# iSecurity Firewall

## User Guide
## Version 18.26

www.razlee.com

# Contents

# About this Manual

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

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

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

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

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

## Intended Audience

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

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

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

## Native IBM i (OS/400) User Interface

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

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

## Conventions Used in the Document

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

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

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

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

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

***STRFW*** **> 81 > 32**

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

## Menus

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

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

## Data Entry Screens

Data entry screens include many convenient features such as:

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

The following describes the different data entry screens.

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

The following function keys may appear on data entry screens.

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

## Legal Notice

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

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



Manual Revised: Tuesday, March 12, 2024

## Contacts

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

# Introducing Firewall

Firewall is a comprehensive network security solution for the IBM i (AS/400). It completely secures your system against external threats initiated via the network and 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.

Although Firewall was not designed to protect your command line usage. It will secure *STRSQL* command line usage for 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, the 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

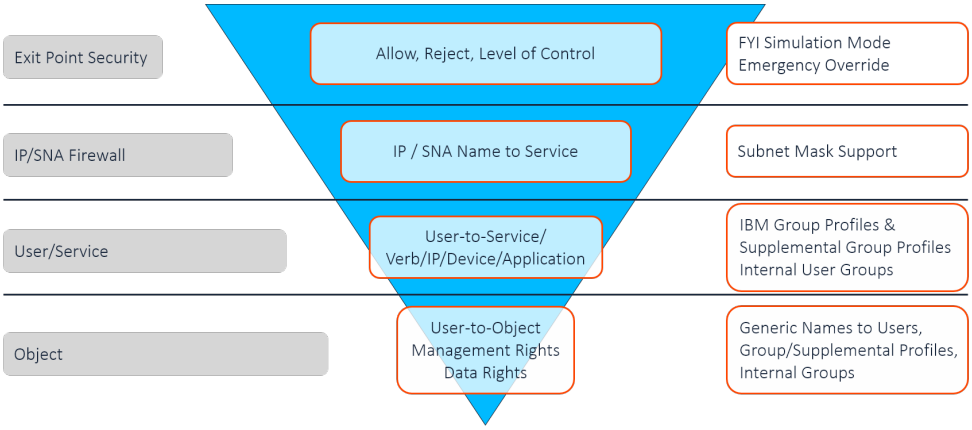
## Top-Down Security Design

Top-Down security design means that the process of designing and applying security rules follows the most efficient logical path possible. 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.

### Server Security

System i security is based on four basic levels:



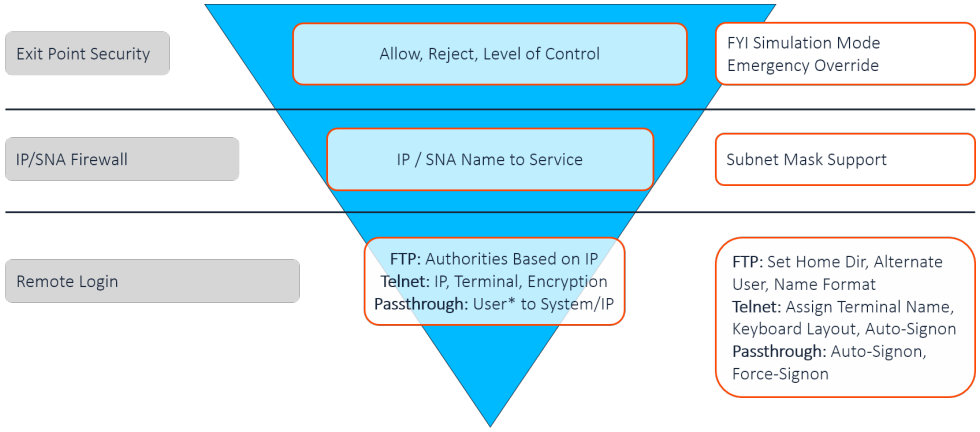

- Server/Exit Point Security
- TCP/IP Address Firewall Security
- User-to-Service Security
- Object Security

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.

### Logon Security

Logon security uses a similar set of levels, tailored to the specific requirements for logging in:




- Server/Exit Point Security
- IP/SNA Firewall
- Remote Login Security

## Multi Thread Support

Calling programs from threads other than the main one forces 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 designed to improve their capability to work in secondary threads when the relevant system APIs can use them.

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.

### FYI Simulation Mode

Using FYI Simulation Mode, you can 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. With this feature, you can test your rules under actual working conditions without adversely affecting user access.

FYI Simulation Mode may be enabled globally for all activity or enabled for individual function servers to test security rules for those servers without affecting rules that apply to others.

### Emergency Override

With the Emergency Override feature, you can temporarily override all existing security rules, allowing or rejecting all activity. This feature is useful when you need 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. With this user-friendly feature you can view historical activity together with the security rule currently in effect on a single screen. You 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 you install Firewall for the first time.

### Logging

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. You can display or print selected records from the Activity Log by entering the Display Firewall Log command (***DSPFWLOG***) on any command line or from numerous locations on Firewall menus and data screens.

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

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

No user, including QSECOFR, can 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.

Authorized users can:

- Set the number of days that data is kept online.
- Change the logging options for individual servers (exit points).
- Change the logging options per user.

## Query Wizard

With the powerful Query Wizard, you can design custom output reports that show exactly the data you need without programming or technical knowledge. You 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, HTML, or PDF file saved on the System i.

Using highly detailed filter criteria, you can select only the records you need by using Boolean operators and the ability to combine complex logical conditions. Firewall's flexibility enables you to specify the sort order according to multiple fields. All reports can run automatically and be e-mailed to the system administrator.

## 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.

## User Security

Firewall offers optimized basic user security. You can create a single user security definition in several ways:

### %Groups

Assign a user to a user group (similar to the option of selecting members for each of the user groups).

### Services

Same as the previous method of user-to-service definitions

### IP

Same as the Location group rules, but only applicable to single users.

### Device Names

Only for Telnet sign on. Same as Location group rules, but only applicable to single users

## Intrusion Detection

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

## 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 the F10 key 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 are.

- 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

# Getting Started with Firewall

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

NOTE: 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, you should carefully consider defining security rules that will maximize protection for your organization against intrusion and user abuse--without adversely affecting legitimate user access or system response time. Before beginning these steps, you should complete the process of identifying which specific servers and objects are to be protected and which users should be granted access rights to them.

To **install** Firewall and other iSecurity products, follow the steps in the iSecurity Installation Guide.

To **configure** Firewall and define your first security rules according to your organization's security policies, follow these steps, in order:

1. Obtain and enter the **authorization code** (temporary or permanent), as shown in "Configuring Firewall" on page 32, if you have not already done so.
2. **Start** Firewall, as shown in "Starting Firewall" on page 27.
3. Enable the **FYI Simulation Mode** on a global basis, as shown in "Running Firewall in FYI Simulation mode" on page 536.
4. Review the basic **system configuration** parameters and change those necessary to meet your organizational needs, as shown in "Configuring Firewall" on page 32.
5. 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, as shown in "Modifying Firewall Settings for Servers" on page 58.

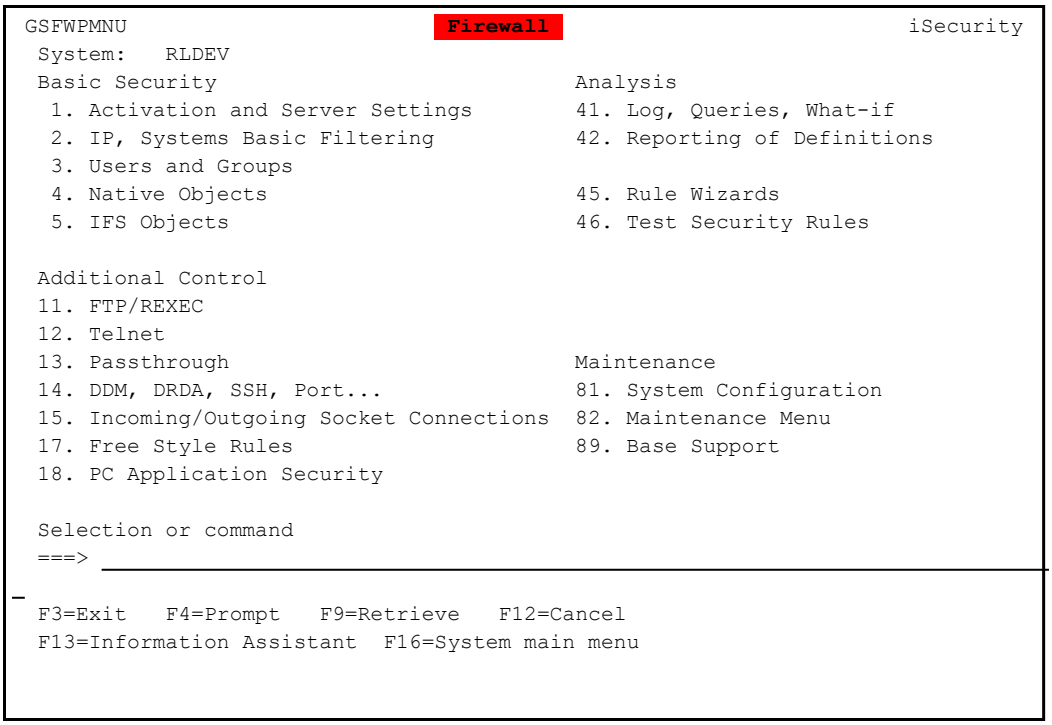
6. After a suitable period of activity (several days or weeks), use the Rule Wizards to analyze the logged activity and to **define security rules** based upon your organizational security policies, as shown in "Building Firewall Rules with the Rule Wizards" on page 437.
7. Use the Activity Log and the Query Wizard to **analyze activities** not covered by the Rule Wizards, as shown in "Adding and Modifying Queries" on page 476. Define appropriate rules based on this analysis.
8. **Create Users, User Groups and Time Groups** according to your organizational requirements, as shown in "Setting Firewall Rules for Users and Groups" on page 226.
9. 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.
10. **Disable the FYI Simulation Mode**, as shown in "Running Firewall in FYI Simulation mode" on page 536. From this point forward unauthorized user access will be blocked.

# Starting Firewall

To **start Firewall**, you must have the *SECOFR special authority.

Type the command ***STRFW*** (Start Firewall) on any command line.

The **Firewall Main Menu** appears.




To access many product features, you may also need to enter a product password. The default product password in **QSECOFR**. Change this password as soon as possible.

# Managing Operators' Authorities

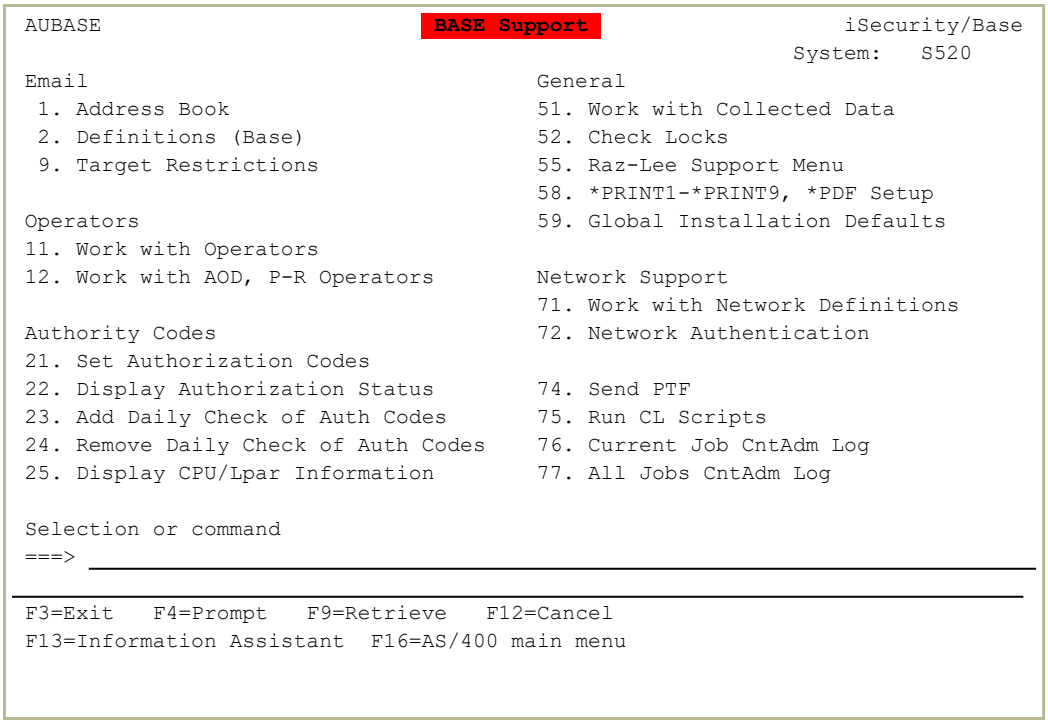
The iSecurity suite uses a single, standardized set of screens for managing operators' authorities.

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 **open** the **BASE Support** screen for iSecurity, select **89. Base Support** from the **Firewall Main Menu** (*STRFW* **> 89**).

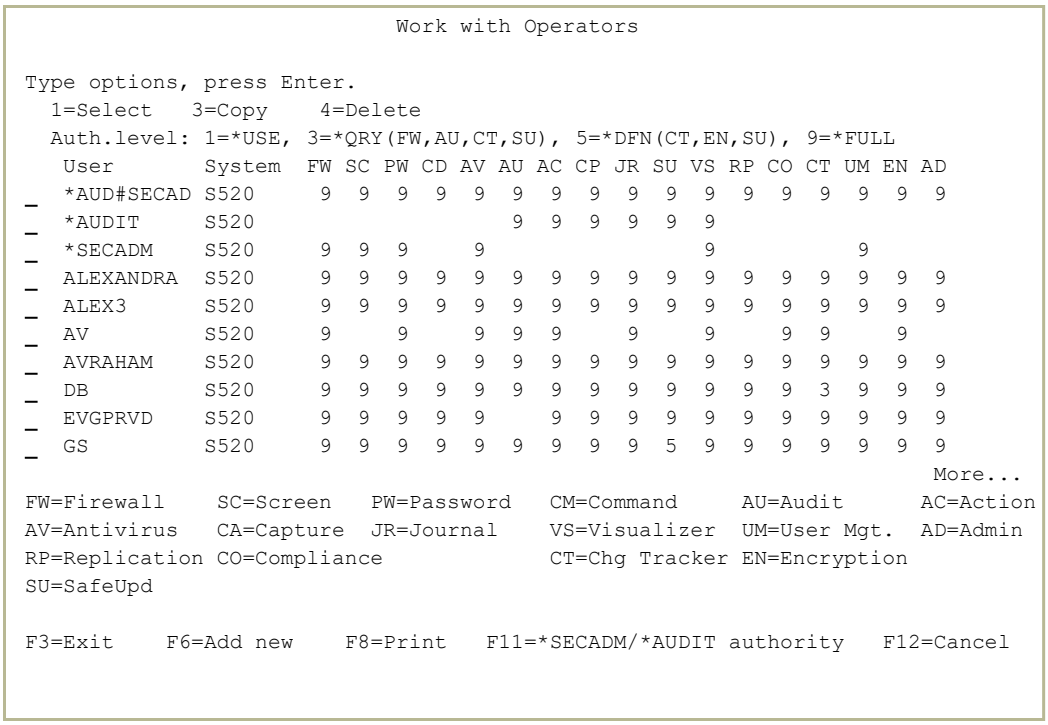
To **open** the **ATP Maintenance Menu** screen for iSecurity, select **82. Maintenance Menu** from the **Anti-Ransomware** screen (*STRFW* **> 82**).

The **BASE Support** screen appears:




To **manage operators' authorities**, select **11. Work with Operators** from the **BASE Support** screen.

The **Work with Operators** screen appears:




The body of the screen shows information on users and groups on the system. Each line shows the name of the user or group, the name of the system, and a series of columns corresponding to iSecurity products. The first, **FW**, shows the authority level for Firewall.

There are three default groups, shown at the top of the list:

- ***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 the Work with Operators screen 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.

To **modify an operator's authorities**, enter **1** in the **Opt** column for that operator.

The **Modify Operator** screen appears:

```
                              Modify Operator

Operator  . . . . . .    JOE
System  . . . . . .      S520             *ALL, Name
Password  . . . . . .    *SAME            Name, *SAME, *BLANK

Auth.level: 1=*USE, 3=*QRY(FW,AU,CT,SU), 5=*DFN(CT,EN,SU), 9=*FULL
Firewall  . . . . . FW 9        Screen  . . . . . SC 9
Password  . . . . . PW 9        Command . . . . . CD 9
AntiVirus . . . . . AV 9        Audit . . . . . AU 9
Action  . . . . . AC 9          Capture . . . . . CA 9
Journal . . . . . JR 9          Safe Update . . . . . SU 9
Visualizer  . . . . . VS 9      Replication . . . . . RP 9
Compliance  . . . . . CO 9      Change Tracker  . . . . . CT 9
User Management . . . . . UM 9  Encryption  . . . . . EN 9
Administrator . . . . . AD 9

The Report Generator is used by most modules and requires 1 or 3 in Audit.
Consider 1 or 3 for your auditors (with 3 they can create/modify queries).
*APR=Approver.


F3=Exit    F12=Cancel
```

The read-only **Operator** and **System** fields show the operator and system's names. If the settings are for all known systems and are to be imported automatically when the same operator is defined on a new system, the **System** field shows ***ALL**.

The **Password** field contains the user's password for iSecurity products, including Firewall. Possible values include:

- The password string itself.
- ***SAME**: The same as the user's system password.
- ***BLANK**: The password is empty.

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

  If the organization wishes to have the default to be ***BLANK** than they have to enter the command:

*CRTDTAARA SMZTMPC/DFTPWD *char 10*

The fields in the body of the screen show the user's authorization levels for each product.

The Firewall level is set in the numeric**Firewall...FW** field. Possible values are:

- **1=*USE**: The user can use Firewallbut cannot create or modify queries.
- **3=*QRY**: The user can use Firewall, including creating or modifying queries.
- **9=*FULL**: The user has full control over Firewall.

To add an operator, press the F6 key from the Work with Operators screen. The Add Operator screen appears, which is identical to the Modify Operator screen, except that you can enter values in the Operator or System fields.

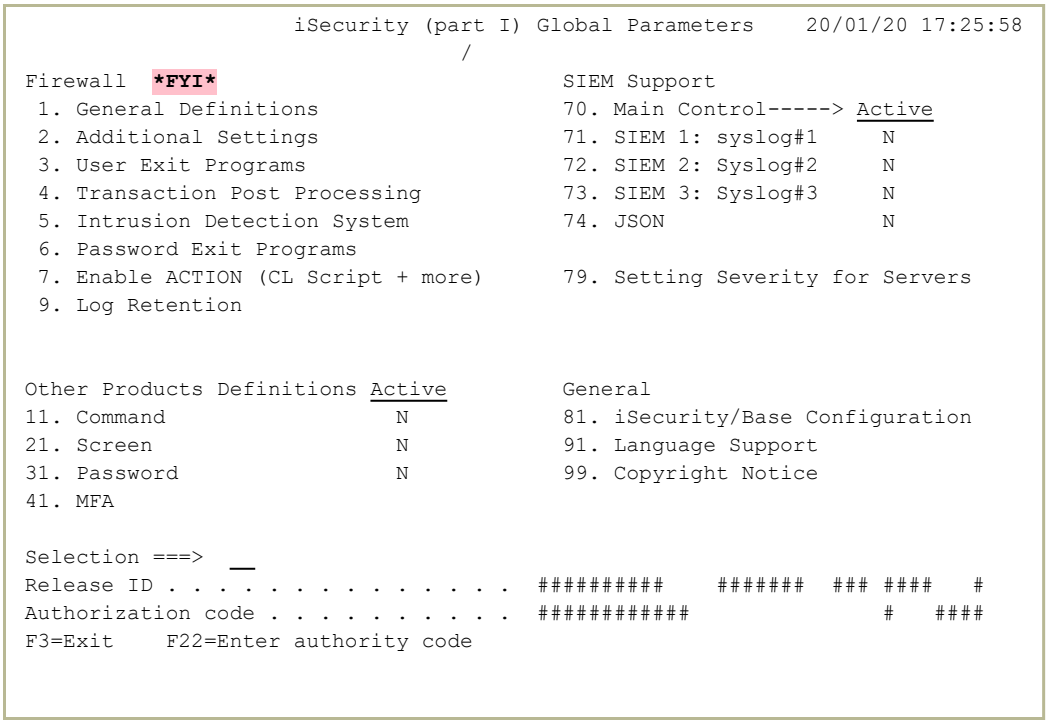
To copy an editor's authorities over all products, enter **3** in the **Opt** column for that operator on the Work with Operators screen. The Copy Operator screen appears, with the current operator and system in the **From:** area. Enter the new operator, system, and password in the **To:** area.

To delete a user's authorities for all the products, enter **4** in the **Opt** column for that operator on the Work with Operators screen. The Delete Operator screen appears, confirming that you wish to delete the user.

# Configuring Firewall

To **configure** Firewall, select **81. System Configuration** from the Firewall Main Menu.

The **iSecurity (part I) Global Parameters** screen appears:




To set **general definitions** for Firewall, including triggering emergency override or FYI simulation modes and determining the order in which logs and queries are displayed, select **1. General Definitions**. The **Firewall General Definitions** screen appears, as shown in "Setting General Definitions for Firewall" on page 42.

To set **additional definitions**, including aspects of SQL handling and whether to inherit certain in-product authorities, select **2. Additional Settings**. The **Firewall Additional Settings** screen appears, as shown in "Setting Additional Definitions for Firewall" on page 34.

To set the **programs called** after requests are accepted or rejected, for particular applications, or before the system is powered down, select **3. User Exit Programs**. The **Firewall User Exit Programs** screen appears, as shown in "Setting User Exit Programs for Firewall" on page 38.

To set the data queues used to bind Firewall with external products when transactions are accepted or rejected, select **4. Transaction Post Processing**. The Firewall Transaction Post Processing Data Queues screen appears, as shown in "Setting Data Queues for Post-Processing of Firewall Transactions" on page 40.

To set how Firewall reacts to intrusions, select **5. Intrusion Detection System**. The Firewall Intrusion Detection System screen appears, as shown in "Setting Up a Firewall Intrusion Detection System" on page 61.

To set the programs that supply and validate passwords for FTP and WSG, select **6. Password Exit Programs**. The Firewall Password Exit Programs screen appears, as shown in "Setting Password Exit Programs for FTP in Firewall" on page 41.

To enable or disable iSecurity Action for Firewall, select **7. Enable Action (CL Script + more)**. The Enable Real-Time Detection screen appears, as shown in "Enabling Action for Firewall" on page 46.

To set how long logs are retained and how they are backed up, select **9. Log Retention**. The Log & Journal Retention screen appears, as shown in "Setting Log Retention and Backup for Firewall" on page 48.

To enter your authorization code for Firewall, press the F22 (Shift+F10) key. Type the code in the **Authorization code** field, then press Enter.

## Setting Additional Definitions for Firewall

To set **further definitions** for Firewall (in addition to those shown in "Setting General Definitions for Firewall" on page 42), select **2. Additional Settings** from the **iSecurity (part I) Global Parameters** screen (*STRFW* **> 81**), as shown in "Configuring Firewall" on page 32.

The **Firewall Additional Settings** screen appears.

```
                        Firewall Additional Settings

Analyze cmds in QCMDEXC,QCAPCMD  . . .  SQL: Y  Rmt Cmd: Y  FTP: Y  DDM: Y
Analyze calls to QSYS,QGY pgms . . . .  SQL: Y  Rmt Pgm: N
Inherit In-product DB2 authorities . .  1  1=No, 2=Yes, 3=No, Usr/Grp found-stop
                                           4=Yes, Allowed only
Inherit In-product IFS authorities . .  1  1=No, 2=Yes, from higher dir,
                                           3=Yes, from higher dir or file*
                                           4=Yes, from higher dir Allowed only
Skip activities of user or grpprf  . .  __________  __________  __________
Skip SQL parsing if final decision was taken at (leave blank for parsing)
               Global level . . . . .  _  1=Always, 2=Allow, 3=Reject
               IP level . . . . . . .  _  1=Always, 2=Allow, 3=Reject
               User level . . . . . .  _  1=Always, 2=Selected users
               For 2: user or grpprf.  __________  __________  __________
Action for SQL that cannot be parsed .  1  1=Allow, 2=Allow+Extended log
                                           5=Reject, 6=Reject+Extended log
Log internal act: iSec, SYS, ShowCase.  N  Y=Yes, N=No
Log SQL Execute, Open & Fetch... stmts  N  Y=Yes, N=No

Check FTP Logon PWD by product . . . .  N  Y=Yes (not recommanded), N=No

F3=Exit   F12=Previous
```

The screen contains the following fields:

**Analyze cmds in QCMDEXC,QCAPCMD**

Enables analysis of commands within the defined servers (**SQL**, **Remote CMD**, **FTP**, and **DDM**) when these commands are called by *QCMDEXC* or *QCAPCMD*. With this analysis, you see calls to other programs/commands that are embedded within *QCMDEXC* or *QCAPCMD*.

There are four subfields, for

- **SQL**
- **Rmt Cmd** (Remote CMD)
- **FTP**
- **DDM**

Possible values for each are:

- **Y**: Analyze commands called for this server within *QCMDEXC* and *QCAPCMD*. (Recommended.)
- **N**: Do not analyze commands.

**Analyze calls to QSYS,QGY pgms**

Enables analysis of programs that reside in the *QSYS* library within the SQL and Remote Program servers. Such calls are normally permitted calls to APIs and should not need analysis.

There are subfields for the two servers, **SQL** and **Rmt Pgm**.

Possible values for each are:

- **Y**: Analyze the program calls.
- **N**: Do not analyze the program calls. (Recommended.)

**Inherit In-product DB2 authorities**

More specific authority takes preference over more generic authority concerning the object name in Native Object Security.

The field has these possible values:

- 1: No
- 2: Yes
- 3: No, Usr/Grp found-stop
- 4: Yes, Allowed only

**Inherit In-product IFS authorities**

For IFS files, whether priority is given to the security for higher-level directories containing an object or to the more specific security rules for lower-level directories or generic files.

The field has these possible values:

- **1**: Give priority to lower-level directories, or to the generic or specific file's authorities.
- **2**: Give priority to higher-level directories' authorities.
- **3**: Give priority to higher-level directories or generic files' authority over that of lower-level directories or generic files.

**Skip activities of user or grpprf**

Up to three user profiles or group profiles whose activity is accepted without any Firewall checking.

**Skip SQL parsing if final decision was taken at**

Eliminate SQL parsing when not needed. This option can be activated based on the level on which the decision was taken and the type of the decision.

If the system decided at the **Global** or **IP** level whether to accept or reject the SQL activity, it could still decide to parse the SQL afterward. In that case:

- **(blank)** : Regardless of the decision, it never skips parsing the SQL
- **1**: Regardless of the decision, it always skips parsing the SQL.
- **2**: If the decision was to allow the activity, it skips parsing the SQL.
- **3**: If the decision was to reject the activity, it skips parsing the SQL.

If the decision was made at the **User** level:

- **(blank)** Regardless of the decision, it never skips parsing the SQL
- **1**: Regardless of the decision, it always skips parsing the SQL.
- **2**: Regardless of the decision, it skips parsing for up to three users or groups listed on the next line.

**Action for SQL that cannot be parsed**

Take these actions if Firewall cannot parse the commands within an SQL statement.

- **1**: Allow the transaction.
- **2**: Allow the transaction and write the unparsed SQL statement to an extended log.
- **5**: Reject the transaction
- **6**: Reject the transaction and write the unparsed SQL statement to an extended log.

**Log internal act: iSec, SYS, ShowCase.**

Whether to log internal activity by other iSecurity products, the operating system, and ShowCase. This is usually set to **N**.

**Log SQL Execute, Open & Fetch... stmts**

Whether to log the SQL Execute, Open, and Fetch statements. Since these are already scanned when the SQL statement is prepared, this can usually be set to **N**.

**Check FTP Logon PWD by product**

Whether Firewall should check logon passwords rather than letting the operating system do it.

## Setting User Exit Programs for Firewall

To set **user exit programs** for Firewall, select **`3. User Exit Programs`** from the **iSecurity (part I) Global Parameters** screen (*STRFW* **`> 81`**), as shown in "Configuring Firewall" on page 32.

The **Firewall User Exit Programs** screen appears.

```
                        Firewall User Exit Programs

Type options, press Enter.

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

  Enable Application Level Security    *STD______          Name, *NONE, *STD
    Library . . . . . . . . . . . .    __________          Name, *LIBL
  GUI product identifies itself and continues without farther inspections.
  For *STD value initial identification program SMZ8/GSASTDR should be
  called for Remote Server and SMZ8/GSASTDPROC for SQL Server.
  Call parameters are:
  <Application name> - *CHAR 20, <Identification key> - *CHAR 50

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

F3=Exit   F12=Previous
```

In each of the three cases on this screen, you can enter:

- The name of a program (or **`*NONE`**)
- The name of the library containing the program (or **`*LIBL`**)

You can set exit programs for:

**`Allow/Reject Request`**

An additional check done after Firewall accepts or rejects an access request. The result of the program can override the earlier decision.

**`Enable Application Level Security`**

Which program to use to check application passwords.

To use **standard programs** (SMZ8/GSASTDR for Remote Server or SMZ8/GSASTDPROC for SQL Server), set the field to ***STD**.

To **use a different program**, enter its name in this field and its library in the **Library** subfield.

**Pre Power Down System**

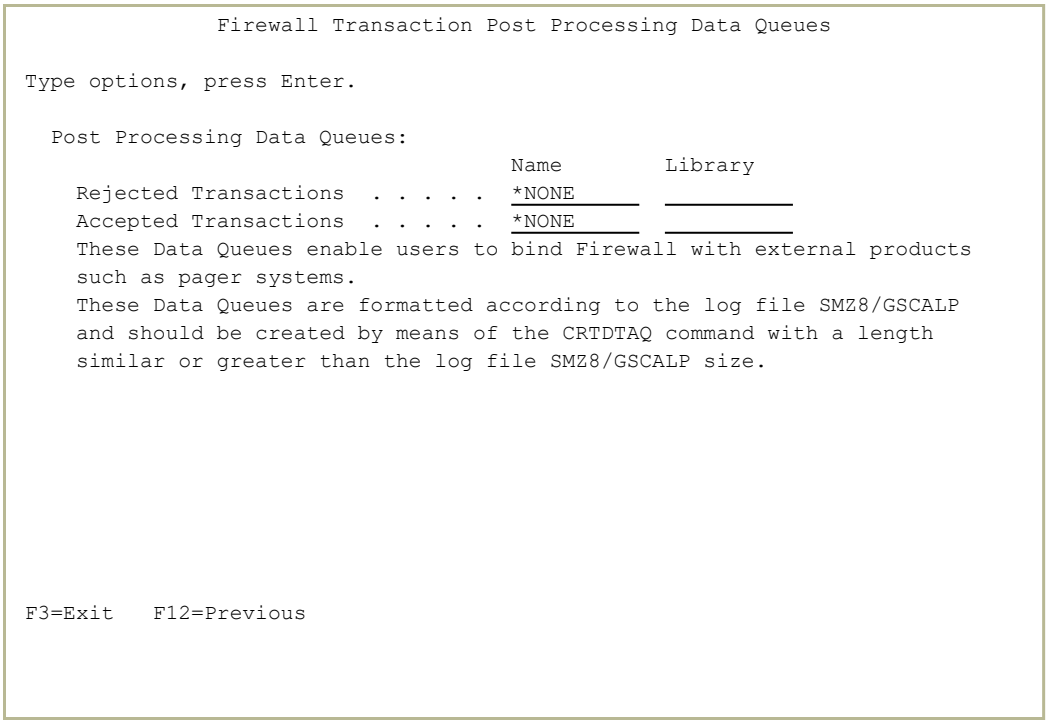
A program run before the system powers down.

NOTE: You can also set user exit programs for specific servers, as shown in "Modifying Firewall Settings for Servers" on page 58.

# Setting Data Queues for Post-Processing of Firewall Transactions

To set the **data queues** used to bind Firewall with external products when transactions are accepted or rejected, select **4. Transaction Post Processing** from the **iSecurity (part I) Global Parameters** screen (*STRFW* **> 81**), as shown in "Configuring Firewall" on page 32.

The **Firewall Transaction Post Processing Data Queues** screen appears.




The screen contains fields for the **Name** and **Library** of the data queues to be used for **Rejected Transactions** or for **Accepted Transactions**.

If no data queue is used for either case, set the **Name** field to ***NONE**.

These data queues should be created by means of the *CRTDTAQ* command and be formatted according to the log file SMZ8/GSCALP, with a length equal or greater to that of the log file.

## Setting Password Exit Programs for FTP in Firewall

To **set the programs that Firewall users to validate passwords** for FTP access, select **`6. Password Access Programs`** from the **iSecurity (part I) Global Parameters** screen (*STRFW* **`> 81`**), as shown in "Configuring Firewall" on page 32.

Firewall uses these programs if the **`Validation Password`** or **`Alt Password`** fields for *ALTLOGON are set to **`*PGM`** in the **Add FTP/REXEC User** screen (shown in "Adding a User for Incoming FTP/REXEC Logons" on page 71) and related screens.

The **Firewall Password Exit Programs** screen appears.

```
                      Firewall Password Exit Programs

Type options, press Enter.

  Incoming Password Validation  . .    *NONE       Name, *NONE
    Library . . . . . . . . . . . .    _____       Name, *LIBL
  This program validates the incoming passwords for FTP, if *PGM is specified.
  Example program SMZ8/GRSOURCE PWPWDE#A.


  OS/400 Actual Password supplier .    *NONE       Name, *NONE
    Library . . . . . . . . . . . .    _____       Name, *LIBL
  This program supplies the system password for FTP/WSG, if *PGM is specified.
  Example program SMZ8/GRSOURCE PWPWDE#A.




F3=Exit   F12=Previous
```

The screen contains fields for a program name and **Library** for **`Incoming Password Validation`** and the **`OS/400 Actual Password supplier`**. The program SMZ8/GRSOURCE PWPWDE#A can serve as an example for each.

## Setting General Definitions for Firewall

To set many **definitions affecting Firewall**, select **`1. General Definitions`** from the **Firewall General Definitions** screen (*STRFW* **`> 81 > 1`**), as shown in "Configuring Firewall" on page 32.

The **Firewall General Definitions** screen appears.

```
                        Firewall General Definitions

Type options, press Enter.
Emergency override ALL Security setting .  0      0=Regular (no override)
                                                  1=Allow        3=Reject
                                                  2=Allow+Log    4=Reject+Log
Work in *FYI* (Simulation) mode . . . . .  Y      Y=Yes, N=No
*FYI* is an acronym for "For Your Information". In this 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 Group and Supplemental profile  . .  Y      Y=Yes, N=No

Enable Super Speed Processing . . . . . .  Y      Y=Yes, N=No
The functionality of the product is not affected by this setting.
Set this value to N, well before you plan a "Hot Upgrade" of the product.
This will enable temporary suspension of the activity during installation.
Hot upgrade is safe . . . . . .  N      (See manual)
Wizard Group by . . . . . .  4      1=*USER  2=*GRPPRF 3=*USRGRP
                                    4=*GROUP 5=*ALLGRP 6=*ALL
Start log display from  . . . . . .  N      N=Newest, O=Oldest
Start query display from  . . . . . .  O      N=Newest, O=Oldest

F3=Exit   F12=Previous
```

The screen contains the following fields:

**`Emergency override ALL Security setting`**

Use this in emergencies to override all settings. The values and results are the same as if using the **Firewall Emergency Override** window as shown in "Overriding Firewall Settings in Emergencies" on page 537

- **`0: Regular (no override):`** Obey all rules as usual. Leave the field set to this unless there is an emergency.
- **`1: Allow:`** Allow all activity without logging.
- **`2: Allow+Log:`** Allow all activity and log it.
- **`3: Reject:`** Reject all activity without logging.
- **`4: Reject+Log`**: Reject all access requests and log them. Use this setting to react to and trace intrusions.

**Work in *FYI* (Simulation) mode**

In FYI (For Your Information) Simulation mode, Firewall logs activity and its responses to it, but does not reject any activity or trigger other actions. You can use FYI mode to collect records of activity on your system that you can then use to train the Rule Wizards in creating Firewall rules that are optimized for your system.

To start FYI Simulation mode, set this field to **Y**.

To end FYI Simulation mode, set this field to **N**.

**Enable Super Speed Processing**

During normal activity, set **Enable Super Speed Processing** to **Y**. This keeps programs and their values in memory and keeps their files open, saving performance, since some tables are read into the memory at the beginning of each load. Files remain in memory for one minute (although they remained for ten minutes in the past). That duration is based on the minutes on the system clock rather than by counting sixty seconds. Thus, for example, a file read into memory at 00:00:30 would remain until 00:01:00 (not 00:01:30).

A transaction that arrives in a different minute is processed normally. The program ends after it closes all files and completely releases memory.

In general, this should be set at **Y** to allow for the faster processing. However, leaving files in memory prevents hot upgrades, in which new versions are loaded into memory while instances of the existing version are still running.

Set this field to **N** some time before you do a hot upgrade, to allow existing Firewall processes to complete and be cleared from memory.

**Hot upgrade is safe**

This read-only field is set to **N** if super speed processing has been enabled since the last hot upgrade. If it shows **N**, set the **Enable Super Speed Processing** field to **N**, wait for a reasonable time, then use the Work with Database SQL Server Jobs screen

(*STRFW* **> 1 > 29**) to see which jobs may have been loaded with Firewall and might need to be ended before the upgrade.

**Wizard Group by**

The default value by which report output is grouped, as used in the Report Wizards (*STRFW* **> 45 > 4-6** and **41-61**). Possible values are:

- ***USER**: Grouped by the user name.
- ***GRPPRF**: If a user is a member of a single group, the user's activity is included under the group.
  Otherwise, the activity is shown under the username.
- ***USRGRP**: If the user is a member of multiple groups, the user's activity is included under the first of those groups.
  Otherwise, the activity is shown under the username.
- ***GROUP**: If the user is a member of a single group, the user's activity is included under that group.
  Otherwise, if the user is a member of multiple groups, the user's activity is listed under the first of those groups.
  Otherwise (if the user is not a member of any groups), the activity is shown under the username.
- ***ALLGRP**: If the user is a member of a single group plus up to fifteen supplemental groups. the user's activity is shown for each of those groups.
- ***ALL**: If the user is a member of a single group plus up to fifteen supplemental groups. the user's activity is shown for each of those groups.
  Otherwise, if the user is a member of multiple groups, the user's activity is listed under the first of those groups.
  Otherwise (if the user is not a member of any groups), the activity is shown under the username.

**Start log display**

Sets the order in which records in log displays appear. Possible values are:

- **N**: Show the newest records first
- **O**: Show the oldest records first.

**Start query display**

Sets the order in which records in query results appear. Possible values are:

- **N**: Show the newest records first
- **O**: Show the oldest records first.

## Enabling Action for Firewall

To enable or disable iSecurity Action for Firewall, select **`7. Enable Action (CL Script + more)`** from the iSecurity (part I) Global Parameters screen (*STRFW* **`> 81`**), as shown in "Configuring Firewall" on page 32.

The Enable Real-Time Detection screen appears:

```
                          Enable Real-Time Detection

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

Action must be installed and running in order to take advantage of this
functionality.

Type options, press Enter.

  Enable ACTION for Firewall . .  1      4=By Server definition
                                         1=Global override - Stop using ACTION
                                         2=Global override - Send rejects
                                         3=Global override - Send all

  Enable ACTION for Screen . . .  Y      Y, N



F3=Exit  F12=Previous
```

The **`Enable ACTION for Firewall`** field can take these numeric values:

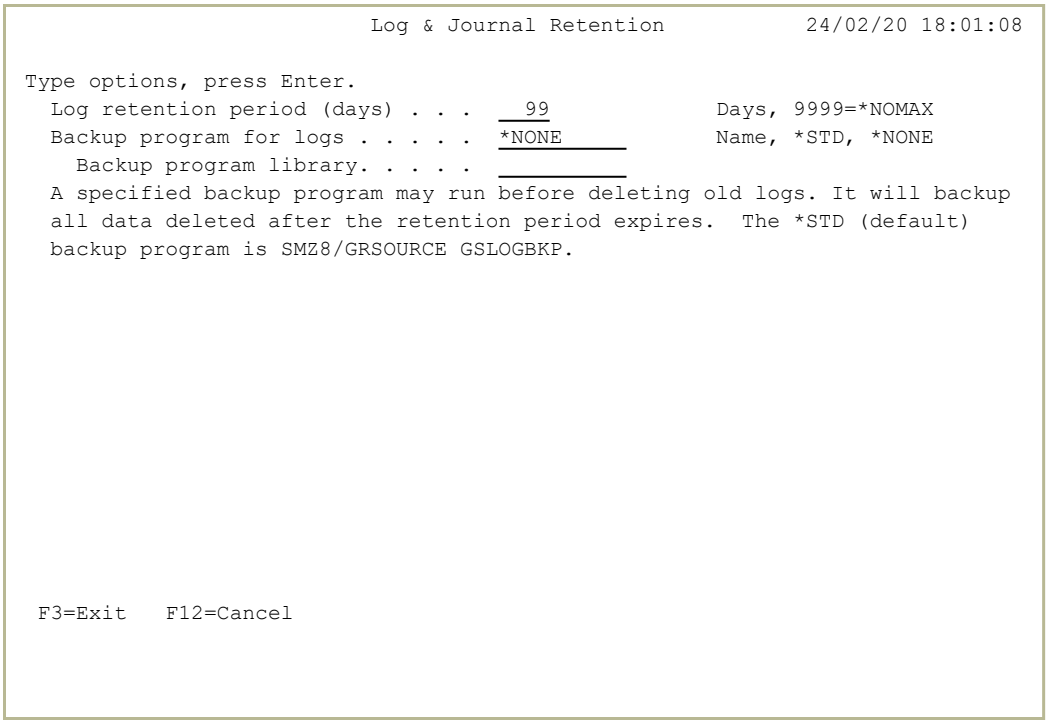
- **`1=Global override - Stop using ACTION`**: Sends no transaction messages to Action.
- **`2=Global override - Send rejects`**: Only sends messages about rejected transactions to Action.
- **`3=Global override - Send all`**: Sends messages about all transactions, either accepted or rejected, to Action.
- **`4=By Server Definition`**: Action is enabled or disabled for each server independently. You can set this via the Modify Server Security screen, as shown in "Modifying Firewall Settings for Servers" on page 58.

These choices are only effective if Action is installed and running on your system.

## Setting Log Retention and Backup for Firewall

To set how long logs are retained and how they are backed up, select **9. Log Retention** from the iSecurity (part I) Global Parameters screen (*STRFW* **> 81**), as shown in "Configuring Firewall" on page 32.

The Log & Journal Retention screen appears.

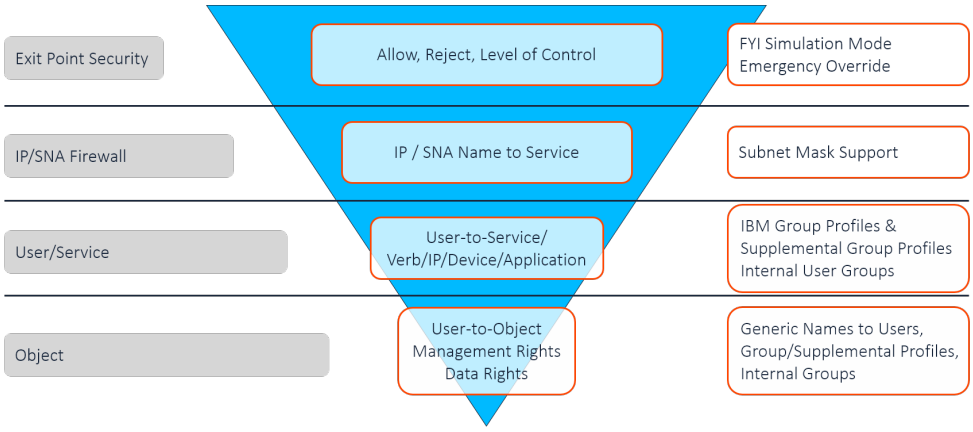



Set the **Log retention period (days)** field to the number of days for which you want logs to be retained on the system. If you set this to **9999**, logs are kept indefinitely.

In the **Backup program for logs** fields, you can set the name and library of a program to run before old logs are deleted. If you keep this at the default value of ***STD**, the backup program is *SMZ8/GRSOURCE GSLOGBKP*. If you set this to ***NONE**, no backup program is run.

# Creating and Modifying Firewall Rules

When a user requests access to an exit point on the IBM i, coming either from within the system or outside of it, Firewall uses its **layered security model** to test whether the access should be accepted or rejected.



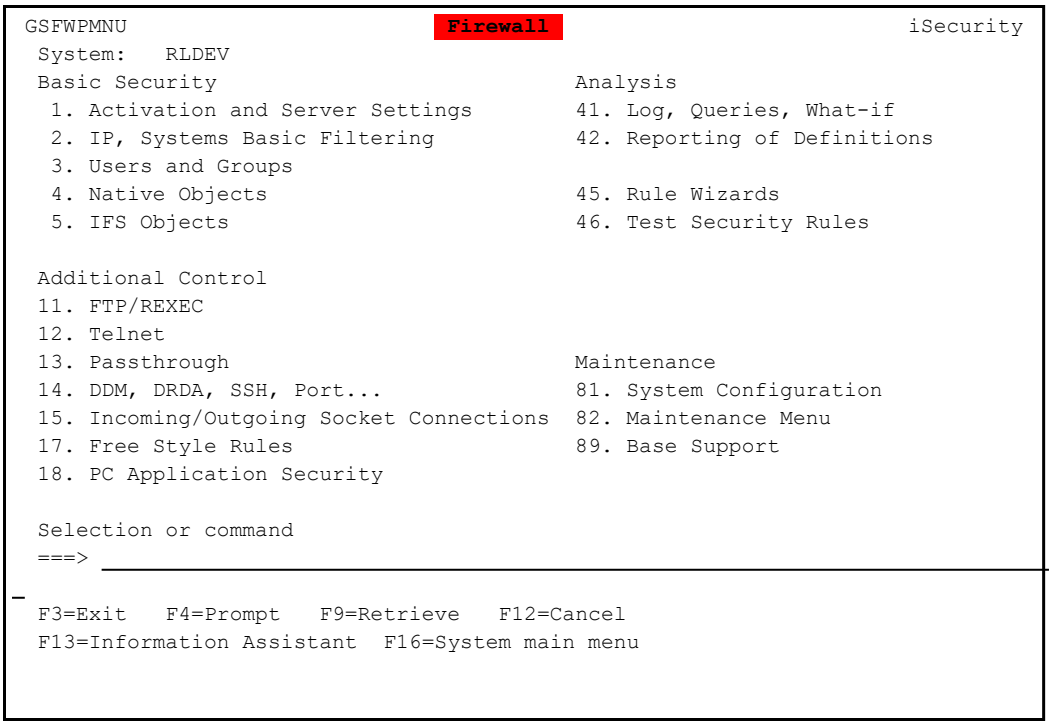

It first checks whether access to the **exit point** itself is allowed.

If that is accepted, it checks whether access from the **IP or IPv6 address or SNA system nam**e requesting incoming access or to the IP address to which the user is requesting outgoing access is allowed.

If that is also accepted, it checks whether the specific **user**, or the group to which the user belongs, is allowed to access that service.

Finally, if that is accepted, it checks whether access is allowed to the native or IFS **object** on the system is allowed.

The request is only accepted if it has passed all four layers of checks. If it fails any check, it is rejected without the need to check the layers further in.




You can create and modify the rules used to filter access at each level from the **Firewall** Main Menu (*STRFW*).

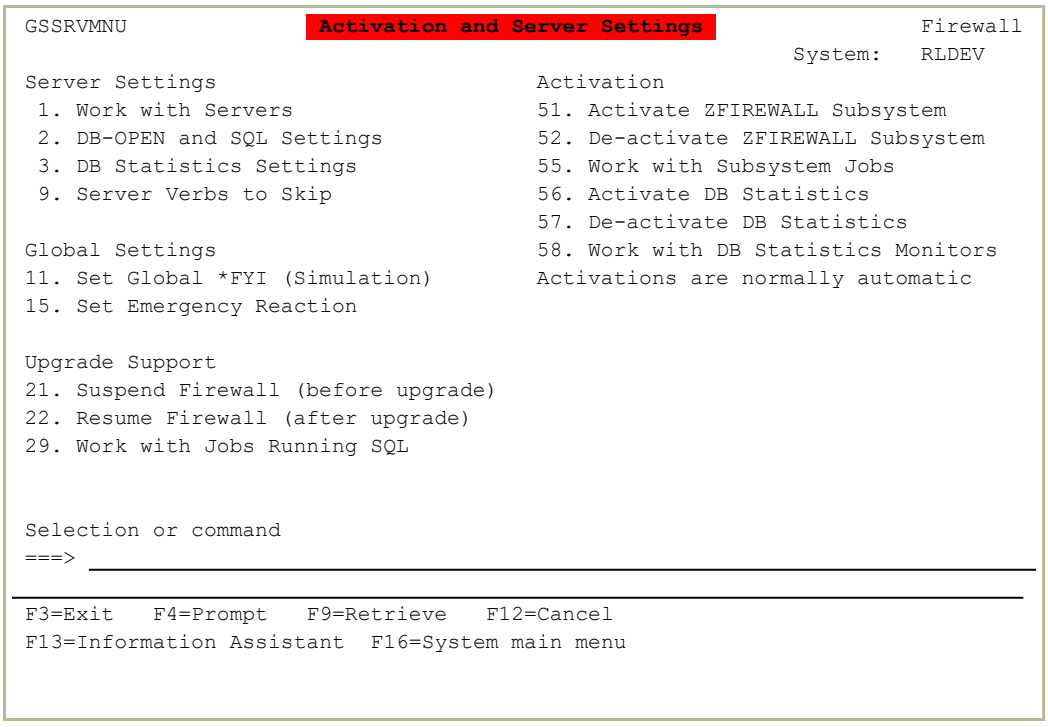
- To create and modify rules based on **exit points**, select **1. Activation and Server Settings** from the Firewall Main Menu. The **Activation and Server Settings** screen appears, as shown in "Setting Firewall Rules by Server" on page 52.
- To create and modify rules based on **IP and IPv6 addresses and remote system names**, select **2. IP, Systems Basic Filtering** from the **Firewall** Main Menu. The **Work with Dynamic Filtering** screen appears, as shown in "Setting Firewall Rules for IP Addresses or System Names" on page 154.
- To create and modify rules based on **users and groups**, select **3. Users and Groups** from the **Firewall** Main Menu. The **Work with Users** screen appears, as shown in "Setting Firewall Rules for Users and Groups" on page 226.
- To create and modify rules based on **native objects**, select **4. Native Objects** from the **Firewall** Main Menu. The **Native Object Security** screen appears, as shown in "Setting Firewall Rules for Native Objects" on page 305.

- To create and modify rules based on **IFS objects**, select **5. IFS Objects** from the **Firewall** Main Menu. The **IFS Security** screen appears, as shown in "Setting Firewall Rules for IFS Objects" on page 404.
- To create and modify rules for **PC applications** accessing the system, select **18. PC Application Security** from the **Firewall** Main Menu. The **Work with Client-Application Security** screen appears, as shown in "Securing PC Client Applications" on page 523.
- To **display definitions and to change rules for users, groups, and addresses**, select **42. Reporting of Definitions** from the **Firewall** Main Menu. The **Definitions** screen appears, as shown in "Displaying Definitions and Changing Occurrences of Users and Addresses" on page 466.

# Setting Firewall Rules by Server

The first layer at which Firewall filters activity is that of servers or exit points. To establish rules for these filters, select **1. Activation and Server Settings** from the Firewall Main Menu (*STRFW*).

The Activation and Server Settings screen appears:




The menu contains options regarding starting and stopping Firewall, working with database statistics, and other related matters. These options directly affect server settings.

To secure individual servers and establish related settings, select **1. Work with Servers**. The Work with Server Security screen appears, as shown in "Setting Firewall Rules for Servers" on page 54.

To create and modify settings for DB-OPEN and SQL, select **2. DB-OPEN and SQL Settings**. The Setting DB-OPEN and SQL screen appears, as shown in "Controlling DBOPEN and SQL Access" on page 148.

To control logging of database access statistics, select **3. DB Statistics Settings**. The Work with DB Statistics - Information to Record screen appears, as shown in "Recording Database Access Statistics" on page 530.

To specify verbs or subcommands that Firewall is to skip when checking activity on specific servers, select **9. Server Verbs to Skip**. The Skip Servers Subcommands screen appears, as shown in "Setting Server Verbs to Skip" on page 153.

To set additional controls for specific servers, including logon methods and license management, see "Setting Additional Firewall Controls for Specific Servers" on page 66

To set free-style rules, which run additional checks on servers based on a wider set of criteria, see "Setting Free-Style Firewall Rules for Servers" on page 457.

To activate statistics collection, select **56. Activate DB Statistics**. The Start DB Statistics Collection (STRDBSTT) screen appears. Press Enter to confirm that statistics collection is to begin. The DB#MON job in the ZFIREWALL subsystem starts.

To de-activate statistics collection, select **57. De-Activate DB Statistics**. The End DB Statistics Collection (ENDDBSTT) screen appears. Press Enter to confirm that statistics collection is to stop. The DB#MON job in the ZFIREWALL subsystem ends

To view and manage database statistics, select **58. Work with DB Statistics Monitors**. The DB Statistics - Monitors with Status screen appears, as shown in "Viewing Database Statistics" on page 521.

## Setting Firewall Rules for Servers

To set **Firewall rules for individual servers**, select **`1. Work with Servers`** from the **Activation and Server Settings** screen (*STRFW* **`> 1`**) as shown in "Setting Firewall Rules by Server" on page 52.

The **Work with Server Security** screen appears.

```
 Global *FYI* Mode Active Work with Server Security

 Type options, press Enter.                          Subset . . . . . _________
   1=Select  5=About Server  6=Display FW Log
                                                                          User
                  IP   Log FYI                                            Exit
Opt Secure Level    Free Act  Server                                      Pgm
 _  No                        Database Server - SQL access & Showcase  SQL
 _  No                        Open Database                           DBOPEN
 _  No                        Database Server - data base access      NDB
 _  No                        Database Server - object information    OBJINF
 _  No                        Remote Command/Program Call             RMTSRV
 _  No                        File Server (*)                         FILSRV
 _  No                        Telnet Device Initialization            TELNET
 _  No                        Telnet Device Termination               TELOFF
 _  Yes    Allow     Y  Y N Y Sign-On Completed (*)                   SIGNON
 _  No                        Original Data Queue Server              ORDTAQ
                                                                       More...
 (*) Changing the "Secure" parameter requires restarting Host Server or IPL
 Modify data, or press Enter to confirm.
 F3=Exit             F8=Print     F9=Object security   F10=Logon security
 F11=User security   F12=Cancel   F22=Global setting   F23=FYI    F24=Emergency
```

After the **`Opt`** column, it shows these fields for each server on the system:

**`Secure`**

- **`Yes`**: the server is secured by Firewall.
- **`No`**: the server is not secured by Firewall. The other fields, other than **`Server`**, are shown as empty.
  NOTE: If the field shows the value **`Other`**, an external program, other than Firewall, is registered on its exit point.

**`Level`**

The level of security for the server. Possible values are:

- **Allow**: All activity is allowed
- **Full**: Activity is checked based on both the user and the object being accessed. For Logon-related exit points, logon limitation rules (as shown in "Setting Additional Firewall Controls for Specific Servers" on page 66) are active. Otherwise, user limitation rules are active.
- **Usr>Srv**: Activity is checked based on the user
- **Reject**: All activity is rejected

**IP**

Whether outgoing IP addresses are checked.

- **Y**: Yes
- **[blank]**: No

**Free**

Whether to check for relevant Free-Style Rules (as shown in "Setting Free-Style Firewall Rules for Servers" on page 457).

- **Y**: Yes
- **[blank]**: No

**Log**

Whether activity is logged.

- **Y**: Yes
- **N**: No
- **R**: Rejected activity only

**Act**

Whether iSecurity Action reacts to activity.

- **Y**: Yes
- **N**: No
- **R**: Rejected activity only

**FYI**

Whether the server is running in FYI mode (as shown in "Running Firewall in FYI Simulation mode" on page 536)

- **Y**: Enable FYI mode for this server, regardless of whether FYI mode is enabled for Firewall in general.
- **[blank]**: Follow the general setting for Firewall.

**Server**

A long, free-form text name followed by the server's brief system-defined name.

If the long name ends in "(*)", changing the value of the **Secure** field requires restarting the server itself or a complete IPL.

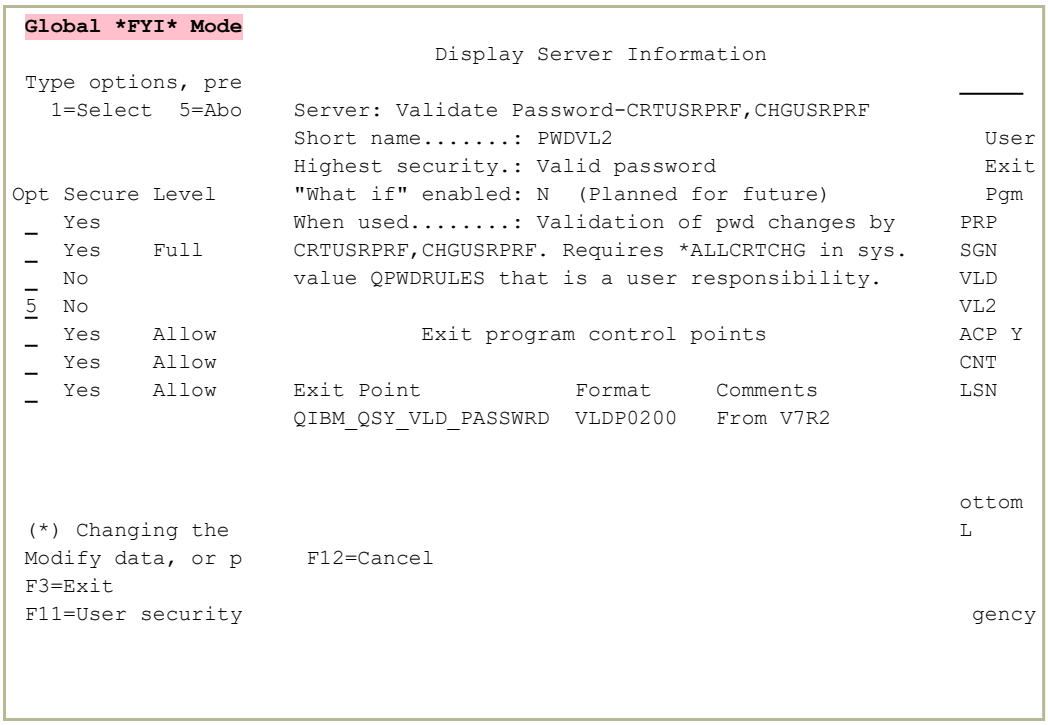
**User Exit Pgm**

Whether activity triggers a server-specific user exit program.

- **Y**: Yes
- **N**: No
- **[blank]**: default

To view more detailed information about the server's security settings and to modify them, type **1** in the **Opt** column for that server and press Enter. The Modify Server Security screen appears, as shown in "Modifying Firewall Settings for Servers" on page 58.

To see further information about the server, including its exit program control points, type **5** in the **Opt** column for that server and press Enter. The Display Server Information window appears:



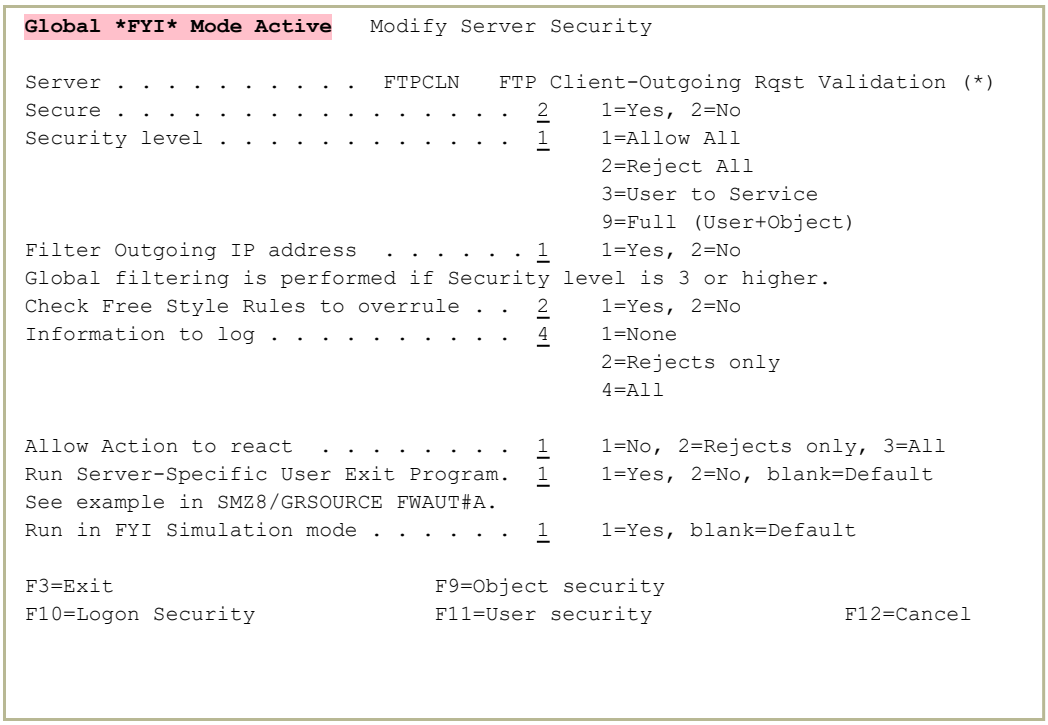
The window shows the highest security level for the server, whether FYI mode is enabled for it, and other important information. In the example it shows that the PWDLVL2 server requires that the user set the value **QPWDRULES** to ***ALLCRTCHG**.

To display the Firewall log for that server, type **6** in the **Opt** column for that server on the Work with Server Security screen and press Enter. The Display Firewall Log (DSPFWLOG) screen appears, as shown in "Displaying Firewall Logs" on page 516.

## Modifying Firewall Settings for Servers

To **view detailed information about the server's security settings and to modify them**, enter **1** in the **Opt** column for that server on the **Work with Server Security** screen (*STRFW* **> 1**) (as shown in "Setting Firewall Rules for Servers" on page 54).

The **Modify Server Security** screen appears:



```
Global *FYI* Mode Active   Modify Server Security

Server . . . . . .  FTPCLN   FTP Client-Outgoing Rqst Validation (*)
Secure . . . . . .  2    1=Yes, 2=No
Security level . . . . . .  1    1=Allow All
                                 2=Reject All
                                 3=User to Service
                                 9=Full (User+Object)
Filter Outgoing IP address  . . . . . 1    1=Yes, 2=No
Global filtering is performed if Security level is 3 or higher.
Check Free Style Rules to overrule . .  2    1=Yes, 2=No
Information to log . . . . . .  4    1=None
                                 2=Rejects only
                                 4=All

Allow Action to react  . . . . . .  1    1=No, 2=Rejects only, 3=All
Run Server-Specific User Exit Program.  1    1=Yes, 2=No, blank=Default
See example in SMZ8/GRSOURCE FWAUT#A.
Run in FYI Simulation mode . . . . . .  1    1=Yes, blank=Default

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

The screen contains the following many of these fields, depending on which parameters are applicable for that server:

**Server**

A brief, system-determined name for the server, followed by a free-form text description. If the field ends in "**(*)**", you must restart the server or IPL the system if you change its **Secure** status in the next field.

**Secure**

Whether the server is secured via Firewall.

- **1**: Yes
- **2**: No

**Security level**

The level of security for the server. Possible values are:

- **1**: All activity is allowed
- **2**: All activity is rejected
- **3**: Activity is checked based on the user. If you are using OS/400 Native Object Security, use this option to examine security based only on the user. If Native Object Security rejects the access, it remains rejected, even if user-based Firewall rules would accept it.
- **9**: Activity is checked based on both the user and the object being accessed. For Logon-related exit points, logon limitation rules (as shown in "Setting Additional Firewall Controls for Specific Servers" on page 66) are active. Otherwise, user limitation rules (as shown in "Setting Firewall Rules for Users and Groups" on page 226) are active. If you are using OS/400 Native Object Security, using Firewall object security via this option may be redundant and have no effect.

**Filter Outgoing IP address**

Whether server is filtered based on an outgoing IP address.

- **1**: Yes
- **2**: No

**Check Free Style Rules to overrule**

Whether to check for relevant Free-Style Rules (as shown in "Setting Free-Style Firewall Rules for Servers" on page 457)

- **Y**: Yes
- **[blank]**: No

**Information to Log**

Whether activity is logged.

- **1**: All
- **2**: Rejected activity only
- **4**: No

**Allow Action to react**

Whether iSecurity Action reacts to activity.

- **1**: All
- **2**: Rejected activity only
- **4**: No

**Run Server-Specific User Exit Program**

Whether activity triggers a server-specific user exit program.

- **1**: Yes (as shown in "Setting User Exit Programs for Firewall" on page 38)
- **2**: No
- **[blank]**: default

**Run in FYI Simulation mode**

Whether the server is running in FYI mode (as shown in "Running Firewall in FYI Simulation mode" on page 536)

NOTE: The SSHD server does not support FYI mode.

- **Y**: Yes
- **[blank]**: default, based on whether Firewall as a whole is running in FYI mode

## Setting Up a Firewall Intrusion Detection System

To set how Firewall **reacts to intrusions**, select **5. Intrusion Detection System**, from the **iSecurity (part I) Global Parameters** screen (***STRFW > 81***), as shown in "Configuring Firewall" on page 32.

The **Firewall Intrusion Detection System** screen appears:

```
                    Firewall Intrusion Detection System

Setting up an Intrusion Detection System:           Name        Library
Send rejects to message queue or QSYSOPR  . .       *NONE       __________
At the monitoring workstation, enter: CHGMSGQ DLVRY(*BREAK) SEV(0)
This causes rejection messages to break-in with a beep.

When intrusion is detected:                       | Real Mode  | *FYI Mode  |
End the offending interactive session . . . .     |     N      |     N      |
Send message to the user  . . . . . . . . . .     |     N      |     N      |
Disable user (F15 for exceptions) . . . . . .     |     N      |     N      |
Email Security Admin (Y, M=1/Min, D=6/Min)  .     |     N      |     N      |
  Email: ALEXM@RAZLEE.COM                                                   |
Run Action (If Action installed)  . . . . . .     | __________ |            |
Write to QAUDJRN (security audit journal) . .     |     N      |     N      |
Audit journal code is U. Journal entry type is FW. Data format: SMZ8/GSCALP

Screening of Allowed Activity:
Send allowed messages to message queue  . . .       *NONE       __________


F3=Exit   F12=Previous    F15=Disable exceptions
```

The screen contains the following sections and fields:

**Setting up an Intrusion Detection System**

**Send rejects to message queue or QSYSOPR**

Enter the **Name** and **Library** of a message queue to which rejects will be sent, or **QSYSOPR**.

If you are sending messages to a monitoring workstation, enter the command *CHGMSGQ DLVRY(*BREAK) SEV(0)* at the workstation to cause the messages to break in with a beep.

**When intrusion is detected**

These items have two fields apiece which take **Y** (yes) or **N** (no) values, except as noted. The fields under the label ***FYI Mode** control how Firewall responds to intrusions when it is running in

FYI simulation mode (as shown in "Running Firewall in FYI Simulation mode" on page 536). The fields under the label **Real Mode** control how Firewall responds when running normally.

**End the offending interactive session**

End the interactive session in which the intrusion occurred.

**Send a message to the user**

Send a message to the user of the session in which the intrusion occurred.

**Disable user (F15 for exceptions)**

Disable the account of the user in whose session the intrusion occurred.

To set users whose accounts are not disabled if intrusions occur in their sessions, press the F15 (Shift+F3) key. The Auto-Disable Exceptions screen appears, as shown in "Setting Users who Are Never Disabled by the Firewall Intrusion Detection System" on page 64.

**Email Security Admin (Y, M=1/Min, D=6/Min)**

Email a message to the Security Admin. Possible values are:

- **Y**: Email all messages.
- **M**: Email no more than one message per minute.
- **D**: Email no more than six messages per minute.

Enter the email address of the Security Admin in the **Email:** sub-field.

**Run Action (if Action installed)**

If the iSecurity Acton product is installed, perform the indicated named actions.

**Write to QAUDJRN (security audit journal)**

Log the intrusion to QAUDJRN with the data format used in the file SMZ8/GSCALP. Use the audit journal code "**U**" and the Journal entry format "**FW**".

### Screening of Allowed Activity

#### Send allowed messages to message queue

Whether to send messages about accepted activity to the message queue.

## Setting Users who Are Never Disabled by the Firewall Intrusion Detection System

To **create and modify the list of users** whose accounts your Firewall intrusion detection system must never disable, press the **F15 (Shift+F3)** key from the **Firewall Intrusion Detection System** screen (*STRFW* **> 81 > 5**) as shown in "Setting Up a Firewall Intrusion Detection System" on page 61.

The **Auto-Disable Exceptions** screen appears:

```
                          Auto-Disable Exceptions

Specify user names or generic* that should NEVER be disabled automatically.
                                                Position:    _________
Type options, press Enter.
  4=Delete
Opt User        Description
    QSNADS      IBM-supplied User Profile
    QSPL        Internal Spool User Profile
    QSPLJOB     Internal Spool User Profile
    QSRV        Service User Profile
    QSRVBAS     Basic Service User Profile
    QSYS        Internal System User Profile
    QTCP        Internal TCP/IP User Profile
    QTFTP       IBM-supplied User Profile
 _  QTIVOLI     TIVOLI PRODUCTS OWNING PROFILE
 _  QTIVROOT    TIVOLI ALL OBJECT AUTHORITY PROFILE
 _  QTIVUSER    TIVOLI GENERAL USER PROFILE
    QTSTRQS     Test Request User Profile
                                                                      Bottom
Users defined in the Auto-Disable exception list, are considered excluded.
F3=Exit    F6=Add new    F12=Cancel
```

The body of the screen lists users whose accounts are never disabled by intrusion detection systems, even if Firewall rules say to disable the user.

Each line shows the **User** name and a free form **Description** of the account.

Some users cannot be removed from the list. Their **User** names appear in purple.

For accounts that can be removed from the list, the user name appears in green, preceded by an **Opt** field.

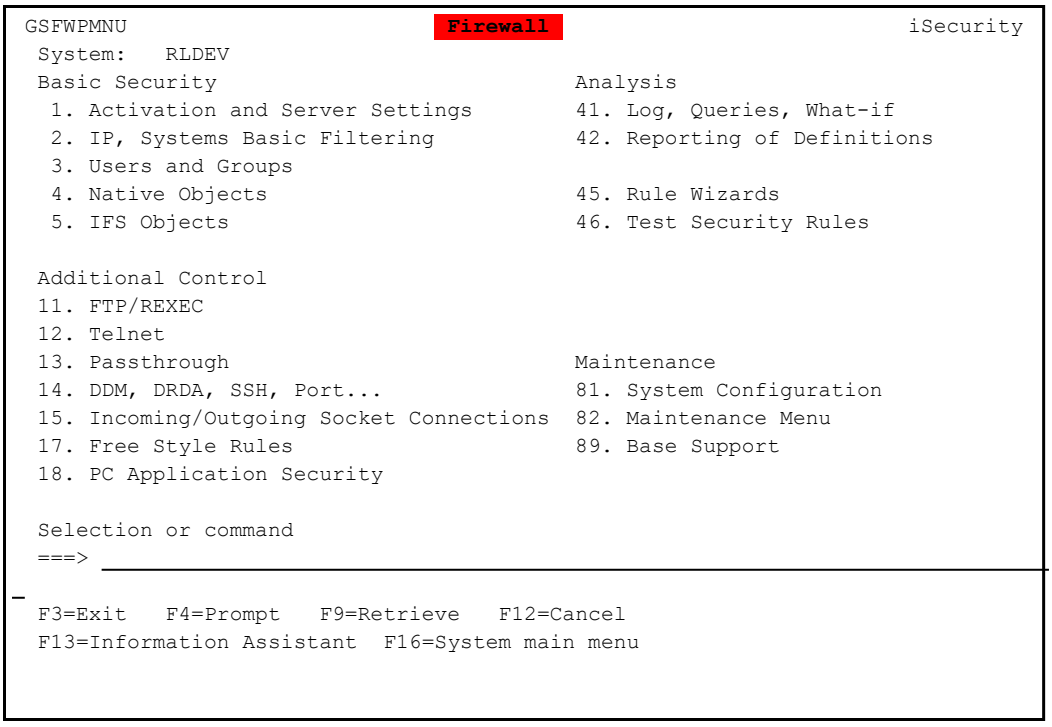
To **remove** one of these accounts from the list, enter **4** in the **Opt** field for the account. The account is removed from the list without prompting for confirmation, and the display returns to the top of the list.

To **add** accounts to the list, press the **F6** key. The **Add Users to Exception List** screen appears, with a column of blank fields in which you can enter user names. For a list of all users from which you can select names, press the **F7** key within that screen. The **Apply to Selected Users** window appears, in which you can select names by entering **1** in the **Sel** field for that user and pressing **Enter**.

## Setting Additional Firewall Controls for Specific Servers

You can set additional controls for specific servers. These rules can substitute different user IDs for some types of logons, manage licenses, and specify times during which these connections might be made.

These specifications are grouped under **Additional Control** on the Firewall Main Menu:




To set controls for FTP and REXEC under both IPv4 and IPv6, select **11. FTP/REXEC**. The FTP/REXEC Login Security screen appears, as shown in "Setting Additional Controls and Displaying Logs for FTP/REXEC" on page 68.

To set controls for Telnet Logons under both IPv4 and IPv6, select **12. Telnet**. The Telnet Security screen appears, as shown in "Setting Additional Controls and Displaying Logs for Telnet" on page 96.

To set controls for Passthrough Logons, select **13. Passthrough**. The Passthrough Security screen appears, as shown in "Setting Additional Controls and Displaying Logs for Passthrough Logons" on page 116.

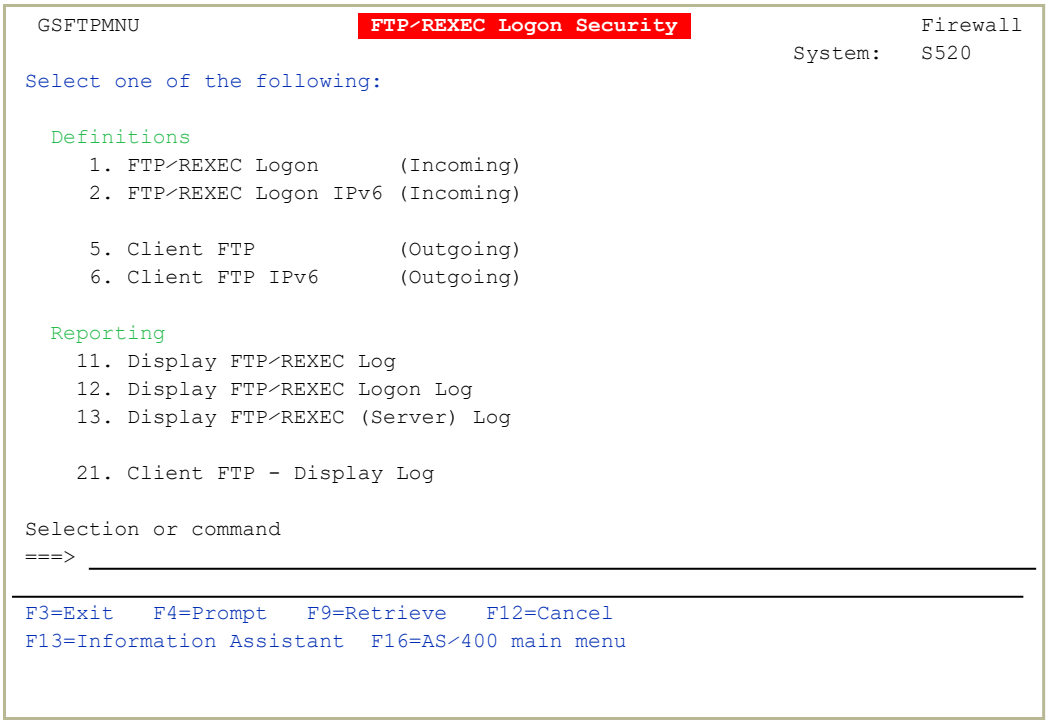
To set controls for DDM, DRDA, DHCP, and SSHD, as well as setting TCP/IP port restrictions and managing licenses for other products, select **14. DDM, DRDA, SSH, Port...** The Work with Advanced Security screen appears, as shown in "Setting Additional Firewall Rules and Displaying Logs for DDM, DRDA, DHCP, and Other Servers" on page 125.

To set controls for Incoming and Outgoing Socket Connections, select **15. Incoming/Outgoing Socket Connections**. The Incoming/Outgoing Connection Rules screen appears, as shown in "Setting Firewall Rules for Socket Connections" on page 446.

To control access to PC Applications, select **18. PC Application Security**. The Work with Client-Application Security screen appears, as shown in "Securing PC Client Applications" on page 523.

# Setting Additional Controls and Displaying Logs for FTP/REXEC

To **set additional controls for FTP and REXEC and to display their logs**, select **`11. FTP/REXEC`** from the Firewall Main Menu (*STRFW*). The **FTP/REXEC Logon Security** screen appears:




To **set controls** for FTP/REXEC, select these options under **`Definitions`**:

- To set controls for **incoming FTP/REXEC logons**, select **`1. FTP/REXEC Logon (Incoming)`**. The **Work with FTP/REXEC Logon Security** screen appears, as shown in "Setting Additional Controls for Incoming FTP/REXEC Logons" on page 70.
- To set controls for **incoming IPv6 FTP/REXEC logons**, select **`2. FTP/REXEC Logon IPv6 (Incoming)`**. The **Work with FTP/REXEC Logon Security IPv6** screen appears, as shown in "Setting Additional Controls for Incoming IPv6 FTP REXEC Logons" on page 77.
- To set controls for **outgoing client FTP connections**, select **`5. Client FTP (Outgoing)`**. The **Work with Client FTP Security** screen appears, as shown in "Setting Additional Controls for Outgoing FTP Connections" on page 84.

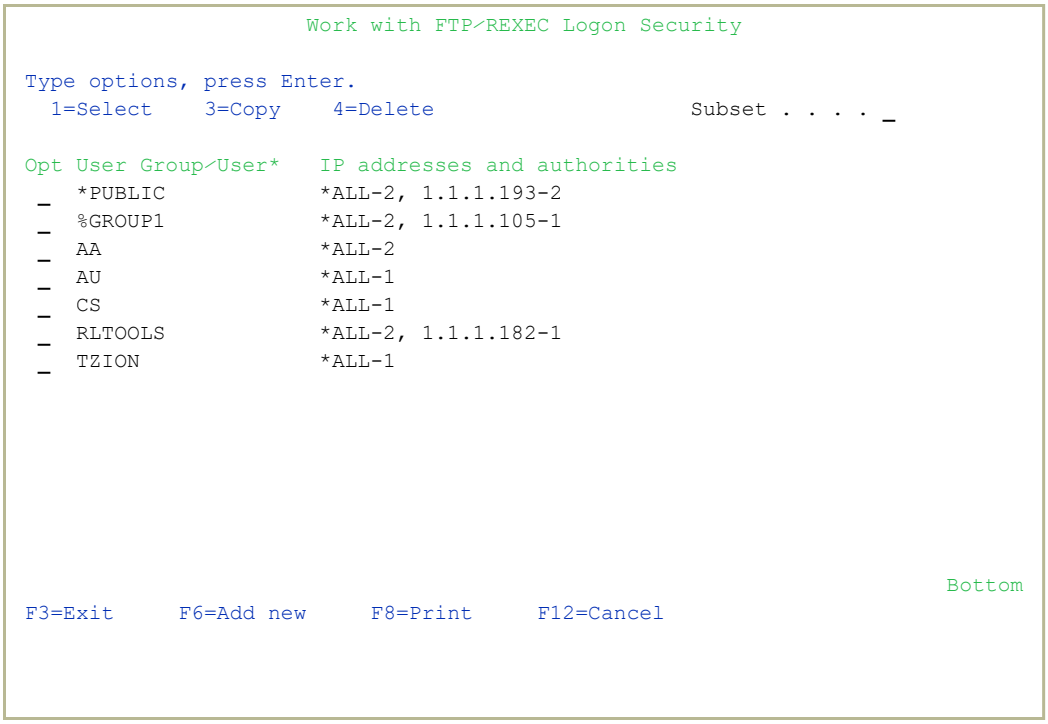
- To set controls for outgoing IPv6 client FTP connections, select **6. Client FTP IPv6 (Outgoing)** . The Work with Client FTP Security IPv6 screen appears, as shown in "Setting Additional Controls for Outgoing IPv6 FTP Connections" on page 90.

To display reports for FTP/REXEC, select these items under **Reporting.** Each item displays the Display Firewall Log (DSPFWLOG) (as shown in "Displaying Firewall Logs" on page 516) with appropriate settings:

- To display a log of all FTP/REXEC connections, select **11. Display FTP/REXEC Log**. The Display Firewall Log (DSPFWLOG) screen appears with the **Type** field set to ***FTP**.
- To display a log of FTP/REXEC logons, select **12. Display FTP/REXEC Logon Log**. The Display Firewall Log (DSPFWLOG) screen appears with the **Type** field set to ***FTPLOG**.
- To display a log of the FTP/REXEC server, select **13. Display FTP/REXEC (Server) Log**. The Display Firewall Log (DSPFWLOG) screen appears with the **Type** field set to ***FTPSRV**.
- To display a log of outgoing FTP connections, select **21. Client FTP - Display Log**. The Display Firewall Log (DSPFWLOG) screen appears with the **Type** field set to ***FTPCLN**.

## Setting Additional Controls for Incoming FTP/REXEC Logons

To **set additional controls for incoming FTP/REXEC logons**, select **1 . FTP/REXEC Logon (Incoming)** from the **FTP/REXEC Logon Security** screen (*STRFW* **> 11**). The **Work with FTP/REXEC Logon Security** screen appears:




The body of the screen consists of three fields, starting with an **Opt** field for entering options. Each line refers to a single user or group and its authorities for incoming FTP/REXEC logons.

The **User Group/User*** field contains the name of a user or group. This can also be a generic* name. The value ***PUBLIC** refers to all users or groups for whom no more specific information is shown.

The **IP addresses and authorities** field contains a list of IP address ranges and authorities, shown as the address range, a dash, and a digit **1** through **3** where:

- **1**: **Accept** logon requests
- **2**: **Reject** logon requests

- **3**: Require an **ALTLOGON** connection to connect, as set on the Modify FTP/REXEC Logon User screen, shown at "Modifying a User for Incoming FTP/REXEC Logons" on page 73.

Thus, for example, a value of ***ALL-2, 1.1.1.105-1** shows that all FTP/REXEC logon requests are rejected, except those from the IP address **1.1.1.105**, which are accepted.

To add information for a user or group, press the F6 key. The Add FTP/REXEC Logon User screen appears, as shown in "Adding a User for Incoming FTP/REXEC Logons" below.

To modify information for a user or group, enter **1** in the **Opt** field for that user or group. The Modify FTP/REXEC Logon User screen appears, as shown in "Modifying a User for Incoming FTP/REXEC Logons" on page 73.

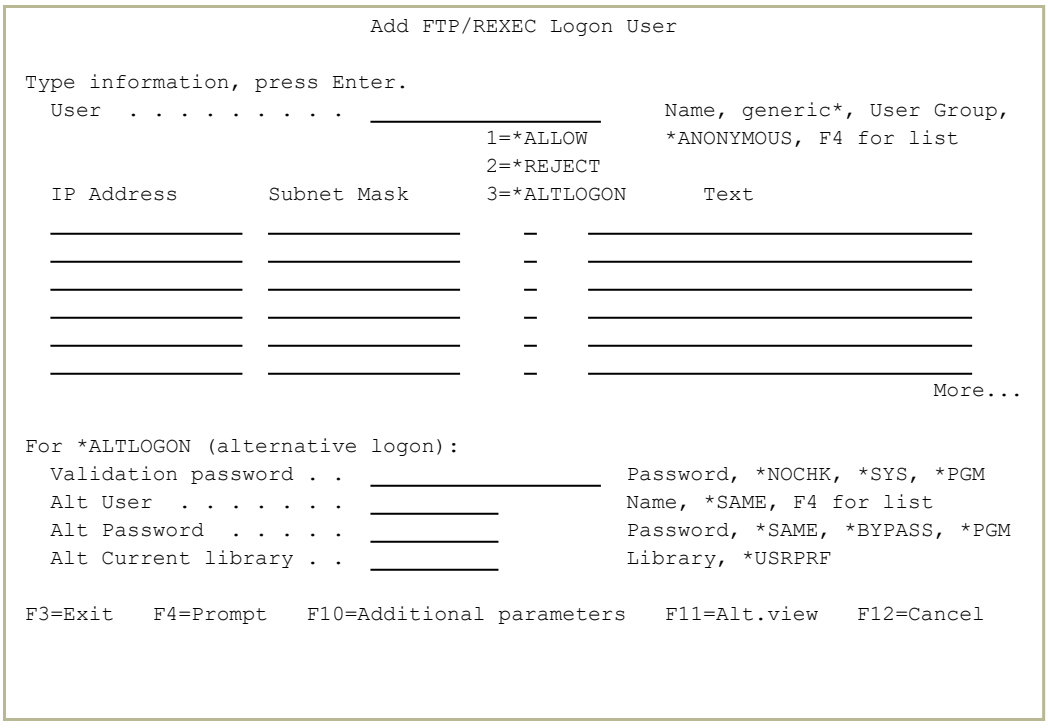
To copy information from one user or group to another, enter **3** in the **Opt** field for the original user or group. The Copy FTP/REXEC Logon User screen appears, as shown in "Copying a User for Incoming FTP REXEC Logons" on page 74.

To delete information for a user or a group, enter **4** in the **Opt** field for the user or group. The Delete FTP/REXEC Logon User screen appears, as shown in "Deleting a User for Incoming FTP/REXEC Logons" on page 75.

## Adding a User for Incoming FTP/REXEC Logons

To add a new user for incoming FTP/REXEC logons, press the F6 key from the Work with FTP/REXEC Logon Security screen (*STRFW* **> 11 > 1**), as shown in "Setting Additional Controls for Incoming FTP/REXEC Logons" on the previous page.

The Add FTP/REXEC Logon User screen appears:




Enter the name of the new user or group in the **User** field. This can be a specific or generic* name. Use the value ***ANONYMOUS** for anonymous connections. For a list of possible values, press the F4 key.

The body of the screen is made up of lines that can refer to different IP address ranges. Possible values include:

**IP Address**

The IP address that begins the range.

**Subnet mask**

The subnet mask for the address range. For a list of possible subnet masks, showing the number of addresses that the range would include, press the F4 key.

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

How Firewall responds to requests by the user for incoming FTP/REXEC logons from this IP range. Possible values include:

- 1: Accept logon requests
- 2: Reject logon requests

- **3**: Require an **ALTLOGON** connection to connect, as set on the Modify FTP/REXEC Logon User screen, shown at "Modifying a User for Incoming FTP/REXEC Logons" below.

**Text**

A free-form text description of the rule.

If you are using ***ALTLOGON**, as indicated in IBM documentation, the user takes on a different identity, including that user's authority settings. Set the section of the screen labeled **For*ALTLOGON (alternative logon):** to appropriate values.

After entering information in these fields, press the Enter key.

## Modifying a User for Incoming FTP/REXEC Logons

To modify information for a user or group for incoming FTP/REXEC logons, enter **1** in the **Opt** field for that user or group on the Work with FTP/REXEC Logon Security screen (*STRFW* **> 11 > 1**) as shown in "Setting Additional Controls for Incoming IPv6 FTP REXEC Logons" on page 77.

The Modify FTP/REXEC Logon User screen appears:

```
                        Modify FTP/REXEC Logon User

Type information, press Enter.
  User  . . . . . .  RLTOOLS
                                    1=*ALLOW
                                    2=*REJECT
  IP Address       Subnet Mask      3=*ALTLOGON      Text
  *ALL             0.0.0.0            2
  1.1.1.182        255.255.255.255    1
  _____________    _____________      _
  _____________    _____________      _
  _____________    _____________      _
  _____________    _____________      _
                                                          More...

For *ALTLOGON (alternative logon):
  Validation password . .  *SYS              Password, *NOCHK, *SYS, *PGM
  Alt User  . . . . . .  *SAME              Name, *SAME, F4 for list
  Alt Password  . . . . .  *SAME            Password, *SAME, *BYPASS, *PGM
  Alt Current library . .  *USRPRF          Library, *USRPRF

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

The read-only **User** field shows the name of the user or group.

The body of the screen is made up of lines that can refer to different IP address ranges. To modify the information for the user, you can edit or clear existing lines or add new ones.

Possible field values include:

**IP Address**

The IP address that begins the range.

**Subnet mask**

The subnet mask for the address range. For a list of possible subnet masks, showing the number of addresses that the range would include, press the F4 key.

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

How Firewall responds to requests by the user for incoming FTP/REXEC logons from this IP range. Possible values include:

- **1**: Accept logon requests
- **2**: Reject logon requests
- **3**: Require an **ALTLOGON** connection to connect, as set below.

**Text**

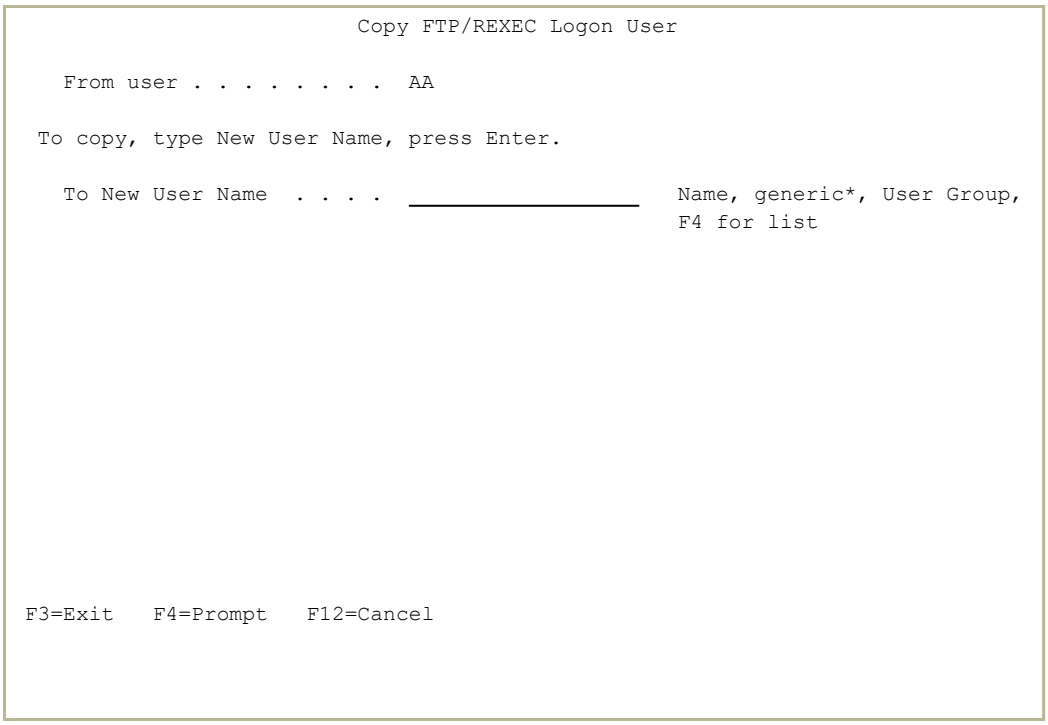
A free-form text description of the rule.

If you are using ***ALTLOGON**, as indicated in IBM documentation, the user takes on a different identity, including that user's authority settings. Set the section of the screen labeled **For*ALTLOGON (alternative logon):** to appropriate values.

## Copying a User for Incoming FTP REXEC Logons

To copy information from a user or group to another for incoming FTP/REXEC logons, enter **3** in the **Opt** field for that user or group on the Work with FTP/REXEC Logon Security screen (*STRFW* **> 11 > 1**) as shown in "Setting Additional Controls for Incoming FTP/REXEC Logons" on page 70.

The Copy FTP/REXEC Logon User screen appears:



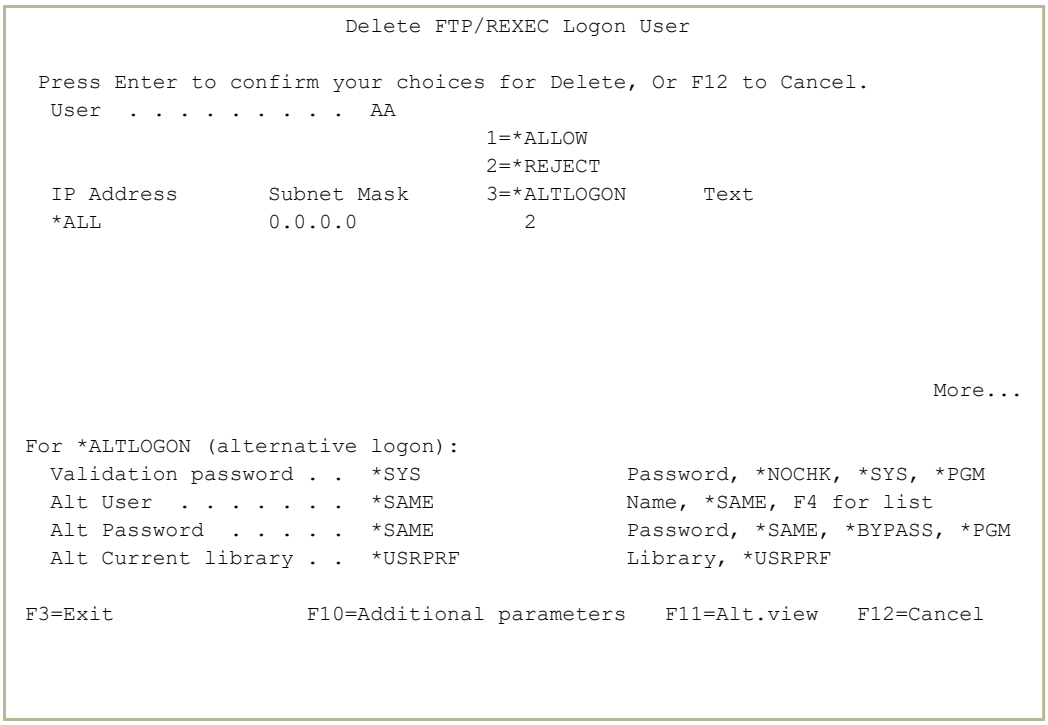

The read-only **From user** field shows the name of the user or group whose information you are copying.

Enter the name of the user or group to whom you are copying the information in the **To New User Name** field. This can be a single or generic* name. For a list of possibilities, press the **F4** key.

## Deleting a User for Incoming FTP/REXEC Logons

To **delete information for a user or group for incoming FTP/REXEC logons**, enter **4** in the **Opt** field for that user or group on the **Work with FTP/REXEC Logon Security** screen (*STRFW* **> 11 > 1**) as shown in "Setting Additional Controls for Incoming FTP/REXEC Logons" on page 70.

The **Delete FTP/REXEC Logon User** screen appears:




All the fields on the screen are read-only, showing the current information for the user.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Additional Controls for Incoming IPv6 FTP REXEC Logons

To set additional controls for incoming IPv6 FTP/REXEC logons, select **2. FTP/REXEC Logon IPv6 (Incoming)** from the FTP/REXEC Logon Security screen *(STRFW > 11*). The Work with FTP/REXEC Logon Security IPv6 screen appears:

```
                  Work with FTP/REXEC Logon Security IPv6

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

    User Group/
Opt User*              IPv6 addresses and authorities
 _  *PUBLIC            *ALL-2, 13::-1, 16::-1, 1234::-1
 _  %U52               *ALL-2, 1:1::-1
 _  AA                 *ALL-2, 12:28::-1, 12:28::-2, 12:28::-2, 2001:DB8:0: ...
 _  BB                 *ALL-2, 1:2::-2, 1:2::-3
 _  BBAA               *ALL-2, 1:2:3:4:5:6:7:8-1, 1:2:3:4:5:6:7:8-1
 _  GS                 *ALL-1, 8:7:6:5:4:3:2:1-1, 8:7:6:5:4:3:2:1-1, 1234:0 ...
 _  PP                 *ALL-2, 13:14::-1
 _  TT                 *ALL-2, 23::-1, 24::-1, 32::-1
 _  XER                *ALL-2, 55:66:77:88::-1
 _  XER2               *ALL-2




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

The body of the screen consists of three fields, starting with an **Opt** field for entering options. Each line refers to a single user or group and its authorities for incoming FTP/REXEC logons.

The **User Group/User*** field contains the name of a user or group. This can also be a generic* name. The value ***PUBLIC** refers to all users or groups for whom no more specific information is shown.

The **IPv6 addresses and authorities** field contains a list of IPv6 address ranges and authorities, shown as the address range, a dash, and a digit **1** through **3** where:

- **1**: Accept logon requests
- **2**: Reject logon requests

- **3**: Require an **ALTLOGON** connection to connect, as set on the Modify FTP/REXEC Logon User screen, shown at "Modifying a User for Incoming IPv6 FTP REXEC Logons" on page 80.

Thus, for example, a value of ***ALL-2, 1:1::-1** shows that all IPv6 FTP/REXEC logon requests are rejected, except those from the IPv6 address range beginning with **1:1::**, which are accepted.

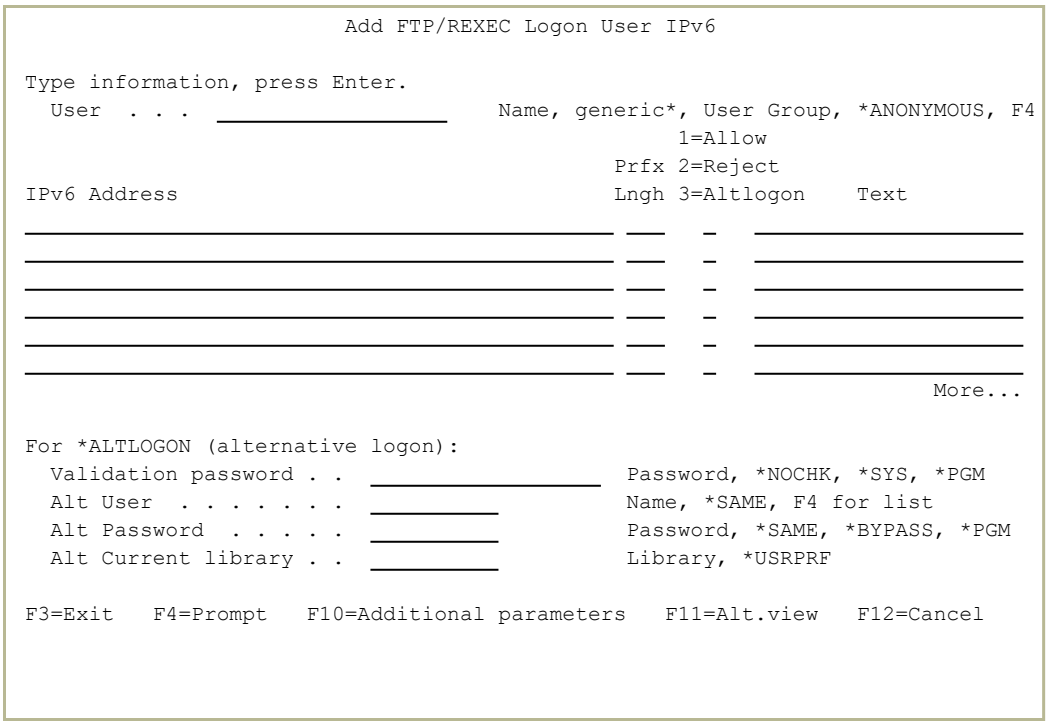
You can perform the following actions from this screen:

- To add information for a user or group, press the F6 key. The Add FTP/REXEC Logon User IPv6 screen appears, as shown in "Adding a User for Incoming IPv6 FTP REXEC Logons" below.
- To modify information for a user or group, type **1** in the **Opt** field for that user or group and press Enter. The Modify FTP/REXEC Logon User IPv6 screen appears, as shown in "Modifying a User for Incoming IPv6 FTP REXEC Logons" on page 80.
- To copy information from one user or group to another, type **3** in the **Opt** field for the original user or group and press Enter. The Copy FTP/REXEC Logon User IPv6 screen appears, as shown in "Copying a User for Incoming IPv6 FTP/REXEC Logons" on page 82.
- To delete information for a user or a group, type **4** in the **Opt** field for the user or group and press Enter. The Delete FTP/REXEC Logon User IPv6 screen appears, as shown in "Deleting a User for Incoming IPv6 FTP/REXEC Logons" on page 82.

## Adding a User for Incoming IPv6 FTP REXEC Logons

To add a new user for incoming FTP/REXEC logons, press the F6 key from the Work with FTP/REXEC Logon Security IPv6 screen (*STRFW* **> 11 > 2**), as shown in "Setting Additional Controls for Incoming IPv6 FTP REXEC Logons" on the previous page.

The Add FTP/REXEC Logon User IPv6 screen appears:




Enter the name of the new user or group in the **User** field. This can be a specific or generic* name. Use the value ***ANONYMOUS** for anonymous connections. For a list of possible values, press the **F4** key.

The body of the screen is made up of lines that can refer to different IPv6 address ranges. Possible values include:

**IPv6 Address**

The IPv6 address for the range of addresses. In addition to an IPv6 address, you can set this field to ***ALL** for rules applied to all IPv6 ranges that aren't otherwise specified.

**Address prefix length**

The length of the IPv6 address prefix. This can be set to from **1-128**.

**1=Allow 2=Reject 3=Altlogon**

How Firewall responds to requests by the user for incoming FTP/REXEC logons from this IPv6 range. Possible values include:

- **1**: **Accept** logon requests
- **2**: **Reject** logon requests

- **3**: Require an **ALTLOGON** connection to connect, as set on the Modify FTP/REXEC Logon User screen, shown at "Modifying a User for Outgoing IPv6 FTP Connections" on page 93.

**Text**

A free-form text description of the rule.

If you are using ***ALTLOGON**, as indicated in IBM documentation, the user takes on a different identity, including that user's authority settings. Set the section of the screen labeled **For*ALTLOGON (alternative logon):** to appropriate values.

After entering information in these fields, press the Enter key.

## Modifying a User for Incoming IPv6 FTP REXEC Logons

To modify information for a user or group for incoming FTP/REXEC logons, type **1** in the **Opt** field for that user or group on the Work with FTP/REXEC Logon Security IPv6 screen (STRFW **> 11 > 2**) as shown in "Setting Additional Controls for Incoming IPv6 FTP REXEC Logons" on page 77, and press Enter.

The Modify FTP/REXEC Logon User IPv6 screen appears:

```
                      Modify FTP/REXEC Logon User IPv6

Type information, press Enter.
  User  . . .  AA
                                                    1=Allow
                                                Prfx 2=Reject
IPv6 Address                                    Lngh 3=Altlogon    Text
*ALL                                                 2
12:28::                                         120  1
12:28::                                         124  2
12:28::                                         128  2   Text2
2001:DB8:0:8::                                   61  1
                                                     -
                                                                    More...

For *ALTLOGON (alternative logon):
  Validation password . .  _________________  Password, *NOCHK, *SYS, *PGM
  Alt User  . . . . . .  AA                  Name, *SAME, F4 for list
  Alt Password  . . . . .  **********        Password, *SAME, *BYPASS, *PGM
  Alt Current library . .  __________        Library, *USRPRF

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

The read-only **User** field shows the name of the user or group.

The body of the screen is made up of lines that can refer to different IPv6 address ranges. To modify the information for the user, you can edit or clear existing lines or add new ones.

Possible values include:

**IPv6 Address**

The IPv6 address for the range of addresses. In addition to an IPv6 address, you can set this field to ***ALL** for rules applied to all IPv6 ranges that aren't otherwise specified.

**Address prefix length**

The length of the IPv6 address prefix. This can be set to from **1-128**.

**1=Allow 2=Reject 3=Altlogon**

How Firewall responds to requests by the user for incoming FTP/REXEC logons from this IPv6 range. Possible values include:

- **1**: Accept logon requests
- **2**: Reject logon requests
- **3**: Require an **ALTLOGON** connection to connect, as set on the Modify FTP/REXEC Logon User screen, shown at "Modifying a User for Incoming FTP/REXEC Logons" on page 73.

**Text**

A free-form text description of the rule.

If you are using ***ALTLOGON**, as indicated in IBM documentation, the user takes on a different identity, including that user's authority settings. Set the section of the screen labeled **For*ALTLOGON (alternative logon):** to appropriate values.

After entering information in these fields, press the Enter key.

## Copying a User for Incoming IPv6 FTP/REXEC Logons

To **copy information from a user or group to another for incoming IPv6 FTP/REXEC logons**, enter **3** in the **Opt** field for that user or group on the **Work with FTP/REXEC Logon Security IPv6** screen (*STRFW* **> 11 > 2**) as shown in "Setting Additional Controls for Incoming IPv6 FTP REXEC Logons" on page 77.

The **Copy FTP/REXEC Logon User IPv6** screen appears:

```
                        Copy FTP/REXEC Logon User IPv6

   From user . . . . . .  AA

 To copy, type New User Name, press Enter.

   To New User Name  . . . .  _________________   Name, generic*, User Group,
                                                  F4 for list









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

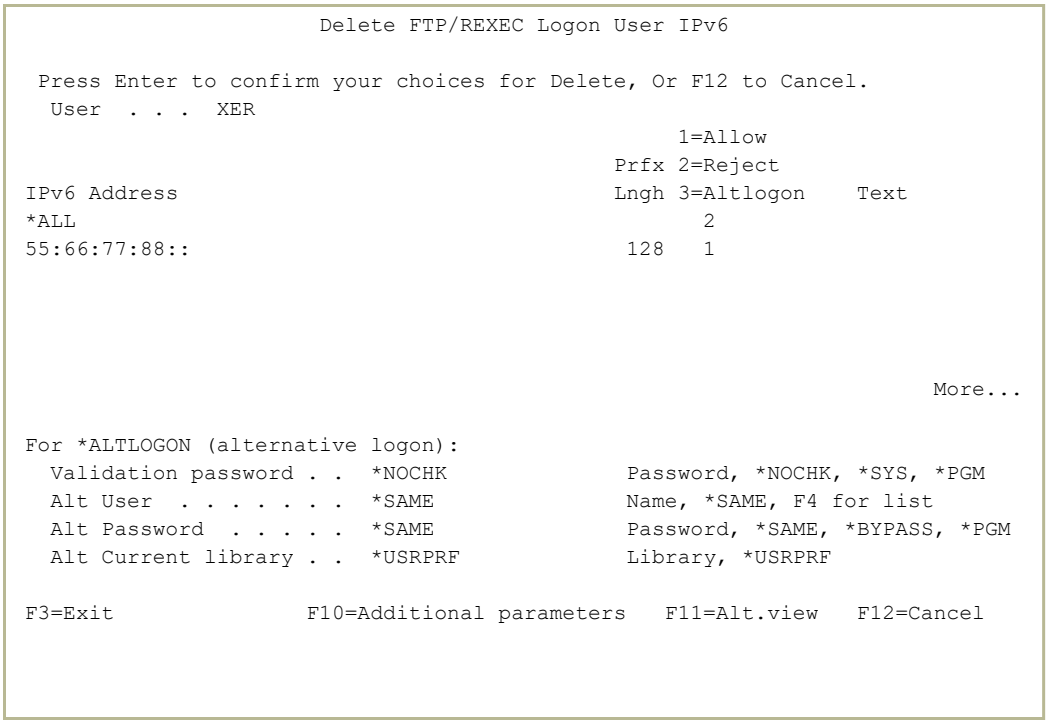
The read-only **From user** field shows the name of the user or group whose information you are copying.

Enter the name of the user or group to whom you are copying the information in the **To New User Name** field. This can be a single or generic* name. For a list of possibilities, press the **F4** key.

## Deleting a User for Incoming IPv6 FTP/REXEC Logons

To **delete** information for a user or group for incoming IPv6 FTP/REXEC logons, enter **4** in the **Opt** field for that user or group on the **Work with FTP/REXEC Logon Security IPv6** screen (*STRFW* **> 11 > 2**) as shown in "Setting Additional Controls for Incoming IPv6 FTP REXEC Logons" on page 77.

The **Delete FTP/REXEC Logon User IPv6** screen appears:




All the fields on the screen are read-only, showing the current information for the user.

Press **Enter** to confirm the deletion and return to the previous screen.

Press the **F12** key to cancel the deletion and return to the previous screen.

## Setting Additional Controls for Outgoing FTP Connections

To **set additional controls** for outgoing FTP connections, select **`5. Client FTP (Outgoing)`** from the **FTP/REXEC Logon Security** screen *(STRFW* **`> 11`**).

The **Work with Client FTP Security** screen appears:

```
                        Work with Client FTP Security

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

Opt User Group/User*   Outgoing IP addresses and authorities
 _   *PUBLIC            *ALL-1
 _   %GUI               *ALL-2, 1.1.1.29-1
 _   %QA                *ALL-1
 _   QQ                 *ALL-2, 1.1.1.212-1
 _   QSECOFR            *ALL-1, 1.1.1.131-1, 1.1.1.163-1, 1.1.1.227-1
 _   TEVG               *ALL-2, 1.1.1.212-1

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

The body of the screen consists of three fields, starting with an **`Opt`** field for entering options. Each line refers to a single user or group and its authorities for outgoing Client FTP connections.

The **`User Group/User*`** field contains the name of a user or group. This can also be a generic* name. The value **`*PUBLIC`** refers to all users or groups for whom no more specific information is shown.

The **`Outgoing IP addresses and authorities`** field contains a list of IP address ranges and authorities, shown as the address range, a dash, and either the digit **`1`** to allow FTP requests or **`2`** to reject them.

Thus, for example, a value of **`*ALL-2, 1.1.1.105-1`** shows that all outgoing Client FTP requests are rejected, except those from the IP address **`1.1.1.105`**, which are allowed.

You can perform the following actions from this screen:

To **add** information for a user or group, press the **F6** key. The **Add FTP Client User** screen appears, as shown in "Adding a User for Outgoing FTP Connections" below.

To **modify** information for a user or group, enter **1** in the **Opt** field for that user or group. The **Modify FTP Client User** screen appears, as shown in "Modifying a User for Outgoing FTP Connections" on the next page.

To **copy** information from one user or group to another, enter **3** in the **Opt** field for the original user or group. The **Copy FTP Client User** screen appears, as shown in "Copying a User for Outgoing FTP Connections" on page 88.

To **delete** information for a user or a group, enter **4** in the **Opt** field for the user or group. The **Delete FTP Client User** screen appears, as shown in "Deleting a User for Outgoing FTP Connections" on page 88.

## Adding a User for Outgoing FTP Connections

To **add a new user** for outgoing FTP connections, press the **F6** key from the **Work with Client FTP Security** screen (*STRFW* **> 11 > 5**), as shown in "Setting Additional Controls for Outgoing IPv6 FTP Connections" on page 90.

The **Add FTP Client User** screen appears:

```
                          Add FTP Client User

Type information, press Enter.
  User  . . . . . .  _________          Name, generic*, User Group,
                                        F4 for list
  Outgoing                          1=Allow
  IP Address       Subnet Mask      2=Reject         Text
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
  _______________  _______________    _   ____________________________
                                                              More...

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

Enter the name of the new user or group in the **User** field. This can be a specific or generic* name. For a list of possible values, press the F4 key.

The body of the screen is made up of lines that can refer to different IP address ranges. Possible values include:

**Outgoing IP Address**

The IP address that begins the range.

**Subnet mask**

The subnet mask for the address range. For a list of possible subnet masks, showing the number of addresses that the range would include, press the F4 key.

**1=Allow 2=Reject**

How Firewall responds to requests by the user for outgoing FTP connections to this IP range. Possible values include:

- **1**: Accept connection requests
- **2**: Reject connection requests

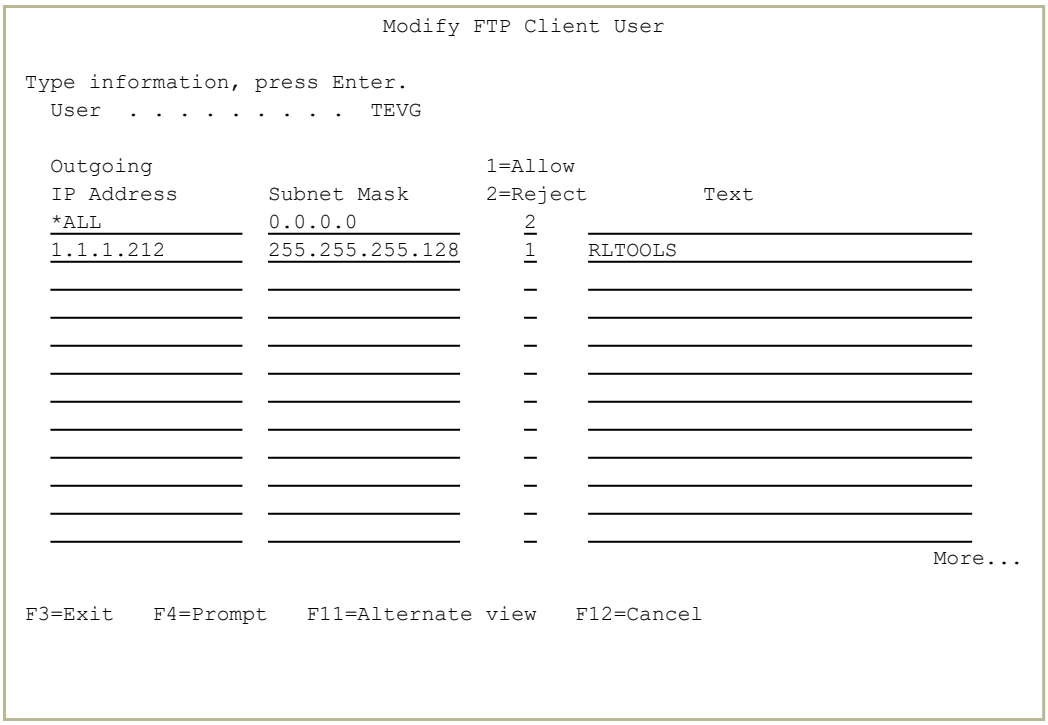
**Text**

A free-form text description of the rule.

## Modifying a User for Outgoing FTP Connections

To modify information for a user or group for outgoing FTP connections, enter **1** in the **Opt** field for that user or group on the Work with Client FTP Security screen (*STRFW* **> 11 > 5**) as shown in "Setting Additional Controls for Outgoing FTP Connections" on page 84.

The Modify FTP Client User screen appears:




The read-only **User** field shows the name of the user or group.

The body of the screen is made up of lines that can refer to different IP address ranges. To modify the information for the user, you can edit or clear existing lines or add new ones.

Possible field values include:

**IP Address**

The IP address that begins the range.

**Subnet mask**

The subnet mask for the address range. For a list of possible subnet masks, showing the number of addresses that the range would include, press the **F4** key.

**1=Allow 2=Reject**

How Firewall responds to requests by the user for outgoing FTP connections to this IP range. Possible values include:

- **1**: Accept
- **2**: Reject

**Text**

A free-form text description of the rule.

## Copying a User for Outgoing FTP Connections

To **copy** information from a user or group to another for outgoing FTP connections, enter **3** in the **Opt** field for that user or group on the **Work with Client FTP Security** screen (*STRFW* **> 11 > 5**) as shown in "Setting Additional Controls for Outgoing FTP Connections" on page 84.

The **Copy FTP/REXEC Logon User** screen appears:

```
                        Copy FTP/REXEC Logon User

  From user . . . . . .  AA

To copy, type New User Name, press Enter.

