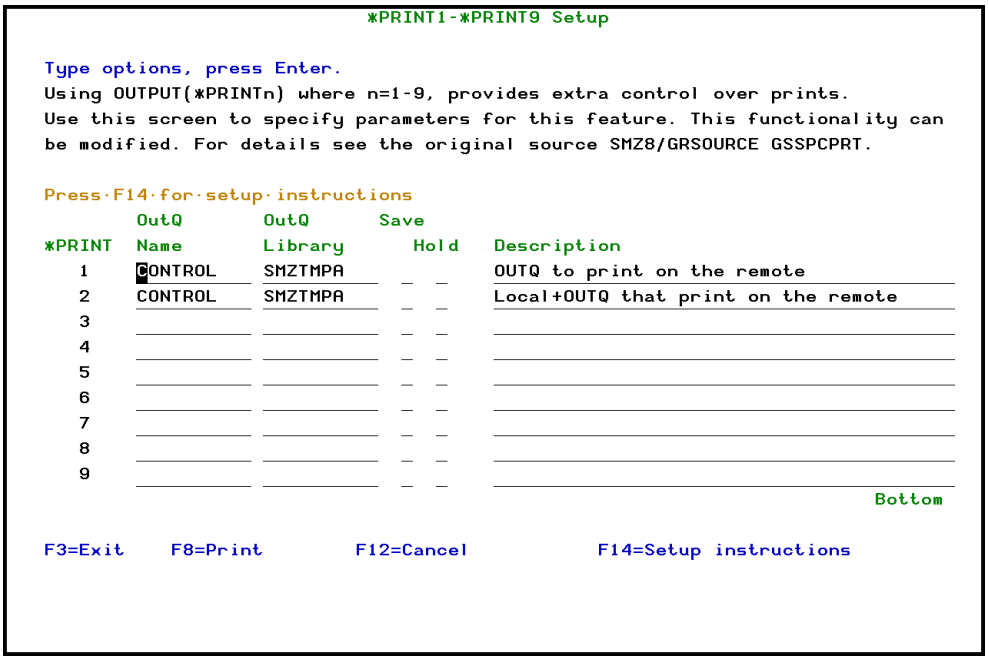


Figure 11-33. *PRINT1 - *PRINT9 Setup Screen

Field	
***PRINT**	The number of the special PRINT parameter.
OutQ Name	The name of the Output Queue that will receive output directed to this PRINT parameter.
OutQ Library	The name of library that contains the Output Queue that will receive output directed to this PRINT parameter.
Save	**Y**, **N**. Controls the Save File parameter for all Print Files sent to this output queue.
Hold	**Y**, **N**. Controls the Hold File parameter for all Print Files sent to this output queue.
Description	Type a meaningful description.

4. 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) TRANS-
FORM(*NO)
+     INTNETADR('IP of remote')
```

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)
+   RMTPRTQ(MYOUTQ)   AUTOSTRWTR(1) CNNTYPE(*IP) TRANSFORM(*NO)
+   INTNETADR(1.1.1.100)
```

*PDF Setup

In release 6.1 and up the operating system supports the direct production of *PDF prints. In the absence of such support, a standard *PDF is printed by other means. When the operating system *PDF capability exists, it is used, and the Query Generator uses the printer file **SMZ4/AUQRYPDF** to print the *PDF.

This file is shipped with the following parameters:

```
CHGPRTF FILE(SMZ4/AUQRYPDF) LPI(8) CPI(15) PAGRTT(*COR)
```

You can change the attributes of this printer file to suit your organizations specific requirements. Such changes must be re-applied after each iSecurity/Base (SMZ4) upgrade.

To define PDF printers, perform the following:

1. Select **59. *PRINT1-*PRINT9, *PDF Setup** in the Maintenance Menu. The **Printer Files Setup** screen appears.
2. Type **2** and press **Enter**. The ***PDF Setup** screen appears.
3. Follow the instructions on the screen.

Password Specific

Copy Dictionary Language

Copy dictionary language from one file to another library.

1. Select **82 > 41. Copy Dictionary Language (CPYDICLNG)** screen appears.

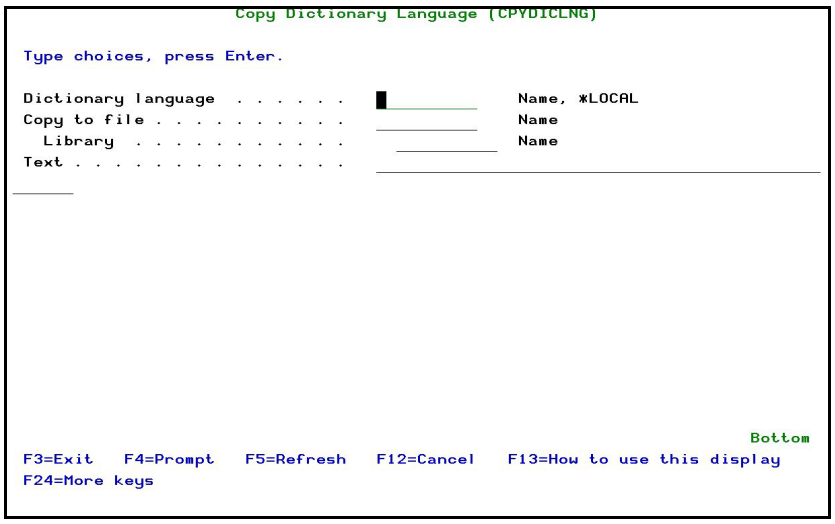


Figure 11-34. Copy Dictionary Language Screen

2. Type in the relevant parameters as described:

Field	
Dictionary language	***LOCAL** = Location of dictionary language **Name** = Name of dictionary language.
Copy to file	**Name** = Name of file to copy to.
Library	**Name** = Name of library to copy to.
Text	free text to search

3. Press **Enter**.

Import Dictionary language

Import dictionary language from one file to another library.

1. Select **82 > 42. Import Dictionary Language (IMPDICLNG)** screen appears.

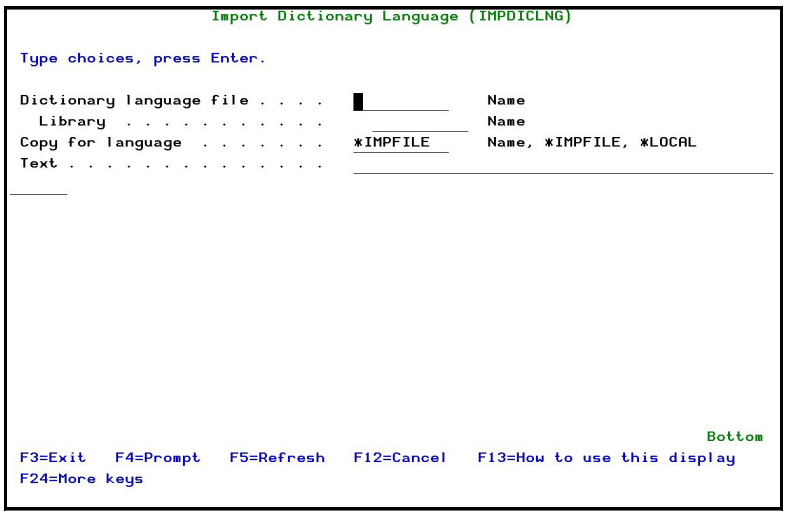


Figure 11-35. Import Dictionary Language Screen

2. Type in the relevant parameters as described:

Field	
Dictionary language file	**Name** = Name of dictionary language.
Library	**Name** = Name of library to copy to.
Copy to file	**Name** = Name of file to copy to.
Text	free text to search

Trace Definition Modifications

Add Journal

To record the system physical files changes in the data library:

1. Select **82 > 71. Add Journal**. The **Create Journal - Confirmation** screen appears.

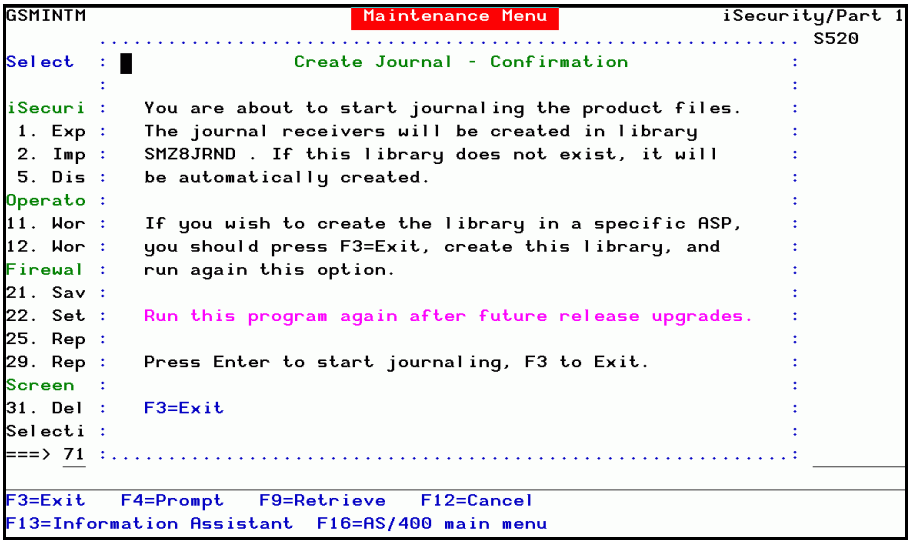


Figure 11-36. Create Journal - Confirmation Screen

2. Press **Enter** to confirm. The process of journaling the product files begins. The journal receivers will be created in library **SMZ8JRND**. If this library does not exist, it will be automatically created.

NOTE: If you wish to create the library in a different ASP, you should press **F3=Exit**, create this library, and run this option again.

NOTE: You must re-run this option after every release upgrade.

Remove Journal

To end the journaling of changes in the system physical files:

1. Select **82 > 72. Remove Journal**. The **End Journal - Confirmation** screen appears.

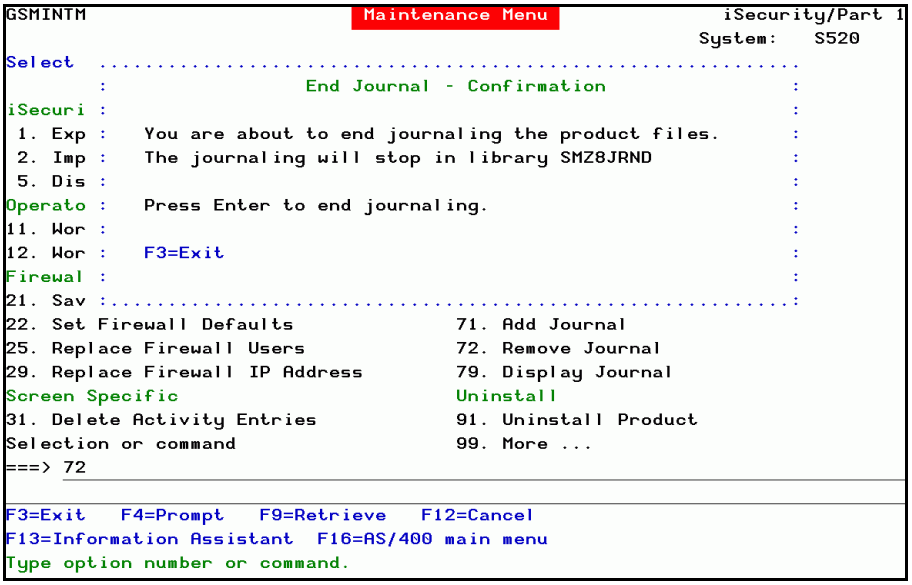


Figure 11-37. End Journal - Confirmation Screen

2. Press **Enter** to confirm.

Tracing Changes in Product Definitions

Firewall as well as all iSecurity modules allow tracing of product definitions by use of DB-Journaling and the completely free use of the AP-Journal for this reporting.

To enable this option, follow:

1. Set definition files to be journaled (**STRFW 82 > 71**) (Add Journal on page 237).
2. Set Global Installation (**STRFW 89 > 59**) (Global Installation Defaults on page 266).
   - Auto jrn def files on install = **Y**
   - Use AP-Journal to trace def chgs =**Y**
3. Trace changes (**STRFW 82 > 79**) (Display Journal on page 239).

