

User Guide

NetIQ® Security Solutions for iSeries - PSSecure™

September 4, 2008



THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 1995-2008 NetIQ Corporation, all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveReporting, ADcheck, Aegis, AppAnalyzer, AppManager, the cube logo design, Change Administrator, Change Guardian, Compliance Suite, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowing is Everything, Knowledge Scripts, Mission Critical Software for E-Business, MP3check, NetConnect, NetIQ, the NetIQ logo, the NetIQ Partner Network design, Patch Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Risk and Compliance Center, Secure Configuration Manager, Security Administration Suite, Security Analyzer, Security Manager, Server Consolidator, VigilEnt, Vivinet, Vulnerability Manager, Work Smarter, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Contents

About This Book and the Library	xii
Conventions	xiii
About NetIQ Corporation	xiv

Chapter 1

Installation and Product Access **1**

Introduction	1
Product Access	2
How to Use a Menu	2
Option 2 PPSecure	3
Option 70 Utilities Menu	3
Option 80 Enter Access Codes	3
Option 90 Signoff	4

Chapter 2

Secure Menuing System **5**

Features	5
Procedures for Installation	6
Libraries	6
Menu & Security Concepts	7
Concepts Overview	7
Applications	8
Description	8
Functions	9
Description	9
Function Types	9
Process Types	10

Menus	10
Menu Types	11
Option Selection	11
Fast-Path Selection	11
Function Keys	12
Date and Time Formats	14
User Defined Function Keys	14
Panel Options	15
Security	15
Application	15
User	16
Group Profile	16
Auth Lists	16
Function Authority	16
Special Function Authority	17
Activity Audit	17
Audit	17
Job Environment	17
Overview	17
Group Job Processing	18
General Topics	19
Reporting	19
Help Text	19
Viewing Options	19
Menu & Security Limitations	20
System Limits	20
Starting Menu & Security (STRMS Command)	20
APPL Parameter	21
FUNCTION Parameter	21
TYPE Parameter	21
Example STRMS Commands	22
Examples	22
STRMENU	23

Menu & Security Default Menu	23
Default Menu	24
Option 2 Create New Application	25
Option 3 Work With Application Definitions	27
Application Select	28
Option 4 User Security & Administration	29
Option 5 Action Bar Demo - Oper. Application	30
MS Main Menu	31
Option 1 Applications Menu	32
Option 1 Create New Application	34
Option 2 Select Other Application	35
Option 3 Update Application	36
Option 4 Work With Job Parameters	39
Option 2 Function/Options Menu	48
Option 1 Work With Cmds (Commands) & Programs	48
Option 2 Work With Menus	61
Create Menu	63
Function Update	64
Menu Update	65
Menu Options Update	68
Option 3 Work With Action Bars	69
Option 4 Work With Function Keys	76
Option 5 Work With Help Text	81
Option 6 Function & Menu Reports	83
Option 3 User Security & Administration	84
Option 1 Work With Users	85
Option 2 Work With Auth (Authorization) Lists	95
Option 3 User/Security Reports	100
Option 99 Mass User Load & Delete	101
Option 11 Work With Companies	102
Option 12 Installation Defaults Update	104

Option 4 Audit Menu	106
Option 1 View Audit Activity	107
Option 2 Audit Reports Menu	112
Option 3 Clear Audit Activity	112
Option 5 Reports Menu	113
Option 1 Application by Code	113
Option 2 User/Security Reports	114
Option 3 Function & Menu Reports	122
Option 4 Audit Reports Menu	129
Option 6 Select Other Application	133

Chapter 3

Profile & Password Management 135

System Overview	135
Function	136
Main Menu	137
Option 1 General Options Menu	138
Option 1 Work With User Profiles	139
Option 2 Report of Users	143
Option 4 Load New User Profiles	144
Option 5 Clean Up User Profiles	144
Option 15 Reactivate Profile From Archive	145
Option 16 Change Defaults (DISABLE DELETE +)	146
Option 17 User Profile Exclusions	152
Option 18 Archived Profiles Report	153

Option 2 Profile Synchronizer Menu	154
Option 1 Profiles To Exclude	155
Option 2 Distributed Systems	156
Option 3 Profile Distribution Report	159
Option 4 Profile Synchronizer Defaults	160
Option 5 Test Distribution Of Profile Change	161
Option 6 Synchronizer Debugging Options	163
Option 7 Purge Synchronizer Messages	163
Option 8 Profile Synchronizer Installation	164
Option 9 Profile Synchronizer Uninstall	164
Option 10 Add User Profile Exit Programs	165
Option 11 Remove User Profile Exit Programs	165
Verifying Profile and Password Synchronization on Multiple Systems	165
Verification Procedure	165
Option 3 Profile Templates Menu	175
Option 1 Maintain Permissible Values	176
Option 2 Maintain User Profile Templates	182
Option 3 Create a Profile Based On Template	199
Option 4 Change User Profile Based on Template	200
Option 4 iSeries Password System Values	213
Option 5 User Prompted Passwords Menu	214
Option 1 Users to Exclude From Password Prompting	214
Option 2 Test User Prompted Passwords	217
Option 3 Defaults For User Prompted Passwords	220
About User Prompted Passwords	222
Routing Entry Install	223
Initial Program Install	224

Option 6 System Generated Passwords Menu	225
Option 1 Generate and Display a Password for One User	225
Option 2 Auto Generate and Print Passwords	226
Option 3 Display Profiles Pending Pwd Change	230
Option 4 Change Profiles to Use Generated Passwords	231
Option 5 Users To Exclude From Password Generation	233
Option 6 Defaults For System Generated Passwords	234
Profile and Password Management and the OS	237
iSeries Considerations	237
System Values	237
PC Software	238
Profile Synchronizer	238

Chapter 4

Object Authority Management 239

Authority Templates	239
Key Conventions	240
Option 1 Work With Templates	243
Option 2 Work With Groups	263
Option 3 Work With Filters	267
Option 10 Non-Comp Report/Force Compliance	269
Option 11 Work With Non-Compliant Objects	271
Creating a New Authority Template	272
Option 20 Generate Authority File (PS Audit)	275

Chapter 5

Inactive Session Monitor 279

Introduction	279
Function	280
Main Menu	281
Display the Menu	281
Option 1 Start Inactive Session Monitor	282

Option 2 Stop Inactive Session Monitor	282
Option 3 Change Workstation Exclusions	283
Option 4 Display/Change User Profile Exclusions	288
Option 5 Display/Change Program Exclusions	292
Option 6 Display/Change System Parameters	293
Maintain Subsystem List	297
Maintain Inactive Session Monitor Timing	298
Maintain Inactive Session Monitor Messages	300
System Parameters Outside Of Inactive Session Monitor	301
Option 7 Timeout Log Report	303
Report Layout	304
Option 8 Dflts & Info for PS DSCJOB/SIGNOFF	305
Option 9 Display/Change Controller Exclusions	312
Option 10 Display ISM Statistics	313
Option 11 Work with ZASBS Subsystem Jobs	314
Inactive Session Monitor And The iSeries Operating System	315
Performance Enhancement	315

Chapter 6

Secure File Editor	317
System Overview	317
Main Menu	319
Option 1 File Maintenance	319
Option 2 Display Audit Log	320
Option 3 Display File Fields	320
Option 4 Maintain File Authorities	320
Option 5 Clear the Work Files	320
Option 6 Purge Audit Log	320
Option 7 Enter System Parameters	320
Option 1 File Maintenance	321
The Main Screen	322
Positioning the File	323

Windowing the Display	325
Changing Data	326
Deleting Records	330
Function Keys	331
Key Field Information	333
Displaying Field Descriptions	334
File Information	335
Adding Records	336
The Scan Function	337
More keys	338
Another View of the Data	339
Query	341
Selecting Records	341
Key Fields	343
Processing the Query	343
Database Relationships	344
Member List	345
Positioning to Top or Bottom	346
Windowing Left and Right	346
Option 2 Display Audit Log	348
The Secure File Editor Database Log Report	350
Option 3 Display File Fields	351
Option 4 Maintain File Authorities	353
Option 5 Clear the Work Files	354
Option 6 Purge Audit Data	355
Option 7 Enter System Parameters	356

Chapter 7

Utilities Menu 357

Utilities Menu	357
Option 1 Authorize Users to Products	358
Option 2 Maintain Option Authorities	359

Option 3 VigilEnt Agent Access Control	363
Option 11 Display PSAudit authorized users	364
Option 12 Display PSSecure authorized users	364
Option 13 Display PSDetect authorized users	364
Option 14 Display PSCOMMON authorized users	364
Other Utility Options	364
Save Spool File Utility	364
Set Up	365
Using The Save Spool File Utility	365
Attaching Spool File Documents To an Email	366
Creating A Batch Subsystem	368

Index	369
--------------	------------

About This Book and the Library

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

Intended Audience

This book provides information for individuals responsible for understanding PSSecure 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

Provide 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 - PSAudit
- NetIQ Security Solutions for iSeries - Remote Request Management
- NetIQ Security Solutions for iSeries - PSDetect
- NetIQ Security Solutions for iSeries - PSPasswordManager
- 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	<ul style="list-style-type: none">• Window and menu items• Technical terms, when introduced
<i>Italics</i>	<ul style="list-style-type: none">• Book and CD-ROM titles• Variable names and values• Emphasized words
Fixed Font	<ul style="list-style-type: none">• File and folder names• Commands and code examples• Text you must type• Text (output) displayed in the command-line interface
Brackets, such as <code>[value]</code>	<ul style="list-style-type: none">• Optional parameters of a command
Braces, such as <code>{value}</code>	<ul style="list-style-type: none">• Required parameters of a command
Logical OR, such as <code>value1 value2</code>	<ul style="list-style-type: none">• 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
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

Installation and Product Access

Introduction

The Product Installation and Upgrade function allows easy installation and upgrade of the iSeries products in batch or interactively, through prompted displays, and status messages. For more information about installing the NetIQ Security Solutions for iSeries products, see the *Installation Guide for NetIQ Security Solutions for iSeries*.

You may choose to distribute the products to other iSeries servers on a network so they can be installed or upgraded there without having to use a tape or CD drive.

To access NetIQ Corporation products after installation or upgrade, type **PSMENU** on a command entry line and press Enter. The PSMENU* objects are installed in library QGPL.

Product Access

The Product Access Menu lets you select the product component you want to access. To reach this menu, use command PSMENU.

```
PSMENUUD                      NetIQ Product Access Menu                      ANYSERVER
ANYUSER                        8/12/08  14:14:49

Select one of the following:

    1. PSAudit                  (V8.1.0000)
    2. PSSecure                 (V8.1.0000)
    3. PSDetect                 (V8.1.0000)
    4. PSPwdMgr                 (V8.1.0000)
    5. PSPrvMgr                 (V8.1.0000)

    70. Utilities menu

    80. Enter access codes

    90. Signoff

Selection
====>

F3=Exit   F4=Prompt   F10=Command entry   F12=Cancel
F13=Information Assistant   F16=AS/400 main menu
```

How to Use a Menu

To select a menu option, type the option number and press **Enter**.

To run a command: Press **F10**, type the command and press **Enter**

For assistance in selecting a command: Press **F4** without typing anything

For assistance in entering a command: Type the command and press **F4**

If you do not know the entire menu name you can use a generic name. For example, GO US* will show a list of all menus that start with US.

Option 2 PSSecure

Helps you to manage your iSeries by improving system security. For a detailed description of each option, see the corresponding chapter in this user guide.

Note

The documentation for Remote Request Management is located in the *User Guide for NetIQ Security Solutions for iSeries – Remote Request Management (RRM)*.

```
PSO                               NetIQ Corporation          MTABD      Date: 7/30/08
                                PSSecure Main Menu          QPADEV0008 Time: 11:04:01

Select one of the following:

 1 Secure Menuing System
 2 Profile & Password Management
 3 Remote Request Management
 4 Object Authority Management
 5 Inactive Session Monitor
 6 Secure File Editor

Enter Option or Function/Type ==> _____

F1=Help      F3=Exit      F6=Messages  F9=Window    F10=Cmd Line
F12=Previous F13=Attention F14=Batch Jobs F18=Reports
```

Option 70 Utilities Menu

Authorizes users and displays authorized users of all products.

Option 80 Enter Access Codes

Displays the screen for entering software access codes.

Option 90 Signoff

Terminates the user's session.

Function Keys

F3 = Exit - Ends the current task and returns to the display from which the task was started.

F4 = Prompt - Provides assistance in 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**. For assistance in entering a command, type the command and press **F4**.

F12 = Cancel - Cancels present screen and returns to the previous screen.

F13 = Information Assistant - Displays the Information Assistant menu with several types of assistance available. This function key provides access to 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

F16 = System Main Menu - Takes you to the system main menu.

Enter - Submits information on the display for processing.

Help - Provides additional information about using the display.

Print - Prints information currently shown on the display.

Chapter 2

Secure Menuing System

Features

The Secure Menuing System is a complete menu and security application for your iSeries applications. It provides a flexible interface to all of your programs and commands with user-defined action bars, pull-down windows, or standard menus.

Secure Menuing System includes a user-friendly design with comprehensive security management. These functions can be incorporated into new systems or used as a shell to standardize and control access to existing applications. Individual features include:

- Dynamic specification of action bars, pull-down and pop-up windows, and standard menu options designed to user requirements.
- Eliminates menu coding.
- Enables execution of commands, programs, and menus.
- Security management of menu options can be defined by function, user, group profile, authorization list, and time/date specification.
- Customization of colors, borders, and titles.
- Fully definable function keys.
- User-defined Help text can be created for each option.
- Multi-application groupings.

- Complete auditing of options and users.
- Group job support enables execution of action bars over existing programs without code modifications.
- Extensive on-line inquiry and reporting capabilities.

Procedures for Installation

For installation and upgrade instructions, see the *Installation Guide for NetIQ Security Solutions for iSeries*.

Caution

When upgrading a previous version of PSSECURE, be sure to back up the Secure Menuing System libraries before processing these installation instructions.

After Installation:

- Follow the instructions in this manual for starting the Secure Menuing System with the STRMS command, and creating your own application definitions.
- Go to the User Security & Administration menu to set up your user definitions. See *Work With Users*. For users that need the ability to maintain application and authorization list definitions, you must now give them special authority *YES or grant specific authority to selected items using the F13=Appl Admin and F14=Auth List Admin function keys.

Libraries

The files and components of the Secure Menuing System reside in libraries PSCOMMON and PSSECURE.

Menu & Security Concepts

Concepts Overview

Secure Menuing System is designed to be a flexible and easy-to-use utility. However, there are a number of concepts that you should understand before setting up your own applications.

You can control access to any existing commands or programs through the system. All options are user-definable without requiring additional coding. Access to these user-defined processes is based on the parameters that you setup using simple menus and screens.

The Secure Menuing System organizes your processes in the following manner:

- They are contained within application groups
- Defined by functions
- Executed depending on function types
- Initiated from action bars, menus, or the STRMS command.

In other words, you set up a process within an application environment. The application group commands function together, such as all order entry functions in the 'OE' application. You define the command or call parameter string needed to initiate each process as a "function". Both interactive and batch routines can be controlled by the application. Each function has an associated "function type" which identifies the process as a command, program, menu, or action bar. This function type determines how the process is to be executed by the system. Each process can then be initiated from either an action bar, menu, or the STRMS command.

All menu options and function key processing are user-definable. You can control access security by function, user, group profile, or authorization list. Finally, a complete audit trail of system activity can be printed or viewed online.

One of the most powerful features of the Secure Menuing System is that you can use it to control group job and attention key processing to give you added capabilities to your current systems. An example might be to set up the attention key to display an action bar while you are currently in your Order Entry module. You could then view pull-down menus, go to other applications to check inventory, display your calendar, and return to exactly where you were originally to finish processing the order. All of this new functionality can be added to existing systems without changing a single line of source code.

This chapter will provide more information on each of these topics.

Applications

Description

Definitions in the Secure Menuing System are divided into applications for efficiency and security. A two character code is used as an identifier to group common functions together. An example would be to group all processes associated with an Order Entry system into an application called 'OE'.

This application concept provides the following benefits:

- All common processes are grouped together.
- You can use a single application or multiple applications, depending on the needs of the organization.
- Since only the functions described to the current application are available, the user is prevented from accessing unauthorized functions.
- Application authorization can be secured as needed.

Applications can be started by using the Start Menu & System command (STRMS). Once in an application, only options defined for that application are available on menus and action bars. However, you may setup your function key definitions to enable you to process functions defined across multiple application boundaries.

Functions

Description

A function is the base description in which each process is defined to the Secure Menuing System. A 10-character function code is used as a unique identifier for each process. A function is grouped into applications and can be defined as either a command, program, menu, or action bar type. Functions can be processed in interactive or batch modes. They can be initiated from action bars, menus, or function keys.

When defining a function, each function code must be unique within an application. You must describe the command string and parameter list that is used to process the function, such as CALL program or any other command statement. The Administrator also can describe authorization rights, Help Text, default group job processes, and audit settings.

Function Types

Each function has a designated 4-character function type code that determines whether the process is a CL command, program, menu, or action bar. The Secure Menuing System controls processing based on the function type. The details of each function type are as follows:

***CMD** - The function is a CL command.

***PGM** - The function is a program. The function command string contains the CALL parameters required by the program.

***MNU** - The function is a menu. A menu displays a list of options that can be selected by the user. Each option is a function that is defined within the system. The Page Up and Page Down keys can be used to roll the screen to display all available options. Menus can be displayed as standard full screen, pull-down, or pop-up windows depending on the menu type code.

***ACT** - The function is an action bar that appears at the top of the screen and overlays the existing display. An action bar contains a number of options (functions) that can be selected by the user. Only 5 options are displayed at one time. However, the user can use the roll keys to view other options.

Process Types

The process type code determines how each function is to be executed. Functions can run in either interactive or batch mode. You have the option of specifying the process type for each function.

***INTER** - Process the function Interactively at the user's screen.

***BATCH** - Process the function in the Batch subsystem. Batch processing is typically used for report type functions and other long running jobs that do not require interaction with a user.

Menus

Menu and Action Bar type functions enable the user to view and select defined options. These functions have a number of features that are important to understand.

Menu Types

Each menu function can be processed depending on an 8-character menu type code. The processing options of the menu do not change, however, the way in which the menu is displayed is based on the menu type.

***ACTBAR** - The menu is displayed as an action bar across the top of the screen. All action bars are automatically defined as menu type ***ACTBAR**.

***PULLDOWN** - The pull-down menu is displayed as a window and appears under the action bar option that was selected. Only one pull-down window is displayed at a time.

***POPUP** - The pop-up menu is displayed as a window. Up to 4 cascading levels of windows can be displayed at any given time.

***STD1** - The standard SAA type full screen menu similar to the menus found on the iSeries in a single column format.

***STD2** - The standard SAA type full screen menu in a two column format.

Option Selection

Action Bar and Menu options can be selected in a number of different ways. The method you choose should depend on the requirements of your environment. Options can be selected in the following ways:

- **Cursor Sensitive Selection** - The user moves the cursor to the location of the option text and presses Enter. This method is particularly useful when using a mouse-enabled 5250 emulator.
- **Function Key Selection** - An option can be initiated by pressing its defined function key.

Fast-Path Selection

The Secure Menuing System offers fast-path methods that enable the user to select options immediately, without having to go through multiple options and menus. Fast-path can be used in two different ways.

Function Name and Type

An option can be selected by entering the name of the function (and its type, if multiple functions of the same name exist on the menu option). A window selection screen can also be displayed from which to select a function name.

Multiple Option Numbers

Multiple options can be entered into the menu option line to indicate that you want to process an option contained in lower level menus. The system will automatically cascade through the menus and process the desired option.

The fast path options must be delimited between each number with a blank, comma, period, or slash. For example, the fast-path options to process option 3 on sub-menu 2 are entered in one of the following ways:

- 1/2/3
- 1.2.3
- 1 2 3

If you include an invalid option in the fast-path string, processing will continue as far as possible. Once a process has finished, you will remain on the last menu processed by the fast-path command.

Function Keys

All of the panels within the Secure Menuing System use standard CUA compliant function keys. Menu function keys and security standard function keys are defined as follows:

F3=Exit - Ends the current task and returns to the display from which the task was started.

F4=Browse - Display a browse selection panel listing the current records in the file.

F5=Refresh - Refresh the current screen to display current information.

F6=Messages - Displays system messages sent to a message queue. For specific information about messages, put the cursor on the message you want information about and press **Enter**.

F9=Window - Lists the valid entries for the edited field nearest to the current cursor position.

F11=Delete - Delete the record from the data base file that is currently displayed on screen. This function always offers the opportunity to cancel the delete.

F12=Previous - Return to previous menu or display.

Enter=Update - Press **Enter** to update the data base file with details displayed on the data entry screens.

Help Key - Displays Help Text for the current field or panel. You can also set up the F1 key to display the Help screens for your own applications. In addition to the standard function keys within the system, you also have the ability to set up your own function key definitions on all menus and action bars.

The following function keys can also be found on menus and action bars:

F10=Command Line - Displays a menu command line.

F13=Attention - Calls attention key handling program ATTENTION in *LIBL. The PSSecure/SMS program ATTENTION in library PSCOMMON will display the Menu, Window, or Action Bar indicated by the Default Application Code, Function, and Function Type specified for the SMS User Profile.

F14=Batch - Displays information about your jobs submitted for batch processing.

F18=Report - Displays a list of your generated reports and other output.

Date and Time Formats

The format of the date fields is MM/DD/YY

MM Month

DD Day

YY Year

The format of the time fields is HH:MM:SS

HH Hours

MM Minutes

SS Seconds

User Defined Function Keys

User-defined function keys can be defined using the Work With Function Keys menu. Up to 24 function key definitions can be placed into a function key group. You can set up as many function key groups as needed by your organization, and each function key group can be utilized by multiple applications.

Each function key definition specifies processing for a function that has been setup within the Secure Menuing System. This integration insures that the function keys will only be allowed for users that are authorized.

In addition to functions, the following special function key definitions can be used for special processes.

***HELP** - Displays the user-defined Help Text for the function or option that the cursor is on.

***EXIT** - Ends the current task and takes you back to where the process started.

***PREV** - Processing is returned to the previous program.

***WINDOW** - Displays a window list of available options.

***MORE** - Displays a list of additional function keys that are available for selection.

Panel Options

The list panels within Secure Menuing System use standard CUA compliant options. Options are entered in front of the desired record to execute the following processes:

1=Select - Select the record for further processing.

2=Update - Display the detailed update panel of the selected record for modification.

4=Delete - Delete the selected record. A confirmation panel will be displayed allowing you to cancel before the delete is actually processed.

5=Display - Show the detailed display panel for the selected record to see more information.

Security

SMS enables definition of security using a number of methods such as no authorization checks, special user authority, group profiles, authorization lists, and individual user/function authorization. Any combination of these security methods can be added to the system plan, depending on the organization's needs.

These authority concepts are similar to the iSeries method of securing objects, but also provide additional control over function access by specifying date and time ranges that authorization is permitted. All users are initially authorized to SMS. Authority to secure SMS objects is managed through the authorization list PS PSSSMS.

Application

The application definition contains a field that enables you to specify whether authorization checking should be made for functions within the application. Simply specify ***YES** for authorization checks or ***NO** for no checking.

User

You can create separate profile authority rules for individual users of the system if desired. Users that do not have specific authority rules adopt the *DEFAULT user profile authorization rights. You may also identify those users that have special authority to all functions by changing the Special Authority flag to *YES. Normally, most users would have this special authority value set to *NO, which would prevent them from accessing all functions.

Group Profile

Each user can be assigned to a User Profile Group to simplify authority checking. The user profile group can be assigned to authorization lists and special function/user authority lists to specify authority for all users in the group without having to identify each user individually.

Auth Lists

Authorization Lists are similar to user profiles in that you can use them to simplify your authorization strategy by identifying individual user and group profile authority rules in a single list. This authorization list is then assigned to each function that you want these rules applied to.

The authorization list definition lets you specify Public Authorization, in addition to individual users and group profile access. Each of these user access rules can also be controlled by date and time ranges.

Function Authority

The definition of each function allows you to specify whether authorization checking is required. There may be some common functions that are available to all users and therefore do not require any checks.

For those functions that do require checking, Public Authority can be specified, as well as an associated authorization list detailing additional requirements.

Special Function Authority

Each function definition enables creating detailed authorization rules for individual users and group profiles. Each of these user access rules can also be controlled by date and time ranges.

Activity Audit

Audit

You can monitor user access to menu functions by establishing an audit to check for activity at three levels of processing in the following order of priority:

1. All functions and users in the application
2. Specific users
3. Specific functions

Audit transactions are created based on the audit flag rules defined for the user, application, and function levels. Once the system activity has been logged, the Administrator can see the audit information either through on-line panels or printed reports. For more information, see “Option 4 Audit Menu” on page 106.

Job Environment

Overview

The job environment specifies the library list, job descriptions, queues, priorities, etc. that interactive and batch jobs will be processed in. You can specify job environments using the Job Parameters feature of the Secure Menuing System.

Job Parameters can be set up for individual applications or can be used within multiple applications.

Each application definition lets you identify default job parameters for the application. Job Parameters can also be identified within each function definition to override the environment for processing of the function.

If no job parameter code is specified for the application or function, processing will continue to use the current environment without changing it. In addition, the Secure Menuing System will reestablish the initial library list when the user exits the system.

Group Job Processing

Group Jobs are an i5/OS system feature that enables users to initiate one or more interactive sessions without having to sign on multiple times. You can have each session display a different panel and then “hot-key” from one session to another with the use of the attention key.

The Secure Menuing System has taken advantage of this group job processing capability by enabling you to specify the function that is to be processed when the attention key is pressed. The power of this feature can be described in a simple example. You can be viewing an existing order entry panel that was accessed from the Secure Menuing System. If the customer asked for inventory information, or wanted to change an address, you can press the attention key to display an action bar or pop-up window providing access to the inventory or customer master systems. Once this processing has been finished, you can then return to the exact same place on the order entry screen.

Note

All of these new system capabilities are provided through group job processing without changing a single line of existing source code.

The default function that is processed when the attention key is pressed can be set up at three different levels based on your needs. Each of these levels overrides the previous level.

- User
- Application
- Function

General Topics

Reporting

The Secure Menuing System provides a number of reporting options to view the system definitions for all users, authority, commands, programs, menus, action bars, function keys, and Help Text. These reports are separated into sub-menus for ease of use. For more information, see “Option 5 Reports Menu” on page 113 of this manual.

Help Text

The Secure Menuing System provides comprehensive on-line Help Text for all panels and fields in the system. In addition, you can establish user-defined function Help Text for all processes that you set up in the system.

Viewing Options

The Secure Menuing System lets you specify the viewing level of menu and action bar options that are not authorized to the user. This specification is made at the application level with the Display Non-Authorized Flag.

A value of *YES would display all non-authorized options but would not allow the user to select the option for processing. A value of *NO would exclude the non-authorized function from the option list. The viewing option you choose should depend on the requirements of your organization.

Menu & Security Limitations

System Limits

The Secure Menuing System has the following limitations:

- A limit of 5 action bar options are displayed at a time. The roll/page keys can be used to display additional options if they are available.
- Up to 5 pull-down windows are available depending on action bar option position on the screen. Only one pull-down window is displayed at a time.
- A limit of 10 menu options are displayed in pull-down and pop-up windows. The roll/page keys can be used to display additional options if they are available.
- Up to 4 cascading levels of pop-up windows may be displayed at any one time.
- Once an action bar, pull-down, or pop-up window is selected, all additional lower level menus will be displayed in a pop-up format regardless of the menu type that is defined in the system.
- Standard full screen type menus may have up to 150 lower levels per branch. If a standard type menu is displayed as the first menu, all lower level menus will be displayed as a standard menu regardless of the menu type. However, if an action bar option is selected from a standard type menu, then the subsequent lower level menus of the action bar will be displayed as windows.

Starting Menu & Security (STRMS Command)

The Start Menu & System (STRMS) command provides an easy way of specifying the application, function, and function type that you want to process in the Secure Menuing System. The Start Menu and Security command can be used with parameters to access specific application functions, or without parameters to display the default Menu & Security Processing Menu.

APPL Parameter

- application to be entered
- name
- 2 character name of application

FUNCTION Parameter

The function or default process that is to be used.

***USER** - Process the default application, function, and type that is specified for this user in Secure Menuing System.

***APPL** - Process the default function and type that is specified for this application.

***LIST** - Display a selection window of all applications, functions, and types. You can specify delimiting criteria for the list by identifying either the application name or type that you want to list. The window list screen is also displayed if the user has not identified all 3 parameters when processing the STRMS command.

name - The 10 character name of the function.

TYPE Parameter

The type of function that is to be processed. Only action bar and menu type functions can be initiated with the STRMS command.

- ***ACT** - Process an action bar.
- ***MNU** - Process a menu.

Example STRMS Commands

This section lists a number of examples of using the STRMS command to initiate processes that are defined within the Secure Menuing System. You can use this command to enter the Menu and Security Maintenance routines, the operations training example, and also any new user-defined applications.

For purposes of these examples, user defined application codes are 'aa', and user defined functions are 'fffffffffff'.

Examples

To access the default Menu & Security Default Menu:

```
STRMS
```

To access the Menu & Security Main Menu:

```
STRMS APPL(MS) FUNCTION(AUTOMENU) TYPE(*MNU)
```

To access the Menu & Security definitions using an action bar format:

```
STRMS APPL(MS) FUNCTION(AUTOMENU) TYPE(*ACT)
```

To initiate the Operations Demonstration Action Bar:

```
STRMS APPL(OP) FUNCTION(OPERATIONS) TYPE(*ACT)
```

To process a specific application menu:

```
STRMS APPL(aa) FUNCTION(fffffffffff) TYPE(*MNU)
```

To initiate the default function defined for a user:

```
STRMS FUNCTION(*USER)
```

To initiate the default function defined for an application:

```
STRMS FUNCTION(*APPL)
```

To display a selection list of all available menus in application 'aa':

```
STRMS APPL(aa) FUNCTION(*LIST) TYPE(*MNU)
```

Note

You can use the STRMS command within your own CL programs, menus, or from a command entry line.

STRMENU

The STRMENU command lets you invoke a menu belonging to a different SMS application than the one calling it. For example, from an OE (Order Entry) menu, you can invoke a menu in the AR (Accounts Receivable) SMS application.

You can also specify this command within your programs to enable your programs to be called by other applications through an SMS menu.

The parameters of the STRMENU command are the same as those for the STRMS command.

Menu & Security Default Menu

The Menu & Security default menu provides an easy method of entering the system. This menu can be bypassed by using the STRMS parameters to indicate a specific function to access.

Default Menu

Enter the STRMS command without parameters. The default menu is displayed as follows:

MSCL050	Menu & Security Default Menu	Date: 6/14/00 Time: 13:49:38
Select one of the following:		
<ul style="list-style-type: none">1 Process Application2 Create New Application3 Work With Application Definitions4 Work With User Security & Administration5 Action Bar Demonstration - Operations Application		
Enter Option ==> _		
F3=Exit F12=Previous		

Select the desired option for processing. Each of these options is discussed in more detail in the appropriate section of this manual.

Option 1 Process Application

Displays a window of all available applications. By selecting an option, the associated application menu is displayed.

Option 2 Create New Application

Lets you define a new application description to the system.

Option 3 Work With Application Definitions

Enables the creation and modification of all definitions within each application.

Option 4 Work With User Security & Administration

Allows the establishment of user authority and security rules.

Option 5 Action Bar Demonstration

Displays the Operations Application Demonstration. This facility will give you an idea of how action bars and window menus can be used to give the look and feel of a PC application.

Option 2 Create New Application

Creating your own application, function, and security definitions is completely user-definable without the need for programming.

To set up your own definitions:

1. Enter the Secure Menuing System Main Menu with the STRMS command using the following parameters.

```
STRMS APPL(MS) FUNCTION(AUTOMENU) TYPE(*MNU)
```

Note

You can also enter application definitions using the STRMS command without any parameters to display the Menu & Security Default Menu. Select option 3 to work with application definitions.

2. Select Option 6 (Select other application).
3. The Applications Select panel will appear with a list of available applications. Press **F8=Add** to create a new application. Enter the required information for the new application definition.

4. The following application codes are reserved: MS, OP, PA, PC, PD, PJ, PM, PS, PU.
5. Select the newly created application from the Applications Selection window.
6. The Application Menu lets you change applications, create a new application definition, or set up job parameters.
7. Use the Function/Options Menu to display a pull-down menu of all function definition options. You must create function definitions in the order they are applied to the system:
 - Command and program function definitions are created first. You can specify the function name, command string, Help Text, authority rules and audit flag.
 - The definitions for menus are then created. The command and program functions are added to the option list of each menu. If your options process sub-menus, you must define the lower level sub-menu first.
 - The Action Bar definitions are then created with options defined to process either menu, command or program type functions. These functions must already have been defined before this step.
8. Use the User Security & Administration Menu to set up the definitions for all users that will be accessing the Secure Menuing System. Define the details of any authorization lists that will be needed.
9. Use the Reports Menu to print complete cross-reference information on all application definitions.
10. Once your function definitions have been established, you can process the new application using the STRMS command. Use the appropriate parameters to access the highest level action bar or menu.
11. Once the system is in production, the Audit Menu enables you to view system access activity for specified users and functions.

For more information on any of these topics, see the appropriate section in this manual.

Option 3 Work With Application Definitions

You can create and update user defined application definitions using the Menu & Security Main Menu. This menu can be accessed by two methods:

- Select Option 3 of the Menu & Security Default Menu.

OR

- Use the STRMS command with the following parameters:

STRMS APPL(MS) FUNCTION(AUTOMENU) TYPE(*MNU)

Select Option 6 Select Other Application. The Application Select Panel is displayed, allowing you to select or create the application that you are interested in working with. The Main Menu will then appear allowing selection of application, function/option, security/user, audit, and reporting options.

Application Select

The Application Select Panel enables selection of an existing application, or the creation of new application definitions.

MSMB010	Application Select	Date: 6/14/00 Time: 13:33:52
Position list to		Application Code . . _
Type option, press Enter. 1=Select		
Appl Code	Application Description	
- MS	Auto Menu Definitions	
- OP	Operations	
- PA	PSAudit	
- PB	Test application - PMB	
- PC	PentaSafe Main Menu	
- PD	PSDetect	
- PJ	JDE-Software Appl Menu	
- PM	PSSam	
- PS	PSSecure	
- PU	PentaSafe Utilities	
- RR	SQL Auditing	
- SQ	test auditing	
F3=Exit F8=Add F12=Previous		

Select any of the existing definitions by typing 1 in the option field. You can position the list to a specific application by entering the code in the position to field. To add a new definition, press **F8=Add**. The Application Create screen will appear allowing the entry of the application code. After selecting the desired application, the Menu & Security Main Menu will be displayed.

Option 4 User Security & Administration

You can use this option to enroll users in SMS, manage SMS authorization lists, run SMS reports related to user authority, and change SMS installation defaults.

This menu is accessed by selecting option 3 on the Menu & Security Main Menu.

SECURITY	PentaSafe, Inc.	CAS	Date: 7/01/99
	User Security & Administration	QPADEV0001	Time: 15:00:37

Select one of the following:

Work With User Security	Work With System Administration
1 Work With Users	11 Work With Companies
2 Work With Auth Lists	12 Installation Defaults Update
3 User/Security Reports	

99 Mass User Load & Delete

-

Enter Option or Function/Type ==> _____

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Type the option number in the command line. For more information about options, command line entry, fast-path selection, and function keys, see “Menu & Security Concepts” on page 7.

Option 5 Action Bar Demo - Oper. Application

This action bar has been designed to allow you to process computer operator functions directly from the Menu System. These functions are similar to the processing options available from the i5/OS Main Menu (Go Main).

The Action Bar Demonstration is displayed as follows:

GENERAL	PROGRAM	COMM MENU
.....		
Select one of the following:		
1 Process Application		
2 Create New Application		
3 Work With Application Definitions		
4 Work With User Security & Administration		
5 Action Bar Demonstration - Operations Application		
Enter Option ==> 5		
F1=Help	F3=Exit	F6=Messages
F12=Previous	F13=Attention	F14=Batch Jobs
		F9=Window
		F10=Cmd Line
		F18=Reports

Tip
Try these functions to learn how the Menu & Security Action Bar can be used to initiate processes.

- Add your own computer operator functions to this action bar.
- Incorporate them into your systems.

MS Main Menu

The Menu & Security Main Menu is displayed as follows:

AUTOMENU	PentaSafe Security Technologies Menu & Security Main Menu	CAS QPADEV0000	Date: 6/14/00 Time: 13:58:50
----------	--	-------------------	---------------------------------

Select one of the following:

- 1 Applications Menu
- 2 Function/Options Menu
- 3 User Security & Administration
- 4 Audit Menu
- 5 Reports Menu
- 6 Select Other Application

Enter Option or Function/Type ==> _____

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Each action bar option is described below. See the sections on Security, Applications, Menu Setup, Audit, and Reports for more information about these action bar options.

Option 1 Applications Menu

The Applications Menu is used for maintaining application and job parameter information.

Option 2 Function/Options Menu

The Function/Options Menu allows definition of all commands, programs, menus, action bars, function keys, and Help Text.

Option 3 User Security & Administration

The User Security & Administration Menu is used to enroll users and manage user authority.

Option 4 Audit Menu

The Audit Menu enables you to view and report on user activity in the system.

Option 5 Reports Menu

The Reports Menu allows the printing of various system definition and cross-reference reports.

Option 6 Select Other Application

This option enables you to select another application to work with.

Option 1 Applications Menu

The Applications Menu contains options that let you create and maintain application and job parameter information.

The Applications Menu is accessed by selecting Option 1 on the Menu & Security Main Menu.

APPL MENU	PentaSafe Security Technologies	CAS	D.
	Applications Menu	QPADEV0000	T.
Select one of the following:			
1 Create New Application			
2 Select Other Application			
3 Update Application			
4 Work With Job Parameters			
Enter Option or Function/Type ==> _____			
F1=Help	F3=Exit	F6=Messages	F9=Window
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports

Select the desired option or enter the option number in the command line. For more information about options, command line entry, fast-path selection, and function keys, see “Menu & Security Concepts” on page 7.

Option 1 Create New Application

The Create New Application Panel enables the entry of a new application code.

```
MSRS010                               Application Select          Date: 6/07/99
                                                                              Time: 13:25:41

Application Code . . _
```

F3=Exit F12=Previous

Application Code - The application code identifies the application that the user is currently working with. The menu functions are separated into application groups identified by application codes. Menu functions can be grouped into one large application or multiple application groupings, depending on the needs of the organization. The following Application Code are reserved: MS, OP, PA, PC, PD, PJ, PM, PS, PU.

Application Update - When an application code is input, the Application Update panel is displayed to enable the entry of detailed application information. For more information, see “Option 3 Update Application” on page 36.

Option 2 Select Other Application

The Application Select panel lists all current applications codes that are currently defined to Secure Menuing System.

MSMB010		Application Select		Date: 6/07/99	
				Time: 13:29:56	
Position list to			Application Code . . _		
Type option, press Enter. 1=Select					
Appl	Application				
Code	Description				
= JB	Jim's Application				
- MS	Auto Menu Definitions				
- OP	Operations				
- PA	PSAudit				
- PC	PentaSafe Main Menu				
- PD	PSDetect				
- PJ	JDE-Software Appl Menu				
- PM	PSSam				
- PS	PSSecure				
- PU	PentaSafe Utilities				
F3=Exit F8=Add F12=Previous					

Select any of the existing definitions by typing 1 in the option field. You can position the list to a specific application by entering the code in the position-to field. To add a new definition, press **F8=Add**. The Application Create screen will appear allowing the entry of the application code. Once an application has been selected or a new application code has been entered, the Application Update screen will be displayed.

Function Key

The following special function key is available on this panel:

F8=Add - The Add function key lets you create new application codes.

Option 3 Update Application

The Application Update function allows you to specify detailed information needed for each application.

Application Update

The Application Update Panel is displayed as follows:

MSKM010

Application Update

Date: 9/14/08
Time: 9:18:02
*Update

Application Code . . MS

Application Descr. . Auto Menu Definitions

Job Parameters Code. AUTOMENU

Auto Menu Job Parameters

Display Non-Auth . . *YES

Check Authority. . . *YES

Audit Activity . . . *NONE

Default Func Code. . _____

Default Func Type. . _____

Function Descr . . . _____

Start-Up Program . . _____

Library. _____

Exit Program MSRP106

Library. *LIBL

F3=Exit

F5=Refresh

F9=Window

F11=Delete

F12=Previous

Enter=Update

Application Code - The application code identifies the application that the user is currently working with. The following application codes are reserved: MS, OP, PA, PC, PD, PJ, PM, PS, PU.

Application Description - The description of the application code.

Job Parameters Code - The Job Parameters Code defines the processing environment for a function. Function job parameters include such things as job description, job queue, output queue, priority, and library list. Each job parameter code is unique within an application. Job parameters can be overridden for individual functions.

Job Parameters Description - Displays the description of the Job Parameters Code.

Display Non-Authorized Options - The Display Non-Authorized Options flag controls whether functions that are not authorized to a user are displayed on action bars and menus. This setting applies to the entire application.

Possible values are:

- *YES Display all options. Non-Authorized options will appear, but will be protected and not highlighted on the screen
- *NO Do not display options that are not authorized to the user.

Check Authority - The check authority flag lets you specify authorization checking for individual functions or an entire application.

Possible values are:

- *YES Check user's authority to menu functions.
- *NO Do not check user's authority to menu functions.

Application Level Authority - Authority checking can be set up for an application by setting Check Authority to *YES. The system will then check the user's authority to each function. All authority checking in the system can be turned off by setting this field to *NO at the application level.

Function Level Authority - Authorization checking for individual functions can be performed by specifying *YES for this field in the function update panels. The system then checks to see if the current user has authority to the option before it is processed.

Note

Function level authority is only checked if the application is set to Check Authority *YES.

Audit Activity - The audit activity flag allows you to monitor user access to functions. Audit activity can be monitored at three levels of processing in the following order of priority.

1. All functions and users in the application
2. Specific users
3. Specific functions

Possible values are:

- *YES** Produce an audit transaction, override higher levels
- *NO** Do not generate an audit transaction, override higher
- *NONE** Auditing is based on criteria at other levels

Audit transactions will be created based on the rules defined in the following table. Each lower level overrides the higher levels.

Generate Audit Flag Specification			
Transaction	Application	User	Function
No	*NO or *NONE	*NO or *NONE	*NO or *NONE
Yes	*NO or *NONE	*NO or *NONE	*YES
Yes	*NO or *NONE	*YES	*NONE
No	*NO or *NONE	*YES	*NO
Yes	*YES	*NONE	*NONE
No	*YES	*NO or *NONE	*NO
No	*YES*	NO	*NONE
Yes	*YES*	YES	*NONE
No	*YES*	YES	*NO

Default Function Code - This function code with the Default Function Type identifies the function to be processed when the user presses the attention “hot-key” while running another option. For more information, see “Function Code - Displays the function code that was specified on the browse or create panels.” on page 52.

Default Function Type - The 4 character function type code further identifies the default function as *MNU or *ACT.

Function Description - Displays the description of the default function. The description cannot be changed on this panel.

Start-Up Program - The 10 character Start-Up Program field is used to specify a program to run before the first menu application panel is displayed. This allows you to tailor the menu system to work in your environment for any special processing that is needed for the Local Data Area, QTEMP library, etc.

Note

The start-up program is executed after the job parameters have been setup for the session, but before the first function is processed.

Start-Up Program Library - The library that contains the start-up program.

Exit Program - Lets you specify a program to run at the end of a user's session in the menu application. Special processing such as clean-up routines and reporting can be performed by the exit program.

Note

The exit program is processed after the user ends the menu session, but before the menu system processes its own clean-up routines.

Exit Program Library - The library that contains the exit program.

Delete Application - Use the F11=Delete Function key to delete the application and all its function definitions.

Option 4 Work With Job Parameters

These panels enable you to set up the processing environment for applications and functions through the use of job parameter codes. The job parameter defines the library list, job description, job queue, output queue, etc., for each function.

Job Parameters Browse

The Work With Job Parameters panel lists all parameter codes currently defined in SMS. You can position the list to a specific job parameter by entering the code in the position-to field.

MSMB020

Work With Job Parameters

Date: 9/14/08
Time: 11:06:56

Position list to

Job Parameters Code. _____

Type option, press Enter
1=Select 3=Copy 4=Delete

Parameters	
Code	Description
AUTOMENU	Auto Menu Job Parameters
PKTEST	
PSAPARM	PSAudit Environment
PSCPARM	PS* Common Environment
PSDPARM	PSDetect Environment
PSMPARM	VigilEnt Agent for World
PSSPARM	PSSecure Environment

Bottom

F1=Help

F3=Exit

F8=Add

F12=Previous

- 1=Select** - Select any of the existing definitions by typing **1** in the option field. After selecting, the Job Parameter Update panel will be displayed.
- 3=Copy** - Allows you to copy a parameter’s definition to another name. After selecting, a window will be displayed prompting for the new code.
- 4=Delete** - Deletes the job parameter code description.

Function Key

The following special function key is available on this panel:

F8=Add - Add a new Job Parameter Code definition. The Job Parameter Select panel will appear allowing the entry of the new parameter code.

Add Job Parameters

The Job Parameters Select panel enables the entry of a new parameter code.

```
MSRS020                      Job Parameters Select                      Date:  6/07/99
                               Time: 14:36:27

Job Parameters Code.  _____

F3=Exit      F4=Browse      F5=Refresh      F12=Previous      Enter=Select
```

Job Parameters Code - The 10 character Job Parameters Code lets you establish the processing environment for a function. Job parameters include such things as job descriptions, job queues, output queues, priorities, and library lists. Each job parameter code is unique within an application. Job parameters can be setup for an entire application, a menu, or can be overridden for each individual function.

Function Keys

The following function keys are available on this panel:

F4=Browse - Shows the Work With Job Parameters panel.

F5=Refresh - Updates the panel.

Job Parameters Update

The Job Parameters Update Panel lets you establish and maintain detailed information for each parameter code.

MSKM020

Job Parameters Update

Date: 6/07/99
Time: 15:01:27
*Update

Job Parameters Code. AUTOMENU

Job Parms Descr. . . . Auto Menu Job Parameters

Job Description. . . . MSJOB

Library. *LIBL

JOBQ *JOB

Library. *LIBL

Job Priority *JOB

Output Priority. . . *JOB

System Lib List. . . *CURRENT

Current Lib List . . *CRTDFT

Initial Lib List . . *CURRENT

Print Device *CURRENT

OUTQ *CURRENT

Library. *LIBL

Hold on Job Queue. . *JOB

Message Queue. . . . *USRPRF

Library. *LIBL

F3=Exit F5=Refresh F11=Delete F12=Previous Enter=Update

Job Parameters Code - Displays the 10 character job parameters code that was specified on the previous screen.

Job Parameters Description - The description of the job parameters code.

Job Description - The job description to use for submitted jobs. Possible values are:

***USRPRF** The job description of the user profile running the submitted job is used.

Name The job description used for the submitted job.

Job Description Library - The library where the job description resides. Possible values are:

*LIBL	The library list is used to locate the job description
Lib-name	The library where the job description name is located

JOB Queue - The job queue where the submitted job is placed. Possible values are:

*JOBQ	The submitted job is placed on the job queue named in the specified job description
Jobq-name	The name of the job queue where the submitted job is placed

JOBQ Library - The library containing the specified JOBQ. Possible values are:

*LIBL	The library list used to locate the job queue named in the specified job description
Lib-name	The name of the library where the JOBQ is located

Job Priority - Specifies the scheduling priority for the submitted job. Valid values range from 1 through 9 (where 1 is the highest priority and 9 is the lowest priority). Possible values are:

*JOBQ	The scheduling priority specified in the job description is used
Priority	Specify a value, ranging from 1 through 9, for the scheduling priority for the job

Output Priority - The output priority for spooled output files that are produced by the submitted job (the highest priority is 1 and the lowest priority is 9). Possible values are:

*JOBQ	The output priority specified in the job description is used for the job
Priority	Specify a value, ranging from 1 through 9, for the priority of the output files of the submitted job

System Library List - The system portion of the library list being used by the submitted job. Possible values are:

- *CURRENT The system portion of the library list of the submitting job is used
- *SYSVAL The library list specified in the system value (QSYSLIBL) at the time the job is started is used for the submitted job

Current Library - The current library associated with the job being run. The possible values are:

- *CURRENT The current library for the job
- *USRPRF The current library specified in the user profile of the submitted job is used.
- *CRTDFT There is no current library for the job. If objects are created in the current library, the QGPL library is used as the default library.
- Lib-name Specify the name of the library that is used as the current library for the job.

Initial Library List - The initial user portion of the library list that is used by the submitted job to search for any object names that are needed. Note that duplication of libraries in the library list is not allowed. Possible values are:

- *CURRENT The user portion of the library list being used by the current job is used for the submitted job.
- *LIST The library list specified on the job parameter library list panel (next screen) is used
- *JOB The library list specified in the job description, which is used with the current job, is used for the submitted job.
- *SYSVAL The system default user library list is used
- *NONE No user libraries are specified, only the system portion of the library list is used

Print Device - The default printer device for this job. Possible values are:

- *CURRENT** The printer device being used by the job that is currently running is used by the job.
- *USRPRF** The printer device specified in the user profile under which the submitted job runs is used.
- *SYSVAL** The printer device specified in the system value QPRTDEV is used for the submitted job.
- *JOB** The printer device specified in the job description is used for the submitted job.

Device-name Specify the name of the printer device that is used for the submitted job.

Output Queue - The default output queue that is used for spooled output produced by the submitted job. Possible values are:

- *CURRENT** The output queue used by the current job is used for the submitted job.
- *USRPRF** The output queue in the user profile, under which the submitted job runs, is used as the output queue for the submitted job.
- *DEV** The output queue associated with the specified printer device is used.
- *JOB** The output queue named in the job description used with the submitted job is used.

Name Specify the name of the output queue that is used for the submitted job.

OUTQ Library - The library that contains the specified output queue. Possible values are:

- *LIBL** The library list is used to locate the output queue.

Name The name of the library where the OUTQ resides.

Hold on Job Queue - Specifies whether the submitted job is held at the time that it is put in the job queue. A job placed on the job queue in the hold state is held until it is released by the RLSJOB command, canceled by the ENDJOB command, or removed from the job queue by the CLRJOBQ command. Possible values are:

- *JOBD The value specified in the job description determines whether the job is held when it is put in the queue.
- *NO The job is not held when it is put in the job queue.
- *YES When the job is put in the job queue, it is held until released or ended.

Message Queue - The message queue where a completion message is sent when the submitted job has completed running either normally or abnormally. Possible values are:

- *USRPRF A completion message is sent to the message queue specified in the user profile of the submitted job.
- *WRKSTN A completion message is sent to the message queue of the workstation from which the job was submitted
- *NONE No completion message is sent

MSGQ Library - Specifies the name of the library containing the message queue. Possible values are:

- *LIBL The library list is used to locate the message queue name
- Name The name of the library where the message queue name is located

Delete Job Parameters

The F11=Delete Function key will delete the Job Parameter and Library List information associated with it.

Library List Update

The Library List Update Panel lets you list all of the libraries that the job will use when processing.

MSTM030		Library List Update	Date: 6/07/99
			Time: 15:18:50
Job	Job		
Parameters	Parameter		
Code	Description		
AUTOMENU	Auto Menu Job Parameters		
Type details, press Enter.			*Update
4=Delete			
Opt	Library Sequence	Library Name	
=	2	QTEMP	
-	4	PSCOMMON	
-	6	PSSECURE	
-	8	QGPL	
-	-		
-	-		
-	-		
-	-		
-	-		
F3=Exit		F12=Previous	Enter=Update

Library Sequence - The library sequence specifies the order in which libraries will be searched by functions to find objects if no specific libraries have been identified by operations. You can change the order by changing the sequence numbers. New libraries can be added to the search list by entering an existing library name and sequence number.

Library Name - The name of the library that will be part of the library list. This must be a valid library object on the system.

Option 2 Function/Options Menu

The Functions & Options Menu enables you to work with all system definitions for commands, programs, menus, action bars, function keys, and Help Text. You can also access the function reports menu from this panel.

This menu is accessed by selecting Option 2 on the Menu & Security Main Menu.

MENU SETUP	PentaSafe Security Technologies, Inc	ANYUSER	Date: 9/21/08
	Function/Options Menu	QPADEV000B	Time: 13:16:51
Select one of the following:			
1 Work With Cmds & Programs			
2 Work With Menus			
3 Work With Action Bars			
4 Work With Function Keys			
5 Work With Help Text			
6 Function & Menu Reports			
Enter Option or Function/Type ==> _____			
F1=Help	F3=Exit	F6=Messages	F9=Window
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports
F10=Cmd Line			

Select the desired option or enter the option number in the command line. For more information about options, fast-path selection, and function keys, see “Menu & Security Concepts” on page 7.

Option 1 Work With Cmds (Commands) & Programs

Lets you define the details of each command and program that is processed in the system.

Commands & Programs Browse

The Work With Commands & Programs screen lists all functions currently defined to SMS. You can position the list to a specific command or program function by entering the code in the position-to field.

MSMB207

Work With Commands & Programs

Date: 6/07/99
Time: 15:40:32

Position list to

Function Code.

Function Type Code

Type option, press Enter

1=Select

3=Copy

4=Delete

9=User Security

Function Code	Func Type	Function Description
JDBSPLF	*CMD	Print files
JDBWRKA	*CMD	Work Jobs

Bottom

F1=Help

F3=Exit

F8=Add

F12=Previous

Select any of the existing definitions by typing 1 in the option field.

Once a command or program has been selected or a new function has been entered, the Function Update screen will be displayed.

Options

1=Select - Select any of the existing definitions by typing 1 in the option field. You can position the list to a specific menu function by entering the code in the position to field. When a function is selected or a new function has been entered, the Function Update screen will be displayed.

3=Copy - Allows you to copy this menu definitions to another name.

4=Delete - Delete any of the existing definitions by typing **4** in the option field.

9=User Security - Gives you a list of user profiles and lets you see which have authorization.

Function Key

The following special function key is available on this panel:

F8=Add - Adds a new definition. The Function Create screen will appear allowing the entry of the function code. The create function key allows you to specify new command and program function codes to the system.