  To New User Name  . . . .  _________________   Name, generic*, User Group,
                                                 F4 for list









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

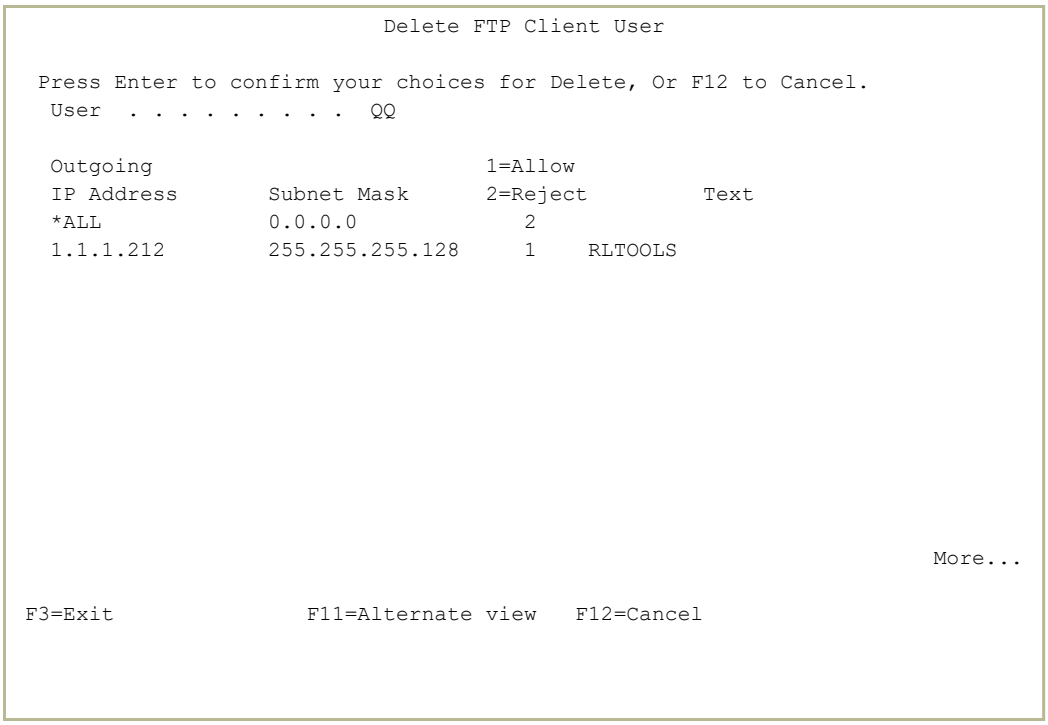
The read-only **From user** field shows the name of the user or group whose information you are copying.

Enter the name of the user or group to whom you are copying the information in the **To New User Name** field. This can be a single or generic* name. For a list of possibilities, press the **F4** key.

## Deleting a User for Outgoing FTP Connections

To **delete** information for a user or group for outgoing FTP connections, enter **4** in the **Opt** field for that user or group on the **Work with Client FTP Security** screen (*STRFW* **> 11 > 5**) as shown in "Setting Additional Controls for Outgoing FTP Connections" on page 84.

The **Delete FTP/REXEC Logon User** screen appears:




All the fields on the screen are read-only, showing the current information for the user.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Additional Controls for Outgoing IPv6 FTP Connections

To **set additional controls** for outgoing IPv6 FTP connections, select **6. Client FTP IPv6 (Outgoing)** from the **FTP/REXEC Logon Security** screen *(STRFW* **> 11**).

The **Work with Client FTP Security IPv6** screen appears:

```
                    Work with Client FTP Security IPv6

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

    User Group/
Opt User*      Outgoing IPv6 addresses and authorities
 _  *PUBLIC    *ALL-2, 22::-1, 11::-1
 _  %#TEST2    *ALL-2
 _  AA1        *ALL-2, 013::-1, 13:93:12::-2, 017:15:13::-1, 1234:0098:0000 ...
 _  ABC        *ALL-1, ::1-2, 13:14:15::-1
 _  G*         *ALL-2, 1234:56::-1
 _  QQ         *ALL-2, 13:14:15::-1, 13:93:12::-2
 _  XER        *ALL-2, 55:66:77:88::-1
 _  XER2       *ALL-2
 _  ZZZXXX     *ALL-2




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

The body of the screen consists of three fields, starting with an **Opt** field for entering options. Each line refers to a single user or group and its authorities for outgoing Client FTP connections.

The **User Group/User*** field contains the name of a user or group. This can also be a generic* name. The value ***PUBLIC** refers to all users or groups for whom no more specific information is shown.

The **Outgoing IPv6 addresses and authorities** field contains a list of IPv6 address ranges and authorities, shown as the address range, a dash, and either the digit **1** to allow FTP requests or **2** to reject them.

Thus, for example, a value of ***ALL-2, 55.66.77.88-1** shows that all outgoing Client IPv6 FTP requests are rejected, except those from the IP address **55.66.77.88**, which are allowed.

You can perform the following actions from this screen:

To **add** information for a user or group, press the **F6** key. The **Add FTP Client User IPv6** screen appears, as shown in "Adding a User for Outgoing IPv6 FTP Connections" below.

To **modify** information for a user or group, enter **1** in the **Opt** field for that user or group. The **Modify FTP Client User IPv6** screen appears, as shown in "Modifying a User for Outgoing IPv6 FTP Connections" on page 93.

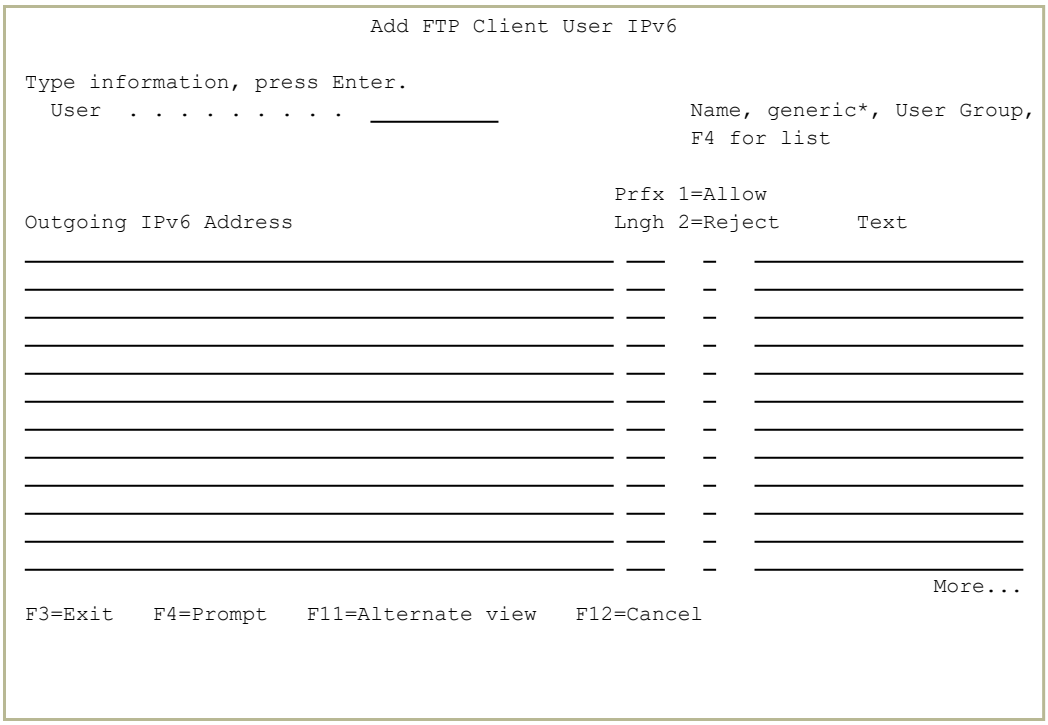
To **copy** information from one user or group to another, enter **3** in the **Opt** field for the original user or group. The **Copy FTP Client User** screen appears, as shown in "Copying a User for Outgoing IPv6 FTP Connections" on page 94.

To **delete** information for a user or a group, enter **4** in the **Opt** field for the user or group. The **Delete FTP Client User IPv6** screen appears, as shown in "Deleting a User for Outgoing IPv6 FTP Connections" on page 95.

## Adding a User for Outgoing IPv6 FTP Connections

To **add a new user** for outgoing FTP connections, press the **F6** key from the **Work withClient FTP Security IPv6** screen (*STRFW* **> 11 > 6**), as shown in "Setting Additional Controls for Outgoing IPv6 FTP Connections" on the previous page.

The **Add FTP Client User IPv6** screen appears:




Enter the name of the new user or group in the **User** field. This can be a specific or generic* name. For a list of possible values, press the **F4** key.

The body of the screen is made up of lines that can refer to different IPv6 address ranges. Possible values include:

**IPv6 Address**

The IPv6 address for the range of addresses. In addition to an IPv6 address, you can set this field to ***ALL** for rules applied to all IPv6 ranges that aren't otherwise specified.

**Address prefix length**

The length of the IPv6 address prefix. This can be set to from **1-128**.

**1=Allow 2=Reject**

How Firewall responds to requests by the user for outgoing FTP connections to this IPv6 range. Possible values include:

- **1**: **Accept** requests
- **2**: **Reject** requests

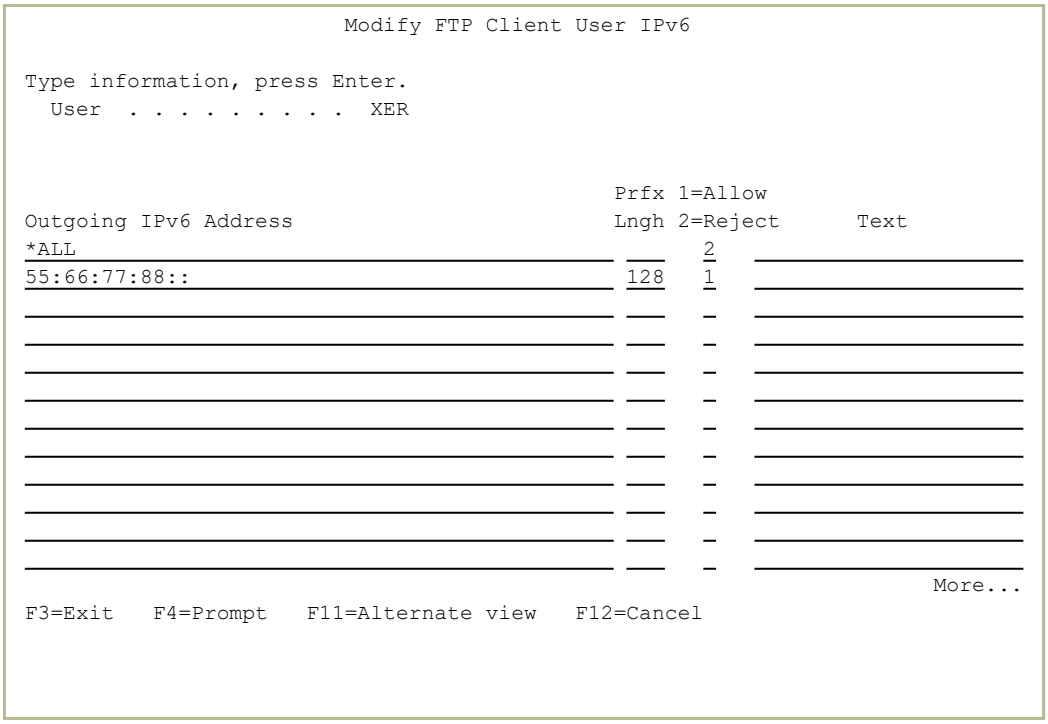
**Text**

A free-form text description of the rule.

## Modifying a User for Outgoing IPv6 FTP Connections

To **modify** information for a user or group for outgoing IPv6 FTP connections, type **1** in the **Opt** field for that user or group on the **Work with Client FTP Security IPv6** screen (*STRFW* **> 11 > 6**) as shown in "Setting Additional Controls for Outgoing IPv6 FTP Connections" on page 90, and press **Enter**.

The **Modify FTP Client User IPv6** screen appears:




The read-only **User** field shows the name of the user or group.

The body of the screen is made up of lines that can refer to different IPv6 address ranges. To modify the information for the user, you can edit or clear existing lines or add new ones.

Possible values include:

**IPv6 Address**

The IPv6 address for the range of addresses. In addition to an IPv6 address, you can set this field to ***ALL** for rules applied to all IPv6 ranges that aren't otherwise specified.

**Address prefix length**

The length of the IPv6 address prefix. This can be set to from **1-128**.

**1=Allow 2=Reject**

How Firewall responds to requests by the user for outgoing FTP connections to this IPv6 range. Possible values include:

- **1**: Accept
- **2**: Reject

**Text**

A free-form text description of the rule.

## Copying a User for Outgoing IPv6 FTP Connections

To copy information from a user or group to another for outgoing IPv6 FTP connections, enter **3** in the **Opt** field for that user or group on the Work with Client FTP Security IPv6 screen (*STRFW* **> 11 > 6**) as shown in "Setting Additional Controls for Outgoing IPv6 FTP Connections" on page 90.

The Copy FTP/REXEC Logon User IPv6 screen appears:

```
                        Copy FTP Client User IPv6

   From user . . . . . .  AA1

 To copy, type New User Name, press Enter.

   To New User Name  . . . .  _________       Name, generic*, User Group,
                                              F4 for list

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

The read-only **From user** field shows the name of the user or group whose information you are copying.

Enter the name of the user or group to whom you are copying the information in the **To New User Name** field. This can be a single or generic* name. For a list of possibilities, press the **F4** key.

## Deleting a User for Outgoing IPv6 FTP Connections

To **delete** information for a user or group for outgoing IPv6 FTP connections, enter **4** in the **Opt** field for that user or group on the **Work with Client FTP Security IPv6** screen (*STRFW* **> 11 > 6**) as shown in "Setting Additional Controls for Outgoing IPv6 FTP Connections" on page 90.

The **Delete FTP/REXEC Logon User IPv6** screen appears:

```
                        Delete FTP Client User IPv6

 Press Enter to confirm your choices for Delete, Or F12 to Cancel.
  User  . . . . . .  XER


                                              Prfx 1=Allow
Outgoing IPv6 Address                         Lngh 2=Reject      Text
*ALL                                                 2
55:66:77:88::                                  128   1

                                                                    More...
F3=Exit              F11=Alternate view   F12=Cancel
```

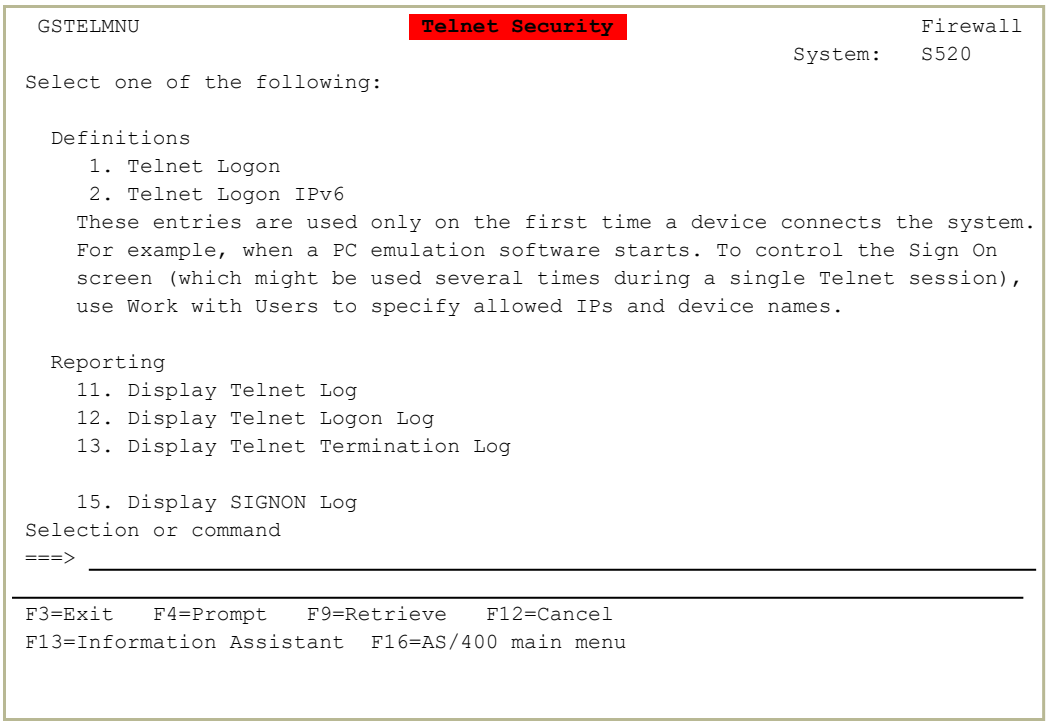
All the fields on the screen are read-only, showing the current information for the user.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Additional Controls and Displaying Logs for Telnet

To **set additional controls for Telnet** for both IPv4 and IPv6 and to display their logs, select **12. Telnet** from the Firewall Main Menu (*STRFW*). The **Telnet Security** screen appears:




These entries are only used the first time that a device connects to the system, such as when PC emulation software starts. To control the **Sign On** screen (which might be used several times during a single Telnet session), use the **Work with Users** screen to specify permitted IP addresses and device names, as shown in "Setting Firewall Rules for Users, Groups, and Applications" on page 223.

To **set controls for Telnet logons**, select **1. Telnet Logon**. The **Work with Telnet Logon Security** screen appears, as shown in "Setting Additional Controls for Telnet Logons" on page 98.

To **set controls for Telnet IPv6 logons**, select **2. Telnet Logon IPv6**. The **Work with TELNET Logon Security IPv6** screen appears, as shown in "Setting Additional Controls for IPv6 Telnet Logons" on page 107.

To display a log of all Telnet connections, select **11. Display Telnet Log**. The Display Firewall Log (DSPFWLOG) screen appears (as shown in "Displaying Firewall Logs" on page 516) with the **Type** field set to ***TELINF**.

To display a log of Telnet logons, select **12. Display Telnet Logon Log**. The Display Firewall Log (DSPFWLOG) screen appears (as shown in "Displaying Firewall Logs" on page 516) with the **Type** field set to ***FTPLOG**.

To display a log of Telnet terminations, select **13. Telnet Termination Log**. The Display Firewall Log (DSPFWLOG) screen appears (as shown in "Displaying Firewall Logs" on page 516) with the **Type** field set to ***TELOFF**.

To display a log of Sign ons, select **15. Display SIGNON Log**. The Display Firewall Log (DSPFWLOG) screen appears (as shown in "Displaying Firewall Logs" on page 516) with the **Type** field set to ***SIGNON**.

## Setting Additional Controls for Telnet Logons

To **set controls for Telnet logons**, select **`1. Telnet Logon`** from the **Telnet Security** screen (*STRFW* **`> 12`**) as shown in "Setting Additional Controls and Displaying Logs for Telnet" on page 96.

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       Subnet Mask       Terminal   vld  Logon         Terminal
 _  *ALL             0.0.0.0           *ALL        0   *REJECT
 _  1.1.1.3          255.255.255.254   *ALL        0   *ACCEPT       *SAME
 _  1.1.1.156        255.255.255.255   *ALL        0   *ACCEPT       KOM*
 _  1.1.1.156        255.255.255.255   AB*         0   *ACCEPT       LOM*
 _  1.1.1.156        255.255.255.255   ABCD        0   *ACCEPT       MOM*
 _  1.1.1.159        255.255.255.255   *ALL        0   *ACCEPT       AAA03
 _  1.1.1.198        255.255.255.255   *ALL        0   *ACCEPT       *SAME
 _  10.130.0.0       255.255.0.0       *ALL        0   *ACCEPT       *SAME
 _  178.249.3.48     255.255.255.255   *ALL        0   *REJECT




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

The body of the screen consists of seven fields, starting with an **`Opt`** field for entering options. Each line refers to a single IP address range.

The remaining fields are:

**`IP Address`**

The IP address that begins the range.

**`Subnet mask`**

The subnet mask for the address range.

**`Incoming Terminal`**

The terminal sending the request. This can be a single name, a generic* name, **`*ALL`**, or **`*BLANKS`**. For a list of known terminal names, press the **F4** key.

**Min pwd vld**

The minimum password validation level needed for the logon. The possibilities include:

- **0**: No password
- **1**: With password
- **2**: Encrypted password
- **3**: SSL connection

**Logon**

How Firewall responds to the logon request. The possibilities include:

- ***ACCEPT**: Accept logon request
- ***REJECT**: Reject logon request
- ***AUTOSIGNON**: Sign on automatically if permitted by system configuration
- ***FRCSIGNON**: Force the user to sign on even if the system is configured to accept an automatic signon.
- ***ACCEPTSIP**: Accept logon request if it is from the same IP as your system.

**Assigned Terminal**

The name assigned to the terminal if the logon is accepted. This can be an exact name, a generic* name, ***SAME**, or ***SYSTEM.**

To add Firewall settings for an IP address range, press the F6 key. The Add TELNET Logon Security Setting screen appears, as shown in "Adding Firewall Settings for Telnet Logons" on the next page.

To modify Firewall settings for an IP address range, enter **1** in the **Opt** field for that IP address range. The Modify TELNET Logon Security Setting screen appears, as shown in "Modifying Firewall Settings for Telnet Logons" on page 102.

To copy Firewall settings from one IP address range to another, enter **3** in the **Opt** field for the original IP address range. The Copy TELNET Logon Security Setting screen appears, as shown in "Copying Firewall Settings for Telnet Logons" on page 104.

To **delete** Firewall settings for an IP address range, enter **4** in the **Opt** field for the IP address range. The **Delete TELNET Logon Security Setting** screen appears, as shown in "Deleting Firewall Settings for Telnet Logons" on page 106.

## Adding Firewall Settings for Telnet Logons

To **add** Firewall settings for Telnet logins from an IP address range, press the **F6** key on the **Work with Telnet Logon Security** screen (*STRFW* **> 12 > 1**) as shown in "Setting Additional Controls for Telnet Logons" on page 98.

The **Add TELNET Logon Security Setting** screen appears:

```
                    Add TELNET Logon Security Setting

Type information, press Enter.
Selection criteria:
  IP Address  . . . . . _________________  Address, F4 for list
  Subnet mask . . . . . _________________  F4 for list
  Incoming terminal name  *ALL           Generic*, *ALL, *BLANKS, F4=List
  Minimum pwd validation  0              0=No password, 1=With password
Process:                                 2=Encrypted pwd, 3=Connection SSL
  Limit to Time Group . . _____________  Name, F4 for list
  Logon type  . . . . . . _              1=*ACCEPT, 2=*REJECT, 3=*AUTOSIGNON
For Logon= 1/3/4/5:                      4=*FRCSIGNON, 5=*ACCEPT FOR SAME IP
  Assign terminal name  . *SAME          Generic*, *SAME, *SYSTEM, F4=List
  Set new Code page . . . _____
          Character set . _____
          Keyboard layout ___
For *AUTOSIGNON Logon:
  Alt User  . . . . . . . _____________  Name, *SAME, F4 for list
  Alt Current library . . _____________  Name, *SAME
  Alt Program to call . . _____________  Name, *SAME
  Alt Initial Menu  . . . _____________  Name, *SAME

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

Enter values for the following fields:

**IP Address**

The IP address that begins the range. For a list of possible addresses, press the **F4** key.

**Subnet mask**

The subnet mask for the address range. For a list of possible subnet masks, showing the number of addresses that the range

would include, press the F4 key.

**Incoming terminal name**

The terminal sending the request. This can be a single name, a generic* name, ***ALL**, or ***BLANKS**. For a list of known terminal names, press the F4 key.

**Minimum pwd validation**

The minimum password validation level needed for the logon. The possibilities include:

- **0**: No password
- **1**: With password
- **2**: Encrypted password
- **3**: SSL connection

**Time group**

If set, Telnet connections from this IP addressrange can only be made during the times defined for this time group.

**Logon**

How Firewall responds to the logon request. The possibilities include:

- **1: *ACCEPT**: Accept logon request
- **2: *REJECT**: Reject logon request
- **3: *AUTOSIGNON**: Sign on automatically if permitted by system configuration
- **4: *FRCSIGNON**: Force the user to sign on even if the system is configured to accept an automatic signon.
- **5: *ACCEPTSIP**: Accept logon request if it is from the same IP as your system.

**Assigned Terminal**

The name assigned to the terminal if the logon is accepted. This can be an exact name, a generic* name, ***SAME**, or ***SYSTEM.**

**Set new**

**Code page**

**Character set**

**Keyboard layout**

Set these fields as needed, as described in IBM documentation at https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_71/rzaiw/rzaiwdevdesc.htm

After entering information in these fields, press the **Enter** key.

If you have set the **Logon** field to **3** (***AUTOSIGNON**), set the fields in the **For *AUTOSIGNON Logon** section to appropriate values, as indicated by OS/400 documentation.

## Modifying Firewall Settings for Telnet Logons

To **modify** Firewall settings for Telnet logins from an IP address range, type **1** in the **Opt** field for that address range on the **Work with Telnet Logon Security** screen (*STRFW* **> 12 > 1**) as shown in "Setting Additional Controls for Telnet Logons" on page 98.

The **Modify TELNET Logon Security Setting** screen appears:

```
                    Modify TELNET Logon Security setting

Type information, press Enter.
Selection criteria:
  IP Address  . . . . . .  1.1.1.3          Address, F4 for list
  Subnet mask . . . . . .  255.255.255.254  F4 for list
  Incoming terminal name   *ALL             Generic*, *ALL, *BLANKS, F4=List
  Minimum pwd validation   0                0=No password, 1=With password
Process:                                    2=Encrypted pwd, 3=Connection SSL
  Limit to Time Group . .  _____            Name, F4 for list
  Logon type  . . . . . .  1                1=*ACCEPT, 2=*REJECT, 3=*AUTOSIGNON
For Logon= 1/3/4/5:                         4=*FRCSIGNON, 5=*ACCEPT FOR SAME IP
  Assign terminal name  .  *SAME            Generic*, *SAME, *SYSTEM, F4=List
  Set new Code page . . .  _____
          Character set .  _____
          Keyboard layout  ___
For *AUTOSIGNON Logon:
  Alt User  . . . . . .  _____              Name, *SAME, F4 for list
  Alt Current library . .  _____            Name, *SAME
  Alt Program to call . .  _____            Name, *SAME
  Alt Initial Menu  . . .  _____            Name, *SAME

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

Enter or change values for the following fields:

**IP Address**

The IP address that begins the range. For a list of possible addresses, press the F4 key.

**Subnet mask**

The subnet mask for the address range. For a list of possible subnet masks, showing the number of addresses that the range would include, press the F4 key.

**Incoming terminal name**

The terminal sending the request. This can be a single name, a generic* name, ***ALL**, or ***BLANKS**. For a list of known terminal names, press the F4 key.

**Minimum pwd validation**

The minimum password validation level needed for the logon. The possibilities include:

- **0**: No password
- **1**: With password
- **2**: Encrypted password
- **3**: SSL connection

**Limit to Time group**

If set, Telnet connections from this IP addressrange can only be made during the times defined for this time group (as shown in "Defining Time Groups" on page 504).

**Logon**

How Firewall responds to the logon request. The possibilities include:

- **1: *ACCEPT**: Accept logon request
- **2: *REJECT**: Reject logon request
- **3: *AUTOSIGNON**: Sign on automatically if permitted by system configuration
- **4: *FRCSIGNON**: Force the user to sign on even if the system is configured to accept an automatic signon.

- **5: *ACCEPTSIP**: Accept logon request if it is from the same IP as your system.

**Assigned Terminal**

The name assigned to the terminal if the logon is accepted. This can be an exact name, a generic* name, ***SAME**, or ***SYSTEM.**

**Set new**

**Code page**

**Character set**

**Keyboard layout**

Set these fields as needed, as described in IBM documentation at https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_71/rzaiw/rzaiwdevdesc.htm

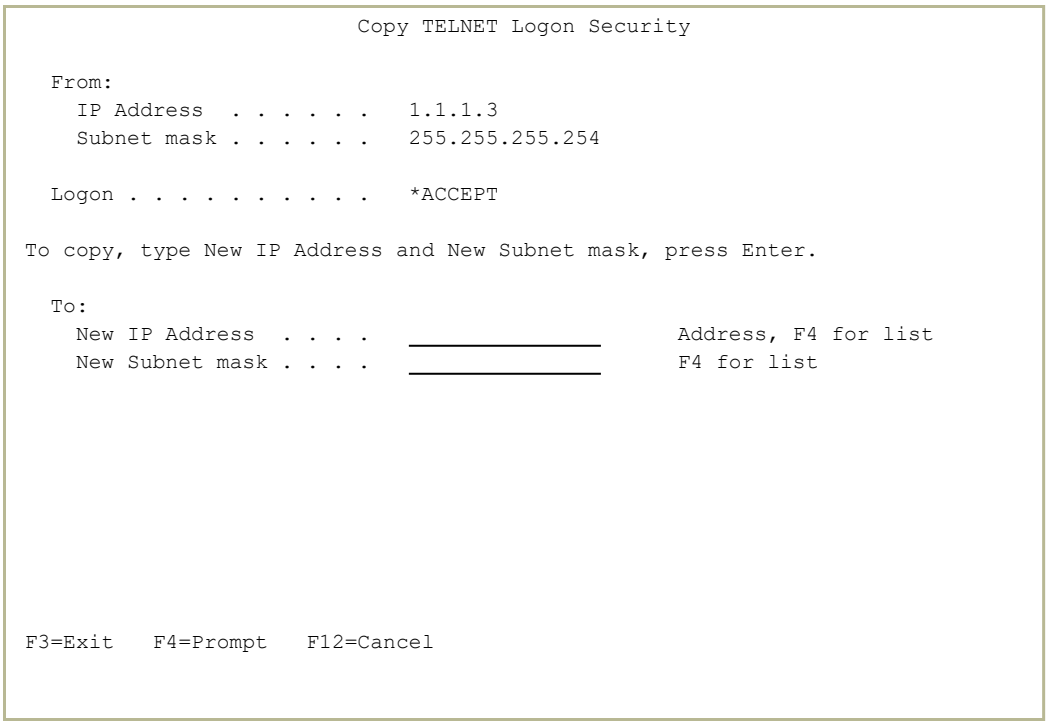
After entering information in these fields, press the **Enter** key.

If you have set the **Logon** field to **3** (*AUTOSIGNON), set the fields in the **For *AUTOSIGNON Logon** section to appropriate values, as indicated by OS/400 documentation.

## Copying Firewall Settings for Telnet Logons

To **copy** Firewall settings for Telnet logins from one IP address range to another, type **3** in the **Opt** field for the original address range on the **Work with Telnet Logon Security** screen (*STRFW* **> 12 > 1**) as shown in "Setting Additional Controls for Telnet Logons" on page 98.

The **Copy TELNET Logon Security** screen appears:




The first three fields, **IP Address**, **Subnet mask**, and **Logon**, show the original IP address range and how Firewall is set to react to Telnet logon requests from that range. The possible values for the **Logon** field include:

- ***ACCEPT**: Accept logon request
- ***REJECT**: Reject logon request
- ***AUTOSIGNON**: Sign on automatically if permitted by system configuration
- ***FRCSIGNON**: Force the user to sign on even if the system is configured to accept an automatic signon.
- ***ACCEPTSIP**: Accept logon request if it is from the same IP as your system.

Enter the information for the new IP address range into the remaining fields:

**New IP Address**

The IP address that begins the range. For a list of possible addresses, press the **F4** key.

**New Subnet mask**

The subnet mask for the address range. For a list of possible subnet masks, showing the number of addresses that the range would include, press the **F4** key.

## Deleting Firewall Settings for Telnet Logons

To **delete** Firewall settings for Telnet logins for an IP address range, enter **4** in the **Opt** field for the address range on the **Work with Telnet Logon Security** screen (***STRFW > 12 > 1***) as shown in "Setting Additional Controls for Telnet Logons" on page 98.

The **Delete TELNET Logon Security Setting** screen appears:

```
                    Delete TELNET Logon Security Setting

 Press Enter to confirm your choices for Delete, Or F12 to Cancel.
Selection criteria:
  IP Address  . . . . . .  10.130.0.0
  Subnet mask . . . . . .  255.255.0.0      F4 for list
  Incoming terminal name   *ALL
  Minimum pwd validation   0                0=No password, 1=With password
Process:                                    2=Encrypted pwd, 3=Connection SSL
  Limit to Time Group . .                   Name, F4 for list
  Logon type  . . . . . .  1
For Logon= 1/3/4/5:                         4=*FRCSIGNON, 5=*ACCEPT FOR SAME IP
  Assign terminal name  .  *SAME            Generic*, *SAME, *SYSTEM, F4=List
  Set new Code page . . .  _____
          Character set .  _____
          Keyboard layout  ___
For *AUTOSIGNON Logon:
  Alt User  . . . . . .                     Name, *SAME, F4 for list
  Alt Current library . .                   Name, *SAME
  Alt Program to call . .                   Name, *SAME
  Alt Initial Menu  . . .                   Name, *SAME

F3=Exit              F12=Cancel
```

All the fields on the screen are read-only, showing the current information for the IP address range.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Additional Controls for IPv6 Telnet Logons

To **set controls for IPv6 Telnet logons**, select **`2. Telnet Logon IPv6`** from the **Telnet Security** screen (***STRFW > 12***) as shown in "Setting Additional Controls and Displaying Logs for Telnet" on page 96.

The **Work with Telnet Logon Security IPv6** screen appears:

```
                    Work with TELNET Logon Security IPv6

 Type options, press Enter.                          Subset . . . _______________
   1=Select  3=Copy  4=Delete  5=IP range                          Min
                                                  Prfx Incoming  pwd
Opt IPv6 Address                                  Lngh Terminal  vld Logon
 _  *ALL                                               *ALL       0  *ACCEPT
 _  *ALL                                               ISE        0  *ACCEPT
 _  12:13:14:15:16::                                120 *ALL       0  *ACCEPT
 _  55:66:77:88::                                   128 *ALL       0  *AUTOSIGNON
 _  111:012::                                       108 *ALL       0  *ACCEPT
 _  1111:2222:3333:4444:5555:6666:7777:8888         124 *ALL       0  *ACCEPT
 _  1111:2222:3333:4444:5555:6666:7777:8888         125 *ALL       0  *ACCEPT
 _  1111:2222:3333:4444:5555:6666:7777:8888         126 *ALL       0  *ACCEPT
 _  1111:2222:3333:4444:5555:6666:7777:8888         127 *ALL       0  *ACCEPT
 _  1111:2222:3333:4444:5555:6666:7777:8888         128 *ALL       0  *ACCEPT
 _  1134:0::                                        124 *ALL       0  *ACCEPT
 _  1234:0::                                        128 *ALL       0  *AUTOSIGNON
 _  1234:0056:0000::                                128 *ALL       0  *ACCEPT
 _  2001:DB8:0:8::                                  61 *ALL       0  *ACCEPT
                                                                      More...
 F3=Exit   F5=Refresh   F6=Add new   F8=Print                        F12=Cancel
```

The body of the screen consists of seven fields, starting with an **`Opt`** field for entering options. Each line refers to a single IP address range.

The remaining fields are:

**`IPv6 Address`**

The IPv6 address for the range, or *ALL, representing all addresses that are not otherwise listed.

**`Prfx Lngh`**

The prefix length for the range of addresses.

**`Incoming Terminal`**

The terminal sending the request. This can be a single name, a generic* name, **`*ALL`**, or **`*BLANKS`**.

**Min pwd vld**

The minimum password validation level needed for the logon. The possibilities include:

- **0**: No password
- **1**: With password
- **2**: Encrypted password
- **3**: SSL connection

**Logon**

How Firewall responds to the logon request. The possibilities include:

- ***ACCEPT**: Accept logon request
- ***REJECT**: Reject logon request
- ***AUTOSIGNON**: Sign on automatically if permitted by system configuration
- ***FRCSIGNON**: Force the user to sign on even if the system is configured to accept an automatic signon.
- ***ACCEPTSIP**: Accept logon request if it is from the same IP as your system.

To add information for an IPv6 address range, press the F6 key. The Add Telnet Logon Security Setting IPv6 screen appears, as shown in "Adding Firewall Settings for IPv6 Telnet Logons" on the facing page.

To modify information for an IPv6 address range, enter **1** in the **Opt** field for that IPv6 address range. The Modify Telnet Logon Security Setting IPv6 screen appears, as shown in "Modifying Firewall Settings for IPv6 Telnet Logons" on page 111.

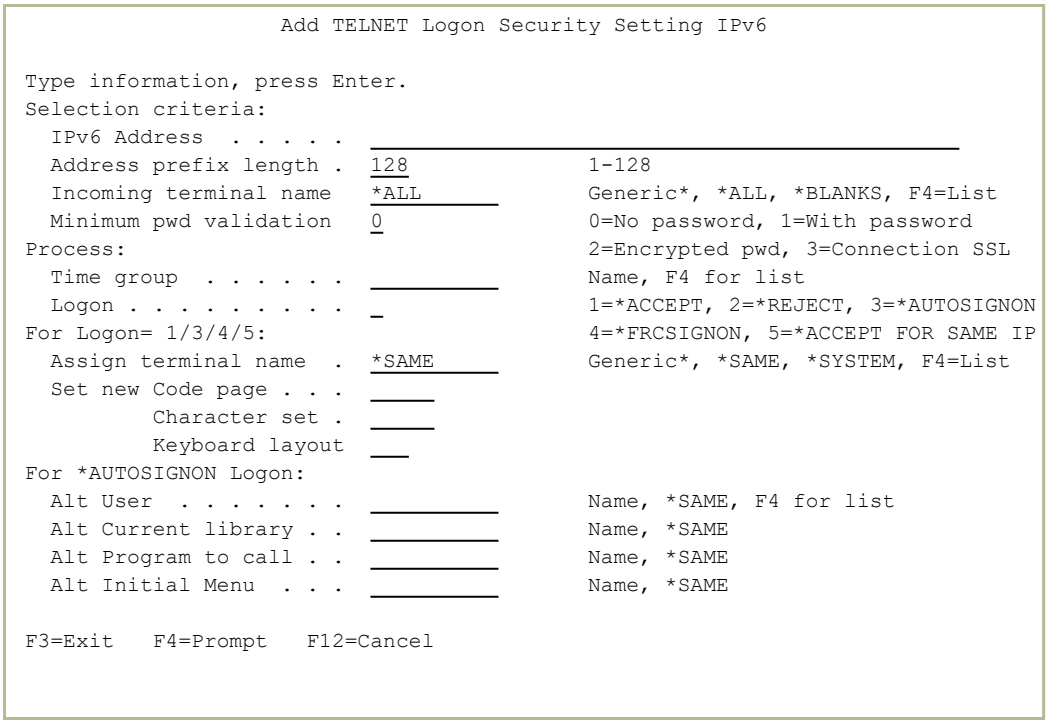
To copy information from one IPv6 address range to another, enter **3** in the **Opt** field for the original IPv6 address range. The Copy Telnet Logon Security screen appears, as shown in "Copying Firewall Settings for IPv6 Telnet Logons" on page 113.

To delete information for an IPv6 address range, enter **4** in the **Opt** field for the IPv6 address range. The Delete Telnet Logon Security Setting IPv6 screen appears, as shown in "Deleting Firewall Settings for IPv6 Telnet Logons" on page 115.

## Adding Firewall Settings for IPv6 Telnet Logons

To **add Firewall Settings for Telnet logins** from an IPv6 address range, press the **F6** key from the **Work with Telnet Logon Security IPv6** screen (***STRFW > 12 > 2***) as shown in "Setting Additional Controls for IPv6 Telnet Logons" on page 107.

The **Add TELNET Logon Security Setting IPv6** screen appears:




Enter values for the following fields:

**IPv6 Address**

The IPv6 address for the range, or *ALL, representing all addresses that are not otherwise listed.

**Address prefix length**

The prefix length for the range of addresses.

**Incoming terminal name**

The terminal sending the request. This can be a single name, a generic* name, ***ALL**, or ***BLANKS**. For a list of known terminal names, press the **F4** key.

**Minimum pwd validation**

The minimum password validation level needed for the logon. The possibilities include:

- **0**: No password
- **1**: With password
- **2**: Encrypted password
- **3**: SSL connection

**Time group**

If set, Telnet connections from this IPv6 range can only be made during the times defined for this time group.

**Logon**

How Firewall responds to the logon request. The possibilities include:

- **1: *ACCEPT**: Accept logon request
- **2: *REJECT**: Reject logon request
- **3: *AUTOSIGNON**: Sign on automatically if permitted by system configuration
- **4: *FRCSIGNON**: Force the user to sign on even if the system is configured to accept an automatic signon.
- **5: *ACCEPTSIP**: Accept logon request if it is from the same IP as your system.

**Assign terminal name**

The name assigned to the terminal if the logon is accepted. This can be an exact name, a generic* name, ***SAME**, or ***SYSTEM.**

**Set new**

**Code page**

**Character set**

**Keyboard layout**

Set these fields as needed, as described in IBM documentation at https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_71/rzaiw/rzaiwdevdesc.htm

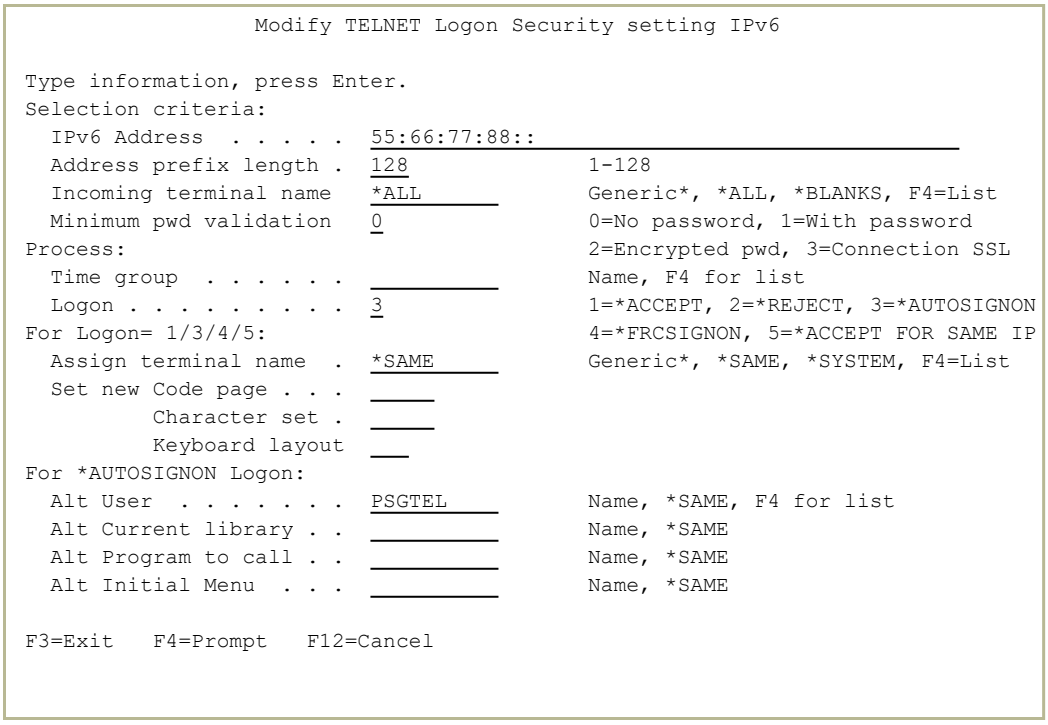
After entering information in these fields, press the **Enter** key.

If you have set the **Logon** field to **3** (*AUTOSIGNON), set the fields in the **For *AUTOSIGNON Logon** section to appropriate values, as indicated by OS/400 documentation.

## Modifying Firewall Settings for IPv6 Telnet Logons

To **modify Firewall settings for Telnet logins** from an IPv6 address range, enter **1** in the **Opt** field for that address range on the **Work with Telnet Logon Security IPv6** screen (*STRFW* **> 12 > 1**) as shown in "Setting Additional Controls for IPv6 Telnet Logons" on page 107.

The **Modify TELNET Logon Security Setting IPv6** screen appears:




Enter or change values for the following fields:

**IPv6 Address**

The IPv6 address for the range, or *ALL, representing all addresses that are not otherwise listed.

**Address prefix length**

The prefix length for the range of addresses.

**Incoming terminal name**

The terminal sending the request. This can be a single name, a generic* name, ***ALL**, or ***BLANKS**. For a list of known terminal names, press the F4 key.

**Minimum pwd validation**

The minimum password validation level needed for the logon. The possibilities include:

- **0**: No password
- **1**: With password
- **2**: Encrypted password
- **3**: SSL connection

**Time group**

If set, Telnet connections from this IPv6 range can only be made during the times defined for this time group (as shown in "Defining Time Groups" on page 504).

**Logon**

How Firewall responds to the logon request. The possibilities include:

- **1: *ACCEPT**: Accept logon request
- **2: *REJECT**: Reject logon request
- **3: *AUTOSIGNON**: Sign on automatically if permitted by system configuration
- **4: *FRCSIGNON**: Force the user to sign on even if the system is configured to accept an automatic signon.
- **5: *ACCEPTSIP**: Accept logon request if it is from the same IP as your system.

**Assign terminal name**

The name assigned to the terminal if the logon is accepted. This can be an exact name, a generic* name, ***SAME**, or ***SYSTEM.**

**Set new**

**Code page**

**Character set**

**Keyboard layout**

Set these fields as needed, as described in IBM documentation at https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_71/rzaiw/rzaiwdevdesc.htm

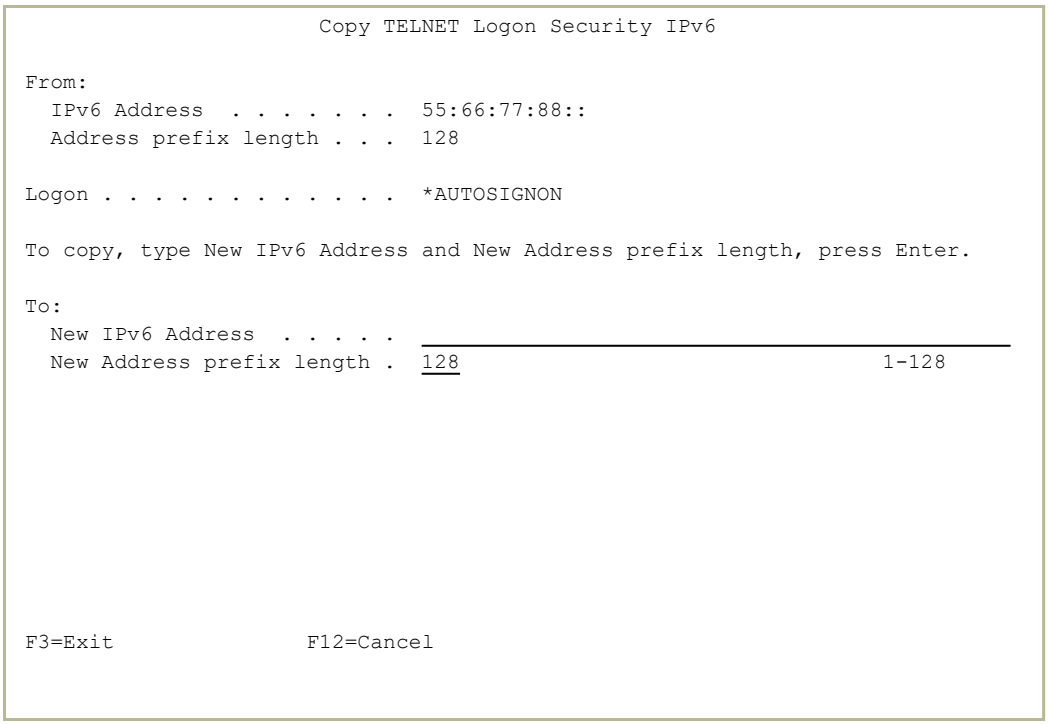
After entering information in these fields, press the **Enter** key.

If you have set the **Logon** field to **3** (*AUTOSIGNON), set the fields in the **For *AUTOSIGNON Logon** section to appropriate values, as indicated by OS/400 documentation.

## Copying Firewall Settings for IPv6 Telnet Logons

To **copy** Firewall settings for Telnet logins from one IPv6 address range to another, enter **3** in the **Opt** field for the original address range on the **Work with Telnet Logon Security IPv6** screen (*STRFW* **> 12 > 2**) as shown in "Setting Additional Controls for IPv6 Telnet Logons" on page 107.

The **Copy TELNET Logon Security IPv6** screen appears:




The first three fields, **IPv6 Address**, **Address prefix length**, and **Logon**, show the original IP address range and how Firewall is set to react to Telnet logon requests from that range. The possible values for the **Logon** field include:

- ***ACCEPT**: Accept logon request
- ***REJECT**: Reject logon request
- ***AUTOSIGNON**: Sign on automatically if permitted by system configuration
- ***FRCSIGNON**: Force the user to sign on even if the system is configured to accept an automatic signon.
- ***ACCEPTSIP**: Accept logon request if it is from the same IP as your system.

Enter the information for the new IP address range into the remaining fields:

**New IPv6 Address**

The IPv6 address for the range, or ***ALL**, representing all addresses that are not otherwise listed.

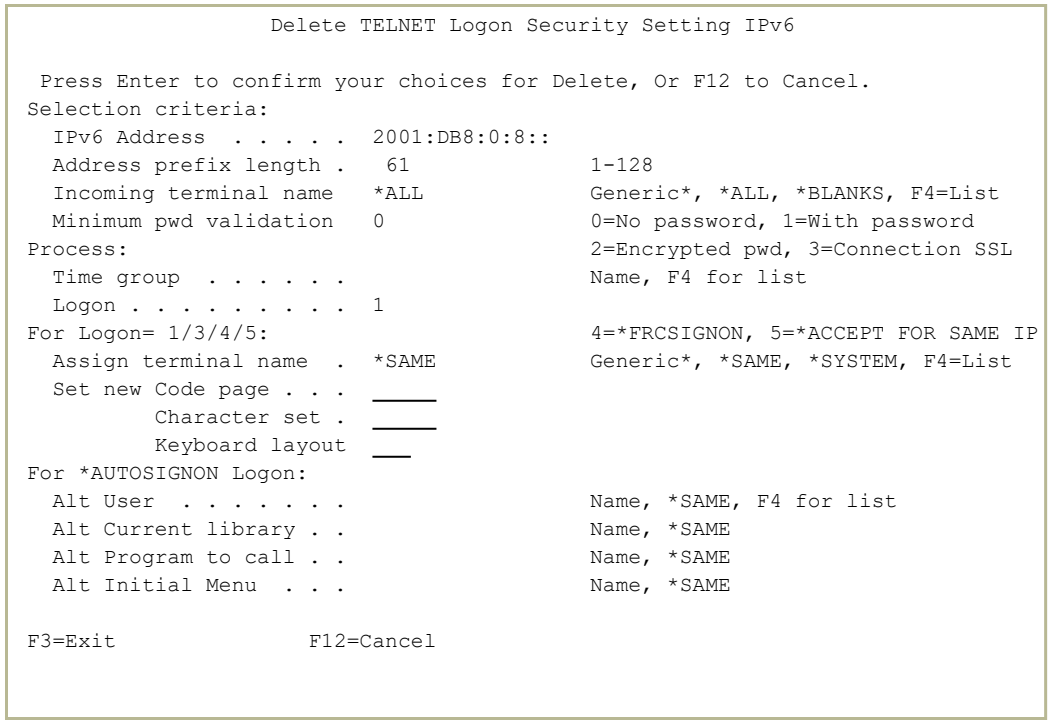
**New Address prefix length**

The prefix length for the range of addresses.

## Deleting Firewall Settings for IPv6 Telnet Logons

To **delete** Firewall settings for Telnet logons from an IPv6 address range, type **4** in the **Opt** field for the address range on the **Work with Telnet Logon Security IPv6** screen (*STRFW* **> 12 > 2**) as shown in "Setting Additional Controls for IPv6 Telnet Logons" on page 107.

The **Delete TELNET Logon Security Setting IPv6** screen appears:




All the fields on the screen are read-only, showing the current information for the IPv6 address range.

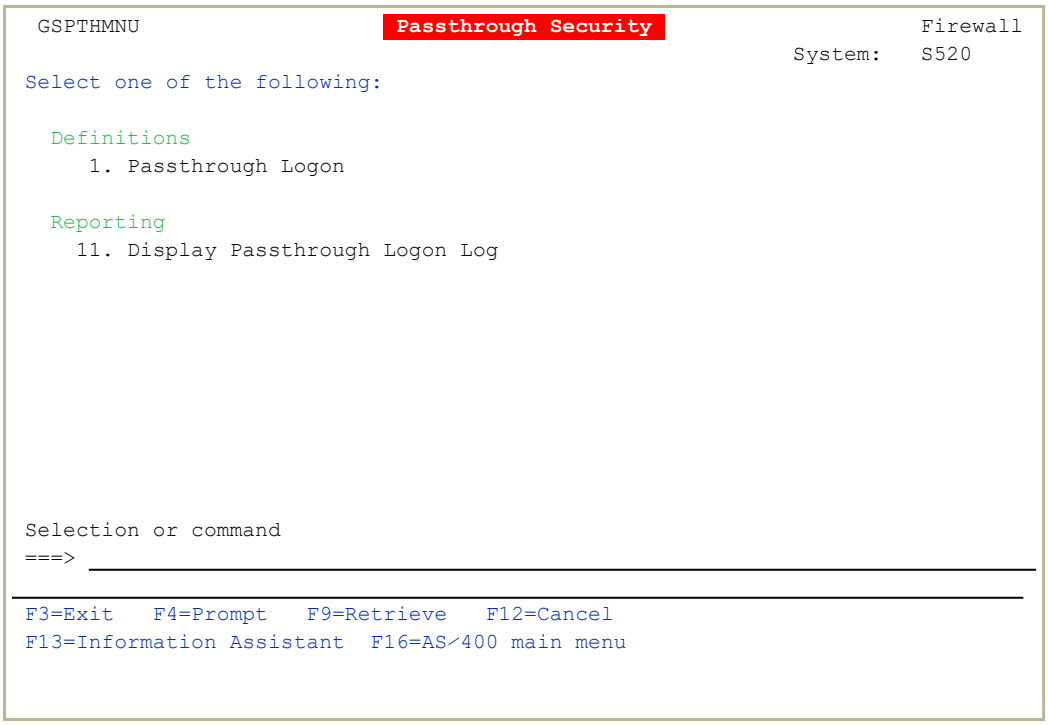
To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

# Setting Additional Controls and Displaying Logs for Passthrough Logons

To **set additional controls** for passthrough logons and to display their logs, select **13. Passthrough** from the **Firewall Main Menu** (*STRFW*).

The **Passthrough Security** screen appears:




To **set controls** for passthrough logons, select **1. Passthrough Logon**. The **Work with Passthrough Security** screen appears, as shown in "Setting Additional Controls for Passthrough Logons" on the facing page.

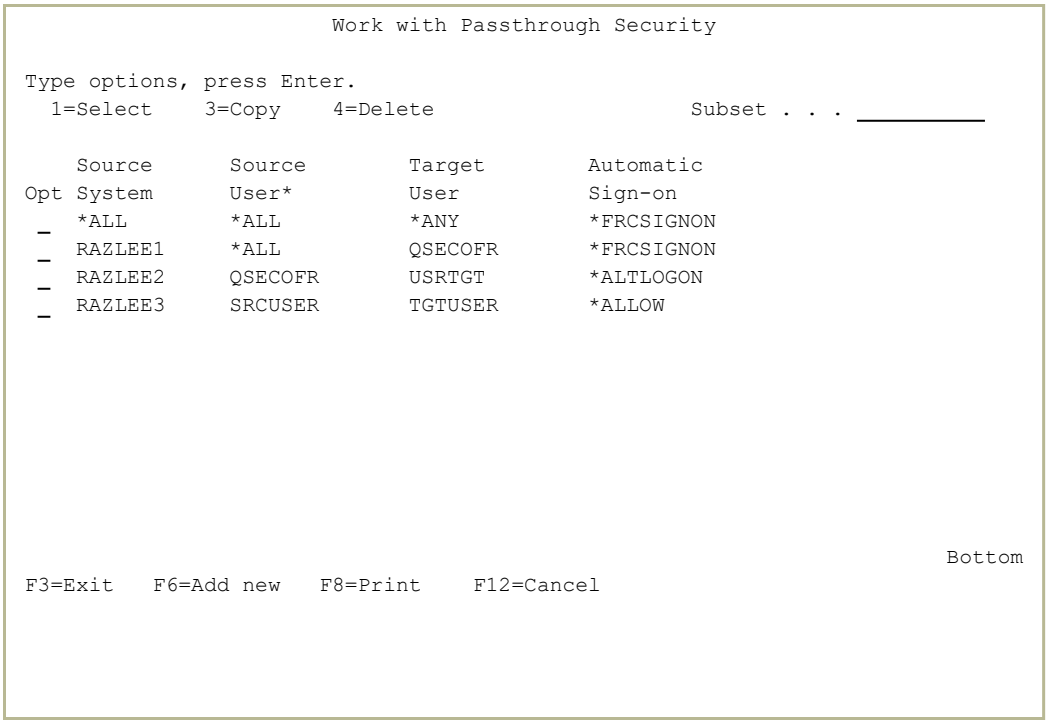
To **display reports** on passthrough logons, select **11. Display Passthrough Logon Log**. The **Display Firewall Log (DSPFWLOG)** screen (as shown in "Displaying Firewall Logs" on page 516) appears with the **Type** field set to ***RMTSGN**.

To exit this screen, press the **F3** or **F12** key.

## Setting Additional Controls for Passthrough Logons

To **set controls for Passthrough logons,** select **`1. Passthrough Logon`** from the **Passthrough Security** screen (*STRFW* **`> 13`**) as shown in "Setting Additional Controls and Displaying Logs for Passthrough Logons" on the previous page.

The **Work with Passthrough Security** screen appears:



```
                        Work with Passthrough Security

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

    Source      Source        Target        Automatic
Opt System      User*         User          Sign-on
 _  *ALL        *ALL          *ANY          *FRCSIGNON
 _  RAZLEE1     *ALL          QSECOFR       *FRCSIGNON
 _  RAZLEE2     QSECOFR       USRTGT        *ALTLOGON
 _  RAZLEE3     SRCUSER       TGTUSER       *ALLOW

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

Passthrough logons are considered for distinct or generic request patterns, in which a **Source User** on a **Source System** requests to connect to the current system as a **Target User**.

The body of the screen consists of five fields, starting with an **`Opt`** field for entering options. Each line refers to one request pattern.

The remaining fields are:

**`Source System`**

The name of the system from which the user is logging on. This can be a single name or generic* name or **`*ALL`** for all systems for which there are no more specific rules.

**Source User**

A user name from the remote system. This can be a single name or generic* name or ***ALL** for all users for whom there are no more specific rules.

**Target User**

The user on the current system as whom the remote user would like to log on. This can be a single user name, ***SAME** to connect as the same user, or ***ANY** for any user name. For a list of known users, press the F4 key.

**Automatic Sign-on**

How Firewall reacts to the sign-on attempt. Possible values include:

- ***ACCEPT**: Accept logon request
- ***REJECT**: Reject logon request
- ***FRCSIGNON**: Force the user to sign on even if the system is configured to accept an automatic signon.
- ***ALTLOGON**: Accept logon request if it is from the same IP as your system.

To add Firewall settings for a user and system, press the F6 key. The Add Passthrough Security screen appears, as shown in "Adding Firewall Settings for Passthrough Logons" on the facing page.

To modify Firewall settings for a user and system, enter **1** in the **Opt** field for that user and system. The Modify Passthrough Security screen appears, as shown in "Modifying Firewall Settings for Passthrough Logons" on page 120.

To copy Firewall settings from user and system to another, enter **3** in the **Opt** field for the original user and system. The Copy Passthrough Security screen appears, as shown in "Copying Firewall Settings for Passthrough Logons" on page 122.

To delete Firewall settings for a user and system, enter **4** in the **Opt** field for the user and system. The Delete Passthrough Security screen appears, as shown in "Deleting Firewall Settings for Passthrough Logons" on page 124.

## Adding Firewall Settings for Passthrough Logons

Passthrough logons are considered for distinct or generic **request patterns**, in which a **Source User** on a **Source System** requests to connect to the current system as a **Target User**.

To **add** Firewall settings for a request pattern, press the **F6** key from the **Passthrough Security** screen (***STRFW > 13 > 1***) as shown in "Setting Additional Controls for Passthrough Logons" on page 117.

The **Add Passthrough Security** screen appears:

```
                        Add Passthrough Security

Type choices, press Enter.

  Source system . . . . . _______          Name, *ALL
  Source user . . . . . . *ALL_____        Name, generic*, *ALL
  Target user . . . . . . *ANY_____        Name, *SAME, *ANY, F4 for list

  Time group  . . . . . _________          Name, F4 for list

  Automatic sign-on . . . . . _            1=*ALLOW
                                           2=*REJECT
                                           3=*FRCSIGNON
                                           4=*ALTLOGON
Automatic sign-on parameters for *ALTLOGON:
  User profile  . . . . . _________        Name, F4 for list
  Initial program . . . . . _________
  Initial menu  . . . . . _________
  Current library . . . . . _________


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

Enter values for the following fields:

**Source System**

The name of the system from which the user is logging on. This can be a single name or generic* name or ***ALL** for all systems for which there are no more specific rules.

**Source User**

A user name from the remote system. This can be a single name or generic* name or ***ALL** for all users for whom there are no more specific rules.

**Target User**

The user on the current system as whom the remote user would like to log on. This can be a single user name, ***SAME** to connect as the same user, or ***ANY** for any user name. For a list of known users, press the F4 key.

**Time group**

If set, passthrough logons by this user and group can only be made during the times defined for this time group (as shown in "Defining Time Groups" on page 504).

**Automatic Sign-on**

How Firewall reacts to the sign-on attempt. Possible values include:

- **1: *ACCEPT**: Accept logon request
- **2: *REJECT**: Reject logon request
- **3: *FRCSIGNON**: Force the user to sign on even if the system is configured to accept an automatic signon.
- **4: *ALTLOGON**: Automatically logon with parameters as set below.

After entering information in these fields, press the Enter key.

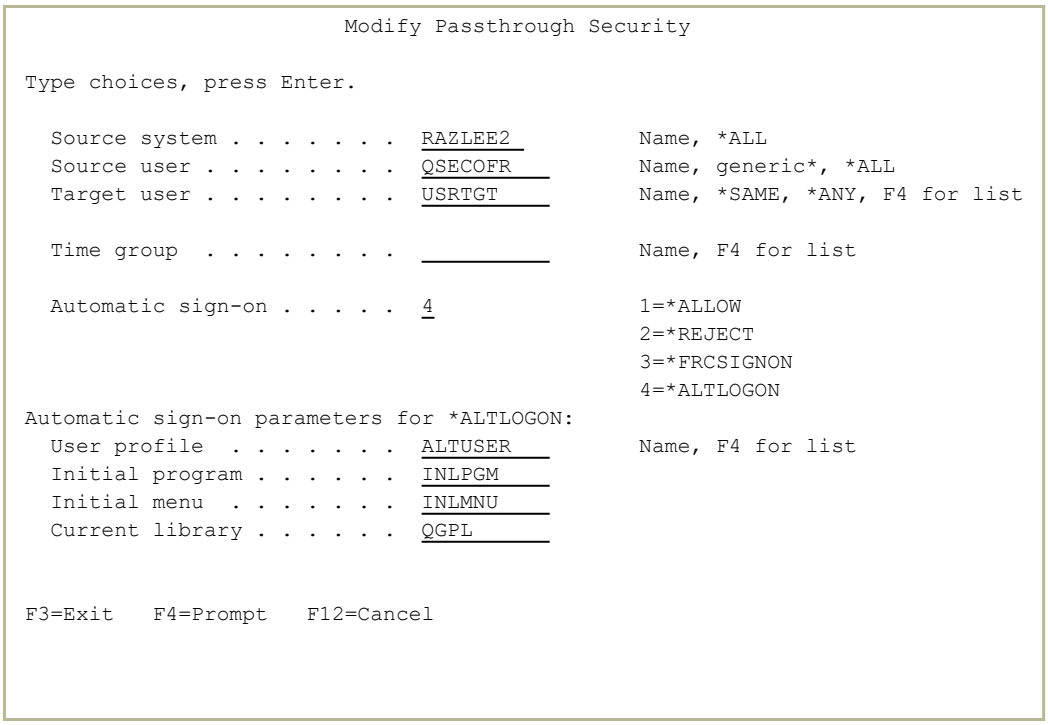
If you have set the **Logon** field to **4** (***ALTLOGON**), set the fields in the **Automatic sign-on parameters for *ALTLOGON** section to appropriate values, as indicated by OS/400 documentation.

## Modifying Firewall Settings for Passthrough Logons

Passthrough logons are considered for distinct or generic request patterns, in which a Source User on a Source System requests to connect to the current system as a Target User.

To modify Firewall settings for a request pattern, enter **1** in the **Opt** field for that pattern on the Passthrough Security screen (*STRFW* **> 13 > 1**) as shown in "Setting Additional Controls for Passthrough Logons" on page 117.

The Modify Passthrough Security screen appears:




Enter values for the following fields:

**Source System**

The name of the system from which the user is logging on. This can be a single name or generic* name or ***ALL** for all systems for which there are no more specific rules.

**Source User**

A user name from the remote system. This can be a single name or generic* name or ***ALL** for all users for whom there are no more specific rules.

**Target User**

The user on the current system as whom the remote user would like to log on. This can be a single user name, ***SAME** to connect as the same user, or ***ANY** for any user name. For a list of known users, press the **F4** key.

**Time group**

If set, passthrough logons by this user and group can only be made during the times defined for this time group (as shown in "Defining Time Groups" on page 504).

**Automatic Sign-on**

How Firewall reacts to the sign-on attempt. Possible values include:

- **1: *ACCEPT**: Accept logon request
- **2: *REJECT**: Reject logon request
- **3: *FRCSIGNON**: Force the user to sign on even if the system is configured to accept an automatic signon.
- **4: *ALTLOGON**: Automatically logon with parameters as set below.

If you are using ***ALTLOGON**, as indicated in IBM documentation, the user takes on a different identity, including that user's authority settings. Set the section of the screen labeled **Automatic sign-on parameters for *ALTLOGON:** to appropriate values.

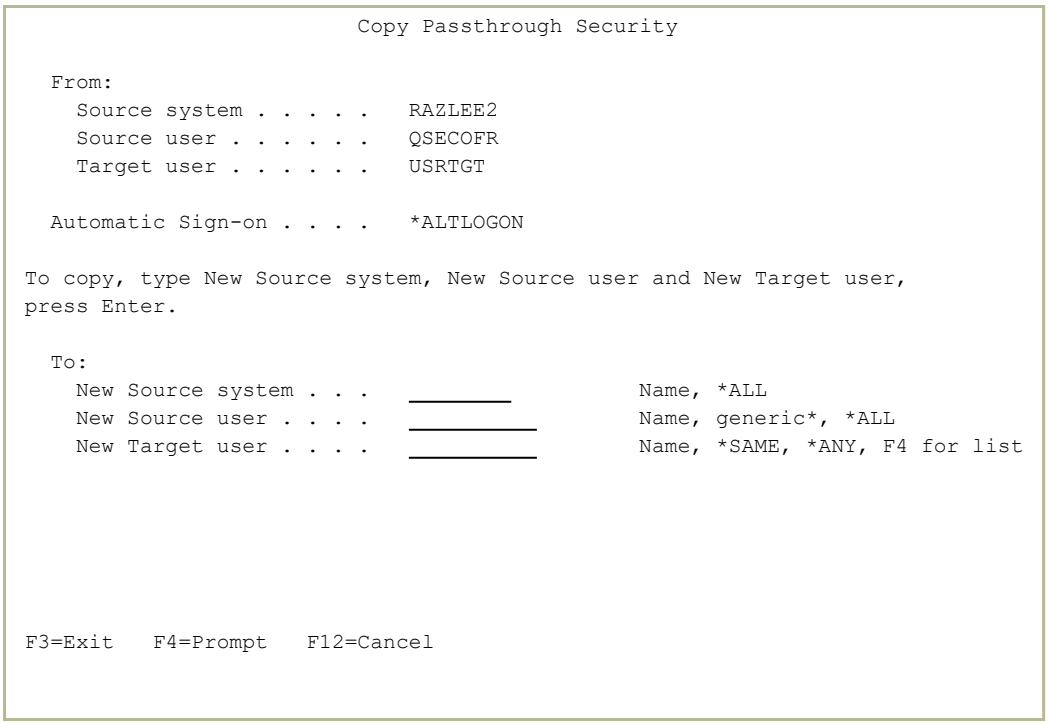
After entering information in these fields, press the Enter key.

## Copying Firewall Settings for Passthrough Logons

Passthrough logons are considered for distinct or generic request patterns, in which a Source User on a Source System requests to connect to the current system as a Target User.

To copy Firewall settings from one request pattern to another, enter **3** in the **Opt** field for that item on the Passthrough Security screen (*STRFW* **> 13 > 1**) as shown in "Setting Additional Controls for Passthrough Logons" on page 117.

The Copy Passthrough Security screen appears:




The first four fields, in the **From:** section, show the values for the original request.

Enter information for the new request pattern into the remaining fields, in the **To:** section:

**New Source System**

The name of the system from which the user is logging on. This can be a single name or generic* name or ***ALL** for all systems for which there are no more specific rules.

**New Source User**

A user name from the remote system. This can be a single name or generic* name or ***ALL** for all users for whom there are no more specific rules.

**New Target User**

The user on the current system as whom the remote user would like to log on. This can be a single user name, ***SAME** to connect as the same user, or ***ANY** for any user name. For a list of known users, press the F4 key.

## Deleting Firewall Settings for Passthrough Logons

Passthrough logons are considered for distinct or generic request patterns, in which a **Source User** on a **Source System** requests to connect to the current system as a **Target User**.

To **delete** Firewall settings for a request pattern, enter **4** in the **Opt** field for that pattern on the **Passthrough Security** screen (*STRFW* **> 13 > 1**) as shown in "Setting Additional Controls for Passthrough Logons" on page 117.

The **Delete Passthrough Security** screen appears:

```
                        Delete Passthrough Security

Press Enter to confirm your choices for Delete.
Press F12=Cancel to return to change your choices.

Source      Source        Target        Automatic
System      User          User          Sign-on
RAZLEE3     SRCUSER       TGTUSER       *ALLOW

                                                                    Bottom


F3=Exit   F12=Cancel
```

All the fields on the screen are read-only, showing the current information for the request pattern.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Additional Firewall Rules and Displaying Logs for DDM, DRDA, DHCP, and Other Servers

To **set additional rules for DDM, DRDA, and SSHD** servers, display logs or DHCP security and license management, and set TCP/IP Port restrictions, select **`14. DDM, DRDA, SSH, Port...`** from the **Firewall Main Menu** (*STRFW*).

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 security
TCP/IP Port Restrictions               or in user profile grouping.
21. Work with TCP/IP Port Restrictions




Selection or command
===> _____________________________________________________________________
_____________________________________________________________________________
F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

To **set parameters** for specified servers and products:

**`For`** DDM **`and`** DRDA**`,`**

to substitute a local user before Firewall does its checks when specified users connect from external systems, select **`1. Pre-check user replacement`**. The **Work with DDM/DRDA Pre-check User Replacement** screen appears, as shown in "Setting Firewall Rules for DDM/DRDA Pre-check User Replacement" on page 128.

**For** DRDA,

to substitute a local user after Firewall does its checks when specified users connect from external systems, select **5. DRDA post-check user replacement**. The Work with DRDA Post-check User Replacement screen appears, as shown in "Setting Firewall Rules for DRDA Post-check User Replacement" on page 133.

**For** TCP/IP **and** UDP,

to set the range of ports that a user can access, select **21. Work with TCP/IP Port Restrictions**. The Work with TCP/IP Port Restrictions screen appears, as shown in "Setting Firewall Rules for TCP/IP Port Restriction" on page 138.

**For** licensed products,

to set which features of the products the user is allowed to use, select **41. License Management**. The Work with License Security screen appears, as shown in "Setting Firewall Rules for Licensed Products" on page 143.

To display logs for specified servers and products:

**For** DHCP,

to display the DHCP security log, select **15. Display DHCP Security Log**. The Display Firewall Log (DSPFWLOG) screen appears, as shown in "Displaying Firewall Logs" on page 516, with the **Type** field set to ***DHCP**.

**For** licensed products,

to display the license management log, select **15. Display DHCP Security log**. The Display Firewall Log (DSPFWLOG) screen appears, as shown in "Displaying Firewall Logs" on page 516, with the **Type** field set to ***LICMGT**.

To set up SSHD Security to restart after changes in

- SSHD Security, as shown in "Modifying Firewall Settings for Servers" on page 58, or
- User profile grouping, as shown in "Modifying Firewall Settings for a User" on page 246,

**To** activate the current setting **immediately,**

select **51. Activate current setting**.

The Set Firewall Special Security (SETFWSPC) screen appears, with the **Option** field set to ***RESTART**.

To activate the setting immediately, press Enter.

To cancel the activation, press the F12 key.

**To** use the current setting **the next time that SSHD restarts,**

select **55. Prepare Setting For Next Start**.

The Set Firewall Special Security (SETFWSPC) screen appears, with the **Option** field set to ***PREPARE**.

To activate the setting the next time that you restart SSHD, press Enter.

To cancel the activation, press the F12 key.

To exit this screen, press the F3 or F12 key.

## Setting Firewall Rules for DDM/DRDA Pre-check User Replacement

To **view and set rules** for pre-check user replacement for DDM or DRDA connections, select **1. Pre-check user replacement** from the **Work with Advanced Security** screen (*STRFW*> **14**), as shown in "Setting Additional Firewall Rules and Displaying Logs for DDM, DRDA, DHCP, and Other Servers" on page 125.

The **Work with DDM/DRDA Pre-check User Replacement** screen appears:

```
                Work with DDM/DRDA Pre-check User Replacement

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

    Source      Source      User to
Opt Location    User*       Check
 _  AA          A           A
 _  AS400NK1    ITCMN       ITCMN
 _  QQ          V           VOVA

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

The body of the screen consists of four fields, starting with an **Opt** field for entering options. Each line refers to one user or group of users from a particular locations.

The remaining fields are:

**Source Location**

The name of the system from which the user is connecting.

**Source User***

A user name from the remote system. This can be a single name or generic* name or ***ALL** for all users for whom there are no more specific rules.

**User to check**

The user on the current system whose authority Firewall checks before doing its other checks.

To **add** Firewall rules for a user and system, press the **F6** key. The **Add DDM/DRDA Pre-check User Replacement** screen appears, as shown in "Adding Firewall Rules for DDM/DRDA Pre-check User Replacement" below.

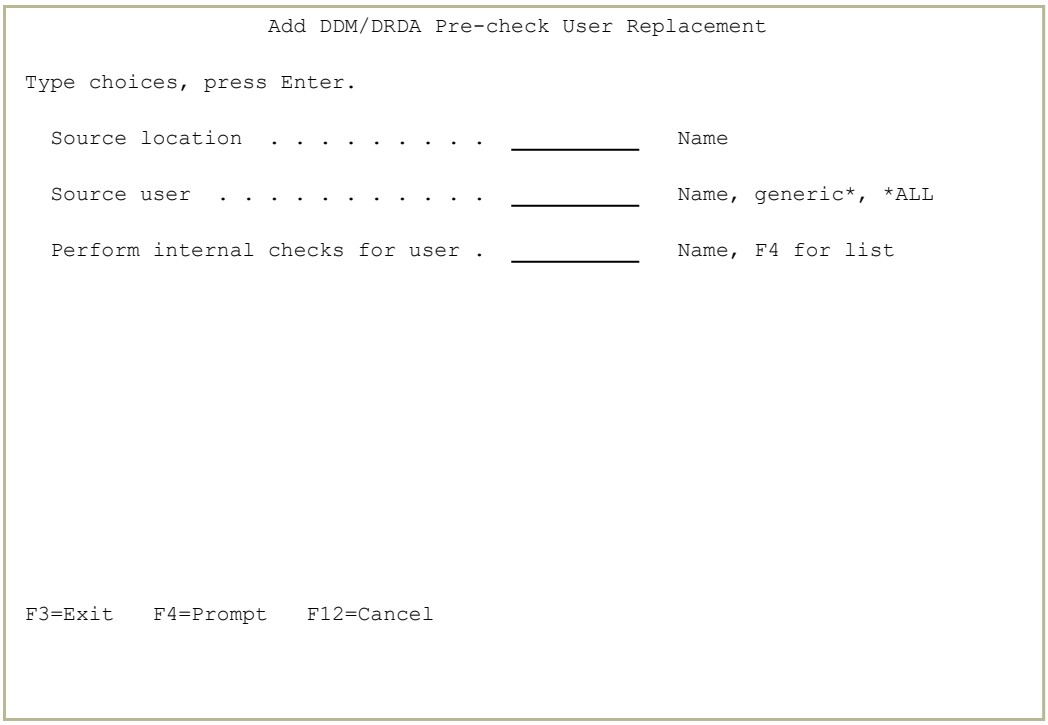
To **modify** Firewall rules for a user and system, enter **1** in the **Opt** field for that user and system. The **Modify DDM/DRDA Pre-check User Replacement** screen appears, as shown in "Modifying Firewall Rules for DDM/DRDA Pre-check User Replacement" on the next page.

To **delete** Firewall settings for a user and system, enter **4** in the **Opt** field for the user and system. The **Delete DDM/DRDA Pre-check User Replacement** screen appears, as shown in "Deleting Firewall Rules for DDM/DRDA Pre-check User Replacement" on page 131.

## Adding Firewall Rules for DDM/DRDA Pre-check User Replacement

To **add Firewall rules for DDM/DRDA pre-check user replacement** for a user and system, press the **F6** key from the **Work with DDM/DRDA Pre-check User Replacement** screen (*STRFW* **> 14 > 1** ) as seen in "Setting Firewall Rules for DDM/DRDA Pre-check User Replacement" on the previous page.

The **Add DDM/DRDA Pre-check User Replacement** screen appears:




Enter values for the following fields:

**Source location**

The name of the system from which the user is connecting.

**Source user**

A user name from the remote system. This can be a single name or generic* name or ***ALL** for all users for whom there are no more specific rules.

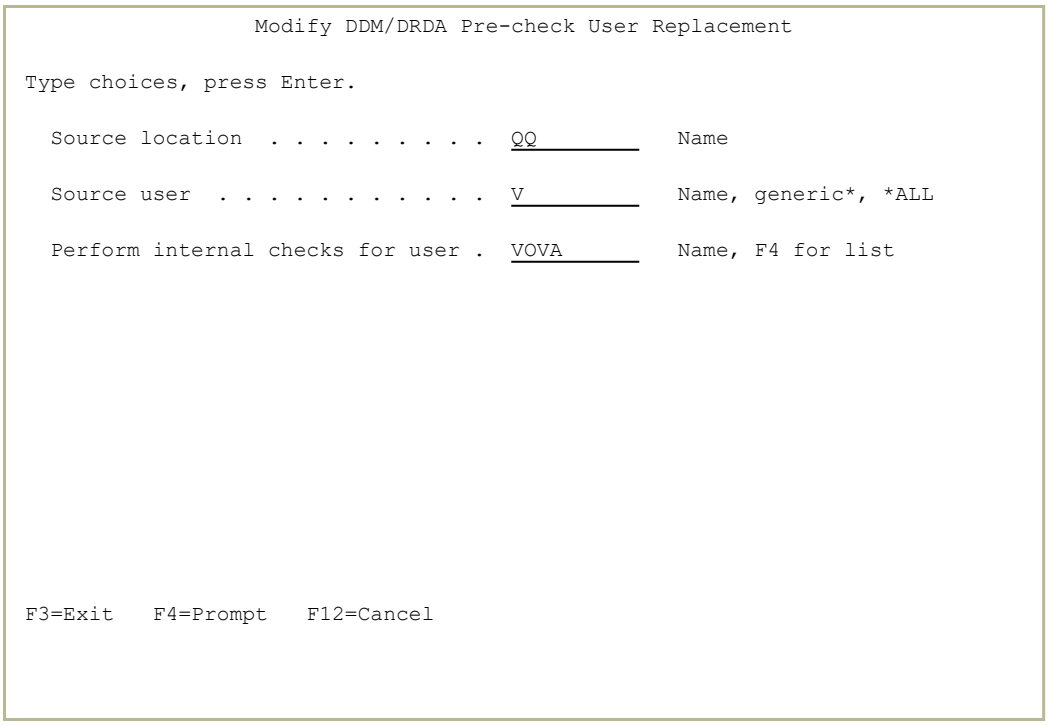
**Perform internal checks for user**

The user on the current system whose authority Firewall checks before doing its other checks. For a list of known users, press the F4 key.

## Modifying Firewall Rules for DDM/DRDA Pre-check User Replacement

To modify Firewall rules for DDM/DRDA pre-check user replacement for a user and system, enter **1** in the **Opt** field for that user and system on the Work with DDM/DRDA Pre-check User Replacement screen (*STRFW* **> 14 > 1** ) as seen in "Setting Firewall Rules for DDM/DRDA Pre-check User Replacement" on page 128.

The Modify DDM/DRDA Pre-check User Replacement screen appears:




Enter or change values for the following fields:

**Source location**

The name of the system from which the user is connecting.

**Source user**

A user name from the remote system. This can be a single name or generic* name or ***ALL** for all users for whom there are no more specific rules.

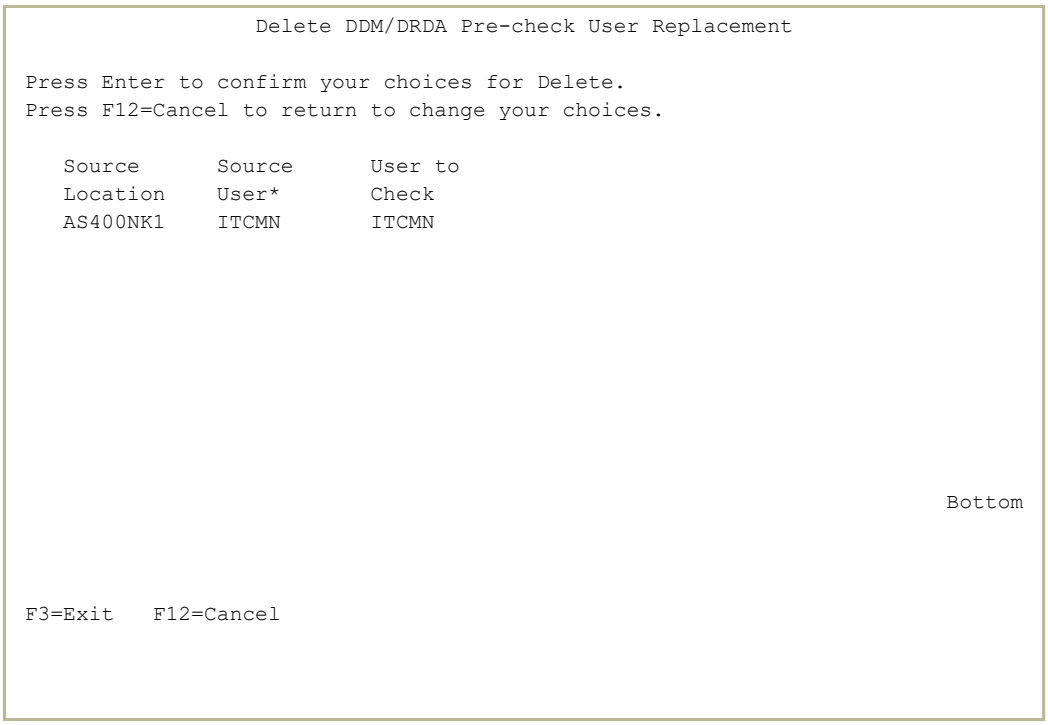
**Perform internal checks for user**

The user on the current system whose authority Firewall checks before doing its other checks. For a list of known users, press the **F4** key.

## Deleting Firewall Rules for DDM/DRDA Pre-check User Replacement

To **delete Firewall rules for DDM/DRDA pre-check user replacement** for a user and system, type **4** in the **Opt** field for that user and system on the **Work with DDM/DRDA Pre-check User Replacement** screen (*STRFW* **> 14 > 1**) as seen in "Setting Firewall Rules for DDM/DRDA Pre-check User Replacement" on page 128.

The **Delete DDM/DRDA Pre-check User Replacement** screen appears:




All the fields on the screen are read-only, showing the current information for the user and system.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Firewall Rules for DRDA Post-check User Replacement

**To view and set rules for post-check user replacement** for DRDA connections, select **`5. DRDA Post-check user replacement`** from the **Work with Advanced Security** screen (***STRFW > 14***), as shown in "Setting Additional Firewall Rules and Displaying Logs for DDM, DRDA, DHCP, and Other Servers" on page 125.

The **Work with DRDA Post-check User Replacement** screen appears:

```
                  Work with DRDA Post-check User Replacement

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

    Source      Source      User for OS/400
Opt Location    User*       Security checks
 _  A           KING1         KING2
 _  AS400NKZ    ITCMN         ITCMN
 _  QQQ         V             VOVA

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

The body of the screen consists of four fields, starting with an **`Opt`** field for entering options. Each line refers to one user or group of users from a particular locations.

The remaining fields are:

**`Source Location`**

The name of the system from which the user is connecting.

**`Source User*`**

A user name from the remote system. This can be a single name or generic* name or **`*ALL`** for all users for whom there are no more specific rules.

**User for OS/400 Security checks**

The user on the current system whose authority Firewall checks after doing its other checks.

To **add** Firewall rules for a user and system, press the **F6** key. The **Add DRDA Post-check User Replacement** screen appears, as shown in "Adding Firewall Rules for DRDA Post-check User Replacement" below.

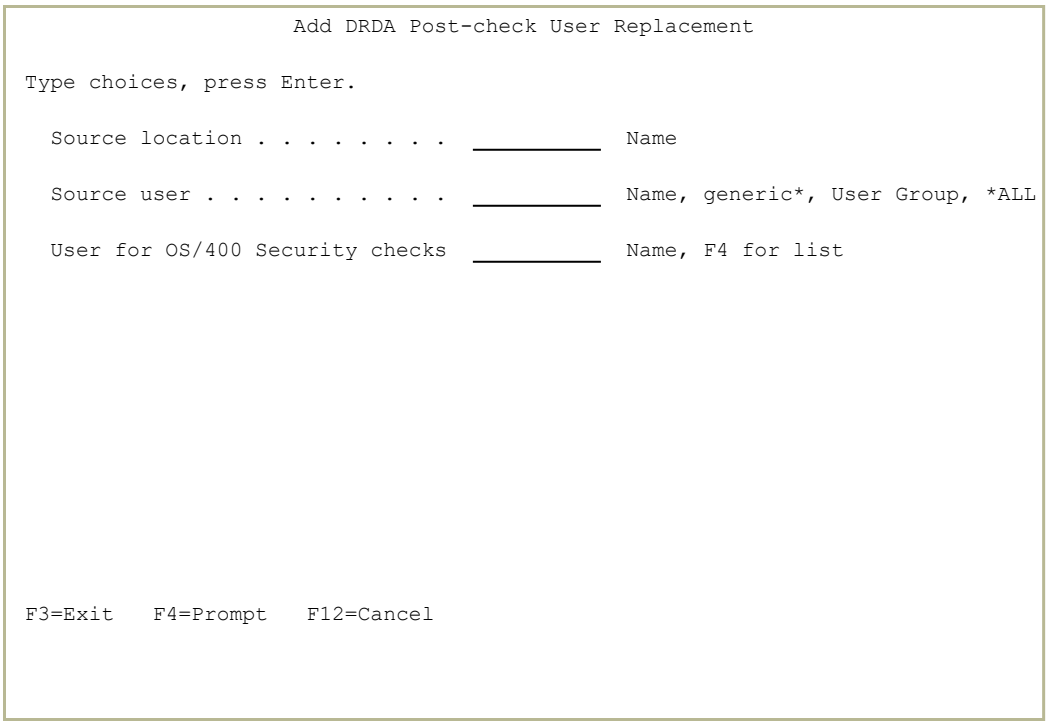
To **modify** Firewall rules for a user and system, enter **1** in the **Opt** field for that user and system. The **Modify DRDA Post-check User Replacement** screen appears, as shown in "Modifying Firewall Rules for DRDA Post-check User Replacement" on the facing page.

To **delete** Firewall settings for a user and system, enter **4** in the **Opt** field for the user and system. The **Delete DRDA Post-check User Replacement** screen appears, as shown in "Deleting Firewall Rules for DRDA Post-check User Replacement" on page 137.

## Adding Firewall Rules for DRDA Post-check User Replacement

To **add Firewall rules for DRDA post-check user replacement** for a user and system, press the **F6** key from the **Work with DRDA Post-check User Replacement** screen (*STRFW* **> 14 > 5** ) as seen in "Setting Firewall Rules for DRDA Post-check User Replacement" on the previous page.

The **Add DRDA Post-check User Replacement** screen appears:




Enter values for the following fields:

**Source location**

The name of the system from which the user is connecting.

**Source user**

A user name from the remote system. This can be a single name or generic* name or ***ALL** for all users for whom there are no more specific rules.

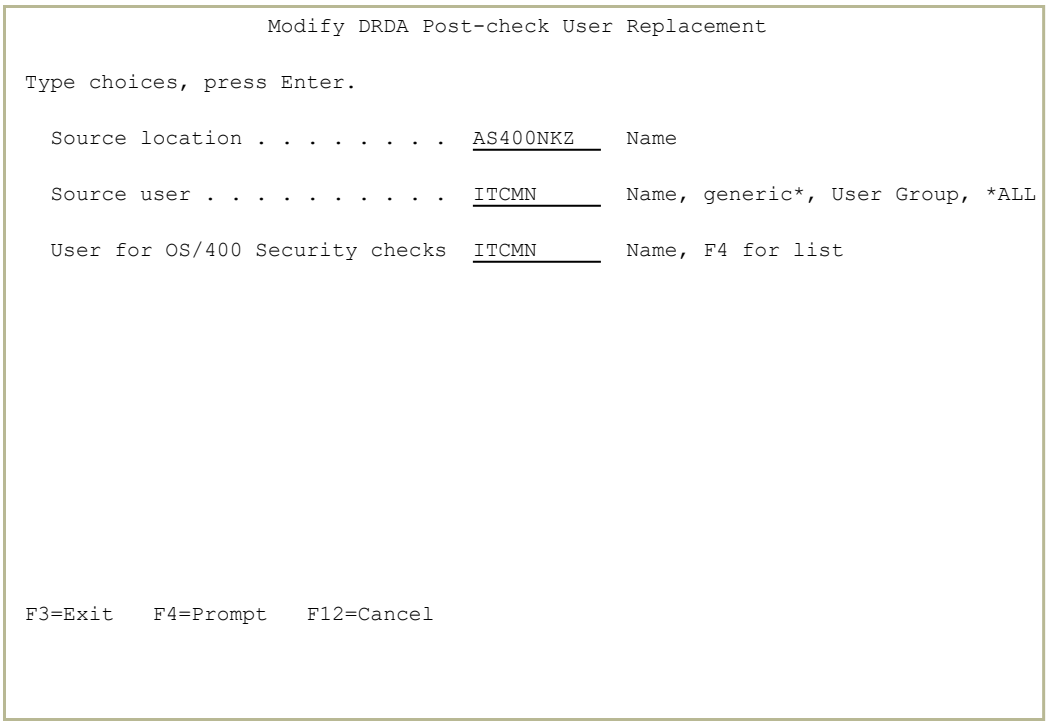
**User for OS/400 Security checks**

The user on the current system whose authority Firewall checks after doing its other checks. For a list of known users, press the **F4** key.

## Modifying Firewall Rules for DRDA Post-check User Replacement

To **modify Firewall rules for DRDA post-check user replacement** for a user and system, enter **1** in the **Opt** field for that user and system on the **Work with DRDA Post-check User Replacement** screen (*STRFW* **> 14 > 5**) as shown in "Setting Firewall Rules for DRDA Post-check User Replacement" on page 133.

The **Modify DRDA Post-check User Replacement** screen appears:




Enter or change values for the following fields:

**Source location**

The name of the system from which the user is connecting.

**Source user**

A user name from the remote system. This can be a single name or generic* name or ***ALL** for all users for whom there are no more specific rules.

**User for OS/400 Security checks**

The user on the current system whose authority Firewall checks after doing its other checks. For a list of known users, press the **F4** key.

## Deleting Firewall Rules for DRDA Post-check User Replacement

To **delete Firewall rules for DRDA post-check user replacement** for a user and system, type **4** in the **Opt** field for that user and system on the **Work with DRDA Post-check User Replacement** screen (*STRFW* **> 14 > 5**) as seen in "Setting Firewall Rules for DRDA Post-check User Replacement" on page 133.

The **Delete DRDA Post-check User Replacement** screen appears:

```
                  Delete DRDA Post-check User Replacement

Press Enter to confirm your choices for Delete.
Press F12=Cancel to return to change your choices.

   Source      Source      User for OS/400
   Location    User        Security checks
   AS400NKZ    ITCMN         ITCMN

                                                                  Bottom


F3=Exit   F12=Cancel
```

All the fields on the screen are read-only, showing the current information for the user and system.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Firewall Rules for TCP/IP Port Restriction

You can set restrictions on TCP/IP ports so that only specified users or groups can access them for either TCP or UDO traffic or both.

NOTE: While you can set restrictions for any ports, restricting ports 1-1024 may clash with other TCP/IP activity on your system, so you should avoid restricting them.

Firewall's port restriction interface is a graphical representation of the OS/400 *CFGTCP* command, which is described further in IBM documentation.

Port restrictions are enforced at all times, even if Firewall is working in FYI mode (as shown in "Running Firewall in FYI Simulation mode" on page 536).

To **view and set rules** for TCP/IP port restrictions, select **`21. Work with TCP/IP Port Restrictions`** from the **Work with Advanced Security** screen (*STRFW* **`> 14`**), as shown in "Setting Additional Firewall Rules and Displaying Logs for DDM, DRDA, DHCP, and Other Servers" on page 125.

The **Work with TCP/IP Port Restrictions** screen appears:

```
                     Work with TCP/IP Port Restrictions
                                                          System:   S520
Type options, press Enter.
  4=Delete

                         Allowed
Opt   Port-Range  Type   For User    Port description
 _     5000  5500  TCP    EVGTST
 _    22222 33333  TCP    EVGTST
 _    22222 33333  UDP    EVGTST









                                                                    Bottom
WARNING: o Using port numbers in range 1-1024 may affect TCP/IP processing.
         o Port restrictions are enforced even in *FYI mode.
F3=Exit    F6=Add new    F7=Sort by User    F8=Print                  F12=Cancel
```

The body of the screen contains lines for each port restriction. Each contains several fields. After the initial **Opt** field, they are:

**Port-Range**

A pair of fields showing the starting and ending port numbers for the range restricted by this rule. If the range only contains a single port, the second field is set to ***ONLY**.

**Type**

The protocols restricted by this rule. This can be set to **TCP**, **UDP**, or ***BOTH**.

**For User**

The user or group whose access is affected by the rule.

**Port description**

A free-form text description of the rule.

To add new port restrictions, press the F6 key. The Add TCP/IP Port Restriction screen appears, as shown in "Adding Firewall Rules for TCP/IP Port Restriction" on the next page.

To delete port restrictions, enter **4** in the **Opt** column for the line showing that restriction. The Delete TCP/IP Port Restrictions screen appears, as shown in "Deleting Firewall Rules for TCP/IP Port Restriction" on page 142.

## Adding Firewall Rules for TCP/IP Port Restriction

To **add new port restrictions**, press the **F6** key from the **Work with TCP/IP Port Restrictions** screen (***STRFW > 14 > 21***) as shown in "Setting Firewall Rules for TCP/IP Port Restriction" on page 138.

The **Add TCP/IP Port Restriction** screen appears:

```
                        Add TCP/IP Port Restriction

Type choices, press Enter.

  Range of port values:

    From port  . . . . . .  _____          1-65535

    To port  . . . . . .  *ONLY          1-65535, *ONLY

  Protocol . . . . . .  BOTH          TCP, UDP, BOTH

  Allowed for user profile . . . . .  _________     Name, %Group, F4 for list

  Allowed for users of Group Profile  N             Y=Yes, N=No


  WARNING: Maximal number of users of Group Profile is limited to 32000.

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

The screen includes the following fields:

**Range of port values:**

**From port**

The lowest port number in the range of ports.

**To port**

The highest number in the range of ports. If the restriction is only for the single port number entered in the From port field, set this to ***ONLY**.

NOTE: While you can set restrictions for any ports, restricting ports 1-1024 may clash with other TCP/IP activity on your system, so you should avoid restricting them.

**Protocol**

The TCP/IP protocol restricted on this port. Possible values are:

- **TCP**
- **UDP**
- **BOTH** (for both TCP and UDP)

**Allowed for user profile**

The user or group allowed to use these ports. Set this to a single name or a %group. To select from a list of known users and groups, press the F4 key.

**Allowed for users of Group Profile**

If the previous field contains a %group name, whether members of that group may use the port. Possible values are:

- **Y**: Yes
- **N**: No

## Deleting Firewall Rules for TCP/IP Port Restriction

To **delete** port restrictions, type **4** in the **Opt** column for the line showing that restriction on the **Work with TCP/IP Port Restrictions** screen (*STRFW* **> 14 > 21**) as shown in "Setting Firewall Rules for TCP/IP Port Restriction" on page 138, and press **Enter**.

The **Delete TCP/IP Port Restrictions** screen appears:

```
                      Delete TCP/IP Port Restrictions
                                                          System:   S520
Press Enter to confirm your choices for Delete.
Press F12=Cancel to return to change your choices.

                       Allowed
      Port-Range  Type  For User    Port description
      5000  5500  TCP   EVGTST

                                                                  More...

F3=Exit    F12=Cancel
```

All the fields on the screen are read-only, showing the current information for the port range.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Firewall Rules for Licensed Products

To **set which users can use licensed software**, including specific features within the software, select **41. License Management** from the **Work with Advanced Security** menu (*STRFW* **> 14**) as shown in "Setting Additional Firewall Rules and Displaying Logs for DDM, DRDA, DHCP, and Other Servers" on page 125.

The **Work with License Security** screen appears:

```
                          Work with License Security

Type options, press Enter.
  1=Select   4=Delete                              Subset . . . ARS:EEN AP

Opt  User          Product     Feature    Allowed
 _   *PUBLIC       *ALL         *ALL
 _   GROUP1        B            C            Y

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

The body of the screen consists of five fields, starting with an **Opt** field for entering options. Each line refers to one combination of a user or group and a product or feature.

The remaining fields are:

**User**

The user or group whose access to the product this rule controls. This can be a single or generic* user or group, or ***PUBLIC** to set rules for all users for whom no more specific rules have been set.

**Product**

The licensed product for which access is being set.

**Feature**

The feature within the licensed product for which access is being set.

**Allowed**

Whether the user or group is allowed to use the product or feature. Set this to **Y** if true.

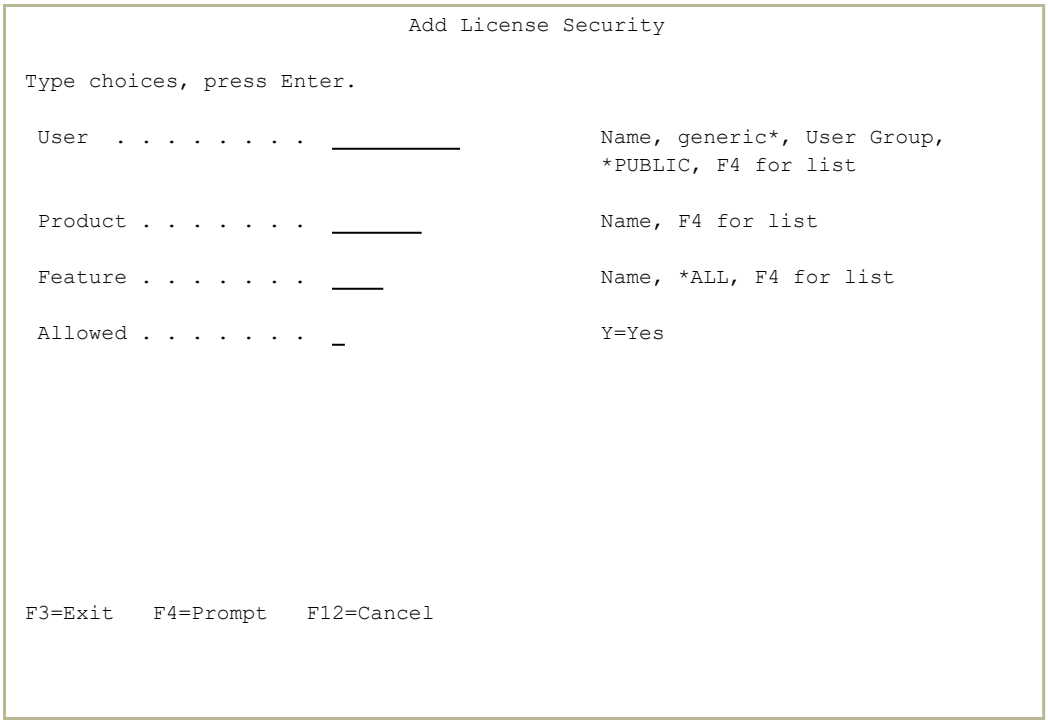
To add information about whether a user can use a product or feature, press the F6 key. The Add License Security screen appears, as shown in "Adding Firewall Rules for Licensed Products" on the facing page.

To delete information about whether a user can use a product or feature, enter **4** in the **Opt** column for that rule. The Delete License Security screen appears, as shown in "Deleting Firewall Rules for Licensed Products" on page 147.

## Adding Firewall Rules for Licensed Products

To **add** information about whether a user can use a product or feature, press the **F6** key from the **Work with License Security** screen (*STRFW* **> 14 > 41**) as shown in "Setting Firewall Rules for Licensed Products" on page 143.

The **Add License Security** screen appears:




Enter values in the following fields:

**User**

The user or group whose access to the product this rule controls. This can be a single or generic* user or group, or ***PUBLIC** to set rules for all users for whom no more specific rules have been set. For a list of known users, press the **F4** key.

**Product**

The licensed product for which access is being set.

For a list of known products, press the **F4** key. The **Select license information** screen appears, showing a list of products and their features. Selecting an item from this list fills in both the **Product** and **Feature** fields.

**Feature**

The feature within the licensed product for which access is being set.

**Allowed**

Whether the user or group is allowed to use the product or feature. Set this to **Y** if true.

## Deleting Firewall Rules for Licensed Products

To **delete** information about whether a user can use a product or feature, type **4** in the **Opt** column for that rule the **Work with License Security** screen (***STRFW > 14 > 41***) as shown in "Setting Firewall Rules for Licensed Products" on page 143, and press **Enter**.

The **Delete License Security** screen appears:

```
                          Work with License Security

Press Enter to confirm your choices for Delete.
Press F12=Cancel to return to change your choices.

 User         Product      Feature     Allowed
 GROUP1       B            C              Y

                                                                      Bottom

F3=Exit    F12=Cancel
```

All the fields on the screen are read-only, showing the current information for the user and product or feature.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Controlling DBOPEN and SQL Access

The DBOPEN and SQL servers can each manage SQL access to objects. Each handles a different, though overlapping, subset of SQL commands.

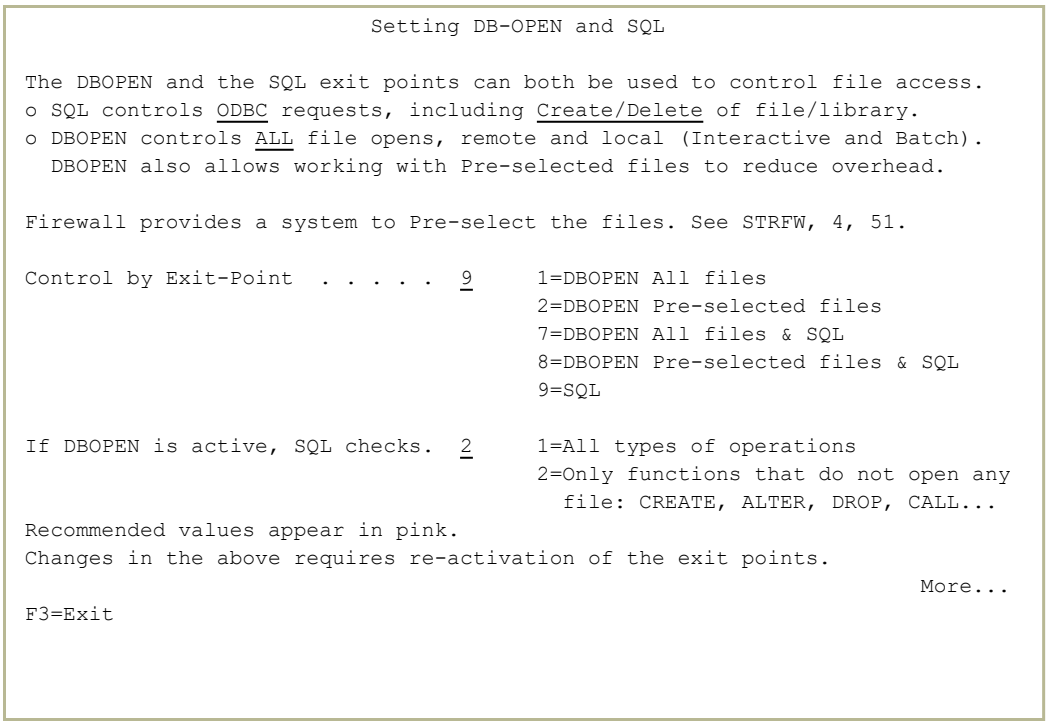
Using DBOPEN has several advantages:

- The SQL server only handles opening files via SQL.
  DBOPEN also handles database files opened in other ways.
- The SQL server only handles file accesses via ODBC from external systems.
  DBOPEN also handles accesses from external systems via other methods, files as well as accesses from within the system, including STRSQL, interactive jobs or standard jobs that are not running as servers.
- The SQL server only looks at accesses before they are parsed.
  DBOPEN also examines them after they are parsed.
- The SQL server needs to parse statements twice, once by OS400 and once by Firewall.
  DBOPEN statements only need to be parsed once, by OS400, with fewer possibilities for issues arising.
- The SQL server needs to check all SQL statements, each time that they are used.
  In DBOPEN, if a file is kept open between consecutive uses of SQL, it only needs to be checked once.
- The SQL server checks accesses to all files.
  You can set DBOPEN to check only accesses to specific files. This can dramatically reduce the number of file checks.

On the other hand, several SQL verbs are only available through the SQL server. Some third-party products also require the SQL server,

To control which access requests are managed by DBOPEN and SQL, select **`2. DBOPEN and SQL Settings`** from the Activation and Server Settings screen (*STRFW*`> 1`) as shown in "Setting Firewall Rules by Server" on page 52.

The Setting DB-OPEN and SQL screen appears:




You can set whether DBOPEN, SQL, or both check file accesses, and whether they handle access to all relevant files or only those that have been pre-selected, through these fields:

**Control by Exit-Point**

Choose from these options:

- **1=DBOPEN All files**: Use DBOPEN for all files. If you choose this option, Firewall does not track accesses via the SQL exit point.
- **2=DBOPEN Pre-selected files**: Use DBOPEN on accesses to files that you have specified via the **Work with Object Auditing Plan** screen (*STRFW* **> 4 > 51**) as shown in "Defining Files for Firewall to Track" on page 391. If you choose this option, Firewall does not track accesses via the SQL exit point, or to objects that have not been selected.
- **7=DBOPEN All files & SQL**: (Recommended) Manage access requests for all files via both the DBOPEN and SQL servers.

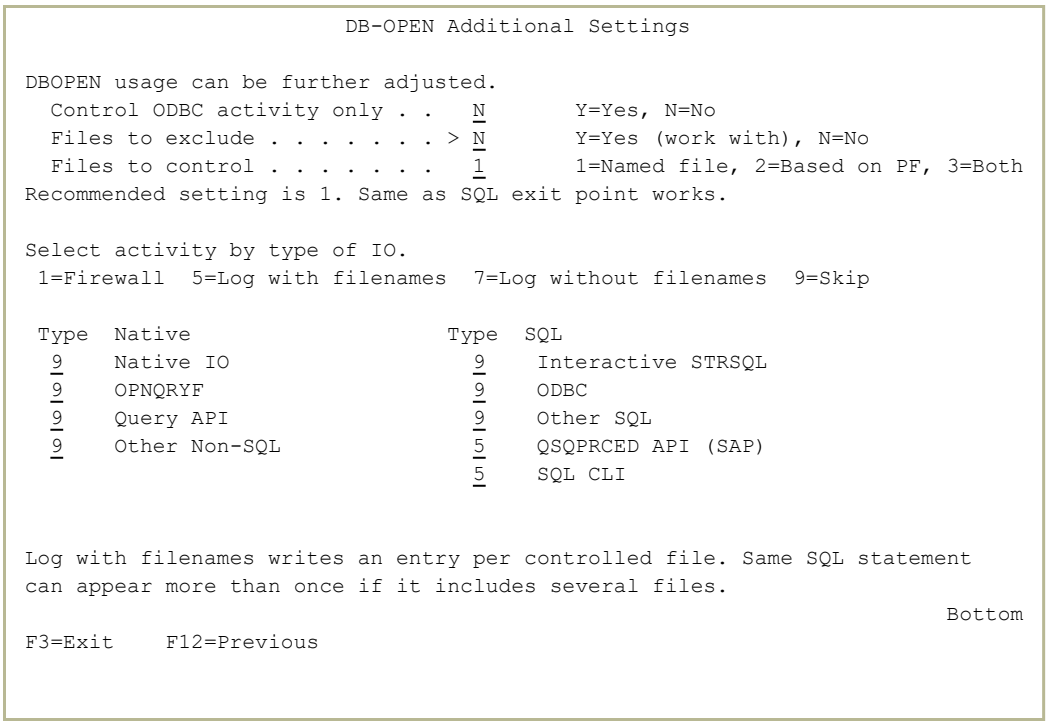
- **8=DBOPEN Pre-selected files & SQL**: (Recommended) Use both DBOPEN and SQL on accesses to files that you have specified via the Work with Object Auditing Plan screen (*STRFW* **> 4 > 51**) as shown in "Defining Files for Firewall to Track" on page 391. If you choose this option, Firewall does not track accesses via the SQL exit point, or to objects that have not been selected.
- **9=SQL**: Use the SQL server for all accesses. If you choose this option, Firewall does not track accesses via the DBOPEN server.

**If DBOPEN is active, SQL checks**

If you have chosen to activate Firewall for both DBOPEN and SQL in options **7** and **8** of **Control by Exit-Point**:

- **1=All types of operations**: Firewall checks both DBOPEN and SQL access for all operations.
- **2=Only functions that do not open any file: CREATE, ALTER, DROP, CALL...**: Firewall only checks the SQL server for accesses that are not available through DBOPEN, which do not open files.

To control further settings for DBOPEN, press the PageDown key. Additional fields appear:




### Control ODBC activity only

If set to **Y**, Firewall only examines file accesses via ODBC and skips examining accesses via other methods.

### Files to exclude

To keep Firewall from examining file accesses to certain files, set this field to **Y**. Press Enter to select the files from a list.

### Files to control

If opening a named View file, whether to check the View file or the physical file on which it is based. Options are:

- **1=Named file**: Check only the named View file.
- **2=Based on PF**: Check only the physical file.
- **3=Both**: Check both the View file and the physical file.

The screen lists several types of input and output access requests that Firewall can examine and log. Enter one of the following values in the **Type** field for each:

- **1=Firewall**: Firewall examines each access request.
- **5=Log with filenames**: Log each access, writing an entry for each file. If an SQL statement accesses multiple file, a separate line appears in the log for each file accessed.

- **7=Log without filenames**: Write a single record to the log for each statement, even if it accesses multiple files.
- **9=Skip**: Skip examining the access request.

## Setting Server Verbs to Skip

To **specify verbs or subcommands** that Firewall is to skip when checking activity on specific servers, select **`9. Server Verbs to Skip`** from the **Activation and Server Settings** screen (*STRFW* **`> 1`**). The **Skip Servers Subcommands** screen appears:


The screen is several pages long. The **`Verb`** column lists command verbs, collected under the servers to which they refer.

To set Firewall to **always skip the verb**, type **`Y`** in the **`Skip`** field to the left of the verb.

To set Firewall **not to skip the verb**, set the **`Skip`** field to blank.

# Setting Firewall Rules for IP Addresses or System Names

Firewall can filter incoming activity by the IP address, IPv6 address , or SNA system name at which it originates. It can filter outgoing activity by the IP address or IPv6 address to which it is sent.

You can examine and create these rules, and use the Rule Wizards to built new rules based on activity in your system's logs, from the **Work with Dynamic Filtering** screen (*STRFW* **> 2**).

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

IP Addresses                            Rule Wizards - Incoming IP
 1. Incoming IP Addresses/Local-jobs    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
```

To filter **incoming** activity by **IP addresses**, select **1. Incoming IP Addresses/Local-jobs**. The **Dynamic Filtering- Incoming IP Address Security** screen appears, as shown in "Setting Firewall Rules for Incoming Activity by IP Addresses" on page 156

To filter **incoming** activity by **IPv6 addresses**, select **2. Incoming IPv6 Addresses**. The **Dynamic Filtering- Incoming IPv6 Address Security** screen appears, as shown in "Setting Firewall Rules for Incoming Activity by IPv6 Addresses" on page 177.

To filter incoming activity by remote system names, select **11. Incoming Remote System Names**. The Dynamic Filtering- Incoming Remote System Name Security screen appears, as shown in "Setting Firewall Rules for Incoming Activity by Remote System Names" on page 183.

To filter outgoing activity by IP addresses, select **5. Incoming IP Addresses**. The Dynamic Filtering- Outgoing IP Address Security screen appears, as shown in "Setting Firewall Rules for Outgoing Activity by IP Address" on page 188.

To filter outgoing activity by IPv6 addresses, select **6. Incoming IPv6 Addresses**. The Dynamic Filtering- Outgoing IPv6 Address Security screen appears, as shown in "Setting Firewall Rules for Outgoing Activity by IPv6 Address" on page 206.

## Setting Firewall Rules for Incoming Activity by IP Addresses

You can **filter incoming activity** by IP address from the **Dynamic Filtering - Incoming IP Address Security** screen. To reach the screen, select **`1. Incoming IP Addresses/Local-jobs`** from the **`Work with Dynamic Filtering`** screen (*STRFW* **`> 2 > 1`**).

```
               Dynamic Filtering- Incoming IP Address Security

Type options, press Enter.
  1=Select  4=Delete                F  Te       R  D
                                    T  ln D TCP M  D Fil
Opt IP Address/*LCL  Subnet Mask    P  et B SGN T  M Srv Text
 _  *ALL             0.0.0.0        Y  Y  Y  Y           *ALL
 _  *LCL-*                          Y  Y  Y  Y  Y  Y  Y
 _  1.1.1.3          255.255.255.254
 _  1.1.1.69         255.255.255.255                  Y  RULE SET BY WIZARD
 _  1.1.1.71         255.255.255.255 Y  Y  Y  Y       Y  RULE SET BY WIZARD
 _  1.1.1.77         255.255.255.255 Y  Y     Y       Y  RULE SET BY WIZARD
 _  1.1.1.79         255.255.255.255 A  A  A  A  A  A     dev.razlee
 _  1.1.1.103        255.255.255.254
 _  1.1.1.105        255.255.255.255 Y  Y  Y  Y  Y  Y  Y  RULE SET BY WIZARD
 _  1.1.1.114        255.255.255.252             Y        test
 _  1.1.1.114        255.255.255.255 Y           Y        RULE SET BY WIZARD
 _  1.1.1.127        255.255.255.255    Y  Y  Y           RULE SET BY WIZARD
                                                                    More...
   FTP includes: FTPLOG, REXLOG
   DDM includes: DDM, DRDA
   DB Server includes: SQLENT, SQL, NDB, OBJINF, DBOPEN
F3=Exit   F6=Add new   F8=Print   F10=Logon security   F12=Cancel
```

The screen shows existing rules for filtering activity coming in via various protocols from specific IP addresses. The entry for **`*ALL`** shows general rules for incoming activity coming from IP addresses that are not listed. The entry for **`*LCL-*`** shows general rules for activity that originates within the same system.

Each of the other lines shows rules for ranges of IP addresses, shown by a specific IP address and Subnet Mask. The following columns show the rules for specific protocols, as shown by the vertical text at the top of each column:

- **`FTP`** including FTPLOG and REXLOG
- **`Telnet`**
- **`DB`** including SQLENT, SQL, NDB, OBJINF, and DBOPEN
- **`TCPSGN`**, the TCP Sign-On Server
- **`RMT`**, for Remote Program/Command Call

- **DDM** including DRDA
- **Fil Srv**, for File Server

For each protocol, the letter in that column shows how the rule handles incoming activity for that protocol from that IP address range:

- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

The final **Text** column shows a freeform text description of the rule.

To add a new rule, press the F6 key. The Dynamic Filtering- Add Incoming IPv6 Address screen appears, as shown in "Adding a Firewall Rule for Incoming Activity by IP Address" on the next page.

To modify an existing rule, type **1** in the **Opt** column for that rule. The Dynamic Filtering- Modify Incoming IP Address screen appears, as shown in "Modifying a Firewall Rule for Incoming Activity by IP Addresses" on page 160

To use the Rule Wizard to develop rules by analyzing your system's recent activity, see "Using the Rule Wizard for Incoming Activity by IP Address" on page 162.

## Adding a Firewall Rule for Incoming Activity by IP Address

To **add a rule for filtering activity by IP address**, press the **F6** key in the **Dynamic Filtering - Incoming IP Address Security** screen, shown in "Setting Firewall Rules for Incoming Activity by IP Addresses" on page 156 (***STRFW > 2 > 1***).

The **Dynamic Filtering - Add Incoming IP Address** screen appears:

```
                  Dynamic Filtering- Add Incoming IP Address

Type choices, press Enter.

IP Address/*LCL.   _______________                    IP, *ALL, *LCL-generic*
Subnet mask  . .   255.255.255.255                    F4 for list
Text . . . . . .   ________________________

                FTP/   Tel-  DB   TCP   Rmt       Fil
                REXEC  net   Srv  SGN   Srv  DDM  Srv
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 . .