Display Journal

To view journaled files:

1. Select **82 > 79. Display Journal**. The **Display Journal Entries** screen appears.

```
                          Display Journal Entries

Journal  . . . . . :   SMZ8            Library  . . . . . :   SMZTMPA
Largest sequence number on this screen  . . . . . : 00000000000000000013
Type options, press Enter.
  5=Display entire entry


Opt    Sequence  Code  Type  Object      Library     Job         Time
_             1   J     PR                        SCPF        14:30:08
5             2   R     PT    GRSTTS      SMZTMPA     AU#STRRTAU  14:37:06
_             4   R     DL    GRSTTS      SMZTMPA     GR#MONITOR  14:37:07
_             5   R     DL    GRSTTS      SMZTMPA     GR#MONITOR  14:37:07
_             6   R     DL    GRSTTS      SMZTMPA     GR#MONITOR  14:37:07
_             7   R     DL    GRSTTS      SMZTMPA     GR#MONITOR  14:37:07
_             8   R     DL    GRSTTS      SMZTMPA     GR#MONITOR  14:37:07
_             9   R     DL    GRSTTS      SMZTMPA     GR#MONITOR  14:37:07
_            10   R     DL    GRSTTS      SMZTMPA     GR#MONITOR  14:37:07
_            11   F     RG    GRSTTS      SMZTMPA     GR#MONITOR  14:37:16
_            12   F     RM    GRSTTS      SMZTMPA     GR#MONITOR  14:37:17
_            13   F     RG    GRHOUR      SMZTMPA     GR#MONITOR  14:37:51
                                                                   More...
F3=Exit    F12=Cancel
```

Figure 11-38. Display Journal Entries Screen

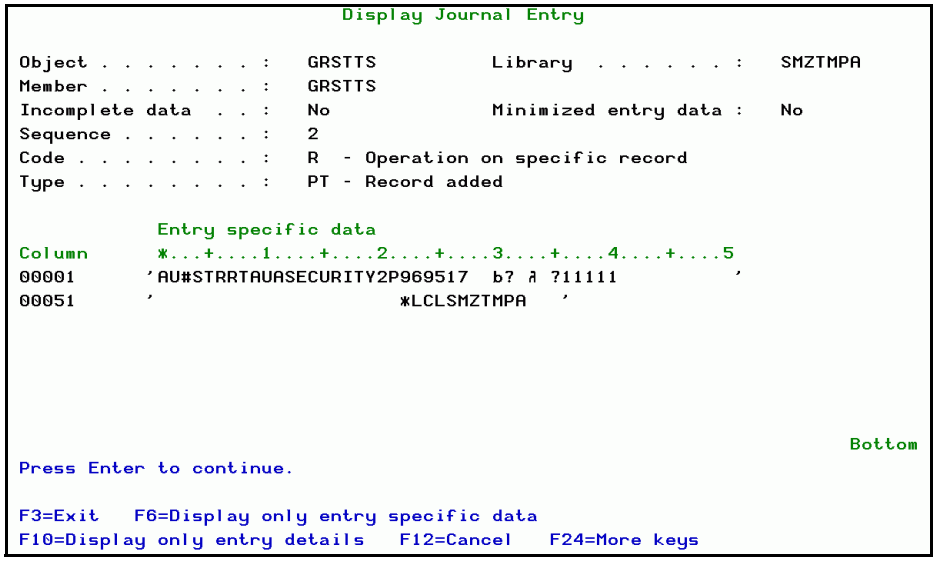


Figure 11-39. Display Journal Entry (Details) Screen

Uninstall

To Uninstall the product:

1. Select **82 > 98. Uninstall Product**, and follow the directions on the screen.

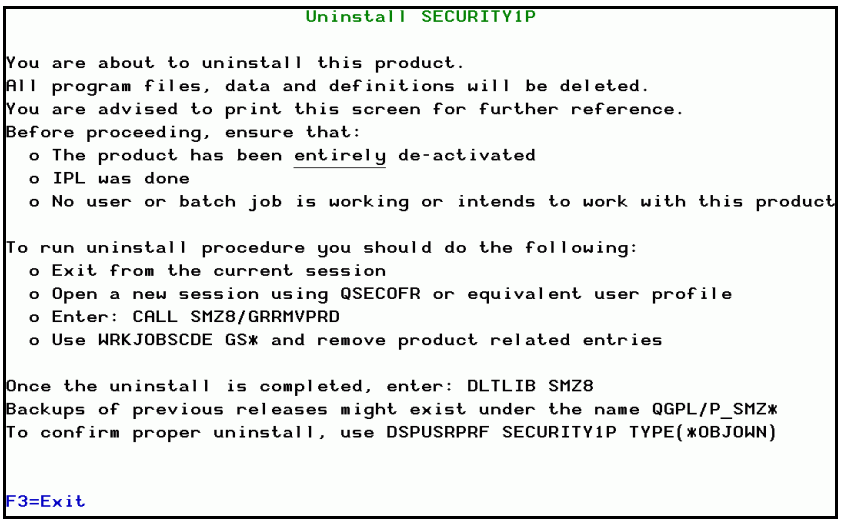


Figure 11-40. Uninstall SECURITY1P Screen

Special Tools

Use Firewall in Parallel

The Firewall product coexists with your Network Security program and collects information in parallel, as a Log.

NOTE: Only one of the products may run in "real" mode. The other program should be set to run in simulation mode.

Disclaimer: Because this option involves running other vendor programs, it is provided as a service which carries no warranty for its consequences.

To work in parallel:

1. Set Firewall to run in simulation mode (FYI), as described in FYI Simulation Mode - Global Setting on page 61.
2. Set Firewall to run in Global FYI mode.
   a. Select **1. Activation and Server Setting** from the Main menu. The **Activation and Server Setting** menu appears.
   b. Select **1. Work with Servers** from the **Activation and Server Setting** menu. The **Work with Server Security** screen appears.
   c. Press **F23=FYI**. The **Firewall *FYI* Simulation Mode** screen appears. Set **Work in *FYI* simulation mode** to **Y**.
3. Extract the name of the other program and define which program is responsible for the exit points.
   a. Select **99. More ...** from the **Maintenance Menu**. The **Maintenance Menu - Part 2** appears.
   b. Select **1. Use Firewall in parallel with other Exit Programs**. The **Run Another Network Security in Parallel** screen appears.

```
GSPRLL          Run Another Network Security in Parallel          Firewall
                                                        System:   S520
iSecurity/Firewall enables you to run a second Network Security system in
parallel. Only one of the products may run in "real" mode. The other system
will be considered as running in simulation mode.
Because this option involves running other vendor systems, it is provided
as a service which carries no warranty for its consequences.

Perform the following procedure:
 1. Verify parallel work availability
 2. Extract the current registration facility setting
 3. Check / Modify the extracted information
 4. Set Firewall to run in simulation (*FYI) mode
 5. Set who decides: Firewall / Parallel system
 6. Activate ZFIREWALL subsystem
 7. Start parallel work (set Firewall in registration facility)

Once the test ends, use option 5 to set the system you choose, as the only one.
Selection or command
===>

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

Figure 11-41. Run Another Network Security in Parallel

c. Select option **2. Extract the current registration facility setting**. This extracts the name of the other exit program.

d. Select option **5. Set who decides: Firewall / Parallel system**. The **Set Parallel System** screen appears.

```
                          Set Parallel System

Type options, press Enter.

Current setting . . . . . .   7

Set Parallel System to run  . .   5   1=Only Firewall runs
                                      5=Run in parallel, Firewall decides
                                      7=Run in parallel, other program decides


Note: Selecting 5 or 7 tells the system which product decision to pass as the
      decision to the OS400. If security should be enforced that system must
      work in "real" mode.




F3=Exit
```

Figure 11-42. Set Parallel System

e. Set the Set Parallel System to run parameter to the appropriate value:

- **1** = No parallel work, Firewall is responsible for exit programs
- **5** = Parallel work, Firewall is responsible for exit programs
- **7** = Parallel work, Firewall is not responsible for exit programs, although users will see the allowed/rejected message as though it comes from Firewall

4. Enable Firewall to work in parallel on all exit points.

a. Select **1. Activation and Server Setting** from the Main menu. The **Activation and Server Setting** menu appears.

b. Select **1. Work with Servers** from the **Activation and Server Setting** menu. The **Work with Server Security** screen appears.

c. Press **F22=Global setting**. The **Global Server Security Settings** screen appears. Set **Skip "Other" exit points** to ***NO** and press **Enter**.

You are now ready to work in parallel mode with another security system.

Consolidate Time Groups

Both Firewall and Audit use time groups. You can consolidate these time groups, to allow for more consistency.

1. Select **82 > 99 > 5. Consolidate Time Groups** from the **Maintenance Menu - Part 2**. The **Consolidate Firewall Time Groups into Audit** screen appears.

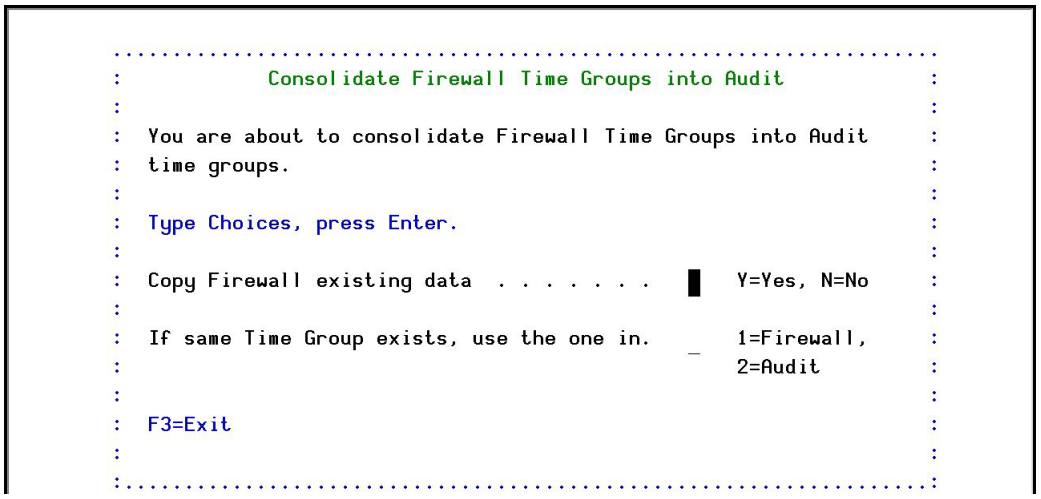


Figure 11-43. Consolidate Firewall Time Groups into Audit

Field	Description
Copy Firewall existing data	Define if to copy the Firewall Time Groups to Audit **Y** = Yes **N** = No
If same Time Group exists, use the one in	If the same named Time Groups exist in both Firewall and Audit, define which Time Groups to use. **1** = Firewall **2** = Audit

2. Enter the parameters to define which Time Groups to use and press **Enter**.

iSecurity Central Administration

The iSecurity Central Administration enables two types of methods to run reports.

To get current information from existing report or query, while adjusting the system parameters only, to collect information from all the groups in the system to output file that can be sent via email.

1. Select **83. Central Administration** from the Main menu. The **iSecurity Central Administration - Firewall** screen appears.

```
GSCNTMN          iSecurity Central Administration - Firewall   iSecurity/CntAdm
                                                               System:   S520
Select one of the following:

Definitions     Use SYSTEM() in the reporting menu to run reports on the network
 1. Work with network definitions
 2. Network Authentication
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                          Communication Log
31. Export Definitions, Update Remote Systems 71. Current Job CntAdm Messages
32. Import Definitions                        72. All Jobs CntAdm Messages

Selection or command
===>

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

Figure 11-44. iSecurity Central Administration - Firewall Screen

2. Select option **1. Work with network definitions**. The **Work with Network Systems** screen appears.

```
                          Work with Network Systems     System type: AS400

Type options, press Enter.
  1=Select     4=Remove     7=Export dfn.    9=Verify communication
                                              Position to . . .

Opt   System     Group
_     BERT       *G1
_     MIKLOS     *G2       test before new release
_     S150       *G1       Razlee
_

                                                                      Bottom
F3=Exit     F6=Add New     F7=Export dfn cmd     F12=Cancel
```

Figure 11-45. Work with Network Systems Screen

3. Press **F6** to define a new network system to work with and press **Enter** to confirm.

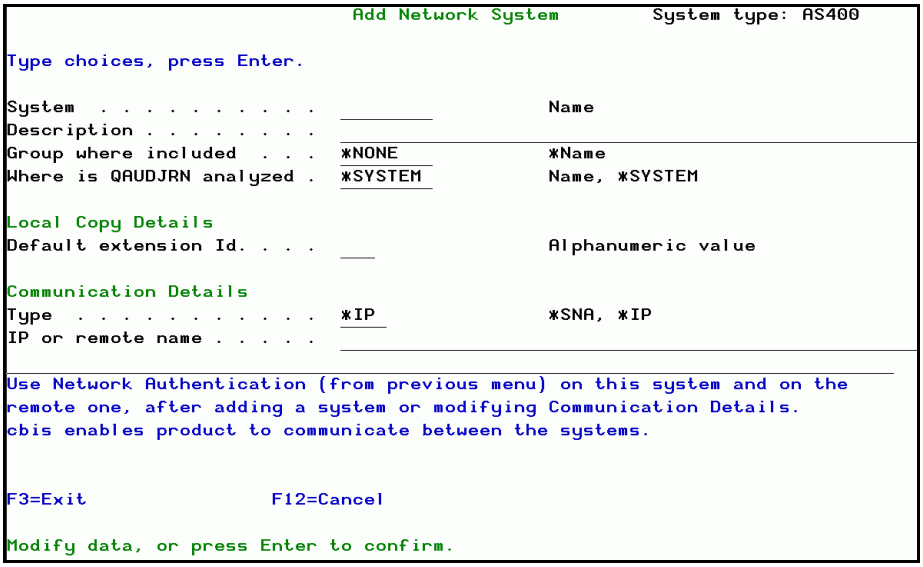


Figure 11-46. Add Network System Screen

To work on remote systems:

Define the same password on all systems and LPARs for user SECURITY2P.