Create Cmd/Pgm

The Function Create Panel enables the entry of a new command and program function codes. The screen is displayed as follows:

```
MSRS200                Function Create                Date: 6/07/99
                                                             Time: 15:49:59

Function Code. . . . _____

Function Type Code . ____ (*CMD, *PGM)

F3=Exit                F12=Previous
```


Function Code - The function code identifies a specific process that is to be executed. The function created from this screen can be either a program or command. It can be processed either interactively or in batch mode. Each function can be listed on any number of menus or action bars depending on the needs of the organization.

Function codes must be unique by type within an application. The function specifies the programs and commands to access, special processing parameters, function level Help Text, and user authority.

Function Type Code - The four character function type code identifies the function as either a command or program. The application controls processing based on this function type. Possible values are:

*CMD Command

*PGM Program

Function Update

The Function Update Panel lets you specify detailed information for each function definition.

MSKM200

Function Update

Date: 6/07/99
Time: 16:06:56
*Update

Function Code . . . JDBWRKA

Function Type Code . *CMD

Long Function Descr. Work with Active Jobs

Std Function Descr. Work Jobs

Short Descr . . wrkactjobs

Process Type Code. . *INTER (*INTER, *BATCH)

Audit Activity . . . *NONE (*YES,*NO,*NONE)

Confirm Screen. *NO (*YES,*NO)

Check Authority. . . *NO (*YES,*NO)

Public Authority . . *NO (*YES,*NO)

Password.

Auth List Code . . .

Job Prompt Pgm. *NO (*YES,*NO)

Prompt Pgm.

Job Parameters Code. . .

Reclaim Resources. . *NO (*YES,*NO)

Prompt Pgm Lib. *LIBL

Dft Appl/Func/Type . _ _ _

Command String . . . WRKACTJOB

F3=Exit

F4=Prompt

F5=Refresh

F9=Window

F11=Delete

F12=Previous

F14=Authority

F15=Menus

F16=User Auth

F21=Text

Function Code - Displays the function code that was specified on the browse or create panels.

Function Type Code - Displays the function type code that was specified on the browse or create panels.

Function Description - There are three different types of function description that are used depending on the type of menu that processes the function. The 34 character Long Description is used on full screen menus. The 25 character Standard Description is used on all window type of menus. The 10 character Short Description is used on action bar menus.

Process Type Code - The process type code determines how each function is to be executed. Functions can run in either interactive or batch mode. Press **F9=Window** for a selection list of all valid codes. Possible values are:

*INTER Interactive

*BATCH Batch

Confirmation Screen - The confirmation screen flag determines whether an option confirmation window will appear when the function is selected from a menu or action bar. Possible values are:

*YES Display the window

*NO Do not display the window

Password - You can assign a password to any function. When the function is selected from an action bar or menu, the user is required to enter the correct password before the function is executed.

Tip

To minimize the risk of compromising an iSeries password, the password selected should be an iSeries user's password.

Note

The password screen will not display unless you must change the confirmation option to *YES.

Audit Activity - The audit activity flag allows you to monitor the access of users to specific functions. An audit can be established to check activity at three levels of processing in the following order of priority.

1. All functions and users in the application
2. Specific users
3. Specific functions

Possible values are:

- *YES** Produce an audit transaction, override higher levels
- *NO** Do not generate an audit transaction, regardless of other levels
- *NONE** Transaction is generated based on criteria of other levels

Audit transactions will be created based on the rules defined in the following table. Each lower level overrides the higher levels.

Generate Audit Transaction	Audit Flag Specification			
	Application	User	Function	
No	*NO or *NONE	*NO or *NONE	*NO or *NONE	
Yes	*NO or *NONE	*NO or *NONE	*YES	
Yes	*NO or *NONE	*YES	*NONE	
No	*NO or *NONE	*YES	*NO	
Yes	*YES	*NONE	*NONE	
No	*YES	*No or *NONE	*NO	
No	*YES	*NO	*NONE	
Yes	*YES	*YES	*NONE	
No	*YES	*YES	*NO	

Check Authority - The check authority flag lets you specify authorization checking for individual functions or an entire application. Possible values are:

- *YES** Check authority for function
- *NO** Ignore all authority checks for this function

Application Level Authority - Authority checking can be set up for an application by setting Check Authority *YES in application update. The system will then check the authorization of each individual user for each function. All authority checking in the system can be turned off by setting this field to *NO at the application level.

Function Level Authority - Authorization checking for individual functions can be established using this field in the function update panels. The system then checks to see if the current user has authority to the option before it is processed. If you do not need to check for a particular function, this field is set to *NO.

Note

Function level authority is only checked if the application is set to check authority *YES.

Public Authority - Public Authority specifies the authority given to users who do not have specific authority to the function, who are not on the authorization list, and whose group has no specific authority to the object. This feature lets you grant or revoke authority to the majority of the users, thereby limiting the number of specific user authorities that are required. The possible values are:

- *YES The user may access the function
- *NO The user cannot access the function

Authorization List Code - The Authorization List Code identifies a list of users and the authorities that each user has to all objects the list secures. Then, when you specify the authority for a function, you can specify an authorization list code. This enables the same authorization list to be used for many functions without giving each user authority to function individually. Each user on the authorization list can have different authority to the set of objects that the list secures. Press **F9=Window** for a selection list of all valid codes.

Authorization List Description - The description of the authorization list.

Job Parameters Code - The Job Parameters Code enables the Systems Administrator to establish the processing environment for a function. Function job parameters include such things as job descriptions, job queues, output queues, priorities, and library lists. Each job parameter code is unique within an application. Job parameters can be setup for an entire application or can be overridden for individual functions. Press **F9=Window** for a selection list of all valid codes.

Job Parameters Description - The description of the job parameters code.

Reclaim Resources - The Reclaim Resources flag lets you specify the processing of the Reclaim Resources (RCLRSC) Command upon exit of the function. The RCLRSC command is used by a controlling program to free static storage and close any files that may have been left open by other programs in the application that are no longer active. Possible values are:

- *YES Yes, process the RCLRSC command
- *NO No, do not process the RCLRSC command

Note

The reclaim resource is only needed for those processes that intentionally leave files open for efficiency purposes.

For more information on RCLRSC, see the IBM Manuals.

Job Prompt - The job prompt parameter indicates that a program will be processed before the execution of the function. This can be any program that you need in your applications for pre-processing, such as report selection screens. The program that will be processed is identified in the following prompt program and library parameters. Possible values are:

*YES Yes, process job prompt program

*NO No, do not process job prompt

Note

After processing the job prompt program, the return code field is checked in the local data area (*LDA), positions 118-119, for blanks to continue processing the function. If you want your users to exit the job prompt program and stop processing, move values into that 2-character position in the LDA. For example, if the user presses F3=Exit on your prompt program, the program will load 03 into the return code in the LDA.

Job Prompt Program & Library - User defined job prompt program and library that is used for preprocessing of the function.

Default Application Code - This 2-character application code identifies the default application to be processed when the user presses the attention “hot-key” while currently running this option. For more information, see the description of the Application Code in “Option 1 Create New Application” on page 34.

Default Function Code - This 10 character function code identifies the default function or task to be processed when the user presses the attention “hot-key” while currently running this option. Press **F9=Window** for a selection list of all valid codes. For more information, see the Function Code in “Option 1 Create New Application” on page 34.

Default Function Type - The 4 character function type code identifies the type of function or task to be processed when the user presses the attention “hot-key” while currently running this option. For more information, see the Function Type in “Create Cmd/Pgm” on page 50.

Function Command Parameter - The function parameter field lets you specify the execution parameters of the command or program that is to be processed. The parameter must not exceed 256 characters in total. If the length of your command string is longer, create a program defining the long string and call it from here.

The following examples are commands that may be specified:

Simple command:	DSPMSG
Command with parameters:	WRKOUTQ PRT01
Program Call command:	CALL PGM123
Start a System/36 Procedure:	STRS36PRC PRC(A123)

All parameter entries have syntax checking performed on the command string to ensure all required parameters are coded, and that all parameters have allowable values. It does not check the processing environment, such as valid program names and library lists. You can request prompting for the parameter by either placing a question mark before the command name of the string or pressing **F4=Prompt**. For example, ?CALL PGM123 is a prompt request on CALL command.

Function Keys

The following special function keys are available on this panel.

F4=Prompt - The prompt function key displays the iSeries command prompt for the command that you enter in the parameter line.

F11=Delete - Deletes the function and all text and authority rules.

F14=Authority - The Function Authority Update Panel enables the specification of detailed Function/User authority rules for the current function being maintained.

F15=Menus - The Menus by Function Panel lists all action bars, menus, and associated options where this function can be executed.

F21=Text - The Help Text Update Panel enables creating and maintaining Help Text for this function.

Function Authority Update

The Function Authority Update Panel lets you establish detailed user or group profile access rights to a function. The screen allows entering multiple user or group profile codes followed by the required function authority rules and date/time ranges.

MSTM270

Function Authority Update

Date: 6/07/99
Time: 16:21:56

Function Code

Func Type

Function Description

JDBWRKA *CMD Work Jobs

Type details, press Enter.
4=Delete

*Add

Opt	User	Func Auth *YES/*NO	Begin Date	End Date	Begin Time	End Time
=			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		

F3=Exit F9=Window F12=Previous Enter=Update

User - The 10 character user identifier specifies the system name given to an individual user or group profile. This name must be the same name as the iSeries user profile. The system can then automatically identify and track information for the user without any manual intervention. Press **F9=Window** for a selection list of all codes.

Function Authority - The authority that a user has to the function. The individual authority a user has to a function overrides any higher level authority specifications. Possible values are:

*YES Grant function access

*NO No access to the function allowed

Begin Date - The begin date range for function authorization. This date enables you to specify periods in which users are allowed or denied access to a function.

End Date - The end date range for function authorization. This date enables you to specify the periods in which users are allowed or denied access to a function.

Begin Time - The begin time range for function authorization. This time field enables you to specify periods in which users are allowed or denied access to a function.

End Time - The end time range for function authorization. This date enables you to specify periods in which users are allowed or denied access to a function.

Menus by Function

The Menus Options by Function Panel lists all action bars, menus, and associated options where this function can be executed.

Note

The information listed on this panel is for display purposes only. No updates can be made.

_MSTE122		Menu Options by Function		Date: 6/30/99
				Time: 18:04:33
Function Code	Func Type	Function Description	Process Type	
JDBWRKA	*CMD	Work Jobs	*INTER	
Menu Code	Menu Description	Menu Opt		
JDBMENU	Jim Menu	2		
JDBMENU	Jim Menu	2		

Help Text Update

The Function Text Update Panel enables creating and maintaining Help Text for this function.

MSTM230

Function Text Update

Date: 6/30/99
Time: 18:35:47

Function	Func	Function
Code	Type	Description
ATTENTION	*PGM	Attention Key Processing

Type details, press Enter.

*Update

4=DeleteH=Highlight On/Off

OptText

=

The Attention Key Processing program enables you to specify the menu option or function key to be used to initiate and pass control to a secondary group job process. This feature allows you to temporarily leave the current screen you are in, process another function that you have defined to the system, and then return to the same place that you left. The command or program that is processed is the default application, function, and type that is identified to the original function.

-

-

-

F3=ExitF12=PreviousEnter=Update

Text - Descriptive text about the function. The user may add as much text as necessary to describe function processing.

Panel Options

The following special panel options are available on this panel:

H=Highlight On/Off - Type **H** to cause the text line to be brighter than other lines when it appears on the Help Text Update panel.

Option 2 Work With Menus

Specify the detailed definition for each menu function and the available option definition for each.

Menu Browse

The Work With Menus panel lists all menu currently defined to SMS.

MSMB204

Work With Menus

Date: 6/30/99
Time: 19:05:11

Position list to

Function Code. . . . _____

Type option, press Enter

1=Select

3=Copy

4=Delete

9=User Security

Function

Code

Description

=

APPL MENU

Applications Menu

-

AUDIT

Audit Menu

-

AUTOMENU

Menu & Security Main Menu

-

MENU SETUP

Function/Options Menu

-

REPORTS

Reports Menu

-

RPTAUDIT

Audit Reports Menu

-

RPTFUNC

Function & Menu Reports

-

RPTSECURTY

User/Security Reports

More...

F1=Help

F3=Exit

F8=Add

F12=Previous

Option

1=Select - Select any of the existing definitions by entering a “1” in the option field. You can position the list to a specific menu function by entering the code in the position to field. Once a menu has been selected or a new menu function has been entered, the Function Update screen will be displayed.

3=Copy - Allows you to copy this menu definitions to another name.

4=Delete - Delete any of the existing definitions by entering 4 in the option field.

9=User Security - Gives you a list of user profiles and lets you see which have authorization.

Function Key

The following function key is available on this panel:

F8=Add - Add a new definition. The function create screen will appear allowing the entry of the menu function code. The Add Function key allows you to specify new menu function codes to the system.

Create Menu

The Function Create Panel enables the entry of a new menu function code. The screen is displayed as follows:

```
MSRS200                Function Create                Date: 6/30/99
                                                             Time: 18:52:07

Function Code. . . .  _____

Function Type Code . *MNU

F9=Exit                F12=Previous
```

Function Code - The 10 character function code identifies a specific menu code that is to be created. Each menu function can be listed on any number of other menus or action bars depending on the needs of the organization.

Function Type Code - The four character function type code identifies the function as a menu. The Secure Menuing System controls processing based on function type. The value *MNU is automatically filled in for you by the system.

Function Update

The Function Update Panel lets you establish and maintain detailed information for each menu function defined to the system.

MSKM200

Function Update

Date: 6/30/99
Time: 19:09:14
*Update

Function Code. . . . MENU SETUP

Function Type Code . *MNU

Long Function Descr. Function/Options Menu

Stnd Function Descr. Function/Options Menu

Short Descr . . . MENU SETUP

Process Type Code. . *INTER

Audit Activity . . . *NONE (*YES,*NO,*NONE)

Check Authority. . . *YES (*YES,*NO)

Public Authority . . *YES (*YES,*NO)

Auth List Code . . .

Job Parameters Code. . .

Reclaim Resources. . *NO (*YES,*NO)

Dft Appl/Func/Type . _ _ _

F3=Exit

F4=Prompt

F5=Refresh

F9=Window

F11=Delete

F12=Previous

F14=Authority

F15=Menus

F16=User Auth

F21=Text

The details of each of the fields on this panel are defined in the Work With Commands & Programs section. This screen is identical except that menu type functions must be defined as an interactive process and do not allow any command string parameter definitions.

For more information about these fields and function keys, see “Option 1 Work With Cmds (Commands) & Programs” on page 48.

Two additional screens follow the Function Update screen. These screens can be accessed by pressing Enter on this screen and on the screen that follows.

Function Key

F11=Delete - Deletes the menu definition.

Menu Update

The Menu Update Panel enables defining additional information about each menu function such as menu type, function key group, and border colors and characters.

MSKM110	Menu Update	Date: 9/24/08
		Time: 14:34:43
Act Bar/Menu Code. .	MENU SETUP	*Update
Menu Description . .	Function/Options Menu	
Menu Type Code . . .	*STD1 Standard 1 Column Menu	
Function Key Group .	PSKEYS PS Function Keys	
Color.	BLU	
Vertical Char. . . .	:	
Horizontal Char. . .	.	
High Intensity (HI).		
Reverse Image (RI) .		
Underline (UL) . . .		
F3=Exit	F5=Refresh	F9=Window
Enter=Update	F11=Delete	F12=Previous

Act Bar/Menu Code - The 10 character action bar/menu code identifies the specific user menu that is being updated. This name is the same as the function code that was entered on the previous panel.

Menu Description - The description of the action bar/menu. This description is the same as the function description entered on the previous panel and is displayed on all menu browse and window programs.

Menu Type Code - The 8 character menu type code identifies the display type of the menu as either action-bar, pull-down, pop-up, or standard. The Secure Menuing System controls processing based on the menu type. Press **F9=Window** for a selection list of all valid codes. Possible values are:

*ACTBAR	Action Bar (only allowed for function type *ACT)
*PULLDWN	Pull-Down Window
*POPOP	Pop-up Window
*STD1	Standard 1 column full screen menu

Menu Type Description - The description of the menu type.

Function Key Group - The function key group enables you to specify the processing of a particular set of function keys for use with action bars or menus. By setting up a group only one time, you greatly reduce the amount of effort required when creating or changing the processing of function keys used on similar panels. The name of the default function key group is *DEFAULT. This can be altered to suit your own shop standards, or you can create your own function key group. Function key groups are not application dependent. Once a group is set up, it is available to all applications.

Function Key Group Description - The description of the function key group.

Color - The three character color code specifies the color of the border around action bars and windows. The user can change the color designations at any time using the action bar and menu maintenance panels. Any changes will immediately take affect when the screen is initiated. Possible color values are:

- GRN: Green
- WHT: White
- RED: Red
- TRQ: Turquoise
- YLW: Yellow
- PNK: Pink
- BLU: Blue

Vertical Character - The vertical character field allows you to specify the character that you want to represent the horizontal border of action bars and menus. Type any character that you choose. It may be beneficial in menus that overlay each other to use combinations of colors and characters to differentiate the panels to the user.

Horizontal Character - The horizontal character field allows you to specify the character that you want to represent the horizontal border of action bars and menus. Type any character that you choose. It may be beneficial in menus that overlay each other to use combinations of colors and characters to differentiate the panels to the user.

High Intensity (HI) - Type Y (yes) to cause the field to be brighter than other fields when it appears. If you type anything other than Y, your entry will be ignored.

Note

If you specify UL, HI, and RI attributes on the work-station for the same field, the field will not be displayed.

Reverse Image (RI) - Type Y (yes) to cause the field characters to appear as dark characters on a light background. If you type anything other than Y, your entry will be ignored.

Note: If you specify UL, HI, and RI on the workstation for the same field, the result is that the field is not displayed.

Underline (UL) - Type Y (yes) to cause a horizontal line to appear immediately beneath the field. If you type anything other than Y, your entry will be ignored.

Note

If you specify UL, HI, and RI attributes on the workstation for the same field, the field will not be displayed.

Delete Menu - The **F11=Delete Function** key will delete the Menu Definition.

Menu Options Update

The Menu Options Update Panel enables assigning existing functions to options on the action bar or menu panels.

MSTM121Menu Options UpdateDate: 6/30/99Time: 19:28:33

MenuCodeMENU SETUP

MenuDescriptionFunction/Options Menu

MenuType*STD1

Function Types

*MNU = Menu

*PGM = Program

*CMD = Command

*Act = Action Bar

*TXT = Text Line

Type option, press Enter4=Delete

Menu Seq	Menu Opt	Function Code	Func Type	Menu Text or Function Description
= 10	1	WRKCMDPGM	*PGM	Work With Cmds & Programs
- 20	2	WRKMENUE	*PGM	Work With Menus
- 30	3	WRKAB	*PGM	Work With Action Bars
- 40	4	WRKKEYS	*PGM	Work With Function Keys
- 50	5	WRKHELPTXT	*PGM	Work With Help Text
- 60	6	RPTFUNC	*MNU	Function & Menu Reports
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-

F1=Help

F3=Exit

F5=Resequenece

F9=Window

F12=Previous

Menu Option Sequence - The option sequence number is used to list menu options in a specific order on the menu. Sequence numbers can be any number from 1 to 99. These values are not required to be unique upon entry however, the system will automatically re-assign sequence numbers to ensure uniqueness for use in fast-path operations.

Function Code - The 10 character function code identifies the specific process that is to be executed on the menu. The function can be either a program, command, action bar, or menu. It can be processed either interactively or in batch mode.

Function Type Code - The function type identifies the function as either a CL command, program, menu, action bar or text line. The Menu and Security application controls processing based on function type. Possible values are:

*CMD	Command
*PGM	Program
*MNU	Menu
*ACT	Action Bar
*TXT	Text Line

Function Description - The description of the function. This information is displayed on all function browse and window panels.

Option 3 Work With Action Bars

Define the detailed requirements for each action bar.

Action Bar Browse

The Work With Action Bars screen lists all current action bar definitions that have been defined to the Secure Menueing System.

MSMB208

Work With Action Bars

Date: 6/30/99
Time: 19:32:59

Position list to Function Code. . . . _____

Type option, press Enter

1=Select 3=Copy 4=Delete 9=User Security

Function Code	Function Description
= AUTOMENU	Auto Menu Main Menu

Bottom

F1=Help F3=Exit F8=Add F12=Previous

Option

1=Select - Select any of the existing definitions by typing **1** in the option field. You can position the list to a specific menu function by entering the code in the position-to field. Once a menu has been selected or a new menu function has been entered, the Function Update screen will be displayed.

3=Copy - Lets you copy this menu definitions to another name.

4=Delete - Delete any of the existing definitions by typing a **4** in the option field.

9=User Security - Gives you a list of user profiles and lets you see which have authorization.

Function Key

The following special function key is available on this panel:

F8=Add - To add a new definition, press **F8=Add**. The Function Create screen will appear allowing the entry of the action bar code.

Create Action Bar

The Function Create Panel enables the entry of a new action bar function code. The screen is displayed as follows:

```

MSRS200                Function Create                Date:  6/30/99
                                                            Time: 19:36:33

Function Code. . . . _____

Function Type Code . *ACT

F3=Exit                F12=Previous

```

Function Code - The 10 character function code identifies a specific action bar code that is to be created. Each action bar function can be listed on any number of other menus or action bars depending on the needs of the organization.

Function Type Code - The four character function type code identifies the function as an action bar. The Secure Menuing System controls processing based on function type. The value *ACT is automatically defaulted by the system.

Function Update

You can establish and manage detailed information for each action bar function defined to the system.

MSKM200

Function Update

Date: 6/30/99
Time: 19:39:11
*Update

Function Code. . . . AUTOMENU

Function Type Code . *ACT

Long Function Descr. Auto Menu Main Menu

Stnd Function Descr. Auto Menu Main Menu Short Descr . . AUTOMENU

Process Type Code. . *INTER

Audit Activity . . . *NONE (*YES,*NO,*NONE) Confirm Screen. *NO (*YES,*NO)

Check Authority. . . *YES (*YES,*NO) Password. . . .

Public Authority . . *YES (*YES,*NO)

Auth List Code . . .

Job Parameters Code. AUTOMENU

Reclaim Resources. . *NO (*YES,*NO)

Dft Appl/Func/Type . OP *ACT OPERATIONS

F3=Exit

F4=Prompt

F5=Refresh

F9=Window

F11=Delete

F12=Previous

F14=Authority

F15=Menus

F16=User Auth

F21=Text

The details of each of the fields on this panel are defined in the Work With Commands & Programs section. This screen is identical except that action bar type functions must be defined as an interactive process and do not allow any command string parameter definitions. For more information about these fields and function keys, see “Option 1 Work With Cmds (Commands) & Programs” on page 48.

Function Key

F11=Delete Action Bar - Deletes the Action Bar Definition.

Action Bar Update

The Action Bar Update Panel enables defining additional information about each action bar function such as menu type, function key group, and border colors and characters.

MSKM110	Action Bar Update	Date: 6/30/99
		Time: 19:44:26
Act Bar/Menu Code. .	AUTOMENU	*Update
Menu Description . .	Auto Menu Main Menu	
Menu Type Code . . .	*STD1	Standard 1 Column Menu
Menu Cmd Line. . . .	*YES	
Function Key Group .	*DEFAULT	Default Function Keys
Color.	BLU	
Horizontal Char. . . .	_	
High Intensity (HI). .	_	
Reverse Image (RI) . .	_	
Underline (UL)	_	
Start-Up Program . .	MSRP105	
Library.	*LIBL	
Exit Program		
Library.	*LIBL	
F3=Exit	F5=Refresh	F9=Window
F11=Delete	F12=Previous	
Enter=Update		

The details of each of the fields on this panel are defined in the Work With Menus section. This screen is identical except that action bar type functions must be defined as Menu Type Code *ACTBAR (this is filled in by the system).

The Action Bar Update Panel also contains the following program start and exit fields not available for menus:

Start-Up Program - The 10 character start-up program field enables you to specify a program to run before the first menu application panels are displayed to the user. This allows you to tailor the Menu System to work in your environment for any special processing that is needed for the Local Data Area, QTEMP library, etc.

Note

The start-up program is executed after the job parameters have been setup for the session, but before the user is displayed the first action bar panel.

Start-Up Program Library - The library that contains the start-up program.

Exit Program - The exit program field lets you specify special processing at the end of a user's session in the menu application such as clean-up routines or reporting.

Note

The exit program is processed after the user ends the menu session, but before the menu system processes its own clean-up routines.

For more information about these fields and function keys, see "Option 2 Work With Menus" on page 61 of this manual.

Exit Program Library - The library that contains the exit program.

Action Bar Options Update

The Menu Options Update Panel allows you to assign functions to options on the action bar or menu Panels.

MSTM121Menu Options UpdateDate: 6/30/99Time: 19:47:29

MenuCodeAUTOMENU

MenuDescriptionAuto Menu Main Menu

MenuType*STD1

Function Types

*MNU = Menu

*PGM = Program

*CMD = Command

*Act = Action Bar

*TXT = Text Line

Type option, press Enter

4=Delete

Menu Seq	Menu Opt	Function Code	Func Type	Menu Text or Function Description
= 10	1	APPL MENU	*MNU	Applications Menu
- 20	2	MENU SETUP	*MNU	Function/Options Menu
- 30	3	SECURITY	*MNU	User Security & Administration
- 40	4	AUDIT	*MNU	Audit Menu
- 50	5	REPORTS	*MNU	Reports Menu
- 60	6	SELECT APP	*PGM	Select Other Application
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-

F1=Help

F3=Exit

F5=Resequenece

F9=Window

F12=Previous

The details of each of the fields on this panel are defined in the Work With Menus section. For more information about these fields and function keys, see “Option 2 Work With Menus” on page 61.

Function Type Code - Identifies the function as a CL command, program, menu, action bar or text line to control processing. Possible values are:

- *CMD

Command
- *PGM

Program
- *MNU

Menu
- *ACT

Action bar
- *TXT

Text line

Option 4 Work With Function Keys

Set up user-defined function keys groups. Each group specifies the definition of all 24 function keys. Action Bar and Menu panels then provide the specified function keys for user selection.

Function Key Group Browse

The Function Work With Function Keys Panel lists all current group definitions that have been defined to the Secure Menuing System.

MSMB130

Work With Function Keys

Date: 7/01/99
Time: 13:52:08

Position list to Function Key Group . _____

Type option, press Enter

1=Select 3=Copy 4=Delete

Key	Function Key Group
= *DEFAULT	Default Function Keys
- PSKEYS	PS Function Keys

Bottom

F1=Help

F3=Exit

F8=Add

F12=Previous

- 1=Select** - Select any of the existing definitions by typing **1** in the option field. You can position the list to a specific function key group by entering the code in the position-to field. Once a function key group has been selected or a new group code has been entered, the Function Key Group Update screen will be displayed.
- 3=Copy** - Allows you to copy this function key definitions to another name.
- 4=Delete** - A function key definition can be deleted by entering **4** in the option field.

Function Key

The following special function key is available on this panel:

F8=Add - Lets you specify new function key group codes to the system. The Function Key Group Select panel will appear allowing the entry of the group code.

Create Function Key Group

The Function Key Group Select Panel enables the entry of a new function key group codes. The screen is displayed as follows:

```
MSRS130                Function Key Group Select                Date: 7/01/99
                                                                Time: 14:00:02

Function Key Group . *DEFAULT
```

Function Key Group - The function key group enables you to specify the processing of a particular set of function keys for use with action bars or menus. By setting up a group only one time, you greatly reduce the amount of effort required when creating or changing the processing of function keys used on similar panels. The name of the default function key group is *DEFAULT. This can be altered to suit your own shop standards. Function key groups are not application dependent. Once a group is set up, it is available to all applications.

Function Key Group Update

The Function Key Group Update Panel enables assigning a group description, function key colors, and attributes.

MSKM130

Function Key Group Update

Date: 7/01/99
Time: 14:14:13
*Update

Function Key Group . *DEFAULT

Func Key Grp Descr . Default Function Keys

Color GRN

High Intensity (HI) . Y

Reverse Image (RI) . =

Underline (UL) . . . _

F3=Exit

F5=Refresh

F11=Delete

F12=Previous

Enter=Update

Function Key Group Description - The description of the function key group.

Color - The three character color code of the function key descriptions. You can change the color designations at any time and the changes will take affect immediately. Possible color values are:

- GRN Green
- WHT White
- RED Red
- TRQ Turquoise
- YLW Yellow

PNK Pink

BLU Blue

High Intensity (UI) - Type Y (yes) to cause the field to be brighter than other fields when it appears on the panel. If you type anything other than Y, your entry will be ignored.

Reverse Image (RI) - Type Y (yes) to cause the field characters to appear as dark characters on a light background. If you type anything other than Y, your entry will be ignored.

Underline (UL) - Type Y (yes) to cause a horizontal line to appear immediately beneath the field. If you type anything other than Y, your entry will be ignored.

Note

If you specify UL, HI, and RI on the workstation for the same field, the field is not displayed.

Delete Function Key Group - Deletes the Function Key Group Definition.

Function Key Group

The Function Key Group Update Panel assigns function key descriptions for a single key group code.

MSTM141

Function Keys Update

Date: 7/01/99
Time: 14:19:35

Function Key Group

Function Key Group Description

*DEFAULT Default Function Keys

Type details, press Enter.
4=Delete

*Update

Opt	Func Key	Function Key Description	Appl Code	Function Code	Func Type	Process Type
=	<u>1</u>	<u>F1=Help</u>	—	<u>*HELP</u>	—	
-	<u>3</u>	<u>F3=Exit</u>	—	<u>*EXIT</u>	—	
-	<u>6</u>	<u>F6=Messages</u>	QP	<u>DSPMSG</u>	<u>*CMD</u>	
-	<u>9</u>	<u>F9=Window</u>	—	<u>*WINDOW</u>	—	
-	<u>10</u>	<u>F10=Cmd Line</u>	QP	<u>CMD WINDOW</u>	<u>*PGM</u>	
-	<u>12</u>	<u>F12=Previous</u>	—	<u>*PREV</u>	—	
-	<u>13</u>	<u>F13=Attention</u>	MS	<u>ATTENTION</u>	<u>*PGM</u>	*INTER
-	<u>14</u>	<u>F14=Batch Jobs</u>	QP	<u>WRKSBMJOB</u>	<u>*CMD</u>	
-	<u>18</u>	<u>F18=Reports</u>	QP	<u>WRKSPLF</u>	<u>*CMD</u>	

F3=Exit

F9=Window

F12=Previous

Enter=Update

Function Key - This field identifies the function key that is to be processed. The function key must be a 2 digit number with a value from 01 to 24. Each function key is unique within a grouping and can be defined only once.

Function Key Description - The function key description is the text that describes a function key. The user may enter up to 15 characters of text. All text should be entered, including the function key designation. For example, if function key 6 is specified to process the DSPMSG command, then the description might be entered as **F6=Messages**. Note that you must enter **F6** if you want it displayed.

Application Code - The 2 character application code identifies the application function that will be processed when the function key is pressed. This can be any application setup in the system, including applications other than the current one being processed.

Function Code - The 10 character function code identifies a specific process that is to be executed when the function key is selected. Each function key definition specifies processing a function that has been setup within the Secure Menuing System. This integration insures that the function keys will only be allowed for users that are authorized. In addition to functions, special function key definitions can be identified to execute special processes.

*HELP	Displays the user-defined Help text for the function or option that the cursor is on
*EXIT	Processing is returned to the process that originated the function
*PREV	Processing is returned to the previous program
*WINDOW	Displays a window list of available options
*MORE	Displays a list of additional function keys that are available for selection

Function Type Code - Enter the associated 2 character function type to identify the function as either a CL command (*CMD), program (*PGM), menu (*MNU), or action bar(*ACT).

Process Type Code - The process type that has been established for the function.

Option 5 Work With Help Text

These panels enable you to maintain the on-line text for each function. You can also access the Help text maintenance screen from within the function definition screens.

Help Text Browse

The Function Select screen lists all current function definitions that have been defined to the Secure Menuing System.

MSMB200

Function Select

Date: 7/01/99
Time: 14:24:57

Position list to

Function Code.

Function Type Code

Type option, press Enter
1=Select 5=Display

Function Code	Func Type	Function Description	Process Type
= ATTENTION	*PGM	Attention Key Processing	*INTER
- JDBMENU	*MNU	Jim Menu	*INTER
- JDBSPLF	*CMD	Print files	*INTER
- JDBWRKA	*CMD	Work Jobs	*INTER

Bottom

F1=Help

F3=Exit

F12=Previous

Select any of the existing definitions by typing 1 in the option field. You can position the list to a specific function by entering the code in the position-to field. Once a function has been selected, the Function Update screen will be displayed.

Help Text Update

The Function Text Update Panel enables entry of on-line cursor sensitive Help Text that is available when processing user-defined functions.

MSTM230

Function Text Update

Date: 7/01/99
Time: 14:36:34

Function Code	Func Type	Function Description
APPL MENU	*MNU	Applications Menu

Type details, press Enter.

*Update

4=Delete H=Highlight On/Off

Opt

Text

-

The Applications Menu contains options that enable the system administrator to work with application and job parameter information._

-

-

-

-

-

-

-

-

-

F3=Exit

F12=Previous

Enter=Update

Text - Descriptive text about the function. You can add as much text as necessary to describe function processing.

Panel Option

The following special panel option is available on this panel.

H=Highlight On/Off - Type **H** to cause the text line to be brighter than other lines when it appears on the Help text panel.

Option 6 Function & Menu Reports

Print listings of system definitions for all commands, programs, menus, action bars function keys, and Help text.

The Function & Menu Reports Window is displayed as follows:

RPTFUNC

PentaSafe Security Technologies, Inc

ANYUSER

Date: 9/21/08

Function & Menu Reports

QPADEV000B

Time: 14:50:04

Select one of the following:

1

Function by Code

2

Functions by Type

3

Commands & Programs

4

Menus

5

Action Bars

6

Options by Menu

7

Functions by Menu

8

Func Keys by Group

9

Functions Assigned to FKX

10

Function Help Text

Enter Option or Function/Type ==>

F1=Help

F3=Exit

F6=Messages

F9=Window

F10=Cmd Line

F12=Previous

F13=Attention

F14=Batch Jobs

F18=Reports

Select the Option for the report that you would like to print.

Option 3 User Security & Administration

You can manage user security information, establish authorization lists, view current system release information, enter the product purchase code, and access security reports menus.

This menu is accessed by selecting option 3 on the Menu & Security Main Menu.

```
SECURITY          PentaSafe Security Technologies, Inc  ANYUSER      Date:  9/21/08
                  User Security & Administration      QPADEV000B    Time: 15:21:18

Select one of the following:

    Work With User Security                                Work With System Administration
    1 Work With Users                                           11 Work With Companies
    2 Work With Auth Lists                                       12 Installation Defaults Update
    3 User/Security Reports

    99 Mass User Load & Delete

Enter Option or Function/Type ==>

F1=Help          F3=Exit          F6=Messages      F9=Window        F10=Cmd Line
F12=Previous     F13=Attention   F14=Batch Jobs   F18=Reports
```

Type the option number in the command line. For more information about options, command line entry, fast-path selection, and function keys, see “Menu & Security Concepts” on page 7.

Option 1 Work With Users

Specify the system authority definition for a user. The user name must be identical to the iSeries user profile name.

User Authority Browse

The Work With Users lists all current users that are defined to Menu & Security.

MSMB300

Work With Users

Date: 7/01/99
Time: 15:07:20

Position list to User

Type option, press Enter
1=Select 3=Copy 4=Delete

	User	Name	Group Profile	Spec Audit Auth Act
=	*DEFAULT	AUTOMENU Default User		*NO *NONE
-	ACM	Created from DEFAULT	*DEFAULT	*NO *NONE
-	AER	Created from DEFAULT	*DEFAULT	*NO *NONE
-	AJT	Created from DEFAULT	*DEFAULT	*NO *NONE
-	AMB	Created from DEFAULT	*DEFAULT	*NO *NONE
-	BAM	Created from DEFAULT	*DEFAULT	*NO *NONE
-	BTF	Created from DEFAULT	*DEFAULT	*NO *NONE
-	BTFT	Created from DEFAULT	*DEFAULT	*NO *NONE

More...

F1=Help F3=Exit F8=Add F12=Previous F15=By Group

Option

1=Select - Select any of the existing user definitions by entering 1 in the option field. You can position the list to a specific user by entering the name in the position-to field.

3=Copy - Copies the user definition & authorized options only to a new user definition.

4=Delete - Deletes the user definition.

Function Keys

The following function keys are available on this panel:

F8=Add - Adds a new user authority definition. The User Create screen will appear allowing the entry of the user name. The create function key allows you to specify new user names to the system.

Note

When creating a new user profile, the user name must match that of the iSeries user profile ID.

F15=By Group - Displays a browse similar to the display above, but sequenced in order of Group Profile.

Create User

The User Authority Select Panel enables the entry of a new user code. The screen is displayed as follows:

```
MSRS300                               User Authority Select      Date:  7/01/99
                                                                              Time: 15:16:32

User . . . . . _____

F3=Exit                               F12=Previous
```

User - The 10 character User Code identifies each user and is unique within the system. This name must be the same as the associated iSeries user profile. The *DEFAULT authority profile is used by the system as a method of determining authorization rights for any users that are not specifically identified within the system.

User Authority Update

You can establish and manage the detailed authority information for each user defined to the system.

MSKM300	User Authority Update	Date: 7/01/99
		Time: 15:20:54
User	*DEFAULT	*Update
User Name.	<u>AUTOMENU Default User</u>	
Group Profile. . . .	<u> </u>	
Special Authority. .	*NO	
Audit Activity . . .	*NONE	
Default Appl Code. .	QP	
Default Func Code. .	OPERATIONS	
Default Func Type. .	*ACT	
Description.	AS/400 Operations	
Default Company. . .	___ PentaSafe, Inc.	
Display Date Format. M	(M=MDY, D=DY, Y=YMD)	
F3=Exit	F9=Window	F11=Delete
F13=Appl Admin	F14=Auth List Admin	F15=Auth List XREF
F17=Option Auth	F12=Previous	F16=Func Auth XREF

User - The user identifier that was specified on the browse or create panels.

User Name - The full name of the user.

Group Profile - The name of the group profile for this user. The group profile code must be a valid user ID. A group profile must not be a member of another group profile. A user can be a member of only one group profile. However, a group can have authority to multiple functions.

You can create a user specifically as a group profile, or you can specify an existing user profile name. Group profiles provide a way to simplify authority management. They make it easier to change authorities that affect every member in the group.

As an example, if a user moves to a new department within an organization requiring different authorization rights, the only authority change needed for the user is to change the group profile parameter to specify the new group name. The user would then automatically adopt the new rights or limitations.

Special Authority - Overrides all application authority specifications and enables the user to process any function. Special authority should be limited to only those users that need access to all functions in the system. This is similar to being the Security Officer within the iSeries. Possible values are:

- *NO No special authority
- *YES The user has special authority

Audit Activity - Lets you to monitor the function access of specific users. Possible values are:

- *YES Produce an audit transaction, override higher levels
- *NO Do not generate an audit transaction, override higher levels
- *NONE The audit transaction is generated based on criteria of other levels

For more information about audit transactions, see the section on Activity Audit under “Menu & Security Concepts” on page 7.

Default Application, Function, Type - Identifies the default function to be processed if one has not been specifically identified when the user enters the Secure Menuing System. It is also used to specify the function type to be initiated when the user presses the attention “hot-key” while running another menu option. Press **F9=Window** for a selection list of all codes.

Default Company - The company code the user accesses when they begin an application. The description for this company will appear at the top of all full screen menus.

Display Date Format - The default format used to display date fields:

- M Display date in MM/DD/YY format
- D Display date in DD/MM/YY format
- Y Display date in YY/MM/DD format

Function Keys

F11=Delete - Deletes the User Definition.

F13=Appl Admin - The Application Administration Authority Update panel lets you grant users the ability to change the Secure Menuing System definitions for the specified application. Without this authority, the user cannot modify applications. Any user that has Special Authority *YES has access to all applications without the need for these entries.

MSTM311

Application Admin Authority

Date: 7/01/99
Time: 15:26:34

User

Name

*DEFAULT AUTOMENU Default User

Type option, press Enter
4=Delete

Application

Code

Description

= —

- —

- —

- —

- —

- —

- —

- —

- —

F3=Exit F9=Window F12=Previous Enter=Update

F14=Auth List Admin - The Authorization List Administration Authority Update Panel lets you grant users the ability to change Secure Menuing System Authorization List definitions. The user cannot modify an authorization list without this authority. Any user that has Special Authority *YES has access to all lists without the need for these entries.

MSTM321

Authorization List Admin Auth

Date: 7/01/99
Time: 15:29:22

User

Name

*DEFAULTAUTOMENU Default User

Type option, press Enter
4=Delete

Authorization

List Code

Description

=

-

-

-

-

-

-

-

-

F3=Exit

F9=Window

F12=Previous

F15=Auth List XREF - Displays the Authorization List by Users inquiry panel detailing all authorization lists the user profile has been assigned to.

```

_MSTE262                               Authorization List by User                               Date: 7/01/99
                                                                              Time: 15:32:35

User      Name
*DEFAULT

Auth      Func  Begin      End      Begin      End
List      Auth  Date       Date     Time       Time

F1=Help      F3=Exit      F12=Previous

```

F16=Func Auth XREF - The User Function Authority inquiry panel lists all functions, regardless of application, where the user has specific authority rules assigned. These rules were established using the function update screens.

```

_MSTE271                                User Function Authority
Date: 7/01/99
Time: 15:34:42

User      Name
*DEFAULT

Appl      Function      Func  Func  Begin      End      Begin      End
Code      Code          Type  Auth  Date       Date     Time       Time

F1=Help      F3=Exit      F12=Previous

```

F17=Option Authorization - The Work with Option Authorization Panel allows the Security Administrator to set up function authorizations for users or group profiles.

MSTM122

Work With Option Authorization

Date: 7/01/99
Time: 15:38:33

Application. . . OP

Menu OPERATIONS AS/400 Operations

User Name. . . . *DEFAULT AUTOMENU Default User

Group Profile. . .

Check Auth. *NO

Spec Auth . *NO

Spec Auth .

Select Option: 1=Grant Auth 2=Remove Auth 3=Next Menu 5=Function
7=Func Auth 9=Auth List

Mnu Function			Func Check	Publ	Auth List
Opt Code	Type	Description	Auth	Auth	Auth Code
= 1 GENERAL	*MNU	General System Tasks	NO	*YES	*NO
- 2 PROGRAM	*MNU	Programming	NO	*YES	*NO
- 3 COMM MENU	*MNU	Communications Menu	NO	*YES	*NO

Bottom

F1=Help

F3=Exit

F9=Goto Menu

F12=Previous

Options

- 1=Grant Auth** - Grants user profile authorization to the selected function.
- 2=Remove Auth** - Removes user profile's authorization to the selected function.
- 3=Next Menu** - Once a menu has been selected, the Work With Option Authorization screen is redisplayed listing the command, program, and menu functions available for the selected menu.
- 5=Function** - Displays function details and allows you to make any necessary changes.
- 7=Func Auth** - Displays the Function Authority Update screen where you may specify user authority with a date and time range.
- 9=Auth List** - Displays the authorization list definitions, if the selected function has an authorization list.

Function Key

The following function key is available on this panel:

F9=Goto Menu - To display another menu, press **F9=Goto Menu**. The Action Bar & Menu Functions window will appear, allowing the selection of another menu.

Function Authority - The authority that a user has to the function. Individual authority overrides any higher level authority specifications. Possible values are:

*YES Grant function access

*NO No access to the function allowed

Check Authority - Lets you specify authorization checking for individual functions or an entire application. Possible values are:

*YES Check authority for function

*NO Ignore all authority checks for this function

Public Authority - Given to users who do not have authority to the function, are not on the authorization list, and whose group has no specific authority to the object. You can grant or revoke authority to the majority of the users, thereby limiting the number of user authorities that are required. The possible values are:

*YES The user may access the function

*NO The user cannot access the function

Authorization List Code - The authorization list code assigned to the function.

Option 2 Work With Auth (Authorization) Lists

You can create Authorization Lists to determine function authority. A list specifies the authorization rights for many users under a single identifier. This list can then be assigned to multiple functions.

The benefit of this security approach is that complex authority rules can be set up to many users and functions without the problem of having to set up many individual user/function security rules. This limits the total number of detailed authorizations that must be set in the system.

Auth List Browse

Lets you select existing users or create new list definitions.

MSMB250

Work With Authorization Lists

Date: 7/01/99
Time: 15:50:13

Position list to Auth List Code . . . _____

Type option, press Enter
1=Select 3=Copy 4=Delete

Auth List	Authorization List
= *DEFAULT	Default Authorization

Bottom

F1=Help

F3=Exit

F8=Add

F12=Previous

Options

1=Select - Select any of the existing list identifiers by typing 1 in the option field. You can position the list to a specific code by entering the name in the position-to field. Once a list has been selected or a new code entered, the Authorization List Header Panel will be displayed.

3=Copy - Lets you copy any authorization to a different name.

4=Delete - Deletes the Authorization List.

Function Key

The following special function key is available on this panel:

F8=Add - Adds a new Authorization List definition. The create screen appears allowing the entry of the new list code.

Create Auth List

The Authorization List Select Panel lets you enter of a new list code. The screen is displayed as follows:

```
MSRS250                Authorization List Select          Date:  7/01/99
                                                                Time: 15:53:11

Auth List Code . . .  _____

F3=Exit                F12=Previous
```

Authorization List Code - The 10 character Authorization List Code identifies a list of users and the authorities each user has to all functions that the list secures. The Authorization List Code is unique within the system.

Auth List Header Update

You can establish and manage the header authorization information for each list.

MSKM250	Authorization List Update	Date: 7/01/99
		Time: 15:59:38
Auth List Code . . .	AP01	*Add
Auth List Descr. . .		
Public Authority . .	<u>*YES</u>	
F3=Exit	F5=Refresh	F11=Delete
Enter=Update	F12=Previous	F14=Functions

Authorization List Code - The Authorization List identifier that was specified on the browse or create panels.

Authorization List Description - The description of the Authorization List.

Public Authority - The authority given to users:

- who do not have specific authority to the function
- who are not on the authorization list
- who are members of a group with no specific authority to the object

You can grant or revoke authority to the majority of users, thereby limiting the number of specific user authorities that are required. The possible values are:

*YES The user may access the function

*NO The user cannot access the function

Function Keys

The following function keys are available on this panel.

F11=Delete - Deletes the Authorization List Definition.

F14=Functions - List of all functions that are associated with the currently displayed authorization list.

Auth List Update

Lists all users and associated security rules described by the list.

MSTM261

Authorization List Update

Date: 7/01/99
Time: 16:04:40

Auth

Authorization

List

List

Code

Description

AP01

Type details, press Enter.

*Add

4=Delete

Opt	User	Func Auth	Begin Date	End Date	Begin Time	End Time
=	OSEC0FR	*YES	0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		
-			0/00/00	0/00/00		

F3=Exit

F9=Window

F12=Previous

Enter=Update

User - The 10 character user identifier specifies the system name given to an individual user. This name must be the same name as the user profile. The system can then automatically identify and track information for the user without any manual intervention. Press **F9=Window** for a selection list of all codes.

Function Authority - The authority that a user has to the function. The individual authority a user has to a function overrides any higher level authority specifications. Possible values are:

*YES Grant function access

*NO No access to the function allowed

Begin Date - The begin date range for function authorization. This date enables you to specify periods in which users are allowed or denied access to a function.

End Date - The end date range for function authorization. This date enables you to specify the periods in which users are allowed or denied access to a function.

Begin Time - The begin time range for function authorization. This time field enables you to specify periods in which users are allowed or denied access to a function.

End Time - The end time range for function authorization. This date enables you to specify periods in which users are allowed or denied access to a function.

Option 3 User/Security Reports

Lets you to print listings containing information on users, group profiles, authorization lists, and special function authority. You can also obtain cross reference reports such as Authorization Lists by User and Special Authority by User.

The User Security Reports Panel displays as follows:

RPTSECURTY	PentaSafe, Inc.	CAS	Date: 7/01/99
	User/Security Reports	QPADEV0001	Time: 16:09:38

Select one of the following:

- 1 User List
- 2 Users by Group Profile
- 3 User Authoriztion Lists
- 4 Auth Lists by User
- 5 Function Authorization
- 6 Special Auth by User
- 7 User Authorization Report
- 8 Menu Hierarchy Report

Enter Option or Function/Type ==> _____

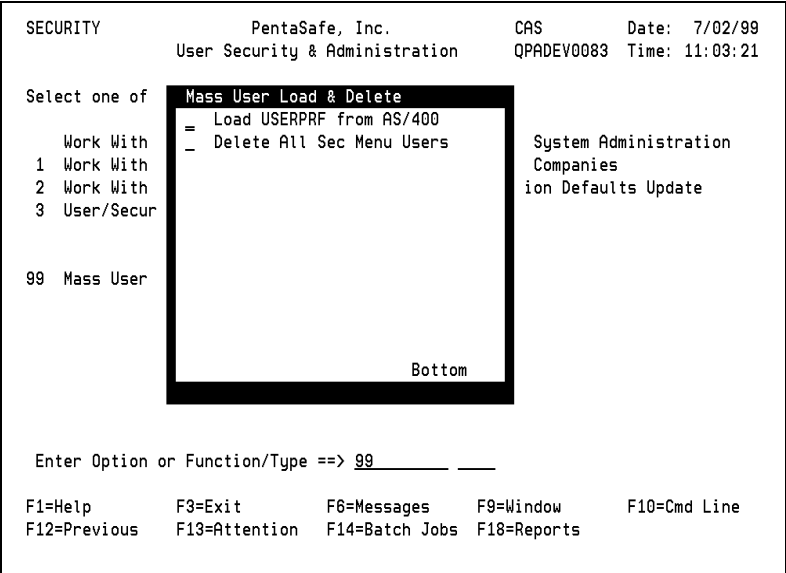
F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

For more information about these reports, see “Option 5 Reports Menu” on page 113.

Option 99 Mass User Load & Delete

For installations that have a large number of iSeries User Profiles, the Mass User Load & Delete options can automatically delete all Secure Menuing System user definitions, or automatically load in profile definitions directly from the system.

The menu appears as a popup screen.



User Load - Processes the Secure Menuing System USERLOAD command. This command allows you to specify either a specific user, a range or all user names. You can identify a current Secure Menuing System user as a default on which to base the new definition. This will automatically create the required definitions for user, function and authorization list definition.

User Delete - Automatically deletes all Secure Menuing System user definitions except those of QSECOFR and *DEFAULT.

Note

The iSeries User Profiles are not deleted.

Option 11 Work With Companies

Lets you create Company Code definitions that will appear at the top of full screen menus. The User Update Panel lets you define what default company the user is assigned to.

The Work With Companies Panel enables the selection of existing companies or the creation of new definitions.

MSMB000	Work With Companies	Date: 7/02/99
		Time: 11:40:20
Position list to		Company Code.
Type option, press Enter		
1=Select 3=Copy 4=Delete		
Company		
Code	Name	
=	PentaSafe, Inc.	
- 22	22 - Demonstration Company	
- 01	PentaSafe, Inc.	
Bottom		
F1=Help	F3=Exit	F8=Add F12=Previous

Options

1=Select - Select any of the existing list identifiers by typing a “1” in the option field. You can position the list to a specific code by entering the name in the position-to field. Once a list has been selected or a new code entered, the Company Update panel will be displayed.

3=Copy - Lets you copy any company definition to a different name.

Function Key

The following special function key is available on this panel:

F8=Add - Adds a new Company Code definition. The Company Select panel will appear allowing the entry of the new company code.

Create Company Code

Lets you enter a new company code. The panel displays as follows:

```
MSRS000                Company Select                Date: 7/02/99
                                                            Time: 11:55:27

Company Code . . . . _

F1=Help                F3=Exit                F12=Previous
```

Option 12 Installation Defaults Update

Lets you control installation wide options for the menu system. Installation defaults include Group Job Control and Exit Message processing.

The Installation Defaults Update window displays as follows:

SECURITY	PentaSafe	Installation Defaults Update	1
	User Sec	Do you want PSSecure/SMS to control group jobs and the attention key? AS/400 User Profile must specify ATNPGM(PSCOMMON/ATTENTION).	5
Select one of the follow		Group Job Control . . . <u>YES</u> (*YES, *NO)	
1 Work With User Secur		Do you want to display the application exit message prompt panel when each user leaves the menu system?	
2 Work With Auth Lists		Display Exit Message. . <u>NO</u> (*YES, *NO)	
3 User/Security Report		Use *LDA to control company processing for your applications?	
99 Mass User Load & Del		Use LDA for Company . . <u>NO</u> (*YES, *NO)	
Enter Option or Functio		Check for new mail items in Office Vision/400?	
F1=Help		Check for New Mail. . . <u>NO</u> (*YES, *NO)	
F3=Exit		Allow entry of function names as options?	
F12=Previous		Allow function name . . <u>YES</u> (*YES, *NO)	
F13=Atte		F3=Exit	F12=Previous

Group Job Control - Do you want Secure Menuing System to control group jobs and the use of the Attention Key? Secure Menuing System will automatically change your interactive session into a group job for use with the Secure Menuing System Attention Key Program PSSECURE/ATTENTION. This parameter works with the iSeries User Profile attention program parameter (ATNPGM). Possible values are *YES or *NO. Note to MAPICS users: Since MAPICS must control its own group jobs, change the value of this parameter to *NO.

Display Exit Message - Controls whether the exit message is displayed when a user leaves the menu system. Possible values are *YES or *NO.

Use LDA for Company - For multi-company applications, use positions 1-2 of the Local Data Area (LDA) for parameter processing. Values are *YES or *NO. If your applications use the LDA for other purposes, change this field to *NO to use the PENTALDA data area in QTEMP.

Check for Mail - Check for new mail items in OfficeVision/400 and display count of items on the full screen menu types *STD1 and *STD2. Possible values are *YES or *NO. If you do not use Office Vision/400, use *NO.

Allow Function Name - Lets you specify whether to a function name and type can be specified in addition to the “normal” menu option number. Specifying *YES permits the user to execute an authorized function that might not be available on the menu being displayed.