SQL statments are not parsed when checks are skipped or rejected.
  FTP includes: FTPLOG, REXLOG
  DDM includes: DDM, DRDA
  DB Server includes: SQLENT, SQL, NDB, OBJINF, DBOPEN
F3=Exit   F4=Prompt   F10=Logon security   F12=Cancel
```

Enter or modify information in the following fields:

**IP Address/*LCL**

The IPv4 address for the address range. In addition to IP addresses, you can set this field to:

- ***ALL** for rules applied to all IP address ranges that aren't otherwise specified
- ***LCL-generic*** for local job or device names.

**Subnet mask**

The subnet mask for the address range. For a list of possible subnet masks, showing the number of addresses that the range would include, press the **F4** key.

**Text**

A free-form text description of the IP address range.

**Secure value**

A letter or blank space showing how the rule handles incoming activity for that address range for the protocol indicated by the label above the column. The protocols include:

- **FTP** including FTPLOG and REXLOG
- **Telnet**
- **DB** including SQLENT, SQL, NDB, OBJINF, and DBOPEN
- **TCPSGN**, the TCP Sign-On Server
- **RMT**, for Remote Program/Command Call
- **DDM** including DRDA
- **Fil Srv**, for File Server

The possible values are:

- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

In many situations, you can dramatically improve performance by using options **B** or **L**. For example, you might use them when an IP address that you know to be well secured and is using SSL, and which doesn't require checking the SQL statements, sends a high volume of requests.

The **Equivalent IP range** field shows a read-only value indicating the range of IP addresses included by the IP address and subnet mask.

## Modifying a Firewall Rule for Incoming Activity by IP Addresses

To **modify an existing rule** for filtering incoming activity by IP address, type **1** in the **Opt** field for that rule in the **Dynamic Filtering - Incoming IP Address Security** screen, shown in "Setting Firewall Rules for Incoming Activity by IP Addresses" on page 156 (***STRFW > 2 > 1***), and press **Enter**.

The **Dynamic Filtering - Modify Incoming IP Address** screen appears:

```
               Dynamic Filtering- Modify Outgoing IP Address

Type choices, press Enter.

IP Address  . . . . .   80.179.26.75                Address, *ALL
Subnet mask . . . . .   255.255.255.224            F4 for list
Text  . . . . . .       RLTOOLS

FTP . . . . . .         Y                          Y=Yes , S=SSL only,
                                                   A=Skip checks
                                                   B=SSL+Skip checks
                                                   L=Skip checks+Log
                                                   M=SSL+Skip checks+Log

Equivalent IP range .   80.179.26.64-80.179.26.95


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



F3=Exit   F4=Select Subnet    F12=Cancel
```

Enter or modify information in the following fields:

**IP Address/*LCL**

The IPv4 address for the address range. In addition to IP addresses, you can set this field to:

- ***ALL** for rules applied to all IP address ranges that aren't otherwise specified
- ***LCL-generic*** for local job or device names.

**Subnet mask**

The subnet mask for the address range. For a list of possible subnet masks, showing the number of addresses that the range would include, press the **F4** key.

**Text**

A free-form text description of the IP address range.

**Secure value**

A letter or blank space showing how the rule handles incoming activity for that address range for the protocol indicated by the label above the column. The protocols include:

- **FTP** including FTPLOG and REXLOG
- **Telnet**
- **DB** including SQLENT, SQL, NDB, OBJINF, and DBOPEN
- **TCPSGN**, the TCP Sign-On Server
- **RMT**, for Remote Program/Command Call
- **DDM** including DRDA
- **Fil Srv**, for File Server

The possible values are:

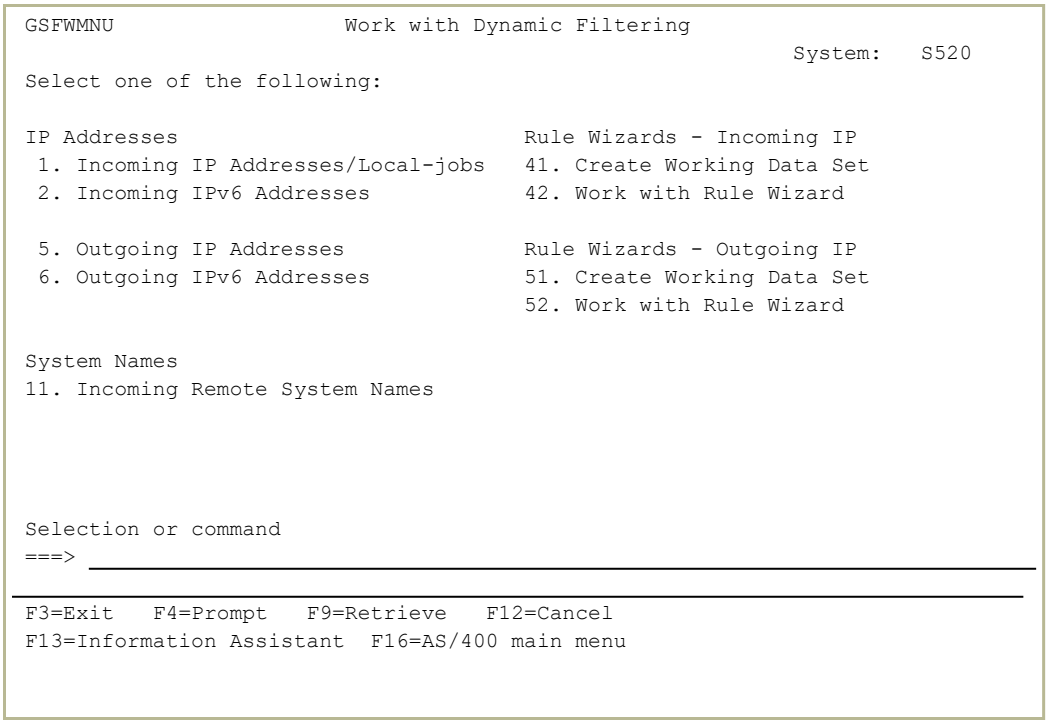
- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

In many situations, you can dramatically improve performance by using options **B** or **L**. For example, you might use them when an IP address that you know to be well secured and is using SSL, and which doesn't require checking the SQL statements, sends a high volume of requests.

The **Equivalent IP range** field shows a read-only value indicating the range of IP addresses included by the IP address and subnet mask.

## Using the Rule Wizard for Incoming Activity by IP Address

Using the Rule Wizard, you can analyze recent activity on your system and use that information to create and modify Firewall rules.



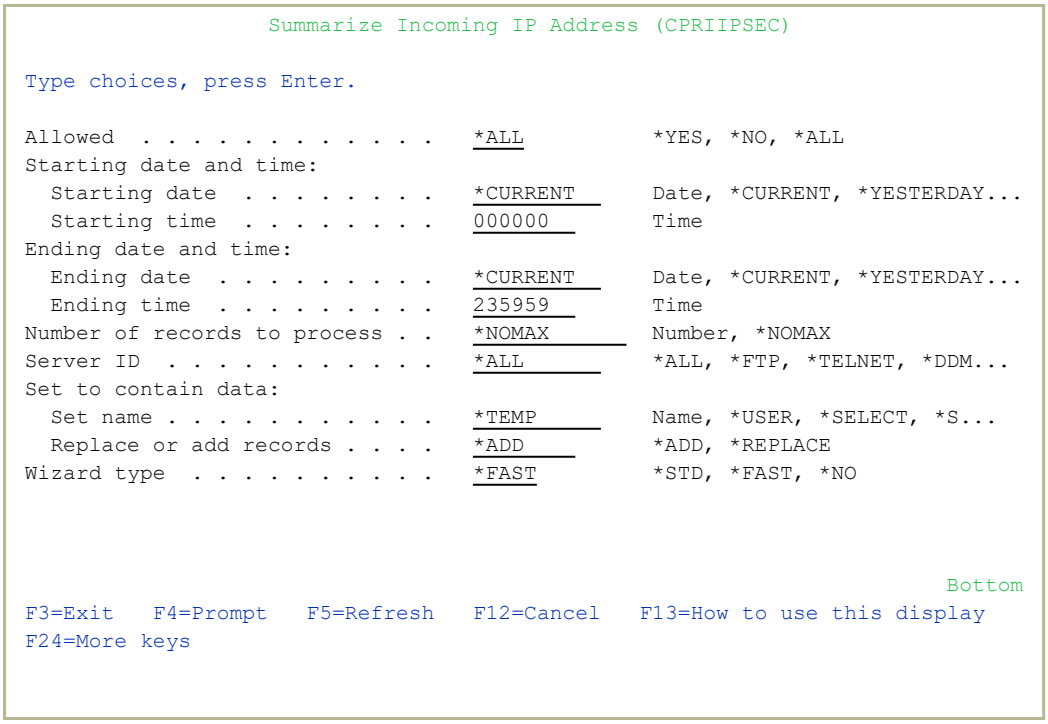

To create a data set for examining activity and developing rules for incoming activity based on IP address, select **41. Create Working Data Set** from the Work with Dynamic Filtering screen *(STRFW > 2*).
The Summarize Incoming IP Address (CPRIIPSEC) screen appears, as shown in "Creating a Data Set of Incoming Activity by IP Address with the Rule Wizard" on the facing page.

To use an existing data set to develop rules, select **42. Work with Rule Wizard** from the Work with Dynamic Filtering screen (*STRFW > 2*).
The Incoming IP Address Wizard (WZRIIPSEC) screen appears, as shown in "Analyzing Recent Data on Incoming Activity by IP Address with the Rule Wizard" on page 166.

## Creating a Data Set of Incoming Activity by IP Address with the Rule Wizard

To **create a data set** for examining activity and developing rules for incoming activity based on IP address, select **41. Create Working Data Set** from the **Work with Dynamic Filtering** screen *(STRFW* **> 2**).

The **Summarize Incoming IP Address (CPRIIPSEC)** screen appears. From this screen, you can construct the command line command that creates the data set.




The screen contains the following fields. Fields that have values other than the defaults are preceded by the "**>**" character:

**Allowed**

Specifies whether the data set includes rejected activity, accepted activity, or both.

- ***YES**: Include only accepted activity
- ***NO:** Include only rejected activity
- ***ALL:** Include both accepted and rejected activity

**Starting data and time**

**Starting date**

The day or date on which the included data begins.

Allowed values include:

- ***CURRENT**: The current date
- ***YESTERDAY**: Yesterday's date
- ***WEEKSTR**: The first day of the current week. By default, this is Sunday.
- ***PRVWEEKS**: The first day of the previous week
- ***MONTHSTR**: The first day of the current month
- ***PRVMONTHS**: The first day of the previous month
- ***YEARSTR**: The first day of the current year
- ***PRVYEARS**: The first day of the previous year
- ***MON**: Monday
- ***TUE**: Tuesday
- ***WED**: Wednesday
- ***THU**: Thursday
- ***FRI**: Friday
- ***SAT**: Saturday
- ***SUN**: Sunday

**Starting time**

The time on the Starting date at which the included data begins, in **HHMMSS** format.

**Ending date**

The day or date on which the included data ends.

Allowed values are the same as for **Starting date**.

**Ending time**

The time on the Starting date at which the included data ends, in **HHMMSS** format.

**Number of records to process**

Collect no more than this number of records. If set to ***NOMAX**, collect all the relevant records.

**Server ID**

The server that the activity is attempting to access. To see a list of possible values, press the F4 key.

**Set to contain data**

**Set name**

The name of the data set that will contain the records. You can set this to your own value or choose one of these options:

- ***TEMP**: The default name for temporary data sets. The data set is removed when the session ends.
- ***USER**: Your user name
- ***S**: Equivalent to ***SELECT**
- ***SELECT**: If the wizard has been run before, a list appears of previous names that had been used for the data set.

**Replace or add records**

If any records already exist in the data set, whether to replace them or add the new records to them.

Possible values include:

- ***ADD**: Add new records to the existing set
- ***REPLACE**: Replace all existing records with the new ones.

**Wizard type**

The type of wizard to be created. Possible values include:

- ***STD**: The Rule Wizard screen that appears next has all the standard options
- ***FAST**: The Rule Wizard screen that appears next has a limited set of options for faster processing, as documented there.
- ***NO**: The data set will only be used to batch processing.

To list and select possible values for many of the fields, place the cursor within the field and press the F4 key.

To reset the values on the screen to their default values, press the F5 key.

## Analyzing Recent Data on Incoming Activity by IP Address with the Rule Wizard

The Rule Wizards analyze data on recent system activity to develop and improve rules for filtering future activity.

To **develop rules to filter incoming activity** by IP Address, first create a data set of recent activity, as shown in "Creating a Data Set of Incoming Activity by IP Address with the Rule Wizard" on page 163.

Once you have created a data set, select **`42. Work with Rule Wizard`** from the **Work with Dynamic Filtering** screen (*STRFW* **`> 2`**).

The **Plan Incoming IP Security** screen appears:

```
                          Plan Incoming IP Security
 Type choices, press Enter.                              Subset . . _______________
  1=Statistics        2=Set by use  3=Allow by use
  4=Delete 5=DSPFWLOG               9=Add similar  C>R=Current to Revised
                                                   Y Allowed      Y=Allow
 Specify revised authority in the R column.        N Rejected     N=Reject
 Press Enter to apply revised authority.           Y Allowed (by generic* rule)
                                                   N Rejected (by generic* rule)
                   FTP/
                   RE-  Tel DB  TCP RMT DDM/ Fil Number of Logged Entries
                   EXEC net Srv SGN Srv DRDA Srv FTP/REX Telnet  ---DB--- File
Opt IP-Address     C>R  C>R C>R C>R C>R C>R  C>R TCPSGN  -RMT--  DDM/DRDA Srv
 _ 1.1.1.137       N _  N _ Y _ N _ N _ N _  N _                     24
 _ 1.1.1.139       Y _  S _ S _ Y _ N _ Y _  Y _                    218
                                                                          Bottom
 F3=Exit    F6=Add New    F8=Print    F11=Alt.view  F12=Cancel
```

Each line on the lower section of the screen shows activity from a single IP address, as shown in the **`IP-Address`** field.

The next set of fields appear in pairs. Each pair shows information on activity from one **protocol** or set of protocols, including:

- **FTP/REXEC** including FTPLOG and TEXLOG
- **Telnet**
- **DB Server** including SQLENT, SQL, NDB, OBJINF, and DBOPEN
- **TCP Sign-in**

- Remote Server
- DDM and DRDA
- File Server

The **pairs of fields** for each are:

- a **letter** on a colored background, showing how Firewall responded to the activity according to current rules
- an **underscore** in which you can revise the rule

The **letter codes** are:

- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

The **color codes** are:

- **Green**: A rule specifically referring to this IP address accepts this activity
- **Red**: A rule specifically referring to this IP address rejects this activity
- **Blue**: A rule for a generic set of IP addresses that includes this one accepts this activity
- **Purple**: A rule for a generic set of IP addresses that includes this one rejects this activity

Thus, for example, the leftmost item on the top line of the list is the letter "N" on a red background on the line with the IP address 1.1.1.69 in the FTP/REXEC column. That indicates that a rule specifically for the IP address 1.1.1.69 rejects all activity via FTP/REXEC ( including FTPLOG and TEXLOG).

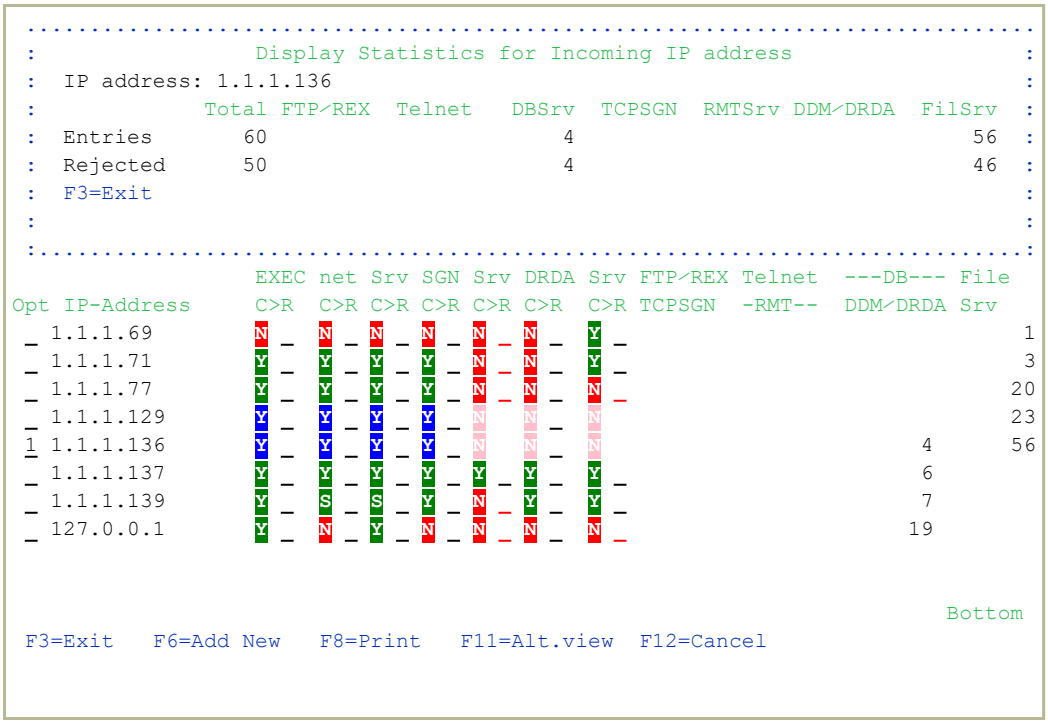
The remaining columns show the number of entries of logged activity within the selected data set from that IP address from several groups of protocols. The protocols are:

- FTP/REXEC and TCP sign-in
- Telnet and Remote Server

- Database Server including SQL access and DDM/DRDA
- File server

Thus, for example, in the fifth line of the list, the IP address 1.1.1.136 requested access to the database server four times and the file server 56 times.

To **view the statistics** on activity on a specific IP address during the time period in the data set, type **1** in the **Opt** column for that IP address and press **Enter**. The **Display Statistics for Incoming IP address** window appears.




In this example, we see that IP address 1.1.1.136 sent sixty requests for access: four to the database server and 56 to the file server. Fifty of them were rejected, including all four for the database server and 46 of the requests to the file server.

To **add** a new rule, press the **F6** key. The **Add Firewall Incoming IP Address** screen appears, as shown in "Adding Firewall Rules for Incoming Activity by IP Address with the Rule Wizard" on the facing page.

To add a rule for a IP address **similar** to an existing one, type **9** in the **Opt** field for that rule and press **Enter**. The **Add Similar Incoming IP Address** screen appears, as shown in "Adding Firewall Rules for a Similar Incoming IP Address with the Rule Wizard" on page 175.

To **change rules based on activity** in the data set, see "Setting Firewall Rules based on Incoming Activity by IP Address with the Rule Wizard" on the next page.

To **change rules manually**, see "Setting Firewall Rules Manually based on Incoming IP Address with the Rule Wizard" on page 173

To **delete** a rule, type **4** in the **Opt** field for that rule and press **Enter**.
NOTE: You are not prompted for confirmation, and the rule is immediately deleted.

To **display the firewall log** entries relevant to this rule, type **5** in the **Opt** field for that rule and press Enter. The **Display Firewall Log** screen appears, as shown in "Displaying Firewall Logs" on page 516.

To **print** the information from the data set, press the **F8** key.

## Adding Firewall Rules for Incoming Activity by IP Address with the Rule Wizard

To **add firewall rules** to filter incoming activity via the Rule Wizard, press the **F6** key from the **Plan Incoming IP Security** screen, shown in "Analyzing Recent Data on Incoming Activity by IP Address with the Rule Wizard" on page 166 (*STRFW* **> 2 > 42**).

The **Add Firewall Incoming IP Address** screen appears:

```
                    Add Firewall Incoming IP Address

Type choices, press Enter.

  IP Address  . . . . . .   _

Y=Yes, N=No, S=SSL only, A=Skip checks, B=SSL+Skip checks, L=Skip checks+Log,
M=SSL+Skip checks+Log
  FTP/REXEC . . . . . .   _              RMT Server . . . . . .    _

  Telnet  . . . . . .     _              DDM/DRDA . . . . . .      _

  DB Server . . . . . .   _              File Server  . . . . .    _

  TCP Signon  . . . . . .   _




F3=Exit    F12=Cancel
```

Enter the IP address to which the new rule will apply in the **IP Address** field.

The screen contains fields for codes that control how Firewall reacts to requests to access servers. The server types are:

- FTP/REXEC including FTPLOG and TEXLOG
- Telnet
- DB Server including SQLENT, SQL, NDB, OBJINF, and DBOPEN
- TCP Sign-in
- Remote Server
- DDM and DRDA
- File Server

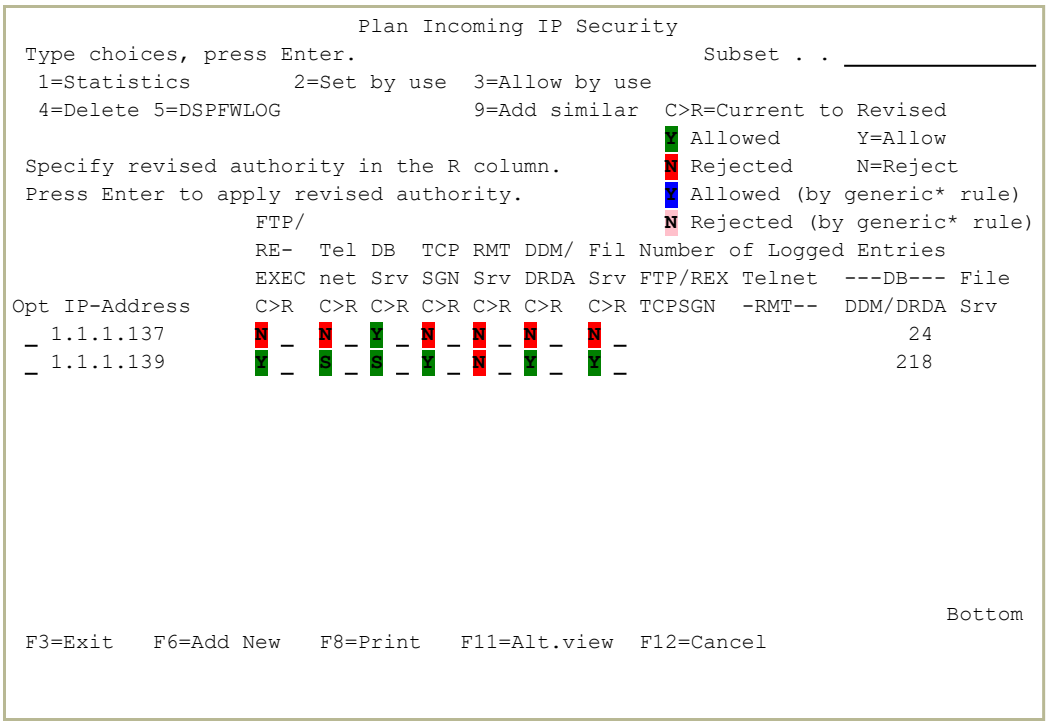
For each server type, enter a letter corresponding to how Firewall is to react to requests to access it. The letters are:

- **Y**: Accepted
- **N**: Rejected
- **S**: Only accepted over SSL connections
- **A**: Accepted, without checking whether SQL statements are valid
- **B**: Only accepted over SSL connections, without checking whether SQL statements are valid
- **L**: Accepted, without either checking whether SQL statements are valid or logging the activity
- **M**: Only accepted over SSL connections, without either checking whether SQL statements are valid or logging the activity.

If you do not enter a letter for a server, requests to access it are handled according to the next highest generic rule that applies to it, up through the rule (if any) for ***ALL**.

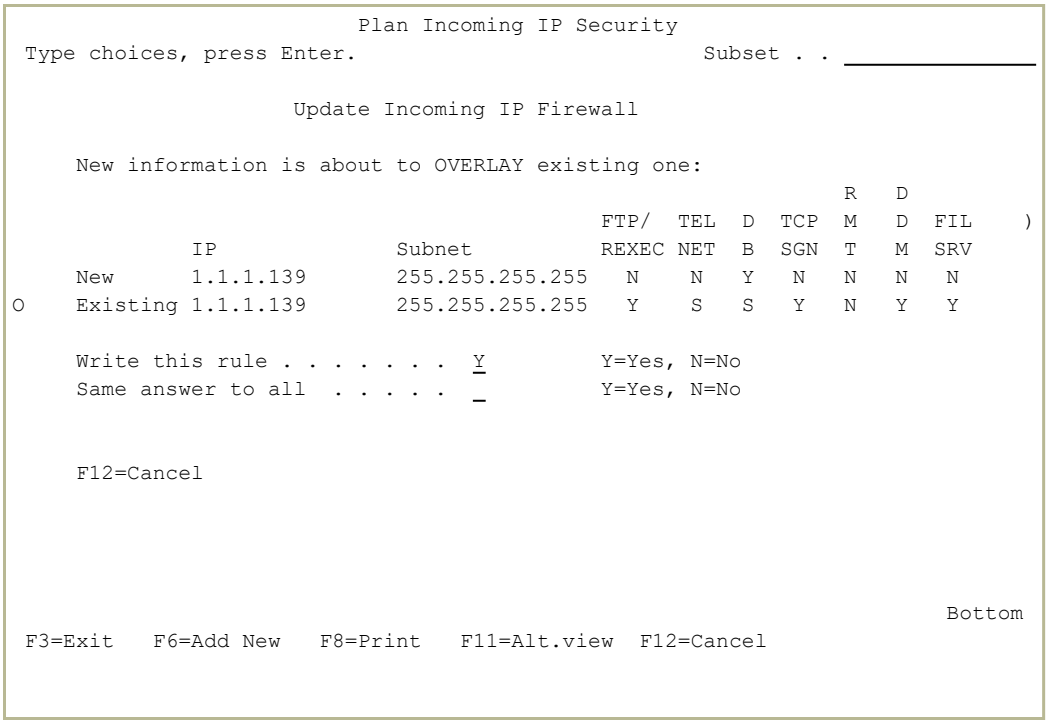
## Setting Firewall Rules based on Incoming Activity by IP Address with the Rule Wizard

To set rules based on the incoming activity analyzed for the Rule Wizard, open the Plan Incoming IP Security screen, as shown in "Analyzing Recent Data on Incoming Activity by IP Address with the Rule Wizard" on page 166 (*STRFW* > 2 > 42).




To set new rules corresponding to **activity seen for the IP Address**, enter **2** in the **Opt** field for that address.

The **Update Incoming IP Firewall** window appears:



In this case, the only activity from IP address 1.1.1.77 requested access to the file server. Therefore, the new rule would allow access to the file server and block access to all the others.

To set new rules corresponding to **how activity differed from the existing rules**, enter **3** in the **Opt** field for that address.

The **Update Incoming IP Firewall** window appears:

```
                          Plan Incoming IP Security
 Type choices, press Enter.                          Subset . . _______________

                      Update Incoming IP Firewall

     New information is about to OVERLAY existing one:
                                                                 R   D
                                            FTP/  TEL  D  TCP  M   D  FIL    )
              IP              Subnet        REXEC NET  B  SGN  T   M  SRV
     New      1.1.1.139       255.255.255.255  Y    S   Y   Y   N   Y   Y
O    Existing 1.1.1.139       255.255.255.255  Y    S   S   Y   N   Y   Y

     Write this rule . . . . . . . Y         Y=Yes, N=No
     Same answer to all  . . . . . _         Y=Yes, N=No


     F12=Cancel




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

Since the only difference between the existing rules and the actual activity for IP address 1.1.1.77 was that access was requested for the file server, which would previously have been rejected, the setting for that server would be changed from **N** to **Y**.

To **save** changes and exit this window, press **Enter**. The Rules Wizard saves the rule being changed and removes the line for that IP Address from the screen. You can see the resulting rule on the **Dynamic Filtering-Incoming IP Address Security** screen, as shown in "Setting Firewall Rules for Incoming Activity by IP Addresses" on page 156 (*STRFW*>**2 > 1**).

To **exit** this window without saving changes, press the **F12** key. The window closes. The changes that would have been made are marked in the columns for those servers in the lines for those IP addresses on the screen. You can then further work with the rules and save them manually, as shown in "Analyzing Recent Data on Incoming Activity by IP Address with the Rule Wizard" on page 166.

## Setting Firewall Rules Manually based on Incoming IP Address with the Rule Wizard

You can only set Firewall rules manually with the rule wizard if you have set the **`Wizard type`** to **`*STD`** when opening the wizard.

To **set rules manually** based on the incoming IP address of the activity in the Rule Wizard, open the **Plan Incoming IP Security** screen, as shown in "Analyzing Recent Data on Incoming Activity by IP Address with the Rule Wizard" on page 166 (***STRFW > 2 > 42***).

```
                          Plan Incoming IP Security
 Type choices, press Enter.                              Subset . . _______________
  1=Statistics        2=Set by use  3=Allow by use
  4=Delete 5=DSPFWLOG               9=Add similar  C>R=Current to Revised
                                                    Y Allowed      Y=Allow
 Specify revised authority in the R column.         N Rejected     N=Reject
 Press Enter to apply revised authority.            Y Allowed (by generic* rule)
                   FTP/                             N Rejected (by generic* rule)
                   RE-  Tel DB  TCP RMT DDM/ Fil Number of Logged Entries
                   EXEC net Srv SGN Srv DRDA Srv FTP/REX Telnet  ---DB--- File
Opt IP-Address     C>R  C>R C>R C>R C>R C>R  C>R TCPSGN  -RMT--  DDM/DRDA Srv
 _ 1.1.1.137       N _  N _ Y _ N _ N _ N _  N _                      24
 _ 1.1.1.139       Y _  S _ S _ Y _ N _ Y _  Y _                     218
                                                                    Bottom
 F3=Exit    F6=Add New    F8=Print    F11=Alt.view  F12=Cancel
```

To **set whether activity for a server from a given IP address is accepted**, enter the letter for the new setting in the column for the relevant server and the row for that IP address. The possible letters are:

- **Y**: Accepted
- **N**: Rejected
- **S**: Only accepted over SSL connections
- **A**: Accepted, without checking whether SQL statements are valid
- **B**: Only accepted over SSL connections, without checking whether SQL statements are valid
- **L**: Accepted, without either checking whether SQL statements are valid or logging the activity
- **M**: Only accepted over SSL connections, without either checking whether SQL statements are valid or logging the activity.

When you have entered all the changes, enter **6** in the **Opt** field for that IP address. The Update Outgoing IP Firewall window appears:

```
                          Plan Incoming IP Security
 Type choices, press Enter.                          Subset . . _______________

                     Update Incoming IP Firewall

     New information is about to OVERLAY existing one:
                                                                R   D
                                             FTP/  TEL  D  TCP  M   D  FIL    )
              IP              Subnet          REXEC NET  B  SGN  T   M  SRV
     New      1.1.1.139       255.255.255.255   N    N   Y   N   N   N   N
O    Existing 1.1.1.139       255.255.255.255   Y    S   S   Y   N   Y   Y

     Write this rule . . . . . . . . Y         Y=Yes, N=No
     Same answer to all  . . . . . . _         Y=Yes, N=No


     F12=Cancel




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

In this case, the only change that had been made was to change the letter for the **FTP/REXEC** server from **N** to **Y**. That item in the rule is changed. The rest of it remains the same.

To **save** changes and exit this window, press **Enter**. The Rules Wizard saves the rule being changed and removes the line for that IP Address from the screen. You can see the resulting rule on the **Dynamic Filtering-Outgoing IP Address Security** screen, as shown in "Setting Firewall Rules for Outgoing Activity by IP Address" on page 188 (*STRFW*>**2 > 1**).

To **exit** this window without saving changes, press the **F12** key. The window closes. The changes that would have been made are marked in the columns for those servers in the lines for those IP addresses on the screen. You can then further work with the rules and save them manually.

## Adding Firewall Rules for a Similar Incoming IP Address with the Rule Wizard

To **add firewall rules** for an incoming IP address similar to an existing one via the Rule Wizard, enter **9** in the **Opt** field for the original IP address from the **Plan Incoming IP Security** screen, shown in "Analyzing Recent Data on Incoming Activity by IP Address with the Rule Wizard" on page 166 (*STRFW* **> 2 > 42**).

The **Add Similar Incoming IP Address** screen appears:

```
                      Add Similar Incoming IP Address

Modify data in field New IP Address.
Modify data in field New Revised authority (optionally).
  New IP Address  . . . . .    1.1.1.139

  New Revised authority:
Y=Yes, N=No, S=SSL only, A=Skip checks, B=SSL+Skip checks, L=Skip checks+Log,
M=SSL+Skip checks+Log
    FTP/REXEC . . . . . .    N           RMT Server . . . . . .     _

    Telnet  . . . . . .      _           DDM/DRDA . . . . . .       _

    DB Server . . . . . .    _           File Server  . . . . .     Y

    TCP Signon  . . . . . .  _




F3=Exit   F12=Cancel
```

The original IP address appears in the **New IP Address** field. Change it to the IP address to which the new rule will apply.

The screen contains fields for codes that control how Firewall reacts to requests to access servers. The fields have entries if the setting for that server type had been changed during the current session for the original IP address.

The server types are:

- FTP/REXEC including FTPLOG and TEXLOG
- Telnet
- DB Server including SQLENT, SQL, NDB, OBJINF, and DBOPEN
- TCP Sign-in
- Remote Server
- DDM and DRDA
- File Server

For each server type, enter a letter or change the existing letter to one corresponding to how Firewall is to react to requests to access it. The letters are:

- **Y**: Accepted
- **N**: Rejected
- **S**: Only accepted over SSL connections
- **A**: Accepted, without checking whether SQL statements are valid
- **B**: Only accepted over SSL connections, without checking whether SQL statements are valid
- **L**: Accepted, without either checking whether SQL statements are valid or logging the activity
- **M**: Only accepted over SSL connections, without either checking whether SQL statements are valid or logging the activity.

If you do not enter a letter for a server or remove an existing letter without replacing it, requests to access it are handled according to the next highest generic rule that applies to it, up through the rule (if any) for ***ALL**.

## Setting Firewall Rules for Incoming Activity by IPv6 Addresses

You can **filter incoming activity by IPv6 address** from the **Dynamic Filtering - Incoming IPv6 Address Security** screen. To reach the screen, select **2. Incoming IPv6 Addresses** from the **Work with Dynamic Filtering** screen(*STRFW* **> 2 > 2**).

The **Dynamic Filtering - Incoming IPv6 Address Security** screen appears.

```
              Dynamic Filtering- Incoming IPv6 Address Security

 Type options, press Enter.                              T   T     F
   1=Select  4=Delete                                    E   C     I
                                                         L   P     L
                                                       F N   S R D S
                                                  Prfx T E D G M D R
Opt IPv6 Address                                  Lngh P T B N T M V Text
 _ *ALL                                                               *ALL
 _ 2001:CF8:2:5D11:3440:B5FF:FE8D:1                128 Y Y   Y Y Y Y


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

The screen shows existing rules for filtering activity coming in via various protocols from specific IPv6 addresses. The entry for ***ALL** shows general rules for incoming activity coming from IPv6 addresses that are not listed.

Each of the other lines shows rules for ranges of IP addresses, shown by a specific IPv6 address and address prefix length. The following columns show the rules for specific protocols, as shown by the vertical text at the top of each column:

- **FTP** including FTPLOG and REXLOG
- **Telnet**
- **DB** including SQLENT, SQL, NDB, OBJINF, and DBOPEN
- **TCPSGN**, the TCP Sign-On Server
- **RMT**, for Remote Program/Command Call

- **DDM** including DRDA
- **Fil Srv**, for File Server

For each protocol, the letter in that column shows how the rule handles incoming activity for that protocol from that IP address range:

- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

The final **Text** column shows a freeform text description of the rule.

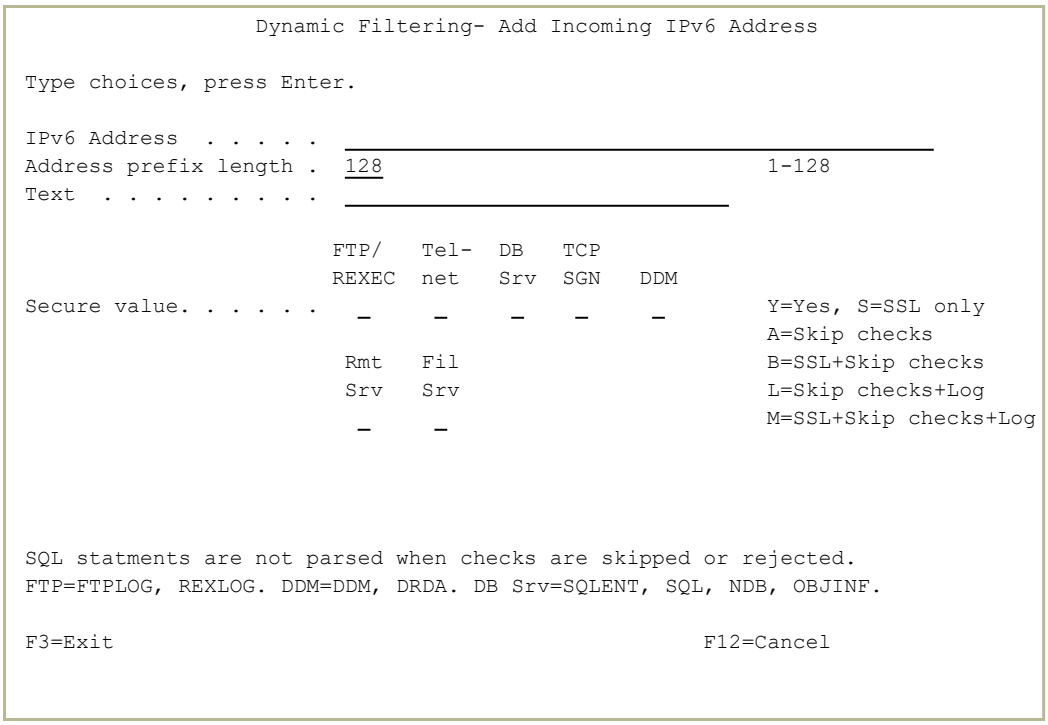
To modify an existing rule, enter **1** in the **Opt** column for that rule. The Dynamic Filtering- Modify Incoming IPv6 Address screen appears, as shown in "Modifying a Firewall Rule for Incoming Activity by IPv6 Addresses" on page 180

To add a new rule, press the F6 key. The Dynamic Filtering- Add Incoming IP Address screen appears, as shown in "Adding a Firewall Rule for Incoming Activity by IP Address" on page 158.

## Adding a Firewall Rule for Incoming Activity by IPv6 Address

To add a rule for filtering activity by a range of IPv6 addresses, press the F6 key in the Dynamic Filtering - Incoming IPv6 Address Security screen, shown in "Setting Firewall Rules for Incoming Activity by IPv6 Addresses" on the previous page (*STRFW > 2 > 2*).

The Dynamic Filtering - Add Incoming IP Address screen appears:




Enter or modify information in the following fields:

**IPv6 Address**

The IPv6 address for the range of addresses. In addition to an IPv6 address, you can set this field to ***ALL** for rules applied to all IPv6 ranges that aren't otherwise specified.

**Address prefix length**

The length of the IPv6 address prefix. This can be set to from 1-128.

**Text**

A free-form text description of the IPv6 address range.

**Secure value**

A letter or blank space showing how the rule handles incoming activity for that address range for the protocol indicated by the label above the column. The protocols include:

- **FTP/REXLOG** including FTPLOG and REXLOG
- **TELNET** for TELNET connections
- **DB Srv** including SQLENT, SQL, NDB, and OBJINF.
- **TCP SGN**, the TCP Sign-On Server

- **DDM** including DRDA
- **Rmt Srv**, for Remote Program/Command Call
- **Fil Srv**, for File Server

The possible values are:

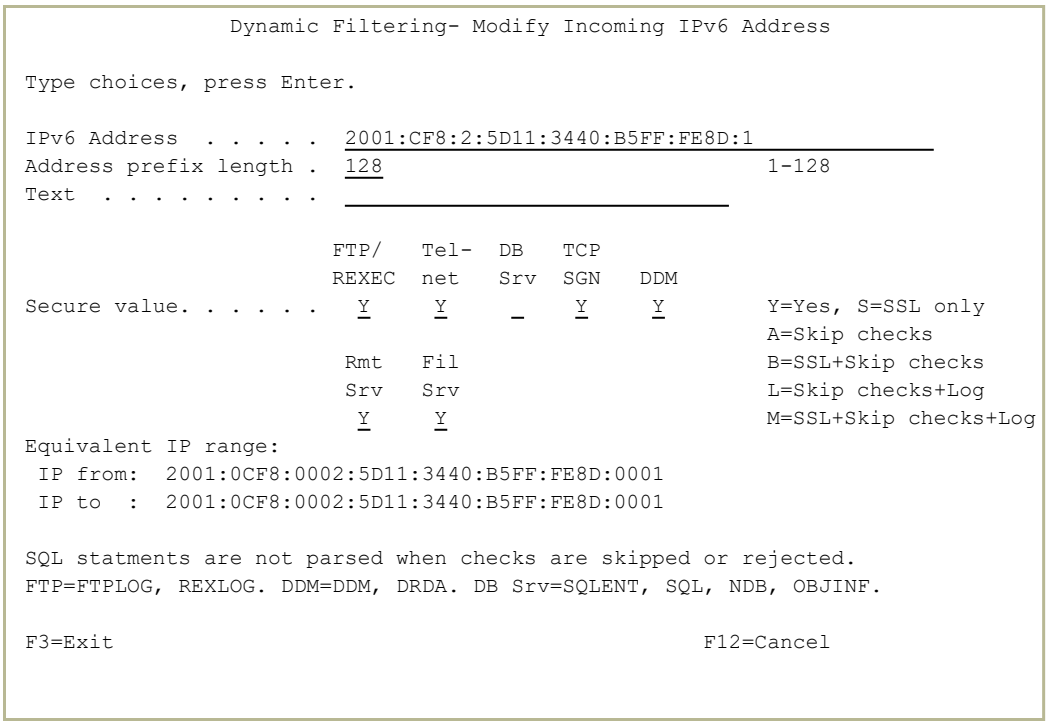
- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

In many situations, you can dramatically improve performance by using options **B** or **L**. For example, you might use them when an IP address that you know to be well secured and is using SSL, and which doesn't require checking the SQL statements, sends a high volume of requests.

## Modifying a Firewall Rule for Incoming Activity by IPv6 Addresses

To modify an existing rule for filtering incoming activity by IPv6 address, enter **1** in the **Opt** field for the rule in the Dynamic Filtering - Incoming IPv6 Address Security screen, shown in "Setting Firewall Rules for Incoming Activity by IPv6 Addresses" on page 177 (*STRFW > 2 > 2*).

The Dynamic Filtering - Modify Incoming IPv6 Address screen appears:




Enter or modify information in the following fields:

**IPv6 Address**

The IPv6 address for the range of addresses. In addition to an IPv6 address, you can set this field to ***ALL** for rules applied to all IPv6 ranges that aren't otherwise specified.

**Address prefix length**

The length of the IPv6 address prefix. This can be set to from 1-128.

**Text**

A free-form text description of the IPv6 address range.

**Secure value**

A letter or blank space showing how the rule handles incoming activity for that address range for the protocol indicated by the label above the column. The protocols include:

- **FTP/REXLOG** including FTPLOG and REXLOG
- **TELNET** for TELNET connections
- **DB Srv** including SQLENT, SQL, NDB, and OBJINF.
- **TCP SGN**, the TCP Sign-On Server

- **DDM** including DRDA
- **Rmt Srv**, for Remote Program/Command Call
- **Fil Srv**, for File Server

The possible values are:

- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

In many situations, you can dramatically improve performance by using options **B** or **L**. For example, you might use them when an IP address that you know to be well secured and is using SSL, and which doesn't require checking the SQL statements, sends a high volume of requests.

## Setting Firewall Rules for Incoming Activity by Remote System Names

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 DDM, DRDA, or Passthrough servers.

You can **filter this activity** from the **Dynamic Filtering - Incoming Remote System Names Security** screen. To reach the screen, select **`11. Incoming Remote System Names`** from the **`Work with Dynamic Filtering`** screen(*STRFW* **`> 2 > 11`**).

The **`Dynamic Filtering - Incoming Remote System Names Security`** screen appears:

```
            Dynamic Filtering- Incoming Remote System Names Security

 Type options, press Enter.
   1=Select  4=Delete
                       PASS-
Opt System*  DDM DRDA THROUGH Text
 _  *ALL      Y
 _  CENTR*                   Central system
 _  EXTERN01  Y   Y          External System 1
 _  EXTERN02             Y   External System 2

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

The screen shows existing rules for filtering activity coming in via various protocols from specific SNA system names. The entry for **`*ALL`** shows general rules for incoming activity coming from system names that are not listed.

Each of the other lines shows rules for specific system names, shown in the **`System*`** column. The following columns show the rules for access via the

**DDM**, **DRDA**, and **PASSTHROUGH** protocols, as shown by the vertical text at the top of each column.

For each protocol, the letter in that column shows how the rule handles incoming activity for that protocol from that system name:

- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

The final **Text** column shows a freeform text description of the rule.

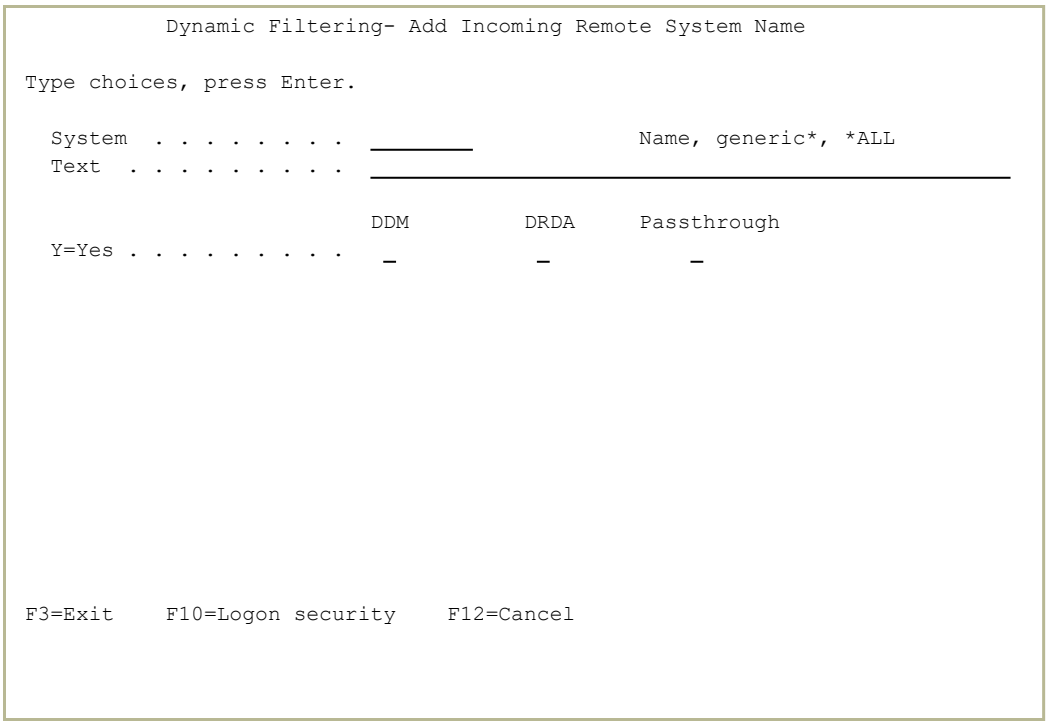
To modify an existing rule, enter **1** in the **Opt** column for that rule.

To add a new rule, press the **F6** key.

## Adding a Firewall Rule for Incoming Activity by Remote System Names

To add a rule for filtering activity by remote system names, press the F6 key in the Dynamic Filtering - Incoming Remote System Names Security screen, shown in "Setting Firewall Rules for Incoming Activity by Remote System Names" on the previous page (*STRFW > 2 > 11*).

The Dynamic Filtering - Incoming Remote System Names Security screen appears:




Enter or modify information in the following fields:

**System**

An SNA system name affected by the rule. This can be a single system name or a generic name ending with an asterisk. If set to ***ALL**, the rule is for all system names not otherwise specified.

**Text**

A free-form text description of the system.

**DDM**

If set to **Y**, Firewall accepts incoming activity via the DDM protocol from that system. If left blank, the activity is rejected.

**DRDA**

If set to **Y**, Firewall accepts incoming activity via the DRDA protocol from that system. If left blank, the activity is rejected.

**Passthrough**

If set to **Y**, Firewall accepts incoming activity via the Passthrough protocol from that system. If left blank, the activity is rejected.

## Modifying a Firewall Rule for Incoming Activity by Remote System Names

To modify an existing rule for filtering incoming activity by remote system name, type **1** in the **Opt** field for that rule in the **Dynamic Filtering - Incoming Remote System Names Security** screen, shown in "Setting Firewall Rules for Incoming Activity by Remote System Names" on page 183 (*STRFW > 2 > 11*), and press **Enter**.

The **Dynamic Filtering - Modify Incoming Remote System Name** screen appears:

```
           Dynamic Filtering- Modify Incoming Remote System Name

Type choices, press Enter.

  System  . . . . . .  *ALL____            Name, generic*, *ALL
  Text  . . . . . .  _

                         DDM         DRDA     Passthrough
  Y=Yes . . . . . .  .   Y           _           _









F3=Exit    F10=Logon security    F12=Cancel
```

Enter or modify information in the following fields:

**System**

An SNA system name affected by the rule. This can be a single system name or a generic name ending with an asterisk. If set to ***ALL**, the rule is for all system names not otherwise specified.

**Text**

A free-form text description of the system.

**DDM**

If set to **Y**, Firewall accepts incoming activity via the DDM protocol from that system. If left blank, the activity is rejected.

**DRDA**

If set to **Y**, Firewall accepts incoming activity via the DRDA protocol from that system. If left blank, the activity is rejected.

**Passthrough**

If set to **Y**, Firewall accepts incoming activity via the Passthrough protocol from that system. If left blank, the activity is rejected.

## Setting Firewall Rules for Outgoing Activity by IP Address

You can filter outgoing activity by IP address from the **Dynamic Filtering - Outgoing IP Address Security** screen. To reach the screen, select **5. Outgoing IP Addresses** from the **Work with Dynamic Filtering** screen (*STRFW* **> 2 > 5**).

```
                Dynamic Filtering- Outgoing IP Address Security

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

Opt IP Address       Subnet Mask     FTP Text
 _  *ALL             0.0.0.0             *ALL
 _  1.1.1.1          255.255.0.0      Y
 _  1.1.1.29         255.255.255.255  Y  fsdf
 _  1.1.1.156        255.255.255.255     RULE SET BY WIZARD
 _  1.1.1.168        255.255.255.255  Y
 _  1.1.1.212        255.255.255.255  Y  RLTOOLS
 _  178.249.3.48     255.255.255.255     RULE SET BY WIZARD
 _  185.113.4.132    255.255.255.255  Y
 _  185.113.4.146    255.255.255.255  Y  RULE SET BY WIZARD
 _  185.113.4.148    255.255.255.255  Y  RULE SET BY WIZARD




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

The screen shows existing rules for filtering activity going out via FTP to specific IP address ranges, as shown by their **IP Address** and **Subnet Mask**. The entry for ***ALL** shows general rules for activity coming going out to IP addresses that are not specifically listed.

The FTP column either is blank or shows a letter indication how Firewall is to filter FTP requests going to that IP Address Range.

- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements

- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

The final **Text** column shows a freeform text description of the rule.

To modify an existing rule, type **1** in the **Opt** column for that rule and press Enter.

To add a new rule, press the **F6** key.

## Adding a Firewall Rule for Outgoing Activity by IP Address

To add a rule for filtering outgoing activity by IP address, press the F6 key in the Dynamic Filtering - Outgoing IP Address Security screen, shown in "Setting Firewall Rules for Outgoing Activity by IP Address" on the previous page (*STRFW > 2 > 5*).

The Dynamic Filtering - Add Outgoing IP Address screen appears:

```
                  Dynamic Filtering- Add Outgoing IP Address

Type choices, press Enter.

IP Address  . . . . .   _____________                Address, *ALL
Subnet mask . . . . .   255.255.255.255              F4 for list
Text  . . . . . . . .   ____________________________

FTP . . . . . . . . .   _                            Y=Yes , S=SSL only,
                                                     A=Skip checks
                                                     B=SSL+Skip checks
                                                     L=Skip checks+Log
                                                     M=SSL+Skip checks+Log




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



F3=Exit   F4=Select Subnet    F12=Cancel
```

Enter or modify information in the following fields:

**IP Address/*LCL**

The IPv4 address for the address range. In addition to IP addresses, you can set this field to ***ALL** for rules applied to all IP address ranges that aren't otherwise specified.

**Subnet mask**

The subnet mask for the address range. For a list of possible subnet masks, showing the number of addresses that the range would include, press the F4 key.

**Text**

A free-form text description of the IP address range.

**FTP**

A letter or blank space showing how the system filters outgoing FTP requests:

The possible values are:

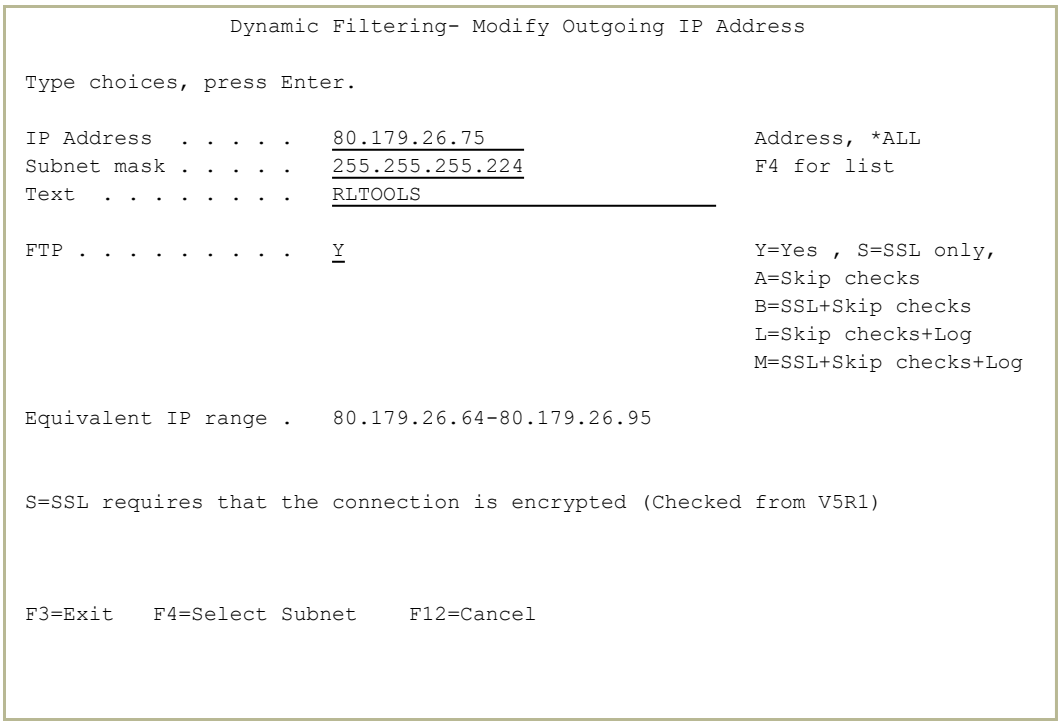
- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

To use options **B**, **M**, and **S**, which use SSL, the connection must be encrypted.

## Modifying a Firewall Rule for Outgoing Activity by IP Address

To modify an existing rule for filtering outgoing activity by IP address, type **1** in the **Opt** field for that rule in the Dynamic Filtering - Outgoing IP Address Security screen, shown in "Setting Firewall Rules for Outgoing Activity by IP Address" on page 188 (*STRFW > 2 > 5*), and press Enter.

The Dynamic Filtering - Modify Outgoing IP Address screen appears:




Enter or modify information in the following fields:

**IP Address/*LCL**

The IPv4 address for the address range. In addition to IP addresses, you can set this field to ***ALL** for rules applied to all IP address ranges that aren't otherwise specified.

**Subnet mask**

The subnet mask for the address range. For a list of possible subnet masks, showing the number of addresses that the range would include, press the **F4** key.

**Text**

A free-form text description of the IP address range.

**FTP**

A letter or blank space showing how the system filters outgoing FTP requests:

The possible values are:

- Blank: Reject all incoming activity
- **A**: Allow activity without checking

- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

To use options **B**, **M**, and **S**, which use SSL, the connection must be encrypted.

The **Equivalent IP range** field shows a read-only value indicating the range of IP addresses included by the IP address and subnet mask.

## Using the Rule Wizard for Outgoing Activity by IP Address

Using the Rule Wizard, you can analyze recent activity on your system and use that information to create and modify Firewall rules.

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

IP Addresses                           Rule Wizards - Incoming IP
 1. Incoming IP Addresses/Local-jobs   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
```

To **create a data set** for examining activity and developing rules for outgoing activity based on IP address, select **51. Create Working Data Set** from the **Work with Dynamic Filtering** screen *(STRFW > 2*).
The **Summarize Outgoing IP Address (CPROIPSEC)** screen appears, as shown in "Creating a Data Set of Outgoing Activity by IP Address with the Rule Wizard" on page 212.

To **use an existing data set** to develop rules, select **52. Work with Rule Wizard** from the **Work with Dynamic Filtering** screen (*STRFW > 2*).
The **Outgoing IP Address Wizard (WZROIPSEC)** screen appears, as shown in "Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard" on page 215.

## Creating a Data Set of Outgoing Activity by IP Address with the Rule Wizard

To **create a data set** for examining activity and developing rules for outgoing activity based on IP address, select **51. Create Working Data Set** from the **Work with Dynamic Filtering** screen *(STRFW > 2*).

The **Summarize Outgoing IP Address (CPROIPSEC)** screen appears. From this screen, you can construct the command line command that creates the data set.

```
                  Summarize Outgoing IP Address (CPROIPSEC)

Type choices, press Enter.

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




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

The screen contains the following fields. Fields that have values other than the defaults are preceded by the "**>**" character:

**Allowed**

Specifies whether the data set includes rejected activity, accepted activity, or both.

- ***YES**: Include only accepted activity
- ***NO:** Include only rejected activity
- ***ALL:** Include both accepted and rejected activity

**Starting data and time**

**Starting date**

The day or date on which the included data begins.

Allowed values include:

- ***CURRENT**: The current date
- ***YESTERDAY**: Yesterday's date
- ***WEEKSTR**: The first day of the current week. By default, this is Sunday.
- ***PRVWEEKS**: The first day of the previous week
- ***MONTHSTR**: The first day of the current month
- ***PRVMONTHS**: The first day of the previous month
- ***YEARSTR**: The first day of the current year
- ***PRVYEARS**: The first day of the previous year
- ***MON**: Monday
- ***TUE**: Tuesday
- ***WED**: Wednesday
- ***THU**: Thursday
- ***FRI**: Friday
- ***SAT**: Saturday
- ***SUN**: Sunday

**Starting time**

The time on the Starting date at which the included data begins, in **HHMMSS** format.

**Ending date**

The day or date on which the included data ends.

Allowed values are the same as for **Starting date**.

**Ending time**

The time on the Starting date at which the included data ends, in **HHMMSS** format.

**Number of records to process**

Collect no more than this number of records. If set to ***NOMAX**, collect all the relevant records.

**Server ID**

The server that the activity is attempting to access. To see a list of possible values, press the F4 key.

**Set to contain data**

**Set name**

The name of the data set that will contain the records. You can set this to your own value or choose one of these options:

- ***TEMP**: The default name for temporary data sets. The data set is removed when the session ends.
- ***USER**: Your user name
- ***S**: Equivalent to ***SELECT**
- ***SELECT**: If the wizard has been run before, a list appears of previous names that had been used for the data set.

**Replace or add records**

If any records already exist in the data set, whether to replace them or add the new records to them.

Possible values include:

- ***ADD**: Add new records to the existing set
- ***REPLACE**: Replace all existing records with the new ones.

**Wizard type**

The type of wizard to be created. Possible values include:

- ***STD**: The Rule Wizard screen that appears next has all the standard options

- ***FAST**: The Rule Wizard screen that appears next has a limited set of options for faster processing, as documented there.
- ***NO**: The data set will only be used to batch processing.

To **list and select** possible values for many of the fields, place the cursor within the field and press the **F4** key.

To **reset** the values on the screen to their default values, press the **F5** key.

## Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard

The Rule Wizards analyze data on recent system activity to develop and improve rules for filtering future activity.

To develop rules to filter incoming activity by IP Address, first create a data set of recent activity, as shown in "Creating a Data Set of Outgoing Activity by IP Address with the Rule Wizard" on page 212.

Once you have created a data set, select **52. Work with Rule Wizard** from the **Work with Dynamic Filtering** screen (*STRFW* **> 2**).

The **Plan Outgoing IP Security** screen appears:

```
                          Plan Outgoing IP Security
 Type choices, press Enter.                              Subset . . _______________
  1=Statistics        2=Set by use  3=Allow by use
  4=Delete 5=DSPFWLOG 6=Create rule 9=Add similar  C>R=Current to Revised
                                                    Y Allowed      Y=Allow
 Specify revised authority in the R column.         N Rejected     N=Reject
                                                    Y Allowed (by generic* rule)
                   FTP/                             N Rejected (by generic* rule)
                   RE-                            Number of Logged Entries
                   EXEC                           FTP/REX
Opt IP-Address     C>R
 _ 1.1.1.105       Y _                                 87
 _ 1.1.1.137       Y _                                  2
 _ 1.1.1.212       Y _                              18237
 _ 127.0.0.1       N _                                  1
 _ 185.113.4.132   Y _                                 38
 _ 185.113.4.146   Y _                                  6
 _ 185.113.4.148   Y _                                225



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

Each line on the lower section of the screen shows activity directed toward a single IP address, as shown in the **IP-Address** field.

The next pair of fields shows information on outgoing activity via FTP/REXEC (including FTPLOG and TEXLOG) to that IP address.

The next set of fields appear in pairs. Each pair shows information on activity from one protocol or set of protocols, including:

The pairs of fields for each are:

- a letter on a colored background, showing how Firewall responded to the activity according to current rules
- an underscore in which you can revise the rule

The letter codes are:

- **Y**: Accepted
- **N**: Rejected
- **S**: Only accepted over SSL connections
- **A**: Accepted, without checking whether SQL statements are valid
- **B**: Only accepted over SSL connections, without checking whether SQL statements are valid
- **L**: Accepted, without either checking whether SQL statements are valid or logging the activity
- **M**: Only accepted over SSL connections, without either checking whether SQL statements are valid or logging the activity.

The color codes are:

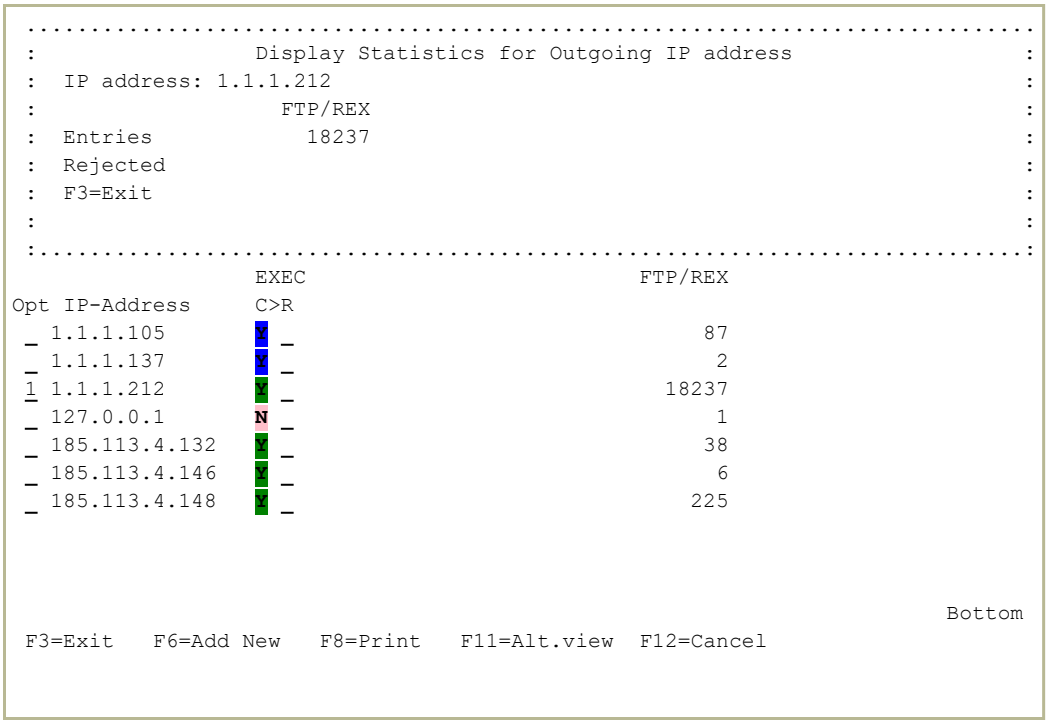
- Green: A rule specifically referring to this IP address accepts this activity
- Red: A rule specifically referring to this IP address rejects this activity
- Blue: A rule for a generic set of IP addresses that includes this one accepts this activity
- Purple: A rule for a generic set of IP addresses that includes this one rejects this activity

Thus, for example, the leftmost item on the top line of the list is the letter "**Y**" on a blue background on the line with the IP address **1.1.1.105** in the **FTP/REXEC** column. That shows that, due to a generic rule, Firewall accepts all activity toward IP address 1.1.1.105 via FTP/REXEC. (In this case, the Dynamic Filtering- Outgoing IP Address Security screen shows that

Firewall allows outgoing FTP requests from the range of IP addresses beginning with 1.1.1.1 with a subnet mask of 255.255.0.0.)

The remaining columns show the number of entries of requests logged toward that IP address via FTP/REXEC. In this case, there were 113 requests for outgoing FTP to 1.1.1.105.

To **view the statistics** on activity on a specific IP address during the time period in the data set, enter **1** in the **Opt** column for that IP address. The **Display Statistics for Outgoing IP address** window appears.




In this case, the window shows that of the 18237 requests for FTP/REXEC to IP address 1.1.1.212, none were rejected.

To **add** a new rule, press the **F6** key. The **Add Firewall Outgoing IP Address** screen appears, as shown in "Adding Firewall Rules for Outgoing Activity by IP Address with the Rule Wizard" on page 219.

To **add** a rule for a IP address **similar** to an existing one, enter **9** in the **Opt** field for that rule. The **Add Similar Incoming IP Address** screen appears, as shown in "Adding Firewall Rules for a Similar Incoming IP Address with the Rule Wizard" on page 175.

To **change rules based on activity** in the data set, see "Setting Firewall Rules based on Outgoing Activity by IP Address with the Rule Wizard" on page 220.

To **change rules manually**, see "Setting Firewall Rules Manually based on Outgoing IP Address with the Rule Wizard" on page 202.

To **delete** a rule, enter **4** in the **Opt** field for that rule. NOTE: You are not prompted for confirmation, and the rule is immediately deleted.

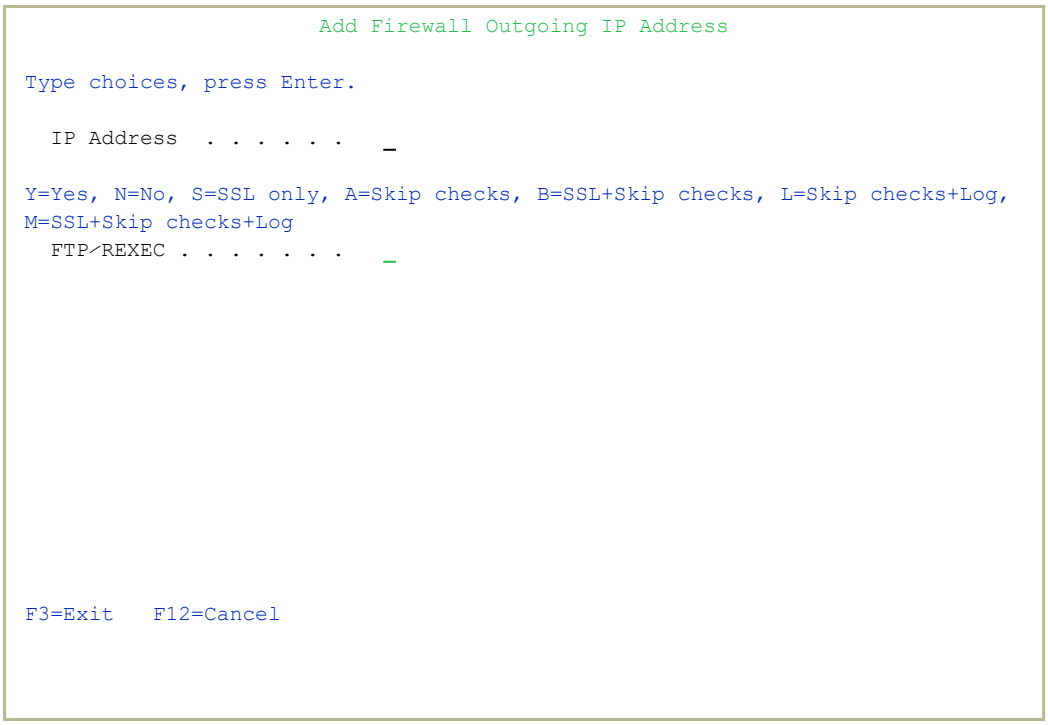
To **display the firewall log** entries relevant to this rule, enter **5** in the **Opt** field for that rule. The **Display Firewall Log** screen appears, as shown in "Displaying Firewall Logs" on page 516.

To **print** the information from the data set, press the **F8** key.

## Adding Firewall Rules for Outgoing Activity by IP Address with the Rule Wizard

To **add firewall rules to filter outgoing activity via the Rule Wizard**, press the **F6** key from the **Plan Outgoing IP Security** screen, shown in "Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard" on page 215 (*STRFW* **> 2 > 52**).

The **Add Firewall Outgoing IP Address** screen appears:



Enter the IP address to which the new rule will apply in the **IP Address** field.

Enter a letter code in the **FTP/REXEC** field showing how Firewall is to react to requests for an outgoing connection via FTP/REXEC (including FTPLOG and REXLOG) to that IP address. The letters are:

- **Y**: Accepted
- **N**: Rejected
- **S**: Only accepted over SSL connections
- **A**: Accepted, without checking whether SQL statements are valid
- **B**: Only accepted over SSL connections, without checking whether SQL statements are valid
- **L**: Accepted, without either checking whether SQL statements are valid or logging the activity
- **M**: Only accepted over SSL connections, without either checking whether SQL statements are valid or logging the activity.

If you do not enter a letter, requests to access it are handled according to the next highest generic rule that applies to it, up through the rule (if any) for ***ALL**.

## Setting Firewall Rules based on Outgoing Activity by IP Address with the Rule Wizard

To set rules based on the outgoing activity analyzed for the Rule Wizard, open the Plan Outgoing IP Security screen, as shown in "Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard" on page 215 (*STRFW* **> 2 > 52**).

```
                          Plan Outgoing IP Security
 Type choices, press Enter.                          Subset . . _______________
  1=Statistics        2=Set by use  3=Allow by use
  4=Delete 5=DSPFWLOG 6=Create rule 9=Add similar  C>R=Current to Revised
                                                    Y Allowed      Y=Allow
 Specify revised authority in the R column.         N Rejected     N=Reject
                                                    Y Allowed (by generic* rule)
                   FTP/                             N Rejected (by generic* rule)
                   RE-                            Number of Logged Entries
                   EXEC                           FTP/REX
Opt IP-Address     C>R
 _ 1.1.1.105       Y _                                 87
 _ 1.1.1.137       Y _                                  2
 _ 1.1.1.212       Y _                              18237
 _ 127.0.0.1       N _                                  1
 _ 185.113.4.132   Y _                                 38
 _ 185.113.4.146   Y _                                  6
 _ 185.113.4.148   Y _                                225


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

To **set new rules corresponding to activity seen for the IP Address**, enter **2** in the **Opt** field for that address. The **Update Outgoing IP Firewall** window appears:

```
                          Plan Outgoing IP Security
 Type choices, press Enter.                          Subset . . _______________
  .....................................................................
  :                  Update Outgoing IP Firewall                      :
  :                                                                   :
  :  Existing generic* rule makes this entry redundant.               :
  :                                                    R   D          :
  :                                          FTP/  TEL  D  TCP  M   D  FIL  : )
  :           IP              Subnet         REXEC NET  B  SGN  T   M  SRV  :
  :  New      80.179.26.75    255.255.255.255   Y                       :
O :  Existing 80.179.26.75    255.255.255.224   Y                       :
  :                                                                   :
  :  Write this rule . . . . . . .  Y          Y=Yes, N=No            :
  :  Same answer to all  . . . . .  _          Y=Yes, N=No            :
  :                                                                   :
  :                                                                   :
  :  F12=Cancel                                                       :
  :                                                                   :
  :...................................................................:


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

The new rule would be specifically for IP address 1.1.1.105, and would accept requests for outdoing FTP/REXEC access from it. In this case, however, Firewall already accepts the requests, since the IP address is within the range starting at 1.1.1.1 with the Subnet mask 255.255.0.0, so the screen suggests that creating the rule would be redundant.

To **set** new rules corresponding to **how activity differed from the existing rules**, enter **3** in the **Opt** field for that address. The **Update Outgoing IP Firewall** window appears. In this case, it would be the same as above.

Since, again, the only difference between the existing rules and the new rule for IP address 1.1.1.105 was that access was requested would be redundant, the screen notes that, and there would not appear to be any point to making the change.

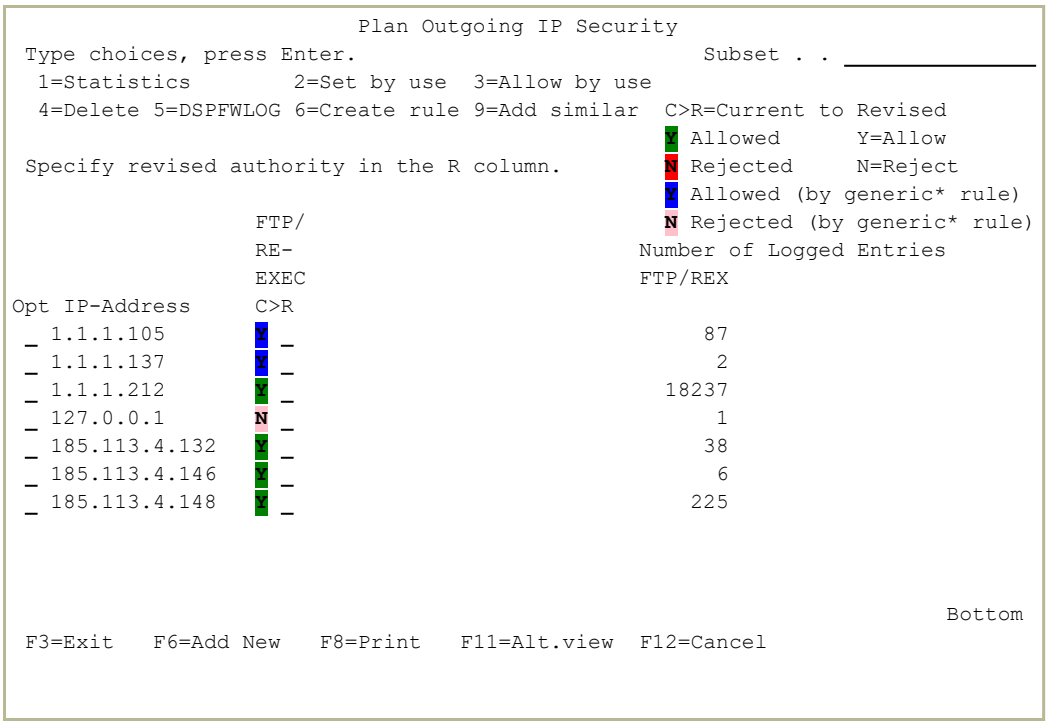
To **save** changes and exit this window, press **Enter**. The Rules Wizard saves the rule being changed and removes the line for that IP Address from the screen. You can see the resulting rule on the **Dynamic Filtering-Outgoing IP Address Security** screen, as shown in "Setting Firewall Rules for Outgoing Activity by IP Address" on page 188 (*STRFW*>**2 > 5**).

To **exit** this window without saving changes, press the **F12** key. The window closes. The changes that would have been made are marked in the columns for those servers in the lines for those IP addresses on the screen. You can then further work with the rules and save them manually, as shown in "Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard" on page 215.

## Setting Firewall Rules Manually based on Outgoing IP Address with the Rule Wizard

You can only set Firewall rules manually with the rule wizard if you have set the **Wizard type** to ***STD** when opening the wizard.

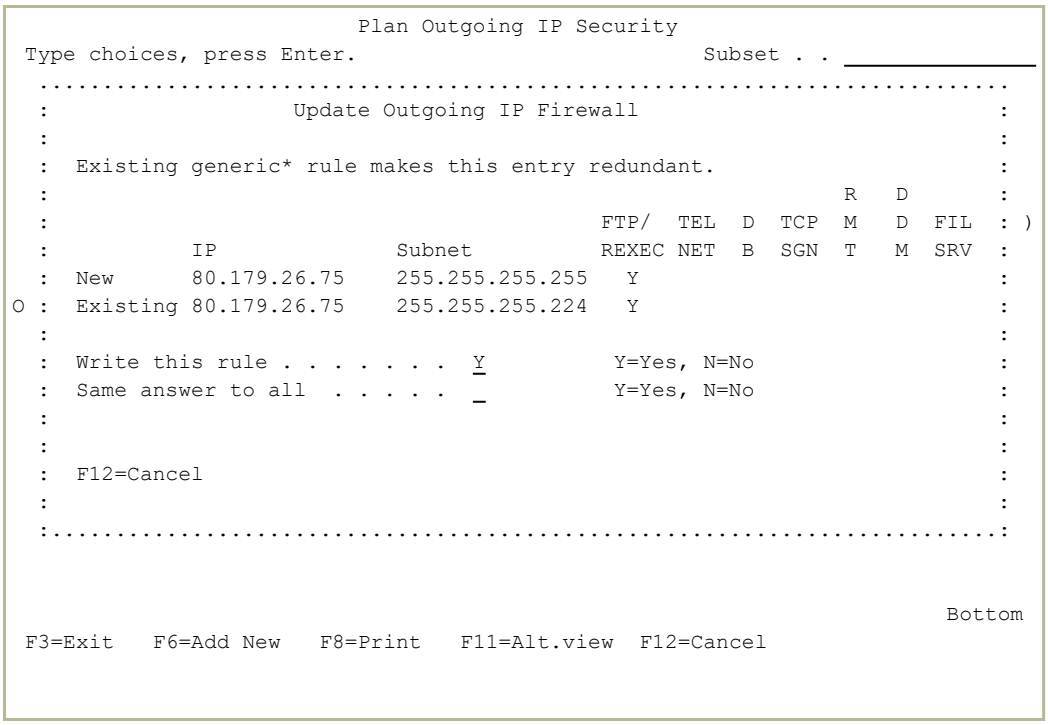
To **set rules manually** based on the outgoing IP address of the activity in the Rule Wizard, open the **Plan Outcoming IP Security** screen, as shown in "Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard" on page 215 (*STRFW* **> 2 > 52**).




To change the setting for outgoing FTP/REXEC requests from one of the listed IP addresses, enter the letter for the new setting in the column for the relevant server and the row for that IP address. The possible letters are:

- **Y**: Accepted
- **N**: Rejected
- **S**: Only accepted over SSL connections
- **A**: Accepted, without checking whether SQL statements are valid
- **B**: Only accepted over SSL connections, without checking whether SQL statements are valid
- **L**: Accepted, without either checking whether SQL statements are valid or logging the activity
- **M**: Only accepted over SSL connections, without either checking whether SQL statements are valid or logging the activity.

When you have entered the change, type **6** in the **Opt** field for that IP address then press **Enter**. The **Update Outgoing IP Firewall** window appears:

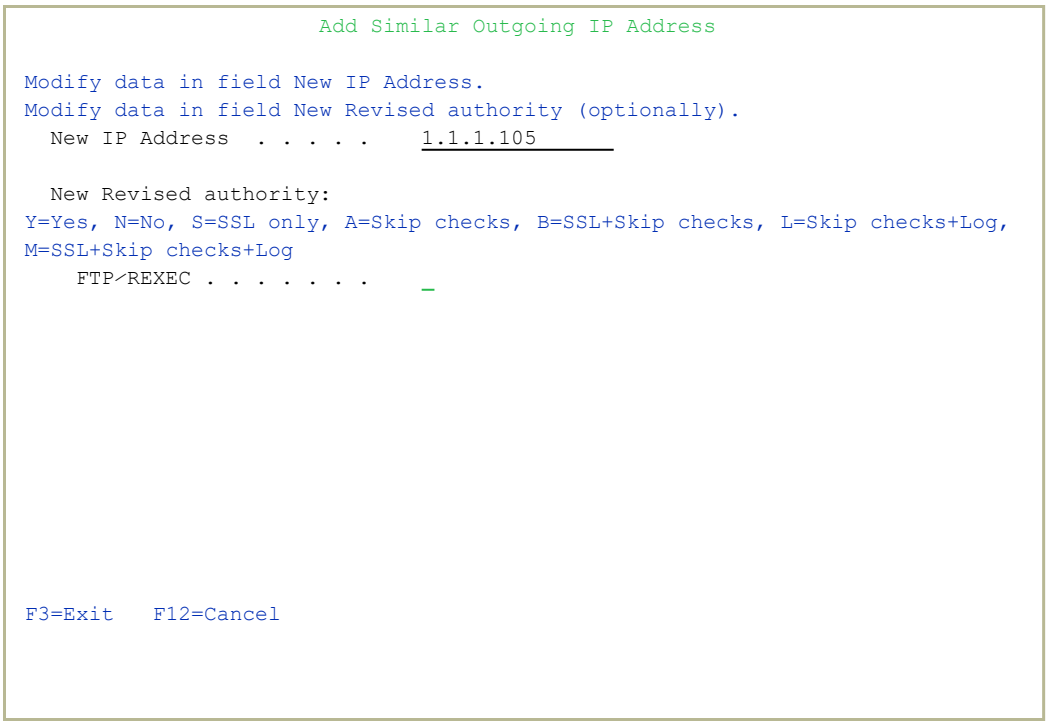



In this case, it would create a specific rule for IP Address 1.1.1.105. Since, in this rule set, it is already included in an existing rule for the IP address range starting at 1.1.1.1 with a subnet mask of 255.255.0.0, Firewall notes that it would be redundant.

## Adding Firewall Rules for a Similar Outgoing IP Address with the Rule Wizard

To add firewall rules for an outgoing IP address similar to an existing one via the Rule Wizard, type **9** in the **Opt** field for the original IP address from the **Plan Outgoing IP Security** screen, shown in "Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard" on page 215 (*STRFW* **> 2 > 52**) then press **Enter**.

The **Add Similar Outgoing IP Address** screen appears:




The original IP address appears in the **New IP Address** field. Change it to the IP address to which the new rule will apply.

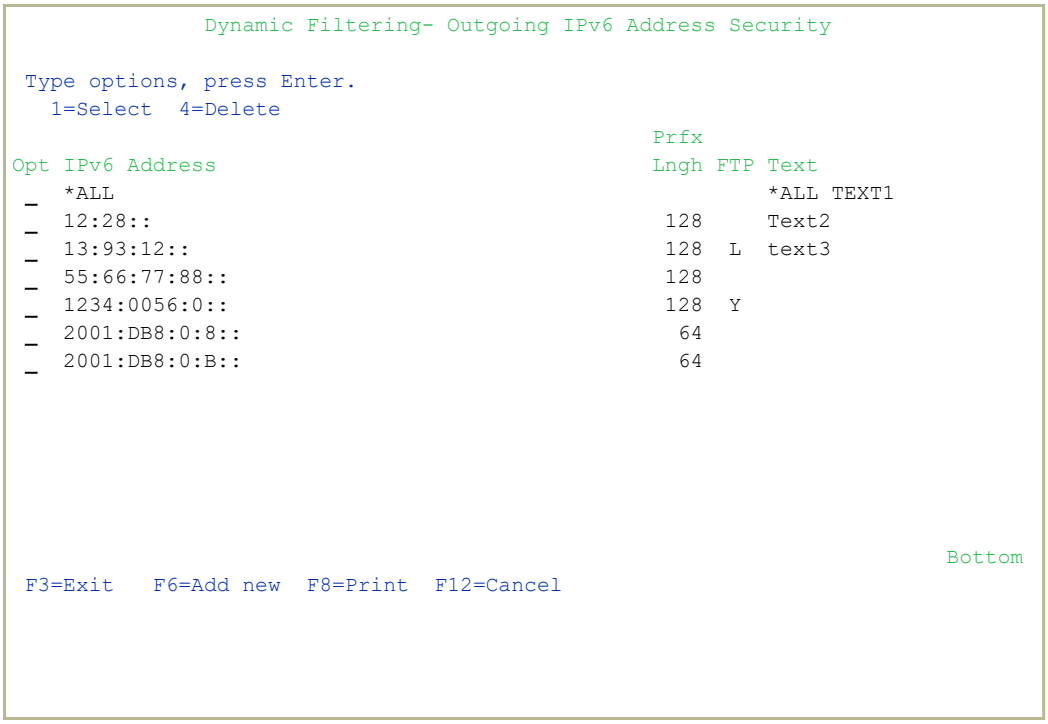
Outgoing requests use a single protocol, FTP/REXEC (including FTPLOG and REXLOG). Enter the letter representing the revised authority in the FTP/REXEC field. The possible values are:

- **Y**: Accepted
- **N**: Rejected
- **S**: Only accepted over SSL connections
- **A**: Accepted, without checking whether SQL statements are valid
- **B**: Only accepted over SSL connections, without checking whether SQL statements are valid
- **L**: Accepted, without either checking whether SQL statements are valid or logging the activity
- **M**: Only accepted over SSL connections, without either checking whether SQL statements are valid or logging the activity.

If you do not enter a letter in the field or remove an existing letter without replacing it, requests to access it are handled according to the next higher generic rule that applies to it, up through the rule (if any) for ***ALL**.

## Setting Firewall Rules for Outgoing Activity by IPv6 Address

You can filter outgoing activity by IPv6 address from the **Dynamic Filtering - Outgoing IPv6 Address Security** screen. To reach the screen, select **`6. Outgoing IPv6 Addresses`** from the **`Work with Dynamic Filtering`** screen(*STRFW* **`> 2 > 5`**).




The screen shows existing rules for filtering outgoing FTP activity from specific IPv6 address ranges, as shown by the **`IPv6 Address`** and **`Prfx Lngth`** (Prefix Length) fields. The entry for **`*ALL`** shows general rules for incoming activity coming from IPv6 addresses that are not listed.

The FTP column either is blank or shows a letter indicating how Firewall is to filter FTP requests going to that IP Address Range.

- Blank: Reject all incoming activity
- **`A`**: Allow activity without checking
- **`B`**: Allow only activity over an SSL connection, without parsing SQL statements
- **`L`**: Log and allow activity, without checking
- **`M`**: Log and allow only activity over an SSL connection, with parsing SQL statements

- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

The final **Text** column shows a freeform text description of the rule.

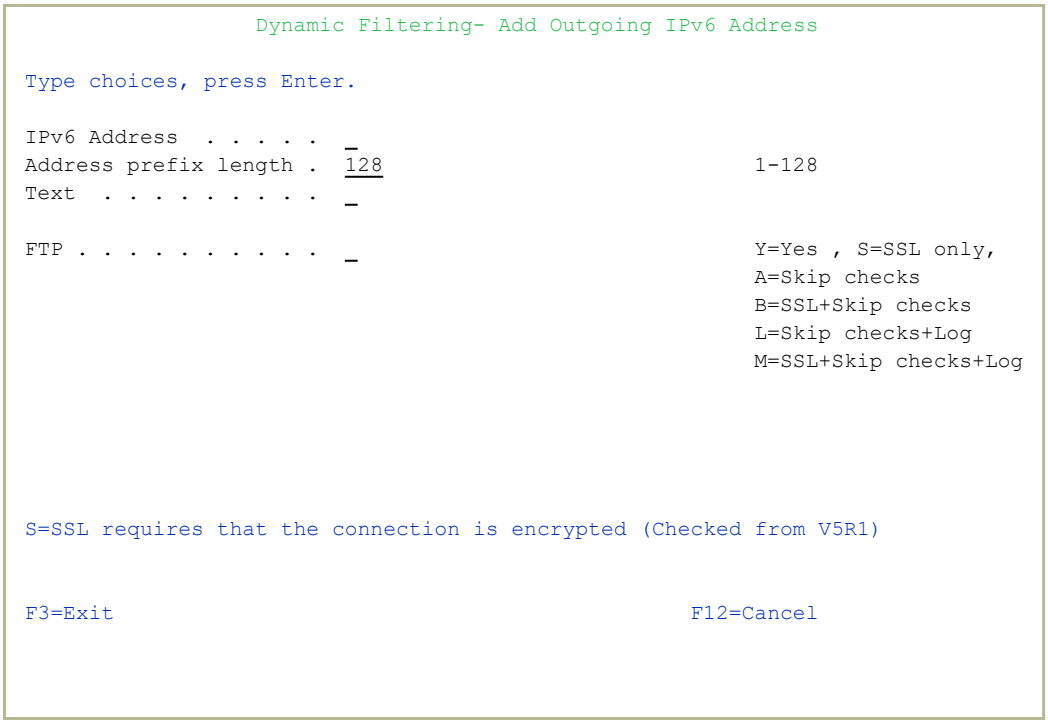
To modify an existing rule, type **1** in the **Opt** column for that rule and press Enter.

To add a new rule, press the **F6** key.

## Adding a Firewall Rule for Outgoing Activity by IPv6 Address

To add a rule for filtering outgoing activity by IP address, press the **F6** key in the **Dynamic Filtering - Outgoing IPv6 Address Security** screen, shown in "Setting Firewall Rules for Outgoing Activity by IP Address" on page 188

The **Dynamic Filtering - Add Outgoing IPv6 Address** screen appears:




Enter or modify information in the following fields:

**IPv6 Address**

The IPv6 address for the range of addresses. In addition to an IPv6 address, you can set this field to *ALL for rules applied to all IPv6 ranges that aren't otherwise specified.

**Address prefix length**

The length of the IPv6 address prefix. This can be set to from 1-128.

**Text**

A free-form text description of the IPv6 address range.

**FTP**

A letter or blank space indicating how Firewall is to filter FTP requests going to that IPv6 Address Range.

The possible values are:

- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

In many situations, you can dramatically improve performance by using options **B** or **L**. For example, you might use them when an IP address that you know to be well secured and is using SSL, and which doesn't require checking the SQL statements, sends a high volume of requests.

## Modifying a Firewall Rule for Outgoing Activity by IPv6 Address

To modify an existing rule for filtering outgoing activity by IPv6 address, enter **1** in the **Opt** field for that rule in the **Dynamic Filtering - Outgoing IP Address Security** screen, shown in "Setting Firewall Rules for Outgoing Activity by IPv6 Address" on page 206 (***STRFW > 2 > 6***).

The **Dynamic Filtering - Modify Outgoing IPv6 Address** screen appears:

```
                Dynamic Filtering- Modify Outgoing IPv6 Address

Type choices, press Enter.

IPv6 Address  . . . . .  12:28::
Address prefix length .  128                          1-128
Text  . . . . . . . . .  Text2

FTP . . . . . . . . . .  _                            Y=Yes , S=SSL only,
                                                      A=Skip checks
                                                      B=SSL+Skip checks
                                                      L=Skip checks+Log
                                                      M=SSL+Skip checks+Log

Equivalent IP range:
  From IP:    0012:0028:0000:0000:0000:0000:0000:0000
  To   IP:    0012:0028:0000:0000:0000:0000:0000:0000

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


F3=Exit                                          F12=Cancel
```

Enter or modify information in the following fields:

**IPv6 Address**

The IPv6 address for the range of addresses. In addition to an IPv6 address, you can set this field to *ALL for rules applied to all IPv6 ranges that aren't otherwise specified.

**Address prefix length**

The length of the IPv6 address prefix. This can be set to from 1-128.

**Text**

A free-form text description of the IPv6 address range.

**FTP**

A letter or blank space indicating how Firewall is to filter FTP requests going to that IPv6 Address Range.

The possible values are:

- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

In many situations, you can dramatically improve performance by using options **B** or **L**. For example, you might use them when an IP address that you know to be well secured and is using SSL, and which doesn't require checking the SQL statements, sends a high volume of requests.

The **Equivalent IPv6 range** field shows a read-only value indicating the range of IPv6 addresses included by the IPv6 address and prefix length.

## Using the Rule Wizard for Outgoing Activity by IP Address

Using the Rule Wizard, you can analyze recent activity on your system and use that information to create and modify Firewall rules.

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

IP Addresses                              Rule Wizards - Incoming IP
 1. Incoming IP Addresses/Local-jobs      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
```

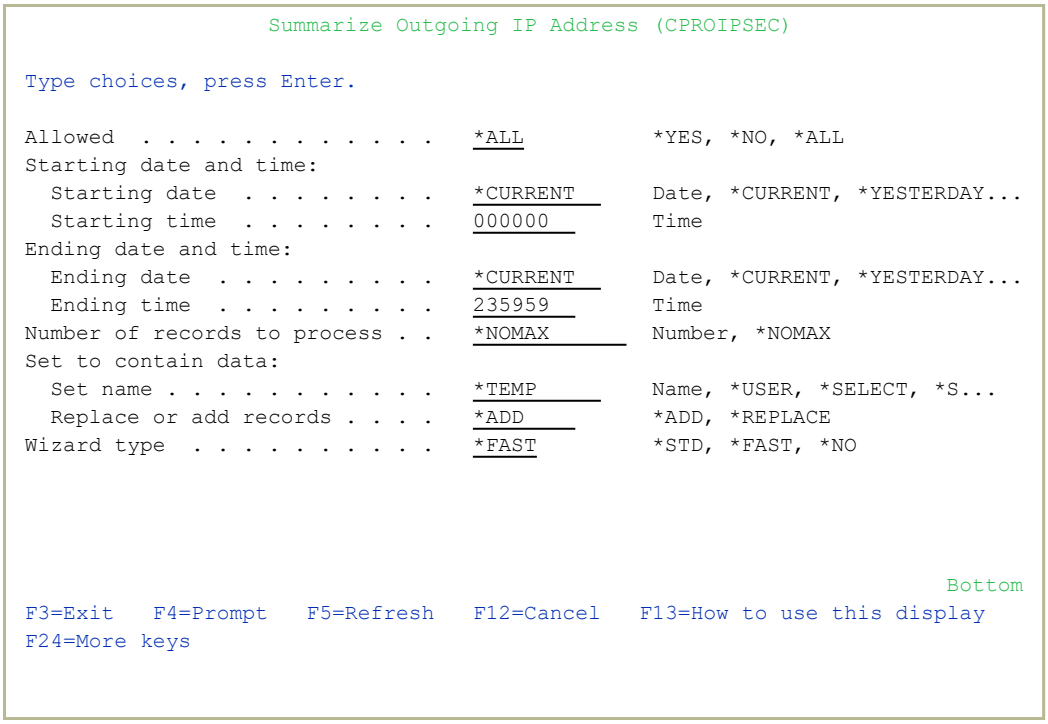
To **create a data set** for examining activity and developing rules for outgoing activity based on IP address, select **`51. Create Working Data Set`** from the **Work with Dynamic Filtering** screen *(STRFW* **`> 2`**).
The **Summarize Outgoing IP Address (CPROIPSEC)** screen appears, as shown in "Creating a Data Set of Outgoing Activity by IP Address with the Rule Wizard" below.

To **use an existing data set** to develop rules, select **`52. Work with Rule Wizard`** from the **Work with Dynamic Filtering** screen (*STRFW* **`> 2`**).
The **Outgoing IP Address Wizard (WZROIPSEC)** screen appears, as shown in "Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard" on page 215.

## Creating a Data Set of Outgoing Activity by IP Address with the Rule Wizard

To **create a data set** for examining activity and developing rules for outgoing activity based on IP address, select **`51. Create Working Data Set`** from the **Work with Dynamic Filtering** screen *(STRFW* **`> 2`**).

The **Summarize Outgoing IP Address (CPROIPSEC)** screen appears. From this screen, you can construct the command line command that creates the data set.




The screen contains the following fields. Fields that have values other than the defaults are preceded by the "**>**" character:

### Allowed

Specifies whether the data set includes rejected activity, accepted activity, or both.

- ***YES**: Include only accepted activity
- ***NO:** Include only rejected activity
- ***ALL:** Include both accepted and rejected activity

### Starting data and time

#### Starting date

The day or date on which the included data begins.

Allowed values include:

- ***CURRENT**: The current date
- ***YESTERDAY**: Yesterday's date

- ***WEEKSTR**: The first day of the current week. By default, this is Sunday.
- ***PRVWEEKS**: The first day of the previous week
- ***MONTHSTR**: The first day of the current month
- ***PRVMONTHS**: The first day of the previous month
- ***YEARSTR**: The first day of the current year
- ***PRVYEARS**: The first day of the previous year
- ***MON**: Monday
- ***TUE**: Tuesday
- ***WED**: Wednesday
- ***THU**: Thursday
- ***FRI**: Friday
- ***SAT**: Saturday
- ***SUN**: Sunday

**Starting time**

The time on the Starting date at which the included data begins, in **HHMMSS** format.

**Ending date**

The day or date on which the included data ends.

Allowed values are the same as for **Starting date**.

**Ending time**

The time on the Starting date at which the included data ends, in **HHMMSS** format.

**Number of records to process**

Collect no more than this number of records. If set to ***NOMAX**, collect all the relevant records.

**Server ID**

The server that the activity is attempting to access. To see a list of possible values, press the F4 key.

**Set to contain data**

**Set name**

The name of the data set that will contain the records. You can set this to your own value or choose one of these

options:

- ***TEMP**: The default name for temporary data sets. The data set is removed when the session ends.
- ***USER**: Your user name
- ***S**: Equivalent to ***SELECT**
- ***SELECT**: If the wizard has been run before, a list appears of previous names that had been used for the data set.

**Replace or add records**

If any records already exist in the data set, whether to replace them or add the new records to them.

Possible values include:

- ***ADD**: Add new records to the existing set
- ***REPLACE**: Replace all existing records with the new ones.

**Wizard type**

The type of wizard to be created. Possible values include:

- ***STD**: The Rule Wizard screen that appears next has all the standard options
- ***FAST**: The Rule Wizard screen that appears next has a limited set of options for faster processing, as documented there.
- ***NO**: The data set will only be used to batch processing.

To list and select possible values for many of the fields, place the cursor within the field and press the F4 key.

To reset the values on the screen to their default values, press the F5 key.

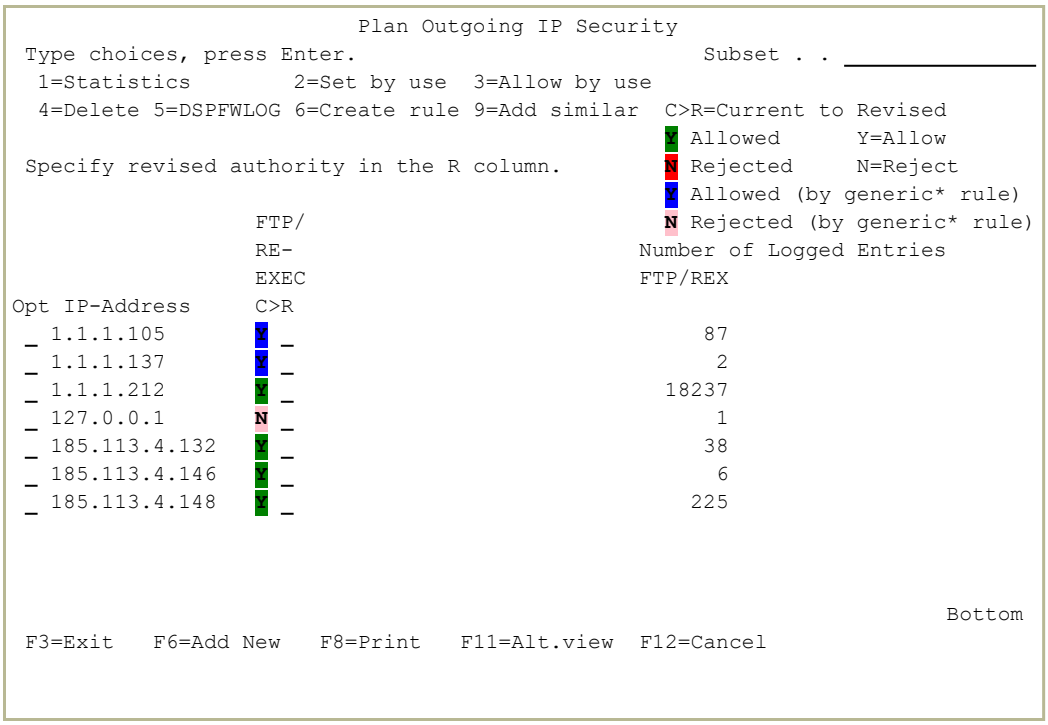
## Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard

The Rule Wizards analyze data on recent system activity to develop and improve rules for filtering future activity.

To develop rules to filter incoming activity by IP Address, first create a data set of recent activity, as shown in "Creating a Data Set of Outgoing Activity by IP Address with the Rule Wizard" on page 212.

Once you have created a data set, select **52. Work with Rule Wizard** from the **Work with Dynamic Filtering** screen (*STRFW* **> 2**).

The **Plan Outgoing IP Security** screen appears:




Each line on the lower section of the screen shows activity directed toward a single IP address, as shown in the **IP-Address** field.

The next pair of fields shows information on outgoing activity via FTP/REXEC (including FTPLOG and TEXLOG) to that IP address.

The next set of fields appear in pairs. Each pair shows information on activity from one **protocol** or set of protocols, including:

The **pairs of fields** for each are:

- a **letter** on a colored background, showing how Firewall responded to the activity according to current rules
- an **underscore** in which you can revise the rule

The **letter codes** are:

- **Y**: Accepted
- **N**: Rejected
- **S**: Only accepted over SSL connections
- **A**: Accepted, without checking whether SQL statements are valid
- **B**: Only accepted over SSL connections, without checking whether SQL statements are valid
- **L**: Accepted, without either checking whether SQL statements are valid or logging the activity
- **M**: Only accepted over SSL connections, without either checking whether SQL statements are valid or logging the activity.

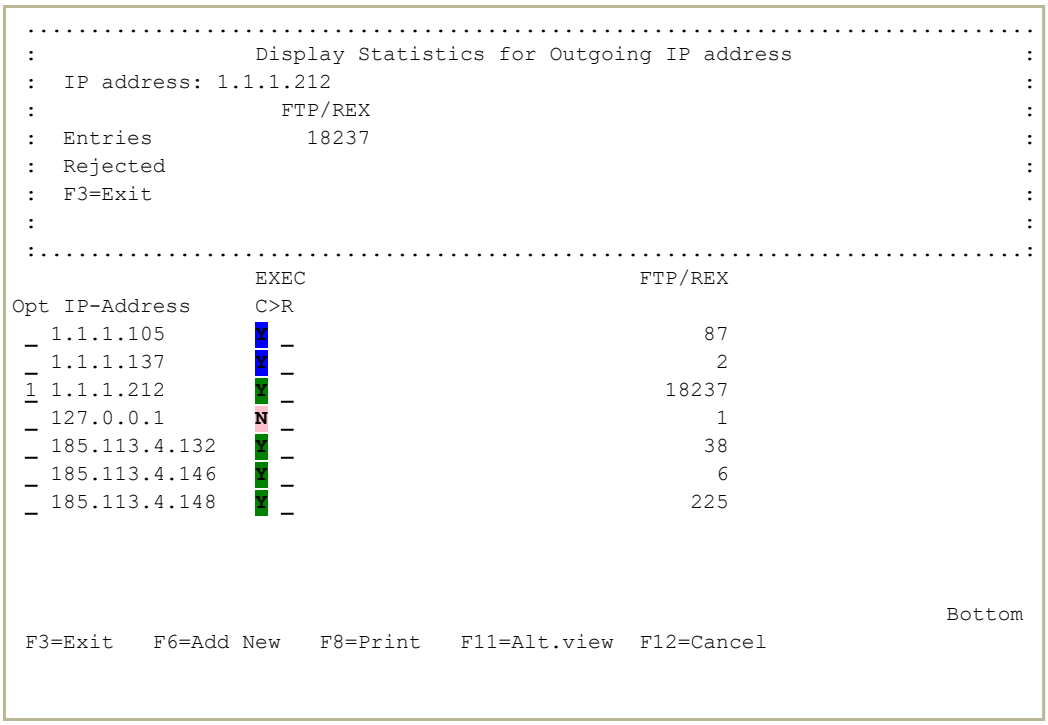
The color codes are:

- Green: A rule specifically referring to this IP address accepts this activity
- Red: A rule specifically referring to this IP address rejects this activity
- Blue: A rule for a generic set of IP addresses that includes this one accepts this activity
- Purple: A rule for a generic set of IP addresses that includes this one rejects this activity

Thus, for example, the leftmost item on the top line of the list is the letter "**Y**" on a blue background on the line with the IP address **1.1.1.105** in the **FTP/REXEC** column. That shows that, due to a generic rule, Firewall accepts all activity toward IP address 1.1.1.105 via FTP/REXEC. (In this case, the Dynamic Filtering- Outgoing IP Address Security screen shows that Firewall allows outgoing FTP requests from the range of IP addresses beginning with 1.1.1.1 with a subnet mask of 255.255.0.0.)

The remaining columns show the number of entries of requests logged toward that IP address via FTP/REXEC. In this case, there were 113 requests for outgoing FTP to 1.1.1.105.

To view the statistics on activity on a specific IP address during the time period in the data set, enter **1** in the **Opt** column for that IP address. The Display Statistics for Outgoing IP address window appears.




In this case, the window shows that of the 18237 requests for FTP/REXEC to IP address 1.1.1.212, none were rejected.

To **add** a new rule, press the **F6** key. The **Add Firewall Outgoing IP Address** screen appears, as shown in "Adding Firewall Rules for Outgoing Activity by IP Address with the Rule Wizard" on the facing page.

To **add** a rule for a IP address **similar** to an existing one, enter **9** in the **Opt** field for that rule. The **Add Similar Incoming IP Address** screen appears, as shown in "Adding Firewall Rules for a Similar Incoming IP Address with the Rule Wizard" on page 175.

To **change rules based on activity** in the data set, see "Setting Firewall Rules based on Outgoing Activity by IP Address with the Rule Wizard" on page 220.

To **change rules manually**, see "Setting Firewall Rules Manually based on Outgoing IP Address with the Rule Wizard" on page 202.

To **delete** a rule, enter **4** in the **Opt** field for that rule. NOTE: You are not prompted for confirmation, and the rule is immediately deleted.

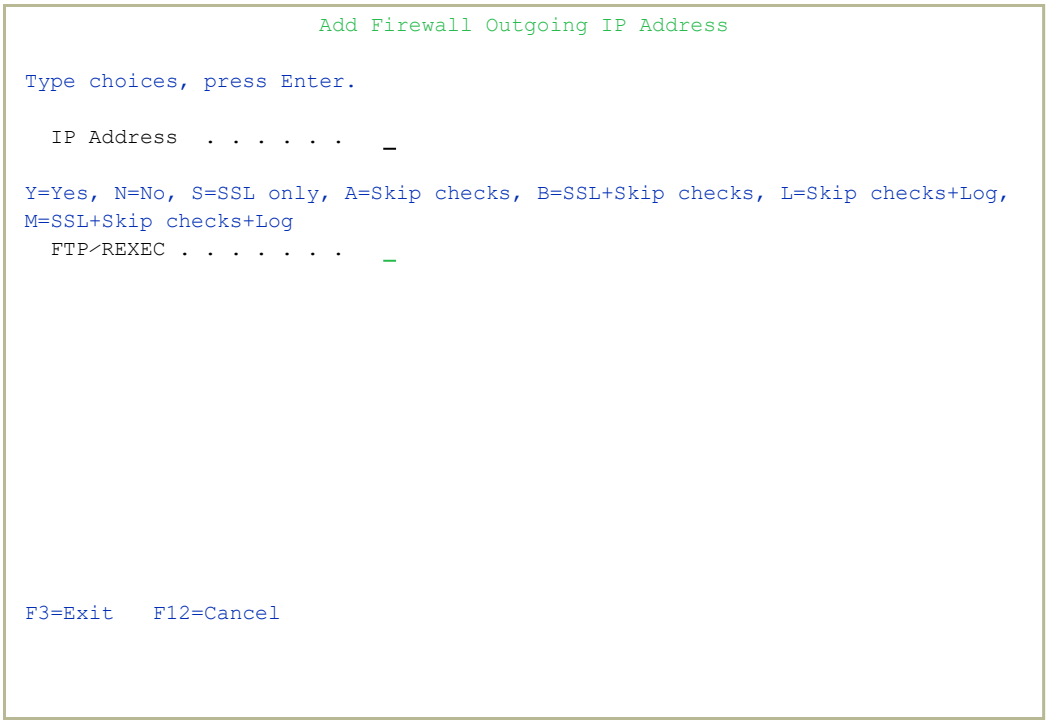
To **display the firewall log** entries relevant to this rule, enter **5** in the **Opt** field for that rule. The **Display Firewall Log** screen appears, as shown in "Displaying Firewall Logs" on page 516.

To **print** the information from the data set, press the **F8** key.

## Adding Firewall Rules for Outgoing Activity by IP Address with the Rule Wizard

To **add firewall rules to filter outgoing activity via the Rule Wizard**, press the **F6** key from the **Plan Outgoing IP Security** screen, shown in "Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard" on page 215 (***STRFW* > 2 > 52**).

The **Add Firewall Outgoing IP Address** screen appears:




Enter the IP address to which the new rule will apply in the **IP Address** field.

Enter a letter code in the **FTP/REXEC** field showing how Firewall is to react to requests for an outgoing connection via FTP/REXEC (including FTPLOG and REXLOG) to that IP address. The letters are:

- **Y**: Accepted
- **N**: Rejected
- **S**: Only accepted over SSL connections
- **A**: Accepted, without checking whether SQL statements are valid

- **B**: Only accepted over SSL connections, without checking whether SQL statements are valid
- **L**: Accepted, without either checking whether SQL statements are valid or logging the activity
- **M**: Only accepted over SSL connections, without either checking whether SQL statements are valid or logging the activity.

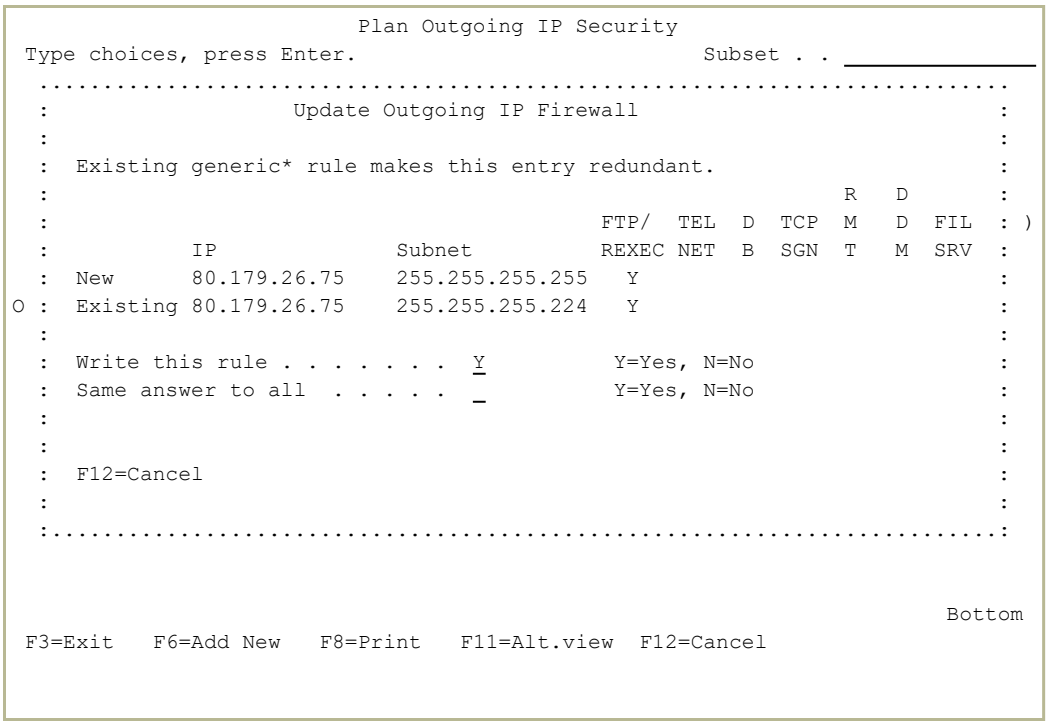
If you do not enter a letter, requests to access it are handled according to the next highest generic rule that applies to it, up through the rule (if any) for ***ALL**.