1. Select **83 > 2. Network Authentication**. The **Network Authentication** screen appears.
2. Enter and confirm the password for the SECURITY2P user and press **Enter**.

NOTE: Values entered in this screen are **not** preserved in any iSecurity file. They are only used to set the user profile password and to set server authentication entries. Also, ensure that System Value QRETSVRSEC is set to **1**.

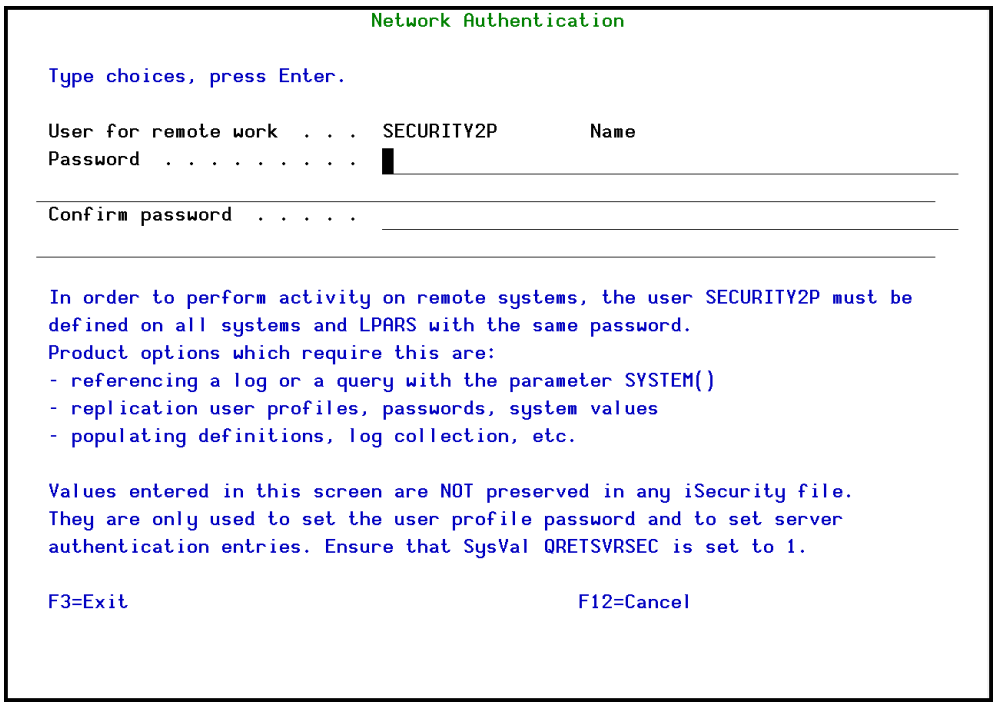


Figure 11-47. Network Authentication Screen

To run the reports on a copy of data library of a remote system:

1. Select **83 > 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***

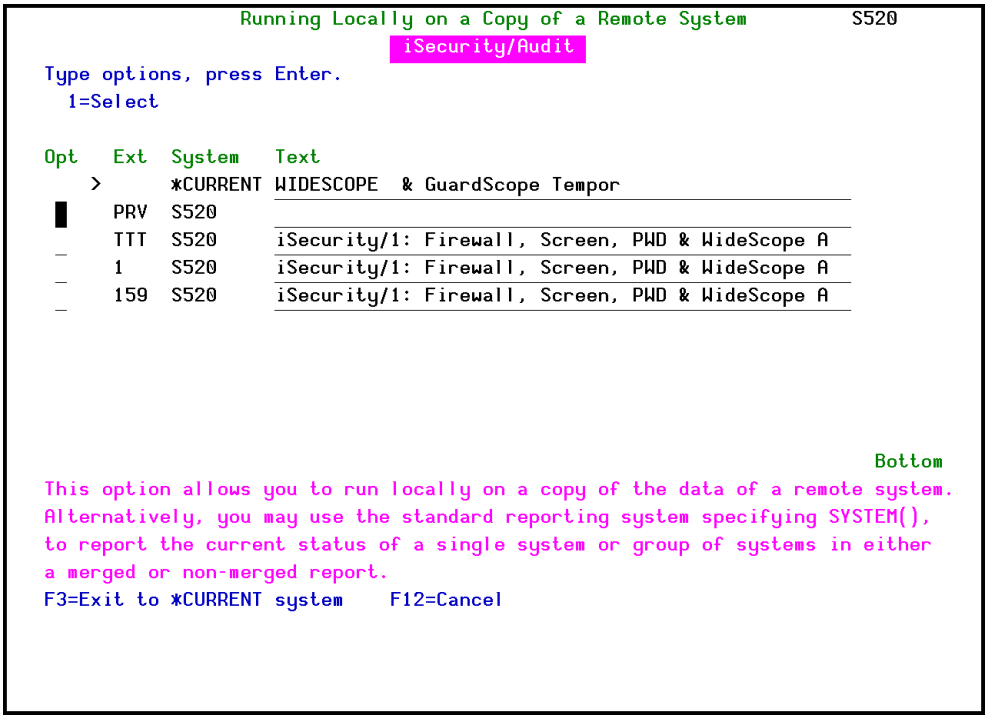


Figure 11-48. Running Locally on a Copy of a Remote System

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):

1. Select **83 > 31. Export Definitions, Update Remote Systems**. The **Export iSecurity/Part 1 Defns. (EXPS1DFN)** screen appears.

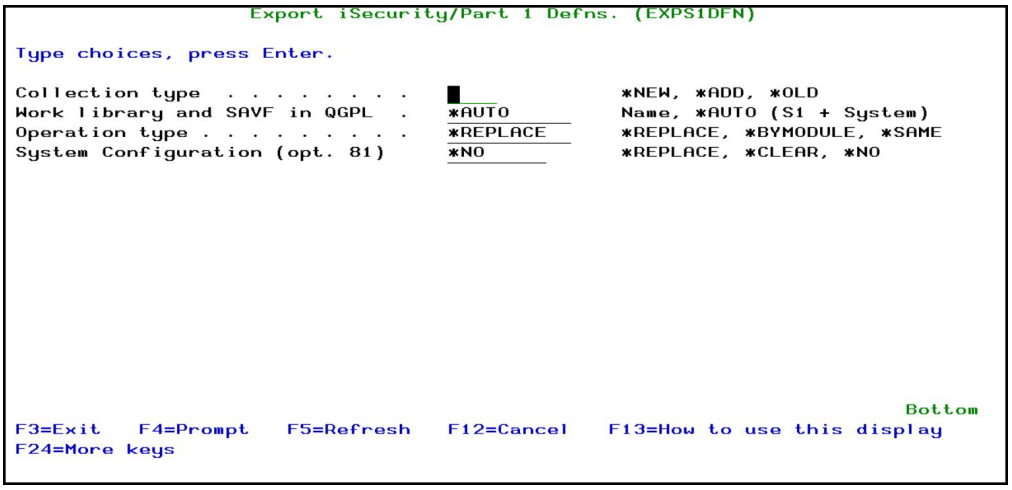


Figure 11-49. Export iSecurity/Part 1 Defns. (EXPS1DFN)

To restore a distribution package of the definitions created (import):

1. Select **83 > 32. Import Definitions**. The **Import iSecurity/Part 1 Defns. (IMPS1DFN)** screen appears.

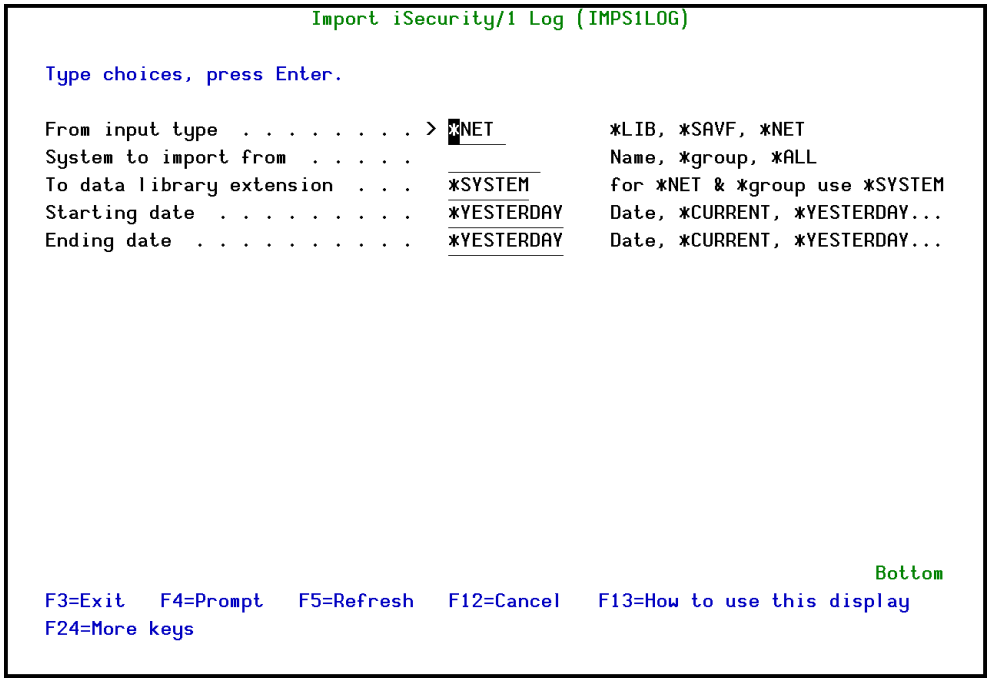


Figure 11-50. Import iSecurityPart 1 Defns. (IMPS1DFN) Screen

Base Support

The **BASE Support** menu enables you to work with various settings that are common for all modules of iSecurity. This menu, with all its options, is in all iSecurity major modules. To access the **BASE Support** menu, select **89. BASE Support** from the **Firewall** main menu.

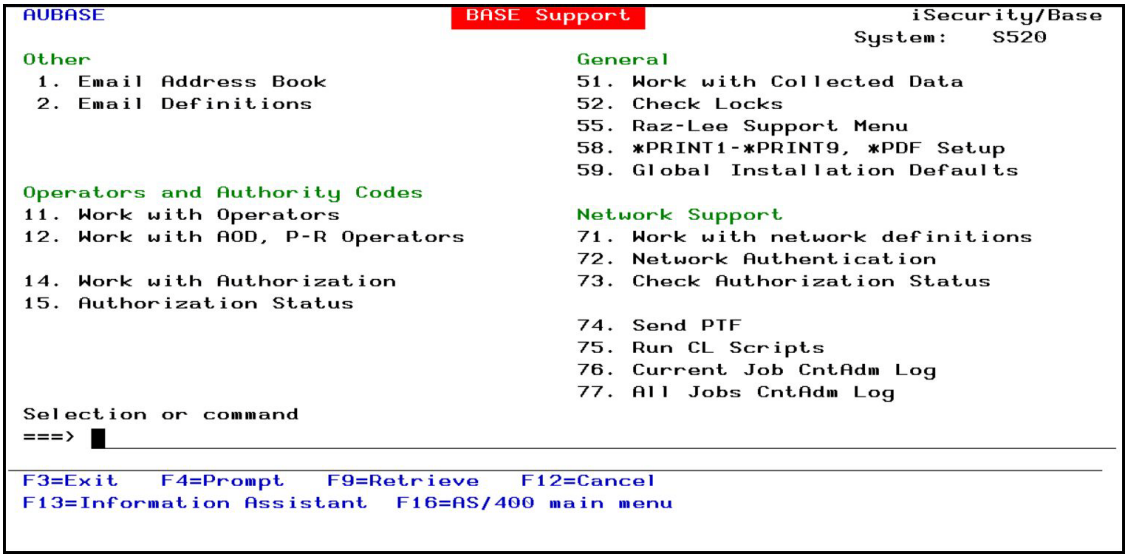


Figure 11-51. BASE Support menu

Other

Email Address Book

You can define the email address to be used for each user profile. You can also use this option to define an email group, with multiple addresses.

