Password Reset™

The Password Management Component of

iSecurity

User Manual
Version 04

RAZ-LEE

Updated: November 11, 2015

Copyright Notice

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

Record your Product Authorization Code Here:

Computer Model:	
Serial Number:	
Authorization Code:	

About this Manual

Who Should Read This Book

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

Product Documentation Overview

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal System i experience. The documentation package includes a variety of materials to get you up to speed with this software quickly and effectively. We hope you find this user manual informative; your feedback is important to us. Please send your comments about this user manual to docs@razlee.com.

Printed Materials

This user manual is the only printed documentation necessary for understanding Password It is available in user-friendly PDF format and may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: http://www.adobe.com/.

Typography Conventions

- Menu options, field names, screen names, and function key names are in **Bold**.
- References to chapters or sections are written in *Italic*.
- IBM i (OS/400) system messages are in ***Bold Italic***.
- IBM i (OS/400) commands are in `New Courier`.
- Key combinations are separated by a dash, for example: **Shift-Tab**.

Table of Contents

Password Reset Overview

One of the biggest time wasters for any organization is password resetting. Various surveys suggest that the time lost for this is up to 40 minutes for each password and that as many as 50% of the help desk calls are for password resets.

Organizations addressing the sensitive issue of how to best manage System i user passwords can now enable their users to reset their own passwords with minimal effort or exposure. **Password Reset**, part of the iSecurity suite, allows users to verify themselves after composing personal questions with answers that only they know.

This unique and reliable solution allows a help desk to automatically assist users, without compromising either security or the efficiency of procedures.

Password Reset is simple to use and administer by all relevant personnel: users, system administrators, and help desk staff. It enables an enterprise to introduce first time use of a straightforward password control mechanism into the organization with minimum overhead, while ensuring that a user's password is not known to anyone except the user.

After a user creates a password profile for self-authentication, which can be edited at any time, the user can reset the password alone or request assistance from the help desk. In the event that a user has forgotten a password when trying to login, the user simply enters FORGOT in the User field and PASSWORD in the Password field. This triggers the self-authentication process that the user set up in advance - personal questions and responses that are also case sensitive.

Control the type and number of challenge questions asked, in addition to the number of reset attempts allowed, all based on your organization's security policy. Unsuccessful attempts to reset passwords trigger automatic notification to the relevant security personnel. Challenge questions discourage fraudulent reset requests and users can set their own default reset password—known only to themselves—which adds another layer of security.

The entire issue can be resolved in minutes and without the help desk, saving the company both valuable time and resources.

Feature	How does it help me
Integrates with other iSecurity products	You can seamlessly add **Password Reset** to your iSecurity suite and get all the benefits of a full audit trail, triggered actions, and so on.
Password templates	Users can be assigned to a specific password template that ensures that all users who need the same type of access have the same level of password security.
Password generation	The passwords that are generated comply with your organization's password policy.
Password Reset classes	Password Reset classes allow you to have different verification policies for different groups of users.
Multi-system	A single reset action allows users to reset their password on all System i systems to which they have access.
Multi-lingual	You can define different languages for different users.
Always available	**Password Reset** is always available for your users, even during non-standard working hours (late nights, weekends, and so on).

Other iSecurity Products

	**Action** intercepts security breaches and other events in real-time and immediately takes appropriate corrective action. Actions may include sending alert messages to key personnel and/or running command scripts or programs that take corrective steps. No effective security policy is complete without **Action**.
	**Anti-Virus** provides virus detection and prevention. Anti-Virus scans, validates, and checks IFS files as they are enrolled or modified, authenticates them, and erases/quarantines infected files. Includes updateable database and simple interface.
	**AP-Journal** automatically manages database changes by documenting and reporting exceptions made to the database journal.
	**Assessment** checks your ports, sign-on attributes, user privileges, passwords, terminals, and more. Results are instantly provided, with a score of your current network security status with its present policy compared to the network if iSecurity were in place.
	**Audit** is a security auditing solution that monitors System i events in real-time. It includes a powerful query generator plus a large number of predefined reports. Audit triggers customized responses to threats via the integrated script processor contained in Action.
	**Authority on Demand** (AOD) provides an advanced solution for emergency access to critical application data and processes, which is one of the most common security slips in System i (IBM i) audits. Current manual approaches to such situations are not only error-prone, but do not comply with regulations and often stringent auditor security requirements.
	**Capture** silently captures and documents user screens for tracking and monitoring – without any effects on system performance. Capture can run in playback mode and can be used to search within texts. It also preserves job logs for subsequent review. Screen captures can be according to user name, IP address, time of day, and more.
	**Change Tracker** automatically tracks modifications in the software and file structure within production libraries. Changes are tracked at both the object and source levels. It does not require any special actions by programmers.
	**Command** monitors and filters commands and their parameters before they are run, enabling you to control each parameter, qualifier or element, in conjunction with the context in which it is about to run. Options include Allow with Changes, and Reject. It includes a comprehensive log, proactive alerting and easily integrates with SIEM.
	**DB-Gate** empowers IBM i customers with exciting data access capabilities, based on Open database Connectivity (ODBC), employing standard IBM i facilities to enable full database-transparent access to remote systems.

	**Firewall** protects and secures all types of access, to and from the System i, within or outside the organization, under all types of communication protocols. Firewall manages user profile status, secures entry via predefined entry points, and profiles activity by time. Its Best Fit Algorithm decreases system burden with no security compromise.
	**Password** is a general-purpose password management product that ensures user passwords cannot be easily guessed or cracked. Password allows you to manage a variety of password security parameters and maintains a history log of attempts to create passwords. This log can easily be displayed or printed.
	**Screen** protects unattended terminals and PC workstations from unauthorized use. It provides adjustable, terminal- and user-specific time-out capabilities. Screen locking and signoff periods may be defined according to variable criteria such as date, time of day or user profile.
	**View** is a unique, patent-pending, field-level solution that hides sensitive fields and records from restricted users. This innovative solution hides credit card numbers, customer names, and so on. Restricted users see asterisks or zeroes instead of real values. View requires no modification to existing applications.
	**Visualizer** is an advanced data warehouse statistical tool with state-of-the-art technology. It provides security-related analysis in GUI and operates on summarized files; hence, it gives immediate answers regardless of the security data amount being accumulated.

Getting Started

This section describes the first steps you need to take when you start working with **Password Reset**, as well as listing the standard field names, option s and command keys used in the product.

Standard Fields, Options, and Command Keys

All standard fields, options and command keys are described in the table below. However, some standard command keys are not documented here as they need to have links in their description in each specific UI (for example, F6).

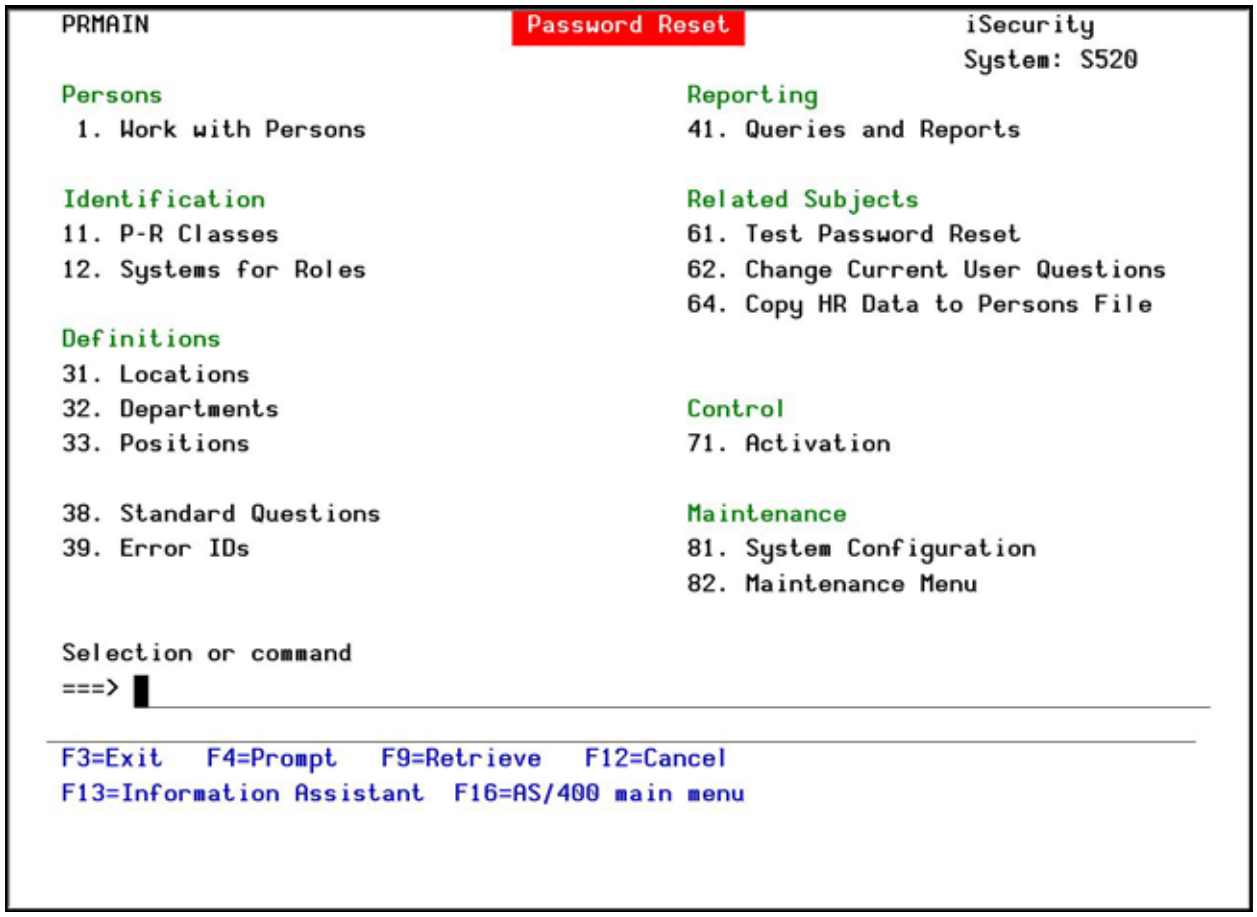
Field/Option/Command Key	Description
Library	Library name. Depending on the context, you may need to enter a specific Library Name, a generic Library Name (for example, ABC*), or you may also be allowed to enter *ALL.
Opt	The option you want to use on the selected item from the list. Put the cursor on the **Opt** field in the appropriate row and then either type the required option in the field or click on the required option in the list of options at the top of the screen.
Subset	Limits the list being displayed to only those members of the list whose value contains the value in the subset field. Use the **Subset** field to make it easier to access the specific value you are searching for.
F3=Exit	Exits from the current display or option, and returns to the calling display. In most cases, any information you have added or changed on the current display is discarded.
F4=Prompt	Displays a prompt window containing additional information about the current input prompt, usually in the form of a list. You may be able to choose any value from this list by typing 1 in the Opt prompt next to the value you want to use. Prompt is context-sensitive. You need to position the cursor on the input prompt to which the information applies before you press **F4**.
F12=Cancel	Exits from the current display or option, and returns to the previous display. Any information you have added or changed on the current display is discarded.
1=Select	Displays the selected item in a list in a screen that allows you to modify the selected item.
3=Copy	Displays a screen that allows you to copy the selected item. You will be able to change the major identifier of the item. You will then the need to select the new item to make all other necessary changes.
4=Delete	Deletes the selected item in a list. You may be asked to confirm your choice before the delete operation is performed.

Accessing Password Reset

You access all **Password Reset** functionality through the **Password Reset** main menu.

To access the system:

- Type `strpwdrst` in the command line and press **Enter**. The **Password Reset** Main Menu appears.



Password Reset Main Menu

Field/Option/Command Key	Description
1. Work with Persons	Opens the **Work with Persons for Password-Reset** screen, where you define and modify User definitions.
11. P-R Classes	Opens the **Work with P-R Classes** screen, where you see a list of available classes.
12. Systems for Roles	Opens the **Work with Systems for Roles** screen, where you can define which systems can be worked on by which Roles.
31. Locations	Opens the **Work with Locations** screen, where you can define the locations of your organization.
32. Departments	Opens the **Work with Departments** screen, where you can define the departments of your organization.
33. Positions	Opens the **Work with Positions** screen, where you can define the positions of your organization.

Field/Option/Command Key	Description
38. Standard Questions	Opens the **Work with Standard Questions** screen, where you can define the standard questions which will be asked for verification.
39. Error IDs	Opens the **Display Message Descriptions** screen to show detailed descriptions of the errors that users may encounter when resetting their passwords.
41. Queries and Reports	Opens the **Queries Menu**, from which you can run the various Password Reset queries and reports.
61. Test Password Reset	Opens the **Test Password Reset** screen, where you can verify that a given person will be able to use the Reset Password self-service functionality.
62. Change Current User Questions	Opens the **Change P-R Questions** screen to allow users to change their own private identification questions.
64. Copy HR Data to Persons File	Opens the **Copy Persons Info From Existing Files** screen, where you can define and control the mapping of the organization's files to the **Password Reset** Person file.
71. Activation	Opens the **Activation** menu, from which you define under which circumstances the system activates the product.
81. System Configuration	Opens the **System Configuration** menu, where you can configure the product and its relationship with other iSecurity products.
82. Maintenance Menu	Opens the **Maintenance** menu, where you can set internal product definitions.

Initial Setup

Before you can work with **Password Reset**, you must ensure that all your staff members are correctly entered to the product database. Use the following workflow to do that:

1. Set up system and control definitions, using the **System Configuration** options.
2. Set up all the information relating to the structure of the organization, using the **Definitions** and **Identification** options.
3. Set up your Users, using the **Persons** options.
4. Set up the special user for **Password Reset**, using the **Create Special User FORGOTyyy** option.

For a more detailed quick guide to initial setup, see the *Password Reset Out of the Box* document.

Working with Password Reset

This section describes all the tasks that you can perform in **Password Reset**. The tasks are described in the order they appear in the **Password Reset** main menu.

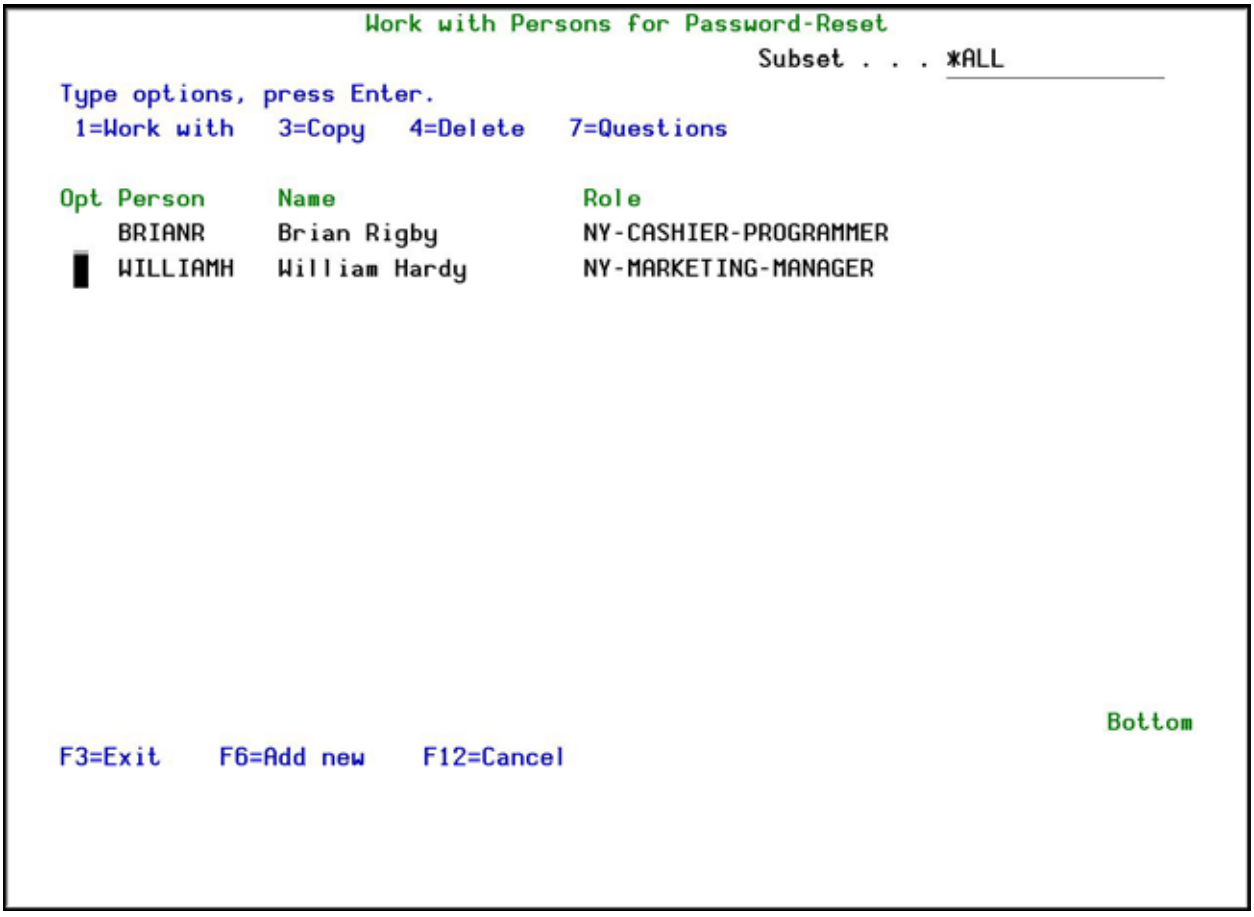
Persons

The Person is the unique ID with which a user is identified to the **Password Reset** system. Usually the Person is the same as the User ID (User Profile) assigned to the user. However, there may be situations where many users are all assigned to the same User ID (for example, when there is a departmental User Profile). There may also be situations where a user is assigned to many User IDs (for example, when company policy requires different IDs for different computers).