## Setting Firewall Rules based on Outgoing Activity by IP Address with the Rule Wizard

To set rules based on the outgoing activity analyzed for the Rule Wizard, open the Plan Outgoing IP Security screen, as shown in "Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard" on page 215 (*STRFW* **> 2 > 52**).

```
                          Plan Outgoing IP Security
 Type choices, press Enter.                          Subset . . _______________
  1=Statistics        2=Set by use  3=Allow by use
  4=Delete 5=DSPFWLOG 6=Create rule 9=Add similar  C>R=Current to Revised
                                                    Y Allowed      Y=Allow
 Specify revised authority in the R column.         N Rejected     N=Reject
                                                    Y Allowed (by generic* rule)
                   FTP/                             N Rejected (by generic* rule)
                   RE-                            Number of Logged Entries
                   EXEC                           FTP/REX
Opt IP-Address     C>R
 _ 1.1.1.105       Y _                                 87
 _ 1.1.1.137       Y _                                  2
 _ 1.1.1.212       Y _                              18237
 _ 127.0.0.1       N _                                  1
 _ 185.113.4.132   Y _                                 38
 _ 185.113.4.146   Y _                                  6
 _ 185.113.4.148   Y _                                225



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

To set new rules corresponding to activity seen for the IP Address, enter **2** in the **Opt** field for that address. The Update Outgoing IP Firewall window appears:




The new rule would be specifically for IP address 1.1.1.105, and would accept requests for outdoing FTP/REXEC access from it. In this case, however, Firewall already accepts the requests, since the IP address is within the range starting at 1.1.1.1 with the Subnet mask 255.255.0.0, so the screen suggests that creating the rule would be redundant.

To **set** new rules corresponding to **how activity differed from the existing rules**, enter **3** in the **Opt** field for that address. The **Update Outgoing IP Firewall** window appears. In this case, it would be the same as above.

Since, again, the only difference between the existing rules and the new rule for IP address 1.1.1.105 was that access was requested would be redundant, the screen notes that, and there would not appear to be any point to making the change.

To **save** changes and exit this window, press **Enter**. The Rules Wizard saves the rule being changed and removes the line for that IP Address from the screen. You can see the resulting rule on the **Dynamic Filtering-Outgoing IP Address Security** screen, as shown in "Setting Firewall Rules for Outgoing Activity by IP Address" on page 188 (***STRFW*>2 > 5**).

To **exit** this window without saving changes, press the **F12** key. The window closes. The changes that would have been made are marked in the columns for those servers in the lines for those IP addresses on the screen. You can then further work with the rules and save them manually, as shown in "Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard" on page 215.

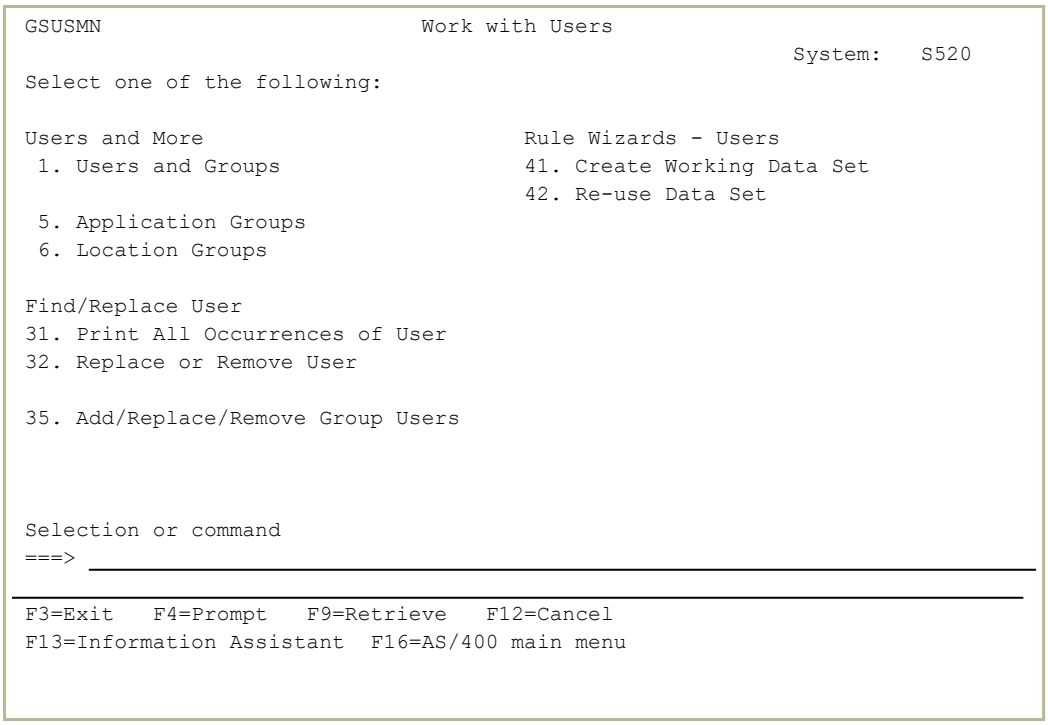
# Setting Firewall Rules for Users, Groups, and Applications

Firewall can filter activity by the user requesting it. Users can be members of multiple groups, including both IBM-defined groups and other Firewall-specific groups based on the applications that the user runs, the user's location, or other ad-hoc criteria. Firewall can also find all instances of a user or group, remove the user or group from the system, or replace the user or group with another.

If the Security Level for a server is set to three or above (as shown in "Modifying Firewall Settings for Servers" on page 58), user-based rules can override the general rules for a server. For example, if the Security Level parameter in the server security rule for the FTP server is set to 3 (user-to-service), the user-to-server rules set here may allow activity for certain users and reject access for others, beyond the general rules for the server.

For the FTP, SQL, Database, and DDM servers, you can establish rules restricting the commands (also known as "verbs") that specified users or groups can perform. For example, you can define that members of the user group %PGMR are not permitted to execute the SQL delete command.

You can examine and create these filter rules, and use the Rule Wizards to built new rules based on users and groups from the **Work with Users** screen (*STRFW* > **3**).




To create and manage rules for users and groups, select **1. Users and Groups**. The Work with User Security screen appears, as shown in "Setting Firewall Rules for Users and Groups" on page 226.

To create and manage rules for application groups, select **5. Application Groups**. The Work with Application Groups screen appears, as shown in "Setting Firewall Rules for Application Groups" on page 271.

To create and manage rules for location groups, select **6. Users and Groups**. The Work with Location Groups screen appears, as shown in "Setting Firewall Rules for Location Groups" on page 278.

To print a report of all rules that affect and groups that include a user, select **31. Print All Occurrences of User**. The Replace FW user (RPLFWUSR) screen appears, with the **Replace to user** field set to ***PRINT**. Enter the name of the user or group in the **Replace from user** field.

To add a member to a Firewall group, replace a member in it, or remove a member from it, select **35. Add/Replace/Remove Group Users**. The Change Firewall User Group (CHGFWGRP) screen appears, as shown in "Adding, Replacing, or Removing Members of Firewall Groups" on page 284.

To remove a user or replace one user with another, select **32. Replace or Remove User**. The Replace FW user (RPLFWUSR) screen appears. Enter the name of the user or group to be replaced or removed in the **Replace to user** field.

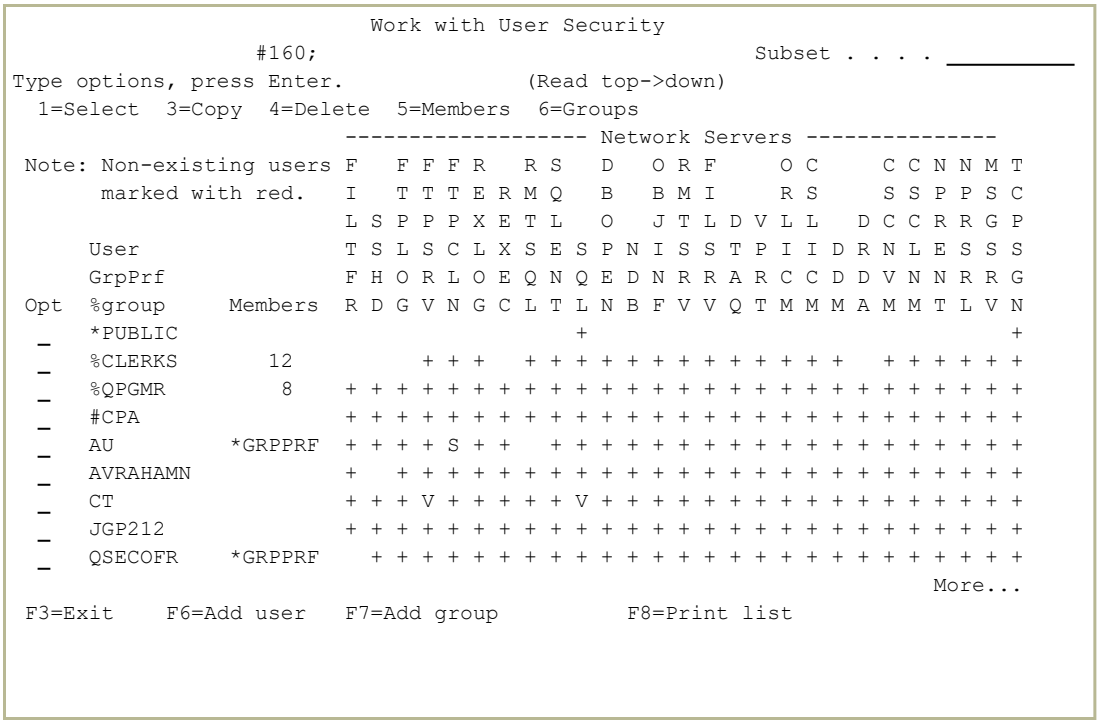
To remove a user or group, enter ***REMOVE** in the **Replace to user** field.

To replace one user or group with another, enter the name of the replacement in the **Replace from user** field.

## Setting Firewall Rules for Users and Groups

To filter incoming activity by users and groups, select **`1. Users and Groups`** from the **`Work with Users`** screen (*STRFW* **`> 3 > 1`**).

The Work with User Security screen appears.



```
                          Work with User Security
                  #160;                                  Subset . . . . _________
Type options, press Enter.                (Read top->down)
  1=Select  3=Copy  4=Delete  5=Members  6=Groups
                         ------------------- Network Servers ---------------
 Note: Non-existing users F   F F F R   R S   D   O R F     O C     C C N N M T
       marked with red.   I   T T T E R M Q   B   B M I     R S     S S P P S C
                          L S P P P X E T L   O   J T L D V L L   D C C R R G P
      User                T S L S C L X S E S P N I S S T P I I D R N L E S S S
      GrpPrf              F H O R L O E Q N Q E D N R R A R C C D D V N N R R G
 Opt  %group     Members  R D G V N G C L T L N B F V V Q T M M M A M M T L V N
  _   *PUBLIC                           +                                    +
  _   %CLERKS       12          + + +   + + + + + + + + + + + +   + + + + + +
  _   %QPGMR         8    + + + + + + + + + + + + + + + + + + + + + + + + + +
  _   #CPA                + + + + + + + + + + + + + + + + + + + + + + + + + +
  _   AU          *GRPPRF  + + + + S + +   + + + + + + + + + + + + + + + + + +
  _   AVRAHAMN             +   + + + + + + + + + + + + + + + + + + + + + + + +
  _   CT                   + + + V + + + + + V + + + + + + + + + + + + + + + +
  _   JGP212               + + + + + + + + + + + + + + + + + + + + + + + + + +
  _   QSECOFR     *GRPPRF    + + + + + + + + + + + + + + + + + + + + + + + + +
                                                                        More...
 F3=Exit    F6=Add user   F7=Add group          F8=Print list
```

Firewall supports both IBM i group profiles and its own Firewall User Groups.

The **`User GrpPrf %group`** column lists users and groups (including both the IBM i **`GrpPrf`** and Firewall's own **`%group`**). The **`Members`** column shows the number of users included in the group.

NOTE: A Firewall user can also serve as a group. If the **`Members`** column for the user is set to **`*GRPPRF`**, other users can be added to a group of the same name via the standard *CHGUSRPRF* screen or command, and inherit the rules and attributes of that user.

The rest of the columns show whether the rules set for users or groups can override the global rules for particular servers. The server names, shown vertically at the top of the column, are:

- **`FILTFR`**: Original File Transfer Function
- **`SSHD`**: SSH,SFTP,SCP- Secured CMD Entry,FTP,COPY
- **`FTPLOG`**: FTP logging

- **FTPSRV**: FTP Server-Incoming Request Validation
- **FTPCLN**: FTP Client-Outgoing Request Validation
- **REXLOG**: Remote execution log
- **REXEC**: REXEC Server Request Validation
- **RMTSQL**: REXEC Server Request Validation
- **SQLENT**: Database Server - entry
- **SQL**: Database Server - SQL access & Show
- **DBOPEN**: Open Database
- **NDB**: Database Server - Database access
- **OBJINF**: Database Server - object information
- **RMTSRV**: Remote Command/Program Call
- **FILSRV**: File Server
- **DTAQ**: Data Queue Server
- **VPRT**: Original Virtual Print Server
- **ORLICM**:
- **CSCICM**:
- **DDM**: DDM request access
- **DRDA**: DDM request access
- **CSCNVM**: Central Server - conversion map
- **CSCLNN**: Central Server - client mgmt
- **NPRENT**: Central Server - client mgmt
- **NPRSRL**: Network Print Server - spool file
- **MSGSRV**: Original Message Server
- **TCPSGN**: Original Message Server

The server status values are:

- **+** : The user may use this server. This does not override global server security rules.
- **V** : For servers that support specific verbs (as shown in "Setting Server Verbs to Skip" on page 153), the user may use those verbs on this server.
- **S** : The user can access the server, skipping the check for object authorizations. This is normally used for batch applications that play the role of servers. It increases performance and simplifies tests for some users.
- Blank : User may not use this server.

To add a user, press the F6 key. The **Add User Security** screen, shown in "Adding Firewall Settings for a User" on page 229, appears.

To **add a group**, press the **F7** key. The **Add User Group Security** screen, shown in "Adding Firewall Settings for a Group" on page 243, appears.

To **print** the list of users and groups and their network server settings, press the **F8** key.

To **modify** the settings for a user or group, enter **1** in the **Opt** column for that user or group.

For a user, the **Modify User Security** screen appears, as shown in "Modifying Firewall Settings for a User" on page 246.
For a group, the **Modify User Group Security** screen appears, as shown in "Modifying Firewall Settings for a Group" on page 264.

To **copy** the settings from one user or group to another, enter **3** in the **Opt** column for that user or group. The **Copy Definition** screen appears, as shown in "Copying Firewall Settings for a User or Group" on page 267

To **delete** the settings for a user or group, enter **4** in the **Opt** column for that user or group. The **Delete User Security** screen appears, as shown in "Deleting Firewall Settings for a User or Group" on page 270.

To **add, remove, or change** the members of a group, enter **5** in the **Opt** column for that group. The **Modify Group of Users** screen appears, as shown in "Changing the Members of a Firewall Group" on page 269

To **list** the groups that include a user, enter **6** in the **Opt** column for that user. The **List of User Groups with User** window appears, as shown in "Displaying a List of Groups that Include a User" on page 268.

## Adding Firewall Settings for a User

To **add Firewall settings for a user**, press the **F6** key in the **Work with User Security** screen, shown in "Setting Firewall Rules for Users and Groups" on page 226 (*STRFW > 3 > 1*).

The **Add User Security** screen appears.

```
                            Add User Security

User/GrpPrf . . . . . . . . . . .  __________  Name, F4 for list

Authorities
  1. Services                                  FTP, SQL, NDB, DDM ...
  2. IP
  3. IPv6
  4. Device names                              for SIGNON only
  5. Services/Locations by %Groups             %FINANCE, %#EXCEL, %@NEWYORK ...
  6. Chg/Swap users for obj authority          Assign alt. users by services
Selection ===>                  _

Add %Group/GrpPrf & SupPrf Auth .  _           Y=Yes, N=No, blank=Default ( Y )
User allowed to work during . . .  __________  Time group, *NEVER=Allow by grp
Ensure user work from a single IP  N           Y=Yes, I=Interactive only, N=No
Special treatment for this user .  _           F=FYI, S=Skip: Allow, no log

Check (in FW) Native obj auth . .  3           1=Allow all, 2=Reject all, 3=Yes
Check (in FW) IFS auth  . . . . .  3           1=Allow all, 2=Reject all, 3=Yes
F3=Exit         F4=Prompt
F9=Object security              F10=Logon security          F12=Cancel
```

Type the user's name in the **User/GrpPrf** field. To select users from a list, press the **F4** key.

Through the options in the **Authorities** list, you can create specific rules for a user or group.

**1. Services**

To create filters based on services (such as **FTP**, **SQL**, **NBD**, or **DDM**), enter **1** in the **Selection** field. The **Add User to Server Security** screen appears, as shown in "Adding Firewall Settings for a User based on Services" on page 232.

**2. IP**

To create filters based on IP addresses, enter **2** in the **Selection** field. The **Work with User IP Validation** screen

appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IP Address" on page 189.

**3. IPv6**

To create filters based on IPv6 addresses, enter **3** in the **Selection** field. The Work with User IPv6 Validation screen appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IPv6 Address" on page 208.

**4. Device name**

To create filters based on SNA system names, enter **4** in the **Selection** field. The Work with Sign-On Device Validation screen appears, as shown in "Adding a Firewall Rule for Incoming Activity by Remote System Names" on page 184.

**5. Services/Locations by %Groups**

You can create groups of users based on applications that they use, locations in which they work, or other criteria. To add members to these group or to remove them, enter **5** in the **Selection** field. The Define Allowed Groups screen appears, as shown in "Adding a User to Firewall Groups" on page 239.

**6. Chg/Swap users for obj authority**

To have the user assume the authority of a different user when using particular servers, enter **6** in the **Selection** field. The Work with Alternative Users screen appears, as shown in "Adding Firewall Settings for a User to Assume Different Authority for a Server" on page 241.

These options control more aspects of the user's authority:

**Add %Group/GrpPrf & SupPrf Auth**

To add authority settings from the group that include this user, type **Y**.

To prevent adding authority settings from the groups that include this user, type **N**,

To use the default settings, as defined in "Setting Additional Definitions for Firewall" on page 34, leave the field blank.

**User allowed to work during**

To limit the user to working within a specified range of hours of the day or days of the week, enter the name of a time group with those time settings (as shown in "Defining Time Groups" on page 504).

To use the default settings for the server, enter ***NEVER**.

**Ensure single IP use**

To limit the user to working from one IP address at a time, type **Y**. The user may have multiple sessions open at a time, but they must all be from the same IP address.

To limit the user's interactive sessions to one IP address at a time, type **I**. This does not affect the user's batch jobs.

To allow the user to work from multiple IP addresses simultaneously, type **N**.

**Special treatment for this user**

To handle all the user's activity in FYI mode (as shown in "Running Firewall in FYI Simulation mode" on page 536), type **F**.

To allow all activity by this user without any checks or logging, type **S**.

**Check (in FW) Native auth**

To allow the user to access all native objects, without checking native security rules for the object, type **1**.

To reject all attempts by the user to access IFS objects, without checking native security rules for the object,, type **2**.

To check all attempts by the user to access IFS objects against Firewall native security rules, type **3**.

**Check (in FW) IFS auth**

To allow the user to access all IFS objects, without checking IFS security rules for the object, type **1**.

To reject all attempts by the user to access IFS objects, without checking IFS security rules for the object,, type **2**.

To **check** all attempts by the user to access IFS objects against Firewall IFS security rules, type **3**.

## Adding Firewall Settings for a User based on Services

To **create filters based on services** (such as FTP, SQL, NBD, or DDM), enter **1** in the **Selection** field of the **Add User Security** screen, shown in "Adding Firewall Settings for a User" on page 229 (***STRFW > 3 > 1, F6***).

The **Add User to Server Security** screen appears.

```
                        Add User to Server Security

User . . . . . .  PLONY
                                                      Subset . . . .  _
>> Set: 1=Allow (+), 2=Reject, 3=By Verb (V), 4=Allow+Skip object check (S)
   Log: 1=No, 2=Rejects, 4=All, blank=By server setting
       Server     User            Supports
Server Control    Allowed Set Log Verbs
FILTFR No         Yes      _          Original File Transfer Function
SSHD   No         Yes      _          SSH,SFTP,SCP- Secured CMD Entry,FTP,COPY
FTPLOG No         Yes      _          FTP Server Logon
FTPSRV No         Yes      _      Yes FTP Server-Incoming Rqst Validation
FTPCLN Usr>srv    Yes      _      Yes FTP Client-Outgoing Rqst Validation
REXLOG No         Yes      _          REXEC Server Logon
REXEC  No         Yes      _          REXEC Server Request Validation
RMTSQL No         Yes      _      Yes Original Remote SQL Server
SQLENT No         Yes      _          Database Server - entry
SQL    Full       Yes      _      Yes Database Server - SQL access & Showcase
DBOPEN No         Yes      _      Yes Open Database
                                                                    More...
F3=Exit    F4=Prompt    F8=Print    F9=Object security    F10=Logon security
F11=Modify Set/Log      F12=Cancel                        F23=Reject all
```

Each line of the main part of the screen contains the settings for a single service. It includes these fields:

**Server**

The short name of the server.

**Server Control**

The current general settings for the service, as set in "Setting Firewall Rules for Servers" on page 54.

**User Allowed**

The setting for the user or group and server. It can be set to:

- **Yes**: Accept requests
- **No**: Reject requests
- **By Verb**: The response depends on the verb used (such as **DELETE**, **INSERT**, **COPY**), determined by entering **3** in the **Set** column.

**Set**

Type one of the following values and press Enter to change the setting for this user or group and server. (To toggle the entry prompt between the **Set** and **Log** fields, press the F11 key.)

- **1**. Allow all requests
- **2**. Reject all requests
- **3**. If the **Verb Support** field is set to **Yes**, establish settings based on verbs that the server interprets. The Modify Server Verb Authority screen appears, as shown in "Modifying Firewall Settings for a User based on Server Verbs" on page 253.
- **4**. Allow all requests, skipping object checks.

**Log**

Type one of the following values to set whether Firewall logs requests to this server. (To toggle the entry prompt between the **Set** and **Log** fields, press the F11 key.)

- Blank: No change
- **1**: None
- **2**: Rejects
- **4**: All

**Supports Verbs**

If the server accepts distinct verbs, this shows **Yes**, and you can enter settings for the verbs by entering **3** in the **Set** column.

**(unlabeled)**

A free-form text description of the server

To **establish settings based on verbs** for a server that shows **Yes** in its **Verb Support** column, enter **3** in the **Set** column. The **Modifying Server Verb Authority** appears, as shown in "Modifying Firewall Settings for a User based on Server Verbs" on page 253.

To **reject** all requests on all servers, press the **F23** key (**Shift+F11**).

## Adding Firewall Settings for a User based on Server Verbs

For some services such as FTP and SQL, you can set Firewall to respond in different ways to different verbs for the same server. For example, you can set an FTP server to accept *LIST* commands but reject *DELETE* commands.

To **add settings based on verbs**, enter **3** in the **Set** field for a server for which the **Supports Verbs** column is set to **Yes** on the **Add User to Server Security** screen (as shown in "Adding Firewall Settings for a User based on Services" on page 232).

The **Modify Server Verb Authority** screen appears.

```
                        Modify Server Verb Authority

User . . . . . .  PLONY
Server . . . . . .  FTP Server-Incoming Rqst Validation

Type choices, press Enter.
 1=Accept  2=Reject  3=Skip (Allow, no log)  4=By verb (of the SQL server)

     Current
Opt  Status   Verb
 _   Accept   Put - Send file from AS/400 to Client
 _   Accept   Get - Receive file from Client to AS/400
 _   Accept   DELETE - Delete file
 _   Accept   RNFR, RNTO - Rename file
 _   Accept   MKD, XMDK - Directory/Library creation
 _   Accept   RMD, XRMD - Directory/Library deletion
 _   Accept   RCMD - Run CL command
 _   Accept   Set current directory
 _   Accept   LIST, NLIST - List files
                                                                      Bottom

F3=Exit                         F12=Cancel
```

Each line shows the settings for a single verb for the server, including the **Verb** itself, a text description of the verb, and its **Current Status**.

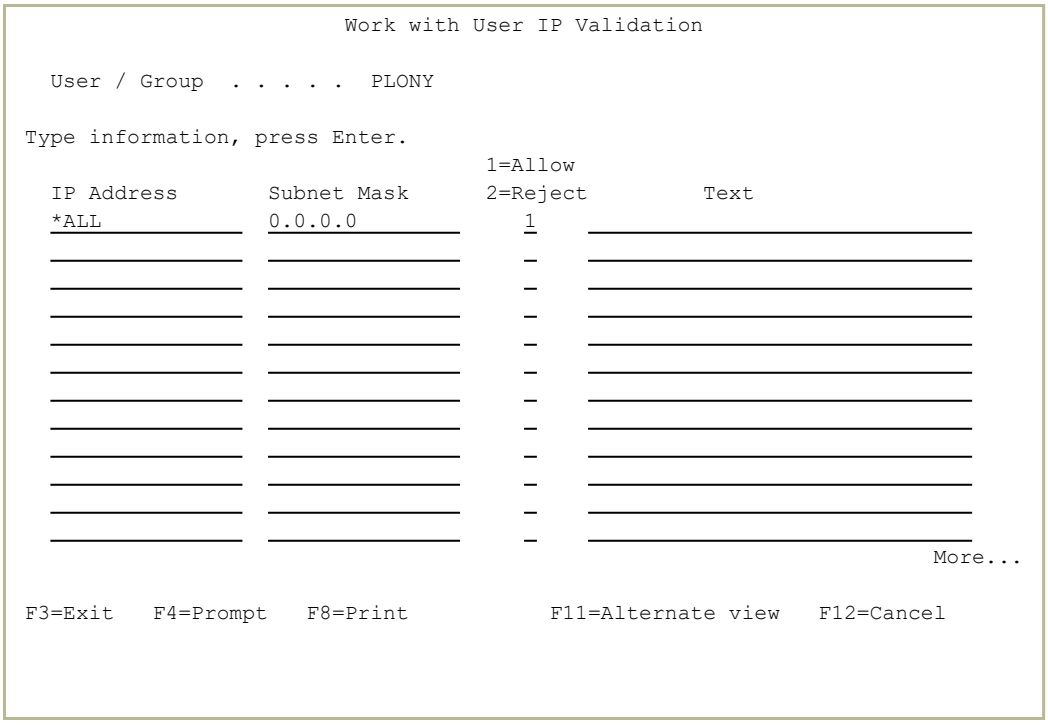
Enter one of these values in the **Opt** field to change that status:

1. **Accept** the activity using that verb.
2. **Reject** the activity using that verb.
3. Accept the activity using that verb, but **skip** both checking its validity and logging it.
4. For the **DBOPEN** server only: use the value for the corresponding SQL verb.

## Adding Firewall Settings for a User based on IP Addresses

To **add or modify Firewall settings for a user based on IP Addresses**, enter **2** in the **Selection** field of the **Add User Security** screen, shown in "Adding Firewall Settings for a User" on page 229 (STRFW **> 3 > 1, F6, Selection: 2**)

The **Work with User IP Validation** screen appears:




For each range of IP addresses, the screen shows:

**IP Address**

The IP address for the range

**Subnet Mask**

The subnet mask for the range of addresses. Press the **F4** key to see possible values.

**1=Allow 2=Reject**

Set this field to

1. to **allow** activity to and from these IP addresses
2. to **reject** activity to and from these IP addresses

**Text**

A free-form text description of the address range.

For an **alternate view**, showing the numerical range of addresses below the **IPv6 Address** field, press the **F11** key.

To **print** the information from the screen, press the **F8** key.

## Adding Firewall Settings for a User based on IPv6 Addresses

To **add Firewall settings for a user based on IPv6 Addresses**, enter **3** in the **Selection** field of the **Add User Security** screen, shown in "Adding Firewall Settings for a User" on page 229 (STRFW **> 3 > 1, F6, Selection: 3**).

The **Work with User IPv6 Validation** screen appears:

```
                        Work with User IPv6 Validation

Type information, press Enter.    ('Y'/'N' are not saved until pressing Enter)
  User / Group  . . . . .  PLONY
                                              Prfx 1=Alw
IPv6 Address                                  Lngh 2=Rjc Text
*ALL                                           ___   1   ____________________
1234::0056::                                   128   1   ____________________
                                               ___   _   ____________________
                                               ___   _   ____________________
                                               ___   _   ____________________
                                               ___   _   ____________________
                                               ___   _   ____________________
                                               ___   _   ____________________
                                               ___   _   ____________________
                                               ___   _   ____________________
                                               ___   _   ____________________
                                               ___   _   ____________________
                                                                      More...


F3=Exit       F8=Print    F11=Alternate view     F12=Cancel
```

For each range of IPv6 addresses, the screen shows:

**IPv6 Address**

The IPv6 address for the range, or ***ALL**, representing all addresses that are not otherwise listed.

**Prfx Lngh**

The prefix length for the range of addresses.

**1=Allow 2=Reject**

Set this field to

1. to allow activity to and from this IP address
2. to reject activity to and from this IP address

**Text**

A free-form text description of the address range.

For an alternate view, showing the numerical range of addresses below the **Text** field, press the F11 key.

To print the information from the screen, press the F8 key.

## Adding Firewall Settings for a User based on Sign-On Devices

To **add Firewall settings for a user based on sign-on Devices**, enter **4** in the **Selection** field of the **Add User Security** screen, shown in "Adding Firewall Settings for a User" on page 229 (*STRFW* **> 3 > 1, F6, Selection: 4**).

The **Work with Sign-On Device Validation** screen appears:

```
                    Work with Sign-On Device Validation


  User / Group  . . . . . .  PLONY


Type information, press Enter.
  Y=Yes

  Device*      Allow
  *ALL          Y
  _________     _
  _________     _
  _________     _
  _________     _
  _________     _
  _________     _
  _________     _
  _________     _
  _________     _                                                  More...
F3=Exit     F8=Print                                  F12=Cancel
```

For each device, the screen shows:

**Device***

The name of the device. This can be a generic name, indicating a set of devices, or ***ALL**, representing all devices not otherwise listed.

**Allow**

If set to **Y**, access from these devices is allowed. If left blank, access is rejected.

To **print** the information from the screen, press the **F8** key.

## Adding a User to Firewall Groups

To add a user to Firewall groups,

- type **5** in the **Selection** field of the **Add User Security** screen, shown in "Adding Firewall Settings for a User" on page 229 (*STRFW* **> 3 > 1, F6, Selection: 5**) or
- type **5** in the **Selection** field of the **Modify User Security** screen, shown in "Modifying Firewall Settings for a User" on page 246 (*STRFW* **> 3 > 1, Opt: 1, Selection: 5**)

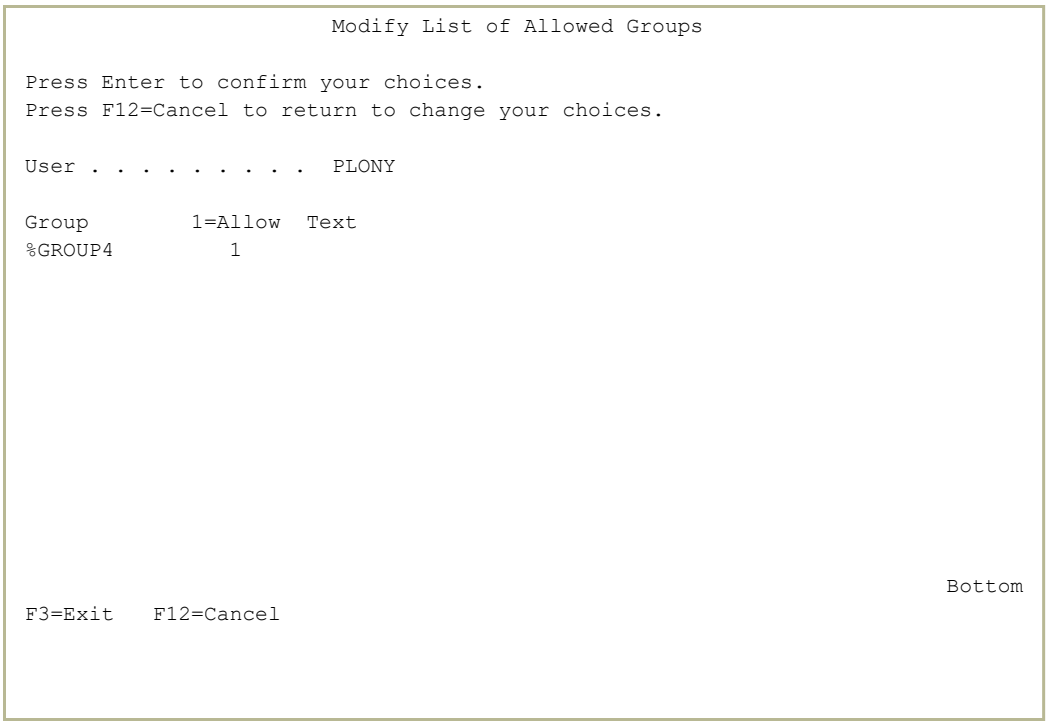
The **Define Allowed Groups** screen appears.

```
                          Define Allowed Groups

User . . . . . .  AEQWE

Type options, press Enter.
  1=Allow

Opt  Group
                Applications
 _   %#ACCOUNT
 _   %#GUI
 _   %#PGM
 _   %#SALES
 _   %#TEST2
 _   %#TEST3
                Locations
 _   %@FLOOR1
 _   %@FLOOR2
 _   %@GUI
                User Groups
                                                                      More...
F3=Exit   F12=Cancel
```

The **Groups** column lists Firewall groups that include the user, broken out into **Applications**, **Locations**, and other **User Groups**.

To **include the user in a group**, type **1** in the **Opt** column for that group.

The **Modify List of Allowed Groups** screen appears.




To **confirm** your choices, press Enter.
To **return** to the Define Allowed Groups screen to change your choices, press the **F12** key.

## Adding Firewall Settings for a User to Assume Different Authority for a Server

To **add Firewall settings for a user to assume a different user's authority** for specified servers, enter **6** in the **Selection** field of the **Add User Security** screen, shown in "Adding Firewall Settings for a User" on page 229 (*STRFW* **> 3 > 1, F6, Selection: 6**).

The **Work with Alternative Users** screen appears:

```
                        Work with Alternative Users

  User . . . . . . . . . . EXAM
  You can define an alternative way of checking object authority. This is done
  by service. Specify a "User" whose authority (without groups) will be
  checked in Firewall. If Swap=Y, this extends to system authority ches..
              Check per   Swap user
  Server      "User"       (Y-Yes)
  FTPSRV      __________      _      FTP Server-Incoming Rqst Validation
  FTPCLN      __________      _      FTP Client-Outgoing Rqst Validation
  REXEC       __________      _      REXEC Server Request Validation
  RMTSQL      __________      _      Original Remote SQL Server
  SQL         __________      _      Database Server - SQL access & Show
  NDB         __________      _      Database Server - data base access
  RMTSRV      __________      _      Remote Command/Program Call
  FILSRV      __________      _      File Server
  DTAQ        __________      _      Data Queue Server
  FILTFR      __________      _      Original File Transfer Function


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

The screen shows a list of servers known to Firewall. Each line contains a short Server name and longer text description for the server, and the following fields:

**Check per "User"**

The username of another user. If the user exists, the current user assumes the object authority settings for that user when working with that server within iSecurity. To see a list of possible users, press the **F4** key.

**Swap User (Y-Yes)**

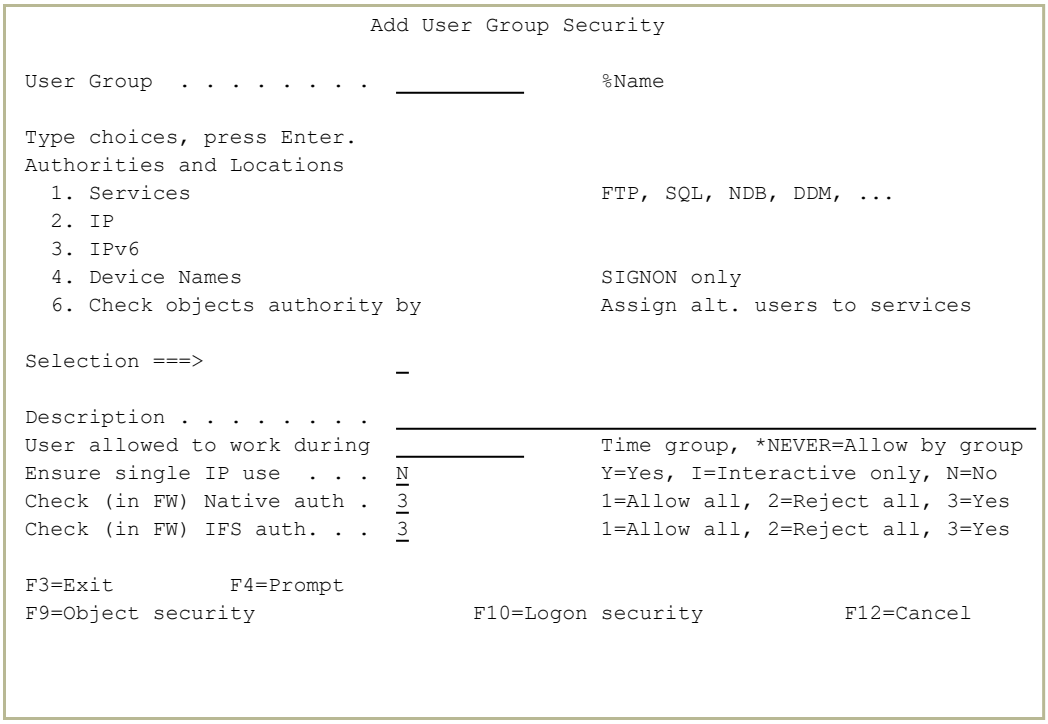
If this is set to **Y**, any activity by that user on the server is reported to the operating system as being by the user named in the **Check per "User"** field. If the user does not exist, the attempt to swap object authorities fails.

Otherwise, while the user assumes the authority of the user listed in the **Check per "User"** field, the activity is reported and logged as being by the current user.

## Adding Firewall Settings for a Group

To **add Firewall settings for a group**, press the **F7** key in the **Work with User Security** screen, shown in "Setting Firewall Rules for Users and Groups" on page 226 (***STRFW > 3 > 1***).

The **Add User Group Security** screen appears.




Type the group's name in the **User Group** field. To select a group from a list, press the **F4** key. The group's name must begin with a percent sign, as in **%NAME**.

Through the options in the **Authorities and Locations** list, you can create specific filters for the group that can override the server's general settings. A close-arrow ("**>**") before an item shows that its settings have already been changed from the default to a new value.

**1. Services**

To create filters based on services (such as **FTP**, **SQL**, **NBD**, or **DDM**), enter **1** in the **Selection** field. The **Add User to Server Security** screen appears, as shown in "Adding Firewall Settings for a User based on Services" on page 232.

**2. IP**

To create filters based on IP addresses, enter **2** in the **Selection** field. The Work with User IP Validation screen appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IP Address" on page 189.

**3. IPv6**

To create filters based on IPv6 addresses, enter **3** in the **Selection** field. The Work with User IPv6 Validation screen appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IPv6 Address" on page 208.

**4. Device name**

To create filters based on SNA system names, enter **4** in the **Selection** field. The Work with Sign-On Device Validation screen appears, as shown in "Adding a Firewall Rule for Incoming Activity by Remote System Names" on page 184.

**6. Chg/Swap users for obj authority**

To have the user assume the authority of a different user when using particular servers, enter **6** in the **Selection** field. The Work with Alternative Users screen appears, as shown in "Adding Firewall Settings for a User to Assume Different Authority for a Server" on page 241.

The fields below these control other aspects of user security:

**Description**

A free-form text description of the group

**User allowed to work during**

To limit the group to working within a specified range of hours of the day or days of the week, enter the name of a time group with those time settings (as shown in "Defining Time Groups" on page 504).

To use the default settings for the server, enter ***NEVER**.

**Ensure single IP use**

To limit the group to working from one IP address at a time, type **Y**. The group may have multiple sessions open at a time, but they

must all be from the same IP address.

To limit the group's interactive sessions to one IP address at a time, type **I**. This does not affect the group's batch jobs.

To allow the group to work from multiple IP addresses simultaneously, type **N**.

**Check (in FW) Native auth**

To allow the group to access all native objects, type **1**.

To reject all attempts by the group to access native objects,, type 2.

To check all attempts by the group to access native objects against Firewall settings set elsewhere, type 3.

**Check (in FW) IFS auth**

To allow the group to access all IFS objects, type **1**.

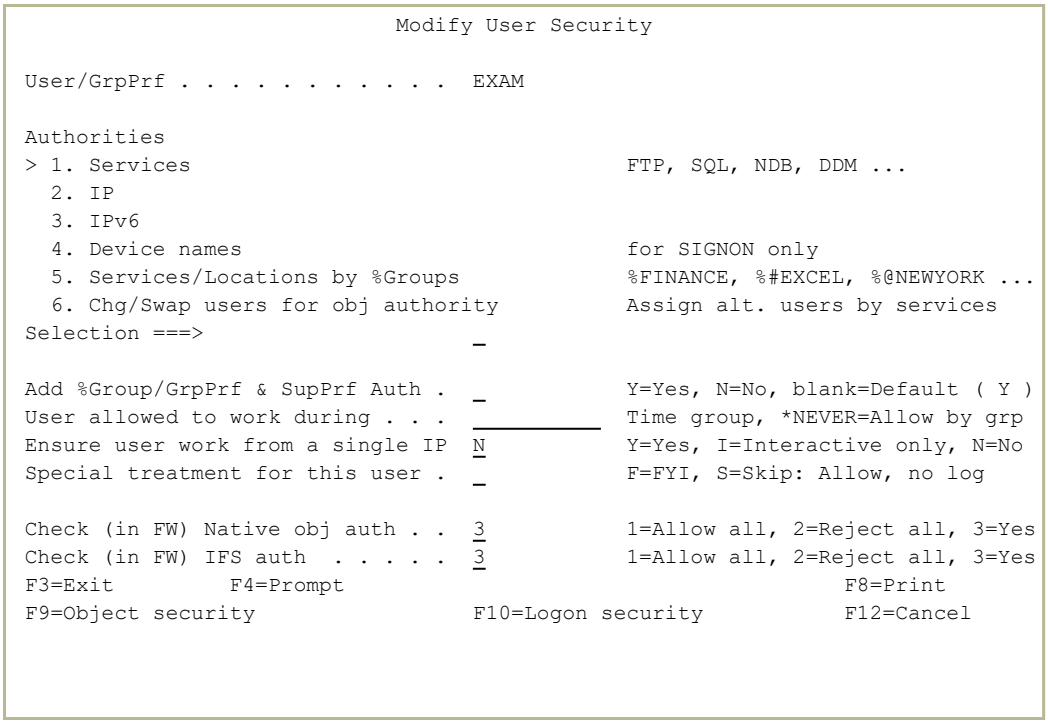
To reject all attempts by the group to access IFS objects,, type **2**.

To check all attempts by the group to access IFS objects against Firewall settings set elsewhere, type **3**.

## Modifying Firewall Settings for a User

To **modify Firewall settings for a user**, enter **1** in the **Opt** column for the user on the **Work with User Security** screen, shown in "Setting Firewall Rules for Users and Groups" on page 226 (***STRFW > 3 > 1***).

The **Modify User Security** screen appears.




The read-only **User/GrpPrf** field shows the user name.

Through the options in the **Authorities** list, you can create specific filters for a user that can override the server's general settings. A close-arrow ("**>**") before an item shows that its settings have already been changed from the default to a new value.

### 1. Services

To create filters based on services (such as **FTP**, **SQL**, **NBD**, or **DDM**), enter **1** in the **Selection** field. The **Add User to Server Security** screen appears, as shown in "Adding Firewall Settings for a User based on Services" on page 232.

**2. IP**

To create filters based on IP addresses, enter **2** in the **Selection** field. The Work with User IP Validation screen appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IP Address" on page 189.

**3. IPv6**

To create filters based on IPv6 addresses, enter **3** in the **Selection** field. The Work with User IPv6 Validation screen appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IPv6 Address" on page 208.

**4. Device name**

To create filters based on SNA system names, enter **4** in the **Selection** field. The Work with Sign-On Device Validation screen appears, as shown in "Adding a Firewall Rule for Incoming Activity by Remote System Names" on page 184.

**5. Services/Locations by %Groups**

You can create groups of users based on applications that they use, locations in which they work, or other criteria. To add members to these group or to remove them, enter **5** in the **Selection** field. The Define Allowed Groups screen appears, as shown in "Adding a User to Firewall Groups" on page 239.

**6. Chg/Swap users for obj authority**

To have the user assume the authority of a different user when using particular servers, enter **6** in the **Selection** field. The Work with Alternative Users screen appears, as shown in "Adding Firewall Settings for a User to Assume Different Authority for a Server" on page 241.

These options control more aspects of the user's authority:

**Add %Group/GrpPrf & SupPrf Auth**

To add authority settings from the group that include this user, type **Y**.

To prevent adding authority settings from the groups that include this user, type **N**,

To use the default settings, as defined in "Setting Additional Definitions for Firewall" on page 34, leave the field blank.

**User allowed to work during**

To limit the user to working within a specified range of hours of the day or days of the week, enter the name of a time group with those time settings (as shown in "Defining Time Groups" on page 504).

To use the default settings for the server, enter ***NEVER**.

**Ensure single IP use**

To limit the user to working from one IP address at a time, type **Y**. The user may have multiple sessions open at a time, but they must all be from the same IP address.

To limit the user's interactive sessions to one IP address at a time, type **I**. This does not affect the user's batch jobs.

To allow the user to work from multiple IP addresses simultaneously, type **N**.

**Special treatment for this user**

To handle all the user's activity in FYI mode (as shown in "Running Firewall in FYI Simulation mode" on page 536), type **F**.

To allow all activity by this user without any checks or logging, type **S**.

**Check (in FW) Native auth**

To allow the user to access all native objects, without checking native security rules for the object, type **1**.

To reject all attempts by the user to access IFS objects, without checking native security rules for the object,, type **2**.

To check all attempts by the user to access IFS objects against Firewall native security rules, type **3**.

**Check (in FW) IFS auth**

To allow the user to access all IFS objects, without checking IFS security rules for the object, type **1**.

To **reject** all attempts by the user to access IFS objects, without checking IFS security rules for the object,, type **2**.

To **check** all attempts by the user to access IFS objects against Firewall IFS security rules, type **3**.

## Modifying Firewall Settings for a User or Group based on Services

To **create filters based on services** (such as FTP, SQL, NBD, or DDM), enter **1** in the **Selection** field of the **Modify User Security** screen, shown in "Modifying Firewall Settings for a User" on page 246 (*STRFW* **> 3 > 1, 1**).

The **Modify User to Server Security** screen appears:

```
                      Modify User to Server Security

User . . . . . .  EXAM
                                                Subset . . . .  _________
>> Set: 1=Allow (+), 2=Reject, 3=By Verb (V), 4=Allow+Skip object check (S)
   Log: 1=No, 2=Rejects, 4=All, blank=By server setting
       Server     User            Supports
Server Control    Allowed Set Log Verbs
FILTFR No         Yes       _           Original File Transfer Function
SSHD   No         Yes       _           SSH,SFTP,SCP- Secured CMD Entry,FTP,COPY
FTPLOG No         Yes       _           FTP Server Logon
FTPSRV No         Yes       _       Yes FTP Server-Incoming Rqst Validation
FTPCLN No         Yes       _       Yes FTP Client-Outgoing Rqst Validation
REXLOG No         Yes       _           REXEC Server Logon
REXEC  No         Yes       _           REXEC Server Request Validation
RMTSQL No         Yes       _       Yes Original Remote SQL Server
SQLENT No         Yes       _           Database Server - entry
SQL    Allow      By verb   _       Yes Database Server - SQL access & Showcase
DBOPEN No         Yes       _       Yes Open Database
                                                                    More...
F3=Exit    F4=Prompt    F8=Print    F9=Object security    F10=Logon security
F11=Modify Set/Log      F12=Cancel                        F23=Reject all
```

Each line of the main part of the screen contains the settings for a single service. It includes these fields:

**Server**

The short name of the server.

**Server Control**

The current general settings for the service, as set in "Setting Firewall Rules for Servers" on page 54.

**User Allowed**

The setting for the user or group and server. It can be set to:

- **Yes**: Accept requests
- **No**: Reject requests
- **By Verb**: The response depends on the verb used (such as **DELETE**, **INSERT**, **COPY**), determined by entering **3** in the **Set** column.

**Set**

Type one of the following values and press Enter to change the setting for this user or group and server. (To toggle the entry prompt between the **Set** and **Log** fields, press the F11 key.)

- **1**. Allow all requests
- **2**. Reject all requests
- **3**. If the **Verb Support** field is set to **Yes**, establish settings based on verbs that the server interprets. The Modify Server Verb Authority screen appears, as shown in "Modifying Firewall Settings for a User based on Server Verbs" on page 253.
- **4**. Allow all requests, skipping object checks.

**Log**

Type one of the following values to set whether Firewall logs requests to this server. (To toggle the entry prompt between the **Set** and **Log** fields, press the F11 key.)

- Blank: No change
- **1**: None
- **2**: Rejects
- **4**: All

**Supports Verbs**

If the server accepts distinct verbs, this shows **Yes**, and you can enter settings for the verbs by entering **3** in the **Set** column.

**(unlabeled)**

A free-form text description of the server

To establish settings based on verbs for a server that shows **Yes** in its **Verb Support** column, enter **3** in the **Set** column. The Modifying Server Verb Authority appears, as shown in "Modifying Firewall Settings for a User based on Server Verbs" on the facing page.

To reject all requests on all servers, press the **F23** key (**Shift+F11**).

# Modifying Firewall Settings for a User based on Server Verbs

For some services such as FTP and SQL, you can set Firewall to respond in different ways to different verbs for the same server. For example, you can set an FTP server to accept *LIST* commands but reject *DELETE* commands.

To **modify settings based on verbs**, enter **3** in the **Set** field for a server for which the **Verb Support** column is set to **Yes** on the **Modify User Security** screen (as shown in "Modifying Firewall Settings for a User or Group based on Services" on page 250).

The **Modify Server Verb Authority** screen appears.

```
                        Modify Server Verb Authority

User . . . . . .  PLONY
Server . . . . . .  FTP Server-Incoming Rqst Validation

Type choices, press Enter.
 1=Accept  2=Reject  3=Skip (Allow, no log)  4=By verb (of the SQL server)

     Current
Opt  Status   Verb
 _   Accept   Put - Send file from AS/400 to Client
 _   Accept   Get - Receive file from Client to AS/400
 _   Accept   DELETE - Delete file
 _   Accept   RNFR, RNTO - Rename file
 _   Accept   MKD, XMDK - Directory/Library creation
 _   Accept   RMD, XRMD - Directory/Library deletion
 _   Accept   RCMD - Run CL command
 _   Accept   Set current directory
 _   Accept   LIST, NLIST - List files
                                                                        Bottom

F3=Exit                         F12=Cancel
```

Each line shows the settings for a single verb for the server, including the **Verb** itself, a text description of the verb, and its **Current Status**.

Enter one of these values in the **Opt** field to change that status:

1. **Accept** the activity using that verb.
2. **Reject** the activity using that verb.
3. Accept the activity using that verb, but **skip** both checking its validity and logging it.

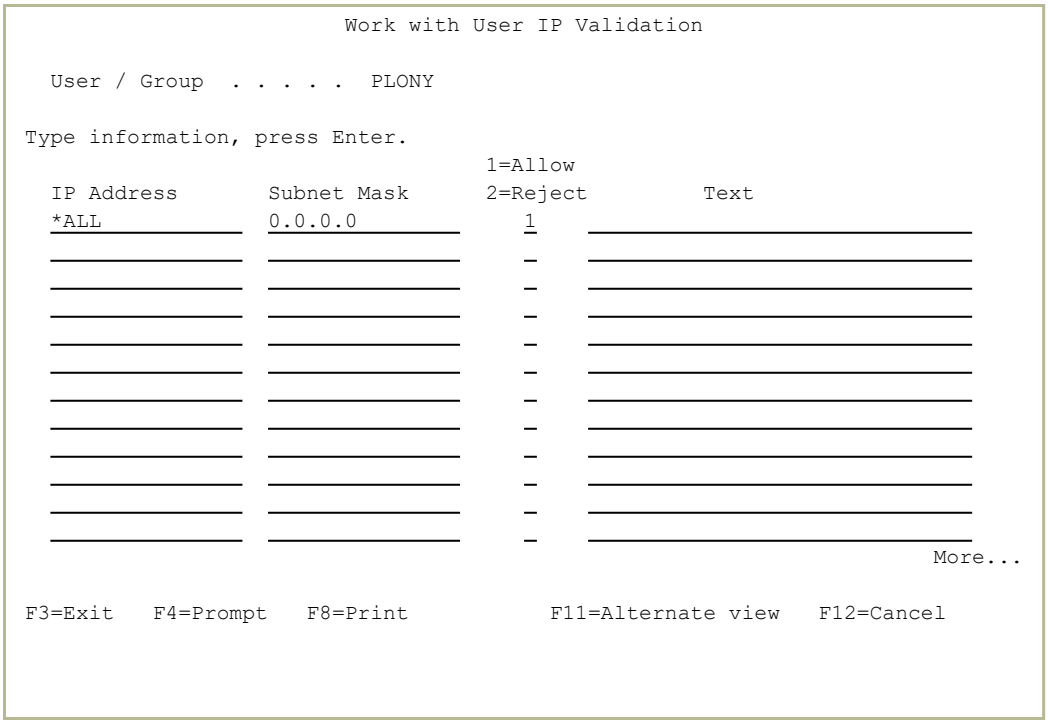
4. For the **DBOPEN** server only: use the value for the corresponding SQL verb.

# Modifying Firewall Settings for a User or Group based on IP Addresses

To **modify Firewall settings for a user** based on IP Addresses, type **2** in the **Selection** field of the **Modify User Security** screen, shown in "Modifying Firewall Settings for a User" on page 246 (STRFW **> 3 > 1, Opt: 1, Selection: 2**)

To **modify Firewall settings for a group** based on IP Addresses, type **2** in the **Selection** field of the **Modify User Group Security** screen, shown in "Modifying Firewall Settings for a Group" on page 264 (STRFW **> 3 > 1, Opt: 1, Selection: 2**)

The **Work with User IP Validation** screen appears:




For each range of IP addresses, the screen shows:

**IP Address**

The IP address for the range

**Subnet Mask**

The subnet mask for the range of addresses. Press the **F4** key to see possible values.

**1=Allow 2=Reject**

Set this field to

1. to allow activity to and from these IP addresses
2. to reject activity to and from these IP addresses

**Text**

A free-form text description of the address range.

For an alternate view, showing the numerical range of addresses below the **IPv6 Address** field, press the F11 key.

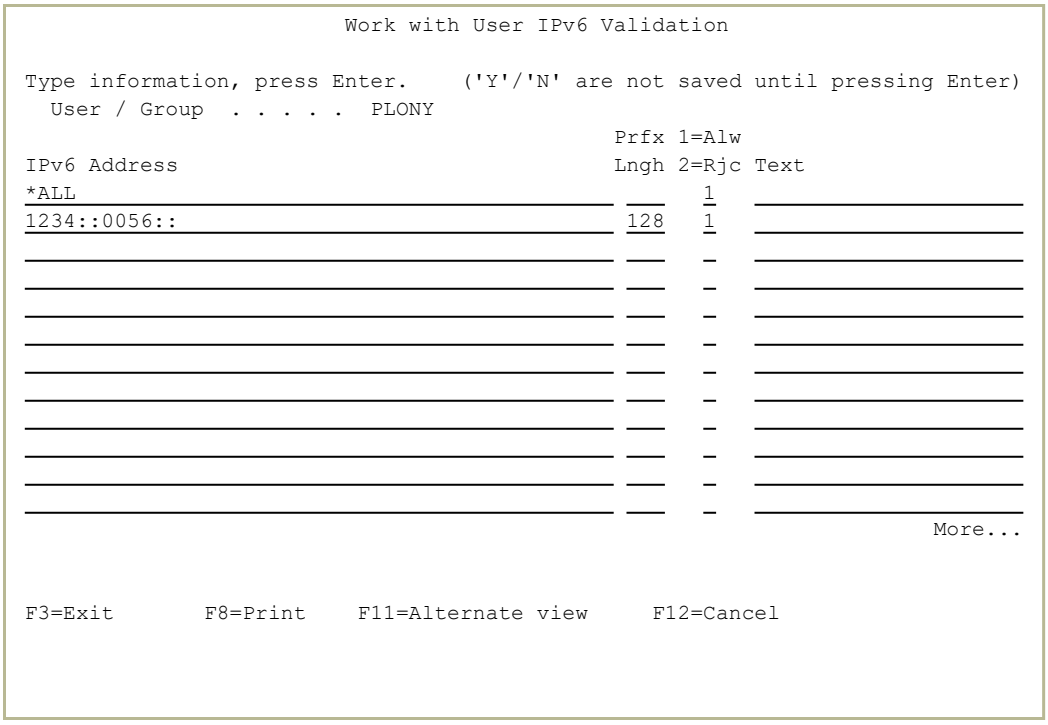
To print the information from the screen, press the F8 key.

# Modifying Firewall Settings for a User or Group based on IPv6 Addresses

To **modify Firewall settings for a user** based on IPv6 Addresses, enter **3** in the **Selection** field of the **Modify User Security** screen, shown in "Modifying Firewall Settings for a User" on page 246 (*STRFW* **> 3 > 1, Opt: 1, Selection: 3**).

To **modify Firewall settings for a group** based on IPv6 Addresses, enter **3** in the **Selection** field of the **Modify User Group Security** screen, shown in "Modifying Firewall Settings for a Group" on page 264 (*STRFW* **> 3 > 1, Opt: 1, Selection: 3**).

The **Work with User IPv6 Validation** screen appears:




For each range of IPv6 addresses, the screen shows:

**IPv6 Address**

The IPv6 address for the range, or ***ALL**, representing all addresses that are not otherwise listed.

**Prfx Lngh**

The prefix length for the range of addresses.

**1=Allow 2=Reject**

Set this field to

1. to allow activity to and from this IP address
2. to reject activity to and from this IP address

**Text**

A free-form text description of the address range.

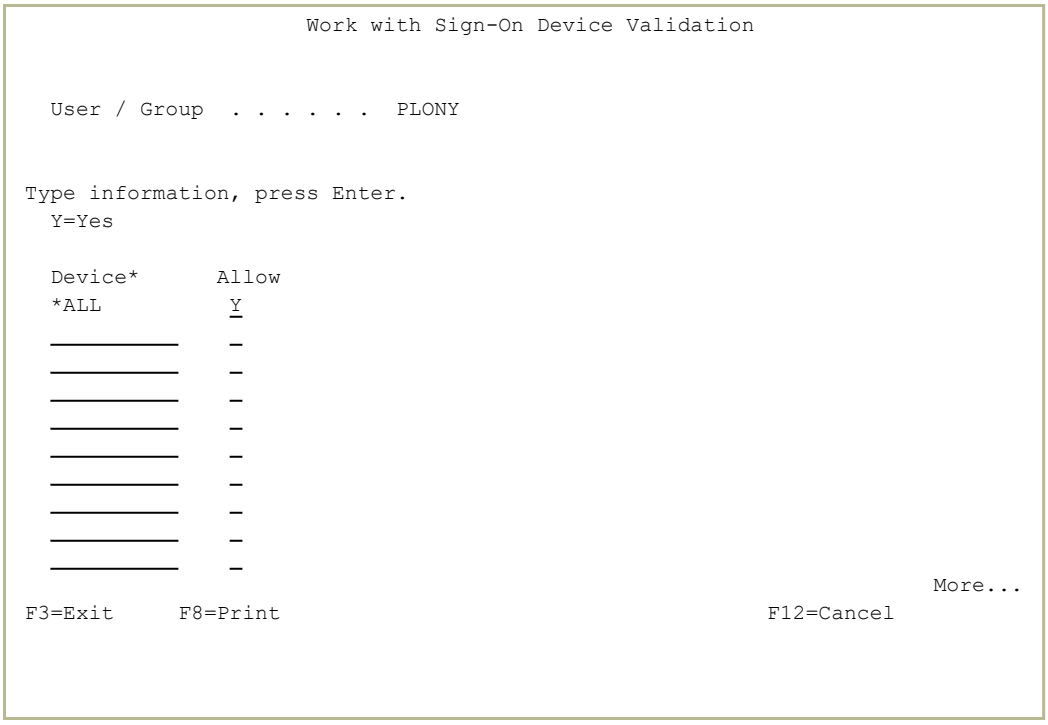
For an alternate view, showing the numerical range of addresses below the **Text** field, press the F11 key.

To print the information from the screen, press the F8 key.

## Modifying Firewall Settings for a User based on Sign-On Devices

To **modify Firewall settings for a user based on sign-on devices**, enter **4** in the **Selection** field of the **Modify User Security** screen, shown in "Modifying Firewall Settings for a User" on page 246 (*STRFW* **> 3 > 1, Opt: 1, Selection: 4**).

The **Work with Sign-On Device Validation** screen appears:




For each device, the screen shows:

**Device***

The name of the device. This can be a generic name, indicating a set of devices, or ***ALL**, representing all devices not otherwise listed.

**Allow**

If set to **Y**, access from these devices is allowed. If left blank, access is rejected.

To **print** the information from the screen, press the **F8** key.

## Removing a User from Firewall Groups

To remove a user from Firewall groups,

- enter **5** in the **Selection** field of the Add User Security screen, shown in "Adding Firewall Settings for a User" on page 229 (*STRFW* **> 3 > 1, F6, Selection: 5**) or
- enter **5** in the **Selection** field of the Modify User Security screen, shown in "Modifying Firewall Settings for a User" on page 246 (*STRFW* **> 3 > 1, Opt: 1, Selection: 5**)

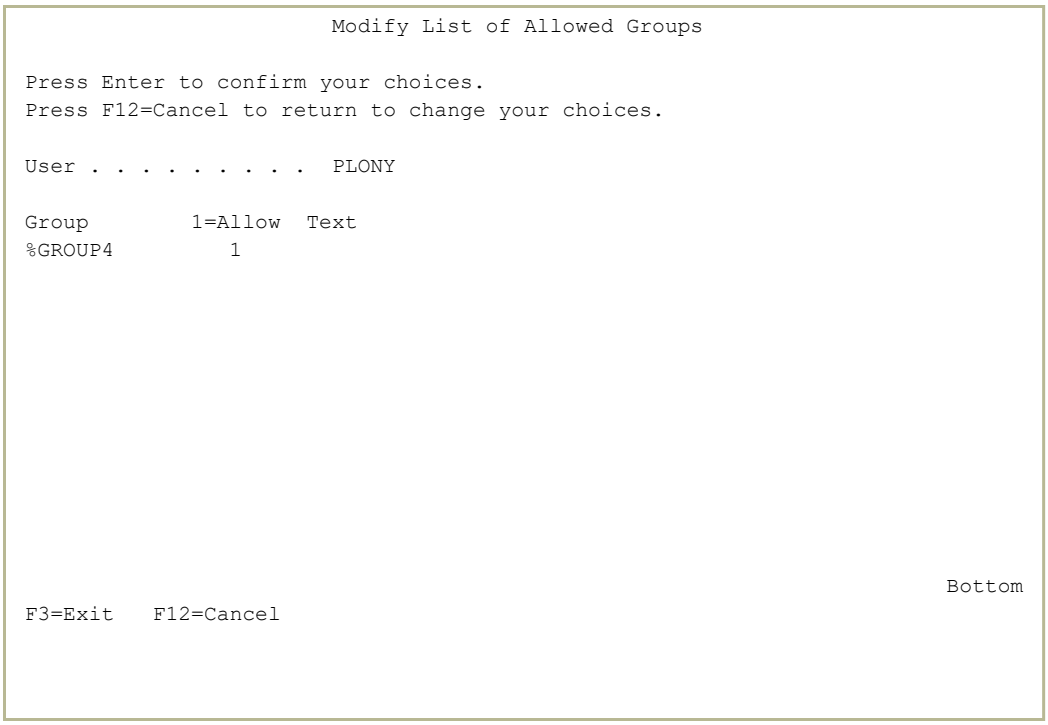
The Define Allowed Groups screen appears.

```
                          Define Allowed Groups

User . . . . . .  AEQWE

Type options, press Enter.
  1=Allow

Opt  Group
                Applications
 _   %#ACCOUNT
 _   %#GUI
 _   %#PGM
 _   %#SALES
 _   %#TEST2
 _   %#TEST3
                Locations
 _   %@FLOOR1
 _   %@FLOOR2
 _   %@GUI
                User Groups
                                                                      More...
F3=Exit    F12=Cancel
```

The **Groups** column lists Firewall groups that include the user, broken out into **Applications**, **Locations**, and other **User Groups**.

To remove the user from the group, clear the **Opt** field for that group, leaving it blank.

The Modify List of Allowed Groups screen appears.




To **confirm** your choices, press Enter.
To **return** to the Define Allowed Groups screen to change your choices, press the **F12** key.

# Modifying Firewall Settings for a User to Assume Different Authority for a Server

To **add or modify Firewall settings** for a user to assume a different user's authority for specified servers, enter **4** in the **Selection** field of the **Modify User Security** screen, shown in "Modifying Firewall Settings for a User" on page 246 (*STRFW* **> 3 > 1, Opt: 1, Selection: 6**).

The **Work with Alternative Users** screen appears:

```
                        Work with Alternative Users

  User . . . . . . . . . . EXAM
  You can define an alternative way of checking object authority. This is done
  by service. Specify a "User" whose authority (without groups) will be
  checked in Firewall. If Swap=Y, this extends to system authority ches..
              Check per   Swap user
  Server      "User"        (Y-Yes)
  FTPSRV      __________      _      FTP Server-Incoming Rqst Validation
  FTPCLN      __________      _      FTP Client-Outgoing Rqst Validation
  REXEC       __________      _      REXEC Server Request Validation
  RMTSQL      __________      _      Original Remote SQL Server
  SQL         __________      _      Database Server - SQL access & Show
  NDB         __________      _      Database Server - data base access
  RMTSRV      __________      _      Remote Command/Program Call
  FILSRV      __________      _      File Server
  DTAQ        __________      _      Data Queue Server
  FILTFR      __________      _      Original File Transfer Function


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

The screen shows a list of servers known to Firewall. Each line contains a short Server name and longer text description for the server, and the following fields:

**Check per "User"**

The username of another user. If the user exists, the current user assumes the authority settings for that user when working with that server within iSecurity. To see a list of possible users, press the **F4** key.

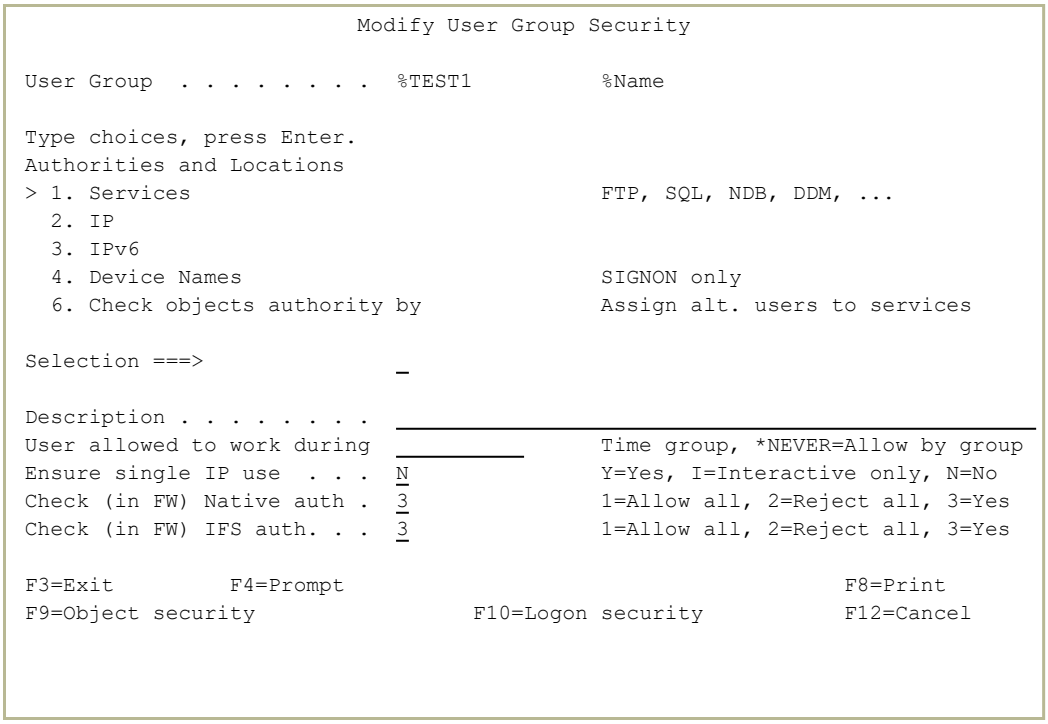
**Swap User (Y-Yes)**

If this is set to **Y**, the current user takes on the identity of that user when using that server throughout the IBM i system. Any logs of actions will show that they were performed by the alternate user, not the current user. If the user does not exist, the attempt to swap authorities fails.

## Modifying Firewall Settings for a Group

To **modify Firewall settings for a group**, enter **1** in the **Opt** column for the group on the **Work with User Security** screen, shown in "Setting Firewall Rules for Users and Groups" on page 226 (*STRFW > 3 > 1*).

The **Modify User Group Security** screen appears.




The read-only **User Group** field shows the user name.

Through the options in the **Authorities and Locations** list, you can create specific filters for the group that can override the server's general settings. A close-arrow ("**>**") before an item shows that its settings have already been changed from the default to a new value.

**1. Services**

To create filters based on services (such as **FTP**, **SQL**, **NBD**, or **DDM**), enter **1** in the **Selection** field. The **Add User to Server Security** screen appears, as shown in "Adding Firewall Settings for a User based on Services" on page 232.

**2. IP**

To create filters based on IP addresses, enter **2** in the **Selection** field. The Work with User IP Validation screen appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IP Address" on page 189.

**3. IPv6**

To create filters based on IPv6 addresses, enter **3** in the **Selection** field. The Work with User IPv6 Validation screen appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IPv6 Address" on page 208.

**4. Device name**

To create filters based on SNA system names, enter **4** in the **Selection** field. The Work with Sign-On Device Validation screen appears, as shown in "Adding a Firewall Rule for Incoming Activity by Remote System Names" on page 184.

**5. Services/Locations by %Groups**

You can create groups of users based on applications that they use, locations in which they work, or other criteria. To add members to these group or to remove them, enter **5** in the **Selection** field. The Define Allowed Groups screen appears, as shown in "Adding a User to Firewall Groups" on page 239.

**6. Check objects authority by**

To have the user assume the authority of a different user when using particular servers, type **6** in the **Selection** field and press Enter. The Work with Alternative Users screen appears, as shown in "Adding Firewall Settings for a User to Assume Different Authority for a Server" on page 241.

These options control more aspects of the group members' authority:

**Description**

A free-form text description of the group

**User allowed to work during**

To limit the group to working within a specified range of hours of the day or days of the week, enter the name of a time group with

those time settings (as shown in "Defining Time Groups" on page 504).

To use the default settings for the server, enter ***NEVER**.

**Ensure single IP use**

To limit the group to working from one IP address at a time, type **Y**. The group may have multiple sessions open at a time, but they must all be from the same IP address.

To limit the group's interactive sessions to one IP address at a time, type **I**. This does not affect the group's batch jobs.

To allow the group to work from multiple IP addresses simultaneously, type **N**.

**Check (in FW) Native auth**

To allow the group to access all native objects, type **1**.

To reject all attempts by the group to access native objects,, type 2.

To check all attempts by the group to access native objects against Firewall settings set elsewhere, type 3.

**Check (in FW) IFS auth**

To allow the group to access all IFS objects, type **1**.

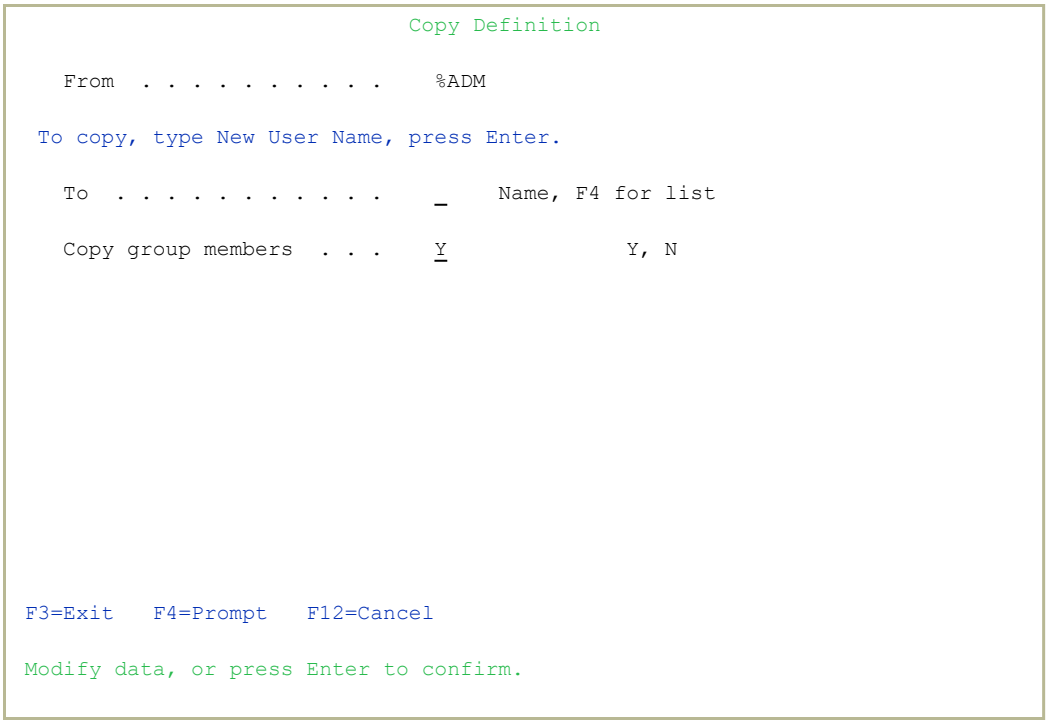
To reject all attempts by the group to access IFS objects,, type **2**.

To check all attempts by the group to access IFS objects against Firewall settings set elsewhere, type **3**.

## Copying Firewall Settings for a User or Group

To **copy the Firewall settings from one user or group to another**, enter **3** in the **Opt** field for the original user or group in the **Work with User Security** screen, shown in "Setting Firewall Rules for Users and Groups" on page 226 (*STRFW > 3 > 1*).

The **Copy Definition** screen appears.




The read-only **From** field shows the name of the original user or group.

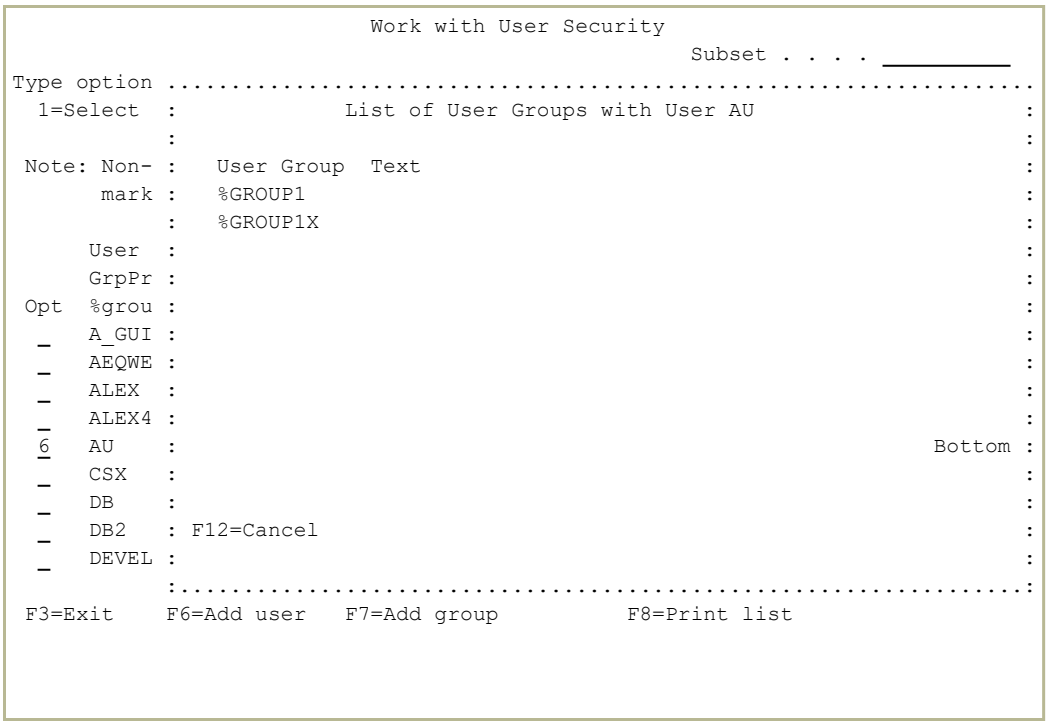
Type the name of the new user or group in the **To** field. Place the cursor in the field and press the **F4** key to select from a list.

If you are copying a list, to copy the members of the list to the new list, type **Y** in the **Copy group members field**. Otherwise, set it to **N**.

## Displaying a List of Groups that Include a User

To **display a list of Firewall groups that include a user**, enter **6** in the **Opt** field for the user in the **Work with User Security** screen, shown in "Setting Firewall Rules for Users and Groups" on page 226 (*STRFW > 3 > 1*).

The **List of User Groups with User** window appears.




The window shows the name of each group that includes the user, along with a text description of the group, if one has been entered.

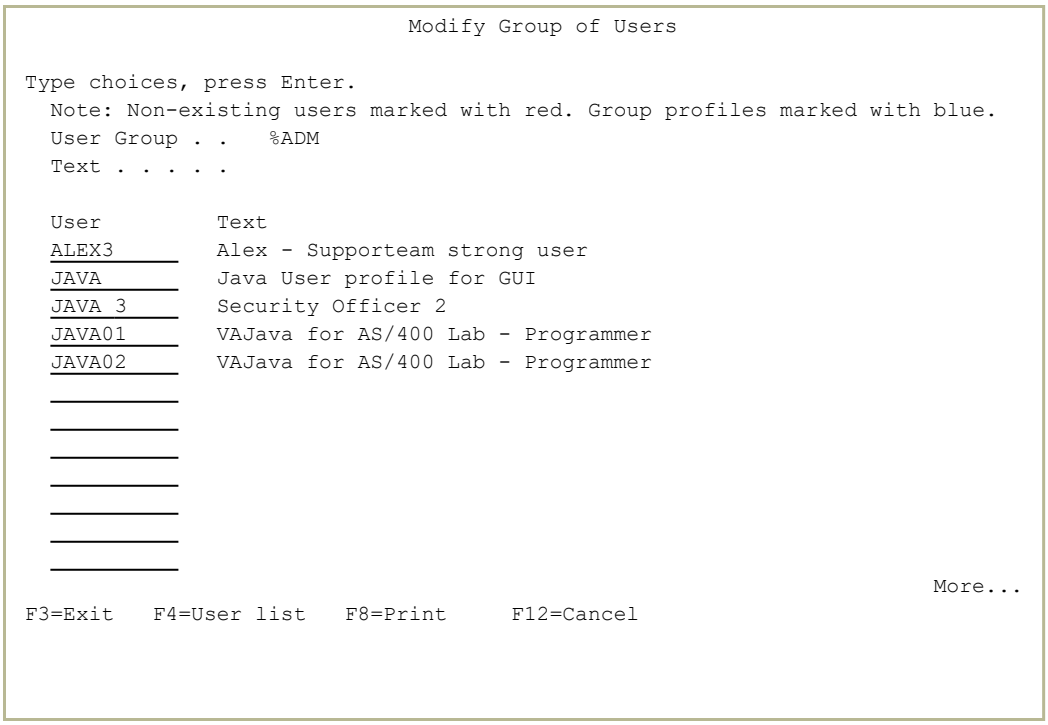
To **close the window**, press the **F12** key.

To **add or remove the user from groups**, see "Changing the Members of a Firewall Group" on the facing page.

## Changing the Members of a Firewall Group

To **add, remove, or change the members of a Firewall group**, enter **5** in the **Opt** field for the group in the **Work with User Security** screen, shown in "Setting Firewall Rules for Users and Groups" on page 226 (*STRFW > 3 > 1*).

The **Modify Group of Users** screen appears.




To **remove** a user from the group, erase the user's name from the list.

To **add** a user to the group, type the user's name in the **User** field. To select users from a list, press the **F4** key.

## Deleting Firewall Settings for a User or Group

To **delete the Firewall settings for a user or group**, enter **4** in the **Opt** field for the user or group in the **Work with User Security** screen, shown in "Setting Firewall Rules for Users and Groups" on page 226 (*STRFW > 3 > 1*).

NOTE: You may not delete settings for a group that has members. Before doing so, remove the group's members, as shown in "Changing the Members of a Firewall Group" on the previous page.

Otherwise, the **Delete User Security** screen appears.

```
                          Delete User Security
Press Enter to confirm the Delete, F12 to cancel.
User/GrpPrf . . . . . . . . . . .  AEQWE

Authorities
  1. Services                                FTP, SQL, NDB, DDM ...
  2. IP
  3. IPv6
  4. Device names                            for SIGNON only
  5. Services/Locations by %Groups           %FINANCE, %#EXCEL, %@NEWYORK ...
  6. Chg/Swap users for obj authority        Assign alt. users by services


Special treat this user activity.            S=Skip, F=FYI, blank=No chg
Add %Group/GrpPrf & SupPrf Auth .            Y=Yes, N=No, blank=Default
User allow, GrpPrf & SupPrf Auth.            Time group, *NEVER
Ensure user work from a single IP  N         Y=Yes, I=for INT only, N=No
In-product Native obj authority .  3         1=*ALLOBJ, 2=*EXCLUDE, 3=No chg
In-product IFS obj authority  . .  3         1=*ALLOBJ, 2=*EXCLUDE, 3=No chg

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

The read-only **User/GrpPrf** field shows the name of the user or group whose settings you are deleting.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Firewall Rules for Application Groups

Users who run particular applications often need to access a related group of servers. You can create an Application Group for those users, indicating which servers they may use without further checking. The name of an Application Group consists of a percent sign ("**%**"), a number sign ("**#**"), and the name of the application. For example, the group of users who run OPNAV would be **%#OPNAV**.

Users in Application Groups inherit the group's services and its authorities.

You can **define and modify Application Groups** from the **Work with Application Groups** screen. To reach the screen, select **5. Application Groups** from the **Work with Users** screen (*STRFW* **> 3 > 1**).

The **Work with Application Groups** screen appears.

```
                        Work with Application Groups
                                                    Subset . . . . _________
Type options, press Enter.                (Read top->down)
  1=Select  3=Copy  4=Delete  5=Members
                        ------------------- Network Servers ---------------
                        F   F F F R   R S   D   O R F     O C     C C N N M T
                        I   T T T E R M Q   B   B M I     R S     S S P P S C
                        L S P P P X E T L   O   J T L D V L L   D C C R R G P
                        T S L S C L X S E S P N I S S T P I I D R N L E S S S
                        F H O R L O E Q N Q E D N R R A R C C D D V N N R R G
 Opt  Appl.Group Members  R D G V N G C L T L N B F V V Q T M M M A M M T L V N
  _    %#ACCOUNT      2    + + + + + + + + + + + + + + + + + + + + + + + + + +
  _    %#GUI          1    + + + + + + + + + V + + + + + + + + + + + + + + + +
  _    %#PGM               + + + + + + + + + + + + + + + + + + + + + + + + + +
  _    %#SALES             + + + + + + + + + + + + + + + + + + + + + + + + + +
  _    %#TEST2             + + + + + + + + + + + + + + + + + + + + + + + + + +
  _    %#TEST3             + + + + + + + + + + + + + + + + + + + + + + + + + +


                                                                        Bottom
 Users in a group inherit its services & obj authorities.
 F3=Exit    F6=Add new    F8=Print list
```

The **Appl. Group** column lists Application Groups known to Firewall. The **Members** column shows the number of users included in the group.

The rest of the columns show whether the rules set for users or groups can override the global rules for particular servers. The server names, shown vertically at the top of the column, are:

- **FILTFR**: Original File Transfer Function
- **SSHD**: SSH,SFTP,SCP- Secured CMD Entry,FTP,COPY
- **FTPLOG**: FTP logging
- **FTPSRV**: FTP Server-Incoming Request Validation
- **FTPCLN**: FTP Client-Outgoing Request Validation
- **REXLOG**: Remote execution log
- **REXEC**: REXEC Server Request Validation
- **RMTSQL**: REXEC Server Request Validation
- **SQLENT**: Database Server - entry
- **SQL**: Database Server - SQL access & Show
- **DBOPEN**: Open Database
- **NDB**: Database Server - Database access
- **OBJINF**: Database Server - object information
- **RMTSRV**: Remote Command/Program Call
- **FILSRV**: File Server
- **DTAQ**: Data Queue Server
- **VPRT**: Original Virtual Print Server
- **ORLICM**:
- **CSCICM**:
- **DDM**: DDM request access
- **DRDA**: DDM request access
- **CSCNVM**: Central Server - conversion map
- **CSCLNN**: Central Server - client mgmt
- **NPRENT**: Central Server - client mgmt
- **NPRSRL**: Network Print Server - spool file
- **MSGSRV**: Original Message Server
- **TCPSGN**: Original Message Server

The server status values are:

- **+** : The user may use this server. This does not override global server security rules.
- **V** : For servers that support specific verbs (as shown in "Setting Server Verbs to Skip" on page 153), the user may use those verbs on this server.
- **S** : The user can access the server, skipping the check for object authorizations. This is normally used for batch applications that play the role

of servers. It increases performance and simplifies tests for some users.

- Blank : User may not use this server.

To **add a group**, press the **F6** key. The **Add Application Group Security** screen appears, as shown in "Adding Firewall Settings for an Application Group" on the next page.

To **print** the list of groups and their network server settings, press the **F8** key.

To **modify** the settings for a group, enter **1** in the **Opt** column for that group. The **Modify Application Group Security** screen appears, as shown in "Modifying Firewall Settings for an Application Group" on page 276.

To **copy** the settings from one group to another, enter **3** in the **Opt** column for that group. The **Copy Definition** screen appears, as shown in "Copying Firewall Settings for a User or Group" on page 267

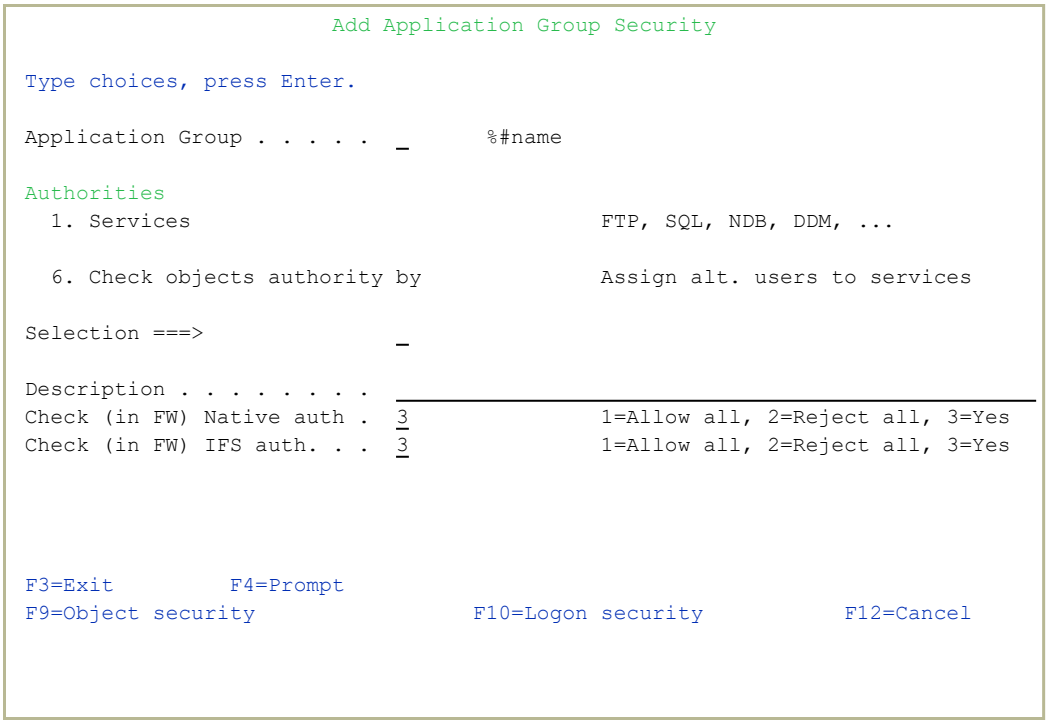
To **delete** the settings for a user or group, enter **4** in the **Opt** column for that user or group. The **Delete User Security** screen appears, as shown in "Deleting Firewall Settings for a User or Group" on page 270

To **add, remove, or change** the members of a group, enter **5** in the **Opt** column for that group. The **Modify Group of Users** screen appears, as shown in "Changing the Members of a Firewall Group" on page 269

## Adding Firewall Settings for an Application Group

To **add Firewall settings for an application group**, press the **F6** key in the **Work with Application Groups** screen, shown in "Setting Firewall Rules for Application Groups" on page 271 (***STRFW > 3 > 5***).

The **Add Application Group Security** screen appears.




Type the group's name in the **Application Group** field. To select a group from a list, press the **F4** key. The group's name must consist of a percent sign ("**%**"), a number sign ("**#**"), and the name of the relevant application, as in **%#OPSNAV**.

Through the options in the **Authorities and Locations** list, you can create specific filters for the group that can override the server's general settings. A close-arrow ("**>**") before an item shows that its settings have already been changed from the default to a new value.

### 1. Services

To create filters based on services (such as **FTP**, **SQL**, **NBD**, or **DDM**), enter **1** in the **Selection** field. The **Add User to Server Security** screen appears, as shown in "Adding Firewall Settings for a User based on Services" on page 232.

**6. Check objects authority by**

To have the user assume the authority of a different user when using particular servers, type **6** in the **Selection** field and press Enter. The Work with Alternative Users screen appears, as shown in "Adding Firewall Settings for a User to Assume Different Authority for a Server" on page 241.

The fields below these control other aspects of user security:

**Description**

A free-form text description of the group.

**Check (in FW) Native auth**

To allow the group to access all native objects, type **1**.

To reject all attempts by the group to access native objects,, type 2.

To check all attempts by the group to access native objects against Firewall settings set elsewhere, type 3.

**Check (in FW) IFS auth**

To allow the group to access all IFS objects, type **1**.

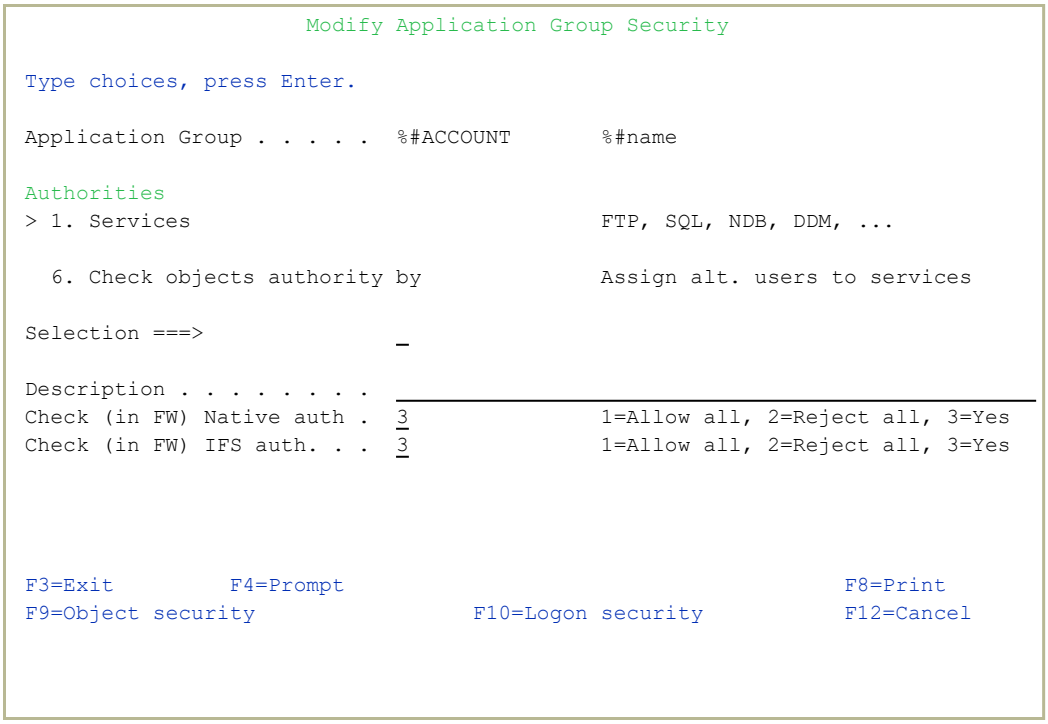
To reject all attempts by the group to access IFS objects,, type **2**.

To check all attempts by the group to access IFS objects against Firewall settings set elsewhere, type **3**.

## Modifying Firewall Settings for an Application Group

To **modify Firewall settings for an application group,** enter **1** in the **Opt** field for the group on the **Work with Application Groups** screen, shown in "Setting Firewall Rules for Application Groups" on page 271 (*STRFW > 3 > 5*), then press **Enter**.

The **Modify Application Group Security** screen appears.




The read-only **Application Group** field shows the name of the group.

Through the options in the **Authorities and Locations** list, you can create specific filters for the group that can override the server's general settings. A close-arrow ("**>**") before an item shows that its settings have already been changed from the default to a new value.

### 1. Services

To create filters based on services (such as **FTP**, **SQL**, **NBD**, or **DDM**), enter **1** in the **Selection** field. The **Add User to Server Security** screen appears, as shown in "Adding Firewall Settings for a User based on Services" on page 232.

**6. Check objects authority by**

To have the user assume the authority of a different user when using particular servers, type **6** in the **Selection** field and press Enter. The Work with Alternative Users screen appears, as shown in "Adding Firewall Settings for a User to Assume Different Authority for a Server" on page 241.

The fields below these control other aspects of user security:

**Description**

A free-form text description of the group.

**Check (in FW) Native auth**

To allow the group to access all native objects, type **1**.

To reject all attempts by the group to access native objects,, type 2.

To check all attempts by the group to access native objects against Firewall settings set elsewhere, type 3.

**Check (in FW) IFS auth**

To allow the group to access all IFS objects, type **1**.

To reject all attempts by the group to access IFS objects,, type **2**.

To check all attempts by the group to access IFS objects against Firewall settings set elsewhere, type **3**.

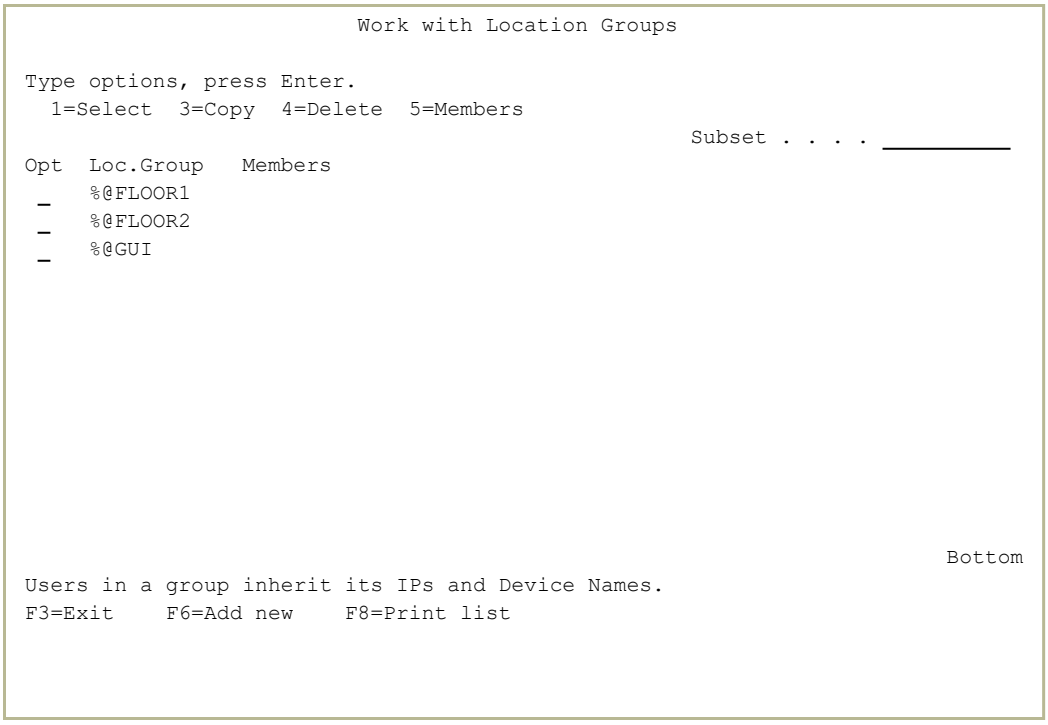
## Setting Firewall Rules for Location Groups

Users who share a common location, as defined by IP addresses and device names, can form Location Groups. The names of these groups consist of a percent symbol ("**%**"), an at symbol ("**@**"), and the name of the location. For example, users in a Chicago branch office can be added to a **%@CHICAGO** group and limited to working from IP addresses in that area.

Users in Location Groups inherit the group's services and its authorities.

You can **define and modify Location Groups** from the **Work with Location Groups** screen. To reach the screen, select **6. Location Groups** from the **Work with Users** screen (*STRFW* **> 3 > 1**).

The **Work with Location Groups** screen appears.




The **Loc. Group** column lists Application Groups known to Firewall. The **Members** column shows the number of users included in the group.

To **add a group**, press the **F6** key. The **Add Location Group Security** screen appears, as shown in "Adding Firewall Settings for a Location Group" on page 280.

To **print** the list of groups and their network server settings, press the **F8** key.

To **modify** the settings for a group, enter **1** in the **Opt** column for that group. The **Modify Location Group Security** screen appears, as shown in "Modifying Firewall Settings for a Location Group" on page 282.

To **copy** the settings from one group to another, enter **3** in the **Opt** column for that group. The **Copy Definition** screen appears, as shown in "Copying Firewall Settings for a User or Group" on page 267

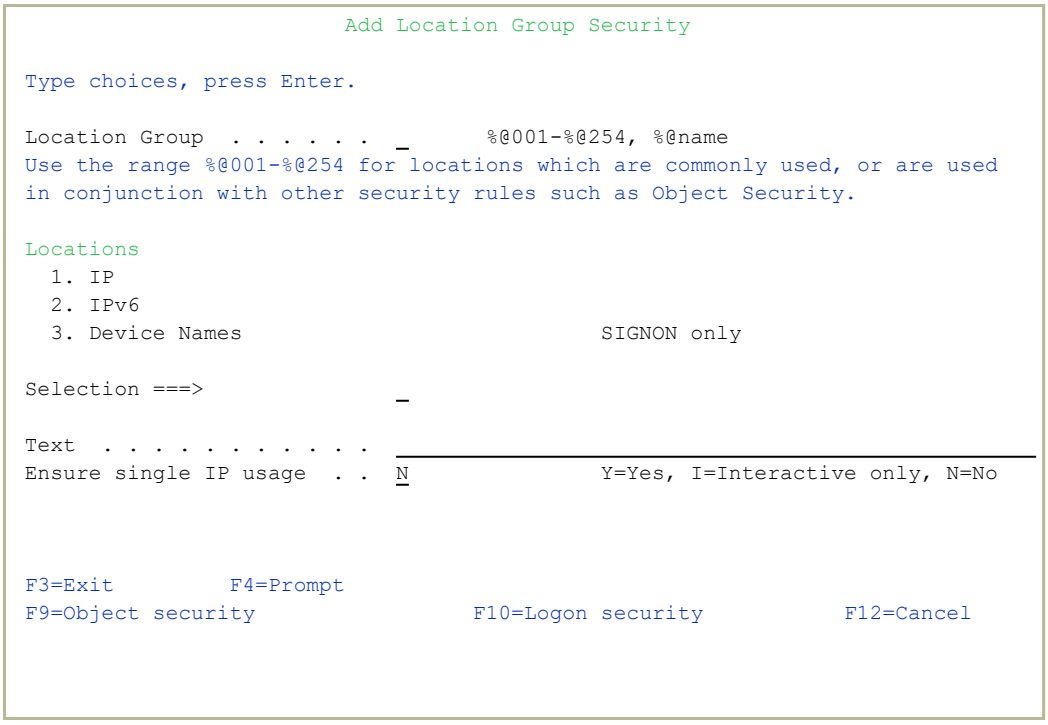
To **delete** the settings for a user or group, enter **4** in the **Opt** column for that user or group. The **Delete User Security** screen appears, as shown in "Deleting Firewall Settings for a User or Group" on page 270

To **add, remove, or change** the members of a group, enter **5** in the **Opt** column for that group. The **Modify Group of Users** screen appears, as shown in "Changing the Members of a Firewall Group" on page 269

## Adding Firewall Settings for a Location Group

To **add Firewall settings for a location group**, press the **F6** key in the **Work with Location Groups** screen, shown in "Setting Firewall Rules for Location Groups" on page 278 (***STRFW > 3 > 6***).

The **Add Location Group Security** screen appears.




Type the group's name in the **Location Group** field. To select a group from a list, press the **F4** key. The group's name must consist of a percent sign ("**%**"), a number sign ("**#**"), and either a three-digit number from **001** to **254** (such as **%@123**) or the name of the location (such as **%@CHICAGO**).

Through the options in the **Locations** list, you can create specific filters for the group that can override the server's general settings. A close-arrow ("**>**") before an item shows that its settings have already been changed from the default to a new value.

**1. IP**

To create filters based on IP addresses, type **1** in the **Selection** field and press **Enter**. The **Work with User IP Validation** screen appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IP Address" on page 189.

**2. IPv6**

To create filters based on IPv6 addresses, type **2** in the **Selection** field and press Enter. The Work with User IPv6 Validation screen appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IPv6 Address" on page 208.

**3. Device name**

To create filters based on SNA system names, type **3** in the **Selection** field and press Enter. The Work with Sign-On Device Validation screen appears, as shown in "Adding a Firewall Rule for Incoming Activity by Remote System Names" on page 184.

The fields below these control other aspects of user security:

**Description**

A free-form text description of the group.

**Ensure single IP use**

To limit the group to working from one IP address at a time, type **Y**. The group may have multiple sessions open at a time, but they must all be from the same IP address.

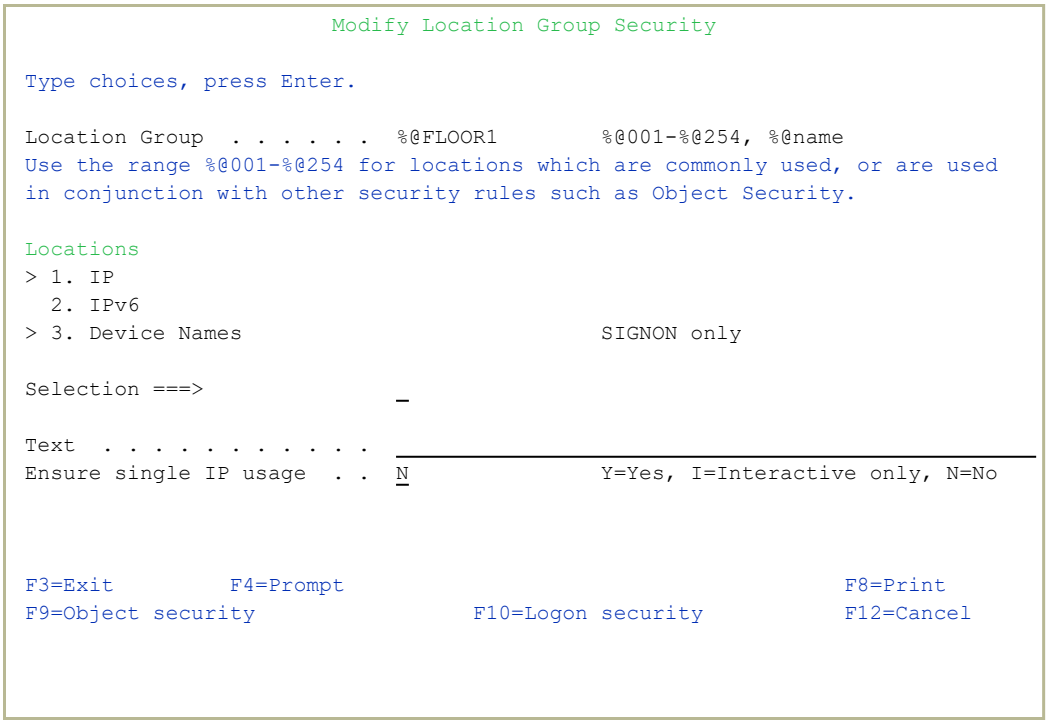
To limit the group's interactive sessions to one IP address at a time, type **I**. This does not affect the group's batch jobs.

To allow the group to work from multiple IP addresses simultaneously, type **N**.

## Modifying Firewall Settings for a Location Group

To **modify Firewall settings for a location group**, enter **1** in the **Opt** field for that group on the **Work with Location Groups** screen, shown in "Setting Firewall Rules for Location Groups" on page 278 (*STRFW > 3 > 6*).

The **Modify Location Group Security** screen appears.




The read-only **Location Group** field shows the name of the group.

Through the options in the **Locations** list, you can create specific filters for the group that can override the server's general settings. A close-arrow ("**>**") before an item shows that its settings have already been changed from the default to a new value.

**1. IP**

To create filters based on IP addresses, type **1** in the **Selection** field and press **Enter**. The **Work with User IP Validation** screen appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IP Address" on page 189.

**2. IPv6**

To create filters based on IPv6 addresses, type **2** in the **Selection** field and press Enter. The Work with User IPv6 Validation screen appears, as shown in "Adding a Firewall Rule for Outgoing Activity by IPv6 Address" on page 208.

**3. Device name**

To create filters based on SNA system names, type **3** in the **Selection** field and press Enter. The Work with Sign-On Device Validation screen appears, as shown in "Adding a Firewall Rule for Incoming Activity by Remote System Names" on page 184.

The fields below these control other aspects of user security:

**Description**

A free-form text description of the group.

**Ensure single IP use**

To limit the group to working from one IP address at a time, type **Y**. The group may have multiple sessions open at a time, but they must all be from the same IP address.

To limit the group's interactive sessions to one IP address at a time, type **I**. This does not affect the group's batch jobs.

To allow the group to work from multiple IP addresses simultaneously, type **N**.

# Adding, Replacing, or Removing Members of Firewall Groups

To **add** a member to a Firewall group, **replace** a member in it, or **remove** a member from it, select **35. Add/Replace/Remove Group Users** from the **Work with Users** screen (*STRFW***> 3**).

The **Change Firewall User Group (CHGFWGRP)** screen appears:

```
                    Change Firewall User Group (CHGFWGRP)

Type choices, press Enter.

Firewall '%group'  . . . . . .   _____________  '%group'
User profile . . . . . . . . .   __________     Name, *GRPPRF
               + for more values __________
Group profile and its users  . .  *NONE_____    Name, *NONE
Option . . . . . . . . . . . . .  *ADD____      *ADD, *REMOVE, *REPLACE









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

The screen contains these fields:

**Firewall '%group'**

The name of the Firewall group. It must begin with a percent sign ('**%**').

**User profile**

The name of a user to be added, removed, or replaced. To set this to the users of a system Group Profile, enter ***GRPPRF** and enter the name of the group in the **Group profile and its users** field.

**+ for more users**

To work with more than one user, enter a plus sign ('**+**') in this field. The Specify More Values for Parameter USRPRF screen appears, in which you can enter more names.

**Group profile and its users**

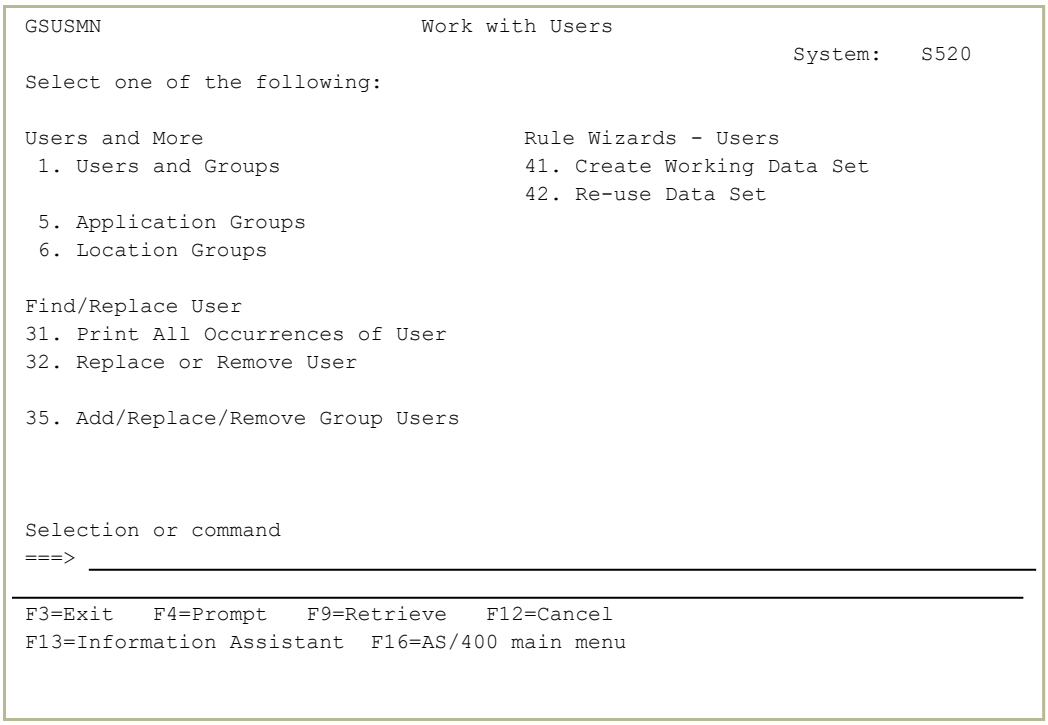
If the **User profile** field is set to ***GRPPRF**, the name of the group whose membership is changing. If you are not changing a system group, leave the default value of ***NONE**.

**Option**

To add, remove, or replace the specified users, set this file to ***ADD**, *REMOVE, or ***REPLACE**, respectively.

# Using the Rule Wizard for Users and Groups

Using the Rule Wizard, you can analyze recent activity on your system and use that information to create and modify Firewall rules.




To create a data set for examining activity and developing rules for activity based on the user or group requesting it, select **41. Create Working Data Set** from the Work with Users screen *(STRFW > 3*).

The Summarize User AS/400 Log (CPRUSRSEC) screen appears, as shown in "Creating a Data Set for Users and Groups with the Rule Wizard" on the facing page.

To use an existing data set to develop rules, select **42. Re-use Data Set** from the Work with Users screen (*STRFW > 3*).

The Summarize User AS/400 Log (CPRUSRSEC) screen appears, as shown in "Analyzing Recent Data on Users and Groups with the Rule Wizard" on page 291.

## Creating a Data Set for Users and Groups with the Rule Wizard

To **create a data set** for examining activity and developing rules for outgoing activity based the users and groups requesting it, select **41. Create Working Data Set** from the **Work with Users** screen *(STRFW* **> 3**).

The **Summarize User AS/400 Log (CPRUSRSEC)** screen appears. From this screen, you can construct the command line command that creates the data set.

```
                    Summarize User AS/400 Log (CPRUSRSEC)

Type choices, press Enter.

User . . . . . .  *ALL          Name, *ALL
Group by . . . . . .  *DFT      *DFT, *USER, *GRPPRF...
Allowed  . . . . . .  *ALL      *YES, *NO, *ALL
Starting date and time:
  Starting date  . . . . . .  *CURRENT    Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . .  000000      Time
Ending date and time:
  Ending date  . . . . . .  *CURRENT      Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . .  235959        Time
Number of records to process . .  *NOMAX  Number, *NOMAX
Server ID  . . . . . .  *ALL             *ALL, *FILTFR, *FTPLOG...




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

The screen contains the following fields. Fields that have values other than the defaults are preceded by the "**>**" character:

**User, <GrpPrf or '%GROUP'**

The user or group requesting the activity. This can be a user name, a generic* name, a group name, a group profile, or ***ALL** for all users.

**Group by**

How the result are grouped in the data set. Possible values include:

- ***DFT**: The default grouping of data within rule wizards, as set in the **Wizard Group by** parameter in the **Firewall General Definitions** screen.
- ***USER**: Grouped by the user name.
- ***GRPPRF**: If a user is a member of a single group, the user's activity is included under the group.

  Otherwise, the activity is shown under the username.
- ***USRGRP**: If the user is a member of multiple groups, the user's activity is included under the first of those groups.

  Otherwise, the activity is shown under the username.
- ***GROUP**: If the user is a member of a single group, the user's activity is included under that group.

  Otherwise, if the user is a member of multiple groups, the user's activity is listed under the first of those groups.

  Otherwise (if the user is not a member of any groups), the activity is shown under the username.
- ***ALLGRP**: If the user is a member of a single group plus up to fifteen supplemental groups. the user's activity is shown for each of those groups.
- ***ALL**: If the user is a member of a single group plus up to fifteen supplemental groups. the user's activity is shown for each of those groups.

  Otherwise, if the user is a member of multiple groups, the user's activity is listed under the first of those groups.

  Otherwise (if the user is not a member of any groups), the activity is shown under the username.

**Allowed**

Specifies whether the data set includes rejected activity, accepted activity, or both.

- ***YES**: Include only accepted activity
- ***NO:** Include only rejected activity

- ***ALL:** Include both accepted and rejected activity

**Starting data and time**

**Starting date**

The day or date on which the included data begins.

Allowed values include:

- ***CURRENT**: The current date
- ***YESTERDAY**: Yesterday's date
- ***WEEKSTR**: The first day of the current week. By default, this is Sunday.
- ***PRVWEEKS**: The first day of the previous week
- ***MONTHSTR**: The first day of the current month
- ***PRVMONTHS**: The first day of the previous month
- ***YEARSTR**: The first day of the current year
- ***PRVYEARS**: The first day of the previous year
- ***MON**: Monday
- ***TUE**: Tuesday
- ***WED**: Wednesday
- ***THU**: Thursday
- ***FRI**: Friday
- ***SAT**: Saturday
- ***SUN**: Sunday

**Starting time**

The time on the Starting date at which the included data begins, in **HHMMSS** format.

**Ending date**

The day or date on which the included data ends.

Allowed values are the same as for **Starting date**.

**Ending time**

The time on the Starting date at which the included data ends, in **HHMMSS** format.

**Number of records to process**

Collect no more than this number of records. If set to ***NOMAX**, collect all the relevant records.

**Server ID**

The server that the activity is attempting to access. To see a list of possible values, press the F4 key.

When you press Enter, more fields appear:

**Set to contain data**

**Set name**

The name of the data set that will contain the records. You can set this to your own value or choose one of these options:

- ***TEMP**: The default name for temporary data sets. The data set is removed when the session ends.
- ***USER**: Your user name
- ***S**: Equivalent to ***SELECT**
- ***SELECT**: If the wizard has been run before, a list appears of previous names that had been used for the data set.

**Replace or add records**

If any records already exist in the data set, whether to replace them or add the new records to them.

Possible values include:

- ***ADD**: Add new records to the existing set
- ***REPLACE**: Replace all existing records with the new ones.

**Wizard type**

The type of wizard to be created. Possible values include:

- ***STD**: The Rule Wizard screen that appears next has all the standard options
- ***FAST**: The Rule Wizard screen that appears next has a limited set of options for faster processing, as documented there.
- ***NO**: The data set will only be used to batch processing.

# Analyzing Recent Data on Users and Groups with the Rule Wizard

The Rule Wizards analyze data on recent system activity to develop and improve rules for filtering future activity.

To **develop rules to filter incoming activity by the user or group requesting it**, first create a data set of recent activity, as shown in "Creating a Data Set for Users and Groups with the Rule Wizard" on page 287.

Once you have created a data set, select **`42. Re-use Data Set`** from the **Work with Users** screen (*STRFW* **`> 3`**).

The **Plan User Security** screen appears:

```
                              Plan User Security
Type choices, press Enter.                          Subset . . __________ Exists _
 2=Set by use 4=Dlt 5=DSPFWLOG 6=Crt rule 7=Stats G=Groups U=Users E=CHGUSRPRF
   Specific rule exists  F F F F R   R S   D   O R F     O C     C C N N M T
   No specific rule      I T T T E R M Q   B   B M I     R S     S S P P S C
 Current: Y, V=By verb   L P P P X E T L   O   J T L D V L L   D C C R R G P
 Revised: Y, N           T L S C L X S E S P N I S S T P I I D R N L E S S S
     User Grp/ Exi-      F O R L O E Q N Q E D N R R A R C C D D V N N P R G
 Opt User      sts       R G V N G C L T L N B F V V Q T M M M A M M T L V N
  _  %ADM          Current Y Y Y Y Y Y Y Y V Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y
                   Done      Y Y Y           Y                             Y
                   Revised _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
  _  %GROUP1       Current Y Y Y Y Y Y Y Y Y Y Y Y V Y Y Y Y Y Y Y Y Y Y Y Y
                   Done      Y Y
                   Revised _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
  _  DB          Y Current Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y
                   Done                  Y Y                             Y
                   Revised _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
  _  QLWISVR       Y Current
                   Done                    Y
                   Revised _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
                                                                       More...
 F3=Exit    F6=Add New    F8=Print    F12=Cancel  F17=Set by use globally
```

Much of the screen is made up of groups of three lines.

The **`User Group/User`** field on the first line shows the user or group to whom the rules apply. If the name is on a green background, a rule set applies directly to that server. If the name is on a pink background, the user or group is included in rules for a generic group.

The rest of each of the lines shows the rules for a set of servers for one user or group.

Each server is shown in a separate column with the name spelled vertically at the top of the column:

- **FILTFR**: Original File Transfer Function
- **FTPLOG**: FTP Server Logon
- **FTPSRV**: FTP Server-Incoming Request Validation
- **FTPCLN**: FTP Client-Outgoing Request Validation
- **REXLOG**: REXEC Server Logon
- **REXEC**: REXEC Server Request Validation
- **RMTSQL**: Original Remote SQL Server
- **SQLENT**: Database Server - entry
- **SQL**: Database Server - SQL access & Showcase
- **DBOPEN**: Open Database
- **NDB**: Database Server - data base access
- **OBJINF**: Database Server - object information
- **RMTSRV**: Remote Command/Program Call
- **FILSRV**: File Server
- **DTAQ**: Data Queue Server
- **VPRT**: Original Virtual Print Server
- **ORLICM**: Original License Management Server
- **CSLICM**: Central Server - license management
- **DDM**: DDM request access
- **DRDA**: DRDA Distributed Relational DB access
- **CSCNVM**: Central Server - conversion map
- **CSCLNM**: Central Server - client management
- **NPRENT**: Network Print Server - entry
- **NPRSPL**: Network Print Server - spool file
- **MSGSRV**: Original Message Server
- **TCPSGN**: TCP Signon Server

Each of the three lines shows the state of rules for the relevant user or group.

- **Current** shows the rules for each server as they now stand. Possible values include:
  - **Y**: Access requests are accepted
  - **N**: Access requests are rejected
  - **V**: Access requests depend on the server verb used
  - Blank: No rule is set. The user or group inherits the rule for the next higher group, up through ***ALL**
- **Done** shows the results of the actual activity found for that user or group and server in the data set
- **Revised** shows the changes that you are making to the rules

To view the statistics on activity by a specific user during the time period in the data set, enter **7** in the **Opt** column for that use. The Statistics by Server for User screen appears.

To view a list of the users in a group, enter **G** in the **Opt** column for that group. The List of Users in User Group window appears, listing the users in the group.

To view a list of the groups containing a user, enter **U** in the **Opt** column for that group. The List of Users in Group Profile window appears, listing the users in the group.

To add rules for a new user, press the F6 key. The Add User Security screen appears, as shown in "Adding Firewall Rules for Users and Groups with the Rule Wizard" on page 295.

To change rules based on activity in the data set, see "Setting Firewall Rules based on Activity for Users and Groups with the Rule Wizard" on page 298.

To change rules based on activity globally, press the F17 key (Shift+F5). The rules for all the users and groups in the data set change, accepting activity on all servers that the user or group had accessed during the period that the data set covered.

To change rules manually, see "Setting Firewall Rules Manually based on Users and Groups with the Rule Wizard" on page 300.

To delete the rules for a user, enter **4** in the **Opt** field for that user. NOTE: You are not prompted for confirmation, and the user's rules are immediately deleted.

