# User Guide

## NetIQ® Security Solutions for iSeries - PSPasswordManager™

**September 3, 2008**

# Contents

# About This Book and the Library

The user guide provides conceptual information about the NetIQ Security Solutions for iSeries - PSPasswordManager feature (PSPasswordManager). This book defines terminology and various related concepts.

## Intended Audience

This book provides information for individuals responsible for understanding PSPasswordManager concepts.

## Other Information in the Library

The library provides the following information resources:

**Trial Guide**
Provides general information about the product and guides you through the trial and evaluation process.

**Installation Guide**
Provides detailed planning and installation information.

**User Guides**
Provides conceptual information about the NetIQ Security Solutions for iSeries product. These books also provide an overview of the user interfaces and the Help. The following user guides are available:

- NetIQ Security Solutions for iSeries - PSSecure
- NetIQ Security Solutions for iSeries - Remote Request Management
- NetIQ Security Solutions for iSeries - PSDetect
- NetIQ Security Solutions for iSeries - PSAudit
- NetIQ Security Solutions for iSeries - Privilege Manager

**Help**
Provides definitions for each field and each window.

# Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

| Convention | Use |
|---|---|
| **Bold** | • Window and menu items<br>• Technical terms, when introduced |
| *Italics* | • Book and CD-ROM titles<br>• Variable names and values<br>• Emphasized words |
| `Fixed Font` | • File and folder names<br>• Commands and code examples<br>• Text you must type<br>• Text (output) displayed in the command-line interface |
| Brackets, such as [*value*] | • Optional parameters of a command |
| Braces, such as {*value*} | • Required parameters of a command |
| Logical OR, such as *value1* \| *value2* | • Exclusive parameters. Choose one parameter. |

# About NetIQ Corporation

NetIQ Corporation, an Attachmate business, is a leading provider of comprehensive systems and security management solutions that help enterprises maximize IT service delivery and efficiency. With more than 12,000 customers worldwide, NetIQ solutions yield measurable business value and results that dynamic organizations demand. Best-of-breed solutions from NetIQ Corporation help IT organizations deliver critical business services, mitigate operational risk, and document policy compliance. The company's portfolio of award-winning management solutions includes IT Process Automation, Systems Management, Security Management, Configuration Control and Enterprise Administration. For more information, please visit www.netiq.com

## Contacting NetIQ Corporation

Please contact us with your questions and comments. We look forward to hearing from you. For support around the world, please contact your local partner. For a complete list of our partners, please see our Web site. If you cannot contact your partner, please contact our Technical Support team.

| | |
|---|---|
| **Telephone:** | 713-418-5000<br>888-323-6768 (only in the United States and Canada) |
| **Sales Email:** | info@netiq.com |
| **Support:** | www.netiq.com/support |
| **Web Site:** | www.netiq.com |

# Chapter 1
# Introduction

In addition to using predefined word lists, PSPasswordManager checks for compliance with iSeries password composition rules. This capability provides greater control over how users create or change their own passwords.

The exit point program for the CHGPWD function prevents the use of weak passwords. These features make PSPasswordManager an indispensable tool for iSeries Security Administrators.

## Weak and Strong Passwords

What is a weak password? Essentially, a weak password is one that can be identified by either a password cracker program or common sense attacks—like using one's family member names, college alma maters, and so on.

What makes a strong password? A strong password is one that is not easily guessed. With PSPwdMgr, you can determine in minutes if users are employing strong passwords and ensure password policies are implemented on a continuing basis.

**To create a strong password:**

1. Use a random combination of characters, numbers and, if possible, symbols. ***The best password is one that is totally random to everyone else but the user.***
    - Do not use words found in dictionaries of any language.
    - Do not use abbreviations.
    - Do not use proper names.
    - Do not use keyboard patterns (i.e. QWERTY).
    - Do not use scientific terms (Astronomy, Biology, etc.) Cartoons, Biblical terms, Movies, Myths, Number Patterns (i.e. primes 135711), Short Phrases (i.e. ILUVYOU), Places, Science Fiction, Shakespeare, Songs, Sports, etc.
    - Do not use a password that matches a userid.
2. Avoid the following algorithms which are coded into password cracker programs. Do not rely on these manipulations of common words to create a strong password. You can configure PSPwdMgr to check for all of the following:
    - Adding numeric suffixes to words.
    - Removing embedded vowels from words.
    - Reversing words.
    - Substituting "1"s for "I"s, "0"s for "O"s, "2"s for "Z"s, "5"s for "S"s - and vice versa.
    - Using dates (i.e. birthdays, anniversaries, etc.).
    - Using PIN (4 digit) numbers.
    - Using "Line-of-sight" words. For example, "Sony" if you are using a Sony monitor.
3. Change passwords often. The more frequently passwords are changed, the less vulnerable they are to attack.

PSPassword Manager, the first iSeries password checking tool, has the following capabilities:

- Uses a default dictionary containing over 124,000 words to scan one's iSeries - quickly checking for weak or easily identified passwords.
- Provides the capability to take increasingly strong action against users who do not change their weak password.
- Sends users notification via their message queue informing them that they have a weak password.
- Disables users to force them to change their password at next signon.
- Changes users' passwords to *NONE - not allowing them to signon until they contact the Security Administrator.
- Keeps a running total of the number of times users have been identified with weak passwords.
- Maintains a record of every user's previous 32 passwords. When a user forgets their password and request that the password be reset, the Help Desk or Security Administrator can verify the request is from a valid users by having the user provide an old password.

# Chapter 2
# Product Access

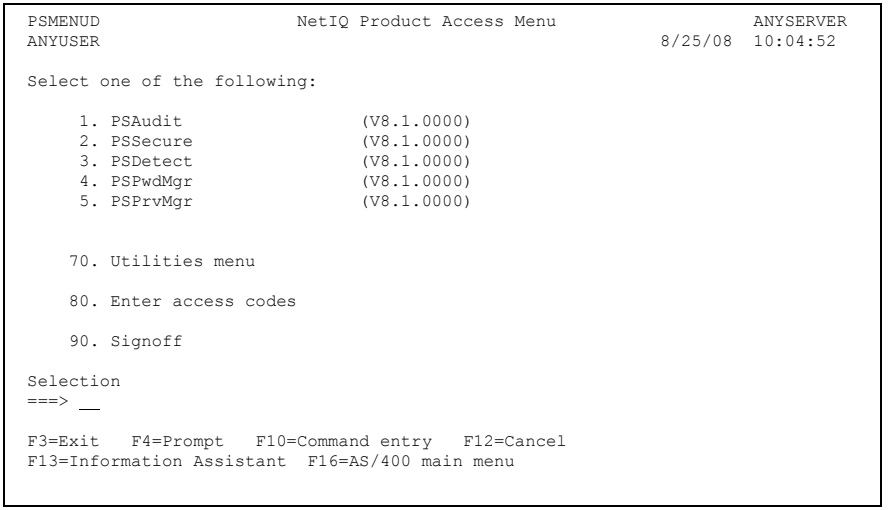
PSPasswordManager has a set of tools aimed at monitoring your system for weak passwords. A weak password is a password that is easily guessed; either because it is an everyday word, a name, or an easy keyboard combination like QWERTY.

