Password™

The Password Management Component of

iSecurity

User Manual
Version 16

RAZ-LEE

Copyright Notice

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

Record your Product Authorization Code Here:

Computer Model:	
Serial Number:	
Authorization Code:	

About This Manual

Who Should Read This Book

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

Product Documentation Overview

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

Printed Materials

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

Password includes a single user manual that covers the following topics:

- Introduction
- Installation
- Start-up and Initial Configuration
- Using **Password**

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

On-Line Help

System i context sensitive help is available at any time by pressing the **F1** key. A help window appears containing explanatory text that relates to the function or option currently in use.

Typography Conventions

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

Table of Contents

1

Chapter 1: Introduction to Password

Product Overview

Password security is the first line of defense in System i access security. **Password** is a general-purpose password management product that ensures user passwords cannot be easily guessed or cracked.

The product includes user-modifiable dictionaries containing thousands of common words and other text strings that are unsuitable for use as passwords. The software checks all passwords that are modified using the ***CHGPWD*** command. Users cannot assign any words contained in these dictionaries as passwords. **Password** does not perform validation on passwords assigned to users by the system administrator while creating or modifying user profiles.

Password also allows you to manage a variety of password security parameters and maintains a history log of attempts to create passwords. This log can easily be displayed or printed.

Potential intruders now have one more barrier preventing unauthorized access to your system.

Key Features

- 3 user-modifiable password validation dictionaries
- Multiple language dictionaries
- Password and sign-on parameter definition
- History log of user attempts to change passwords

Effective Passwords

Password security is useful only when password information is limited only to the relevant user. An effective password is one that cannot be easily guessed by an intruder or hacked using password cracking software.

The most effective passwords contain seemingly random series of characters, but are easy to for users to remember. If a user has to write his password down in order to remember it, somebody else can easily steal or copy it. Users should change their passwords periodically and should avoid reusing old passwords.

Password provides you with powerful tools to ensure that user passwords are always effective.

Note: Password is part of the Firewall package. No other changes have been made since v15.

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 These 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

User Interface

Password is designed with user friendliness in mind. The user interface follows standard System i CUA conventions. All product functionality is available from the product menus. Many features are accessible both via menus and by entering commands on the command line.

Menus

Product menus allow rapid 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, type the option number and press **Enter**.

The command line is available in nearly all product menus. If the command line is not available (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 filter with generic text support

The following table describes the various data entry screen options.

- 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 the **Tab** or **Shift-Tab** keys.
- 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**.

Function Keys

The following function keys may appear on data entry screens:

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

New in version 15.7

iSecurity Password dictionary supports custom, site-specific algorithms.

In addition to the primary and secondary language dictionaries, **iSecurity Password** also supports a customized dictionary designed according to the customer’s needs.

Define **iSecurity Password** to support your algorithm on the Dictionaries page in menu option **STRPWD →81 →21.**

New in version 14.5

Password reports on new exit points (QIBM_QSY_VLD_Passwrd
and QIBM_QSY_CHK_Passwrd) via product option **5. Set Password and Sign-on Parameters** which supports new operating system 6.1 system values. The first is invoked before the password is changed and the second is invoked after.

Passwords are changed by command CHGUSRPRF.

Other iSecurity Products

Compliance Evaluator enables managers to quickly check the compliance of their systems with industry and corporate policies based on customizable user-friendly reports.

Action automatically intercepts and responds to security breaches, system activity events, QHST contents, and other message queues. Inquiring messages can be automatically answered. Alerts are sent by e-mail, SMS, pagers, or the message queues. Easy-to-use Rule Wizard helps define rules and actions.

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

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

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

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

Firewall protects and secures all types of access, to and from the System i, within or outside the organization, under all types of communication protocols. Firewall manages user profile status, secures entry via predefined entry points, and profiles activity by time. Its Best Fit Algorithm decreases system burden with no security compromise.

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

View is a unique, patent-pending, field-level solution that hides sensitive fields and records from restricted users. This innovative solution hides credit card numbers, customer names, etc. Restricted users see asterisks or zeros instead of real values. View requires no modification to existing applications.

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

2

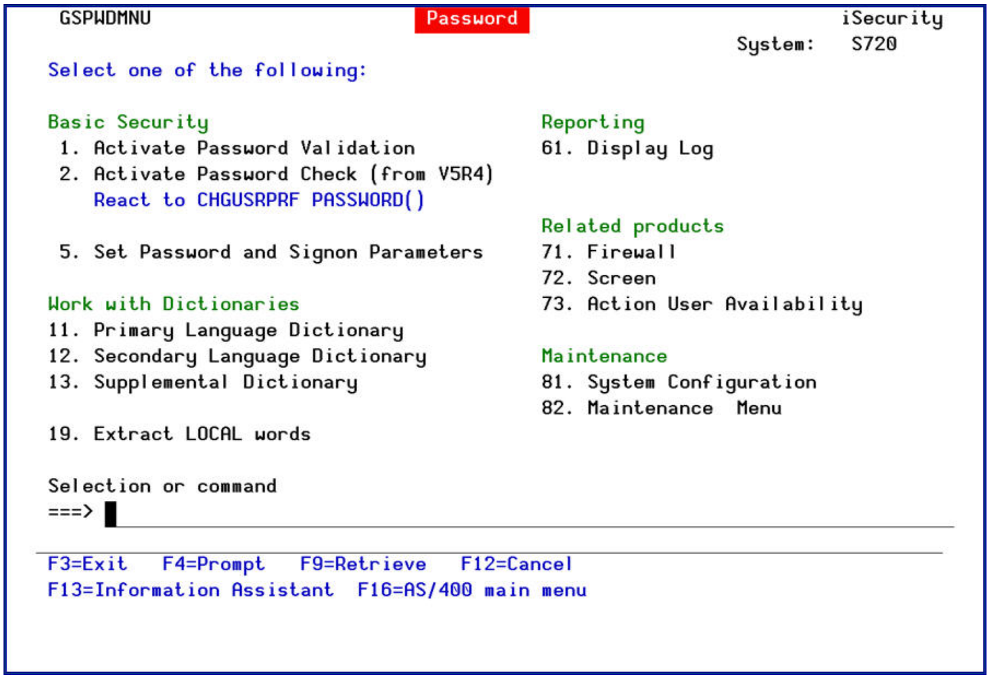
Chapter 2: Getting Started

This chapter describes the steps necessary in order to begin using **Password** effectively. These steps include the following:

- Opening Password
- Entering the Authorization Code
- Changing the iSecurity Password
- Selecting the Password Dictionary Language
- Creating New Password Dictionary Languages
- Activating Password Validation