1. Select **89 > 1. Email Address Book**. The **Work with Email Address Book** screen appears.

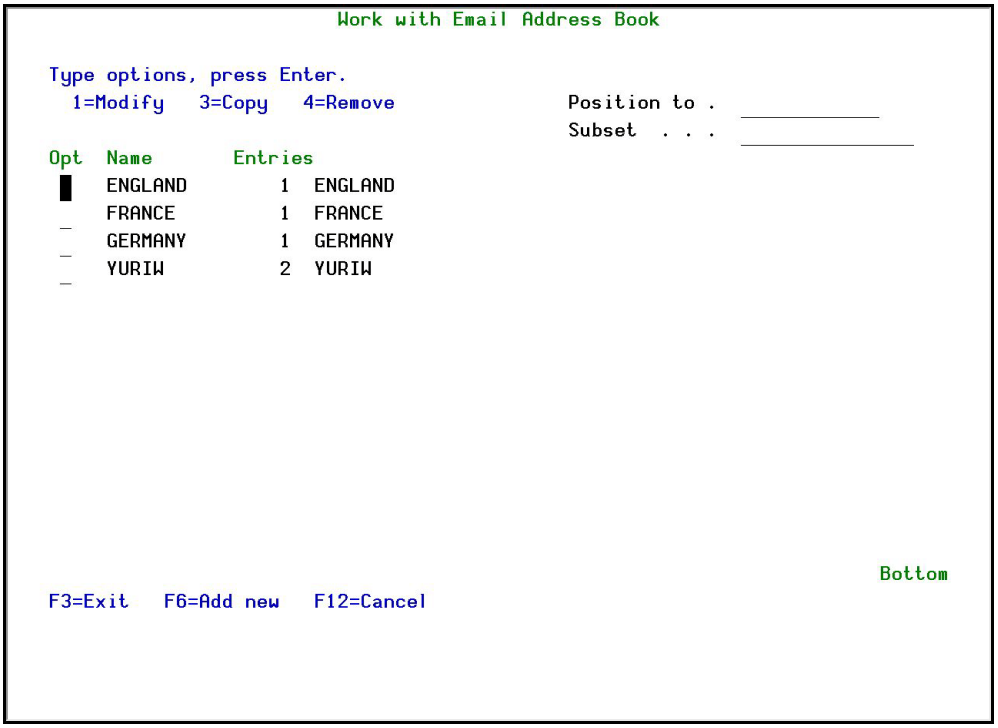


Figure 11-52. Work with Email Address Book

2. Press **F6** to add a new address entry (or type **1** next to a name to modify it). The **Add Email Name** screen appears.

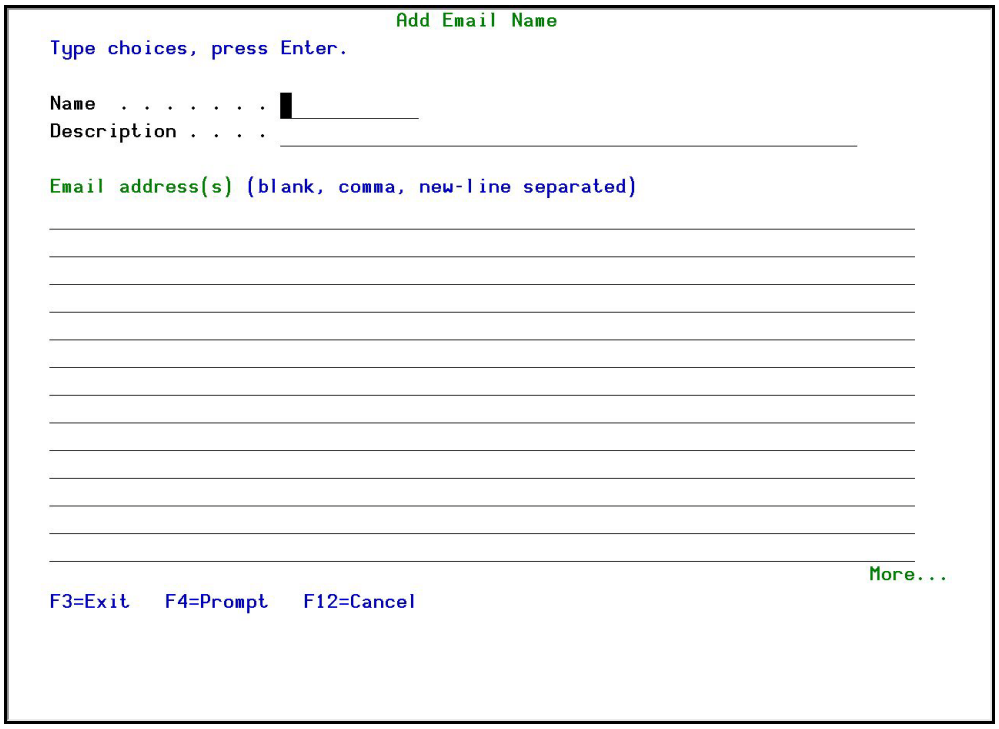


Figure 11-53. Add Email Name

3. Enter a **Name**, **Description**, and all the associated email addresses and press **Enter**.

Email Definitions

Firewall can send out automatic emails for events that you define.

1. Select **89 > 2. Email Definitions**. The **E-mail Definitions** screen appears.

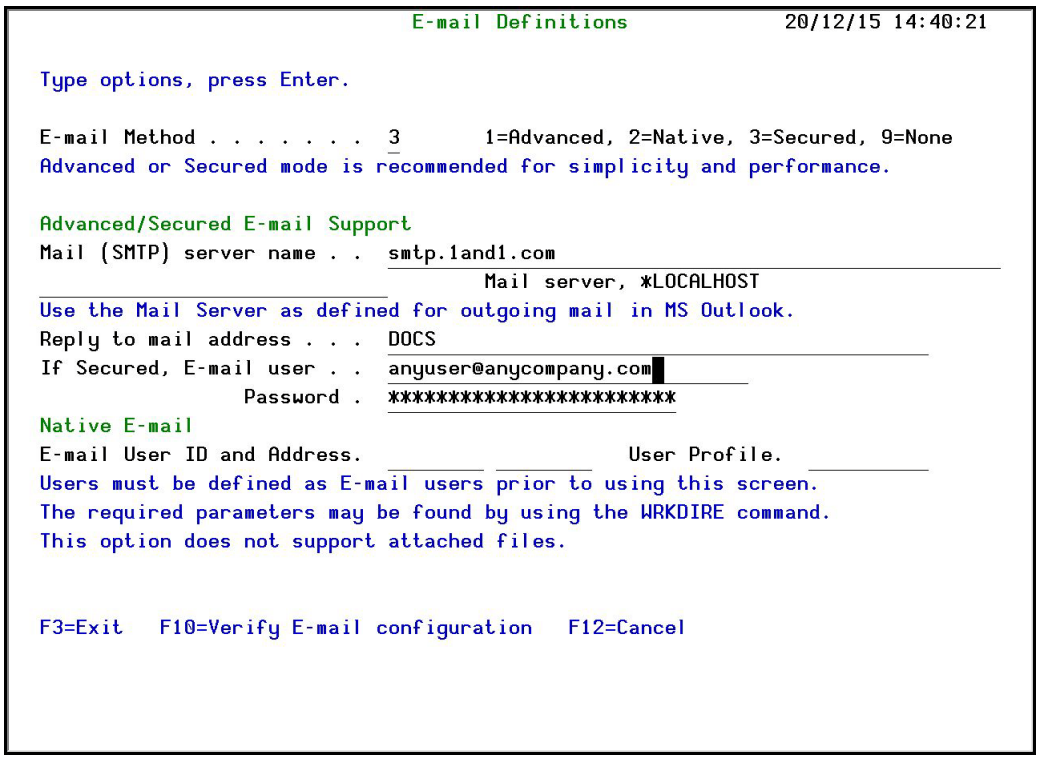


Figure 11-54. Email Definitions

Field	Description
E-mail Method	**1=Advanced** **2=Native** **3=Secured** **9=None** Advanced or Secured mode is recommended for simplicity and performance. Note: If using **2=Native**, Users must be defined as E-mail users prior to using this screen. The required parameters may be found by using the WRKDIRE command. This option does not support attached files
Mail (SMTP) server name	The name of the STMP server or ***LOCALHOST**
Reply to mail address	The e-mail address to receive replies
If secured, email user and Password	If you chose **1=Advanced** or **3=Secured** for the E-mail method, enter the email user that will be used to send the emails and the password of that user
Email user ID and Address	If you chose **2=Native** for the E-mail method, enter the user ID and address that will be used to send the emails
User Profile	If you chose **2=Native** for the E-mail method, enter the user profile that will be used to send the emails

Field	Description
F10=Verify E-mail configuration	Press **F10** to open a dialog that allows you to confirm the change to email definitions and sends a confirmation email to the **Reply to mail address**. You should check that the confirmation email is received. If it is not received, there is a problem with your email definitions.

2. Enter the required fields and press **Enter**.

Operators and Authority Codes

Work with Operators

The Operators' authority 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 you use Work with Operators to define all users who have ***SECADM**, ***AUDIT** or ***AUD#SECAD** privileges, but do not have all object authority. The **Work with Operators** screen has Usr (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 your organization wants the default to be *BLANK, then the following command must be used:

CRTDTAARA SMZTMPC/DFTPWD *char 10

This command creates a data area called DFTPWD in library SMZTMPC. The data area is 10 bytes long and is blank.

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:

1. Select **89 > 11. Work with Operators**. The **Work with Operators** screen appears.

```
                          Work with Operators

Type options, press Enter.
  1=Select   3=Copy    4=Delete
                     Auth.level: 1=*USE, 9=*FULL, 3=*QRY(FW,AU,CT), 5=*DFN(CT)
   User       System  FW SC PW CM AV AU AC CP JR VW VS RP NO CT PR UM EN ADM
 _ *AUD#SECAD S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9
 _ *AUDIT     S520                 9  9  9  9  9     9
 _ *SECADM    S520     9  9  9     9              9  9              9
 _ ALEX       S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9     9
 _ AU         S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9     9
 _ AV         S520     9  9  9     9  9  9  9  9  9  9  9  9  9  9  9  9  9
 _ EVGTST     S520     9  9  9     9  9  9  9  9  9  9  9  9        9  9  9
 _ JAVA       S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9
 _ JR         S520     9  9  9     9  9  9  9  9  9  9  9  9  9     9     9
 _ LOWUSR     S520
 _                                                                  More...
FW=Firewall    SC=Screen   PW=Password   CM=Command     AU=Audit      AC=Action
AV=Antivirus   CP=Capture  JR=Journal    VS=Visualizer  UM=User Mgt.  ADM=Admin
RP=Replication NO=Native Obj.Compliance  CT=Chg Tracker PR=Pwd Reset  VW=View
EN=Encryption/Tokenization

F3=Exit    F6=Add new    F8=Print   F11=*SECADM/*AUDIT authority   F12=Cancel
```

Figure 11-55. Work with Operators

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

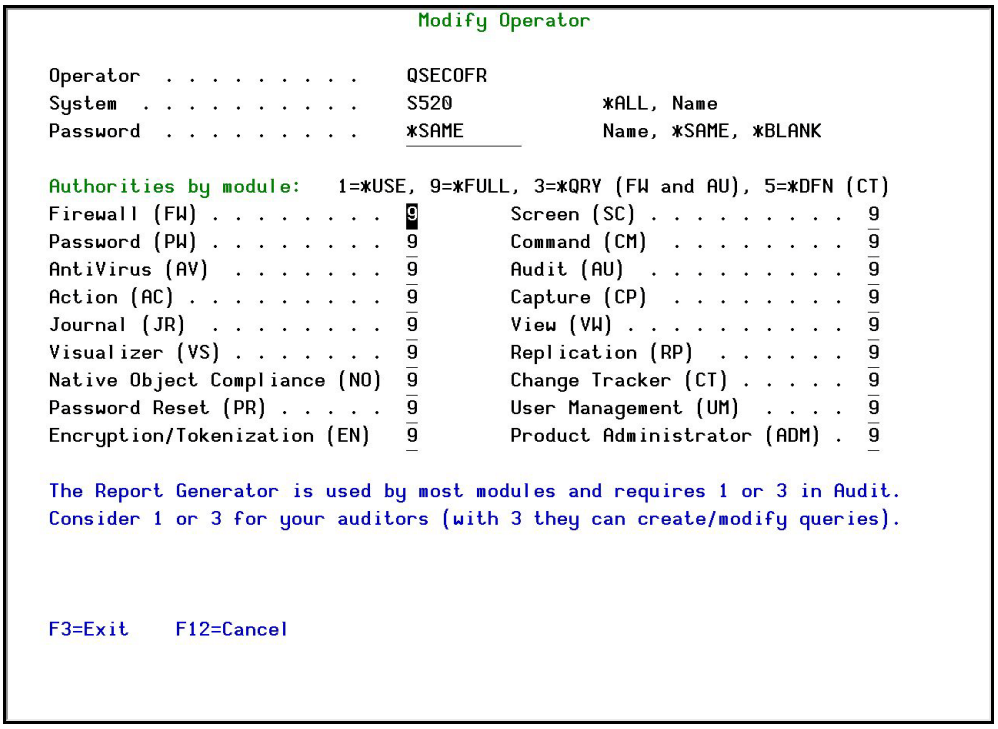


Figure 11-56. Modify Operator

Field	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
5 = *DFN	For Firewall use

Most modules use the Report Generator, which requires access to the Audit module. For all users who will use the Report Generator, you should define their access to the Audit module as either 1 or 3. Option 1 should be used for users who will only be running queries. Use option 3 for all users who will also be creating/modifying queries.