Option 4 Audit Menu

Select additional sub-menus to view and report audit activity information that has been captured by the system. You can also clear the data in the audit logs using the clear audit activity option. This menu is accessed by selecting Option 4 on the Menu & Security Main Menu.

AUDIT

PentaSafe Security Technologies

CAS

Date: 6/15/00

Audit Menu

QPADEV0000

Time: 11:18:55

Select one of the following:

1 View Audit Activity

2 Audit Reports Menu

3 Clear Audit Activity

Enter Option or Function/Type ==> _____

F1=Help

F3=Exit

F6=Messages

F9=Window

F10=Cmd Line

F12=Previous

F13=Attention

F14=Batch Jobs

F18=Reports

Enter the option number in the command line. For more information about options, command line entry, fast-path selection, and function keys, see “Menu & Security Concepts” on page 7.

Option 1 View Audit Activity

This function enables you to select options to display the detailed activity information that is contained in the audit logs. These options allow you to view activity in sequence of Date/Time, User, or Function/Type. The Audit Activity Menu is displayed as follows:

```

VIEWAUDIT          PentaSafe Security Technologies      CAS
                   View Audit Activity                  QPADEV000

Select one of the following:

 1 View Activity by Date
 2 View Activity by User
 3 View Activity by Function

Enter Option or Function/Type ==> _____

F1=Help           F3=Exit           F6=Messages       F9=Window
F12=Previous      F13=Attention      F14=Batch Jobs    F18=Reports

```

Enter the option number in the command line. For more information about options, command line entry, fast-path selection, and function keys, see “Menu & Security Concepts” on page 7.

Option 1 View Audit Activity by Date

Displays multiple records of audit activity in ascending order of date and time. You can also position the screen to start at a particular date or time.

MSMB240

Audit Activity by Date

Date: 6/15/00
Time: 11:27:45

Position list to

Audit Date 0/00/00

Audit Time

Type option, press Enter
1=Select 5=Display

	Audit Date	Audit Time	User	Appl Code	Function Code	Func Type	Process Type
-	1/27/00	084414	JDB	MS	WRKMENU	*PGM	*INTER
-	1/31/00	085013	RPD	MS	WRKMENU	*PGM	*INTER
-	1/31/00	123913	RPD	MS	WRKMENU	*PGM	*INTER
-	2/02/00	102826	RPD	MS	WRKMENU	*PGM	*INTER
-	2/02/00	102826	RPD	MS	WRKMENU	*PGM	*INTER
-	2/02/00	112326	RPD	MS	WRKMENU	*PGM	*INTER
-	2/02/00	112326	RPD	MS	WRKMENU	*PGM	*INTER
-	2/03/00	081350	RPD	MS	WRKMENU	*PGM	*INTER

More....

F1=Help

F3=Exit

F12=Previous

F16=By User

F17=By Func

Select any of the activity records to view detailed information by typing a “1” in the option field. You can also position the information on the panel using the following position-to fields:

Audit Date - The date when the audit transaction was recorded. The system will assign this automatically for each audit record.

Audit Time - The time when the audit transaction was recorded. The system assigns the time automatically for each audit record.

User - Identifies the audited menu user.

Appl Code - Identifies the audited application.

Function Code - Identifies the audited function within the application.

Function Type - Identifies the type of the Function Code.

Process Type - Identifies whether the function is interactive (*INTER) or batch (*BATCH).

Option 2 Audit Activity by User

Lets you display a list of audit activity records in user sequence. This enables the Administrator to identify all activity for a particular user.

MSMB241		Audit Activity by User				Date: 6/15/00	
						Time: 11:33:09	
Position list to		User		<u> </u>			
		Audit Date		<u>0/00/00</u>			
Type option, press Enter		Audit Time		<u> </u>			
1=Select							
	Audit	Audit	Appl	Function	Func	Proc	
User	Date	Time	Code	Code	Type	Type	
- ARP	3/21/00	152746	MS	AUDIT	*MNU	*INTER	
- ARP	3/21/00	152856	MS	AUDIT	*MNU	*INTER	
- ARP	3/21/00	153032	MS	AUDIT	*MNU	*INTER	
- ARP	4/07/00	101247	MS	APPL MENU	*MNU	*INTER	
- ARP	4/07/00	101247	MS	MENU SETUP	*MNU	*INTER	
- ARP	4/07/00	101247	MS	WRKMENU	*PGM	*INTER	
- ARP	4/07/00	101854	MS	MENU SETUP	*MNU	*INTER	
- ARP	4/07/00	101854	MS	WRKMENU	*PGM	*INTER	
							More....
F1=Help		F3=Exit		F12=Previous			

Select any of the activity records to view detailed information by typing **1** in the option field. You can also position the information on the panel using the following position-to fields:

User - The 10 character user identifier specifies the system name given to an individual user. This name must be the same name as the user profile. The system can then automatically identify and track information for the user without any manual intervention.

Audit Date - The date when the audit transaction was recorded. The system will assign this automatically for each audit record.

Audit Time - The time when the audit transaction was recorded. The system assigns the time automatically for each audit record.

Appl Code - Identifies the audited application.

Function Code - Identifies the audited function within the application.

Function Type - Identifies the type of the Function Code.

Process Type - Identifies whether the function is interactive (*INTER) or batch (*BATCH).

Option 3 Audit Activity by Function

Displays multiple records of audit activity in order of application, function, and function type. You can also position the display to start at a particular record in the file.

MSMB242

Audit Activity by Function

Date: 6/15/00
Time: 11:35:23

Position list to

Application Code . . . _

Function Code. . . . _

Function Type Code . _

Audit Date 0/00/00

Audit Time _

Type option, press Enter
1=Select

Appl Code	Function Code	Func Type	Audit Date	Audit Time	User
- MS	APPL MENU	*MNU	3/14/00	142935	UXR
- MS	APPL MENU	*MNU	3/15/00	120533	UXR
- MS	APPL MENU	*MNU	3/15/00	120533	UXR
- MS	APPL MENU	*MNU	3/15/00	153803	RPD
- MS	APPL MENU	*MNU	3/15/00	155038	RPD
- MS	APPL MENU	*MNU	3/15/00	165731	UXR
- MS	APPL MENU	*MNU	3/16/00	072050	RPD

More....

F1=Help

F3=Exit

F12=Previous

Select any of the activity records to view detailed information by typing 1 in the option field. You can also position the information on the panel using the following position-to fields:

Application Code - The two character application code identifies the application that is to be delimited.

Function Code - The 10 character function code identifies a specific process that is to be listed on the screen.

Function Type Code - The four character function type identifies the specific function type that is to be listed.

Audit Date - The date when the audit transaction was recorded will be listed on the screen. The system will assign this automatically for each audit record.

Audit Time - The time when the audit transaction was recorded. The system assigns the time automatically for each audit record.

User - The User Profile is listed.

Option 2 Audit Reports Menu

This menu contains reporting options for listing information contained in the audit activity logs. Reports can be printed to analyze system activity in sequence of Date/Time, Function/Type, and User.

The Audit Reports Menu is displayed as follows:

REPORTS	PentaSafe Security Technologies, Inc	ANYUSER	Date: 9/21/08
	Reports Menu	QPADEV000B	Time: 17:05:25

Select one of the following:

- 1 Application by Code
- 2 User/Security Reports
- 3 Function & Menu Reports
- 4 Audit Reports Menu

Enter Option or Function/Type ==> _____

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Type the option number in the command line. For more information about options, command line entry, fast-path selection, and function keys, see “Menu & Security Concepts” on page 7.

Option 3 Clear Audit Activity

You can delete all history records from the audit activity log. Type the option number on the command line and press **Enter**. The audit history is cleared.

Option 5 Reports Menu

The Work With Reports Menu enables you to print the application report and display other report menus for security, function, menu, and audit information.

This menu is accessed by selecting Reports Menu (Option 5) on the Menu & Security Main Menu.

REPORTS	PentaSafe Security Technologies	CAS	Date:
	Reports Menu	QPADEV0000	Time:
Select one of the following:			
1 Application by Code			
2 User/Security Reports			
3 Function & Menu Reports			
4 Audit Reports Menu			
Enter Option or Function/Type ==> _____			
F1=Help	F3=Exit	F6=Messages	F9=Window
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports
F10=C			

Enter the option number on the command line. For more information about options, command line entry, fast-path selection, and function keys, see “Menu & Security Concepts” on page 7.

Option 1 Application by Code

This report lists detailed information for all applications, and is submitted to batch for processing.

The Application by Code Report lists the parameters for each application. This report is submitted to batch.

MSMR010 Applications Report			User: ANYUSER			Date: 2/23/08		Time: 16:18:07 Page: 1			
Appl Application	Job	Dsply	Menu	Check	Audit	Dflt	Dflt	Start-Up	Start-Up	Exit	Exit
Code Description	Parms	Non-	Cmd	Auth	Act	Func	Type	Program	Pgm Lib	Program	Pgm Lib
		Auth	Line								
EX	Elite TIE Export System	EXJPARM	*NO	*YES	*NO	*NONE			*LIBL		*LIBL
RD	Personal Menus		*NO	*YES	*NO	*NONE		EXI000	*LIBL	EXI001	*LIBL
HE	test		*YES	*YES	*NO	*NONE			*LIBL		*LIBL
KK	KK Test Environment		*YES	*YES	*NO	*NONE			*LIBL		*LIBL
LN	Test Application		*NO	*YES	*NO	*NONE			*LIBL		*LIBL
MK	PENTA Prospector	PENTAMK	*NO	*YES	*NO	*NONE	MAIN ACT	*ACT MKI000	*LIBL	MKI001	*LIBL
MS	Auto Menu Definitions	AUTOMENU	*YES	*YES	*NO	*NONE				MSRP106	*LIBL
OP	Operations		*YES	*YES	*NO	*NONE	OPERATIONS	*ACT	*LIBL		*LIBL
RG	Rockefeller Group		*YES	*YES	*NO	*NONE			*LIBL		*LIBL
SD	Training Application		*YES	*YES	*NO	*NONE			*LIBL		*LIBL
TE	Test Environment for SH		*NO	*YES	*NO	*NONE			*LIBL		*LIBL
TO	Training Office Depot		*NO	*YES	*NO	*NONE			*LIBL		*LIBL
TR	Training Application		*NO	*YES	*YES	*NONE			*LIBL		*LIBL
TS	Test Application		*YES	*YES	*NO	*NONE			*LIBL		*LIBL

Option 2 User/Security Reports

This menu lists options allowing you to print reports containing information on users, group profiles, authorization lists, and special function authority. You can also obtain cross reference reports such as authorization lists by user, and special authority by user.

The User/Security Reports Menu is displayed as follows:

RPTSECURTY	PentaSafe Security Technologies	CAS	Date: 6/15/00
	User/Security Reports	QPADEV0000	Time: 12:36:20

Select one of the following:

- 1 User List
- 2 Users by Group Profile
- 3 User Authoriztion Lists
- 4 Auth Lists by User
- 5 Function Authorization
- 6 Special Auth by User
- 7 User Authorization Report
- 8 Menu Hierarchy Report

Enter Option or Function/Type ==> _____

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Enter the option number in the command line. The following reports are available from this menu.

Option 1 User List

The User List Report prints the details of each user in the system. This report is submitted to batch.

MSMR300	User Authority User: ALE		Date: 2/25/08	Time: 14:38:57		Page: 1	
User	Name	Group Profile	Spec Auth	Audit Activity	Dflt Appl	Dflt Func Code	Dflt Type
*DEFAULT	AUTOMENU Default User		*YES	*NONE	OP	OPERATIONS	*ACT
ALE	Anna Ethridge		*YES	*NONE			
AMADMIN1	AutoMenu Administrator testEHD		*NO	*NONE	HD	MENU_ZP	*MNU
AMADMIN2	AutoMenu Administrator testEHD		*NO	*NONE	HE	MENU_ZP	*MNU
ASR	Andrea Russel	*DEFAULT	*NO	*NONE	OP	OPERATIONS	*ACT
AUTO	Prospector user for Auto Prods		*NO	*NONE			
BAM	Created from DEFAULT	*DEFAULT	*YES	*NONE	OP	OPERATIONS	*ACT
BOB	Created from DEFAULT	*DEFAULT	*YES	*NONE	MK	MAIN	*MNU
BWE	Brian W. Earley, Contractor		*NO	*NONE			
CHARLIE	Charlie Crider		*NO	*NONE	MK	MAIN ACT	*ACT
COMMTTEST	Created from DEFAULT	*DEFAULT	*YES	*NONE	OP	OPERATIONS	*ACT
CONSOLE	RSS - Console Profile		*NO	*NONE	MK	MAIN ACT	*ACT
CSC	Christopher S. Criezis		*NO	*NONE			
DAS	Douglas A. Strain		*NO	*NONE			
DEY	Created from DEFAULT	*DEFAULT	*YES	*NONE	OP	OPERATIONS	*ACT
DLC	Dan Clark		*YES	*NONE	OP	OPERATIONS	*ACT

Option 2 Users by Group Profile

The User by Group Profile Report lists all of the users that are associated with a group profile. This report is submitted to batch.

MSMR301	User By Group Profile		User: ALE	Date: 2/25/08	Time: 14:41:47 Page: 1		
Group Profile	User	Name	Spec Auth	Audit Activity	Dflt Appl	Dflt Func Code	Dflt Type
	*DEFAULT	AUTOMENU Default User	*YES	*NONE	OP	OPERATIONS	*ACT
	ALE	Anna Ethridge	*YES	*NONE			
	AMADMIN1	AutoMenu Administrator testEHD	*NO	*NONE	HD	MENU_ZP	*MNU
	AMADMIN2	AutoMenu Administrator testEHD	*NO	*NONE	HE	MENU_ZP	*MNU
	AUTO	Prospector user for Auto Prods	*NO	*NONE			
	BWE	Brian W. Earley, Contractor	*NO	*NONE			
	CHARLIE	Charlie Crider	*NO	*NONE	MK	MAIN ACT	*ACT
	CONSOLE	RSS - Console Profile	*NO	*NONE	MK	MAIN ACT	*ACT
	CSC	Christopher S. Criezis	*NO	*NONE			
	DAS	Douglas A. Strain	*NO	*NONE			
	DLC	Dan Clark	*YES	*NONE	OP	OPERATIONS	*ACT
	GAW	Greg White	*NO	*NONE			
	GCG	George Grenrood	*NO	*NONE			
	GDC	Gray Geiselman	*NO	*NONE			
	GENERAL	General User	*NO	*NONE			
	GPM	Gary McNeel, Jr.	*NO	*NONE			

Option 3 User Authorization Lists

The User Authorization List Report prints detailed security information for each Authorization List. This report is submitted to batch.

MSMR260	User by Authorization List		User: ALE		Date: 2/25/08	Time: 14:43:35		Page: 1	
Auth List	Auth List Description	Publ Auth	User	Name	Func	BeginEnd Auth	Begin Date	End DateTime	Time
*DEFAULT	Default Authorization	*NO	QSECOFR	Security Officer	*YES	0/00/00		0/00/00	000000 00000
EHD	test	ALE	Anna Ethridge		0/00/00		0/00/00	000000	00000
		EHD	ELI			0/00/00		0/00/00	000000 00000
Number of records processed = 3									
End of report.									

Option 4 Auth Lists by User

The Authorization List by User Report prints all of the Authorization Lists assigned to each user. This report is submitted to batch.

MSMR262		Authorization List by User		User: ALE	Date: 2/25/08	Time: 14:45:17		Page: 1		
User	Name	List	Auth Description	Auth List	Func Date	Begin Date	End	Begin Time	End Time	Pub Aut
ALE	Anna Ethridge	EHD	test				0/00/00	0/00/00		000000
000000 *YE										
EHD	ELI	EHD	test				0/00/00	0/00/00		000000
000000 *YE										
QSECOFR	Security Officer		*DEFAULT	Default Authorization		*YES	0/00/00	0/00/00		000000
000000 *NO										
Number of records processed = 3										
End of report.										

Option 5 Function Authorization

The Function Authorization Report lists the special user authorization information defined for each function. This report is submitted to batch.

MSMR270		Special Authority by Function		User: ALE		Date: 2/25/08		Time: 14:46:54		Page: 1	
Appl	Function	Func	Function	User	Name	Func Begin	End	Begin	End		
Code	Code	Type	Description			Auth Date	Date	Time	Time		
EX	AAUP	*PGM		AMADMIN2	AutoMenu Administrator	testEHD*NO	00/00/00	0/00/00	0000000000000000		
				ASR	Andrea Russel	*NO	0/00/00	0/00/00	000000	000000	
				JCP	Jennifer Purucker	*NO	0/00/00	0/00/00	0000000000	000000	
	EXF000	*PGM		KAK	Keith Kreuer	*NO	0/00/00	0/00/00	000000	000000	
	EXF030	*PGM		KAK	Keith Kreuer	*NO	0/00/00	0/00/00	000000	000000	
LN	DISPLAY	*CMD		CHARLIE	CHARLIE Crider	*YES	0/00/00	0/00/00	000000	000000	
				CONSOLE	RSS - Console Profile	*YES	0/00/00	0/00/00	0000000000	000000	
				KAK	Keith Kreuer	*YES	0/00/00	0/00/00	000000	000000	
MK	MKF000	*PGM		*DEFAULT	AUTOMENU Default User	*NO	0/00/00	0/00/00	0000000000	000000	
	MKF310	*PGM		KAK	Keith Kreuer	*YES	0/00/00	0/00/00	000000	000000	
MS	RPT111	*PGMMenu Hierarchy Report		REH	Robert Haynes	*YES	0/00/00	0/00/00	000000	000000	
	RPT300	*PGMUser List		REH	Robert Haynes	*YES	0/00/00	0/00/00	000000	000000	
	RPT301	*PGMUsers by Group Profile		REH	Robert Haynes	*YES	0/00/00	0/00/00	000000	000000	
	WRKCMDPGM	*PGMWork With Cmds & Programs		REH	Robert Haynes	*YES	11/16/94	11/16/94	000000	151500	
OP	CMD WINDOW	*PGM		CHARLIE	CHARLIE Crider	*NO	0/00/00	0/00/00	000000	000000	
					CONSOLE	RSS - Console Profile	*NO	0/00/00	0/00/00		
000000 000000											

Option 6 Special Auth by User

The Special Authorization by User Report lists all of the special function authorization that is defined for each user. This report is submitted to batch.

MSMR271		Special Authority by User		User: ALE	Date: 2/25/08	Time: 14:49:19	Page:		
User Time	Name	Appl Code	Function Code	Func Type	Function Description	Func Begin Auth Date	End Date	Begin Date	End Time
	*DEFAULT	AUTOMENU Default User	MK MKF000	*PGM		*NO	0/00/00	0/00/00	000000
			OP GENERAL	*MNU		*NO	0/00/00	0/00/00	000000
	AMADMIN2	AutoMenu Administrator	test EHDEX	AAUP	*PGM	*NO	0/00/00	0/00/00	000000
			ASR	AAUP		*NO	0/00/00	0/00/00	000000
	CHARLIE	Charlie Crider	LN	DISPLAY		*YES	0/00/00	0/00/00	000000
			OP	CMD WINDOW		*NO	0/00/00	0/00/00	000000
			TR	COMMAND	*PGM	*YES	0/00/00	0/00/00	000000
			DISPLAY	*CMD		*YES	0/00/00	0/00/00	000000
			T1	AAUP	*PGM	*YES	0/00/00	0/00/00	000000
			ALOG	*CMD		*YES	0/00/00	0/00/00	000000
				MAIN1	*CMD	*YES	5/20/94	6/30/94	000000
				MAIN111		*YES	5/20/94	6/30/94	000000
				MAIN12	*CMD	*YES	0/00/00	0/00/00	000000
				MAIN4		*NO	0/00/00	0/00/00	000000
				T2	*PGM	*YES	0/00/00	0/00/00	000000
				CMDENTRY2		*YES	0/00/00	0/00/00	000000

Option 7 User Authorization Report

The User Authorization Report lists all functions for each user and indicates whether the user has access to the function. When the report is executed, the following parameter window is displayed enabling you to specify reporting options.

RPTSECURTY	PentaSafe Security Technologies	CAS	Date: 6/15/00
	User/Security Reports	QPADEV0000	Time: 12:39:13

Select one of the following:

- 1 User List
- 2 Users by Group Profile
- 3 User Authorization Lists
- 4 Auth Lists by User
- 5 Function Authorization
- 6 Special Auth by User
- 7 User Authorization Repo
- 8 Menu Hierarchy Report

User Authorization Report

Enter a valid User Id or *ALL to select all users for the report.

User Id . . . _____

Select print option to list all functions, authorized functions, or not authorized.

Print Option. *ALL (*ALL, *YES, *NO)

F1=Help F3=Exit F4=List F12=Previous

Enter Option or Function/T

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Enter a valid User ID or press **F4=List** to display a list of all valid user profiles. Type *ALL in the User ID field if you want to print the report for all users. The print option allows you to print all functions (*ALL), just those that the user has authority to (*YES), or those that the user does not have authority to process (*NO).

Layout

Once all parameters are selected, press **Enter** and the following report will be submitted to batch.

MSMR302		User Authorization Report			User: CAS	Page: 1	Date: 7/07/08 Time: 13:16:16
Appl	Function	Func	Function	Function			
Code	Code	Type	Description	Authorized			
User.	CAS	Created from DEFAULT					
	ATTENTION	*PGM	Attention Key Processing	YES			
	JDBMENU	*MNU	Jim's Menu	YES			
	JDBSPLF	*CMD	Work with Spool Files	YES			
	JDBWRKA	*CMD	Work with Active Jobs	YES			
	MS	*MNU		YES			
JB	JDBMENU	*MNU	Jim's Menu	YES			
JB	JDBSPLF	*CMD	Work with Spool Files	YES			
JB	JDBWRKA	*CMD	Work with Active Jobs	YES			
MS	APPL MENU	*MNU	Applications Menu	YES			
MS	ATTENTION	*PGM	Attention Key Processing	YES			
MS	AUDIT	*MNU	Audit Menu	YES			
MS	AUDTRYDATE	*PGM	View Activity by Date	YES			
MS	AUDTRYFUNC	*PGM	View Activity by Function	YES			
MS	AUDTRYUSER	*PGM	View Activity by User	YES			
MS	AUTOMENU	*ACT	Auto Menu Main Menu	YES			
MS	AUTOMENU	*MNU	Menu & Security Main Menu	YES			
MS	CLEARAUDIT	*PGM	Clear Audit Activity	YES			
MS	CRTAPPL	*PGM	Create New Application	YES			
MS	EXITMSG	*PGM	Installation Defaults Update	YES			
MS	MENU SETUP	*MNU	Function/Options Menu	YES			

Option 8 Menu Hierarchy Report

The Menu Hierarchy Report lists all functions by menu option sequence for each user. The report indicates whether the user has access to the function. When the report is executed, the following parameter window is displayed enabling you to specify reporting options.

RPTSECURTY	PentaSafe Security Technologies	CAS	Date: 6/15/00
	User/Security Reports	QPADEV0000	Time: 12:42:55

Select one of the following:

- 1 User List
- 2 Users by Group Profile
- 3 User Authorization Lists
- 4 Auth Lists by User
- 5 Function Authorization
- 6 Special Auth by User
- 7 User Authorization Repo
- 8 Menu Hierarchy Report

Menu Hierarchy Selection

Enter a valid User Id or *ALL to select all users for the report.
User Id . . . *ALL _____

Enter a specific menu to start the hierarchy or *USER to start at the user default menu.
Application . . . _____ name
Function. . . _____ name, *USER
Type. _____ *MNU, *ACT

F1=Help F3=Exit F4=List F12=Previous

Enter Option or Function/T

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Enter a valid User ID or press **F4=List** to display a list of user profiles. Type *ALL in the User ID field if you want to print the report for all users.

Select a primary menu or action bar as a starting point for the hierarchy list by entering the specific application, function and type. This is typically the Main Menu or Action Bar process for your application. If each user has a different starting menu, type *USER to start the hierarchy at the default menu that has been established for the user. See the User Authority Update screen for more information on user defaults.

Layout

Once all parameters are selected, press **Enter** and the following report will be submitted to batch.

MSMR111				User Authorization Report		User: CAS		Page: 1	Date: 7/07/08
								Time: 13:16:40	
Appl Code	Menu Code	Menu Type	Menu/Action Bar Description	Function Authorized	Opt Seq	Function Code	Function Type	Function Description	
User.	*DEFAULT	AUTOMENU	Default User						
OP	OPERATIONS	*ACTBAR	AS/400 Operations	YES				Options	
				YES	1	GENERAL	*MNU	General System Tasks	
				YES	2	PROGRAM	*MNU	Programming	
				YES	3	COMM MENU	*MNU	Communications Menu	
OP	GENERAL	*PULLDWN	General System Tasks	YES				Options	
				YES	1	WRKJOB	*CMD	Work With Job	
				YES	2	WRKROUTQ	*CMD	Work With Output Queues	
				YES	3	WRKACTJOB	*CMD	Work With Active Jobs	
				YES	4	WRKWTR	*CMD	Work With Printers	
				YES	5	WRKJOBQ	*CMD	Work With Job Queues	
				YES	6	WRKSBJMJOB	*CMD	Work With Submitted Jobs	
				YES	7	PROGRAM	*MNU	Programming	
OP	PROGRAM	*PULLDWN	Programming	YES				Options	
				YES	1	STRPDM	*CMD	Start PDM	
				YES	2	STRSDA	*CMD	Start Screen Design Aid	
				YES	3	STRDFU	*CMD	Start Data File Utility	
				YES	4	STRQRY	*CMD	Start Query	
----- Options									

Option 3 Function & Menu Reports

Lets you print listings of system definitions for all commands, programs, menus, action bars, function keys, and help text.

The Function Reports Menu is displayed as follows:

RPTFUNC	PentaSafe Security Technologies	CAS	Date: 6/15/00
	Function & Menu Reports	QPADEV0000	Time: 12:45:32

Select one of the following:

- 1 Function by Code
- 2 Functions by Type
- 3 Commands & Programs
- 4 Menus
- 5 Action Bars
- 6 Options by Menu
- 7 Functions by Menu
- 8 Func Keys by Group
- 9 Functions Assigned to FKY
- 10 Function Help Text

Enter Option or Function/Type ==> _____

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Select the desired option and type the option number on the command line. The following reports are available from the menu above:

Option 1 Function by Code

Lists all functions defined to the system in sequence of application, function, and function type. This report is submitted to batch.

MSMR200		Function by Code		User: CAS		Date: 7/07/08		Time: 13:56:37		Page: 1		
Appl Code	Function Code	Func Type	Function Description	Process Type	Rclm Rsrc	Audit Act	Check Auth List	Publ Auth	Job Parameters	Dflt Default Appl	Dflt Func Code	Dflt Type
JB	ATTENTION	*PGM	Attention Key Processing	*INTER	*NO	*NONE	*YES *DEFAULT	*NO				
	JDBMENU	*MNU	Jim Menu	*INTER	*NO	*NONE	*NO	*NO				
	JDBSPLF	*CMD	Print files	*INTER	*NO	*NONE	*NO	*NO				
	JDBWRKA	*CMD	Work Jobs	*INTER	*NO	*NONE	*NO	*NO				
	MS	*MNU		*INTER	*NO	*NONE	*YES	*NO				
	JDBMENU	*MNU	Jim Menu	*INTER	*NO	*NONE	*NO	*NO				
	JDBSPLF	*CMD	Work Reports	*INTER	*NO	*NONE	*NO	*NO				
	JDBWRKA	*CMD	Work with Jobs	*INTER	*NO	*NONE	*NO	*NO				
	MS	*MNU		*INTER	*NO	*NONE	*YES	*NO				
	APPL MENU	*MNU	Applications Menu	*INTER	*NO	*NONE	*YES	*YES				
MS	ATTENTION	*PGM	Attention Key Processing	*INTER	*NO	*NONE	*YES *DEFAULT	*NO				
	AUDIT	*MNU	Audit Menu	*INTER	*NO	*NONE	*YES	*YES				
	AUDTBYDATE	*PGM	View Activity by Date	*INTER	*NO	*NONE	*YES	*NO				
	AUDTBYFUNC	*PGM	View Activity by Function	*INTER	*NO	*NONE	*YES	*NO				
	AUDTBYUSER	*PGM	View Activity by User	*INTER	*NO	*NONE	*YES	*NO				
	AUTOMENU	*ACT	Auto Menu Main Menu	*INTER	*NO	*NONE	*YES	*YES	AUTOMENU	OP	OPERATIONS	*ACT
		*MNU	Menu & Security Main Menu	*INTER	*NO	*NONE	*YES	*YES				
	CLEARAUDIT	*PGM	Clear Audit Activity	*INTER	*NO	*NONE	*YES	*NO				
	CRTAPPL	*PGM	Create New Application	*INTER	*NO	*NONE	*YES	*NO				
	EXITMSG	*PGM	Installation Defaults Upd	*INTER	*NO	*NONE	*YES	*NO				
MENU SETUP		*MNU	Function/Options Menu	*INTER	*NO	*NONE	*YES	*YES				
	MS RELEASE	*PGM	MS System Release Level	*INTER	*NO	*NONE	*YES	*NO				
	PURCHASE	*PGM	Purchase Prompt Panel	*INTER	*NO	*NONE	*YES	*NO				

Option 2 Functions by Type

Lists all functions in sequence of function type. This report is submitted to batch.

MSMR202		Function by Type		User: CAS		Date: 7/07/08		Time: 14:20:39		Page: 1			
Appl Code	Func Code	Function Type	Function Description	Process Type	Rclm Rsrc	Audit Act	Check Auth	Auth List	Publ Job Auth	Job Parameters	Dflt Appl	Default Func Code	Dflt Type
	*CMD	JDBSPLF	Print files	*INTER	*NO	*NONE	*NO		*NO				
		JDBWRKA	Work Jobs	*INTER	*NO	*NONE	*NO		*NO				
	*MNU	JDBMENU	Jim Menu	*INTER	*NO	*NONE	*NO		*NO				
		MS		*INTER	*NO	*NONE	*YES		*NO				
	*PGM	ATTENTION	Attention Key Processing	*INTER	*NO	*NONE	*YES	*DEFAULT	*NO				
JB	*CMD	JDBSPLF	Work Reports	*INTER	*NO	*NONE	*NO		*NO				
		JDBWRKA	Work with Jobs	*INTER	*NO	*NONE	*NO		*NO				
	*MNU	JDBMENU	Jim Menu	*INTER	*NO	*NONE	*NO		*NO				
MS	*ACT	AUTOMENU	Auto Menu Main Menu	*INTER	*NO	*NONE	*YES		*YES	AUTOMENU	OP	OPERATIONS	*ACT
	*CMD	USERDEL	Delete All Sec Menu Users	*INTER	*NO	*NONE	*YES		*YES				
		USERLOAD	Load USERPRF from AS/400	*INTER	*NO	*NONE	*YES		*NO				
	*MNU	APPL MENU	Applications Menu	*INTER	*NO	*NONE	*YES		*YES				
		AUDIT	Audit Menu	*INTER	*NO	*NONE	*YES		*YES				
		AUTOMENU	Menu & Security Main Menu	*INTER	*NO	*NONE	*YES		*YES				
		MENU SETUP	Function/Options Menu	*INTER	*NO	*NONE	*YES		*YES				
		REPORTS	Reports Menu	*INTER	*NO	*NONE	*YES		*YES				

Option 3 Commands & Programs

Lists detailed information of all command and program function types in code sequence. This function is submitted to batch.

MSMR207		Command & Program Functions		User: CAS		Date: 7/07/08		Time: 14:28:42		Page: 1		1	
Appl	Function	Func	Process	Rclm	Audit	Check	Auth	Publ	Job	Dflt	Dflt	Dflt	
Code	Code	Description	Type	Type	Rsrc	Act	Auth	Auth	Parameters	Apppl	Func	Code	Type
	ATTENTION	*PGM Attention Key Processing	*INTER	*NO	*NONE	*YES	*DEFAULT	*NO					
	JDBSPLF	*CMD Print files	*INTER	*NO	*NONE	*NO		*NO					
	JDBWRKA	*CMD Work Jobs	*INTER	*NO	*NONE	*NO		*NO					
JB	JDBSPLF	*CMD Work Reports	*INTER	*NO	*NONE	*NO		*NO					
	JDBWRKA	*CMD Work with Jobs	*INTER	*NO	*NONE	*NO		*NO					
MS	ATTENTION	*PGM Attention Key Processing	*INTER	*NO	*NONE	*YES	*DEFAULT	*NO					
	AUDTBYDATE	*PGM View Activity by Date	*INTER	*NO	*NONE	*YES		*NO					
	AUDTBYFUNC	*PGM View Activity by Function	*INTER	*NO	*NONE	*YES		*NO					
	AUDTBYUSER	*PGM View Activity by User	*INTER	*NO	*NONE	*YES		*NO					
	CLEARAUDIT	*PGM Clear Audit Activity	*INTER	*NO	*NONE	*YES		*NO					
	CRTAPPL	*PGM Create New Application	*INTER	*NO	*NONE	*YES		*NO					
	EXITMSG	*PGM Installation Defaults Upd	*INTER	*NO	*NONE	*YES		*NO					
	MS RELEASE	*PGM MS System Release Level	*INTER	*NO	*NONE	*YES		*NO					
	PURCHASE	*PGM Purchase Prompt Panel	*INTER	*NO	*NONE	*YES		*NO					

Option 4 Menus

Lists all menu type functions in code sequence. This report is submitted to batch.

MSMR204		Menu Functions		User: CAS		Date: 7/07/08		Time: 15:07:09		Page: 1	
Appl	Function	Func	Function	Process	Rclm	Audit	Check	Auth		Publ	Job
Code	Code	Type	Description	Type	Rsrc	Act	Auth	List		Auth	Parameters
	JDBMENU	*MNU	Jim Menu	*INTER	*NO	*NONE	*NO			*NO	
	MS	*MNU		*INTER	*NO	*NONE	*YES			*NO	
JB	JDBMENU	*MNU	Jim Menu	*INTER	*NO	*NONE	*NO			*NO	
MS	APPL MENU	*MNU	Applications Menu	*INTER	*NO	*NONE	*YES			*YES	
	AUDIT	*MNU	Audit Menu	*INTER	*NO	*NONE	*YES			*YES	
	AUTOMENU	*MNU	Menu & Security Main Menu	*INTER	*NO	*NONE	*YES			*YES	
	MENU SETUP	*MNU	Function/Options Menu	*INTER	*NO	*NONE	*YES			*YES	
	REPORTS	*MNU	Reports Menu	*INTER	*NO	*NONE	*YES			*YES	
	RPTAUDIT	*MNU	Audit Reports Menu	*INTER	*NO	*NONE	*YES			*NO	
	RPTFUNC	*MNU	Function & Menu Reports	*INTER	*NO	*NONE	*YES			*NO	
	RPTSECURITY	*MNU	User/Security Reports	*INTER	*NO	*NONE	*YES			*NO	
	SECURITY	*MNU	User Security Menu	*INTER	*NO	*NONE	*YES			*YES	
	USRMSSG	*MNU	User Load & Delete	*INTER	*NO	*NONE	*YES			*NO	
	VIEWAUDIT	*MNU	View Audit Activity	*INTER	*NO	*NONE	*YES			*NO	
OP	COMM MENU	*MNU	Communications Menu	*INTER	*NO	*NONE	*YES			*NO	

Option 5 Action Bars

Lists detailed information on all action bar function types. This report is submitted to batch.

MSMR208		Action Bar Functions		User: CAS		Date: 7/07/08		Time: 15:19:32		Page: 1	
Appl Function Code Code	Func Function Type Description	Process Type	Rclm Rsrc	Audit Act	Check Auth	Auth List	Publ Job Auth Parameters	Dflt Appl	Dflt Func	Dflt Code	Dflt Type
MS	AUTOMENU	*ACT	Auto Menu	Main Menu							
OP	OPERATIONS	*ACT	AS/400	Operations							
		*INTER	*NO	*NONE	*YES		*YES	AUTOMENU	OP	OPERATIONS	*ACT
		*INTER	*NO	*NONE	*YES		*NO				

Number of records processed = 2
End of report.

Option 6 Options by Menu

Lists each menu/action bar along with the processing options that are available. This function is submitted to batch for processing.

MSMR120		Options by Menu/Action Bar		User: CAS		Date: 7/07/08		Time: 15:30:17		Page: 1	
Appl Code	Menu Code	Menu Type	Menu/Action Bar Description	Opt Seq	Function Code	Func Type	Function Description	Process Type			
	JDBMENU	*POPUP	Jim Menu	1	JDBSPLF	*CMD	Print files	*INTER			
					JDBSPLF	*CMD	Print files	*INTER			
				2	JDBWRKA	*CMD	Work Jobs	*INTER			
					JDBWRKA	*CMD	Work Jobs	*INTER			
JB	JDBMENU	*POPUP	Jim Menu	1	JDBSPLF	*CMD	Print files	*INTER			
					JDBSPLF	*CMD	Print files	*INTER			
				2	JDBWRKA	*CMD	Work Jobs	*INTER			
					JDBWRKA	*CMD	Work Jobs	*INTER			
MS	APPL MENU			1	CRTAPPL	*PGM					
				2	SELECT APP	*PGM					
				3	WRKAPPL	*PGM					
				4	WRKJOBPARM	*PGM					
	AUDIT			1	VIEWAUDIT	*MNU					
				2	RPTAUDIT	*MNU					
				3	CLEARAUDIT	*PGM					
	AUTOMENU			1	APPL MENU	*MNU					
				2	MENU SETUP	*MNU					
				3	SECURITY	*MNU					
				4	AUDIT	*MNU					
				5	REPORTS	*MNU					
				6	SELECT APP	*PGM					
	MENU SETUP			1	WRKCMDFPGM	*PGM					
				2	WRKMENU	*PGM					
				3	WRKAB	*PGM					
				4	WRKKEYS	*PGM					
				5	WRKHELPTXT	*PGM					
				6	RPTFUNC	*MNU					
	REPORTS			1	RPT010	*PGM					

Option 7 Functions by Menu

Lists the menus on which each function is defined. This process is submitted to batch.

MSMR122		Func Assigned to Menus/Act Bar		User: CAS	Date: 7/07/08	Time: 15:35:38	Page: 1	
Appl Code	Function Code	Func Type	Function Description	Process Type	Menu Code	Menu Type	Menu/Action Bar Description	Opt Seq
JB	JDBSPLF	*CMD	Print files	*INTER	JDBMENU	*POPUP	Jim Menu	1
						*POPUP	Jim Menu	1
	JDBWRKA	*CMD	Work Jobs	*INTER	JDBMENU	*POPUP	Jim Menu	2
						*POPUP	Jim Menu	2
	JDBSPLF	*CMD	Print files	*INTER	JDBMENU	*POPUP	Jim Menu	1
						*POPUP	Jim Menu	1
JB	JDBWRKA	*CMD	Work Jobs	*INTER	JDBMENU	*POPUP	Jim Menu	2
						*POPUP	Jim Menu	2
						*POPUP	Jim Menu	2
						*POPUP	Jim Menu	2
						*POPUP	Jim Menu	2
						*POPUP	Jim Menu	2
MS		*TXT			SECURITY			
	APPL MENU	*MNU			AUTOMENU			1
	AUDIT	*MNU			AUTOMENU			4
	AUDTBYDATE	*PGM			VIEWAUDIT			1
	AUDTBYFUNC	*PGM			VIEWAUDIT			3
	AUDTBYUSER	*PGM			VIEWAUDIT			2
	CLEARAUDIT	*PGM			AUDIT			3
	CRTAPPL	*PGM			APPL MENU			1
	EXITMSG	*PGM			SECURITY			12
	MENU SETUP	*MNU			AUTOMENU			2
	REPORTS	*MNU			AUTOMENU			5
	RPTAUDIT	*MNU			AUDIT			2
					REPORTS			4

Option 8 Func Keys by Group

Lists the details of all function key groups. This report is submitted to batch.

MSMR140		Function Keys by Group		User: CAS	Date: 7/07/08	Time: 15:39:47		Page: 1	
Function Key Group	Function Key Group Description	Func Key	Function Key Description	Appl Code	Function Code	Func Type	Function Description	Process Type	
*DEFAULT	Default Function Keys	1	F1=Help		*HELP				
		3	F3=Exit		*EXIT				
		6	F6=Messages	OP	DSPMSG	*CMD			
		9	F9=Window		*WINDOW				
		10	F10=Cmd Line	OP	CMD WINDOW	*PGM			
		12	F12=Previous		*PREV				
		13	F13=Attention	MS	ATTENTION	*PGM	Attention Key Processing	*INTER	
		14	F14=Batch Jobs	OP	WRKSBMJOB	*CMD			
		18	F18=Reports	OP	WRKSPLF	*CMD			
		24	F24=More Keys		*MORE				
		1	F1=Help		*HELP				
		3	F3=Exit		*EXIT				
		6	F6=Messages	OP	DSPMSG	*CMD			
		9	F9=Window		*WINDOW				
PSKEYS	PS Function Keys	10	F10=Cmd Line	OP	CMD WINDOW	*PGM			
		12	F12=Previous		*PREV				
		13	F13=Attention	MS	ATTENTION	*PGM	Attention Key Processing	*INTER	
		14	F14=Batch Jobs	OP	WRKSBMJOB	*CMD			
		18	F18=Reports	OP	WRKSPLF	*CMD			
		24	F24=More Keys		*MORE				
		Number of records processed = 20							
		End of report.							

Option 9 Functions Assigned to FKY

Lists all of the key groups that are assigned to each function. This report is submitted to batch.

MSMR142		Functions Assigned to FKeys		User: CAS	Date: 7/07/08	Time: 15:45:00		Page: 1
Appl Code	Function Code	Func Type	Function Description	Function Key Group	Function Key Group Description	Func Key	Function Key Descr	
	*EXIT			*DEFAULT	Default Function Keys	3	F3=Exit	
				PSKEYS	PS Function Keys	3	F3=Exit	
	*HELP			*DEFAULT	Default Function Keys	1	F1=Help	
				PSKEYS	PS Function Keys	1	F1=Help	
	*MORE			*DEFAULT	Default Function Keys	24	F24=More Keys	
				PSKEYS	PS Function Keys	24	F24=More Keys	
	*PREV			*DEFAULT	Default Function Keys	12	F12=Previous	
				PSKEYS	PS Function Keys	12	F12=Previous	
	*WINDOW			*DEFAULT	Default Function Keys	9	F9=Window	
				PSKEYS	PS Function Keys	9	F9=Window	
MS	ATTENTION	*PGM	Attention Key Processing	*DEFAULT	Default Function Keys	13	F13=Attention	
				PSKEYS	PS Function Keys	13	F13=Attention	
OP	CMD WINDOW	*PGM		*DEFAULT	Default Function Keys	10	F10=Cmd Line	
				PSKEYS	PS Function Keys	10	F10=Cmd Line	
	DSPMSG	*CMD		*DEFAULT	Default Function Keys	6	F6=Messages	
				PSKEYS	PS Function Keys	6	F6=Messages	
	WRKSBMJOB	*CMD		*DEFAULT	Default Function Keys	14	F14=Batch Jobs	
				PSKEYS	PS Function Keys	14	F14=Batch Jobs	
	WRKSPLF	*CMD		*DEFAULT	Default Function Keys	18	F18=Reports	
				PSKEYS	PS Function Keys	18	F18=Reports	
Number of records processed = 20								
End of report.								

Option 10 Function Help Text

Lists the Help text that has been specified for each function in the system. This report is submitted to batch.

MSMR230 Function Help Text				User: CAS	Date: 7/07/08	Time: 15:48:39	Page: 1
Appl	Function	Func	Function	Text			
Code	Code	Type	Description				
	ATTENTION	*PGM	Attention Key Processing	The Attention Key Processing program enables you to specify the menu option or function key to be used to initiate and pass control to a secondary group job process. This feature allows you to temporarily leave the current screen you are in, process another function that you have defined to the system, and then return to the same place that you left. The command or program that is processed is the default application, function, and type that is identified to the original function.			
MSKE185							
MS	APPL MENU	*MNU		The Applications Menu contains options that enable the system administrator to work with application and job parameter information.			
	ATTENTION	*PGM	Attention Key Processing	The Attention Key Processing program enables you to specify the menu option or function key to be used to initiate and pass control to a secondary group job process. This feature allows you to temporarily leave the current screen you are in, process another function that you have defined to the system, and then return to the same place that you left. The command or program that is processed is the default application, function, and type that is identified to the original function.			
AUDIT				The Audit Menu enables you to select additional sub-menus to			
	AUDTBYDATE	*PGM		This View Activity by Date option enables you to display multiple			

Option 4 Audit Reports Menu

Displays reporting options for listing information contained in the Audit Activity logs. Reports can be printed to analyze system activity in sequence of:

- Date/Time
- Function/Type
- User

The Audit reports Menu is displayed as follows:

RPTAUDIT	PentaSafe Security Technologies	CAS	Date: 6/15/00
	Audit Reports Menu	QPADEV0000	Time: 11:37:54

Select one of the following:

- 1 Audit Activity by Date
- 2 Audit Activity by User
- 3 Audit Activity by Func

Enter Option or Function/Type ==> _____

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Select the desired option and enter the option number on the command line. The following reports are available from the menu above:

Option 1 Audit Activity by Date

Lists the detailed information contained in the audit log in sequence of Date, Time. This report is submitted to batch.

MSMR240		Audit Activity by Date			User: CAS		Date: 7/07/08	Time: 16:37:38		Page: 1
Audit Date	Audit Time	User	Appl Code	Function Code	Func Type	Function Description	Process Type	Processed From Function	Proc From Type	
9/18/95	092816	KAK	MS	AUTOMENU	*MNU		*INTER	STRMS	*CMD	
	092827	KAK	MS	SECURITY	*MNU		*INTER	AUTOMENU	*MNU	
		KAK	MS	AUDIT	*MNU		*INTER	AUTOMENU	*MNU	
		KAK	MS	VIEWAUDIT	*MNU		*INTER	AUDIT	*MNU	
		KAK	MS	AUDTBYDATE	*PGM		*INTER	VIEWAUDIT	*MNU	
		KAK	MS	MENU SETUP	*MNU		*INTER	AUTOMENU	*MNU	
		KAK	MS	WRKCMDPGM	*PGM		*INTER	MENU SETUP	*MNU	
		KAK	MS	AUDIT	*MNU		*INTER	AUTOMENU	*MNU	
		KAK	MS	RPTAUDIT	*MNU		*INTER	AUDIT	*MNU	
		KAK	MS	RPT240	*PGM		*BATCH	RPTAUDIT	*MNU	
		KAK	MS	WRKSBMJOB	*CMD		*INTER	RPTAUDIT	*MNU	
		KAK	MS	MENU SETUP	*MNU		*INTER	AUTOMENU	*MNU	
		KAK	MS	WRKCMDPGM	*PGM		*INTER	MENU SETUP	*MNU	
		KAK	MS	APPL MENU	*MNU		*INTER	AUTOMENU	*MNU	
		KAK	MS	WRKAPPL	*PGM		*INTER	APPL MENU	*MNU	
		KAK	MS	WRKJOBPFARM	*PGM		*INTER	APPL MENU	*MNU	
		KAK	MS	CMD WINDOW	*PGM		*INTER	APPL MENU	*MNU	
		KAK	MS	MENU SETUP	*MNU		*INTER	AUTOMENU	*MNU	
		KAK	MS	WRKCMDPGM	*PGM		*INTER	MENU SETUP	*MNU	
		KAK	MS	SECURITY	*MNU		*INTER	AUTOMENU	*MNU	
		KAK	MS	WRKUSER	*PGM		*INTER	SECURITY	*MNU	
		KAK	MS	APPL MENU	*MNU		*INTER	AUTOMENU	*MNU	
		KAK	MS	WRKAPPL	*PGM		*INTER	APPL MENU	*MNU	
Number of records processed =			23							
End of report.										

Option 2 Audit Activity by User

Lists detailed audit information contained in the audit log in user sequence. This report is submitted to batch.

MSMR241	Audit Activity by User				User: CAS		Date: 7/07/08	Time: 16:41:40		Page: 1
User	Audit Date	Audit Time	Appl Code	Function Code	Func Type	Function Description	Process Type	Processed From Function	Proc From Type	
KAK	9/18/95	092816	MS	AUTOMENU	*MNU		*INTER	STRMS	*CMD	
		092827	MS	SECURITY	*MNU		*INTER	AUTOMENU	*MNU	
			MS	AUDIT	*MNU		*INTER	AUTOMENU	*MNU	
			MS	VIEWAUDIT	*MNU		*INTER	AUDIT	*MNU	
			MS	AUDTBYDATE	*PGM		*INTER	VIEWAUDIT	*MNU	
			MS	MENU SETUP	*MNU		*INTER	AUTOMENU	*MNU	
			MS	WRKCMDPGM	*PGM		*INTER	MENU SETUP	*MNU	
			MS	AUDIT	*MNU		*INTER	AUTOMENU	*MNU	
			MS	RPTAUDIT	*MNU		*INTER	AUDIT	*MNU	
			MS	RPT240	*PGM		*BATCH	RPTAUDIT	*MNU	
			MS	WRKSSBJOB	*CMD		*INTER	RPTAUDIT	*MNU	
			MS	MENU SETUP	*MNU		*INTER	AUTOMENU	*MNU	
			MS	WRKCMDPGM	*PGM		*INTER	MENU SETUP	*MNU	
			MS	APPL MENU	*MNU		*INTER	AUTOMENU	*MNU	
			MS	WRKAPPL	*PGM		*INTER	APPL MENU	*MNU	
			MS	WRKJOBPARM	*PGM		*INTER	APPL MENU	*MNU	
			MS	CMD WINDOW	*PGM		*INTER	APPL MENU	*MNU	
			MS	MENU SETUP	*MNU		*INTER	AUTOMENU	*MNU	
			MS	WRKCMDPGM	*PGM		*INTER	MENU SETUP	*MNU	
			MS	SECURITY	*MNU		*INTER	AUTOMENU	*MNU	
			MS	WRKUSER	*PGM		*INTER	SECURITY	*MNU	
			MS	APPL MENU	*MNU		*INTER	AUTOMENU	*MNU	
			MS	WRKAPPL	*PGM		*INTER	APPL MENU	*MNU	
Number of records processed = 23										
End of report.										

Option 3 Audit Activity by Function

Lists the detailed activity information contained in the audit log in sequence of application, function, and function type. This report is submitted to batch.

MSMR241	Audit Activity by User				User: CAS	Date: 7/07/08	Time: 16:41:40	Page: 1	
User	Audit Date	Audit Time	Appl Code	Function Code	Func Type	Function Description	Process Type	Processed From Function	Proc From Type
KAK	9/18/95	092816 092827	MS	AUTOMENU	*MNU		*INTER	STRMS	*CMD
			MS	SECURITY	*MNU		*INTER	AUTOMENU	*MNU
			MS	AUDIT	*MNU		*INTER	AUTOMENU	*MNU
			MS	VIEWAUDIT	*MNU		*INTER	AUDIT	*MNU
			MS	AUDTBYDATE	*PGM		*INTER	VIEWAUDIT	*MNU
			MS	MENU SETUP	*MNU		*INTER	AUTOMENU	*MNU
			MS	WRKCMDPGM	*PGM		*INTER	MENU SETUP	*MNU
			MS	AUDIT	*MNU		*INTER	AUTOMENU	*MNU
			MS	RPTAUDIT	*MNU		*INTER	AUDIT	*MNU
			MS	RPT240	*PGM		*BATCH	RPTAUDIT	*MNU
			MS	WRKSBMJOB	*CMD		*INTER	RPTAUDIT	*MNU
			MS	MENU SETUP	*MNU		*INTER	AUTOMENU	*MNU
			MS	WRKCMDPGM	*PGM		*INTER	MENU SETUP	*MNU
			MS	APPL MENU	*MNU		*INTER	AUTOMENU	*MNU
			MS	WRKAPPL	*PGM		*INTER	APPL MENU	*MNU
			MS	WRKJOBPARM	*PGM		*INTER	APPL MENU	*MNU
			MS	CMD WINDOW	*PGM		*INTER	APPL MENU	*MNU
			MS	MENU SETUP	*MNU		*INTER	AUTOMENU	*MNU
			MS	WRKCMDPGM	*PGM		*INTER	MENU SETUP	*MNU
			MS	SECURITY	*MNU		*INTER	AUTOMENU	*MNU
			MS	WRKUSER	*PGM		*INTER	SECURITY	*MNU
			MS	APPL MENU	*MNU		*INTER	AUTOMENU	*MNU
			MS	WRKAPPL	*PGM		*INTER	APPL MENU	*MNU
Number of records processed =			23						
End of report.									

Option 6 Select Other Application

This option enables you to select another application for modification of menu and security definitions. The Application Browse Panel lists all current application codes that are defined to the Secure Menuing System.

For more information on selecting, creating new, and updating applications, see the MS Main Menu section, beginning with “Option 1 Applications Menu” on page 32.

Chapter 3

Profile & Password Management

System Overview

Profile and Password Management is designed to help you manage user profiles and control your users' passwords easily, securely, and efficiently on a network of iSeries servers. The downsizing trend of recent times has left many IS departments understaffed, but with increased responsibilities. With this in mind, NetIQ Security Solutions for iSeries has a tool to ease the chore of maintaining user profiles. The task of creating, changing, and deleting user profiles can now be delegated to a non-technical user or to a System Operator through the use of the Profile Templates.

Additionally, with the many problems in recent years regarding computer security and computer networks, one of the main concerns identified by auditors is the regular changing of passwords. With the Profile Synchronizer feature of Profile and Password Management, a user can now easily have the same password on each iSeries system to which he or she has access by simply changing their password on any one of the networked systems. Profile and Password Management will automatically change the user's password on each networked system.

Because the sharing of passwords is commonplace in most computer environments, another inevitable problem is the selection of passwords. Most users select their own passwords. Normally, they choose something easy to remember, such as a spouse's name or birth date. But passwords that are easy to remember are also easy to figure out by an unauthorized user. This explains why auditors have cracked down severely on password procedures. Profile and Password Management will help you secure your computer and satisfy the auditors' requirements for password procedures.

Function

Profile and Password Management offers two methods to create passwords. The first method, System Generated Passwords, will allow you to generate new, random passwords for your users, then change them at a later date after the users have been notified. The second method, User Prompted Passwords, will allow each user to change his own password based on an expiration time period. Either method can utilize the Profile Synchronizer feature of Profile and Password Management.