Create a New Person

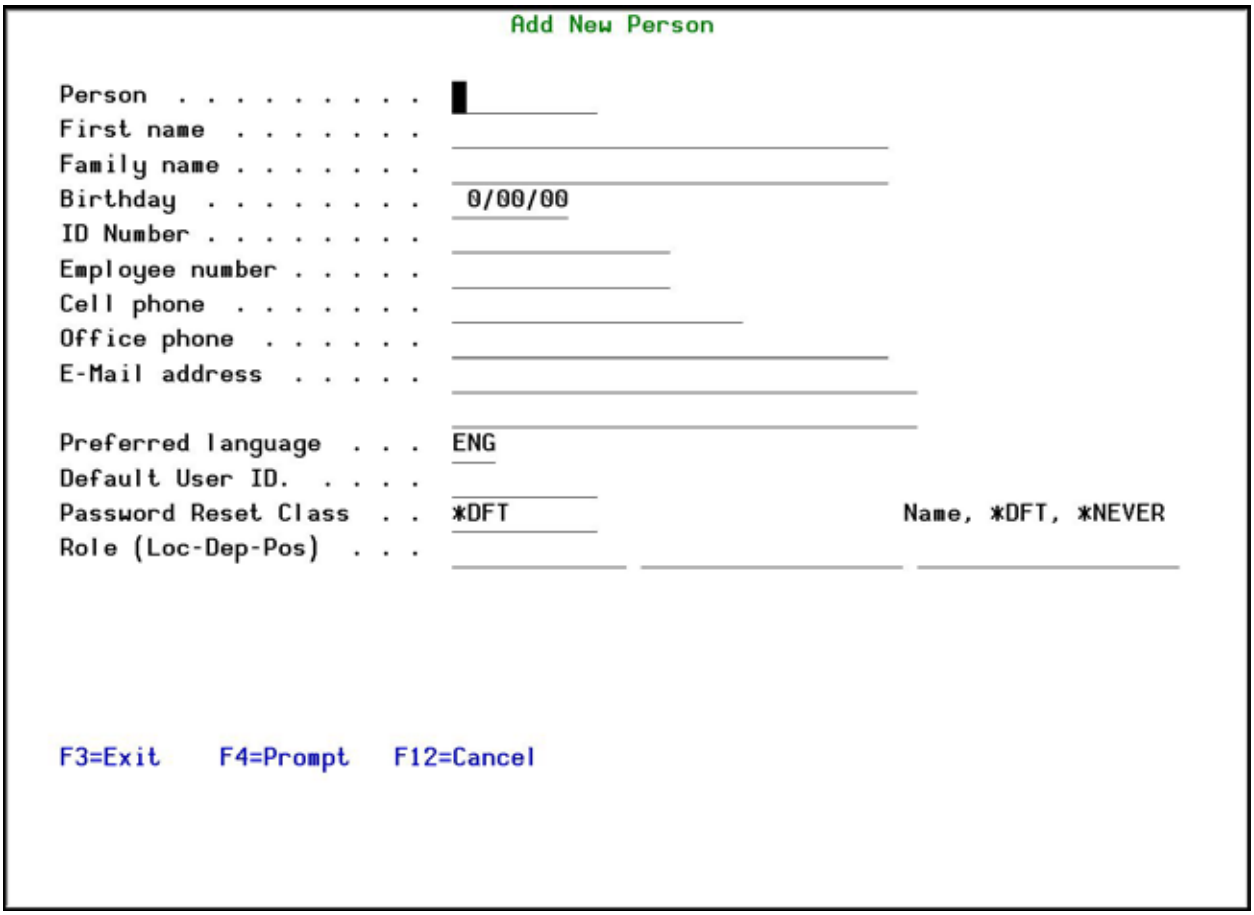
To add persons:

1. Select **1. Work with Persons** in the **Password Reset** main menu. The **Work with Persons for Password-Reset** screen appears.



Work with Persons for Password-Reset screen

2. Press **F6=Add new**. The **Add New Person** screen appears.



Add New Person screen

Field/Option/Command Key	Description
Person	The unique identifier of the Person.
First name	The first name of the Person.
Family name	The family name or surname of the Person.
Birthday	The birthday of the Person – can be used for the unique identification of the Person.
ID Number	The national ID number of the person – can be used for the unique identification of the Person.
Employee number	The employee number of the Person within the organization - can be used for the unique identification of the Person.
Cell phone	The cell phone number of the Person – can be used for the unique identification of the Person. Can also be used to send notification of a new password.
Office phone	The office phone number of the Person – can be used for the unique identification of the Person.

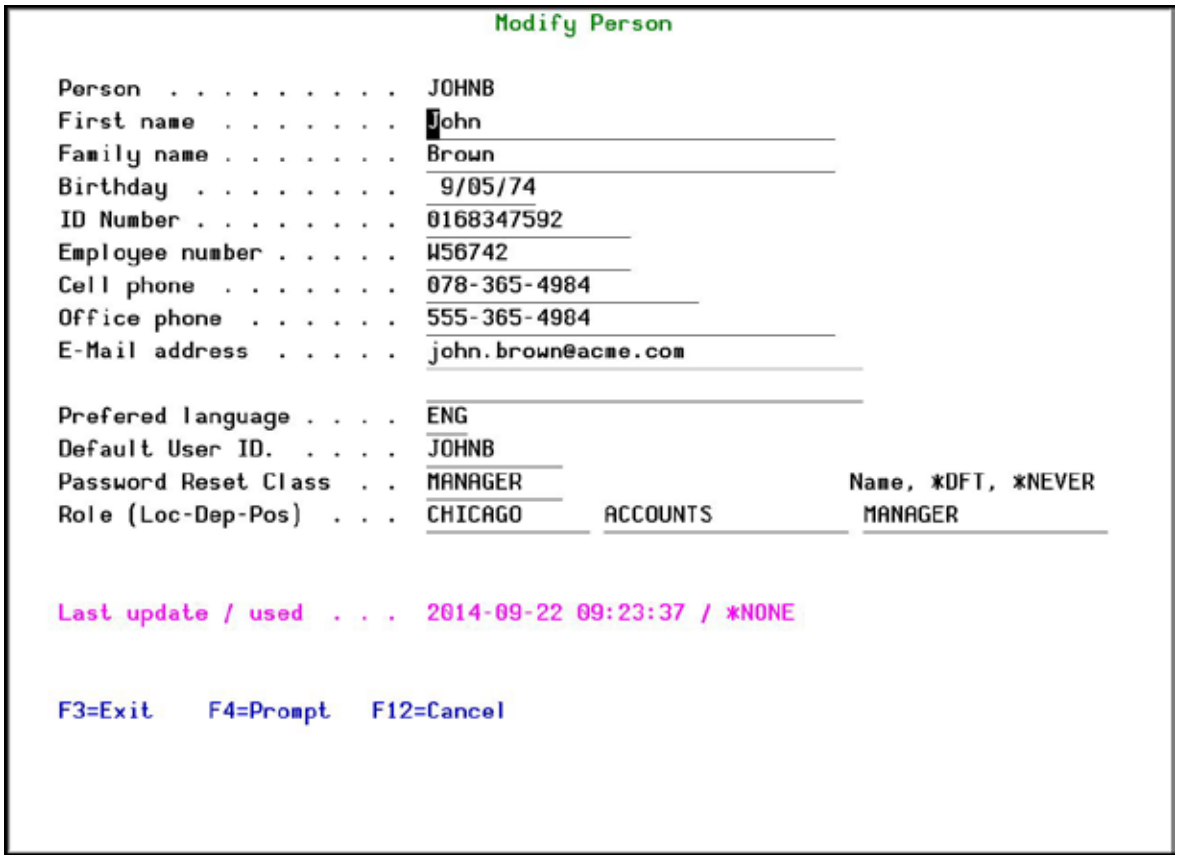
Field/Option/Command Key	Description
E-Mail address	The email address of the person - can be used for the unique identification of the Person. Can also be used to send notification of a new password. If the Password Reset Class you give to this person states that only email addresses in a specific domain can be used, ensure that this address is in that domain.
Preferred language	Define the language in which this person will receive identity verification questions. Press **F4** to see a list of possible options.
Default User ID	The preferred User ID of the Person on the IBM i. It is used to create the User Profiles for the Person.
Password Reset class	Define the Password Reset class to which the person belongs. Press **F4** to see a list of possible options. If you do not want one of the options, you can enter either *DFT to use default settings or *NEVER to define the Password Reset class will not be used. The Password Reset class defines how verification will be performed for the user when resetting passwords.
Role (Loc-Dep-Pos)	The combination of Location, Department, and Position defines the Role (permissions profile) for the user. It is used to define to which systems the user should be provisioned.

3. Enter the Person definitions and press **Enter**. The new Person is added and now appears in the **Work with Persons for Password-Reset** screen.

Modify a Person

To modify persons:

1. Select **1. Work with Persons** in the **Password Reset** main menu. The **Work with Persons for Password-Reset** screen appears.
2. Select the Person to modify and press **1=Select**. The **Modify Person** screen appears.



Modify Person screen

Field/Option/Command Key	Description
Person	The unique identifier of the Person (read only)
First name	The first name of the Person.
Family name	The family name or surname of the Person.
Birthday	The birthday of the Person – can be used for the unique identification of the Person.
ID Number	The national ID number of the person – can be used for the unique identification of the Person.
Employee number	The employee number of the Person within the organization - can be used for the unique identification of the Person.
Cell phone	The cell phone number of the Person – can be used for the unique identification of the Person. Can also be used to send notification of a new password.
Office phone	The office phone number of the Person – can be used for the unique identification of the Person.
E-Mail address	The email address of the person - can be used for the unique identification of the Person. Can also be used to send notification of a new password. If the Password Reset Class you give to this person states that only email addresses in a specific domain can be used, ensure that this address is in that domain.

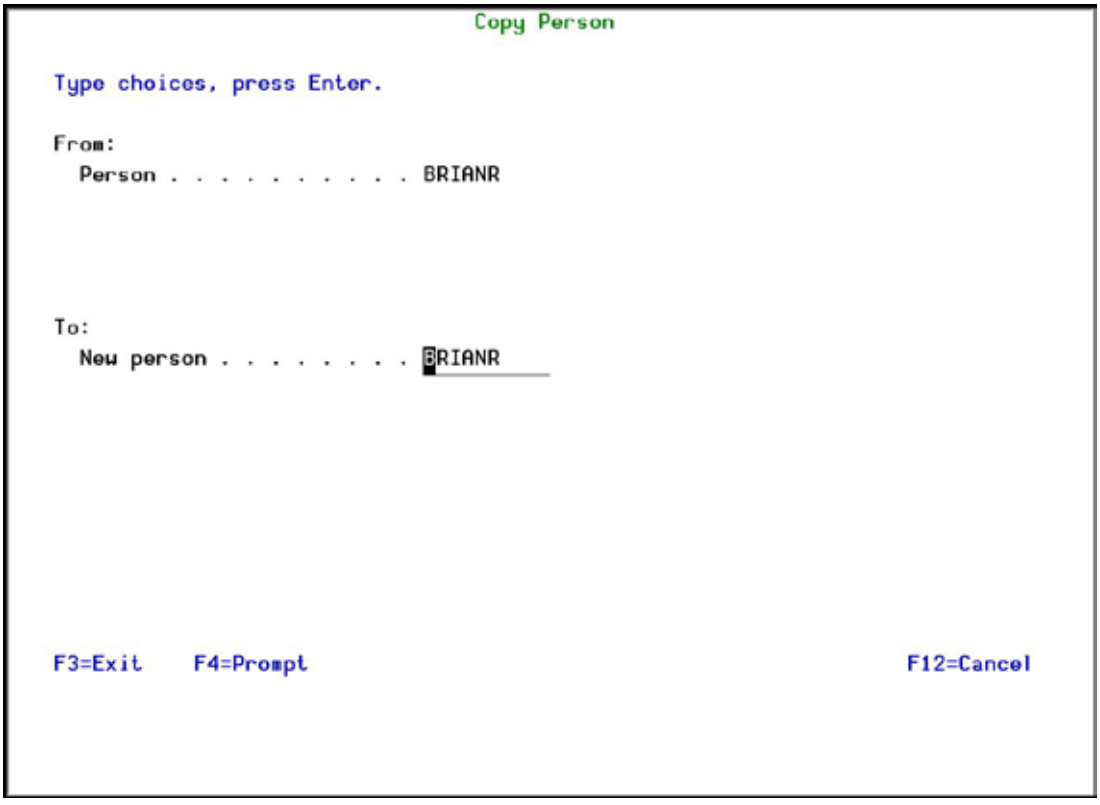
Field/Option/Command Key	Description
Preferred language	Define the language in which this person will receive identity verification questions. Press **F4** to see a list of possible options.
Default User ID	The preferred User ID of the Person on the IBM i. It is used to create the User Profiles for the Person.
Password Reset class	Define the Password Reset class to which the person belongs. Press **F4** to see a list of possible options. If you do not want one of the options, you can enter either *DFT to use default settings or *NEVER to define the Password Reset class will not be used. The Password Reset class defines how verification will be performed for the user when resetting passwords.
Role (Loc-Dep-Pos)	The combination of Location, Department, and Position defines the Role (permissions profile) for the user. It is used to define to which systems the user should be provisioned.

3. Update the Person definitions as required and press **Enter**. The Person is updated and the updated information now appears in the **Work with Persons for Password-Reset** screen.

Copy a Person

To copy persons:

1. Select **1. Work with Persons** in the **Password Reset** main menu. The **Work with Persons for Password-Reset** screen appears.
2. Select the Person to copy and press **3=Copy**. The **Copy Person** screen appears.



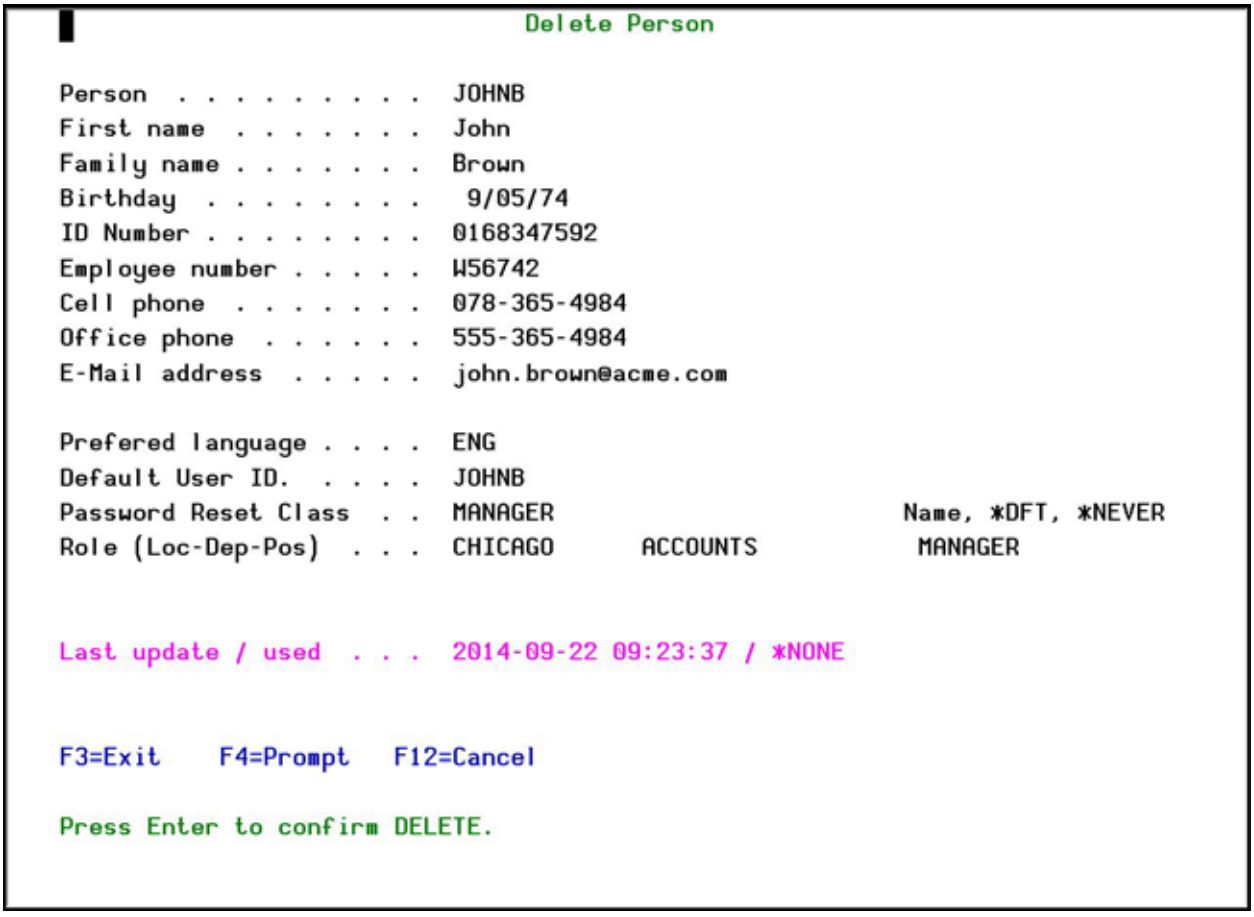
Copy Person screen

3. Enter the name of the **New Person** and press **Enter**. The Person is created and the updated information now appears in the **Work with Persons for Password-Reset** screen.
   You should make sure that you modify all unique information.

Delete a Person

To delete persons:

1. Select **1. Work with Persons** in the **Password Reset** main menu. The **Work with Persons for Password-Reset** screen appears.
2. Select the Person to delete and press **4=Delete**. The **Delete Person** screen appears.