You must have the *ALLOBJ and *SECADM special authorities and enter your password to run this program.

As a guard against misuse, a message is sent to PSDetect (if present) the first time you run this program in a session. You must re-enter the password every time you use this program. If the password entered is incorrect another message is sent to PSDetect.

**To access PSPasswordManager:**

1. On the iSeries Main Menu command entry line, type **PSMENU**. Press **ENTER**. The PSMENU command is installed in library QGPL.




The following function keys are available from the NetIQ Product Access Menu:

**F3=Exit**

Exits the NetIQ Product Access Menu and returns you to the iSeries Main Menu.

**F4=Prompt**

Provides assistance on entering or selecting a command.

**F10=Command Entry**

Provides access to the command line entry program. To run a command, type the command and press **ENTER**. For assistance in selecting a command, press **F4** (Prompt) without typing anything. When entering a command, type the command and then press **F4**.

**F12=Cancel**

Cancels the present screen and returns you to the iSeries Main Menu.

**F13=Information Assistant**

Displays the Information Assistant menu. This screen shows several types of assistance that are available. Press this key to access more information about the iSeries system, such as:

- What's new for this release of the iSeries systems.
- What new enhancements and functions will be available for the next release.
- How to comment on information.
- Where to look for iSeries information in books online.

2. Select Option 4 (PSPwdMgr) and press **ENTER**.

```
PM7000           PentaSafe Password Manager (PSPWDM)
                                                        System : ANYSERVER


               This program deals with sensitive matters and
               requires that you have Security Officer type
               authority on this installation.

               Any use of this program will result in an Alert
               message being sent to PSDetect, if installed.


               Please enter your password:









F3=Exit
```

3. In the **Please enter your password** field, type the password for that user profile, and press **ENTER**. You must re-enter the password every time you use this program. If the password entered is incorrect a message is sent to PSDetect (if present).

```
PM7001               PentaSafe Password Manager Menu
                                                        System : ANYSERVER
Select one of the following:

     1. Work with users with weak passwords

     2. Produce report on users with weak passwords

     3. Check if a user has given a valid old password

     4. Work with wordlists for weak password checking

     5. Customize messages to send to users







Selection
===>
F3=Exit   F9=Command line   F10=Display job log   F12=Cancel
```

The following function keys are available on the PSPasswordManager Menu:

**F3=Exit**
Press F3 to exit Password Manager.

**F9=Command line**
A command line popup window is displayed and lets you execute i5/OS commands. You will run with the authority of your user profile.

**F10=Display job log**
Displays the job log for the current job. Diagnostic messages can be examined. Press F10 again to see more details.

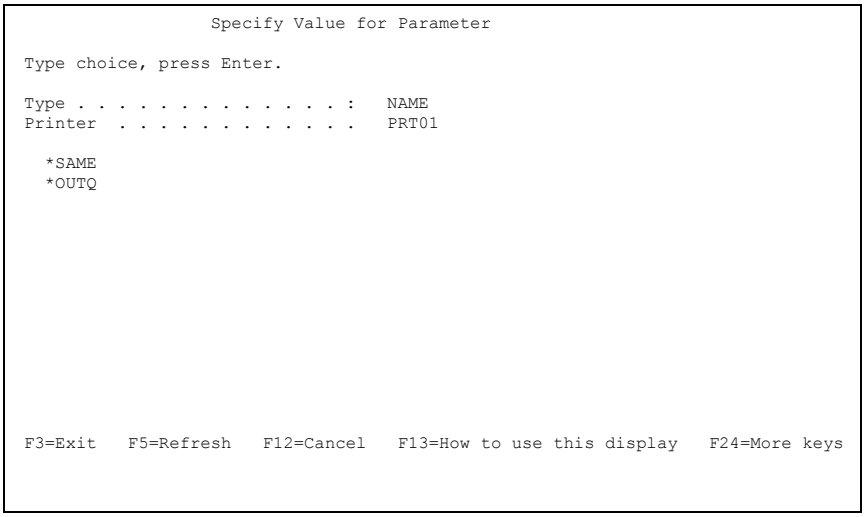
**F12=Cancel**
Returns you to the PSPasswordManager entry screen.

# Generic Prompting Screen

The generic prompting screen is used to display a list of valid values or options for the parameter or field being prompted. In most cases when **F4** (Prompt) is invoked, the screen is displayed.

**To access the generic prompting screen:**

1. From any PSPasswordManager screen, press **F4** (Prompt).




2. On the **Generic user profile** entry field, type the name you want to use, and press **ENTER**. You will be returned to the previous screen.

# Accessing Help

Help is available for every screen and for many fields. The F1=Help function key does not display on any screen. This section tells you how to access PSPasswordManager's help features.

**To get help on a field:**

1. Place the cursor on a field. Press **F1** (Help). The help screen for that field is displayed.
2. Press **F3** (Exit help) to return to the previous screen.

**To get general help:**

1. Place the cursor outside of a field, or on the screen title and press **F1** (Help). General help information for all fields is displayed.
2. Press **F3** (Exit help) to return to the previous screen. The following function keys are available from the help screen:

   **F2=FAQ**
   Shows a list of Frequently Asked Questions with a short answer to each.

   **F3=Exit help**
   Exits the help screen and takes you back to the previous screen.

   **F10=Move to top**
   Returns you to the first help page on the current topic.

   **F12=Cancel**
   Return to the previous screen.

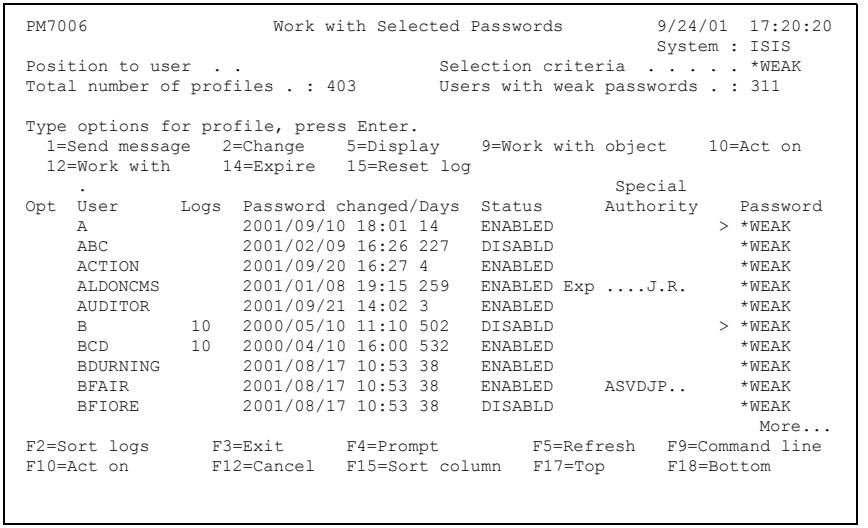
# Chapter 3
# Using PSPasswordManager

## Work with Selected Passwords

The Work with Selected Passwords option, gives security administrators the ability to monitor users with weak passwords. You can take corrective actions as needed to secure system resources that are accessed with those passwords.

**To work with selected profiles:**

1. On the PSPasswordManager main menu, select Option 1 (Work with users with weak passwords) and press **ENTER**.




2. On the **Position to user** entry field, type a name or name pattern to locate a user profile.

3. On the **Selection criteria** entry field, type one of the following values:

| | |
|---|---|
| *WEAK | Lists user profiles with passwords that are considered weak. |
| *SIGNON | Lists user profiles that have passwords. |
| *ALL | Lists all user profiles. |

You can also check for "weak" passwords individually when you use the i5/OS Change Password function. For more information, see "Check for Weak Password Using Change Function" on page 23.

**Total number of profiles**
This field contains the total number of user profiles defined on this system.

**Users with weak passwords**
This field contains the number of users with passwords that meet the PSPasswordManager criteria of "weak".

**4.** On the **Opt** column entry fields, specify one of the options described below. Each of the columns displayed can be sorted by using **F2** (Sort logs) for a position-to sort or **F15** (Sort column) to select a column for sorting.

---

**Note**
Only the options displayed on the current page are executed.

---

**1=Send message**
Lets the security administrator send a message to users who have weak passwords, notifying them to select a stronger password. Two predefined messages can be sent to a user for one of the following reasons.

- The user's password has been identified as weak.
- The user's password has the same value as the user's ID.

These messages can be modified by the security administrator by changing the message text associated with each message. To do this, use Option 3 Check if a user has given a valid old password on the PSPasswordManager main menu.

**2=Change**
Lets the security administrator change the attributes of a user profile using the IBM command CHGUSRPRF. To use this option, you need the same authorization required to run PSPasswordManager.

**5=Display**

Lets the security administrator display the attributes of a user profile using the IBM command DSPUSRPRF. To use this option, you need the appropriate authorization.

**9=Work with object**

Lets the security administrator display the attributes of a user profile object using the IBM command WRKOBJ. With the appropriate authorization, you can also edit user profile object authorities.

**10=Act on**

Lets the security administrator perform one or more of the following actions:

- Send a message of the risk to the user.
- Log the user as having a weak password.
- Expire a user profile.
- Reset a user password to *NONE.
- Change the user's status to *ENABLED or *DISABLED.

**12=Work with**

Lets the security administrator manage the user profiles selected.

**14=Expire**

Lets the security administrator expire a user profile. Expiration forces users to change their current passwords the next time they sign on to the system. To reactivate a user profile, use option **10** (Act on).

**15=Reset log**

Lets the security administrator reset the log entry for selected user profiles. To clear all log entries, press **F10** then **F9**, and then specify Option **4**.

Resetting the logs lets the security administrator monitor violations from user profiles with weak passwords. This enables them to take corrective action if needed.

Following are descriptions of the column fields on the Work with Selected Passwords screen:

**User**

This column contains the name of the iSeries user profile.

**Logs**

This column contains the number of times that the security administrator has logged the user (or all users, with **F10**) for having a weak password. This type of logging lets the security administrator keep track of users who repeatedly have weak passwords.

**Password changed**

This column contains the date and time when the password for this user profile was last changed.

**Days**

This column contains the number of days since the password for this user profile was last changed.

**Status**

This column contains the user profile status. Normally, **ENABLED** or **DISABLD**.

If the user profile is in the iSeries internal User Password table but the user profile cannot be found, the status is indicated as **MISSING**. If the password has expired, the status is indicated as **Exp**.

**Special Authority**

The following table shows the special authority cases that can be granted to the user or adopted from the group special authorities.

| Code | Authority | Description |
|---|---|---|
| A | *ALLOBJ | All object authority |
| S | *SECADM | Security administrator authority |
| V | *SERVICE | Service tools authority |
| D | *AUDIT | Audit authority |

| Code | Authority | Description |
|---|---|---|
| J | *JOBCTL | Job control authority |
| P | *SPLCTL | Spooling authority |
| R | *SAVSYS | Save/restore authority |
| I | *IOSYSCFG | I/O system configuration authority |

For online explanations of these codes, on the Work with Selected Passwords screen, place the cursor on the Special Authority column and press **F1** (Help).

**>**

A single greater-than sign (>) is displayed for each profile that has a weak password and does not conform to the current i5/OS system values for passwords.

**Password**

This column contains the strength or weakness of the password. The values are listed below:

| | |
|---|---|
| *STRONG | Meets the security criteria of PSPasswordManager and the operating system. |
| > *WEAK | Does not meet the security criteria of PSPasswordManager, but meets the security criteria of the operating system. |
| *WEAK | Does not meet the security criteria of PSPasswordManager or the operating system. |
| *NONE | A password does not exist for this user profile. |

The following function keys are available on the Work with Selected Passwords screen:

**F2=Sort**
A position-to sort function. To use this function, position your cursor over the column that you want to sort and press **F2**. After you press **ENTER**, the data you requested is displayed at the top of the column. The other data is displayed in ascending order. Or, if only a few user profiles are showing, press **F2** repeatedly until the list is sorted as desired. A dot above the column indicates which column is being sorted.

**F3=Exit**
Pressing this function key will take you back to the PSPasswordManager main menu.

**F4=Prompt**
Displays the Specify Value for Parameter screen. For more information, see "Generic Prompting Screen" on page 9.

**F5=Refresh**
Re-displays the screen with current results.

**F9=Command line**
Displays a command line popup window and executes i5/OS commands.

**F10=Act on**
Lets you perform the following actions:

- Log the user.
- Send a message to the user.
- Set the password to *NONE.
- Expire the password for the user.
- Change the user's status.