Opening Password

1. To start **Password**, type ***STRPWD*** on the command line. The main menu appears after a few moments.



```
  GSPWDMNU                        Password                         iSecurity
                                                           System:    S720
 Select one of the following:

 Basic Security                                Reporting
  1. Activate Password Validation              61. Display Log
  2. Activate Password Check (from V5R4)
     React to CHGUSRPRF PASSWORD()
                                               Related products
  5. Set Password and Signon Parameters        71. Firewall
                                               72. Screen
 Work with Dictionaries                        73. Action User Availability
 11. Primary Language Dictionary
 12. Secondary Language Dictionary             Maintenance
 13. Supplemental Dictionary                   81. System Configuration
                                               82. Maintenance  Menu
 19. Extract LOCAL words

 Selection or command
 ===> _______________________________________________________________________

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

Password Main Menu

2. Proceed to the following steps.

Entering the Authorization Code

In order to use this product you must obtain a valid authorization code. If you did not enter the authorization code during the installation procedure, perform the following steps at this time:

1. Select **81. System Configuration** from the main menu.
2. Press **F22**.
3. Enter the authorization code in the field provided. Press **Enter** to continue.

Changing the iSecurity Password

An additional, product-specific password may be required to access certain features. The default password is ***QSECOFR***. It is highly recommended that you change this password immediately after using the product for the first time.

To change the product specific password,

1. Select **81. System Configuration** from the main menu.
2. Select **92. Modify Password** from **Global Parameters** menu.
3. Type the new password and confirmation in the spaces provided.

Modifying Operators' Authorities

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

There are three default groups:

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

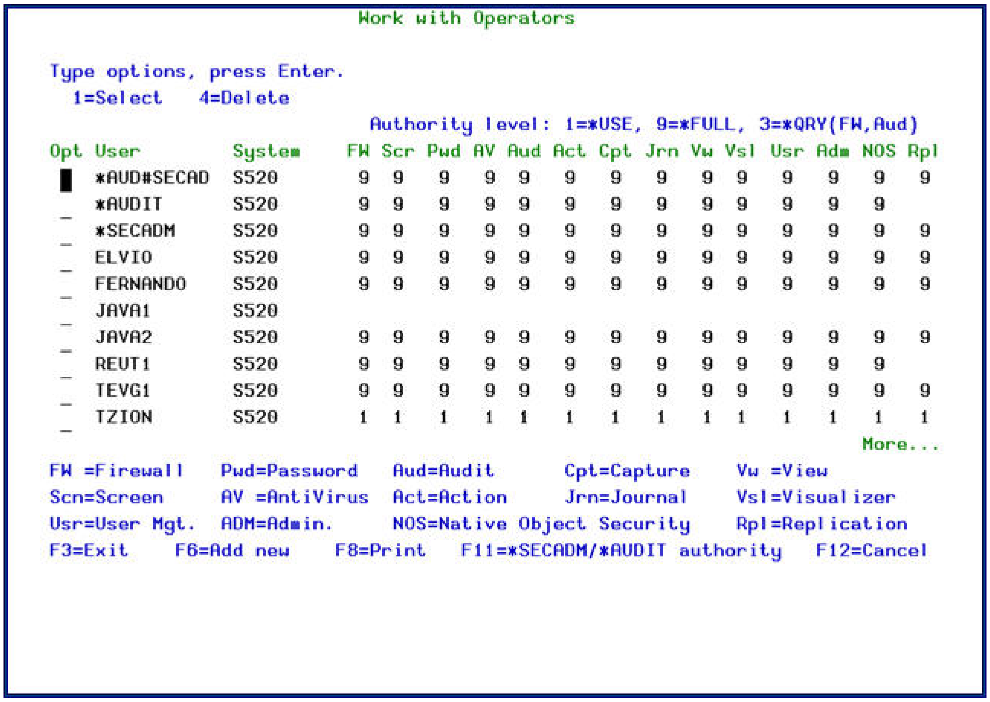
By default, all three groups use the same password (***QSECOFR***).

You may add more operators, delete them, or give them authorities and passwords according to your own judgment. You even have the option of making the new operators' definitions apply to all your systems; therefore, upon import, they will work on every system.

NOTE: *When upgrading **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 upgrading is to edit those authorities.*

To modify operators' authorities, follow this procedure.

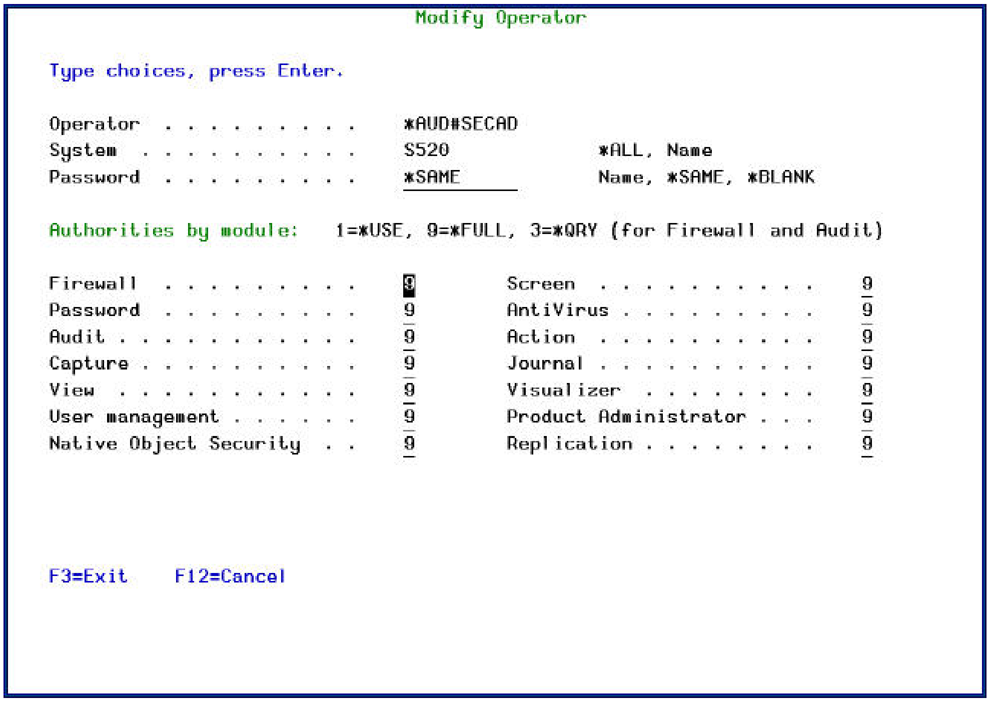
1. Select **82. Maintenance Menu** from the main menu. The **Maintenance Menu** appears.
2. Select **11. Work with Operators** from the **Maintenance Menu**. The **Work with Operators** screen appears.



```
                              Work with Operators

 Type options, press Enter.
   1=Select    4=Delete
                                 Authority level: 1=*USE, 9=*FULL, 3=*QRY(FW,Aud)
 Opt User        System     FW Scr Pwd AV Aud Act Cpt Jrn Vw Vsl Usr Adm NOS Rpl
  █  *AUD#SECAD  S520        9  9   9   9  9   9   9   9   9  9   9   9   9   9
  _  *AUDIT      S520        9  9   9   9  9   9   9   9   9  9   9   9   9
  _  *SECADM     S520        9  9   9   9  9   9   9   9   9  9   9   9   9   9
  _  ELVIO       S520        9  9   9   9  9   9   9   9   9  9   9   9   9   9
  _  FERNANDO    S520        9  9   9   9  9   9   9   9   9  9   9   9   9   9
  _  JAVA1       S520
  _  JAVA2       S520        9  9   9   9  9   9   9   9   9  9   9   9   9   9
  _  REUT1       S520        9  9   9   9  9   9   9   9   9  9   9   9   9
  _  TEVG1       S520        9  9   9   9  9   9   9   9   9  9   9   9   9   9
  _  TZION       S520        1  1   1   1  1   1   1   1   1  1   1   1   1   1
                                                                         More...
 FW =Firewall   Pwd=Password   Aud=Audit       Cpt=Capture    Vw =View
 Scn=Screen     AV =AntiVirus  Act=Action      Jrn=Journal    Vsl=Visualizer
 Usr=User Mgt.  ADM=Admin.     NOS=Native Object Security     Rpl=Replication
 F3=Exit     F6=Add new    F8=Print    F11=*SECADM/*AUDIT authority    F12=Cancel
```

Work with Operators

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



```
                                  Modify Operator

 Type choices, press Enter.