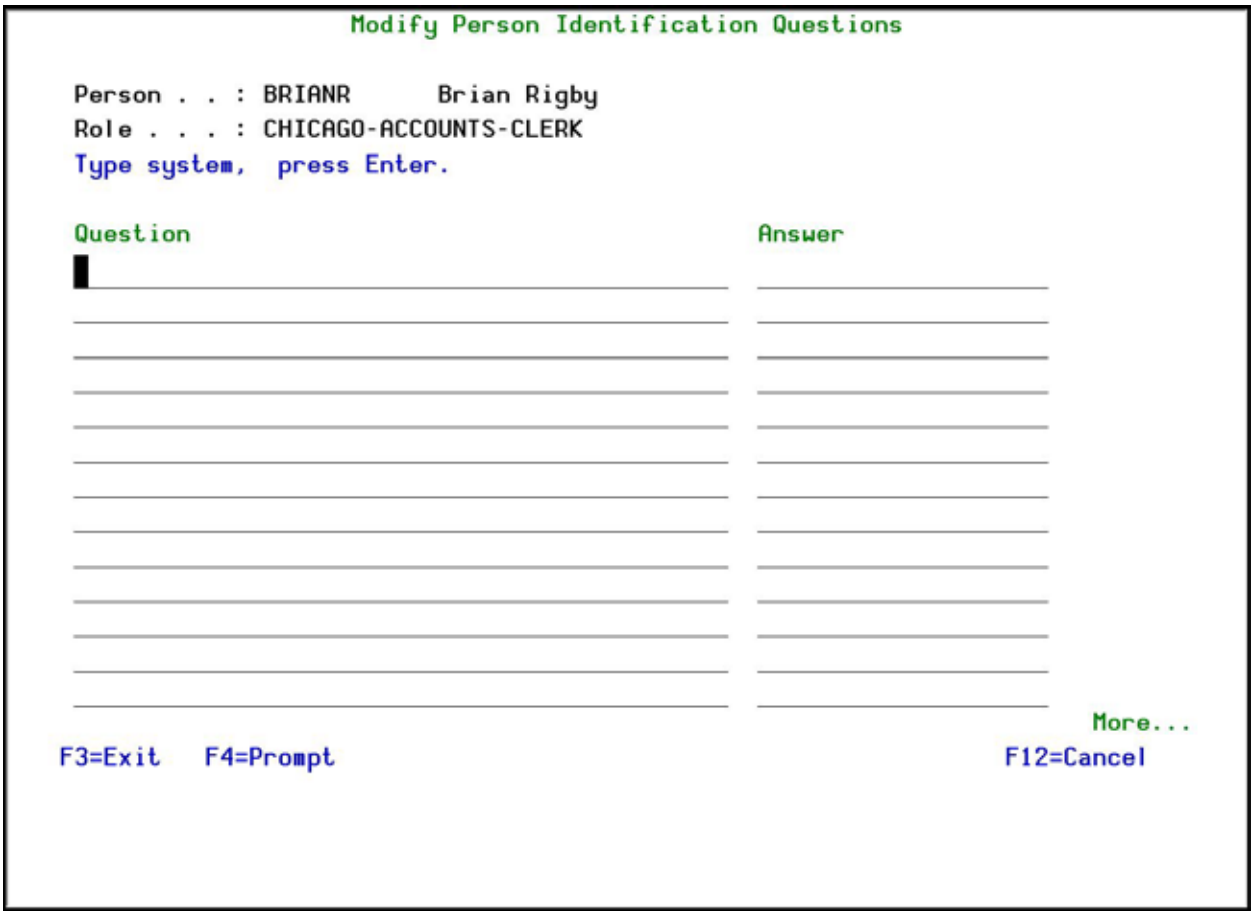
Delete Person screen

3. Press **Enter**. The Person is deleted and the updated **Work with Persons for Password-Reset** screen appears.

Add Private Questions for a Person

To add private questions for a person

1. Select **1. Work with Persons** in the **Password Reset** main menu. The **Work with Persons for Password-Reset** screen appears.
2. Select the Person to which you want to add private questions and press **7=Questions**. The **Modify Person Identification Questions** screen appears.



Modify Person Identification Questions screen

Field/Option/Command Key	Description
Question	Enter the questions that will help to uniquely identify the Person. Only the Person should know the answer. Type in any question or use **F4** to select from a list of commonly used questions. You can enter as many questions as you want, but you must enter at least as many questions as will be asked at Password Reset time.
Answer	The answer to the question. Existing answers are shown as asterisks. Remember that the response process when resetting your password is case sensitive. If you use capital letters here, you have to remember to use them when answering the questions in the reset process.

3. Add as many questions and answers as you want. Ensure that there are at least as many questions as required in the **P-R Class** of the person.
4. Press **Enter**. You are returned to the **Work with Persons for Password-Reset** screen.

Delete Private Questions for a Person

To delete private questions for a person

1. Select **1. Work with Persons** in the **Password Reset** main menu. The **Work with Persons for Password-Reset** screen appears.

2. Select the Person from which you want to delete private questions and press **7=Questions**. The **Modify Person Identification** Screen appears.
3. Delete as many questions and answers as you want. Ensure that when you finish, there are at least as many questions as required in the P-R Class of the person.
4. Press **Enter**. You are returned to the **Work with Persons for Password-Reset** screen.

Identification

Password Reset classes define which identification procedures will be run when an attempt is made to reset a password and how the new passwords will be sent to users.

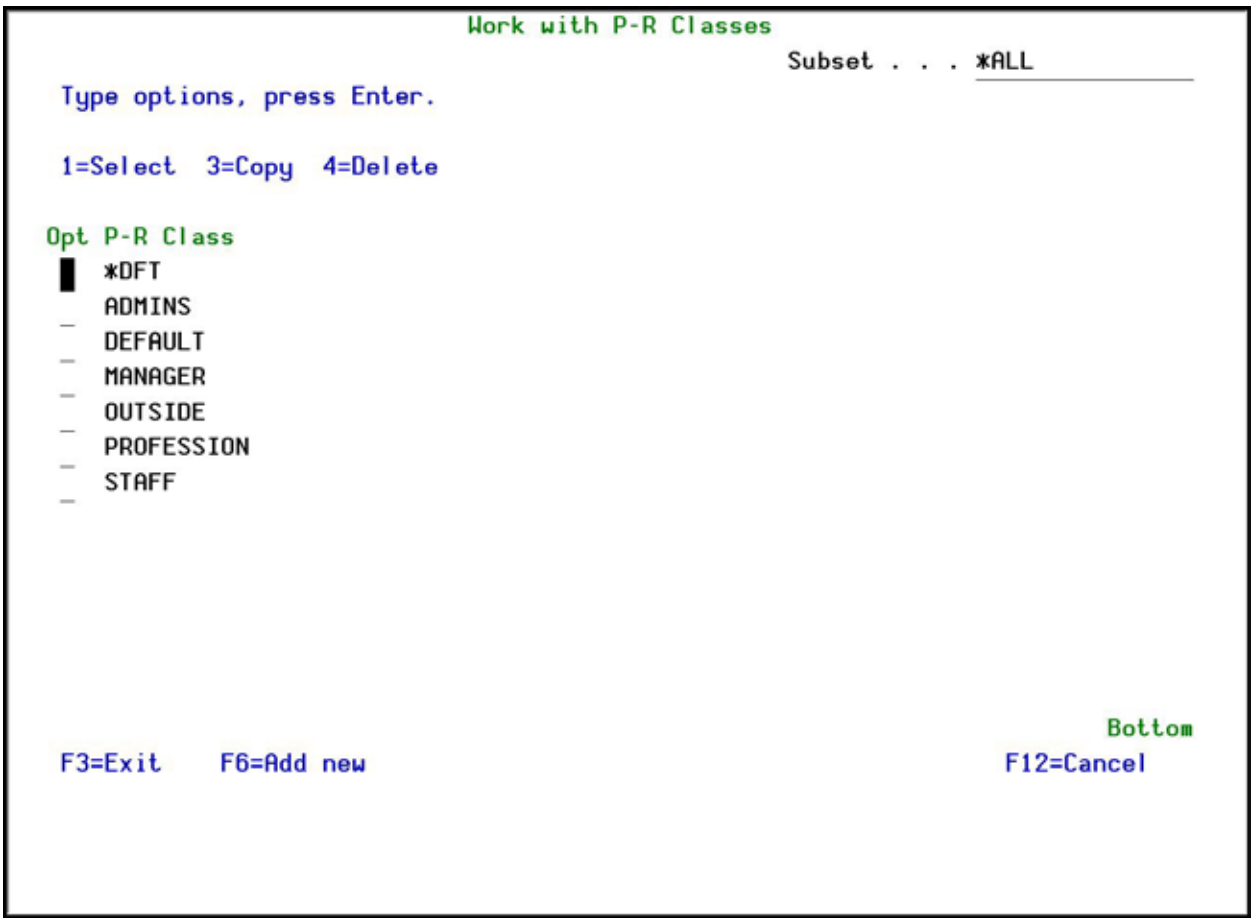
Roles are used to define which Systems are available for all User Profiles that belong to a specific combination of Location/Department/Position in your organization.

Add P-R Classes

Password Reset classes define which identification procedures will be run when an attempt is made to reset a password and how the new passwords will be sent to users. Password Reset classes are used to ensure identical behavior for certain types of users, regardless of their physical location, to which department they belong, or to what job they perform. For example, you might want to have a set of identification procedures for all managers in your organization and a different set of identification procedures for all non-supervisory staff.

To add Password Reset classes:

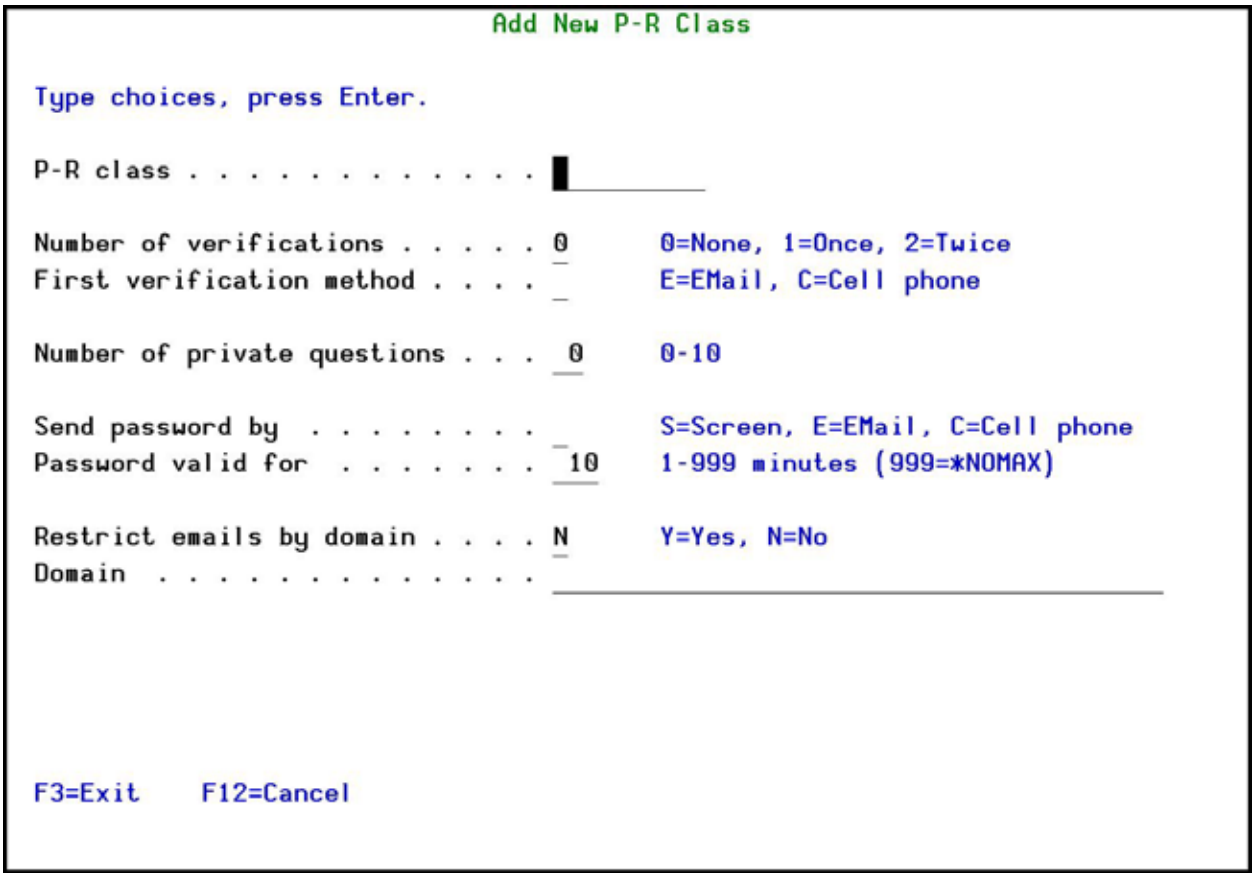
1. Select **11. P-R Classes** in the **Password Reset** main menu. The **Work with P-R Classes** screen appears.



Work with P-R Classes screen

Field/Option/Command Key	Description
P-R Class	The Classes that can be assigned to a User.
F6=Add new	Opens the **Add New P-R Class** screen.

2. Press **F6=Add new**. The **Add New P-R Class** screen appears.



Add New PR-Class screen

Field/Option/Command Key	Description
P-R Class	The name of the Class being added. The field is mandatory.
Number of verifications	Set the number of times Users with this Class will have to verify the new password. **0=None** (default value) **1=Once** **2=Twice**
First verification method	Set the method by which Users with this Class verify the new password. **E=Email** (default value) **C=Cell phone**
Number of private questions	In addition to the standard questions, you can also add private questions to be asked for identification purposes. The questions asked will be taken at random from a list of private questions. Ensure that when you create a Person using a P-R Class the appropriate number of private questions are defined. **0-10**. 0 = default value.
Send password by	Set the method to send the new password to all Users with this Class. **S=Screen** **E=Email** (default value) **C=Cell phone**

Field/Option/Command Key	Description
Password valid for	Set the time in minutes for which the new password will be valid for Users with this Class. The maximum time is 998 minutes (16 hours 38 minutes). If you enter 999, the password will never expire. **1-999** minutes (999=*NOMAX) (10 = default value)
Restrict emails by domain	Users with this Class can only receive their new password by mail if it is in a specific domain. For example, an organization may want to allow new passwords to go only to email addresses on its own servers. **N=No** (default value) **Y=Yes**
Domain	If **Restrict emails by domain** = **Y**, enter the domain to which the emails are restricted.

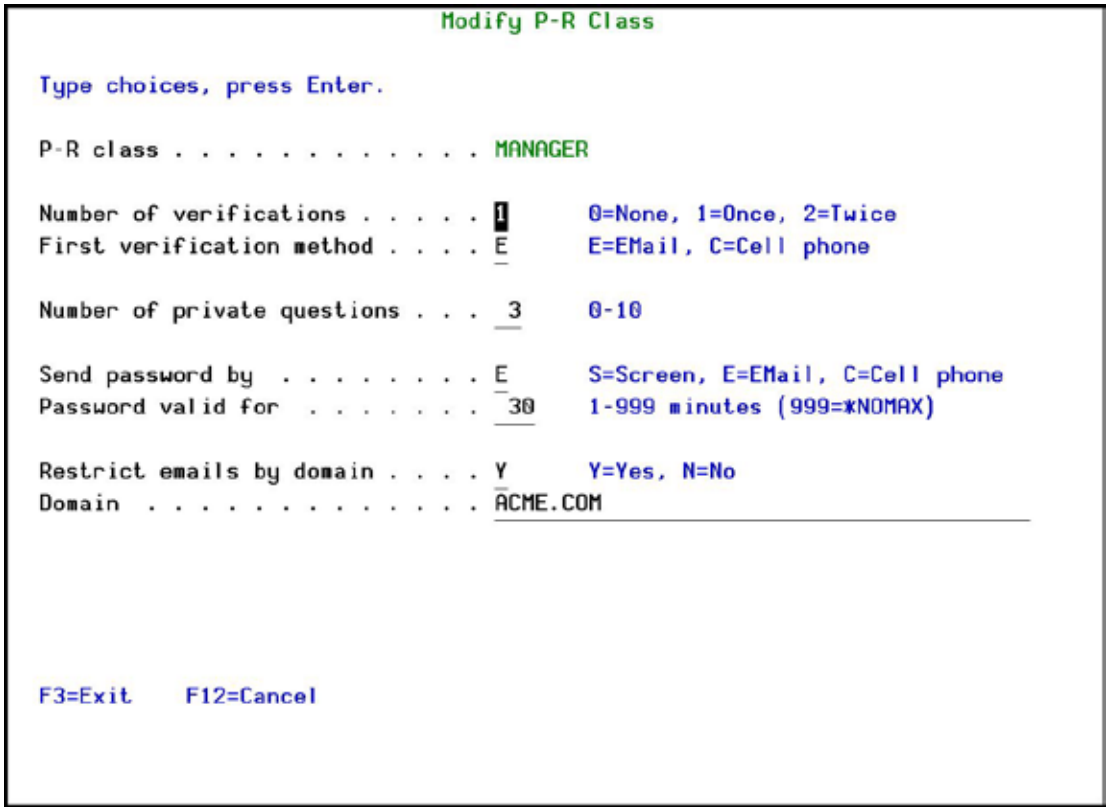
3. Enter the Password Reset Class definitions and press **Enter**. The new Password Reset Class is added and now appears in the **Work with P-R Classes** screen.

Modify P-R Classes

Password Reset classes define the verification process to be used when users reset their passwords.

To modify Password Reset classes:

1. Select **11. P-R Classes** in the **Password Reset** main menu. The **Work with P-R Classes** screen appears.
2. Select the P-R Class to modify and press **1=Select**. The **Modify P-R Class** screen appears.