For more information, see "Act on Weak Passwords" on page 20.

**F12=Cancel**
Re-displays the previous screen.

**F15=Sort Column**
Lets you select one of the field columns displayed for sorting.

**F17=Top**
Positions the cursor at the beginning of the user profile list.

**F18=Bottom**
Positions the cursor at the end of the user profile list.

# Act on Weak Passwords

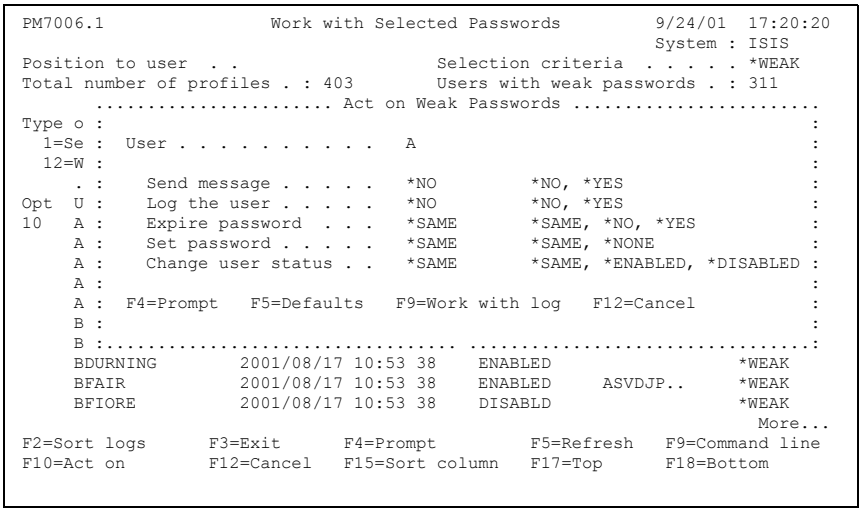
The **F10** (Act on) function key enables the security administrator to act upon a user with a weak password. This section describes the actions to take when dealing with a user who has a weak password.

Using **F10** (Act on) the security administrator can:

- Send a message of the risk to the user.
- Log the user as having a weak password.
- Expire the user's password.
- Reset the user's password to *NONE.
- Change the user's status (*ENABLE or *DISABLE).

**To act on weak passwords:**

1. From the Work with Selected Passwords screen, press **F10** (Act on).




2. On the **User** entry field, accept the default `*ALL` to make changes that will affect all users, type the name of the user you want to act on, or type `Generic*` which will apply the changes to all profiles that start with whatever is before the "*".

3. On the **Send message** entry field, accept the default `*NO` to do nothing or type `*YES` to send a message.

   The security administrator can use this option to send a message to users, notifying them to take action because of the risk posed by an insecure password. A predefined message is sent to a user for the following reasons:

   - The user's password has been identified as weak.
   - The user's password is the user's ID.

   These messages can be modified by changing the message text associated with each message. Use Option 5 Customize messages to send to users on the Password Manager main menu. If the message cannot be sent because there is no message queue associated with the profile, a message is sent to QSYSOPR instead.

4. On the **Log the user** entry field, accept the default *NO to do nothing or type *YES to increase the log count by one for the user. This enables you to keep track of repeat offenders. You can reset the log count back to zero by using option 15 (Reset log) on the Word with Selected Passwords screen.

5. On the **Expire password** entry field, accept the default *SAME, do not change the expiration value for the password, type *NO to reactivate the expired password, or type *YES to expire the password for the user profile.

   Expiration will force the users to change their current password the next time they sign on to the system. To reactivate a user, use the *ACTV option.

6. On the **Set password** entry field, accept the default *SAME, do not change the password value, or type *NONE to prevent the user from signing on until the security administrator re-assigns a new password.

7. On the **Change user status** entry field, accept the default *SAME, do not change the user's current status, type *ENABLED to allow the user to sign-on, or type *DISABLED which will not allow the user to sign-on.

---

**Note**

The system will disable a user profile if the number of failed sign-on attempts reaches the limit specified on the QMAXSIGN system value and option 2 or 3 has been specified on the QMAXSGNACN system value.

---

The following function keys are available from the "Act on Weak Passwords" screen:

**F4=Prompt**

Displays a screen showing a list of valid values for the field that the cursor is on when you press **F4**.

**F5=Defaults**

Pressing this function key restores the default values for all options. The default values are set so that executing the actions have no effect. You must specify different options when making changes to the profile.

**F9=Work with log**

Lets you work with the log object. You can delete the log here to reset the counts for all users. A new (empty) log is then automatically created.

**F12=Cancel**

Returns you to the Work with Selected Passwords screen.

# Check for Weak Password Using Change Function

You can check for weak passwords when you use the i5/OS Change Password function, by enabling the PSPasswordManager Password Validation program before you make the change. When a password is changed using the **CHGPWD** command, the validation program automatically tests the new password for weakness.

**To check a weak password:**

1. From the Work with Selected Profiles screen, press **F9** (Command line).
2. On the **command** entry line, type the following command and then press **ENTER**:

   WRKSYSVAL QPWDVLDPGM

```
                          Work with System Values
                                                              System:   ANYSERVER
Position to  . . . . . .  __________   Starting characters of system value
Subset by Type . . . . .  ________      F4 for list

Type options, press Enter.
  2=Change   5=Display

       System
Option Value       Type     Description
       QPWDVLDPGM  *SEC     Password validation program









Command
===> ____________________________________________________________________________
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display names only
F12=Cancel
```

3. On the **Position to** entry field, type ***TOP** to go to the top of the list, ***BOT** to go to the bottom of the list, or type the starting characters of the system value you are trying to find.

4. On the **Starting characters of system value** entry field, type the starting characters of the system value you want to work with.

5. On the **Subset by Type** entry field, type a system value. Press **F4** to view a list of system values. Below is a list of the system values that are available for this field.

| | |
|---|---|
| *ALL | All system values |
| *ALC | Allocation |
| *DATTIM | Date and Time |
| *EDT | Editing |
| *LIBL | Library list |
| *MSG | Message and logging |
| *SEC | Security |
| *STG | Storage |
| *SYSCTL | System control |

6. On the **Option** entry field, type `2` (Change) and press **ENTER**.

7. Make sure that `PM0013C` is displayed in the **Password validation program** entry field. Press **ENTER**.

8. On the **Command** entry line, type the following command and then press **ENTER**:

   CHGPWD

9. On the **Current Password** entry field, type the user's current password.

10. On the **New password** and **New password (to verify)** entry fields, type the new password to be used. Press **ENTER**.