With the first method, User Prompted Passwords, each user changes his own password. Under this method, each time the user signs on to the system, the password is checked to see if it has expired. If the password has expired, the user will be immediately prompted to enter a new password. This second method has two variations- i5/OS User Prompted Passwords and NetIQ User Prompted Passwords. The i5/OS User Prompted Passwords variation requires that a Password Validation Program be used.

The NetIQ User Prompted Password variation has several tailoring options such as variable password usage, expiration days, variable history log, and masking value designs.

With the second method, System Generated Passwords, simply select the Auto Generate and Print Passwords option and the system will assign new user passwords. The user profile is not actually changed at this time, only the password is generated. Upon completion of the Generate and Print job, you will have a "Notification of Password Change" report with one user profile and password per page to distribute to your users. The report will inform your users of their new passwords and the effective date.

When you are ready to actually change the passwords, select the “Change user profiles” option and the new passwords will be effective the next time the users sign on to the system.

Main Menu

Selecting Option 2 from the PSSecure Menu screen will take you to the Profile and Password Management Main Menu. The Main Menu contains all of the options you need to operate Profile and Password Management.

PS2	PentaSafe Security Technologies Profile & Password Management	CAS QPADEV0000C	Date: 8/29/00 Time: 9:41:26
-----	--	--------------------	--------------------------------

Select one of the following:

- 1 General Options Menu
- 2 Profile Synchronizer Menu
- 3 Profile Templates Menu
- 4 AS/400 Password System Values
- 5 PS User-Prompted Passwords Menu
- 6 PS System-Generated Passwords Menu

Enter Option or Function/Type ==> _____

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Option 1 General Options Menu

Lets anyone with *SECOFR or *SECADM authority work with users of Profile and Password Management. This menu also supplies a report of ALL users on your system.

PS21	PentaSafe Security Technologies, Inc	ANYUSER	Date: 9/15/08
	General Options Menu	QPADEV000P	Time: 16:26:11

Select one of the following:

- 1 Work with user profiles
- 2 Report of Users
- 4 Load New User Profiles
- 5 Clean up user profile files

User Profile Management

- 15 Reactivate Profile From Archive
- 16 Change Defaults (DISABLE DELETE +)
- 17 User Profile Exclusions
- 18 Archived User Profiles Report

Enter Option or Function/Type ==>

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Option 1 Work With User Profiles

This option allows you to work with users of Profile and Password Management, and those who have changed their passwords via Profile and Password Management.

Note

If you changed a user profile without using Option 4 (Load New User Profiles) on the Profile and Password Management General Options Menu (page 138), the changes will not appear on the Work with Users screen.

ZPRP13T1	Profile and Password Management				6/07,
ISIS	Work With Users				
Type Options, press Enter.					
1=Display 2=Edit 3=Copy 4=Delete 5=Disable 6=Enable 7=Expire Passw					
8=Display Selected Info					
1					
	(1)	(2)	(3)		
Opt	User	Group	Template	Change	Description
—	AAA	*NONE	SBL4	2000-06-01	CHANGED DESCRIPTION I
—	AAAAAA	*NONE	SBL4	2000-06-05	CHANGED DESCRIPTION
—	AAA1	*NONE	SBL4	2000-06-05	NEW DESCRIPTION
—	AA12	*NONE	PMBTST	2000-06-05	CHANGING DESCRIPTION
—	AA12CPY	*NONE	SBL4	2000-06-05	CHANGING DESCRIPTION
—	ABCD	*NONE	SUTEMP	2000-06-05	test1
—	ABCDEF	*NONE	STEST	2000-06-05	abcdefgh user profile
—	ABCSU1	*NONE	PAYROLL	2000-06-05	ABC BLANK TEMPLATE
—	ABCTST	*NONE	STEST	2000-06-05	*BLANK
—	ACCCUSTPRF	*NONE	SUTEMP	2000-06-05	
					More
F3=Exit F5=Refresh F6=Add F7=Work with Template F8=Work with Archive					
(c) Copyright 1999, PentaSafe, Inc.					

Options

1 = **Display** - Displays basic user profile information as provided by IBM's DSPUSRPRF command, such as:

- Previous sign-on date and time
- sign-on attempts not valid

- status (*enabled/*disabled)
- date password last changed

2 = Change - Lets you make changes to a user profile. The current values are displayed.

3 = Copy - Copies a user profile's attributes and prompts with the CRTUSRPRF command.

4 = Delete - Accesses the Work with Users screen to confirm the deletion of the selected user profile. Press Enter to confirm the deletion and return to the Work with Users screen. To return to the Work with Users screen without deleting the displayed user profile, press F12 (Cancel).

If you try to delete a user profile that owns objects, a pop-up window displays requiring you to enter a user profile that will be assigned the owned objects. Type the user profile in the **User profile to own objects** field, and press **Enter** to delete the selected user profile and transfer ownership of the objects. To cancel the delete function and return to the Work with Users screen, press **F12**.

ZPRP13T3	Profile and Password Management	13:09:51	9/24/08
ANYSYSTEM	Work With Users		

Work With Users
Press Enter to confirm your choices for Delete.

Opt Us	User profile USER1 owns objects.	xt
4 US	To delete user profile USER1, owned objects must be transferred to another user.	
	User profile to own objects _____	
	F12=Cancel	

Bottom

F3=Exit F12=Cancel

Searching for all owned objects for USER1.

5 = Disable - Changes the user profile so it is not valid for sign-on.

6 = Enable - Changes the user profile so that it is valid for sign-on.

7 = Expire Password - Force the expiration of a user profile's password. If a password validation program is in use and the password expiration interval is other than *NOMAX, the operating system will prompt for the new password. If not, the NetIQ Security Solutions for iSeries user Prompted Password method will be activated if it has been implemented.

8 = Display selected information - Displays the selected information.

Column - Type the number of the column (1-Sort by User, 2-Sort by Group, 3-Sort by Template) that you want to use to sort data on the screen and press **Enter**. The data appears in ascending order. When any of the above options are used and **Enter** is pressed, the data on the screen is rearranged and sorted by the column entered in the sort field.

The fields above the User, Group and Template, are 'position to' fields for the respective columns. To position to a specific User, enter the User name (partially or fully) and the data is repositioned to the nearest value of the position-to User column entry.

Sort Criteria (1) - Type the name of a user profile and press **Enter**. The user profile is repositioned to the top of the column. The remaining user profiles are listed below in ascending order.

Sort Criteria (2) - Type the name of a group profile and press **Enter**. The first user profile associated with the group profile is repositioned to the top of the column. The remaining group profiles are listed below in ascending order.

Sort Criteria (3) - Type the name of a template and press **Enter**. The first user profile based on the template is repositioned to the top of the column. The remaining profiles are listed below in ascending order.

User - The user you select to administer.

Group - The name of the group profile associated with the user profile.

Template - The name of the template the profile is assigned to.

Change - The date the record was last changed.

Description - User defined text that briefly describes the group.

Function Keys

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

F3=Exit - Returns you to the General Options menu.

F5=Refresh - Will redisplay the screen, reflecting any changes made. All entries in the **Opt** and the Selection Criteria columns are cleared from the screen.

F6=Add - Press **F6** to create a new user profile based on the selected template. Type **1** next to the desired template and press **Enter**. When a template has been selected, you are taken to a screen to create the new user profile with all the parameters populated from the template selected. These parameters can be changed to the values valid for that template. The fields can be prompted by pressing **F4**. A window appears showing the values valid for that field.

F7=Work with Templates - Lets you manage user profile templates.

F8=Work with Archive - Lets you work with archived user profiles. Type **6** next to the profile you want to reactivate.

Attn - Displays an action bar for general system tasks, programming tasks, and communication tasks.

Option 2 Report of Users

Lets you specify the parameters for printing a report. This report includes all user profiles on your system and is not limited to Profile and Password Management users. You can list single or multiple user profiles, and specify the report sort and processing environment. The report contains information such as user, group, class, password change and sign-on dates, and invalid sign-on attempts.

ZPCL11	Profile and Password management User Information Report	08:12:08 5/22/00 System: ISIS
Type the following and press Enter:		
User profile.....	<u>*ALL</u>	(*ALL, generic*, or single user profile)
Sort for report.....	<u>U</u>	(U=User profile, G=Group profile)
How to run report...	<u>I</u>	(I=Interactive, B=Batch)
Jobq for batch job..	<u>QBATCH</u>	
Outq for report.....	<u>QPRINT</u>	
Hold output.....	<u>*NO</u>	(*YES, *NO)
Number of copies....	<u>1</u>	
<hr/>		
Data elements on report:	User profile Group profile User class	User profile text Last password change date Previous signon date Number of invalid signon attempts
F3=Exit	ENTER=Submit/Run	

Report Layout

A sample User Report is as follows:

Display Spooled File										Page/Line	1/2
File	QSYSPRT									Columns	1 - 130
Control											
Find											
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9...+...0...+...1...+...2...+...											
ZPRP11	ISIS	PROFILE AND PASSWORD MANAGEMENT USER PROFILE REPORT							8/29/08	14:44:17	Page:
Selection: *ALL											
Sort: by USER											
User	Group	Profile	User Class	Profile	Password	Previous	Invalid	Signon			
Profile	Profile			Crt Date	Chg Date	Exp Date	SignonDt	Attempts	User Profile Text		
=====											
0AAA	*NONE	*USER		00/06/14	00/06/14	00/07/29	00/00/00		TEST PROFILE		
AAA	*NONE	*USER		00/04/10	00/04/10	00/04/30	00/00/00		CHANGED DESCRIPTION FOR PROFILE		
AAAAA	*NONE	*USER		00/06/20	00/06/20	00/08/04	00/06/20		TEST		
AAAAAA	*NONE	*USER		00/04/13	00/04/13	00/05/28	00/00/00		CHANGED DESCRIPTION		
AAAAATEST	*NONE	*USER		00/06/28	00/06/28	00/08/12	00/00/00		TEST		
AAAA1	RPD	*USER		00/06/20	00/06/20	00/08/04	00/06/20		TEST		
AAAA2	*NONE	*USER		00/06/20	00/06/20	00/08/04	00/06/20		TEST		
AA1	*NONE	*USER		00/05/10	00/05/10	00/06/24	00/00/00		NEW DESCRIPTION		
AA1	*NONE	*USER		00/06/13	00/06/13	00/07/28	00/00/00				
AA12	*NONE	*USER		00/04/10	00/04/10	00/05/25	00/00/00		CHANGING DESCRIPTION		
AA12CPY	*NONE	*USER		00/05/15	00/05/15	00/06/29	00/00/00		CHANGING DESCRIPTION		
AA2	*NONE	*USER		00/06/13	00/06/13	00/07/28	00/00/00				
											More.
F3=Exit	F12=Cancel	F19=Left	F20=Right	F24=More keys							

Option 4 Load New User Profiles

Loads new user profiles by loading the Work With Users file. By loading this file, you can work with user profiles through Option 1. Work with Users.

Option 5 Clean Up User Profiles

Cleans up the user profiles used by Profile and Password Management. This option will delete records for non-existent user profiles from the files used by Work With User Profiles.

User Profile Management

Allows automatic disabling, deletion and archiving of unused profiles. Archived profiles can be re-activated. Profiles in the archive are automatically deleted after a user-specified number of days.

To start using the User Profile Management tool:

1. Select Option 17 to add user profile exclusions and press **Enter**. Enter the user profiles that should not be disabled, such as Q*, and press **Enter**, then press **F3** to Exit.
2. Select Option 16 to change the defaults and press **Enter**. Specify the desired values and press **Enter**.
3. Use **F7** to schedule the job that will disable, delete and archive profiles. Specify the desired job scheduling options and press **Enter**.

Option 15 Reactivate Profile From Archive

Displays the list of user profiles in the archive of deleted profiles.

To reactivate a profile, select it from the list with Option 6 and press **Enter**. Use **F3** to Exit. Profiles are reactivated with expired default passwords.

ISIS
ZPRP27

Work with Archived User Profiles

8/29/00
17:33:16

Type choices, press Enter.
6=Reactivate profile

Position to . . . : _____

Opt	Profile	Date Archived	Description
-	AAA2	5/26/00	
-	CLST	8/05/00	
-	CVELL	6/15/00	
-	GAVIN	8/05/00	
-	GRPCODP	5/15/00	WALK LIKE AN EGYPTIAN
-	JACK1	8/09/00	ADM/400 Self Study Exercise - Developer 1
-	JACK2	8/08/00	ADM/400 Self Study Exercise - Developer 1
-	JDBMENU1	5/18/00	Menu User
-	JDBMENU1	5/18/00	Menu User
-	JDBPGMR	5/18/00	JDB PROGRAMMER PROFILE
-	JDBPGMR	5/18/00	JDB PROGRAMMER PROFILE

More...

F3=Exit
F12=Previous

Position to - Repositions a specific user profile to the top of the column. The remaining profiles are listed in ascending order.

Option 16 Change Defaults (DISABLE DELETE +)

Allows changing of the User Profile Management defaults and scheduling of the job that disables, deletes, and archives user profiles.

ZPDF20	User Profile Management	16:36:11	9/15/01
PSSecure	Default Values	System:	ANYSERVER
Number of days of inactivity until User Profile is disabled:		<u>90</u>	
Number of days of inactivity until User Profile is deleted:		<u>180</u>	
After delete, do you want the User Profile to be archived?:		<u>Y</u> (Y/N)	
Archive user profiles deleted outside of PSSECURE?:		<u>N</u> (Y/N)	
If archived, how long do you want to retain? (0=Always)		<u>999</u>	
Print report of profiles disabled by UPM:		<u>Y</u> (Y/N)	
Method for determining eligible profiles:		<u>*DEFAULT</u>	
Delete profiles with password of *NONE?		<u>Y</u> (Y/N)	
Object owner for objects owned by deleted profiles:		<u>QDFTOWN</u>	
Delete pending distributions of profiles eligible for delete:		<u>Y</u> (Y/N)	
Delete profiles enrolled in OfficeVision/400 on this system:		<u>N</u> (Y/N)	
If Y, specify owner for DLOs of deleted profiles:		<u></u>	
Propagate (synchronize) profile changes by UPM:		<u>Y</u> (Y/N)	
F3=Exit	F7=Schedule UPM	Enter=Update defaults	

The option to “Archive profiles deleted outside of PSSECURE” allows profiles to be archived when deleted through UPM or any other place on the system. It is not possible to delete profiles that are included in the User Profile Exclusions from any place on the system while this option has a value of ‘Y’.

Caution

If you delete user profiles with a password of *NONE, be sure to include any profiles in the User Exclusions file that are required for software compatibility, such as IBM profiles (Q*) and NetIQ profiles (PS*).

When a user profile is deleted, the following options are used (the value specified for “Object owner” in the defaults is used in place of “object-owner”):

OWNOBJOPT(*CHGOWN object-owner) PGPOPT(*CHGPGP object-owner)

The “Method for determining eligible profiles” can be one of the following:

*DEFAULT	Uses the system date to age the user profiles against the Last Used Date or against the Creation Date if the Last Used Date is blank.
*PRVACTDT	Uses the most recent of the following dates: User Profile Previous Sign-on Date, User Profile Password Last Changed Date, Object Description's Last Used Date, Object Description's Creation Date.

Function Keys

The following function keys are available for this screen:

F3=Exit - Exits the current display without running the command.

F7=Schedule UPM - The scheduling of the UPM job:

- disables profiles inactive for the number of days specified on the display
- deletes disabled profiles inactive for the number of days specified
- archives deleted profiles
- purges profiles from the archive file that have been archived for the number of days specified

These tasks are performed based on the entry of values on the display. This is a periodic job that runs every night of the week (default) and performs the clean up of user profiles on the system.

Note

When you specify the date and time on this command, the job is submitted to the specified job queue. This command does not guarantee that the job will begin running at the scheduled time, however. The job will not begin running if the job queue is held or attached to an inactive subsystem, or if the maximum number of active jobs in the subsystem has been reached.

Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Job name > PSPROFILE

Name, *JOBID

Command to run > CALL PGM(PSSecure/2PCL53) PARM(*ALL)

Frequency > *WEEKLY

Schedule date, or > *NONE

*ONCE, *WEEKLY, *MONTHLY

Date, *CURRENT, *MONTHSTR...

F3=Exit

F4=Prompt

F5=Refresh

F10=Additional parameters

F12=Cancel

F13=How to use this display

F24=More keys

More...

Job name - The name of the job schedule entry. The possible values are:

- | | |
|--------|---|
| Name | The name of the job schedule entry |
| *JOBID | The job description specified on the JOBID parameter is used for the name of the job schedule entry |

Command to run - The command that runs in the submitted job. The IBM-supplied default routing program QCMD must be used when the job is started or the job will not run. The command string you specify has a maximum of 512 characters.

Frequency - How often the job is submitted to run. Possible values are:

*ONCE	Job is submitted once
*WEEKLY	Job is submitted on the same day or days of each week at the scheduled time
*MONTHLY	Job is submitted on the same day or days of each month at the scheduled time

Schedule date, or - The date on which the job is submitted to run. Possible values are:

- *NONE** No start date is specified
- Date** The date in the job date format
- *CURRENT** Job is submitted on the current date
- *MONTHSTR** Job is submitted on the first day of the month

Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Schedule day

> *MON

> *TUE

> *WED

> *THU

> *FRI

> *SAT

> *SUN

Schedule time

> 010101

*NONE, *ALL, *MON, *TUE...

Time, *CURRENT

Additional Parameters

Job description

> ZPJ0BD

Library

> PSSECURE

Text 'description'

> 'User Profile Management'

Name, *USRPRF

Name, *LIBL, *CURLIB

F3=Exit

F4=Prompt

F5=Refresh

F10=Additional parameters

F12=Cancel

F13=How to use this display

F24=More keys

Bottom

Schedule day - The day of the week on which the job is submitted. If today is the day of the week specified on this parameter and the time specified on the Schedule time parameter has not passed, the job is submitted today. Otherwise, the job is submitted on the next occurrence of the specified day. For example, if schedule day (*FRI) and schedule time (12:00:00) are specified and you are adding this job schedule entry at 11:00 a.m. on a Friday, the job is submitted today. If you are adding the entry at 4:00 p.m. on a Friday, the job is submitted on the following Friday. The possible values are:

- *NONE** No start day
- *ALL** Submitted every day
- *WED** Submitted on Wednesday
- *THU** Submitted on Thursday

*MON	Submitted on Monday	*FRI	Submitted on Friday
*TUE	Submitted on Tuesday	*SAT	Submitted on Saturday

Schedule Time - The time on the scheduled date the job is submitted to run. The possible values are:

***Current** - Job is submitted at the current time. If you specify schedule time (*CURRENT) and schedule date (*CURRENT), the job is immediately submitted to the job queue.

time - The time you want the job to be submitted. The time is specified in 24 hour format and can be used with or without a time separator:

- Without a time separator, specify a string of 4 or 6 digits (hhmm or hhmmss) where hh=hours, mm=minutes, and ss=seconds. Valid values for hh range from 00 to 23. Valid values for mm and ss range from 00 to 59.
- With a time separator, specify a string of 5 or 8 digits where the time separator specified for your job is used to separate the hours, minutes, and seconds. If this command is entered from the command line, the string must be enclosed in apostrophes. If a time separator other than the separator specified for your job is used, this command will fail.

Function Keys

The following function keys are available for the Add Job Schedule Entry displays. Some keys may not be active on all displays:

F3=Exit - Exits the current display without running the command.

F4=Prompt - Shows the permissible values for the entry field. If the cursor is on an entry field for a parameter of TYPE(*COMMAND) or TYPE(*CMDSTR), a prompt display for the command is shown.

F5=Refresh - Restores the screen data to a previous state or updates the screen with current statistics.

F10=Additional parameters - Shows entry fields for the parameters that are not commonly used.

- F12=Cancel - Returns you to the previous menu or display panel.
- F13=How to use this display - Help for the prompt display or associated display you are currently using.
- F24=More Keys - Additional function keys that can be used for the current display.
- Enter=Update defaults - Press Enter to accept changes made to default values.

Option 17 User Profile Exclusions

Specify the user profiles that should not be disabled. Typically the Q* profiles should not be disabled, but the list should also include profiles used for communications only.

ZPDF15
User Profile Management
09:33:43
8/30/00

PSSecure
System: ISIS

Enter the profiles to exclude from User Profile Management(DISABLE DELETE):
Notes:

Generic rules apply for the User Profile. (i.e. Q* or PGMR*)

User Profile

A*
AS*
B*
C*
CC*
CLP
D*
DA*
DB*
DS*
E*

More...

Enter=Update
F3=Exit
F5=Refresh
F6=Add

User Profile - Type a user profile name under the User column and press Enter to position the display at the specified user profile.

Functions

F3=Exit - Ends the current task and returns to the display where you began the task. Any options or changes that you typed will not be processed.

F5=Refresh - Returns you to the first screen and sorts data in the User Profile column in ascending order.

F6=Add - Takes you to the bottom of the list of entries where new user profiles can be added.

Option 18 Archived Profiles Report

Displays a date range prompt for selecting archived user profiles to include on the report. The report is then submitted to batch.

ZPCL26 CAS	Profile and Password management Archived User Profile Report	13:25:43 10/07/00 System: THIS
Type the following and press Enter:		
From Date <u>123199</u> to Date <u>013100</u> (MMDDYY)		
F3=Exit	ENTER=Submit	F12=Cancel

Option 2 Profile Synchronizer Menu

The Profile Synchronizer Menu is accessed from Option 2 on the Main Menu. It allows specification of global defaults and other information pertaining to distribution of passwords across a network of iSeries servers. Use the options on this menu to install, configure, and manage your networked iSeries servers for automatic password synchronization.

You must specify the profiles to exclude from distribution for synchronization separately, from the profiles to exclude from user-prompted and system generated passwords. Profile Synchronizer jobs run under user profile PENTAZP and will be submitted to jobq QCTL in QSYS.

PS22	PentaSafe Security Technologies Profile Synchronizer Menu	CAS QPADEV000H	Date: 8/30/00 Time: 9:45:44
Select one of the following:			
1 Profiles To Exclude			
2 Distributed Systems			
3 Profile Distribution Report			
4 Profile Synchronizer Defaults			
5 Test Distribution of Profile Change			
6 Synchronizer Debugging Options			
7 Purge Synchronizer Messages			
8 Profile Synchronizer Installation			
9 Profile Synchronizer Uninstall			
10 Add User Profile Exit Programs			
11 Remove User Profile Exit Programs			
Enter Option or Function/Type ==> _____			
F1=Help	F3=Exit	F6=Messages	F9=Window
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports
F10=Cmd Line			

Profile and password synchronization can be performed using TCP/IP (using Anynet configured for APPC over TCP/IP). Set up instructions are available from NetIQ Corporation.

Option 1 Profiles To Exclude

The Profile Exclusions screen can be used to specify whether a user's password should be sent to another system for synchronization and whether requests from other systems can be accepted to change the user's password.

ZPDF33

Profile and Password Management
Maintain Distributed Profile Exclusions

15:35:32
System: ANYSERVER

9/17/08

Enter the user profiles to be handled by exception:

<u>User Profile</u>	<u>Profile Changes</u>		<u>Password Changes</u>	
	<u>Send</u>	<u>Accept</u>	<u>Send</u>	<u>Accept</u>
USER1	N	N	N	N
USER2	Y	Y	Y	Y
USER3	Y	Y	Y	Y
USER4	Y	Y	Y	Y
USER5	N	N	N	N
USER6	Y	Y	Y	Y
USER7	N	N	Y	N
USER8	Y	Y	Y	Y

Enter=Update F3=Exit F5=Refresh F6=Add

By default, Q* profiles are excluded from profile synchronization.

Options

User Profile - Specify the user profile requiring special handling. To ‘position-to’ a specific User Profile, enter the user name in the first blank field under the User Profile column heading and press **Enter**. The user is repositioned to the top of the column. Other user profiles are listed below in ascending order. This feature eliminates the need to page down repeatedly to get to the desired user.

Profile Change Send:

- Specify “Y” to send profile changes for this user to other systems.
- Specify “N” to prohibit sending profile changes for this user to other systems.

Profile Change Accept:

- Specify “Y” to accept and apply profile changes for this user from other systems.
- Specify “N” to deny profile changes for this user from other systems.

Password Change Send:

- Specify “Y” to send password changes for this user to other systems.
- Specify “N” to prohibit sending password changes for this user to other systems.

Password Change Accept:

- Specify “Y” to accept and apply password changes for this user from other systems.
- Specify “N” to deny password changes for this user from other systems.

Function Keys

The following function keys are available on this screen:

F3=Exit - Ends the current task and returns to the display where you began the task. Any options or changes that you typed will not be processed.

F5=Refresh - Returns you to the first screen and sorts the User Profile column data in ascending order.

F6=Add - Takes you to the bottom of the list of entries where new user profiles can be added.

Option 2 Distributed Systems

Use the Distributed Systems screen to specify the names of the systems to and from which you will be distributing and receiving profile and password changes.

Before using this feature, you must run Option 8 to install Profile Synchronizer.

```
ZPDF32                               Profile and Password Management          15:10:43      9/17/08
                                     Maintain Distributed Systems Table       System:   ANYSERVER

Enter the names of systems with which profile changes are exchanged
or type options and press Enter:

1=ADDIRE/ADDNETJOBE           4=RMVDIRE/RMVNETJOBE           9=Start passthru


    Target      Profile Changes      Password Changes      -- Entries Exist? --
 Opt  System     Send    Recv         Send    Recv        NtwkJob    DistDir
- - - - -
-    BESSIE      Y        Y            Y        N            Y        Y
-    ISHTAR      N        N            Y        N            Y        Y
-    THIS        Y        Y            Y        N            Y        Y
-    _____  -        -            -        -            -        -
-    _____  -        -            -        -            -        -
-    _____  -        -            -        -            -        -
-    _____  -        -            -        -            -        -
-    _____  -        -            -        -            -        -
-    _____  -        -            -        -            -        -
-    _____  -        -            -        -            -        -
-    _____  -        -            -        -            -        -
-    _____  -        -            -        -            -        -
+
Enter=Update                      F3=Exit
F9=Load remote names              F10=WRKDIRE             F11=WRKNETJOBE
```

In the example above, password changes will be sent out, but Profile and Password Management cannot apply a password change received from another system.

Options

The following options are available on this screen:

1 = ADDIRE/ADDNETJOB - Use this option if either of the “Entries Exist” columns shows an 'N'.

4 = RMVDIRE/RMVNETJOBE - Removes a system from the network.

9 = Start Passthru - Access a target system without having to exit Profile and Password Management Menu.

Target System - The system to which profile changes are propagated.

Profile Changes Send - Send user profile changes to the specified system.

Profile Changes Recv - Receive and apply user profile changes from the specified system.

Password Changes Send - Send password changes to the specified system.

Password Changes Recv - Receive and apply password changes from the specified system.

Entries Exist Ntwkjob - Denotes whether Network Job Entries exist for Profile Synchronizer on the source system (not the target system).

Entries Exist DistDir - Denotes whether Distribution Directory Entries exist for Profile Synchronizer on the source system (not the target system).

Function Keys

The following function keys are available on this screen:

F9=Load remote names - Loads the names of all target systems known to your iSeries.

F10=WRKDIRE - Displays all directory entries, allowing you to manage your system directory as well as access other functions.

F11=WRKNETJOBE - Displays control information for input stream placement. There is one network job entry for each user or distribution group who can submit jobs to this system.

Option 3 Profile Distribution Report

Lets you specify parameters for printing an audit log of distributed profile changes.

ZPCL38	Profile and Password Management Distribution Messages Report	11:26:11 5/22/00 System: ISIS
--------	---	----------------------------------

Type the following and press Enter:

User profile.....	<u>*ALL</u>	(*ALL, generic*, or single user profile)
Sort code.....	<u>U</u>	(U=User profile, S=System name)
How to run.....	<u>I</u>	(I=Interactive, B=Batch)
Jobque for batch..	<u>QBATCH</u>	
Output queue.....	<u>QPRINT</u>	
Hold output?.....	<u>*NO</u>	(*YES, *NO)
Number of copies..	<u>1</u>	(01 - 99)

Data elements on report:

1) User profile	4) Date/time of message
2) Source system	5) Message text
3) Target system	6) System that logged message

ENTER=Submit/Run F3=Exit

The Profile Distribution Report lists messages logged by the profile and password synchronization process that identifies:

- User Profile
- Source (origin) and Target system names
- The message
- Message date and time
- The name of the system that recorded the message

Option 4 Profile Synchronizer Defaults

This option is reached by selecting Option 4 from the Profile Synchronizer Menu.

ZPDF0125
Version: 6.2

Profile and Password Management
Profile Synchronizer Defaults

11:32:45 5/22/00
System: ISIS

Type the following and press Enter:

Receive and apply profile changes ... Y

Send user profile changes..... Y

Receive and apply password changes... Y

Send password changes..... Y

History retention days (for purge)... 090

Mode description name for pass-thru.. PENTA

Jobq/Library for synchronizer jobs... QCTL QSYS

F3=Exit

Receive and Apply Profile Changes - Global option within Profile and Password Management. Will override similar specifications made at other levels. Specify “N” to reject requests from other systems to change, create, or delete user profiles. Specify “Y” to receive and apply requests from other systems to change, create, or delete user profiles.

Send User Profile Changes - Global option within Profile and Password Management. Will override similar specifications made at other levels. Specify “Y” to send requests to change, create, or delete user profiles from your system to another. Specify “N” to prohibit sending requests to change, create, or delete user profiles from your system to another.

Receive and Apply Password Changes - Global option within Profile and Password Management. Will override similar specifications made at other levels. Specify “N” to reject requests from other systems to change passwords for your system. Specify “Y” to receive and apply requests from other systems to change passwords for your system.

Send Password Changes - Global option within Profile and Password Management. Will override similar specifications made at other levels. Specify “Y” to send password changes from your system to another. Specify “N” to prohibit sending password changes from your system to another.

History Retention Days - Number of days to age distribution auditing data before it is eligible for purging.

Mode Description Name for Pass-thru - Mode description to use to start a workstation pass-thru session.

Jobq/Library for synchronizer jobs - The job queue where you place the Profile and Password Synchronization jobs.

Option 5 Test Distribution Of Profile Change

Lets you change your password to test for its correct distribution. None of the i5/OS password composition system values are enforced at this time.

To test the distribution of a changed password, run program ZPCL28 in library PSSECURE, either from a menu or command line.

```

Change Password
ISIS
Password last changed . . . . . : 05/22/00
Type choices, press Enter.
Current password . . . . .
New password . . . . .
New password (to verify) . . . . .
F3=Exit      F12=Cancel

```


Option 6 Synchronizer Debugging Options

This option will normally be used to gather information for Profile and Password Management problem determination. If it becomes necessary to fax this information to NetIQ Corporation, first print a fax cover letter (Option 6 on item 1).

ZPDF2901 Version: 6.2	Profile and Password Management Debugging Options	14:58:26 5/22/00 System: ISIS
Type options, press Enter. 5=Display 6=Print		
<u>Opt</u>	<u>Debug information</u>	<u>Opt</u> <u>Debug information</u>
-	1. Fax cover letter	- 15. Network attributes
-	2. User profile	- 16. Serial number
-	3. User messages	- 17. Password system values
-	4. Job description	- 18. Distribution queues
-	5. Jobque QCTL	- 19. Routing table
-	6. Subsystem QCTL	- 20. Distribution queue status
-	7. Subsystem QSNADS	- 21. Distribution log
-	8. Message Log	- 22. QSYSOPR messages
-	9. QHST messages	
-	10. Distribution directory	
-	11. Network job entries	
-	12. Synchronizer defaults	
-	13. Distributed systems	
-	14. User profile exclusions	
F3=Exit		Output queue: <u>SAFE</u>

Option 7 Purge Synchronizer Messages

Deletes messages from Profile Synchronizer's message queue and from the Distribution Messages Audit Log if they are older than the number of days specified for "History Retention Days" in the Profile Synchronizer defaults option. Press **Enter** to view the confirmation panel.

To schedule this function in your job scheduler, call these programs:

```
CALL PSSECURE/ZPCL40 PARM(' ')
```

```
CALL PSSECURE/ZPRP40 PARM(' ')
```

Option 8 Profile Synchronizer Installation

Automatically configures Profile Synchronizer to distribute passwords to other iSeries servers, which must already be configured for SNADS. Profile and password synchronization can be performed using TCP/IP (using Anynet configured for APPC over TCP/IP). Set up instructions are available from NetIQ Corporation.

ZPDF30
Version: 6.2

Profile and Password Management
Profile Synchronizer Installation

10:25:01 6/15/00
System: ISIS

The Profile Synchronizer installation will perform the following:

- 1) Create job description PENTA2P in library PSSECURE
- 2) Create user profile and message queue PENTA2P
- 3) Change the Network Attribute for "Job Action" (JOBACN) to "*SEARCH". Current value for JOBACN is *SEARCH
- 4) Add network job entries for user named in step 2
- 5) Add system distribution directory entries for user named in step 2
- 6) Add user profile exit point programs

The password validation program named PM0013C in library PSSECURE should include the following statement to distribute the new password if the validations are passed: CALL PGM(PSSECURE/ZPCL22 PARM(new_pwd) Substitute "new_pwd" with the variable for the new password.

Press Enter to proceed with the installation or F3 to cancel it.

F3=Exit

Prompt screens are provided for confirmation. This option can be run as many times as desired.

Option 9 Profile Synchronizer Uninstall

Deletes Profile and Password Management internal objects for Profile Synchronizer. Profile Synchronizer entries in the Distribution Directory and in the Network Job Routing Table are also removed. A confirmation prompt is provided to allow canceling the option.

Option 10 Add User Profile Exit Programs

Assigns User Profile Security Exit Programs to the QIBM_QSY_XXX_PROFILE exit points, where “XXX” is CRT, CHG, and DLT. These exit programs are used for User Profile Synchronization.

Option 11 Remove User Profile Exit Programs

Removes the NetIQ Security Solutions for iSeries User Profile Security Exit Programs used for User Profile Synchronization.

Verifying Profile and Password Synchronization on Multiple Systems

To simplify the administration of networks with multiple iSeries systems, we recommend that you synchronize the network attributes that control profiles and profile passwords. Although you can specify different values for the Current system name (SYSNAME), the Local control point name (LCLCPNAME), and the Local location name (LCLLOCNAME), synchronization of these values will facilitate the process of applying maintenance and changes throughout your network. Using PSSecure for iSeries, you can synchronize the network attributes for all iSeries systems in your network by performing the following procedure.

Verification Procedure

You can verify synchronization of profiles and profile passwords on multiple iSeries systems in a network.

To verify synchronization:

1. On the source system, from the NetIQ Product Access screen, select option 2 PSSecure. Press **Enter**.
2. Press **F10** (Command line). On the command entry line, type **DSPNETA** and press **Enter**.

Display Network Attributes			System:	LIFE
Current system name	:	LIFE		
Pending system name	:			
Local network ID	:	APPN		
Local control point name	:	MYTH		
Default local location	:	DIFF		
Default mode	:	BLANK		
APPN node type	:	*ENDNODE		
Data compression	:	*NONE		
Intermediate data compression	:	*NONE		
Maximum number of intermediate sessions	:	200		
Route addition resistance	:	128		
Server network ID/control point name	:	*LCLNETID	*ANY	

3. Note the values shown in the following fields in the preceding figure:

- Current system name
- Local control point name
- Default local location

You will need to verify these values for the target system when you display the details of the distribution queue (Step 3), the routing table (Step 4), and the directory entry (Step 5).

4. On the source system, verify correct configuration of the distribution queue for the target system by performing the following step:
 - a. On a command line, type `CFGDSTSRV OPTION(*SELECT)` and press **Enter**.

Configure Distribution Services

Type choice, press Enter.

Type of distribution services information to configure . . .	-	1=Distribution queues 2=Routing table 3=Secondary system name table
---	---	---

F3=ExitF12=Cancel

5. On the **Type of distribution services information to configure** entry field, type **1** (Distribution queues) and press **Enter**.

Configure Distribution Queues

Position to _____

Type options, press Enter.
2=Change 4=Remove 5=Display details

Opt	Queue Name	Queue Type	Remote Location Name	Mode Name	Remote Net ID
-	QSMTPQ	*RPDS	TCPIPL0C	*NETATR	*LOC
-	THAT	*SNADS	THAT	*NETATR	*LOC

F3=Exit F5=Refresh F6=Add distribution queue

F10=Work with distribution queues F12=Cancel

Bottom

6. Locate the distribution queue for your target system. On the **Opt** entry field beside it, type 5 (Display details) and press **Enter**.

Note

The values specified in the **Mode Name** field and the **Remote Net ID** field must be the same on the source system and the target system.

Display Details of Distribution Queue		Page 1 of 2
Queue	: THAT	
Queue type	: *SNADS	
Remote location name	: THAT	
Mode	: *NETATR	
Remote net ID	: *LOC	
Local location name	: *LOC	
Normal priority:		
Send time:		
From/To	: :	
Force	: :	
Send depth	: 1	
High priority:		
Send time:		
From/To	: :	
Force	: :	
Send depth	: 1	
Press Enter to continue.		
F3=Exit F12=Cancel		
More...		

7. On the source system, verify the configuration of the routing table for the target system by performing the following steps:
 - a. Press **F12** (Cancel) twice to return to the Configure Distribution Services screen.
 - b. In the **Type of distribution services information to configure** entry field, type **2** (Routing table) and press **Enter**.

Configure Routing Table

Type options, press Enter.
2=Change 4=Remove 5=Display details

Opt	Name	Group	Description
-	TCPIP		TCP/IP Routing
-	THAT		Send to THAT

F3=Exit
F12=Cancel

F5=Refresh

F6=Add routing table entry

Bottom

8. Locate the routing table entry for your target system. In the **Opt** entry field beside it, type 5 (Display details) and press **Enter**.

```

_                               Display Details of Routing Table Entry

Destination system
name/Group . . . . . : THAT
Description . . . . . : Send to THAT
Service level:
Fast:
    Queue name . . . . . : THAT
    Maximum hops . . . . : *DFT
Status:
    Queue name . . . . . : THAT
    Maximum hops . . . . : *DFT
Data high:
    Queue name . . . . . : THAT
    Maximum hops . . . . : *DFT
Data low:
    Queue name . . . . . : THAT
    Maximum hops . . . . : *DFT

Press Enter to continue.

F3=Exit      F12=Cancel
```

9. Verify that the name displayed in the **Destination system name/Group** field on the source system, is the same as the name displayed in the **Current system name** field on the Display Network Attributes screen located on the target system.

10. On the source system, verify the newly created directory entries by performing the following step:

a. On a command line, type **WRKDIRE** and press **Enter**.

```
Work with Directory Entries

Type options, press Enter.
  1=Add      2=Change  4=Remove  5=Display details  8=Print details
  7=Rename   8=Assign different ID to description  9=Add another description

Opt  User ID  Address  Description
--  -
=    *ANY     THAT    THAT SYSTEM
-    UID      ISIS    User, PentaSafe R&D
-    UID      LIFE    User, PentaSafe R&D
-    UID      LIFE    User
-    PENTAZP   LIFE    PentaSafe User Profile Synchronizer
-    PENTAZP   TCPILOC  PentaSafe User Profile Synchronizer
-    PENTAZP   THAT    PentaSafe User Profile Synchronizer
-    PSafe     PENTA401  PentaSafe Technical Support at 888-400-2834
-    QDFTOWN   QDFTOWN  Default Owner
-    QDOC      QDOC     Internal Document Owner
-    QFSNOTES  QFSNOTES  INTERNAL LOTUS NOTES INTEGRATION PROFILE
-    QLPAUTO   QLPAUTO   Licensed Program Automatic User

More...

F3=Exit      F5=Refresh  F8=Work with nicknames  F11=Sort by description
F12=Cancel   F13=Work with departments  F17=Position to  F24=More keys
```

11. Locate the directory entries for user PENTAZP address THAT. On the **Opt** entry field beside it, type 5 (Display details) and press **Enter**.

Display Directory Entry Details	
User ID/Address	PENTAZP THAT
Description	PentaSafe User Profile Synchronizer
System name/Group	THAT
User profile	
Network user ID	PENTAZP THAT
Name:	
Last	
First	
Middle	
Preferred	
Full	
Department	
Job title	
Company	
	More...
Press Enter to continue.	
F3=Exit	F12=Cancel
F18=Display location details	
F19=Display name for SMTP	F20=Display user-defined fields

12. Verify that the system name shown is the same as the system name specified in the **Destination system name/Group** field on the Display Details of Routing Entry screen.
13. On the source system, verify the settings of the APPC device by performing the following step:
 - a. On a command line, type the following command and press **Enter**.

WRKDEVD DEVD(xxxxxxx)

where xxxxxxx = the name of the APPC device that is used to connect to your target system

14. Locate the APPC device entry. On the **Opt** field entry line beside it, type 5 (Display) and press **Enter**.

Display Device Description		LIFE
		29/01/01 17:14:24
Device description	: THAT00	
Option	: *BASIC	
Category of device	: *APPC	
Automatically created	: YES	
Remote location	: THAT	
Online at IPL	: *NO	
Local location	: DIFF	
Remote network identifier	: *NETATR	
Attached controller	: THAT	
Message queue	: QSYSOPR	
Library	: *LIBL	
Local location address	: 00	
APPN-capable	: *YES	
Single session:		
Single session capable	: *NO	
		More...
Press Enter to continue		
F3=Exit F11=Display keywords F12=Cancel		

15. Verify that the system name displayed in the **Local location** field on the Display Device Description screen is the same as the system name displayed in the **Default local location** field on the Display Network Attributes screen.
16. Repeat Steps 1-6 for each target system that you want to use the same profile and profile password as the source system.

Option 3 Profile Templates Menu

This is the User Profile Templates menu. To access this menu, select Option 3 from the main menu.

PS23	PentaSafe Security Technologies Profile Templates Menu	CAS QP4DEV0000	Date: 6/09/00 Time: 9:33:43
------	---	-------------------	--------------------------------

Select one of the following:

- 1 Maintain Permissible Values
- 2 Maintain User Profile Templates
- 3 Create a Profile Based on Template
- 4 Change a Profile Based on Template

Enter Option or Function/Type ==> _____

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cnd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

You will be able to create user profile templates, select the parameter values to use for each template, and authorize others to the templates. Profiles can also be maintained using the templates.

The person responsible for creating and changing user profiles based on templates authorized by the security administrator, can access only Options 3 and 4 by using command STRMS APPL(PS) FUNCTION(PS23U) TYPE(*MNU). In order to allow a user to use this command, grant the user *USE authority to libraries PSCOMMON and PSSECURE by using the EDTOBJAUT command.

Option 1 Maintain Permissible Values

You can customize the permissible values which are available for selection when templates are created or changed.

Add and delete permissible values for each of the following template parameters and designate one or more of the permissible values as recommended default values:

- Password
- Current library
- Initial program and library
- Initial menu and library
- Password expiration interval
- Maximum allowed storage
- Highest schedule priority
- Job description and library
- Group profile
- Supplemental groups
- Accounting code
- Document password
- Message queue and library
- Severity code filter
- Print device
- Output queue and library
- Attention program and library
- Sort sequence and library
- Language ID
- Country ID
- CCSID

- UID
- GID
- Home directory

You can also designate one or more of the available permissible values as recommended default values for each of the following template parameters:

- Set password to expired
- Status
- User class
- Assistance level
- Limit capabilities
- Special authority
- Special environment
- Display sign-on information
- Limit device sessions
- Keyboard buffering
- Group authority
- Group authority type
- Delivery
- User options
- Authority

Note

The list of permissible values is restricted, so you cannot modify the list.

Maintain User Profile Parameters screen:

ISIS
ZPRP70

Maintain User Profile Parameters
Permissible Values

5/22/00
15:34:09

Type choices, press Enter.
2=Edit

Opt	Parameter	Description
-	PASSWORD	User password
-	PWDEXP	Set password to expired
-	STATUS	Status
-	USRCLS	User class
-	ASTLVL	Assistance level
-	CURLIB	Current library
-	INLPGM	Initial program to call
-	INLPGMLIB	Initial program library
-	INLMNU	Initial menu
-	INLMNULIB	Initial menu library
-	LNTCPB	Limit capabilities

More...

F3=Exit
F12=Previous

Select the parameter for the list of permissible values to be modified. You will be able to add and delete permissible values for the selected parameter, as well as specify its default value.

Option

Perform permissible operations on individual parameters. Type the option number next to a parameter name and press **Enter**. You can type the same option next to more than one parameter at a time.

2=Edit - Type 2 to edit one or more parameters.

Function Keys

The following function keys are available on this screen:

F3=Exit - Exit the program.

F12=Previous - Return to previous screen.

Parameter Permissible Values Selection Prompt

Add or delete permissible values. You can also designate one or more permissible value as a recommended default value.

ARGUS	Maintain User Profile Parameters	6/14/99
ZPRP70	Permissible Values	12:42:44
Parameter name : PASSWORD		
Parameter description . : User password		
Type choices, press Enter.		
2=Edit 4=Delete		
<u>Opt</u>	<u>Permissible values</u>	<u>Default</u>
=	*ANY	
-	*NONE	
-	*USRPRF	Y
F3=Exit F6=Add F12=Previous		Bottom

Option

The following options are available on this screen:

2=Edit - Edit the permissible value definition.

4=Delete - Delete a permissible value from the list. This option is only valid for parameters whose list of permissible values can be modified.

Function Keys

The following function keys are available from this screen.

F3=Exit - Exit the program.

F6=Add - Add a permissible value for the selected parameter. This function key is only valid for parameters whose list of permissible values can be modified.

F12=Previous - Returns to the Parameter Selection prompt.

Parameter Permissible Values Detail Screen

ARGUS ZPRP70	Maintain User Profile Parameters Permissible Values	6/14/99 12:46:09
-----------------	--	---------------------

Type choices, press Enter.

Parameter name : PASSWORD
Parameter description . : User password

Permissible value . : *ANY
Default (Y/N) . . : =

F3=Exit F12=Previous

Specify the permissible value for the selected parameter. The permissible value may be designated as a recommended default by entering a “Y” in the DEFAULT field. An “N” in the DEFAULT field designates the permissible value as an optional value for the selected parameter.

Function Keys

The following function keys are available on this screen:

F3=Exit - Exit the current application or display.

F12=Previous - Return to the Permissible Values selection prompt without updating the current permissible value.

Option 2 Maintain User Profile Templates

Lets you create, manage, and grant authorization to User Profile Templates.

ARGUS
ZPRP71

Work with User Profile Templates

6/14/99
12:50:50

Position to : _____

Type options, press Enter.
2=Edit 4=Delete 5=Display 13=Change Description 15=Edit Authority

Opt	Template	Description
—	JDEUSER	JDE USER
—	QPGMR_	PROGRAMMER AND BATCH USER
—	QPGMR_	PROGRAMMER AND BATCH USER
—	QSECOFR_	SECURITY OFFICER
—	QSYSOPR_	SYSTEM OPERATOR
—	QUSER_	WORK STATION USER

Bottom

F3=Exit F6=Create F12=Previous

- Position to** - Type a partial or full template name and press Enter.
- 2=Edit** - Allows a User Profile Template definition to be changed.
- 4=Delete** - Deletes a User Profile Template.
- 5=Display** - View a User Profile Template definition without the ability to change its definition.
- 13=Change Description** - Change a User Profile Template (256 characters of text) description without the ability to display or change any other detail.

15=Edit Authority - Grant user authority for selected User Profile Templates. User Profiles can only be created and changed using authorized templates. Usage of the template can be restricted to the CRTUSRPRF or CHGUSRPRF function. When template authority is granted, *USE authority is also granted for the following objects:

- PSCHGUSRPR *CMD
- PSCRTUSRPR *CMD
- ZPCL75 *PGM

Users authorized to create and change profiles using the templates should only have access to the PSCHGUSRPR and PSCRTUSRPR commands as menu options.

Note

SECOFR authority is required to grant others authority to templates.

A user must have *SECOFR authority to grant template authority to other users. In the example below, option 15=Edit Authority is not allowed for the user since he does not belong to the *SECOFR user class. A message appears at the bottom of the screen informing the user that he does not have sufficient authority to grant access to the template.

```
ANYSERVER                      Work with User Profile Templates          9/17/08
ZPRP71                          15:59:37

Position to . . . . . :_____

Type options, press Enter.
  2=Edit  4=Delete  5=Display  13=Change Description  15=Edit Authority

Opt  Template  Description
15   AAAA      TEST TEMPLATE
____ BBBAGAIN   BOB'S NEXT TEST TEMPLATE
____ BBBTSTSUSQ BOB'S TEST OF 1 DEFAULT, 3 ALLOWABLE SUPPLEMENTAL GROUPS FOR
____ BBBTST40   BOB'S TEST FOR 0 SUPPLEMENTAL GROUPS
____ BBBTST41   BOB'S TEST FOR 1 SUPPLEMENTAL GROUP
____ BBBTST42   BOB'S TEST FOR 2 SUPPLEMENTAL GROUPS
____ BBBTST44   BOB'S TEST FOR 4 SUPPLEMENTAL GROUPS
____ CCCC      FUNCTION TO CHANGE PASSWORD VALUES
____ JJJJ      TEST
____ NEW       NEW TEMPLATE

More...

F3=Exit      F6=Create      F12=Previous

User not authorized to alter or create templates; *SECOFR authority required.
```

Function Keys

The following function keys are available on this screen:

F3=Exit - Exit the program.

F6=Create - Create a template.

F12=Previous - Return to the previous screen.

Create/Change User Profile Template

ARGUS	Create a User Profile Template	6/14/99
ZPRP71		12:55:34

Type choices, press Enter.

Template name . . OPGMR

Template description . . PROGRAMMER AND BATCH USER

F3=Exit

F12=Previous

Specify the template name and a description. When editing a User Profile Template, you cannot change the template name, only the template description. After pressing enter and all edits have been satisfied, the User Profile Template detail screen-1 is displayed.

Function Keys

The following function keys are available on this screen:

F3=Exit - Exit the program.

F12=Previous - Return to the User Profile Template selection panel.

User Profile Template Detail Screens

When creating a User Profile Template, the parameter values will initially contain the parameter default. When editing an existing User Profile Template, the parameters will initially contain the previously specified values.

Use **F4** or “?” followed by a blank on a field where the cursor is positioned to display the permissible values selection window for that field. Any previously selected values are marked as selected. If no values have been previously specified, the defaults will be marked as selected.

Entering a “+” followed by a blank in the first position of a field will display a window allowing entry of the desired values for the selected parameter. The previously specified values will be shown in addition to providing for entry of additional values. If no values have been previously specified, the defaults will be shown, in addition to providing for the entry of additional values.

Page Down will advance you to the next detail screen. **Page Up** will return you to the previous detail screen.

Pressing **Enter** performs error checking on the template definition currently being defined. If any errors are found, corresponding messages will be displayed at the bottom of the screen.

When all edits have been satisfied, the template will be created and you will be returned to the User Profile Template Selection prompt. There are a total of four detail screens containing all the required parameters needed to create or change a User Profile Template.

Function Keys for Detail Screens

?-	Display values
F4	Display values
+-	Values for selected parameter
F3	Exit the program without update to any template currently being defined
F12	Returns you to User Profile Template name and description prompt. No updates will be performed on the currently selected template
Page Down	Move to the next detail screen
Page Up	Move to the previous detail screen
Enter	Perform error check

Detail Screen 1

ARGUS

Create a User Profile Template

6/16/99

ZPRP71

16:26:38

Type choices, press Enter.

Template name . . QPGMR

Template description . . PROGRAMMER AND BATCH USER

User password

Set password to expired

Status

User class

Assistance level

Current library

Initial program to call

Library

Initial menu

Library

Limit capabilities

Special authority

+ for more values

*USRPRF

*NO

*ENABLED

*USER

*SYSVAL

*CRTDFT

*NONE

*LIBL

MAIN

*LIBL

*NO

*USRCLS

F3=Exit

F4=Permissible values

F12=Previous

More...

This User Profile Template detail screen requires the following User Profile Template parameters:

- User Password
- Set Password to expired
- Status
- User Class
- Assistance level
- Current library
- Initial program to call
- Initial menu
- Limit capabilities
- Special authority

Function Keys

The following function keys are available for this screen:

F3=Exit - Exit the program.

F4=Permissible values - Displays the permissible values.

F12=Previous - Return to the previous screen.

Detail Screen 2

ARGUS	Edit a User Profile Template	6/16/99
ZPRP71		16:34:53
Additional parameters		
Type choices, press Enter.		
Template name . . OPGMR		
Template description . . PROGRAMMER AND BATCH USER		
Special environment	*SYSVAL	
Display sign-on information . .	*SYSVAL	
Password expiration interval . .	*SYSVAL	
Limit device sessions	*SYSVAL	
Keyboard buffering	*SYSVAL	
Maximum allowed storage	*NOMAX	
Highest schedule priority . . .	3	
Job description	QDFTJOB	
Library	*LIBL	
Group profile	*NONE	
Owner	*USRPRF	
Group authority	*NONE	
Group authority type	*PRIVATE	
		More...
F3=Exit	F4=Permissible values	F12=Previous

Enter the following User Profile Template parameters:

- Special environment
- Display sign-on information
- Password expiration interval
- Limit device sessions
- Keyboard buffering
- Maximum allowed storage
- Highest schedule priority
- Job description
- Group profile
- Owner

- Group authority
- Group authority type

Function Keys

The following function keys are available on this screen:

F3=Exit - Exit the program.

F4=Permissible values - Displays the permissible values.

F12=Previous - Return to the previous screen.

Detail Screen 3

ARGUS ZPRP71	Edit a User Profile Template	6/16/99 16:38:05
Additional parameters		
Type choices, press Enter.		
Template name . . . QPGMR		
Template description . . . PROGRAMMER AND BATCH USER		
Supplemental groups		
+ for more values		
Accounting code	*BLANK	
Document password	*NONE	
Message queue	*USRPRF	
Library	*LIBL	
Delivery	*NOTIFY	
Severity code filter	0	
Print device	*WRKSTN	
Output queue	*WRKSTN	
Library	*LIBL	
Attention program	*SYSVAL	
Library	*LIBL	
		More...
F3=Exit	F4=Permissible values	F12=Previous

Enter the following User Profile Template parameters:

- Supplemental groups
- Accounting code

- Message Queue
- Delivery
- Severity code filter
- Print device
- Output Queue
- Attention program

Function Keys

The following function keys are available for this screen:

F3=Exit - Exit the program.

