iSecurity Password

User Guide
Version 18.32

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

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

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

Native IBM i (OS/400) User Interface

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

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

Conventions Used in the Document

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

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

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

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

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

STRAOD **> 81 > 32**

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

Menus

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

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

Data Entry Screens

Data entry screens include many convenient features such as:

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

The following describes the different data entry screens.

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

The following function keys may appear on data entry screens.

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

Legal Notice

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

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

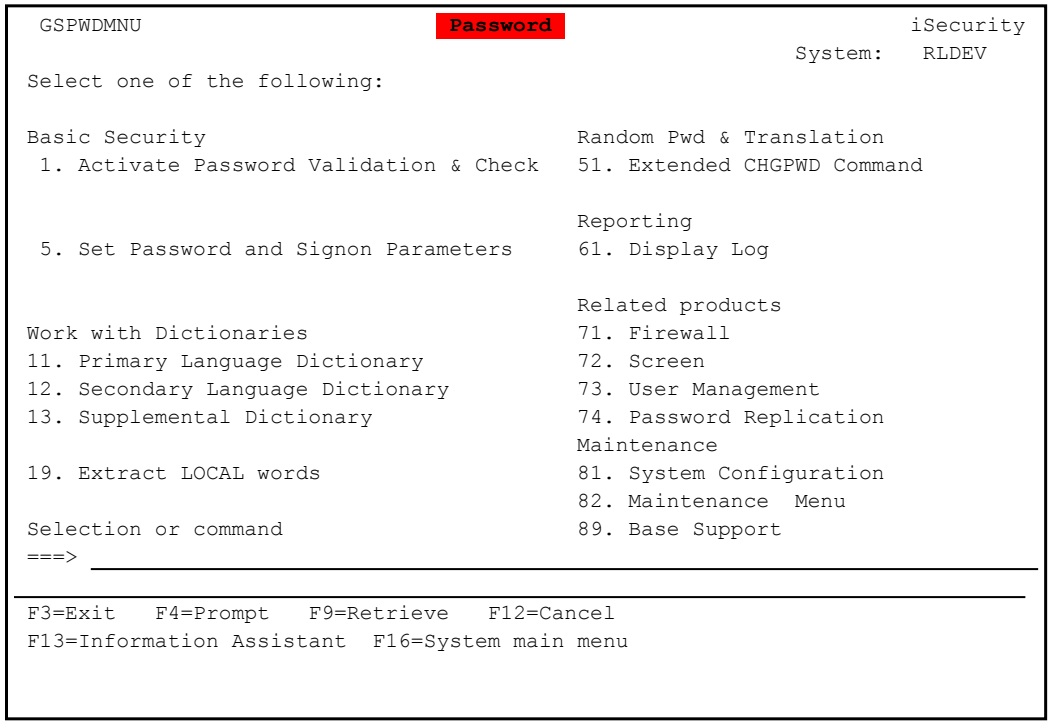
Manual Revised: Thursday, June 9, 2022

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)

Starting Password

1. Enter ***STRSEC*** in the command line in the new screen. The iSecurity screen appears.
2. Enter **1** in the command line or type ***STRPWD*** and press **Enter** twice. The Password main screen appears.



Creating Effective Passwords

Password security is effective only when password information is limited to their respective users. An effective password is one that cannot be easily guessed by an intruder or hacked using password cracking software.

Tips for creating effective passwords:

- Use a seemingly random combination of letters, numbers and punctuation marks
- Mix upper and lower case letters in your password
- Make your passwords as long as possible, at least 6 characters
- Avoid the use of repetitive characters or numerical strings
- Avoid writing down your password where somebody else can copy or find it

Avoid using the following easy-to-guess passwords:

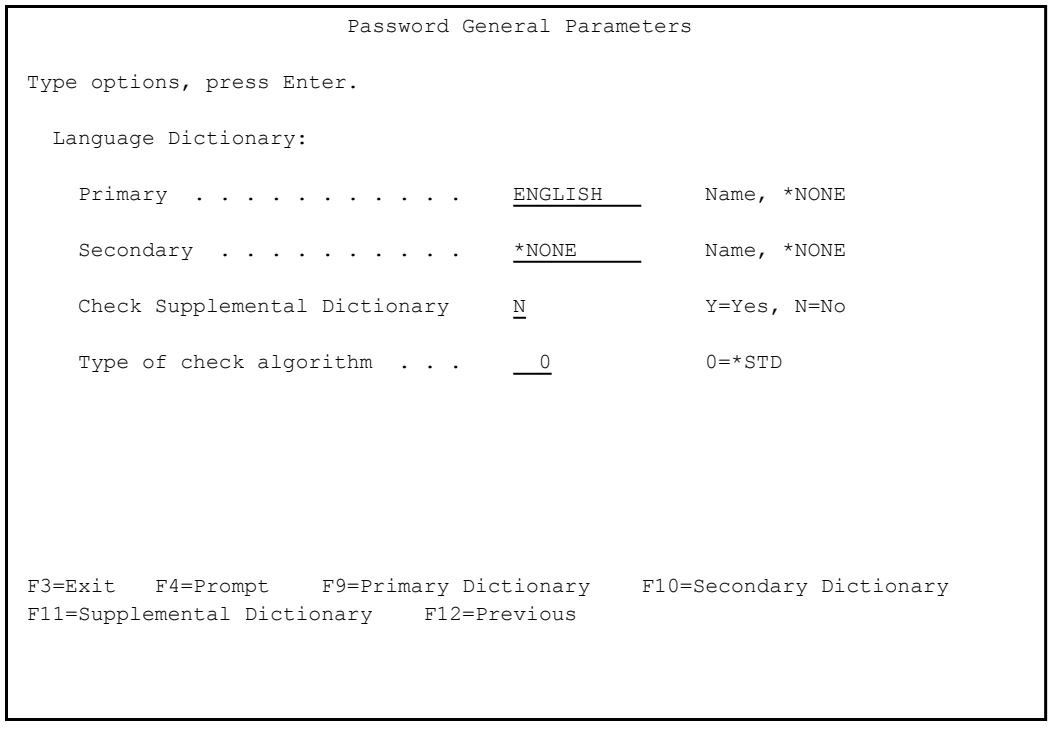
- Your user name or e-mail address
- Names of family members, friends, pets, famous people, places, companies, etc.
- Common phrases or quotations
- Dates, such as birthdays, anniversaries, holidays, hire dates, etc.
- Common numerical strings such as: ID numbers, PIN numbers, etc.
- Common keyboard patterns, such as “QWERTY”, or “ASDF”
- Abbreviations or acronyms

Selecting the Password Dictionary Language

Password validates new passwords by using up to three separate validation dictionaries simultaneously. The **primary** and **secondary** language dictionaries allow you to validate passwords in two different languages. The supplemental dictionary can be used as a special dictionary that is maintained separately from the language dictionaries. For example, you may wish to add all user names to the supplemental dictionary in order to prevent people from using their user names as passwords. You may also use the supplemental dictionary to support a third language.

By default, only the primary dictionary is enabled, and it is configured to use the English language dictionary. Perform the following steps to assign languages to the primary and secondary dictionaries.

1. Make certain that the desired dictionary language exists. The procedure for creating a new dictionary language appears in the following section.
2. Select **81 > 31** from the main menu. The **Password General Parameters** screen appears.