11. If the new password is weak, the following message displays at the bottom of the screen. If the password is strong, no message is displayed and the change is accepted.

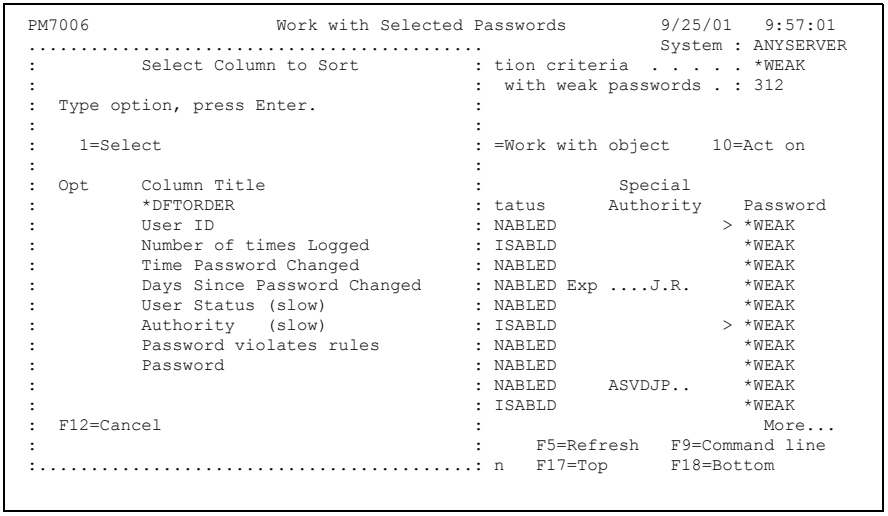
    ```
    Change rejected. The password is easily guessed.
    ```

# Select Column to Sort on

This function enables the security administrator to select one of the columns presented for sorting by that column.

**To select a column:**

1. On the Work with Selected Passwords screen, press **F15** (Sort Column).




2. On the **Opt** entry field, type **1** (Select) next to the column title you want to sort. Press **ENTER**.

   If you select *DFTORDER, the sort changes back to the primary sort order for this function.

   After pressing **ENTER**, the Work with Selected Passwords screen is re-displayed. The list is now sorted by the column title chosen.

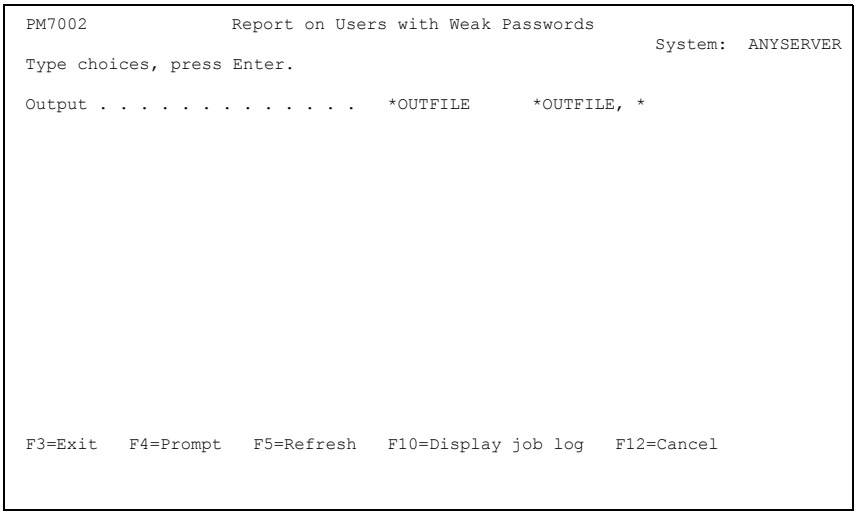
# Produce Report on Users with Weak Passwords

This option produces an output file containing the user information (where license allows) of weak user passwords. A security administrator can use this file to create a report of users with weak passwords, automate a solution to expire or disable the user profile in some other way, or use the file in what other way the administrator deems appropriate.

**Warning**
It is strongly recommended that the security administrator take action(s) to properly secure this file from abuse and/or misuse.

**To create a report:**

1. From the PSPasswordManager main menu, select Option 2 Produce Outfile with Report, and press **ENTER**.



2. On the **Output** entry field, accept the default ***OUTFILE** to send the output to a user-specified file, or type "*****" to send output to a Work with list screen. Press **ENTER.**

```
PM7002              Report on Users with Weak Passwords
                                                        System : ANYSERVER
Type choices, press Enter.

Output . . . . . . . . . . . . . > *OUTFILE      *OUTFILE, *
File to receive output . . . . .   _________      Name
  Library  . . . . . . . . . . .     QTEMP       QTEMP, *CURLIB, Name
Output member options:
  Member to receive output . . .   *FILE         Name, *FILE
  Add or replace records . . . .   *REPLACE      *ADD, *REPLACE

Report options:
  Include Status/Authority . . .   *NO           *NO, *YES
  Include passwords  . . . . . .   *NO           *NO, *YES
  Include all users  . . . . . .   *NO           *NO, *YES




F3=Exit   F4=Prompt   F5=Refresh   F10=Display job log   F12=Cancel
F13=Work with outfile report       F14=Work with *ALL files
```

3. On the **File to receive output** entry field, type the qualified name of an output file that is to receive the list of users with weak passwords and the related information. This information may include passwords if the customer has licensed that option.

4. On the **Library** entry field, accept the default **QTEMP** to place the file in, ***CURLIB** the current library, or type the name of the Library that you want to place the file in.

5. On the **Member to receive output** entry field, accept the default ***FILE** to assign a name to the file member with the same name as the file, or type the name of the member that is to contain the output data.

6. On the **Add or replace records** entry field, accept the default ***ADD** to add records to the end of an existing file, or ***REPLACE** to replace or overwrite existing records with the new records created with this execution.

7. On the **Include Status/Authority** entry field, accept the default ***NO** to not include the status and authority data fields, or select ***YES** to include the status and authority data fields

---

**Note**

Generating the data for these fields could take an extended period of time dependent upon the current number of user profiles, group authorities, etc.

---

8. On the **Include passwords** entry field, accept the default ***NO** to not include passwords, or select ***YES** to include user passwords. They will be sent to the outfile not encrypted. You must have an appropriate license for this option to have effect.

9. On the **Include all users** entry field, accept the default ***NO** to include only users with weak passwords, or select ***YES** to report all users.

   The following function keys are available from the Report on Users with Weak Passwords screen 2.