Modify PR-Class screen

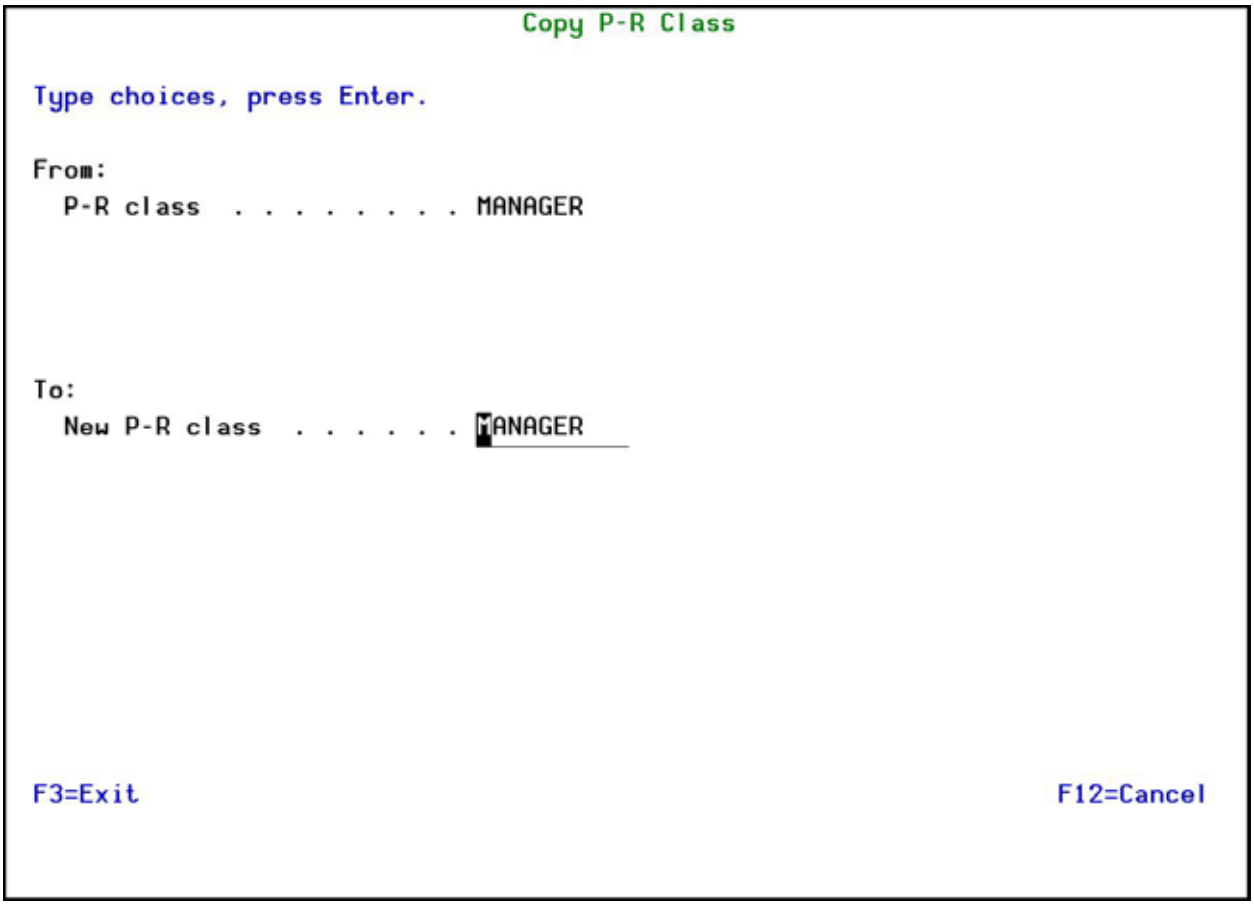
Field/Option/Command Key	Description
Number of verifications	Set the number of times Users with this Class will have to verify the new password. **0=None** (default value) **1=Once** **2=Twice**
First verification method	Set the method by which Users with this Class verify the new password. **E=Email** (default value) **C=Cell phone**
Number of private questions	In addition to the standard questions, you can also add private questions to be asked for identification purposes. The questions asked will be taken at random from a list of private questions. Ensure that when you create a Person using a P-R Class, the appropriate number of private questions are defined. **0-10**. 0 = default value.
Send password by	Set the method to send to new password to all Users with this Class. **S=Screen** **E=Email** (default value) **C=Cell phone**
Password valid for	Set the time in minutes for which the new password will be valid for Users with this Class. The maximum time is 998 minutes (16 hours 38 minutes). If you enter 999, the password will never expire. **1-999** minutes (**999**=***NOMAX**) (**10** = default value)
Restrict emails by domain	Users with this Class can only receive their new password by mail if it is in a specific domain. For example, an organization may want to allow new passwords to go only to email addresses on its own servers. **N=No** (default value) **Y=Yes**
Domain	If **Restrict emails by domain** = **Y**, enter the domain to which the emails are restricted.

3. Update the P-R Class definitions as required and press **Enter**. The P-R Class is updated and the updated information now appears in the **Work with P-R Classes** screen.

Copy P-R Classes

To copy Password Reset classes:

1. Select **11. P-R Classes** in the **Password Reset** main menu. The **Work with P-R Classes** screen appears.
2. Select the P-R Class to modify and press **3=Copy**. The **Copy P-R Class** screen appears.



Copy PR-Class screen

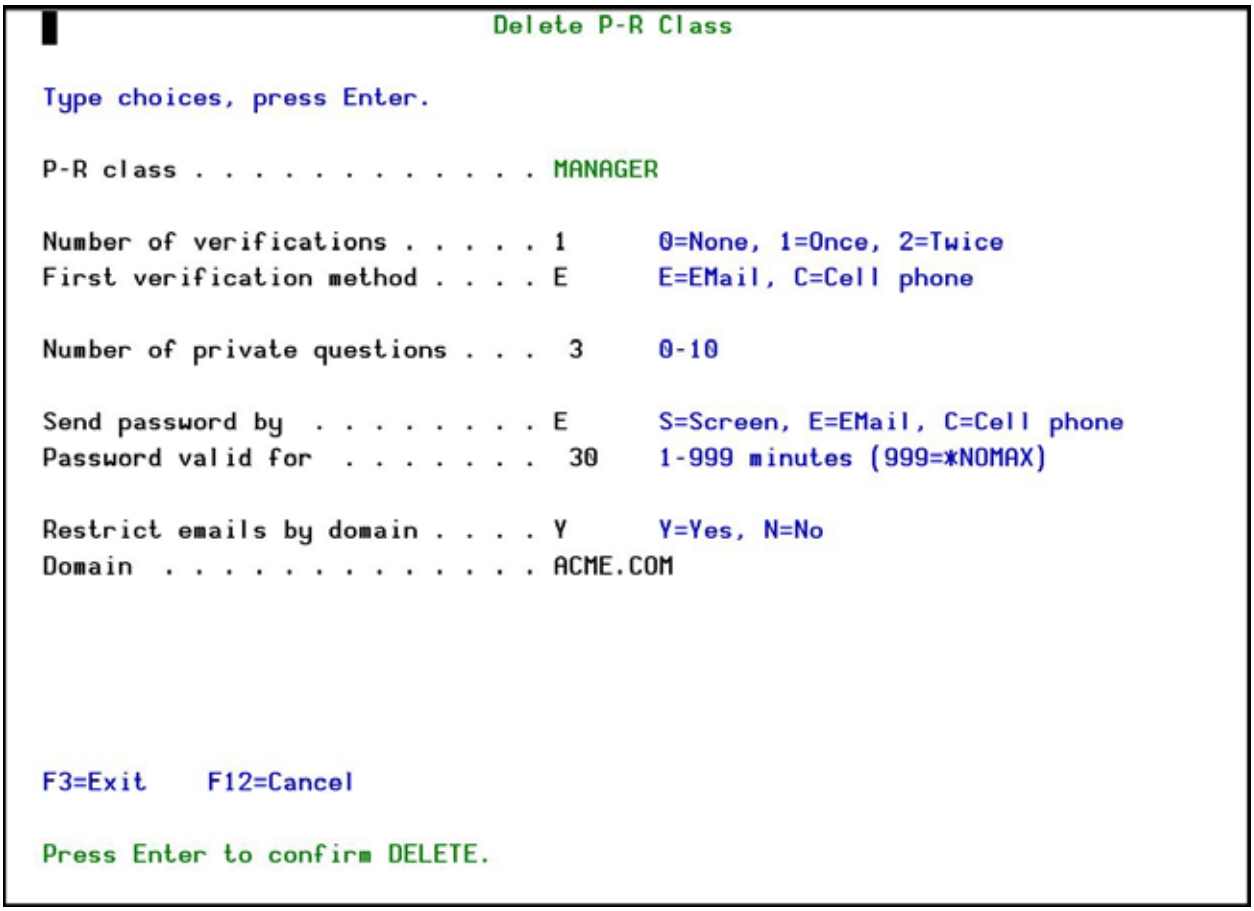
Field/Option/Command Key	Description
From P-R class	The class being copied (Read Only).
To New P-R class	The unique identifier of the new class.

3. Enter the name of the new P-R Class and press **Enter**. The P-R Class is added and now appears in the **Work with P-R Classes** screen.
4. Modify the new P-R Class as described in the **Modify P-R Classes** task (start at step 2).

Delete a P-R Class

To delete persons:

1. Select **11. P-R Classes** in the **Password Reset** main menu. The **Work with P-R Classes** screen appears.
2. Select the P-R Class to modify and press **4=Delete**. The **Delete P-R Class** screen appears.



Delete PR-Class screen

3. Press **Enter**. The P-R Class is deleted and the updated **Work with P-R Classes** screen appears.

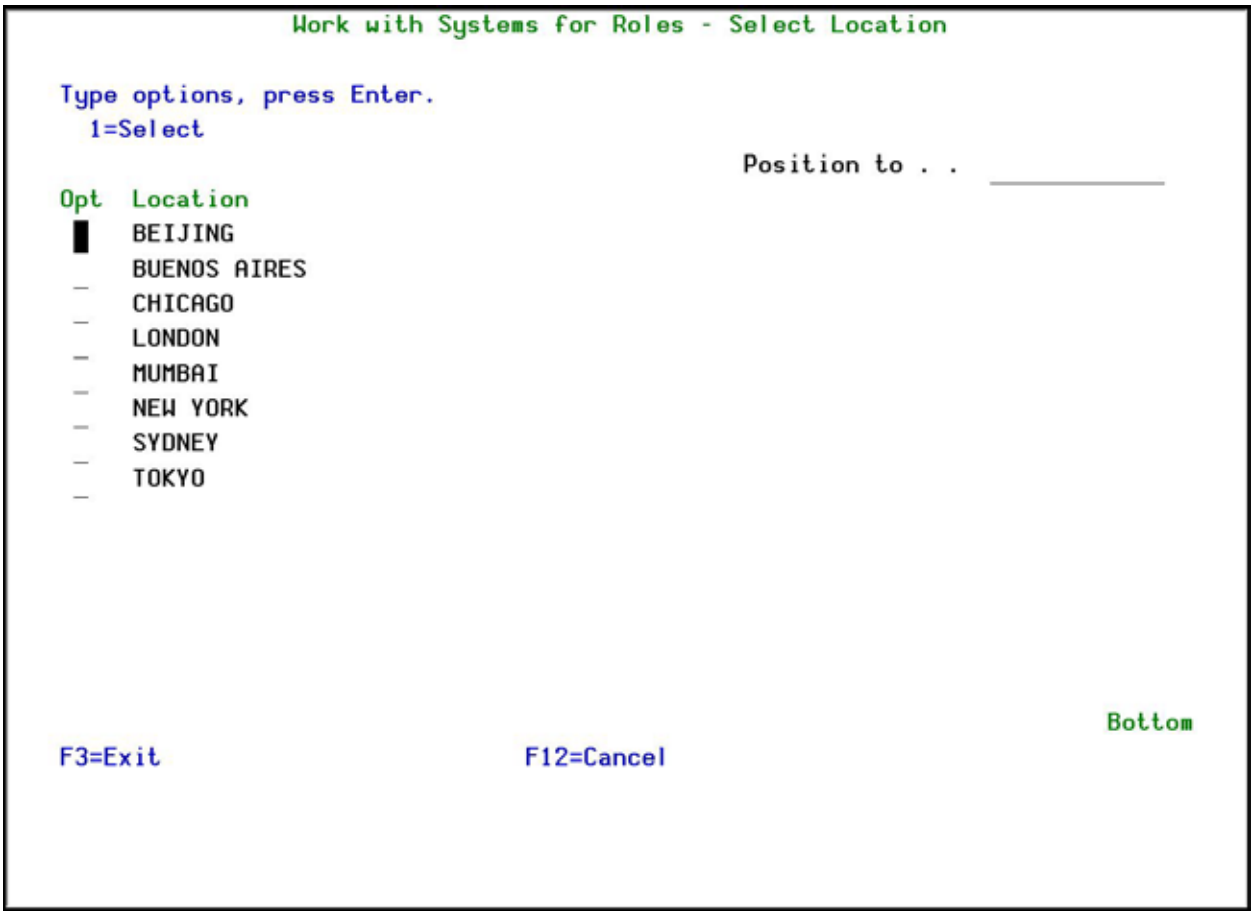
Add a Role/System

Roles are used to define which Systems are available for all User Profiles that belong to a specific combination of Location/Department/Position in your organization. This ensures that when users reset their passwords, the password is only sent to Systems to which they are allowed to work on. For example, your organization may have a separate system dedicated to each separate physical location. Alternatively, systems may be dedicated to the specific departments across locations, so that all finance departments use one system and all manufacturing departments use a different computer.

Note: You do not need to define every possible combination of Location/Department/Position as a role, as not all combinations will exist in your organization. For example, your Finance Department may only exist in one location, and in the same location there probably isn't a Manufacturing Department.

To add a Role/System:

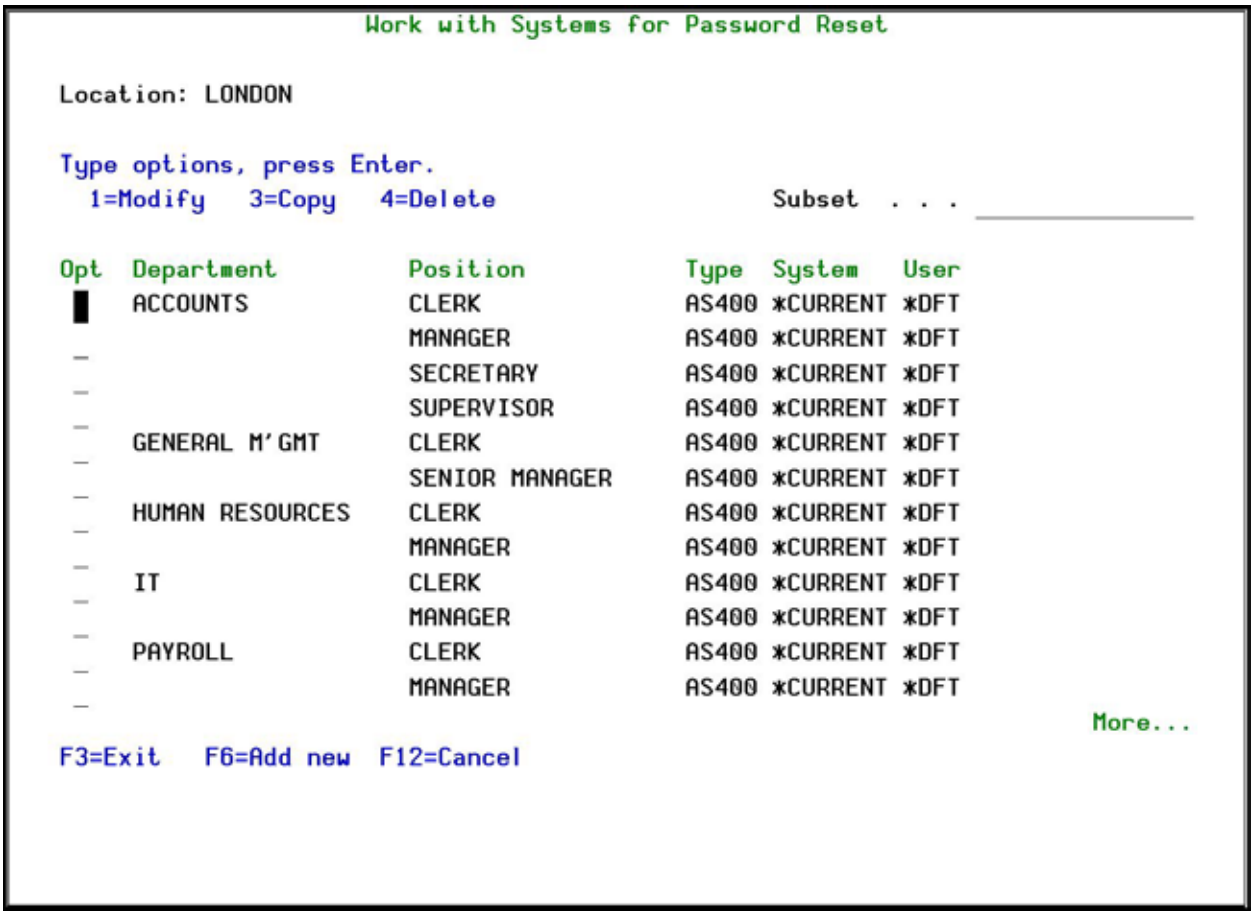
1. Select **12. Systems for Roles** in the **Password Reset** main menu. The **Work with Systems for Roles – Select Location** screen appears.



Work with Systems for Roles – Select Location screen

Field/Option/Command Key	Description
1=Select	Opens the **Work with Systems for Password Reset** screen.
Location	The locations in your organization.