 Operator  . . . . . . . . .   *AUD#SECAD
 System  . . . . . . . . . .   S520            *ALL, Name
 Password  . . . . . . . . .   *SAME           Name, *SAME, *BLANK

 Authorities by module:   1=*USE, 9=*FULL, 3=*QRY (for Firewall and Audit)

 Firewall  . . . . . . . . .   9        Screen  . . . . . . . . . .   9
 Password  . . . . . . . . .   9        AntiVirus . . . . . . . . .   9
 Audit . . . . . . . . . . .   9        Action  . . . . . . . . . .   9
 Capture . . . . . . . . . .   9        Journal . . . . . . . . . .   9
 View  . . . . . . . . . . .   9        Visualizer  . . . . . . . .   9
 User management . . . . . .   9        Product Administrator . . .   9
 Native Object Security  . .   9        Replication . . . . . . . .   9



 F3=Exit    F12=Cancel
```

Modify Operator

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

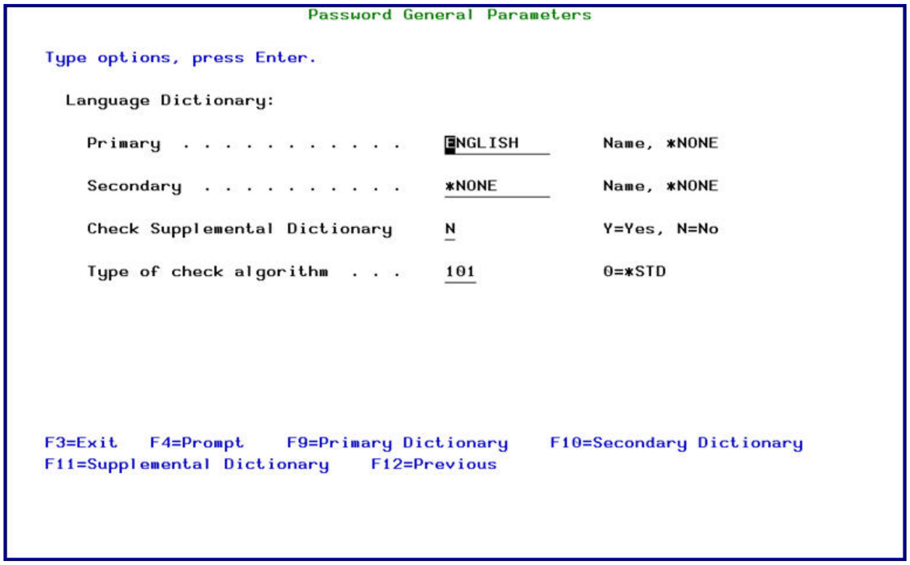
4. Set authorities and press **Enter**.

Selecting the Password Dictionary Language

Password can validate 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 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. System Configuration** from the main menu.
3. Select **21. Password Dictionaries** from the **Global Parameters** menu.



```
                          Password General Parameters

 Type options, press Enter.

   Language Dictionary:

     Primary  . . . . . . . . . . .    ENGLISH        Name, *NONE

     Secondary  . . . . . . . . . .    *NONE          Name, *NONE

     Check Supplemental Dictionary     N              Y=Yes, N=No

     Type of check algorithm  . . .    101            0=*STD




 F3=Exit   F4=Prompt   F9=Primary Dictionary   F10=Secondary Dictionary
 F11=Supplemental Dictionary   F12=Previous
```

Password General Definitions

4. 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.

5. If you wish to use the supplemental dictionary, type "**Y**" in the **Check Supplemental Dictionary** field. Otherwise, type "**N**".

6. 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.

7. Press **F3** to exit and continue.

Creating New Password Dictionaries in Additional Languages

Password is shipped with a default English dictionary. Dictionaries in other languages may also be included, according to your location and preference.

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

1. Select **82. Maintenance Menu** from the main menu.

2. Select **75. Copy Dictionary Language** from the **Maintenance** menu. This step copies the specified dictionary into a temporary external file for translation.

3. Use a file editor, such as **FileScope**, to translate and enter data into the temporary file.

4. Select **76. Import Dictionary Language** to import the translated dictionary from the temporary file into the **Password** dictionary.

5. Follow the procedure in the preceding section to assign the dictionary to either the primary or secondary dictionary.

Extracting Local Words

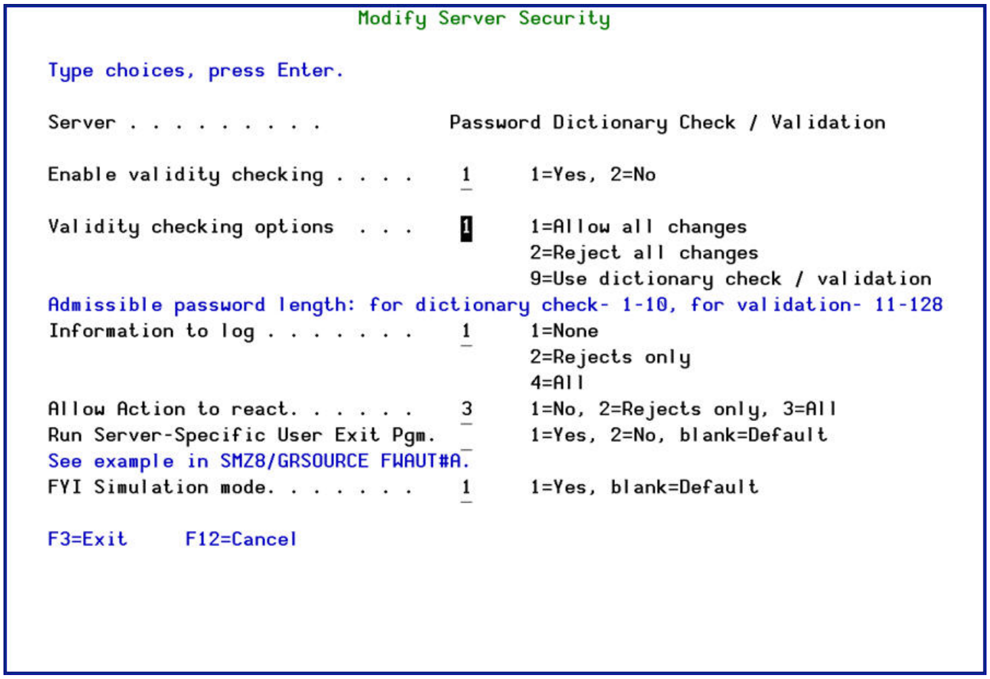
The **Extracting Local Words** option, (**19** from the main menu), builds a dictionary of words, relevant only for organizational purposes, that **Password** will not allow to be used in passwords. This dictionary is relevant only for organizational purposes. **Password** takes these words from user names, devices, and descriptive texts and places them in this dictionary. This option runs in batch.

Activating Password Validation

You must activate the password validation feature in order to enable dictionary checking. The activation procedure also allows you to specify which password change attempts will be recorded in the history log.

To activate password validation:

1. Select **1. Activate Password Validation** from the main menu. The **Modify Server Security** screen appears.