3. Set authorities and press **Enter.**

   A message appears to inform 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.

Work with AOD, P-R Operators

To modify operators authorities:

1. Select **89 > 12. Work with AOD, P-R Operators**. 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    AOD PR  USP  Adm
 _  *AUD#SECAD    S520        9   9    9    9
 _  ALEX          S520        9   9    5    9
 _  AV            S520        9             9
 _  JAVA2         S520        9   9    9    9
 _  LOWUSR        S520        9   9    9    9
 _  OD            S520        9   9    9    9
 _  OS            *ALL
 _  TZION         S520        9   9    9    9
 _  WEAKUSR       S520        9
 _  YORAM         S520        9             9
 _

                                                                      Bottom
AOD=Authority on Demand   PR=Password Reset    USP=User Provisioning
                                               Adm=Administrator
F3=Exit    F6=Add new    F8=Print   F11=*SECADM/*AUDIT authority   F12=Cancel
```

Figure 11-57. Work with Operators - AOD

2. 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  . . . . . .      S520             *ALL, Name
Password  . . . . . .    *SAME            Name, *SAME, *BLANK

Authorities by subject:
Authority on Demand . . . .  9             1=*USE, 4=Limited *EMERGENCY
                                           5=*EMERGENCY, 8=Limited *FULL
                                           9=*FULL
Password Reset  . . . . . .  9             1=*USE, 9=*FULL
User Provisioning . . . . .  9             1=*USE, 5=*ENTRY, 9=*FULL
Product Administrator . . .  9             1=*USE, 9=*FULL

Note: Emergency operator can enable or modify emergency rules. This allows
      solving of critical problems without the intervention of the security
      administrator.
      The term Limited denotes that the user cannot change PIN codes.

F3=Exit    F12=Cancel
```

Figure 11-58. Modify Operator - AOD

Field	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
5 = *DFN	For Firewall use

3. Set authorities and press **Enter**.

   A message appears to inform 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.

Work with Authorization

You can insert license keys for multiple products on the computer using one screen.