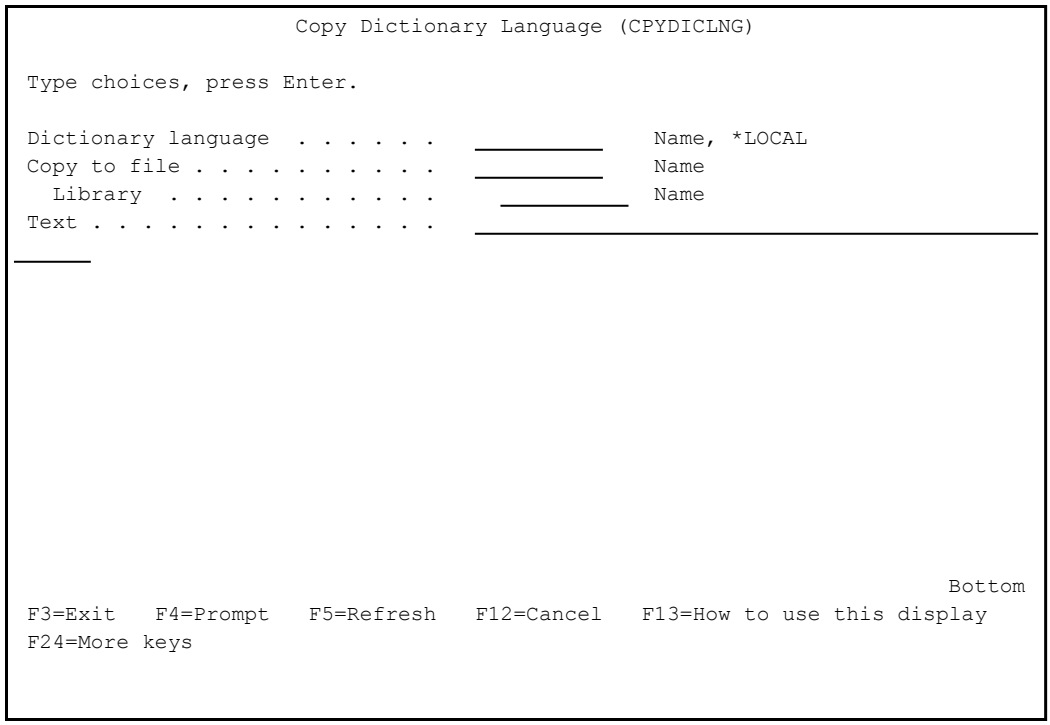


3. Type the correct name of an existing dictionary language in the **Primary** and/or **Secondary** fields. Enter ***NONE** in the **Secondary** field if you do not wish to use it.
4. If you wish to use the supplemental dictionary, type "**Y**" in the **Check Supplemental Dictionary** field. Otherwise, type "**N**".
5. In case of a special custom made algorithm, type your algorithm code as defined by Raz-Lee Security in the **Type of check algorithm** field. Otherwise type **0** for the standard definitions.
6. Press **F3** to exit and continue.

Creating New Password Dictionary Languages

Password is shipped with a default English dictionary language. Other dictionary languages may also be included, depending on your location.

You may also create your own customized dictionary languages. These languages may be assigned using the procedure described above. To create a new dictionary language, perform the following steps:

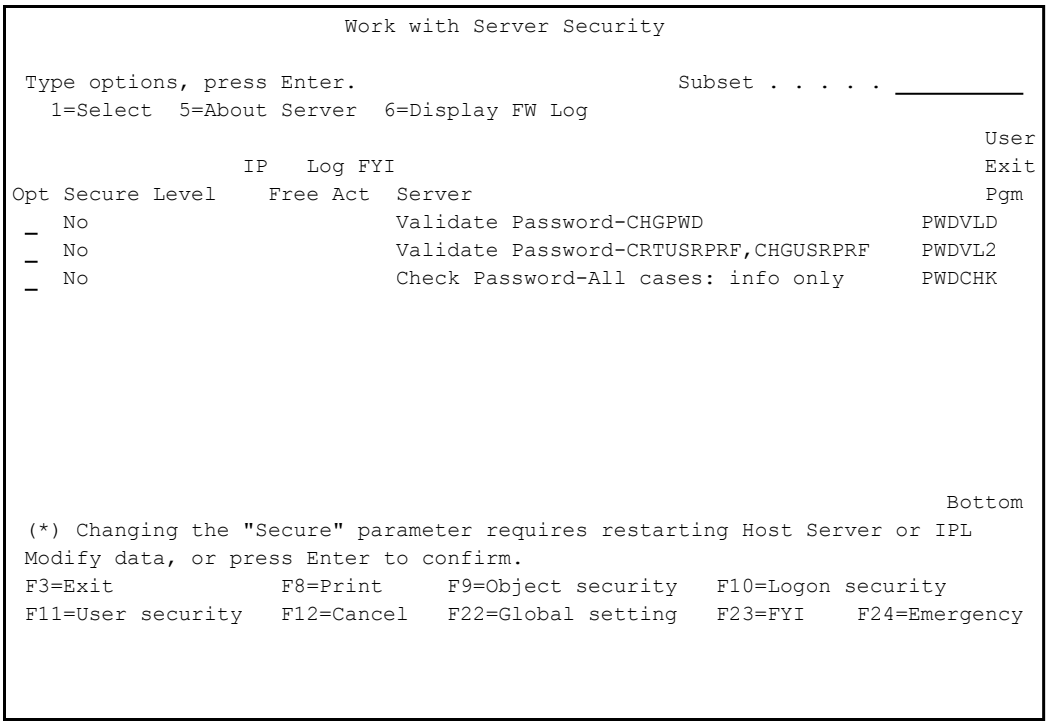


1. Select **82 > 41** from the main menu. This step copies the specified dictionary language into a temporary external file for translation.
2. Use a file editor, such as FileScope, to translate and enter data into the temporary file.
3. Select **42. Import Dictionary Language** to import the translated dictionary from the temporary file into the Password dictionary.
4. Follow the procedure in the preceding section to assign the dictionary language to either the primary or secondary dictionary.

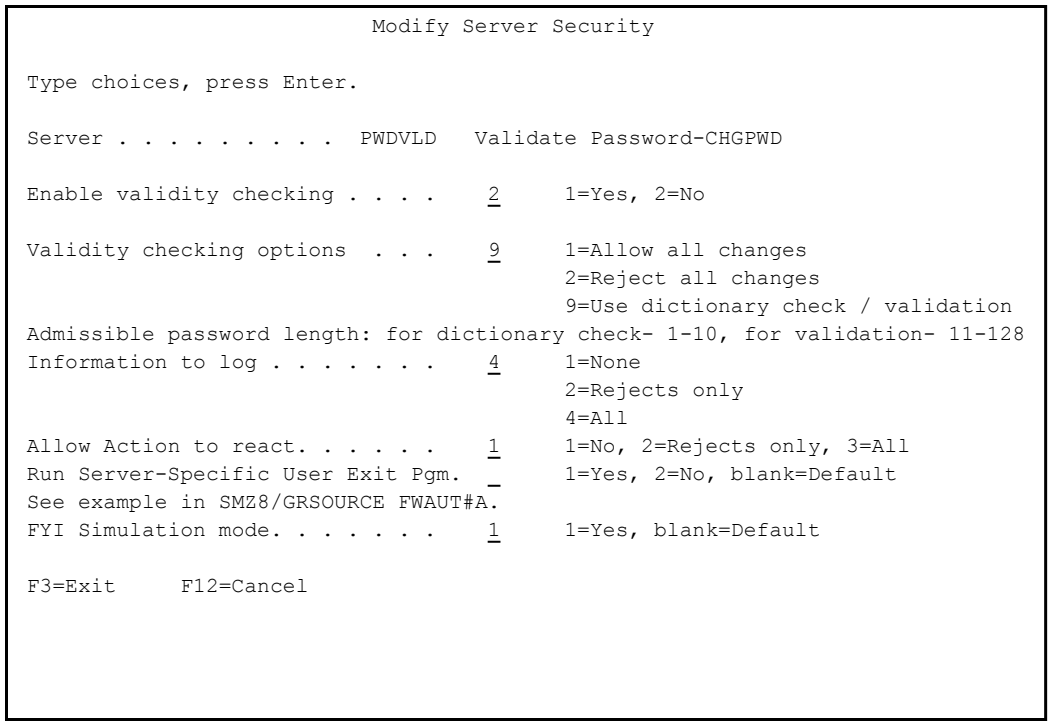
Activating Password Validation

Activate the password validation feature in order to enable dictionary checking.

1. Select **`1. Activate Password Validation`** from the Main menu. **The Work with Server Security** screen appears, showing the servers relevant to Password.



2. To view and modify information for each server, enter 1 in the **`Opt`** field in the line for that server. The **Modify Server Security** screen appears.



3. Type **1** (Yes) in the **Enable validity checking** field.
4. Type **9** (Use dictionary checking) in the **Validity checking options** field.
5. Type **4** (All) in the **Information to log** field.
6. Press **Enter** to continue.

Password validation is now active. Whenever a user attempts to change his password by using the *CHGPWD* command, Password checks to see if the proposed new password appears in any of the active language dictionaries.