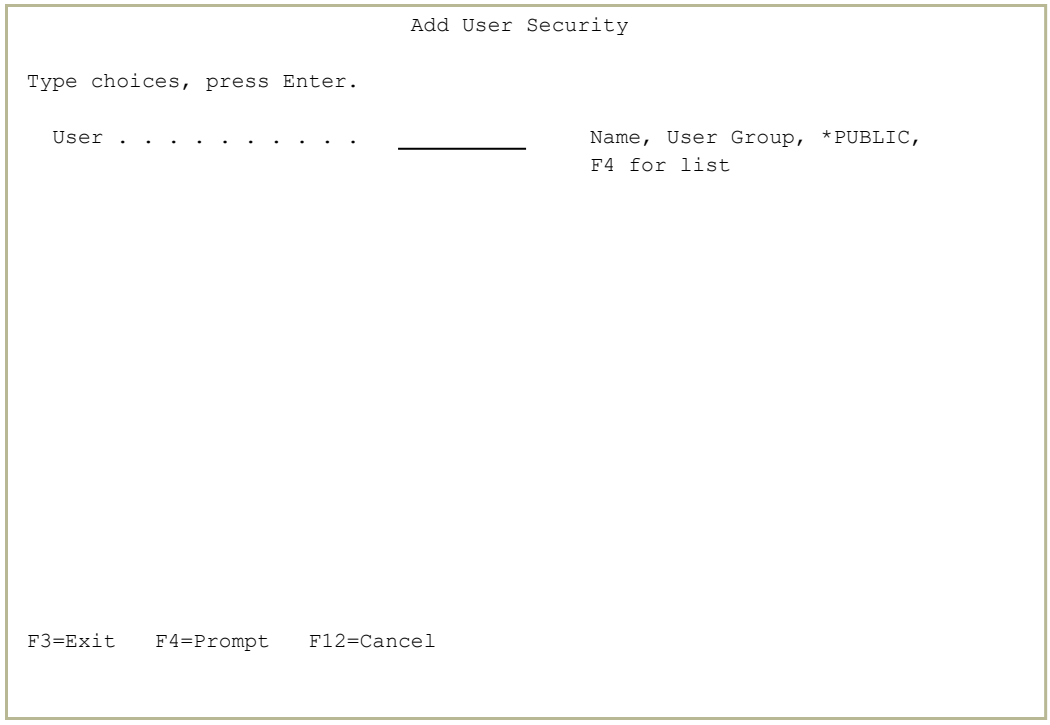
To **display the firewall log** entries relevant to this user, enter **5** in the **Opt** field for that rule. The **Display Firewall Log** screen appears, as shown in "Displaying Firewall Logs" on page 516.

To **print** the information from the data set, press the **F8** key.

## Adding Firewall Rules for Users and Groups with the Rule Wizard

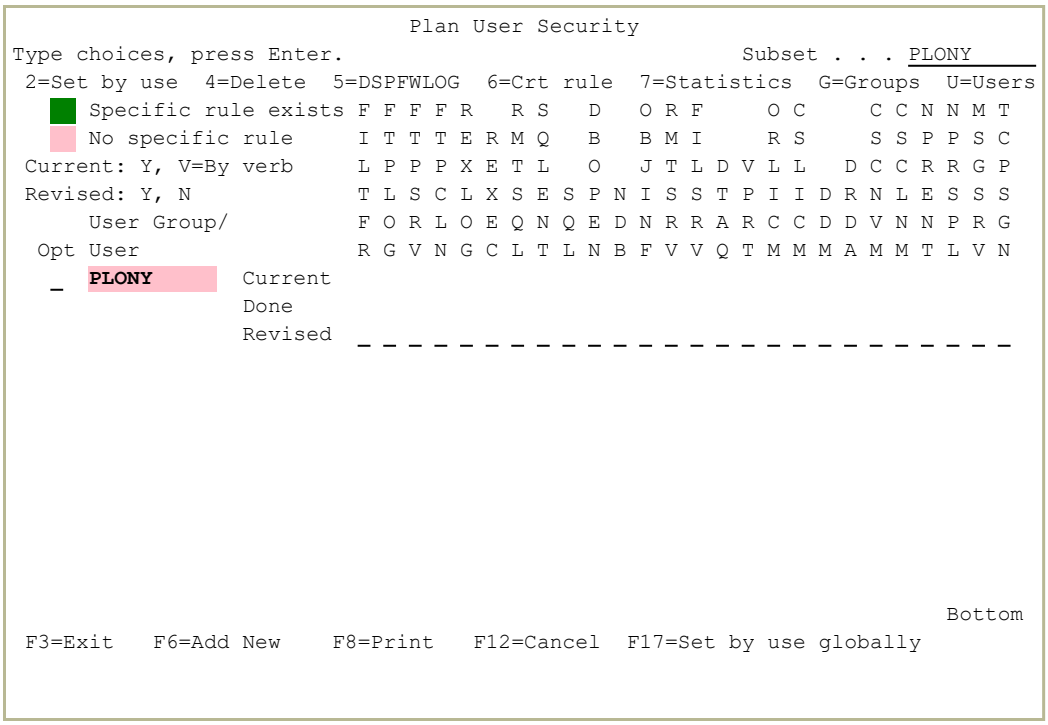
To **add firewall rules to filter activity by users and groups** via the Rule Wizard, press the **F6** key from the **Plan User Security** screen, shown in "Analyzing Recent Data on Users and Groups with the Rule Wizard" on page 291 (***STRFW*** **> 3 > 42**).

The **Add User Security** screen appears:




Type the name of the user or group for which you are creating the rule and press Enter. You can select from a list of existing users or groups by pressing the **F4** key.

The **Plan User Security** screen appears, with an empty record for the new user:




The screen includes a list of servers, displayed vertically, along with a Revised flied for each, in which you can enter new rule values for that user using that server.

The servers include:

- **FILTFR**: Original File Transfer Function
- **FTPLOG**: FTP Server Logon
- **FTPSRV**: FTP Server-Incoming Request Validation
- **FTPCLN**: FTP Client-Outgoing Request Validation
- **REXLOG**: REXEC Server Logon
- **REXEC**: REXEC Server Request Validation
- **RMTSQL**: Original Remote SQL Server
- **SQLENT**: Database Server - entry
- **SQL**: Database Server - SQL access & Showcase
- **DBOPEN**: Open Database
- **NDB**: Database Server - data base access
- **OBJINF**: Database Server - object information
- **RMTSRV**: Remote Command/Program Call
- **FILSRV**: File Server
- **DTAQ**: Data Queue Server
- **VPRT**: Original Virtual Print Server

- **ORLICM**: Original License Management Server
- **CSLICM**: Central Server - license management
- **DDM**: DDM request access
- **DRDA**: DRDA Distributed Relational DB access
- **CSCNVM**: Central Server - conversion map
- **CSCLNM**: Central Server - client management
- **NPRENT**: Network Print Server - entry
- **NPRSPL**: Network Print Server - spool file
- **MSGSRV**: Original Message Server
- **TCPSGN**: TCP Signon Server

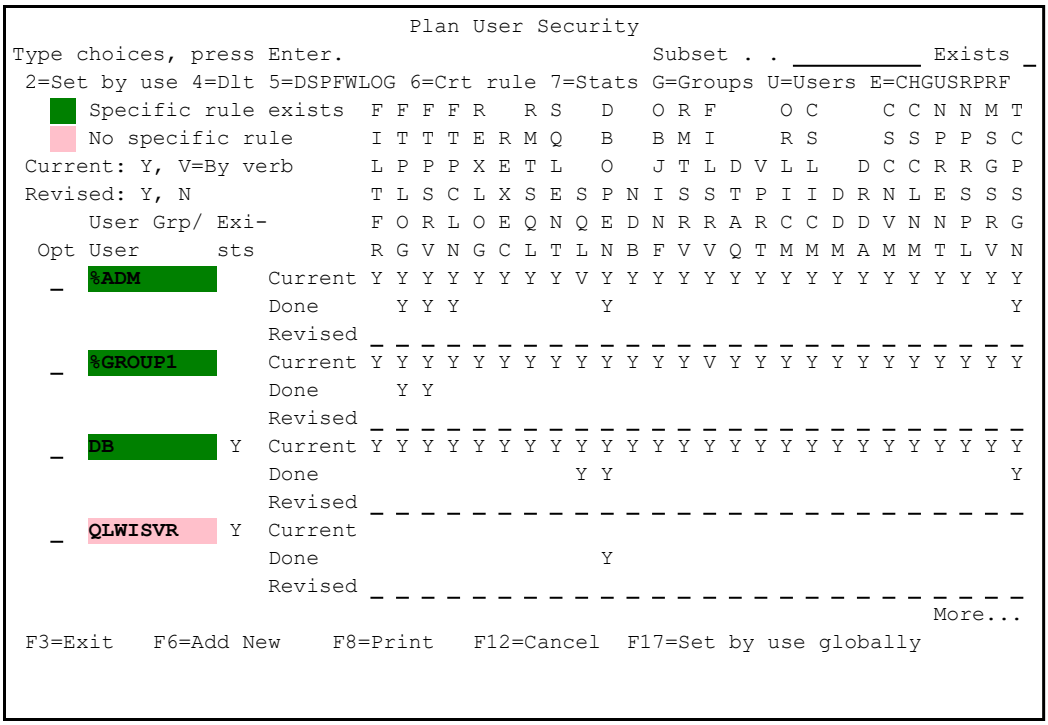
To accept requests from that user on that server, enter **Y** in the **Revised** field for that user on that server.

To reject requests from that user on that server, enter **N** in the **Revised** field for that user on that server.

If you do not make an entry for a server, the user or group inherits the rule from the next group up, up through ***ALL**.

# Setting Firewall Rules based on Activity for Users and Groups with the Rule Wizard

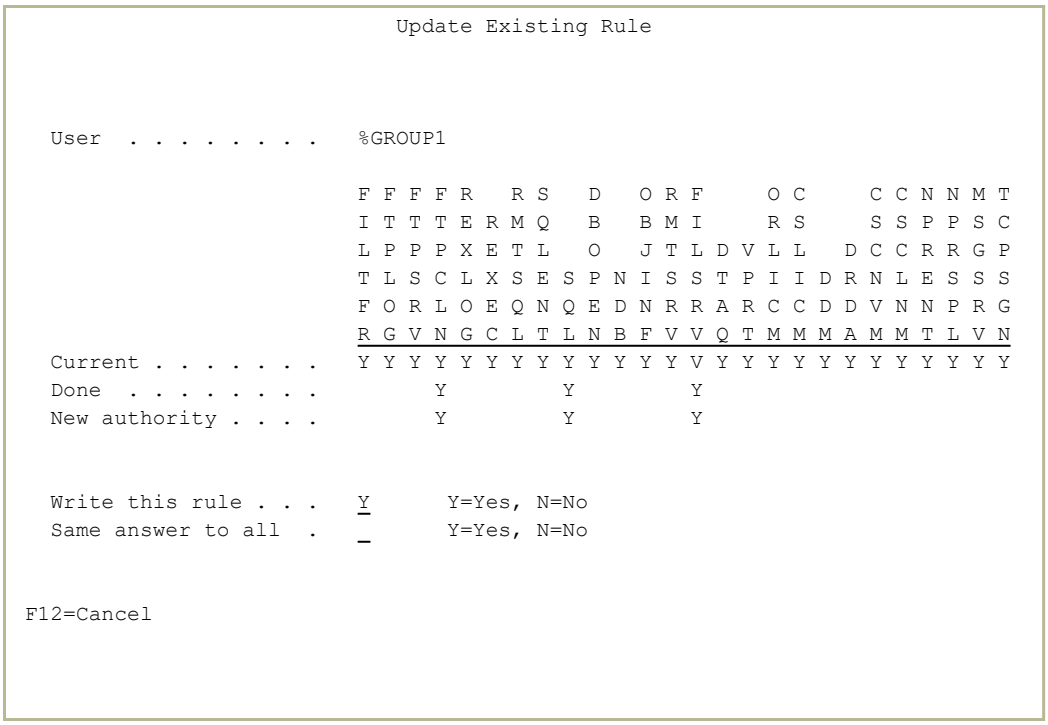
To **set rules based on the activity of users and groups** analyzed for the Rule Wizard, open the **Plan Outgoing IP Security** screen, as shown "Analyzing Recent Data on Users and Groups with the Rule Wizard" on page 291 (*STRFW* **> 3 > 42**).




For each user or group, the **Done** row shows the actual activity via each server during the time specified for the data set. This corresponds to the information shown if you select **7=Statistics** for that user or group. For example, the **Done** row for the group **%GROUP1** shows activity for the **DBOPEN**, **CSLICM**, **DRDA**, and **CSCNVM** servers.

To **create rules based on the activity for a user or group**, type **2** in the **Opt** field next to the user or group's name and press **Enter**.

The **Update Existing Rule** screen appears:



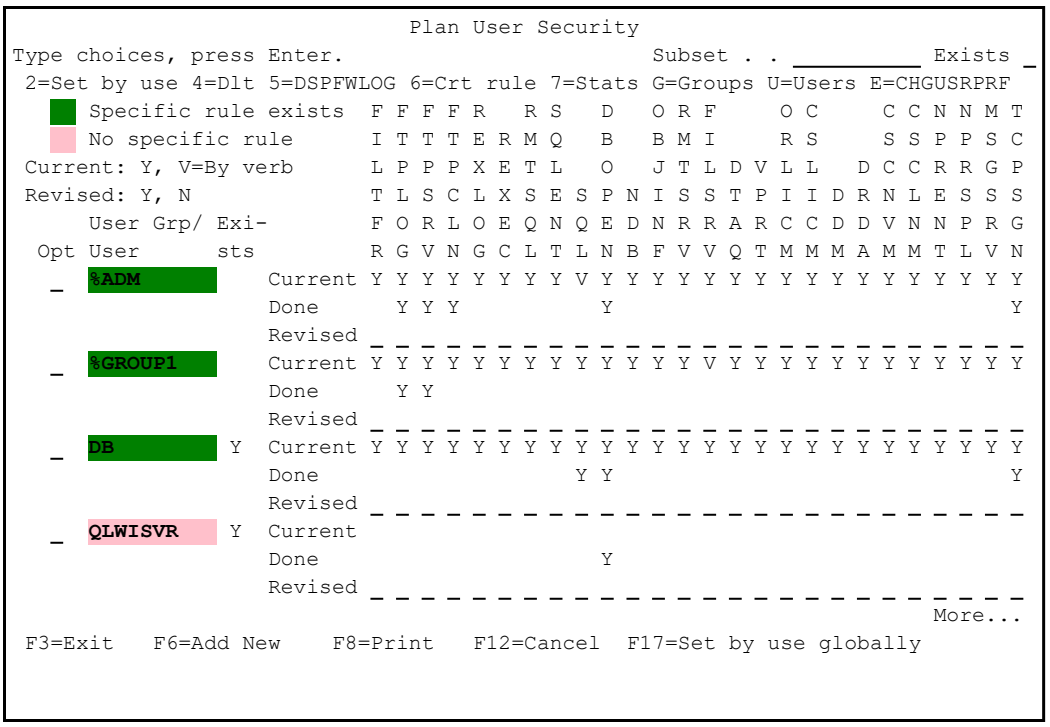

To **create a rule** corresponding to the user or group's activity within the data set, type **Y** in the **Write this rule** field.

To **accept the rule** based on activity each time that you create it within this session, type **Y** in the **Same answer to all** field.

# Setting Firewall Rules Manually based on Users and Groups with the Rule Wizard

NOTE: You can only set Firewall rules manually with the rule wizard if you have set the **`Wizard type`** to **`*STD`** when opening the wizard.

To **set rules manually based on the users or groups** requesting the activity in the Rule Wizard, open the **Plan User Security** screen, as shown in "Analyzing Recent Data on Users and Groups with the Rule Wizard" on page 291 (*STRFW* **`> 2 > 42`**).




Much of the screen is made up of groups of three lines.

The **`User Group/User`** field on the first line shows the user or group to whom the rules apply. If the name is on a green background, a rule set applies directly to that user. If the name is on a pink background, the user or group is included in rules for a generic group.

The **`Exists`** field is set to **`Y`** if the user profile exists in the system. An additional **`Exists`** field appears next to the **`Subset`** field at the top of the screen to enable filtering on this value.

The rest of each of the lines shows the rules for a set of servers for one user or group.

Each server is shown in a separate column with the name spelled vertically at the top of the column:

- **FILTFR**: Original File Transfer Function
- **FTPLOG**: FTP Server Logon
- **FTPSRV**: FTP Server-Incoming Request Validation
- **FTPCLN**: FTP Client-Outgoing Request Validation
- **REXLOG**: REXEC Server Logon
- **REXEC**: REXEC Server Request Validation
- **RMTSQL**: Original Remote SQL Server
- **SQLENT**: Database Server - entry
- **SQL**: Database Server - SQL access & Showcase
- **DBOPEN**: Open Database
- **NDB**: Database Server - data base access
- **OBJINF**: Database Server - object information
- **RMTSRV**: Remote Command/Program Call
- **FILSRV**: File Server
- **DTAQ**: Data Queue Server
- **VPRT**: Original Virtual Print Server
- **ORLICM**: Original License Management Server
- **CSLICM**: Central Server - license management
- **DDM**: DDM request access
- **DRDA**: DRDA Distributed Relational DB access
- **CSCNVM**: Central Server - conversion map
- **CSCLNM**: Central Server - client management
- **NPRENT**: Network Print Server - entry
- **NPRSPL**: Network Print Server - spool file
- **MSGSRV**: Original Message Server
- **TCPSGN**: TCP Signon Server

Each of the three lines shows the state of rules for the relevant user or group.

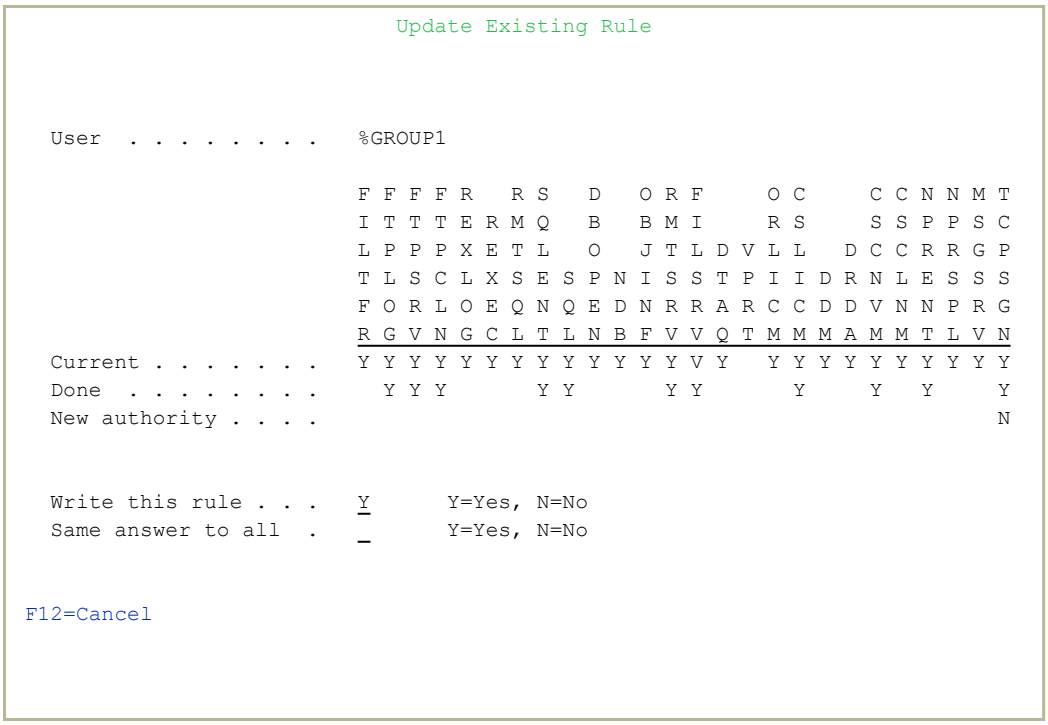
- **Current** shows the rules for each server as they now stand. Possible values include:
  - **Y**: Access requests are accepted
  - **N**: Access requests are rejected
  - **V**: Access requests depend on the server verb used
  - Blank: No rule is set. The user or group inherits the rule for the next higher group, up through ***ALL**
- **Done** shows the results of the actual activity found for that user or group and server in the data set
- **Revised** shows the changes that you are making to the rules

To make changes manually, set the values in the columns for the servers for which you want to change in the **Revised** row for the user. You can set these to **Y** to accept access requests or **N** to reject them.

NOTE: While the **Current** line may show a **V** for servers for which access is determined by the verbs used, the setting can only be changed to that via the Modify Server Verb Authority screen, as shown in "Modifying Firewall Settings for a User based on Server Verbs" on page 253.

When you have set all the needed values, type **6** in the **Opt** field next to the name of the user or group for which you are changing the values.

The Update Existing Rule screen appears:




In this case, the rule being created for the group **%GROUP1** would reject access requests to the **TCPSGN** (TCP Sign-in) server. The other setting would be cleared, and would inherit the value from the next higher group, up to ***ALL**.

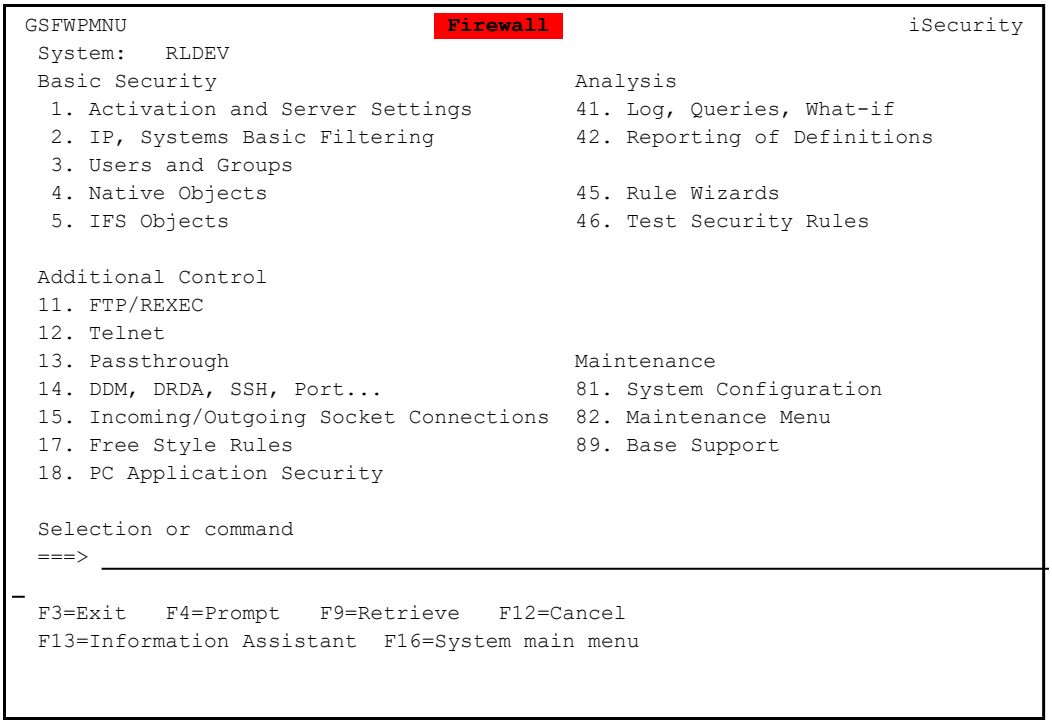
To **create this rule** manually, type **Y** in the **Write this rule** field.

To **accept the rule** each time that you create it manually within this session, type **Y** in the **Same answer to all** field.

# Setting Firewall Rules for Objects

Firewall can filter activity based on the object for which it is requesting access. The objects can include both native objects (such as files, libraries. data queues, printer files, programs, and commands) and IFS objects (which are usually shared from Windows systems).

You can add and modify these filter rules via menu options on the main Firewall screen.




To **add and modify rules for Native Objects**, type **4** and press **Enter**. The **Native Object Security** screen appears, as shown in "Setting Firewall Rules for Native Objects" on the facing page.

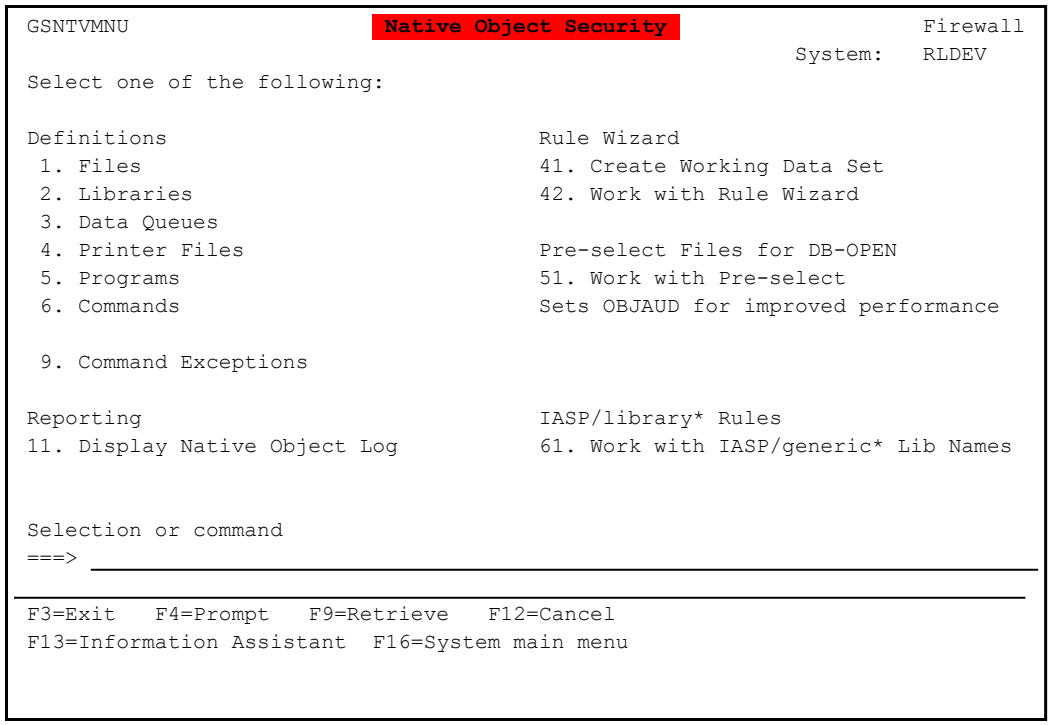
To **add and modify rules for IFS Objects**, type **5** and press **Enter**. The **IFS Security** screen appears, as shown in "Setting Firewall Rules for IFS Objects" on page 404.

## Setting Firewall Rules for Native Objects

Firewall can filter activity in different ways for the different categories of native objects.

To **select the object type**s, select **`4. Native Objects`** on the main Firewall screen (***STRFW > 4***).

The **Native Object Security** screen appears.




To add and modify filter rules based on **files**, type **1** and press **Enter**. The **Work with Native AS/400 File Security** screen appears, as shown in "Setting Firewall Rules for Native Files" on page 307.

To add and modify filter rules based on **libraries**, type **2** and press **Enter**. The **Work with Native AS/400 Library Security** screen appears, as shown in "Setting Firewall Rules for Libraries" on page 317.

To add and modify filter rules based on **data queues**, type **3** and press **Enter**. The **Work with Native AS/400 Data Queue Security** screen appears, as shown in "Setting Firewall Rules for Data Queues" on page 326.

To add and modify filter rules based on **printer files**, type **4** and press **Enter**. The **Work with Native AS/400 Print File Security** screen appears, as shown in "Setting Firewall Rules for Printer Files" on page 336.

To add and modify filter rules based on **programs**, type **5** and press **Enter**. The **Work with Native AS/400 Program Security** screen appears, as shown in "Setting Firewall Rules for Programs" on page 345.

To add and modify filter rules based on **commands**, type **6** and press **Enter**. The **Work with Native AS/400 Command Security** screen appears, as shown in "Setting Firewall Rules for Commands" on page 354.

To add and modify filter rules based on **command exceptions**, type **9** and press **Enter**. The **Work with Command Exceptions** screen appears, as shown in "Creating Exceptions to Command Filtering Rules" on page 363.

To **pre-select** files for DB-OPEN, type **51** and press Enter. The **Pre-select Files for DB-OPEN** screen opens, as shown in Pre-selecting Files for DB-OPEN.

To **substitute** filter rules for objects in a policy library for objects in specified other libraries, type **61** and press **Enter**. The **Work with IASP/generic* Lib Names** screen appears, as shown in "Substituting Firewall Rules for Native Objects with Rules from a Policy Library" on page 402.

## Setting Firewall Rules for Native Files

You can specify which users can read and write specific files, as well as who can create, delete, rename, or do other operations to the file through the **Work with Native AS/400 File Security** screen.

To **filter activity by native files** on which it would operate, select **1. Files** from the **Native Object Security** screen, as shown in "Setting Firewall Rules for Native Objects" on page 305 (*STRFW* **> 4**).

The **Work with Native AS/400 File Security** screen appears:

```
                    Work with Native AS/400 File Security

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

Opt File        Library      ---------------------- Users ----------------------
 _  *ALL        *ALL         A*          JAVA        LEVI        QSECOFR     ...
 _  DISPLAY_JO  *UNDFN       %EVG
 _  AA2         *USRLIBL
 _  DEMOPF      *USRLIBL     *PUBLIC     %CLOP       %TEST
 _  GSILOGP     *USRLIBL     EVGTST      OO          PP          RR          ...
 _  TEST0001    *USRLIBL
 _  TX*         #DFULIB      %QA         D*          DD*         QPGMR
 _  *ALL        ALEX         *PUBLIC
 _  A*          ALEX         %TEST1
 _  DEMOPF      ALEX         *PUBLIC     %TEST       ALEX3       TEVG
 _  PCI*        ALEX         %DDD        %GROUP1     A*          AEQE
 _  TEST1       ALEX         %SUPPORT
 _  GLPITRN     AP#FIL134    AUREA
 _  QRPGLESRC   AU           A*          AU          B*          TT          ...
                                                                        More...
 F3=Exit    F6=Add new    F8=Print    F12=Cancel
```

Each line of the list contains the following fields:

**File**

The name of the file. This can also be a generic name ending in an asterisk ("*****") or ***ALL**, which refer to all the relevant items in the library named in the next field for which more specific settings have not been created.

**Library**

The name of the library containing the files or files. This can also be a special name beginning with an asterisk ("*****") or ***ALL**, which refers to all the relevant files in all the relevant libraries. For

example, the File **TEST1** in the Library ***ALL** refers to any file named TEST1 in any library.

**Users**

A list of up to four users or groups for which particular authorities have been set. If there are more than four, an ellipsis ("...") appears in a fifth column. Selecting the file by entering **1** in the **Opt** field displays a screen with the entire list of users.

To create settings for a **new** file, press the **F6** key. The **Add Native AS/400 File Security** screen appears, as shown in "Adding Firewall Rules for Native Files" on the facing page.

To **print** the information from this screen, press the **F8** key.

To **modify** the settings for a file, enter **1** in the **Opt** field for the file. The **Modify Native AS/400 File Security** screen appears, as shown in "Modifying Firewall Rules for Native Files" on page 312.

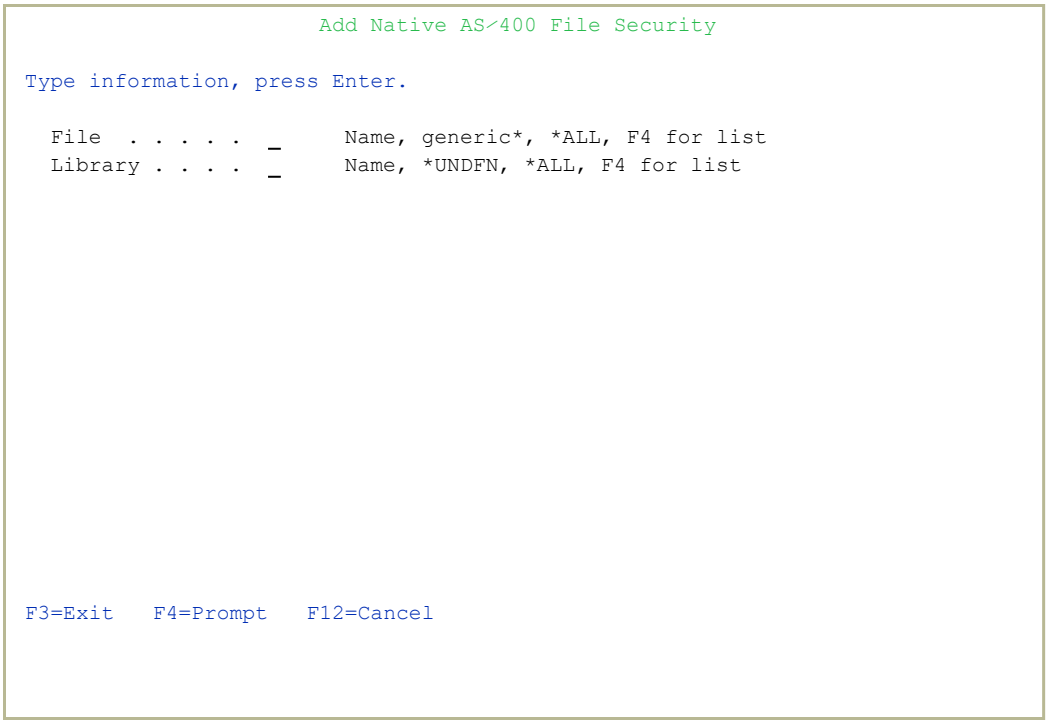
To **copy** settings for one file or library to another, enter **3** in the **Opt** field for the file. The **Copy Object Security** screen appears, as shown in "Copying Firewall Rules for Native Files" on page 314.

To **delete** the settings for a file, enter **4** in the **Opt** field for the file. The **Delete Native AS/400 File Security** screen appears, as shown in "Deleting Firewall Rules for Native Files" on page 316.

## Adding Firewall Rules for Native Files

To **add rules for native files** showing which users may operate on them, press the **F6** key on the **Work with Native AS/400 File Security** screen, as shown in "Setting Firewall Rules for Native Files" on page 307 (*STRFW* **> 4 > 1**).

The **Add Native AS/400 File Security** screen appears:




Enter information into the following fields:

**File**

The name of the file. This can also be a generic name ending in an asterisk ("*****") or ***ALL**, which refer to all the relevant items in the library named in the next field for which more specific settings have not been created. To see a list of files, place the cursor in this field and press the **F4** key.

**Library**

The name of the library containing the file. This can also be ***UNDFN**, which refers to an undefined library, or ***ALL**, which refers to all libraries for which more specific settings for that file

have not been created. To see a list of libraries, place the cursor in this field and press the F4 key.

Press Enter to confirm these values. More fields appear on the screen:

```
                      Add Native AS/400 File Security

Type information, press Enter.

  File  . . . . . .  *ALL
  Library . . . . .  *ALL
  Location Group ID .  ___         1-254    Access is restricted by location

Define user authority, press Enter.
  Y=Yes  S=Skip (Allow, no log)
 User*, %Group  Location |----- DATA -----|----------- FILE MANAGEMENT -------|
 Group profile  Group ID | Read     Write |  Create   Delete   Rename   Other |
  *PUBLIC                  _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
                                                                   More...
F3=Exit   F4=Prompt    F11=Enable locations      F12=Cancel
```

In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may operate on that file.

Each of the single-character fields may be set to **Y** for **Yes** or **S** to **Skip** (allowing the operation without logging).

In each line of the rest of the screen, you can indicate how a specified user or group may operate on the file:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the F4 key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the F11 key.

**DATA Read**

If set to **Y**, the user or group may read the data in the file.

**DATA Write**

If set to **Y**, the user or group may write data to the file.

**FILE MANAGEMENT Create**

If set to **Y**, the user or group may create the file.

**FILE MANAGEMENT Delete**

If set to **Y**, the user or group may delete the file.

**FILE MANAGEMENT Rename**

If set to **Y**, the user or group may rename the file.

**FILE MANAGEMENT Other**

If set to **Y**, the user or group may perform other operations on the file.

## Modifying Firewall Rules for Native Files

To **modify rules for a native file** that show which users may operate on it, enter **1** in the **Opt** field for that file on the **Work with Native AS/400 File Security** screen, as shown in "Setting Firewall Rules for Native Files" on page 307 (*STRFW* **> 4 > 1**).

The **Modify Native AS/400 File Security** screen appears:

```
                    Modify Native AS/400 File Security

Type information, press Enter.

  File  . . . . . .  DEMOPF
  Library . . . . .  *USRLIBL
  Location Group ID .  12         1-254    Access is restricted by location

Define user authority, press Enter.
  Y=Yes
 User*, %Group  Location |----- DATA -----|----------- FILE MANAGEMENT -------|
 Group profile  Group ID | Read     Write |  Create   Delete   Rename   Other |
  *PUBLIC                  _        Y        Y        _        _        _
  %CLOP                    _        _        _        _        _        _
  %TEST                    Y        Y        _        _        Y        Y
  __________               _        _        _        _        _        _
  __________               _        _        _        _        _        _
  __________               _        _        _        _        _        _
  __________               _        _        _        _        _        _
  __________               _        _        _        _        _        _
                                                                    More...
F3=Exit   F4=Prompt    F11=Enable locations      F12=Cancel
```

The read-only **File** and **Library** fields show the users or group to whom these rules apply.

In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may operate on that file.

Each of the single-character fields may be set to **Y** for **Yes** or **S** to **Skip** (allowing the operation without logging).

In each line of the rest of the screen, you can indicate how a specified user or group may operate on the file:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the F4 key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the F11 key.

**DATA Read**

If set to **Y**, the user or group may read the data in the file.

**DATA Write**

If set to **Y**, the user or group may write data to the file.

**FILE MANAGEMENT Create**

If set to **Y**, the user or group may create the file.

**FILE MANAGEMENT Delete**

If set to **Y**, the user or group may delete the file.

**FILE MANAGEMENT Rename**

If set to **Y**, the user or group may rename the file.

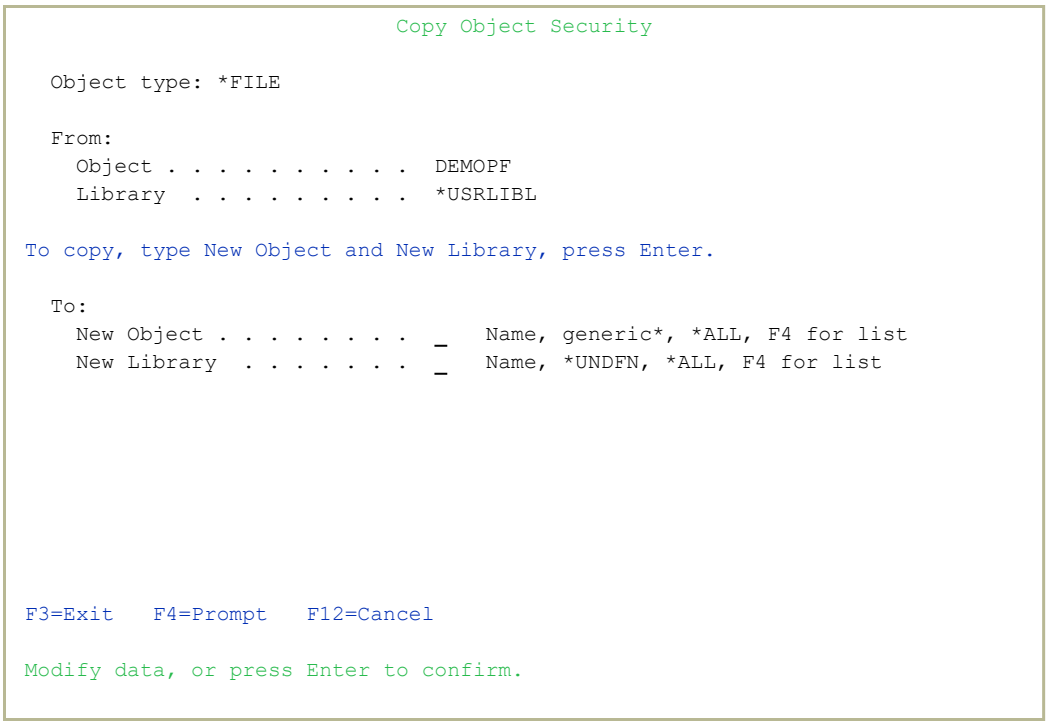
**FILE MANAGEMENT Other**

If set to **Y**, the user or group may perform other operations on the file.

## Copying Firewall Rules for Native Files

To copy rules for one file or group of files to another that show which users may operate on them, enter **3** in the **Opt** field for that file on the Work with Native AS/400 File Security screen, as shown in "Setting Firewall Rules for Native Files" on page 307 (*STRFW* **> 4 > 1**).

The Copy Object Security screen appears:




The read-only **Object Type** field shows the type of object for which rules are being copied. For files, this is ***FILE**.

The read-only **Object** and **Library** fields show the object and library for which rules are being copied.

The remaining fields indicate the file or files to which the rules are being copied:

**New Object**

The name of the file. This can also be a generic name ending in an asterisk ("*") or ***ALL**, which refers to all the relevant items in the library named in the next field for which more specific settings have not been created. To see a list of files, place the cursor in this field and press the F4 key.

**New Library**

The name of the library containing the file. This can also be ***UNDFN**, which refers to an undefined library, or ***ALL**, which refers to all libraries for which more specific settings for that file have not been created. To see a list of libraries, place the cursor in this field and press the F4 key

## Deleting Firewall Rules for Native Files

To **delete rules that show which users may operate on a file or group of files**, enter **4** in the **Opt** field for that file on the **Work with Native AS/400 File Security** screen, as shown in "Setting Firewall Rules for Native Files" on page 307 (*STRFW* **> 4 > 1**).

The **Delete Native AS/400 File Security** screen appears:

```
                     Modify Native AS/400 File Security

Type information, press Enter.

  File  . . . . . .  DEMOPF
  Library . . . . .  *USRLIBL
  Location Group ID .  12         1-254    Access is restricted by location

Define user authority, press Enter.
  Y=Yes
 User*, %Group  Location |----- DATA -----|----------- FILE MANAGEMENT -------|
 Group profile  Group ID | Read     Write |  Create   Delete   Rename   Other |
  *PUBLIC                  _        Y        Y        _        _        _
  %CLOP                    _        _        _        _        _        _
  %TEST                    Y        Y        _        _        Y        Y
  __________               _        _        _        _        _        _
  __________               _        _        _        _        _        _
  __________               _        _        _        _        _        _
  __________               _        _        _        _        _        _
  __________               _        _        _        _        _        _
                                                                    More...
F3=Exit   F4=Prompt    F11=Enable locations      F12=Cancel
```

All of the fields on the screen are read-only.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Firewall Rules for Libraries

You can specify which users can read and write specific libraries, as well as who can create, delete, rename, or do other operations to the libraries through the **Work with Native AS/400 Library Security** screen.

To **filter activity by libraries on which it would operate**, select **2 . Libraries** from the **Native Object Security** screen, as shown in "Setting Firewall Rules for Native Objects" on page 305 (*STRFW* **> 4**).

The **Work with Native AS/400 Library Security** screen appears:

```
                  Work with Native AS/400 Library Security

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

Opt Library                 ---------------------- Users ----------------------
 _  *ALL
 _  ALEX                    %TEST1
 _  CVB
 _  LN                      A*
 _  RAZLEE                  %DEVELOP1   QQ
 _  RAZLEE2                 %DEVELOP2
 _  SRFF

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

Each line of the list contains the following fields:

**Library**

The name of the library. This can also be a special name beginning with an asterisk ("*****") or ***ALL**, which refers to all libraries.

**Users**

A list of up to four users or groups for which particular authorities have been set. If there are more than four, an ellipsis ("...")

appears in a fifth column. Selecting the file by entering **1** in the **Opt** field displays a screen with the entire list of users.

To create settings for a **new** library, press the **F6** key. The **Add Native AS/400 Library Security** screen appears, as shown in "Adding Firewall Rules for Libraries" on the facing page.

To **print** the information from this screen, press the **F8** key.

To **modify** the settings for a library, enter **1** in the **Opt** field for the library. The **Modify Native AS/400 Library Security** screen appears, as shown in "Adding Firewall Rules for Libraries" on the facing page.

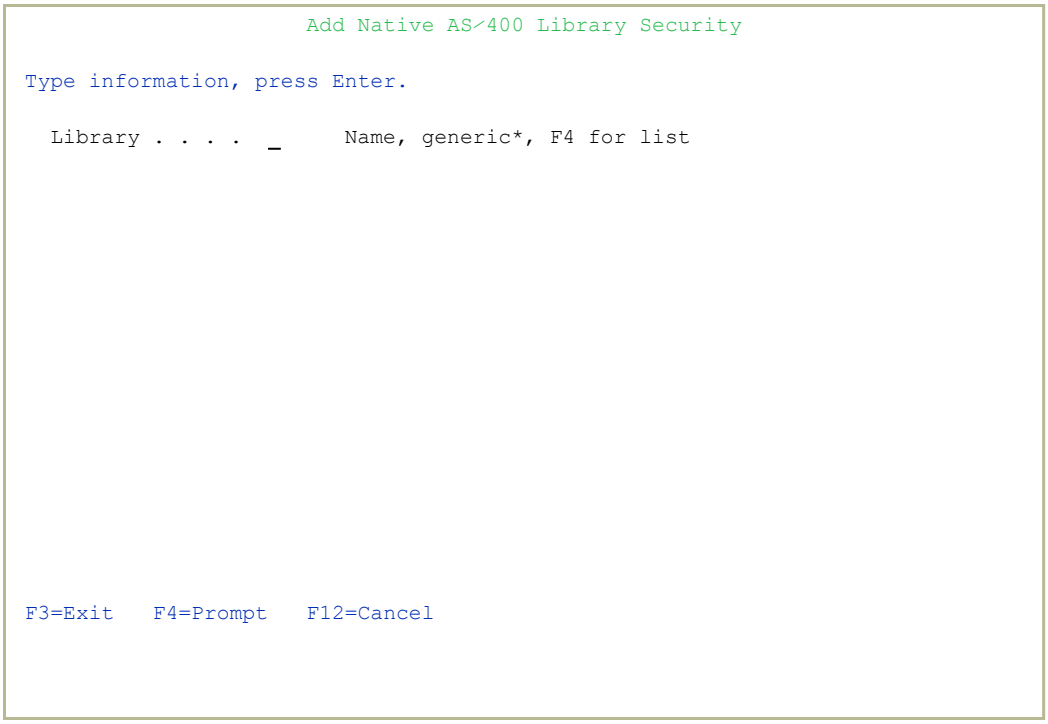
To **copy** settings for one library to another, enter **3** in the **Opt** field for the library. The **Copy Object Security** screen appears, as shown in "Copying Firewall Rules for Libraries" on page 324.

To **delete** the settings for a library, enter **4** in the **Opt** field for the librar. The **Delete Native AS/400 Library Security** screen appears, as shown in "Deleting Firewall Rules for Libraries" on page 325.

## Adding Firewall Rules for Libraries

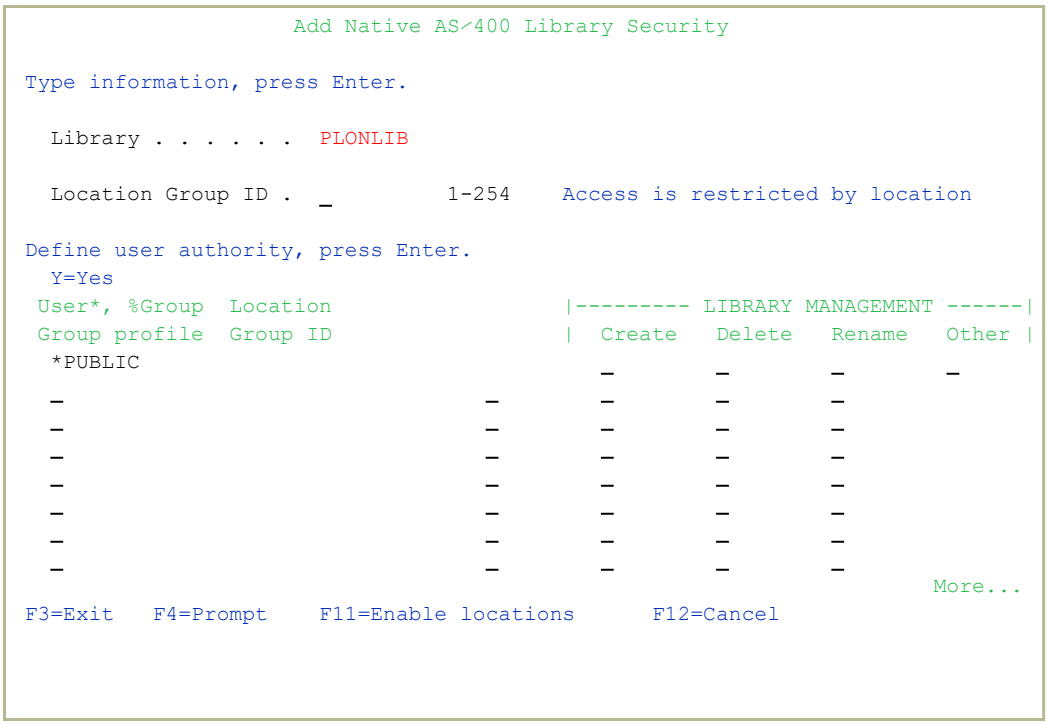
To **add rules for libraries showing which users may operate on them**, press the **F6** key on the **Work with Native AS/400 Library Security** screen, as shown in "Setting Firewall Rules for Libraries" on page 317 (*STRFW* **> 4 > 2**).

The **Add Native AS/400 File Security** screen appears:




Enter the name of the library in the **Library** field. This can also be a generic name ending in an asterisk ("*"). Press the **F4** key to see a list.

Press **Enter** to confirm this value. More fields appear on the screen:




In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may operate on that library.

In each line of the rest of the screen, you can indicate how a specified user or group may operate on the file:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the **F4** key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the **F11** key.

**LIBRARY MANAGEMENT Create**

If set to **Y**, the user or group may create the library.

**LIBRARY MANAGEMENT Delete**

If set to **Y**, the user or group may delete the library.

**LIBRARY MANAGEMENT Rename**

If set to **Y**, the user or group may rename the library.

**LIBRARY MANAGEMENT Other**

If set to **Y**, the user or group may perform other operations on the library.

## Modifying Firewall Rules for Libraries

To **modify rules for a library** showing which users may may operate on it, enter **1** in the **Opt** field for that library on the **Work with Native AS/400 Library Security** screen, as shown in "Setting Firewall Rules for Native Files" on page 307 (*STRFW* **> 4 > 1**).

The **Modify Native AS/400 Library Security** screen appears:

```
                    Modify Native AS/400 Library Security

Type information, press Enter.

  Library . . . . . .  RAZLEE

  Location Group ID .  _          1-254    Access is restricted by location

Define user authority, press Enter.
  Y=Yes
 User*, %Group  Location                  |--------- LIBRARY MANAGEMENT ------|
 Group profile  Group ID                  |  Create   Delete   Rename   Other |
  *PUBLIC                                    _        _        _        _
  %DEVELOP1                                  Y        Y        Y        Y
  QQ                                         Y        _        _        _
  _                                  _       _        _        _
  _                                  _       _        _        _
  _                                  _       _        _        _
  _                                  _       _        _        _
  _                                  _       _        _        _
                                                                   More...
F3=Exit    F4=Prompt    F11=Enable locations      F12=Cancel
```

In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may operate on that library.

In each line of the rest of the screen, you can indicate how a specified user or group may operate on the file:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the **F4** key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the F11 key.

**LIBRARY MANAGEMENT Create**

If set to **Y**, the user or group may create the library.

**LIBRARY MANAGEMENT Delete**

If set to **Y**, the user or group may delete the library.

**LIBRARY MANAGEMENT Rename**

If set to **Y**, the user or group may rename the library.

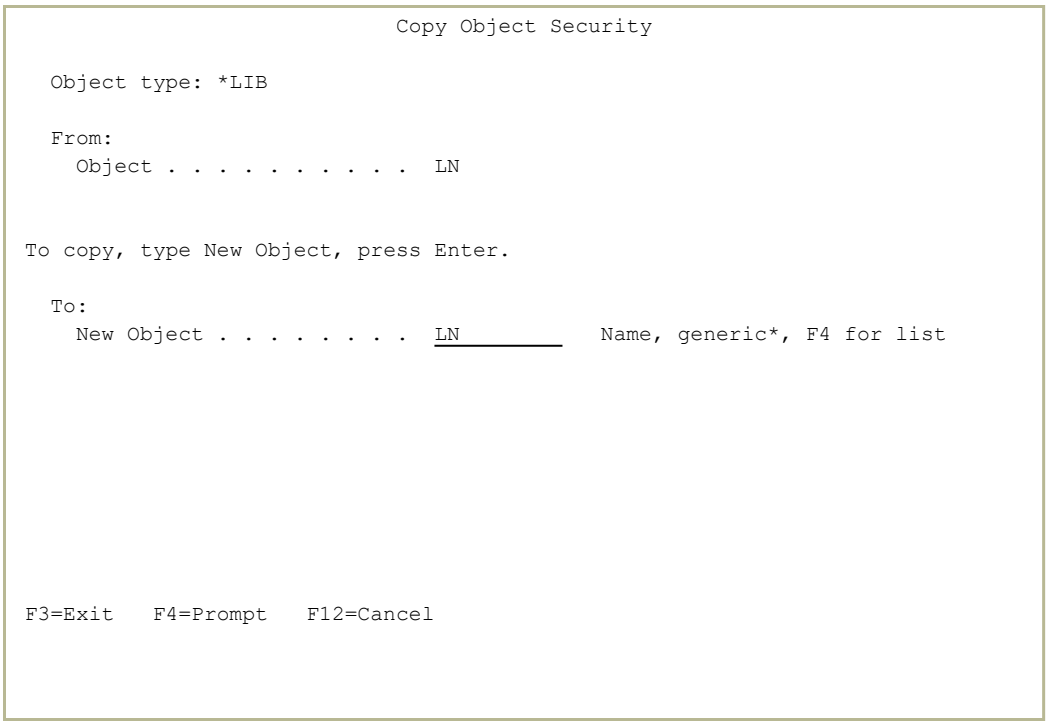
**LIBRARY MANAGEMENT Other**

If set to **Y**, the user or group may perform other operations on the library.

## Copying Firewall Rules for Libraries

To **copy rules for one library to another** that show which users may operate on them, enter **3** in the **Opt** field for that library on the **Work with Native AS/400 Library Security** screen, as shown in "Setting Firewall Rules for Libraries" on page 317 (*STRFW* **> 4 > 2**).

The **Copy Object Security** screen appears:




The read-only **Object Type** field shows the type of object for which rules are being copied. For libraries, this is ***LIB**.

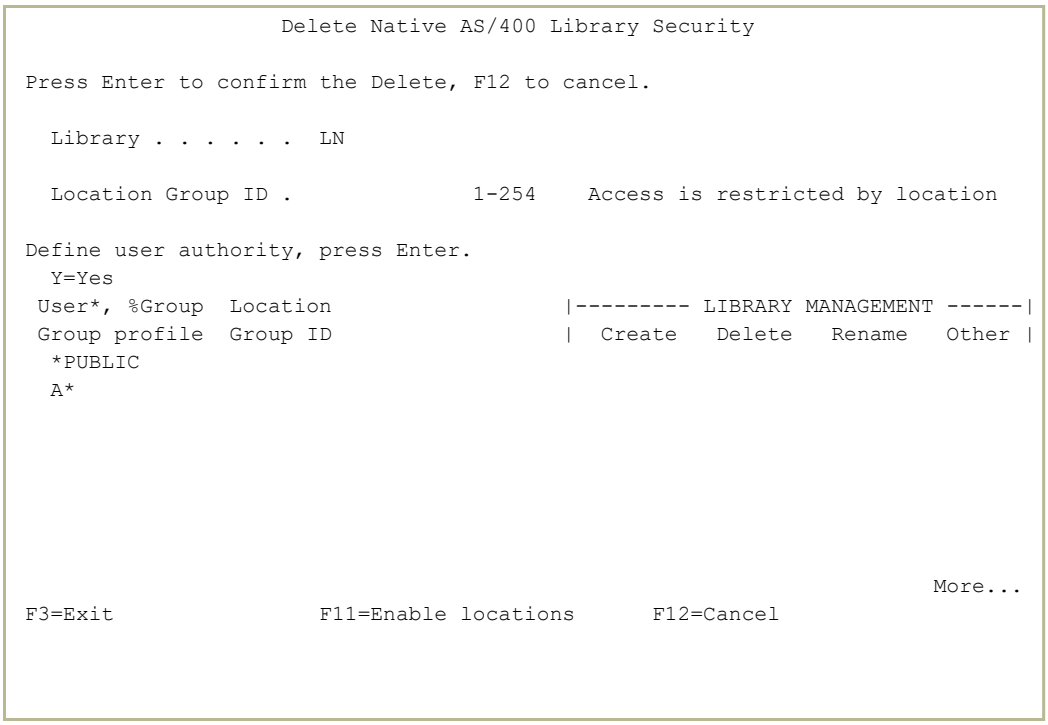
The read-only **Object** field shows the library for which rules are being copied.

The **New Object** field indicates the library to which the rules are being copied. This can also be a generic name ending in an asterisk ("*****") or ***ALL**, which refers to all libraries for which more specific settings have not been created. To see a list of files, place the cursor in this field and press the **F4** key.

## Deleting Firewall Rules for Libraries

To **delete rules that show which users may operate on a library**, type **4** in the **Opt** field for that file on the **Work with Native AS/400 Library Security** screen, as shown in "Setting Firewall Rules for Libraries" on page 317 (*STRFW* **> 4 > 2**) and press **Enter**.

The **Delete Native AS/400 Library Security** screen appears:




All of the fields on the screen are read-only.

To **confirm** the deletion and return to the previous screen, press **Enter**.

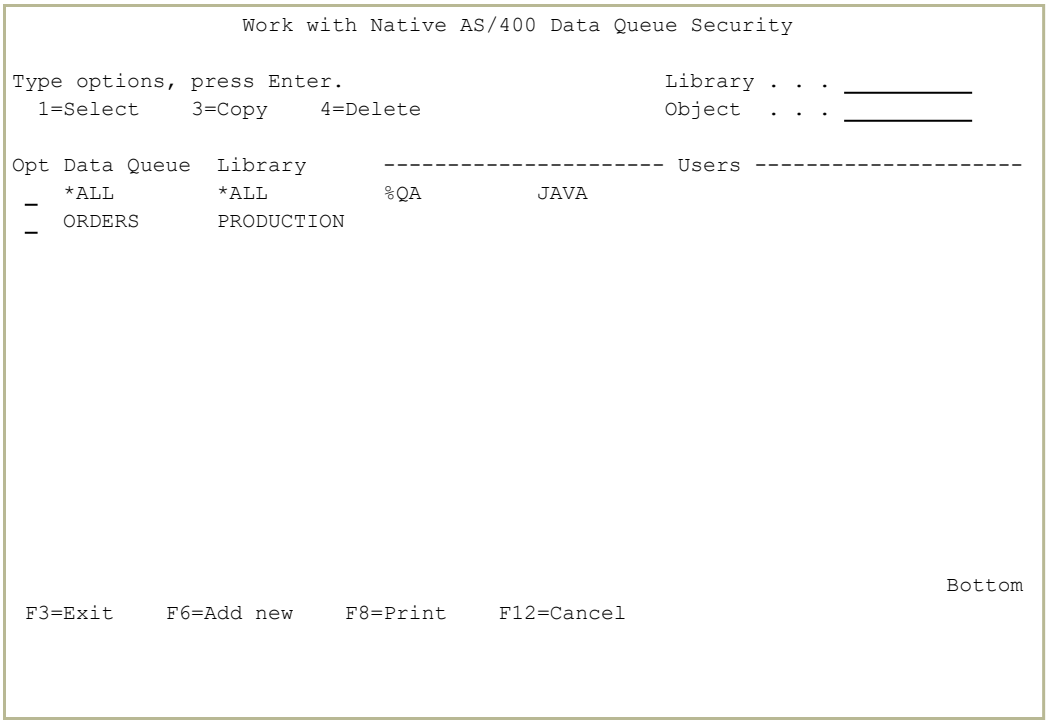
To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Firewall Rules for Data Queues

You can specify which users can read and write specific data queues, as well as who can create or delete them through the **Work with Native AS/400 Data Queue Security** screen.

To **filter activity by data queues** on which it would operate, select **`3. Data Queues`** from the **Native Object Security** screen, as shown in "Setting Firewall Rules for Native Objects" on page 305 (***STRFW > 4***).

The **Work with Native AS/400 Data Queue Security** screen appears:




Each line of the list contains the following fields:

**`Data Queue`**

The name of the data queue. This can also be a generic name ending in an asterisk ("**`*`**") or **`*ALL`**, which refer to all the relevant data queues in the library named in the next field for which more specific settings have not been created.

**`Library`**

The name of the library containing the data queues. This can also be a special name beginning with an asterisk ("**`*`**") or **`*ALL`**, which

refers to all the relevant data queues in all the relevant libraries. For example, the File **TEST1** in the Library ***ALL** refers to any file data queue TEST1 in any library.

**Users**

A list of up to four users or groups for which particular authorities have been set. If there are more than four, an ellipsis ("...") appears in a fifth column. Selecting the data queue by entering **1** in the **Opt** field displays a screen with the entire list of users.

To create settings for a **new** file, press the **F6** key. The **Add Native AS/400 Data Queue Security** screen appears, as shown in "Adding Firewall Rules for Data Queues" on the next page.

To **print** the information from this screen, press the **F8** key.

To **modify** the settings for a Data Queue, enter **1** in the **Opt** field for the data queue. The **Modify Native AS/400 Data Queue Security** screen appears, as shown in "Modifying Firewall Rules for Data Queues" on page 331.

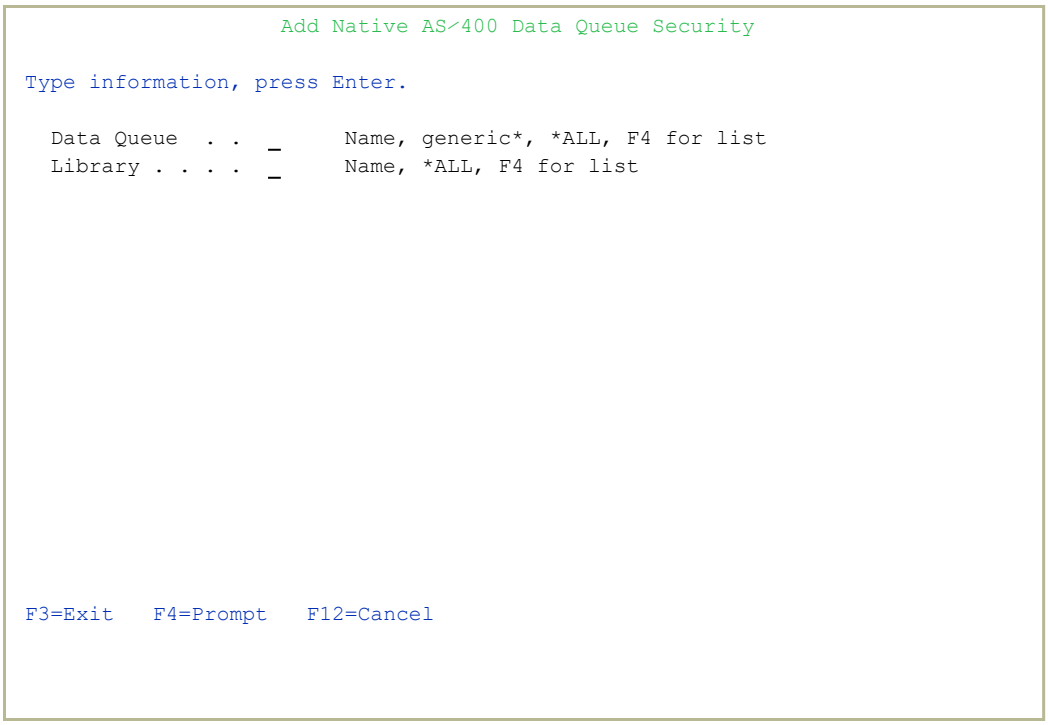
To **copy** settings for one data queue to another, enter **3** in the **Opt** field for the data queue. The **Copy Object Security** screen appears, as shown in "Copying Firewall Rules for Data Queues" on page 333.

To **delete** the settings for a data queue, enter **4** in the **Opt** field for the data queue. The **Delete Native AS/400 Data Queue Security** screen appears, as shown in "Deleting Firewall Rules for Data Queues" on page 335.

## Adding Firewall Rules for Data Queues

To **add rules for data queues showing which users may operate on them**, press the **F6** key on the **Work with Native AS/400 Data Queue Security** screen, as shown in "Setting Firewall Rules for Data Queues" on page 326 (*STRFW* **> 4 > 3**).

The **Add Native AS/400 Data Queue Security** screen appears:




Enter information into the following fields:

**Data Queue**

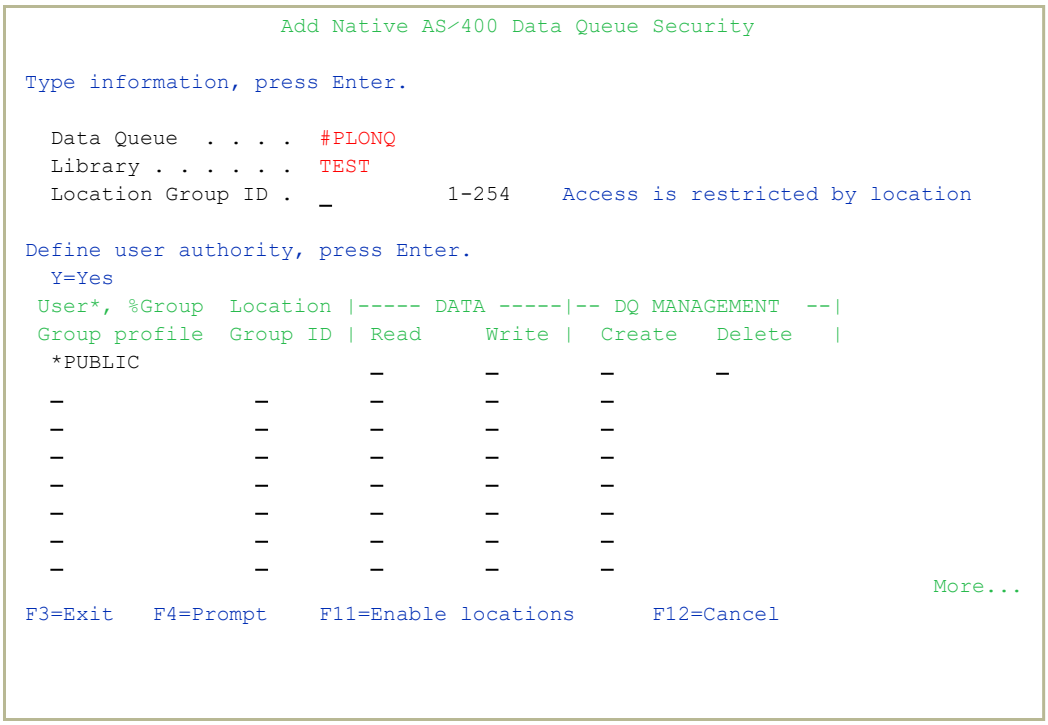
The name of the data queue. This can also be a generic name ending in an asterisk ("*****") or ***ALL**, which refer to all the relevant items in the library named in the next field for which more specific settings have not been created. Once you have entered a library name in the next field, you can see a list of data queues by placing the cursor in this field and pressing the **F4** key.

**Library**

The name of the library containing the data queue. This can also be ***ALL**, which refers to all libraries for which more specific

settings for that data queue have not been created. To see a list of libraries, place the cursor in this field and press the F4 key.

Press Enter to confirm these values. More fields appear on the screen:




In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may operate on that data queue.

In each line of the rest of the screen, you can indicate how a specified user or group may operate on the data queue:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the F4 key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the F11 key.

**DATA Read**

If set to **Y**, the user or group may read the data in the data queue.

**DATA Write**

If set to **Y**, the user or group may write data to the data queue.

**DQ MANAGEMENT Create**

If set to **Y**, the user or group may create the data queue.

**DQ MANAGEMENT Delete**

If set to **Y**, the user or group may delete the data queue.

## Modifying Firewall Rules for Data Queues

To **modify rules for a data queue showing which users may operate on it**, enter **1** in the **Opt** field for that data queue on the **Work with Native AS/400 Data Queue Security** screen, as shown in "Setting Firewall Rules for Data Queues" on page 326(*STRFW* **> 4 > 3**).

The **Modify Native AS/400 Data Queue Security** screen appears:

```
                  Modify Native AS/400 Data Queue Security

Type information, press Enter.

  Data Queue  . . . .  ORDERS
  Library . . . . . .  PRODUCTION
  Location Group ID .  _          1-254    Access is restricted by location

Define user authority, press Enter.
  Y=Yes
 User*, %Group  Location |----- DATA -----|-- DQ MANAGEMENT  --|
 Group profile  Group ID | Read     Write |  Create   Delete   |
  *PUBLIC                _        _       _        _
  _              _       _        _       _
  _              _       _        _       _
  _              _       _        _       _
  _              _       _        _       _
  _              _       _        _       _
  _              _       _        _       _
  _              _       _        _       _                              More...
F3=Exit   F4=Prompt    F11=Enable locations      F12=Cancel
```

The read-only **Data Queue** and **Library** fields show the users or group to whom these rules apply.

In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may operate on that data queue.

In each line of the rest of the screen, you can indicate how a specified user or group may operate on the data queue:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the **F4** key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the F11 key.

**DATA Read**

If set to **Y**, the user or group may read the data in the data queue.

**DATA Write**

If set to **Y**, the user or group may write data to the data queue.

**DQ MANAGEMENT Create**

If set to **Y**, the user or group may create the data queue.

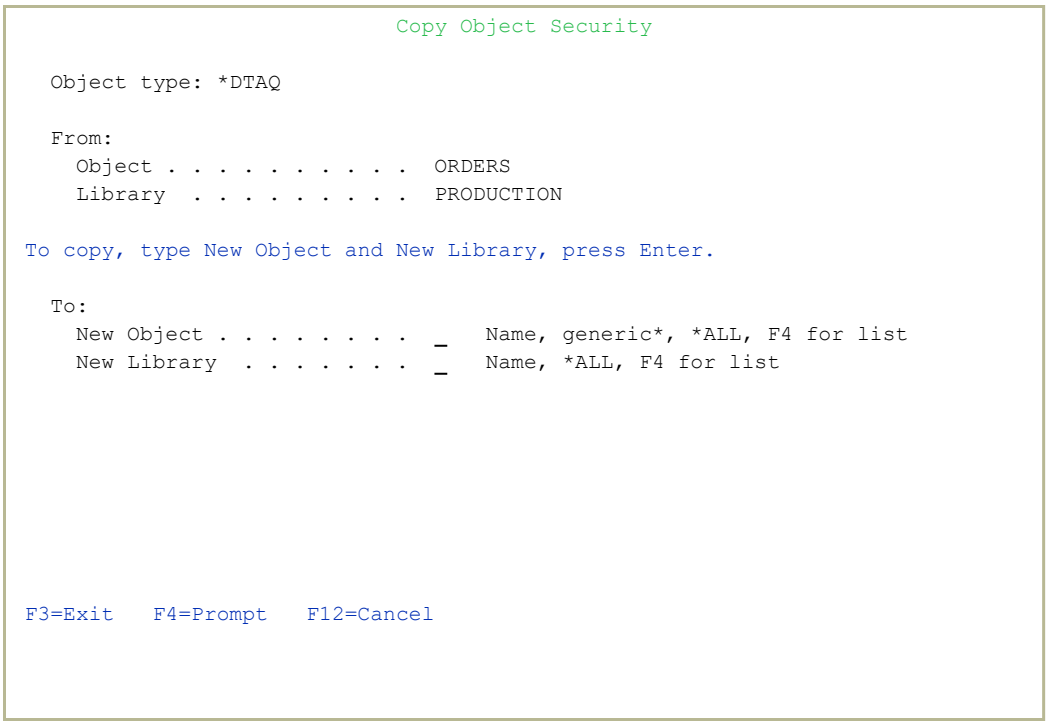
**DQ MANAGEMENT Delete**

If set to **Y**, the user or group may delete the data queue.

## Copying Firewall Rules for Data Queues

To **copy rules for one data queue to another** that show which users may operate on them, enter **3** in the **Opt** field for that data queue on the **Work with Native AS/400 Data Queue Security** screen, as shown in "Setting Firewall Rules for Data Queues" on page 326 (*STRFW* **> 4 > 3**).

The **Copy Object Security** screen appears:




The read-only **Object Type** field shows the type of object for which rules are being copied. For data queues, this is ***DTAQ**.

The read-only **Object** and **Library** fields show the object and library for which rules are being copied.

The remaining fields indicate the data queue to which the rules are being copied:

**New Object**

The name of the data queue. This can also be a generic name ending in an asterisk ("*") or ***ALL**, which refers to all the relevant items in the library named in the next field for which more specific settings have not been created. Once you have entered a library

name in the next field, you can see a list of data queues by placing the cursor in this field and pressing the F4 key.

**New Library**

The name of the library containing the data queue. This can also ***ALL**, which refers to all libraries for which more specific settings for that data queue have not been created. To see a list of libraries, place the cursor in this field and press the F4 key

## Deleting Firewall Rules for Data Queues

To **delete rules that show which users may operate on a data queue**, enter **4** in the **Opt** field for that data queue on the **Work with Native AS/400 Data Queue Security** screen, as shown in "Setting Firewall Rules for Data Queues" on page 326 (*STRFW* **> 4 > 1**).

The **Delete Native AS/400 Data Queue Security** screen appears:

```
                  Delete Native AS/400 Data Queue Security

Press Enter to confirm the Delete, F12 to cancel.

  Data Queue  . . . .  ORDERS
  Library . . . . . .  PRODUCTION
  Location Group ID .              1-254    Access is restricted by location

Define user authority, press Enter.
  Y=Yes
 User*, %Group  Location |----- DATA -----|-- DQ MANAGEMENT  --|
 Group profile  Group ID | Read     Write |  Create   Delete   |
  *PUBLIC

                                                                      More...
F3=Exit               F11=Enable locations      F12=Cancel
```

All of the fields on the screen are read-only.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Firewall Rules for Printer Files

You can specify which users can open specific printer files through the **Work with Native AS/400 Print File Security** screen.

To **filter activity by print files that it would open**, select **`4. Printer Files`** from the **Native Object Security** screen, as shown in "Setting Firewall Rules for Native Objects" on page 305 (***STRFW > 4***).

The **Work with Native AS/400 Print File Security** screen appears:

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

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

Opt Print File  Library      ---------------------- Users ---------------------
 _  *ALL        *ALL
 _  TEST_GUI    *ALL         ALEX
 _  TEST_NATIV  *ALL         ALEX
 _  A           B
 _  T           S            Q

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

Each line of the list contains the following fields:

**`Print File`**

The name of the print file. This can also be a generic name ending in an asterisk ("**`*`**") or **`*ALL`**, which refer to all the relevant print files in the library named in the next field for which more specific settings have not been created.

**`Library`**

The name of the library containing the print files. This can also be a special name beginning with an asterisk ("**`*`**") or **`*ALL`**, which refers to all the relevant print files in all the relevant libraries. For

example, the File **TEST1** in the Library ***ALL** refers to any file print file
**TEST1** in any library.

**Users**

A list of up to four users or groups for which particular authorities have been set. If there are more than four, an ellipsis ("...") appears in a fifth column. Selecting the print file by entering **1** in the **Opt** field displays a screen with the entire list of users.

To create settings for a **new** file, press the **F6** key. The **Add Native AS/400 Print File Security** screen appears, as shown in "Adding Firewall Rules for Printer Files" on the next page.

To **print** the information from this screen, press the **F8** key.

To **modify** the settings for a file, enter **1** in the **Opt** field for the print file. The **Modify Native AS/400 Print File Security** screen appears, as shown in "Modifying Firewall Rules for Printer Files" on page 340.

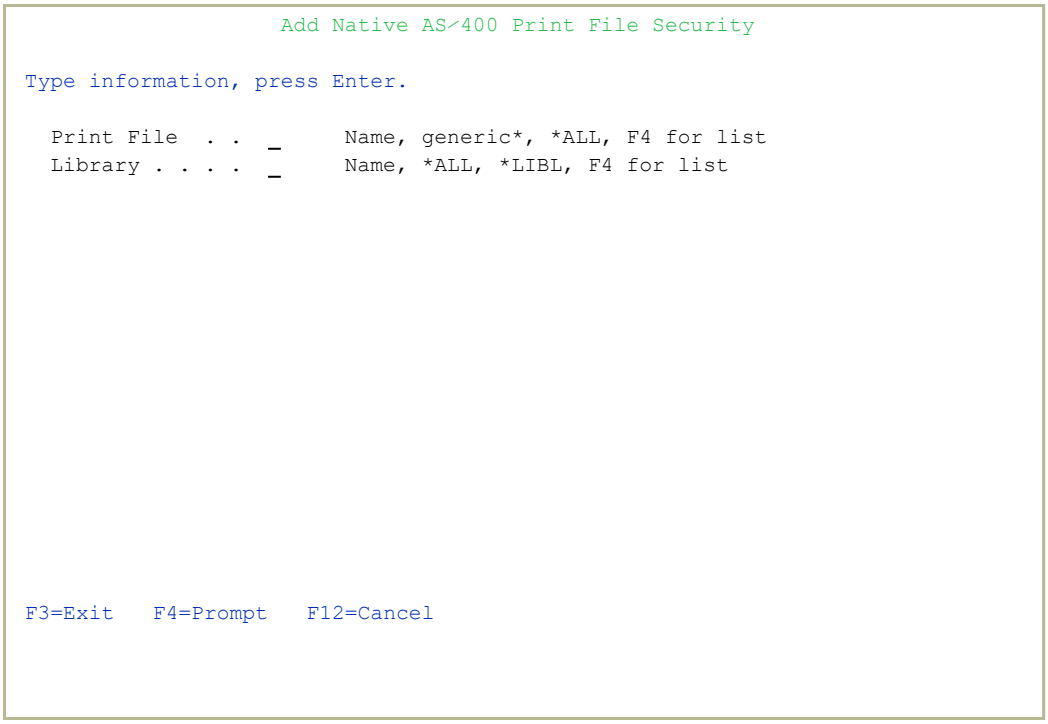
To **copy** settings for one print file to another, enter **3** in the **Opt** field for the print file. The **Copy Object Security** screen appears, as shown in "Copying Firewall Rules for Printer Files" on page 342.

To **delete** the settings for a print file, enter **4** in the **Opt** field for the print file. The **Delete Native AS/400 Print File Security** screen appears, as shown in "Deleting Firewall Rules for Printer Files" on page 344.

## Adding Firewall Rules for Printer Files

To **add rules for print files showing which users may open them**, press the **F6** key on the **Work with Native AS/400 Print File Security** screen, as shown in "Setting Firewall Rules for Printer Files" on page 336 (*STRFW* **> 4 > 4**).

The **Add Native AS/400 Print File Security** screen appears:




Enter information into the following fields:

**Print File**

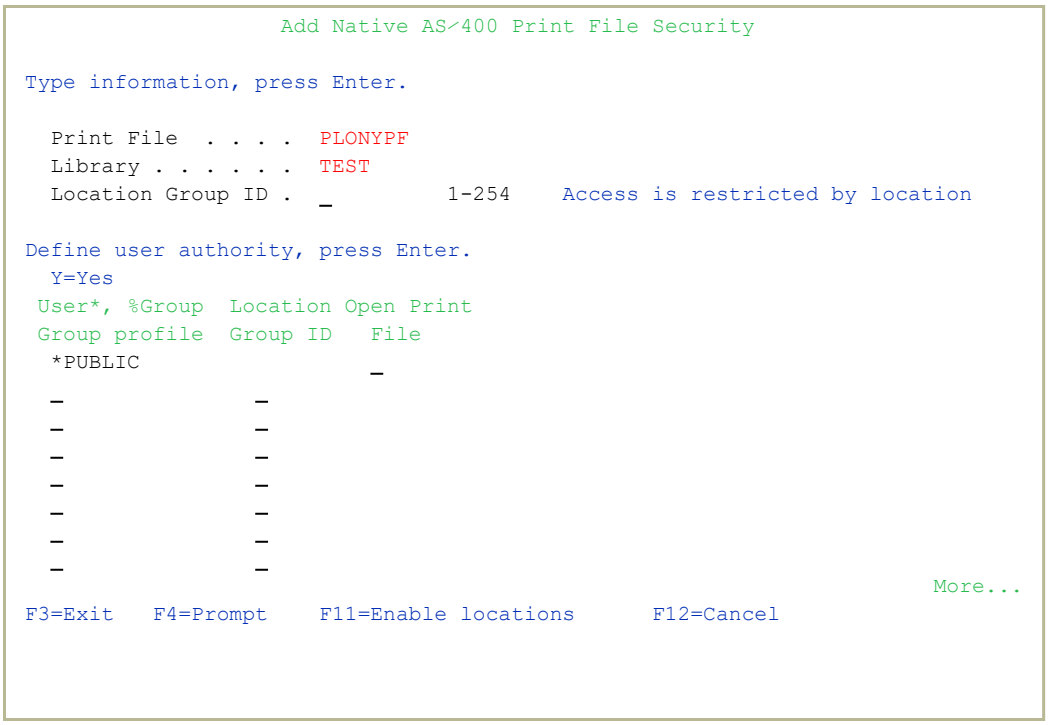
The name of the print file. This can also be a generic name ending in an asterisk ("*****") or ***ALL**, which refer to all the relevant items in the library named in the next field for which more specific settings have not been created. Once you have entered a library name in the next field, you can see a list of print files by placing the cursor in this field and pressing the **F4** key.

**Library**

The name of the library containing the print file. This can also be ***ALL**, which refers to all libraries for which more specific settings

for that print file have not been created. To see a list of libraries, place the cursor in this field and press the F4 key.

Press Enter to confirm these values. More fields appear on the screen:




In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may open that print file.

In each line of the rest of the screen, you can indicate whether a specified user or group may open the print file:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the F4 key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the F11 key.

**Open Print File**

If set to **Y**, the user or group may open the print file.

## Modifying Firewall Rules for Printer Files

To **modify rules for a printer file** showing which users may open it, enter **1** in the **Opt** field for that print file on the **Work with Native AS/400 Print File Security** screen, as shown in "Setting Firewall Rules for Printer Files" on page 336 (*STRFW* **> 4 > 4**).

The **Modify Native AS/400 Print File Security** screen appears:

```
                  Modify Native AS/400 Print File Security

Type information, press Enter.

  Print File  . . . .  TEST_NATIV
  Library . . . . . .  *ALL
  Location Group ID .  ___          1-254    Access is restricted by location

Define user authority, press Enter.
  Y=Yes
 User*, %Group  Location Open Print
 Group profile  Group ID   File
  *PUBLIC                  _
  ALEX_____                Y
  _________                _
  _________                _
  _________                _
  _________                _
  _________                _
  _________                _
                                                                    More...
F3=Exit   F4=Prompt    F11=Enable locations      F12=Cancel
```

The read-only **Print File** and **Library** fields show the print file and library to which these rules apply.

In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may open that print file.

In each line of the rest of the screen, you can indicate whether a specified user or group may open the print file:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the **F4** key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the F11 key.

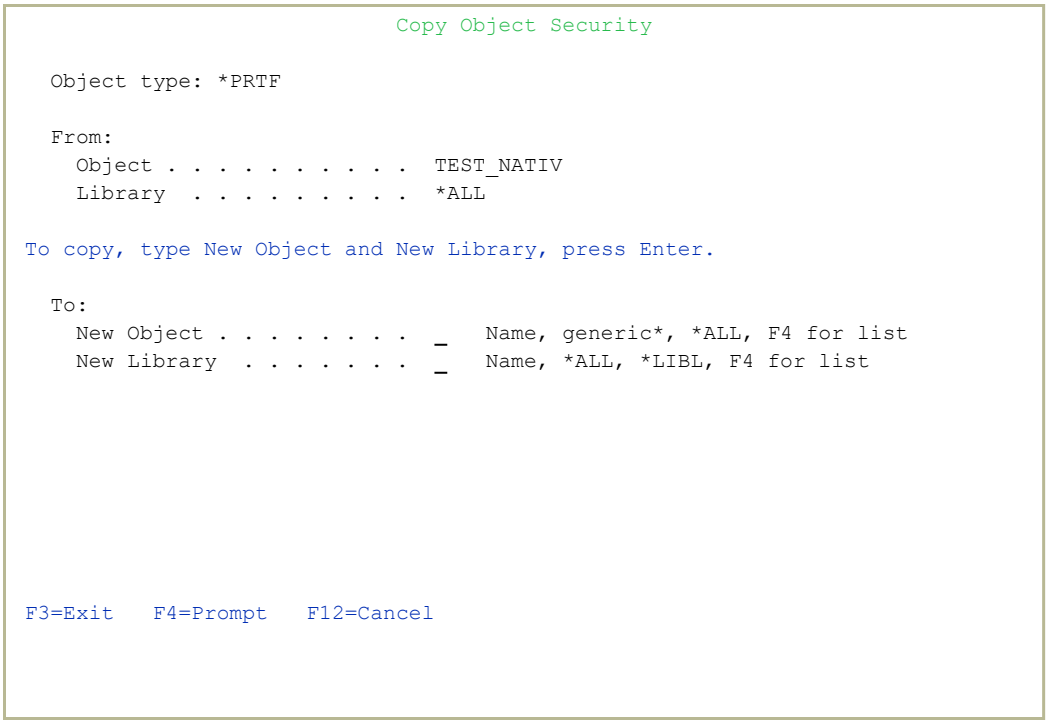
**Open Print File**

If set to **Y**, the user or group may open the print file.

## Copying Firewall Rules for Printer Files

To **copy rules for one printer file to another** that show which users may open them, enter **3** in the **Opt** field for that printer file on the **Work with Native AS/400 Print File Security** screen, as shown in "Setting Firewall Rules for Printer Files" on page 336 (*STRFW* **> 4 > 4**).

The **Copy Object Security** screen appears:




The read-only **Object Type** field shows the type of object for which rules are being copied. For printer files, this is ***PRTF**.

The read-only **Object** and **Library** fields show the object and library for which rules are being copied.

The remaining fields indicate the printer file to which the rules are being copied:

**New Object**

The name of the printer file. This can also be a generic name ending in an asterisk ("*****") or ***ALL**, which refers to all the relevant items in the library named in the next field for which more specific settings have not been created. To see a list of files, place the cursor in this field and press the **F4** key.

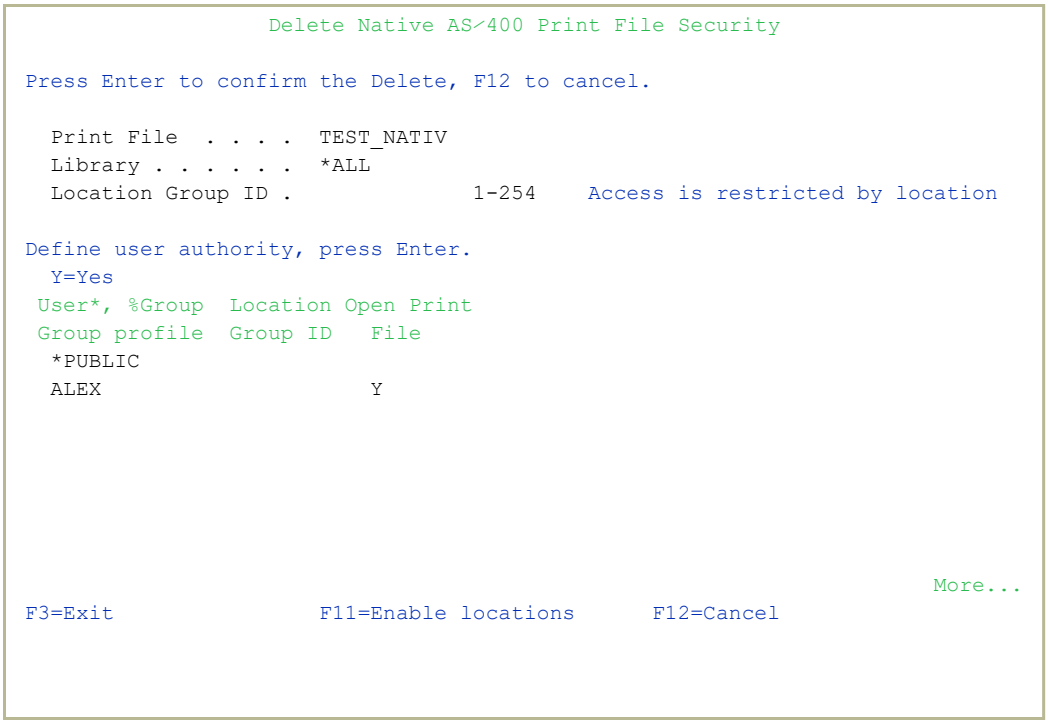
**New Library**

The name of the library containing the printer file. This can also be ***LIBL** or ***ALL**, which refers to all libraries for which more specific settings for that printer file have not been created. To see a list of libraries, place the cursor in this field and press the **F4** key

## Deleting Firewall Rules for Printer Files

To **delete rules that show which users may open a printer file**, enter **4** in the **Opt** field for that printer file on the **Work with Native AS/400 Print File Security** screen, as shown in "Setting Firewall Rules for Printer Files" on page 336 (***STRFW* > 4 > 4**).

The **Delete Native AS/400 Print File Security** screen appears:




All of the fields on the screen are read-only.

To **confirm** the deletion and return to the previous screen, press **Enter**.

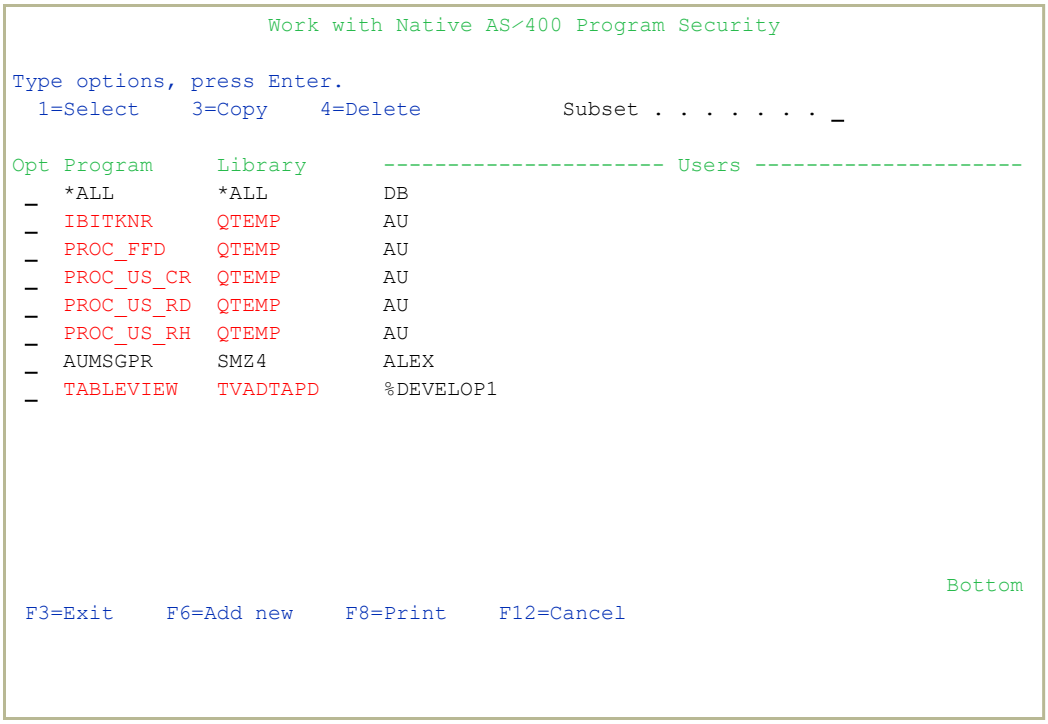
To **cancel** the deletion and return to the previous screen, press the **F12** key.

# Setting Firewall Rules for Programs

You can specify which users can run specific programs through the **Work with Native AS/400 Program Security** screen.

To **filter activity by programs that it would run**, select **5. Programs** from the **Native Object Security** screen, as shown in "Setting Firewall Rules for Native Objects" on page 305 (*STRFW* **> 4**).

The **Work with Native AS/400 Program Security** screen appears:




Each line of the list contains the following fields:

**Program**

The name of the program. This can also be a generic name ending in an asterisk ("*****") or ***ALL**, which refer to all the relevant programs in the library named in the next field for which more specific settings have not been created.

**Library**

The name of the library containing the programs. This can also be a special name beginning with an asterisk ("*****") or ***ALL**, which refers to all the relevant programs in all the relevant libraries. For

example, the program **TEST1** in the Library ***ALL** refers to any program
**TEST1** in any library.

**Users**

A list of up to four users or groups for which particular authorities have been set. If there are more than four, an ellipsis ("...") appears in a fifth column. Selecting the program by entering **1** in the **Opt** field displays a screen with the entire list of users.

To create settings for a **new** program, press the **F6** key. The **Add Native AS/400 Program Security** screen appears, as shown in "Adding Firewall Rules for Programs" on the facing page.

To **print** the information from this screen, press the **F8** key.

To **modify** the settings for a program, enter **1** in the **Opt** field for the program. The **Modify Native AS/400 Program Security** screen appears, as shown in "Modifying Firewall Rules for Programs" on page 349.

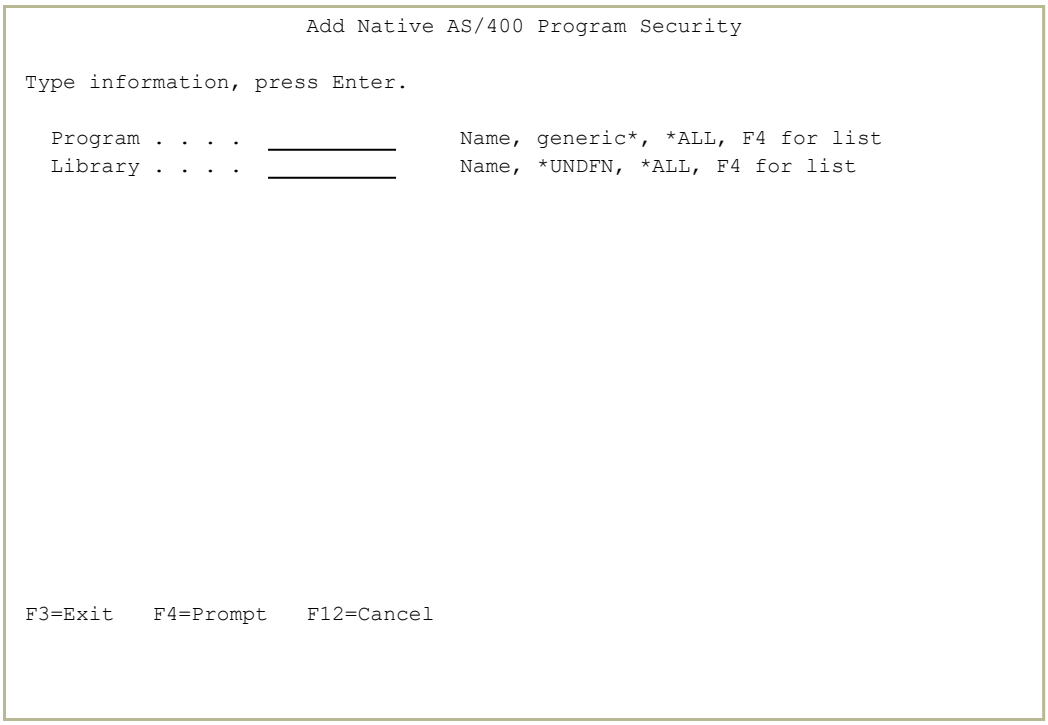
To **copy** settings for one program to another, enter **3** in the **Opt** field for the program. The **Copy Object Security** screen appears, as shown in "Copying Firewall Rules for Programs" on page 351.

To **delete** the settings for a program, enter **4** in the **Opt** field for the program. The **Delete Native AS/400 Program Security** screen appears, as shown in "Deleting Firewall Rules for Programs" on page 353.

## Adding Firewall Rules for Programs

To **add rules for programs** showing which users may run them, press the **F6** key on the **Work with Native AS/400 Program Security** screen, as shown in "Setting Firewall Rules for Programs" on page 345 (*STRFW* **> 4 > 5**).

The **Add Native AS/400 Program Security** screen appears:




Enter information into the following fields:

**Program**

The name of the program. This can also be a generic name ending in an asterisk ("*****") or ***ALL**, which refer to all the relevant items in the library named in the next field for which more specific settings have not been created. Once you have entered a library name in the next field, you can see a list of programs by placing the cursor in this field and pressing the **F4** key.

**Library**

The name of the library containing the print file. This can also be ***UNDFN**, which refers to an undefined value, or ***ALL**, which refers to all libraries for which more specific settings for that print

file have not been created. To see a list of libraries, place the cursor in this field and press the F4 key.

Press Enter to confirm these values. More fields appear on the screen:

```
                      Add Native AS/400 File Security

Type information, press Enter.

  File  . . . . . .  *ALL
  Library . . . . .  *ALL
  Location Group ID .  ___         1-254    Access is restricted by location

Define user authority, press Enter.
  Y=Yes  S=Skip (Allow, no log)
 User*, %Group  Location |----- DATA -----|----------- FILE MANAGEMENT -------|
 Group profile  Group ID | Read     Write |  Create   Delete   Rename   Other |
  *PUBLIC                  _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
  __________               _        _       _        _        _        _
                                                                   More...
F3=Exit   F4=Prompt    F11=Enable locations      F12=Cancel
```

In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may run that program.

In each line of the rest of the screen, you can indicate whether a specified user or group may run the program:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the F4 key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the F11 key.

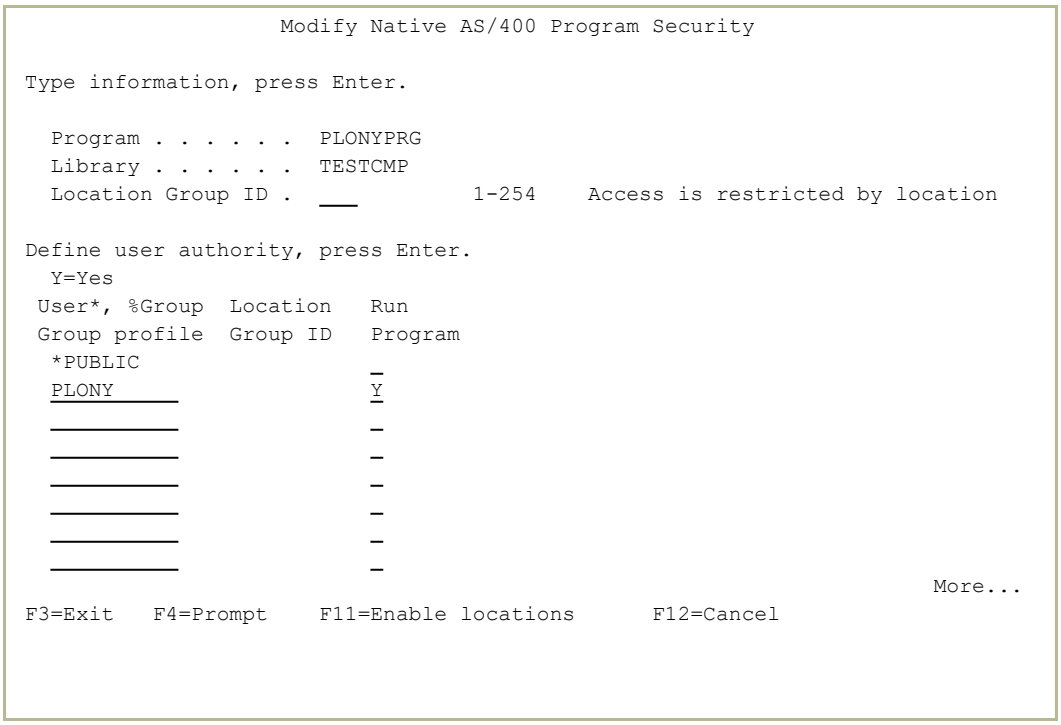
**Run Program**

If set to **Y**, the user or group may run the program.

## Modifying Firewall Rules for Programs

To **modify rules for a program** showing which users may run it, enter **1** in the **Opt** field for that program on the **Work with Native AS/400 Program Security** screen, as shown in "Setting Firewall Rules for Programs" on page 345 (*STRFW* **> 4 > 5**).

The **Modify Native AS/400 Program** screen appears:




The read-only **Program** and **Library** fields show the program and library to which these rules apply.

In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may run that program.

In each line of the rest of the screen, you can indicate whether a specified user or group may run the program:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the **F4** key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the F11 key.

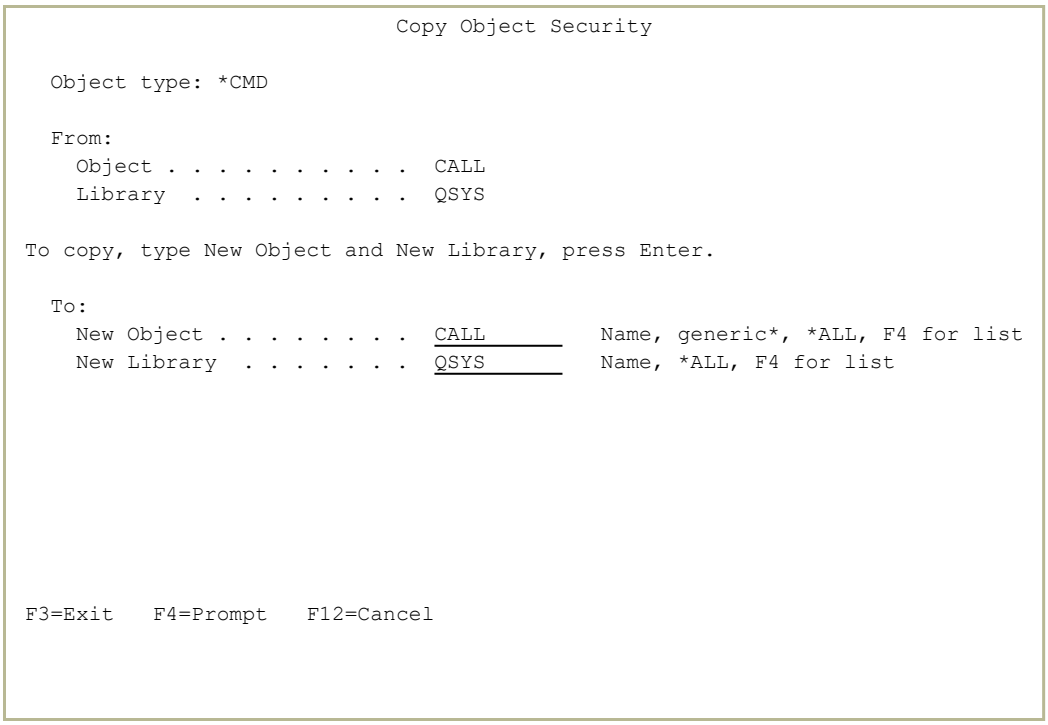
**Run Program**

If set to **Y**, the user or group may run the program.

## Copying Firewall Rules for Programs

To **copy rules for one program to another** that show which users may run them, enter **3** in the **Opt** field for that program on the **Work with Native AS/400 Program Security** screen, as shown in "Setting Firewall Rules for Programs" on page 345 (*STRFW* **> 4 > 5**).

The **Copy Object Security** screen appears:




The read-only **Object Type** field shows the type of object for which rules are being copied. For programs, this is ***PGM**.

The read-only **Object** and **Library** fields show the object and library for which rules are being copied.

The remaining fields indicate the program to which the rules are being copied:

**New Object**

The name of the program. This can also be a generic name ending in an asterisk ("*") or ***ALL**, which refers to all the relevant items in the library named in the next field for which more specific settings have not been created. To see a list of files, place the cursor in this field and press the **F4** key.

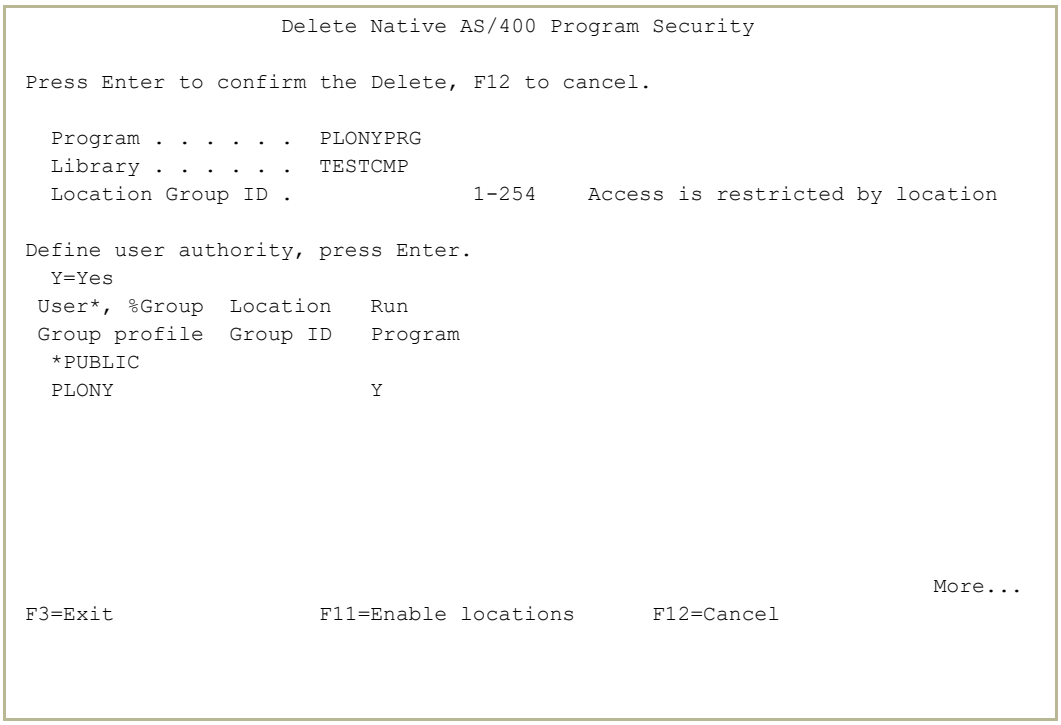
**New Library**

The name of the library containing the program. This can also be ***UNDFN** for undefined values or ***ALL**, which refers to all libraries for which more specific settings for that program have not been created. To see a list of libraries, place the cursor in this field and press the F4 key

## Deleting Firewall Rules for Programs

To **delete rules that show which users may run a program**, enter **4** in the **Opt** field for that program on the **Work with Native AS/400 Program Security** screen, as shown in "Setting Firewall Rules for Programs" on page 345 (*STRFW* **> 4 > 5**).

The **Delete Native AS/400 Program Security** screen appears:




All of the fields on the screen are read-only.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Setting Firewall Rules for Commands

You can specify which users can run specific commands through the **Work with Native AS/400 Command Security** screen.

To **filter activity by commands that it would run**, select **6. Commands** from the **Native Object Security** screen, as shown in "Setting Firewall Rules for Native Objects" on page 305 (*STRFW* **> 4**).

The **Work with Native AS/400 Command Security** screen appears:

```
                    Work with Native AS/400 Command Security

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

Opt Command     Library      ---------------------- Users ----------------------
 _  *ALL        *ALL         *PUBLIC     %DEVELOP1   %DEVELOP2   SECURITY2P
 _  DLTF        *ALL         %DEVELOP1   %DEVELOP2   JAVA
 _  DSPFD       *ALL         %DEVELOP1   %DEVELOP2   JAVA
 _  DSPFFD      *ALL         %DEVELOP1   %DEVELOP2   JAVA
 _  DSPLIBL     *ALL         %DEVELOP1   QSECOFR
 _  CALL        QSYS         %JAVA       QSECOFR     SECURITY2P
 _  DLTUSRSPC   QSYS         %JAVA
 _  SBMJOB      QSYS         JAVA




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

Each line of the list contains the following fields:

**Command**

The name of the command. This can also be a generic name ending in an asterisk ("*****") or ***ALL**, which refer to all the relevant commands in the library named in the next field for which more specific settings have not been created.

**Library**

The name of the library containing the commands. This can also be a special name beginning with an asterisk ("*****") or ***ALL**, which refers to all the relevant libraries. For

example, the command **TEST1** in the Library ***ALL** refers to any command
**TEST1** in any library.

**Users**

A list of up to four users or groups for which particular authorities have been set. If there are more than four, an ellipsis ("...") appears in a fifth column. Selecting the command by entering **1** in the **Opt** field displays a screen with the entire list of users.

To create settings for a **new** command, press the **F6** key. The **Add Native AS/400 Command Security** screen appears, as shown in "Adding Firewall Rules for Commands" on the next page.

To **print** the information from this screen, press the **F8** key.

To **modify** the settings for a file, enter **1** in the **Opt** field for the command. The **Modify Native AS/400 Command Security** screen appears, as shown in "Modifying Firewall Rules for Commands" on page 358.

To **copy** settings for one command to another, enter **3** in the **Opt** field for the command. The **Copy Object Security** screen appears, as shown in "Copying Firewall Rules for Commands" on page 360.

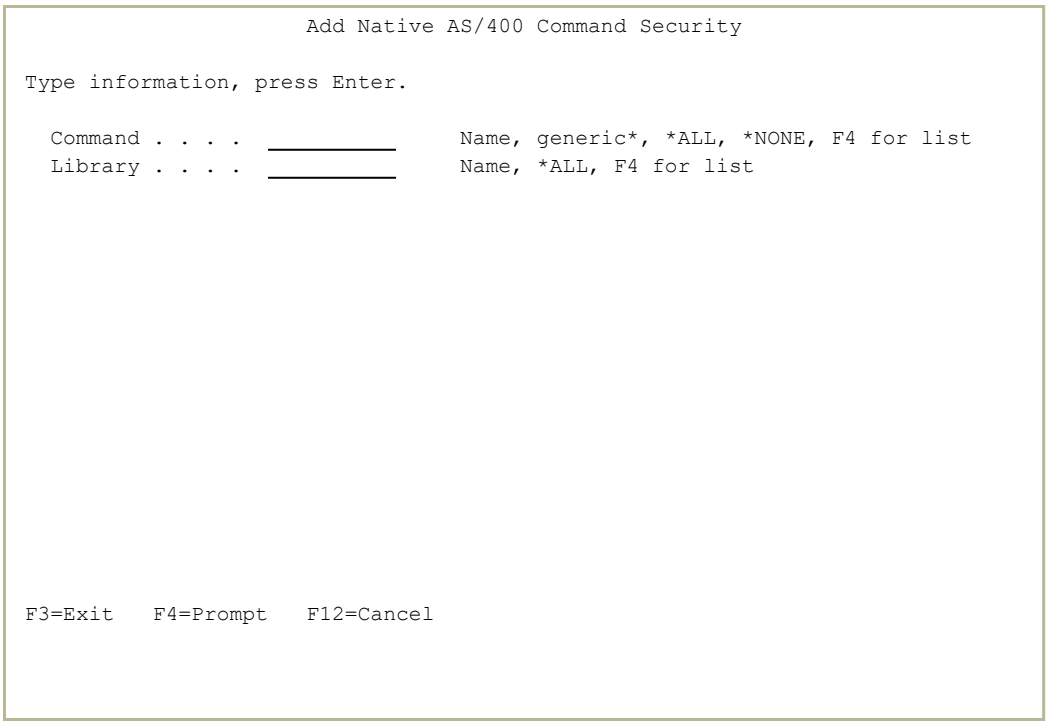
To **delete** the settings for a command, enter **4** in the **Opt** field for the command. The **Delete Native AS/400 Command Security** screen appears, as shown in "Deleting Firewall Rules for Commands" on page 362.

To create and manage **exceptions** to command rules, specifying that Firewall can accept commands that it would normally reject if the commands include specific additional parameters, select **9. Command Exceptions** from the **Native Object Security** screen, as shown in "Setting Firewall Rules for Native Objects" on page 305 (*STRFW* **> 4**).

## Adding Firewall Rules for Commands

To **add rules for commands showing which users may run them**, press the **F6** key on the **Work with Native AS/400 Command Security** screen, as shown in "Setting Firewall Rules for Commands" on page 354 (*STRFW* **> 4 > 6**).

The **Add Native AS/400 Command Security** screen appears:




Enter information into the following fields:

**Command**

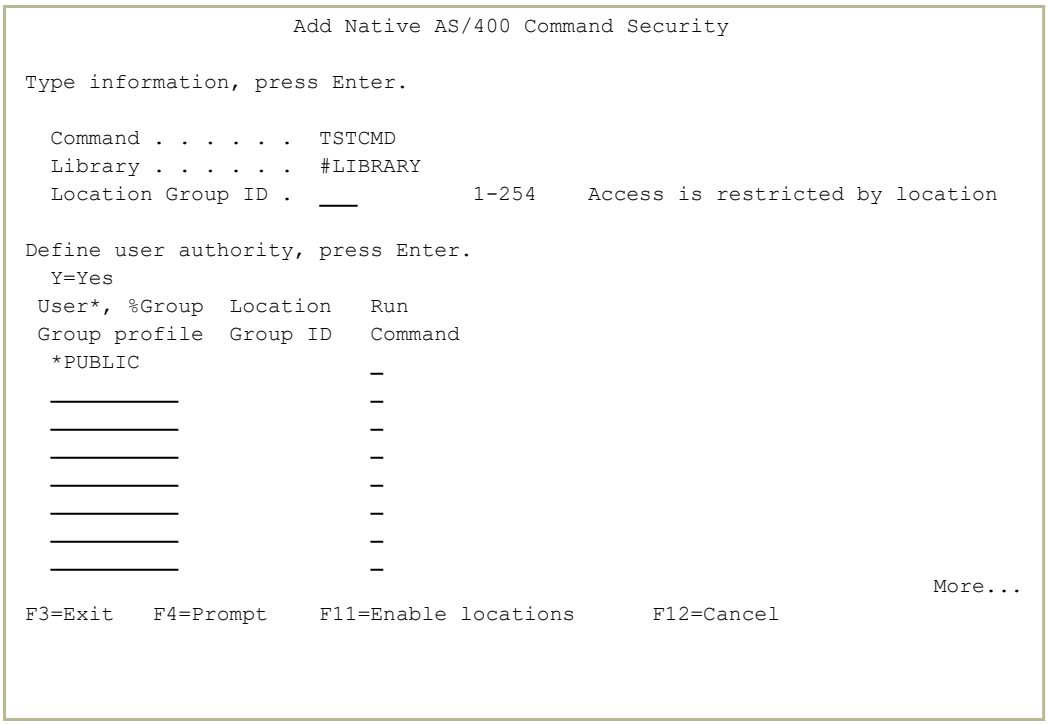
The name of the command. This can also be a generic name ending in an asterisk ("*****") or ***ALL**, which refer to all the relevant items in the library named in the next field for which more specific settings have not been created. Once you have entered a library name in the next field, you can see a list of commands by placing the cursor in this field and pressing the **F4** key.

**Library**

The name of the library containing the print file. This can also be ***UNDFN**, which refers to an undefined value, or ***ALL**, which refers to all libraries for which more specific settings for that print

file have not been created. To see a list of libraries, place the cursor in this field and press the F4 key.

Press Enter to confirm these values. More fields appear on the screen:




In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may run that command.

In each line of the rest of the screen, you can indicate whether a specified user or group may run the command:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the F4 key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the F11 key.

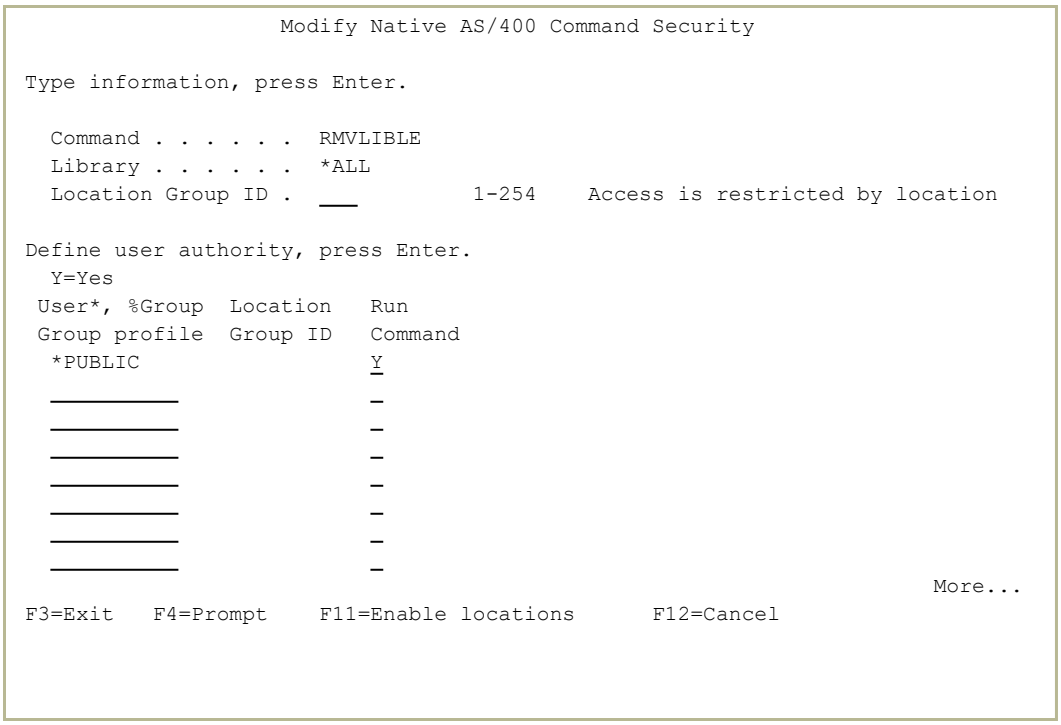
**Run Command**

If set to **Y**, the user or group may run the command.