1. Select **89 > 14. Work with Authorization**. The **Add iSecurity Authorization** screen appears.

```
                    Add iSecurity Authorization (ADDISAUT)

Type choices, press Enter.

*BASE, Audit, Action:
  Part 1 . . . . . .   *SAME          4..., *SAME
  Part 2 (optional)  . . . . . .
Compliance, Replication:
  Part 1 . . . . . .   *SAME          N..., *SAME
  Part 2 (optional)  . . . . . .
Firewall, Screen, Password:
  Part 1 . . . . . .   *SAME          8..., *SAME
  Part 2 (optional)  . . . . . .
Capture:
  Part 1 . . . . . .   *SAME          C..., *SAME
  Part 2 (optional)  . . . . . .
AP-Journal:
  Part 1 . . . . . .   *SAME          J..., *SAME
  Part 2 (optional)  . . . . . .

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

Figure 11-59. Add iSecurity Authorization (ADDISAUT)

2. Enter the required parameters and press **Enter**.

Authorization Status

You can display the current authorization status of all installed iSecurity products on the local system.

1. Select **89 > 15. Authorization Status**. The **Status of iSecurity Authorization** screen appears.

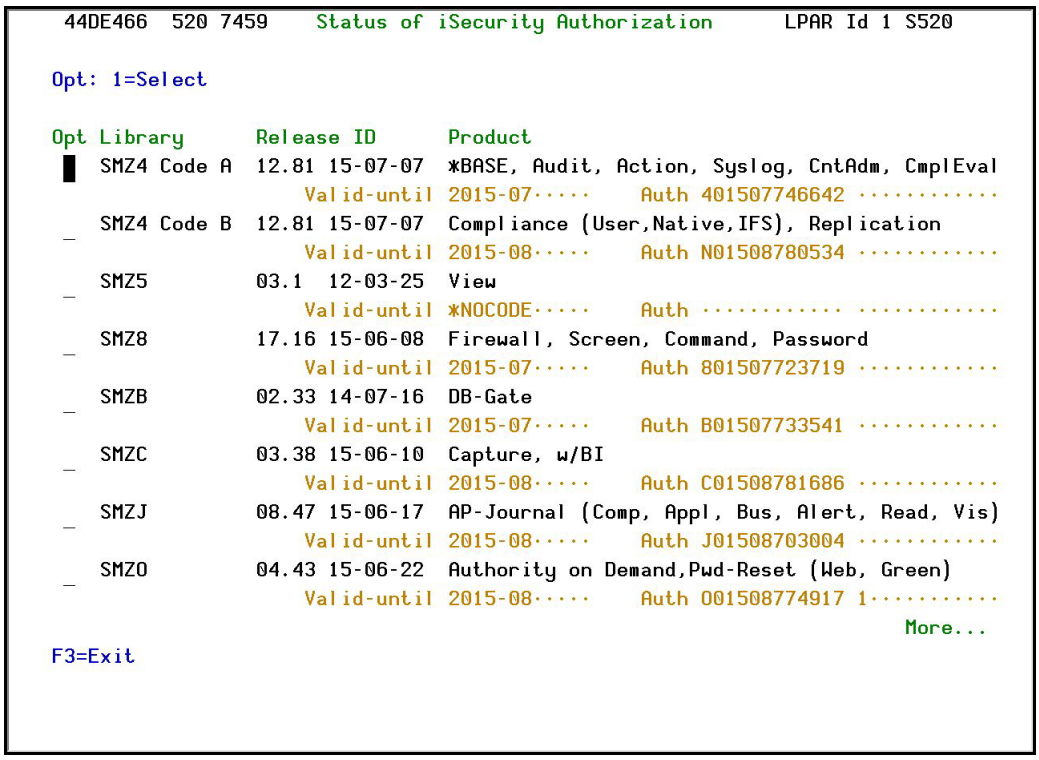


Figure 11-60. Status of iSecurity Authorization

2. Select a specific line and type **1** in the **Opt** field to see the authority details of one specific product.

NOTE: Codes that will expire in less than 14 days appear in pink
Permanent codes have deliberately been hidden in this screenshot.

General

Work with Collected Data

Administrators can view summaries of journal contents of various products by day, showing the number of entries for each day together with the amount of disk space occupied. Administrators can optionally delete individual days to conserve disk space.

1. Select **89 > 51. Work with Collected Data**. The **Work with Collected Data** screen appears.

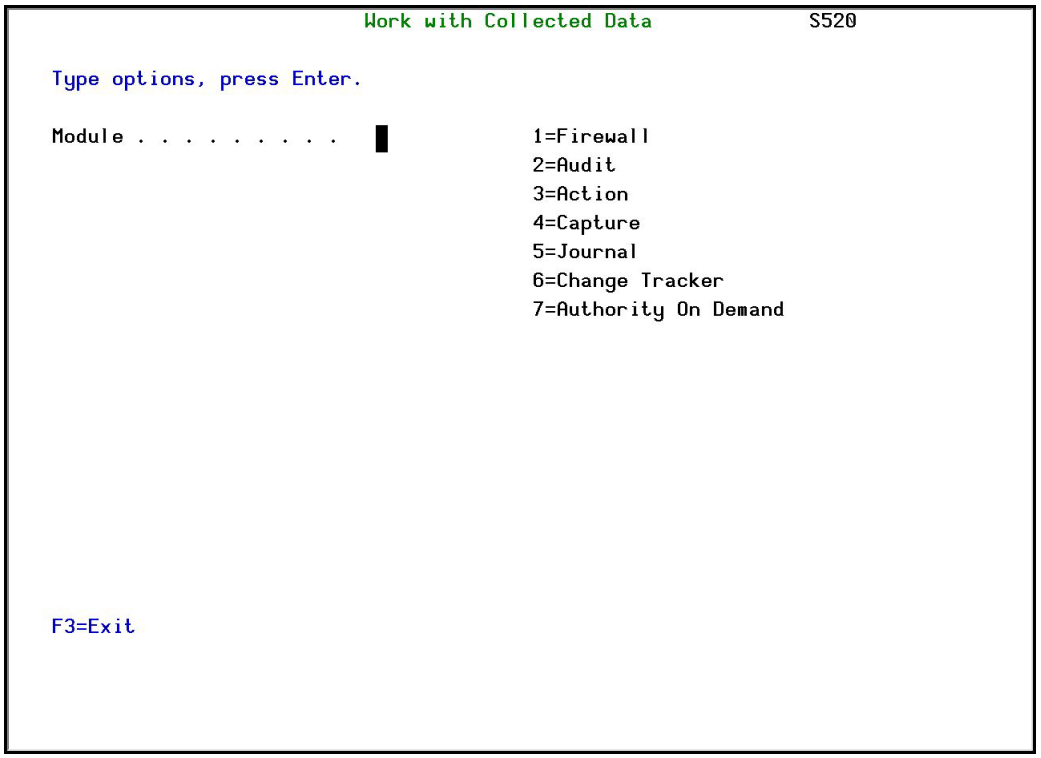


Figure 11-61. Work with Collected Data

2. Enter **1 (Firewall)** and press **Enter**. The **Work with Collected Data - Firewall** screen appears.

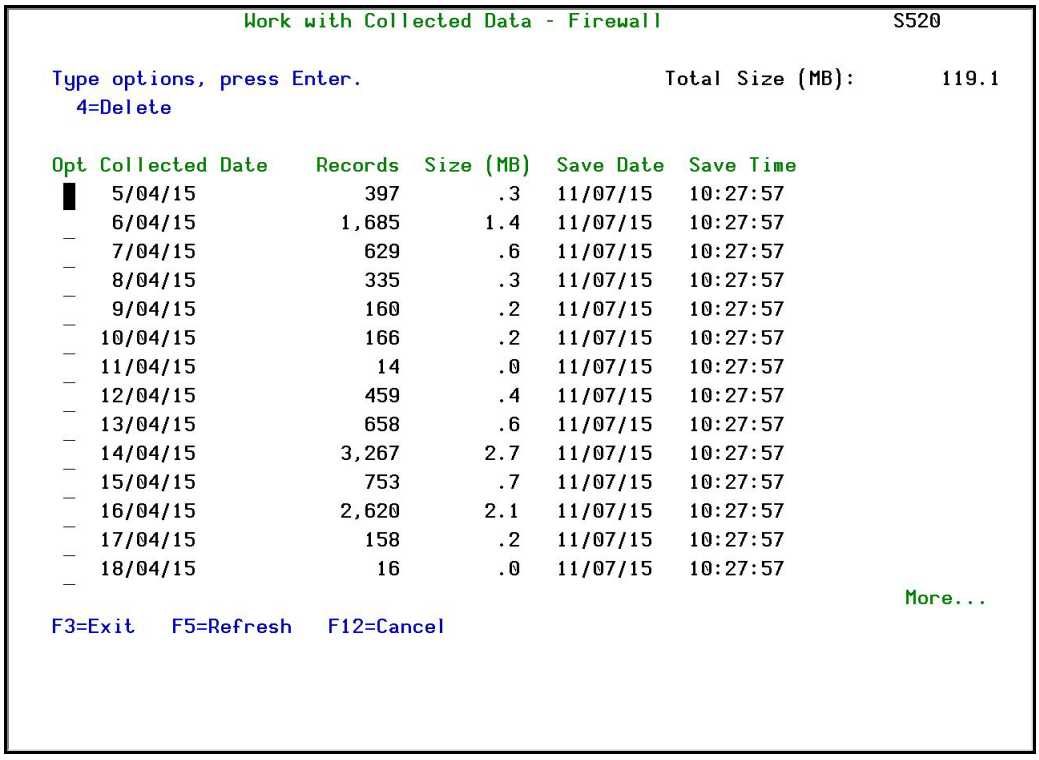


Figure 11-62. Work with Collected Data - Firewall

3. Select **4** to delete data from specific date(s) and press **Enter**.

Check Locks

You need to run this option before you upgrade your system to check if any of the **Firewall** files are being used. If they are, you must ensure that they are not in use before you run the upgrade.

1. Select **89 > 52. Check Locks**. The **Check Locks** screen appears.

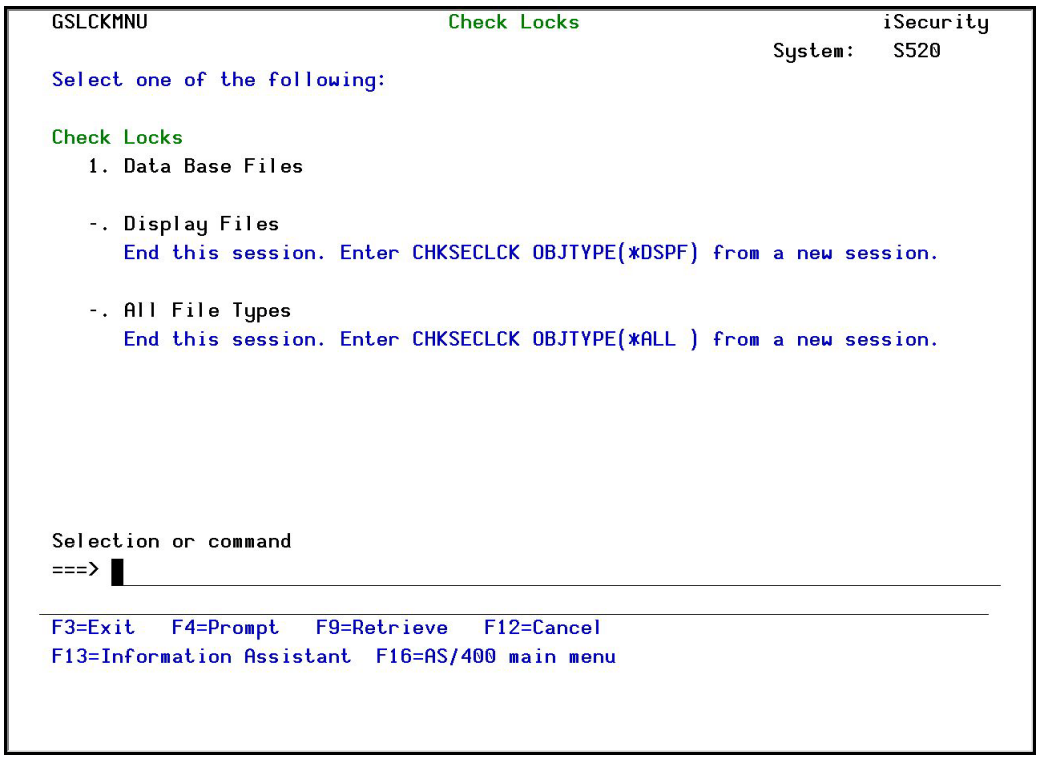


Figure 11-63. Check Locks

2. Follow the instructions on the screen.

Raz-Lee Support Menu

NOTE: Raz-Lee Support Menu is intended for users that have undergone training to use this menu. Please do not attempt to use it without the appropriate training.

- Select **89 > 55. Raz-Lee Support Menu**. The **iSecurity Tools ** Raz-Lee Support Restricted Usage **** screen appears.

*PRINT1 - *PRINT9 Setup

Firewall allows you to define up to nine specific printers to which you can send printed output. These may be local or remote printers. ***PRINT1-*PRINT9** are special values which you can enter in the **OUTPUT** parameter of any commands or options that support printed output.

Output to one 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 predefined. ***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:

1. Select **89 > 58. *PRINT1 - *PRINT9, PDF Setup**. The **Printer Files Setup** screen appears.

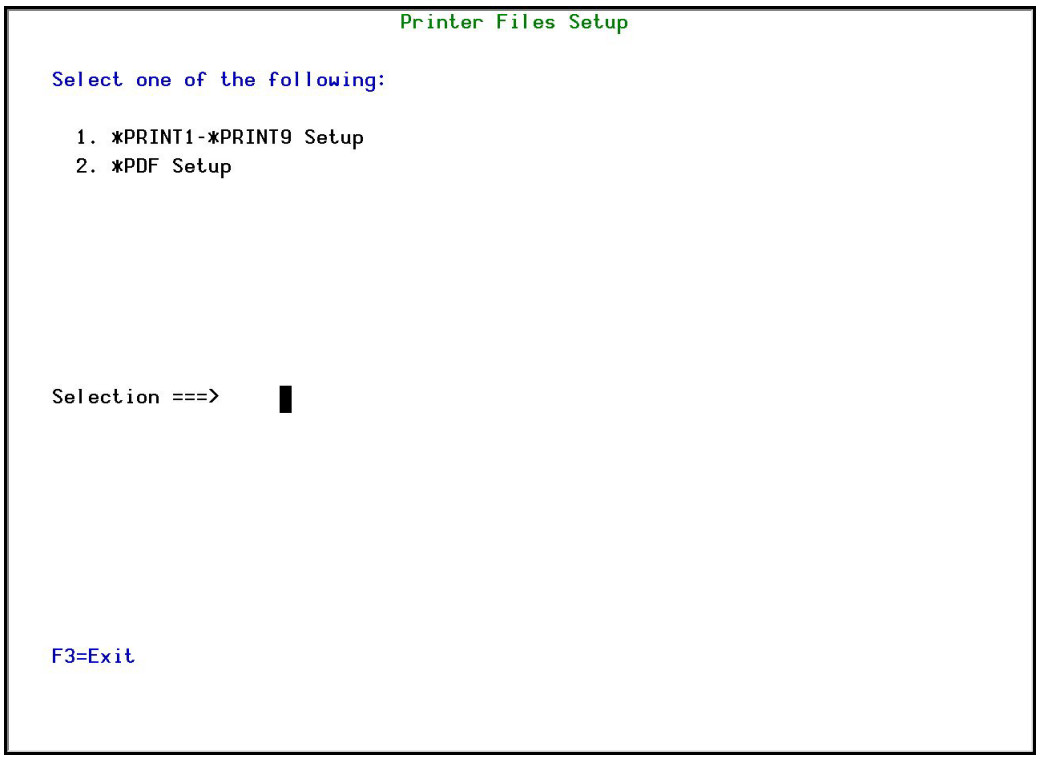


Figure 11-64. Printer Files Setup

2. Enter **1** and press **Enter**. The ***PRINT - *PRINT9 Setup** screen appears.

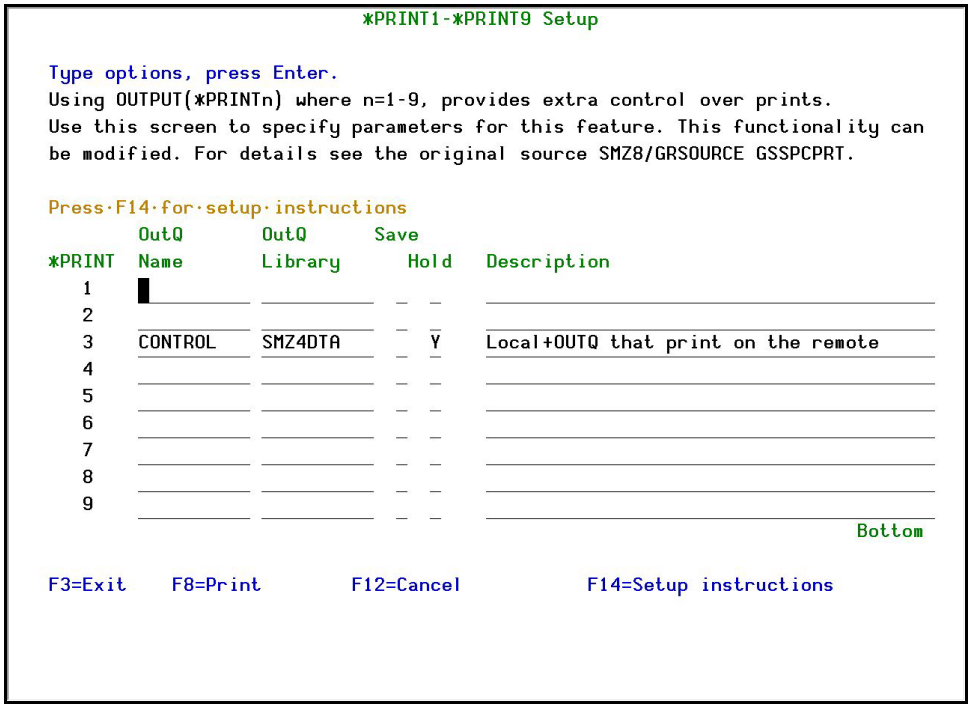


Figure 11-65. *PRINT - *PRINT9 Setup

3. Enter the name of the local output queue and library as shown in the above example. You can optionally enter a description.

Field	Description
OutQ name	The name of the local output queue
OutQ Library	The library of the local output queue
Save	**Y** = Yes **N** = No
Hold	**Y** = Yes **N** = No
Description	Enter a meaningful description (optional)

4. 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
OUTQ()	Name of the local output queue
RMTPRTQ()	Name of the remote output queue
INTNETADR()	IP address of the remote system

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, ***PRINT4** 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)
+    RMTPRTQ(MYOUTQ) AUTOSTRWTR(1) CNNTYPE(*IP) TRANSFORM(*NO)
+    INTNETADR(1.1.1.100)
```

PDF Setup

The operating system, from release 6.1, directly produces *PDF prints. In the absence of such support a standard *PDF is printed by other means.

To define PDF printers:

1. Select **89 > 58. *PRINT1 - *PRINT9, PDF Setup** from the **BASE Support** menu. The **Printer Files Setup** screen appears.