F4=Permissible values - Displays the permissible values.

F12=Previous - Return to the previous screen.

Detail Screen 4

ARGUS	Edit a User Profile Template	6/16/99
ZPRP71		16:43:12
Additional parameters		
Type choices, press Enter.		
Template name . . .	QPGMR	
Template description . .	PROGRAMMER AND BATCH USER	
Sort sequence	*SYSVAL	
Library	*LIBL	
Language ID	*SYSVAL	
Country ID	*SYSVAL	
Coded character set ID	*SYSVAL	
User options		
	+ for more values	
User ID number	*GEN	
Group ID number	*NONE	
Home directory	*USRPRF	
Authority	*EXCLUDE	
		Bottom
F3=Exit	F4=Permissible values	F12=Previous

Enter the following User Profile Template parameters:

- Sort sequence
- Language ID
- Country ID
- Coded character set ID
- User options
- User ID number
- Group ID number
- Home directory
- Authority

Function Keys

The following function keys are available on this screen:

F3=Exit - Exit the program.

F4=Permissible values - Displays the permissible values.

F12=Previous - Return to the previous screen.

Permissible Values

Each of the template definition parameters specified in detail screens 1,2,3 and 4, have a set of valid entries or Permissible Values that are specific to each parameter. These Permissible Values may be keyed in directly through the Permissible Values entry window or may be selected from a list displayed via the Permissible Values selection window. When using the Permissible Values selection window you can specify selections for that parameter as either recommended default values (Option 9) or optional values (Option 1).

Entering the “+” character in the first position of a field followed by a blank will display a window allowing the user to key the desired values for the selected parameter.

Pressing function key **F4** for the field the cursor is positioned in or entering the “?” character in the first position of a field followed by a blank will display the permissible values selection window for that field.

Permissible Values Entry Window

Entering the “+” character in the first position of a field followed by a blank will display a window allowing the user to key the desired values for the selected parameter. The previously specified values will be shown in addition to providing for entry of additional values. If no values have been previously specified, the defaults will be shown in addition to providing for the entry of additional values.

Example - Permissible values for User Options parameter:

ARGUS ZPRP71	Edit a User Profile Template	6/16/99 16:43:12
Additional parameters		
Type choices, press Enter.		
Template name . . QPGMR		
Template description . . PROGRAMMER AND BATCH USER		
Sort sequence	*SYSVAL	
Library	*LTBL	
Language ID	*SYSVAL	
Country ID	*SYSVAL	
Coded character set ID	*SYSVAL	
User options	+	
+ for more values		
User ID number	*GEN	
Group ID number	*NONE	
Home directory	*USRPRF	
Authority *EXCLUDE		
		Bottom
F3=Exit	F4=Permissible values	F12=Previous

The below screen shows the selection window for Additional Parameters available for the user options (USROPT) parameter. This screen is the result of typing “+” followed by a blank in the user options parameter and pressing **Enter**.

ARGUS

Edit a User Profile Template

6/16/99

2

17:36:28

Specify More Values for Parameter
USROPT

Type choices, press Enter.
Additional Parameters

User options

9=Default

Y

*NONE

-

-

-

-

More...

F3=Exit

F12=Cancel

ameters

ATCH_USER

AL

AL

AL

AL

RF

UDE

F3=Exit

F4=Permissible values

F12=Previous

Bottom

To exclude a value, blank it out. You may also type valid values directly into the prompt fields. Press **Enter** when finished to return to previous screen.

Permissible Values Selection Window

Display the permissible values selection window by pressing function key **F4** on the field the cursor is positioned in, or by entering a “?” followed by a blank.

The previously selected values will be marked as selected. If no values have been specified, the defaults will be marked as selected.

When using the Permissible Values selection window you can specify selections for that parameter as either recommended default values or optional values.

ARGUS ZPRP71	Edit a User Profile Template	6/16/99 17:41:33
Additional parameters		
Type choices, press Enter.		
Template name . . QPGMR		
Template description . . PROGRAMMER AND BATCH USER		
Sort sequence *SYSVAL		
Library *LTBL		
Language ID *SYSVAL		
Country ID *SYSVAL		
Coded character set ID *SYSVAL		
User options ?		
+ for more values		
User ID number *GEN		
Group ID number *NONE		
Home directory *USRPRF		
Authority *EXCLUDE		
Bottom		
F3=Exit F4=Permissible values F12=Previous		

The below screen shows the selection window for permissible values available for the user options (USROPT) parameter. You can access this screen by typing a “?” followed by a blank in the user options parameter and then pressing **Enter**.

ARGUS

Edit a User Profile Template

6/16/99

2

17:47:31

Select Permissible Values

ameters

Template . . QPGMR

Type choices, press Enter.

1=Allow 9=Default

USROPT

Opt	User options
-	*CLKWD
-	*EXPERT
-	*HLPFULL
1	*NONE
=	*NOSTMSG
-	*PRTMSG
-	*ROLLKEY
-	*STSMSG

Bottom

UDE

F3=Exit F12=Cancel

=Previous

Bottom

Prompt request in wrong position.

+

Press **Enter** when finished with selections to return to previous screen.

Edit User Profile Template Authority

Select Option 15 from the Maintain User Profile Templates screen.

The Edit Profile Template Authority function allows a user of type *SECOFR to grant usage authority for User Profile Templates to specific users. The Create and Change User Profile functions are restricted through the User Profile Template Authority definitions. A *SECOFR type user can grant or revoke the Create and/or Change User Profile authorities for any user there by granting or revoking the capability of that user to Create and/or Change a User Profile.

ISIS		Edit User Profile Template Authority		8/30/00	
ZPRP73				16:59:45	
Template name : <u>PAYROLL</u>					
Type changes to current authorities, press Enter.					
<u>User</u>	-Authorized for Use With-				
	<u>CRTUSRPRF</u>		<u>Y/N</u>	<u>CHGUSRPRF</u>	
<u>RPD</u>	<u>Y</u>			<u>Y</u>	
<u>SUELL</u>	<u>Y</u>			<u>N</u>	
					Bottom
F3=Exit		F6=Add User		F12=Previous	

Type Y in the CRTUSRPRF field to grant the corresponding user the authority to create user profiles based on the selected template via the “Maintain User Profile Based on Template” screen. To revoke the authority, blank the field.

Type Y in the CHGUSRPRF field to grant the corresponding user the authority to change user profiles based on the selected Template, via the “Maintain User Profile Based on Template” program. To revoke the authority, blank the field.

You can delete a user from the authorization list by blanking out the user’s name, the assigned authority flags, and pressing the **Enter** key.

Function Keys

The following function keys are available for this screen:

F3=Exit - Exit the program without updating changes subsequent to the last time the Enter key was pressed.

F6=Add User - Lets you add users to the User Profile Template Usage authorization list. When function key **F6** is pressed, a blank entry will be provided at the top of the screen for entering the user profile name to be added. Pressing Enter after typing the name of the profile will add the user to the list. Authorities may be specified at the time the user is added or at a later time.

F12=Previous - Exit the screen without updating changes subsequent to the last time the **Enter** key was pressed.

Add User to Profile Template Authority

ARGUS

Edit User Profile Template Authority

6/16/99

ZPRP73

18:03:19

Template name : QPGMR

Type changes to current authorities, press Enter.

User

-Authorized for Use With-

CRTUSRPRF

CHGUSRPRF

Y/N

JMS

Y

Y

Bottom

F3=Exit

F12=Previous

User - Valid user profile.

CRTUSRPRF - Type Y to grant authority to create a new user profile based on the selected template via the “Maintain User Profile Based on Template” screen.

CHGUSRPRF - Type Y to grant authority to change user profiles based on selected template via the “Maintain User Profile Based on Template” screen.

Option 3 Create a Profile Based On Template

The “Maintain User Profile Based on Template” option allows authorized users to create User Profiles. The Create User Profile functions are restricted through the User Profile Template Authority definitions. A *SECOFR type user can grant or revoke the Create User Profile authorities for any user thereby granting or revoking the capability of that user to Create a User Profile.

This option is intended for use by the person responsible for creating user profiles based on templates authorized by the security administrator. To make this option available to other end users, authorize those users to the desired template(s) and instruct them to execute command PSSECURE/PSCRTUSRPR.

ARGUS	Create User Profile Based On Template	6/17/99
ZPRP75		14:19:05
Position to : _____		
Type options, press Enter.		
1=Select		
<u>Opt</u>	<u>Template</u>	<u>Description</u>
-	QPGMR_	PROGRAMMER AND BATCH USER
Bottom		
F3=Exit	F7=Change USRPRF	F12=Cancel

When this option is chosen, the user is shown a list of templates to create the user profile from. You can only see those templates that you have authority to. These include templates associated with the user, group, and supplemental group profiles of the user.

1=Select - Selects a User Profile Template to be used as a basis for creating the user profile. The permissible values for the user profile parameters are determined by the assigned template definitions. When a User Profile is created, the Create User Profile parameters are loaded with their corresponding permissible values specified by the assigned template. The user can then further customize the profile definition by choosing from the available permissible values for each of the profile parameters. After selecting a User Profile with an assigned associated template, press **Enter** to display the “Maintain User Profile Based On Template” screen.

Function Keys

The following function keys are available for this screen:

F3=Exit - Exit the program.

F7=Change USRPRF - Toggle to the Change User Profile Based On Template prompt.

F12=Cancel - Return to previous screen.

Option 4 Change User Profile Based on Template

The Change User Profile functions are restricted through the User Profile Template Authority definitions. A *SECOFR type user can grant or revoke the Change User Profile authorities for any user thereby granting or revoking the capability of that user to Change a User Profile.

This option is intended for use by the person responsible for changing user profiles based on templates authorized by the security administrator. To make this option available to other end users, authorize those users to the desired templates and instruct them to execute command PSSECURE/PSCHGUSRPR.

Note

Users with insufficient authority are restricted from changing profiles or re-assigning profile templates as follows:

- You can change a profile based on a template that you are directly authorized to use.
 - You can change a profile based on a group profile or a supplemental profile that you are authorized to use.
 - If the profile you are trying to edit is based on a template that you do not have access to, the profile cannot be changed.
 - To change a profile that is not associated with a template, you must have *SECOFR special authorities or be authorized to the UNASSIGNED template. This template eliminates the need to grant *SECOFR authorities to enable you to change profiles.
-

Change User Profile Based on Template

ARGUS
ZPRP75

Change User Profile Based On Template

6/17/99
14:58:06

Position to : _____

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

Opt	User	Text
-	A	
-	AAA	DMH TEST PROFILE
-	AAC	Alicia A. Collins
-	ABC123XYZ	
-	ACM	Andrew Clayton Medlenka
-	AER	Alan E. Rivers
-	AJT	Aaron Tucci
-	AKP	Arron K. Poffenberger
-	AMAPICS	AMAPICS USER PROFILE
-	AMB	Adam Backman - PS

More...

F3=Exit

F7=Create USRPRF

F12=Cancel

2=Edit - The permissible values for the user profile parameters are determined by the assigned template definitions. When a User Profile is changed, the Change User Profile parameters are loaded with the corresponding permissible values specified by the assigned template. The user can then further customize the profile definition by choosing from the available permissible values for each of the profile parameters. After selecting a User Profile with an assigned associated template, press **Enter**. The “Maintain User Profile Based On Template” screen-1 will be displayed. If there is no associated template assigned to the User Profile being selected for change, the user will be prompted to select and assign a template when **Enter** is pressed.

5=Display - Displays the User Profile and its parameter values for the selected user profile.

Function Keys

The following function keys are available for this screen:

F3=Exit - Exit the program.

F7=Create USRPRF - Toggle to the “Create User Profile Based On Template” prompt.

F12=Cancel - Exit the program.

Maintain User Profile Based On Template Screen-1

ARGUS ZPRP75	Maintain User Profile Based on Template	6/17/99 15:09:58
Type choices, press Enter.		
Template name . . . : QPGMR		
Template description : PROGRAMMER AND BATCH USER		
User profile : GAS		
Text 'description' : GARY SMITH		
More...		
F3=Exit	F12=Previous	F17=Chg Template Assigned

Function keys

The following function keys are available for this screen:

F3=Exit - Exit the program.

F12=Previous - Exit the program.

F17=Chg Template Assigned - Display the “Change User Profile Assigned Template” prompt. After requesting to create, change or reassign a User Profile, the “Maintain User Profile Based On Template” screen-1 is displayed. When creating a User Profile, you must specify the User Profile name and text description. When changing a User Profile you can not change the profile name. You can only change the text description. After pressing **Enter** and all edits have been satisfied, the “Maintain User Profile Based On Template” detail screen is displayed.

To reassign a profile to a different template using the Work With Users screen, you must have one of the following:

- Authority to the template of the profile you are changing
- *SECOFR authority
- Authority to the UNASSIGNED template

Here, you can take F17=Change Template Assigned to view the list of templates you are assigned to. Select one of these templates to reassign the selected user profile.

ISIS

Change User Profile Assigned Template

6/87/

ZPRP75

16:02:

Position to : _____

Type options, press Enter.

1=Select

<u>Opt</u>	<u>Template</u>	<u>Description</u>
-	STEST	TEST TEMPLATE

Bottom

F3=Exit

F12=Cancel

Select a template to (re)assign SUELL.

User Profile Template Detail Screens 2, 3, 4 and 5

When creating or changing a User Profile, the available permissible values for the user profile parameters are determined by the assigned template definition. When a User Profile is created or changed, the User Profile parameters are loaded with their corresponding permissible values specified by the associated template. The user can then further customize the Profile definition by choosing from the available permissible values for each of the profile parameters.

Keys used to perform functions:

F3	Exits the screen without creating or updating the User Profile currently being defined.
F4	Displays the permissible values selection window for the parameter on which the cursor is positioned. The user can then further customize the profile definition by choosing from the available permissible values for that parameter. The permissible values selection window can also be displayed by entering a “?” in the first position of a field followed by a blank.
F12	Returns to the “Maintain User Profile Based On Template” screen-1, without creating or updating the User Profile currently being defined.
Roll Forward/ Page Down	Roll Forward/Advances to the next detail screen for all detail screens except detail screen 5, which is the last detail screen.
Roll Back/ Page Up	Returns to the previous detail screen for all detail screens except detail screen 1, which is the first detail screen.
Enter Key	Perform error checking on the User Profile definition currently being defined. If any errors are found, the corresponding error messages will be displayed at the bottom of the screen. When all edits have been satisfied the User Profile will be either be created or changed and you will be returned to the “Changed User Profile Based On Template” prompt.

There are a total of five detail screens containing all the required parameters needed to create or change a User Profile.

Detail screen-2

ARGUS	Maintain User Profile Based on Template	6/17/99
ZPRP75		15:20:53

Type choices, press Enter.

Template . . .	QPGMR	PROGRAMMER AND BATCH USER
User Profile :	GAS	GARY SMITH

User password	*USRPRF
Set password to expired	*NO
Status	*ENABLED
User class	*PGMR
Assistance level	*INTERMED
Current library	*CRTDFT
Initial program to call	PENTAINIT
Library	*LIBL
Initial menu	PENTA01
Library	*LIBL
Limit capabilities	*NO
Special authority	
+ for more values	

More...

F3=Exit F4=Permissible values F12=Previous

The User Profile detail screen-2 requires the entry of the following parameters:

- User Password
- Set Password to expired
- Status
- User Class
- Assistance level
- Current library
- Initial program to call
- Initial menu
- Limit capabilities
- Special authority

Detail screen-3

ARGUS	Maintain User Profile Based on Template	6/17/99
ZPRP75		15:24:56
Additional parameters		
Type choices, press Enter.		
Template . . . : QPGMR	PROGRAMMER AND BATCH USER	
User Profile : GAS	GARY SMITH	
Special environment	<u>*SYSVAL</u>	
Display sign-on information . .	<u>*SYSVAL</u>	
Password expiration interval . .	<u>*SYSVAL</u>	
Limit device sessions	<u>*SYSVAL</u>	
Keyboard buffering	<u>*SYSVAL</u>	
Maximum allowed storage	<u>*NOMAX</u>	
Highest schedule priority . . .	<u>3</u>	
Job description	<u>QDFTJOB</u>	
Library	<u>QGPL</u>	
Group profile	<u>*NONE</u>	
Owner	<u>*USRPRF</u>	
Group authority	<u>*NONE</u>	
Group authority type	<u>*PRIVATE</u>	
		More...
F3=Exit	F4=Permissible values	F12=Previous

The User Profile detail screen-3 requires the entry of the following parameters:

- Special environment
- Display sign-on information
- Password expiration interval
- Limit device sessions
- Keyboard buffering
- Maximum allowed storage
- Highest schedule priority
- Job description
- Group profile
- Owner

- Group authority
- Group authority type

Detail screen-4

ARGUS	Maintain User Profile Based on Template	6/17/99
ZPRP75		15:28:31
Additional parameters		
Type choices, press Enter.		
Template . . . : <u>OPGMR</u>	<u>PROGRAMMER AND BATCH USER</u>	
User Profile : <u>GAS</u>	<u>GARY SMITH</u>	
Supplemental groups <u> </u>		
+ for more values <u> </u>		
Accounting code	<u>*BLANK</u>	
Document password	<u>*NONE</u>	
Message queue	<u>AAC</u>	
Library	<u>QUSRSYS</u>	
Delivery	<u>*BREAK</u>	
Severity code filter	<u>00</u>	
Print device	<u>*WRKSTN</u>	
Output queue	<u>SAFE</u>	
Library	<u>QUSRSYS</u>	
Attention program	<u>ATTENTION</u>	
Library	<u>AUTOMENU</u>	
		More...
F3=Exit	F4=Permissible values	F12=Previous

The User Profile detail screen-4 requires the entry of the following parameters:

- Supplemental groups
- Accounting code
- Message Queue
- Delivery
- Severity code filter
- Print device
- Output Queue
- Attention program

Detail screen-5

ARGUS	Maintain User Profile Based on Template	6/17/99
ZPRP75		15:32:20
Additional parameters		
Type choices, press Enter.		
Template . . .	QPGMR	PROGRAMMER AND BATCH USER
User Profile :	GAS	GARY SMITH
Sort sequence *SYSVAL		
Library		
Language ID *SYSVAL		
Country ID *SYSVAL		
Coded character set ID *SYSVAL		
User options *NONE		
+ for more values		
User ID number *SAME		
Group ID number *SAME		
Home directory *USRPRF		
Authority		
Bottom		
F3=Exit F4=Permissible values F12=Previous		

The User Profile detail screen-5 requires the entry of the following parameters:

- Sort sequence
- Language ID
- Country ID
- Coded character set ID
- User options
- User ID number
- Group ID number
- Home directory
- Authority

Change User Profile Assigned Template Prompt

From the “Maintain User Profile on Template” screen, press **F17** to access the “Change User Profile Assigned Template” screen.

ARGUS
ZPRP75

Change User Profile Assigned Template

6/17/99
15:50:23

Position to : _____

Type options, press Enter.
1=Select

Opt	Template	Description
-	QPGMR_	PROGRAMMER AND BATCH USER

Bottom

F3=Exit
F12=Cancel

Selects and re-assigns a new User Profile Template to be used as a basis for changing the user profile. The permissible values for the user profile parameters are determined by the assigned template definitions. When a user profile is changed, the Change User Profile parameters are loaded with their corresponding permissible values specified by the assigned template. The user can then further customize the profile definition by choosing from the available permissible values for each of the profile parameters. After selecting an assigned associated template, press **Enter**. The “Maintain User Profile Based On Template” detail screen-1 will be displayed.

1=Select - Choose the desired template from the list presented and press **Enter**.

Function Keys

The following function keys are available for this screen:

F3=Exit - Exit the program.

F12=Cancel - Return to the “Maintain User Profile Based On Template” detail screen without changing the assigned Template for the User Profile currently being defined.

Permissible Values - Display the permissible values selection window by using function key **F4** for the field the cursor is positioned in, or entering the “?” character in the first position of a field followed by a blank.

Each of the User Profile parameters specified in the detail screens 2, 3, 4 and 5 have a set of valid entries or Permissible Values that are specific to each parameter. These Permissible Values may be selected from a list displayed from the Permissible Values Selection window. The Permissible Values Selection window allows the user to further customize the profile definition by choosing from the available permissible values for that parameter.

Permissible values selection window

ARGUS
Z

Maintain User Profile Based on Template

6/17/99
16:14:43

Select Permissible Values

Template . . QPGMR_

Type choices, press Enter.
1=Select

Opt PASSWORD

= *SAME

Bottom

F3=Exit F12=Cancel

BATCH USER

ins

LED

RMED

FT

INIT

BL

01

BL

=Previous

More...

You can now further customize the profile definition by choosing from the available permissible values for that parameter.

Function Keys

The following function keys are available for this screen:

F3=Exit - Exit the program without creating or updating the User Profile currently being defined.

F12=Cancel - Return you to the “Maintain User Profile Based On Template” detail screen without creating or updating the User Profile currently being defined.

Option 4 iSeries Password System Values

This option is used primarily to change the “Password Expiration Interval” and the “Password Validation Program” system values. All other password-related system values can be customized from this screen.

If your system already uses a Password Validation Program (PVP), change it to call program ZPCL22 in PSSECURE, passing it the new password parameter (10 bytes, character). If a PVP is not in use, change system value QPWDVLDPGM to specify program ZPPVP in library PSSECURE. System value QPWDEXPITV should also be changed to a sensible value other than *NOMAX, typically set at 90 (days). Help text for system values is available by pressing **Help**.

ZPDF3701	Profile and Password Management	16:21:59	6/17/99
Version: 6.1	Password-Related OS/400 System Values	System:	ARGUS

Password expiration interval.....	<u>999</u>	(1-366, 999)
Password validation program.....	<u>ZPPVP</u>	Lib: <u>PSSECURE</u>

Maximum length of password.....	<u>10</u>	(1 - 10)
Minimum length of password.....	<u>1</u>	(1 - 10)
Require digit in password.....	<u>N</u>	(Y N)
Allow adjacent digits in password (ccc55).....	<u>Y</u>	(Y N)
Allow repeating characters in password (BBBnn)....	<u>Y</u>	(Y N or X)
(X means characters cannot be used consecutively)		
Limit characters in password (a,e,i,o,u, etc.)....	<u>*NONE</u>	(A-Z, 0-9, #, \$, _, @)
Limit password character positions.....	<u>N</u>	(Y N)
(i.e. JOHN1 changed to JOHN2 is not allowed)		
Duplicate password control.....	<u>0</u>	(0, 4, 6, 8, 10, 12, 18, 24, 32)
(0 means pwd can be same as one previously used, 4 means a pwd must be different than the prev 4.)		

ENTER=Update F3=Exit F9=Wrk Pwd Sys Values HELP=Help

Option 5 User Prompted Passwords Menu

The Security Officer can specify the users to exclude from prompting for a new password, as well as the defaults to use when prompting for passwords. Changes to the defaults can be immediately tested using Option 2 “Test User Prompted Passwords”.

PS25

PentaSafe Security Technologies
PS User-Prompted Passwords Menu

CAS
QPADEV0000

Date: 6/1
Time: 7:51

Select one of the following:

1 Users to Exclude From Pwd Promptng

2 Test User Prompted Passwords

3 Defaults For User Prompted Psswrds

Enter Option or Function/Type ==> _____

F1=Help

F3=Exit

F6=Messages

F9=Window

F10=Cnd Li

F12=Previous

F13=Attention

F14=Batch Jobs

F18=Reports

Option 1 Users to Exclude From Password Prompting

Option 1 from the User Prompted Passwords Menu lets you exclude users from User Prompted Passwords and System Generated User Passwords.

The screen displays the User Profile that is to be excluded and the number of days which will pass before a user will be prompted to change the password again.

Change User Exclusions

Lets you specify the user profiles to be excluded from prompting for a new password, or from auto generation of a new password.

ZPDF05	Profile and Password Management	07:49:31	6/07
	Change User Exclusions	System:	ISIS

Enter the profiles to exclude from auto password generation (either method)
Notes: 1) "# of Days" must be blank for User Prompted to be excluded.
2) Generic rules apply for the User Profile. (i.e. Q* or PGMR*)

User Profile	# of Days	(Day override for User Prompted ONLY	1-3
AAA	20		
ACD	20		
B39Q	3		
CAS	120		
CEJK	30		
DNEOR9	39		
EUI23	22		
KDK393	20		
LDK2	30		
NJC39	30		

Enter=Update F3=Exit F5=Refresh F6=Add
No user exclusions exist.

Note

To update User Exclusions, you must press **Enter** prior to exiting this screen.

This feature also gives you the ability to specify the number of days which will pass before the user is prompted to change the password again. The number of days only applies to the User Prompted Passwords method of Profile and Password Management. The value entered here will override the value that was set as the default for User Prompted Passwords. If you would like a user totally excluded from the User Prompted method of Profile and Password Management, then leave this value blank. This list of exclusions applies to the User Prompted Passwords and System Generated User Passwords.

Generics

By placing an asterisk (*) after the prefix of a generic type name, you are able to exclude a set of users. For example, any user profile that begins with Q* will be excluded from Profile and Password Management. This works well for systems that use generic type naming conventions for their user profiles.

Options - The following options are available for this screen:

User Profile - The user you want to set exclusions for. This field lets you position to a specific profile by typing a User Profile in the first field of this column and pressing Enter.

of Days - Enter the number of days that will pass before the user is prompted to change the password again.

Function Keys

The following function keys are available for this screen:

F3=Exit - Ends the current task and returns to the display where you began the task. Any options or changes that you typed will not be processed.

F5=Refresh - Returns you to the first screen and sorts data in the User Profile column in ascending order.

F6=Add - Takes you to the bottom of the list of entries where new user profiles can be added.

Option 2 Test User Prompted Passwords

Lets you test the User Prompted Password screen without first signing off.

_ZPRP04	Password Security Screen	16:28:55	6/17/99
User ID----->	CAS	System:	ARGUS
<div style="border: 2px solid black; padding: 10px; margin: 20px auto; width: fit-content;"><p>1 days till password change. You can press CMD 7 to change now.</p></div>			
Last successful signon was on 6/17/99 at 13:55:42 from			
These fields allow you to give your users some informative text when they sign on to the system.			
If you want the Security Screen to be displayed only when the password needs to be changed, change the display flag.			
PRESS ENTER TO CONTINUE			
F3=Exit			F7=Change your password NOW

Change Your Password

Once a user is prompted by this screen, you can then change the password. The system will then prompt the user to verify the new password. However, the password is valid only if it meets criteria set up on the Defaults for User Prompted Passwords screen (Option 3).

This screen shows the Security Officer exactly what to expect when Profile and Password Management prompts the user for a new password.

For daily use, this initial screen is optional. But when the user's password is expired, this screen is not optional. The user will have to enter a new password.

Note

If you would like a user to test the User Prompted Passwords method, have the user call the program ZPCL10 in the library PSSECURE to access the Security Screen.

Password Security Screen

The below screen is seen by the user upon expiration of the password.

ZPRP04	Password Security Screen	14:00:29 6/21/99 System: ARGUS
User ID-----> CAS		
Current password-> _	YOUR PASSWORD HAS EXPIRED; ENTER YOUR CURRENT	
New password----->	PASSWORD AND THEN ENTER A NEW PASSWORD.	
MASK-----> CCCNN		
Rules for your NEW password:		
1. You cannot use any of your previous <u>5</u> passwords.		
2. Your new password must follow the pattern of the MASK.		
-Enter a Character (A-Z) above each C		
-Enter a Number (0-9) above each N		
-Enter a Character or a Number for each X		
3. You cannot have any repeating characters.		
Last successful signon was on 6/21/99 at 11:00:53 from DSP0000002		
These fields allow you to give your users some informative text when they sign on to the system.		
If you want the Security Screen to be displayed only when the password needs to be changed, change the display flag.		
PRESS ENTER TO CONTINUE		
F3=Exit		

New Password

When a user's password has expired, the user will be prompted by the screen above. At this time, the user must enter the current password. A new password must also be entered according to the rules outlined on the screen. These rules are set up by the Security Officer on the Defaults for User Prompted Passwords screen. Additional rules may apply that are not displayed. Below the rules, more user information is shown that the Security Officer has the ability to change. After the user presses Enter, a second screen is displayed. The user must now re-enter the new password for verification.

Accessing the Password Screen From Your Menus

You can allow users to access the Profile and Password Management Security screen from a menu, so they can change their passwords when they want to. For example, if user XYZ loaned his password to another person, user XYZ would want to change his password the next time he signs on to the system. Specify the following command in your menu:

```
CALL PSSECURE/ZPCL10
```

User XYZ can then press **F7** to prompt the change to his password.

Option 3 Defaults For User Prompted Passwords

Gives the Security Officer the ability to set default values used for User Prompted Passwords.

ZPDF0133	Profile and Password Management	16:50:25	6/17/99
Version: 6.1	Defaults For User Prompted Passwords	System:	ARGUS

Mask for user prompted passwords..... CCCNN (C N X)

Number of days for password prompt..... 45 (1 - 365)

Number of levels for old passwords..... 5 (2 - 32)

Maximum length of password..... 10 (3 - 10)

Disallow adjacent characters (AAA11)..... Y (Y N)

Disallow vowels in password (a e i o u)..... Y (Y N)

Disallow repeating character positions..... Y (Y N)

(i.e. JOHN1 changed to JOHN2 is not allowed)

Display the security screen (# days of warning)... Y 0 (Y/N, 0-365)

Screen title for security screen: Password Security Screen

Informative text These fields allow you to give your users some informative
for security text when they sign on to the system.
screen:
If you want the Security Screen to be displayed only when
the password needs to be changed, change the display flag.

ENTER=Update F3=Exit

Mask for User Prompted Passwords

Lets you set the mask for User Prompted Passwords. Your mask will consist of a combination of Cs, Ns, and Xs. The number of Cs, Ns, and Xs will determine the length of your User Prompted Passwords.

- Cs represent alphabetic characters (A - Z).
- Ns represent numeric characters (0 - 9).
- Xs represent alphabetic or numeric characters (A - Z or 0 - 9).

Mask guidelines:

- The first character must be a C.
- Your mask must be at least three characters long.
- Your mask cannot exceed 10 characters in length.
- No embedded blanks are allowed.
- You can only use Cs, Ns, and Xs in the mask.

Number of Days - Determines the number of days that will pass before a user is prompted to change their password. Specify a value from 1 to 365.

For the password prompting feature to take effect, the value specified for must be less than the system value specified for Password expiration interval (QPWDEXPITV).

Number of Levels - Users tend to use old passwords when they are prompted to change their existing password. To eliminate this unsecured procedure from occurring, you can set the number of password levels accordingly. Set the number of levels from 1 to 32.

Maximum Length - Set a maximum length in characters for the password entered. You can also set a minimum using the mask.

Note

You cannot make the maximum length less than the password mask. Enter a number between 3 and 10.

Disallow Adjacent Characters - Specifies whether adjacent characters and numbers are allowed in passwords.

Disallow Vowels - You can exclude vowels (a, e, i, o, u) from being used in a password. This will prevent users from choosing easy words or names in their password. Type Y if you want to exclude vowels.

Disallow Repeating Characters - An “N” value for this option will perform edit checks on repeating characters as indicated in the following examples:

- AA123 is invalid.
- AB133 is invalid.
- AB123 is valid.

A “Y” value for this option will not perform edit checks on repeating characters.

Prevent Similar Passwords - You can prevent users from entering similar passwords each time they are required to change their password (i.e. JOHN1 → JOHN2). This would not be allowed because the “J”, “O”, “H” and “N” are considered repeating characters. The user would be required to enter a completely different password from the previous password. Type Y if you want to disallow similar passwords.

Display the Security Screen - A “Y” value for this option will display the Security Screen each time the user logs on to the system. The Security Screen displays the last time a user logged on and information was entered by the Security Officer. The user also has the ability to change a password.

The number of days warning is specified here so the system can give advance notice of password expiration.

Screen Title and Text - This allows you to create your own title and informative text for the security screen.

About User Prompted Passwords

When using the User Prompted Passwords method, all jobs must be routed through a specified path. This path must first execute specific security programs. After the security programs have completed execution, the job will be re-routed to its normal processing. This is accomplished by either adding routing steps to your interactive subsystems or changing your initial program.

Routing Entry Install

You can implement Profile and Password Management by adding routing steps to your interactive subsystems. If you have any questions, please call Technical Support BEFORE you attempt this procedure.

To add routing steps to your interactive subsystems:

1. Identify the interactive subsystems where you want User Prompted Passwords to run. Two routing entries must be added to each interactive subsystem on your system.

Note

This step must be done for each interactive subsystem you identified.

2. Substitute the subsystem name in the appropriate commands. You need to add two routing entries to your interactive subsystem. In this example, we will be using QINTER as our interactive subsystem. Our job description for QINTER has a routing data equal to QCMDI, which is why the Compare Value for the first routing entry uses QCMDI. If your initial routing entry is different, specify it in the first routing entry.

- ENDSBS QINTER *IMMED
- ADDRTGE SBSD(QINTER) SEQNBR(x) CMPVAL('QCMDI')
PGM(PSSecure/ZPCL06) POOLID(2)

Note

The POOLID parameter should be equal to the POOLID where the subsystem is currently running. The CMPVAL parameter should be equal to the current compared value that the job description uses. You will get a warning message for this command. The warning notes that 'QCMDI' already exists. This can be ignored.

- ADDRTGE SBSD(QINTER)SEQNBR(2) CMPVAL('ZPASS') PGM(QCMD) POOLID(2)
- STRSBS QINTER

Note

If you have any problems after this procedure, and you want to put your interactive subsystem back to its original state, simply remove the two routing steps that was added with the RMVRTGE command.

Initial Program Install

You can also implement Profile and Password Management by changing your initial program in your user profile by following the instructions below (this method may be easier than using routing entries).

To change your initial program:

1. Grant *PUBLIC *USE authority to program PSSECURE/ZPRP04.
2. Add the following code to your initial programs:

```
ADDLIB  PSSECURE
```

```
CALL    ZPRP04 'Y'
```

```
RMVLIB  PSSECURE
```

Note

This source code is contained in member INITIALPGM of file SOURCE in library PSSECURE. Each user profile whose initial program includes the three statements in step 2 above will utilize Profile and Password Management.

Option 6 System Generated Passwords Menu

The System Generated Passwords menu enables the Security Officer to generate and apply passwords for selected users.

PS26	PentaSafe Security Technologies	CAS	Date: 6/09/00
	PS System-Generated Passwords Menu	QPADEV0000	Time: 11:10:03

Select one of the following:

- 1 Generate & Disply a Pwd for a User
- 2 Auto Generate and Print Passwords
- 3 Disply Profiles Pending Pwd Change
- 4 Change Profiles to Use Genned Pwds
- 5 Users to Exclude From Pwd Generatn
- 6 Defaults For System Generated Pwds

Enter Option or Function/Type ==> _____

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Option 1 Generate and Display a Password for One User

This option, which is also available as command ZPGENPWD, is primarily intended to generate a password for a new user profile so the Security Officer can determine a user's password. It will prompt for the user profile and then show a window containing the password.

This feature is convenient when a user forgets a password. When the password is generated, the user profile's password expires and must be changed at the next sign-on.

Passwords are generated using the System Generated Passwords defaults.

Note

Command ZPGENPWD can be executed from a command line or set up as a PDM option. You must qualify ZPGENPWD to PSSECURE if PSSECURE is not in your library list.

Option 2 Auto Generate and Print Passwords

Lets you generate random passwords for one or all of the user profiles on your system and print the new passwords for distribution.

ZPDF0141	Profile and Password Management	11:54:10	6/21/99
Version: 6.1	Auto Generate & Print Passwords	System:	ARGUS
User, Gen*, *ALL, GROUP... <u>*ALL</u> (i.e. CHARLIE, AP*, *ALL)			
Effective date..... <u> </u> / <u> </u> / <u> </u> (MDY - for reporting purposes only)			
Mask for your passwords... <u>CCNNX</u>			
Report title (40 char).... <u>NOTIFICATION OF PASSWORD CHANGE</u>			
center here			
Text on document:			
(3 lines, 50 char. each) <u>YOUR PASSWORD WILL BE CHANGED ON THE EFFECTIVE</u>			
<u>DATE LISTED ABOVE. PLEASE CALL X9999 IF YOUR NEW</u>			
<u>PASSWORD DOES NOT WORK AFTER THAT DATE.</u>			
<u>Job information:</u>		<u>Forms information:</u>	
Jobque.....	<u>QBATCH</u>	Output queue.....	<u>QPRINT</u>
Hold job on jobque..	<u>*NO</u>	Hold spool file....	<u>*YES</u>
		Number of copies....	<u>1</u>
		Lines per page.....	<u>66</u>
		Lines per inch.....	<u>6</u>
		Overflow line nbr...	<u>060</u>
ENTER=Submit F3=Exit			

Note

Some user profiles do not have a password. QSPL is one example. If a user profile does not have a password, none will be generated for it.

User, Generic, All, or Group Files

Generate new passwords for one user, a group of generic users, members of Group Profiles (and the Group Profiles, if they have passwords), or all of your users. This feature is convenient for users who forget new passwords. You can generate passwords as follows:

- Generate a password for only one user by specifying the user profile. (i.e., CHARLIE)
- Generate passwords for a group of users by specifying the generic group name followed by an asterisk. (i.e., all of the users in Accounts Payable would be AP*).
- Generate passwords for ALL users by specifying *ALL.
- Generate passwords for group profile members by specifying the full group profile name (it cannot be a generic name).

Note

Users in the exclusion file will be excluded from this method.

Process Environment - For efficiency and security reasons, the Generate and Print process ALWAYS runs in the BATCH environment.

Text Options

At the time of submittal, you can temporarily change your defaults for the text you want to appear on the printed document.

Effective Date	Used for reporting purposes only. The date you enter here will only appear on the printed document next to effective date. You still need to run Option 3 to actually change the passwords of the user profiles.
Mask for your passwords	The pattern of digits and characters to use, where c=character, n=digit, and x=either character or digit.

Report Title	40 characters used as a heading
Text on Document	3 lines of 50 characters each are available for you to put special notes on the printed document. In the previous example, a phone number is listed for the users if they have any questions or problems.

Job Information

Temporarily override your defaults for the Job Information. For example, if you wanted to run this job in a special jobque, you have the ability to temporarily override that here. If you want the change to be permanent, use Option 4 from the Main Menu to change your defaults.

Jobque	The Job Queue where you want this job to enter the system
Hold jobque	You can hold the job in the JOBQ with this feature

Forms Information

Temporarily override your defaults for the Forms Information. For example, if you want to send the change notices to a special OUTQ, you have the ability to temporarily override that here. If you want the change to be permanent, use Option 4 from the Main Menu to change your defaults.

OUTQue	The Output Queue where the change notices are to be printed
Hold Spool File	You can hold the change notices in the OUTQ until you are ready to print them
Number of copies	Specify the number of copies of each change notice you want to print
Lines per page	Specify the number of lines per page depending on your form size
Lines per inch	Specify the number of printed lines per inch on your forms
Overflow line nbr	Specify the overflow line number of your forms

Notification of Password Change Report

Produces a report for each user profile pending change to the generated password. Each notice is printed on its own page. To print this report, see “Option 2 Auto Generate and Print Passwords” on page 226.

The change notice was designed to fit in an envelope. If you want to change the layout of the change notice, the source for printer file ZPPRTF is located in source file SOURCE in library PSSECURE.

Report Layout

A sample Notification of Password Change Report is as follows:

```

                                     Display Spooled File
File . . . . . ZPPRTF                                     Page/Line 1/2
Control . . . . . _____                               Columns 1 - 130
Find . . . . . _____
*.....1.....+...2.....+...3.....+...4.....+...5.....+...6.....+...7.....+...8.....+...9.....+...0.....+...1.....+...2.....+...3
ZPPR01                                                    6/21/99
*****
***          NOTIFICATION OF PASSWORD CHANGE          ***
***
*** SYSTEM NAME:      RCQ PRO                          ***
***
*** USER PROFILE:     CAS                              ***
***                   Cynthia Sitton                    ***
***
*** NEW PASSWORD:      DV93B                          ***
***
*** EFFECTIVE DATE:    06/21/99                        -      ***
***
*** SPECIAL INSTRUCTIONS:
***   YOUR PASSWORD WILL BE CHANGED ON THE EFFECTIVE   ***
***   DATE LISTED ABOVE. PLEASE CALL X9999 IF YOUR NEW ***
***   PASSWORD DOES NOT WORK AFTER THAT DATE.         ***
*****
F3=Exit  F12=Cancel  F19=Left  F20=Right  F24=More keys                                     More...
```

Fields - The Notification of Password Change contains the following information:

- Report Title** 40 characters.
- System Name** Contains the name of the system where the password was generated. (VERY IMPORTANT FOR MULTIPLE SYSTEM USERS!)

Function Key

The following function key is available for this screen:

F11=Remove ALL pending - Removes all records from the “pending” file, which is a work file containing the records in the list shown above.

Option 4 Change Profiles to Use Generated Passwords

Change the specified user profile(s) to use the password generated using Option 2 (Auto Generate and Print Password). Change one or ALL of the user profiles that have passwords generated.

```

ZPDF0143          Profile and Password Management      14:42:10    6/21/99
Version: 6.1      Change Profiles with Generated Passwords  System:  ARGUS

Enter user or group profile, gen*, or *ALL..... _____

Change user profiles interactively or in batch.. I   I = Interactive
                                                B = Batch

Jobque for batch job..... QBATCH_____

Last date passwords were generated..... 06/21/99

ENTER=Run      F3=Exit

```

User, Group, Generic, or All Profiles - Change the password for one user, a group, generic users, or all of the user profiles. After you generate the new password, you can make the following changes:

- If you want to change only one user, specify that user profile.
- If you want to change a group of user profiles, specify the generic group name followed by an asterisk.
- If you want to change all user profiles, specify *ALL.

Processing Environment - This process can be run interactively or in batch:

- to run this job interactively, type **I** in the Submit field.
- to run this job in the batch environment, type **B** in the Submit field.

Jobq - The Job Queue (JOBQ) where you want this job to enter the system (Batch run only).

Last Date Passwords Generated - Displayed only for reference, the date when the Generate and Print option was last used.

Output - This process will NOT generate any printed output.

Option 5 Users To Exclude From Password Generation

The Users to Exclude from Password Generation function is used to specify which users should not have passwords automatically generated and changed.

```
ZPDF05                               Profile and Password Management      15:30:20   6/15/80
                                     Change User Exclusions          System:  ISIS
```

Enter the profiles to exclude from auto password generation (either method):

Notes: 1) "# of Days" must be blank for User Prompted to be excluded.
2) Generic rules apply for the User Profile. (i.e. Q* or PGMR*)

<u>User Profile</u>	<u># of Days</u>	(Day override for User Prompted ONLY 1-365)
.....		
AAA	20	
AAA1	20	
CAS	24	
PMB	45	
SVELL	10	
.....	
.....	
.....	
.....	
.....	
.....	

+

Enter=Update F3=Exit F5=Refresh F6=Add

Change User Exclusions - The user profiles to be excluded from prompting for a new password or from auto generation of a new password.

Note

To update User Exclusions, press **Enter** prior to exiting this screen.

This feature gives you the ability to specify the number of days which will pass before the user is prompted to change the password again. The number of days only applies to the User Prompted Passwords method of Profile and Password Management. The value entered here will override the value that was set as the default for User Prompted Passwords. If you would like a user totally excluded, then leave this value blank. This list of exclusions applies to the User Prompted Passwords and System Generated User Passwords.

Generics - By placing an asterisk (*) after the prefix of a generic type name, you are able to exclude a set of users. For example, any user profile that begins with Q* will be excluded from Profile and Password Management. This works well for systems that use generic type naming conventions for their user profiles.

Option 6 Defaults For System Generated Passwords

Lets you specify defaults for automatic generation of passwords. You can enter your text, job, and forms information once. You do not have to re-enter the information every time you use the application.

ZPDF0145	Profile and Password Management	14:54:22	6/21/99
Version: 6.1	Defaults For Generated Passwords	System:	ARGUS
Mask for your passwords... <u>CCNNX</u> (C N X - min 3 char, first must be C)			
System name on report.... <u>RCO PRO</u>			
Report title (40 char).... <u>NOTIFICATION OF PASSWORD CHANGE</u> center here			
Text on document: (3 lines, 50 char. each) <u>YOUR PASSWORD WILL BE CHANGED ON THE EFFECTIVE</u> <u>DATE LISTED ABOVE. PLEASE CALL X9999 IF YOUR NEW</u> <u>PASSWORD DOES NOT WORK AFTER THAT DATE.</u>			
<u>Job Information:</u>		<u>Forms Information:</u>	
Jobque..... <u>QBATCH</u>		Output queue..... <u>QPRINT</u>	
Hold job on jobque.. <u>*NO</u> (*YES *NO)		Hold spool file.... <u>*YES</u> (*YES *NO)	
		Number of copies.... <u>1</u>	
		Lines per page..... <u>66</u>	
		Lines per inch..... <u>6</u>	
		Overflow line nbr... <u>060</u>	
ENTER=Update F3=Exit			

Mask for System Generated Passwords - This feature lets you specify the mask for your randomly generated passwords. Your mask will consist of a combination of Cs, Ns, and Xs. The number of Cs, Ns, and Xs will determine the length of your generated passwords.

- Cs represent alphabetic characters (A - Z).
- Ns represent numeric characters (0 - 9).
- Xs represent alphabetic or numeric characters (A - Z or 0 - 9).

Mask guidelines:

- The first character must be a C.
- Your mask must be at least 3 characters long.
- Your mask cannot exceed 10 characters in length.
- No embedded blanks are allowed.
- You can only use Cs, Ns, or Xs in the mask.

Note

If you change your password mask, ALL user profiles with a password change pending will be cleared. This is necessary because the Generate and Change will not be synchronized.

Text Options - These fields are printed on the change notice. You can set them once and then make minor modifications when you actually generate and print.

Report Title	40 characters used as a heading.
Additional Text	3 lines of 50 characters, each are available for you to put special notes on the printed document. In the previous example, a phone number is listed for users if they have any questions or problems.

Job Information - Lets you set the job information as to how they will be submitted.

Jobque	The job queue where you want this job to enter the system
Hold jobque	You can hold the job in the jobque with this feature

Forms Information - These fields allow you to set the forms information for the type of forms you will be using to print your change notices.

OUTQue	The Output Queue where the change notices are to be printed.
Hold Spool file	You can hold the change notices in the OUTQ until you are ready to print them.
Number of Copies	Specify the number of copies of each change notice you want to print
Lines per Page	Specify the number of lines per page, depending on your form size
Lines per Inch	Specify the number of printed lines per inch on your forms
Overflow line nbr	Specify the overflow line number for your forms

Forms Tip - There is a special form envelope offered by some vendors which is already sealed. You can type or print on the outside of the envelope, but you must open to read it. This means you can print an address on the outside of the envelope and the password on the inside.

Test System Generated Passwords - Because the Profile and Password Management software can change the passwords for ALL users, be certain of your options on the selection screen. In particular, the user profiles to be excluded that are specified by the Main Menu Option 5, submenu Option 1.

Before you test the application, please read the entire User Reference Guide.

It is suggested that you try the System Generated Passwords method for two or three test users. Running through the application a few times will give you confidence in it and a feel for how long each process takes.

Note

The options referenced below are from “Option 6 System Generated Passwords Menu” on page 225.

Testing Random Generated Passwords - When testing this method, you must set the Defaults for System Generated Passwords (Option 6) according to your specifications. Then you can run the Auto Generate and Print passwords (Option 2) for a few user profiles. When this is complete, it will provide you with documentation on the passwords that have been generated. Compare the information shown on the Notification of Password Change document with the values shown on the screen for Option 2 to verify the correct generation of passwords and output.

Next, select Option 3, Display the User Profiles Pending Change. This provides the Security Officer with a list of user profiles pending password change. This is helpful for determining which users have not changed their passwords.

Then, select Option 4, Change User Profiles to use Generated Passwords. Run this option for each user profile that you selected in Option 2. Once this is done, the process is complete.

There is one final check and that is, can your users sign on?

Profile and Password Management and the OS

iSeries Considerations

Profile and Password Management does not affect or change the Operating System/400. As a matter of fact, the iSeries servers “password system” does not need to be turned on in order for Profile and Password Management to function. Profile and Password Management will perform all validity checks, prompt for password change, and change passwords without any changes to the iSeries System Values.

System Values

The Profile Synchronizer feature requires that, at a minimum, two iSeries System Values (QPWDVLDPGM and QPWDEXPITV) be used, and directory and network job routing table entries be added for SNADS.

PC Software

Passwords embedded in PC software for iSeries access, such as Rumba/400, Client Access/400, and PC support will not be changed by Profile and Password Management Profile Synchronizer. However, NetIQ Corporation provides an API which can be run on a PC (using the RCMD command, for example) to change a user's password on an iSeries. Use the following command to call the API:

```
CALL PGM(PSSecure/ZPCL16) PARM(user_profile password)
```

Profile Synchronizer

The SNADS subsystem must be active on the source and the target systems for the Profile Synchronizer to work.

Profile and password synchronization can be performed using TCP/IP and any network configured for APPC. For assistance in setting up the Profile Synchronizer in your environment, contact Technical Support.

Chapter 4

Object Authority Management

Authority Templates

Authority templates facilitate object-level security on your iSeries. You can use authority templates as a standard to which objects in a library must comply.

A template for the specified authority compares objects in a library. You can run a report to show which objects are out of compliance with a specified template. Once you know which objects are out of compliance, you can force all objects to comply with the template or force individual objects to comply with the template.

PS4	NetIQ Corporation Object Authority Management	KRAMERM QPADEV000J	Date: 9/03/08 Time: 11:33:27
Select one of the following:			
1 Work With Templates			
2 Work With Groups			
3 Work With Filters			
10 Non-Comp Report/Force Compliance			
11 Work With Non-Compliant Objects			
20 Generate Authority File (PSAudit)			
Enter Option or Function/Type ==> _____			
F1=Help	F3=Exit	F6=Messages	F9=Window
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports
F10=Cmd Line			

Key Conventions

Option and Function

All the panels within Object Authority Management use CUA standard panel options and function keys.

In addition to the standard keys within the system, you also have the ability to set up your own function key definitions on menus and action bars. For more information, see “User Defined Function Keys” on page 14.

Option

You can enter options in front of the record you want to modify to execute processes on individual objects. Type the option number next to a record and press ENTER. You can type the same option next to multiple objects before you press ENTER, and you can type a different option number next to each object.

The following table lists standard options within Object Authority Management:

OPTION	DESCRIPTION
2=Edit	Lets you change a record.
4=Delete	Lets you delete a record.
5=Display	Displays more information on objects. You can see the contents or attributes of an object depending on the object type.
7=Detail	Lets you edit, delete, or display dependent records within a group.

Function Keys

The following table lists standard function keys available in Object Authority Management:

FUNCTION KEY	DESCRIPTION
F1=Help	Provides information about using the screen or specific fields on the screen. If the cursor is not positioned in a field, help shows for the entire screen.
F3=Exit	Ends the current task and returns to the screen where you began the task. Any options or changes that you typed are not processed.
F5=Refresh	Restores the screen data to a previous state or updates the screen with current statistics.
F6=Add	Lets you add a record to the current file.

FUNCTION KEY	DESCRIPTION
F7=Review	Lets you sort and position records by specifying a sort column number and entering key position data in the place provided.
F8=Browse	Lets you page through records by entering name patterns and pressing ENTER.
F10=Cmd Line	Displays a command line that lets you enter system commands. This option is available only on the OAM main menu.
F12=Cancel	Cancels processing of any options or changes that you have typed on the current display and returns to the previous display.
F13=Repeat	Repeats the option you type in the entry fields below your current position on the screen.
F17=Audit Stamp	Lets you view and audit changes to the current record. You can view the date and time the record was changed, the workstation where the change was made, the user who made the change, and the program where the change was made. F15 lets you move this window to another area on the screen.

Option 1 Work With Templates

Use this option to work with all defined authority templates.

Work With Authority Templates

Position to Template. . . . _____

Type options, press Enter.
2=Change 4=Delete 5=Use(Report/Comply)
Exceptions: 6=Type 7=Owner by Type 8=Object 9=Owner by Object
10=Authorization List by Type 11=Authorization List by Object

Opt Template	Description
— CASAUTHOBJ	AUTHORIZATION LIST BY OBJECT
— CASAUTHYP	AUTHORIZATION LIST BY TYPE
— CASOBJECT	OBJECT AUTHORITY
— CASOWNOBJ	OWNER BY OBJECT AUTHORITY
— CASOWNTYP	OWNER BY TYPE AUTHORITY
— CASTYPE	AUTHORITY TEMPLATE
— CSTES1	TSTEMPLATE
— MAIN	SDASDF
— PMBTST1	OBJECT AUTHORITY TEMPLATE
— PMBTST2	USER PROFILE

More...

F3=Exit F6=Add new template F12=Cancel F17=Top F18=Bottom

Position to Template - This field is used for repositioning a name in the template column, not for creating a subset of the list. The list is sorted by template and description.

Options

2=Change - Lets you change the contents or attributes of an existing authority template. F8 (Edit Authorities) also allows the object authorities of the template to be changed.

5=Use (Report/Comply) - Generates a report showing non-compliance, or forces all objects to comply by changing the non-compliant objects' authority to match the template. Specify the following:

- the output file generated for authorities
- whether to generate a report or force the object to comply
- the JOBQ in which you want the report to run.

Prompt for Report or Compliance	
Template. . . . :	MAIN
Description . . :	SDASDF
File/Library. . :	_____ (file generated for authorities)
Comply flag . . :	<u>N</u> (Y=Change authorities N=Report Only)
JOBQ. :	<u>QBATCH</u>
F3=Exit ENTER=Submit	

Note

If this is a compliance job (Comply flag = Y), all objects in the specified library will be changed with the authorities specified in the authority template. After the compliance job is complete, the specified output file must be regenerated (OAM - Option 3) to reflect changes. In addition, the objects must not be in use while the job is running. The job should be run after hours at a time when there is very little or no other activity.

If this is an audit job (Comply flag = N), information will be written to a file used by the View/Change Non-Compliant Objects option.