Working with Password Dictionaries

All three dictionaries are fully customizable. To freely add or delete words from any active dictionary, specify it as the primary, secondary or supplemental dictionary language.

Adding Words to a Language Dictionary

1. Select one of the dictionaries from the **Work with Dictionaries** section of the main menu.

Dictionary	Description
Primary/ Secondary Language	Allows you to validate passwords in two differentlanguages.
Supplemental Dictionary	Can be used as a special dictionary that is maintainedseparatelyfromthe language dictionaries

2. Press **F6**. The **Add Word to Password Validation Dictionary** screen appears.
3. Enter the new word(s) on the **Add Word** screen and press **Enter** to continue.

```
                  Password Validation Dictionary Maintenance

Primary Password Dictionary for language:   ENGLISH
Type options, press Enter.
  4=Delete
                                          Position to  . . . . . _________

Opt Word
 _  A
 _  AARDVAR
 _  AARDWOL
 _  ABA
 _  ABACA
 _  ABACI
 _  ABACK
 _  ABACUS
 _  ABACUSE
 _  ABAFT
 _  ABALONE
 _  ABANDON

                                                                      More...
F3=Exit    F6=Add new            F12=Cancel
```

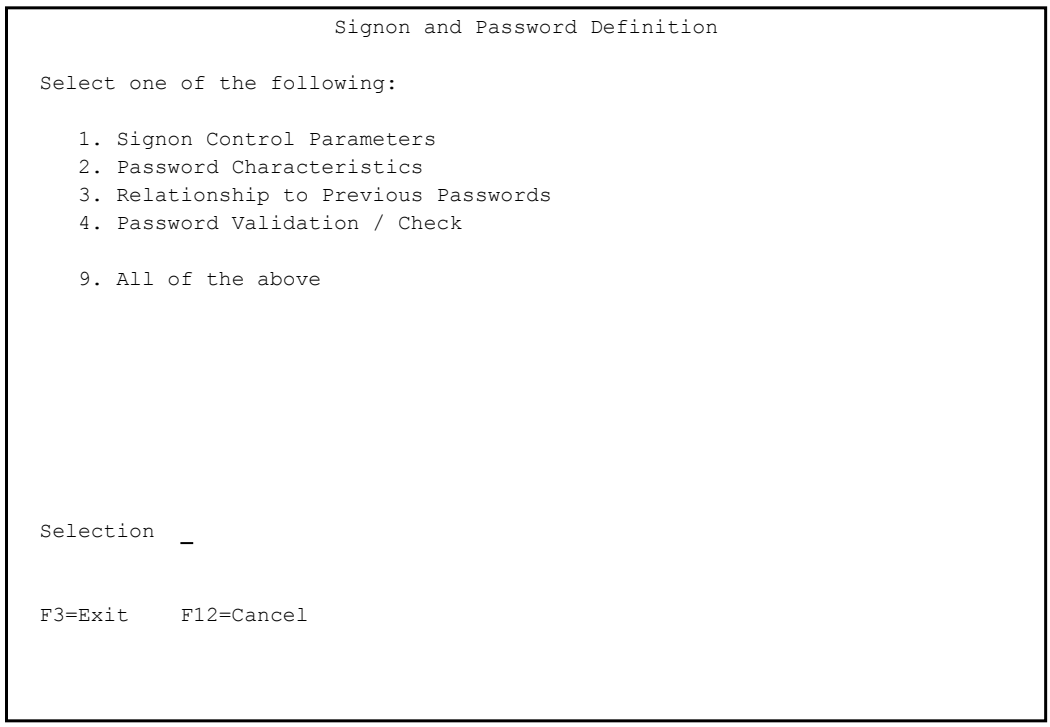
Deleting Words from a Language Dictionary

1. Select one of the dictionaries from the **Work with Dictionaries** section of the main menu.
2. Navigate to the desired word.
3. Type **4** in the space to the left of the word.
4. Press **Enter** to continue.