## Modifying Firewall Rules for Commands

To **modify rules for a command showing which users may run it**, enter **1** in the **Opt** field for that command on the **Work with Native AS/400 Command Security** screen, as shown in "Setting Firewall Rules for Commands" on page 354 (*STRFW* **> 4 > 6**).

The **Modify Native AS/400 Command** screen appears:




The read-only **Command** and **Library** fields show the command and library to which these rules apply.

In the **Location Group ID** field, you can specify a numbered location group from **1** through **254**, as shown in . Only members of that group may run that command.

In each line of the rest of the screen, you can indicate whether a specified user or group may run the command:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the **F4** key.

**Location Group ID**

If location groups are enabled, this rule may be restricted to a given numbered location group. To enable location groups, press the F11 key.

**Run Command**

If set to **Y**, the user or group may run the command.

## Copying Firewall Rules for Commands

To copy rules for one command to another that show which users may run them, enter **3** in the **Opt** field for that command on the Work with Native AS/400 Command Security screen, as shown in "Setting Firewall Rules for Commands" on page 354 (*STRFW* **> 4 > 6**).

The Copy Object Security screen appears:

```
                          Copy Object Security

  Object type: *CMD

  From:
    Object . . . . . .  CALL
    Library  . . . . . .  QSYS

To copy, type New Object and New Library, press Enter.

  To:
    New Object . . . . . .  CALL        Name, generic*, *ALL, F4 for list
    New Library  . . . . . .  QSYS      Name, *ALL, F4 for list

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

The read-only **Object Type** field shows the type of object for which rules are being copied. For commands, this is ***CMD**.

The read-only **Object** and **Library** fields show the object and library for which rules are being copied.

The remaining fields indicate the command to which the rules are being copied:

**New Object**

The name of the command. This can also be a generic name ending in an asterisk ("*****") or ***ALL**, which refers to all the relevant items in the library named in the next field for which more specific settings have not been created. To see a list of files, place the cursor in this field and press the F4 key.

**New Library**

The name of the library containing the command. This can also be ***UNDFN** for undefined values or ***ALL**, which refers to all libraries for which more specific settings for that command have not been created. To see a list of libraries, place the cursor in this field and press the F4 key

## Deleting Firewall Rules for Commands

To **delete rules that show which users may run a command**, enter **4** in the **Opt** field for that command on the **Work with Native AS/400 Command Security** screen, as shown in "Setting Firewall Rules for Commands" on page 354 (***STRFW*** **> 4 > 6**).

The **Delete Native AS/400 Command Security** screen appears:

```
                    Delete Native AS/400 Command Security

Press Enter to confirm the Delete, F12 to cancel.

  Command . . . . . .  CALL
  Library . . . . . .  QSYS
  Location Group ID .              1-254    Access is restricted by location

Define user authority, press Enter.
  Y=Yes
 User*, %Group  Location   Run
 Group profile  Group ID   Command
  *PUBLIC
  %JAVA                    Y
  QSECOFR                  Y
  SECURITY2P               Y




                                                                        More...
F3=Exit                F11=Enable locations      F12=Cancel
```

All of the fields on the screen are read-only.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Creating Exceptions to Command Filtering Rules

Firewall can include exception to the rules for filtering commands. You can specify that Firewall can accept commands that it would normally reject if the commands include specific additional parameters.

To specify exceptions to command rules, select **9. Command Exceptions** from the Native Object Security screen, as shown in "Setting Firewall Rules for Native Objects" on page 305 (*STRFW* > **4**).

The Work with Command Exceptions screen appears.

```
                        Work with Command Exceptions

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

Opt  Beginning of command and parameters                    Users
 _   CALL EVGTST/TDSPPGM (SMZ8 GSEPNTR)                     EVGTST
 _   CALL EVGTST/TDSPPGM PARM(SMZ8 GSEPNTR)                 EVGTST

                                                                    Bottom

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

Each line of the list contains the following fields:

**Command**

The command, with the additional parameters. Rules for running the command with parameters that begin with those shown here override the more general rules for the command.

**Users**

The first user from the list of users for whom this exception is valid. If there are more users, an ellipsis (". . .") follows the name.

When you modify the exception via the **Modify Command Exception** screen, you can see and manage the full list of users.

To create settings for a **new** command exception, press the **F6** key. The **Add Command Exception** screen appears, as shown in "Adding Exceptions to Command Rules" on the facing page.

To **print** the information from this screen, press the **F8** key.

To **display** more information about the command exception, press the **F11** key.

To **modify** a command exception, enter **1** in the **Opt** field for the exception. The **Modify Command Exception** screen appears, as shown in "Modifying Exceptions to Command Rules" on page 368.

To **copy** settings for one command exception to another, enter **3** in the **Opt** field for the exception. The **Copy Command Exception** screen appears, as shown in "Copying Exceptions to Command Rules" on page 370.

To **delete** the settings for a command exception, enter **4** in the **Opt** field for the command. The **Delete Command Exceptions** screen appears, as shown in "Deleting Exceptions to Command Rules" on page 371.

## Adding Exceptions to Command Rules

To **add exceptions to command rules**, press the **F6** key from the **Work with Command Exceptions** screen, as shown in "Creating Exceptions to Command Filtering Rules" on page 363 (*STRFW* **> 4 > 9**).

The **Add Command Exception** screen appears:

```
                          Add Command Exception

Type information, press Enter.

Command . . .  _____________________________________________________________
               _____________________________________________________________

Commands which are about to be rejected based on the Firewall rules are
reviewed against this Command Exception to see if an exception that would
allow them exists.

Specify the command and its parameters up to the position you wish to check.
The test will ignore quotes and double-quotes.
Multiple blanks are treated as a single blank.
Do not put Asterisks at the end.









F3=Exit    F12=Cancel
```

Type the beginning of the command exception in the Command field, including the parameters that must begin the command for it to be excluded. For example, the entered command might be "*CALL PARM1 PARM2*".

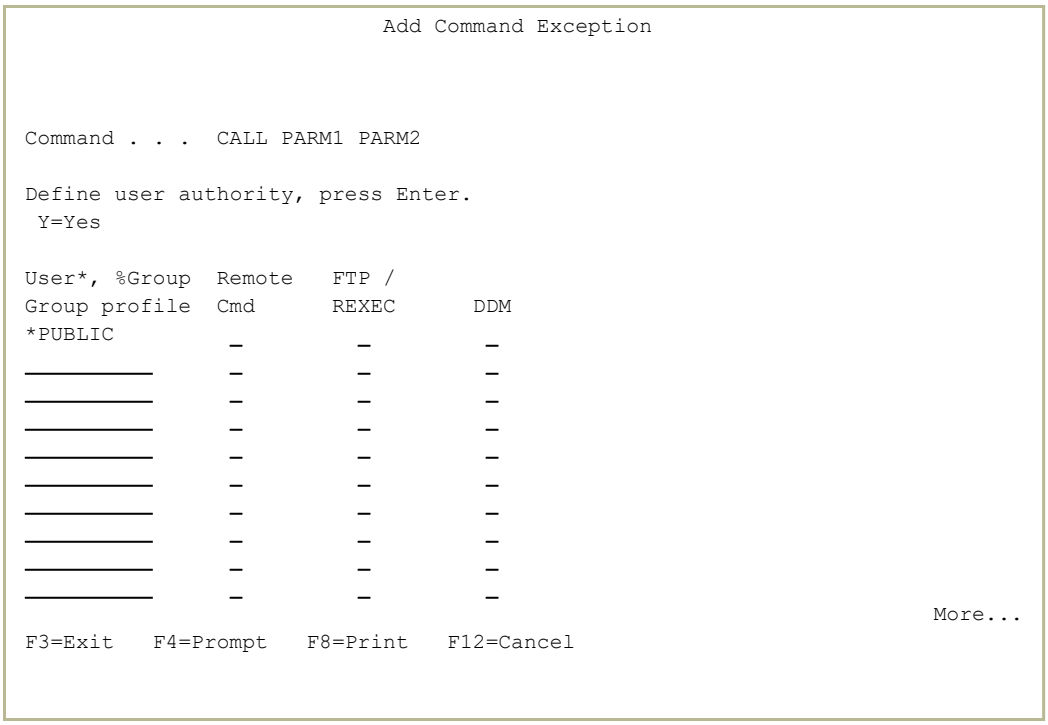
For an entered command to match the exception, its initial characters, though the length of the string entered here, must match precisely, except that:

- Quotation marks (**'**) and double quotes (**"**) are ignored
- Multiple consecutive blanks are considered as a single blank

In entering the string,

- The command must not end with an asterisk ("*****").

When you have the command, press **Enter**. More fields appear on the screen:




The list that appears specifies users and the protocols that they might be using for which the exception is being made.

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the F4 key. The value **%PUBLIC** refers to all users for whom other exceptions have not been set for this command.

**Remote Cmd**

If set to Y, the user may run the command with these parameters via the Remote Command protocol.

**FTP/REXEC**

If set to Y, the user may run the command with these parameters via the FTP or REXEC protocols.

**DDM**

If set to Y, the user may run the command with these parameters via the DDM protocol.

Thus, for example, if

- the **Command** field is set to **CALL THISPARM THATPARM**
- The **User*, %Group, Group profile** is set to **%PLONYGRP**
- the **DDM** field is set to **Y**

members of the group **%PLONYGRP** may run commands beginning with *CALL THISPARM THATPARM* via the **DDM** protocol, even if the *CALL* command would normally be rejected.

To print the list of exceptions from this screen, press the F8 key.

## Modifying Exceptions to Command Rules

To **modify exceptions to command rules**, involving the users and protocols for which the exception is allowed, enter **1** in the **Opt** field for that command on the **Work with Command Exceptions** screen, as shown in "Creating Exceptions to Command Filtering Rules" on page 363 (*STRFW* **> 4 > 9**).

To **modify the command string itself**, copy the exceptions from the old command to the new one, (as shown in "Copying Exceptions to Command Rules" on page 370) then delete the old one (as shown in "Deleting Exceptions to Command Rules" on page 371).

The **Modify Command Exception** screen appears:

```
                          Modify Command Exception



Command . . .  CALL EVGTST/TDSPPGM (SMZ8 GSEPNTR)

Define user authority, press Enter.
 Y=Yes

User*, %Group  Remote   FTP /
Group profile  Cmd      REXEC      DDM
*PUBLIC          _        _         _
EVGTST           _        _         _
_____            _        _         _
_____            _        _         _
_____            _        _         _
_____            _        _         _
_____            _        _         _
_____            _        _         _
_____            _        _         _
_____            _        _         _
                                                                  More...
F3=Exit   F4=Prompt   F8=Print   F12=Cancel
```

The read-only Command field shows the command for which the exceptions are made.

For an entered command to match the exception, its initial characters, through the length of the string entered here, must match precisely, except that:

- Quotation marks (**'**) and double quotes (**"**) are ignored
- Multiple consecutive blanks are considered as a single blank

In entering the string,

- The command must not end with an asterisk ("*****").

The remaining fields show the users and protocols for whom the exception is valid:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the F4 key. The value **%PUBLIC** refers to all users for whom other exceptions have not been set for this command.

**Remote Cmd**

If set to Y, the user may run the command with these parameters via the Remote Command protocol.

**FTP/REXEC**

If set to Y, the user may run the command with these parameters via the FTP or REXEC protocols.

**DDM**

If set to Y, the user may run the command with these parameters via the DDM protocol.

Thus, for example, if

- the **Command** field is set to **CALL THISPARM THATPARM**
- The **User*, %Group, Group profile** is set to **%PLONYGRP**
- the **DDM** field is set to **Y**

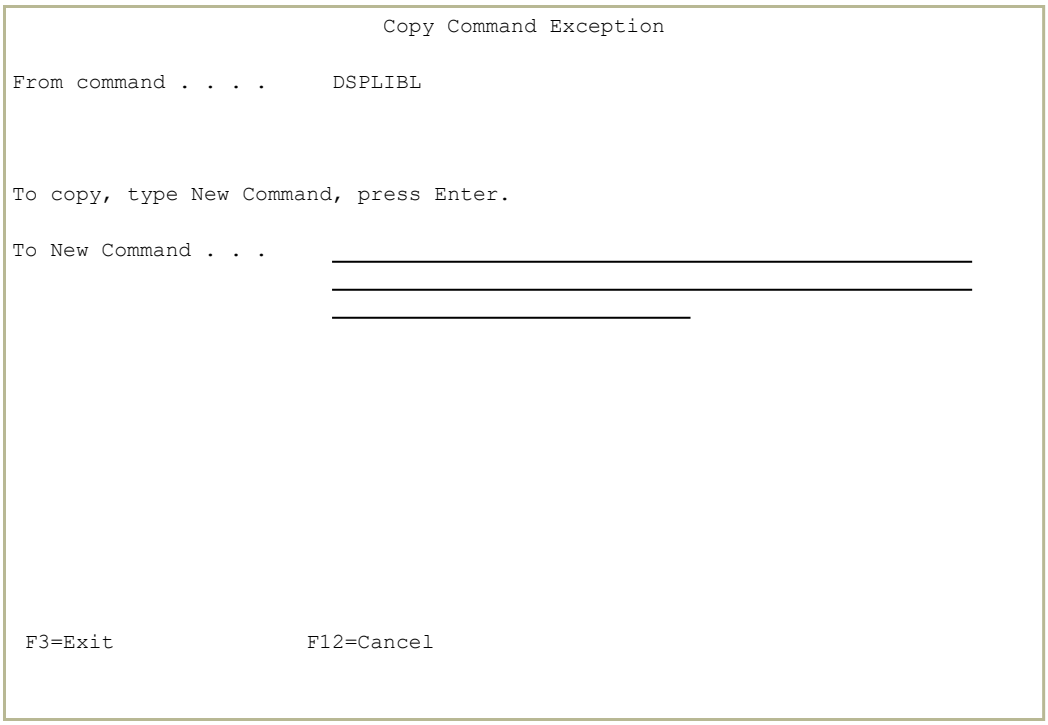
members of the group **%PLONYGRP** may run commands beginning with *CALL THISPARM THATPARM* via the **DDM** protocol, even if the *CALL* command would normally be rejected.

To print the list of exceptions from this screen, press the F8 key.

## Copying Exceptions to Command Rules

To **copy exceptions to command rules** from one command string to another, enter **3** in the **Opt** field for that command on the **Work with Command Exceptions** screen, as shown in "Creating Exceptions to Command Filtering Rules" on page 363 (*STRFW* **> 4 > 9**).

The **Copy Command Exception** screen appears:




The read-only **From command** field shows the command from which you are copying the exception.

Enter the new command to which the exceptions are to be copied, into the **To New Command** field.

For an entered command to match the new command string, its initial characters, through the length of the string entered here, must match precisely, except that:

- Quotation marks (**'**) and double quotes (**"**) are ignored
- Multiple consecutive blanks are considered as a single blank

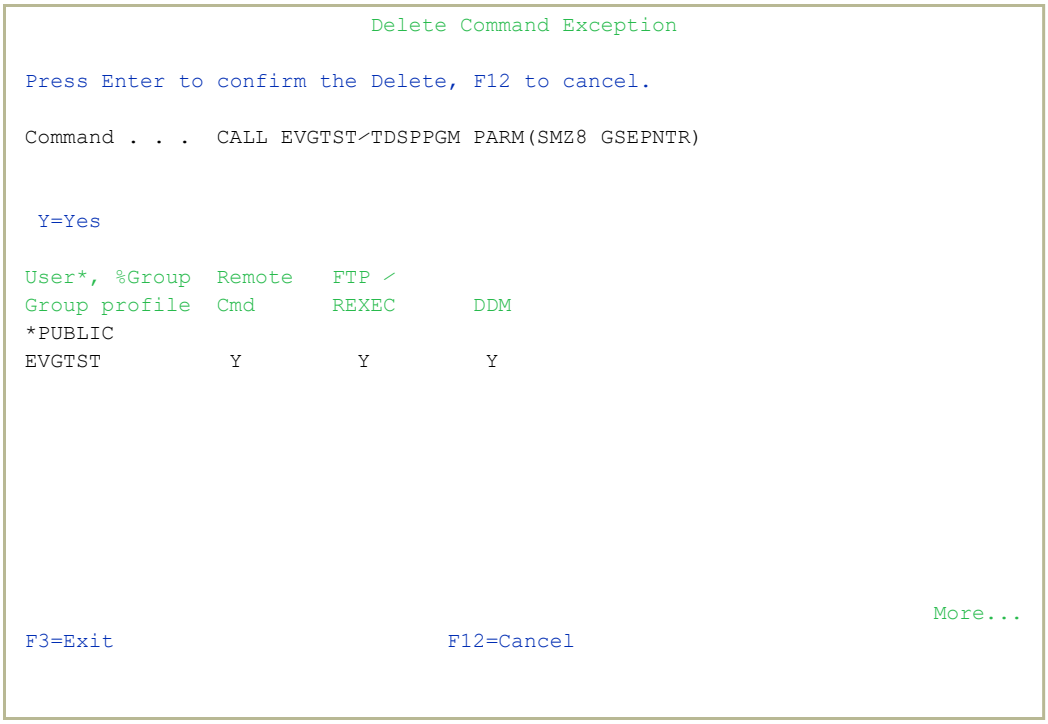
In entering the string,

- The command must not end with an asterisk ("*****").

## Deleting Exceptions to Command Rules

To **delete exceptions to command rules**, enter **4** in the **Opt** field for that command on the **Work with Command Exceptions** screen, as shown in "Creating Exceptions to Command Filtering Rules" on page 363 (*STRFW* **> 4 > 9**).

The **Delete Command Exception** screen appears:



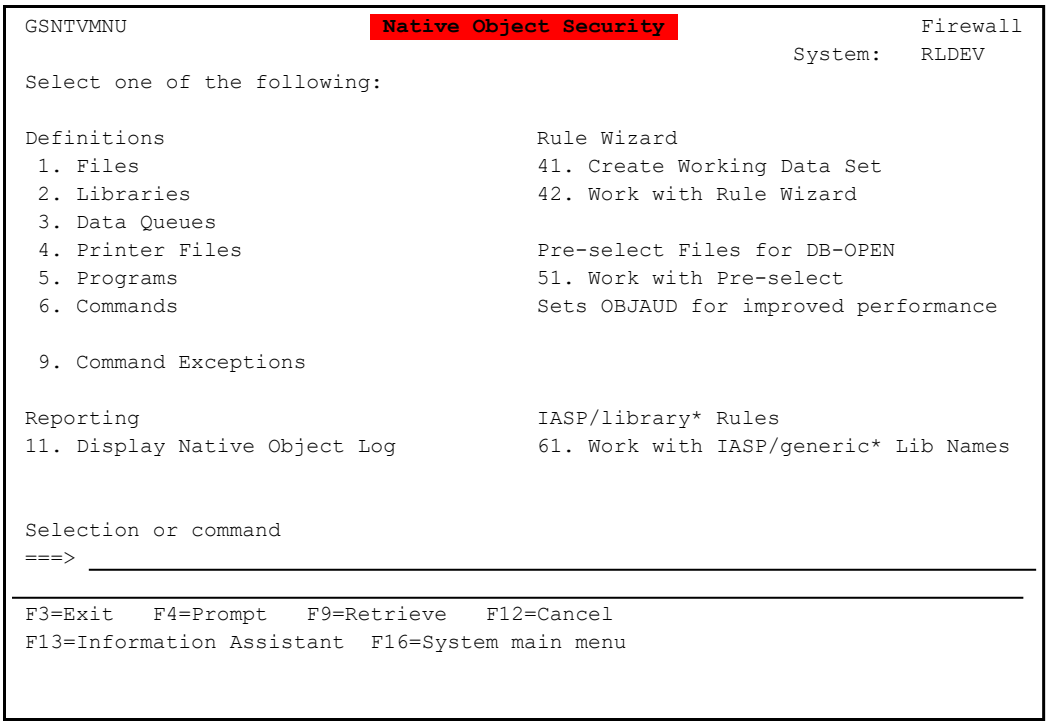

All of the fields on the screen are read-only.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

# Using the Rule Wizard for Native Objects

Using the Rule Wizard, you can analyze recent activity on your system and use that information to create and modify Firewall rules.




To **create a data set** for examining activity and developing rules for incoming activity based on native objects on which it requests to operate, select **`41. Create Working Data Set`** from the **Native Object Security** screen (*STRFW* **`> 4`**).

The **Summarize Native AS/400 Log (CPRNTVSEC)** screen appears, as shown in "Creating a Data Set on Native Objects with the Rule Wizard" on the facing page.

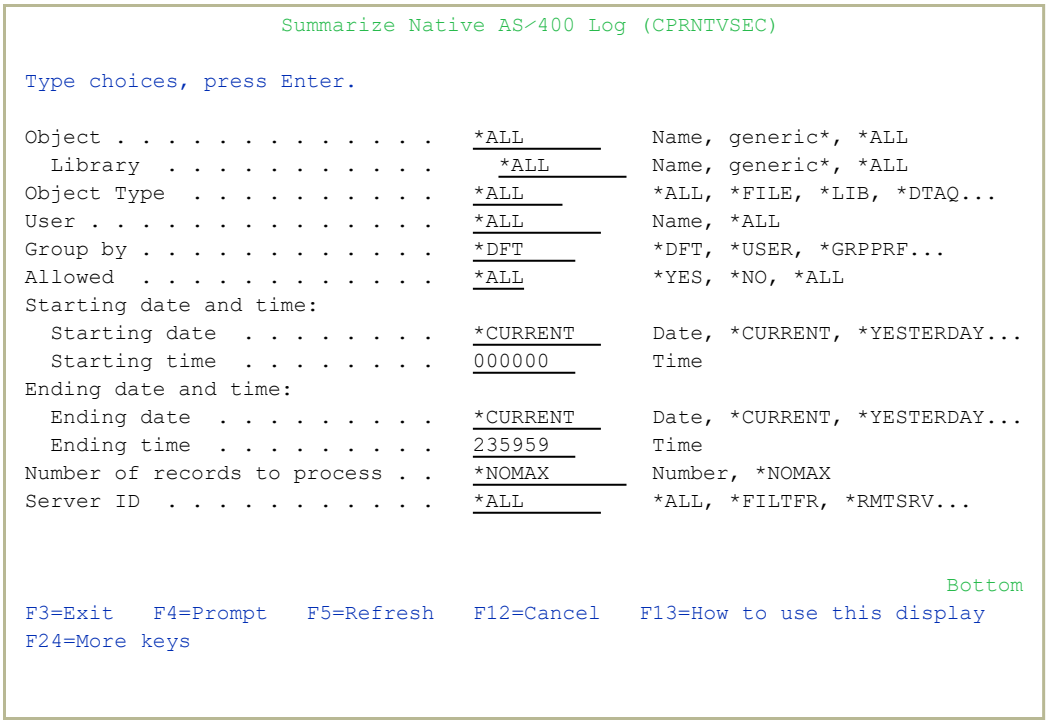
To **use an existing data set** to develop rules, select **`42. Work with Rule Wizard`** from the **Native Object Security** screen (*STRFW* **`> 4`**).

The **Native AS/400 Objects Wizard (WZRNTVSEC)** screen appears, as shown in "Analyzing Recent Data on Native Objects with the Rule Wizard" on page 379,

## Creating a Data Set on Native Objects with the Rule Wizard

To **create a data set** for examining activity and developing rules for outgoing activity based on native objects on which it requests to operate, select **41. Create Working Data Set** from the **Native Object Security** screen *(STRFW > 4*).

The **Summarize Native AS/400 Log (CPRNTVSEC)** screen appears.




The screen contains the following fields. Fields that have values other than the defaults are preceded by the "**>**" character:

**Object**

The object on which the activity requests to operate. This can be the name of the specific object, a generic name ending in an asterisk ("*****"), or ***ALL** for all objects.

**Library**

The library containing the object on which the activity requests to operate. This can be the name of the specific library, a generic name ending in an asterisk ("*****"), or ***ALL** for all libraries.

**Object Type**

The type of object on which the activity requests to operate. Possible values include:

- ***ALL**: All objects
- ***FILE**: Files
- ***LIB**: Libraries
- ***DTAQ**: Data queues
- ***PRTF**: Printer files
- ***PGM**: Programs
- ***CMD**: Commands

**User, <GrpPrf or '%GROUP'**

The user or group requesting the activity. This can be a user name, a generic* name, a group name, a group profile, or ***ALL** for all users.

**Group by**

How the result are grouped in the data set. Possible values include:

- ***DFT**: The default grouping of data within rule wizards, as set in the **Wizard Group by** parameter in the **Firewall General Definitions** screen.
- ***USER**: Grouped by the user name.
- ***GRPPRF**: If a user is a member of a single group, the user's activity is included under the group.
  Otherwise, the activity is shown under the username.
- ***USRGRP**: If the user is a member of multiple groups, the user's activity is included under the first of those groups.
  Otherwise, the activity is shown under the username.
- ***GROUP**: If the user is a member of a single group, the user's activity is included under that group.
  Otherwise, if the user is a member of multiple groups, the user's activity is listed under the first of those groups.
  Otherwise (if the user is not a member of any groups), the activity is shown under the username.

- ***ALLGRP**: If the user is a member of a single group plus up to fifteen supplemental groups. the user's activity is shown for each of those groups.
- ***ALL**: If the user is a member of a single group plus up to fifteen supplemental groups. the user's activity is shown for each of those groups.

  Otherwise, if the user is a member of multiple groups, the user's activity is listed under the first of those groups.

  Otherwise (if the user is not a member of any groups), the activity is shown under the username.

**Allowed**

Specifies whether the data set includes rejected activity, accepted activity, or both.

- ***YES**: Include only accepted activity
- ***NO:** Include only rejected activity
- ***ALL:** Include both accepted and rejected activity

**Starting data and time**

**Starting date**

The day or date on which the included data begins.

Allowed values include:

- ***CURRENT**: The current date
- ***YESTERDAY**: Yesterday's date
- ***WEEKSTR**: The first day of the current week. By default, this is Sunday.
- ***PRVWEEKS**: The first day of the previous week
- ***MONTHSTR**: The first day of the current month
- ***PRVMONTHS**: The first day of the previous month
- ***YEARSTR**: The first day of the current year
- ***PRVYEARS**: The first day of the previous year
- ***MON**: Monday
- ***TUE**: Tuesday
- ***WED**: Wednesday
- ***THU**: Thursday
- ***FRI**: Friday

- ***SAT**: Saturday
- ***SUN**: Sunday

**Starting time**

The time on the Starting date at which the included data begins, in **HHMMSS** format.

**Ending date**

The day or date on which the included data ends.

Allowed values are the same as for **Starting date**.

**Ending time**

The time on the Starting date at which the included data ends, in **HHMMSS** format.

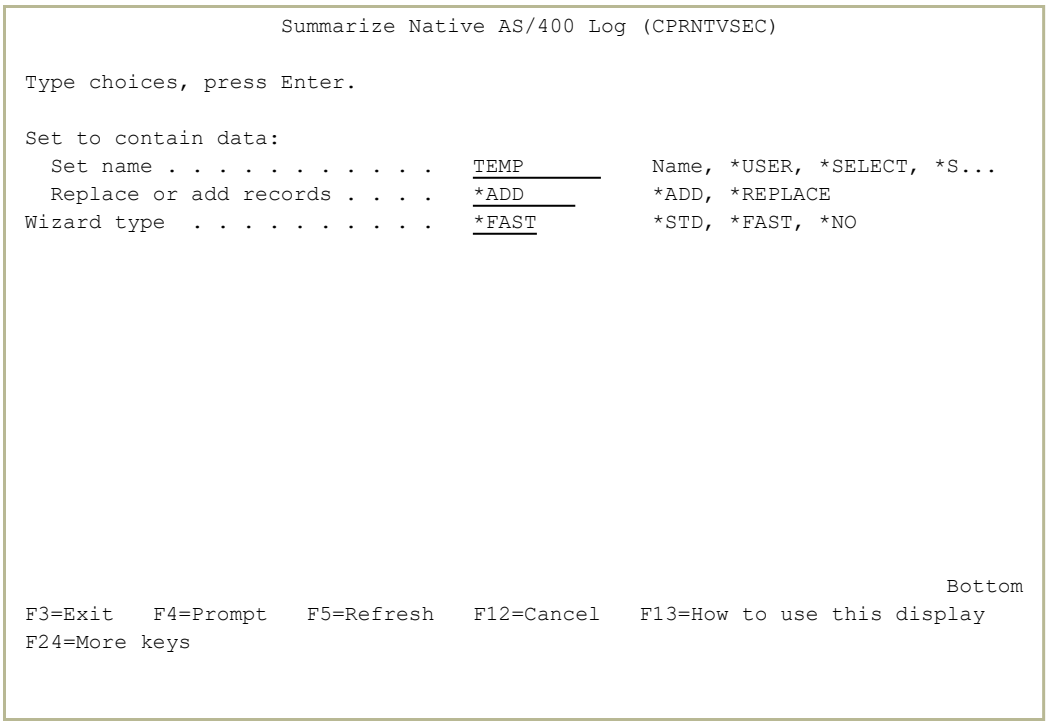
**Number of records to process**

Collect no more than this number of records. If set to ***NOMAX**, collect all the relevant records.

**Server ID**

The server that the activity is attempting to access. To see a list of possible values, press the F4 key.

When you press Enter, more fields appear. Press the Page Down key to display them:




## Set to contain data

### Set name

The name of the data set that will contain the records. You can set this to your own value or choose one of these options:

- ***TEMP**: The default name for temporary data sets. The data set is removed when the session ends.
- ***USER**: Your user name
- ***S**: Equivalent to ***SELECT**
- ***SELECT**: If the wizard has been run before, a list appears of previous names that had been used for the data set.

### Replace or add records

If any records already exist in the data set, whether to replace them or add the new records to them.

Possible values include:

- ***ADD**: Add new records to the existing set
- ***REPLACE**: Replace all existing records with the new ones.

**Wizard type**

The type of wizard to be created. Possible values include:

- ***STD**: The Rule Wizard screen that appears next has all the standard options
- ***FAST**: The Rule Wizard screen that appears next has a limited set of options for faster processing, as documented there.
- ***NO**: The data set will only be used to batch processing.

To list and select possible values for many of the fields, place the cursor within the field and press the F4 key.

To reset the values on the screen to their default values, press the F5 key.

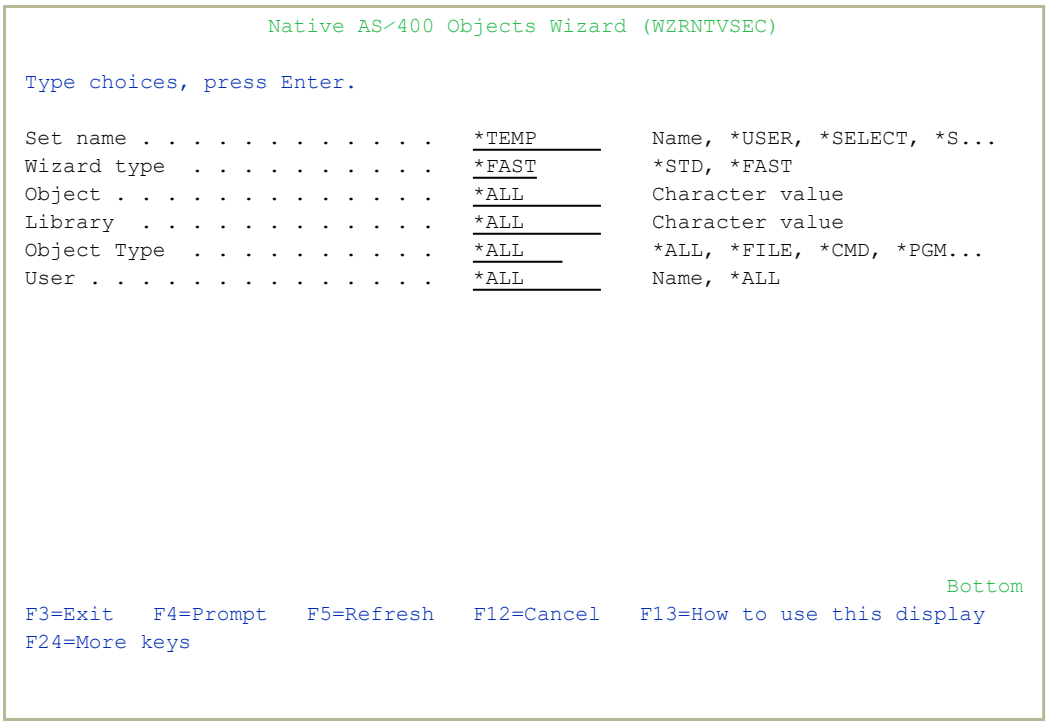
# Analyzing Recent Data on Native Objects with the Rule Wizard

The Rule Wizards analyze data on recent system activity to develop and improve rules for filtering future activity.

To **develop rules to filter incoming activity by the native object** on which it is requesting to operate, first create a data set of recent activity, as shown in "Creating a Data Set on Native Objects with the Rule Wizard" on page 373.

Once you have created a data set, select **`42. Work with Rule Wizard`** from the **Native Object Security** screen (*STRFW* **`> 4`**).

The **Native AS/400 Objects Wizard (WZRNTVSEC)** screen appears:




To select the existing data set and additional specifications to use with the wizard, enter values in the following fields:

**`Set name`**

The name of the data set that will contain the records. You can set this to your own value or choose one of these options:

- ***TEMP**: The default name for temporary data sets. The data set is removed when the session ends.
- ***USER**: Your user name
- ***S**: Equivalent to ***SELECT**
- ***SELECT**: If the wizard has been run before, a list appears of previous names that had been used for the data set.

**Wizard type**

The type of wizard to be created. Possible values include:

- ***STD**: The Rule Wizard screen that appears next has all the standard options
- ***FAST**: The Rule Wizard screen that appears next has a limited set of options for faster processing, as documented there.
- ***NO**: The data set will only be used to batch processing.

**Object**

The object on which the activity requests to operate. This can be the name of the specific object, a generic name ending in an asterisk ("*****"), or ***ALL** for all objects.

**Library**

The library containing the object on which the activity requests to operate. This can be the name of the specific library, a generic name ending in an asterisk ("*****"), or ***ALL** for all libraries.

**Object Type**

The type of object on which the activity requests to operate. Possible values include:

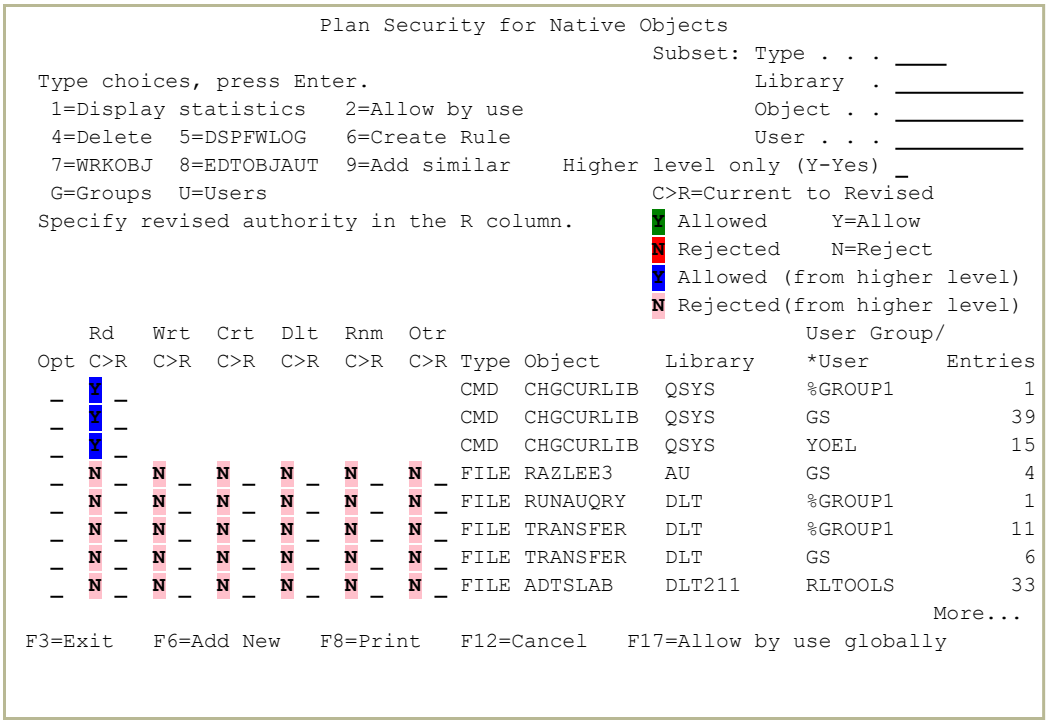
- ***ALL**: All objects
- ***FILE**: Files
- ***LIB**: Libraries
- ***DTAQ**: Data queues
- ***PRTF**: Printer files
- ***PGM**: Programs
- ***CMD**: Commands

**User, <GrpPrf or '%GROUP'**

The user or group requesting the activity. This can be a user name, a generic* name, a group name, a group profile, or ***ALL** for all users.

After entering the specifications, press **Enter**.

The **Plan Security for Native Objects** screen appears:




Each line on the lower part of the screen represents requests within the data set by a single user or group to access a single object.

After the **Opt** field, the first six pairs of fields show ways that objects can be accessed. (Some are not possible, and therefore not included, for some types of objects.)

- **Rd**: Read
- **Wrt**: Write
- **Crt**: Create
- **Dlt**: Delete
- **Rnm**: Rename
- **Otr**: Other

The **pairs of fields** for each are:

- a **letter** on a colored background, showing how Firewall responded to the activity according to current rules
- an **underscore** in which you can revise the rule

The **letter codes** are:

- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

The **color codes** are:

- **Green**: A rule specifically referring to this user or group and object accepts this activity
- **Red**: A rule specifically referring to this user or group and object rejects this activity
- **Blue**: A rule for a generic set of users, groups, or objects that includes this one accepts this activity
- **Purple**: A rule for a generic set of users, groups, or objects that includes this one rejects this activity

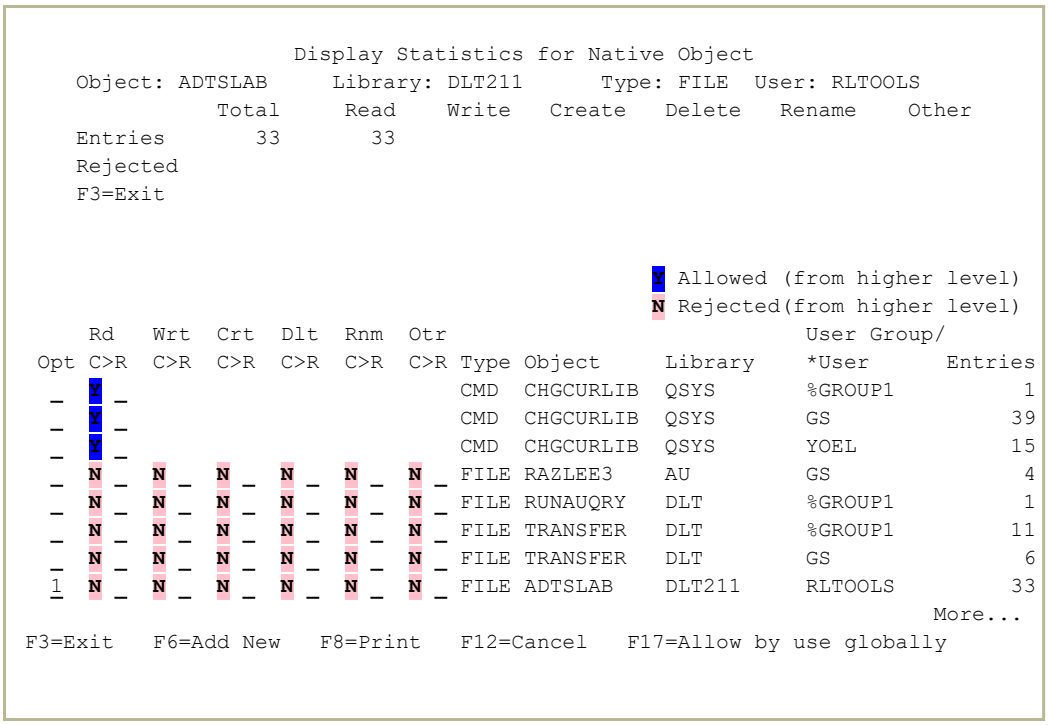
The following fields show the object **Type**, the **Object** name, and the **Library** that contains it.

The **User Group/*User** field shows the name of the user or group whose made the requests.

The **Entries** field shows the number of requests made during the time period in the data set.

Thus, for example, the first item on the bottom of the screen shows that the user **RLTOOLS** is allowed, because of a group or generic set of users to which it or the object belongs, to read the **file** named **ADTSLAB** in the **DLT211** library, and had requested to do so **33** times within the time period of the data set.

To **view the statistics** on activity by a specific user or group on a specific object during the time period in the data set, type **1** in the **Opt** column for that row and press **Enter**. The **Display Statistics for Native Object** window appears.



```
                  Display Statistics for Native Object
   Object: ADTSLAB     Library: DLT211      Type: FILE  User: RLTOOLS
              Total     Read    Write   Create   Delete   Rename    Other
   Entries       33       33
   Rejected
   F3=Exit


                                                  Y Allowed (from higher level)
                                                  N Rejected(from higher level)
     Rd   Wrt  Crt  Dlt  Rnm  Otr                              User Group/
 Opt C>R  C>R  C>R  C>R  C>R  C>R Type Object     Library     *User      Entries
  _  Y _                          CMD  CHGCURLIB  QSYS        %GROUP1          1
  _  Y _                          CMD  CHGCURLIB  QSYS        GS              39
  _  Y _                          CMD  CHGCURLIB  QSYS        YOEL            15
  _  N _  N _  N _  N _  N _  N _ FILE RAZLEE3    AU          GS               4
  _  N _  N _  N _  N _  N _  N _ FILE RUNAUQRY   DLT         %GROUP1          1
  _  N _  N _  N _  N _  N _  N _ FILE TRANSFER   DLT         %GROUP1         11
  _  N _  N _  N _  N _  N _  N _ FILE TRANSFER   DLT         GS               6
  1  N _  N _  N _  N _  N _  N _ FILE ADTSLAB    DLT211      RLTOOLS         33
                                                                       More...
F3=Exit   F6=Add New   F8=Print   F12=Cancel   F17=Allow by use globally
```

Continuing from the previous example, we see that the user requested to access the file 33 times. All of them were for Read access and none of them was rejected.

To **add** a new rule, press the **F6** key. The **Add Native AS/400 Revised Security** screen appears, as shown in "Analyzing Recent Data on Native Objects with the Rule Wizard" on page 379.

To **add a rule for an object and a user or group similar** to an existing one, enter **9** in the **Opt** field for that rule. The **Add Similar Revised Security** screen appears, as shown in "Adding Firewall Rules for Native Files" on page 309.

To **change rules based on activity** in the data set, enter **2** in the **Opt** field. If a rule had set a particular activity on an object by a user or group to be rejected, a specific new rule is set for that activity, object, and user to accept it. Otherwise, the option has no effect. NOTE: If the rule is changed, it disappears from the screen.

To **change rules manually**, see "Setting Firewall Rules Manually based on Native Objects with the Rule Wizard" on page 387

To **delete** a rule, enter **4** in the **Opt** field for that rule. NOTE: You are not prompted for confirmation, and the rule is immediately deleted.

To **display the firewall log** entries relevant to this rule, enter **5** in the **Opt** field for that rule. The **Display Firewall Log** screen appears, as shown in "Displaying Firewall Logs" on page 516.

To **view a list of the users in a group**, enter **G** in the **Opt** column for that group. The **List of Users in User Group** window appears, listing the users in the group.

To **view a list of the groups containing a user**, enter **U** in the **Opt** column for that group. The **List of Users in Group Profile** window appears, listing the users in the group.

To **work with the object** in a rule, enter **7** in the **Opt** column for the rule. The OS/400 **Work with Objects** screen appears.

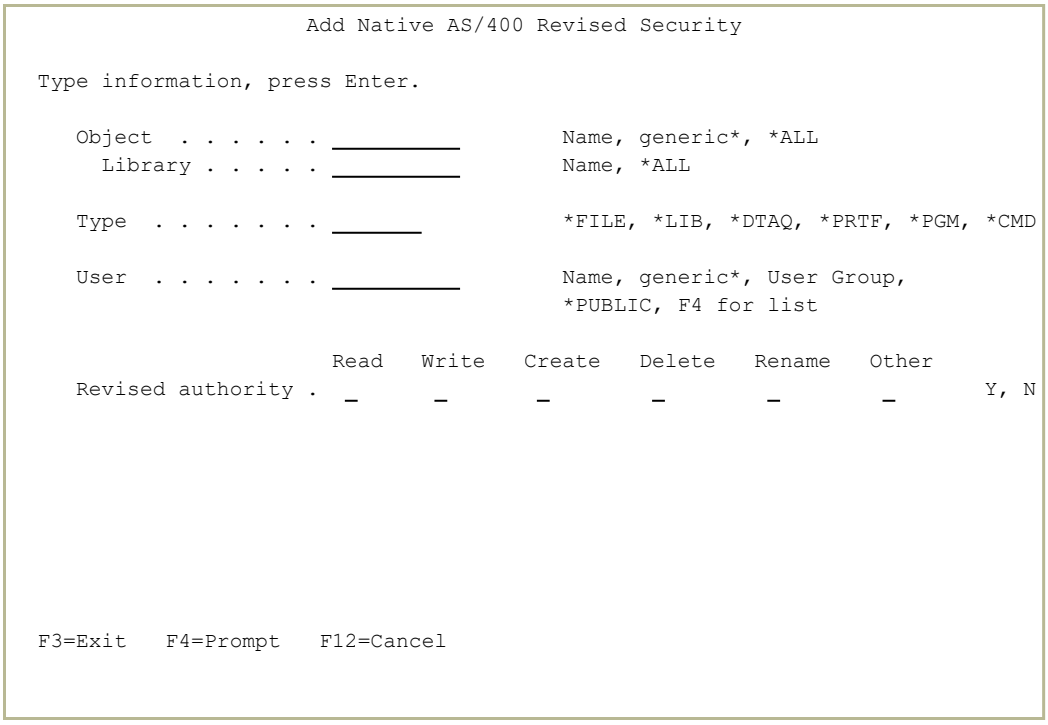
To **edit the object authority** for the object in a rule, enter **8** in the **Opt** column for the rule. The OS/400 **Edit Object Authority** screen appears, as described in IBM documentation.

To **print** the information from the data set, press the **F8** key.

## Adding Firewall Rules for Native Objects with the Rule Wizard

To **add firewall rules to filter activity by the native objects** on which it would operate via the Rule Wizard, press the **F6** key from the **Plan Security for Native Objects** screen, shown in "Analyzing Recent Data on Native Objects with the Rule Wizard" on page 379 (***STRFW > 4 > 42***).

The **Add Native AS/400 Revised Security** screen appears:




The first four fields on the screen specify the objects and users to which the rule would apply:

**Object**

The object on which the activity requests to operate. This can be the name of the specific object, a generic name ending in an asterisk ("*****"), or ***ALL** for all objects.

**Library**

The library containing the object on which the activity requests to operate. This can be the name of the specific

library, a generic name ending in an asterisk ("*****"), or ***ALL** for all libraries.

**Type**

The type of object on which the activity requests to operate. To see a set of possible values, press the F4 key.

**User, <GrpPrf or '%GROUP'**

The user or group requesting the activity. This can be a user name, a generic* name, a group name, a group profile, or ***ALL** for all users.

The **Revised Authority** fields indicate whether the user or group may perform each of a set of operations (**Read**, **Write**, **Create**, **Delete**, **Rename**, or **Other**) on the object. Set these to **Y** to accept the requests or **N** to reject them. If a field is left blank, it inherits the value from the next higher group, up through ***PUBLIC**.

## Setting Firewall Rules Manually based on Native Objects with the Rule Wizard

NOTE: You can only set Firewall rules manually with the rule wizard if you have set the **Wizard type** to ***STD** when opening the wizard.

To **set rules manually based on the users or groups** requesting the activity in the Rule Wizard, open the **Plan User Security** screen, as shown in "Analyzing Recent Data on Users and Groups with the Rule Wizard" on page 291 (*STRFW* **> 2 > 42**).

```
                      Plan Security for Native Objects
                                                 Subset: Type . . . ____
Type choices, press Enter.                               Library  . __________
 1=Display statistics   2=Allow by use                   Object . . __________
 4=Delete  5=DSPFWLOG   6=Create Rule                    User . . . __________
 7=WRKOBJ  8=EDTOBJAUT  9=Add similar    Higher level only (Y-Yes) _
 G=Groups  U=Users                       C>R=Current to Revised
Specify revised authority in the R column.  Y Allowed     Y=Allow
                                            N Rejected    N=Reject
                                            Y Allowed (from higher level)
                                            N Rejected(from higher level)
    Rd   Wrt  Crt  Dlt  Rnm  Otr                              User Group/
Opt C>R  C>R  C>R  C>R  C>R  C>R Type Object     Library     *User      Entries
 _  Y _                          CMD  CHGCURLIB  QSYS        %GROUP1          1
 _  Y _                          CMD  CHGCURLIB  QSYS        GS              39
 _  Y _                          CMD  CHGCURLIB  QSYS        YOEL            15
 _  N _  N _  N _  N _  N _  N _ FILE RAZLEE3    AU          GS               4
 _  N _  N _  N _  N _  N _  N _ FILE RUNAUQRY   DLT         %GROUP1          1
 _  N _  N _  N _  N _  N _  N _ FILE TRANSFER   DLT         %GROUP1         11
 _  N _  N _  N _  N _  N _  N _ FILE TRANSFER   DLT         GS               6
 _  N _  N _  N _  N _  N _  N _ FILE ADTSLAB    DLT211      RLTOOLS         33
                                                                      More...
F3=Exit   F6=Add New   F8=Print   F12=Cancel   F17=Allow by use globally
```

Enter new values in the second field of each column for which you want to change access in the rows for the appropriate rule. You can enter **Y** to accept requests or **N** to reject requests.

NOTE: While the **Current** line may show a **V** for servers for which access is determined by the verbs used, the setting can only be changed to that via the **Modify Server Verb Authority** screen, as shown in "Modifying Firewall Settings for a User based on Server Verbs" on page 253.

In this example, to accept requests to read the file **ADTSLAB** in the library **DLT211** by the user **RLTOOLS**, type **Y** in the second column under **Rd** in the last line on the screen.

When you have entered the letters for the changes in the appropriate columns, enter **6** in the **Opt** field for the rule.

The rule that you have changed disappears from the screen. You can see its changed value by checking the Definitions screen for that object, as shown in "Setting Firewall Rules for Native Objects" on page 305.

## Adding Firewall Rules for a Similar Native Object with the Rule Wizard

To **add firewall rules for a combination of a user or group requesting access to an object similar to an existing one** via the Rule Wizard, type **9** in the **Opt** field for the original rule from the **Plan Security for Native Objects** screen, shown in "Analyzing Recent Data on Native Objects with the Rule Wizard" on page 379 (***STRFW* > 4 > 42**) then press **Enter**.

The **Add Similar Revised Security** screen appears:

```
                        Add Similar Revised Security

 Modify data at least in one of the fields - New Object/Library/User.
 Modify data in field New Revised authority (optionally).
 Press Enter.


   New Object  . . . . .   CA          Name, generic*, *ALL
     New Library . . . .   DLT211       Name, *ALL

   Type  . . . . . .   *FILE

   New User  . . . . . .   RLTOOLS      Name, generic*, User Group,
                                        *PUBLIC, F4 for list

                           Read   Write   Create   Delete   Rename   Other
   New Revised authority    _      _       _        _        _        _    Y, N




  F3=Exit   F4=Prompt   F12=Cancel
Modify data, or press Enter to confirm.
```

The first four fields on the screen show the values from the original rule as defaults. You can change each of them except **Type** to represent the new object:

**New Object**

The object on which the activity requests to operate. This can be the name of the specific object, a generic name ending in an asterisk ("*****"), or ***ALL** for all objects.

**New Library**

The library containing the object on which the activity requests to operate. This can be the name of the specific library, a generic name ending in an asterisk ("*****"), or ***ALL** for all libraries.

**Type**

The type of object on which the activity requests to operate. To see a set of possible values, press the F4 key.

**New User**

The user or group requesting the activity. This can be a user name, a generic* name, a group name, or ***PUBLIC** for all users.

The **New Revised Authority** fields indicate whether the user or group may perform each of a set of operations (**Read**, **Write**, **Create**, **Delete**, **Rename**, or **Other**) on the object. Set these to **Y** to accept the requests or **N** to reject them. If a field is left blank, it inherits the value from the next higher group, up through ***PUBLIC**.

## Defining Files for Firewall to Track

While Firewall can track and log all accesses to all of your data files, this can place a heavy load on your resources. Some files are less critical than others and do not need to be watched as intently.

As shown in "Controlling DBOPEN and SQL Access" on page 148, you can set Firewall to

- track attempts to access a limited set of files and
- limit the types of accesses that it tracks to
    - only those that change the files or
    - only those specified in the user profile of the person requesting the access.

Defining the set of files takes place in two stages:

- Planning and creating the set of files
- Checking and implementing the changes.

## Planning Changes to the Set of Files that Firewall Tracks

To plan changes to the set of files, select **51. Plan Object Auditing** from the Native Object Security screen (*STRFW > 4*) as shown in "Setting Firewall Rules for Native Objects" on page 305.

The Work with Object Auditing Plan screen appears:

```
                      Work with Object Auditing Plan

Type options, press Enter.                          Position to . _________
  1=Modify  3=Copy  4=Remove  5=Check library       Subset  . . . _______________

Opt Library     Object      Type        Value
 _  SMZ1DTA     *ALL        *FILE       *CHANGE
 _  TZION       *ALL        *FILE       *CHANGE
 _  VICTOR      *ALL        *FILE       *CHANGE

                                                                          Bottom
F3=Exit  F6=Add new(based on cursor)  F12=Cancel  F13=Repeat  F14=Clear repeat
```

The body of the screen lists files that Firewall is to track. For each it shows the standard **Opt** field followed by:

**Library**

A library containing the files.

**Object**

The name or generic* name of the files within the library. If set to ***ALL**, all files in the library are tracked.

**Type**

The type of objects to be tracked. This is always ***FILE**.

**Value**

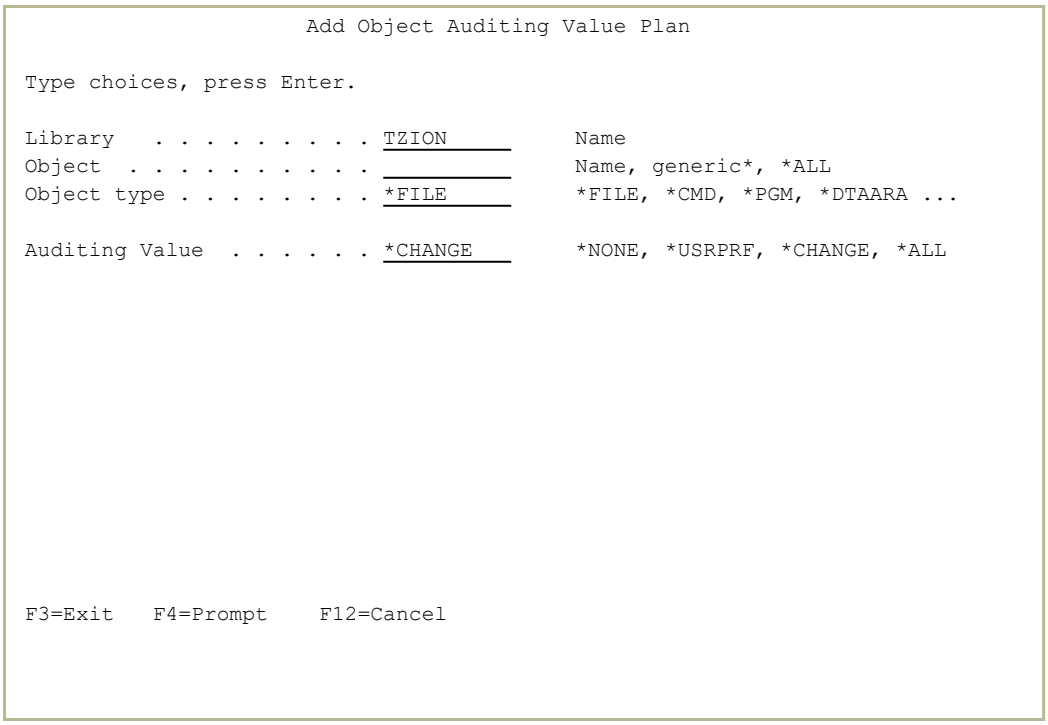
The access attempts that Firewall tracks for these files. The auditing value can be:

- ***NONE**: No access attempts.
- ***USRPRF**: Set by the user's profile definition.
- ***CHANGE**: Attempts to change the file or its contents, but not attempts to read it.
- ***ALL**: All access attempts.

## Adding Files for Firewall to Track

To **add a new set of files** for Firewall to track, place the cursor in the **Opt** field of a line for similar files on the **Work with Object Auditing Plan** screen, and press the **F6** key.

The **Add Object Auditing Value Plan** screen appears:




The fields that appear correspond to those on the previous screen. Values for several fields are filled with those from the original item.

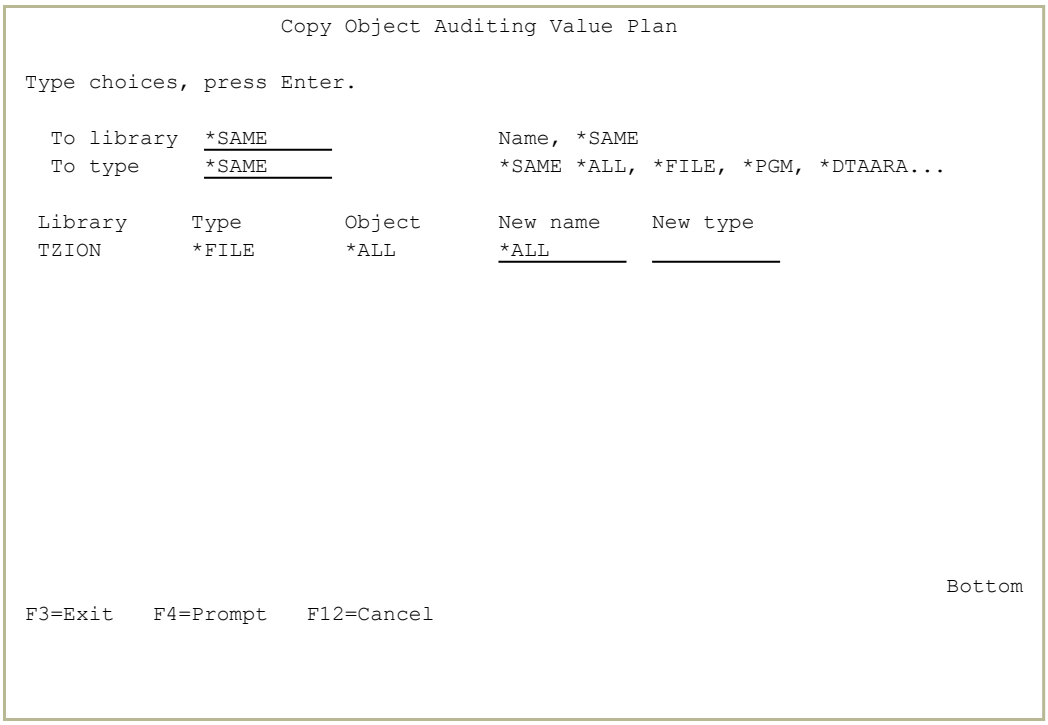
Change the auditing values to those for the new set of files and press **Enter**. To confirm the values, press **Enter** again.

The **Work with Object Auditing Plan** screen reappears with the new item added.

## Copying Auditing Values for Files

To **copy the auditing values from one set of files to another**, enter **3** in the **Opt** field for the item on the **Work with Object Auditing Plan** screen.

The **Copy Object Auditing Value Plan** screen appears:




The fields at the top of the screen show the location of the new set of files:

**To library**

The library containing the new group of files. To keep the same library as the original set, use the default value of ***SAME**.

**To type**

The type of files to be considered. When defining files for Firewall to examine, this is always ***FILE**.

The body of the screen has lines for each copy to be made. After the standard **Opt** field, the **Library**, **Type**, and **Object** fields show the values of the original set. The remaining two are:

**New name**

For the specification for the new group of files within the library specified in the **To library** field. This can be a name, a

generic* name, or ***ALL**.

**New type**

The object type of new group of files, if it differs from the type set in the **To type** field. When defining files for Firewall to examine, this is always ***FILE**, so it can be left blank.

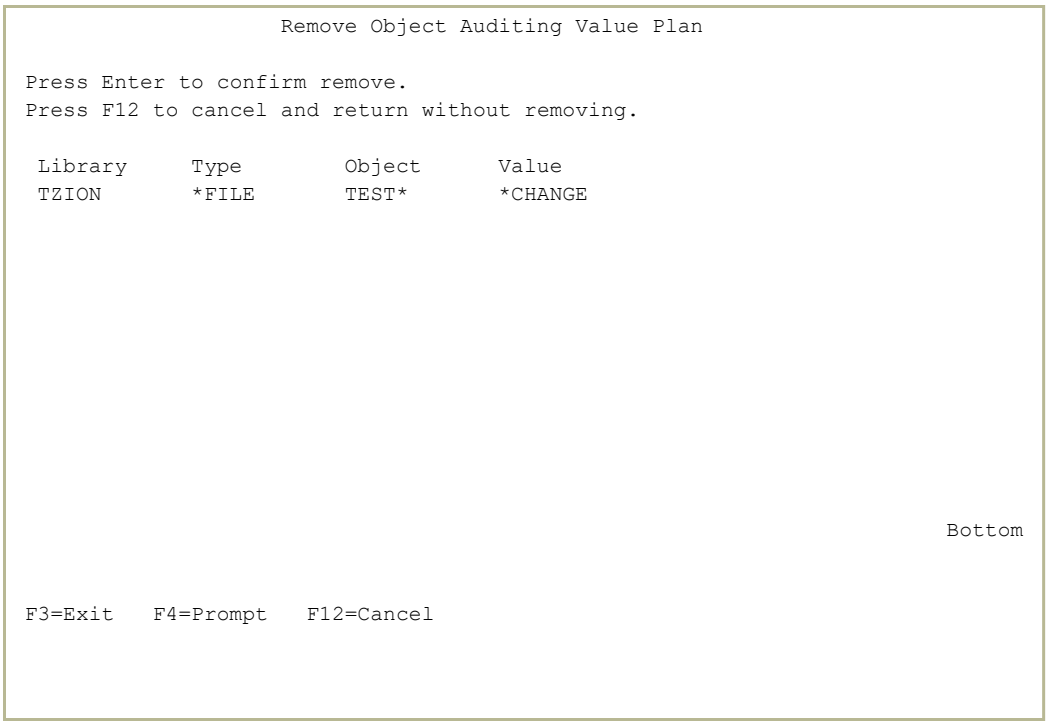
When you have entered values into the needed fields, press Enter. Fields that had been left blank are filled in with values based on what was entered in other fields. To confirm the changes, press Enter again.

The Work with Object Auditing Plan screen reappears with the new items added.

## Removing Files from the Set for Firewall to Track

To **remove files from the set** that Firewall examines, enter **4** in the **Opt** field for the item on the **Work with Object Auditing Plan** screen.

The **Remove Object Auditing Value Plan** screen appears:




The body of the screen shows the set of files that you had selected for removal.

To **confirm the removal**, press **Enter**.

To **cancel the removal**, press the **F12** key.

The **Work with Object Auditing Plan** screen reappears.

## Checking and Implementing Changes to the Set of Files that Firewall Tracks

To **check the changes that are planned** to the set of files before implementing them, select **`52. Check Object Auditing`** from the **Native Object Security** screen (*STRFW > 4*) as shown in "Setting Firewall Rules for Native Objects" on page 305.

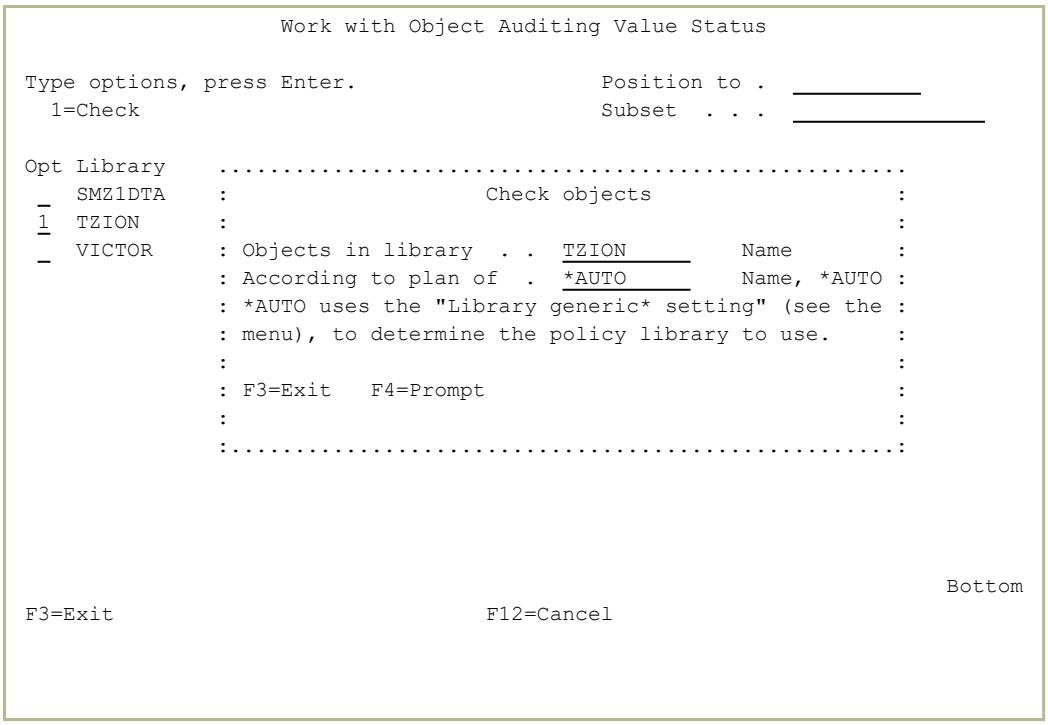
The **Work with Object Auditing Value Status** screen appears:

```
                    Work with Object Auditing Value Status

Type options, press Enter.                  Position to .  _________
  1=Check                                   Subset  . . .  _______________

Opt Library
 _  SMZ1DTA     FileScope  Temporary library (A)
 _  TZION
 _  VICTOR      Victor training

                                                                    Bottom
F3=Exit                              F12=Cancel
```

Each line on the body of the screen lists the name and a free-form text description of each library that contains files that Firewall is currently examining or will examine once the changes are set.

To **see the current and planned auditing values** for each file within the library, enter **`1`** in the **`Opt`** field for that line.

The **Check Objects** window appears.




The window contains two fields:

**Objects in library**

The name of the library containing the files.

**According to plan of**

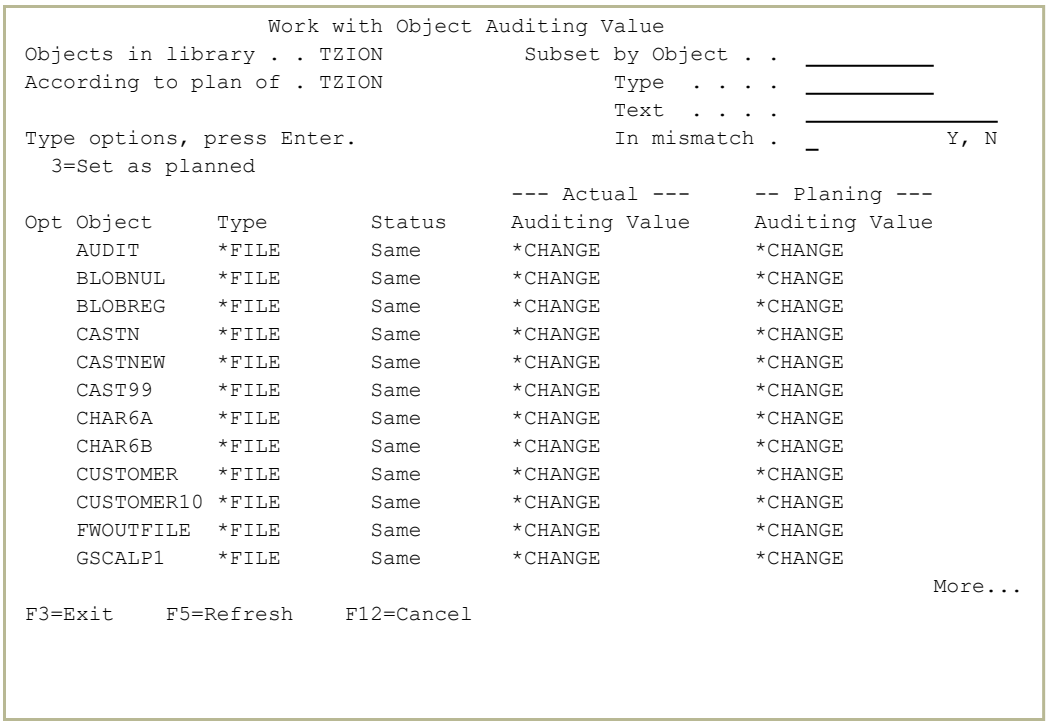
Firewall can check the contents of one library according to the rules for another one.

To use the rules for a different library, enter its name in this field.

To use a predefined setting for another library to use, as shown in "Substituting Firewall Rules for Native Objects with Rules from a Policy Library" on page 402 set this field to ***AUTO**.

To view the files in the library, press Enter.

The Work with Object Auditing Value screen appears.




The body of the screen contains a line for each file in the library.

To see only files for which change is planned, type **Y** in the **Is mismatch** field toward the top of the screen and press Enter.

To see only files for which change is not planned, enter **N** in the **Is mismatch** field toward the top of the screen and press Enter.

For each file, it shows these fields:

**Opt**

This standard field is only available for files that are set to be changed.

**Object**

The name of the file.

**Type**

The type of object. In this context, it is always ***FILE**.

**Status**

If a change is planned, Not same. If change is planned, Same.

**Actual Auditing Value**

The current auditing value for the file. The value can be:

- ***NONE**: No access attempts.
- ***USRPRF**: Set by the user's profile definition.
- ***CHANGE**: Attempts to change the file or its contents, but not attempts to read it.
- ***ALL**: All access attempts.

**Planned Auditing Value**

The planned auditing value for the file. If no change in value is planned, it is the same as the previous field.

To implement the changes for a file, enter **3** in the Opt field on the line for that file. The standard Change Object Auditing (CHGOBJAUD) screen appears. Press Enter to confirm the change.

# Substituting Firewall Rules for Native Objects with Rules from a Policy Library

You can direct Firewall to use its rules for one library for others. In this way, if you set the rules for that policy library, you can apply them to multiple other libraries and work with that single set rather than having to keep a separate set of rules for each library.

To **substitute rules** for one library with the rules for others, select **61. Work with IASP/generic* Lib Names** from the **Native Object Security** screen (*STRFW* **> 4**), as shown in "Setting Firewall Rules for Native Objects" on page 305.

The **Work with ASP/generic* Library Names** screen appears:

```
                    Work with ASP/generic* Library Names
Check the rules of the Policy Library for objects in an ASP/generic* library.

Type options, press Enter.
  1=Select  4=Delete                                Subset . . . _________
                      Policy
Opt  ASP  Library*    Library
 _        DEMO        TESTDB
 _        DEMO2       DB
 _        QGP*        X
 _        TESTBOX     QQQQQQQ
 _    33  QGPL        QGPLIASP




                                                                      Bottom
Use this screen to eliminate repetitive rules in cases where there is a set
of libraries which require similar Native Object rules.
For testing purposes only, the check will be conducted on the Template Library.
F3=Exit    F6=Add new    F8=Print    F12=Cancel
```

The body of the screen contains lines representing each single or generic* library for which rules from another library are substituted. After the standard **Opt** field, the fields are:

**ASP**

If the library is in an Auxiliary Storage Pool, the number of the ASP.

**Library***

The name or generic name of the library that uses rules from a policy library

**Library**

The library from which the rules are substituted.

To **add** a new rule substitution, press the **F6** key. The **Add Policy Library** appears, with the same fields as on this screen. Enter the values for the libraries for and from which rules are to be replaced.

To **modify** the listing for a library, changing the policy library from which the rules are substituted for it, enter **1** in the **Opt** field for that library. The **Modify Policy Library** appears, in which you can make that change.

To **delete** a listing, so that rules will no longer be substituted for a library, enter **4** in the **Opt** field for that library. The **Delete Policy Libraries** screen appears, confirming the deletion.

# Setting Firewall Rules for IFS Objects

To **filter activity on IFS Objects**, select **5. IFS Objects** from the main Firewall screen and press **Enter**.

The **IFS Security** screen appears.

```
 GSIFSMNU                          IFS Security                        Firewall
                                                                System:   S520
Select one of the following:

Definitions                                 Rule Wizard
 1. IFS Object Usage                        41. Create Working Data Set
                                            42. Work with Rule Wizard
Reporting
11. Display IFS Log

                                            IASP/IFS handling
                                            61. IASP/IFS Prefix Replacement




Selection or command
===> _____________________________________________________________________

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

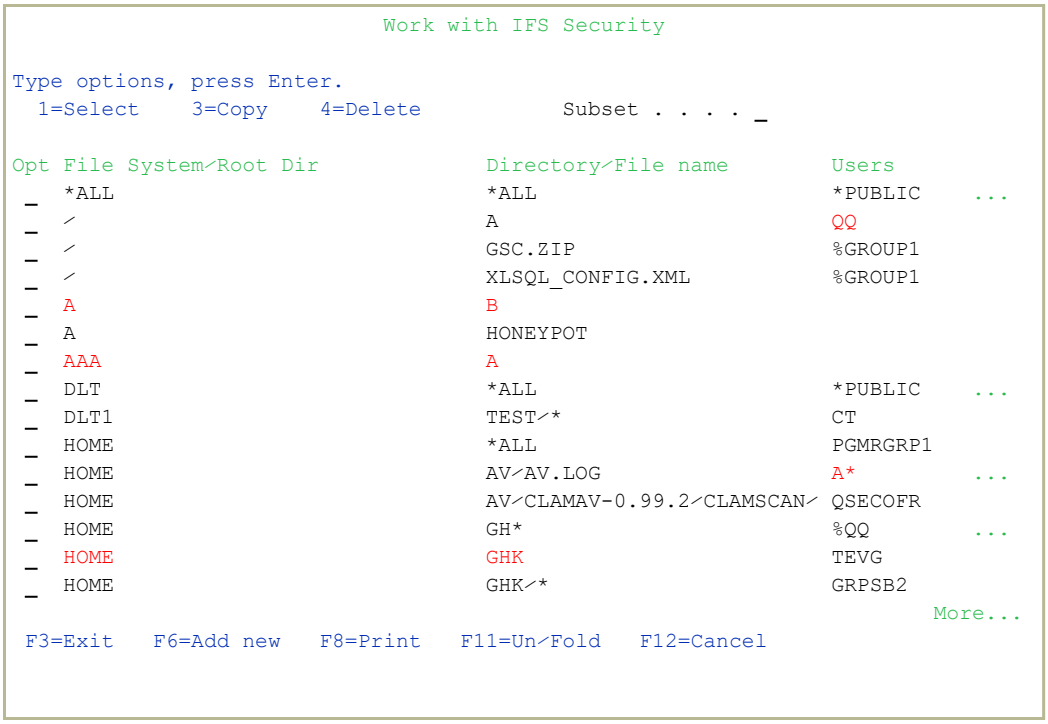
To **add and modify rules** for filtering IFS objects, type **1** and press **Enter**. The **Work with IFS Security** screen appears, as shown in "Setting Firewall Rules for IFS Files and Directories" on the facing page.

To **add and modify folder prefixes** that are replaced in checking IFS objects, type **61** and press **Enter**. The **Work with IASP/IFS Replacements** screen appears, as shown in "Replacing File Paths when Checking IASP/IFS Authority" on page 430.

## Setting Firewall Rules for IFS Files and Directories

To **add and modify rules for filtering IFS objects**, type **1** on the **IFS Security** screen, as shown in "Setting Firewall Rules for IFS Objects" on the previous page (*STRFW* **>** **6**) and press **Enter**.

The **Work with IFS Security** screen appears:




Each line of the list contains the following fields:

**File System/Root Dir**

The file system or root directory containing the objects.

**Directory/File Name**

The path to the object, beneath the file system or root directory shown in the previous column. If it ends in an asterisk ("*****"), it refers to all the files and folders within that directory.

**Users**

The first of the list of users or group to which the rule refers. If it is blank, the rule is the default for all users (***PUBLIC**). If the rule is for more than one user or group, the field is followed by an ellipsis ("**. . .**").

To **add** a rule, press the **F6** key. The **Add IFS Security** screen appears, as shown in "Adding Firewall Rules for IFS Files and Folders" on the facing page.

To **print** the information from this screen, press the **F8** key.

To **modify** a rule, type **1** in the **Opt** field for the rule and press **Enter**. The **Modify IFS Security** screen appears, as shown in "Modifying Firewall Rules for IFS Files and Folders" on page 410.

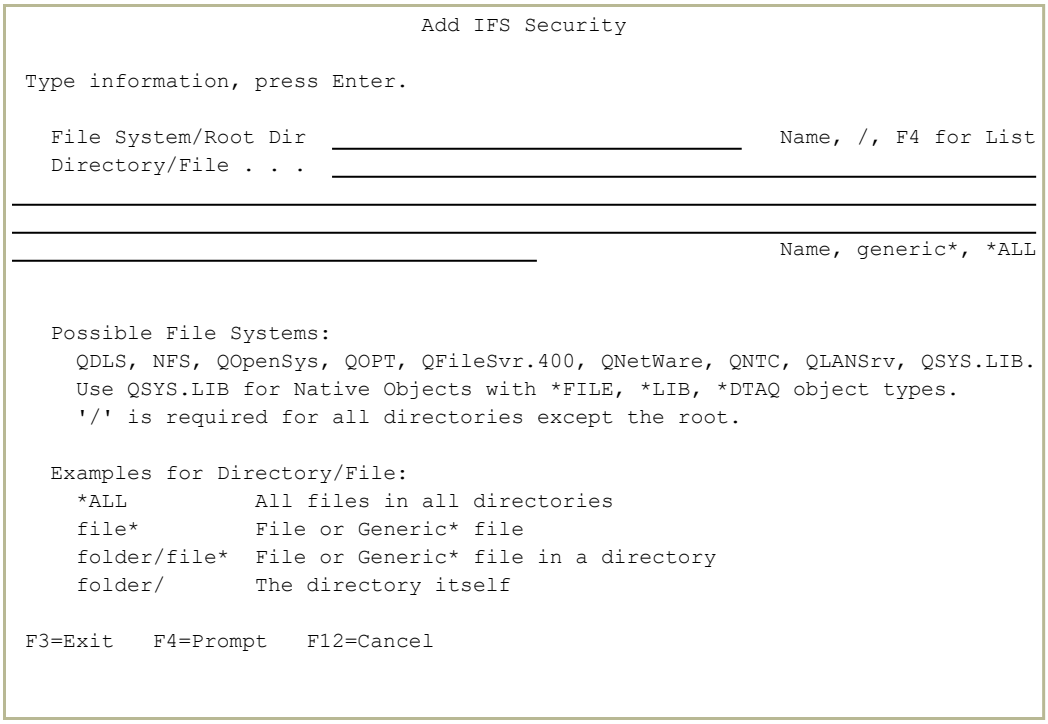
To **copy** settings for one file or directory to another, type **3** in the **Opt** field for the rule and press **Enter**. The **Copy IFS Security** screen appears, as shown in "Copying Firewall Rules for IFS Files and Folders" on page 412.

To **delete** the settings for a file or directory, type **4** in the **Opt** field for the rule and press **Enter**. The **Delete Native AS/400 Command Security** screen appears, as shown in "Deleting Firewall Rules for IFS Files and Folders" on page 436.

## Adding Firewall Rules for IFS Files and Folders

To **add rules for filtering IFS files and folders**, press the **F6** key on the **Work with IFS Security** screen, as shown in "Setting Firewall Rules for IFS Files and Directories" on page 405 (***STRFW* > 6 > 1**).

The **Add IFS Security** screen appears:




The screen contains the following fields:

**File System/Root Dir**

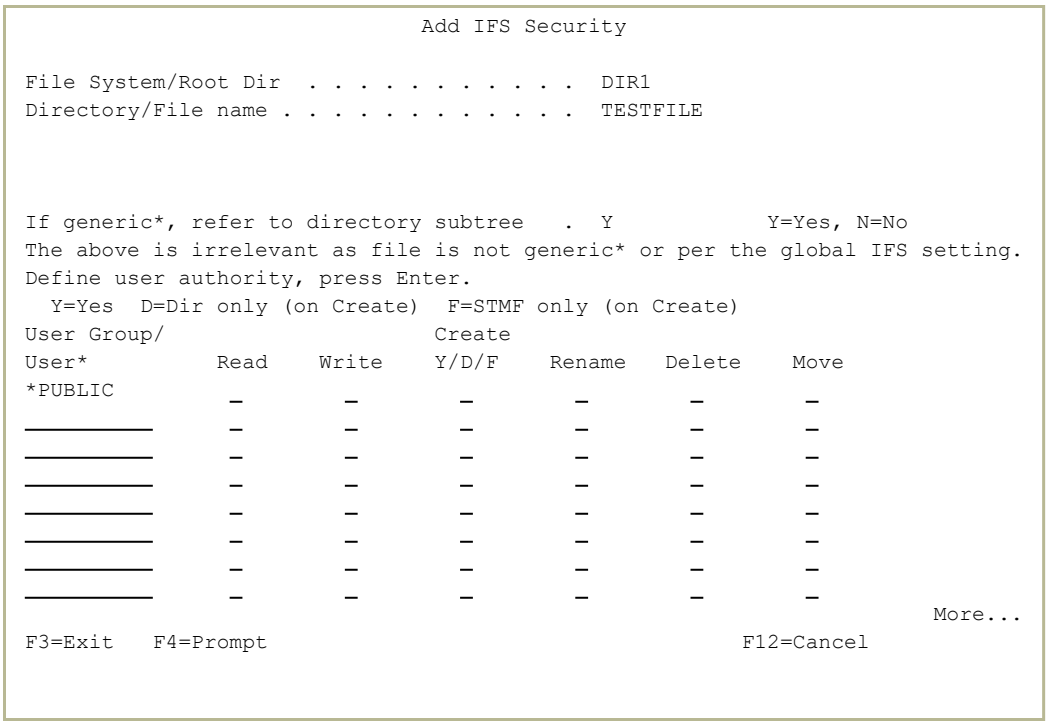
The file system or root directory containing the objects. To see a list of existing file systems, press the **F4** key.

**Directory/File**

The path to the object, beneath the file system or root directory shown in the previous field. If it ends in an asterisk ("*****"), it refers to all the files and folders within that directory. If it ends in a slash ("**/**"), it refers to the directory itself.

When you have entered these values, press **Enter**.

A second **Add IFS Security** screen appears:




The screen contains a field labeled **If generic* - refer to directory structure**.

- If the **Directory/File name** field ends in an asterisk ("*"):
  - To refer to all matching objects in the current directory, as well as in directories below the specified one that match the name, type **Y**.
  - To refer only to objects within the current directory and not those below it, type **N**.
- Otherwise (if **the Directory/File** name field does not end in an asterisk), this field is ignored.

Each line on the rest of the screen contains rules for specific users or groups of users requesting authority to act on the objects. The lines contain these fields:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the **F4** key. If it is *PUBLIC, the rule is for all users for whom further rules for accessing these objects have not been specified.

**Read**

If set to **Y**, the user or group may read this object.

**Create/Write**

If set to **Y**, the user or group may create or write to this object.

**Rename**

If set to **Y**, the user or group may rename this object.

**Delete**

If set to **Y**, the user or group may delete this object.

**Move**

If set to Y, the user or group may move this object.

## Modifying Firewall Rules for IFS Files and Folders

To **modify rules for filtering IFS files and folders**, enter **1** in the **Opt** field for the rule on the **Work with IFS Security** screen, as shown in "Setting Firewall Rules for IFS Files and Directories" on page 405 (*STRFW* **> 6 > 1**).

The **Modify IFS Security** screen appears:

```
                            Modify IFS Security

File System/Root Dir  . . . . . . . . . . .  TT3
Directory/File name . . . . . . . . . . . .  YY3



If generic*, refer to directory subtree   .  Y            Y=Yes, N=No
The above is irrelevant as file is not generic* or per the global IFS setting.
Define user authority, press Enter.
  Y=Yes  D=Dir only (on Create)  F=STMF only (on Create)
User Group/                        Create
User*          Read    Write    Y/D/F    Rename   Delete    Move
*PUBLIC          _       Y        _        _        Y        _
QQ               Y       _        _        Y        _        Y
QQ2              _       Y        _        _        Y        _
QQ3              Y       _        _        Y        _        Y
_____            _       _        _        _        _        _
_____            _       _        _        _        _        _
_____            _       _        _        _        _        _
_____            _       _        _        _        _        _
                                                                More...
F3=Exit   F4=Prompt   F8=Print   F9=Print File System   F12=Cancel
```

The read-only **File System/Root Dir** and **Directory/File name** fields show the path to the objects to which the rules refer.

The screen contains a field labeled **If generic* - refer to directory structure**.

- If the **Directory/File name** field ends in an asterisk ("*"):
  - To refer to all matching objects in the current directory, as well as in directories below the specified one that match the name, type **Y**.
  - To refer only to objects within the current directory and not those below it, type **N**.
- Otherwise (if **the Directory/File** name field does not end in an asterisk), this field is ignored.

Each line on the rest of the screen contains rules for specific users or groups of users requesting authority to act on the objects. The lines contain these fields:

**User*, %Group, Group profile**

The name or generic name of a user or group for whom you are creating these settings. To see a list of possible users or groups, press the **F4** key. If it is *PUBLIC, the rule is for all users for whom further rules for accessing these objects have not been specified.

**Read**

If set to **Y**, the user or group may read this object.

**Write**

If set to **Y**, the user or group may write to this object.

**Create**

Whether the user can create the object. Possible values are:

- **Y**: User may create directories and files
- **D**: User may only create directories
- **F**: User may only create files

**Rename**

If set to **Y**, the user or group may rename this object.

**Delete**

If set to **Y**, the user or group may delete this object.

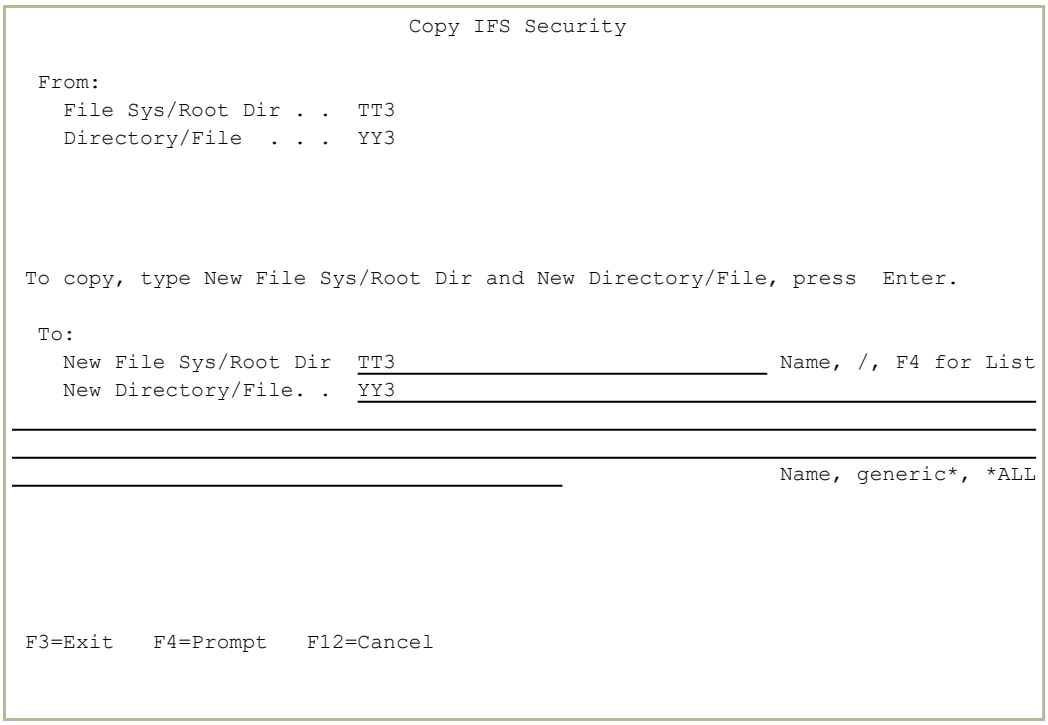
**Move**

If set to Y, the user or group may move this object.

## Copying Firewall Rules for IFS Files and Folders

To **copy rules for filtering IFS files and folders** from one object or set of objects to another, enter **3** in the **Opt** field for the rule on the **Work with IFS Security** screen, as shown in "Setting Firewall Rules for IFS Files and Directories" on page 405 (*STRFW* **> 6 > 1**).

The **Copy IFS Security** screen appears:




The read-only **File System/Root Dir** and **Directory/File name** fields show the path to the objects to which the rules originally refer.

Enter the values for the object for which the rules will be copied into the remaining fields:

**New File System/Root Dir**

The file system or root directory containing the objects. To see a list of existing file systems, press the **F4** key.

**New Directory/File**

The path to the object, beneath the file system or root directory shown in the previous field. If it ends in an asterisk ("*****"), it refers

to all the files and folders within that directory. If it ends in a slash ("**/**"), it refers to the directory itself.

## Deleting Firewall Rules for IFS Files and Folders

To **delete rules that show which users may operate on an IFS file or group of files**, enter **4** in the **Opt** field for that file on the **Work with IFS Security** screen, as shown in "Setting Firewall Rules for IFS Files and Directories" on page 405 (***STRFW* > 6 > 1**).

The **Delete IFS Security** screen appears:

```
                            Delete IFS Security

File System/Root Dir  . . . . . .  TT3
Directory/File name . . . . . .  YY3



If generic*, refer to directory subtree   .  Y            Y=Yes, N=No
The above is irrelevant as file is not generic* or per the global IFS setting.
Press Enter to confirm the Delete, F12 to cancel.
  Y=Yes  D=Dir only (on Create)  F=STMF only (on Create)
User Group/                      Create
User*          Read    Write    Y/D/F    Rename   Delete    Move
*PUBLIC                  Y                          Y
QQ              Y                         Y                Y
QQ2                      Y                          Y
QQ3             Y                         Y                Y




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

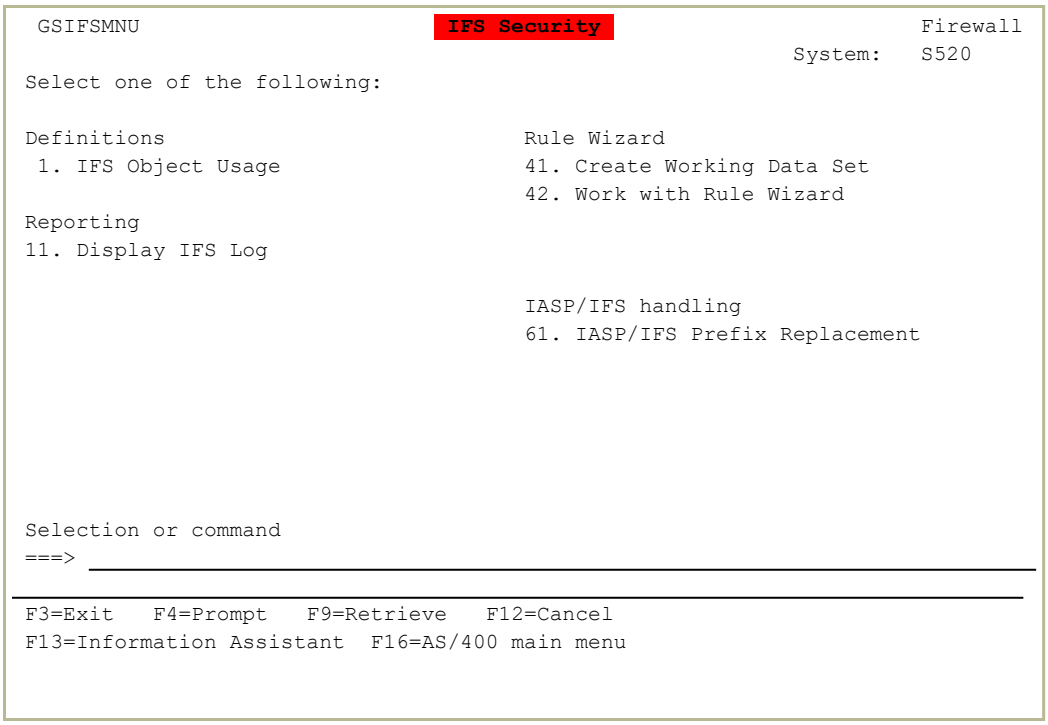
All of the fields on the screen are read-only.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Using the Rule Wizard for IFS Objects

Using the Rule Wizard, you can analyze recent activity on your system and use that information to create and modify Firewall rules.




- To **create a data set** for examining activity and developing rules for incoming activity based on IFS objects on which it requests to operate, select **`41. Create Working Data Set`** from the **IFS Security** screen (*STRFW* **`> 5`**).
  The **Summarize IFS Objects Log (CPRIFSSEC)** screen appears, as shown in "Creating a Data Set on IFS Objects with the Rule Wizard" on the next page.
- To **use an existing data set** to develop rules, select **`42. Work with Rule Wizard`** from the **IFS Security** screen (*STRFW* **`> 4`**).
  The **IFS Objects Wizard (WZRIFSSEC)** screen appears, as shown in "Analyzing Recent Data on IFS Objects with the Rule Wizard" on page 420.

## Creating a Data Set on IFS Objects with the Rule Wizard

To **create a data set** for examining activity and developing rules for outgoing activity based on IFS objects on which it requests to operate, select **41. Create Working Data Set** from the **IFS Security** screen *(STRFW* **> 5**).

The **Summarize IFS Objects Log (CPRIFSSEC)** screen appears. From this screen, you can construct the command line command that creates the data set.

```
                    Summarize IFS objects Log (CPRIFSSEC)

Type choices, press Enter.

File System ("/" for root dir)     *ALL
Directory/File name contains . .   *ALL
_____
User . . . . . . . . . . . . . .   *ALL          Name, *ALL
Group by . . . . . . . . . . . .   *DFT          *DFT, *USER, *GRPPRF...
Allowed  . . . . . . . . . . . .   *ALL          *YES, *NO, *ALL
Starting date and time:
  Starting date  . . . . . . . .   *CURRENT      Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . . . .   000000        Time
Ending date and time:
  Ending date  . . . . . . . . .   *CURRENT      Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . . . . .   235959        Time
Number of records to process . .   *NOMAX        Number, *NOMAX
Server ID  . . . . . . . . . . .   *ALL          *ALL, *FILSRV, *FTPSRV...


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

The screen contains the following fields. Fields that have values other than the defaults are preceded by the "**>**" character:

**File System ("/" for root dir)**

The file system or root directory containing the objects, or ***ALL** for all file systems and directories. To see a list of existing file systems, press the **F4** key.

**Directory/File name contains**

The path to the object, beneath the file system or root directory shown in the previous field, or ***ALL** for all file systems beneath the one specified in the previous field. If it ends in an asterisk

("*****"), it refers to all the files and folders within that directory. If it ends in a slash ("**/**"), it refers to the directory itself.

**User, <GrpPrf or '%GROUP'**

The user or group requesting the activity. This can be a user name, a generic* name, a group name, a group profile, or ***ALL** for all users.

**Group by**

How the result are grouped in the data set. Possible values include:

- ***DFT**: The default grouping of data within rule wizards, as set in the **Wizard Group by** parameter in the **Firewall General Definitions** screen.
- ***USER**: Grouped by the user name.
- ***GRPPRF**: If a user is a member of a single group, the user's activity is included under the group.
  Otherwise, the activity is shown under the username.
- ***USRGRP**: If the user is a member of multiple groups, the user's activity is included under the first of those groups.
  Otherwise, the activity is shown under the username.
- ***GROUP**: If the user is a member of a single group, the user's activity is included under that group.
  Otherwise, if the user is a member of multiple groups, the user's activity is listed under the first of those groups.
  Otherwise (if the user is not a member of any groups), the activity is shown under the username.
- ***ALLGRP**: If the user is a member of a single group plus up to fifteen supplemental groups. the user's activity is shown for each of those groups.
- ***ALL**: If the user is a member of a single group plus up to fifteen supplemental groups. the user's activity is shown for each of those groups.
  Otherwise, if the user is a member of multiple groups, the user's activity is listed under the first of those groups.

Otherwise (if the user is not a member of any groups), the activity is shown under the username.

**Allowed**

Specifies whether the data set includes rejected activity, accepted activity, or both.

- ***YES**: Include only accepted activity
- ***NO:** Include only rejected activity
- ***ALL:** Include both accepted and rejected activity

**Starting data and time**

**Starting date**

The day or date on which the included data begins.

Allowed values include:

- ***CURRENT**: The current date
- ***YESTERDAY**: Yesterday's date
- ***WEEKSTR**: The first day of the current week. By default, this is Sunday.
- ***PRVWEEKS**: The first day of the previous week
- ***MONTHSTR**: The first day of the current month
- ***PRVMONTHS**: The first day of the previous month
- ***YEARSTR**: The first day of the current year
- ***PRVYEARS**: The first day of the previous year
- ***MON**: Monday
- ***TUE**: Tuesday
- ***WED**: Wednesday
- ***THU**: Thursday
- ***FRI**: Friday
- ***SAT**: Saturday
- ***SUN**: Sunday

**Starting time**

The time on the Starting date at which the included data begins, in **HHMMSS** format.

**Ending date**

The day or date on which the included data ends.

Allowed values are the same as for **Starting date**.

**Ending time**

The time on the Starting date at which the included data ends, in **HHMMSS** format.

**Number of records to process**

Collect no more than this number of records. If set to ***NOMAX**, collect all the relevant records.

**Server ID**

The server that the activity is attempting to access. To see a list of possible values, press the F4 key.

To list and select possible values for many of the fields, place the cursor within the field and press the F4 key.

To reset the values on the screen to their default values, press the F5 key.

# Analyzing Recent Data on IFS Objects with the Rule Wizard

The Rule Wizards analyze data on recent system activity to develop and improve rules for filtering future activity.

To develop rules to filter incoming activity by the IFS object on which it is requesting to operate, first create a data set of recent activity, as shown in "Creating a Data Set on IFS Objects with the Rule Wizard" on page 416.

Once you have created a data set, select **`42. Work with Rule Wizard`** from the **IFS Security** screen (*STRFW* **`> 5`**).

The **Plan IFS Security** screen appears:

```
                              Plan IFS Security   Subset:
Type choices, press Enter.                     File Sys/Root _____________________
 1=Statistics  2=Allow by use  3=Display     Dir/Filename _____________________
 4=Delete      5=DSPFWLOG                       Grp/User _
 7=WRKLNK      8=WRKAUT        9=Add similar    Higher level only (Y-Yes)  _
 G=Groups      U=Users                           C>R=Current to Revised
Specify revised authority in the R column.      Y Allowed      Y=Allow
Press Enter to apply revised authority.         N Rejected     N=Reject
                                                Y Allowed (from higher level)
    Rd   Wrt  Rnm  Dlt  Mov File Sys/           N Rejected(from higher level)
Opt C>R  C>R  C>R  C>R  C>R Root Dir    Directory/File name   Grp/User Entries
 _  N _  N _  N _  N _  N _ HOME        N501232/BLABLAX#.TXT  232X            4
 _  N _  N _  N _  N _  N _ HOME        N501232/NEW FOLDER    232X            6
 _  N _  N _  N _  N _  N _ HOME        N501232/TEST          232X            2
 _  N _  N _  N _  N _  N _ HOME        PTF/PC050003.DAT      %GROUP1         8
 _  N _  N _  N _  N _  N _ HOME        PTF/PC050003.TXT      %GROUP1         4
 _  N _  N _  N _  N _  N _ HOME        PTF/PJ090014.DAT      %GROUP1         2
 _  N _  N _  N _  N _  N _ HOME        PTF/PJ090016.DAT      %GROUP1        10
 _  N _  N _  N _  N _  N _ HOME        PTF/PJ090016.TXT      %GROUP1         4
 _  N _  N _  N _  N _  N _ HOME        PTF/PO050016.DAT      %GROUP1        38
                                                                       More...
F3=Exit   F6=Add New   F8=Print   F12=Cancel   F17=Allow by use globally
```

Each line on the lower part of the screen represents requests within the data set by a single user or group to access a single object.

After the **`Opt`** field, the first five pairs of fields show ways that objects can be accessed.

- **`Rd`**: Read
- **`Wrt`**: Write
- **`Rnm`**: Rename
- **`Dlt`**: Delete
- **`Mov`**: Move

The **pairs of fields** for each are:

- a **letter** on a colored background, showing how Firewall responded to the activity according to current rules
- an **underscore** in which you can revise the rule

The **letter codes** are:

- Blank: Reject all incoming activity
- **A**: Allow activity without checking
- **B**: Allow only activity over an SSL connection, without parsing SQL statements
- **L**: Log and allow activity, without checking
- **M**: Log and allow only activity over an SSL connection, with parsing SQL statements
- **S**: Allow only activity over an SSL connection
- **Y**: Allow activity after parsing any SQL statement in the activity

The **color codes** are:

- **Green**: A rule specifically referring to this user or group and object accepts this activity
- **Red**: A rule specifically referring to this user or group and object rejects this activity
- **Blue**: A rule for a generic set of users, groups, or objects that includes this one accepts this activity
- **Purple**: A rule for a generic set of users, groups, or objects that includes this one rejects this activity

The following fields show the location of the object and the user or group accessing it.

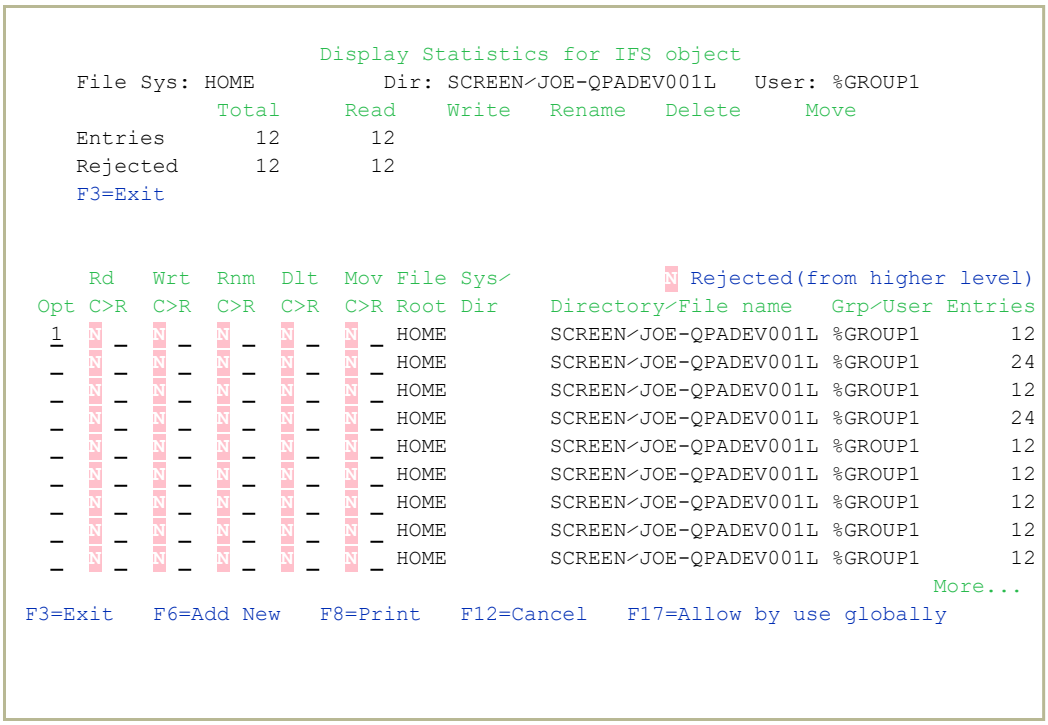
The **File Sys/Root Dir** field shows the file system or root directory containing the object.

The **Directory/File name** field shows the directory containing the object and the file name of the object itself. The field is truncated to twenty characters. To **see the full file path**, type **3** in the **Opt** field for the rule and press **Enter**.

The **Entries** field shows the number of requests made during the time period in the data set.

Thus, in the example, the first item on the bottom of the screen shows that the group **%GROUP1** is **not allowed**, because of a group or generic set of users to which it or the object belongs, to read a file with a name that begins with the string **JOE-QPADEV001L** within the **SCREEN** directory in the **HOME** filesystem and had requested to do so **12** times within the time period of the data set. Entering **3** in the **Opt** field for the rule reveals that the full file name is **SCREEN/JOE-QPADEV001L-191202-183959.HTML**.

To **view the statistics** on activity by a specific user or group on a specific object during the time period in the data set, type **1** in the **Opt** column for that row and press **Enter**. The **Display Statistics for IFS object** window appears.




Continuing from the previous example, we see that members of **%GROUP1** requested to access the file twelve times. All of them were for Read access and all of them were rejected.

To **add** a new rule, press the **F6** key. The **Add Native AS/400 Revised Security** screen appears, as shown in .

To add a rule for an object and a user or group **similar** to an existing one, type **9** in the **Opt** field for that rule and press **Enter**. The **Add Similar Revised Security** screen appears, as shown in "Adding Firewall Rules for a Similar IFS Object with the Rule Wizard" on page 428.

To **change rules based on activity** in the data set, type **5** in the **Opt** field for that rule and press **Enter**. If a rule had set a particular activity on an object by a user or group to be rejected, a specific new rule is set for that activity, object, and user to accept it. Otherwise, the option has no effect.

To **change rules manually**, see "Setting Firewall Rules Manually based on IFS Objects with the Rule Wizard" on page 426.

To **delete** a rule, type **4** in the **Opt** field for that rule and press **Enter**.
NOTE: You are not prompted for confirmation, and the rule is immediately deleted.

To **display the firewall log** entries relevant to this rule, type **5** in the **Opt** field for that rule and press **Enter**. The **Display Firewall Log** screen appears, as shown in "Displaying Firewall Logs" on page 516.

To view a list of the **users in a group**, type **G** in the **Opt** column for that group and press **Enter**. The **List of Users in User Group** window appears, listing the users in the group.

To view a list of the **groups containing a user**, type **U** in the **Opt** column for that group and press **Enter**. The **List of Users in Group Profile** window appears, listing the users in the group.

To **work with object links** in a rule, type **7** in the **Opt** column for the rule and press **Enter**. The OS/400 **WOrk with Object Links** screen appears, as described in IBM documentation.

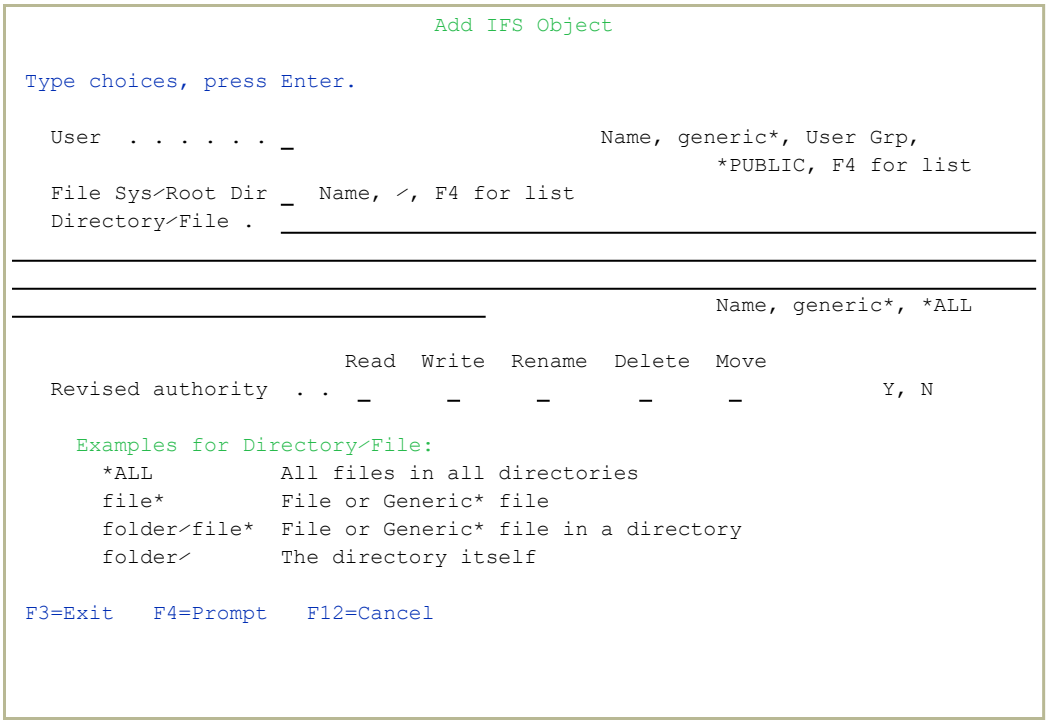
To **edit the object authority** for the object in a rule, type **8** in the **Opt** column for the rule and press **Enter**. The OS/400 **Work with Authority** screen appears, as described in IBM documentation.

To **print** the information from the data set, press the **F8** key.

## Adding Firewall Rules for IFS Objects with the Rule Wizard

To add firewall rules to filter activity by the IFS objects on which it would operate via the Rule Wizard, press the **F6** key from the **Plan IFS Security** screen, shown in "Analyzing Recent Data on IFS Objects with the Rule Wizard" on page 420 (***STRFW* > 5 > 42**).

The **Add IFS Object** screen appears:




The first three fields on the screen specify the objects and users to which the rule would apply:

**User, <GrpPrf or '%GROUP'**

The user or group requesting the activity. This can be a user name, a generic* name, a group name, a group profile, or ***ALL** for all users.

**File Sys/Root Dir**

The file system or root directory containing the object. This can be a name or the "/" character to indicate the root filesystem. To see a list of possible values, press the **F4** key.

**Directory/File**

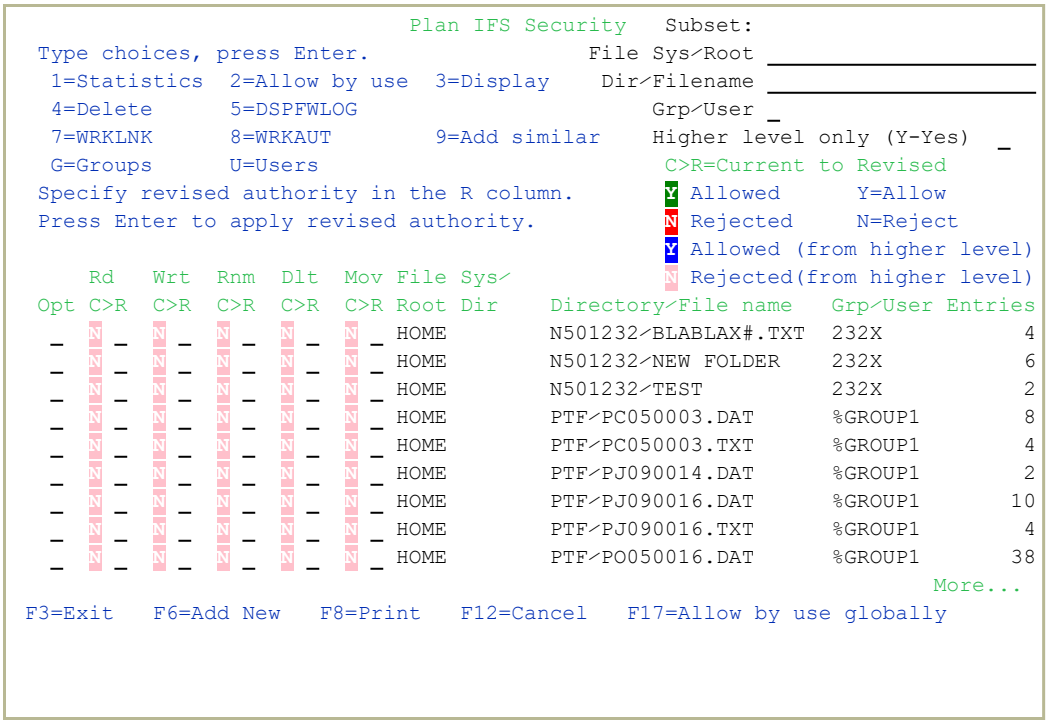
The directory and file to which access would be requested. This can be a single name, a generic* name, or *ALL (representing all the objects within the directory or file system.

The **Revised Authority** fields indicate whether the user or group may perform each of a set of operations (**Read**, **Write**, **Rename**, **Delete**, or **Move**) on the object. Set these to **Y** to accept the requests or **N** to reject them. If a field is left blank, it inherits the value from the next higher group, up through ***PUBLIC**.

## Setting Firewall Rules Manually based on IFS Objects with the Rule Wizard

NOTE: You can only set Firewall rules manually with the rule wizard if you have set the **Wizard type** to ***STD** when opening the wizard.

To set rules manually based on the users or groups requesting the activity in the Rule Wizard, open the **Plan IFS Security** screen, as shown in "Analyzing Recent Data on IFS Objects with the Rule Wizard" on page 420 (*STRFW* **> 5 > 42**).




Enter new values in the second field of each column for which you want to change access in the rows for the appropriate rule. You can enter **Y** to accept requests or **N** to reject requests.

NOTE: While the **Current** line may show a **V** for servers for which access is determined by the verbs used, the setting can only be changed to that via the **Modify Server Verb Authority** screen, as shown in "Modifying Firewall Settings for a User based on Server Verbs" on page 253.

In this example, to accept requests to read the file **N501232/BLABLAX#.TXT** in the file system **HOME** by the user **232X**, type **Y** in the second column in the top line under **Rd**.

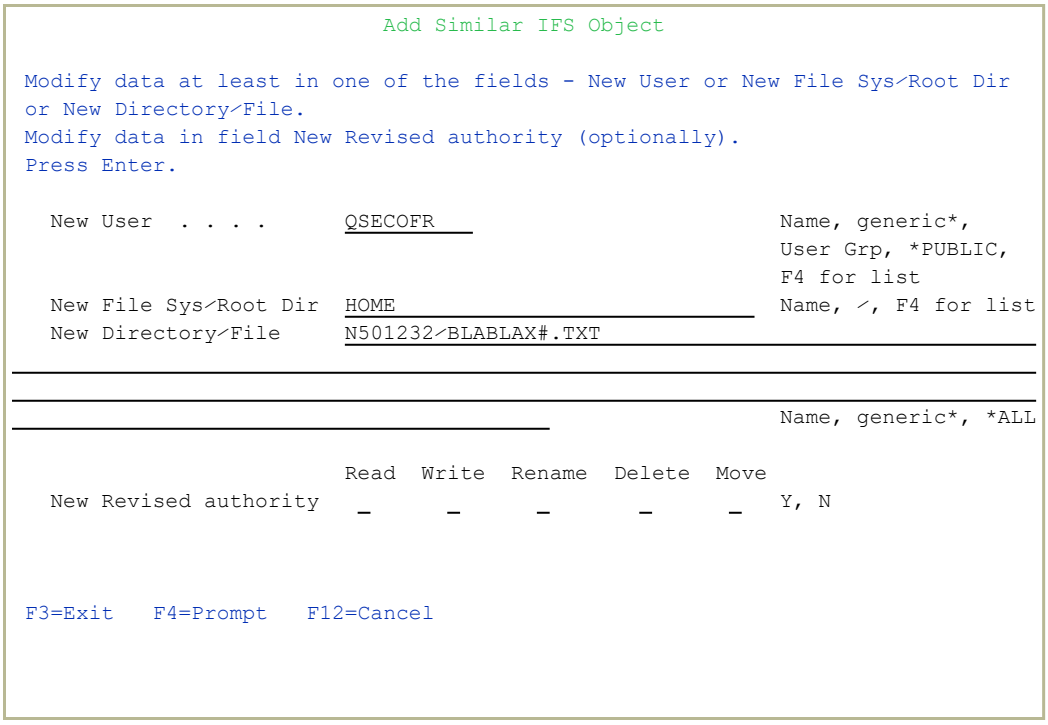
When you have entered the letters for the changes in the appropriate columns, type **6** in the **Opt** field for the rule and press Enter.

The rule that you have changed disappears from the screen. You can see its changed value by checking the Work with IFS Security screen, as shown in "Setting Firewall Rules for IFS Objects" on page 404.

# Adding Firewall Rules for a Similar IFS Object with the Rule Wizard

To add firewall rules for a combination of a user or group requesting access to and object similar to an existing one via the Rule Wizard, type **9** in the **Opt** field for the original rule from the **Plan IFS Security** screen, shown in "Analyzing Recent Data on IFS Objects with the Rule Wizard" on page 420 (*STRFW* **> 4 > 42**) then press **Enter**.

The **Add Similar IFS Object** screen appears:




The first three fields on the screen show the values from the original rule as defaults. You can change each of them to represent the new object:

**New User**

The user or group requesting the activity. This can be a user name, a generic* name, a group name, or ***PUBLIC** for all users. To see a list of possible values, press the **F4** key.

**New File Sys/Root Dir**

The file system or root directory containing the object on which the activity requests to operate. This can be the name of the

specific file system or directory or the "/" character. To see a list of possible values, press the F4 key.

**New Directory/File**

The directory or file on which the activity requests to operate. This can be the name of the specific object, a generic name ending in an asterisk ("*****"), or ***ALL** for all objects.

The **New Revised Authority** fields indicate whether the user or group may perform each of a set of operations (**Read**, **Write**, **Rename**, **Delete**, or **Move**) on the object. Set these to **Y** to accept the requests or **N** to reject them. If a field is left blank, it inherits the value from the next higher group, up through ***PUBLIC**.

## Replacing File Paths when Checking IASP/IFS Authority

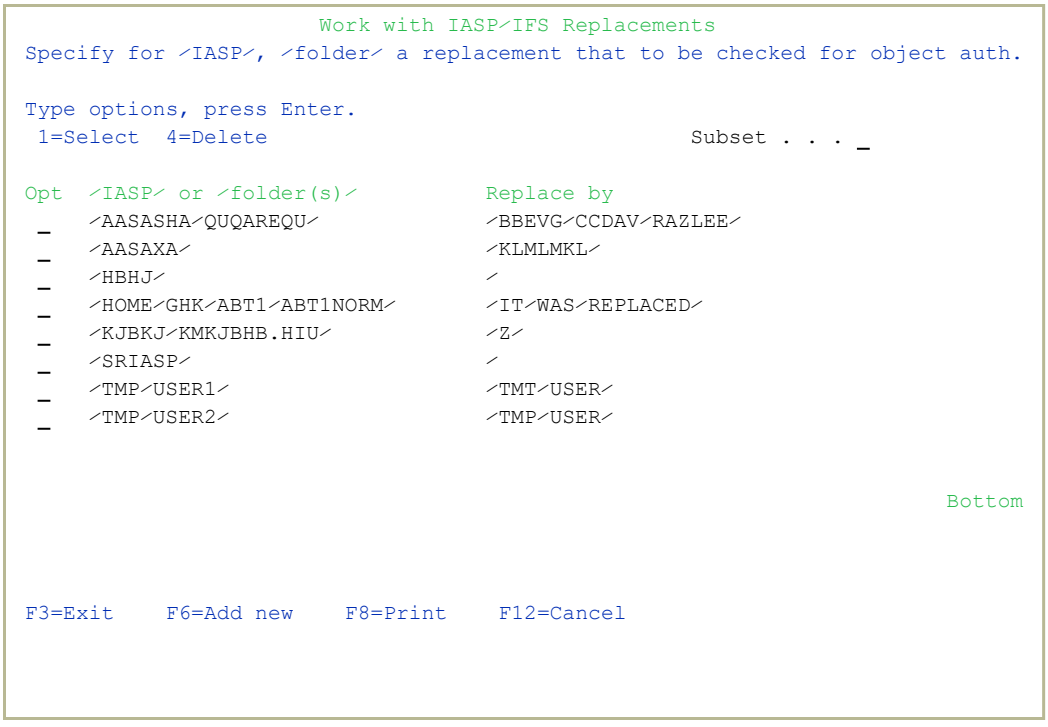
You can specify replacement paths when checking authority for IASP/IFS objects. When checking an object on a particular path, Firewall can actually check a different path, substituting the beginning of one path with the other.

Although multiple IASPs may contain the same library, carrying similar objects, the security needed for each object in those libraries may differ.

You can easily set different Firewall rules for the differing objects. To do this, equate an imaginary library name for each combination on ASP and library except the first. Use this name to define all Firewall rules for the objects in these libraries. The equated name must not be a name of an existing library.

Using the equation system, you can equate several library names or even several generic library names to the same equate name. This is most useful when you have several libraries with the same objects requiring similar security rules, such as if you would store data for multiple years or multiple factories on the same system.

To specify the replacement paths, select **`61. IASP/IFS Prefix Replacement`** from the **IFS Security** screen (*STRFW* **`> 5`**). The **Work with IASP/IFS Replacements** screen appears:



To **add** a new replacement, press the **F6** key. The **Add IASP/IFS Replacement** screen appears, as shown in "Adding Replacement Paths for Checking IASP/IFS Authority" on the next page.

To **print** the list, press the **F8** key.

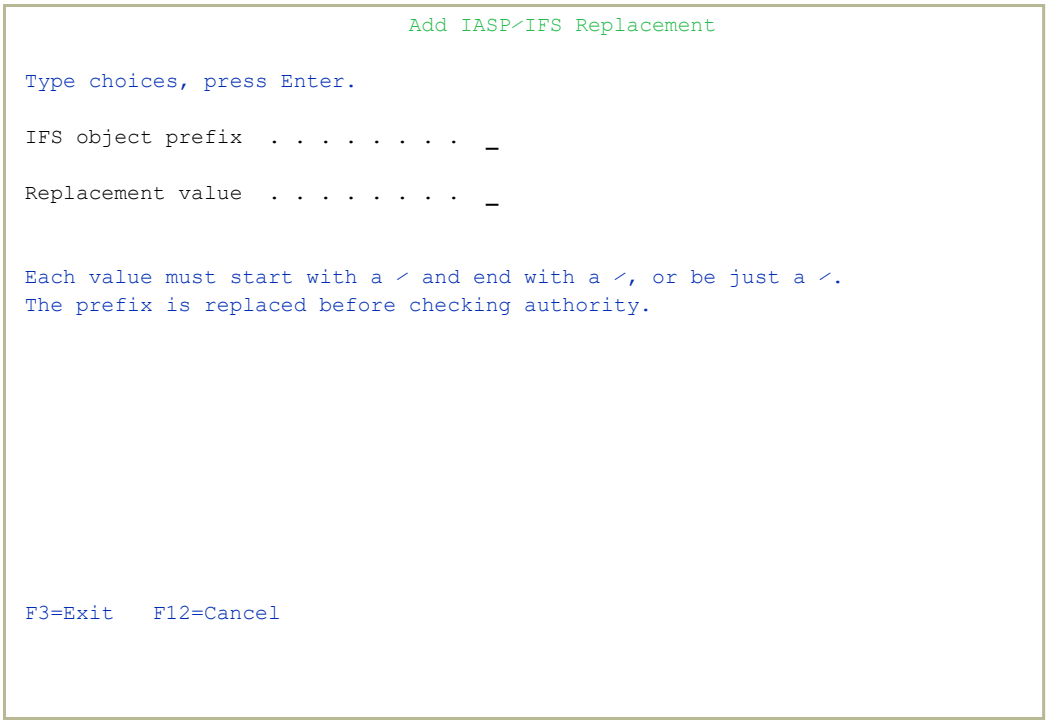
To **modify** a replacement, type **1** in the **Opt** field for that replacement and press **Enter**. The **Modify IASP/IFS Replacement** screen appears, as shown in "Modifying Replacement Paths for Checking IASP IFS Authority" on page 433.

To **delete** a replacement, type **4** in the **Opt** field for that replacement and press **Enter**. The **Delete IASP/IFS Replacement** screen appears, as shown in "Deleting Replacement Paths for Checking IASP IFS Authority" on page 435.

## Adding Replacement Paths for Checking IASP/IFS Authority

To add replacement paths for checking IASP/IFS authority, press the F6 key on the **Work with IASP/IFS Replacements** screen, as shown in "Replacing File Paths when Checking IASP/IFS Authority" on page 430 (***STRFW* > 5 > 61**).

The **Add IASP/IFS Replacement** screen appears:




The screen contains two fields:

**IFS object prefix**

The string to be replaced from the object's original path. It must begin and end with a slash ("**/**") or be a single slash on its own (for a root directory).

**Replacement value**

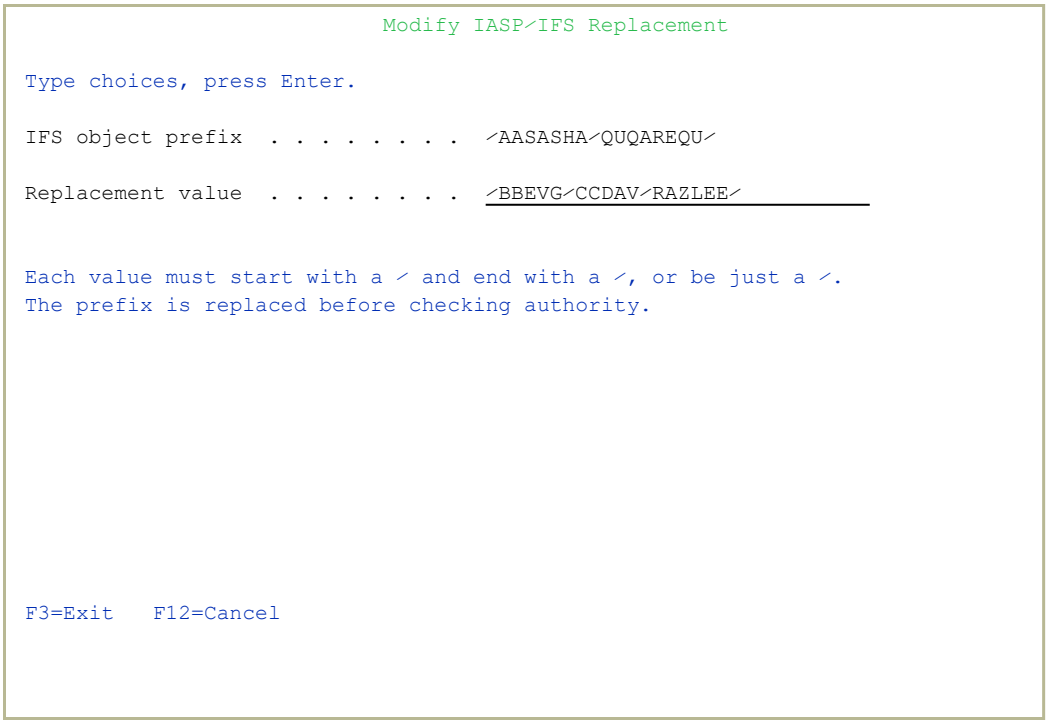
The replacement string. It also must begin and end with a slash ("**/**") or be a single slash on its own (for a root directory).

For example, if the IFS object prefix is **/tmp/original/here/** and the Replacement value is **/newpath/there/**, a file named **/tmp/original/here/sample.txt** would be checked for object authority as if it were **/newpath/there/sample.txt** .

# Modifying Replacement Paths for Checking IASP IFS Authority

To modify replacement paths for checking IASP/IFS authority, type **1** in the **Opt** field of the line for that replacement on the **Work with IASP/IFS Replacements** screen, as shown in "Replacing File Paths when Checking IASP/IFS Authority" on page 430 (***STRFW* > 5 > 61**).

The **Modify IASP/IFS Replacement** screen appears:




The screen contains two fields:

**IFS object prefix**

The string to be replaced from the object's original path. It must begin and end with a slash ("**/**") or be a single slash on its own (for a root directory).

This field is read-only. To modify this string in the replacement, you must create a new replacement rule (as shown in "Adding Replacement Paths for Checking IASP/IFS Authority" on the previous page) then delete the current one.

**Replacement value**

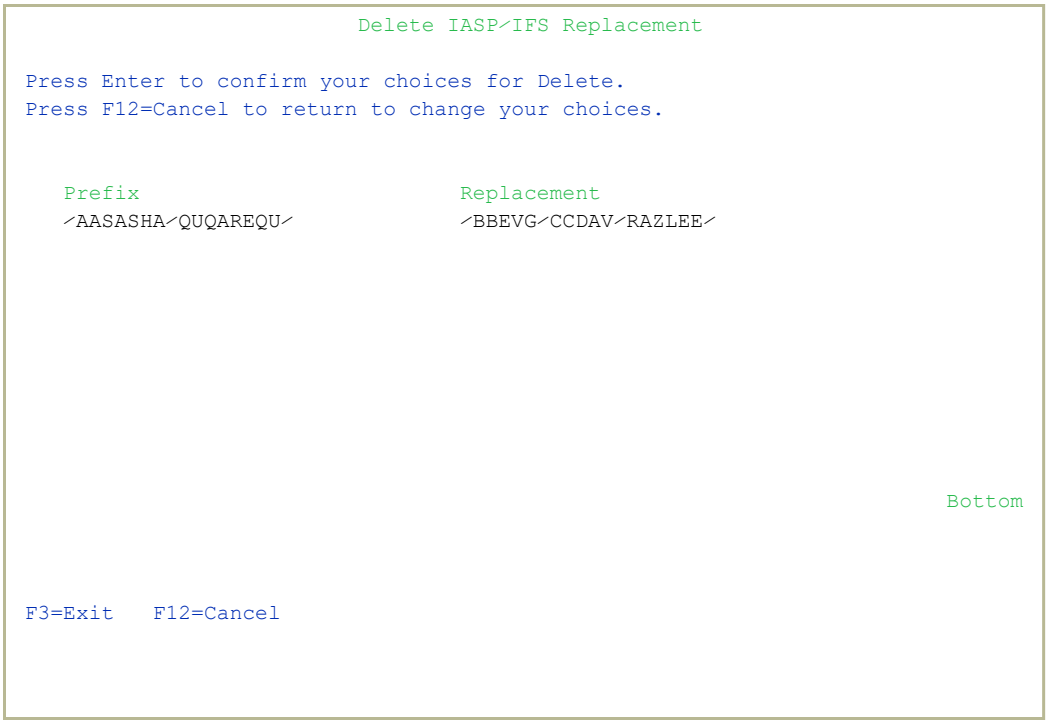
The replacement string. It also must begin and end with a slash ("**/**") or be a single slash on its own (for a root directory).

For example, if the IFS object prefix is **/tmp/original/here/** and the Replacement value is **/newpath/there/**, a file named **/tmp/original/here/sample.txt** would be checked for object authority as if it were **/newpath/there/sample.txt** .

## Deleting Replacement Paths for Checking IASP IFS Authority

To delete replacement paths for checking IASP/IFS authority, type **4** in the **Opt** field of the line for that replacement on the **Work with IASP/IFS Replacements** screen, as shown in "Replacing File Paths when Checking IASP/IFS Authority" on page 430 (***STRFW* > 5 > 61**).

The **Delete IASP/IFS Replacement** screen appears:




Both of the fields on the screen are read-only.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

## Deleting Firewall Rules for IFS Files and Folders

To **delete rules that show which users may operate on an IFS file or group of files**, enter **4** in the **Opt** field for that file on the **Work with IFS Security** screen, as shown in "Setting Firewall Rules for IFS Files and Directories" on page 405 (***STRFW* > 6 > 1**).

The **Delete IFS Security** screen appears:

```
                            Delete IFS Security

File System/Root Dir  . . . . . .  TT3
Directory/File name . . . . . . .  YY3



If generic*, refer to directory subtree   .  Y            Y=Yes, N=No
The above is irrelevant as file is not generic* or per the global IFS setting.
Press Enter to confirm the Delete, F12 to cancel.
  Y=Yes  D=Dir only (on Create)  F=STMF only (on Create)
User Group/                      Create
User*          Read    Write     Y/D/F    Rename   Delete    Move
*PUBLIC                  Y                           Y
QQ              Y                          Y                Y
QQ2                      Y                           Y
QQ3             Y                          Y                Y




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

All of the fields on the screen are read-only.