```
                              Modify Server Security

 Type choices, press Enter.

 Server . . . . . . . . .           Password Dictionary Check / Validation

 Enable validity checking . . . .    1      1=Yes, 2=No

 Validity checking options  . . .    1      1=Allow all changes
                                            2=Reject all changes
                                            9=Use dictionary check / validation
 Admissible password length: for dictionary check- 1-10, for validation- 11-128
 Information to log . . . . . . .    1      1=None
                                            2=Rejects only
                                            4=All
 Allow Action to react. . . . . .    3      1=No, 2=Rejects only, 3=All
 Run Server-Specific User Exit Pgm.  _      1=Yes, 2=No, blank=Default
 See example in SMZ8/GRSOURCE FWAUT#A.
 FYI Simulation mode. . . . . . .    1      1=Yes, blank=Default

 F3=Exit     F12=Cancel
```

Modify Server Security

2. Modify the parameters as needed and press **Enter** to confirm. **Password** validation is now active.

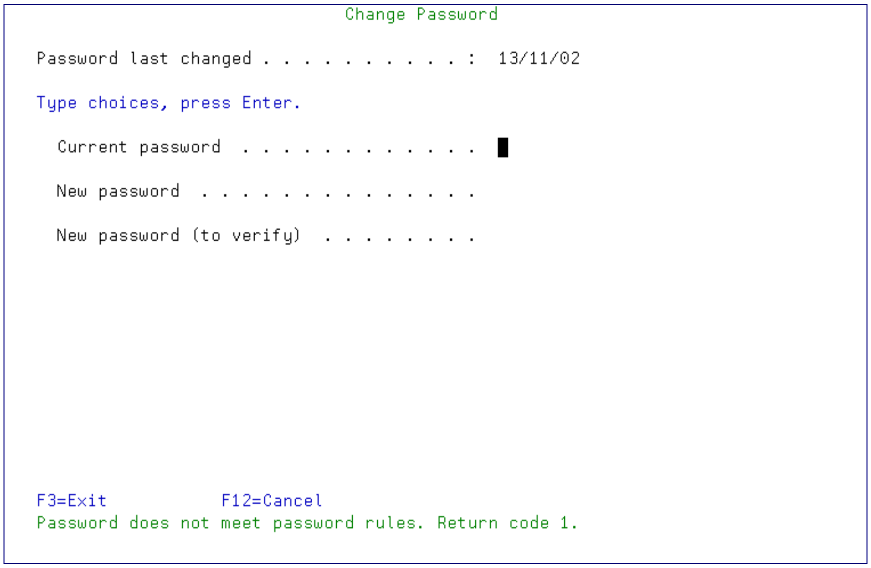
The following table explains the options contained on this screen:

Options	Description
Enable Validity Checking	**1=Yes** Enable dictionary checking **2=No** Do not use dictionary checking
Validity Checking Options	**1=Allow all changes** Allow all password changes (no dictionary checking) **2=Reject all changes** Reject all user password changes (no dictionary checking) **9=Use dictionary changes** Reject if password appears in the dictionaries
Information to Log	**None** = No transactions logging **Rejects only** = Log rejected only password change attempts **All** = Log all password change attempts
Allow Action to React	**1** =**No** (disables the **Firewall** real-time detection rules for this server) **2** = **Rejects only** (will activate **Firewall** real-time detection rules only on rejections from this server) **3** = **All** (will activate **Firewall** real-time detection rules for all accesses from this server)
Run Server Specific User Exit Pgm.	**Yes** =Run a specific exit program after passing **Firewall** rules for this server **No** = If a general exit program exists, it will not be activated for this server. **Blank** = global setting
FYI Simulation Mode	The FYI Simulation Mode allows you to simulate the application of security rules without physically rejecting any activity. All "rejected" transactions are recorded in the Activity Log as such but the activity is allowed to proceed without interruption. This feature allows you to test your rules under actual working conditions without adversely affecting user access. **1** = Enable FYI Simulation mode for this server only **Blank** = Use global parameter for all servers (System Configuration)

3

Chapter 3: Password in Action

Upon activation, **Password** works silently in the background. 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.



```
                              Change Password

 Password last changed . . . . . . . . . . :  13/11/02

 Type choices, press Enter.

   Current password  . . . . . . . . . . . .

   New password  . . . . . . . . . . . . . .

   New password (to verify)  . . . . . . . .