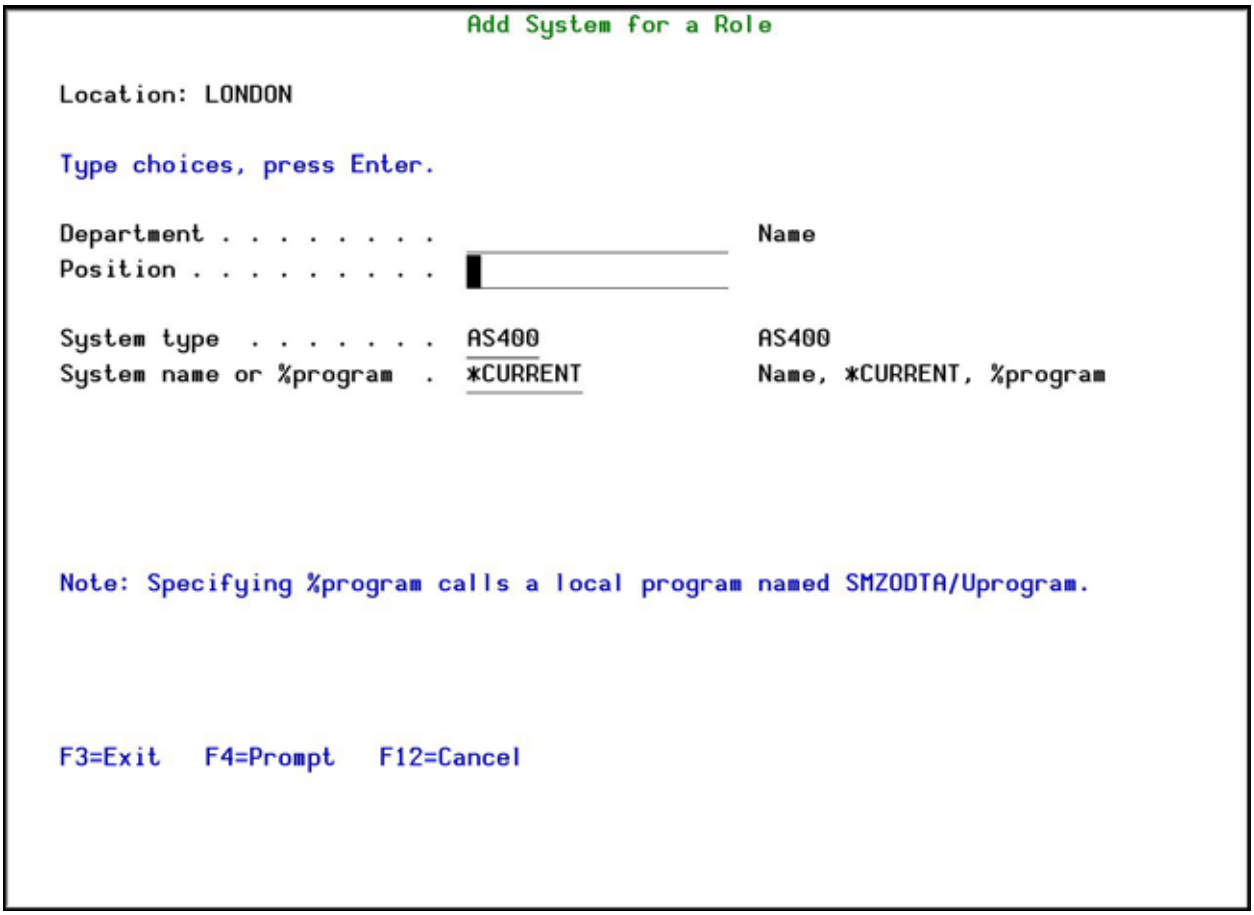
2. Select the Location to work with and press **1=Select**. The **Work with Systems for Password Reset** screen appears.



Work with Systems for Password Reset screen

Field/Option/Command Key	Description
1=Modify	Opens the **Modify System for a Role** screen
3=Copy	Opens the **Copy a System** screen
4=Delete	Opens the **Delete a System** screen
Location	The selected location.
Department	The departments that exist at the selected Location
Position	The positions that exist in the department
Type	The type of computer system that users in this role (location/department/position) can work on
System	The name of the specific computer system to be used when opening a User for users in this role (location/department/position)
User	The User to be used when opening a User for persons in this role (location/department/position)
F6=Add new	Opens the **Add System for a Role** screen

3. Press **F6=Add new**. The **Add System for a Role** screen appears.



Add System for a Role screen

Field/Option/Command Key	Description
Location	The selected location
Department	The department for the role
Position	The position for the role
System type	The type of computer system that users in this role (location/department/position) can work on
System name or %program	The name of the specific computer system to be used when opening a User for users in this role (location/department/position) **Name** = Use the specific named computer ***CURRENT** = Use the computer where the operation is run **%Program** = Call a local program to provide the computer name. The program called is **SMZODTA/UPROGRAM**

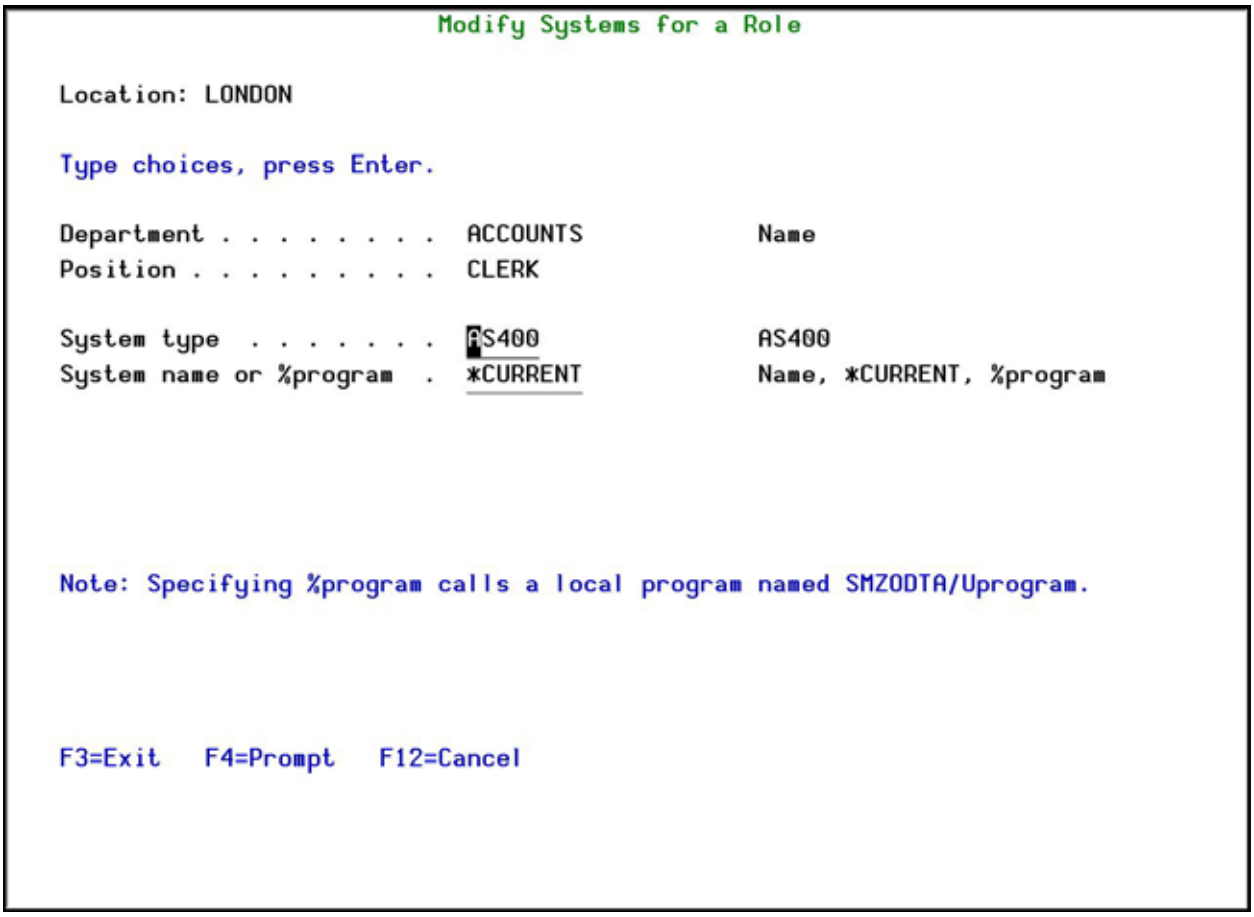
4. Enter the Role and System definitions and press **Enter**. The new Role and System now appears in the **Work with Systems for Password Reset** screen.

Modify the System for a Role

To modify a Role/System:

1. Select **12. Systems for Roles** in the **Password Reset** main menu. The **Work with Systems for Roles – Select Location** screen appears.

2. Select the Location to work with and press **1=Select**. The **Work with Systems for Password Reset** screen appears.
3. Select the Role/System to modify and press **1=Modify**. The **Modify System for a Role** screen appears.



Modify System for a Role screen

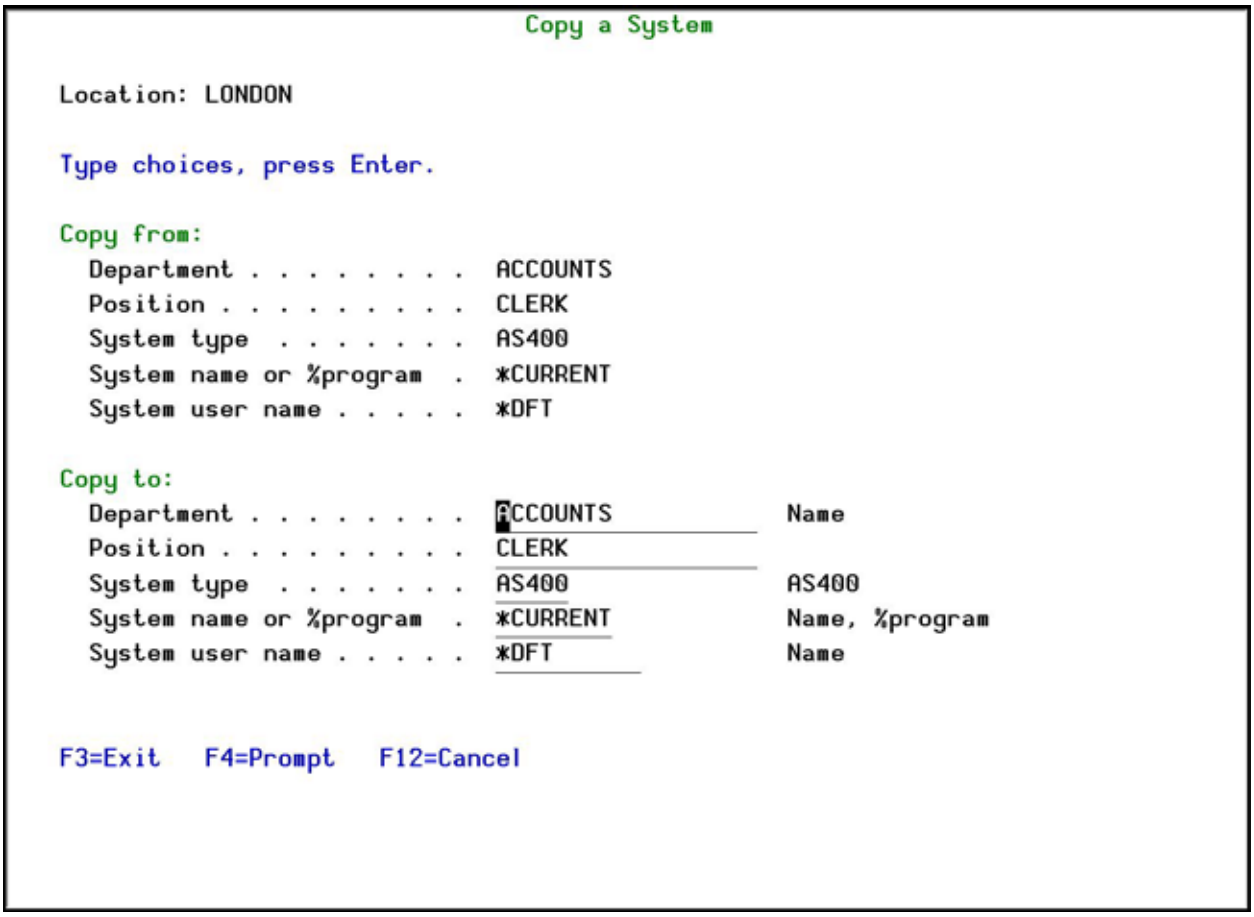
Field/Option/Command Key	Description
Location	The selected location
Department	The department for the role
Position	The position for the role
System type	The type of computer system that users in this role (location/department/position) can work on
System name or %program	The name of the specific computer system to be used when opening a User for users in this role (location/department/position) **Name** = Use the specific named computer ***CURRENT** = Use the computer where the operation is run **%Program** = Call a local program to provide the computer name. The program called is **SMZODTA/UPROGRAM**

4. Modify the System definitions and press **Enter**. The updated Role and System now appears in the **Work with Systems for Password Reset** screen.

Copy a Role/System

To copy a Role/System:

1. Select **12. Systems for Roles** in the **Password Reset** main menu. The **Work with Systems for Roles – Select Location** screen appears.
2. Select the Location to work with and press **1=Select**. The **Work with Systems for Password Reset** screen appears.
3. Select the Role/System to copy and press **3=Copy**. The **Copy a System** screen appears.



Copy a System screen

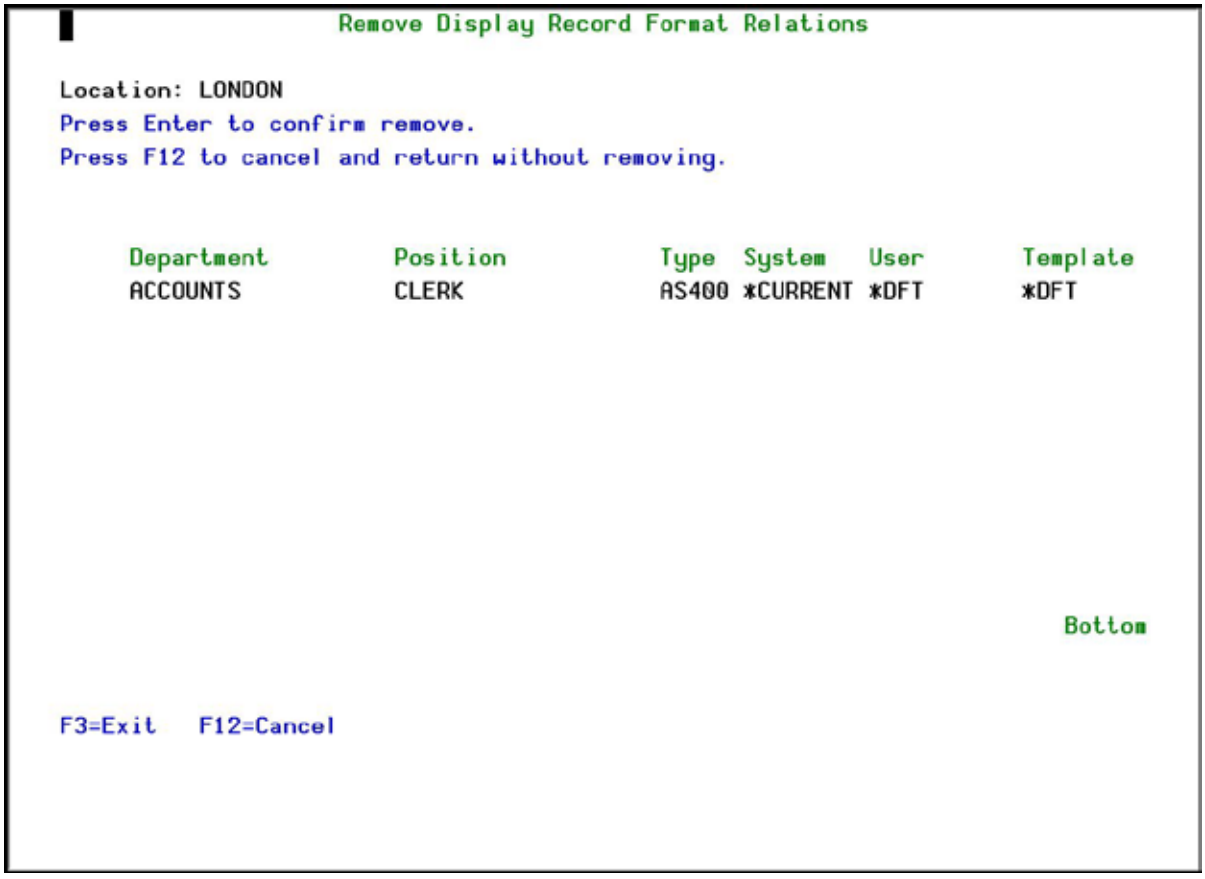
Field/Option/Command Key	Description
Location	The selected location.
Department	The department for the role
Position	The position for the role
System type	The type of computer system that users in this role (location/department/position) can work on
System name or %program	The name of the specific computer system to be used when opening a User for users in this role (location/department/position) **Name** = Use the specific named computer ***CURRENT** = Use the computer where the operation is run **%Program** = Call a local program to provide the computer name. The program called is **SMZODTA/UPROGRAM**

4. Enter the new Role and System definitions and press **Enter**. The new Role and System appears in the **Work with Systems for Password Reset** screen.
5. Modify the new Role/System as described in the **Modify the System for a Role** task (start at step 2).

Delete a Role/System

To delete a Role/System:

1. Select **12. Systems for Roles** in the **Password Reset** main menu. The **Work with Systems for Roles – Select Location** screen appears.
2. Select the Location to work with and press **1=Select**. The **Work with Systems for Password Reset** screen appears.
3. Select the Role/System to delete and press **4=Delete**. The **Delete a System** screen appears.