To **confirm** the deletion and return to the previous screen, press **Enter**.

To **cancel** the deletion and return to the previous screen, press the **F12** key.

# Building Firewall Rules with the Rule Wizards

Firewall's unique Rule Wizards feature makes security rule definition a snap, even for non-technical system administrators. Using the Wizards, you can easily build customized rules for your system based on the activity that happens on it. You can examine, create, and modify rules in real time and easily check the results.

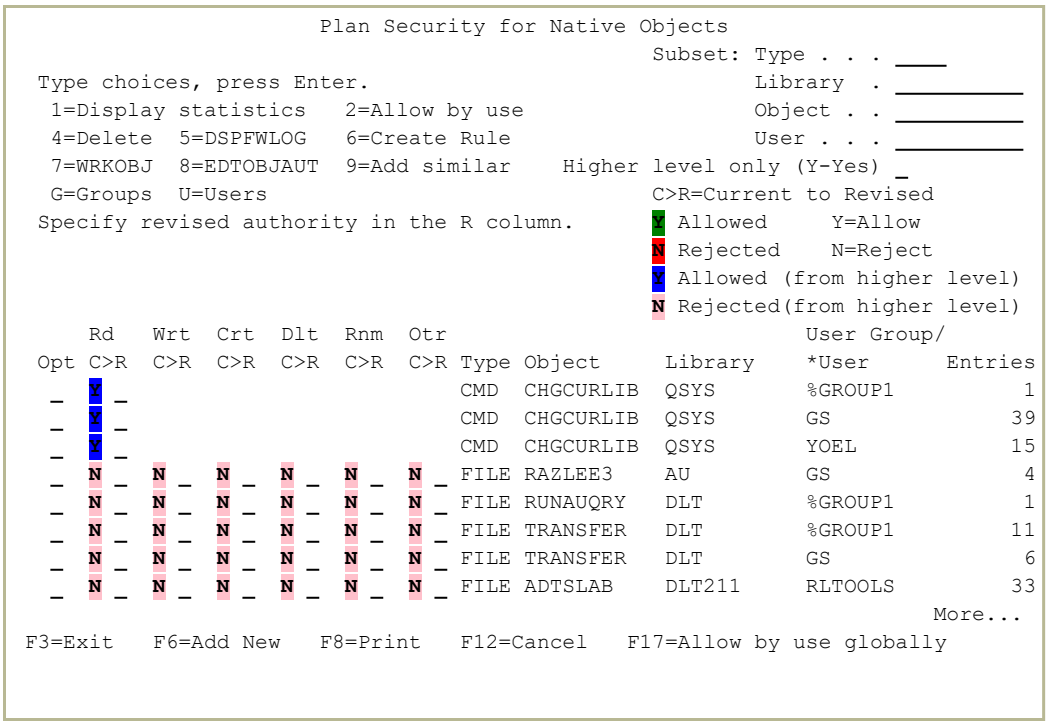
The Wizards use a simple two-step process. First, you have Firewall examine its logs of activity requests, looking specifically at criteria (corresponding to the iSecurity Layered Security Design) such as:

- the **Server or Exit Point** (such as FTP, Telnet, SSHD, and DBOPEN) on which the activity was requested
- the **IP addresees or SNA system names** to or from which the request was sent
- the **User or Group** requesting the activity
- the **Native or IFS object** on which the activity would operate

```
                    Summarize Native AS/400 Log (CPRNTVSEC)

Type choices, press Enter.

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


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

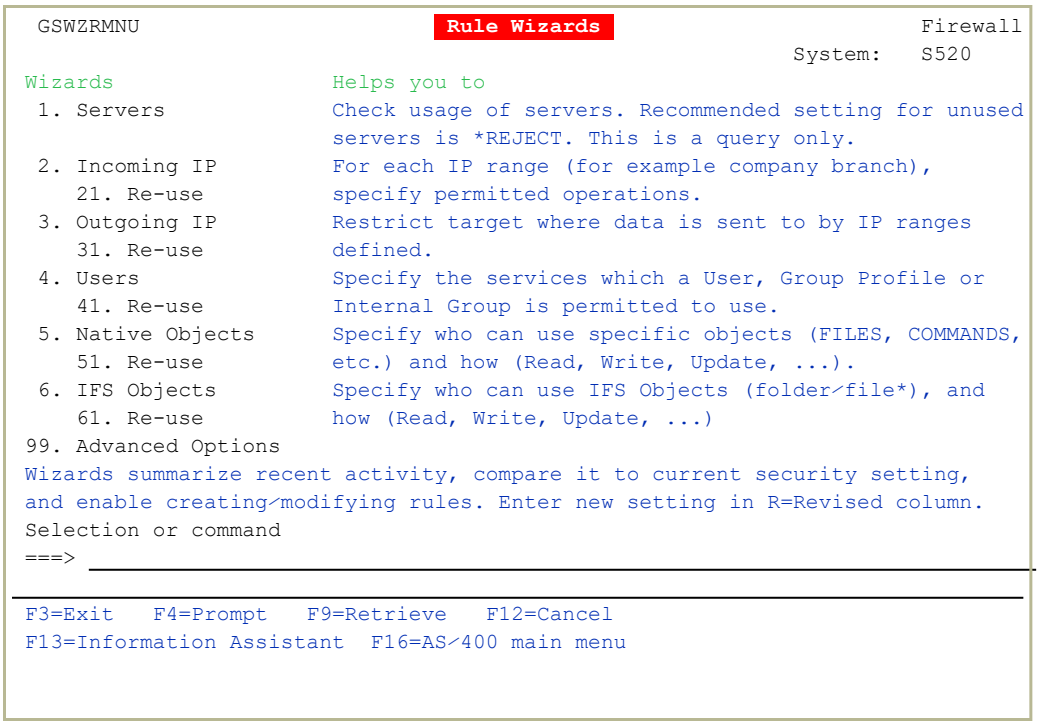
You can focus your search further by specifying the date and time that the activity began and ended as well as whether the activity was accepted or rejected. You can group the result by different criteria.

From the main screen for each Wizard, you can see a visual presentation of the rules that are in effect and of their results. You can see further information about the rules, delete and change them, and automatically adjust them so that they correspond to the activity that actually happened during that time.




To **run the Rule Wizards**, type **45** on the command line from the main Firewall screen (*STRFW* **> 45**). (You can also reach specific Wizards from other points within the system.)

The main Rule Wizards screen appears:




You can run the Rule Wizards from this screen, as well as from other points within Firewall:

- **Servers or Exit Points**
  - To see the current security state of the Servers or Exit Points, type **1** and press **Enter**. The **Transaction Summary by Type for User** screen appears, as shown in "Displaying Firewall Activity by Server" on page 442.
- **Incoming IP ranges or SNA System names**
  - To **collect information** and create rules based on the Incoming IP ranges or SNA System names from which requests came, type **2** and press **Enter**. The **Summarize Incoming IP Address (CPRIIPSEC)** screen appears, as shown in "Creating a Data Set of Incoming Activity by IP Address with the Rule Wizard" on page 163.
  - To **create rules** based on data about Incoming IP ranges or SNA System names that you have already collected, type **21** and press **Enter**. The **Plan Incoming IP Security** screen appears, as shown in "Analyzing Recent Data on Incoming Activity by IP Address with the Rule Wizard" on page 166

- Outgoing IP ranges
  - To collect information and create rules based on the Outgoing IP ranges to which requests were sent, type **3** and press Enter. The Summarize Outgoing IP Address (CPROIPSEC) screen appears, as shown in "Creating a Data Set of Outgoing Activity by IP Address with the Rule Wizard" on page 212.
  - To create rules based on data about Outgoing IP ranges that you have already collected, type **31** and press Enter. The Plan Outgoing IP Security screen appears, as shown in "Analyzing Recent Data on Outgoing Activity by IP Address with the Rule Wizard" on page 215
- Users and Groups
  - To collect information and create rules based on the Users and Groups requesting the activity, type **4** and press Enter. The Summarize User AS/400 Log (CPRUSRSEC) screen appears, as shown in "Creating a Data Set for Users and Groups with the Rule Wizard" on page 287.
  - To create rules based on data about Users and Groups that you have already collected, type **41** and press Enter. The Plan User Security screen appears, as shown in "Analyzing Recent Data on Users and Groups with the Rule Wizard" on page 291.
- Native Objects
  - To collect information and create rules based on the Native Objects on which the activity would operate, type **5** and press Enter. The Summarize Native AS/400 Log (CPRNTVSEC) screen appears, as shown in "Creating a Data Set on Native Objects with the Rule Wizard" on page 373.
  - To create rules based on data about Native Objects that you have already collected, type **51** and press Enter. The Plan Security for Native Objects screen appears, as shown in "Analyzing Recent Data on Native Objects with the Rule Wizard" on page 379.

- IFS Objects
  - To collect information and create rules based on the IFS Objects on which the activity would operate, type **6** and press **Enter**, The **Summarize .IFS Objects Log (CPRIFSSEC)** screen appears, as shown in "Creating a Data Set on IFS Objects with the Rule Wizard" on page 416.
  - To create rules based on data about IFS Objects that you have already collected, type **51** and press **Enter**. The **Plan IFS Security** screen appears, as shown in "Analyzing Recent Data on IFS Objects with the Rule Wizard" on page 420.

## Displaying Firewall Activity by Server

To **display information on each of the servers** on your system, select **1. Servers** from the **Rule Wizards** screen (*STRFW* **> 45**) as shown in "Building Firewall Rules with the Rule Wizards" on page 437.

NOTE: This functionality is limited and differs significantly from the other Rule Wizards.

The **Display User Activity (DSPFWUSRA)** screen appears:

```
                    Display User Activity (DSPFWUSRA)

Type choices, press Enter.

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

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

Enter information into the screen's fields:

**User, <GrpPrf or '%GROUP'**

The user or group requesting the activity. This can be a user name, a generic* name, a group name, a group profile, or ***ALL** for all users.

**Display last minutes**

To view activity in the immediate past, enter a number corresponding to the number of minutes that you would like to check. For example, to check activity in the past 120 minutes,

enter **120** in this field. This value would override starting and ending date and time fields.

**Starting data and time**

**Starting date**

The day or date on which the included data begins.

Allowed values include:

- ***CURRENT**: The current date
- ***YESTERDAY**: Yesterday's date
- ***WEEKSTR**: The first day of the current week. By default, this is Sunday.
- ***PRVWEEKS**: The first day of the previous week
- ***MONTHSTR**: The first day of the current month
- ***PRVMONTHS**: The first day of the previous month
- ***YEARSTR**: The first day of the current year
- ***PRVYEARS**: The first day of the previous year
- ***MON**: Monday
- ***TUE**: Tuesday
- ***WED**: Wednesday
- ***THU**: Thursday
- ***FRI**: Friday
- ***SAT**: Saturday
- ***SUN**: Sunday

**Starting time**

The time on the Starting date at which the included data begins, in **HHMMSS** format.

**Ending date**

The day or date on which the included data ends.

Allowed values are the same as for **Starting date**.

**Ending time**

The time on the Starting date at which the included data ends, in **HHMMSS** format.

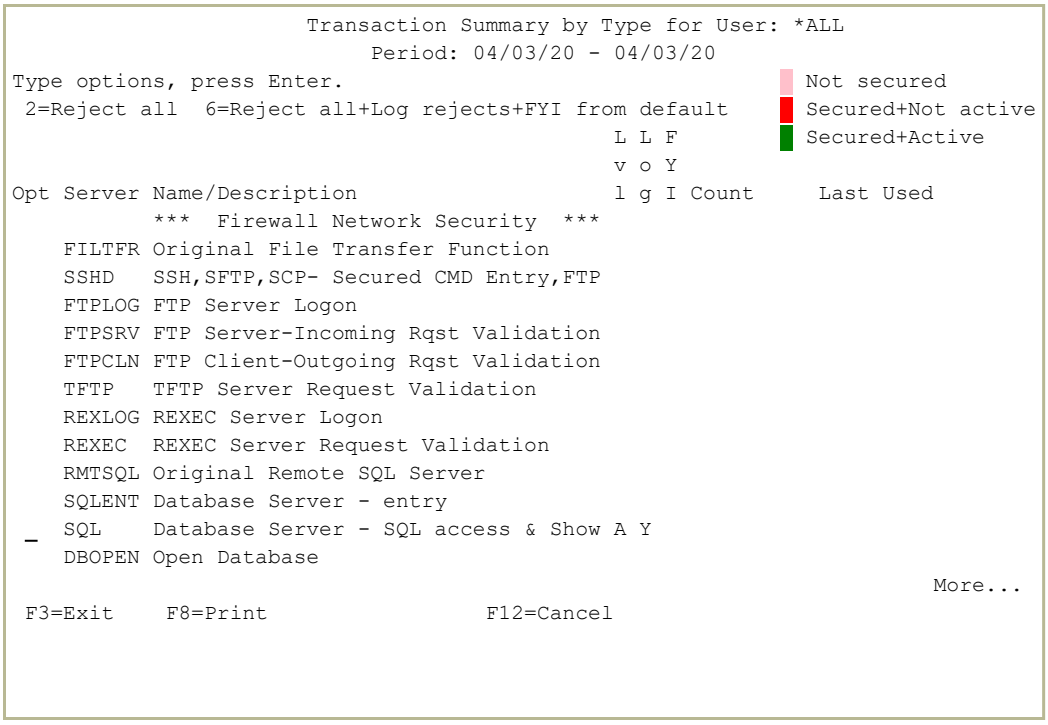
**Server ID**

The server that the activity is attempting to access. To see a list of possible values, press the **F4** key.

**Output**

The destination for the output. To continue on the screen, leave it as the default asterisk ("*****"). Set the field to a value from ***PRINT1** through ***PRINT9** to send it to another destination, as defined within iSecurity Base Configuration.

Press **Enter** to continue to the next screen. The **Transaction Summary by Type for User** screen appears:




The body of the screen lists the servers available on the system. For each, the **Server** field shows a brief name for the server, and the **Name/Description field** contains a free-form text description.

Servers with text shown in **purple** are not secured by Firewall.

Servers shown in **red** are secured but not active. The display shows these additional fields for them:

**Opt**

To reject all activity via this server, set this field to **2**.

To reject all activity, logging the rejected activity and running in FYI mode (as described in "Running Firewall in FYI Simulation mode" on page 536), set this field to **6**.

**Lvl**

The level of security at the server. Possible values include:

- **A**: Allow
- **F**: Full
- **U**: User

**Log**

Shows **Y** if the server activity is logged.

**FYI**

Shows **Y** if the server is running in FYI mode.

Servers shown in green are secured with active protection from Firewall. The **Lvl**, **Log**, and **FYI** fields are shown as they are for the previous category. The **Opt** field is not used. In addition, they show these fields:

**Count**

The number of access requests for the server in the selected time frame.

**Last Used**

The date and time of the last access request in the selected time frame.

## Setting Firewall Rules for Socket Connections

Sockets are communications connection endpoints that you can name and address in a network. You can create Firewall rules to control them.

You can enable sockets from the **Work with Server Security** screen (*STRFW*> **1 > 1**) as shown in "Setting Firewall Rules for Servers" on page 54. To enable accepting, connecting to, or listening on socket connect, you must enable the **Socket Accept (SKTACP)**, **Socket Connect (SKTCNT)**, and **Socket Listen (SKTLSN)** servers, respectively.

To **set Firewall rules for socket connections**, select **15. Incoming/Outgoing Socket Connections** from the main Firewall menu. The **Incoming/Outgoing Connection Rules** screen appears:

```
GSSKMNU              Incoming/Outgoing Connection Rules
 System:   RLDEV
 Select one of the following:

 Definitions
  1. Incoming Connection Rules
  2. Outgoing Connection Rules

  5. IP-Group Definitions


 Reporting
 11. Display Socket Log
 12. Display Socket Connect Log
 13. Display Socket Accept Log
 14. Display Socket Listen Log


 Selection or command
 ===> ____________________________________________________________________
_
 F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
 F13=Information Assistant  F16=System main menu
```

The rules can refer either to ranges of IP addresses specified within the rules or to named IP-Groups, which can refer to sets of IP addresses that are not continuous, indicating which are included or excluded.

To **view and specify IP-Groups**, select **5. IP-Group Definitions**. The **Work with IP-Groups** screen appears, as shown in "Defining IP-Groups for Socket Connections" on page 448.

To set incoming connection rules, select **1. Incoming Connection Rules**. The Work with Incoming Connection Rules screen appears, as shown in "Setting Firewall Rules for Incoming Socket Connections" on page 451.

To set outgoing connection rules, select **2. Outgoing Connection Rules**. The Work with Outgoing Connection Rules screen appears, as shown in "Setting Firewall Rules for Outgoing Socket Connections" on page 454.

To view logs of all socket actions or of only those that connect to, accept connections from, or listen to sockets, select options **11**, **12**, **13**, or **14**, respectively. The Display Firewall Log (DSPFWLOG) screen appears, as shown in "Displaying Firewall Logs" on page 516, with appropriate values set in its **Type** field.

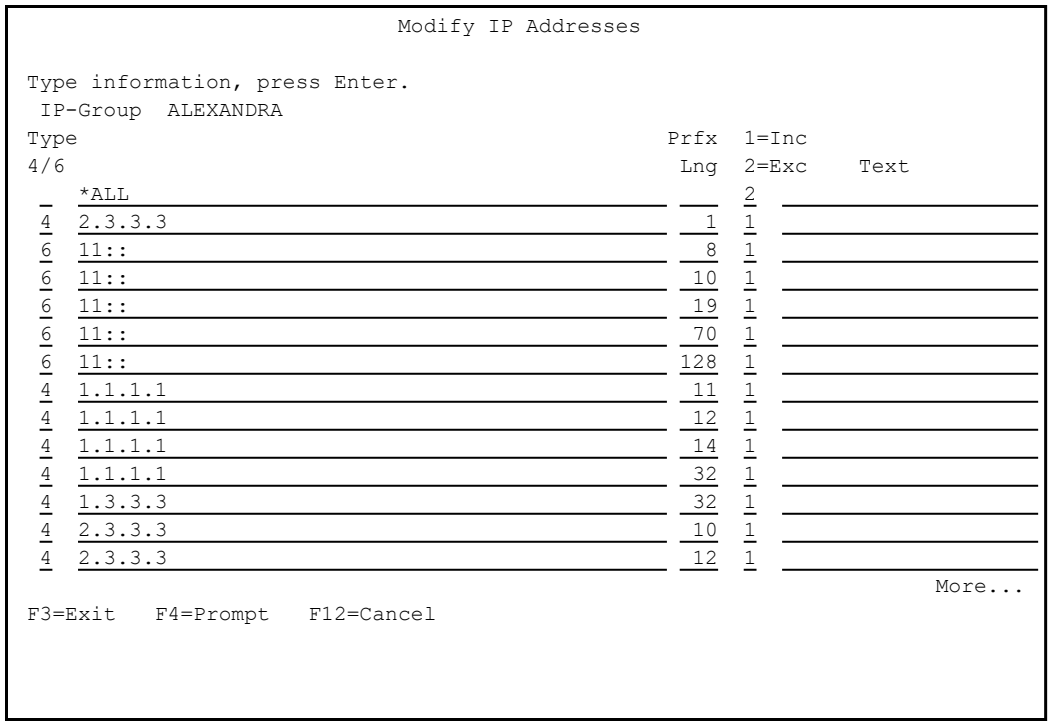
## Defining IP-Groups for Socket Connections

IP-Groups refer to sets of IP addresses that are not continuous, indicating which are included or excluded.

To **define IP-Groups**, select **`5. IP-Group Definitions`** from the **Incoming/Outgoing Connection Rules** menu (*STRFW*`> 15`) as shown in "Setting Firewall Rules for Socket Connections" on page 446. The **Work with IP-Groups** screen appears:

```
                              Work with IP-Groups

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

Opt  IP-Group
 _   *NONE
 _   ALEXANDRA
 _   ALEXPC
 _   ALL WORLD
 _   EVGENY-PC
 _   LINUX
 _   ONEANDONE
 _   RAZLEE3
 _   RLDEMO
 _   RLDEV
 _   RLPRV
 _   RL74A
 _   TEST
 _   TESTX
                                                                    More...
F3=Exit   F6=Add new
```

To **see** and **edit the definition** of an IP-Group, enter **`1`** in the **`Opt`** field for that group. The **Modify IP Addresses** screen appears:




Each line on the body of the screen shows one range of IPv4 or IPv6 addresses and indicates whether the rule includes or excludes it. The lines are considered to be joined by logical ANDs. Firewall uses a Best Fit algorithm to determine the rules for a connection. The rules that fit the current connection most precisely take precedence over more general rules.

For each line, the screen shows these fields:

**Type 4/6**

If set to **4**, the rule is for IPv4 addresses.

If set to **6**, the rule is for IPv6 addresses.

**IP Address** (unlabeled)

The first address of the IP address range.

**Prfx Lng**

For IP address ranges, the number of bits in the address, beginning at the start, that must match the first address to be included.

For IPv4 addresses, the maximum number is 32, meaning that the addresses must match exactly.

For IPv6 addresses, the maximum is 128.

**1=Inc 2=Exc**

If set to **1**, the IP address range is **included** and socket connections from it are **permitted**.

If set to **2**, the IP address range is **excluded** and socket connections from it are **forbidden**.

**Text**

A free-form text description of the rule.

## Setting Firewall Rules for Incoming Socket Connections

To set **incoming connection** rules, select **1. Incoming Connection Rules** from the **Incoming/Outgoing Connection Rules** screen. The **Work with Incoming Connection Rules** screen appears:

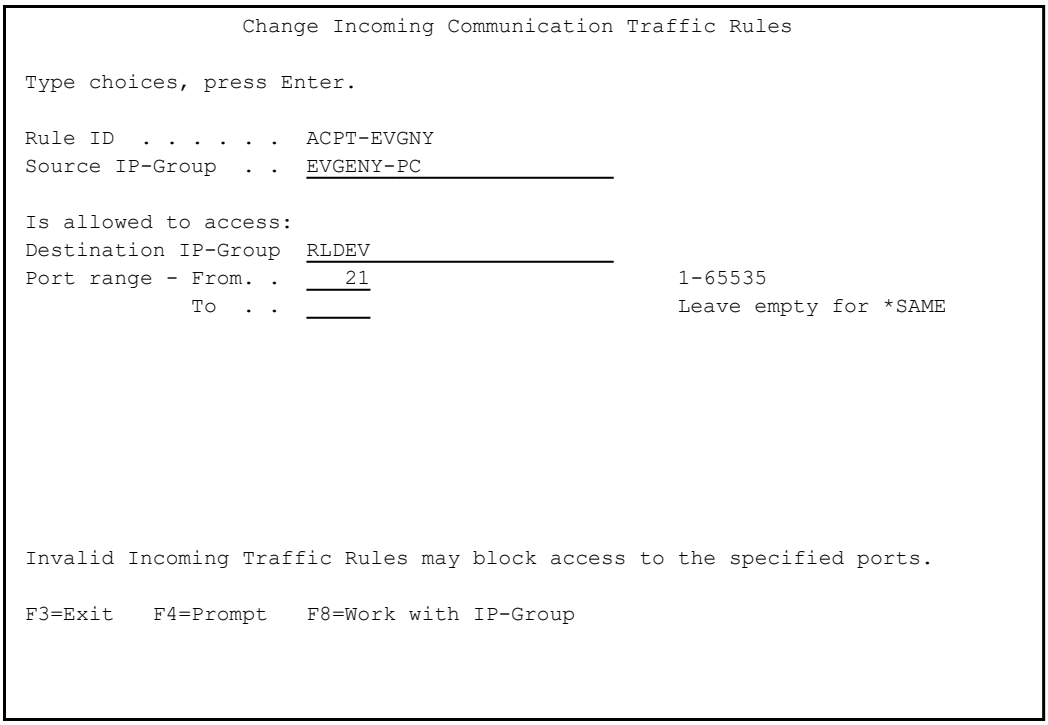
```
                    Work with Incoming Connection Rules
                                        Position to . .  _______________
Type options, press Enter.              Subset by text.  ____________________
 1=Select  4=Remove                            by port.  _____

Opt  Rule ID    Source IP-Group          Allowed to Connect to     Port-range
 _   ACPT-EVGNY EVGENY-PC                RLDEV                       21
 _   ACPT-TZION TZION-PC                 RLDEV                       21    22
 _   ALEXANDRA  RLDEV                    RAZLEE3A-4-ALEXANDRA        21
 _   ALEXANDRA1 ALEXPC                   ALEXANDRA                    7    11
 _   ALEXANDRA3 TZION-PC                 ALEXANDRA1                   2
 _   FOR DEMO   ALL WORLD                RLDEV                       21
 _   FVG        TZION-PC                 RLDEV                       50
 _   NOGA3      *NONE                    RLDEV                       28    90
                                                                      Bottom
Unmentioned Ports are allowed.
F3=Exit   F6=Add new   F8=Work with IP-Groups   F9=IP-Group info (by cursor)
```

Each line on the body of the screen describes a single rule. Each rule is named with a unique **Rule ID**, It permits connections from IP addresses that are in the IP group (as shown in "Defining IP-Groups for Socket Connections" on page 448) indicated in the **Source IP-Group** field to IP addresses in the IP group listed in the **Allowed to Connect to** field using the port or range of ports indicated in the **Port-range** field. (IP-Groups whose names appear in red have not been defined.)

For example, the rule in the first line is named **ACPT-EVGNY**. It allows connections from the IP group **EVGENY-PC** to the IP group **RLDEV** through port **21**.

To **see** a summary of **information about an IP group**, place the cursor on the name of the group and press the **F9** key. A window appears with the information.

To **change** the settings of an existing rule, enter **1** in the **Opt** field for that line. The **Change Incoming Communication Traffic Rules** screen appears:




The fields on this screen correspond to those on the previous screen:

**Rule ID**

The name that the rule was given when created. (Read-Only)

**Source IP-Group**

The IP-Group from which the rule allows access. To select from a list of existing IP-Groups or to create one (as shown in [[? FILL THIS IN ?]], press the **F4** key.

**Destination IP-Group**

The IP-Group to which the rule allows access. To select from a list of existing IP-Groups or to create one (as shown in [[? FILL THIS IN ?]], press the **F4** key.

**Port range - From**

The number of the port, or the lowest number in the port range, to which the rule gives access.

**Port range - To**

The highest number in the port range to which the rule gives access. If the rule is for a single port, leave this field empty.

To **create** a new rule, press the **F6** key on the **Work with Incoming Connection Rules** screen. The **Add Incoming Communication Traffic Rules** screen appears. It is the same as the **Change Incoming Communication Traffic Rules** screen, except that you must enter a name for the new rule in the **`Rule ID`** field.

## Setting Firewall Rules for Outgoing Socket Connections

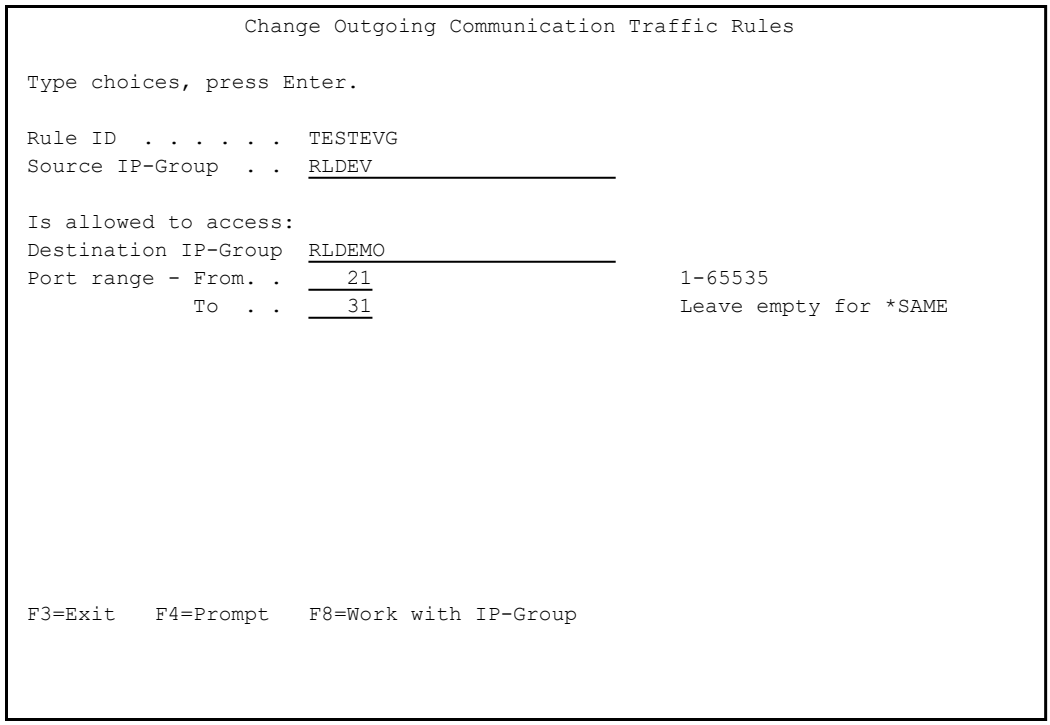
To set **outgoing connection** rules, select **2. Outgoing Connection Rules** from the **Incoming/Outgoing Connection Rules** screen. The **Work with Outgoing Connection Rules** screen appears:

```
                    Work with Outgoing Connection Rules
                                        Position to . .  _______________
Type options, press Enter.              Subset by text.  ____________________
 1=Select  4=Remove                            by port.  _____

Opt  Rule ID    Source IP-Group          Allowed to Connect to     Port-range
 _   TESTEVG    RLDEV                    RLDEMO                      21    31
 _   TESTEVG2   RLDEV                    RL74A                       21    31
 _   TESTEVG3   RLDEV                    LINUX                       21    25

                                                                        Bottom
Unmentioned Ports are allowed.
F3=Exit   F6=Add new   F8=Work with IP-Groups   F9=IP-Group info (by cursor)
```

Each line on the body of the screen describes a single rule. Each rule is named with a unique **Rule ID**, It permits connections from IP addresses that are in the IP group (as shown in "Defining IP-Groups for Socket Connections" on page 448) indicated in the **Source IP-Group** field to IP addresses in the IP group listed in the **Allowed to Connect to** field using the port or range of ports indicated in the **Port-range** field. (IP-Groups whose names appear in red have not been defined.)

For example, the rule in the first line is named **TESTEVG**. It allows connections from the IP group **RLDEV** to the IP group **RLDEMO** through ports **21** through **31**.

To **change** the settings of an existing rule, enter **1** in the **Opt** field for that line. The **Change Outgoing Communication Traffic Rules** screen appears:




The fields on this screen correspond to those on the previous screen:

**Rule ID**

The name that the rule was given when created. (Read-Only)

**Source IP-Group**

The IP-Group from which the rule allows access. To select from a list of existing IP-Groups or to create one (as shown in [[? FILL THIS IN ?]], press the **F4** key.

**Destination IP-Group**

The IP-Group to which the rule allows access. To select from a list of existing IP-Groups or to create one (as shown in [[? FILL THIS IN ?]], press the **F4** key.

**Port range - From**

The number of the port, or the lowest number in the port range, to which the rule gives access.

**Port range - To**

The highest number in the port range to which the rule gives access. If the rule is for a single port, leave this field empty.

To **create** a new rule, press the **F6** key on the **Work with Outgoing Connection Rules** screen. The **Add Outgoing Communication Traffic Rules** screen appears. It is the same as the **Change Outgoing Communication Traffic Rules** screen, except that you must enter a name for the new rule in the **Rule ID** field.

## Setting Free-Style Firewall Rules for Servers

Free-Style rules can use a wide variety of criteria and operators to create further rules based of servers. If the **Free** field on the entry for the server on the Work for Server Security screen is set to **Y** (as shown in "Setting Firewall Rules for Servers" on page 54), Firewall runs free-style rules after the other rules for the server.

To set free-style rules for a server, select **15. Free Style Rules for Socket & Others** from the Firewall main menu.

The Work with Firewall Real-Time Rules screen appears:

```
                    Work with Firewall Real-Time Rules
                        Firewall Free-Style Rules

                                       Subset by entry  . . __
                                         by description . . _______________
Type option, press Enter.                by classification. _  C=Compliance,..
  1=Select  3=Copy  4=Delete          8=Msg  9=Explanation & Classification

Opt Entry Seq Alw          Description
 _    04   __1.0 Y          *SQL Database Server - SQL access
 _    45   __1.0 Y          *DBOPEN Open Database
 _         __2.0 Y          *DBOPEN Open Database
 _    47   __1.0 Y          *SKTACP Socket Accept
 _    50   __1.0 Y          *DBSTT Database statistics
 _         __2.0 Y          *DBSTT Database statistics




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

Each line of the body of the screen refers to a single rule. It contains several fields after the Opt field:

**Entry**

The entry type for the server.

**Seq**

A number determining the order in which rules run. Rules for a given server run together. For example, rules for a given server with the **Seq** values **1.0, 1.1, 2.0, 4.0** would run in that

order, regardless of the order in which they appear in the displayed list.

**Alw**

Whether Firewall allows or rejects access requests that match the rule. Possible values are:

- **Y**: Allow
- **N**: Reject

**Description**

A description of the rule. If no description has been entered, this shows the standard description of the entry type.

To add a rule, press the F6 key. The Add Selection Rule screen appears, as shown in "Adding Free-Style Firewall Rules for Servers" on the facing page. After you enter initial data, corresponding to the fields here, the Filter Conditions screen appears, as shown in "Setting the Order of Rules" on page 462, where you set the detailed criteria for the filter.

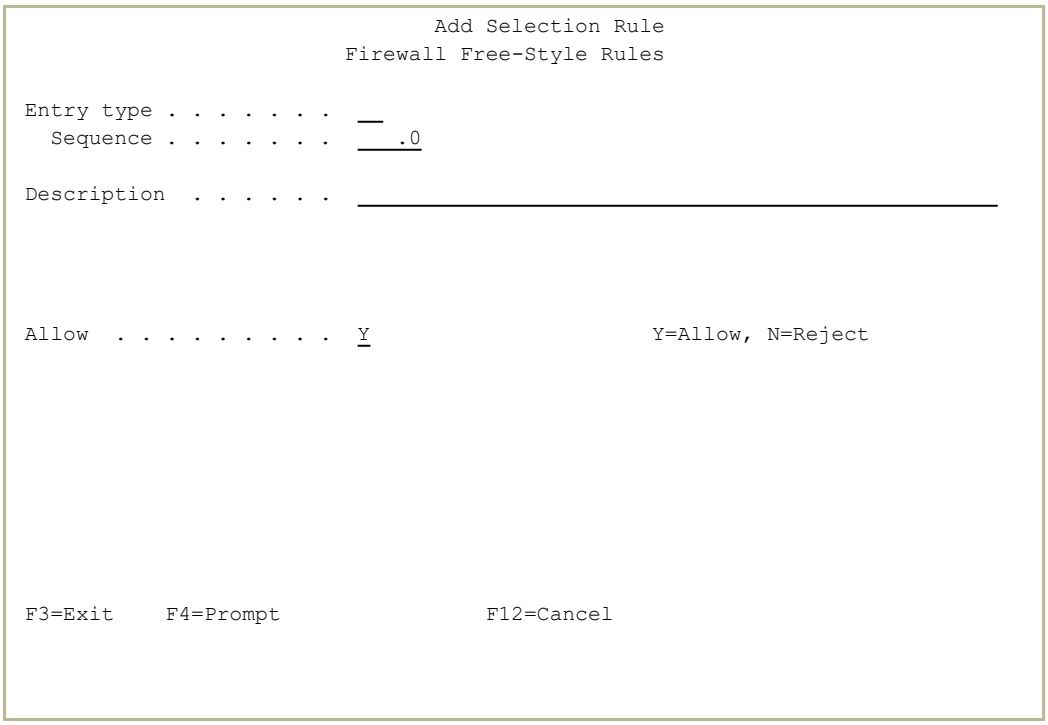
To perform the following tasks, enter the corresponding digits in the **Opt** column for the rule:

- **1**: Modify a rule. The Modify Selection Rule screen appears, where you modify the rule by a process similar to adding a new one.
- **3**: Copy a rule. The Copy Selection Rule screen appears, in which you create the copied rule based on the current one.
- **4**: Delete a rule. The Delete Selection Rule screen appears, confirming that you wish to delete the rule.
- **8**: Create or modify a message to be sent if the rule triggers a response via Action.
- **9**: See and enter more information about a rule.

## Adding Free-Style Firewall Rules for Servers

To **add** a free-style rule, press the **F6** key from the **Work with Firewall Real-Time Rules** screen (***STRFW > 15***) as shown in "Setting Firewall Rules for Servers" on page 54.

The **Add Selection Rule** screen appears:




Enter information in the following fields:

**Entry type**

The entry type for the server. To select the value from a list of valid entry types, press the F4 key.

**Sequence**

A number determining the order in which rules run. For example, rules with the **Sequence** values **1.0, 1.1, 2.0, 4.0** would run in that order, regardless of the order in which they appear in the displayed list.

**Description**

A free-form description of the rule.

**Allow**

Whether Firewall allows or rejects access requests that match the rule. Possible values are:

- **Y**: Allow
- **N**: Reject

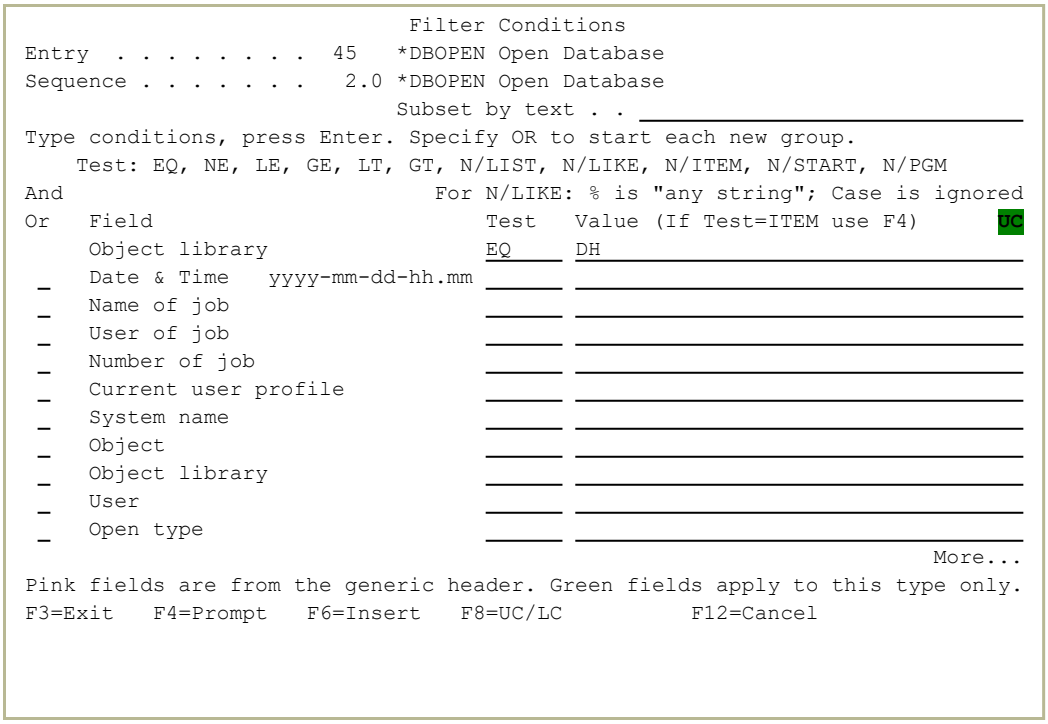
To continue creating the rule when you have entered values for the fields, press Enter. The Filter Conditions screen appears, as shown in "Setting the Order of Rules" on page 462.

To exit the screen without saving the values, press the F12 key.

## Setting Filter Conditions

Using the **Filter Conditions** screen, you can combine tests on any number of fields in a record to determine the system's response. In Firewall, you can set tests on access requests to various servers to determine whether the system accepts or rejects the request.

Within Firewall, the screen appears when you add or modify a free-style rule for filtering access to servers (***STRFW* > 15, F6** or **Opt 1**).




The read-only fields at the top of the screen show the entry type of the server, as both a numerical code and a text description, followed by the relative sequence number in which the filter runs and a text description of the filter (or, if that has not been set, a repetition of the server description).

Each line on the body of the screen shows a single test to be done on the record or request being checked. They include four fields:

**And/Or**

How this test connects to the ones above it, as described below. (This field does not appear on the first line, since no test precedes it.)

**Field**

The name of the field within the record or request being checked. The items in this field are read-only. If they appear in green, they are the names of fields defined for files on that server or entry type. If they appear in pink, they are generic fields referring to the event or request being tested.

**Test**

How the Field is compared to the Value, using comparators shown below.

**Value**

The value against which the Field is tested.

This field is case sensitive, unless the **Test** field is set to **LIKE** or **NLIKE**. The two characters shown in a black-on-green field at the right end of the line of field labels about the first line of the body of the screen shows the Caps-Lock state. If the field shows "UC", typed characters are entered as uppercase. If it shows "LC", typed characters are entered as lowercase. To toggle between them, press the F8 key.

## Setting the Order of Rules

Tests are run in the order that they appear in the list, from the top down. Tests that you have defined appear at the top of the list. Lines without tests appear below them and are ignored by the filter.

To insert a test above a line showing a defined test, place the cursor on the line containing that test and press the F6 key. The Select Multiple Fields window appears, showing the list of generic fields and fields known to the server. To select the field to test, type **1** in its **Opt** field and press Enter. A line for a test based on the field appears on the Filter Conditions screen above the line on which you had placed the cursor.

To **insert a test after the last defined test**, place the cursor on a line below that test and press the **F6** key. The **Select Multiple Fields** window appears, showing the list of generic fields and fields known to the server. To select the field to test, type **1** in its **Opt** field and press **Enter**. The window closes and a line for a test based on the field appears on the **Filter Conditions** screen below the last of the defined tests.

To **delete a test**, clear the Test and Value fields from the line showing the test. The line is removed when the screen refreshes.

To **move a test**, insert an identical test in the new position then clear the original test.

## Test Comparison Operators

The **Test** field can be set to the following values:

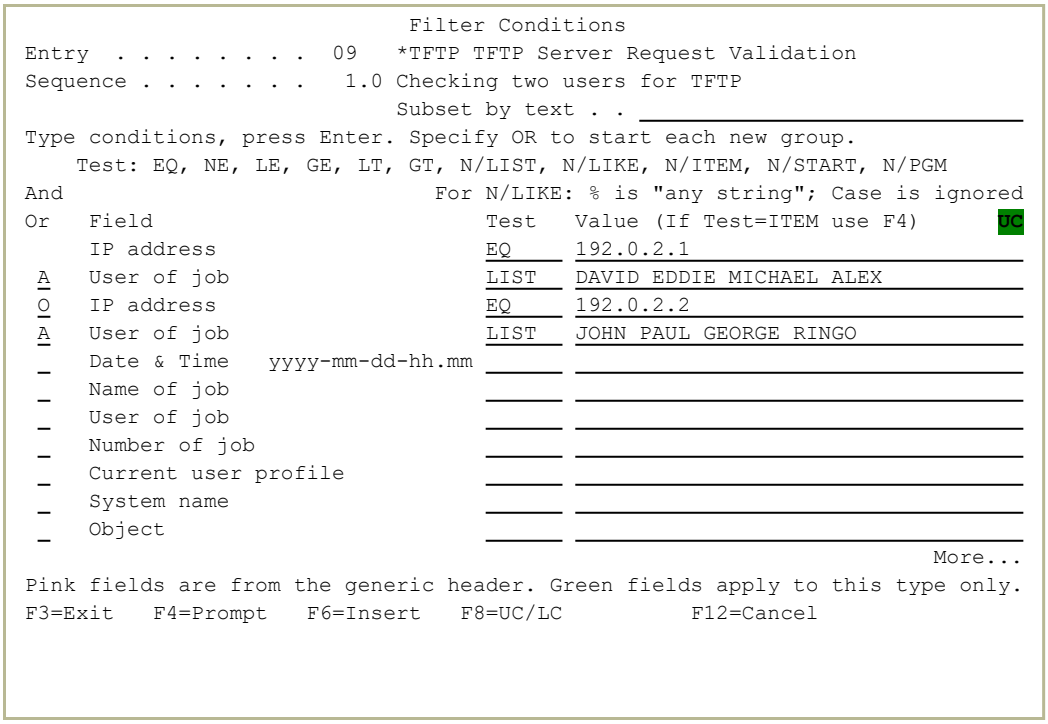
- **EQ**: **Equal to**. The field contents are identical to those of the **Value** field.
- **NE**: **Not equal to**. The field contents are not identical to those of the **Value** field.
- **LT**: **Less than**. The field contents are less than those of the **Value** field.
- **LE**: **Less than or equal to**. The field contents are less than or equal to those of the **Value** field.
- **GT**: **Greater than**. The field contents are greater than those of the **Value** field.
- **GE**: **Greater than or equal to**. The field contents are greater than or equal to those of the **Value** field.
- **LIST**: **Included in list**. The field contents are included in a space-separated list in the **Value** field. For example, "BLUE" is included in the list "RED BLUE GREEN". (**LIST** is not effective if you might be checking values that contain spaces, such as "NEW YORK" or "VAN HALEN". To check those, either create a group to be used with **ITEM** or combine a set of **EQ** tests.)

- **NLIST**: Not included in list. The field contents are not included in a space-separated list in the **Value** field. For example, "YELLOW" is not included in the list "RED BLUE GREEN". (Like **LIST**, **NLIST** is not effective if you might be checking values that contain spaces.)
- **LIKE**: Matches a substring search. The field contents match the string in the Value field. The "%" character can be used as a wild card in the **Value** field. For example, if the field contents consists of the string "PURPLE", it would be **LIKE** the **Value** field string "%URP%".
- **NLIKE**: Does not match a substring search. The field contents do not match the string in the **Value** field. The "%" character can be used as a wild card in the **Value** field. For example, if the field contents consists of the string "ORANGE", it would be **NLIKE** the **Value** field string "%URP%".
- **ITEM**: True if the value of the **Field** field is a member of a group named in the **Value** field. After entering **ITEM** in the **Test** field, place the cursor in the Value field and press the F4 key. The Select Subject window appears, containing a list of groups known to the system. To select a group from this list, type **1** in the **Opt** field for that group and press the Enter key. To work with the groups, including editing or removing them, press the F6 key.
- **NITEM**: True if the value of the **Field** field is not a member of a group named in the **Value** field. You can select a group from a list as shown for the **ITEM** operator.
- **START**: True if the value of the **Field** field begins with the characters in the **Value** field.
- **NSTART**: True if the value of the **Field** field does not begin with the characters in the **Value** field.
- **PGM**:True if a specific user program, run against the **Field** contents, returns a value of True. Indicate the program in the **Value** field as "LIBRARY/PROGRAM".
- **NPGM**: True if a specific user program, run against the **Field** contents, returns a value of False. Indicate the program in the **Value** field as "LIBRARY/PROGRAM".

## Combining Tests with the And/Or Field

By default, consecutive tests on the screen are combined. The result is True only if the result of each of the tests is True.

If the line for a test contains the letter "**O**" (for "Or") in its **And/Or** field, it causes the filter to consider the tests included on the screen as two distinct groups. If either the group of tests before the line with the "**O**" or the group of tests beginning with and following that line are all True, the result is True.




In this example, using values for iSecurity/Firewall, the filter conditions are true if either

- The IP address is 192.0.2.1 and the user is any of DAVID, EDDIE, MICHAEL, or ALEX, or
- The IP address is 192.0.2.2 and the user is any of JOHN, PAUL, GEORGE, or RINGO.

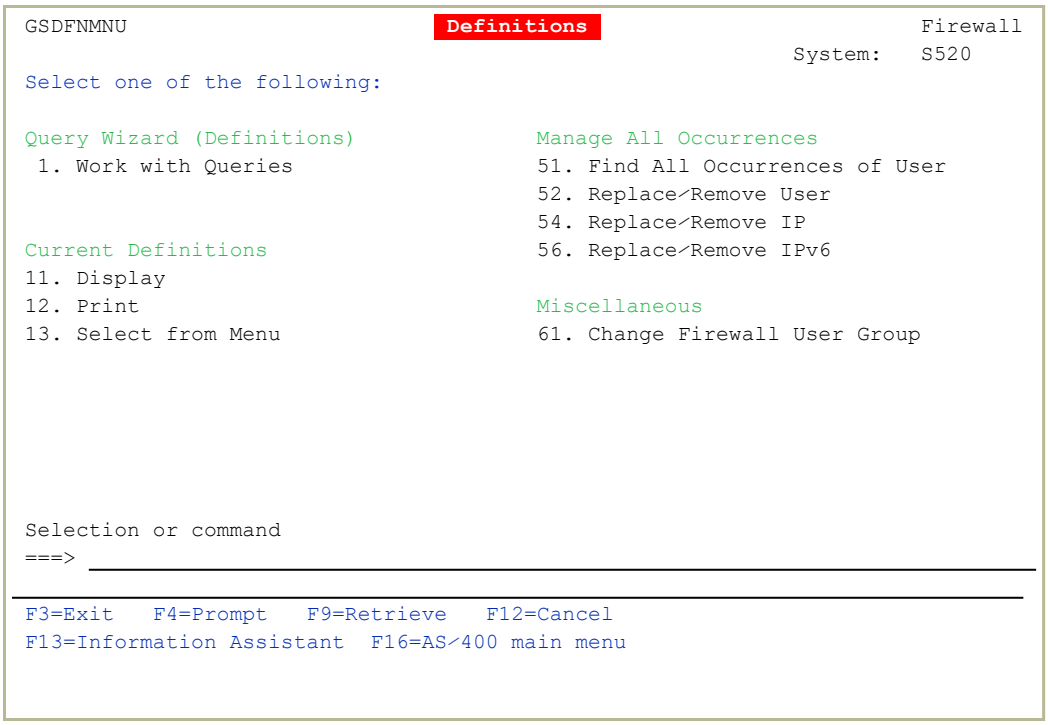
This follows standard logic operations, where AND has precedence over OR, as shown in IBM documentation at https://www.ibm.com/support/knowledgecenter/SSLTBW_2.4.0/com.ibm.zos.v2r4.f54dg00/ispdg170.htm

# Displaying Definitions and Changing Occurrences of Users and Addresses

To **display definitions and to change rules for users, groups, and addresses**,

select **42. Reporting of Definitions** from the **Firewall** main menu.

The **Definitions** screen appears:




To **view and modify query definitions**,

select **1. Work with Queries**. The **Work with Queries** screen appears, as shown in "Creating and Running Queries" on page 473.

To **display query definitions**,

select **11. Display**. The **Display Security I Definitions (DSPS1DFN)** screen appears, as shown in "Running Predefined Reports" on page 513

To **print query definitions**,

select **12. Print**. The **Display Security I Definitions (DSPS1DFN)** screen appears, as shown in "Running Predefined Reports" on

page 513, with the **Output** field, when it appears, set to ***PRINT**.

To select definitions to display or print from a menu,

select **13. Select from Menu**. The Definition Reporting - By Subject screen appears, as shown in "Running Predefined Reports" on page 513.

To print a report of all rules that affect and groups that include a user,

select **51. Print All Occurrences of User**. The Replace FW user (RPLFWUSR) screen appears, with the **Replace to user** field set to ***PRINT**. Enter the name of the user or group in the **Replace from user** field. The report is sent to a spool file.

To remove rules that affect a user or group, or to replace one user or group affected by rules with another,

select **52. Replace/Remove User**. The Replace FW user (RPLFWUSR) screen appears. Enter the name of the user or group to be replaced or removed in the **Replace to user** field.

To remove rules that affect a user or group, enter ***REMOVE** in the **Replace to user** field.

NOTE: Whenever you remove a user from your system, use this screen to remove the rules for that user.

To replace one user or group affected by rules with another, enter the name of the replacement in the **Replace from user** field.

To remove rules that affect an IP address range , replace one IP address range affected by rules with another, or print a report of rules affecting that range,

select **54. Replace/Remove IP**. The Replace FW IP (RPLFWIP) screen appears. Enter the IP address in the **From IP** field and the subnet mask (or ***ANY**) in the **From SubNet Mask** field.

To remove rules that affect an IP address range, enter ***REMOVE** in the **To IP, *REMOVE, *PRINT** field.

To replace one IP address range affected by rules with another,

enter the IP address in the **To IP, *REMOVE, *PRINT** field and the subnet mask (or *SAME) in the **To SubNet Mask** field.

To print rules that affect an IP address, enter ***PRINT** in the **To IP, *REMOVE, *PRINT** field.

To remove rules that affect an IPv6 address range , replace one IPv6 address range affected by rules with another,

select **56. Replace/Remove IPv6**. The Replace FW IPv6 (RPLFWIPV6) screen appears. Enter the IPv6 address in the **From IPv6** field and the prefix length (or ***ANY)** in the **From Prefix Length** field.

To remove rules that affect an IPv6 address range, enter ***REMOVE** in the **To IPv6, *REMOVE** field.

To replace one IPv6 address range affected by rules with another,

enter the IPv6 address in the **To IPv6, *REMOVE** field and the prefix length (or ***SAME**) in the **To Prefix Length** field.

To add a member to a Firewall group, replace a member in it, or remove a member from it,

select **61. Change Firewall User Group**. The Change Firewall User Group (CHGFWGRP) screen appears as shown in "Adding, Replacing, or Removing Members of Firewall Groups" on page 284.

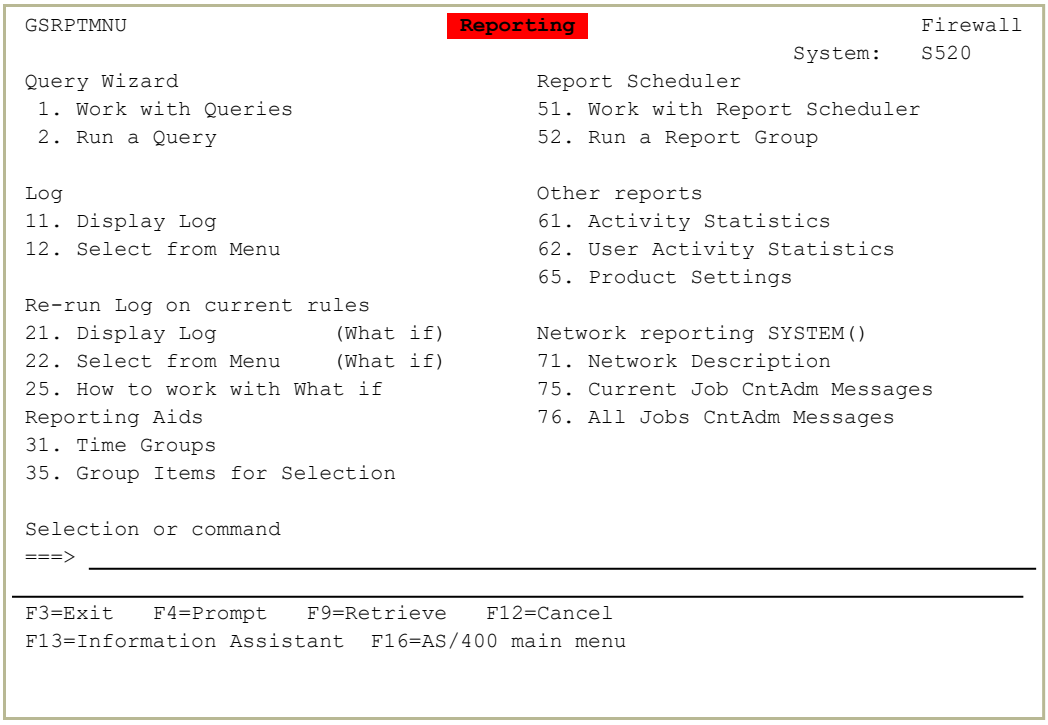
# Creating and Running Firewall Queries and Reports

Firewall includes powerful tools for creating and viewing queries, reports, and logs. Many of these tools are also available within other iSecurity products, giving a consistent experience in using them.

Among Firewall's unique capabilities, it can test rule sets in "What if?" mode against existing logs, to see how they would respond to actual recorded events that your system has experienced.

To work with these features, select **41. Log, Queries, What-if** from the **Firewall Main Menu**.

The **Reporting** screen appears:




**To work with queries:**

**To create and modify queries,**

select **1. Work with Queries**. The **Work with Queries** screen appears, as shown in "Adding and Modifying Queries" on page 476.

**To** run existing queries,

select **2. Run a Query**. The Run Firewall Query (RUNFWQRY) screen appears, as shown in "Running Queries" on page 491.

**To** work with logs:

**To** display the Firewall log,

select **11. Display Log**. The Display Firewall Log (DSPFWLOG) screen appears, as shown in "Displaying Firewall Logs" on page 516.

**To** display filtered logs for specific subjects,

select **12. Select from Menu**. The Logs by Subjects screen appears. Each item on that screen runs the Display Firewall Log (DSPFWLOG) screen, with different presets selected to filter or organize the output by that item.

**To** run "What if" tests on the Firewall log,

select **21. Display Log (What if)**. The Display Firewall Log (DSPFWLOG) screen appears, with the **Recalculate and display** field set to ***YES**. From this screen, you can select a time period in the past and other parameters. Firewall processes the log from that time with the current security settings, so you can see how the current rules would respond to access requests that had happened during that time.

**To** run "What if" tests for specific subjects,

select **22. Select from Menu (What if)**. Each item on that screen runs the Display Firewall Log (DSPFWLOG) screen, with different presets selected to filter or organize the output by that item, and the **Recalculate and display** field set to ***YES**. From that screen, you can select a time period in the past and other parameters. Firewall processes the log from that time with the current security settings, so you can see how the current rules would respond to access requests corresponding to that item that had happened during that time.

**To** work with groups

**To** create and modify time groups,

select **31. Time Groups**. The Define Time Groups screen appears, as shown in "Defining Time Groups" on page 504. Using time groups, you can define sets of time-based filters, such as the days and times of work shifts, to use in queries.

**To** create and modify groups of users,

within Firewall, open the Work with User Security screen (*SCRFW* **> 3 > 1**) as shown in "Setting Firewall Rules for Users and Groups" on page 226.

**To** create and modify classes of groups of users and other objects,

select **35. Group Items for Selection**. The Work with Classes of Groups screen opens, as shown in "Defining Groups of Items" on page 508.

**To** work with reports

**To** run groups of reports,

select **52. Run a Report Group**. The Run Report Group (RUNRPTGRP) screen appears, as shown in "Running Report Groups On Demand" on page 512.

**To** schedule reports to run,

select **51. Work with Report Scheduler**. The Work with Report Scheduler screen appears, as shown in "Scheduling Reports" on page 495.

**To** run reports on all users' activity,

select **61. Activity Statistics**. The Display User Activity (DSPFWUSRA) screen appears, as shown in "Displaying Firewall Activity by Server" on page 442, with the **User** field set to ***ALL**.

**To** run reports on a single user's activity,

select **62. User Activity Statistics.** The Display User Activity (DSPFWUSRA) screen appears, as shown in

"Displaying Firewall Activity by Server" on page 442, with the **User** field empty.

**To** run reports on servers,

select **65. Product Settings**. The Definition Reporting - By Subject screen appears, as shown in "Running Predefined Reports" on page 513.

**To** view other network and system information,

**To** ping and test DDM connections for network systems,

select **71. Network Description**. The standard Display Network Systems screen appears.

**To** view Central Administration messages for current jobs,

select **75. Current Job CntAdm Messages**. The Display Messages screen appears, showing the job log for the current job.

**To** view Central Administration messages for all jobs,

select **76. All Jobs CntAdm Messages**. The Display Messages screen appears, showing the job log for all jobs.

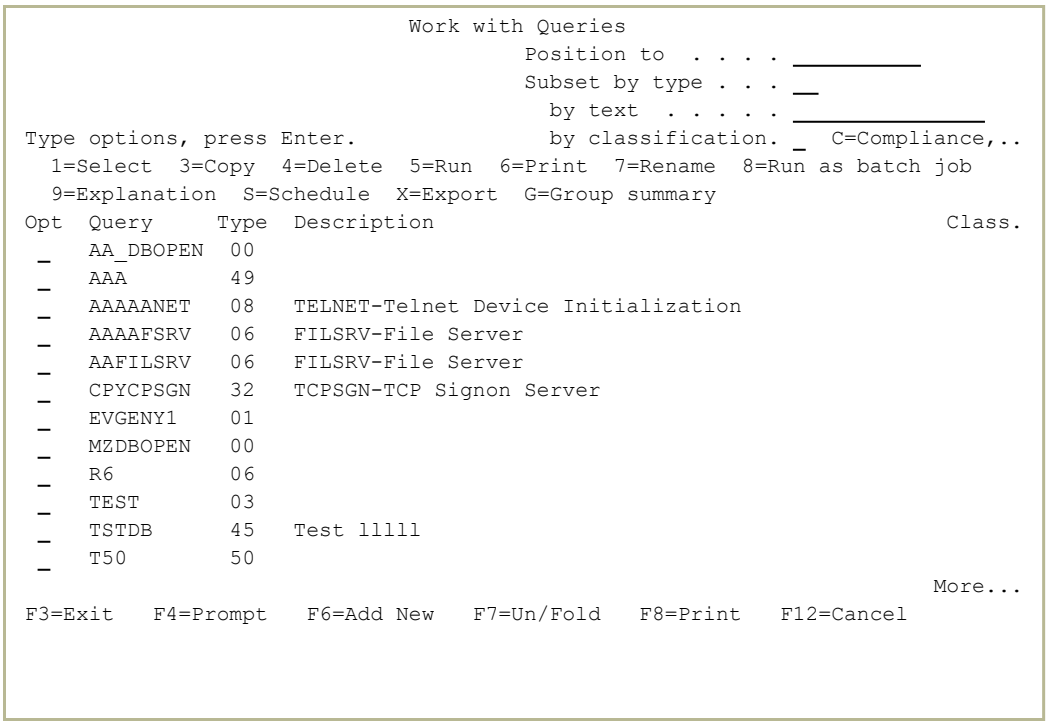
To exit the screen, press the F3 or F12 key.

## Creating and Running Queries

The Query Wizard is a powerful tool that allows you to select exactly which events and actions you wish to examine and to specify the format of the printed or displayed output. You create query definitions using a series of parameter screens covering the various components.

To **open the Query Wizard** within Firewall, select **`1. Work with Queries`** from the **Reporting** menu (***STRFW > 41 > 1***), as shown in "Creating and Running Firewall Queries and Reports" on page 469.

The **`Work with Queries`** screen appears.



```
                              Work with Queries
                                       Position to  . . . . _________
                                       Subset by type . . . __
                                         by text  . . . . . _______________
Type options, press Enter.               by classification. _  C=Compliance,..
  1=Select  3=Copy  4=Delete  5=Run  6=Print  7=Rename  8=Run as batch job
  9=Explanation  S=Schedule  X=Export  G=Group summary
Opt  Query     Type  Description                                      Class.
 _   AA_DBOPEN  00
 _   AAA        49
 _   AAAAANET   08   TELNET-Telnet Device Initialization
 _   AAAAFSRV   06   FILSRV-File Server
 _   AAFILSRV   06   FILSRV-File Server
 _   CPYCPSGN   32   TCPSGN-TCP Signon Server
 _   EVGENY1    01
 _   MZDBOPEN   00
 _   R6         06
 _   TEST       03
 _   TSTDB      45   Test llll
 _   T50        50
                                                                    More...
F3=Exit   F4=Prompt   F6=Add New   F7=Un/Fold   F8=Print   F12=Cancel
```

The body of the screen lists existing queries. After the **`Opt`** field for entering options, it has the following fields:

**`Query`**

A unique name for the query

**`Type`**

The query information type. Press the **F4** key for a list of available query types.

**Description**

A free-form text description of the query

**Class.**

Letters or digits for classifications of queries. Predefined values include

- **C**: Compliance (SOX/ISO17799/PCI, etc)
- **U**: User
- **O**: Object
- **S**:System Values
- **N**: Network

You can freely define meanings for the digits **0** through **9**.

To **add** a new query, press the **F6** key. The **Add Query** screen appears, as shown in "Adding and Modifying Queries" on page 476.

To **view or modify further information** on a query, type **1** in the **Opt** field for the query and press **Enter**. The **Modify Query** screen appears, as shown in "Adding and Modifying Queries" on page 476.

To **view or modify the classification and explanation** of a query, type **9** in the **Opt** field for the query and press **Enter**. The **Query Explanation and Classification** screen appears. Enter classification characters (as shown for the **Class** field above) in the **Classification** list field. Enter a free-form explanation of the query in the **Query explanation** field, which is printed on output reports that include headers.

To **view or modify summaries** included in the query output, type **G** (for Group Summary) in the **Opt** field for the query and press **Enter**. The **Modify Query Summary Definitions** screen appears, as shown in "Modifying Query Summary Definitions" on page 487.

To **copy** information from one query to another, type **3** in the **Opt** field for the query and press **Enter**. The **Copy Query** window opens. The read-only **From** field shows the name and description of the original query. Enter the name and a free-form description for the new query in the **To** fields.

To **rename** a query, type **7** in the **Opt** field for the query and press **Enter**. The **Rename Query** window opens. The read-only **From** field shows the name and description of the original query. Enter the new name and description for the query in the **To** fields.

To **delete** a query, type **4** in the **Opt** field for the query and press **Enter**. The **Delete Query** window opens. Press **Enter** to confirm the deletion or the **F12** key to cancel it.

To **run a query interactively**, type **5** in the **Opt** field for the query and press **Enter**. The **Run Firewall Query (RUNFWQRY)** screen appears (as shown in "Running Queries" on page 491) with the query name in its **Query** field and the Output field set to *****, which immediately sends the output to the screen.

To **run a query interactively and print the output**, type **5** in the **Opt** field for the query and press **Enter**. The **Run Firewall Query (RUNFWQRY)** screen appears (as shown in "Running Queries" on page 491) with the query name in its **Query** field and the Output field set to ***PRINT**, which immediately sends the output to the screen.

To **run a query as a batch job**, type **8** in the **Opt** field for the query and press **Enter**. The **Run Firewall Query (RUNFWQRY)** screen appears (as shown in "Running Queries" on page 491) with the query name in its **Query** field and the Output field set to ***BATCH**, which immediately sends the output to the screen.

To **schedule** a query to run regularly as part of a report group, type **S** in the **Opt** field for the query and press **Enter**. The **Schedule Query** screen appears, as shown in "Scheduling Queries" on page 485.

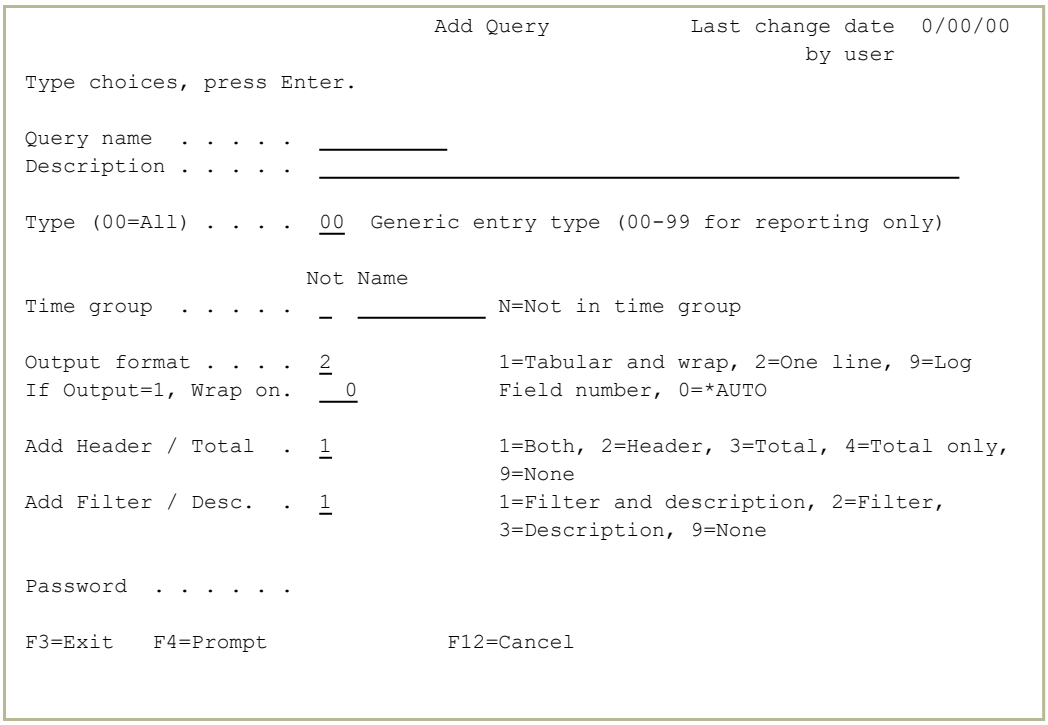
To **export** a query definition, type **X** in the **Opt** field for the query and press **Enter**. A confirmation line stating that the definition has been exported appears at the bottom of the screen. After you have finished working with this screen and press **F3** to exit, the **Export iSecurity Query Definitions** screen appears. You can specify whether to export the definition to a particular system, a group of systems, or to all. If you set the field to ***NONE**, it is exported to a save file with a name indicated on the last line of that screen.

## Adding and Modifying Queries

To **add** a new query, press the **F6** key from the **Work with Queries** screen *(STRFW **>** **41** **>** **1**)* as shown in "Creating and Running Queries" on page 473.

To **modify** an existing query, enter **1** in the **Opt** field for the query on the **Work with Queries** screen.

The **Add Query** or **Modify Query** screen appears. (The only differences between them are the screen title and that some fields for the **Modify Query** screen are read-only, as noted in their descriptions.)



```
                              Add Query           Last change date  0/00/00
                                                           by user
Type choices, press Enter.

Query name  . . . . .  __________
Description . . . . .  ____________________________________________________

Type (00=All) . . . .  00  Generic entry type (00-99 for reporting only)

                      Not Name
Time group  . . . . .  _  __________ N=Not in time group

Output format . . . .  2             1=Tabular and wrap, 2=One line, 9=Log
If Output=1, Wrap on.  __0           Field number, 0=*AUTO

Add Header / Total  .  1             1=Both, 2=Header, 3=Total, 4=Total only,
                                     9=None
Add Filter / Desc.  .  1             1=Filter and description, 2=Filter,
                                     3=Description, 9=None

Password  . . . . . .

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

The screen contains the following fields:

**Query name**

A unique name for the query. Do not begin the name with the letter "**Z**", which is reserved for queries included with iSecurity products. (For **Modify Query**, this field is read-only.)

**Description**

A free-form description of the query.

**Type (00-All)**

A code indicating the type of the query. For a list of possible values, press the F4 key. (For Modify Query, this field is read-only.)

The type **$9** is a special value, with which you can use the output from any command as input for the query. If you set this field to **$9**, the Spool File Query Selection screen appears after this screen, in which you can specify the command.

**Time group**

Restrict information to times within a named time group or, if the first one-character field is set to **N**, to times outside of it. For a list of valid time groups, press the F4 key.

**Output format**

The format in which each line of output appears. Possible values are:

- **1**: Display in tabular format. If the data is longer than an output line, wrap on the field of the data indicated on the next field of this screen.
- **2**: Display in tabular format on a single line.
- **9**: Display in log format.

**If Output=1, Wrap on**

If the **Output format** field is set to **1**, the number of the data field on which to start a new line. If this field is set to **0**, wrap output to the next line at the start of any data field that would cause the output to exceed its maximum line length.

**Add Header / Total**

Whether the output should include field headers or a summary of totals. Possible values include:

- **1**: Include both the headers and summary.
- **2**: Include only the header.
- **3**: Include the summary.
- **4**: Omit the body of the report and include the summary.
- **9**: Include neither headers nor summary.

**Add Filter / Desc.**

Whether the output should include a listing of the query's filter conditions or a text description of them. Possible values include:

- **1**: Include both filter and description.
- **2**: Include only the header
- **3**: Description
- **4**: Include neither filter nor description.

**Password**

Add a password to this query to protect it from being changed. This is a hidden field, without an underline marking its location. It begins on the same line as its label, in the same column as the entry areas for the other fields.

After entering values for the fields, press **Enter**.

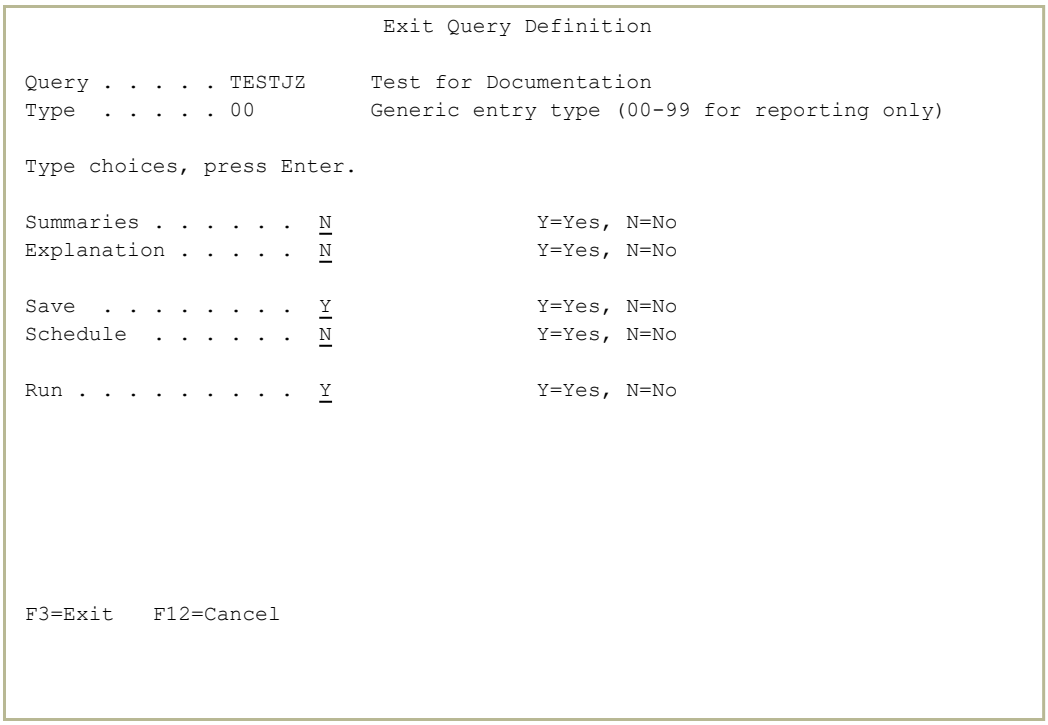
If you set the **Type (00-All)** field to **$9**, the **Spool File Query Selection** screen appears. Specify the command string, then press **Enter**.

The **Filter Conditions** screen appears, as shown in "Setting the Order of Rules" on page 462. Set the filter conditions for the query, then press **Enter**,

The **Select Output Fields** screen appears, as shown in "Selecting Output Fields for Queries and Reports" on page 481. Select the output fields and the order in which they appear on lines of output, then press **Enter**.

The **Select Sort Fields** screen appears, as shown in "Selecting Sort Fields for Queries and Reports" on page 483. Select the order in which the data records will be sorted in the output, then press **Enter**.

The **Exit Query Definition** screen appears:




The screen includes the following fields. For each, enter **Y** for "Yes" or **N** for "No".

**Summaries**

Whether the output include a summary of totals. If set to **Y**, the Modify Query Summary Definitions screen appears after you press Enter, as shown in "Modifying Query Summary Definitions" on page 487.

**Explanation**

Whether the output should include text description in its header. If set to **Y**, the Query Explanation and Classification screen appears after you press Enter, as shown in "Creating Query Classifications and Explanations" on page 489.

**Save**

Whether to save the query definition.

**Schedule**

Whether to add the query to a group to run on a schedule. If set to **Y**, the Schedule Query screen appears after you press Enter, as shown in "Scheduling Queries" on page 485.

**Run**

Whether to run the query immediately. If set to **Y**, the Run Firewall Query (RUNFWQRY) screen appears after you press Enter, as shown in .

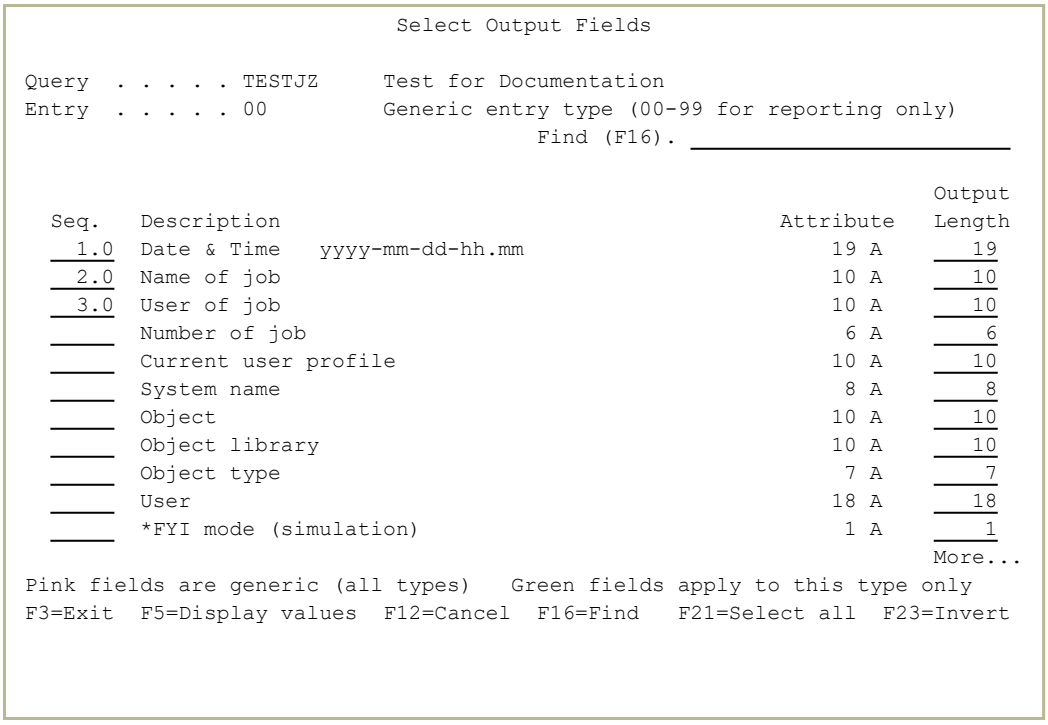
To save your selections and exit the screen, press Enter. The additional screens related to your selections appear.

To exit the screen without saving your selections, press the F12 key.

# Selecting Output Fields for Queries and Reports

The **Select Output Fields** screen specifies the fields to appear in a query and the order in which they appear in each record.

The screen appears in the process of adding or modifying queries, as shown in "Adding and Modifying Queries" on page 476.



```
                          Select Output Fields

Query  . . . . . TESTJZ     Test for Documentation
Entry  . . . . . 00         Generic entry type (00-99 for reporting only)
                                    Find (F16). _____________________________


                                                                        Output
  Seq.   Description                                          Attribute  Length
   1.0   Date & Time   yyyy-mm-dd-hh.mm                          19 A      19
   2.0   Name of job                                            10 A      10
   3.0   User of job                                            10 A      10
         Number of job                                           6 A       6
         Current user profile                                   10 A      10
         System name                                             8 A       8
         Object                                                 10 A      10
         Object library                                         10 A      10
         Object type                                             7 A       7
         User                                                   18 A      18
         *FYI mode (simulation)                                  1 A       1
                                                                        More...
Pink fields are generic (all types)   Green fields apply to this type only
F3=Exit  F5=Display values  F12=Cancel  F16=Find   F21=Select all  F23=Invert
```

The read-only **Query** field shows the name and description of the query.

The read-only **Entry** field shows the code and description of the entry type that the query processes.

The body of the screen contains one line for each field defined for the entry type specified for the query (shown in green) as well as one for each of several generic fields that do not depend on the entry type (shown in pink).

Each contains the following fields:

**Seq.**

A number determining the order in which the fields appear. For example, fields with the **Seq** values **1.0, 1.1, 2.0, 4.0** would appear in that order, regardless of the order in which they appear in the displayed list.

**Description**

A read-only text description of the field, as defined for that entry type or generic field.

**Attribute**

A pair of read-only fields showing the length and type of the field, as defined for that entry type or generic field.

**Output Length**

The number of characters allocated for the field contents in the output.

To find a field in the list, enter a string from the field name in the **Find** field and press the F16 (Shift+F4) key. The cursor moves from the current field to the next field with a name that includes that string. If there are no more field names containing the string in the rest of the list, it searches from the beginning.

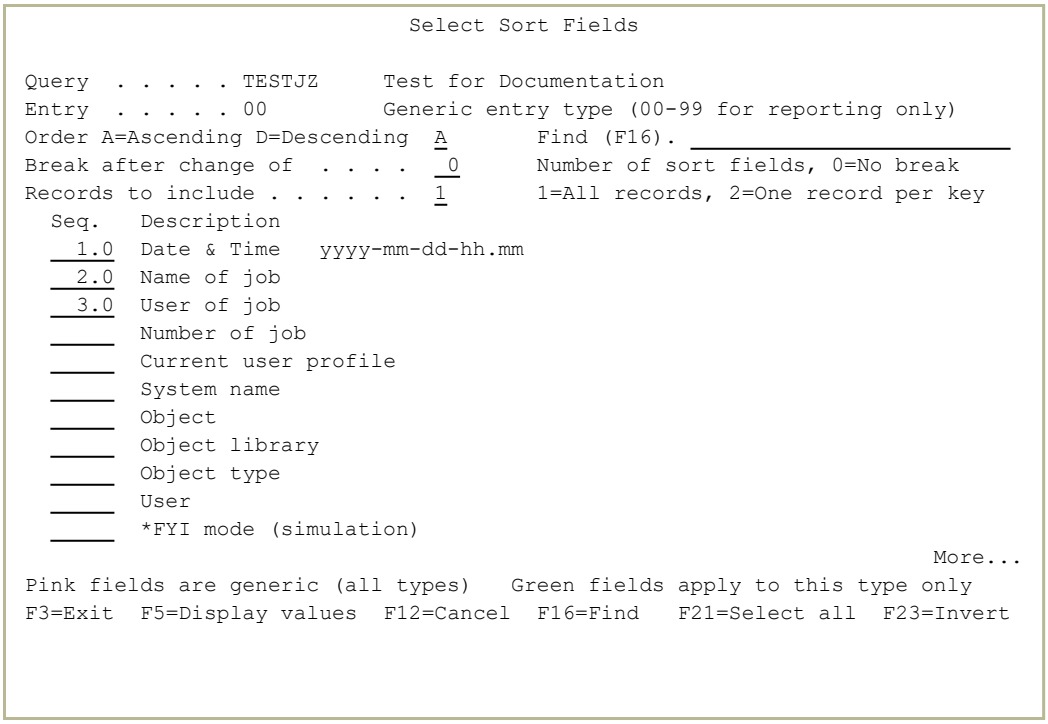
To select all fields, press the F21 (Shift+F9) key.

To invert the selection, selecting all fields that are not currently selected and deselecting those that are, press the F23 (Shift+F11) key.

# Selecting Sort Fields for Queries and Reports

The **Select Sort Fields** screen specifies the fields by which data is sorted in a query.

The screen appears in the process of adding or modifying queries, as shown in "Adding and Modifying Queries" on page 476.




The read-only **Query** field shows the name and description of the query.

The read-only **Entry** field shows the code and description of the entry type that the query processes.

The following fields control the presentation of the records:

**Order A=Ascending D=Descending**

The order in which the sorted records appear in the output.

**Break after change of**

The number of changes in sort fields that trigger a break in the output. If set to **0**, there are no breaks.

**Records to include**

Whether to include only records on which values of sorted fields change. Possible values are:

- **1**: Include all records
- **2**: Include only the records on which values change.

The body of the screen contains one line for each field defined for the entry type specified for the query (shown in green) as well as one for each of several generic fields that do not depend on the entry type (shown in pink).

Each contains the following fields:

**Seq.**

A number determining the priority with which the records are sorted. For example, fields with the **Seq** values **1.0, 1.1, 2.0, 4.0** would have sort priorities in that order, regardless of the order in which they appear in the displayed list.

**Description**

A read-only text description of the field, as defined for that entry type or generic field.

To find a field in the list, enter a string from the field name in the **Find** field and press the F16 (Shift+F4) key. The cursor moves from the current field to the next field with a name that includes that string. If there are no more field names containing the string in the rest of the list, it searches from the beginning.

To select all fields, press the F21 (Shift+F9) key.

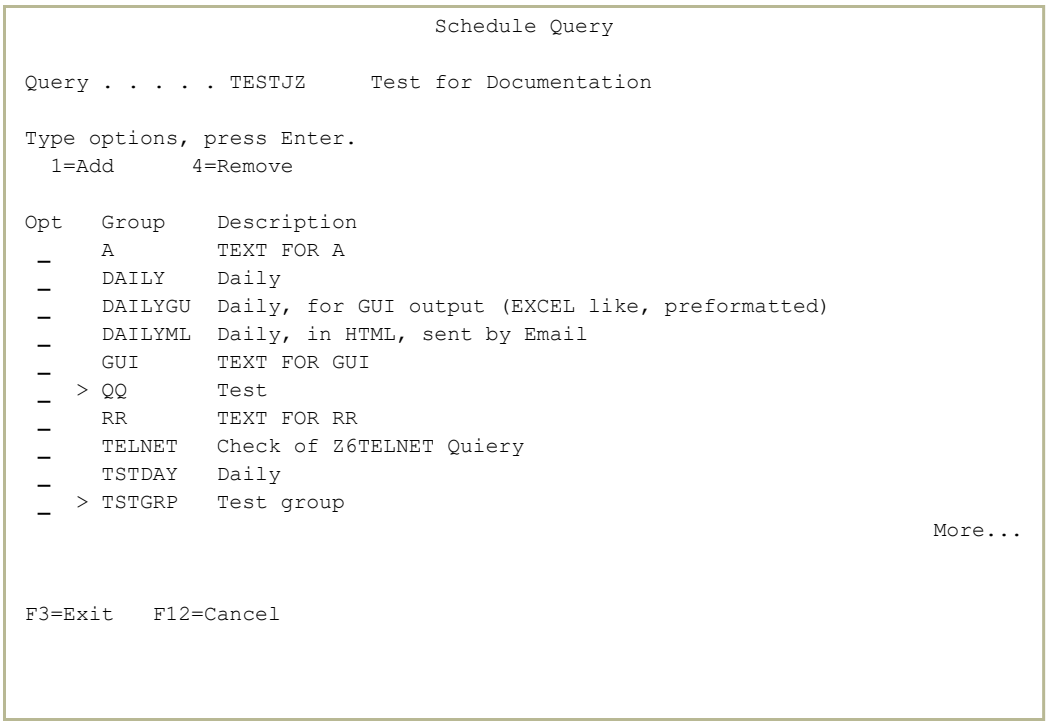
To invert the selection, selecting all fields that are not currently selected and deselecting those that are, press the F23 (Shift+F11) key.

## Scheduling Queries

With the **Schedule Query** screen, you can specify when a query is to run by adding it to schedule groups (as shown in "Defining Groups of Items" on page 508) or removing it from them.

To schedule a query, type **S** in the **Opt** field for that query on the **Work with Queries** screen (*STRFW* **> 14 > 1**) as shown in "Creating and Running Queries" on page 473.

The screen also appears in the process of adding or modifying queries if the **Schedule Query** field on the **Exit Query Definition** screen is set to **Y** (as shown in "Adding and Modifying Queries" on page 476).




The read-only **Query** field shows the name and text description of the query being scheduled.

The body of the screen contains a line for each of the existing schedule groups. In each, the **Group** field shows the name of the group and the **Description** field shows a text description.

If a group contains the query being scheduled, its **Group** field is preceded by an open-arrow (the "**>**" character).

To **add** the query to a schedule group, type **1** in the **Opt** field for that group and press **Enter**.

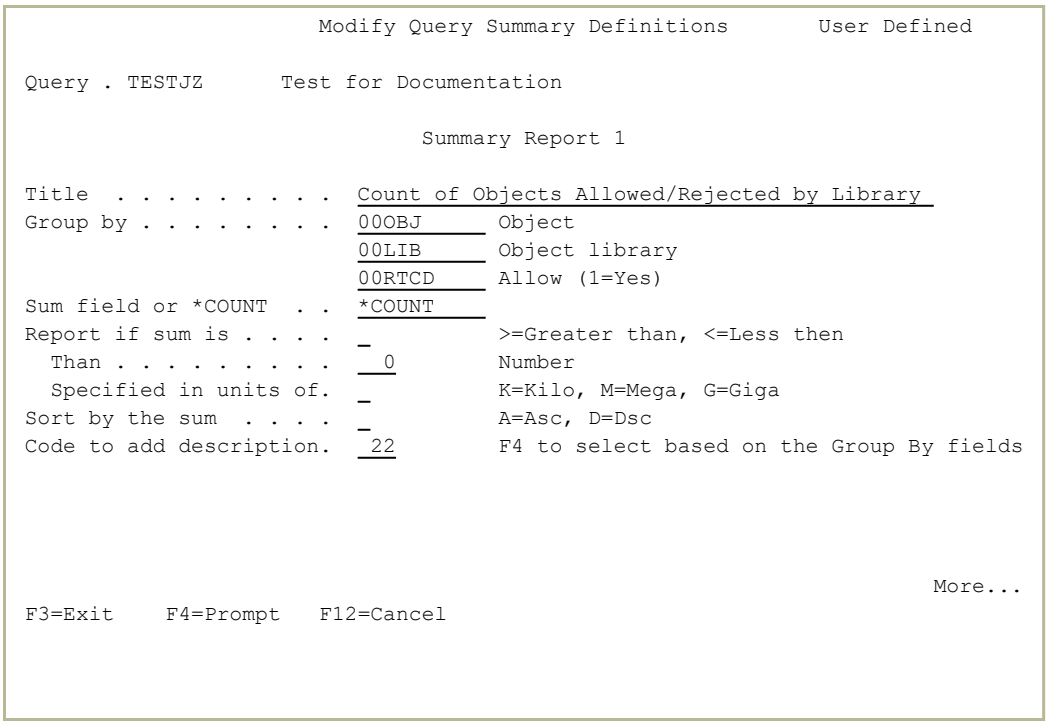
To **remove** the query from a schedule group, type **4** in the **Opt** field for that group and press **Enter**.

## Modifying Query Summary Definitions

With the **Modify Query Summary Definition** screen, you can group together data records to create and modify summaries that appear in query output.

To **create summary groups** for a query, type **G** in the **Opt** field for that query on the **Work with Queries** screen (*STRFW* **> 41 > 1**) as shown in "Creating and Running Queries" on page 473.

The screen also appears in the process of adding or modifying queries if the **Summaries** field on the **Exit Query Definition** screen is set to **Y** (as shown in "Adding and Modifying Queries" on page 476).



```
                      Modify Query Summary Definitions       User Defined

Query . TESTJZ      Test for Documentation

                                Summary Report 1

Title  . . . . . .  Count of Objects Allowed/Rejected by Library
Group by . . . . .  00OBJ       Object
                    00LIB       Object library
                    00RTCD      Allow (1=Yes)
Sum field or *COUNT  . .  *COUNT
Report if sum is . . . .  _         >=Greater than, <=Less then
  Than . . . . . .  __0       Number
  Specified in units of.  _         K=Kilo, M=Mega, G=Giga
Sort by the sum  . . . .  _         A=Asc, D=Dsc
Code to add description.  _22       F4 to select based on the Group By fields




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

The screen includes fields for creating up to three summaries. These appear on successive pages, which you can reach by pressing the **Page Down** key.

The fields for each are:

**Query**

A read-only field showing the name and text description of the query.

**Title**

A free-form text title for the summary.

**Group by**

How to group items in the output.

A group of three subfields set the fields by which items in the report are grouped. You can set this via the **Code to add description** field or by pressing the F4 key in each field to select the fields from a list.

**Sum field or *COUNT**

The field from the record for which the sum of values since the last summary is shown, or ***COUNT** to show the number of records.

**Report if the sum is**

Whether the summary appears if the sum is greater than the value in the **Than** field or when it is less. Possible values are:

- **>** : Greater than
- **<** : Less than

**Than**

The value to which the sum is compared.

**Specified in units of**

Units to which the values are rounded and displayed:

- **K**: Kilo
- **M**: Mega
- **G**: Giga

**Sort by the sum**

Possible values are:

- **A**: Ascending
- **D**: Descending

**Code to add description**

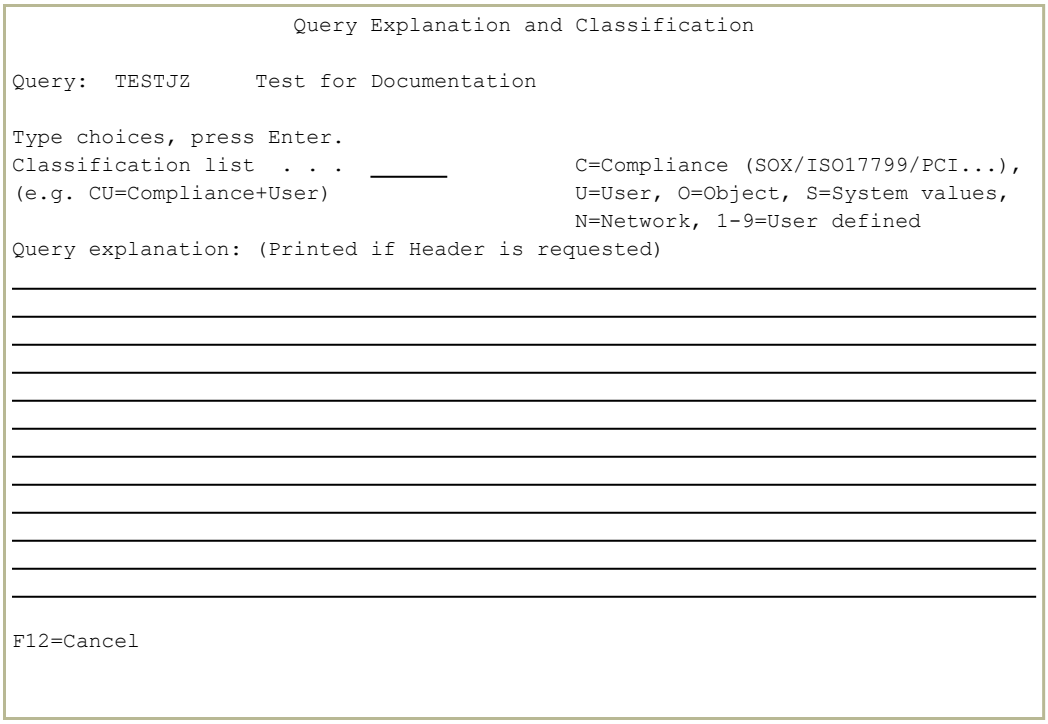
A code specifying groups of items to place in the three subfields of the **Group by** field. Press the F4 key to see a list of the field sets.

## Creating Query Classifications and Explanations

With the **Query Classification and Explanation** screen, you can create and modify classifications for your query as well as text explanations of the query that can be printed in the header of the output.

To **create classifications and an explanation for a query**, enter **9** in the **Opt** field for that query on the **Work with Queries** screen (*STRFW* **> 14 > 1**) as shown in "Creating and Running Queries" on page 473.

The screen also appears in the process of adding or modifying queries if the **Explanation** field on the **Exit Query Definition** screen is set to **Y** (as shown in "Adding and Modifying Queries" on page 476).




The body of the screen includes the following fields:

**Classification list**

Letters or digits for classifications of queries. These codes appear in the line for the query on the **Work with Queries** screen (*STRFW* **> 14 > 1**) as shown in "Creating and Running Queries" on page 473.

Predefined values include

- **C**: Compliance (SOX/ISO17799/PCI, etc)
- **U**: User
- **O**: Object
- **S**:System Values
- **N**: Network

You can freely define meanings for the digits **0** through **9**.

**Query explanation**

A free-form text explanation of the query. The text is printed in the header of the output if the **Add Header / Total** field is set to **1** or **2** on the Add Query or Modify Query screen as shown in "Adding and Modifying Queries" on page 476.

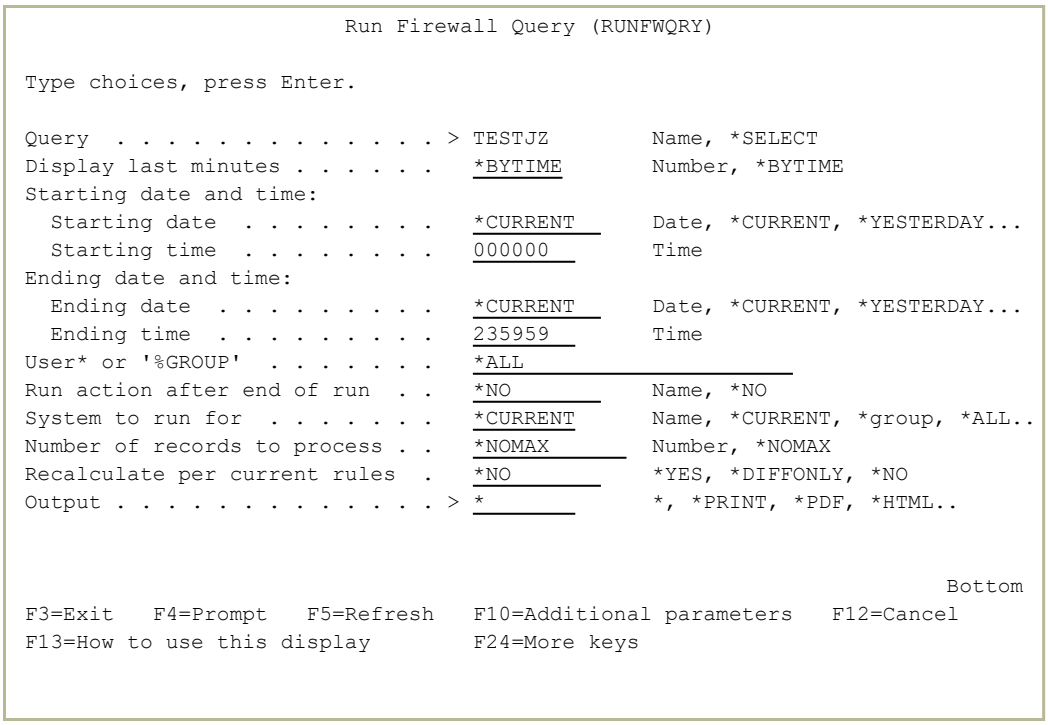
## Running Queries

You can run queries from several points within Firewall.

To **run queries directly**, select **2. Run a Query** from the **Reporting** menu (*STRFW* **> 41**).

You can also **run queries** by entering **5** in the **Opt** field for the query in the **Work with Queries** screen (*STRFW* **> 41 > 1**) as shown in "Creating and Running Queries" on page 473.

The **Run Firewall Query (RUNFWQRY)** screen appears:



```
                        Run Firewall Query (RUNFWQRY)

Type choices, press Enter.