 F3=Exit          F12=Cancel
 Password does not meet password rules. Return code 1.
```

Change Password

If contained in the dictionaries, the software rejects the new password and the above error message appears. If logging is enabled, the attempt is recorded in the history log for review by the security officer or system administrator.

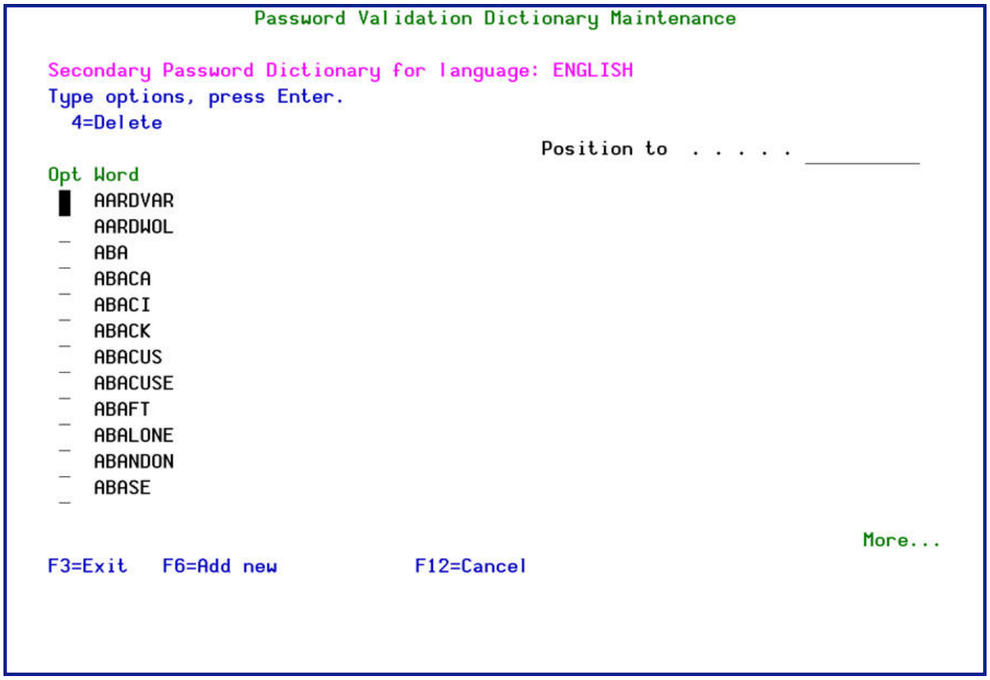
Password only monitors changes made using the ***CHGPWD*** command. Password assignment, changes made using the ***CHGUSRPRF***/***CRTUSRPRF*** commands, or changes made using third party software are not monitored or validated.

For this reason, only the system administrator and security officer should be granted access to these commands, as well as other commands that control password assignment.

Working with Password Dictionaries

All three dictionaries are fully user customizable. You can freely add or delete words from any active dictionary. In order to modify a dictionary language, you must first specify it as either the primary, secondary or supplemental dictionary language. See *Selecting the Password Dictionary Language* in *Chapter 3* for details.

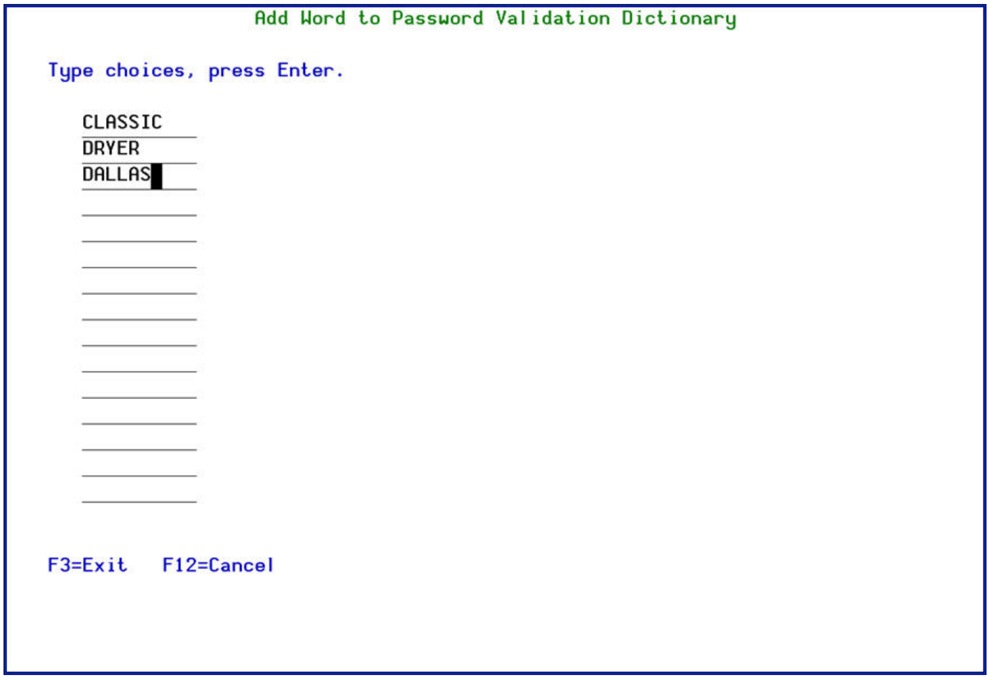
1. To add words to a language dictionary, select one of the dictionaries from the **Work with Dictionaries** section of the main menu. The **Password Validation Dictionary Maintenance** screen appears. An example is shown below, with English as the primary language.



```
                     Password Validation Dictionary Maintenance

 Secondary Password Dictionary for language: ENGLISH
 Type options, press Enter.
   4=Delete
                                           Position to  . . . . .  __________
 Opt Word
  █  AARDVAR
  _  AARDWOL
  _  ABA
  _  ABACA
  _  ABACI
  _  ABACK
  _  ABACUS
  _  ABACUSE
  _  ABAFT
  _  ABALONE
  _  ABANDON
  _  ABASE
                                                                      More...
 F3=Exit   F6=Add new           F12=Cancel
```

Password Validation Dictionary Maintenance

2. Press **F6** to access the **Add Word to Password Validation Dictionary** screen.



```
                     Add Word to Password Validation Dictionary

 Type choices, press Enter.

    CLASSIC
    DRYER
    DALLAS















 F3=Exit   F12=Cancel
```

Add Word to Password Validation Dictionary

3. Enter the new word(s) on the **Add Word to Password Validation** screen and press **Enter** to continue.

4. To **delete** a word from a language dictionary,

- Select one of the dictionaries from the **Work with Dictionaries** section of the main menu.
- Navigate to the desired word.
- Type a **4** in the space to the left of the word.

5. Press **Enter** to continue.

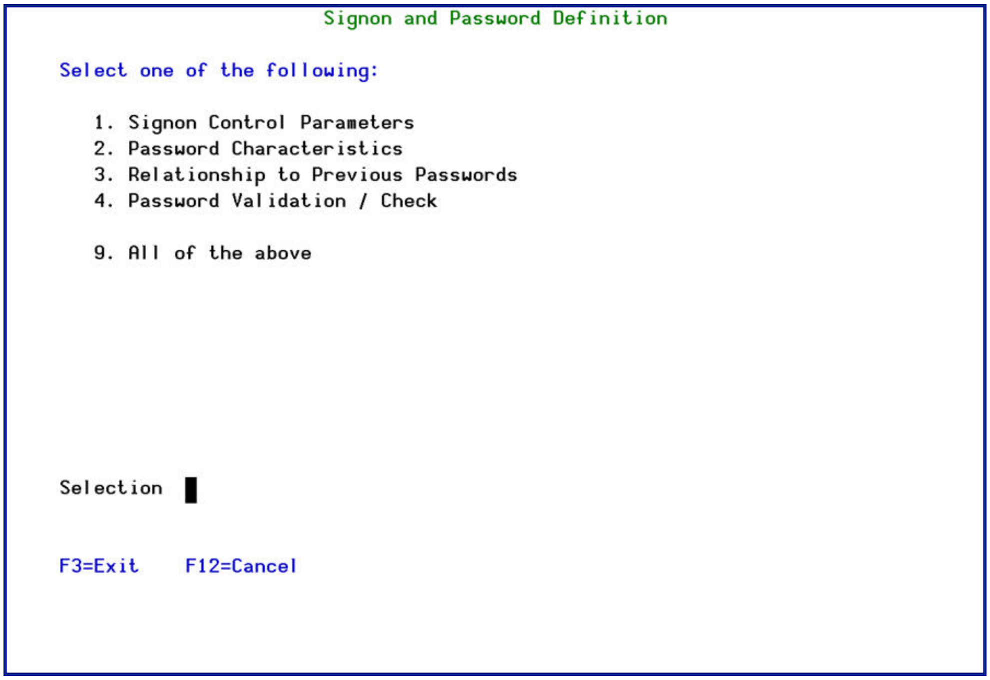
Working With Password & Sign-on Parameters

Effective password administration dictates that 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 determining the action to be taken when this number is exceeded
- Control the display of previous sign-on attempt data
- Define which terminals the ***QSECOFR*** can use
- Define minimum and maximum password length
- Determine rules governing the use of different character types in passwords
- Define password expiration periods
- Define rules specifying when or if a user can re-use an old password

To work with password and sign-on parameters:

1. Select **5. Set Password and Sign-on Parameters** from the main menu.

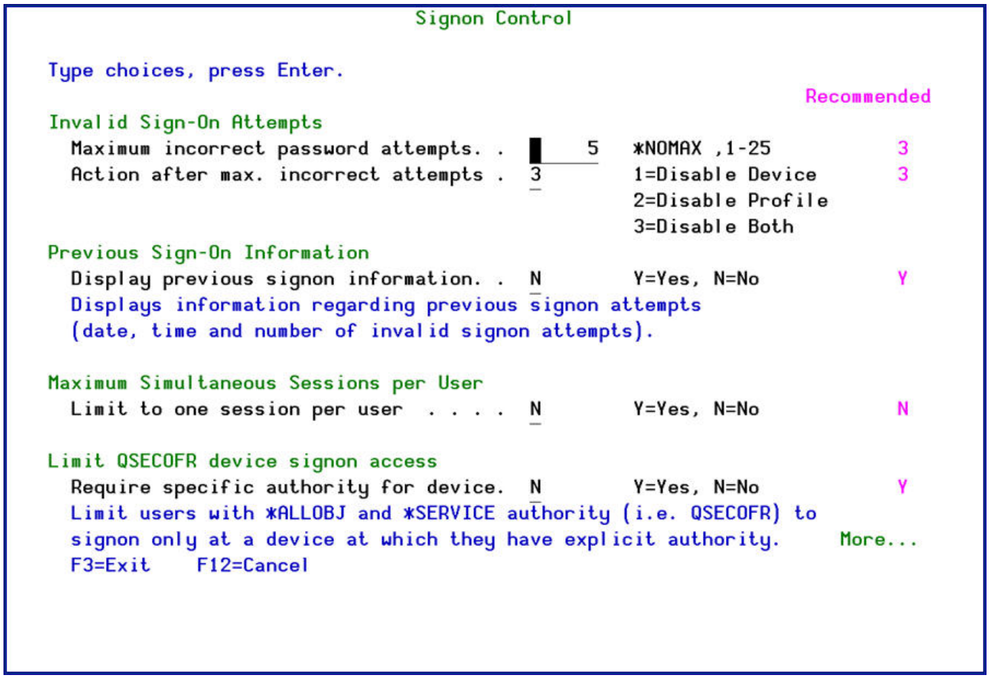