Delete a System screen

4. Press **Enter**. The Role/System is deleted and the updated **Work with Systems for Password Reset** screen appears.

Definitions

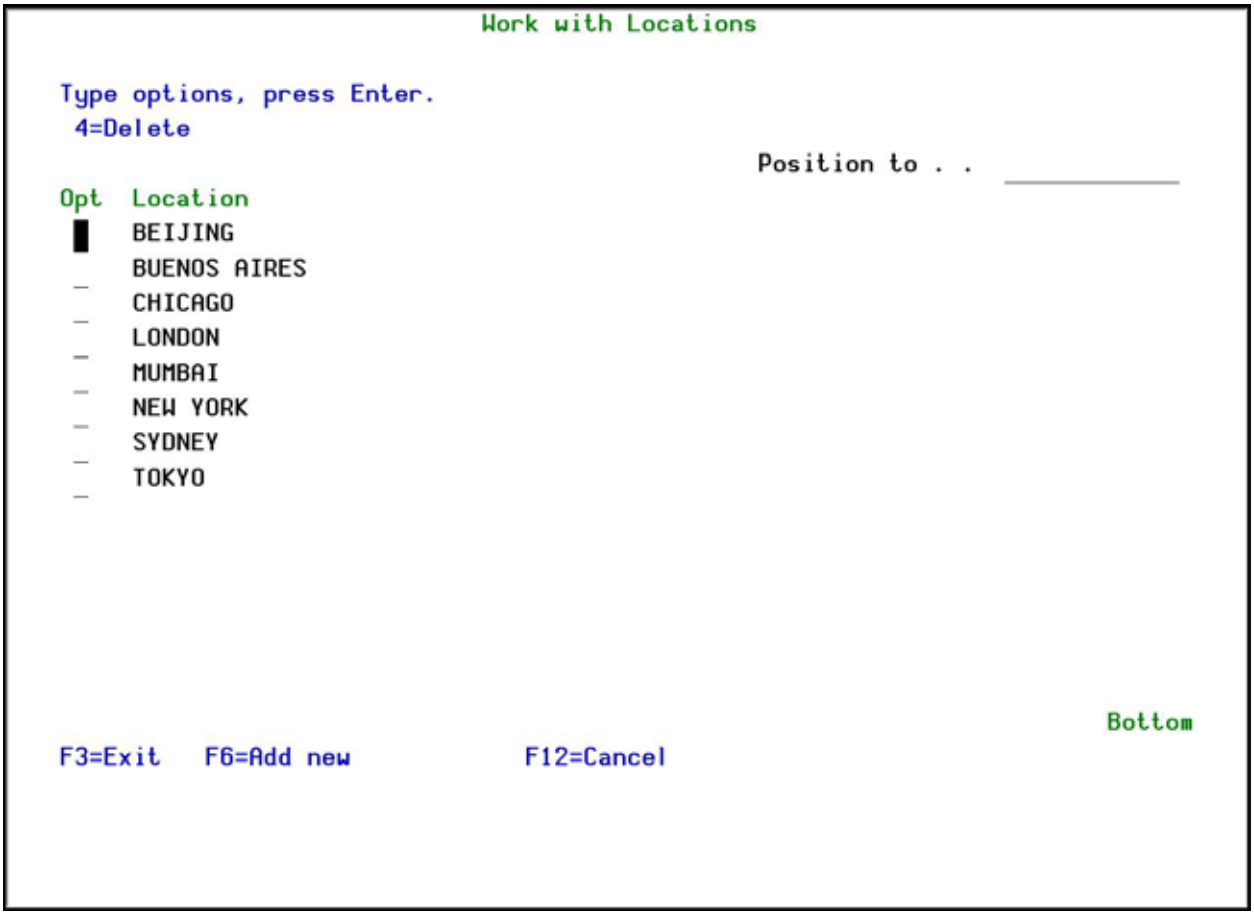
Define the locations, departments, and positions (job titles) that are used in your organization. Together, these three make up the different roles in the organization.

Add a Location

You can add up to 15 Locations at one time. The Locations are used to define Roles in **Password Reset**. You should set the location at the correct level to define the Roles for your organization; country, city, or even district.

To add a Location:

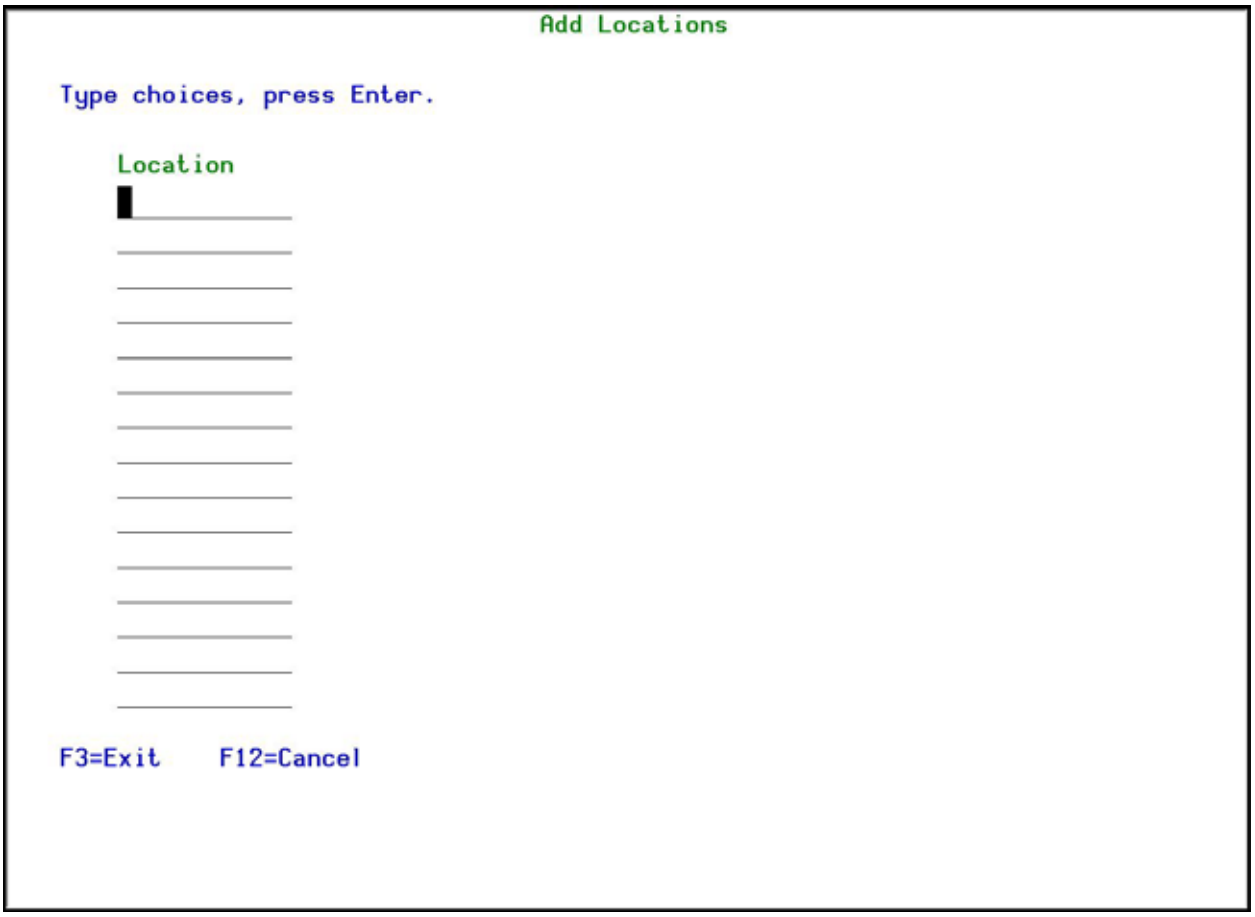
1. Select **31. Locations** in the **Password Reset** main menu. The **Work with Locations** screen appears.



Work with Locations screen

Field/Option/Command Key	Description
4=Delete	Opens the **Delete Locations** screen.
Location	The locations in your organization.
F6=Add new	Opens the **Add Locations** screen.

2. Press **F6=Add new**. The **Add Locations** screen appears.



Add Locations screen

Field/Option/Command Key	Description
Location	The locations in your organization.

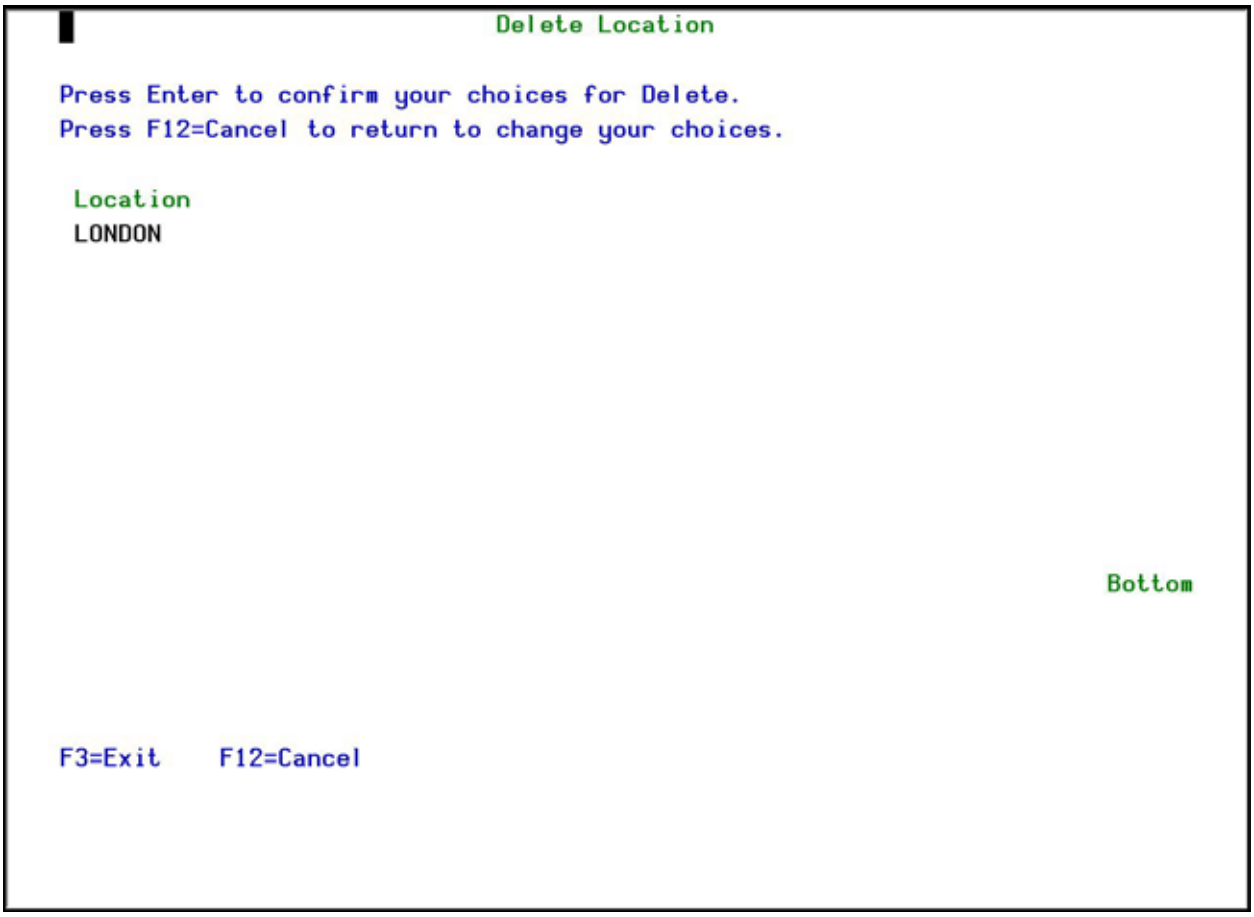
3. Enter the new Locations and press **Enter**. The new Locations now appear in the **Work with Locations** screen.

Delete a Location

To delete a Location:

1. Select **31. Locations** in the **Password Reset** main menu. The **Work with Locations** screen appears.

2. Select the Location to be deleted and press **4=Delete**. The **Delete Locations** screen appears.



Delete Locations screen

3. Press **Enter**. The Location is deleted and the updated **Work with Locations** screen appears.

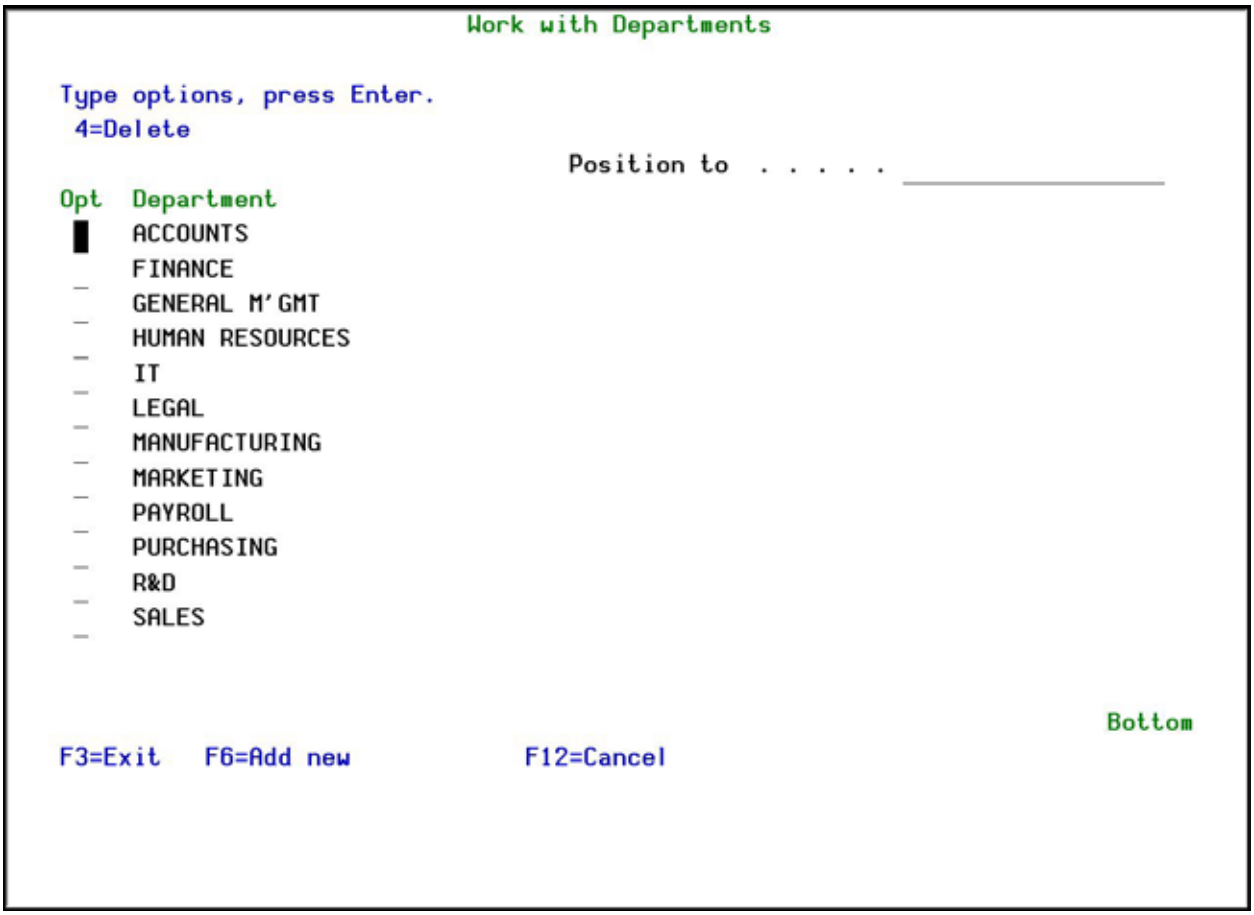
Note: You cannot delete a Location that is used in a Role/System.

Add a Department

You can add up to 15 Departments at one time. The Departments are used to define Roles in **Password Reset**. You should set the department at the correct level for your organization so that you can define Roles. For some organizations, defining a Finance department may be sufficient. Other organizations may need to split the Finance department into its sub-departments, such as Planning, Accounts Receivable, Accounts Payable, and so on.