   **F3=Exit**
   Exits the current screen and returns you to the PSPasswordManager main menu.

   **F4=Prompt**
   Displays a screen that lists the valid values for the field that the cursor is on.

   **F5=Refresh**
   Refreshes the screen with your previous selections.

   **F10=Display job log**
   Displays the job log for the current job so that diagnostic or other lower level messages can be reviewed.

   **F12=Cancel**
   Exits the current screen and returns you to the PSPasswordManager main menu.

**F13=Work with outfile report**
Lets you work with the report in the outfile you specified.

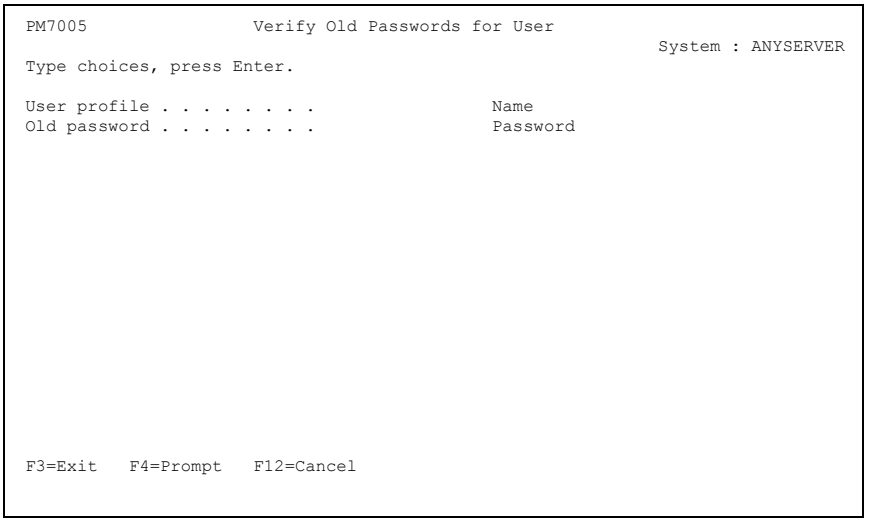
**F14=Work with *ALL files**
Allows you to work with all files in the library that you specified in Step **4** of "Produce Report on Users with Weak Passwords".

# Verify Old Passwords for User

The Check Old Passwords for User function enables a security administrator or help desk personnel, to verify that a given password for a user actually was an earlier password for this user. This old password can then be used to reset the current password for a user (perhaps one they forgot) to the previous password (or the one they remember).

**To check old passwords:**

1. On the PSPasswordManager Menu, select Option 3 Check if a user has given a valid old password, and press **ENTER**.



2. On the **User profile** entry field, type the name of the user profile that is being tested for the existence of a previous password.

3. On the **Old password** entry field, type the password to be tested. Press **ENTER**.

   The Verify Old Passwords for User Screen 2 is displayed. You can reset or expire the user profile password from this screen. Also shown, are the number of times the password being tested has been used for the last 32 passwords of the user profile.

```
PM7005                Verify Old Passwords for User
                                                        System : ANYSERVER
Type choices, press Enter.

User profile . . . . . .   ANYUSER      Name
Old password . . . . . .                 Password
Change password  . . . . .   *NO        *NO, *NEW, *OLD, *USRPRF
  Enter new password . . . .             Password (if *NEW was specified)
    Expire password  . . . .   *YES      *YES, *SAME, *NO



               1            9           17           25
               2           10           18           26
               3           11           19           27
               4           12           20           28
               5           13           21           29
               6           14           22           30
               7           15           23           31
               8           16           24           32


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

4. On the **Old password** entry field, enter the password to be tested.

5. On the **Change password** entry field, accept the default ***NO** not to change the user password, type ***NEW** to reset the user profile to a new password to be specified, type ***OLD** to reset the user profile password to the old password being tested, or type ***USRPRF** to reset the user profile password to the same name as the user profile name. The *USRPRF option is usually used in conjunction with Expire password = *YES.

6. If you typed ***NEW** in the **Change password** entry field, then on the **Enter new password** entry field, type the new password for the user profile.

7. On the **Expire password** entry field, accept the default *YES to expire the user password, type *SAME to leave the expiration value of the password unchanged, or type *NO to leave the password active. The *NO option should be used if a previous password is to be used to reset the user profile password to the old password given.

8. Press **ENTER** to start execution with selected options. If a new user profile name is given, the old password must also be entered for verification.

9. To exit the Verify Old Passwords for User screen, press **F3** (Exit).

   The following function keys are available on Verify Old Passwords for User screen 1 and screen 2.

   **F3=Exit**
   Exits the current screen and returns you to the Password Manager Menu.

   **F4=Prompt**
   Prompts the user with a list of valid values for the field that the cursor is on.

   **F12=Cancel**
   Returns you to the previous screen.

# Work with Word Lists

Word lists are members of source files in libraries of your choice. Each record can contain several words delimited by blanks. Because SEU can only edit members with less than 32,768 records, you should break very large lists into several smaller lists.

The words from the word lists are used to create entries in the Master Word Inventory. Each entry consists of two fields:

- The encrypted value for the word used as a password.
- The actual word itself.

**To work with word lists:**

1. On the PSPasswordManager main menu, select Option 4 Work with Word Lists, and press **ENTER**.

```
PM7004                    Work with Word Lists
                                                        System : ANYSERVER
Type choices, press Enter.

Word list member . . . . . .  _________   Name, F4 for list
  Source file  . . . . . .    PMTXF       Name
  Library  . . . . . . . .    PSSECURE    Name, *LIBL, *CURLIB

Type options for each word:

Add numeric suffix to words  . .  *NO       *NO, *YES  Range  . . 1 to 9
Remove embedded vowels . . . . .  *NO       *NO, *YES  Vowels . . AEIOU
Replace characters . . . . . .    *NO       *NO, *YES  Replace  . IO > 10
Double-up words  . . . . . .      *NO       *NO, *YES  Max size . 5
Reverse word . . . . . .          *NO       *NO, *YES  Max size . 7

Type options for additional entries:

Include dates  . . . . . .        *NO       *NO, *YES  Format . . MMDDYY
Include PIN numbers  . . . . .    *NO       *NO, *YES  Format . . 4-DIGIT