```
                     Signon and Password Definition

  Select one of the following:

     1. Signon Control Parameters
     2. Password Characteristics
     3. Relationship to Previous Passwords
     4. Password Validation / Check

     9. All of the above









  Selection



  F3=Exit    F12=Cancel
```

Sign-on and Password Definition

2. Select the one of the parameter groups or select **9. All of the above**. Scroll through all of the definition screens from any of the parameter groups by using the **PgUp** and **PgDn** keys.
3. Enter the modified parameters and press **Enter** to continue, or scroll to another parameter screen.
4. Parameter modifications take effect immediately once you press the **Enter** key.
5. Each screen displays a recommended value for the parameters. Details and options for each are discussed in detail on the following pages.

Sign-on Control

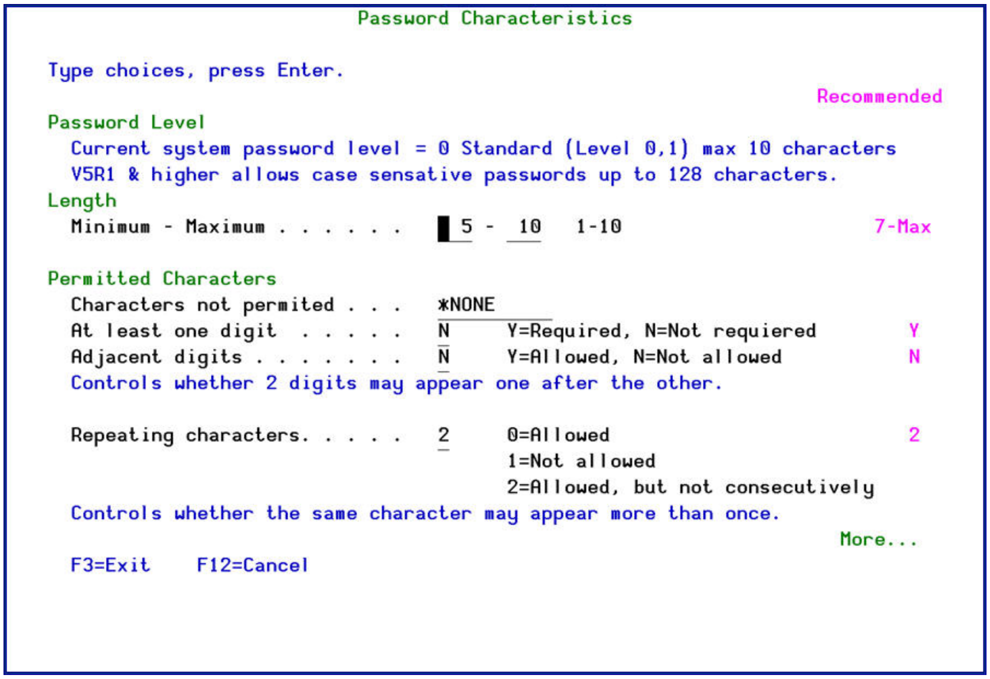


```
                                  Signon Control

 Type choices, press Enter.
                                                                      Recommended
 Invalid Sign-On Attempts
   Maximum incorrect password attempts. .     5    *NOMAX ,1-25            3
   Action after max. incorrect attempts .  3       1=Disable Device        3
                                                   2=Disable Profile
                                                   3=Disable Both
 Previous Sign-On Information
   Display previous signon information. .  N       Y=Yes, N=No             Y
   Displays information regarding previous signon attempts
   (date, time and number of invalid signon attempts).

 Maximum Simultaneous Sessions per User
   Limit to one session per user  . . . .  N       Y=Yes, N=No             N