To add a Department:

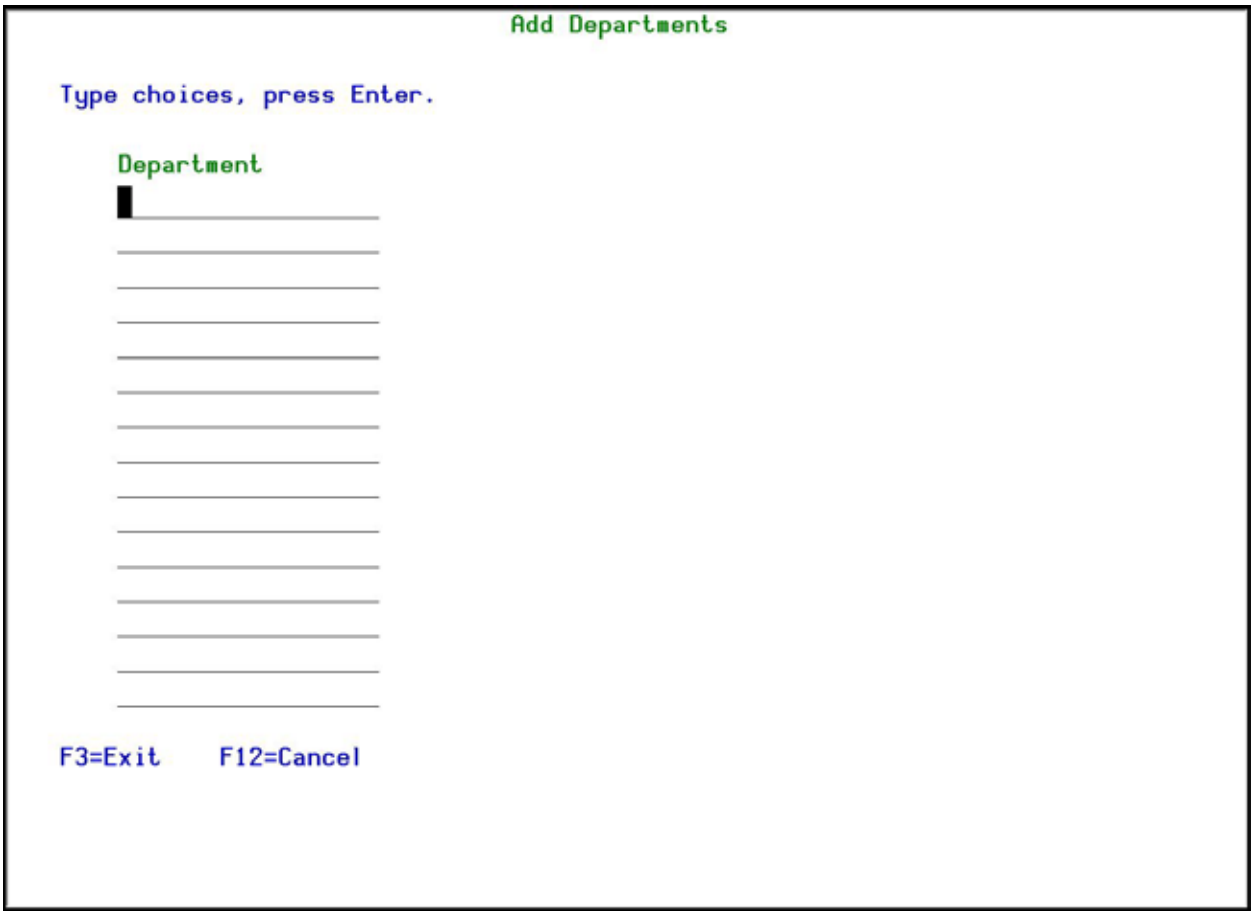
1. Select **32. Departments** in the **Password Reset** main menu. The **Work with Departments** screen appears.



Work with Departments screen

Field/Option/Command Key	Description
4=Delete	Opens the **Delete Departments** screen.
Department	The departments in your organization.
F6=Add new	Opens the **Add Departments** screen.

2. Press **F6=Add new**. The **Add Departments** appears.



Add departments screen

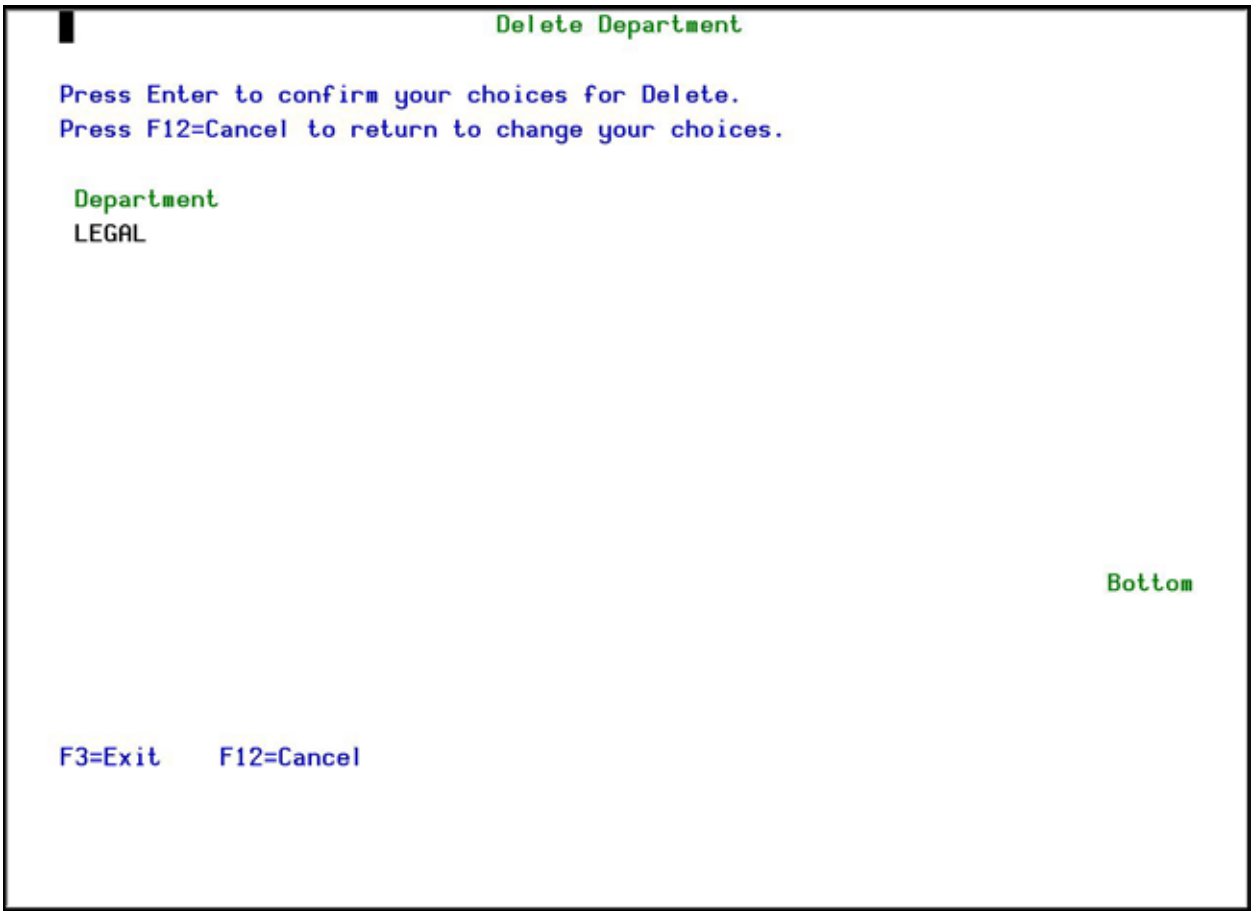
Field/Option/Command Key	Description
Department	The departments in your organization.

3. Enter the new Departments and press **Enter**. The new Departments now appear in the **Work with Departments** screen.

Delete a Department

To delete a Department:

1. Select **32. Departments** in the **Password Reset** main menu. The **Work with Departments** screen appears.
2. Select the Department to be deleted and press **4=Delete**. The Delete Departments screen appears.



Delete Departments screen

3. Press **Enter**. The Department is deleted and the updated **Work with Departments** screen appears.

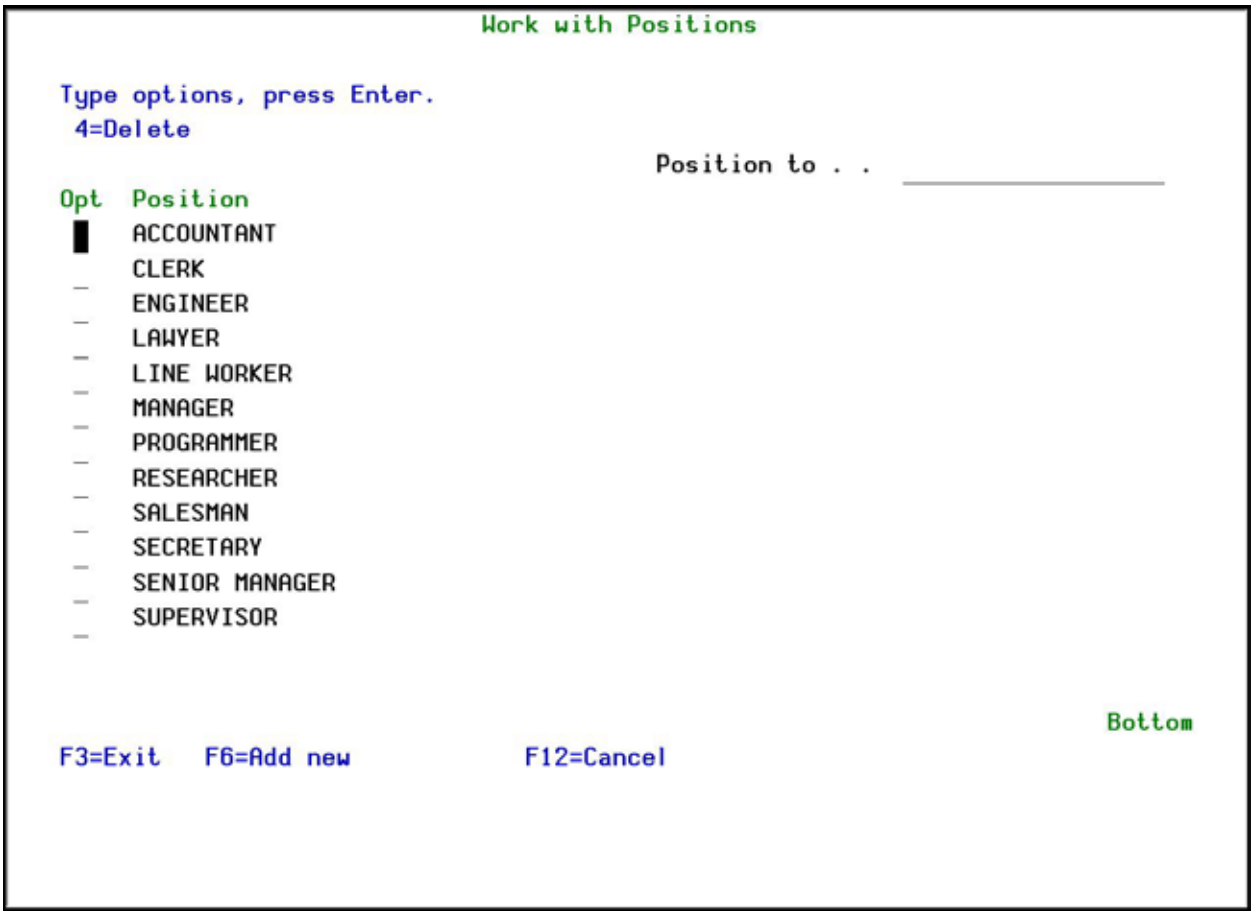
Note: You cannot delete a Department that is used in a Role/System.

Add a Position

You can add up to 15 Positions at one time. The Positions are used to define Roles in **Password Reset**. You should set the position at the correct level for your organization so that you can define Roles. For some organizations, defining a position of Driver may be sufficient. Other organizations may need to define different types of Driver, such as Fork Lift Driver, Truck Driver, Tractor Driver, and so on.

To add a Position:

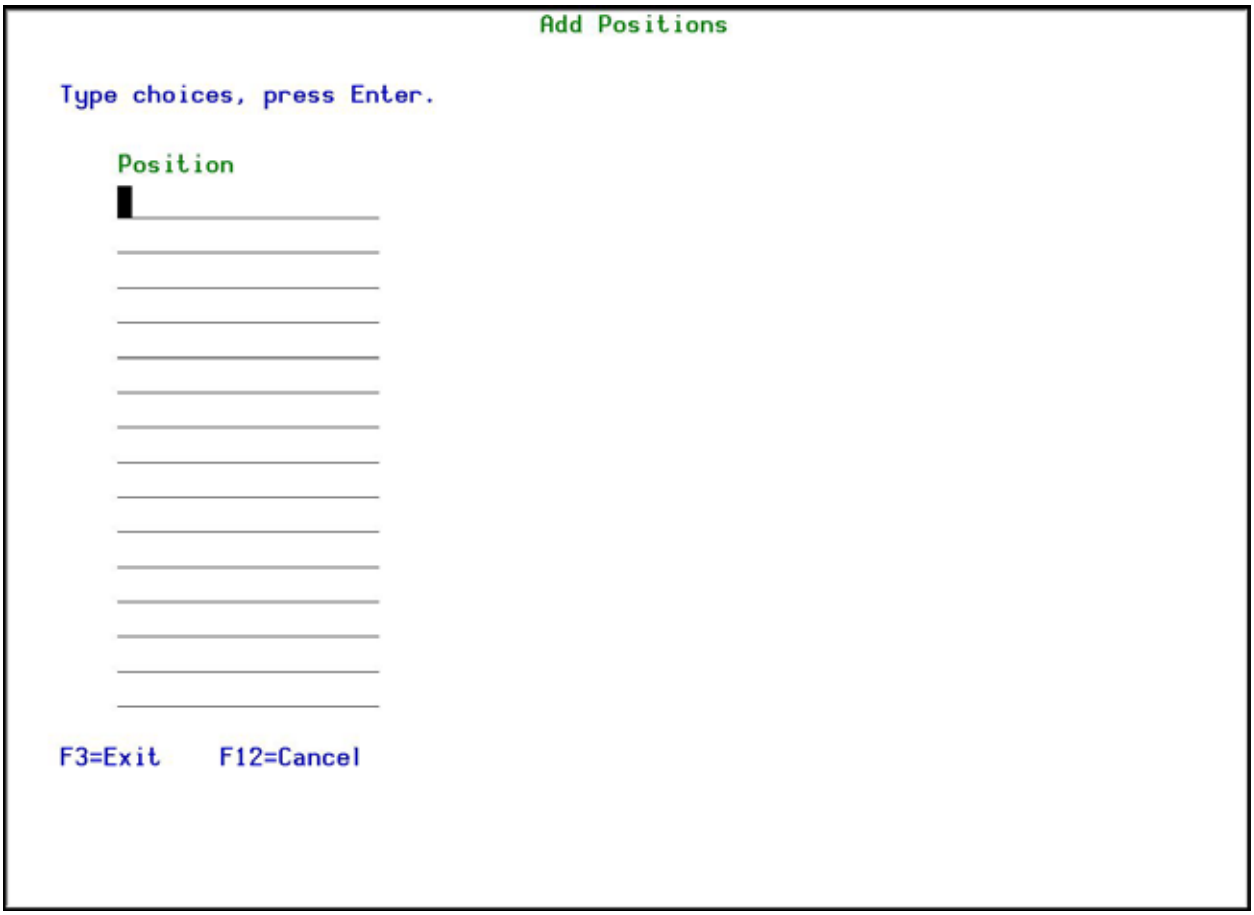
1. Select **33. Positions** in the **Password Reset** main menu. The **Work with Positions** screen appears.



Work with Positions screen

Field/Option/Command Key	Description
4=Delete	Opens the **Delete Positions** screen.
Position	The Positions in your organization.
F6=Add new	Opens the **Add Positions** screen.

2. Press **F6=Add new**. The **Add Positions** screen appears.



Add Positions screen

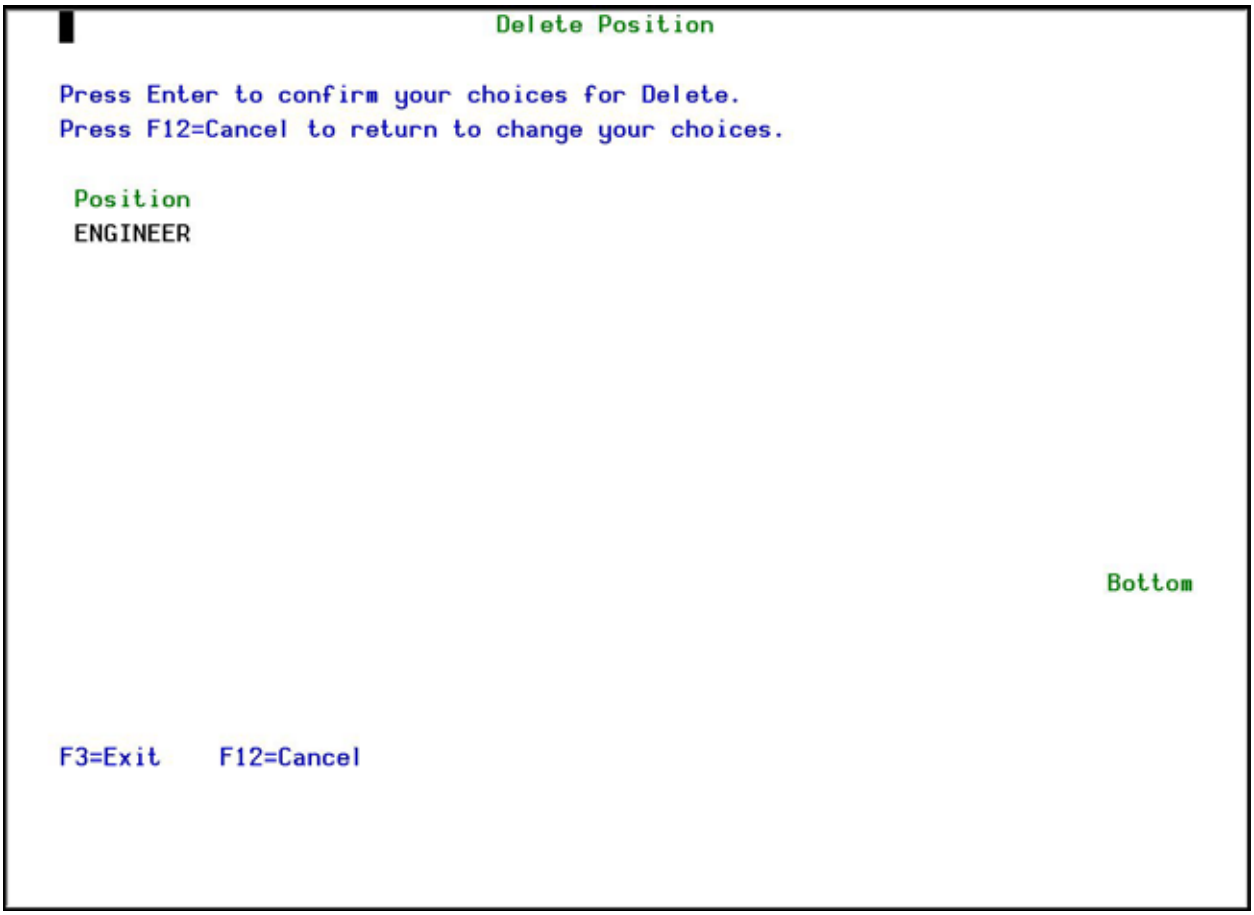
Field/Option/Command Key	Description
Position	The positions in your organization.