F3=Exit   F2=Show count   F4=Prompt   F5=Refresh   F9=Command line  F12=Cancel
```

2. On the **Word list member** entry field, type the member name or press **F4** (Prompt) for a list of member names to choose from. For more information, see "Selecting Word List Members" on page 36.

3. On the **Source file** entry field, accept the default **PMTFX,** or type a name for the source file.

4. On the **Library** entry field, accept the default **PSSECURE** to put the source file in, type the name of a library where you want to place the file, type ***LIBL**, or type ***CURLIB** to place the source file in the current library.

5. On the **Add numeric suffix to words** entry field, accept the default ***NO** to not add a numeric suffix, or type *YES add a numeric suffix to words from 1 to 9. You can specify the starting and ending suffix value.

6. On the **Remove embedded vowels** entry field, accept the default ***NO** do not remove vowels from words, or type ***YES** to remove the vowels. When ***YES** is selected, it removes vowels AEIOU or as you specify from the word.

7. On the **Replace characters** entry field, accept the default ***NO** do not replace any characters, or type ***YES** to replace characters with numbers. For instance, you can change the letters l and O to the digits 1 and 0. The word WISHBONE then becomes W1SHB0NE. You can specify any other characters that you want to replace. by entering them on the **Replace** entry fields.

8. On the **Double-up words** entry field, accept the default ***NO** do not double-up words, or type ***YES** to double-up short words. The word BONE then becomes BONEBONE. You can specify the maximum length of words to double-up on the **Max size** entry field.

9. On the **Reverse word** entry field, accept the default *NO do not reverse the word, or type *YES to reverse the characters of a word. The word BONE then becomes ENOB. You can specify the maximum length of words to reverse in the **Max size** entry field.

10. On the **Include dates** entry field, accept the default ***NO** do not include dates, or type ***YES** to include dates to be added in passwords for word lists and format to be included. For example, Q123199 might be a derived word for the word list to check against current passwords. If you select a password that begins with the letter Q followed by a string of digits only, you do not need to enter the Q when signing on.

11. On the **Include PIN numbers** entry field, accept the default ***NO** do not include PIN numbers, or type ***YES** to let the security administrator create a word list that checks for PIN numbers as current user passwords. You can specify the number of digits on the **Format** entry field.

12. When you are satisfied with your changes press **ENTER**. The following message displays:

    ```
    Updating word inventory....
    ```

    When the file has finished reading the number of words, the following message displays:

    ```
    Finished updating word inventory.
    ```

    The total number of words read, displays at the top right corner of the screen.

The following function keys are available on the Work with Word Lists screen:

**F2=Show count**
Displays the number of words in the Master Word Inventory. For more information, see "Show Number of Word Entries" on page 34.

**F3=Exit**
Exits the current screen and returns you to the Password Manager main menu.

**F4=Prompt**
Prompts the user with a list of valid values for the field that the cursor is on.

**F5=Refresh**
Refresh the screen to you previous selections before the **ENTER** key or any function key was pressed.

**F9=Command**
Displays a command entry line popup window where you execute i5/OS commands.

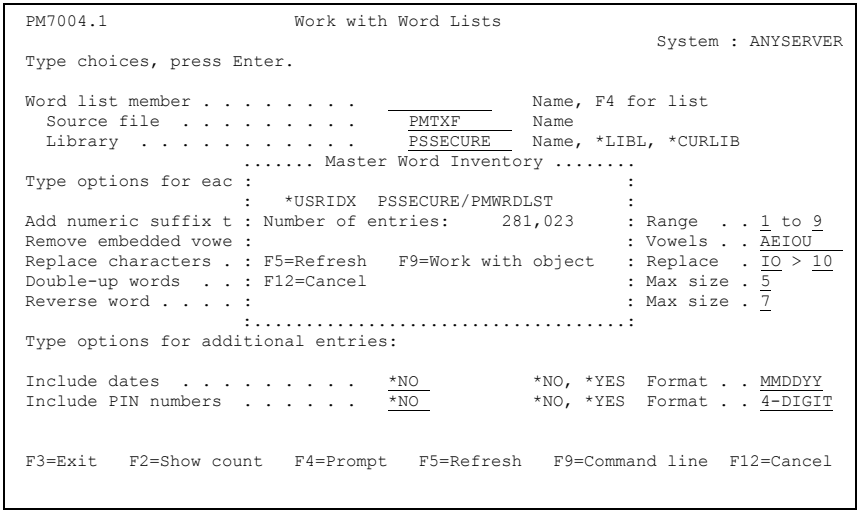
**F12=Cancel**
Exits the current screen and returns you to the previous screen.

# Show Number of Word Entries

The Word Inventory is a User Index. By default, the product is shipped with a Master Inventory already built from members ENGLISH and NAMES of the file PMTXF with all options for a word list specified. Numeric suffixes are built for 1 and 2 only. Dates and PIN numbers are not included. The ALL3 list is then added to the inventory with only the double-up option specified. Adding the same word twice does not result in extra entries in the inventory.

**To work with Master Word Inventory:**

1. From the Work with Word Lists screen, press **F2** (Show Count). The number of words in the Master Word Inventory is shown.




2. If you want to exit the window, press **F12** (Cancel). You are returned to the Work with Word Lists screen. **OR**

3. Select **F5** (Refresh) to retrieve the number of entries again. **OR**

4. Select **F9** (Work with Object) to work with the index. The Work with Objects display shows a list of objects you have authority to use. You can use this list to do some common tasks related to object authority.

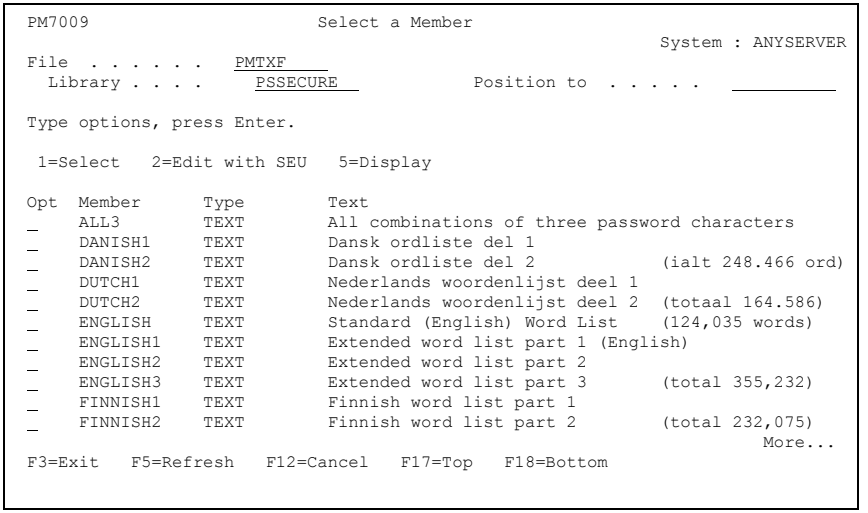
   If you delete the object, it is recreated automatically containing zero entries. You can then begin to add entries to the Inventory object.

# Selecting Word List Members

The Select a Member screen lets you select a word list member from a specified file. You can display or edit a selected word list file member to review or to change the list of words.

**To select word list members:**

1. From the Work with Word Lists screen, press **F4** (Prompt).