 Limit QSECOFR device signon access
   Require specific authority for device.  N       Y=Yes, N=No             Y
   Limit users with *ALLOBJ and *SERVICE authority (i.e. QSECOFR) to
   signon only at a device at which they have explicit authority.     More...
   F3=Exit     F12=Cancel
```

Sign-on Control

Option	Description
Invalid Sign-on Attempts	Prevents unauthorized users from trying to guess a password by limiting unsuccessful sign-on attempts
Maximum incorrect attempts	***NOMAX** = Unlimited invalid attempts Number between 1-25
Action after maximum attempts	**1**=Disable sign-on device **2**=Disable user profile **3**=Disable both sign-on device and user profile
Previous Sign-on Information	Prevents unauthorized individuals from viewing a user's previous sign-on parameters
Display previous sign-on information	**Y**=Display previous sign-on information **N**=Do not display previous sign-on information
Maximum Simultaneous Sessions	Limits users to only one simultaneous session
Limit to one session per user	**Y**=Users may have only 1 active session **N**=Users may have multiple active sessions
Limit QSECOFR	Prevents security officers from using production terminals and accessing data that they are not authorized to view
Require device authority	**Y**=May only sign-on at a terminal where he has authority **N**=May sign on at any terminal

Password Characteristics

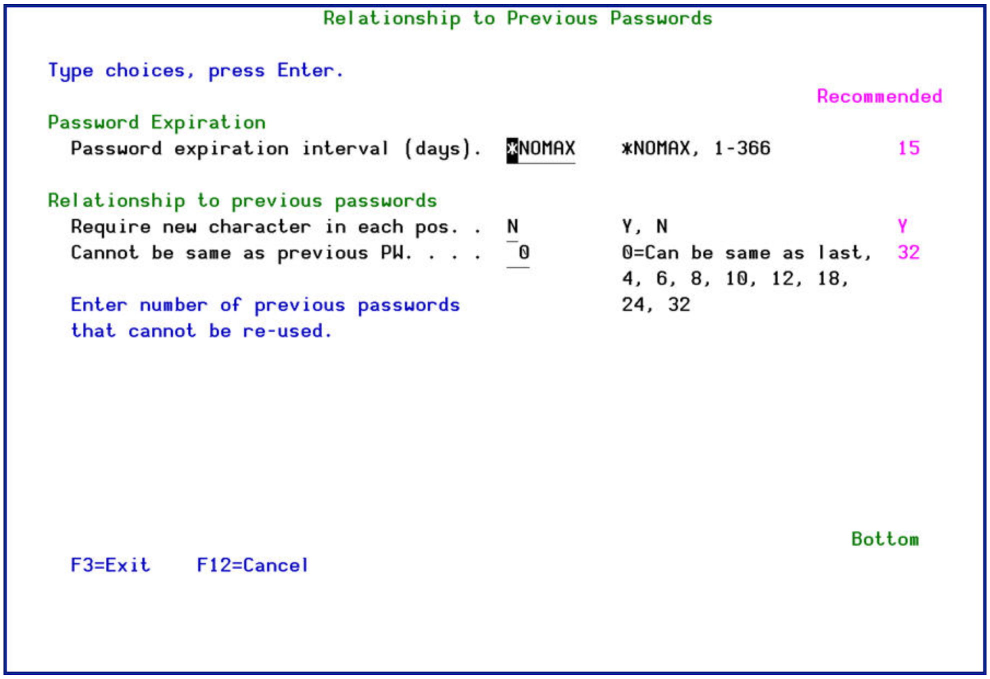


```
                              Password Characteristics

  Type choices, press Enter.
                                                                   Recommended
  Password Level
    Current system password level = 0 Standard (Level 0,1) max 10 characters
    V5R1 & higher allows case sensative passwords up to 128 characters.
  Length
    Minimum - Maximum . . . . . .   5 -  10   1-10                     7-Max

  Permitted Characters
    Characters not permited . . .   *NONE
    At least one digit  . . . . .   N     Y=Required, N=Not requiered      Y
    Adjacent digits . . . . . . .   N     Y=Allowed, N=Not allowed         N
    Controls whether 2 digits may appear one after the other.

    Repeating characters. . . . .   2     0=Allowed                        2
                                          1=Not allowed
                                          2=Allowed, but not consecutively
    Controls whether the same character may appear more than once.
                                                                   More...
    F3=Exit    F12=Cancel
```

Password Characteristics

Option	Description
Length	Minimum and maximum password length
Minimum, Maximum	Between 1 and 10 characters
Permitted Characters	Controlling specific characters and character patterns helps prevent easily guessed passwords
Characters not permitted	List characters that cannot be used in passwords ***NONE**=no character restrictions
At least on digit	**Y**=Password must contain at least one number **N**=Numbers not required
Adjacent digits	**Y**=Two or more numbers may appear next to each other **N**=Numbers may not appear next to each other
Repeating characters	**0**=Password may contain the same character more than once **1**=Password may not contain the same character more than once **2**=Password may contain the same character, but not consecutively

Relationships to Previous Passwords

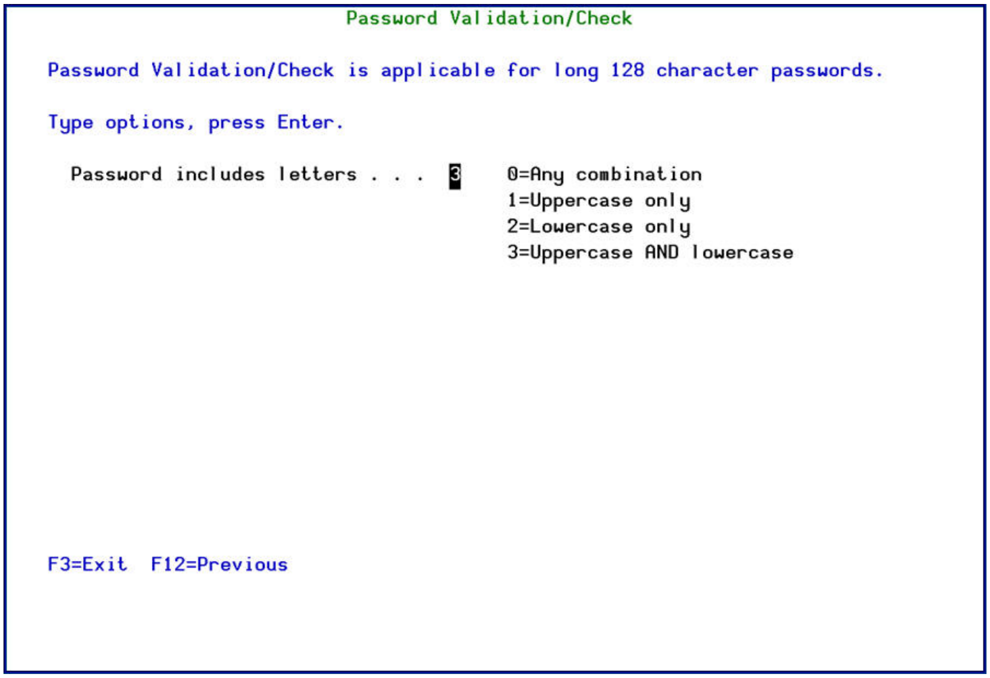


```
                    Relationship to Previous Passwords

 Type choices, press Enter.
                                                            Recommended
 Password Expiration
   Password expiration interval (days).  *NOMAX    *NOMAX, 1-366        15

 Relationship to previous passwords
   Require new character in each pos. .  N         Y, N                 Y
   Cannot be same as previous PW. . . .  0         0=Can be same as last, 32
                                                   4, 6, 8, 10, 12, 18,
   Enter number of previous passwords              24, 32
   that cannot be re-used.







                                                                  Bottom
   F3=Exit    F12=Cancel
```

Relationships to Previous Passwords

Option	Description
Password Expiration	Requires users to periodically change passwords
Expiration Interval	***NOMAX**=Users not required to change passwords **1-366**=Number of days after which users must change passwords
Relationship to Previous Passwords	Controls whether a user can reuse all or part of a previous password Prevents users from using similar passwords
Require new character in each position	**Y**=Each character of a new password must be different from the previous **N**=No restrictions on character positions
Cannot be same as previous password	User may reuse a password after the specified number of password changes: 4,6,8,10,12,18,24,32 **0**=User may reuse passwords at will

Password Validation / Check



```
                                Password Validation/Check

 Password Validation/Check is applicable for long 128 character passwords.

 Type options, press Enter.