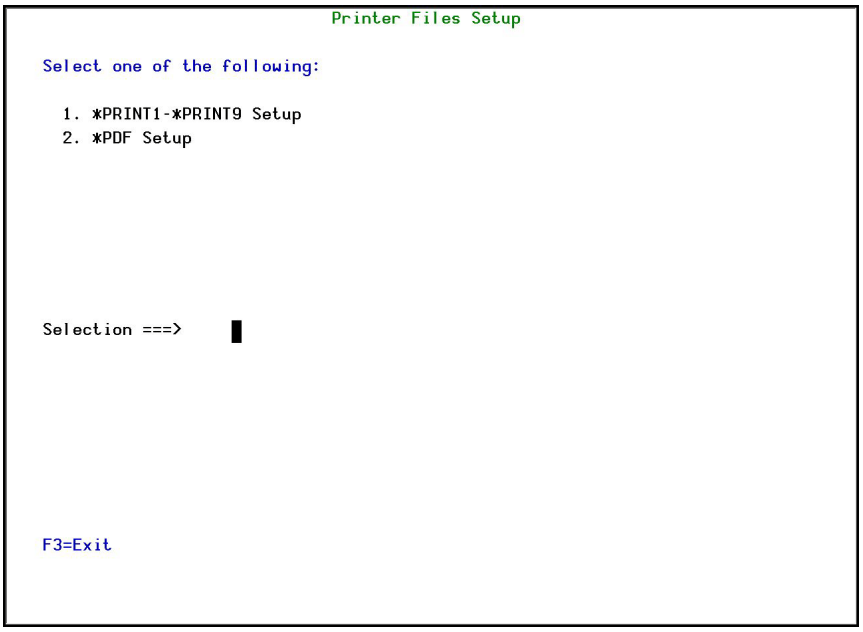


Figure 11-66. Printer Files Setup

2. Enter **2** and press **Enter**. The ***PDF Setup** screen appears.

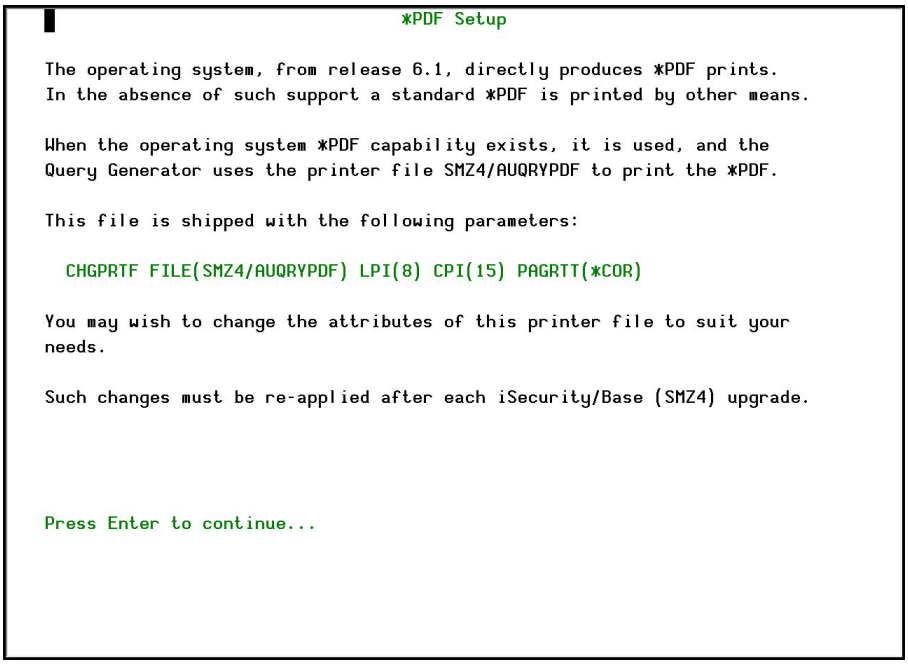


Figure 11-67. *PDF Setup

3. Follow the instructions on the screen.

NOTE: You must re-perform this task after every upgrade of **Firewall**.

Global Installation Defaults

You can set the parameters that iSecurity uses to control the Installation and upgrade processes.

1. Select **89 > 59. Global Installation Defaults**. The **Global Installation Defaults** screen appears.

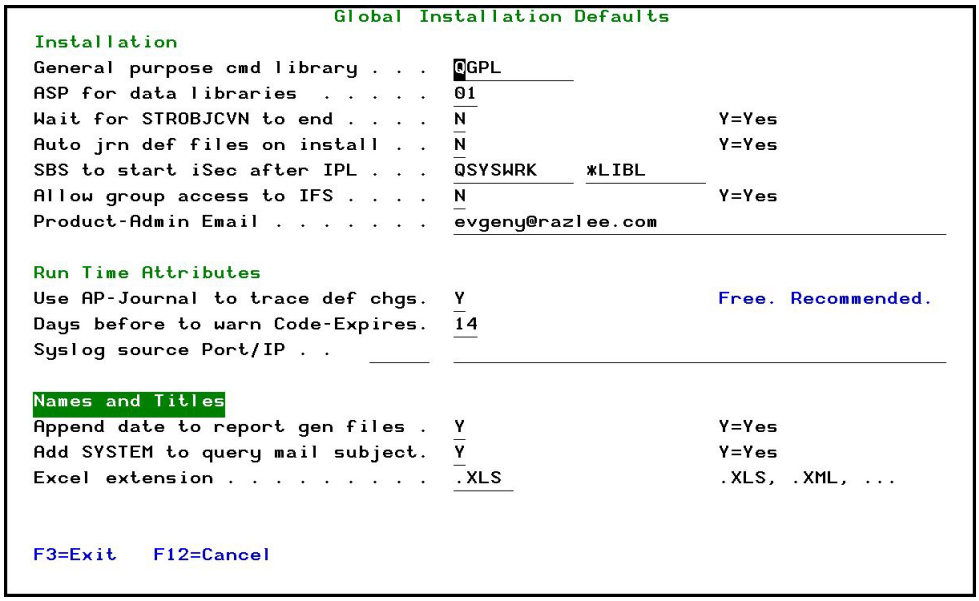


Figure 11-68. Global Installation Defaults

Parameter	Description
Installation:	
General purpose cmd library	An alternative library to QGPL from which all **STR***, **RUN***, and ***INIT** commands will be run.
ASP for data libraries	• Products being installed for the first time will be installed to this ASP. This refers to the product library and data library (for example, SMZ4, SMZ4DTA) • In some products such as AP-Journal, other libraries are created. For example, in the AP-Journal a library is created per application. When created you are prompted with the CRTLIB (Create Library) so that you can set the ASP number. • Change the current ASP of the library. All future upgrades will use this ASP. • All products will try to preserve the current ASP at upgrade time. Due to its sensitivity, you should check it.
Wait for STROBJCVN to end	**Y**=Yes **N**=No When installing the product on an OS400 version which is not the one that it was created for, objects require conversion and this is normally done in a batch job sent to work parallel to the installation. If you want the conversion to run inline, (wait until it ends), this field should be set to **Y**.
Auto jrn def files on install	Install auto journal definition files on installation.
SBS to start iSec after IPL	Use QSYSWRK or your own Subsystem for initial load of product.

Parameter	Description
Allow group access to IFS	**Y**=Yes **N**=No Allow access to IFS from group profiles.
Product-Admin Email	Admin email for follow-up.
Run Time Attributes:	The attributes of the run-time.
Use AP-Journal to trace def chgs.	**Y**=Yes **N**=No If you want to use the self-journaling option that will allow you to trace all changes made to iSecurity products, enter **Y**.
Days before to warn Code-Expires.	The number of days to warn prior to code expiry.
Syslog source Port/IP	Syslog source port number or IP address.
Names and Titles:	
Append date to report gen files.	Add date/s to report generation files.
Add SYSTEM to query mail subject.	Add system/s to query mail subject.
Excel extension	The extension to be used when creating Excel files **.XLS** **.XML**

2. Enter the required parameters and press **Enter**.

NOTE: You should not change any of the values in this screen without first consulting with Raz-Lee support staff at support@razlee.com.

Network Support

Work with Network Definitions

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 files that can be sent via email.

1. Select **89 > 71. Work with network definitions**. The **Work with Network Systems** screen appears.

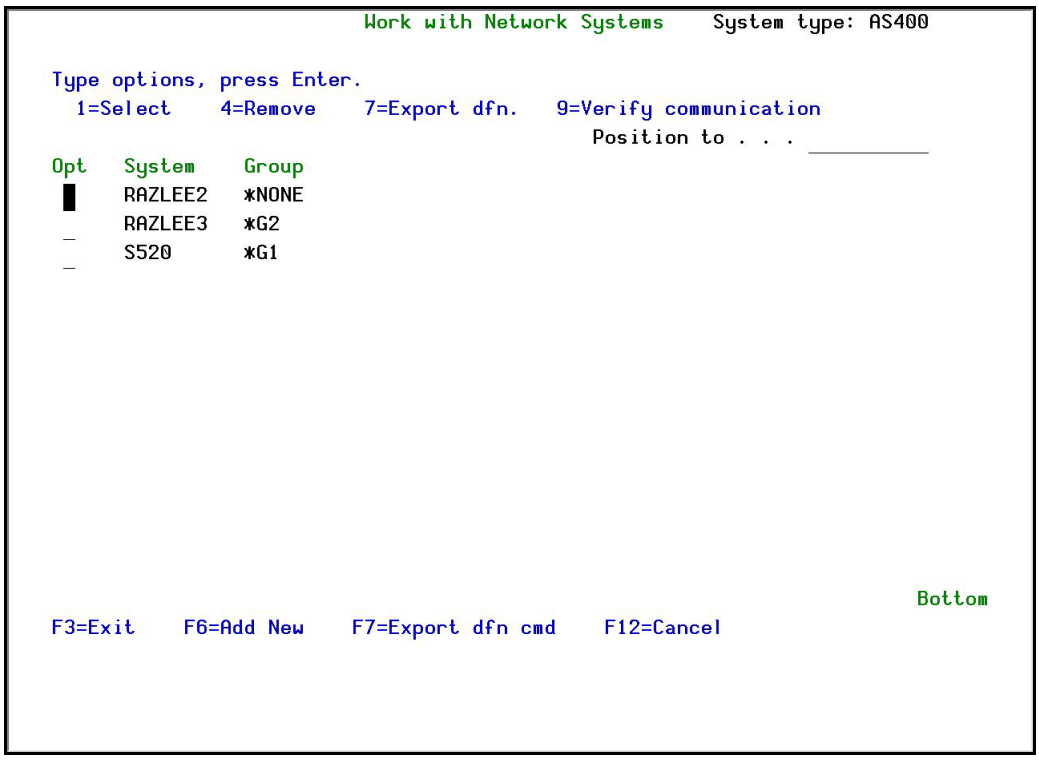


Figure 11-69. Work with Network Systems

2. Press **F6** to define a new network system to work with. The **Add Network System** screen appears.

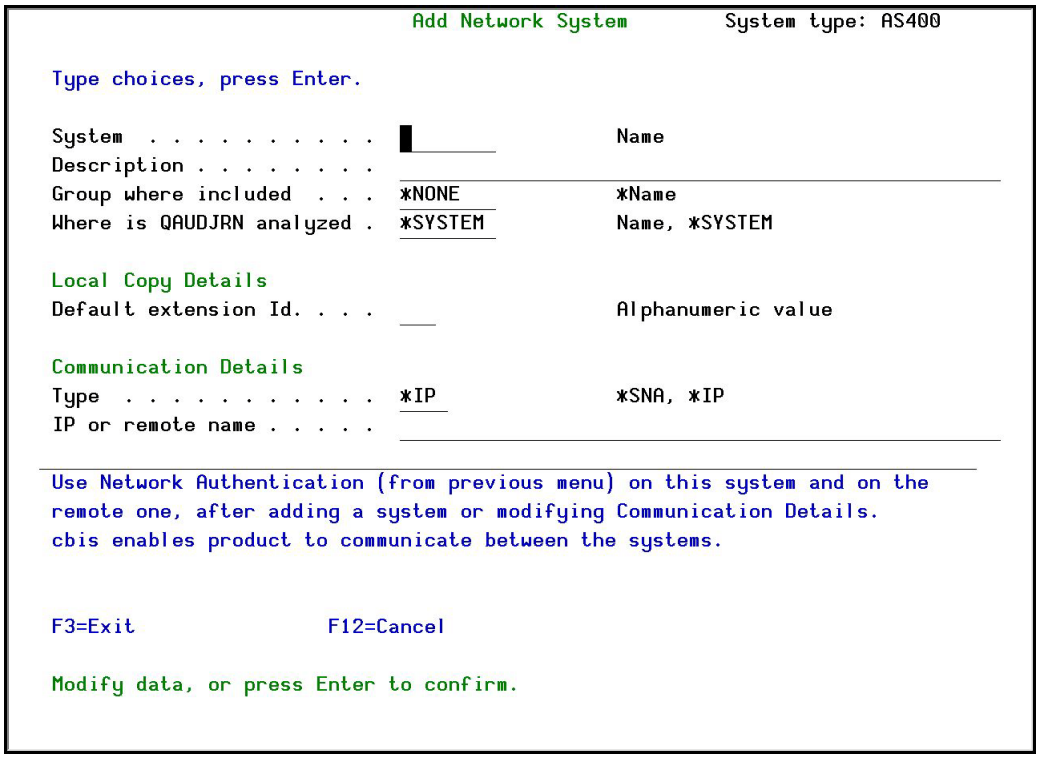


Figure 11-70. Add Network System

Parameter	Description
System	The name of the system
Description	A meaningful description of the system
Group where included	Enter the name of the group to which the system is assigned
Where is QAUDJRN analyzed	Give the name of the System where QAUDJRN is analyzed. Enter *SYSTEM if it is analyzed locally.
Default extension ID	Enter the extension ID for local copy details
Type	The type of communication this system uses ***SNA** ***IP**
IP or Remote Name	Enter the IP address or SNA Name, depending on the **Type** of communication you defined

3. Enter your required definitions and press **Enter to confirm**.

Network Authentication

To perform activity on remote systems, you must define the user SECURITY2P with the same password on all systems and LPARS with the same password.