Report Layout - The following sample shows the format of the Object Authority Non-Compliance Report:

AT004R1		Object Authority Non-Compliance Report										09/03/08	PAGE	1
TEMPLATE USED: EX1		CHANGE AUTHORITIES: N												
-----Object----- -----Data-----														
Library	Object	Type	Auth.	Opr	Mgt	Ext	Alt	Ref	Rd	Add	Upd	Del	Exc	Reason
EX1	A	*PGM												Object Owner does not match Template
		QSECOFR	*ALL	X		X	X	X	X	X	X	X	X	Object User not found on Template
		*PUBLIC	*CHANGE	X						X	X	X	X	Authority does not match Template
EX1	QAUOOP	*FILE												Object Owner does not match Template
		QSECOFR	*ALL	X		X	X	X	X	X	X	X	X	Object User not found on Template
		PSOBJOWN	*USE	X						X			X	Object User not found on Template
*** END OF REPORT ***														

The compliance flag selected is shown in the report heading. If the compliance flag is set to flag=Y, a list of all the objects changed from non-compliant to compliant is displayed. If all objects are already in compliance (whether the compliance flag=Y or N), only the library name is displayed.

6=Type - Use this option to maintain exceptions to the template for object types and object attributes.

```

AT0102T1                                7:20:15    6/02/2000
ISIS                                  PentaSafe Security Technologies, Inc    Review

```

Template PMBTST1 OBJECT AUTHORITY TEMPLATE

Type options, press Enter.

2=Edit 4=Delete 5=Display

1

	(1)	(2)	(3)	
Object	Object	User	Object	
Opt Type	Attribute	Profile	Authority	
— *DTAARA	*ALL	*PUBLIC	*EXCLUDE	
— *DTAARA	*ALL	PMB	*ALL	
— *DTAARA	*ALL	PMBT123456	*ALL	
— *FILE	*ALL	*PUBLIC	*EXCLUDE	
— *FILE	*ALL	PMB	*ALL	
— *PGM	*ALL	*PUBLIC	*EXCLUDE	
— *PGM	*ALL	PMB	*ALL	
— *PGM	*ALL	PMBT123456	*ALL	
— *USRSPC	*ALL	*PUBLIC	*EXCLUDE	

More...

F1=Help F3=Exit F6=Add F7=Review F8=Browse

F13=Repeat

(c) Pentasafe Security Technologies, Inc. 2000

Column - Type the number of the column that you want to use to sort records, and press ENTER. The data appears in ascending order. Only one of the column numbers shown can be entered in the column field.

Sort Criteria (1) - Type the name of the object type and press ENTER. The first record containing the object type is repositioned to the top of the column. Other records are listed below in ascending order by object type.

Sort Criteria (2) - Type the name of the object attribute and press ENTER. The first record containing the specified object attribute is repositioned to the top of the column. Other exceptions are listed below in ascending order by object attribute.

Sort Criteria (3) - Type the name of the User Profile and press ENTER. The first record containing the specified user profile is repositioned to the top of the column. Other exceptions are listed below in ascending order by User Profile.

OBJECT TYPE - The object type you select to administer, such as command (*CMD), file (*FILE), or program (*PGM).

Object Attribute - The object attribute you select to administer

User Profile - The user profile you select to administer. The value *PUBLIC defines the authorities of all users who are not specifically named and are not members of the authorization list used to secure the object.

Object Authority - The authority of a user to access the selected object. The following system-defined object authority levels are valid values for this field:

- ***ALL** - Allows all operations on the object except those that are limited to the owner or controlled by authorization list management authority.
- ***CHANGE** - Allows all operations on the object except those that are limited to the owner or controlled by:
 - object existence authority
 - object alter authority
 - object reference authority or
 - object management authority
- ***EXCLUDE** - Prohibits operations on the object.

- ***USE** - Allows access to the object attributes and use of the object. The user cannot change the object.
- **USER DEF** - Displayed by the system when the object authorities and data authorities do not match any of the predefined object authority levels above. You display the authorities by pressing the “display detail” function key. The value ***AUTL** is also valid when public authorities are being defined. It indicates that the public authority specifications in the authorization list used by this object should be used to determine public authority.

F6=Add - Lets you add an exception for object type and attribute.

AT0102B	Type and Attribute Exception Maintenance		7:22:33	6/02/2000
ISIS	PentaSafe Security Technologies, Inc		Add	
Template	PMBTST1			
Object Type	*PGM			
Object Attribute	RPG			
User Profile	QPGMR			
---- Non Key Fields ----				
Object Authority	*ALL			
-----Object-----				
Opr	Mgt	Exist	Alter	Ref
X	X	X	X	X
-----Data-----				
Read	Add	Upd	Dlt	Exc
X	X	X	X	X
F1=Help F3=Exit F5=Refresh F6=Add F7=Review				
F8=Browse F12=Cancel F17=Audit Stamp				

Object - The authorities of a user to access the selected object. “X” indicates that the user has the specified authority to the object. The following object authorities are valid for this field:

Opr - Object operational authority—allows you to view the object’s attributes and to use the object as specified by the users data authorities.

Mgt - Object management authority—allows you to specify security, to move or rename the object, and to add members if the object is a database file.

Exist - Object existence authority—allows you to control the object’s existence and ownership.

Alter - Object alter authority—provides authority to change the attributes of an object, such as adding or removing triggers for a database file.

Ref - Object reference authority—allows you to specify the object as the first level in a referential constraint. You can type **x** in the field to give authority or delete the **x** in the field or leave the field blank to remove object authorities.

Data - The authorities of a user to access the data contained in a selected object. “X” indicates that the user has the specified authority to the selected object. Following are the specific data authorities available to the user:

- **Read** - Read authority —allows you access the contents of the object.
- **Add** - Add authority —allows you to add entries to the object.
- **Update** - Update authority —allows you to change the content of existing entries in the object.
- **Delete** - Delete authority —allows you to remove entries from the object.
- **Execute** - Execute authority —allows you to run a program or search a library or directory. You can type **x** in the field to give authority. Delete the **x** in the field or leave the field blank to remove object authorities.

7=Owner by Type - Lets you manage exceptions to the template for object owners based on object type.

AT0105T1 Object Owner Exception by Type 7:27:55 6/02/2000

ISIS PentaSafe Security Technologies, Inc Review

Template PMBTST2 USER PROFILE

Type options, press Enter.

2=Edit 4=Delete 5=Display

1

	(1)	(2)	(3)
Opt	Type	Attribute	Owner
—	*DTAARA	*ALL	PMBT
—	*FILE	*ALL	PMB
—	*FILE	DFU	PMBT1
—	*FILE	PF	PMB
—	*PGM	RPG	PMB
—	*USRPRF	*ALL	PMB

F1=Help F3=Exit F6=Add F7=Review F8=Browse

F13=Repeat

(c) Pentasafe Security Technologies, Inc. 2000

Bottom

Column - Type the number of the column that you want to use to sort records, and press ENTER. The data appears in ascending order. Only one of the column numbers shown can be entered in the column field.

Note
You can also sort by entering “POSITION TO” data over one column at a time.

Sort Criteria (1) - Type the name of the object type and press ENTER. The record containing the object type is repositioned to the top of the column. Other objects are listed below in ascending order by Object Type.

Sort Criteria (2) - Type the name of the object attribute and press ENTER. The record containing the object attribute is repositioned to the top of the column. Other records are listed below in ascending order.

Sort Criteria (3) - Type the name of the Object Owner and press ENTER. The record containing the object owner is repositioned to the top of the column. Other records are listed below in ascending order.

- **Object Type** - The object type you selected to administer, such as command (*CMD), file (*FILE), or program (*PGM).
- **Object Attribute** - The object attribute you selected to administer.
- **Object Owner** - The object owner for which the exception is being created.

F6=Add - Lets you add an exception for object owner by type.

```

AT0105B          Object Owner Exception by Type          7:32:06  6/02/2000
ISIS             PentaSafe Security Technologies, Inc    Add

Template . . . . . PMBTST2
Object Type . . . . . *PGM
Object Attribute . . . . . *ALL
Object Owner . . . . . UXR

---- Non Key Fields ----
User Profile . . . . . *SAME
Use Adopt Authority . . . . . *SAME

F1=Help      F3=Exit      F5=Refresh      F6=Add      F7=Review
F8=Browse    F12=Cancel  F17=Audit Stamp

```


User Profile - Specifies whether the authority checking, done while this program is running, should include only the user who is running the program (*USER) or both the user running the program and the program owner (*OWNER). The profiles of the program user or both the program user and the program owner are used to control which objects can be used by the program, including the authority the program has for each object. Only the program owner or a user with QSECOFR authority can change the user profile attribute. The following are valid values for this field:

- ***SAME** - The user profile attribute does not change.
- ***USER** - The program runs under the user profile of the program's user.
- ***OWNER** - The profiles of both the program's owner and the program's user are used when the program is processed. The collective sets of object authority in both user profiles are used to find and access objects during program processing. Authority from the owning user profile's group profile is not included in the authority for the running program.

You can change the object authority by typing a new value over the current value.

Use Adopt Authority - Program adopted authority from previous programs in the call stack, can be used as a source of authority when this program is running. The following are valid values for this field:

- ***SAME** - The "use adopted authority" attribute does not change.
- ***YES** - Program adopted authority from previous call levels is used when this program is running. If an authorization list is specified for the QUSEADPAUT system value, and the user is not authorized to that list, *NO is used.
- ***NO** - Program adopted authority from previous call levels is not used when this program is running.

8=Object - Lets you manage exceptions to the template for specific object names.

AT0103T1 Object Exceptions Maintenance 7:37:39 6/02/2000
ISIS PentaSafe Security Technologies, Inc Review

Template PMBTST1 OBJECT AUTHORITY TEMPLATE
Type options, press Enter.
 2=Edit 4=Delete 5=Display

1

	(1)	(2)	(3)	(4)	
Opt	Object Name	Object Type	Object Attribute	User Profile	Object Authority
—	AABC	*DTAARA	*ALL	*PUBLIC	*EXCLUDE
—	ABCDEF GHIJ	*DTAARA	*ALL	*PUBLIC	*EXCLUDE
—	ABCDEF GHIJ	*DTAARA	*ALL	PMBT10	*ALL
—	A0001	*PGM	*ALL	*PUBLIC	
—	A0002	*PGM	*ALL	*PUBLIC	
—	A0003	*PGM	*ALL	*PUBLIC	
—	A0004	*PGM	*ALL	*PUBLIC	
—	A0005	*PGM	*ALL	*PUBLIC	
—	A0006	*PGM	*ALL	*PUBLIC	

More...

F1=Help F3=Exit F6=Add F7=Review F8=Browse
F13=Repeat
(c) Pentasafe Security Technologies, Inc. 2000

Column - Type the number of the column that you want to use to sort records, and press ENTER. The data appears in ascending order. Only one of the column numbers shown can be entered in the column field.

Note

You can also sort by entering “POSITION TO” data over one column at a time.

Sort Criteria (1) - Type the name of the object and press ENTER. The first record containing the specified object name is repositioned to the top of the column. Other records are listed below in ascending order by object name.

Sort Criteria (2) - Type the name of the object type and press ENTER. The first record containing the specified object type is repositioned to the top of the column. Other records are listed below in ascending order by Object Type.

Sort Criteria (3) - Type the name of the object attribute and press ENTER. The first record containing the specified object attribute is repositioned to the top of the column. Other records are listed below in ascending order by Object Attribute.

Sort Criteria (4) - Type the name of the user and press ENTER. The first record containing the specified user profile is repositioned to the top of the column. Other records are listed below in ascending order by User Profile.

Object Name - The name of the object for which the exception is being created.

Object Type - The object type you selected to administer, such as command (*CMD), file (*FILE), or program (*PGM).

Object Attribute - The object attribute you selected to administer.

User Profile - The user profile you select to administer. The value *PUBLIC defines the authorities of all users who are not specifically named and are not members of the authorization list used to secure the object.

Object Authority - The authority of a user to access the selected object. The following system-defined object authority levels are valid values for this field:

- ***ALL** - Allows all operations on the object except those that are limited to the owner or controlled by authorization list management authority.
- ***CHANGE** - Allows all operations on the object except those that are limited to the owner or controlled by:
 - object existence authority
 - object alter authority
 - object reference authority or
 - object management authority
- ***EXCLUDE** - Prohibits operations on the object.

- ***USE** - Allows access to the object attributes and use of the object. The user cannot change the object.
- **USER DEF** - Displayed by the system when the object authorities and data authorities do not match any of the predefined object authority levels above. You display the authorities by pressing the “display detail” function key. The value ***AUTL** is also valid when public authorities are being defined. It indicates that the public authority specifications in the authorization list used by this object should be used to determine public authority. You can change the object authority by typing a new value over the current value.

F6=Add - Lets you add an exception for an object.

AT0103B	Object Exceptions Maintenance		7:40:21	6/02/2000
ISIS	PentaSafe Security Technologies, Inc		Add	
Template	PMBTST1			
Object Name	CURMDV			
Object Type	*FILE			
Object Attribute	*ALL			
User Profile	CAS			
---- Non Key Fields ----				
Object Authority	*ALL			
-----Object-----				
Opr	Mgt	Exist	Alter	Ref
<u>X</u>	<u>X</u>	<u>X</u>	<u>X</u>	<u>X</u>
-----Data-----				
Read	Add	Upd	Dlt	Exc
<u>X</u>	<u>X</u>	<u>X</u>	<u>X</u>	<u>X</u>
F1=Help F3=Exit F5=Refresh F6=Add F7=Review				
F8=Browse F12=Cancel F17=Audit Stamp				

Object - The authorities of a user to access the selected object. “X” indicates that the user has the specified authority to the object. The following object authorities are valid for this field:

- **Opr** - Object operational authority—allows you to view the object’s attributes and to use the object as specified by the users data authorities.
- **Mgt** - Object management authority—allows you to specify security, to move or rename the object, and to add members if the object is a database file.
- **Exist** - Object existence authority—allows you to control the object’s existence and ownership.
- **Alter** - Object alter authority—provides authority to change the attributes of an object, such as adding or removing triggers for a database file.
- **Ref** - Object reference authority—allows you to specify the object as the first level in a referential constraint. You can type an X in the field to give authority or delete the X in the field or leave the field blank to remove object authorities.
- **Data** - The authorities of a user to access the data contained in a selected object. X indicates that the user has the specified authority to the selected object. Following are the specific data authorities available to the user:
 - **Read** - Read authority—allows you access the contents of the object.
 - **Add** - Add authority—allows you to add entries to the object.
 - **Update** - Update authority—allows you to change the content of existing entries in the object.
 - **Delete** - Delete authority—allows you to remove entries from the object.
 - **Execute** - Execute authority—allows you to run a program or search a library or directory. You can type an X in the field to give authority. Delete the X in the field or leave the field blank to remove object authorities.

9=Owner by Object - Lets you manage exceptions to the template for specific object owners.

```
AT0104T1      Owner Exception List      7:43:46  6/02/2000
ISIS          PentaSafe Security Technologies, Inc  Review

Template . . . . . PMBTST1  OBJECT AUTHORITY TEMPLATE
Type options, press Enter.
  2=Edit      4=Delete      5=Display

1
  (1)      (2)      (3)      (4)
  Object   Object   Object   Object
Opt  Name   Type    Attribute Owner
--  ---
  ABC      *PGM     *ALL     PMB
  TST1     *FILE     *ALL     PMB

F1=Help      F3=Exit      F6=Add      F7=Review      F8=Browse
F13=Repeat
(c) Pentasafe Security Technologies, Inc. 2000
```

Column - Type the number of the column that you want to use to sort records, and press ENTER. The data appears in ascending order. Only one of the column numbers shown can be entered in the column field.

Note
You can also sort by entering “position to” data over one column at a time.

Sort Criteria (1) - Type the name of the object and press ENTER. The first record containing the specified object name is repositioned to the top of the column. Other records are listed below in ascending order by Object Name.

Sort Criteria (2) - Type the name of the object type and press ENTER. The first record containing the specified object type is repositioned to the top of the column. Other records are listed below in ascending order by Object Type.

Sort Criteria (3) - Type the name of the object attribute and press ENTER. The first record containing the specified object attribute is repositioned to the top of the column. Other records are listed below in ascending order by Object Attribute.

Sort Criteria (4) - Type the name of the Object Owner and press ENTER. The first record containing the specified object owner is repositioned to the top of the column. Other records are listed below in ascending order by Object Owner.

- **Object Name** - The name of the object you selected to administer.
- **Object Type** - The object type you selected to administer, such as command (*CMD), file (*FILE), or program (*PGM).
- **Object Attribute** - The object attribute you selected to administer.
- **Object Owner** - The object owner for which the exception is being created.

F6=Add - Allows the user to add an exception for an object owner.

AT0104B		Owner Exception List		7:46:17	6/02/2000
ISIS		PentaSafe Security Technologies, Inc		Add	
Template	PMBTST1				
Object Name	<u>EX1</u>				
Object Type	<u>*PGM</u>				
Object Attribute	<u>*ALL</u>				
Object Owner	<u>ARP</u>				
---- Non Key Fields ----					
User	<u>*SAME</u>				
Authority	<u>*SAME</u>				
F1=Help	F3=Exit	F5=Refresh	F6=Add	F7=Review	
F8=Browse	F12=Cancel	F17=Audit Stamp			

User Profile - Specifies whether the authority checking done while this program is running should include only the user who is running the program (*USER) or both the user who is running the program and the program owner (*OWNER). The profiles of the program user or both the program user and the program owner are used to control which objects can be used by the program, including the authority the program has for each object. Only the program owner or a user with QSECOFR authority can change the user profile attribute. The following are valid for this field:

- ***SAME** - The user profile attribute does not change.
- ***USER** - The program runs under the user profile of the program's user.
- ***OWNER** - The profiles of both the program's owner and the program's user are used when the program is processed. The collective set of object authority in both user profiles are used to find and access objects during program processing. Authority from the user profile's group profile is not included in the authority for the running program.

You can change the object authority by typing a new value over the current value.

Use Adopted Authority - Specifies whether program adopted authority from previous programs in the call stack will be used as a source of authority when this program is running. The following are valid for this field:

- ***SAME** - The use adopted authority attribute does not change.
- ***YES** - Program adopted authority from previous call levels is used when this program is running. If an authorization list is specified for the QUSEADPAUT system value and the user is not authorized to that authorization list, *NO is used.
- ***NO** - Program adopted authority from previous call levels is not used when this program is running.

10=Authorization List by Type - Lets you manage exceptions to the template for specific object types.

```

AT0106T1      Authorization List Exceptions by Type      7:53:33      6/02/2000
ISIS          PentaSafe Security Technologies, Inc      Review

Template . . . . . PMBTST1      OBJECT AUTHORITY TEMPLATE
Type options, press Enter.
  2=Edit      4=Delete      5=Display

1
  (1)      (2)      (3)
  Object      Object      Auth.
Opt  Type      Attribute      List
—   *FILE      *ALL      PSSECURE
—   *PGM      *PGM      PSSECURE

F1=Help      F3=Exit      F6=Add      F7=Review      F8=Browse      Bottom
F13=Repeat
(c) Pentasafe Security Technologies, Inc. 2000

```

Sort Criteria (1) - Type the name of the object type and press ENTER. The first record containing the specified object type is repositioned to the top of the column. Other records are listed below in ascending order by Object Type.

Sort Criteria (2) - Type the name of the object attribute and press ENTER. The first record containing the specified object attribute is repositioned to the top of the column. Other records are listed below in ascending order by Object Attribute.

Sort Criteria (3) - Type the name of the list and press ENTER. The first record containing the specified authorization list is repositioned to the top of the column. Other records are listed below in ascending order by Authorization List.

- **Object Type** - The object type you selected to administer, such as command (*CMD), file (*FILE), or program (*PGM).
- **Object Attribute** - The object attribute you selected to administer.
- **Authorization List** - Used to give a group of users one or more types of authority to objects (such as files or programs) or data in the objects (such as records in a file). The list consists of two or more user IDs and their authorities for system resources. You can create the list by using the Create Authorization List (CRTAUTL) command.

11=Authorization List by Object - Lets you manage exceptions to the template for specific objects.

AT0107T1 Object Authorization List Exceptions 7:55:23 6/02/2000
ISIS PentaSafe Security Technologies, Inc Review

Template MAIN SDASDF
Type options, press Enter.
2=Edit 4=Delete 5=Display

1

	(1)	(2)	(3)	(4)
Opt	Object Name	Object Type	Object Attribute	Auth. List
—	ERE	*PGM	*ALL	PSSECURE
—	SDFAS	*FILE	*ALL	*NONE

F1=Help F3=Exit F6=Add F7=Review F8=Browse

F13=Repeat

(c) Pentasafe Security Technologies, Inc. 2000

Bottom

Column - Type the number of the column that you want to use to sort records, and press ENTER. The data appears in ascending order. Only one of the column numbers shown can be entered in the column field.

Note

You can also sort by entering “POSITION TO” data over one column at a time.

Sort Criteria (1) - Type the name of the object and press ENTER. The first record containing the specified object name is repositioned to the top of the column. Other records are listed below in ascending order by Object Name.

Sort Criteria (2) - Type the name of the object type and press ENTER. The first record containing the specified object type is repositioned to the top of the column. Other records are listed below in ascending order by Object Type.

Sort Criteria (3) - Type the name of the object attribute and press ENTER. The first record containing the specified object attribute is repositioned to the top of the column. Other records are listed below in ascending order by Object Attribute.

- **Object Name** - The name of the object you selected to administer.
- **Object Type** - The object type you selected to administer, such as command (*CMD), file (*FILE), or program (*PGM).
- **Object Attribute** - The object attribute you selected to administer.
- **Authorization List** - An authorization list is used to give a group of users one or more types of authority to objects (such as files or programs) or data in the objects (such as records in a file). The list contains two or more user IDs and their authorities for system resources. The list can be created by using the Create Authorization List (CRTAUTL) command.

Function Key

The following function keys are available from this screen:

F6=Add New Template - Lets you create a new Authority Template. Specify the template's name, description, owner, user profile, and authority adoption. F8 (Edit Authorities) lets you change the object authorities of the template.

AT0102BType and Attribute Exception Maintenance7:22:336/02/2000

ISISPentaSafe Security Technologies, IncAdd

TemplatePMBTST1

Object Type*PGM

Object AttributeRPG

User ProfileQPGMR

---- Non Key Fields ----

Object Authority*ALL

-----Object-----

OprMgtExistAlterRef

XXXXX

-----Data-----

ReadAddUpdDltExc

XXXXX

F1=HelpF3=ExitF5=RefreshF6=AddF7=Review

F8=BrowseF12=CancelF17=Audit Stamp

262 User Guide

Option 2 Work With Groups

Lets you manage named groups of libraries, objects, object types, and/or object attributes. These groups are for use in the STROAMAPI command.

AT0100T1
ISIS

Group Name Maintenance
PentaSafe Security Technologies, Inc

7:58:19
6/02/2000

Review

Type options, press Enter.
2=Edit 4=Delete 5=Display 7=Details

1

(1).

(2).

Group

Opt Name Description

— CTEST01 Group CT1

— EXAMPLE1 pauline's example sdfdfeg

— PMBEX1 Group Example

— PMBTST02 Group Object Test

— PMBTST03 Group Object Attrib Test

— PMBTST04 Object Type Group Test

— PMBTST05 Multiple field group test

— PMBTST06 test by pmbt

— PMBTST07 test group

— PMBTST08 test group

F1=Help F3=Exit F6=Add F7=Review F8=Browse

F13=Repeat

More...

(c) Pentasafe Security Technologies, Inc. 2000

Column - Type the number of the column you want to use to sort records, and press ENTER. The data appears in ascending order. You can enter only one of the column numbers shown in the column field.

Note

You can also sort by entering “POSITION TO” data over one column at a time.

Sort Criteria (1) - Type the name of the group and press ENTER. The first record containing the specified group name repositions to the top of the column. Other records list below in ascending order by Group Name.

Group Name - The name of the group of libraries, objects, object types, and/or object attributes you are creating.

Sort Criteria (2) - Type a description of a group and press ENTER. The first record containing the specified group name repositions to the top of the column. Other records list below in ascending order. Sorting is case sensitive for the Description.

Description - User-defined text that briefly describes the group.

F6=Add - Lets you add a group.

7=Details - Lets you work with the details of the group.

AT0101T1
ISIS

Group Name Maintenance
PentaSafe Security Technologies, Inc

8:05:20
6/02/2000
Review

Group Name . . . PMBTST03 Group Object Attrib Test
Type options, press Enter.
2=Edit 4=Delete 5=Display

1

(1), (2), (3),
Group Object
Opt Type Name Description
— A CLP CLP programs
— A RPG RPG Programs

F1=Help F3=Exit F6=Add F7=Review F8=Browse

F13=Repeat

Bottom

Group Name - The name of the currently selected group.

Column - Type the number of the column you want to use to sort records, and press ENTER. The data appears in ascending order. Only one of the column numbers shown can be entered in the column field.

Note

You can also sort by entering “POSITION TO” data over one column at a time.

Sort Criteria (1) - Type the name of the group type and press ENTER. The first record containing the specified group name repositions to the top of the column. Other records list below in ascending order by Group Type.

Sort Criteria (2) - Type an object name and press ENTER. The first record containing the specified object name is repositioned to the top of the column. Other records are listed below in ascending order by Object Name.

Sort Criteria (3) - Type a description of a group detail and press ENTER. The first record containing the specified description is repositioned to the top of the column. Other records are listed below in ascending order by Description. Sorting is case sensitive for the Description.

Group Type - The letter representing the type of group detail being created. Group Type must be A, L, O, or T.

- **A=Object Attributes** - A collection of object attributes. For example: PF, RPG, or CLP.
- **L=Library** - A collection of libraries.
- **O=Object** - A collection of objects.
- **T=Object Type** - A collection of iSeries object types. For example: *FILE, *PGM, or *DTAARA.

Object Name - The name of the object you selected to administer.

Description - User defined text that describes the object.

F6=Add - Lets you add details for the specified group, such as libraries, objects, attributes, or types.

AT0101B	Group Name Maintenance	8:09:50	6/02/2000
ISIS	PentaSafe Security Technologies, Inc	Add	
Group Name	PMBTST03		
Group Type	0		
Object Name	GRPOBN		
---- Non Key Fields ----			
Description	Example Object		
F1=Help	F3=Exit	F5=Refresh	F6=Add
F8=Browse	F12=Cancel	F17=Audit Stamp	F7=Review

Option 3 Work With Filters

Filters allow you to specify the selection criteria used to limit the data shown on the Object Authority by Object report and thresholds for sending alerts to PSDetect.

AARP50-01

7/30/08
10:24:35

Work with Filters

2=Update 3=Copy 4=Delete 6=Change Alert/Desc

Opt Report **All Filters**

ID	Filter Name	Description	File Name
AAOBJAUTO	DEFAULT	Object Authority by Object	AAOBJAUT

F3=Exit F6=Add New Filter F8=Limit View to DEFAULT F12=Return

Option 2 = Update - To update an existing filter definition, type 2 in the **Opt** field of the filter you want to update and build the filter query definition. To build the filter query definition, select the necessary fields (F4) and specify the necessary criteria. To see all available operation codes, press **F10** (Display Op Codes).

Option 3 = Copy - To copy an existing filter description, type 3 in the **Opt** field of the filter. This option displays the Filter/Threshold Definition screen. The screen displays all the definitions of the filter being copied except the name of the filter.

Option 4 = Delete - To delete an existing filter, type 4 in the **Opt** field of the filter you want to delete.

Option 6 = Change Alert/Desc - To change an existing filters description or alert information, type 6 in the **Opt** field of the filter you want to modify.

F6 = Add new filter - To create a new filter, press F6 (Add New Filter) from the Work with Filters screen and enter the following:

Filter name:	Name of filter (up to 10 characters)
Description:	Filter description (up to 30 characters)
Action:	The action that performs when the threshold is exceeded. You can send an alert to PSDetect or produce a report.
Threshold:	The maximum number of applicable events that occur before the specified action occurs
Message:	The message text to use for the specified action

F8 = Limit View to Default/View All - Toggles the display between showing only the default filters or all defined filters.

Option 10 Non-Comp Report/Force Compliance

The start OAM (STROAMAPI) command lets you force objects to comply to a template or to find out which objects do not comply to a specified template using one step.

Start OAM (STROAMAPI)		
Type choices, press Enter.		
Template	CASAUTHOBJ	Name CASAUTHOBJ...
Library Name	CASAJ	Name, Group, Generic*
	+ for more values	
	CASAJ03	
Object Name	*ALL	Name, Group, Generic*, *ALL
	+ for more values	
	AACLCHM	
Object Type	*ALL	Name, Group, *ALL
	+ for more values	
	*FILE	
Object Attribute	*ALL	Name, Group, *ALL
	+ for more values	
	CLP	
<div style="text-align: right;">Bottom</div> <div> F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel F13=How to use this display F24=More keys Parameter TEMPLATE required. </div> <div style="text-align: right;">+</div>		

Template - The name of the template the objects force to comply to, or objects that compare to for non-compliance.

Library Name - The valid values for this parameter are:

- **Name** - The library name(s) containing the objects.
- **Group** - The group(s) containing the libraries containing the objects.
- **Generic*** - A generic value for a group of libraries.

Object Name - The valid values for this parameter are:

- **Name** - The object name(s).
- **Group** - The group(s) containing the object names.

- **Generic*** - A generic value for a group of objects.
- ***ALL** - All objects in a specified field.

Object Type - The valid values for this parameter are:

- **Name** - The object type(s).
- **Group** - The group(s) containing the object types..
- ***ALL** - All object types in the specified library.

Object Attribute - The valid values for this parameter are:

- **Name** - The object name(s).
- **Group** - The group(s) containing the object attributes.
- ***ALL** - All object attributes in a specified library.

Filter Name - The valid values for this parameter are:

- **Name** - The filter name.
- **DEFAULT** - The default filter.

Audit - The valid values for this parameter are:

- ***YES** - Produces a Non-Compliance Report.
- ***NO** - Does not produce a Non-Compliance Report.

Compliance Flag - The valid values for this parameter are:

- ***YES** - Forces specified object(s) to comply to the specified template.
- ***NO** - Does not force specified object(s) to comply to the template.

Run Interactively - The valid values for this parameter are:

- ***YES** - The STROAMAPI command runs interactively.
- ***NO** - The STROAMAPI command runs in batch.

Option 11 Work With Non-Compliant Objects

Lets you view and/or change all non-compliant objects. Non-compliant objects do not meet the requirements of an authority template.

```

Work With Objects Out of Compliance

Library . . . . . *ALL          Position to . . . . . 
                                Position to type . . . . . 
Type options, press Enter.
 2=Edit authorities  3=Change object owner
 5=Show non-compliance reasons  7=Change to comply

Opt Library   Object      Type  Attribute  Description
-  PMBT       QDIALOCAL  *CLS              Class for QDIALOCAL Job
-  PMBT       QSPL4      *CLS              Spooling Subsystem Class for R
-  PMBT       DDRPTA     *CMD              Journalled Data Report - Access
-  PMBT       PSCHGUSRPR *CMD              Change User Profile as per tem
-  PMBT       PSCRTUSRPR *CMD              Create User Profile as per tem
-  PMBT       PSPFTFTR  *CMD              Transfer PSPTF objects to cent
-  PMBT       STRRRM     *CMD              Display Remote Request Managem
-  PMBT       C##CP2100R *FILE  PF          PSA U5.1 (c) 1998 PentaSafe PS
-  PMBT       CLSPSA     *FILE  SAUF          More...
-  PMBT       CURMDV     *FILE  PF
-  PMBT       EX1        *FILE  PF

F3=Exit  F6=Bring all to compliance  F12=Cancel  F17=Top  F18=Bottom

```

Options

2= Edit authorities - The Edit Object Authority display shows a list of current users authorized to an object and the authority levels assigned. You can add or remove users from the list, as well as change their authority levels.

Note

Caution should be used when changing the public authority on IBM-supplied objects. For example, changing the public authority on the QSYSOPR message queue to be more restrictive than *CHANGE, will cause some system programs to fail. The system programs will not have enough authority to send messages to the QSYSOPR message queue. For more information, refer to the Security - Reference book, SC41-3302.

3= Change object owner - Lets you specify a new owner for an object.

Note

Changing object ownership may cause the ownership recipient's user profile object to exceed its maximum size.

5 = Show non-compliance reasons - Use this option to show why the object is not in compliance.

7 = Change to comply - Lets you set the object's authorities to the authorities of the template. The object must not be in use.

Function Key

The following function key are available from this screen:

F6 = Bring all to compliance - Lets you set all the authorities of listed objects to the authorities of the template. The objects must not be in use.

Note

After all objects are brought into compliance, the generated output authority file must be generated again.

Creating a New Authority Template

To create a new authority template:

1. Identify the application to create a new authority template for. The libraries associated with the chosen application must be known.
2. Define the required authority for the chosen application.
 - Which User Profile will own the objects.
 - Which users will have access and how much access.
3. Use Option 1 (Work with Templates) to work with authority templates.

4. Press F6 (Create New Template) to create a new authority template.
 - Specify the name and description of the new template. It is recommended to use a name that describes the application the template is used for.
 - Specify the User Profile that will own the objects. The owner will have *ALL authority to the objects in the application. The owner should not be the same as the users that use the application since this would give the users all authority.
5. Press F8 (Edit Authorities) to define the specific authorities for the application. It is recommended that users have *USE authority and *PUBLIC have *EXCLUDE authority. This will help secure the application from unknown users.
6. Press ENTER twice and F3 to save the authorities and return to the Object Authority Management menu.
7. Use Option 3 (Generate Authority File) to generate the authority information for the application.
8. In the PSAudit Submittal Window enter the following:
 - Library or group of libraries (generically or by using *USRLIBL) of the application.

Notes

- You can exclude an object with the Filtering feature of PSAudit.
 - This job should be run after hours at a time when there is very little or no other activity. The job will also produce a report of objects contained in the output file. Review this report and if there are any objects which you do not want included, create a filter to exclude them and regenerate the output file.
-
- Output file name. This file will be used to audit and bring objects into compliance. It is recommended that you put your output files into a separate library and give them the same name as the template.

Once this job is completed the application can be audited.

To audit objects and bring them into compliance:

1. Use Option 1 (Work with Authority Templates) and Option 5 (Use(Report/Comply)) on the new template and enter the following:
 - Name of the output file created in step 8 above
 - Comply flag (“Y” to force objects into compliance or “N” to just audit the objects)
 - JOBQ for the job.

Note

If this is a compliance job (Comply flag = Y), all objects in the output file created in step 8 above will be changed with the authorities specified in the authority template. The objects must not be in use when the job is run. The job should be run after hours at a time when there is very little or no other activity.

2. If this is an audit job (Comply flag = N) information will be written to a file used by Option 2 (View/Change Non-Compliant Objects).
 - Option 2 (View/Change Non-Compliant Objects) can now be used to view any objects that do not comply.
 - Periodically repeat steps 7 through 9 to audit the application.

Option 20 Generate Authority File (PS Audit)

Lets you generate an output file containing authority information. This option is only available if you are authorized to NetIQ Security Solution for iSeries - PSAudit.

PS4		NetIQ Corporation		Date: 7/30/08	
		Object Author		PSAudit Submittal Window	
Select one of the following:					
1	Work With Templates				
2	Work With Groups				
3	Work With Filters				
10	Non-Comp Report/Force Compl				
11	Work With Non-Compliant Obj				
20	Generate Authority File (PS				
Enter Option or Function/Type					
F1=Help	F3=Exit				
F12=Previous	F13=Attention				

Object Authority by Object	
ALL/Gen/*USRLIBL/Lib	<u>QGPL</u>
Filter name.	<u>DEFAULT</u>
Output file, *NONE . .	<u>*NONE</u>
Library	<u></u>
*Replace *Add records.	<u>*REPLACE</u>
Run interactively. . .	<u>*NO</u> (*YES-*NO)
OUTQ	<u>QPRINT</u>
JOBQ	<u>QBATCH</u>
Hold on job queue . .	<u>*NO</u> (*YES-*NO)
Enter=Submit F3=Exit F7=Schedule F9=Filter	

Select Option 3 from the menu. The PSAudit Submittal Window appears and will prompt you for a library name. Following are permissible values:

- | | |
|----------|--|
| *ALL | All the libraries in the system, including QSYS are searched. |
| Gen* | The generic library name of the libraries that are searched. A generic name is a character string of one or more characters followed by an asterisk (*). |
| *USRLIBL | Only the libraries listed in the user portion of the job's library list are searched. |
| Lib | The name of the library to be searched. |

Filter name - Specify a report filter name (F9 to define filters).

Output file, *NONE - Output file data that is printed on the report. The file will be created in the specified library if it does not exist. You may run your own queries against files created using this prompt.

***Replace *Add records** - Records will be replaced or added in the output file.

Run interactively - The report will be run interactively or submitted to batch. Specify *NO to submit the job to batch or *YES to run interactively (online).

Note

Some reports may run a long time.

OUTQ - The name of the output queue to route the report to. The output queue should be secured to protect the sensitive nature of some reports.

JOBQ - The name of the job queue to where jobs are submitted when the “Run interactively” field specifies *NO.

Hold on job queue - Specify *NO to submit immediately or *YES to submit and hold the job, which must be released so that it may become active.

Note

For detailed information on standard prompts, refer to “Submittal Window Prompts” in the User Guide for *NetIQ Security Solutions for iSeries - PSAudit*.

Function Keys

The following function keys are available from this screen:

Enter=Submit - Processes requested options (if any). If no options are selected, program is ended.

F3=Exit - Ends the current task and returns to the display from which the task was started. Any information not sent to the system is lost.

F7=Schedule - Displays the “Update ROBOT in Batch (RBTBCHUPD)” panel, where you can schedule batch jobs by adding an entry to the job schedule. A batch job can be submitted once or scheduled to be submitted at regular intervals. You can schedule a report to run daily, weekly or monthly.

F9=Filter - Displays the “Work With Filters” panel, where you can select or add a query filter.

Note

For more information on query filters, refer to the section titled “Working With Filters” in the *User Guide for NetIQ Security Solutions for iSeries - PSAudit*.

Chapter 5

Inactive Session Monitor

Introduction

The Inactive Session Monitor (ISM) is designed to help you effectively handle the physical security of your inactive workstations. The iSeries does an adequate job of protecting your workstations before they are signed on. However, after a user has signed on, there is little the system can do to prevent unauthorized access to your data. For example, after signing on in the morning, users can spend their time entering and adjusting the payroll for the following day. If the users do not sign off at lunch time, the workstations are left signed on and unattended for the next 60 minutes. Such instances when workstations are signed on and unattended present security lapses, and they can happen anytime during the day for any application. EDP auditors are looking more closely at this break in physical security.

ISM can help with the following:

- Secure workstation from unauthorized use.
- Improve availability of communication lines.
- Reduce phone charges by ending inactive dial-up sessions.
- Decrease software license cost of concurrent users by ending inactive users.

Function

Inactive Session Monitor periodically checks the status of all of the interactive jobs on your system. In particular, it looks for jobs that are waiting for user input. When it detects one of these jobs, the Inactive Session Monitor determines how long the job has been waiting. If the wait period exceeds the time limit set by you, the offending job is signed off, disconnected, or held.

Inactive Session Monitor provides you with a full range of options to tailor the application to your specific needs via an easy-to-use menu. Functions on the menu include starting and stopping Inactive Session Monitor, entering your exclusions, changing the system parameters and submitting a report of the jobs signed off.

Tailoring specific options of the product means that you can exclude workstations, user profiles, or even programs from being signed off by Inactive Session Monitor. You can also set the inactive time limit for individual workstations and user profiles.

Inactive Session Monitor supports special environments:

- TCP/IP Sessions
- Pass-Through to other machines
- 3270 Emulation
- MAPICS Software
- CMAS Software
- Group Jobs
- Remote Users
- System Request Jobs
- Disconnects ANY Type of Job

Inactive Session Monitor is flexible:

- Exclude specific programs from being signed off
- Set special time limits by workstation

- Set special time limits by user
- Send your user a warning message before being signed-off

Main Menu

The Main Menu contains all of the options you can use to operate Inactive Session Monitor.

Display the Menu

Any time you execute the command ASO in PSSECURE, the Inactive Session Monitor Main Menu will appear.

```

PS5                      PentaSafe Security Technologies, Inc ANYUSER      Date:  9/18/08
                          Inactive Session Monitor           QPADEV000B  Time: 14:40:15

Select one of the following:

1  Start Inactive Session Monitor
2  Stop Inactive Session Monitor
3  Change Workstation Exclusions
4  Change User Profile Exclusions
5  Display/Change Program Exclusions
6  Display/Change System Parameters
7  Timeout Log Report
8  Dflts & Info for PS DSCJOB/SIGNOFF
9  Change Controller Exclusions
10 Display ISM Statistics
11 Work With ZASBS Subsystem Jobs

Enter Option or Function/Type ==>

F1=Help      F3=Exit      F6=Messages  F9=Window    F10=Cmd Line
F12=Previous F13=Attention F14=Batch Jobs F18=Reports

```

Option 1 Start Inactive Session Monitor

Starts a subsystem called ZASBS. Inactive Session Monitor is an autostart job in the subsystem description.

Enter desired exclusions before starting Inactive Session Monitor. You can automatically start Inactive Session Monitor with your existing startup routine by adding the following command:

```
STRSBS PSSECURE/ZASBS
```

Note

If the job queue ASJQ01 is held, ISM cannot terminate inactive jobs, and the job queue could quickly accumulate hundreds or thousands of entries.

Each time the subsystem is started, ISM message queues (PSSECURE/Z*) created by program ASPGM are deleted.

Note

If program ASPGM is called from users' initial programs and the ISM subsystem, ZASBS, is not active, then message queues will still be created for users when they sign on, but will not be deleted because ISM is not active. If you encounter this situation, you can schedule a job to run periodically to delete these message queues. The job should run the command DLTMSGQ PSSECURE/Z*.

Option 2 Stop Inactive Session Monitor

Terminates the subsystem Inactive Session Monitor is running in. You can add this function to your existing shut down routine by adding the following command:

```
ENDSBS ZASBS
```

You should end subsystem ZASBS prior to backups if you intend to backup library PSSECURE.

Option 3 Change Workstation Exclusions

The Display/Change Workstation Exclusions function (Option 3) lets you change the inactive time limit for workstations or lets you prevent workstations from timing out. If the workstation and the user profile signed on to the workstation have exceptions, Inactive Session Monitor uses either the greater time limit or the total exclusion.

You can change workstation exclusions while Inactive Session Monitor is running. The changes will take effect the next time Inactive Session Monitor performs its periodic check.

ASRP2110:22:06 9/18/08

Display/Change Workstation ExclusionsSystem: ANYSERVER

Enter The Workstations to be excluded from PSSecure/ISM

** O R ** Enter the Workstation and overrides for Time Limit and End of Job

** O R ** Enter a Line Description for PC Support or Remote Jobs

WORKSTATION	TIME LIMIT (min)	SIGN-OFF Options		Vary Off
Name or GEN*	Zero for Never	(E D H S P T)	(A G J)	(Y N)
DSP01	90			
DSP11	30	E	A	Y
PAY*	2	E	A	
PGMR*	0			
Q*	0			
SHOPFLOOR1	2	E	G	
	0			
	0			
	0			
	0			
	0			
	0			+
ISM Defaults--->		30 min	P	J
				N

F3=Exit F6=Devices F9=Timing

Workstation

The specific name of a workstation or the generic name of several workstations to be excluded from the general default parameters specified on the Display/Change System Parameters screen (Option 6).

If you want to add a workstation to the exclusions, move the cursor to the next available line in the **WORKSTATION** column and enter the workstation (device) name. You can add a generic workstation exclusion by placing an asterisk (*) after the prefix of a generic name in the **WORKSTATION** column. This action will exclude all workstations that begin with the prefix that you specify.

Note

APC description names may be entered here, so that Inactive Session Monitor can determine the names of workstations on that line.

To remove a workstation from the exclusions, delete the workstation name from the **WORKSTATION** column.

Time Limit

The number of minutes that a workstation can remain inactive before it times out. Unless you specify a different time limit, this field uses the system parameter default values. To change the inactive time limit for a workstation, specify a new value in the **TIME LIMIT** column. Inactive Session Monitor will use this value to determine the inactive state of the job.

To prevent a workstation from timing out using the default inactive time limit, set the **TIME LIMIT** value to 0.

SIGN-OFF Options (E D H S P T)

When the time out interval is exceeded, the following sign-off options determine how the user's session is ended. ISM functionality is only supported for MAPICS when the **Sign-off options** field is set to 'E' (End Job), 'P' (Disconnect Job), or 'S' (Signoff).

For more information about these sign-off options, see the appropriate IBM manuals.

- E** Ends the job immediately using the iSeries ENDJOB command. The user will not have the opportunity to finish the current function. All record locks will be released and the job will no longer be active on the system. The user will have to sign on again to enter the application.
- D** Disconnects the job. This will not end the job, but will simply overlay a sign-on screen over the current job using the iSeries DSCJOB command. After signing on to the system again, the user will be connected from the job currently running. This option is highly secure, but does not help system performance or release record locks.
- H** Holds the current job using the iSeries HLDJOB command. This will prevent the current job from continuing to process. To continue processing, the held job must be released from another workstation. When released, the held job behaves like a job that is reconnected after having been disconnected. The session will resume processing where it stopped when it was held. When a held job is released, record locks are not released because the job is still active. This option is highly secure, but does not help system performance or release any record locks. If the security administrator wants to prevent the user from continuing to work without intervention, this method is effective.
- S** The job is signed off using the iSeries sign-off command. This feature requires special setup. For more information, see “Option 8 Dflts & Info for PS DSCJOB/SIGNOFF” on page 305.
- P** The job is disconnected using the NetIQ Security Solutions for iSeries Disconnect feature. The Disconnect Job will disconnect any interactive job. This feature requires special setup. For more information, see “Option 8 Dflts & Info for PS DSCJOB/SIGNOFF” on page 305.
- T** The job is issued an End Pass-Through (ENDPASTHR) command. If the job is not passed through from another machine, it will not be affected. For more information, see “Option 8 Dflts & Info for PS DSCJOB/SIGNOFF” on page 305.

Note

If your Sign-off option is set to S, P, or T, a notification is sent to the QSYSOPR message queue if a job cannot be disconnected due to the job not calling ASPGM. To change the message queue receiving these notifications, see “System Parameters Outside Of Inactive Session Monitor” on page 301.

SIGN-OFF Options (A G J)

The following additional options are available when the ENDJOB command (Option E) is used:

- A** All jobs running on the workstation including System Request jobs.
- G** All group jobs associated with the current job.
- J** Ends the current job only.

Vary Off

Whether you want to vary off the workstation after ENDJOB has executed. When a workstation is varied off, the workstation is not usable until it has been varied on from another workstation.

- Y** Vary off the workstation
- N** Do not vary off the workstation

ISM Defaults

The current defaults are displayed in the lower right portion of the screen. If you want to change the defaults, use Option 6 from the Inactive Session Monitor Main Menu.

Function Keys

The following function keys are available from this screen:

F3=Exit - Cancels the current operation and returns to previous screen.

F6=Devices - Displays a scrollable pop-up window with a list of available workstations.

F9=Timing - Allows entry of time variations for the workstation jobs, a feature that is especially helpful for iSeries installations that are spread over different time zones. Exclusions and custom exit programs can also be specified here to be processed at different times for each day of the week. Workstation jobs can also be ended immediately at different times for each day of the week.

Note

ISM timing entries made using **F8** (Maintain ISM timing) from ISM Main Menu Option 6 (Display/Change System Parameters) will supersede timing entries made using **F9** (Timing) from ISM Main Menu Options 3 (Display/Change Workstation Exclusions) and 4 (Display/Change User Profile Exclusions).

Examples

The following examples demonstrate how exclusions can be used to control inactive sessions.

- DSP01 will time out in 90 minutes, instead of 30 minutes (as specified by the default parameters). The job will be disconnected using the Disconnect Job function. Only the current job will be disconnected, and the workstation will not be varied off.
- DSP11 will time out in 30 minutes and will be cancelled with the ENDJOB command. All jobs (including system request jobs) will also be ended. The workstation will be varied off.
- All workstations that begin with PAY* will time out in 2 minutes and will be cancelled with the ENDJOB command. All workstation jobs (including system request jobs) will also be ended. The workstation will not be varied off.
- All workstations that begin with PGMR* will not time out.
- All workstations that begin with Q* will not time out.
- Workstation SHOPFLOOR1 will time out in 2 minutes and will be cancelled with the ENDJOB command, in addition to all group jobs associated with the job. The workstation will not be varied off.

Option 4 Display/Change User Profile Exclusions

Option 4 from the Main Menu allows you to exclude one or more users from being timed out and to change the inactive time for one or more users. If both the workstation and the user profile signed on to it have exclusions, Inactive Session Monitor uses either the greater time limit or the total exclusion.

You can change user exclusions while Inactive Session Monitor is running. Your changes are reflected the next time Inactive Session Monitor performs its periodic check.

```
ASRP22                Display/Change User Profile Exclusions    08:52:04    9/21/08
                                System: ANYSERVER

Enter The User Profiles to be excluded from PSSecure/ISM
** O R **   Enter the User Profile and overrides for Time Limit and End of Job

USER PROFILE      GRP PROF      TIME LIMIT (min)          SIGN-OFF Options        Vary Off
Name or GEN*      (X)           Zero for Never         (E D H S P T) (A G J)  (Y N)

Jim               0
John              1             P
Lisa              5             E             A             Y
Leslie            30            S
QSECOFR           2
QSYSOPR           X             0
                  0
                  0
                  0
                  0
                  0
                  +

ISM Defaults--->    30 min             P             J             N

F3=Exit           F6=Users           F9=Timing
```

USER PROFILE

The specific name of a user profile or the generic name of several user profiles to be excluded from the general default parameters specified on the Display/Change System Parameters screen (Option 6).

If you want to add a user profile to the exclusions, move the cursor to the next available line in the USER PROFILE column and enter the user profile name.

You can add a generic workstation exclusion by placing an asterisk (*) after the prefix of a generic name in the WORKSTATION column. This action will exclude all workstations that begin with the prefix that you specify.

If you want to remove a user profile from the exclusions, delete the user profile name from the USER PROFILE column.

GRP PROF

You can set up group exclusions by specifying **X** under the GRP PROF column. Some shops put their users under group profiles. Group profiles make it easier to administer authority. It will be easier to specify one group profile for twenty users if they are all to be handled the same way. Inactive Session Monitor will give all of the users under that group profile the same parameters as the group profile.

Time Limit

The number of minutes that a user can remain inactive before the session times out. Unless you specify a different time limit, this field uses the system parameter default values. To change the inactive time limit for a user, specify a new value in the TIME LIMIT column. Inactive Session Monitor will use this value to determine the inactive state of the job.

To prevent a workstation from timing out using the default inactive time limit, set the TIME LIMIT value to 0.

SIGN-OFF Options (E D H S P T)

When the time out interval is exceeded, these sign-off options determine how the user's session is ended. For detailed description of available options, see "SIGN-OFF Options (E D H S P T)" on page 284.

Note

If your Sign-off option is set to S, P, or T, a notification is sent to the QSYSOPR message queue if a job cannot be disconnected due to the job not calling ASPGM. To change the message queue receiving these notifications, see "System Parameters Outside Of Inactive Session Monitor" on page 301.

SIGN-OFF Options (A G J)

Options A, G, and J are available when the ENDJOB option is specified. For detailed description of available options, see “SIGN-OFF Options (A G J)” on page 286 for detailed descriptions.

Vary Off

Whether you want to vary off the workstation after ENDJOB has executed. When a workstation is varied off, the workstation is not usable until it has been varied on from another workstation.

- Y** Vary off the workstation
- N** Do not vary off the workstation

ISM Defaults

The current defaults are displayed in the lower right portion of the screen. If you want to change the defaults, use Option 6 from the Inactive Session Monitor Main Menu.

Function Keys

The following function keys are available from this screen:

F3=Exit - Cancels the current operation and returns to previous screen.

F6=Users - Displays a scrollable pop-up window with a list of available user profiles.

F9=Timing - Allows entry of time variations for the user jobs, a feature that is especially helpful for iSeries installations that are spread over different time zones. Exclusions and custom exit programs can also be specified here to be processed at different times for each day of the week. User jobs can also be ended immediately at different times for each day of the week.

Note

ISM Timing entries made using **F8** (Maintain ISM Timing) from ISM Main Menu Option 6 (Display/Change System Parameters) will supersede timing entries made using **F9** (Timing) from ISM Main Menu Options 3 (Display/Change Workstation Exclusions) and 4 (Display/Change User Profile Exclusions).

Example

The following examples demonstrate how exclusions can be used to control inactive sessions.

- JIM will not time out.
- JMS will time out in 1 minute and will be disconnected with the NetIQ Security Solutions for iSeries Disconnect feature.
- KEITH will time out in 5 minutes (instead of 120 minutes) and will be cancelled with the ENDJOB command. All jobs including system request jobs will also be ended. The workstation will be varied off.
- MICHELLE will time out in 30 minutes and will be cancelled with the SIGNOFF command.
- The QSYSOPR and all users under the QSYSOPR group profile will not time out. All of the other users on the system will time out in 120 minutes.
- The QSECOFR will time out in 2 minutes and will be disconnected using the Disconnect feature.

Option 5 Display/Change Program Exclusions

Option 5 from the Main Menu allows you to exclude an interactive job running a particular program from being timed out. Enter the program name in the program exclusion list. The program can be anywhere in the job's invocation stack and still be excluded.

You can change program exclusions while Inactive Session Monitor is running. Your changes are reflected the next time Inactive Session Monitor performs its periodic check.

Program exclusions are checked after user and workstation exclusions and only after a job has qualified for termination.

```

ASRP23                Inactive Session Monitor/ISM          15:03:02    9/18/08
                      Display/Change Program Exclusions      System:    ANYSERVER

Enter the programs to be excluded from PSSecure/ISM:

  Program
  XX12TEST

+

F3=Exit

```

After making changes or additions, press **Enter** before leaving this screen.

Program

To add a program to the exclusions, move the cursor to the next available line in the PROGRAM column and enter the program name. To remove a program from the exclusions list, delete the program name.

Note

To exclude from termination users who are performing 3270 emulation, add program QEM3270 to the program exclusions list.