Query  . . . . . . . . . . . . . > TESTJZ        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
Run action after end of run  . .   *NO          Name, *NO
System to run for  . . . . . . .   *CURRENT     Name, *CURRENT, *group, *ALL..
Number of records to process . .   *NOMAX       Number, *NOMAX
Recalculate per current rules  .   *NO          *YES, *DIFFONLY, *NO
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
```

The screen includes the following fields. Depending on how and from where within Firewallyou are running the query, some fields may already be filled in with read-only values.

**Query**

The name of the query to run. If you have not yet created the query, you can do so from the **Add Query** screen, as shown in "Adding and Modifying Queries" on page 476.

To choose the query after this screen, set this field to the value ***SELECT**.

### Display last minutes

To view activity in the immediate past, enter a number corresponding to the number of minutes that you would like to check. For example, to check activity in the past 120 minutes, enter **120** in this field. This value would override starting and ending date and time fields.

### Starting data and time

#### Starting date

The day or date on which the included data begins.

Allowed values include:

- ***CURRENT**: The current date
- ***YESTERDAY**: Yesterday's date
- ***WEEKSTR**: The first day of the current week. By default, this is Sunday.
- ***PRVWEEKS**: The first day of the previous week
- ***MONTHSTR**: The first day of the current month
- ***PRVMONTHS**: The first day of the previous month
- ***YEARSTR**: The first day of the current year
- ***PRVYEARS**: The first day of the previous year
- ***MON**: Monday
- ***TUE**: Tuesday
- ***WED**: Wednesday
- ***THU**: Thursday
- ***FRI**: Friday
- ***SAT**: Saturday
- ***SUN**: Sunday

#### Starting time

The time on the Starting date at which the included data begins, in **HHMMSS** format.

#### Ending date

The day or date on which the included data ends.

Allowed values are the same as for **Starting date**.

**Ending time**

The time on the Starting date at which the included data ends, in **HHMMSS** format.

**User* or '%GROUP'**

The name of a user, or the generic* name or %GROUP name of a group of users, whose data the query examines.

**Run action after end of run**

If the Query Type of the query is **$8**, the name of an action for the Action product to run after the query. For no action, enter ***NO**.

**System to run for**

Queries can run on information for this system or for others. Possible values include:

- ***CURRENT**: The current system.
- ***ALL**: All systems.
- **Name**: The name of a different system.
- ***group**: A named group of systems.

**Number of records to process**

The maximum number of records to process. To include all records, enter ***NOMAX**.

**Recalculate per current rules**

In running a query, you can either use the results of the Firewall rules that were in effect when the data was recorded, or see how the data would have been handled under current rules (as shown in "Running Firewall in FYI Simulation mode" on page 536). Possible values for this field include:

- ***NO**: Use the results from the rules that were in effect at the time of the events.
- ***YES**: Show how the events would have been handed under the current rules.
- ***DIFFONLY**: Show only the results that would be different if the current rules were in effect rather than those that were at the time.

**Output**

The destinations for output. Possible values include:

- *****: The default output. If running interactively, this is the current screen.
- ***PDF**: Print report to PDF outfile.
- ***HTML**: Print report to HTML outfile.
- ***CSV**: Print report to CSV outfile.
- ***OUTFILE**: Print report as text to an outfile.
- ***PRINT**: Print to default printer.
- ***PRINT[1-9]**: Print to another destination, as defined via the Printer Files Setup screen (*STRFW* **> 89 > 58**).

If you choose a destination that goes to an outfile, additional fields appear for further information.

## Scheduling Reports

With the **Report Scheduler**, you can run predefined report groups automatically, according to a fixed schedule.

Each **report group** contains one or more queries, reports, or history log inquiries that are executed together at a designated time. This is more efficient than running each report on its own, since you only need to define scheduling details and other run-time parameters once for the whole group.

To **create and run report groups** within Firewall, select **`51. Work with Report Scheduler`** from the **Reporting** menu (*STRFW* **`> 41`**), as shown in "Creating and Running Firewall Queries and Reports" on page 469.

The **Work with Report Scheduler** screen appears:

```
                          Work with Report Scheduler
                                      Position to  . . . . _______
                                      Subset by text . . . _________________
Type options, press Enter.
  1=Select   2=Add   3=Copy   4=Delete   5=Run group

Opt Group    Seq  Description                                      Query
 _  A             TEXT FOR A
 _              1  Run FireWall Query                               A
 _              2                                                  TEST
 _              3  TCPSGN-TCP Signon Server                        CPYCPSGN
 _              4                                                  AA_DBOPEN
 _              5  Run FireWall Query                               DSPFWLOG
 _  ABTEST        Test for Documentation
 _              2  Run FireWall Query                               RUNFWQRY
 _              3  Run FireWall Query                               DSPFWLOG
 _  ADOC2          Documentation run weekly on Tuesday
 _              1  Run FireWall Query AA_DBOPEN                     AA_DBOPEN
 _  ADOC3          Monthly run for Documentation
 _  DAILY          Daily
                                                                      More...
F3=Exit    F5=Refresh    F6=Add New Group   F8=Print     F12=Cancel
```

The body of the screen contains a list of report groups and the reports within them.

The groups are listed in alphabetical order. For each, the **`Group`** field contains the group name, and the **`Description`** field contains a free-form text description.

The reports within the group are listed after the group name. Three fields are shown for each report:

**Seq**

The order in which the reports run within the group. This corresponds to the order in which they were added.

**Description**

A free-form text description of the report.

**Query**

The query that the report runs, as defined in "Adding and Modifying Queries" on page 476.

To add a new report group, press the F6 key. The Add Report Group screen appears, as shown in "Adding or Modifying Report Groups" on page 498.

To add a report to a report group, type **2** in the Opt field for either the group or another report within it and press Enter. The Add Report Definition screen appears, as shown in "Adding Reports to Report Groups" on page 502.

To modify a report group, type **1** in the **Opt** field for the group or a report within it and press Enter. The Modify Report Groups screen appears, as shown in "Adding or Modifying Report Groups" on page 498.

To copy a report group, type **3** in the **Opt** field for the group or a report within it and press Enter. The Copy Report Groups screen appears. The read-only **From Report group** field shows the name and description of the original group. Enter the name of the new group in the **To Report group** field.

To delete a report group, type **4** in the **Opt** field for the report group and press Enter. The Delete Report Group window opens. Press Enter to confirm the deletion or the F12 key to cancel it.

To delete a report from a group, type **4** in the **Opt** field for the report and press Enter. The Delete Report Group window opens. Press Enter to confirm the deletion or the F12 key to cancel it.

To **run a report group on demand**, type **5** in the **Opt** field for the report group and press **Enter**. The **Run Report Group (RUNRPTGRP)** screen appears, as shown in "Running Report Groups On Demand" on page 512.

## Adding or Modifying Report Groups

To **add a report group** to the Report Scheduler, press the **F6** key in the **Work with Report Scheduler** screen (*STRFW* **> 41 > 51**) as shown in "Scheduling Reports" on page 495.

To **modify an existing report group**, enter **1** in the **Opt** field for the report group or a report in it in the **Work with Report Scheduler** screen.

The **Add Report Group** or **Modify Report Group** screen appears. They differ only in their title and an additional read-only field on the **Modify Report Group** screen:

```
                              Add Report Group

Report groups are intended to run pre-defined sets of reports automatically
on a periodic basis.
If ZIP(*YES) is specified, all PDF, HTML, CSV will be sent together.
Other individual reports parameters, if defined, override group parameters.
The use of descriptive date values *YESTERDAY, *WEEKSTR... is recommended.

Type choices, press Enter.
  Report Group name . . .  _______       Name  e.g. DAILY, WEEKLY, MONTHLY etc.
  Description . . . . . .  ____________________________________________________




Press Enter to continue to the Define Parameters screen.

F3=Exit                                 F12=Cancel
```

The screen includes the following fields:

**Report Group name**

The name of the group. It may have up to seven alphanumeric characters, beginning with a letter.

**Description**

A free-form text description of the report group.

### Group parameters

On the **Modify Report Group** screen, a read-only field showing the parameters that have already been entered for the group.

After entering this information, press **Enter** twice to confirm it.

The **Define FW Report Group Details (DFNFWGRPD)** screen appears:

```
                  Define FW Report Group Details (DFNFWGRPD)

Type choices, press Enter.

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
System to run for  . . . . .   *CURRENT     Name, *CURRENT, *group, *ALL..
Output . . . . . . . . . . .   *PDF         *, *PRINT, *PDF, *HTML..









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

The screen contains the following fields:

### Starting data and time

#### Starting date

The day or date on which the included data begins.

Allowed values include:

- ***CURRENT**: The current date
- ***YESTERDAY**: Yesterday's date
- ***WEEKSTR**: The first day of the current week. By default, this is Sunday.
- ***PRVWEEKS**: The first day of the previous week
- ***MONTHSTR**: The first day of the current month
- ***PRVMONTHS**: The first day of the previous month
- ***YEARSTR**: The first day of the current year

- ***PRVYEARS**: The first day of the previous year
- ***MON**: Monday
- ***TUE**: Tuesday
- ***WED**: Wednesday
- ***THU**: Thursday
- ***FRI**: Friday
- ***SAT**: Saturday
- ***SUN**: Sunday

**Starting time**

The time on the Starting date at which the included data begins, in **HHMMSS** format.

**Ending date**

The day or date on which the included data ends.

Allowed values are the same as for **Starting date**.

**Ending time**

The time on the Starting date at which the included data ends, in **HHMMSS** format.

**System to run for**

Queries can run on information for this system or for others. Possible values include:

- ***CURRENT**: The current system.
- ***ALL**: All systems.
- **Name**: The name of a different system.
- ***group**: A named group of systems.

**Output**

The destinations for output. Possible values include:

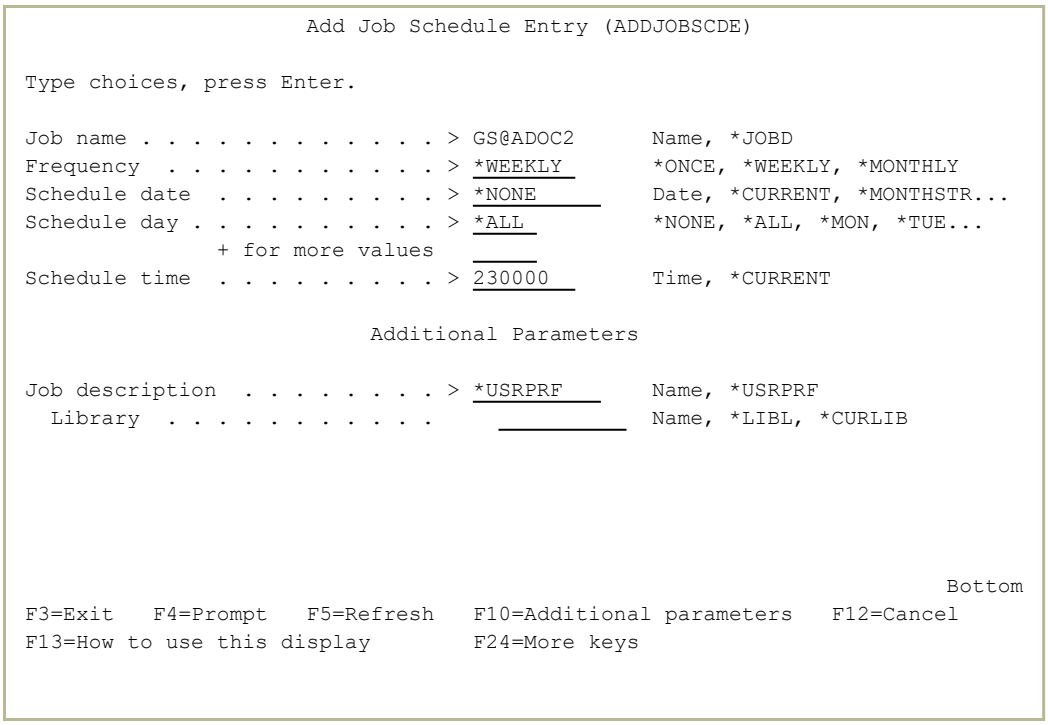
- *****: The default output. If running interactively, this is the current screen.
- ***PDF**: Print report to PDF outfile.
- ***HTML**: Print report to HTML outfile.
- ***CSV**: Print report to CSV outfile.
- ***OUTFILE**: Print report as text to an outfile.
- ***PRINT**: Print to default printer.

- **`*PRINT[1-9]`**: Print to another destination, as defined via the **Printer Files Setup** screen (***STRFW > 89 > 58***).

If you choose a destination that goes to an outfile, additional fields appear for further information.

After entering this information, press **Enter**.

The **Add Job Schedule Entry (ADDJOBSCDE)** screen appears, as shown in IBM documentation at https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_72/cl/addjobscde.htm:




After entering values, press **Enter** to return to the **Work with Report Scheduler** screen.

## Adding Reports to Report Groups

To **add a report to a report group**, enter **2** in the **Opt** field for either the group or another report within it on the **Work with Report Scheduler** screen (*STRFW* **> 41 > 51**) as shown in "Scheduling Reports" on page 495. The **Add Report Definition** screen appears:

```
                          Add Report Definition

Reports in a group run periodically, as per the group definition.
If ZIP(*YES) is specified for the Group, the mail info is taken from the Group.
Other parameters defined for the report, override group parameters.

Group ABTEST     Test for Documentation

Type choices, press Enter.

Report Id.  . . . . . .     4
Description . . . . . .  Run FireWall Query
Reporting command (F7).  RUNFWQRY       Command, F7 or *SELECT to select
                         Run FireWall Query
Report parameters (F4).









F3=Exit    F4=Set Parameters    F7=Select Command               F12=Cancel
```

The screen contains the following fields:

**Group**

A read-only field showing the name and text description of the report group, as set on the **Define FW Report Group Details (DFNFWGRPD)** screen, as seen in "Adding or Modifying Report Groups" on page 498.

**Report ID**

A read-only field showing the numeric report identifier.

**Description**

A free-form text description of the report, as relevant to the report group.

**Reporting command**

The command that runs the report. By default, this is RUNFWQRY. To select other commands, press the F7 key.

**Report parameters**

A read-only field showing the parameters for the Reporting command. To set or change these, press the F4 key. The Run Firewall Query (RUNFWQRY) screen appears, as shown in "Running Queries" on page 491.

## Defining Time Groups

Many of the Firewall rules and reporting features take advantage of the unique **Time Group** feature. With time groups, users can 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 different queries and reports to audit the activities of one group 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 (for activities occurring during the time group periods) for each query or report that covers 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.

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 the application of a rule to specific times and days of the week.

Time group filters can be either:

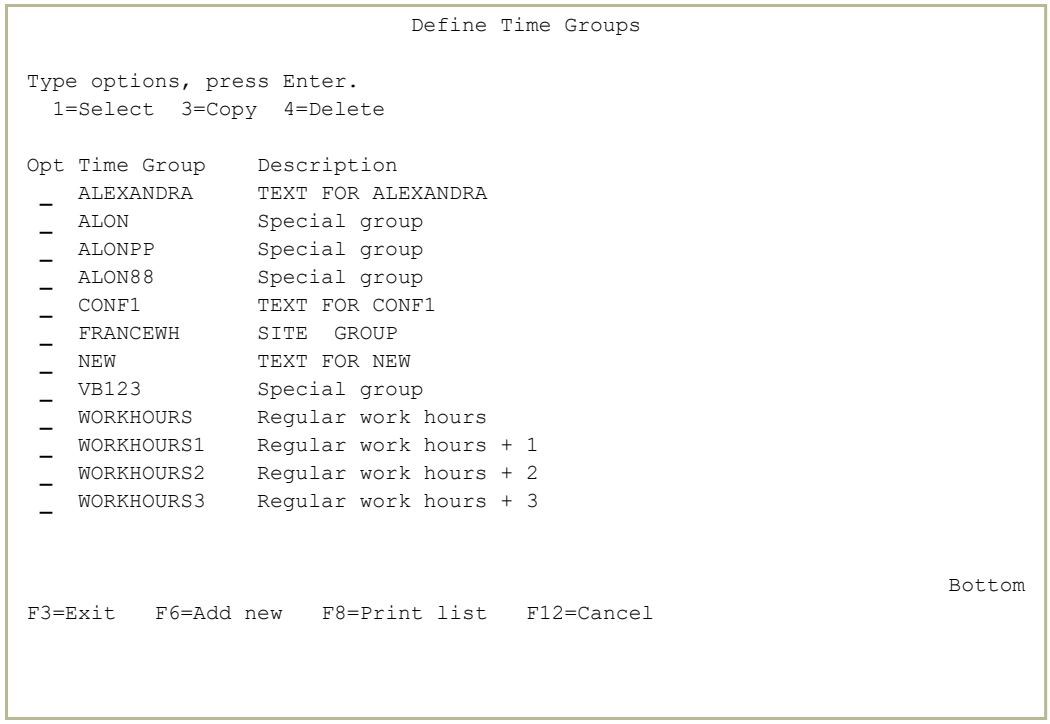
- **Inclusive** - Including all activities occurring during the time group periods
- **Exclusive** - Including all activities not occurring during the time group periods

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.

To **create and modify time groups,** select **31. Time Groups** from the **Reporting**screen, as shown in "Creating and Running Firewall Queries and Reports" on page 469.

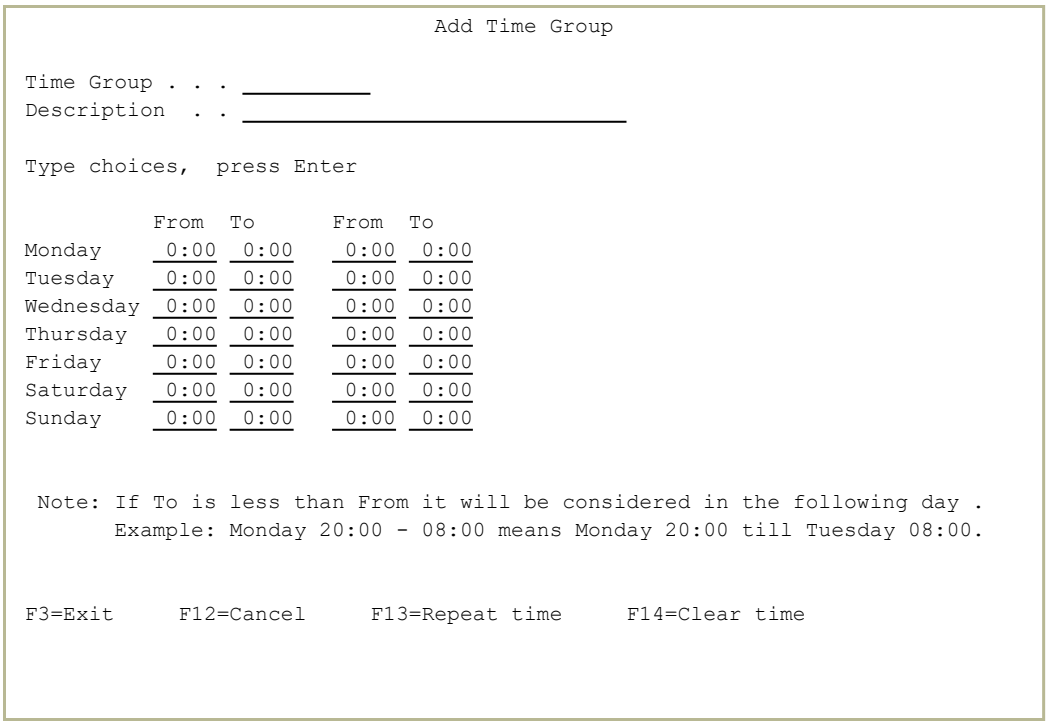
The **Define Time Groups** screen appears:



```
                              Define Time Groups

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

Opt Time Group    Description
 _  ALEXANDRA     TEXT FOR ALEXANDRA
 _  ALON          Special group
 _  ALONPP        Special group
 _  ALON88        Special group
 _  CONF1         TEXT FOR CONF1
 _  FRANCEWH      SITE  GROUP
 _  NEW           TEXT FOR NEW
 _  VB123         Special group
 _  WORKHOURS     Regular work hours
 _  WORKHOURS1    Regular work hours + 1
 _  WORKHOURS2    Regular work hours + 2
 _  WORKHOURS3    Regular work hours + 3


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

Each line in the body of the screen refers to a single time group. After the standard **Opt** field, it shows a unique name for the **Time Group** and a free-form text **Description**.

To **create** a new time group, press the **F6** key. The **Add Time Group** screen appears:




Enter a unique name for the time group in the **Time Group** field and a free-form description in the **Description** field.

The body of the screen has named lines for each day of the week.

Each line has two pairs of fields, with one named **From** and the other named **To**. Each pair specifies a time period during the day. For example, if workers had a shift from 8 AM to 5 PM, with a lunch break from noon to 1 PM, the line for each weekday would show times from **8:00** to **12:00** and from **13:00** to **17:00**.

If the value of the **To** field is less than that of the **From** field, it signifies that the shift continues into the next calendar day. For example, an overnight shift **From23:00To7:00** would run from 11 PM on that day through 7 AM on the next.

To repeat the entered times from the line containing the cursor to those for all other days, press the F13 (Shift+F1) key.

To clear the times from all the lines except for the one containing the cursor, press the F14 (Shift+F2) key.

## Further Operations from the Define Time Groups Screen

To **modify** the times for an existing time group, enter **1** in the **Opt** field for that group. The **Change Time Group** screen appears, with the same set of fields as the **Add Time Group** screen.

To **copy** the settings from one time group to another, enter **3** in the **Opt** field for that group. The **Copy / Replace Time-Group** screen appears. The Time Group for the existing group appears in read-only **From:** fields. Enter the name of the new group in the **To: Time Group** field. If the group already exists, its settings are overwritten.

To **delete** a time group, enter **4** in the **Opt** field for that group. The **Delete Time Group** screen appears. Press **Enter** to confirm the deletion or the **F12** key to cancel it.

## Defining Groups of Items

You can define groups of reports that you can schedule to run together. You can also define classes of groups, so that you can schedule all the groups of reports in the class to run together.

You can also use classes of other types of groups within queries to limit the items on which the query would run. For example, you could create a class **OVERNIGHT** of all Time Groups that work overnight shifts. You could then define a query that only select those users by including a filter with the comparison **ITEM OVERNIGHT** (as shown in "Setting the Order of Rules" on page 462).

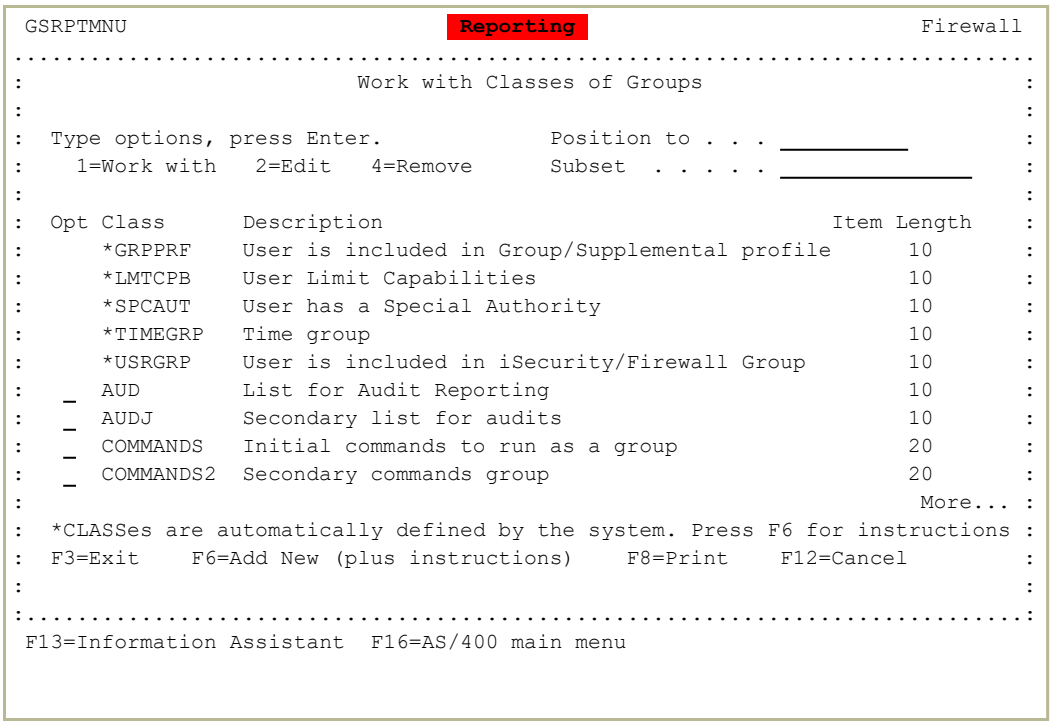
You could also create a class **HQIP** of all IP address groups at an organization's headquarters, then create a query that would exclude them by creating a filter with the comparison **NITEM HQIP**.

To create and modify report groups, select **51. Work with Report Scheduler** from the Reporting menu (*STRFW* **> 41**). The Work with Report Scheduler screen appears, as shown in "Scheduling Reports" on page 495.

To add reports to a group, enter **2** in the **Opt** field for either the group or another report within it in the Work with Report Scheduler screen (*STRFW* **> 41 > 51**). The Add Report Definition screen appears, as shown in "Adding Reports to Report Groups" on page 502.

To create and modify classes and add groups to them, select **35. Group Items for Selection** from the Reporting menu (*STRFW* **> 41**).

The Work with Classes of Groups window appears.




Each line on the body of the screen refers to a single class. For each class, it shows the these fields:

**Class**

A unique name for the class.

**Description**

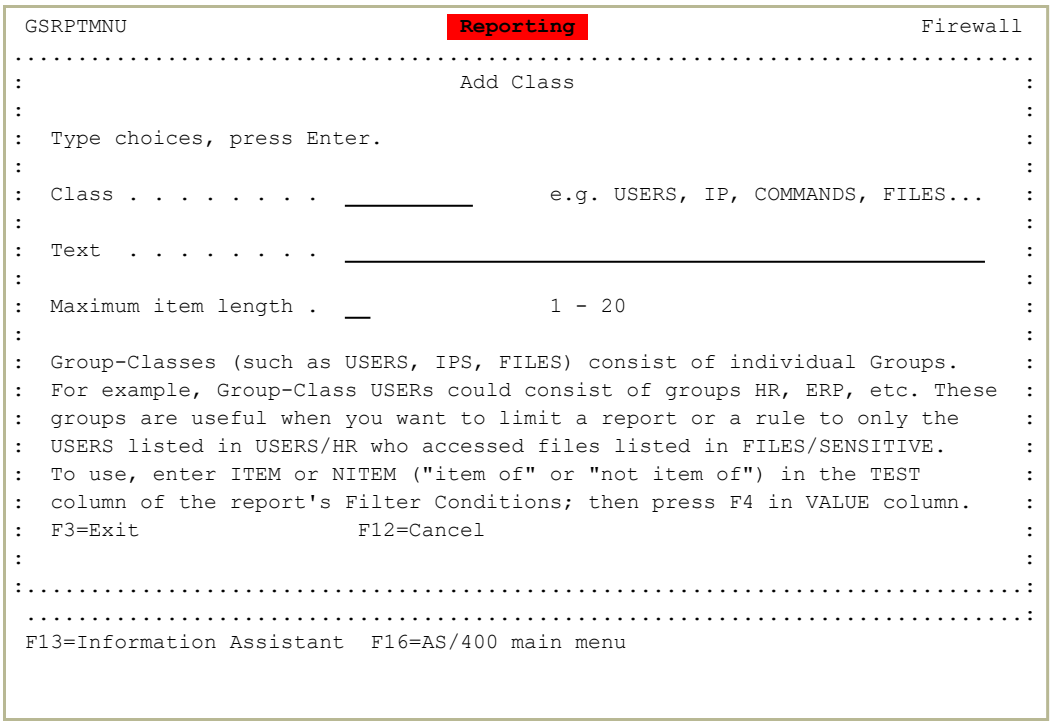
A free-form text description of the class.

**Item Length**

The maximum length of item names in the class, from 0 through 20.

The predefined classes at the start of the list, with names that begin with an asterisk (*****), cannot be altered. The lines for the other classes begin with the standard **Opt** field.

To **add a new class**, press the **F6** key. The **Add Class** window appears:




The window has the same fields as the **Work with Classes of Groups** window. Fill in the values for the new class, then press **Enter**.

The **Work with Groups of** window appears. To add groups, press the **F6** key.

The **Add Group** window appears. Enter the name of the first group and a free-form text description, then press **Enter**.

The **Work with Group Items** window appears. For each item in the group, enter the item name and a free-form text description. After entering items, press **Enter**.The **Work with Groups of** window reappears.

To **modify the list of items within the group**, enter **1** in the **Opt** field for the group.

To **edit the description of a group**, enter **2** in the **Opt** field for the group.

To **remove an item from the group**, enter **4** in the **Opt** field for the group.

## More Operations from the Work with Classes of Groups screen

To **modify the list of groups within the class**, enter **1** in the **Opt** field for the class.

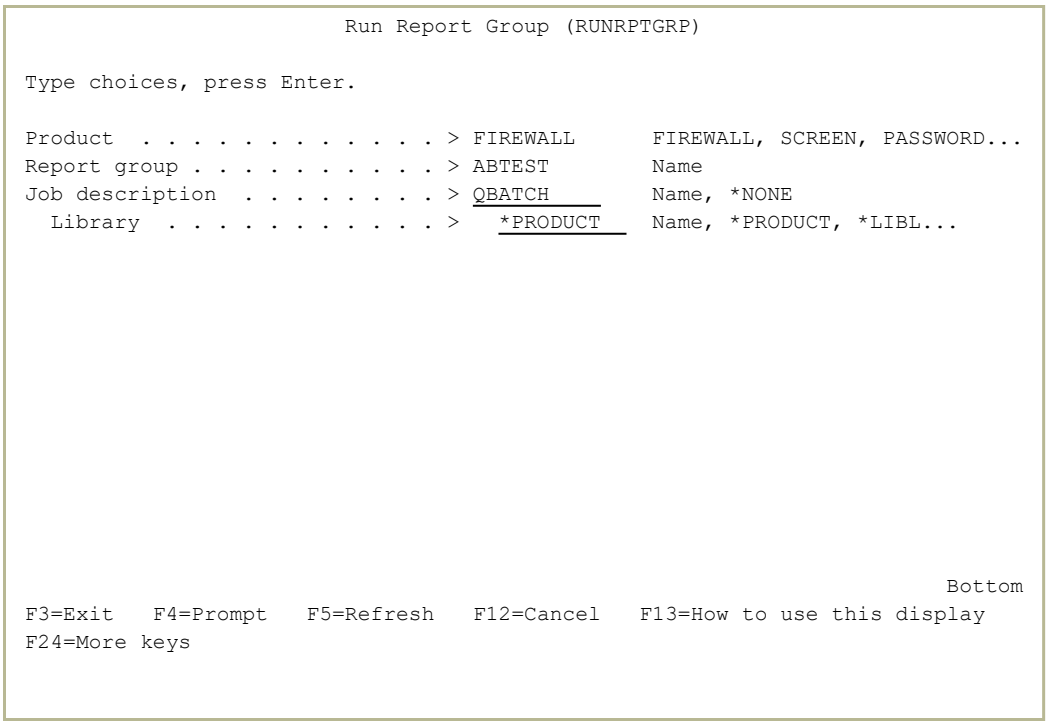
To **edit the description or item length of a class**, enter **2** in the **Opt** field for the class.

To **remove a group from the class**, enter **4** in the **Opt** field for the class.

## Running Report Groups On Demand

To **run report groups on demand**, select **52. Run a Report Group** from the **Reporting** menu (*STRFW* **> 41**), as shown in "Creating and Running Firewall Queries and Reports" on page 469

To **run a report group on demand** from within the Report Scheduler (as shown in "Scheduling Reports" on page 495), type **5** in the **Opt** field for the report group and press **Enter**.




If you have selected the screen from within the **Reporting** menu, enter the name of the report group (as set within the Report Scheduler) in the **Report group** field.

If you have selected the screen from within the Report Scheduler, the name of the product that you are running and the name of the report group appear as read-only values in the **Product** and **Report group** fields.

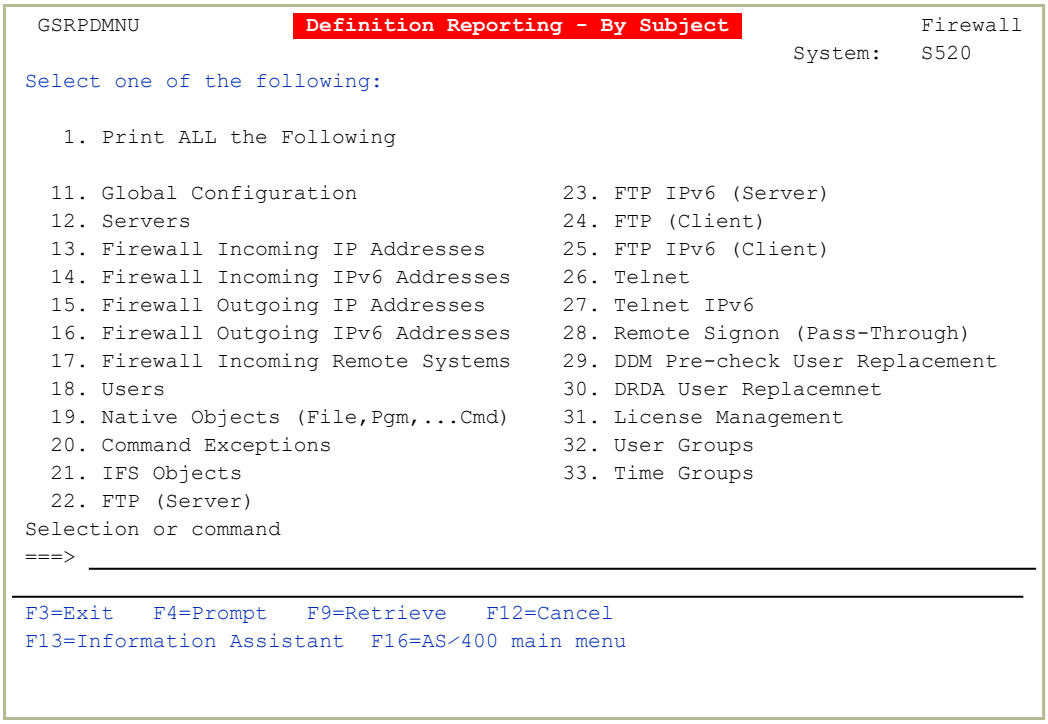
The **Job description** field contains the name of the program to run. To run the report group interactively, enter ***NONE**.

The **Library** field contains the name of the library containing the program. This can be a library name or ***PRODUCT**, ***LIBL**, or ***CURLIB**.

## Running Predefined Reports

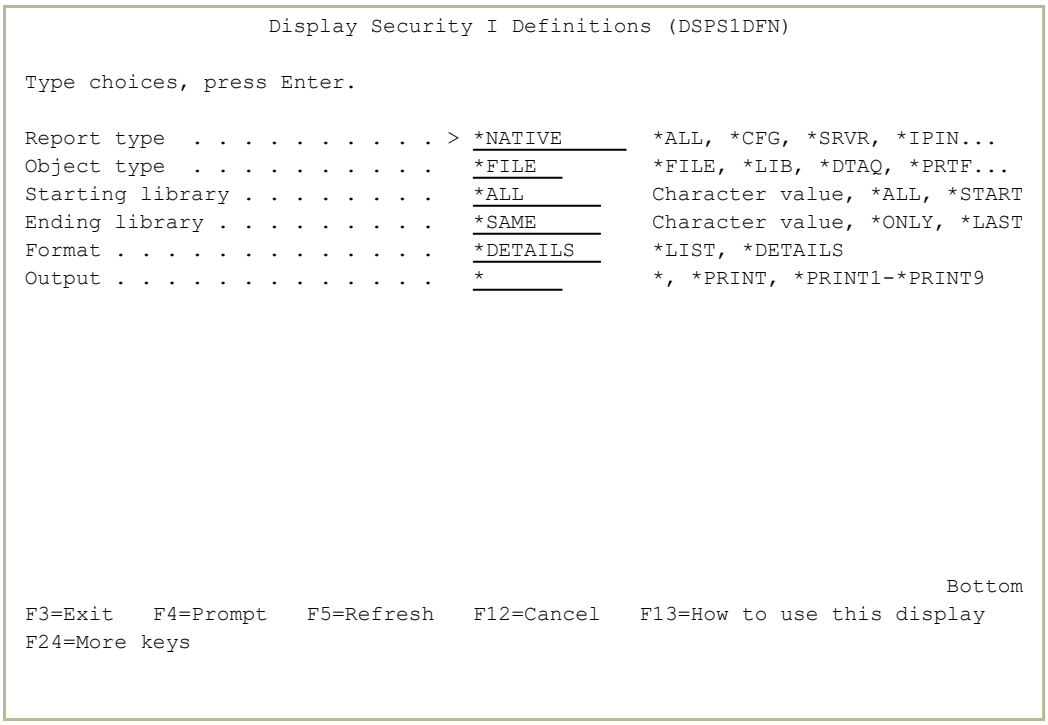
To **run predefined reports** on servers and other objects on your system, select **65. Product Settings** from the **Reporting** menu (*STRFW* **> 41**) as shown in "Creating and Running Firewall Queries and Reports" on page 469.

The **Definition Reporting - By Subject** screen appears.




The menu leads to customized versions of the **Display Security I Definitions (DSPS1DFN)** screen.

For example, if you select **19. Native Objects (File,Pgm,...Cmd)**, the following version of the screen appears:




The screen contains the following fields:

**Report type**

The type of report to run. To see a list of valid values, press the **F4** key. For this Native Objects report, the value is set to ***NATIVE**.

**Object type**

The type of object that the report examines. To see a list of valid values, press the **F4** key.

**Starting library**

If the report includes a range of libraries, the first library in the range. This can be the name of a library, *ALL to include all libraries, or *START to begin with the first library in the system.

**Ending library**

If the report includes a range of libraries, the last library in the range. This can be the name of a library, *ONLY to only include the single library named in the **Starting library** field, or *LAST to end with the last library in the system.

**Format**

The format of the report. The output can contain extended ***DETAILS** or a simpler ***LIST**.

**Output**

The destination for the output. Possible values include:

- *****: The screen
- ***PRINT**: A default printer.
- ***PRINT1 - *PRINT9**: A different printer, defined within iSecurity Base Configuration

The screens for other reports are substantially the same, with small differences relevant to the different server types.

# Displaying Firewall Logs

To **display Firewall logs**, select **`11. Display Log`** from the **Reporting** menu (***STRFW*** **`> 41`**) as shown in "Creating and Running Firewall Queries and Reports" on page 469.

The **Display Firewall Log (DSPFWLOG)** screen appears:

```
                      Display Firewall Log (DSPFWLOG)

Type choices, press Enter.

Display last n minutes . . . . .   *BYTIME       Number, *BYTIME
Starting date and time:
  Starting date  . . . . . . . .   *CURRENT     Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . . . .   000000        Time
Ending date and time:
  Ending date  . . . . . . . . .   *CURRENT     Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . . . . .   235959        Time
User*,<GrpPrf,'%GRP','%<GRP' . .   *ALL
Object . . . . . . . . . . . . .   *ALL         Name, generic*, *ALL
  Library  . . . . . . . . . . .     *ALL       Name, generic*, *ALL, *SYS...
Object Type  . . . . . . . . . .   *ALL         *ALL, *FILE, *LIB, *DTAQ...
IPv4 (generic*) or IPv6  . . . .   *ALL
_____
Prefix length for IPv6 . . . . .   *ALL         1-128, *ALL
Type . . . . . . . . . . . . . .   *ALL         *SELECT, *NATIVE, *IFS...
Allowed  . . . . . . . . . . . .   *ALL         *YES, *NO, *ALL
                                                                    More...
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

NOTE: This screen also appears in other areas of Firewall. In most of them, one or more fields are filled in with values relevant to the option that called the screen. Some omit fields that are not relevant.

The screen includes the following fields:

**`Display last minutes`**

To view activity in the immediate past, enter a number corresponding to the number of minutes that you would like to check. For example, to check activity in the past 120 minutes, enter **`120`** in this field. This value would override starting and ending date and time fields.

**Starting data and time**

**Starting date**

The day or date on which the included data begins.

Allowed values include:

- ***CURRENT**: The current date
- ***YESTERDAY**: Yesterday's date
- ***WEEKSTR**: The first day of the current week. By default, this is Sunday.
- ***PRVWEEKS**: The first day of the previous week
- ***MONTHSTR**: The first day of the current month
- ***PRVMONTHS**: The first day of the previous month
- ***YEARSTR**: The first day of the current year
- ***PRVYEARS**: The first day of the previous year
- ***MON**: Monday
- ***TUE**: Tuesday
- ***WED**: Wednesday
- ***THU**: Thursday
- ***FRI**: Friday
- ***SAT**: Saturday
- ***SUN**: Sunday

**Starting time**

The time on the Starting date at which the included data begins, in **HHMMSS** format.

**Ending date**

The day or date on which the included data ends.

Allowed values are the same as for **Starting date**.

**Ending time**

The time on the Starting date at which the included data ends, in **HHMMSS** format.

**User*,<GrpPrf,'%GRP','%<GRP'**

The user or group requesting the activity. The values can have several forms:

- **User***: A user name or generic* name
- **<GrpPrf**: A group profile, preceded by the '**<**' character
- **'%GRP'**: A group name, preceded by the '**%**' character and surrounded by single quotation marks
- **'%<GRP'**: A group, including the group profile and its users, preceded by the string '**<%**' and surrounded by single quotation marks
- ***ALL**: All users

**Object**

The object on which the activity requests to operate. This can be the name of the specific object, a generic name ending in an asterisk ("*****"), or ***ALL** for all objects.

**Library**

The library containing the object on which the activity requests to operate. This can be the name of the specific library, a generic name ending in an asterisk ("*****"), or ***ALL** for all libraries.

**Object Type**

The type of object on which the activity requests to operate. Possible values include:

- ***ALL**: All objects
- ***FILE**: Files
- ***LIB**: Libraries
- ***DTAQ**: Data queues
- ***PRTF**: Printer files
- ***PGM**: Programs
- ***CMD**: Commands

**IPv4 (generic*) or IPv6**

An IPv4 or IPv6 address on ehich activity requests to operate.

**Prefix length for IPv6**

If the request is filtered by IPv6 address, the prefix length for the addresses. This can be an integer from 1-128 or *ALL to include all values.

**Type**

The type of object on which the activity requests to operate. To see a set of possible values, press the **F4** key.

**Allowed**

Specifies whether the data set includes rejected activity, accepted activity, or both.

- ***YES**: Include only accepted activity
- ***NO:** Include only rejected activity
- ***ALL:** Include both accepted and rejected activity

**Mode of Operation**

Whether to look for information from specific operation modes or for all modes. Possible values are:

- ***FYI**: Firewall ran under FYI Simulation Mode as shown in "Running Firewall in FYI Simulation mode" on page 536.
- ***REAL**: Running actively, not in FYI Simulation Mode.
- ***ALL**: Running in either mode.

**Job name**

Specific or generic* job names that produced the records

**User**

Specific or generic* names of users whose jobs produced the records.

**Number**

The job number.

**Number of records to process**

Collect no more than this number of records. If set to ***NOMAX**, collect all the relevant records.

**Recalculate and Display**

You can recalculate the logs based on the current Firewall settings rather than what was in effect at the time. Possible values are:

- ***YES**: Recalculate the transactions showing whether they would be accepted or rejected under the current rules.

- ***DIFFONLY**: Recalculate the transactions, but only display the results that would be different.
- ***SAMEONLY**: Recalculate the transactions, but only display the results that would remain the same.
- ***NO**: Display the original results.

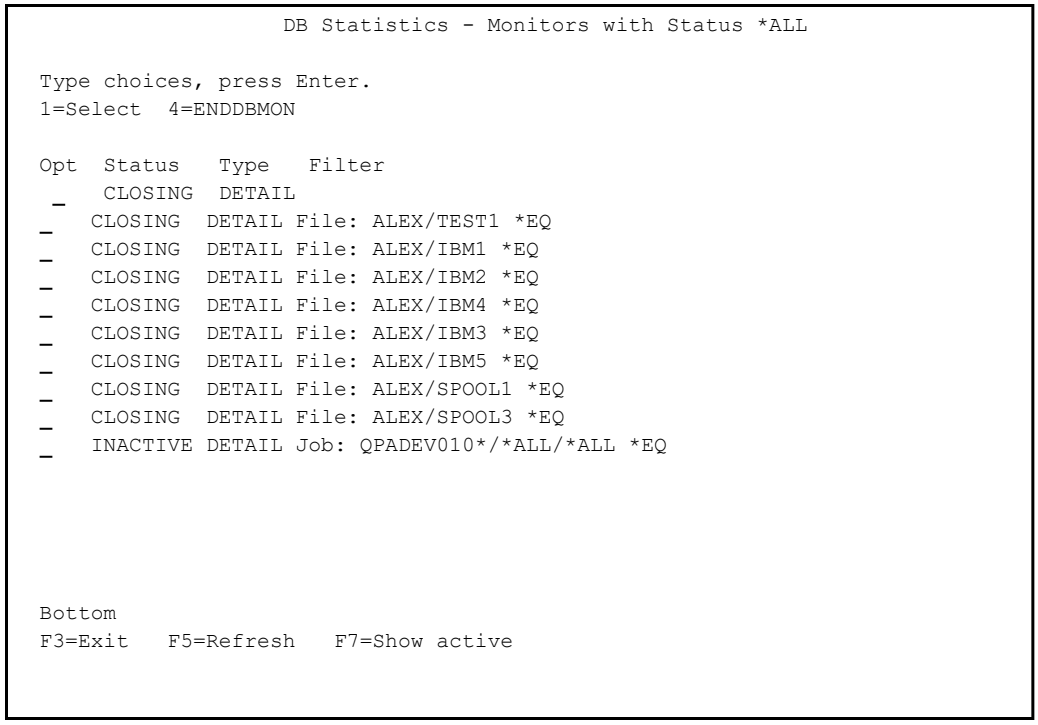
**Output**

The destination for the output. Possible values are:

- *****: The current screen
- ***PRINT**: The default printer
- ***PRINT1** through ***PRINT9**: A printer defined within iSecurity Base Configuration. For details see the original source file **SMZ8/GRSOURCE GSSPCPRT**.
- ***OUTFILE**: An outfile on the system.

## Viewing Database Statistics

To **view and manage database statistics**, select **`58. Work with DB Statistics Monitors`** from the **Activation and Server Settings** screen (***STRFW > 1***). The **DB Statistics - Monitors with Status** screen appears.



```
                  DB Statistics - Monitors with Status *ALL

Type choices, press Enter.
1=Select  4=ENDDBMON

Opt  Status   Type   Filter
 _    CLOSING  DETAIL
_    CLOSING  DETAIL File: ALEX/TEST1 *EQ
_    CLOSING  DETAIL File: ALEX/IBM1 *EQ
_    CLOSING  DETAIL File: ALEX/IBM2 *EQ
_    CLOSING  DETAIL File: ALEX/IBM4 *EQ
_    CLOSING  DETAIL File: ALEX/IBM3 *EQ
_    CLOSING  DETAIL File: ALEX/IBM5 *EQ
_    CLOSING  DETAIL File: ALEX/SPOOL1 *EQ
_    CLOSING  DETAIL File: ALEX/SPOOL3 *EQ
_    INACTIVE DETAIL Job: QPADEV010*/*ALL/*ALL *EQ




Bottom
F3=Exit   F5=Refresh   F7=Show active
```

The screen can either show database monitors that are currently active or all of them. Press the **F7** key to toggle between them.

For each monitor, the body of the screen shows these fields:

**`Status`**

?

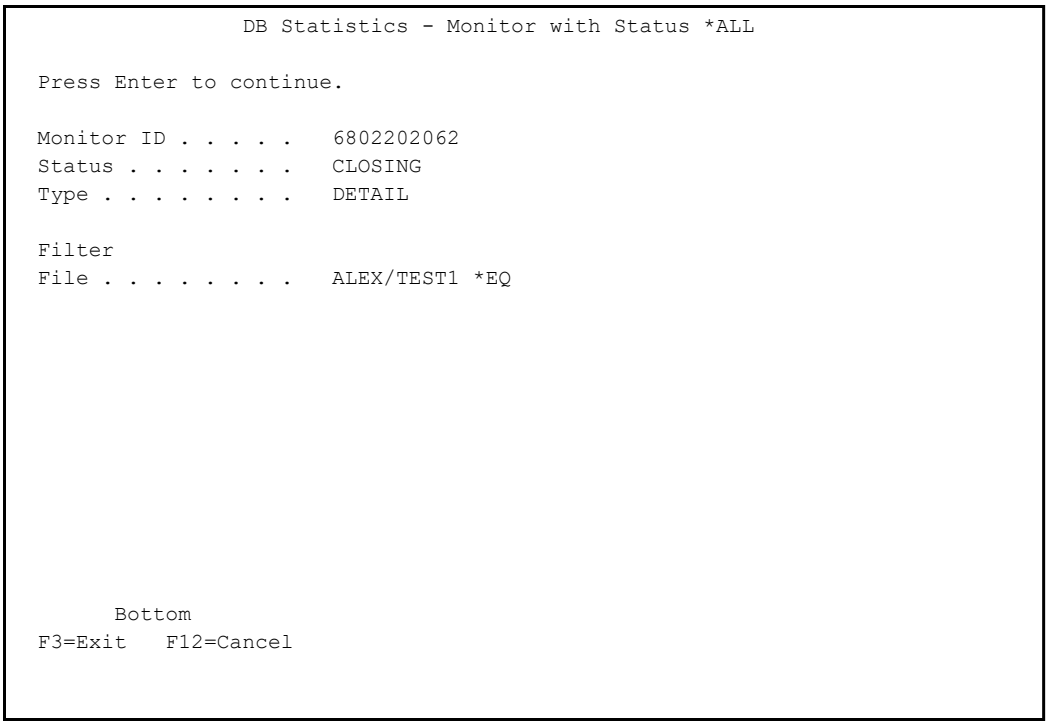
**`Type`**

?

**`Filter`**

?

To **see further information** about a [[???}}, enter 1 on the Opt field for that line. A detail screen appears. In addition to the information on the previous screen, it shows a Monitor ID.

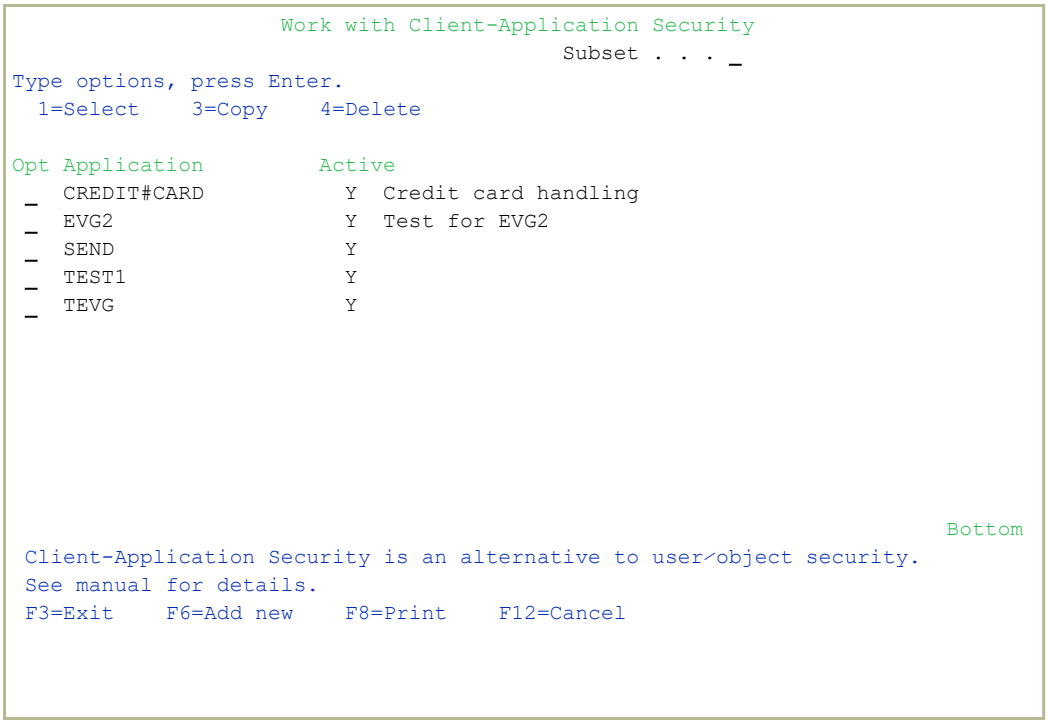

DB Statistics - Monitor with Status *ALL
Press Enter to continue.
Monitor ID . . . . . 6802202062
Status . . . . . CLOSING
Type . . . . . DETAIL
Filter
File . . . . . ALEX/TEST1 *EQ
Bottom
F3=Exit F12=Cancel

## Securing PC Client Applications

Firewall can set security controls for specific PC applications that access your IBM i. When you connect an application for the first time, you are asked for an application name and a key which will identify the application in later connections.

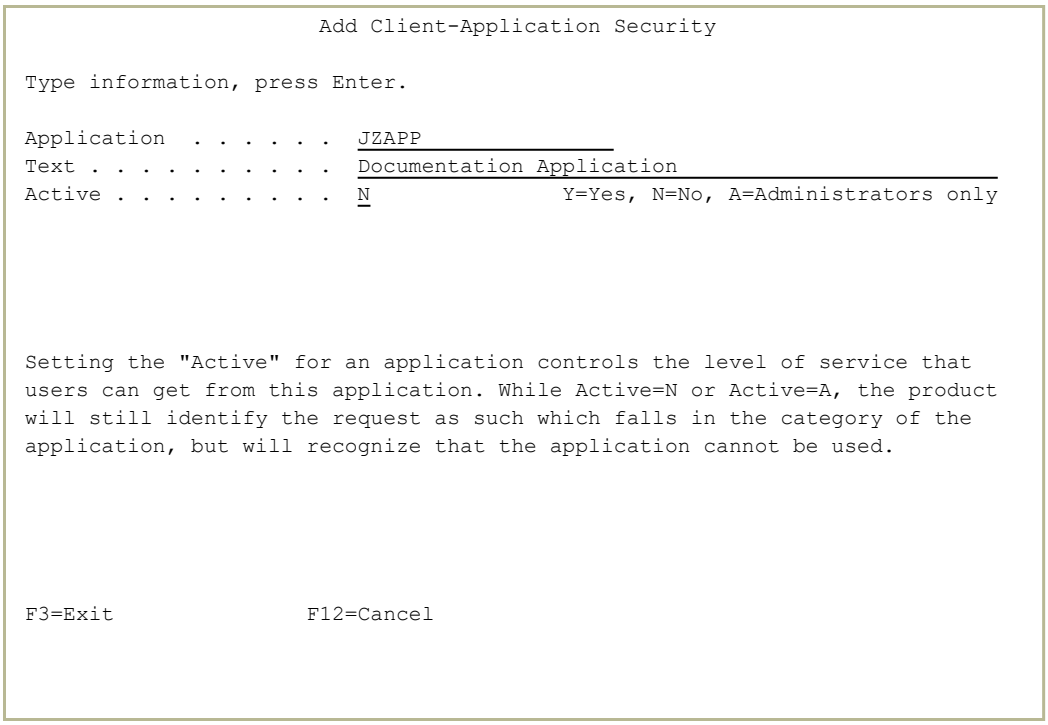
To create **security settings for PC applications** that access your IBM i, select **`18. PC Application Security`** from the Firewall Main Menu.

The **Work with Client-Application Security** screen appears.




The screen shows, for each application, a short name, a free-form text description, and whether Firewall protection for it is active.

To **add security settings for an application**, press the **F6** key. The **Add Client-Application Security** screen appears:




Enter information in the following fields:

**Application**

A unique name for the application.

**Text**

A free-form text description of the application.

**Active**

Who can run the application. Options are:

- **Y=Yes**: Anyone can run the application.
- **N=No**: No one can run the application.
- **A=Administrators only**: Only administrators can run the application.

After entering this information, press **Enter**. A second **Add Client-Application Security** screen appears:

```
                      Add Client-Application Security

Type information, press Enter.
Application  . . . . . .  JZAPP
Text . . . . . .  Documentation Application
Active . . . . . .  N               Y=Yes, N=No, A=Administrators only

                        Servers   Cmd/
General features         SQL      Pgm
Activate . . . . . .  Y        Y      Y=Yes, N=No
Specify which servers will used for the application. Note that Cmd/Pgm (Remote
command, Remote program call) will identify users only when the application
is identified by key.

Authorize App by "user".  *NOCHK      Name, *APP, *USER, *NOCHK
Specify a name which it's authority will be checked to verify the requests
made by the client-application.

Check dynamic IP filter.  N           Y=Yes, N=No
Verify that users are working from their allowed range of IPs.


F3=Exit   F12=Cancel
```

This screen adds three fields of **General features** for the program:

**Activate**

Specifies the servers used for the application. It has two sub-fields:

**Servers SQL**

Use SQL servers

**Cmd/Pgm**

A remote command or remote program call. Users are only identified if the program supplies a key.

**Authorize App by "user"**

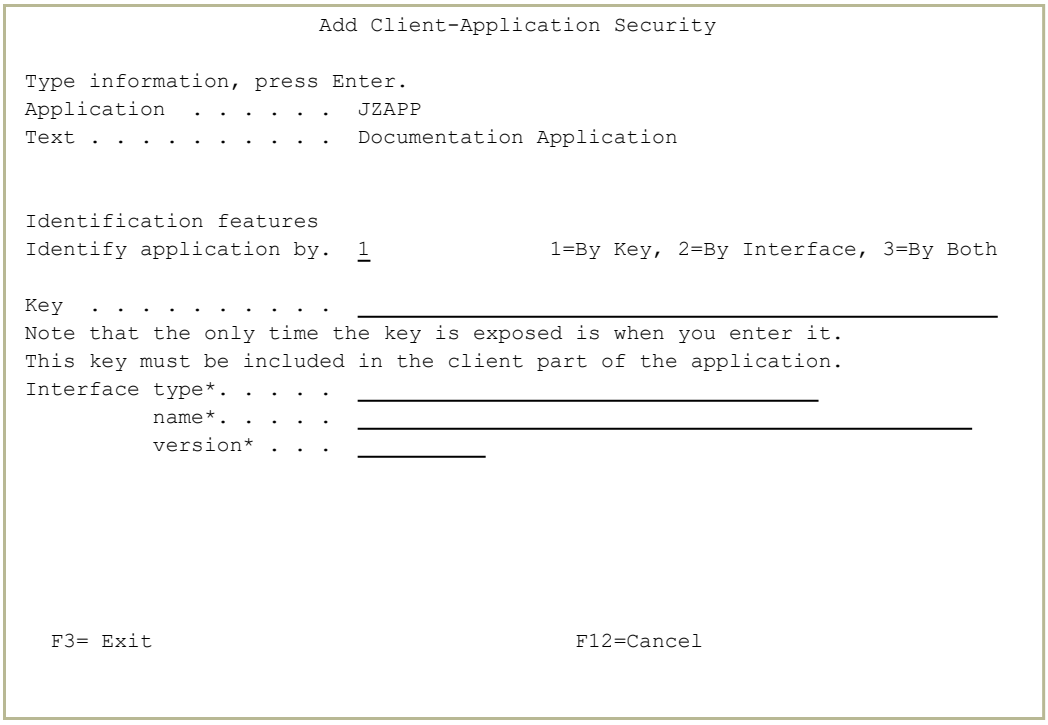
Specifies the user whose authority is checked for application access requests. The options are:

- **Name**: A specific user name.
- ***APP**: The name of the application.
- ***USER**: The current user.
- ***NOCHK**: Do not check.

**Check dynamic IP filter**

Verify that the access request is coming from an accepted IP address range.

After entering this information, press **Enter**. A third **Add Client-Application Security** screen appears:

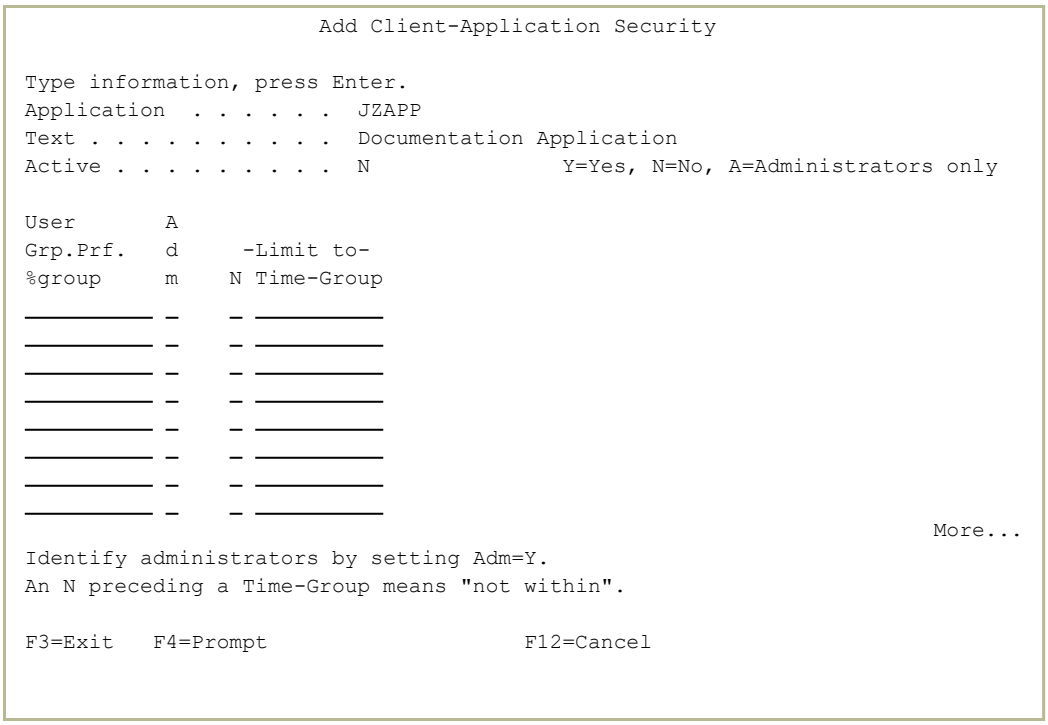



To **identify the application by a key**, enter the key in the **`Key`** field and set the **`Identify application by`** field to **`1`**.

To **identify the application interface**, enter the interface information in the **`Interface type`**, **`name`**, and **`version`** fields and set the **`Identify application by`** field to **`2`**.

To **identify the application by both a key and interface**, enter information into the fields for both and set the **`Identify application by`** field to **`3`**.

After entering this information, press **Enter**. A fourth **Add Client-Application Security** screen appears:




To specify users or groups who can use the application and when they can use them, enter information into the following fields:

**User Grp. Prf. %group**

A single or generic* user or group name. To select from a list, press the **F4** key.

**Adm**

To make the user or group administrators for the application, set this field to **Y**.

**-Limit to-**

**N**

To restrict these users to times excluded from the Time Group in the next field, set this field to **N**.

**Time-Group**

Restrict users to the times specified for a named Time Group (as shown in "Defining Time Groups" on page 504). If the **N** field is set to **N**, restrict them to times excluded from the Time Group.

After entering this information, press Enter. The first **Add Client-Application Security** screen reappears.

## Other Operations from the First Screen

To **modify** Firewall settings for an application, enter **1** in the **Opt** field for the application. The **Modify Client-Application Security** screens appear, following the same sequence as shown for adding an application above.

To **copy** Firewall settings from an existing application to a new one, enter **3** in the **Opt** field for the application.

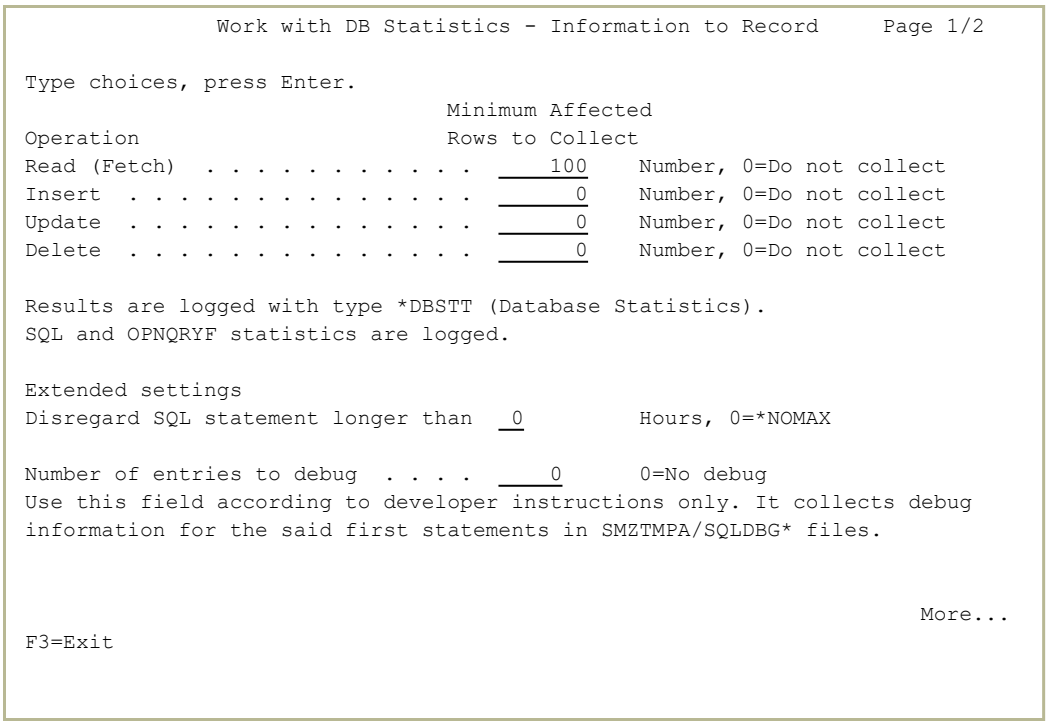
To **delete** an application from the list, enter **4** in the **Opt** field for the application. The **Delete Client-Application Security** screen appears, confirming that you want to delete the Firewall settings for the application.

## Recording Database Access Statistics

Firewall can collect and report statistics on SQL-based database access requests in specified jobs. The statistics collected when the DB#MON job is active and are placed in *DBSTT (database statistics) files when each analyzed job ends.

To **select database statistics to record** in a *DBSTT (database statistics) file, select **3. Database Statistics Settings** from the **Activation and Server Settings** screen (*STRFW* **> 1**).

The **Work with DB Statistics - Information to Record** screen appears:



```
               Work with DB Statistics - Information to Record     Page 1/2

Type choices, press Enter.
                                 Minimum Affected
Operation                        Rows to Collect
Read (Fetch)  . . . . . . . . . .    100    Number, 0=Do not collect
Insert  . . . . . . . . . . . . .      0    Number, 0=Do not collect
Update  . . . . . . . . . . . . .      0    Number, 0=Do not collect
Delete  . . . . . . . . . . . . .      0    Number, 0=Do not collect

Results are logged with type *DBSTT (Database Statistics).
SQL and OPNQRYF statistics are logged.

Extended settings
Disregard SQL statement longer than  0         Hours, 0=*NOMAX

Number of entries to debug  . . . .  0      0=No debug
Use this field according to developer instructions only. It collects debug
information for the said first statements in SMZTMPA/SQLDBG* files.



                                                                      More...
F3=Exit
```

The log collects information for each of four types of SQL operations, **Read (Fetch)**, **Insert**, **Update**, and **Delete**.

To **limit the log** to only include operations of each type that affected a minimum number of rows, set the **Minimum Affected Rows to Collect** field for that information type to the minimum value. For example, if you set the **Minimum Affected Rows to Collect** field for **Insert** operations to **100**, the log will only include operations that inserted at least one hundred rows.

To skip logging one of the types of operations, set the **Minimum Affected Rows to Collect** field for that type to **0**.

To specify more details of the logging process, press the F9 key.

To skip logging SQL statements that have run for a long time, set the **Disregard SQL statement longer than field** to the maximum number of hours that the statement may run continuously while database accesses are being logged. For example, if you set the field to **24**, statements that run continuously for more than 24 hours will not be logged. To include statements regardless of how long they run, set the field to **0**.

Leave the **Number of entries to debug** field set to **0** unless developers have directed you to set it to a different value.

After entering the values on this screen, press Enter. The Work with DB Statistics - Data to Control screen appears:

```
                  Work with DB Statistics - Data to Control        Page 2/2

Type choices, press Enter.
1=Select  4=Delete
Subset  . . .  _______________
Opt  Seq  Description
 _     1  /* Recommended: Use filters to save performance. */
_      2  FTRFILE((ALEX/DEMOPF *EQ))
_      3  FTRFILE((ALEX/TEST1))
_      4  FTRFILE((ALEX/IBM1))
_      5  FTRFILE((ALEX/IBM2))
_      6  FTRFILE((ALEX/IBM4))
_      7  FTRFILE((ALEX/IBM3))
_      8  FTRFILE((ALEX/IBM5))
_      9  FTRFILE((ALEX/SPOOL1))
_     10  FTRFILE((ALEX/SPOOL3))









Bottom
F3=Exit   F6=Add New   F10=Inc/Exclude   F12=Previous
```

The body of the screen lists up to ten tests to be run on the operations to determine if they are to be included in the output. The tests are combined by an implicit AND.

For each test, the line shows its sequence (from 1 to 10) when run, whether it is active, and a **Description**. If the test has been defined, the

Description shows the program code for the test. To see text descriptions for the tests, press the **F10** key.

To **modify a test**, enter **1** in the **Opt** field for that line. The **Modify DB Statistics Definition** screen appears, with fields to set the text description for the test and whether it is active. Press **Enter** to display the **Filter DB Statistics (FTRDBSTT)** screen, in which you can specify whether the database file, user profile, or job name or number are equal or not equal to specific or generic* values.

To **add a test**, press the **F6** key. The **Add DB Statistics Definition screen** appears, in which you can enter new information corresponding to that in the **Modify DB Statistics Definition** screen.

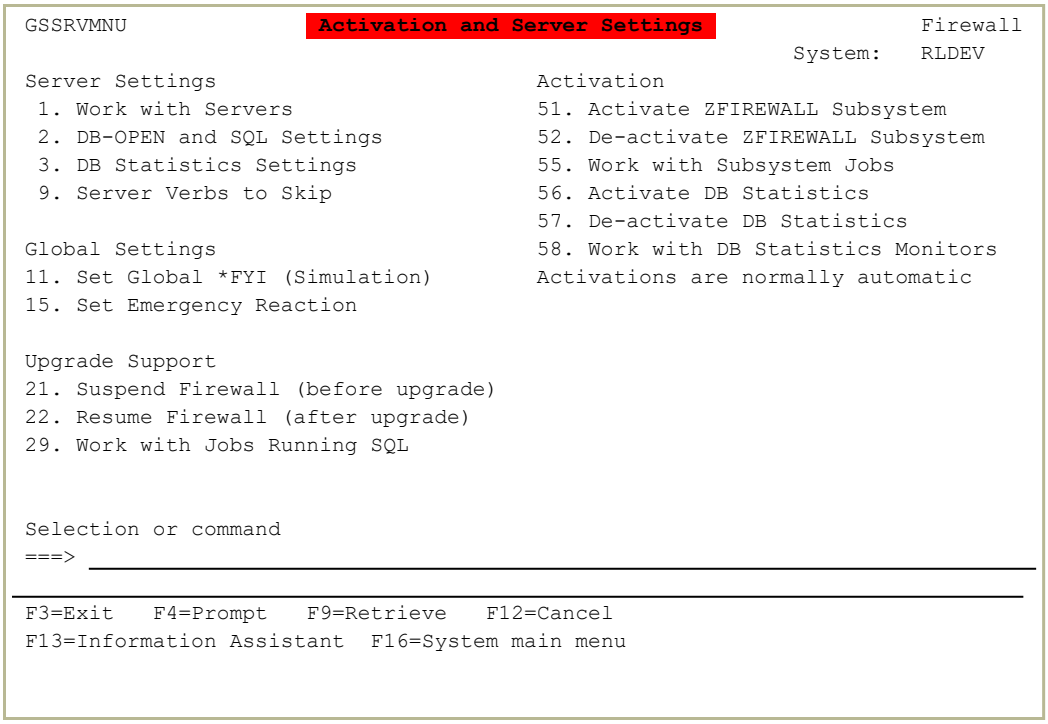
To **delete a test**, enter **4** in the **Opt** field for that line. The **Delete DB Statistics Definitions** screen appears, in which you can confirm the deletion,

## Activating and De-Activating DB Statistics

To **activate statistics collection**, select **`56. Activate DB Statistics`** from the **Activation and Server Settings** screen (*STRFW* **`> 1`**). The **Start DB Statistics Collection (STRDBSTT)** screen appears. Press **Enter** to confirm that statistics collection is to begin. The DB#MON job in the ZFIREWALL subsystem starts.

To **de-activate statistics collection**, select **`57. De-Activate DB Statistics`** from the **Activation and Server Settings** screen (*STRFW* **`> 1`**). The **End DB Statistics Collection (ENDDBSTT)** screen appears. Press **Enter** to confirm that statistics collection is to stop. The DB#MON job in the ZFIREWALL subsystem ends.

# Suspending or De-activating Firewall




NOTE To active and de-activate Firewall activity, use options **21** and **22**, to suspend and resume Firewall. Do not use options 51 and 52, which only activate and deactivate the ZFIREWALL subsystem, unless instructed to do so by technical support. DB statistics activity and sending SIEM are related to subsystem activity. When the subsystem is not active, you might notice delays in writing log entries.

To **suspend Firewall**, select **21. Suspend Firewall (before upgrade)**. The **Set Firewall Security (SETFWSEC)** screen appears with default values for the *SETFWSEC* command for suspending Firewall. To accept the defaults, press **Enter**. All Firewall activity is suspended.

To **resume Firewall** after it has been suspended, select **22. Resume Firewall (after upgrade)**. The **Set Firewall Security (SETFWSEC)** screen appears with default values for the *SETFWSEC* command for resuming Firewall. To accept the defaults, press **Enter**. Firewall activity resumes.

When tech support tells you to de-activate only the ZFIREWALL subsystem, select **52. De-activate ZFIREWALL Subsystem**. The End Subsystem (ENDSBS) screen appears with default values for the ENDSBS command to de-activate Firewall. To accept the defaults, press Enter. The Firewall subsystem, ZFIREWALL, ends, but data continues to be written to the DTAQ.

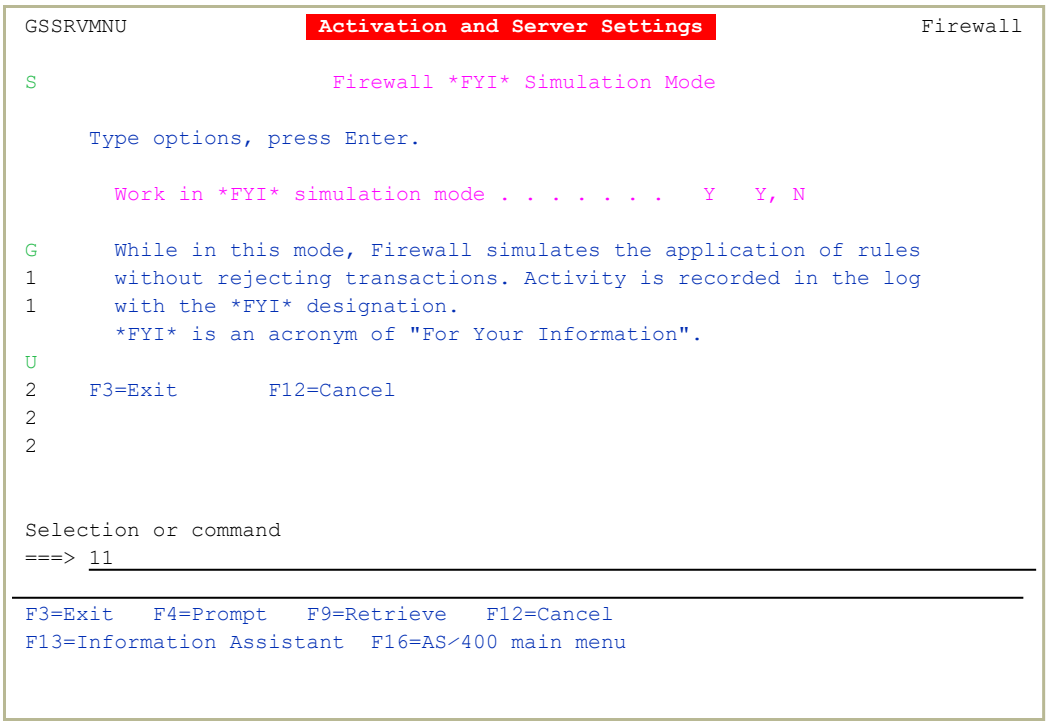
When tech support tells you to re-activate only the ZFIREWALL subsystem, select **51. Activate ZFIREWALL Subsystem**. The Start Subsystem (STRSBS) screen appears with default values for the *STRSBS* command. To accept the defaults, press Enter. The Firewall subsystem, ZFIREWALL, resumes.

## Running Firewall in FYI Simulation mode

In FYI (For Your Information) Simulation mode, Firewall logs activity and its responses to it, but does not reject any activity or trigger other actions. You can use FYI mode to collect records of activity on your system that you can then use to train the Rule Wizards in creating Firewall rules that are optimized for your system.

To start FYI mode, select **11. Set Global *FYI (Simulation)** from the **Activation and Server Settings** menu (STRFW > 1) as shown in "Creating and Modifying Firewall Rules" on page 49.

The **Firewall *FYI* Simulation Mode** window appears:




To **start** FYI Simulation mode, type **Y** in the **Work in *FYI* simulation mode** field.

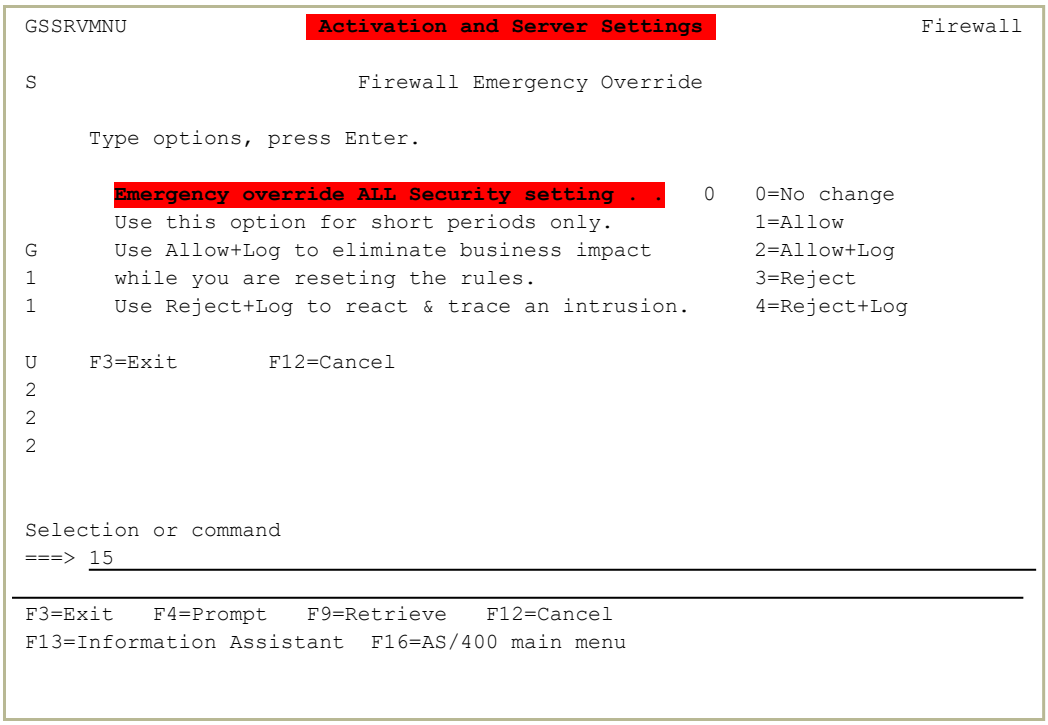
To **end** FYI Simulation mode, type **N** in the **Work in *FYI* simulation mode** field.

## Overriding Firewall Settings in Emergencies

To **override all firewall settings** in emergencies, select **`15. Set Emergency Reaction`** from the **Activation and Server Settings** menu (***STRFW > 1***) as shown in "Creating and Modifying Firewall Rules" on page 49.

You can also open this window by pressing the **F24 (Shift+F12)** key on many screens, such as the **Work with Server Security** screen as shown in "Setting Firewall Rules for Servers" on page 54

The **Firewall Emergency Override** window appears:




The window has a single numeric field with five options:

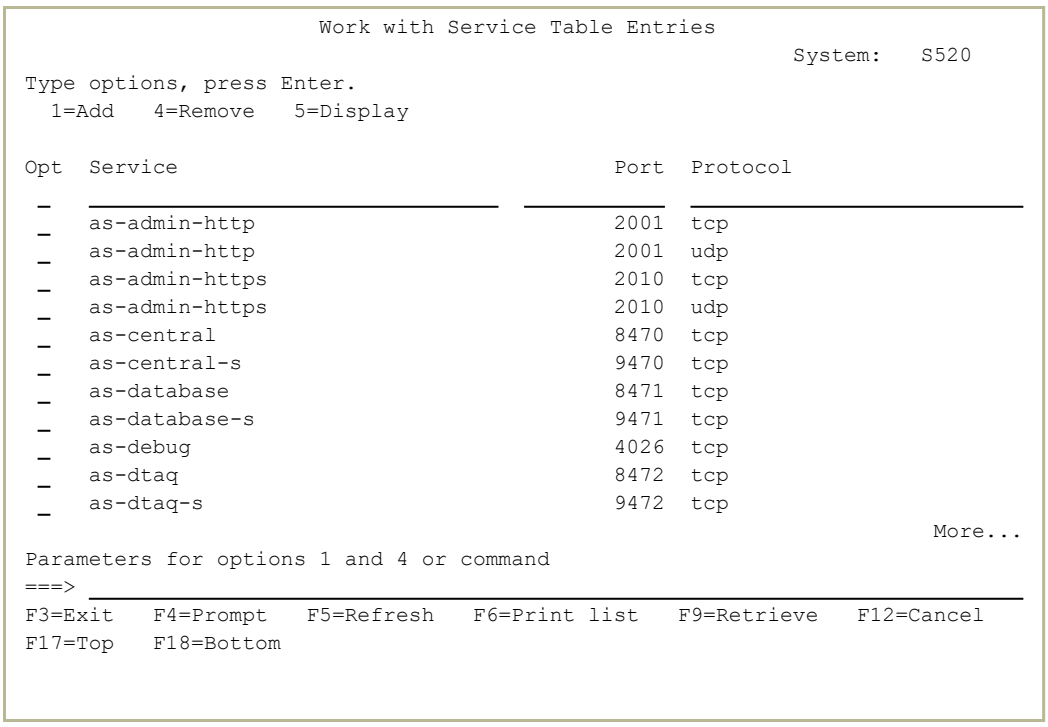
- **`0: No change.`** Obey all rules as usual. Leave the field set to this unless there is an emergency.
- **`1: Allow.`** Allow all activity without logging.
- **`2: Allow+Log.`** Allow all activity and log it.
- **`3: Reject.`** Reject all activity without logging.
- **`4: Reject+Log`**. Reject all access requests and log them. Use this setting to react to and trace intrusions.

## Configuring FTPS

To **use FTPS for Firewall**, you need to switch port 21 to a different port number. Follow these steps:

1. First, assign your own certificate to the FTP server on the IBM i, as shown in IBM documentation at https://www.ibm.com/support/pages/configuring-ssl-ftp-server.
2. Confirm that the user-defined port that you wish to use is not busy or restricted on the IBM i. NOTE: Select a port number greater than 1023. Port 2121 is a common choice for the FTPS port.
3. On the command line, enter the command
   *WRKSRVTBLE*

   The **Work with Service Table Entries** screen appears:



```
                      Work with Service Table Entries
                                                          System:   S520
Type options, press Enter.
  1=Add   4=Remove   5=Display

Opt  Service                                  Port  Protocol
 _   ___________________________________  _____  ____________________________
 _   as-admin-http                          2001  tcp
 _   as-admin-http                          2001  udp
 _   as-admin-https                         2010  tcp
 _   as-admin-https                         2010  udp
 _   as-central                            8470  tcp
 _   as-central-s                          9470  tcp
 _   as-database                           8471  tcp
 _   as-database-s                         9471  tcp
 _   as-debug                              4026  tcp
 _   as-dtaq                               8472  tcp
 _   as-dtaq-s                             9472  tcp
                                                                    More...
Parameters for options 1 and 4 or command
===> ____________________________________________________________________________
F3=Exit   F4=Prompt   F5=Refresh   F6=Print list   F9=Retrieve   F12=Cancel
F17=Top   F18=Bottom
```

4. Type **1** in the **Opt** field on the first line and press **Enter**. The standard **Add Service Table Entry (ADDSRVTBLE)** screen appears.
5. Enter the following values in its fields:
   - **Service**: 'ftp-control'
   - **Port**: the new port number
   - **Protocol**: 'udp'

6. Press the **F4** key, **Enter**, and the **F3** key. The **Work with Service Table Entries** screen reappears.
7. Again, type **1** in the **Opt** field on the first line and press **Enter**. The standard **Add Service Table Entry (ADDSRVTBLE)** screen appears.
8. Enter the following values in its fields:
   - **Service**: 'ftp-control'
   - **Port**: the new port number
   - **Protocol**: 'tcp'
9. Press the **F4** key, **Enter**, and the **F3** key. The **Work with Service Table Entries** screen reappears.
10. Scroll down with the PageDown key until you see lines for the service **ftp-control** and port **21**. For each, enter **4** in the **Opt** field and press **Enter**. The **Confirm Delete of Service Table Entries** screen appears. If the listing of the services to be deleted is correct, press **Enter** to confirm the deletions.
11. To update FTP attributes, disabling insecure FTP and allowing only secure sockets, enter the command

    *CHGFTPA NAMEFMT(*LIB) CURDIR(*CURLIB) ALWSSL(*ONLY)*
12. To restart the FTP server, enter the commands

    *ENDTCPSVR SERVER(*FTP)*

    *STRTCPSVR SERVER(*FTP)*
13. To update the FTPS server data port definitions, enter the commands

    *ENDTCPSVR SERVER(*FTP)*

    *ADDENVVAR ENVVAR(QIBM_FTP_PORT_RANGE) VALUE('1023-65535') LEVEL(*SYS)*

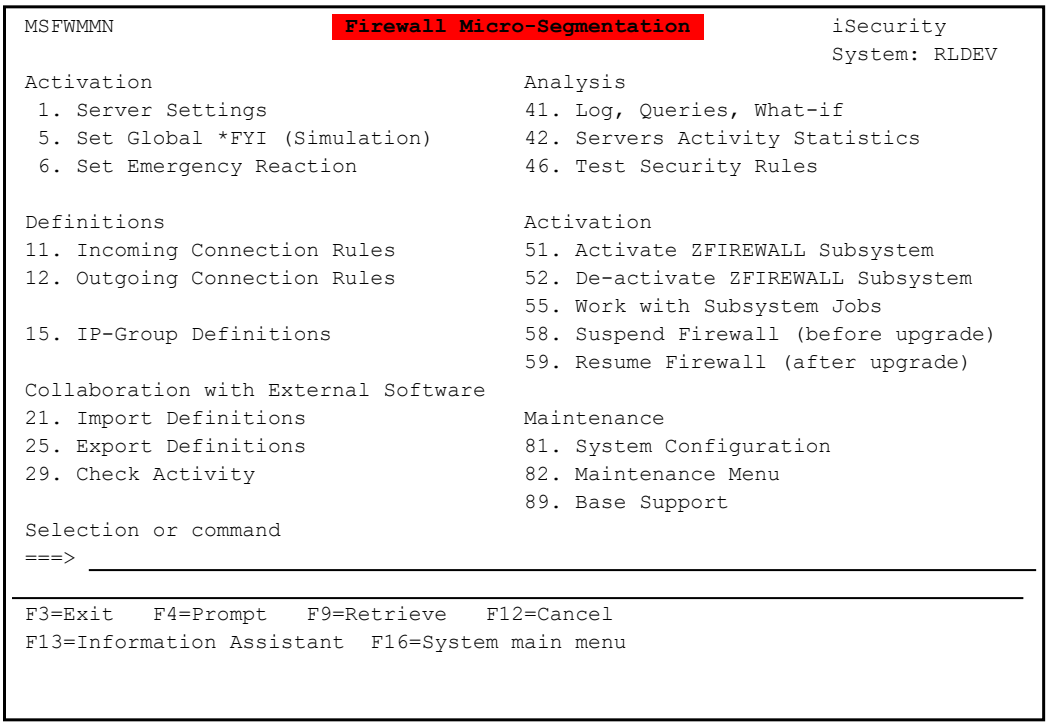
    *WRKENVVAR*

    *STRTCPSVR SERVER(*FTP)*
14. Open all ports higher than 1023 on the firewall (1024-65535) from the Imperva Gateway to the AS/400 server.
15. Check via the main WAN/LAN Firewall rules that the ports are not blocked.
16. If FTPEXITPGM (the FTP exit point program) is enabled on the server, disable it.

# Firewall Micro-Segmentation

**Micro-Segmentation** divides a network into smaller sub-networks with firewalls between them. This can prevent attacks and other issues from spreading within networks, much as Firewall protects the networks as a whole from issues coming in from outside. iSecurity Firewall implements it in collaboration with external vendors.

To work with Firewall Micro-Segmentation, enter ***STRFWMS*** on the command line. The **Firewall Micro-Segmentation** screen appears:




Most of these items connect to screens within the larger Firewall product, with settings focused on Micro-Segmentation.

The menu items lead to the following screens:

### Activation

#### 1. Server Settings

**Work with Server Security** as shown in "Setting Firewall Rules by Server" on page 52. (Only the Socket Exit Points are relevant.)

**5. Set Global *FYI (Simulation)**

Firewall *FYI* Simulation Mode as shown in "Setting Firewall Rules for Servers" on page 54.

**6. Set Emergency Reaction**

Firewall Emergency Override as shown in "Overriding Firewall Settings in Emergencies" on page 537.

**Definitions**

**11. Incoming Connection Rules**

Work with Incoming Connection Rules as shown in "Setting Firewall Rules for Incoming Socket Connections" on page 451.

**12. Outgoing Connection Rules**

Work with Outgoing Connection Rules as shown in "Setting Firewall Rules for Outgoing Socket Connections" on page 454.

**15. IP-Group Definitions**

Work with IP-Groups as shown in "Defining IP-Groups for Socket Connections" on page 448.

**Collaboration with External Software**

**21. Import Definitions Maintenance**

Micro-Segmentation Rules dialog, depending on the external vendor's software.

**25. Export Definitions**

Micro-Segmentation Rules dialog, depending on the external vendor's software.

**29. Check Activity**

Check Firewall Micro-Segmentation Activity, depending on the external vendor's software.

**Analysis**

**41. Log, Queries, What-if**

Socket Reports - Activity. This displays the activity log based on recent events or the activity type, reruns the log based on current rules, or open a Query Wizard for further analysis.

**42. Servers Activity Statistics**

Display User Activity (DSPFWUSRA) as shown in "Displaying Firewall Activity by Server" on page 442.

**46. Test Security Rules**

Check Firewall Security (CHKFWSEC). This checks server functions based on the Local/incoming, Bound, or Remote/destination ports or IPV$/IPV6 addresses.

**Activation**

**51. Activate ZFIREWALL Subsystem**

Start Subsystem (STRSBS) as shown in "Suspending or De-activating Firewall" on page 534

**52. De-activate ZFIREWALL Subsystem**

End Subsystem (ENDSBS) as shown in "Suspending or De-activating Firewall" on page 534.

**55. Work with Subsystem Jobs**

The IBM Work with Subsystem Jobs screen, showing jobs using the ZFIREWALL subsystem.

**58. Suspend Firewall (before upgrade)**

Set Firewall Security (SETFWSEC) as shown in "Suspending or De-activating Firewall" on page 534.

**59. Resume Firewall (after upgrade)**

Set Firewall Security (SETFWSEC) as shown in "Suspending or De-activating Firewall" on page 534.

**Maintenance**

**81. System Configuration**

iSecurity (part I) Global Parameters as shown in "Configuring Firewall" on page 32.

**82. Maintenance Menu**

**Maintenance Menu** as shown in the *iSecurity Installation and Base Support* manual.

**89. Base Support**

BASE Support as shown in the *iSecurity Installation and Base Support* manual.

# Appendix A - Command Help

Delete this text and replace it with your own content.

## Display Firewall Log (DSPFWLOG)

**Where allowed to run:** All environments (*ALL)
**Threadsafe:** No

Parameters
Examples
Error messages

The Display Firewall Log (DSPFWLOG) command displays selected entries from the Firewall log.

Top

# Parameters

| Keyword | Description | Choices | Notes |
|---|---|---|---|
| PRVMIN | Display last n minutes | *Decimal number*, ***BYTIME** | Optional, Positional 1 |
| FROMTIME | Starting date and time | *Element list* | Optional, Positional 2 |
| | Element 1: Starting date | *Date*, ***CURRENT**, *YESTERDAY, *WEEKSTR, *PRVWEEKS, *MONTHSTR, *PRVMONTHS, *YEARSTR, *PRVYEARS, *MON, *TUE, *WED, *THU, *FRI, *SAT, *SUN, *START | |
| | Element 2: Starting time | *Time*, **000000** | |
| TOTIME | Ending date and time | *Element list* | Optional, Positional 3 |
| | Element 1: Ending date | *Date*, ***CURRENT**, *YESTERDAY, *WEEKSTR, *PRVWEEKS, *MONTHSTR, *PRVMONTHS, *YEARSTR, *PRVYEARS, *MON, *TUE, *WED, *THU, *FRI, *SAT, *SUN | |
| | Element 2: Ending time | *Time*, **235959** | |

| | | | |
|---|---|---|---|
| USER | User*,<GrpPrf,'%GRP','%<GRP' | *Character value*, ***ALL**, *NONE | Optional, Positional 5 |
| OBJ | Object | *Qualified object name* | Optional, Positional 6 |
| | Qualifier 1: Object | *Generic name, name*, ***ALL** | |
| | Qualifier 2: Library | *Generic name, name*, ***ALL**, *UNDFN | |
| OBJTYPE | Object Type | ***ALL**, *FILE, *LIB, *DTAQ, *PRTF, *PGM, *CMD | Optional, Positional 7 |
| IPADR | IPv4 (generic*) or IPv6 | *Character value*, ***ALL** | Optional, Positional 8 |
| ADRPFXLEN | Prefix length for IPv6 | 1-128, ***ALL** | Optional, Positional 9 |
| TYPE | Type | *SELECT, *NATIVE, *IFS, *IPIN, *UP, *DOWN, *IPOUT, *USER, *FILTFR, *FTP, *FTPLOG, *FTPSRV, *FTPCLN, *TFTP, *REXINF, *REXLOG, *REXEC, *SSHD, | Optional, Positional 11 |

*SQLSRV,
*RMTSQL, *SQL,
*NDB,
*DBOPEN,
*RMTSRV,
*FILSRV,
*TELINF,
*TELNET,
*TELOFF,
*SIGNON,
*WSG,
*ORDTAQ,
*DTAQ, *VPRT,
*LICMGT,
*ORLICM,
*CSLICM, *SNA,
*DDM, *DRDA,
*RMTSGN,
*USRSEC,
*CSCNVM,
*CSCLNM,
*NPRENT,
*NPRSPL,
*MSGSRV,
*SQLENT,
*OBJINF,
*USRPRF,
*CHGUP,
*CRTUP,
*DLTUPA,
*DLTUPB,
*RSTUP,
*TCPSGN,
*DHCP,
*DHCPAB,

| | | | |
|---|---|---|---|
| | | ***ALL** | |
| ALLOW | Allowed | *YES, *NO, ***ALL** | Optional, Positional 12 |
| MODE | Mode of operation | *REAL, *FYI, ***ALL** | Optional, Positional 13 |
| JOB | Job name | *Qualified job name* | Optional, Positional 14 |
| | Qualifier 1: Job name | *Generic name, name*, ***ALL** | |
| | Qualifier 2: User | *Generic name, name*, ***ALL** | |
| | Qualifier 3: Number | 000000-999999, ***ALL** | |
| NBRRCDS | Number of records to process | *Decimal number*, ***NOMAX** | Optional, Positional 15 |
| RECALC | Recalculate and display | *YES, *DIFFONLY, *SAMEONLY, ***NO** | Optional, Positional 16 |
| OUTPUT | Output | *****, *PRINT, *PRINT1, *PRINT2, *PRINT3, *PRINT4, *PRINT5, *PRINT6, *PRINT7, *PRINT8, *PRINT9, *OUTFILE | Optional, Positional 17 |

| | | | |
|---|---|---|---|
| PRTFMT | Print format | ***SHORT**, *FULL | Optional, Positional 18 |
| OUTFILE | File to receive output | *Qualified object name* | Optional, Positional 19 |
| | Qualifier 1: File to receive output | *Name* | |
| | Qualifier 2: Library | *Name*, ***LIBL** | |
| OUTMBR | Output member options | *Element list* | Optional, Positional 20 |
| | Element 1: Member to receive output | *Name*, ***FIRST** | |
| | Element 2: Replace or add records | ***REPLACE**, *ADD | |
| JOBD | Job description. | Single values: ***NONE** Other values: *Qualified object name* | Optional, Positional 21 |
| | Qualifier 1: Job description. | *Name*, **QBATCH** | |
| | Qualifier 2: Library | *Name*, ***PRODUCT**, *LIBL, *CURLIB | |
| FSYS | File System/Root Dir | *Character value*, ***ALL** | Optional, Positional 22 |
| DOCN | Directory/File name contains | *Character value*, ***ALL** | Optional, Positional 23 |
| OBJOPR | Object operation | ***ALL**, *OBJREAD, *OBJWRT | Optional, Positional 24 |

| | | | |
|---|---|---|---|
| PWDVLD | Password validated (rejected) | *Generic name, name*, ***ALL** | Optional, Positional 25 |
| PRFCMD | User Profile command | ***ALL**, CHANGE, CREATE, 'DELETE_AFT', 'DELETE_BFR', RESTORE | Optional, Positional 26 |
| SRVUSS | Server ID for *USRSEC | ***ALL**, *DRDA, *CSCNVM, *CSCLNM, *NPRENT, *NPRSPL, *MSGSRV, *SQLENT, *OBJINF, *TCPSGN | Optional, Positional 27 |
| PRODID | OS400 product-identifier | *Character value*, ***ALL** | Optional, Positional 28 |
| FEATID | OS400 feature | *Character value*, ***ALL** | Optional, Positional 29 |
| TERM | Screen name | *Generic name, name*, ***ALL**, *BLANKS | Optional, Positional 30 |
| PWDVL | Client password validated | ***ALL**, *YES, *NO, *ENCRYPTED | Optional, Positional 31 |
| SRCLOC | Source location | *Name*, ***ALL** | Optional, Positional 32 |
| SRCUSR | Source user | *Name*, ***ALL** | Optional, |

| | | | |
|---|---|---|---|
| | | | Positional 33 |
| TGTUSR | Target user | *Name*, ***ALL**, *NONE | Optional, Positional 34 |
| SRVNTV | Server ID for *NATIVE | ***ALL**, *FILTFR, *RMTSRV, *SQL, *RMTSQL, *NDB, *DBOPEN, *FTPSRV, *FTPCLN, *TFTP, *REXEC, *DDM, *ORDTAQ, *DTAQ, *VPRT, *FILSRV, *IWCMD | Optional, Positional 35 |
| SRVIFS | Server ID for *IFS | ***ALL**, *FILSRV, *FTPSRV, *FTPCLN, *TFTP, *DDM | Optional, Positional 36 |
| SRVLIC | Server ID for *LICMGT | ***ALL**, *ORLICM, *CSLICM | Optional, Positional 37 |
| SRVIPIN | Server ID for *IPIN | ***ALL**, *FTPLOG, *TFTP, *REXLOG, *WSG, *TELNET, *DDM, *DRDA, *FTPSRV, *REXEC, *SQL, *RMTSRV, *DBOPEN, *TCPSGN | Optional, Positional 38 |
| SRVFTP | Server ID for *FTPCLN | ***ALL**, *FTPLOG, | Optional, |

| | | | |
|---|---|---|---|
| | | *FTPSRV, *FTPCLN, *TFTP, *REXLOG, *REXEC | Positional 39 |
| SRVSNA | Server ID for *SNA | ***ALL**, *DDM, *DRDA, *RMTSGN | Optional, Positional 40 |
| SRVDHCP | Server ID for *DHCP | ***ALL**, *DHCPAB, *DHCPAR, *DHCPRP | Optional, Positional 41 |
| CHADHCP | Client hardware address | *Character value*, ***ALL** | Optional, Positional 42 |
| SRVSCR | Server ID for *SCREEN | ***ALL**, *SCRLCK, *SCRRLS, *SCREND | Optional, Positional 43 |
| DBOQRYT | Ouery type for *DBOPEN | ***ALL**, NTVIO, OPNQRYF, QUERYAPI, OTHRNONSQL, STRSQL, ODBC, OTHERSQL, QSQPRCED, CLI | Optional, Positional 44 |
| DBSTTO | DB Operation | ***ALL**, READ, INSERT, UPDATE, DELETE | Optional, Positional 45 |
| TIMEGRP | Filter by time group | *Element list* | Optional, Positional 4 |
| | Element 1: Relationship | *IN, *OUT, ***NONE** | |
| | Element 2: Time group | *Name*, ***SELECT** | |
| QRY | Filter using query rules | *Name*, ***NONE** | Optional, Positional |

| | | | |
|---|---|---|---|
| | | | 10 |
| START | Start log display | *OLD, *NEW, ***DFT** | Optional, Positional 46 |

Top

## Display last n minutes (PRVMIN)

To view activity in a period of time up to when the report is run, set this parameter to the number of minutes that you would like to check.

***BYTIME**
Use the values set in the FROMTIME and TOTIME parameters.

***decimal-number***
Specify the number of minutes before the time that the query is run to be checked. For example, to see information for the previous five minutes, set this value to "5".

Top

## Starting date and time (FROMTIME)

Specifies the date and time at which the information to be queried begins.

Element 1: Starting date

***CURRENT**
The current date

***YESTERDAY**
Yesterday's date

***WEEKSTR**
The first day of the current week. The starting day is specified in Base Support > Global Installation Defaults > Installation (STRAUD > 89 > 51 > 1).

***PRVWEEKS**
The first day of the previous week

***MONTHSTR**

The first day of the current month

***PRVMONTHS**

The first day of the previous month

***YEARSTR**

The first day of the current year

***PRVYEARS**

The first day of the previous year

***MON**

Monday

***TUE**

Tuesday

***WED**

Wednesday

***THU**

Thursday

***FRI**

Friday

***SAT**

Saturday

***SUN**

Sunday

***START**

The earliest information available.

***date***

Specify the date on which the information to be queried begins. The day must be in YYMMDD format, with or without separators.

### Element 2: Starting time

**000000**

The start of the day.

***time***

The time to begin on the date specified in the previous parameter, in 24-hour HHMMSS format, with or without separators.

Top

## Ending date and time (TOTIME)

Specifies the date and time of the last information to be queried.

### Element 1: Ending date

***CURRENT**

The current date

***YESTERDAY**

Yesterday's date

***WEEKSTR**

The first day of the current week. By default, this is Sunday.

***PRVWEEKS**

The first day of the previous week

***MONTHSTR**

The first day of the current month

***PRVMONTHS**

The first day of the previous month

***YEARSTR**

The first day of the current year

***PRVYEARS**

The first day of the previous year

***MON**

Monday

***TUE**

Tuesday

***WED**

Wednesday

***THU**

Thursday

***FRI**

Friday

***SAT**

Saturday

***SUN**

Sunday

***date***

Specify the date on which the information to be queried ends, in YYMMDD format, with or without separators.

Element 2: Ending time

**235959**
The end of the specified date.

***time***
The time to end on the specified date, in 24-hour HHMMSS format, with or without separators.

Top

## User*,<GrpPrf,'%GRP','%<GRP' (USER)

Specifies the user or group requesting the activity

***ALL**
All users.

***NONE**
Servers that do not have a specific user name.

***character-value***
The user or group. The values can have several forms:

- User*: A user name or generic* name.
- <GrpPrf: A group profile, preceded by the '<' character.
- '%GRP': A group name, preceded by the '%' character and surrounded by single quotation marks.
- '%<GRP': A group, including the group profile and its users, preceded by the string '<%' and surrounded by single quotation marks.

Top

## Object (OBJ)

The object on which the activity requests to operate.

Qualifier 1: Object

***ALL**
Include all objects.

***generic-name***
Include objects with a specified generic name.
***name***
Include objects with a specified name.

Qualifier 2: Library

***ALL**
Include objects from all libraries.
***UNDFN**
The library name is undefined.
***generic-name***
Include objects within libraries with a specified generic name.
***name***
Include objects in libraries with a specified name.

Top

## Object Type (OBJTYPE)

Specifies external object types, as specified in https://www.ibm.com/docs/en/i/7.2?topic=objects-external-object-types

***ALL**
Include all object types.

Top

## IPv4 (generic*) or IPv6 (IPADR)

Specifies IPV4 or IPV6 address ranges to include.

***ALL**
Include all address ranges.
***character-value***
Specific or generic address ranges to include.

Top

## Prefix length for IPv6 (ADRPFXLEN)

Specifies the prefix length for IPV6 addresses.

***ALL**
All prefix lengths.
***1-128***
The prefix length for the range of addresses.

Top

## Type (TYPE)

Include servers that include the specified type of activity or that act on the specified type of objects.

***SELECT**
If running interactively, presents a list of types from which you can choose.
***NATIVE**
Native objects.
***IFS**
IFS objects.
***IPIN**
Incoming IP addresses.
***UP**
Uploading data.
***DOWN**
Downloading data.
***IPOUT**
Outgoing IP addresses.
***USER**
Users or user groups.
***FILTFR**
Original File Transfer Function
***FTP**
File Transfer Function

***FTPLOG**
FTP logging
***FTPSRV**
FTP Server-Incoming Request Validation
***FTPCLN**
FTP Client-Outgoing Request Validation
***TFTP**
TFTP Server Request Validation
***REXINF**
Any information regarding remote execution.
***REXLOG**
Remote execution logs.
***REXEC**
REXEC Server Request Validation.
***SSHD**
SSH,SFTP,SCP- Secured CMD Entry, FTP, COPY
***SQLSRV**
SQL servers.
***RMTSQL**
REXEC Server Request Validation
***SQL**
Database Server - SQL access & Show
***NDB**
Database Server - Database access
***DBOPEN**
Open Database
***RMTSRV**
Remote Command/Program Call
***FILSRV**
File Server
***TELINF**
Any information regarding Telnet.
***TELNET**
Telnet Device Initialization
***TELOFF**
Telnet Device Termination
***SIGNON**

Sign-On completed

***WSG**

WSG Server Sign-On Validation

***ORDTAQ**

Original Data Queue Server

***DTAQ**

Data Queue Server

***VPRT**

Original Virtual Print Server

***LICMGT**

License Management Server

***ORLICM**

Original License Management Server

***CSLICM**

Central Server - license management

***SNA**

The IBM SNA protocol, including DDM, DRDA, and remote signon.

***DDM**

DDM request access

***DRDA**

DDM request access

***RMTSGN**

Remote sign-on (Passthrough)

***USRSEC**

User security.

***CSCNVM**

Central Server - conversion map

***CSCLNM**

Central Server - client management

***NPRENT**

Central Server - client management

***NPRSPL**

Network Print Server - spool file

***MSGSRV**

Original Message Server

***SQLENT**

Database Server - entry

***OBJINF**
Database Server - object information
***USRPRF**
User profiles.
***CHGUP**
Change User Profile
***CRTUP**
Create User Profile
***DLTUPA**
Delete User Profile - after delete
***DLTUPB**
Delete User Profile
***RSTUP**
Restore User Profile
***TCPSGN**
Original Message Server
***DHCP**
DHCP
***DHCPAB**
DHCP Address Binding Notify
***DHCPAR**
DHCP Address Release Notify
***DHCPRP**
DHCP Request Packet Validation
***PWRDWN**
Prepower Down System
***PWD**
Password
***PWDVLD**
Password Dictionary Check / Validation
***PWDVL2**
Password Dictionary Check /Validation fmt2
***PWDCHK**
Password Dictionary Check / Check
***SCREEN**
iSecurity SCREEN
***SKT**

Socket

***SKTACP**

Socket Accept

***SKTCNT**

Socket Connect

***SKTLSN**

Socket Listen

***DBSTT**

Database statistics

***AGENT**

Information related to the Imperva SecureSphere Agent.

***ALL**

All objects

Top

## Allowed (ALLOW)

Specifies whether the data set includes rejected activity, accepted activity, or both.

***YES**

Include only accepted activity

***NO**

Include only rejected activity

***ALL**

Include both accepted and rejected activity

Top

## Mode of operation (MODE)

Whether to look for information from specific operation modes or for all modes.

***REAL**

Running actively, not in FYI Simulation Mode.

***FYI**
Firewall ran under FYI Simulation Mode
***ALL**
Running in either mode.

Top

## Job name (JOB)

Specific or generic* job names that produced the records

### Qualifier 1: Job name

***ALL**
All job names.
***generic-name***
Specify the generic user name of the jobs.
***name***
Specify the user name of the job.

### Qualifier 2: User

***ALL**
All users.
***generic-name***
Specific or generic* names of users whose jobs produced the records.
***name***
Users with the specific name.

### Qualifier 3: Number

***ALL**
All jobs.
***000000-999999***
Jobs with the specific job number.

Top

## Number of records to process (NBRRCDS)

Specifies the maximum number of records to process.

***NOMAX**
Process all records.
***decimal-number***
The maximum number of records to process.

Top

## Recalculate and display (RECALC)

Whether to recalculate the logs based on the current Firewall settings rather than what was in effect at the time.

***YES**
Recalculate the transactions showing whether they would be accepted or rejected under the current rules.
***DIFFONLY**
Recalculate the transactions, but only display the results that would be different.
***SAMEONLY**
Recalculate the transactions, but only display the results that would remain the same.
***NO**
Display the original results.

Top

## Output (OUTPUT)

Specifies the destination for output.

*****
The default output. If running interactively, this is the current screen.
***PRINT**

Print report to PDF outfile.

***PRINT1-9**

User-defined option.

***OUTFILE**

Print report as text to an outfile.

Top

## Print format (PRTFMT)

Specifies the format if output is created.

***SHORT**

Output must only be one line.

***FULL**

Output may be more than one line.

Top

## File to receive output (OUTFILE)

Specifies the database file to which the output of the command is directed. If the file does not exist, this command creates a database file in the specified library.

### Qualifier 1: File to receive output

***name***

Specify the name of the database file to which the command output is directed.

### Qualifier 2: Library

***LIBL**

The library list is used to locate the file. If the file is not found, one is created in the current library. If no current library exists, the file will be created in the QGPL library.

***name***

Specify the name of the library to be searched.

Top

## Output member options (OUTMBR)

Specifies the name of the database file member that receives the output of the command.

Element 1: Member to receive output

***FIRST**

The first member in the file receives the output. If OUTMBR(*FIRST) is specified and the member does not exist, the system creates a member with the name of the file specified for the "File to receive output (OUTFILE)" parameter. If the member already exists, you have the option to add new records to the end of the existing member or clear the member and then add the new records.

***name***

Specify the name of the file member that receives the output. If it does not exist, the system creates it.

Element 2: Replace or add records

***REPLACE**

The system clears the existing member and adds the new records.

***ADD**

The system adds the new records to the end of the existing records.

Top

## Job description. (JOBD)

Specifies the job within which the query will run.

Single values

***NONE**

Run within the job that is running the query.

Qualifier 1: Job description.

**QBATCH**
Run the command in a separate job. Use the QBATCH job description for this.

***name***
Specify the name of the job within which it is to run.

Qualifier 2: Library

***PRODUCT**
QBATCH within the data library for the product.

***LIBL**
Search the Library List for an appropriate library.

***CURLIB**
The program is within the current library.

***name***
The name of the library containing the program.

Top

## File System/Root Dir (FSYS)

Specifies the filesystems for which logs are included.

***ALL**
Include logs for all filesystems.

***character-value***
Include logs for a specified filesystem.

Top

## Directory/File name contains (DOCN)

Include logs for files whose directory or file names contain a specified string.

***ALL**
Include files with all names.

***character-value***

Specify the string which must appear in directory or file names for them to be included.

Top

## Object operation (OBJOPR)

Specifies the operation performed on the object.

***ALL**
Include all operations.
***OBJREAD**
Include READ operations.
***OBJWRT**
Include WRITE operations.

Top

## Password validated (rejected) (PWDVLD)

Passwords that were rejected by the PWDVLD, PWDVL2, or PWDCHK servers. Passwords are most often rejected because they are found in predefined dictionaries.

***ALL**
All rejected passwords.
***generic-name***
A generic string representing rejected passwords.
***name***
A specific rejected password.

Top

## User Profile command (PRFCMD)

Specifies operations on user profiles.

***ALL**
All operations.
**CHANGE**
CHANGE operations.
**CREATE**
CREATE operations.
**'DELETE_AFT'**
DELETE AFTER operations.
**'DELETE_BFR'**
DELETE BEFORE operations.
**RESTORE**
RESTORE operations.

Top

## Server ID for *USRSEC (SRVUSS)

Specifies the server ID for *USRSEC

***ALL**
All servers
***DRDA**
DRDA Distributed Relational DB access
***CSCNVM**
Central Server - conversion map
***CSCLNM**
Central Server - client management
***NPRENT**
Network Print Server - entry
***NPRSPL**
Network Print Server - spool file
***MSGSRV**
Original Message Server
***SQLENT**
Database Server - entry
***OBJINF**
Information about objects

***TCPSGN**
TCP Signon Server

Top

## Product ID (PRODID)

Specifies a product identifier. The identifier must be seven characters in length.

***ALL**
All product identifiers.
***character-value***
A specific product identifier.

Top

## Feature ID (FEATID)

Specifies a feature identifier.

***ALL**
All feature identifiers.
***character-value***
A specific feature identifier.

Top

## Screen name (TERM)

Specifies a terminal (screen) name.

***ALL**
All screen names.
***BLANKS**
No screen name appears.
***generic-name***

Specify the generic screen name.

***name***

A specific screen name.

Top

## Password validated (PWDVL)

Specifies whether Telnet validated the clients' encrypted password (if one was received). The system sets this value if TN5250E Clients send the encrypted password for validation. The password is checked using service functions calls. This allows the exit program to guarantee secure client sign-on process.

***ALL**

All, regardless of whether a password was received or validated.

***YES**

Client clear-text password/passphrase was validated.

***NO**

Client password/passphrase (or Kerberos ticket) was not validated or none was received.

***ENCRYPTED**

Client encrypted password/passphrase (or Kerberos ticket) was validated.

Top

## Source location (SRCLOC)

Specifies the source location for Remote Login.

***ALL**

All source locations.

***name***

Specify the name of a source location.

Top

## Source user (SRCUSR)

Specifies a source user for Remote Login.

***ALL**
All source users.
***name***
Specify the name of a source user.

Top

## Target user (TGTUSR)

Specifies a target user for remote login.

***ALL**
All target users.
***NONE**
No target users.
***name***
Specify the name of a target user.

Top

-

## Server ID for *NATIVE (SRVNTV)

Specifies the Server ID for operations on *NATIVE objects.

***ALL**
All server IDs.
***FILTFR**
Original File Transfer Function
***RMTSRV**
Remote Command/Program Call
***SQL**
Database Server - SQL access & Showcase
***RMTSQL**
Original Remote SQL Server
***NDB**
Database Server - data base access
***DBOPEN**
Open Database
***FTPSRV**
FTP Server-Incoming Request Validation
***FTPCLN**
FTP Client-Outgoing Request Validation
***TFTP**
TFTP Server Request Validation
***REXEC**
REXEC Server Request Validation
***DDM**
DDM request access
***ORDTAQ**
Original Data Queue Server
***DTAQ**
Data Queue Server
***VPRT**
Original Virtual Print Server
***FILSRV**
File Server

Top

-

## Server ID for *IFS (SRVIFS)

Specifies the Server ID for operations on *IFS objects.

***ALL**
All server IDs
***FILSRV**
File Server
***FTPSRV**
FTP Server-Incoming Request Validation
***FTPCLN**
FTP Client-Outgoing Request Validation
***TFTP**
TFTP Server Request Validation
***DDM**
DDM request access

Top

## Server ID for *LICMGT (SRVLIC)

Specifies the License Management server.

***ALL**
All license management servers.
***ORLICM**
Entry is a result of the original license management server.
***CSLICM**
Entry is a result of the central license management server.

Top

-

## Server ID for *IPIN (SRVIPIN)

Specifies server IDs that consider incoming IP addresses.

***ALL**
All server IDs.
***FTPLOG**
FTP Server Logon
***TFTP**
TFTP Server Request Validation
***REXLOG**
REXEC Server Logon
***WSG**
Users or workstations on a LAN
***TELNET**
Telnet Device Initialization
***DDM**
DDM request access
***DRDA**
DRDA Distributed Relational DB access
***FTPSRV**
FTP Server-Incoming Request Validation
***REXEC**
REXEC Server Request Validation
***SQL**
Database Server - SQL access & Showcase
***RMTSRV**
Remote Command/Program Call
***DBOPEN**
Open Database
***TCPSGN**
TCP Signon Server

Top

-

## Server ID for *FTPCLN (SRVFTP)

Specifies server IDs that handle FTP Client-Outgoing Request Validation

***ALL**
All server IDs
***FTPLOG**
FTP Server Logon
***FTPSRV**
FTP Server-Incoming Request Validation
***FTPCLN**
FTP Client-Outgoing Request Validation
***TFTP**
TFTP Server Request Validation
***REXLOG**
REXEC Server Logon
***REXEC**
REXEC Server Request Validation

Top

-

## Server ID for *SNA (SRVSNA)

Specifies server IDs that use the IBM SNA protocol.

***ALL**
All server IDs
***DDM**
DDM request access
***DRDA**
DRDA Distributed Relational DB access
***RMTSGN**
Remote Signon

Top

-

## Server ID for *DHCP (SRVDHCP)

Specifies servers that use the DHCP protocol.

***ALL**
All server IDs
***DHCPAB**
DHCP Address Binding Notify
***DHCPAR**
DHCP Address Release Notify
***DHCPRP**
DHCP Request Packet Validation

Top

-

## Client hardware address (CHADHCP)

Specifies servers that use the client hardware address.

***ALL**
All servers.
***character-value***
Specify the name of the server.

Top

-

## Server ID for *SCREEN (SRVSCR)

Specifies servers that use *SCREEN.

***ALL**
All servers
***SCRLCK**
Screen locked due to timeout.
***SCRRLS**
Screen released.
***SCREND**
Screen jobs ended when timeout passed.

Top

-

## Ouery type for *DBOPEN (DBOQRYT)

Specifies the Query type for *B DBOPEN operations

***ALL**
All query types
**NTVIO**
Native IO
**OPNQRYF**
OPNQRYF
**QUERYAPI**
Query API
**OTHRNONSQL**
Other non-SQL
**STRSQL**
Interactive STRSQL
**ODBC**
ODBC
**OTHERSQL**
Other SQL
**QSQPRCED**
QSQPRCED API (SAP)
**CLI**
SQLCLI

Top

-

## DB Operation (DBSTTO)

Specifies the DB operation.

***ALL**
All operations
**READ**
READ operations
**INSERT**
INSERT operations
**UPDATE**
UPDATE operations
**DELETE**
DELETE operations

Top

-

## Filter by time group (TIMEGRP)

Specifies a defined set of times to be included or excluded.

### Element 1: Relationship

***IN**
Include the timegroup.

***OUT**
Exclude the timegroup.

***NONE**
Do not consider timegroups.

### Element 2: Time group

***SELECT**
If running interactively, present a set of timegroups to consider.

***name***
The name of a specific timegroup.

Top

## Filter using query rules (QRY)

Specifies a named query to run.

***NONE**

Do not run a query.

***name***

Specify the name of the query to run.

Top

-

## Start log display (START)

Specifies whether to display information starting with the oldest or newest records.

***OLD**
Start with the oldest records.
***NEW**
Start with the newest records.
***DFT**
Start with whichever is specified in the default values.

Top

---

Top