Product options which require this are:

- referencing a log or a query with the parameter SYSTEM()
- replication user profiles, passwords, system values
- populating definitions, log collection, and so on

To authenticate the system:

1. Select **89 > 72. Network Authentication**. The **Network Authentication** screen appears.

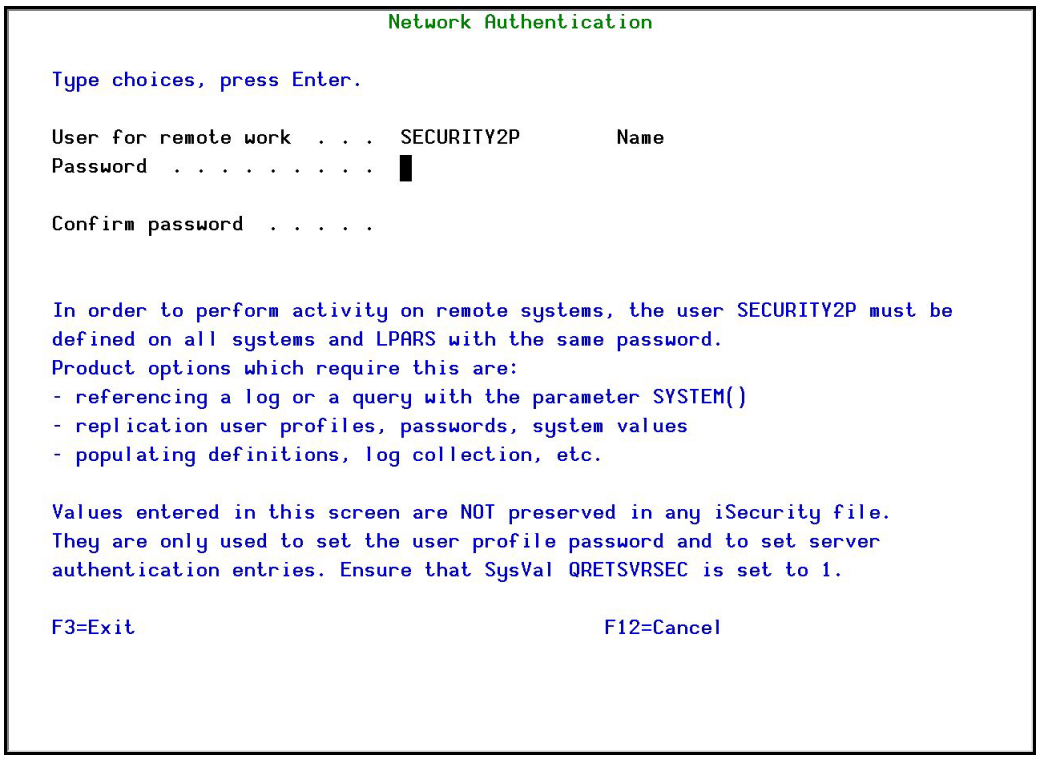


Figure 11-71. Network Authentication

2. Enter the SECURITY2P user password twice and press **Enter**.

NOTE: The values entered in this screen are NOT preserved in any iSecurity file; they are only used to set the user profile password and to set server authentication entries. Ensure that the **Return Server Security Data** system value (**QRETSVRSEC**) is set to **1** (Retain Data).

Check Authorization Status

You can set up the system so that the local *SYSOPR will get messages for all network wide authority problems.

Before you run this command, you must allow the system to run network commands and scripts. See Run CL Scripts on page 274 for more details.

1. Select **89 > 73. Check Network Authority Status**. The **Check Razlee Authorization** screen appears.

```
                    Check Raz-Lee Authorization (CHKISA)

Type choices, press Enter.

Product or *ALL  . . . . . .  *ALL          *ALL, AU, NS, GR, CA, JR...
System to run for  . . . . .  *CURRENT      Name, *CURRENT, *group, *ALL..
Inform *SYSOPR about problems .  *NO        *YES, *NO
Days to warn before expiration    *DFT      Number, *DFT

                          Additional Parameters

Sent from  . . . . . .  *NO          Character value, *NO
By job number  . . . . . .  *NO      Character value, *NO

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

Figure 11-72. Check Raz-Lee Authorization

Parameter	Description
Product or *ALL	***ALL** = report on all products **AU** = Audit **NS** = Native Object Security **GR** = Firewall **CA** = Capture **JR** = AP-Journal **OD** = Authority On Demand **AV** = Anti-Virus **CT** = Change Tracker **DB** = DB-Gate **VW** = View
System to run for	The system to run the authorization check for: **Name** = The name of a specific system in the network ***CURRENT** = The current system ***group** = The name of a group of systems ***ALL** = All systems in the network
Inform *SYSOPR about problems	***YES** = ***NO** =

Parameter	Description
Days to warn before expiration	**Number** = Any system whose expiry date is less than this number of days will be reported. The default number of days is 14. ***DFT**
Sent from	Value ***NO**
By job number	Value ***NO**

2. Enter your required options and press **Enter**.

Send PTF

This option allows you to run of a set of commands that will send objects as a PTF. This option is restricted to iSecurity products only. If you need to send PTFs for other products, please contact Raz-Lee Support.

Before you can use this option, ensure that you define the entire network, as described in Work with Network Definitions on page 268, and that you define user SECURITY2P on all nodes, using the same password, as described in Network Authentication on page 269.

To send PTFs:

1. Select **89 > 74. Send PTF**. The **iSecurity Send PTF** screen appears.

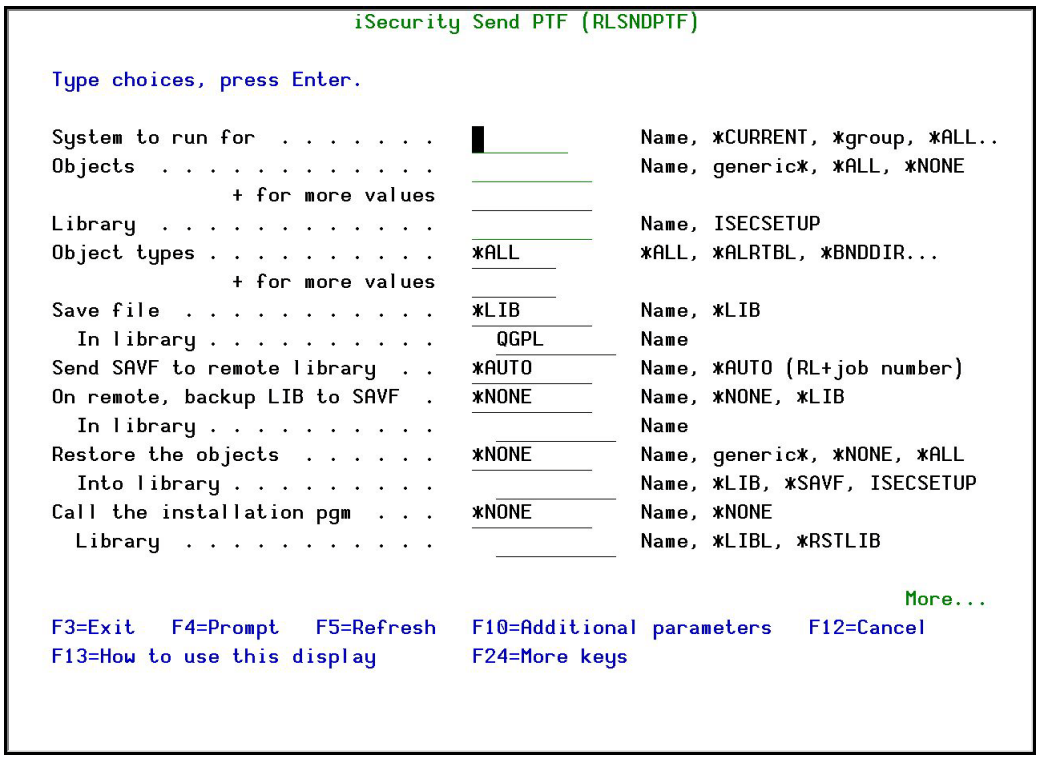


Figure 11-73. iSecurity Send PTF

Parameter	Description
System to run for	The system to run the authorization check for: **Name** = The name of a specific system in the network ***CURRENT** = The current system ***group** = The name of a group of systems ***ALL** = All systems in the network
Objects	The objects you want to send. You can enter multiple values Name = A specific object generic* = A group of objects with the same prefix *ALL= All the objects *NONE= No objects need to be extracted, the SAVF has already been prepared
Library	The name of the library that contains the objects
Object types	The object types to be sent
Save file / Library	The name and library of the SAVF to contain the objects. If you enter ***LIB** for the file name, the name of the library containing the objects will be used. If you enter ***AUTO** as a name for the library, a library will be created with the name of RL<*jobnumber*>
Remote library for SAVF	The name of the remote library to receive the SAVF to contain the objects. If you enter ***AUTO** as a name for the library, a library will be created with the name of RL<*jobnumber*>

Parameter	Description
Restore objects	The objects to be restored **Name** = A specific object **generic*** = A group of objects with the same prefix ***ALL**= Restore all objects ***NONE**= Do not restore any objects
Restore to library	The name of the library to receive the restored objects **Name** = A specific library ***LIB** = the name of the original library containing the objects will be used. ***SAVF**= the same name as the SAVF
Program to run / Library	The name and library of a program to run after the objects have been restored.
Parameters	The parameters for the program that runs after the restore.

2. Enter the required options and press **Enter**.

Run CL Scripts

This option allows you to run of a set of commands either from a file or by entering specific commands as parameters. Each command must be preceded by a label:

LCL: Run the following command on the local system

RMT: Run the following command on the remote system

SNDF: Send the save file (format: library/file) to RLxxxxxxxx/file (xxxxxxxx is the local system name)

You can use this option to define the commands to run to check system authorities, as described in Check Authorization Status on page 271.

Before you can use this option, ensure that you define the entire network, as described in Work with Network Definitions on page 268, and that you define user SECURITY2P on all nodes, using the same password, as described in Network Authentication on page 269.

1. Select **89 > 75. Run CL Scripts**. The **iSecurity Remote Command (RLRMTCMD)** screen appears.

```
                    iSecurity Remote Command (RLRMTCMD)

Type choices, press Enter.

System to run for  . . . . . .  *CURRENT     Name, *CURRENT, *group, *ALL..
Starting system  . . . . . .    *START       Name, *START
Ending system  . . . . . .      *END         Name, *END
Allow run on local system  . . .  *YES       *NO, *YES
Source file for commands . . . .  *CMDS      Name, *CMDS
  Library  . . . . . .                       Name, *LIBL
Source member  . . . . . .                   Name
Cmds-LCL:cmd RMT:cmd SNDF:savf

                + for more values

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

Figure 11-74. iSecurity Remote Command

Parameter	Description
System to run for	The system to run the authorization check for: **Name** = The name of a specific system in the network ***CURRENT** = The current system ***group** = The name of a group of systems ***ALL** = All systems in the network
Starting system	Use to define a the start of a subset within ***group** or ***ALL** This is useful if you want to rerun a command that previously failed
Ending system	Use to define a the end of a subset within ***group** or ***ALL** This is useful if you want to rerun a command that previously failed
Allow run on local system	***YES** = The remote command can run on the local system ***NO** = The remote command cannot run on the local system
Source file for commands	**Name** = The file where the commands to run are stored. ***CMDS** = Use the commands entered below
Library	**Name** = The library that contains the commands source file ***LIBL** =

Parameter	Description
Source member	**Name** = The member that contains the commands
Cmds -LCL:cmd RMT:cmd SNDF:savf	The commands that can be run (if the **Source file for commands** parameter is ***CMDS**): **LCL:cmd** = A command that will be run on the local computer **RMT:cmd** = A command that will be run on a remote computer **SNDF:savf** =

2. Enter the required options and press **Enter**.

Current Job CntAdm Log

Select **89 > 76. Current Job CntAdm Messages** from the **BASE Support** menu to display the current job log.

All Job CntAdm Log

Select **89 > 77. All Jobs CntAdm Messages** from the **BASE Support** menu to display the job log for all jobs.

A

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 security-related exit points covered by iSecurity.

Note that some exit points are interconnected.

Exit Point	Description
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

Exit Point	Description
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_PWRDWNSYS	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
54.QIBM_QSO_ACCEPT	Enables a custom exit program to allow or deny incoming connections based on the restrictions set by the programs.
55.QIBM_QSO_CONNECT	Enables a custom exit program to allow or deny outgoing connections based on the restrictions set by the programs.
56. QIBM_QSO_LISTEN	Enables a custom exit program to allow or deny a socket the ability to listen for connections based on the restrictions set by the programs.