   Password includes letters . . . 3    0=Any combination
                                        1=Uppercase only
                                        2=Lowercase only
                                        3=Uppercase AND lowercase










 F3=Exit  F12=Previous
```

Password Validation / Check

Option	Description
Password includes letters	0=Any combination of Uppercase and/or Lowercase 1=Uppercase only 2=Lowercase only 3=Uppercase AND Lowercase

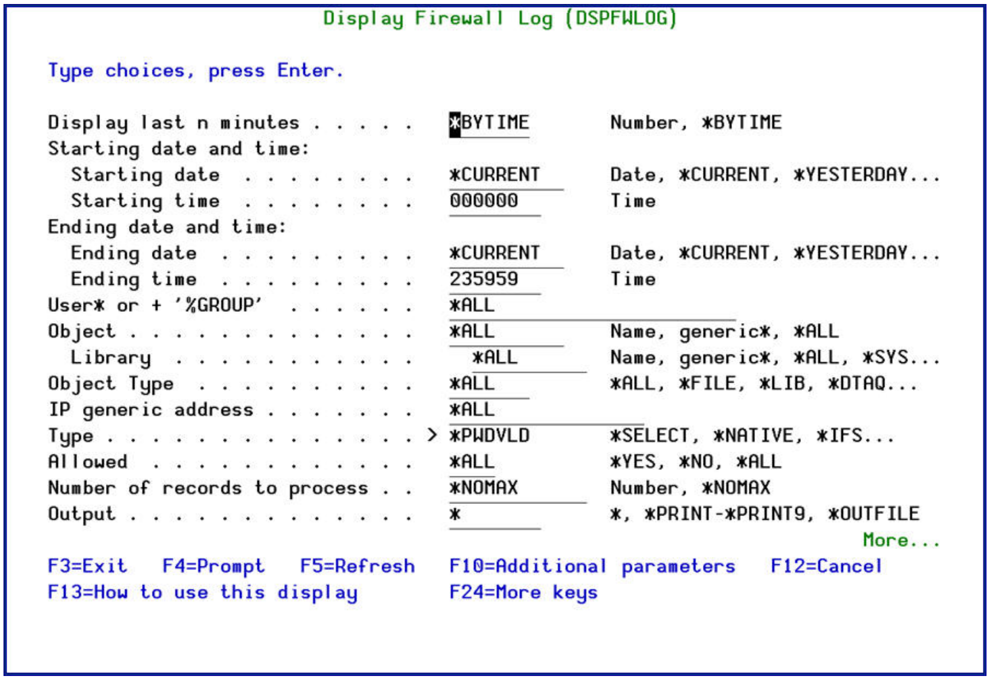
Using the History Log

An important part of effective password administration is a periodic examination of user password change attempts. **Password** provides a detailed history log that can record all user password change attempts, both successful and unsuccessful.

In order to record the use of the history log feature, it is necessary to configure the product to record password change attempts in the log. *See Chapter 3* for details. The recommend 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 Log** 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* or + '%GROUP'  . . . . . .   *ALL
 Object . . . . . . . . . . . . .   *ALL          Name, generic*, *ALL
   Library  . . . . . . . . . . .     *ALL        Name, generic*, *ALL, *SYS...
 Object Type  . . . . . . . . . .   *ALL          *ALL, *FILE, *LIB, *DTAQ...
 IP generic address . . . . . . .   *ALL
 Type . . . . . . . . . . . . . . > *PWDVLD       *SELECT, *NATIVE, *IFS...
 Allowed  . . . . . . . . . . . .   *ALL          *YES, *NO, *ALL
 Number of records to process . .   *NOMAX        Number, *NOMAX
 Output . . . . . . . . . . . . .   *             *, *PRINT-*PRINT9, *OUTFILE
                                                                       More...
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys
```

Display Firewall Log

2. Complete the filter criteria and press **Enter** to continue. The following table describes the selection parameters.

Option	Parameters
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 of minutes. **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 % User Groups

4

Chapter 4: Additional Settings

Integration with Other iSecurity Modules

Password is intended for integration with other **iSecurity** modules, such as **Firewall**, **Screen**, and **Action**. The following table describes access to these modules.

Module	Access
Firewall	**Maintenance Menu**, options **21** and **22** Main menu, option **71**
Action	Main menu, option **73**
Screen	Main menu, option **72** **Maintenance Menu**, option **31**

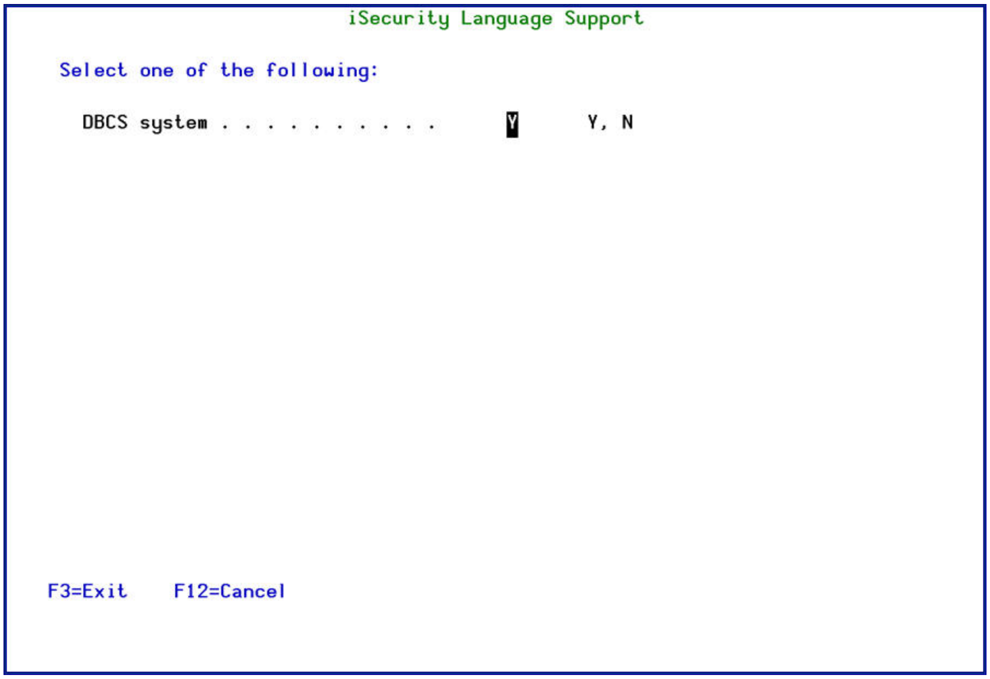
For descriptions and procedures regarding those features, see the product-specific manuals.

Language Support

Double-Byte Character Set (DBCS) is a set of characters in which each character is represented by two bytes. These character sets are commonly used by national languages such as Japanese and Chinese, which have more symbols than can be represented by a single byte.

There are two options: the default setting of '**N**'(does not support DBCS), and '**Y**' (supports DBCS). Choose an option according to your national language.

1. To work with iSecurity Language Support, select option **81. System Configuration**, then option **91. Language Support** from the **iSecurity (part I) Global Parameters** screen. The **iSecurity Language Support** screen appears.
2. Set your desired parameter and press **Enter**.



```
                         iSecurity Language Support

  Select one of the following:

    DBCS system . . . . . . . . . .       Y       Y, N









 F3=Exit    F12=Cancel
```

iSecurity Language Support