Working With Password and Sign-on Parameters

Passwords should conform to a number of guidelines in order to maintain a high level of system security. Password provides you with a number of tools to ensure that user passwords conform to guidelines such as:

- Limit the number of invalid sign-on attempts and determine the action to be taken if this number is exceeded
- Control the display of previous sign-on attempts
- Control which terminals the *QSECOFR* can use
- Define minimum and maximum password length
- Establish rules governing the use of different character types in passwords
- Define password expiration periods
- Establish rules governing the re-use of an old password



1. Select one of the parameter groups or select **`9. All of the above`**. You can scroll through all of the definition screens from any of the parameter groups by using the **`PgUp`** and **`PgDn`** keys.

2. Each screen displays a recommended value for the parameters. Enter the modified parameters and press **Enter** to continue, or scroll to another parameter screen.

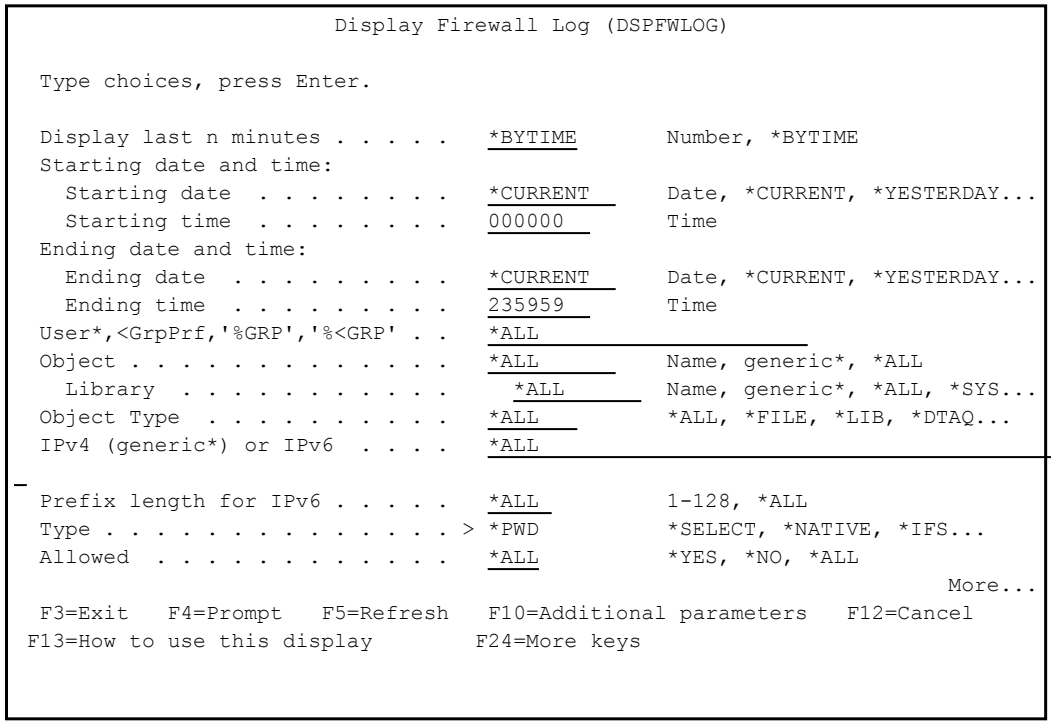
Parameter modifications take effect immediately once you press the **Enter** key.

Displaying the History Log

Password provides a detailed history log that can record all user password change attempts, both successful and unsuccessful.

To use this feature, configure the product to record password change attempts in the log. See Activating Password Validation for details. The recommended setting is **4=All**, which records all change attempts.

To display or print the history log,



1. Select **61. Display Log** from the main menu. The **Display Firewall Log** screen appears.
2. Change default parameters if necessary and press **Enter**.
3. Complete the filter criteria and press **Enter** to continue. The following table describes the selection parameters.

Option/Parameter	Description
Allowed	Password change attempt: **YES** = Password change successful **NO** = Password change rejected
Display last n minutes	Displays only transactions for the last **n** (user specified)number ofminutes. **Number** = Enter the number of minutes to display ***BYTIME** = Use the starting/ending date and time fields
Output	***** = Display log
	PRINT = Print log **OUTFILE** = Save output data as a text file
Password validated (rejected)	Filter according to the proposed new password **Name** = Specific password **Generic*** = All passwords containing the text before the * ***ALL** = All passwords
User* or %Profile	Filter according to specific user or %UserGroups