Function Key

F3=Exit - Cancels the current operation and returns to previous screen.

Option 6 Display/Change System Parameters

Inactive Session Monitor requires two values to work correctly: the default Time Limit and the Check Gap. Although both of these values are pre-set, you can change them at any time to meet your specific needs.

You can change the time limit while Inactive Session Monitor is running. Your changes are reflected the next time Inactive Session Monitor performs its periodic check.

Option 6 from the Main Menu enables you to establish the sign-off requirements for your installation.

ASCL20	Display/Change System Parameters	14:02:07	4/04/08
		System:	ANYSYSTEM
ISM Time limit:	<u>30</u>	(Minutes)	
ISM Check gap:	<u>30</u>	(Seconds)	
Maximum joblog entries:	<u>100</u>	(Integer or *NOMAX)	
Passthru used:	<u>*YES</u>	(*YES *NO)	
3270 Emulation used:	<u>*YES</u>	(*YES *NO)	
Send warning message:	<u>*NO</u>	(*YES *NO)	
Delay of sign-off:	<u>0</u>	(Seconds)	
Monitor system request jobs:	<u>*YES</u>	(*YES *NO)	
Monitor group jobs individually:	<u>*YES</u>	(*YES *NO)	
Monitor line descriptions for PCs:	<u>*NO</u>	(*YES *NO)	
Sign-off options:	<u>P</u>	(E-ENDJOB D-DSCJOB H-HLDJOB)	
(S, P and T have special requirements)		(S-SIGNOFF P-Penta's DSCJOB)	
		(T-ENDPASTHR)	
Additional ENDJOB options:	<u>J</u>	(A-All G-Group J-Job Only)	
Vary off the terminal after ENDJOB:	<u>*NO</u>	(*YES *NO)	
Subsystems to monitor:	<u>*ALL</u>		
F3=Exit	F7=Subsystems	F8=Maintain ISM timing	F10=Maintain ISM messages

ISM Time limit -The number of minutes a workstation or user is allowed to be inactive before Inactive Session Monitor times it out. We have set this value at 30 minutes. You can change this value to any whole number from 1 to 999. System value QINACTITV must be changed to “*NONE” or a value greater than that specified for “ISM Time Limit”.

ISM Check gap - The check gap refers to how often Inactive Session Monitor checks the job for inactivity. The check gap is recorded in seconds. We have set this value at 180 seconds. This means every 180 seconds Inactive Session Monitor “wakes up” and checks the status of the interactive jobs. You can change this value to any whole number from 1 to 999.

Although Inactive Session Monitor uses very little overhead and has a relatively low job priority, you must be realistic in setting this check gap. We have set the value at what we have found to be the optimum time period. However, depending on what you feel is an acceptable variance, you can adjust the value up or down accordingly.

Maximum joblog entries - You can select the number of log entries to be placed in the joblog of the signed off jobs. This allows you to have a more complete joblog on the jobs signed off by Inactive Session Monitor. Keep in mind, however, that the number of log entries you have in the job log have a direct impact on the length of time it takes to sign-off a job.

Passthru used - If you use machine-to-machine communication via SNADS, specify *YES for this value.

3270 Emulation Used - If you use 3270 Emulation, specify *YES for this value.

Send warning message - Specifying *YES here activates the option to send the user a warning message to avoid being signed off. An inquiry message will be sent to the inactive workstation. Inactive Session Monitor will wait a certain number of seconds for a response. This number of seconds is the value entered in “Delay of Sign-Off” field. Specifying *NO in this field will not give the user of the inactive workstation an opportunity to avert being signed off after the inactive time limit is reached. When the user receives the warning message, the user will need to type a letter and press **Enter**.

Delay of Sign-Off - The number of seconds Inactive Session Monitor will wait for a response from a user before signing off when a message is sent to warn user of impending sign-off.

Monitor system request jobs - To monitor system request jobs, specify *YES for this value. With this setting, a system request job will be processed as an inactive job. The same rules apply in determining the inactive time limit and when it has been reached.

Monitor group jobs individually - Inactive Session Monitor will process group jobs individually if you specify *YES for this value and will sign off each group job that exceeds the ISM time limit. The default value *NO causes ISM to look at the currently active group job (that is, not suspended) for inactivity. If the currently active group job has not registered any interactive transactions, all groups under this job will also be terminated.

Monitor line descriptions for PCs - To monitor line descriptions for PC's, set this to *YES and press **Enter** to save the defaults. This feature will activate Inactive Session Monitor to look for a line description in the Workstation Exclusion file.

Sign-off options - When the time out condition has been exceeded, the user can be canceled in a number of ways. See “SIGN-OFF Options (E D H S P T)” on page 284 for a description of each option. ISM functionality is only supported for MAPICS when the Sign-off options field is set to ‘E’ (End Job), ‘P’ (Disconnect Job), or ‘S’ (Signoff).

Additional ENDJOB options - Options A, G, and J, are available when the ENDJOB option is specified. See “SIGN-OFF Options (A G J)” on page 286 for a detailed description.

Vary off the terminal after ENDJOB

Vary off the workstation after ENDJOB. When a workstation is varied off, the workstation is not usable until it has been varied on from another workstation. This does not affect devices on line descriptions for PC’s.

Y Vary off the workstation.

N Do not vary off the workstation.

The Vary Off function is performed only if the “ENDJOB Options” value is “A” for all.

Subsystems to monitor - Displays the first 5 names of subsystems that are specified to be monitored for interactive jobs by Inactive Session Monitor. To display or edit the list of subsystems, press **F7**. This action displays a pop-up entry field that lists all specified subsystems and lets you maintain the list. *ALL is the default value. Do not monitor subsystem QSPL for PC printer sessions.

Function Keys

The following function keys are available from this screen:

F3=Exit - Cancels the current operation and returns to previous screen.

F7=Subsystems - Displays a pop-up entry field that lists the names of subsystems to be monitored and lets you maintain the list. You can specify 1-100 subsystem names that Inactive Session Monitor will monitor for interactive jobs. *ALL is the default value. See “Maintain Subsystem List” on page 297.

F8=Maintain ISM timing - Allows granularity of job termination specifications. For additional information refer to the section titled “Maintain Inactive Session Monitor Timing” on page 298 in this section.

Note

ISM Timing entries made using F8 (Maintain ISM Timing) from ISM Main Menu Option 6 (Display/Change System Parameters) will supersede timing entries made using F9 (Timing) from ISM Main Menu Options 3 (Display/Change Workstation Exclusions) and 4 (Display/Change User Profile Exclusions).

F10=Maintain ISM Messages - Allows you to select the messages sent by the Inactive Session Monitor to your users. For additional information, see “Maintain Inactive Session Monitor Messages” on page 300 in this section.

Maintain Subsystem List

The Maintain Subsystem List function (F7) lets you display or maintain the list of subsystems to be monitored. You can specify is 1-100 subsystem names that Inactive Session Monitor will monitor for interactive jobs. *ALL is the default value. After you have specified the subsystems to be monitored, press **Enter** to save (Update) the changes made or **F12** to cancel the changes.

ASCL20	Display/Change System Parameters	14:02:07	4/04/08
		System:	ANYSYSTEM
ISM Time limit:	<u>1</u>	(Minutes)	
ISM Check gap:	<u>30</u>	(Seconds)	
Maximum joblog entries:	<u>100</u>	(Integer or *NOMAX)	
Passthru used:	<u>*YES</u>	(*YES *NO)	
3270 Emulation used:	<u>*YES</u>	(*YES *NO)	
Send warning message:	<u>*NO</u>	(*YES *NO)	
Delay of sign-off:	<u>0</u>	(Seconds)	
Monitor system request jobs:	: Subsystem	:	
Monitor group jobs individually:	: *ALL	:	
Monitor line descriptions for PC:	: _____	:	
Sign-off options:	: _____	:	DJOB)
(S, P and T have special requ	: _____	:	JOB)
Additional ENDJOB options:	: _____	:)
Vary off the terminal after ENDJ	: _____	:	nly)
	: Enter=Update F12=Cancel	:	More... :
Subsystems to monitor: *ALL	: _____	:	_____
F3=Exit F7=Subsystems F8=Mai	:	:	ges

ISM Time limit - The number of minutes a workstation or user is allowed to be inactive before Inactive Session Monitor times it out. We have set this value at 30 minutes. You can change this value to any whole number from 1 to 999.

Maintain Inactive Session Monitor Timing

Description - To use the timing option (F8) from the Inactive Session Monitor System Parameters screen, simply use an “X” when you want to exclude Inactive Session Monitor from monitoring jobs. When an “I” is specified, these jobs will be ended immediately according to your ENDJOB parameters.

This function can be used prior to backup. This will end the user’s interactive job immediately, no matter what the user is doing.

ASCL20Maintain ISM Timing Parameters13:22:46 6/26/99

Enter an X for the time periods you DO NOT want ISM to monitor.
I for the time periods you want ISM to end jobs IMMEDIATELY
1-9 for your custom program (i.e. a 5 will execute ASCUST5)
(midnight) (noon)

M6amN6pm

Monday:

I

Hour Adjustment:

_0

(0-59)

Tuesday:

I

Enter 30 if you to process
at 6:30 instead of 6:00

Wednesday:

I

Thursday:

I

Friday:

I

Saturday:

Sunday:

M6amN6pm

Example day 1:

XXXXXXXXXXXX

ISM would only monitor jobs from 6pm to 6am. ISM would not
end any jobs during the regular business day.

Example day 2:

XXXXX

II

ISM would monitor jobs from 5am to midnight.
ISM would end jobs immediately from 7PM to 9PM.

Enter=UpdateF3=Exit

298 User Guide

Timing for Workstations and User Profiles

You also have the same option at the user profile or workstation level. You can specify certain workstations to be excluded at different times of the week. A prime example for this option is the iSeries shop that is spread across different time zones. This feature is available using **F9** from Workstation Exclusions Screens.

Note

The Timing exclude option will override the user and workstation options. For example, if you instruct Inactive Session Monitor not to monitor jobs during working hours, Inactive Session Monitor will not monitor any jobs during that time. But if Inactive Session Monitor is monitoring jobs during working hours, you can exclude certain times for users or workstations.

Hour Adjustment

This is used for adjusting the timing feature. For example, if you want to end jobs immediately at 6:15 PM on Friday; type **I** under the **6PM** column on the **Friday** line and then type **15** in the Hour Adjustment field to adjust 6 PM to 6:15 PM.

Custom Programs

Executed at each wake-up during the specified time block. When “I” is used, User Profile and Workstation exceptions are ignored and jobs are ended immediately. No parameters are passed to the custom programs.

Function Keys

The following function keys are available from this screen:

Enter=Update - Updates the Inactive Session Monitor with the changes made to the timing values.

F3=Exit - Cancels the current operation and returns to previous screen.

Maintain Inactive Session Monitor Messages

Description

This screen will allow you to select the messages your users receive from Inactive Session Monitor.

```
ASCL20                Inactive Session Monitor Message Options 09:05:55   9/21/08
                                System:  ANYSERVER

Yes - Continue to send the message.
No  - Do not send this message anymore.

Y/N      Message to be sent
===      =====
N . . . . DISCONTINUE OPERATIONS... PSSECURE/ISM is checking your
           job for program exclusions and will sign you off if...

Y . . . . You were signed-off due to exceeding your inactive time limit
Y . . . . You were disconnected due to exceeding your inactive time limit
Y . . . . Your job was held due to exceeding your inactive time limit

N . . . . Your job is running a program that cannot be cancelled.
           Please continue normal operations.

N . . . . PSSECURE/ISM is signing-off your job. Please discontinue
           operations until a signon display appears.
Y . . . . Your system request job was signed-off due to exceeding
           the inactivity time limit.
N . . . . This job cannot be disconnected at this time. This job...

Enter=Update                F3=Exit
```

Messages

Inactive Session Monitor sends various messages to users to inform them when they were signed off or if they are about to be signed off. You can eliminate some of those messages without recompiling any programs. By pressing F10 from the Inactive Session Monitor System Parameters screen, you will see the various messages, each with a Yes/No option. If you are receiving a message that you do not want to receive, simply change the “Y” to an “N”, and the message will not appear anymore.

System Parameters Outside Of Inactive Session Monitor

You can change certain Inactive Session Monitor system parameters by changing data area values directly. For example, if you want to change the Inactive Session Monitor Time Limit to 60 minutes, use the following command:

```
CHGDTAARA DTAARA(PSSecure/ASDA01 (1 3)) VALUE('060')
```

Similarly, if you want to change Inactive Session Monitor Check Gap to 300 seconds, use the following command:

```
CHGDTAARA DTAARA(PSSecure/ASDA02 (1 3)) VALUE('300')
```

The Change Data Area (CHGDTAARA) commands could be added to a job scheduler for execution at your discretion.

System Parameter	Data Area	Position	Length	Description
Inactive Session Monitor Time Limit	ASDA01	1	3	Minutes (use digits only)
Job Log Entries	ASDA01	10	6	LOGLMT; digits or *NOMAX
Sending Warning Message	ASDA01	20	1	Y/N
Delay of Sign-Off	ASDA01	21	3	Seconds (use digits only)
Monitor System Request Jobs	ASDA01	37	1	Y/N
Inactive Session Monitor Check Gap	ASDA02	1	3	Seconds (use digits only)
Sign-Off Options	ASDA02	10	1	E-ENDJOB D-DSCJOB H-HLDJOB

System Parameter	Data Area	Position	Length	Description
Additional ENDJOB Options	ASDA02	9	1	A-All Jobs
				G-All Group
				J-Job Only
Vary Off Terminal	ASDA02	4	1	Y/N
Message Queue for ASPGM warnings	ASDA06	1	10	Library where the message queue is located
	ASDA06	11	10	Message queue

WARNING: Do not use blanks where only digits are allowed.

Function Keys

The following function keys are available from this screen:

Enter=Update - Updates the Inactive Session Monitor with the selections made on the Message Options screen.

F3=Exit - Cancels the current operation and returns to previous screen.

F10=Cmd entry - Displays a command entry line at the bottom of the screen.

Option 7 Timeout Log Report

Option 7 from the Main Menu submits the Time Log Report. This report lists all of the users and workstations that have been timed out since the last Inactive Session Monitor was started. The report lists the information sorted by workstation and by user profile.

ASCL20	Inactive Session Monitor Report Prompt	08:30:44	9/21/08
Report options:		R	(R-On Request D-Print Daily)
Run time for daily report:		09	(Specify hour of day 00-23)
Selection criteria:			
User	:	*ALL	(*ALL for all users)
Date range	:	9/01/01 to 9/21/01	(MDY format)
Purge data after report is run . . .	:	N	(Y/N)
Outque for report	:	QPRINT	
If you want this report to run daily, specify 'D' for the Report Options. The report will run during the hour specified above.			
If you want to purge the data after the report is run, specify 'Y' in the Purge parameter above.			
If you want to run this report just on request, specify an R for Report Options and press Enter. The report will run immediately.			
If you specify Y for Purge Data, the data will be purged after the report has run.			
Enter=Run/Update		F3=Exit	

Report Options - Report Options determine whether the report will be processed on request or at a specified time.

R Run on Request. The report will be processed when you press **Enter**.

D The report will run daily during the hour specified. Enter the hour from 00 to 23.

Selection Criteria - Determines the report selection criteria for user and time ranges.

User: Enter *ALL to select all users, or enter the specific name of the user profile to be reported.

Date Range: Specify the date range in MDY format.

Purge Data - This flag determines whether the information will be deleted from the file after the report has been processed.

Y Purge the data after the report has been run.

N Do not purge the data.

OUTQ for Report - Specifies the name of the output queue where the printed report will be sent.

Function Keys

The following function keys are available from this screen:

Enter=Run/Update - Runs the Timeout Log Report if the Report Option is ‘R’ for “Run On Request” or updates the Report Options and Selection Criteria if Report Option is ‘D’ for “Print Daily”.

F3=Exit - Cancels the current operation and returns to previous screen.

Report Layout

A sample Timeout Log Report is as follows:

ASRP24	REPORT OF WORKSTATIONS THAT WERE CANCELLED BY PSSECURE/ISM					9/18/08 10:38:43
SELECTION CRITERIA:						
USER..... *ALL						
FROM DATE..... 9/01/01						
TO DATE..... 9/18/01						
WORK STATION	USER PROFILE	JOB NUMBER	DATE	TIME	LIMIT EXPIRED	
-----	-----	-----	-----	-----	-----	
DSP01	MAIL	236385	9/03/01	12:30:45	30 (MIN.)	
DSP01	MAIL	236693	9/04/01	12:32:21	30 (MIN.)	
DSP01	MAL	241185	9/07/01	18:24:01	30 (MIN.)	
QPADEV0001	JPK	241696	9/15/01	18:45:35	30 (MIN.)	
QPADEV0003	RSMIT	240841	9/01/01	18:42:13	30 (MIN.)	
QPADEV0007	BMARL	242657	9/14/01	18:32:01	30 (MIN.)	
ASRP24	REPORT OF USER PROFILES THAT WERE CANCELLED BY PSSECURE/ISM					9/18/01 10:38:43
SELECTION CRITERIA:						
USER..... *ALL						
FROM DATE..... 9/01/01						

IBM Mapics - Inactive Session Monitor (ISM) recognizes when MAPICS is installed on your iSeries and handles it accordingly. When an inactive job is terminated by ISM, it's record in the JOBACT file is deleted, so the system will not initiate a second session when the user signs on again. ISM functionality is only supported for MAPICS when the Sign-off options field is set to 'E' (End Job), 'P' (Disconnect Job), or 'S' (Signoff).

ISM will handle multiple environments of MAPICS/DB.

Option 8 Dflts & Info for PS DSCJOB/SIGNOFF

The iSeries Operating System cannot disconnect the following types of jobs when they are running:

- PC Support jobs using PC organizer or Text Assist
- Pass-Thru jobs
- Some Group jobs
- Server Group jobs
- Client Group jobs

In message file QCPIMSG, there are over ten messages explaining why a job cannot be disconnected. This leaves “audit holes” and frustrates DP managers when their audit is written up with these violations.

Inactive Session Monitor can disconnect or sign-off any type of interactive job on the iSeries.

Option 8 from the Main Menu allows the defaults for the Disconnect screen to be changed:

```

ASCL20                Inactive Session Monitor                13:55:39    6/26/99
                        Information & Defaults for PentaSafe's DSCJOB or SIGNOFF

1 Company name for the top of disconnect screen (40 characters):
      _____
      PentaSafe, Inc.

2 Informational message to display under the company name (70 characters):
      Your job has been Disconnected, enter your password to resume your job

3 Number of minutes after disconnect until job is ended:      180 (0 = Never)

To activate Penta's Disconnect Job, each user must execute the program
ASPGM from PSSECURE. This program will make this job eligible to be
Disconnected or Signed Off by PSSecure/ISM. Below is the code for your
initial program.

      CALL PSSECURE/ASPGM

If you have a user that does not have an initial program, you can
change the user profile to use ASPGM as the initial program.

      CHGUSRPRF USRPRF (user) INLPGM (PSSECURE/ASPGM)

Revoke authority from TFRSECJOB, TFRPASTHR & ENDRQS when disconnected: Y Y/N

Enter-Update                F3=Exit

```

Number 1 and 2 text lines are soft coded. You can modify this text for your company.

Number 3 is the time limit in minutes after disconnect until the job is ended. If Inactive Session Monitor disconnects a job, that job is still active on the system. The default value is 180 minutes. If a job has been disconnected for 180 minutes, Inactive Session Monitor will then end the job. The job will be ended immediately using the ENDJOB command. You can change this value from 1 minute to 999 minutes.

Revoke Authority - Specifies whether to revoke the users' authority to the following commands when the interactive job is suspended with the Disconnect screen:

- TFRSECJOB—Transfer to Secondary Job
- TFRPASTHR—Transfer Pass-Through
- ENDRQS – End Request

If you specify 'Y', the user's authority to the commands is revoked while the job is disconnected and the following conditions occur:

- The Disconnect screen cannot be terminated (cancelled) using the System Request menu option 2 (ENDRQS) to re-enter the suspended job without signing on again.
- The user cannot transfer to other jobs active on the same workstation (TFRSECJOB) that might not be disconnected or suspended (protected by Disconnect screen).
- The user cannot return to the source system (TFRPASTHR) where the pass-through job originated.

User authority to the commands is restored when the user signs on again through the Disconnect screen.

Note

Authority to the commands cannot be revoked from users who have *ALLOBJ Special Authority, so it is important for these users to ALWAYS sign off instead of allowing the session to time out.

Function Keys

The following function keys are available from this screen:

F3= Exit - Cancels the current operation and returns to previous screen.

Below is the Disconnect screen:

```
PentaSafe Security Technologies, Inc. 16:20:54 9/24/08
System: ANYSERVER

Your job has been Disconnected, enter your password to resume your job

User . . . . . ABC
Password . . . . . _____

F6=SIGNOFF      F8=ENDPASTHR      (c) 2001 PentaSafe Security Technologies, Inc.
```

The user can either enter his/her password to resume the job, or press **F6** to sign-off the terminal. After the password has been entered, the job will return to the screen and function where it was disconnected. If the user presses **F6** to sign-off, the job will sign-off normally. The NetIQ Security Solutions for iSeries sign-on screen for disconnected jobs can be invoked from a menu option which calls PSSECURE/ASCL61.

Function Keys

The following function keys are available from this screen:

F6=SIGNOFF - Performs a normal sign off for the disconnected job.

F8=ENDPASTHR - The pass-through session for the disconnected job is ended.

Setup

To use the Disconnect Job and Sign-Off feature, each interactive job must execute a special Inactive Session Monitor program. This code must be entered in the user's initial program or the user profile must be changed to make this program the initial program.

If you do not know what the initial program is for your users, simply display the user profile using the following command:

```
DSPUSRPRF USRPRF (user)
```

On the second page, you will see a value called "Initial Program". If your shop does not have the technical staff to modify this program, please call the NetIQ Corporation technical support staff.

Enter the following lines of code in your initial program:

- CALL PSSECURE/ASPGM
- MONMSG CPF0000

If the user does not have an initial program, you can change the user profile to execute ASGM using the following command:

```
CHGUSRPRF USRPRF (user) INLPGM(PSSECURE/ASPGM)
```

When this program is executed, it prepares the job to be disconnected or signed off by Inactive Session Monitor.

THIS PROGRAM (ASPGM) WILL NOT AFFECT OR CHANGE THE JOB.

Group Jobs Considerations

If your shop uses group jobs, the same code must be entered in the "initial group program" of your group job. When you execute TFRGRPJOB, the parameter INLGRPPGM contains the name of the program that executes when the user starts the group job. Since each group job has a unique job number, it is essential to modify this program, as well.

Group Jobs are ended only when the the Disconnect or the Signoff option is used.

PC Routers and Communication Jobs

Inactive Session Monitor also ends routers and communications jobs associated with interactive sessions.

The typical iSeries sessions now has several sessions associated with it, so it is not easy ending all the sessions associated with a job. It is not enough to just end the interactive session. If the PC router is still active, an intruder can access your iSeries data using your profile.

For remote jobs, the phone connection is still active until all of the associated sessions are ended. This causes three specific problems:

- An active router on a remote PC is a dangerous security breach.
- If the call is long distance, your company incurs additional phone expense.
- If the phone connection is still active, that phone line is not available for the next user.

Inactive Session Monitor can handle this problem for you. When Inactive Session Monitor detects an interactive job as inactive:

- Inactive Session Monitor will end the interactive session.
- Inactive Session Monitor will end all associated jobs under the controller of the interactive job.
- Inactive Session Monitor will vary off the controller which will drop the phone connection.
- Inactive Session Monitor will vary on the controller to prepare it for the next user.

All of the steps listed above can be modified to fit your environment. Since every shop is different, NetIQ Security Solutions for iSeries can setup Inactive Session Monitor to fit your specific environment.

Activate Line Description

To activate Inactive Session Monitor to monitor a line description:

1. Use the following command to display the Inactive Session Monitor Main Menu:
==>PSSECURE/ASO
2. Select Option 6 to modify the “System Parameters”.
3. In the middle of the screen is “Monitor Line Descriptions for PC’s”. Set this to *YES.
4. Press **Enter** to save the defaults. This feature activates Inactive Session Monitor to look for a line description in the Workstation Exclusion file.
5. Press **F3** to return to the Main Menu.
6. Select Option 3 for “Display/Change Workstation Exclusions”.
7. Enter the Line Description under the Workstation column you want to monitor, and the time limit you want to use, then press **Enter**.

Note

The line description must be entered here so that Inactive Session Monitor can determine the name of the controller associated with the job.

8. Press **F3** to return to the Main Menu.

At this point, you are ready to test. Set your default time in the System Parameters to 900. This will prevent Inactive Session Monitor from effecting anyone else on the system while you are testing.

SOURCE CODE: There is some source code provided with the software in PSSECURE/SOURCEAS. Please consult with Technical Support before making modifications.

Option 9 Display/Change Controller Exclusions

Option 9 from the Main Menu allows you to exclude an interactive job running under a particular controller from being timed out. Enter the controller name in the controller exclusion list. The controller name must be one attached to a line description specified in “Option 3 Change Workstation Exclusions” on page 283. Refer to this section for more information.

[illegible]

After making changes, press **Enter** prior to leaving this screen.

When Inactive Session Monitor monitors a line description and terminates users on that line description, it will also end the associated jobs under the controller (such as router jobs), unless the controller is found in the Controller Exclusions file. The time limit specified here pertains to the other jobs on the controller that are associated with a terminated interactive session. The associated jobs will not be ended if another interactive session has been established.

Controller - To add a controller to the exclusions, move the cursor to the next available line in the CONTROLLER column and enter the controller name. To remove a controller from the exclusions, delete the controller name and press **Enter**.

Function Key

The following function key is available from this screen:

F3=Exit - Cancels the current operation and returns to previous screen.

Option 10 Display ISM Statistics

Displays running counts for (a) the number of users that have been sent warning messages and (b) the number of users whose jobs have been jobs ended, held, or disconnected. The counts are reset using **F7**. The “total” line (the third line in the center of the screen) is a counter that cannot be reset.

```
ASCL20S                               Inactive Session Monitor          ANYSERVER
                                      Statistics                        9/19/08  15:17:16

0  warning messages sent since 12/04/00
0  users ended, held, or disconnected since 12/04/00
0  total users ended, held, or disconnected since  2/02/00

(c) PentaSafe Security Technologies, Inc. 2001
F3=Exit  F5=Refresh  F7=Reset counts
```

Function Keys

The following function keys are available from this screen:

F3=Exit - Cancels the current operation and returns to the previous screen.

F5=Refresh - Updates the running count of the number of users that have been sent a warning message, have been ended, held, or disconnected.

F7=Reset counts - Resets the running counts at the bottom of the screen, except for the “total” counter which cannot be reset.

Option 11 Work with ZASBS Subsystem Jobs

Shows the names and status information of jobs being processed by the Inactive Session Monitor subsystem, ZASBS. If the subsystem is active and one of the jobs shown is selected, additional information about that job can be displayed.

Testing

For a quick test of the Inactive Session Monitor product without affecting all of the users on your system:

1. Set the default time limit to 900 minutes.
2. Set a couple of workstations or users to 4 or 5 minutes. This will allow you to isolate a few users without affecting all of the users on the system.

For a quick test of the Disconnect Job or Sign-Off:

1. On the User Exclusion Screen, set one user in the user exclusion file to be disconnected with the Disconnect Job. Enter the user, 1 minute, and a “P” for NetIQ Security Solutions for iSeries disconnect.
2. Sign on as that user and execute the following program: “CALL PSSECURE/ASPGM”. This will prepare that job to be disconnected.
3. Wait several minutes for the job to be disconnected. The actual timing will depend on the setting of your Check Gap.

Inactive Session Monitor And The iSeries Operating System

When Inactive Session Monitor is installed, it will automatically create a user profile called PSSYSOPR. The group profile for PSSYSOPR is QSYSOPR. This is done to eliminate too many messages being sent to the System Operator.

INACTIVE SESSION MONITOR WILL ONLY MONITOR INTERACTIVE JOBS.
NO BATCH JOBS WILL BE AFFECTED BY INACTIVE SESSION MONITOR.

Depending in how subfile programs are coded, the Page Up and Page Down keys may not register as interactive transactions, thereby not registering any keyboard activity.

Performance Enhancement

Inactive Session Monitor uses the WRKACTJOB command to capture information. Inactive Session Monitor only needs the information from your interactive subsystems. You can enter just your interactive subsystems to monitor. This will reduce the overhead of Inactive Session Monitor from 10 to 30%.

In a typical iSeries shop, QINTER and QCTL are the only interactive subsystems. Here are the steps to change Inactive Session Monitor to monitor just those subsystems.

To monitor QINTER and QCTL subsystems:

1. Bring up the Inactive Session Monitor Main Menu using the PSSECURE/ASO command.
2. Select Option 6 to “Change Parameters”.

3. On the bottom third of the screen, you will see “Subsystems to Monitor”. In the first field, the default is *ALL. From left to right, enter your interactive subsystems. So, for QINTER and QCTL, it would look like this:

Subsystems to monitor: QINTER QCTL _____

4. Press **Enter** to save your defaults.
5. By using this feature, Inactive Session Monitor will not have to look at your batch and communication subsystems.

Chapter 6

Secure File Editor

System Overview

NetIQ Corporation offers a secure alternative to Data File Utility with the Secure File Editor. Many Security Officers encounter problems in controlling the use of unauthorized file access by individuals using IBM's Data File Utility (DFU). DFU allows a user to add, change or delete data from any file without producing an internal audit trail of the changes. Secure File Editor automatically creates a detailed log whenever a file alteration is made. The Security Officer can then print an audit trail containing information of which files were accessed and by whom. This audit log will help identify users who are changing data improperly. The Secure File Editor (SFE):

- Provides complete audit capabilities online or in report form for any change made to a secured file.
 - Who
 - When
 - What time
 - What field
 - From what workstation

- Allows search of the Audit Log by:
 - File
 - Library
 - User
 - Workstation
 - Field
 - Any combination of the above (such as, what user changed specific records in a particular month)

Secure File Editor eliminates the drudgery of manipulating files to test new programs, correct data entry errors or search for values in a field. These tasks usually require locating and updating specific records in a file and deleting or adding records. It may even require going through a file dump of the CPYF OUTPUT(*PRINT) command to find the current value in a specific field.

Secure File Editor allows you to interactively view information in any file, whether it is a keyed file, arrival sequence file, logical file or physical file. You can scroll through the records in the file or go instantly to a specific record by key or relative record number. SFE lets you:

- Display records in an easy-to-read spreadsheet form, with the fields arranged in columns. Packed numeric fields are unpacked to be read and updated quickly.
- Scan the file for a specified string to locate the record to change.
- Delete or change a record in single-field or hex mode.
- Create test records by adding data through the DFU-like panels.
- Select only certain fields to display in columnar format for easy comparison.

If there are files with large records, it can be difficult to view pertinent information together. For example, if the Customer Number is in positions 1 - 5 in a record, and the current balance is in positions 230 - 239, it takes a great deal of windowing using IBM's DSPPFM command to get an accurate picture of the data stored in your database. However, with SFE, you can select only the fields that you want to work with.

Secure File Editor offers a great documentation tool, providing an on-line display of the field positions, names and types that make up the record layout of the file you are viewing. A function key allows you to print a hard copy of the field definitions to use in your documentation.

Online Help is provided to guide you through all of the features as you use the system.

Main Menu

The Main Menu contains all of the options you can use to operate Secure File Editor. You can access this menu using command STRSFE (Start Secure File Editor).

PS6	PentaSafe Security Technologies Secure File Editor	CAS QPADEV0000	Date: 6/21/00 Time: 7:46:14
Select one of the following:			
1 File Maintenance			
2 Display Audit Log			
3 Display File Fields			
4 Maintain File Authorities			
5 Clear the Work Files			
6 Purge Audit Log			
7 Enter System Parameters			
Enter Option or Function/Type ==> _____			
F1=Help	F3=Exit	F6=Messages	F9=Window
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports

Option 1 File Maintenance

The File Maintenance option prompts for File, Library, and Member of the file to be edited.

Option 2 Display Audit Log

The Display Audit Log option allows the Security Officer to determine who has changed a file and when that change took place.

Option 3 Display File Fields

The Display File Fields option displays the descriptions of the fields which make up the records in the file.

Option 4 Maintain File Authorities

The Maintain File Authority option allows you to set authorities to files that are accessed by Secure File Editor.

Option 5 Clear the Work Files

Work files are used by Secure File Editor to expedite access to file/field information. This option clears these files.

Option 6 Purge Audit Log

The Purge Audit Log purges data used by the “Display Audit Log” option.

Option 7 Enter System Parameters

The Enter System Parameters option allows you to change the Secure File Editor security parameters. This enables you to log changes that are made to your database and saves ‘Before’ and ‘After’ images of the records that are changed. You can also specify that the person making the change is required to provide a reason why the change was made.

Option 1 File Maintenance

Secure File Editor (DBA)		
Type choices, press Enter.		
Database File	<u>CUSTOMST</u>	Name
Library	<u>QGPI</u>	Name, *LIBL
Member Name	<u>*FIRST</u>	Name, *FIRST
Bottom		
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display		
F24=More keys		

To edit or maintain a file, specify the file name, its library name, member name, and press **Enter**. You can also use command DBA on a command entry line and press F4 to prompt the above screen to appear. Then, enter the appropriate information.

Options

The following options are available on this screen:

Database File - Type the name of the physical or logical file you wish to view.

Library Name - Type the library name to qualify the file name, or allow the command default to use the library list.

Member Name - Type the member name to view or default to the first member.

The Main Screen

S E C U R E F I L E E D I T O R					
File	<u>CUSTMST</u>	Library	<u>QGPL</u>	Member	<u>CUSTMST</u>
Window	<u>00001</u>	Lower Limits. . .	<u>001000001</u>		
Type options, press Enter.					
2=Change 4=Delete 5=Display 6=Print					
	1	2	3		4
.....Opt	CCO#	CCUST#	CCUSTN		CADLN1
1 _	1	1	XYZ COMPANY		ADDRESS LINE 1
2 _	1	3	BEER NUTS SUPPLY STORE INC		432 MALT ROAD
3 _	1	10	MISS MUFFET JR.		11 CURDS WAY
4 _	1	12	ALICE SMITH		557 CHESHIRE DRIVE
5 _	1	16	FAT CAT WEIGHTLOSS INC		400 POUND STREET
6 _	1	24	GOLIATH'S METALWORKS		5 STONES-THROW WAY
7 _	1	38	HUMPTY DUMPTY LINEN SERVICE		36 WALL STREET
8 _	1	40	GILLY'S BEANS INC.		#7-103 GRINDER AVE.
9 _	1	46	DANIEL'S LION TAMING INC		#3-DENSIDE AVE.
10 _	1	50	ABC CORP		123 MAIN
11 _	1	68	COLOR FAST PAINTING CO.		#2-421 GREEN STREET
					More...
F2=Key Fields	F3=Exit	F4=Field info	F5=File info	F6=Create	
F7=Scan bkwd	F8=Scan fwd	F9=Setup scan	F24=More keys		

The preceding screen is the first to be displayed.

The file name, library name, and member name appear as input capable fields. If you wish to view another file or another member in the same file, you may enter the library, file or member name here and the new view will be retrieved.

The records are displayed in a list with the fields arranged in columnar format for easy viewing. All numeric fields are unpacked and edited.

To the left of each record is the relative record number of that record. Above each column is the field name that identifies that field in the record.

There is an option field to the left of each record displayed on the screen. You may enter an option to perform certain tasks on individual records in the file. These options will be covered in detail in a later section.

Positioning the File

SECURE FILE EDITOR					
File	CUSTMST	Library	QGPL	Member	CUSTMST
Window	00001	Lower Limits. .	001000082		
Type options, press Enter.					
2=Change 4=Delete 5=Display 6=Print					
	1	2	3	4	
.....Opt	CCO#	CCUST#	CCUSTN		CADLN1
1 _	1	1	XYZ COMPANY		ADDRESS LINE 1
2 _	1	3	BEER NUTS SUPPLY STORE INC		432 MALT ROAD
3 _	1	10	MISS MUFFET JR.		11 CURDS WAY
4 _	1	12	ALICE SMITH		557 CHESHIRE DRIVE
5 _	1	16	FAT CAT WEIGHTLOSS INC		400 POUND STREET
6 _	1	24	GOLIATH'S METALWORKS		5 STONES-THROW WAY
7 _	1	38	HUMPTY DUMPTY LINEN SERVICE		36 WALL STREET
8 _	1	40	GILLY'S BEANS INC.		#7-103 GRINDER AVE.
9 _	1	46	DANIEL'S LION TAMING INC		#3-DENSIDE AVE.
10 _	1	50	ABC CORP		123 MAIN
11 _	1	68	COLOR FAST PAINTING CO.		#2-421 GREEN STREET
					More...
F2=Key Fields	F3=Exit	F4=Field info	F5=File info	F6=Create	
F7=Scan bkwd	F8=Scan fwd	F9=Setup scan	F24=More keys		
Already at Top of Area.					

You may use the roll key to see more records.

If the file contains a large number of records, it may not be feasible to roll until you reach a record you want to change. You may enter the key of that record into the Lower Limits field at the top of the screen. This will position the file at the record with a key that matches the value entered in the lower limits field.

The above screen shows how to use the lower limits field for faster access to a selected record. In this example, the key field for the file is the Account Name Field CCUST#.

To position the file pointer within CCO #001 to the customer whose number is 82, enter that number in the Lower Limits field as shown below.

SECURE FILE EDITOR

File CUSTMST Library QGPL Member CUSTMST

Window 00001 Lower Limits. . . 001000082

Type options, press Enter.

2=Change 4=Delete 5=Display 6=Print

	1	2	3	4
.....Opt	CCO#	CCUST#	CCUSTN	CADLN1
12 _	1	82	ADAM'S TILLING SERVICE	123 GARDEN LANE
13 _	2	1	FRED BLOGGS SHOE REPAIR	123 ANYSTREET
14 _	2	9	G&P INTERIOR DESIGN STUDIO	3004 WALL ST.
15 _	2	13	BETTY'S BABYSITTING SERVICE	4564 PHILIP STREET
16 _	2	17	JOHN'S TREE TOPPING CO.	#45-MCCLELLAN ST.
17 _	2	20	HAIR BY HARRY INC.	809 BALDWIN ROAD
18 _	2	24	PLAY-TILL-YOU-DROP VIDEOS	9 OBSESSION CIRCLE
19 _	2	27	LA BOUCHERIE DE JACQUE	13 BOVINE PLACE
20 _	2	32	NARCISSUS MIRROR REPAIRS	#2-111 REFLECTION W
21 _	2	34	DICK'S RECORDING STUDIO	3 MINUTE LANE
22 _	2	45	CLEAN-SWEEP MAIDS SERVICE	234 DUSTY LANE

More...

F2=Key Fields F3=Exit F4=Field info F5=File info F6=Create

F7=Scan bkwd F8=Scan fwd F9=Setup scan F24=More keys

The record for customer number 82, is now positioned at the top of the screen for easy access. You may also use **F2** to position the file using the key field screen. This will be covered in the section on Function Keys.

Windowing the Display

```

          S E C U R E   F I L E   E D I T O R

File . . . . . CUSTMST   Library . . . . . OGPL       Member . . . . . CUSTMST
Window . . . . . 00003   Lower Limits. . . 001000082

Type options, press Enter.
  2=Change  4=Delete  5=Display  6=Print

          3              -              4              5
.....Opt CCUSTN          CADLN1          CAD
12 _ ADAM'S TILLING SERVICE      123 GARDEN LANE
13 _ FRED BLOGGS SHOE REPAIR    123 ANYSTREET
14 _ G&P INTERIOR DESIGN STUDIO  3004 WALL ST.
15 _ BETTY'S BABYSITTING SERVICE 4564 PHILIP STREET
16 _ JOHN'S TREE TOPPING CO.     #45-MCCLELLAN ST.
17 _ HAIR BY HARRY INC.         809 BALDWIN ROAD          DUN
18 _ PLAY-TILL-YOU-DROP VIDEOS   9 OBSESSION CIRCLE
19 _ LA BOUCHERIE DE JACQUE      13 BOVINE PLACE
20 _ NARCISSUS MIRROR REPAIRS    #2-111 REFLECTION WAY
21 _ DICK'S RECORDING STUDIO     3 MINUTE LANE
22 _ CLEAN-SWEEP MAIDS SERVICE   234 DUSTY LANE

                                     More...

F2=Key Fields  F3=Exit      F4=Field info  F5=File info  F6=Create
F7=Scan bkwd  F8=Scan fwd  F9=Setup scan  F24=More keys

```

When the main screen is first displayed, the file is positioned so that the first field appears on the left side of the screen.

Notice that there is an input field in the upper left portion of the screen called Window. If you wish to see a column which is not displayed on the screen at this time, you may “window over” to that column by entering the number of that column (field) here.

The screen will now shift to display the selected column (field) on the left side of the screen. If you are looking at view 2 or 3 (explained in a later section), the window field will contain the position in the record rather than the field number to shift to.

Changing Data

```

      S E C U R E   F I L E   E D I T O R

File . . . . . CUSTMST   Library . . . . . QGPL   Member . . . . CUSTMST
Window . . . . . 00001   Lower Limits. . . 001000082

Type options, press Enter.
      2=Change   4=Delete   5=Display   6=Print
      1         2         3         4
.....Opt CC0#   CCUST#   CCUSTN   CADLN1
      12 2     1       82   ADAM'S TILLING SERVICE   123 GARDEN LANE
      13 _     2       1    FRED BLOGGS SHOE REPAIR   123 ANYSTREET
      14 _     2       9    G&P INTERIOR DESIGN STUDIO 3004 WALL ST.
      15 _     2      13   BETTY'S BABYSITTING SERVICE 4564 PHILIP STREET
      16 _     2      17   JOHN'S TREE TOPPING CO.    #45-MCCLELLAN ST.
      17 _     2      20   HAIR BY HARRY INC.         809 BALDWIN ROAD
      18 _     2      24   PLAY-TILL-YOU-DROP VIDEOS   9 OBSESSION CIRCLE
      19 _     2      27   LA BOUCHERIE DE JACQUE     13 BOVINE PLACE
      20 _     2      32   NARCISSUS MIRROR REPAIRS    #2-111 REFLECTION W
      21 _     2      34   DICK'S RECORDING STUDIO     3 MINUTE LANE
      22 _     2      45   CLEAN-SWEEP MAIDS SERVICE   234 DUSTY LANE
                                     More...

F2=Key Fields   F3=Exit       F4=Field info   F5=File info   F6=Create
F7=Scan bkwd   F8=Scan fwd   F9=Setup scan  F24=More keys
```

To change data in a record, type 2 in the option field to the left of the record. In the previous example, we wish to change the record for the first customer.

The first time in an SFE session that a record is either added, changed, or deleted, a prompt may appear for entry of a Reason Description. Up to 240 bytes of text may be entered to describe the reason why the file is being changed. The prompt is displayed if the SFE system parameters defaults specify that the Reason Description is required.

SECURE FILE EDITOR		UPDATE
File...: QGPL/CUSTMST	Member.: CUSTMST	RRN....: 00000012
CCOH.....	<u>001</u>	
CCUST#.....	<u>000082</u>	
CCUSTN.....	<u>ADAM'S TILLING SERVICE</u>	
CADLN1.....	<u>123 GARDEN LANE</u>	
CADLN2.....		
CCITY.....	<u>EDEN</u>	
CSTATE.....	<u>CA</u>	
CZIP1.....	<u>55443</u>	
CZIP2.....	<u>0000</u>	
CAREA.....	<u>111</u>	
CTEL.....	<u>2345678</u>	
CTERMS.....	<u>0</u>	
CACTBL.....	<u>0039411</u>	
CCURDU.....	<u>0007811</u>	
COVR30.....	<u>0008250</u>	
COVR60.....	<u>0016250</u>	
		More...
F3=Exit	F4=Field Info	F7=Hex mode
F10=Print record	F12=Cancel	

After a record is selected to be changed, a detail panel is displayed with each field placed on a separate line as shown above.

The record key is shown at the top to verify the record being changed. Since all fields may not fit on a single display, you may use the roll keys to roll down to the next display to show more fields.

- To return to the main screen without updating this record, use **F12**.
- To print a hard copy of the entire record in a format similar to what is shown on the screen, use **F10**.
- If you wish to view and change the record in hexadecimal format, use **F7** to display a new screen.

The following screen shows that the customer name now includes the word INC.

```

          S E C U R E   F I L E   E D I T O R

File . . . . . CUSTMST   Library . . . . . QGPL       Member . . . CUSTMST
Window . . . . . 00001   Lower Limits. . . 001000082

Type options, press Enter.
  2=Change   4=Delete   5=Display   6=Print
           1         2         3         4
.....Opt CC0#   CCUST#   CCUSTN           CADLN1
12 _      1      82 ADAM'S TILLING SERVICE INC. 123 GARDEN LANE
13 _      2        1 FRED BLOGGS SHOE REPAIR  123 ANYSTREET
14 _      2        9 G&P INTERIOR DESIGN STUDIO 3004 WALL ST.
15 _      2      13 BETTY'S BABYSITTING SERVICE 4564 PHILIP STREET
16 _      2      17 JOHN'S TREE TOPPING CO.    #45-MCCLELLAN ST.
17 _      2      20 HAIR BY HARRY INC.         809 BALDWIN ROAD
18 _      2      24 PLAY-TILL-YOU-DROP VIDEOS  9 OBSESSION CIRCLE
19 _      2      27 LA BOUCHERIE DE JACQUE    13 BOVINE PLACE
20 _      2      32 NARCISSUS MIRROR REPAIRS   #2-111 REFLECTION W
21 _      2      34 DICK'S RECORDING STUDIO   3 MINUTE LANE
22 _      2      45 CLEAN-SWEEP MAIDS SERVICE 234 DUSTY LANE
                                     More...

F2=Key Fields  F3=Exit      F4=Field info  F5=File info  F6=Create
F7=Scan bkwd   F8=Scan fwd   F9=Setup scan F24=More keys

```

Deleting Records

To delete records from the file, you select them with 4 in the option field, and press **Enter**.

```

      S E C U R E   F I L E   E D I T O R

File . . . . . CUSTMST   Library . . . . . QGPL       Member . . . CUSTMST
Window . . . . . 00001   Lower Limits. . . 001000082

Type options, press Enter.
  2=Change  4=Delete  5=Display  6=Print

      1      2      3      4
.....Opt CC0#  CCUST#  CCUSTN  CADLN1
12 4  1      82  ADAM'S TILLING SERVICE INC.  123 GARDEN LANE
13 4  2      1  FRED BLOGGS SHOE REPAIR      123 ANYSTREET
14 4  2      9  G&P INTERIOR DESIGN STUDIO    3004 WALL ST.
15 4  2     13  BETTY'S BABYSITTING SERVICE  4564 PHILIP STREET
16 4  2     17  JOHN'S TREE TOPPING CO.      #45-MCCLELLAN ST.
17 =  2     20  HAIR BY HARRY INC.           809 BALDWIN ROAD
18 _  2     24  PLAY-TILL-YOU-DROP VIDEOS    9 OBSESSION CIRCLE
19 _  2     27  LA BOUCHERIE DE JACQUE      13 BOVINE PLACE
20 _  2     32  NARCISSUS MIRROR REPAIRS    #2-111 REFLECTION W
21 _  2     34  DICK'S RECORDING STUDIO     3 MINUTE LANE
22 _  2     45  CLEAN-SWEEP MAIDS SERVICE   234 DUSTY LANE

                                     More...

F2=Key Fields  F3=Exit      F4=Field info  F5=File info  F6=Create
F7=Scan bkwd  F8=Scan fwd  F9=Setup scan F24=More keys
```

The first time in an SFE session that a record is either added, changed, or deleted, a prompt may appear for entry of a Reason Description. Up to 240 bytes of text may be entered to describe the reason why the file is being changed. The prompt is displayed if the SFE system parameter defaults specify that the Reason Description is required.

A list of the records chosen for deletion is then displayed for confirmation.

```

-                               S E C U R E   F I L E   E D I T O R
                               Confirm Delete of Records

Press Enter to confirm your choices for 4=Delete.
Press F12 to return to change your choices.

      1      2      3      4
.....Opt CC0#  CCUST# CCUSTN  CADLN1
12  4   1      82  ADAM'S TILLING SERVICE INC.  123 GARDEN LANE
13  4   2          1  FRED BLOGGS SHOE REPAIR    123 ANYSTREET
14  4   2          9  G&P INTERIOR DESIGN STUDIO  3004 WALL ST.
15  4   2      13  BETTY'S BABYSITTING SERVICE  4564 PHILIP STREET
16  4   2      17  JOHN'S TREE TOPPING CO.      #45-MCCLELLAN ST.

F12=Cancel                                Bottom
```

Function Keys

Below you will find descriptions of the function keys. Detailed information on each function will be displayed on subsequent pages.

- F2** Show Key Field information.
- F3** Exit the program.
- F4** Shows field definitions. This will display another screen that lists information on each field in the record layout.
- F5** Displays a window of information about the file, such as record length, number of records and number of fields.
- F6** Allows you to create a new record in the file
- F7** Scan backward through the file for a specified string

- F8** Scan forward through the file for a specified string
- F9** Sets up the scan function with the value to scan for and number of records to search.
- F10** Show a different view of the data.
- F13** Query the file with selection parameters
- F14** Shows database relationships for the file
- F15** Shows all members in the file.
- F17** Positions the display at the first record in the file.
- F18** Positions the display at the last record in the file
- F19** Allows you to see information to the left of the current display.
- F20** Allows you to see information to the right of the current display

Key Field Information

To display a list of key fields for the file, use **F2** from the main screen. The window below will appear.

SECURE FILE EDITOR

Display Key Fields

File . . : QGPL/CUSTMST Format . . : RCUSTMS

No.	Field	Value
1	CCO#.....	<u>001</u>
2	CCUST#.....	<u>000082</u>

Bottom

F3=Exit F11=Descriptions F12=Cancel

F2=Key Fields F3=Exit F4=Field info F5=File info F6=Create

F7=Scan bkwd F8=Scan fwd F9=Setup scan F24=More keys

This window contains a list of key fields with the values from the record at the top of the main screen. If you want to reposition the file to another record, you may change the values in the key fields and press **Enter**.

Use **F11** to show a description of the key fields.

Displaying Field Descriptions

To display the descriptions of the fields which make up the records in the file, use **F4** from the main screen. A screen like the one below will be displayed.

```

          S E C U R E   F I L E   E D I T O R
          Display Field Descriptions

File . . . : QGPL/CUSTMST      Format . . . : RCUSTMS      Type . . . : *PHY

Type options, press Enter.
1=Select

Opt Seq Field      Key Typ Length  From  To  Text Description
=   1 CCO#         K01  P    3 00    1    2  Company Number
-   2 CCUST#       K02  P    6 00    3    6  Customer Number
-   3 CCUSTN       A    30    7    36  Customer Name
-   4 CADLN1       A    30    37   66  Address Line 1
-   5 CADLN2       A    30    67   96  Address Line 2
-   6 CCITY        A    20    97  116  City Name
-   7 CSTATE       A     2   117  118  State Abbrev
-   8 CZIP1        P    5 00   119  121  Zip Code
-   9 CZIP2        P    4 00   122  124  Extended Zip Code
-  10 CAREA        P    3 00   125  126  Area Code
-  11 CTEL         P    7 00   127  130  Telephone Number

                                          More...

F3=Exit      F7=Next format    F10=Print all
F12=Cancel   F17=Top                F18=Bottom
  
```

You can also use the DSPFLD command to display descriptions of the fields. You may select only certain fields to display by typing **1** next to those fields you want to see. Key fields will be displayed whether they are selected or not.

- If the file contains more than one format, as in the case of a multi-format logical file, you may use **F7** to show the fields for the next format in the file.
- Use **F10** to print the entire list of field descriptions.
- **F17** will position the display at the first field in the file, **F18** will position it to the last.

File Information

Use **F5** to display information about the file.

A window will appear with the record length, record count, and number of formats for the current file, as shown below.

```

      S E C U R E   F I L E   E D I T O R

File . . . . . CUSTMST   Library . . . . . QGPL   Member . . . CUSTMST
Window . . . . . 00001   Lower Limits. . 001000082

Type options, pre
  2=Change  4=D
      1
.....Opt CC0#
  12 _  1
  13 _  2
  14 _  2
  15 _  2
  16 _  2
  17 _  2
  18 _  2
  19 _  2
  20 _  2
  21 _  2
  22 _  2

      File Information
      -
      File Name . . . . . CUSTMST
      Member Name . . . . . CUSTMST
      Current Records . . .      30
      Max Record Length . .  157
      Number of Formats . .   1
      F3=Exit   F12=Cancel

F2=Key Fields      info      More...
F7=Scan bkwd      F8=Scan fwd  F9=Setup scan  F24=More keys  F6=Create
```

Adding Records

From the main screen you can use **F6** to add new records. A screen like the one below will appear.

S E C U R E F I L E E D I T O R		ADD
File....:	QGPL/CUSTMST	Member.: CUSTMST RRN....: 00000000
CCO#.....	000	
CCUST#.....	000000	
CCUSTN.....		
CADLN1.....		
CADLN2.....		
CCITY.....		
CSTATE.....		
CZIP1.....	00000	
CZIP2.....	0000	
CAREA.....	000	
CTEL.....	00000000	
CTERMS.....	0	
CACTBL.....	00000000	
CCURDU.....	00000000	
COVR30.....	00000000	
COVR60.....	00000000	
F3=Exit F11=Names/Descriptions F12=Cancel		More...

This screen lets you enter data in every field in the record. If there are too many fields to fit on one screen, you may use the Roll Keys to access additional fields. The field names are displayed when the screen is first displayed. Use **F11** to display the descriptive text for the fields instead of the name.

The first time in an SFE session that a record is either added, changed, or deleted, a prompt may appear for entry of a Reason Description. Up to 240 bytes of text may be entered to describe the reason why the file is being changed. The prompt is displayed if the SFE system parameters defaults specify that the Reason Description is required.

The Scan Function

A scan function is available which proves quite useful in locating specific records to be viewed or changed.