```
PM7009                      Select a Member
                                                          System : ANYSERVER
File  . . . . . .   PMTXF
  Library . . . .     PSSECURE            Position to  . . . . .
Type options, press Enter.
 1=Select   2=Edit with SEU   5=Display
Opt  Member      Type        Text
_    ALL3        TEXT        All combinations of three password characters
_    DANISH1     TEXT        Dansk ordliste del 1
_    DANISH2     TEXT        Dansk ordliste del 2            (ialt 248.466 ord)
_    DUTCH1      TEXT        Nederlands woordenlijst deel 1
_    DUTCH2      TEXT        Nederlands woordenlijst deel 2  (totaal 164.586)
_    ENGLISH     TEXT        Standard (English) Word List    (124,035 words)
_    ENGLISH1    TEXT        Extended word list part 1 (English)
_    ENGLISH2    TEXT        Extended word list part 2
_    ENGLISH3    TEXT        Extended word list part 3       (total 355,232)
_    FINNISH1    TEXT        Finnish word list part 1
_    FINNISH2    TEXT        Finnish word list part 2        (total 232,075)
                                                                      More...
F3=Exit   F5=Refresh   F12=Cancel   F17=Top   F18=Bottom
```

2. On the **File** entry field, accept the default PMTXF or type the name of the source file that contains the member you are editing.

3. On the **Library** entry field, accept the default PSSECURE or type the name of the library where the source file is located.

4. On the **Position to** entry field, type the member name you want to view and press **ENTER**. The member is repositioned to the top of the list.

5. In the **Opt** Column entry field, type one of the below listed option numbers next to a specific member. Press **ENTER**.

**1=Select**

When you select this option and press ENTER, the Work with Word Lists screen is displayed. You can edit the word list member selected. You can change the file and library to suit.

**2=Edit with SEU**

When you select this option and press **ENTER**, the Edit screen is displayed. Use this display to edit records in a word list member, if SEU is available.

**5=Display**

When you select this option and press **ENTER**, the Display Physical File Member screen is displayed. The contents of the word list member are listed.

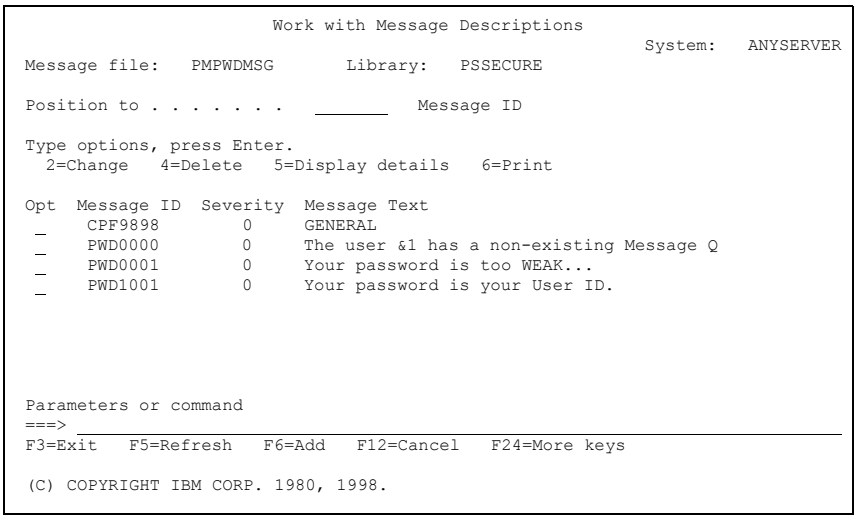
**6.** When finished selecting members, press **F3** (Exit) until you are returned to the PSPasswordManager Menu.

# Work With Message Descriptions

The Work with Message Descriptions display shows you (in message ID sequence) a list of messages in a message file. You can use this list to do some common tasks related to maintaining the list.

**To work with message descriptions:**

1. On the PSPasswordManager Menu, select Option 5 Customize messages to send to users, and press **ENTER**.




**Message file**
The name of the message file that is currently being displayed.

**Library**
The name of the library that contains the message file currently being displayed.

2. On the **Position to** entry field, type all (or one or more of the starting characters) of the name in the Message ID list. Press **ENTER** to position the list. The list is positioned alphabetically, at the item starting with the characters entered.

   If there is no list item that starts with those characters, the list is positioned to the name closest to, and in front of, the position where the name would have displayed.

3. In the **Opt** Column entry field, type one of the below listed option numbers next to a specific Message ID. You can type option numbers next to more than one entry to perform more than one task. Press **ENTER**.

**2=Change**

When you select this option and press **ENTER**, the Change Message Description (CHGMSGD) screen is displayed. This option lets you change a message description.

**4=Delete**

Deletes a message from the message file by using the Remove Message Description (RMVMSGD) command. The command is run without command prompt displays.

**5=Display details**

When you select this option and press **ENTER**, the Select Message Details to Display screen is displayed. From here, you can look at all the parts of a message description.

**6=Print**

Causes all the parts of a message description to be printed.

**Message ID**

The identifier of the message.

**Severity**

A two digit value ranging from 00 through 99. the higher the value, the more severe or important the condition.

**Message Text**

The character string that is the first level text of the message.

**Parameters or command**

You can type parameters on the **Parameters** command line and press **ENTER** to run the command immediately. When you type parameters and more than one option, the parameters are used for all commands that run as a result of the options you select.

Following are function keys that are available on the Work with Message Descriptions screen:

**F3=Exit**
Exits the current screen and returns you to the PSPasswordManager Menu.

**F5=Refresh**
Shows the list again with the most recent information and removes any selections you typed.

**F6=Add**
Displays the Add Message Description (ADDMSGD) screen. You can add a message descriptions.

**F12=Cancel**
Exits the current screen and returns to the previous menu or display.

**F24=More keys**
Shows the following function keys that are defined for this display.

**F4=Prompt**
Provides assistance when entering or selecting a command.

**F9=Retrieve**
Shows the last command you entered on the command line, along with any parameters you included. By pressing this key once, you will receive the last command you ran. By pressing this key twice, you will receive the next to last command that you ran, and so on.

**F22=Display list details**
Displays additional information about the message file that the message descriptions are in.