SECURE FILE EDITOR				
File <u>CUSTMST</u>
Window				
Type options, p	Scan Database			
2=Change 4	Position in Record :			
1	From <u>1</u> 1-9999			
.....Opt CC	To <u>157</u> 1-9999			
12 _	Records to scan . . <u>500</u> 1-9999,*all			
13 _	Scan for string:			
14 _	_____			
15 _	The scan function is case-sensitive.			
16 _	Use upper/lower case for scan string.			
17 _	F7=Scan bkwd F8=Scan fwd			
18 _				
19 _				
20 _				
21 _				
22 _				
F2=Key Fields	F3=Exit	F4=Field info	F5=File info	F6=Create
F7=Scan bkwd	F8=Scan fwd	F9=Setup scan	F24=More keys	

You must first use **F9** to display a window for setting the scan parameters to use for the search. If you know the position in the record where the string is likely to be found, you may enter those positions here. This will improve the speed of the search since the entire record will not have to be scanned.

Enter the number of records to be searched in each pass. Enter up to 25 characters of the string to be located. Use **F7** to scan backward through the file and **F8** to scan forward.

More keys

Press **F24** to display the next set of functions keys available for this display.

SECURE FILE EDITOR

FileCUSTMSTLibraryQGPLMemberCUSTMST

Window00001Lower Limits. . .000000000

Type options, press Enter.

2=Change4=Delete5=Display6=Print

	1	2	3	4
.....Opt	CCO#	CCUST#	CCUSTN	CADLN1
31 _	0	0		
1 _	1	1	XYZ COMPANY	ADDRESS LINE 1
2 _	1	3	BEER NUTS SUPPLY STORE INC	432 MALT ROAD
3 _	1	10	MISS MUFFET JR.	11 CURDS WAY
4 _	1	12	ALICE SMITH	557 CHESHIRE DRIVE
5 _	1	16	FAT CAT WEIGHTLOSS INC	400 POUND STREET
6 _	1	24	GOLIATH'S METALWORKS	5 STONES-THROW WAY
7 _	1	38	HUMPTY DUMPTY LINEN SERVICE	36 WALL STREET
8 _	1	40	GILLY'S BEANS INC.	#7-103 GRINDER AVE.
9 _	1	46	DANIEL'S LION TAMING INC	#3-DENSIDE AVE.
10 _	1	50	ABC CORP	123 MAIN

More...

F10=Toggle viewF13=QueryF14=RelationsF15=Members

F17=TopF18=BottomF19=LeftF20=RightF24=More keys

Another View of the Data

It may not always be convenient to show the data in columnar format. For example, S/36 files that are not externally described will show all the data under one field name.

```

          S E C U R E   F I L E   E D I T O R

File . . . . . CUSTMST   Library . . . . . QGPL       Member . . . . CUSTMST
Window . . . . . 00001   Lower Limits. . . 000000000

Type options, press Enter.
    2=Change  4=Delete  5=Display  6=Print

.....0pt .....+...10.....+...20.....+...30.....+...40.....+...50.....+...60.....+
31 _  *****
 1 _  *****XYZ COMPANY                ADDRESS LINE 1
 2 _  *****BEER NUTS SUPPLY STORE INC  432 MALT ROAD
 3 _  *****MISS MUFFET JR.             11 CURDS WAY
 4 _  *****ALICE SMITH                 557 CHESHIRE DRIVE
 5 _  *****?FAT CAT WEIGHTLOSS INC     400 POUND STREET
 6 _  *****|GOLIATH'S METALWORKS       5 STONES-THROW WAY
 7 _  *****±HUMPTEY DUMPTHEY LINEN SERVICE 36 WALL STREET
 8 _  *****GILLY'S BEANS INC.          #7-103 GRINDER AVE.
 9 _  *****?DANIEL'S LION TAMING INC    #3-DENSIDE AVE.
10 _  *****ABC CORP                   123 MAIN

                                          More...

F10=Toggle view      F13=Query      F14=Relations      F15=Members
F17=Top      F18=Bottom      F19=Left      F20=Right      F24=More keys
Field contains a non-displayable character.
```

Use **F10** to show another view of the data. Instead of field names in the heading, you will just see the position markers to show where the data appears in the record. Packed data will sometimes result in non-displayable characters, which are displayed as asterisks to avoid screen errors.

Use **F10** to show another view of the data.

[illegible]

This time you will see the hexadecimal representation of the data to show the packed data fields as they appear in the file.

Query

You can select records by specifying selection criteria.

Query Selection

File . . QGPL/CUSTOMST

Type Comparisons, press Enter.
Tests: GT, LT, GE, LE, EQ, NE, RG, CT, WC

Field Name	Test	Values (Number, "Character")	Key
CCON#.....	—	_____	—
CCUST#.....	—	_____	—
CCUSTN.....	—	_____	<u>3</u>
CADLN1.....	—	_____	—
CADLN2.....	—	_____	—
CCITY.....	—	_____	<u>2</u>
CSTATE.....	—	_____	<u>1</u>
CZIP1.....	—	_____	—
CZIP2.....	—	_____	—
CAREA.....	—	_____	—
CTEL.....	—	_____	—
CTERMS.....	—	_____	—

More...

F3=Exit F5=Refresh F10=Process F11=Names/Descriptions F12=Cancel

Selecting Records

F13 will display a screen to allow the selection of certain records by querying the file. On this display you specify comparison tests to be used to select the records. Selection criteria may be entered against one or more fields in the file. The screen first displays field names along the left side of the screen. You may use **F11** to toggle to show field descriptions instead.

You can specify one test for each field to determine if the record is to be selected. If the result of the test or the combined result of several tests is true, the record will be displayed. If you do not define any comparison tests, all records in the file will be displayed.

To specify each comparison test, position the cursor next to the field that is to be compared with a constant value that will be typed in the VALUES column. In the TEST column, type the test value (such as EQ for equal, or GT for greater than) that indicates the condition that must exist in the field being tested.

The possible test values are:

GT	greater than
LT	less than
GE	greater
LE	less than or equal to
EQ	equal
NE	not equal
RG	range
CT	contains
WC	wild card

For example, to display all customers in the state of Texas whose name starts with “M”, you would specify a TEST of “EQ” and a VALUE of “TEXAS” in the columns next to field name CSTATE. Then you would also specify a TEST of “RG” (for range) and a VALUE of “Maaaaaaa” “Mzzzzzzzzzz” in the columns next to the CCUSTN field.

If you wanted to find all customers whose address contained the word “Broad” you could specify a TEST of “CT” and a VALUE of “Broad” next to the CADLN1 field. This would then display all customers on Broadway St., Broad Blvd., Broad Meadow Lane, etc.

The wildcard test will select records that match any zero or more characters. Use an asterisk to denote the variable characters. For example, if you entered “WC” for the TEST and “A*C*” for the VALUE next to the CCUSTN field, the query would return records that have a customer name of AC, ABC, Ax C, ABCD, Axxxxxxx C, and so on. If the asterisk were omitted from the end of the search argument, the record would only be selected if the field ends with the character C (only if there is a C in the last position of the field).

Key Fields

The KEY column may be used to alter the sort order of the file. When the screen is first displayed it will show a number next to the fields that are the current key fields for the file. The first key field would have the number 1, the second key field would have the number 2, and so on.

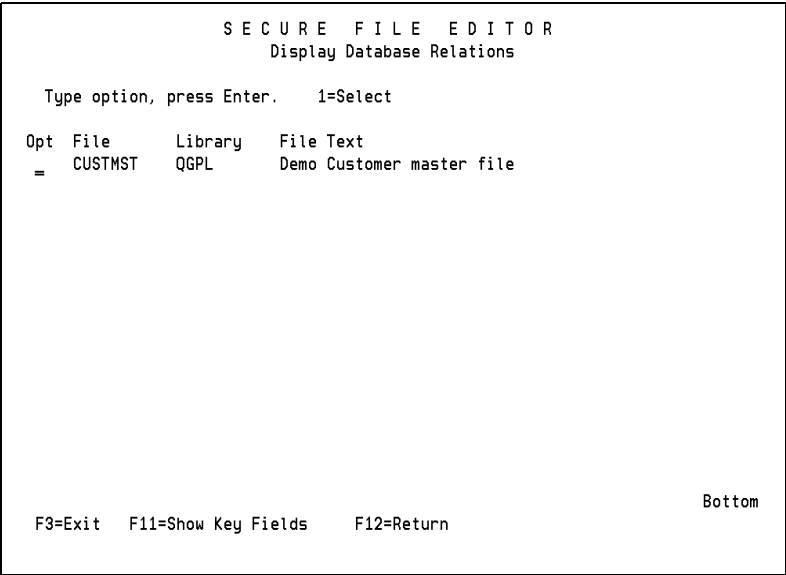
Type in the numbers to correspond with the new sort order for the file. For example, to sort the file under “Query” on page 341 by State, then City, then Customer Name, you would type 1 in the KEY column next to the field CSTATE, type 2 in the KEY column next to CCITY, and type 3 next to CCUSTN.

Processing the Query

To process the query with the values you have entered for the selection and key fields, press **F10**. There will be a slight delay while the file is queried and records are selected.

Database Relationships

F14 will show database relationships for the current file.



If you are currently accessing a logical file, this screen will show the physical file that the logical is built over, and any other logicals built over the same physical. If you are currently accessing a physical file, it will show the physical and any logicals built over it. To access another logical, or the physical, you may type 1 next to the file that you wish to access.

Member List

F15 will display all of the members in the current file.

```
          S E C U R E   F I L E   E D I T O R
          Display Member List Information

File:  QGPL/CUSTOMST

Type option, press Enter.    1=Select

Opt Member      Records      Deleted      Text
=  CUSTMST          31          0  Demo customer master file

                                     Bottom

F3=Exit      F12=Return
```

If you wish to see data in another member, you can select that member by typing **1** in the selection field next to the member name that you want to access.

Positioning to Top or Bottom

When the main screen is first displayed, the first record in the file is positioned on the top line of the display. You can scroll through the file, displaying 11 records at a time on the screen.

SECURE FILE EDITOR

FileCUSTMSTLibraryQGPLMemberCUSTMST

Window00001Lower Limits. . .001000082

Type options, press Enter.

2=Change4=Delete5=Display6=Print

1234

.....OptCCO#CCUST#CCUSTNCADLN1

12_182ADAM'S TILLING SERVICE INC.123 GARDEN LANE

13_21FRED BLOGGS SHOE REPAIR123 ANYSTREET

14_29G&P INTERIOR DESIGN STUDIO3004 WALL ST.

15_213BETTY'S BABYSITTING SERVICE4564 PHILIP STREET

16_217JOHN'S TREE TOPPING CO.#45-MCCLELLAN ST.

17_220HAIR BY HARRY INC.809 BALDWIN ROAD

18_224PLAY-TILL-YOU-DROP VIDEOS9 OBSESSION CIRCLE

19_227LA BOUCHERIE DE JACQUE13 BOVINE PLACE

20_232NARCISSUS MIRROR REPAIRS#2-111 REFLECTION W

21_234DICK'S RECORDING STUDIO3 MINUTE LANE

22_245CLEAN-SWEEP MAIDS SERVICE234 DUSTY LANE

More...

F10=Toggle viewF13=QueryF14=RelationsF15=Members

F17=TopF18=BottomF19=LeftF20=RightF24=More keys

If you want to go to the last record in a large file it could take a very long time to get there. You may use **F18** to position the file to the last record. Conversely, if you are at the end of the file and want to go back to the first record, use **F17** to position at the top.

Windowing Left and Right

When the main screen is first displayed, the file is positioned so that the first field appears on the left side of the screen.

You may use **F20** to shift the display to the field (column) that comes after the last field displayed. In the above example, the last field displayed is the CADLN1, billing address field.

```

          S E C U R E   F I L E   E D I T O R

File . . . . . CUSTMST   Library . . . . . QGPL       Member . . . . CUSTMST
Window . . . . . 00001   Lower Limits. . . 001000082

Type options, press Enter.
  2=Change   4=Delete   5=Display   6=Print
      1       2       3
.....Opt CC0#   CCUST#   CCUSTN
12 _   1       82 ADAM'S TILLING SERVICE INC.   123 GARDEN LANE
13 _   2       1  FRED BLOGGS SHOE REPAIR       123 ANYSTREET
14 _   2       9  G&P INTERIOR DESIGN STUDIO     3004 WALL ST.
15 _   2      13  BETTY'S BABYSITTING SERVICE   4564 PHILIP STREET
16 _   2      17  JOHN'S TREE TOPPING CO.       #45-MCCLELLAN ST.
17 _   2      20  HAIR BY HARRY INC.            809 BALDWIN ROAD
18 _   2      24  PLAY-TILL-YOU-DROP VIDEOS     9 OBSESSION CIRCLE
19 _   2      27  LA BOUCHERIE DE JACQUE        13 BOVINE PLACE
20 _   2      32  NARCISSUS MIRROR REPAIRS      #2-111 REFLECTION W
21 _   2      34  DICK'S RECORDING STUDIO       3 MINUTE LANE
22 _   2      45  CLEAN-SWEEP MAIDS SERVICE     234 DUSTY LANE
                                     More...

F10=Toggle view      F13=Query      F14=Relations      F15=Members
F17=Top      F18=Bottom      F19=Left      F20=Right      F24=More keys

```

F20 will shift the panel to allow you to see data to the right of the current display. By using **F20** on the previous panel, you will see a display like the one below.

F19 will shift the panel to allow you to see data to the left of the current display.

```

      S E C U R E   F I L E   E D I T O R

File . . . . . CUSTMST   Library . . . . . QGPL       Member . . . . CUSTMST
Window . . . . . 00005   Lower Limits. . . 001000082

Type options, press Enter.
  2=Change   4=Delete   5=Display   6=Print

          5
.....Opt CADLN2
12 _
13 _
14 _
15 _
16 _
17 _  DUNCAN WAS HERE
18 _
19 _
20 _
21 _
22 _

          6
          CCITY
          EDEN
          MAINTOWN
          CHESTERFIELD
          CARNARVAN
          BARKLEY
          WIGG
          AUSTEN
          VACHEVILLE
          VISAGE
          GATEWATER
          BROOMSVILLE

          7      8
          CSTATE CZIP1
          CA      55443
          CA      91234
          CA      73633
          BC      92620
          WV      78901
          WI      88888
          CA      44444
          CA      84850
          VI      55566
          IL      56754
          YU      66442
                                More...

F10=Toggle view      F13=Query      F14=Relations      F15=Members
F17=Top      F18=Bottom      F19=Left      F20=Right      F24=More keys
```

Option 2 Display Audit Log

The Audit Log will show who has changed a file and when that change took place. You can also use the command DBALOG to display this information.

The Secure File Editor creates a detailed audit record every time a record is added, changed or deleted from the database. This audit trail can be browsed by File Name, by Field within a file, by User, by Workstation, by Date and Time or any combination of the above parameters.

```

                                Show DBA Audit Log (DBALOG)

Type choices, press Enter.

File . . . . . _____ Name
Library . . . . . _____ Name
Member . . . . . _____ Name
Field Name . . . . . _____ Name
User ID . . . . . _____ Name
Workstation . . . . . _____ Name
Actions to show . . . . . - A=adds C=changes D=deletes
Beginning date . . . . . _____ Date
Beginning time . . . . . _____ *TIME
Ending date . . . . . _____ Date
Ending time . . . . . _____ *TIME
Show Only Changed Fields . . . . . - Y=Yes, N=No

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

```

To use the Audit Log command, select Option 2 from the Secure File Editor Main Menu or type DBALOG on any command line and use **F4** to prompt for parameters, and the above screen will appear. Then, enter the appropriate information.

- File Name:** Type the name of the file for which you wish to view an audit trail.
- Library Name:** Type the library name to qualify the file name, or leave library blank and it will find entries for all files of that name.
- Member name:** Type the member name to view or leave blank to find entries for all members in a file.
- Field Name:** Type a field name to see who has changed a specific field within a file, or leave this parameter blank to see changes made against all fields in the file.

- User ID:

Type a User ID to determine the changes made by a particular user.
- Workstation:

Type a workstation name to determine the changes made from a particular workstation.
- Actions to show:

Type A to see only the records added to a file. Type C to see only changes or type D to see only deletions made. Leaving this parameter blank will show all actions.
- Beginning date/

Beginning time:

Use the date and time parameters to further narrow your search of audit trail entries. The correct date format is MM/DD/YY and the correct time format is HH:MM:SS.

Secure File Editor Audit Log will produce a report that can be viewed on-line or printed in order to show who has made changes that occurred within the selection criteria.

The Secure File Editor Database Log Report

The Secure File Editor logging feature maintains complete “before and after” images of database records changed with Secure File Editor without journaling. This will give an accurate picture of the changes made to your database as well as who made the changes, when, and from what workstation. If the detailed logging option is selected, a report can be printed showing the contents of the individual fields in a database record before and after the changes were made.

The report will print the record in the following format:

3/15/01 9.24.11		S E C U R E F I L E E D I T O R						P A G E 1	
D A T A B A S E L O G									
FILE	LIBRARY	MEMBER	REL REC #	FIELD	A/C/D	USER	WORKSTATN	DATE	TIME
ZPPF03	PSSECURE	ZPPF03	12	LSIGNW	C	PMB	QPADEV000C	9/05/08	22:07:12
REASON:		TESTING							
----- B E F O R E -----									
USER.....: AA2						USER.....: AA2			
LEVEL.....: 01						LEVEL.....: 01			
LCHGD.....: 20000613						LCHGD.....: 20000613			
LSIGND.....: 00000000						LSIGND.....: 00000000			
LSIGNT.....: 000000						LSIGNT.....: 000000			
*LSIGNW.....:						*LSIGNW.....: QPADEV0001			
PASS.....:						PASS.....:			
----- A F T E R -----									
F3=Exit F12=Cancel F19=Left F20=Right F24=More keys									

Records can be selected by File, User, Type (add, change, delete) or Date Range. Records will remain in the log until purged.

The report will include the Reason Description entered when the file was changed, if entry of the Reason Description was required in the Change System Parameters Screen. Data in the Date column as well as the Report Date, are displayed in Job Date Format (*JOB).

Option 3 Display File Fields

Displays the fields and attributes of a file. You can also use the command DSPFLD to display field-level information.

Display File Field Info (DSPFLD)

Type choices, press Enter.

Database File	<u> </u>	Name
Library	<u>*LIBL</u>	Name, *LIBL

Bottom

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

Enter the Database File and Library name, press **Enter**, and the following screen displays:

```

      S E C U R E   F I L E   E D I T O R
      Display Field Descriptions

File . . . : QGPL/CUSTMST      Format . . . : RCUSTMS      Type . . . : *PHY

Type options, press Enter.
  1=Select

Opt Seq Field      Key Typ Length   From   To   Text Description
-   1 CC0#         K01 P    3 00     1     2   Company Number
-   2 CCUST#       K02 P    6 00     3     6   Customer Number
-   3 CCUSTN       A     30     7    36   Customer Name
-   4 CADLN1       A     30    37   66   Address Line 1
-   5 CADLN2       A     30    67   96   Address Line 2
-   6 CCITY        A     20    97  116   City Name
-   7 CSTATE       A      2   117  118   State Abbrev
-   8 CZIP1        P     5 00   119  121   Zip Code
-   9 CZIP2        P     4 00   122  124   Extended Zip Code
-  10 CAREA        P     3 00   125  126   Area Code
-  11 CTEL         P     7 00   127  130   Telephone Number

                                         More...

F3=Exit      F7=Next format      F10=Print all
F12=Cancel   F17=Top                  F18=Bottom
```

The display shown above is also available using command DSPFLD (Display File Fields) on a command line.

- The record format layout can also be printed using **F10**.
- To position to the top of the list, use **F17**.
- Use **F18** to position the screen to the bottom of the field list.

Option 4 Maintain File Authorities

You can set authorities to files that are accessed by Secure File Editor, regardless of the program's object level authority.

Work With File Authorities

Position to Library / File . . . _____

Type option, press Enter.
2=Change 4=Delete

Opt	Library	File	User	Read	Add	Update	Delete
_	PSAUDIT	DDPF55	GAS	Y	Y	Y	Y
_	PSCOMMON	TS115FA	EHD	Y	Y	Y	Y

F3=Exit

F6=Add file record

F11=Sort by User

F12=Cancel

Bottom

Type the command PSSECURE/CHGAUT or select Option 4 from the Secure File Editor main menu. This will present a screen as shown above. This screen lists the files and users and their authorizations. In this example users GAS and EHD can use Secure File Editor to read, add, update, and delete records in file PSAUDIT/DDPF55 and PSCOMMON/TS115FA.

When Command DBA is executed, it first checks authorizations to the file through i5/OS, then it checks the authorizations you have set up through this function. If the Secure File Editor authorization is different, it will override the i5/OS authorization.

Use **F6** to add new records to this authorization file. To change or delete a record, use the appropriate number in the option field.

Maintain File Authorities

File	_____	Name, *ALL
Library	_____	Name, *ALL
User Profile	_____	Name, *ALL
Read Authority	Y	Y=yes, N=no
Add Authority	Y	Y=yes, N=no
Update Authority	Y	Y=yes, N=no
Delete Authority	Y	Y=yes, N=no
F3=Exit F11=Delete F12=Cancel		

When the option to change a record has been entered, the screen shown above will appear. You may change authorities for the user and file by typing **Y** or **N** in the appropriate column.

Option 5 Clear the Work Files

This option will clear Secure File Editor work files that help to speed up processing. There is no prompt or confirmation panel for this option.

You can also use command PSSECURE/CLRDBA (Clear Work Files) on a command line.

Option 6 Purge Audit Data

Use this option to purge the audit trail used by the “Display Audit Log” function. The data can be purged based on various criteria, such as File, User, Workstation, Action (A, C, D), and Beginning and Ending date and time.

You can also purge this audit trail by issuing the command PRGDBALOG.

Purge Audit Log Records (PRGDBALOG)

Type choices, press Enter.

File

Library

Member

Field Name

User ID

Workstation

Actions to show

Beginning date

Beginning time

Ending date

Ending time

Name

Name

Name

Name

Name

Name

A=adds C=changes D=deletes

*DATE

*TIME

*DATE

*TIME

Bottom

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display

F24=More keys

Note

The date format on the screen should be entered in the MM/DD/YY format, and the time format should be entered in the HH:MM:SS format.

Option 7 Enter System Parameters

To change the Secure File Editor security parameters, type the command PSSECURE/CHGDBA or select Option 7 on the Secure File Editor main menu.

```

                S E C U R E   F I L E   E D I T O R
                Change System Parameters

Log changes to your Database? . . . . Y
Save Before & After Images? . . . . Y
Required entry for reason?. . . . Y

F3=Exit      Enter=Update security
```

A screen like above will allow you to change the parameters.

To log changes that are made to your database set the first parameter to Y. This will save the information that can be viewed with the DBALOG command. If you want to save “Before” and “After” images of the records that are changed, set the second parameter to Y. This will allow you to see exactly what data has been changed.

To require mandatory entry of a Reason Description when a record is either added, changed, or deleted the first time in an SFE session, type Y in the prompt field labeled “Required entry for reason?”. The user may enter up to 240 bytes of text to describe the reason why the file is being changed.

Chapter 7

Utilities Menu

Utilities Menu

Use this menu to control and view authorities to NetIQ Security Solutions for iSeries products and specific menus and options. You can also delete the installation library from this menu.

PC0	NetIQ Corporation	Date: 9/03/08
	PentaSafe Utilities	QPADEV000J Time: 11:54:07
Select one of the following:		
1 Authorize users to products		
2 Maintain Option Authorities		
3 VigilEnt Agent Access Control		
11 Display PSAudit authorized users		
12 Display PSSecure authorized users		
13 Display PSDetect authorized users		
14 Display PSCOMMON authorized users		
15 Display PSPrvMgr authorized users		
20 Install Evaluation Data		
Enter Option or Function/Type ==> _____		
F1=Help	F3=Exit	F6=Messages
F12=Previous	F13=Attention	F14=Batch Jobs
		F9=Window
		F10=Cmd Line
		F18=Reports

Option 1 Authorize Users to Products

This option will prompt for the users and products to be authorized. This option will run in batch.



User - Specify the user(s) to whom authority will be granted or revoked from. This is a required parameter.

Product - Specify the Product ID or *ALL.

Authority - Specify the Authority as either *GRANT or *REVOKE.

Authority Administrator - Specify whether the user will be an Authority Administrator. *YES means the user will be able to grant product authority to others. This option will run in batch.

Option 2 Maintain Option Authorities

Allows security maintenance of the authorities on the NetIQ Security Solutions for iSeries menus and options using the PSSecure Secure Menuing System (SMS).

AUTOMENU	PentaSafe Security Technologies Menu & Security Main Menu	CAS QPADEV0000U	Date: 6/21/00 Time: 11:24:32
----------	--	--------------------	---------------------------------

Select one of the following:

- 1 Applications Menu
- 2 Function/Options Menu
- 3 User Security & Administration
- 4 Audit Menu
- 5 Reports Menu
- 6 Select Other Application

Enter Option or Function/Type ==> _____

F1=Help	F3=Exit	F6=Messages	F9=Window	F10=Cmd Line
F12=Previous	F13=Attention	F14=Batch Jobs	F18=Reports	

Following is a sample scenario in which the objectives are:

- Grant USER01 access only to:
- System Auditing and Reporting Menu, Options 2, 3, and 4
- Objects Report Menu, all options
- File/Member Reports Menu, all options
- Library Reports Menu, all options
- Baseline Analysis
- Grant USER02 full access to all menus and options.

To accomplish the objectives above:

1. From the Product Access Menu (PSMENU), select Option 70 (Utilities menu).
2. From the Utilities Menu, select Option 2 (Maintain Option Authorities).
3. If USER01 is not set up in SMS:
 - a. Select Option 3 (User Security & Administration) from the “Menu & Security Main Menu”.
 - b. Select Option 1 (Work With Users) from the “User Security & Administration” menu.
 - c. Scroll through the list of users to confirm whether USER01 is set-up.

If it is not set up, select function key **F8** (Add) to add the user.

Note

The user must be a valid *USRPRF.

For this exercise, type the User Name, leave Group Profile= blank, Special Authority = *NO, Default Appl/Func/Type = PC/PSMENU/*MNU respectively. If it is set up, select Option 1, then verify the parameters are as specified above.

- d. Return to the “Menu & Security main Menu” by pressing **F12** (Previous).
4. From the Menu & Security Main Menu, select Option 6 (Select Other Application).
5. Select application code “PA” (PSAudit) and press **Enter**. The Menu & Security Main Menu is displayed next with application code “PA” shown in the upper left of the screen.

6. Activate security and authorization checks for the application “PSAudit”.

Note

When security and authorization checks are activated for an application, access authorities for all users of that application will need to be specified either at the user level (global) or at the specific menu/option levels. Unless access is explicitly authorized at either the user l

- a. Select Option 1 (Applications Menu) from the “Menu & Security Main Menu”.
 - b. Select Option 3 (Update Application) from the “Applications Menu”.
 - c. Specify *YES for the parameter “Check Authority” and press **Enter**.
 - d. Return to the “Menu & Security Main Menu” by pressing **F12** (Previous).
7. Grant USER01 access to the menus listed in the objectives.
- a. Select Option 2 (Function/Options Menu) from the “Menu & Security Main Menu”.
 - b. Select Option 2 (Work With Menus) from the “Function/Options Menu”.
 - c. From the “Work With Menus” screen select, one by one, all of the menus listed under the Function Code column by entering Option 1 (Select) by each of the function codes and pressing **Enter**. For each of the selected functions (menus) verify that the Check Authority parameter = *YES and the Public Authority parameter = *NO.

- d. Next, from the “Work With Menus” screen, select the following menus (listed under the Function Code column) by entering Option 9 (User Security), one by one, by each of the function codes and press **Enter**.)

PAOP	Audit Main Menu
PA1	System Auditing and Reporting
PA12	Object Reports Menu
PA121	More Object Authority Reports
PA13	File/Member Reports Menu
PA14	Library Reports Menu

- e. After selecting Option 9 for one of the menus listed above (7,d) and pressing **Enter**, the “Function User Authority List” will be displayed. Scroll through the list until you find USER01 and enter Option 1 (Grant Auth) next to it and press **Enter**. This will grant the user access to the menu. Press **F12** (Previous) to return to the “Work With Menus” screen. This must be repeated for each of the menus specified above (7,d).
8. Grant USER01 access to the options listed on each of the menus specified in (7,d).
- a. Return to the “Functions/Options Menu” by pressing **F12** (Previous).
 - b. Select Option 1 (Work With Cmds & Programs) from the “Functions/Options Menu”.
 - c. Find each menu option and enter Option 9 (User Security) next to it and press **Enter**. The “Function User Authority List” is displayed.
 - d. From the “Function User Authority List”, scroll through the list USER01 is found and enter Option 1 (Grant Auth) next to it and press **Enter**. This will grant the user access to the function/menu option. Press **F12** (Previous) to return to the “Work With Commands & Programs” screen.
 - e. Repeat steps 8C and 8D for each of the menu options/functions for which authority/access is to be granted.
9. Grant USER02 full access to all menus and options.

- a. Select Option 3 (User Security & Administration) from the “Menu & Security Main Menu”.
- b. Select Option 1 (Work With Users) from the “User Security & Administration” menu.
- c. Scroll through the list of users to confirm whether USER02 is set up.
If it is not set up, select function key F8 (Add), add the user.

Note

The user must be a valid *USRPRF.

For this exercise, enter the User Name, leave Group Profile = blank, Special Authority = *YES, Default Appl/Func/Type = PC/PSMENU/*MNU respectively. If it is set up, select Option 1, then verify the parameters as specified above.

Note

By specifying Special Authority = *YES for USER02, this will grant USER02 access/authority to all menus and options.

Option 3 VigilEnt Agent Access Control

The VigilEnt Security Agent Access Control is used to control access to the VigilEnt Security Agent by verifying the IP addresses of authorized host systems. To begin using the VigilEnt Security Agent Access Control, the appropriate IP addresses of authorized host systems must be specified using this option. By using this option, you can also edit or delete the IP addresses of existing authorized host systems.

The VigilEnt Security Agent Access Control enables applications such as Secure Configuration Manager and Security Manager to access data from an iSeries system.

Option 11 Display PSAudit authorized users

Presents the Authorization List Display, which shows a list of users that have authority to objects secured by the PSAUDIT authorization list, and the users' authorities. The public authority is also shown.

Option 12 Display PS Secure authorized users

Presents the Authorization List Display for PSSECURE.

Option 13 Display PSDetect authorized users

Presents the Authorization List Display for PSDETECT.

Option 14 Display PSCOMMON authorized users

Presents the Authorization List Display for PSCOMMON.

Other Utility Options

Save Spool File Utility

The primary purpose of this utility is to facilitate the transfer of large spool files from an iSeries to a PC so they can be included as attachments to e-mail for Technical Support.

Set Up

To prepare the utility for use, run the following command:

```
CALL PSCOMMON/PSSAVSPLFS
```

This program will:

- Create a data queue named PSSAVSPLF in library QGPL.
- Create an output queue named PSSAVSPLF in library QGPL.
- Add a directory entry (required by QDLS) for user running the Setup program.
- Create a folder named PENTASF and a subfolder named PSSPLF.
- Grant authority to the folder and subfolder using authorization list PSCOMMON.

Using The Save Spool File Utility

To use the save spool file utility:

1. Move the desired spool files to outque PSSAVSPLF.
2. The spool files must be in RDY status. Each time a spool file is changed to RDY status, it will get saved.
3. A maximum of 99 spool files can be processed at one time.
4. To convert the spool files to database members, run the following command:

```
PSCOMMON/PSSAVSPLF
```

The spool files will be saved to members in file QGPL/PSSAVSPLF.

5. To transfer the spool file database members to documents, run the following command:

```
PSCOMMON/PSTFRMBR
```

The spool file documents will be copied to folder PENTASF/PSSPLF in the QDLS file system.

The documents will have an extension of “.txt” and will be named as follows:

MCYDDDnn

- *M* = Literal ‘M’
- *C* = Century: 0=19xx, 1=20xx
- *Y* = Second digit of the Julian Year, such as 98
- *D* = Julian Day
- *n* = Sequence Number

Attaching Spool File Documents To an Email

Use the “Insert” feature of your email software to attach the desired spool file documents to your e-mail.

To attach spool file document to an email:

If using Microsoft Outlook:

1. Click on Insert
2. Click on File
3. Find and click Network Neighborhood
4. Find and double click the desired iSeries system (takes a few seconds)
5. Double click on QDLS
6. Double click on PENTASF
7. Double click on PSSPLF

8. Double click on the desired spool file document.

Tips

- A Web browser can also be used to view the spool files documents, as in the following example: `\\system.domain.com\QDLS\PENTASF\PSSPLF`
 - A spool file document can be copied to diskette using the “Quick copy” or “send to” feature by right-clicking on it in the browser’s list view.
-

Technical

Default values used by this utility are stored in data area PSCOMMON/PSSAVSPLF, which breaks down as follows:

- 01 - 10: Data queue
- 11 - 20: Data queue library
- 21 - 30: Output file
- 31 - 40: Output file library
- 41 - 43: Output file record length (132 or 198)
- 44 - 44: Delete spool file after saving to database member? Y/N
- 45 - 45: Remove database member after copying to folder? Y/N
- 46 - 95: Folder path
- 96 - 98: Document extension (txt)
- 99 - 100: Reserved for next mbr seq nbr
- 101 - 110: Output queue used by utility
- 111 - 120: Output queue library

You may change the data area values before running program PSCOMMON/PSSAVSPLFS. If spool files are unintentionally sent to the PSSAVSPLF outque, it is recommended that you delete the data queue (DLTDTAQ QGPL/PSSAVSPLF) and rerun the setup program. Program PSSAVSPLFS can be run as needed to recreate objects used by the utility, for example, if the PSSAVSPLF outque or data queue is deleted.

Removing Documents

The documents in the QDLS file system can be removed using either the “Network Neighborhood” on the PC or the Work with Folders (WRKFLR) command on the iSeries.

Using MS Windows Network Neighborhood:

See steps “d” through “h” under “Attaching Spool File Documents To an Email” on page 366, for more information. On the iSeries:

1. At a command entry line, type: WRKFLR PENTASF, press **Enter**.
2. Select Option 5 (Work with documents) for folder PSSPLF, press **Enter**.
3. Select all documents with Option 4 (Delete), press **Enter**, and press **Enter** again at the confirmation prompt.
4. Press **F3** (exit) as necessary until you return to the command entry line.

Creating A Batch Subsystem

Command PSWORK can be used to create or delete a batch subsystem named PSWORK in library PSCOMMON. The related objects of type *CLS and *JOBQ are also named PSWORK.

The subsystem can be used to run any batch job.

Examples:

```
PSWORK ACTION(*CRT)
```

The above command creates the subsystem.

```
PSWORK ACTION(*DLT)
```

The above command deletes the subsystem.

Index

Symbols

*POPUP 11
*PULLDOWN 11
*STD1 11
*STD2 11

Numerics

99 Mass User Load & Delete 101
 User Delete 102
 User Load 102

A

About xii
Access Codes
 Enter Access Codes 3
Accessing the Password Screen From Your
 Menus 219
Act Bar/Menu Code 65
Action Bar Demo - Oper. Application 30
Action Bar Options Update 75
Action Bar Update 73

Action Bars 126
Activity Audit 17
 Audit 17
Add a Workstation 283
Add Job Parameters 41
Add User Profile Exit Programs 165
Add User to Profile Template Authority 198
APPL 21
APPL Parameter 21
Application 15
Application Browse 28
Application by Code 113
Application Code 34, 36
Application Description 36
Application Level Authority 37, 54
Application Update 34, 36
Applications
 Descriptions 8
Applications Menu 32
 Create New Application 34
 Select Other Application 35
 Update Application 36
 Work With Job Parameters 39

- Archived Profiles Report 153
- AS/400 Considerations 237
- AS/400 Password System Values 213
- Audit 17
 - Audit Activity 38, 53
 - Audit Activity by Date 131
 - Audit Activity by Function 133
 - Audit Activity by User 132
 - Audit Menu 106
 - Audit Reports Menu 112
 - View Audit Activity 107
 - Audit Reports Menu 112, 129
 - Audit Activity by Date 131
 - Audit Activity by Function 133
 - Audit Activity by User 132
 - Clear Audit Activity 112
 - Auth List Details Update 99
 - Function Authority 100
 - User 100
 - Auth List Header Update 98
 - Authorization List Code 98
 - Authorization List Description 98
 - Public Authority 98
 - Auth Lists 16
 - Auth Lists by User 117
 - Authorization List Code 55
 - Auto Generate and Print Passwords 226
 - Forms Information 228
 - Job Information 228
 - Notification of Password Change Report 229
 - Report Layout 229
 - Fields 229
 - Text Options 227
 - User, Generic, All, or Group Files 227

C

- Change Defaults (DISABLE DELETE +) 146
- Change Profiles to Use Genned Pwds 231
- Change User Exclusions 215, 233
- Change User Profile Based on Template 200
- Change Workstation Exclusions 283
- Change Your Password 217
- Check Authority 37, 54
- Clean Up User Profiles 144
 - User Profile Management 144
- Clear Audit Activity 112
- Commands & Programs 125
- Commands & Programs Browse 49
- Concepts Overview 7
- Create a Profile Based On Template 199
- Create Action Bar 71
- Create Auth List 97
 - Authorization List Code 97
- Create Cmd/Pgm 50
- Create Company Code 104
- Create Function Key Group 77
- Create Menu 63
- Create New Application 25, 34
 - Application Code 34
 - Application Update 34
- Create User 87
- Create/Change User Profile Template 184

D

- Date and Time Formats 14
- Default Function Code 38, 56
- Default Function Type 39, 57

- Default Menu 24
 - Action Bar Demonstration 25
 - Create New Application 24
 - Process Application 24
 - Work With Application Definitions 25
 - Work With User Security & Administration 25
 - Defaults For System Generated Passwords 234
 - Forms Information 236
 - Job Information 235
 - Mask for System Generated Passwords 235
 - Test PentaSafe System Generated Passwords 236
 - Testing Random Generated Passwords 237
 - Text Options 235
 - Defaults for System Generated Passwords
 - Forms Tip 236
 - Defaults For User Prompted Passwords 220
 - Disallow Adjacent Characters 221
 - Disallow Repeating Characters 222
 - Disallow Vowels 221
 - Display the Security Screen 222
 - Mask for User Prompted Passwords 220
 - Maximum Length 221
 - Number of Days 221
 - Number of Levels 221
 - Prevent Similar Passwords 222
 - Screen Title and Text 222
 - Delete Job Parameters 46
 - Dflts & Info for PS DSCJOB/SIGNOFF 305
 - Active Line Description 311
 - Group Jobs Considerations 309
 - PC Routers and Communication
 - Jobs 310
 - Setup 309
 - Display ISM Statistics 313
 - Display Non-Authorized Options 37
 - Display Profiles Pending Pwd Change 230
 - Display/Change Controller Exclusions 312
 - Display/Change Program Exclusions 292
 - Display/Change System Parameters 293
 - Maintain Inactive Session Monitor Messages 300
 - Maintain Inactive Session Monitor Timing 298
 - System Parameters Outside Of Inactive Session Monitor 301
 - Display/Change User Profile Exclusions 288
 - Distributed Systems 156
- ## E
- Edit User Profile Template Authority 196
 - Example STRMS Commands 22
 - Exit Program 39
 - Exit Program Library 39
- ## F
- Fast-Path Selection 11
 - Function Name and Type 12
 - Multiple Option Numbers 12
 - Func Keys by Group 128
 - Function & Menu Reports 83, 122
 - Action Bars 126
 - Commands & Programs 125
 - Func Keys by Group 128
 - Function by Code 124
 - Function Help Text 129
 - Functions Assigned to FKY 128
 - Functions by Menu 127
 - Functions by Type 125

- Menus 126
 - Options by Menu 127
- Function Authority 16
- Function Authority Update 58
- Function Authorization 118
- Function by Code 124
- Function Code 63
- Function Command Parameter 57
- Function Description 39
- Function Help Text 129
- Function Key Group
 - Application Code 80
 - Function Code 81
 - Function Key 80
 - Function Key Description 80
 - Function Type Code 81
 - Process Type Code 81
- Function Key Group Update
 - Color 78
 - Delete Function Key Group 79
 - Function Key Group 78, 80
 - Group Description 78
 - High Intensity 79
 - Reverse Image 79
 - Underline 79
- Function Keys for Detail Screens 186
- Function Level Authority 37, 54
- FUNCTION Parameter 21
- Function Type Code 51, 63
- Function Update 52
- Function/Option Update
 - Menu Update 65

- Function/Options Menu
 - Create Menu 63
 - Function & Menu Reports 83
 - Function Code 63
 - Function Type Code 63
 - Function Update 64
 - Work With Action Bars 69
 - Work With Cmds & Programs 48
 - Work With Function Keys 76
 - Work With Help Text 81
 - Work With Menus 61
- Function/Options Update
 - Menu Options Update 68
- Functions
 - Description 9
 - Function Types 9
 - Process Types 10
- Functions by Menu 127
- Functions by Type 125
- Functions/Options Menu 48

G

- General Topics 19
 - Help Text 19
 - Reporting 19
 - Viewing Options 19
- Generate and Display a Password for One User 225
- Group Job Control 105

Group Job Processing 18
Group Profile 16, 88

H

Help Text 19
Help Text Update 61
High Intensity 67
Hold on Job Queue 46
Horizontal Character 67

I

Inactive Session Monitor 279
 Change Workstation Exclusions 283
 Dflts & Info for PS DSCJOB/
 SIGNOFF 305
 Display ISM Statistics 313
 Display/Change Controller
 Exclusions 312
 Display/Change Program Exclusions 292
 Display/Change System Parameters 293
 Display/Change User Profile
 Exclusions 288
 Function 280
 Introduction 279
 Main Menu 281
 Start Inactive Session Monitor 282
 Stop Inactive Session Monitor 282
 Timeout Log Report 303
 Report Layout 303, 304
 Work with ZASBS Subsystem Jobs 314
Inactive Session Monitor Menu Display 281
Initial Library List 44
Initial Program Install 224

Installation Defaults Update 104
 Check for Mail 106
 Display Exit Message 105
 Group Job Control 105
 Use LDA for Company 105

J

Job Description Library 43
Job Environment 17
 Group Job Processing 18
 Overview 17
Job Parameters Browse 40
Job Parameters Code 36, 41, 55
Job Parameters Description 36, 42
Job Parameters Update 42
Job Priority 43
JOB Queue 43
JOBQ Library 43

L

Library List Update 47
Library Name 47
Library Sequence 47
LIST 21
Load New User Profiles 144

M

Maintain Inactive Session Monitor
 Messages 300
Maintain Inactive Session Monitor
 Timing 298
 Timing for workstations and User
 Profiles 299
Maintain Permissible Values 176
 Maintain User Profile Parameters

- screen 178
- Parameter Permissible Values Detail Screen 181
- Parameter Permissible Values Selection Prompt 179
- Maintain User Profile Templates 182
 - Create/Change User Profile Template 184
 - Function Keys for Detail Screen 186
 - User Profile Template Detail Screens 185
- Mask for System Generated Passwords 235
- Mask for User Prompted Passwords 220
- Menu & Security Concepts 7
 - Concepts Overview 7
- Menu & Security Default Menu 23
 - Default Menu 24
- Menu & Security Limitations 20
 - System Limits 20
- Menu Hierarchy Report 121
- Menu Option Update
 - Function Code 68
 - Function Description 69
 - Function Type Code 69
- Menu Options Update 68
 - Menu Option Sequence 68
- Menu Types 11
 - *ACTBAR 11
 - *POPUP 11
 - *PULLDOWN 11
 - *STD1 11

- *STD2 11
- Menu Update
 - Color 66
 - Delete Menu 67
 - Function Key Group 66
 - High Intensity 67
 - Horizontal Character 67
 - Menu Type Code 66
 - Menu Type Description 66
 - Reverse Image 67
 - Underline 67
 - Vertical Character 67
- Menus
 - Date and Time Formats 14
 - Fast-Path Selection 11
 - Function Keys 12
 - Menu Types 10, 11
 - Option Selection 11
 - Panel Options 15
 - User Defined Function Keys 14
- Menus by Function 60
- Message Queue 46
- MS Main Menu 31
 - Applications Menu 31
 - Audit Menu 32
 - Functions/Options Menu 31
 - Reports Menu 32
 - Select Other Application 32
 - User Security & Administration 32
- MSGQ Library 46

N

Notification of Password Change Report 229

O

Option Selection 11

Options by Menu 127

Output Priority 43

Output Queue 45

OUTQ Library 45

P

Panel Options 15

Password Security Screen 218

Password, New 219

PC Routers and Communication Jobs 310

PC Software 238

PentaSafe System Generated Passwords

Menu 225

Auto Generate and Print Passwords 226

Change Profiles to Use Genned Pwds 231

Defaults For System Generated

Passwords 234

Display Profiles Pending Pwd

Change 230

Generate and Display a Password for One

User 225

Users To Exclude From Password

Generation 233

PentaSafe User Prompted Passwords Menu

About User Prompted Passwords 222

Defaults For User Prompted

Passwords 220

Initial Program Install 224

Routing Entry Install 223

Test User Prompted Passwords 217

Users to Exclude From Password

Prompting 214

Permissible Values 192

Permissible Values Entry Window 192

Permissible Values Selection Window 194

PPM General Options Menu 138

Change Defaults (DISABLE DELETE
+) 146

Clean Up User Profiles 144

Load New User Profiles 144

Reactivate Profile From Archive 145

Report of Users 143

Report Layout 144

User Profile Exclusions 152

Work With User Profiles 139

PPM General Options Report

Archived Profiles Report 153

Print Device 45

procedure

See how to

Procedures for Installation 6

Libraries 6

Process Type Code 53

Product Access 2

Enter Access Codes 3

How to Use a Menu 2

PSSecure 3

Signoff 4

Software Appl Mods 3

Utilities Menu 3

Product Installation and Upgrade 1

Introduction 1

Product Access 2

Profile & Password Management 135

AS/400 Password System Values 213

Function 136

Main Menu 137

General Options Menu 138

- PentaSafe System Generated Passwords Menu 225
- PentaSafe User Prompted Passwords Menu 214
- Profile Synchronizer Menu 154
- Profile Templates Menu 175
- System Overview 135
- Profile and Password Management and the OS 237
 - AS/400 Considerations 237
 - PC Software 238
 - Profile Synchronizer 238
 - System Values 237
- Profile Distribution Report 159
- Profile Synchronizer 238
- Profile Synchronizer Defaults 160
 - History Retention Days. 161
 - Jobq/Library for synchronizer jobs 161
 - Mode Description Name for Pass-thru 161
- Receive and Apply Password Changes 160
- Receive and Apply Profile CHanges 160
- Send Password Changes 161
- Send User Profile Changes 160
- Profile Synchronizer Installation 164
- Profile Synchronizer Menu 154
 - Add User Profile Exit Programs 165
 - Profile Distribution Report 159
 - Profile Synchronizer Defaults 160
 - Profile Synchronizer Installation 164
 - Profile Synchronizer Uninstall 164
 - Profiles To Exclude 155
 - Purge Synchronizer Messages 163
 - Remove User Profile Exit Programs 165
 - Synchronizer Debugging Options 163
 - Test Distribution of Profile Change 161

- Profile Synchronizer Uninstall 164
- Profile Templates Menu 175
 - Change User Profile Based on Template 200–??
 - Create a Profile Based On Template 199
 - Maintain Permissible Values 176
 - Maintain User Profile Templates 182
- Profiles To Exclude 155
- Public Authority 55, 95
- Purge Synchronizer Messages 163

R

- Reactivate Profile From Archive 145
- Reclaim Resources 55
- Remove User Profile Exit Programs 165
- Report of Users 143
- Reporting 19
- Reports Menu 113
 - Application by Code 113
 - Audit Reports Menu 129
 - Function & Menu Reports 122
 - User/Security Reports 114
- Routing Entry Install 223

S

- Secure Menuing System 5
 - Action Bar Demo - Oper. Application 30
 - Activity Audit 17
 - Applications 8
 - Applications Menu 32
 - Audit Menu 106
 - Create New Application 25
 - Example STRMS Commands 22
 - Features 5
 - Function/Options Menu 48
 - Functions 9

- Job Environment 17
- Menu & Security Concepts 7
- Menu & Security Default Menu 23
- Menu & Security Limitations 20
- Menus 10
- MS Main Menu 31
- Procedures for Installation 6
- Reports Menu 113
- Security 15
 - Select Other Application 133
 - Starting Menu & Security 20
 - STRMENU 23
 - User Security & Administration 29, 84
 - work With Application Definitions 27
- Secure Menuing system
 - General Topics 19
- Security 15
 - Application 15
 - Auth Lists 16
 - Function Authority 16
 - Group Profile 16
 - Special Function Authority 17
 - User 16
- Select Other Application 35
 - Function Keys 35
- Special Auth by User 118
- Special Authority 89
- Special Function Authority 17
- Start Inactive Session Monitor 282
- Starting Menu & Security 20
 - FUNCTION Parameter 21
 - TYPE Parameter 21
- Starting menu & Security
 - APPL Parameter 21

- Start-Up Program 39
- Start-Up Program Library 39
- Stop Inactive Session Monitor 282
- STRMENU 23
- STRMS Command 20
- STRMS Commands
 - Example STRMS Commands 22
 - Examples 22
- Synchronizer Debugging Options 163
- System 135
- System Library List 44
- System Limits 20
- System Parameters Outside Of Inactive
 - Session Monitor 301
- System Values 237

T

- task
 - See how to
- Test Distribution of Profile Change 161
- Test User Prompted Passwords 217
 - Accessing the Password Screen From Your
 - Menus 219
 - Change Your Password 217
 - New Passwords 219
 - Password Security Screen 218
- Timeout Log Report 303
- TYPE Parameter 21

U

- Update Application 36
 - Application Code 36
 - Application Description 36
 - Application Level Authority 37
 - Application Update 36
 - Audit Activity 38

- Check Authority 37
- Default Function Code 38
- Default Function Type 39
- Delete Application 39
- Display Non-Authorized Options 37
- Exit Program 39
- Exit Program Library 39
- Function Description 39
- Function Level Authority 37
- function Level Authority 37
- Job Parameters Code 36
- Job Parameters Description 36
- Start-Up Program 39
- Start-Up Program Library 39
- USER 21
- User 16, 88
- User Authority Browse
 - Function Keys 87
- User Authority Update 88
 - Audit Activity 89
 - Default Application, Function, Type 89
 - Default Company 89
 - Display Date Format 90
 - Function Keys 90
 - Special Authority 89
- User Authorization Lists 117
- User Authorization Report 119
- User Defined Function Keys 14
- User List 116
- User Load 102
- User Profile Exclusions 152
- User Profile Management 144
- User Profile Template Detail Screens 185
 - Add User to Profile Template
 - Authority 198
 - Edit User Profile Template Authority 196

- Permissible Values 192
- Permissible Values Entry Window 192
- User Profile Templates Detail Screens
 - Permissible Values Selection
 - Window 194
- User Security & Administration 29, 84
 - 99 Mass User Load & Delete 101
 - Installation Defaults Update 104
 - User/Security Reports 100
 - Work With Auth Lists 95
 - Work With Companies 102
 - Work With Users 85
- User/Security Reports 100, 114
 - Auth Lists by User 117
 - Function Authorization 118
 - Menu Hierarchy Report 121
 - Special Auth by User 118
 - User Authorization Lists 117
 - User Authorization Report 119
 - User List 116
 - Users by Group Profile 116
- Users To Exclude From Password
 - Generation 233
 - Change User Exclusions 233
- Users to Exclude From Password
 - Prompting 214
 - Change User Exclusions 215

V

- View Audit Activity 107
 - Audit Activity by Function 111
 - Audit Activity by User 109
 - View Audit Activity by Date 108
- Viewing Options 19

W

- Work With Action Bars 69
 - Action ar Options Update 75
 - Action Bar Browse 70
 - Action Bar Update 73
 - Create Action Bar 71
 - Delete Action Bar 72
 - Exit Program 74
 - Exit Program Library 74
 - Function Code 71
 - Function Type Code 75
 - Function Update 72
 - Start-Up Program 74
 - Start-Up Program Library 74
- Work With Application Definitions 27
 - Application Browse 28
- Work With Auth Lists 95
 - Auth List Details Update 99
 - Auth List Header Update 98
 - Create Auth List 97
- Work With Cmds & Programs 48, 55
 - Application Level Authority 54
 - Audit Activity 53
 - Authorization List Code 55
 - Check Authority 54
 - Commands & Programs Browse 49
 - Confirmation Screen 53
 - Create Cmd/Pgm 50
 - Default Application Code 56
 - Default Function Type 57
 - Function Authority Update 58
 - Function Code 51, 52
 - function Command Parameter 57
 - Function Description 52
 - Function Level Authority 54
 - Function Type Code 51
 - Function Update 52
 - Help Text Update 61
 - Job Parameters Code 55
 - Job Parameters Description 55
 - Job Prompt 56
 - Job Prompt Program & Library 56
 - Menus by Function 60
 - Password 53
 - Process Type Code 53
 - Public Authority 55
- Work With Companies 102
 - Create Company Code 104
- Work With Function Keys 76
 - Create Function Key Group 77
 - Function Key Group 77
 - Function Key Group Browse 76
 - Function Key Group Update 78
- Work With Help Text 81
 - Help Text Browse 82
 - Help Text Update 83
- Work With Job Parameters 39
 - Add Job Parameters 41
 - Current Library 44
 - Delete Job Parameters 46
 - Function Keys 40, 41
 - Hold on Job Queue 46
 - Initial Library List 44
 - Job Description 42
 - Job Description Library 43
 - Job Parameters Browse 40
 - Job Parameters Code 41, 42
 - Job Parameters Description 42
 - Job Parameters Update 42
 - Job Priority 43
 - JOB Queue 43
 - JOBQ Library 43
 - Library List Update 47
 - Library Name 47
 - Library Sequence 47
 - Message Queue 46
 - MSGQ Library 46

Output Priority	43	User	88
Output Queue	45	User Authority Browse	86
OUTQ Library	45	User Authority Update	88
Print Device	45	Work with ZASBS Subsystem Jobs	314
System Library List	44	Inactive Session Monitor And The AS/	
Work With Menus	61	400 Operating System	315
Menu Browse	62	Performance Enhancement	315
Work With User Profiles	139	Testing	314
Work With Users	85		
Create User	87		