3. Enter the new Positions and press **Enter**. The new Positions now appear in the **Work with Positions** screen.

Delete a Position

To delete a Position:

1. Select **33. Positions** in the **Password Reset** main menu. The **Work with Positions** screen appears.
2. Select the Position to be deleted and press **4=Delete**. The **Delete Positions** screen appears.



Delete Positions screen

3. Press **Enter**. The Position is deleted and the updated **Work with Positions** screen appears.

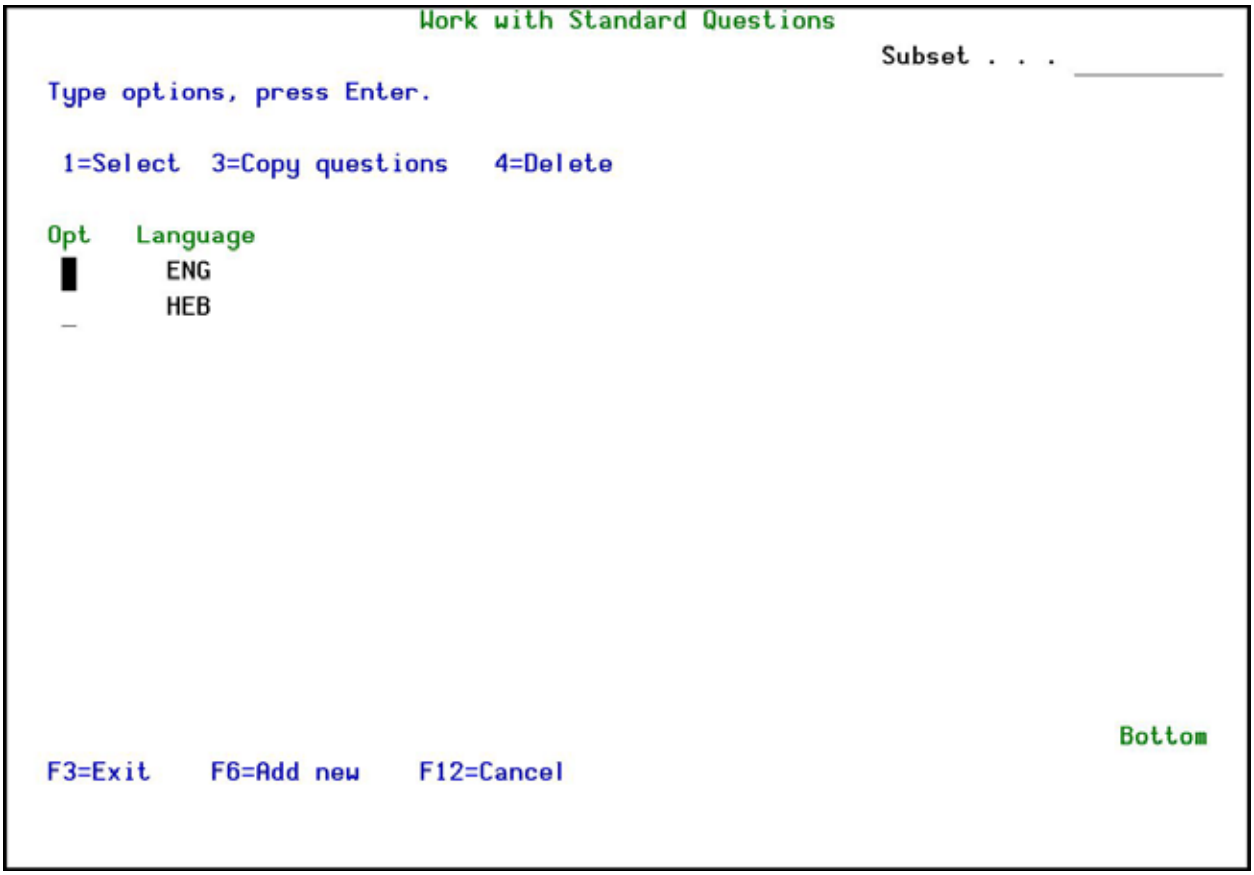
Note: You cannot delete a Position that is used in a Role/System.

Add Standard Questions

In **Password Reset**, you can define a set of standard questions for many languages. These questions can be used for both primary and secondary verification.

To add Standard Questions:

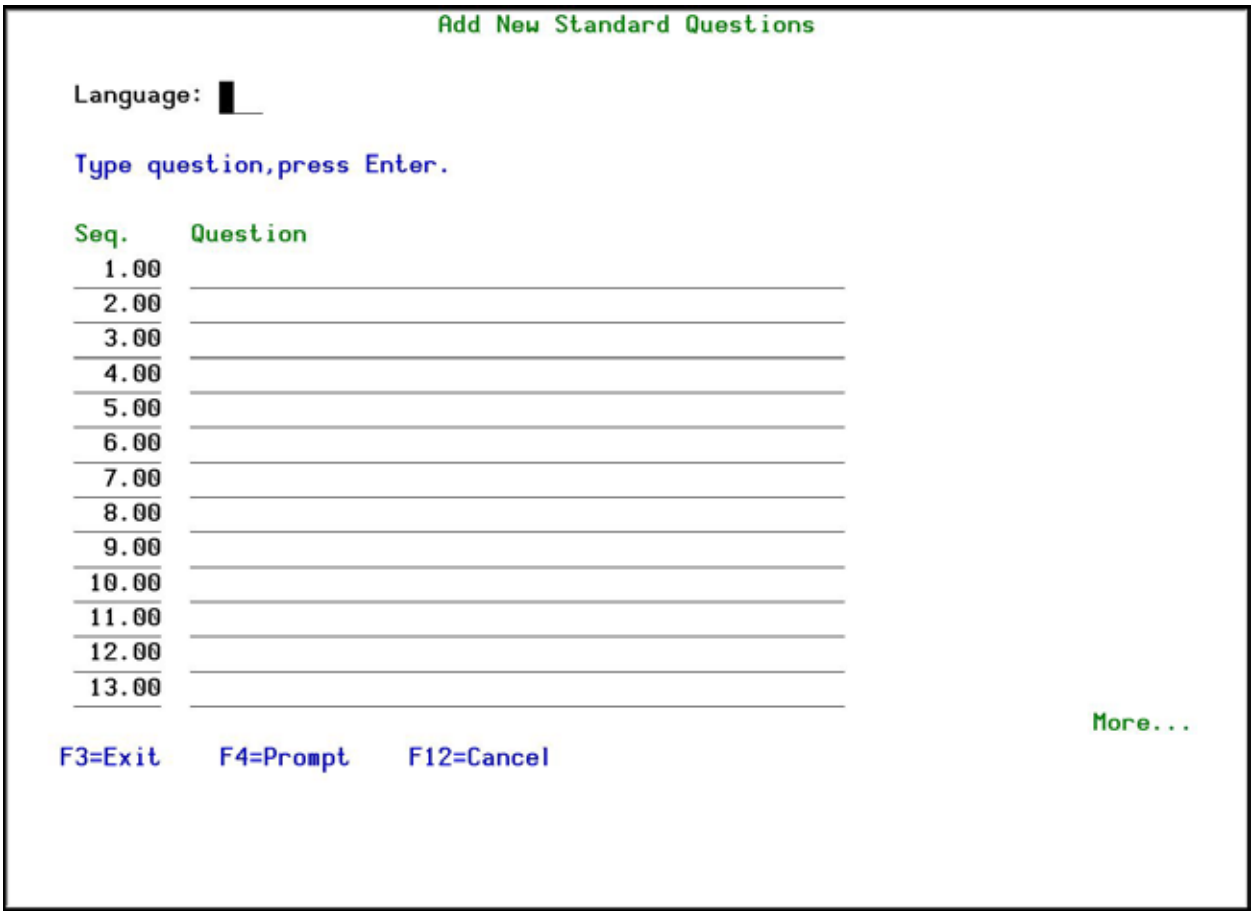
1. Select **38. Standard Questions** in the **Password Reset** main menu. The **Work with Standard Questions** screen appears.



Work with Standard Questions screen

Field/Option/Command Key	Description
1=Select	Opens the **Modify Standard Questions** screen for the selected language.
3=Copy questions	Opens the **Copy Standard Questions** screen for the selected language.
4=Delete	Opens the **Delete Standard Questions** screen for the selected language.
Opt	Enter your chosen option here.
Language	The languages for which Standard Questions are available that can be assigned to a User.
F6=Add new	Opens the **Add New Standard Questions** screen.

2. Press **F6=Add new**. The **Add New Standard Questions** screen appears.



Add Standard Questions screen

Field/Option/Command Key	Description
Language	The language for which questions are being defined. Press **F4** to see a list of possible languages.
Seq.	Sequence number to define the order in which the questions are asked.
Question	A question to which only the Person knows the answer.

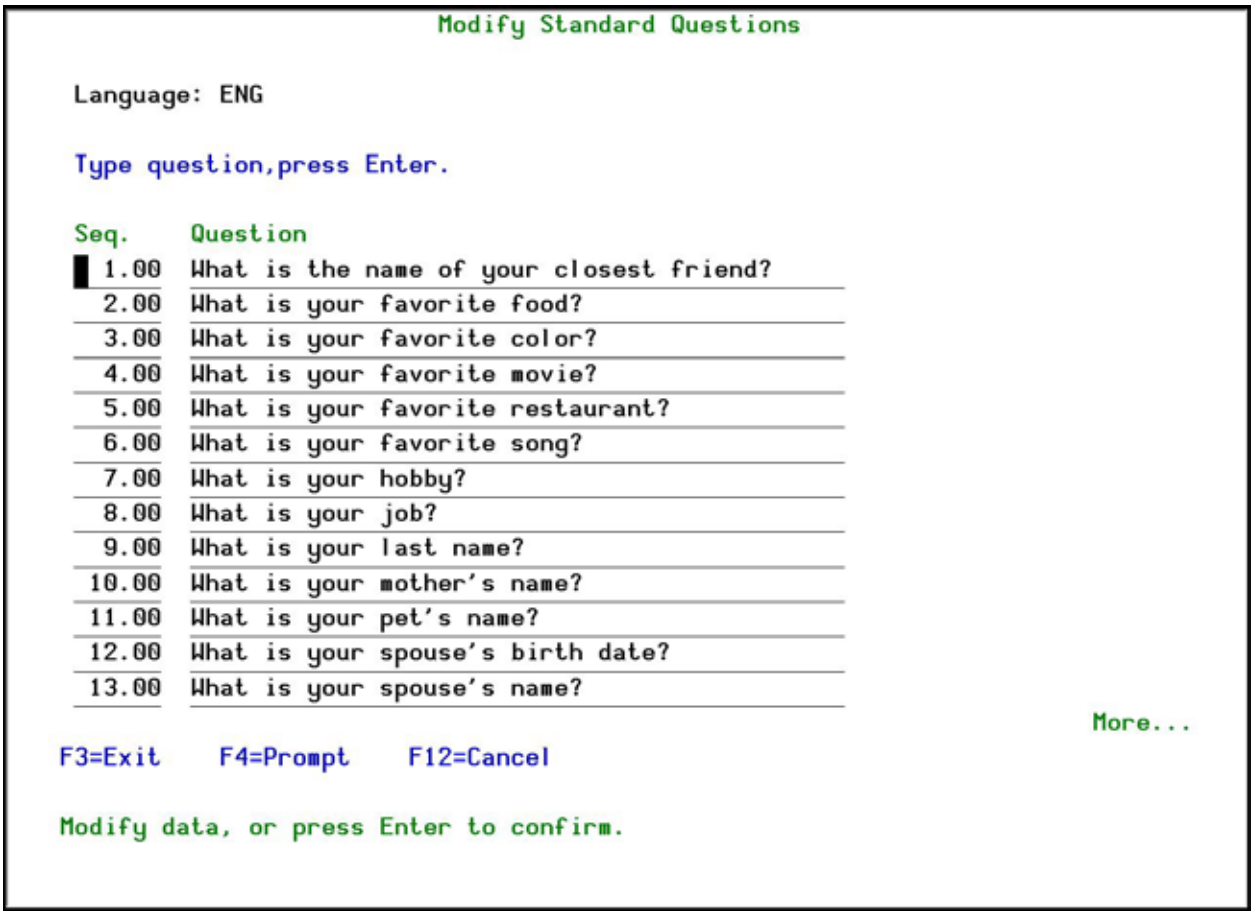
3. Add a new language, enter the appropriate questions and press **Enter**. The new questions are added and the language appears in the **Work with Standard Questions** screen.

Modify Standard Questions

You can modify both the actual questions and also the order in which they will appear.

To modify Standard Questions:

1. Select **38. Standard Questions** in the **Password Reset** main menu. The **Work with Standard Questions** screen appears.
2. Select the language for which you want to modify questions and press **1=Select**. The Modify Standard Questions screen appears.



Modify Standard Questions screen

Field/Option/Command Key	Description
Language	The language for which questions are being defined (read only).
Seq.	Sequence number to define the order in which the questions are asked.
Question	A question to which only the Person knows the answer.

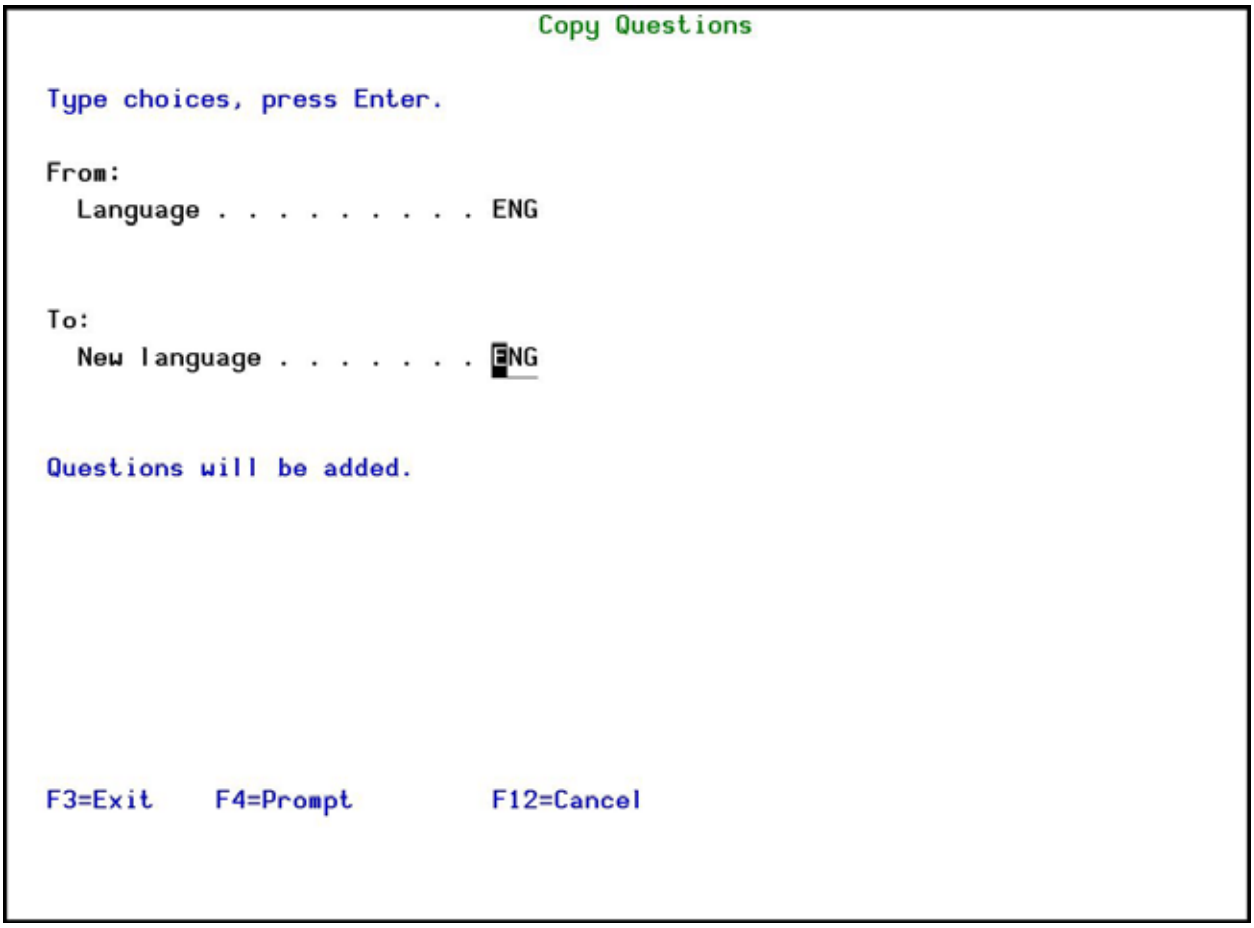
3. Modify the required questions and press **Enter**. You are returned to the **Work with Standard Questions** screen.

Copy Standard Questions

The Copy Standard Questions screen allows you to create questions for a new language by copying questions from an existing language to a new language and then updating the necessary fields in the **Modify Standard Questions** screen.

To copy Standard Questions:

1. Select **38. Standard Questions** in the **Password Reset** main menu. The **Work with Standard Questions** screen appears.
2. Select the language for which you want to copy questions and press **3=Copy**. The **Copy Standard Questions** screen appears.



Copy Standard Questions screen

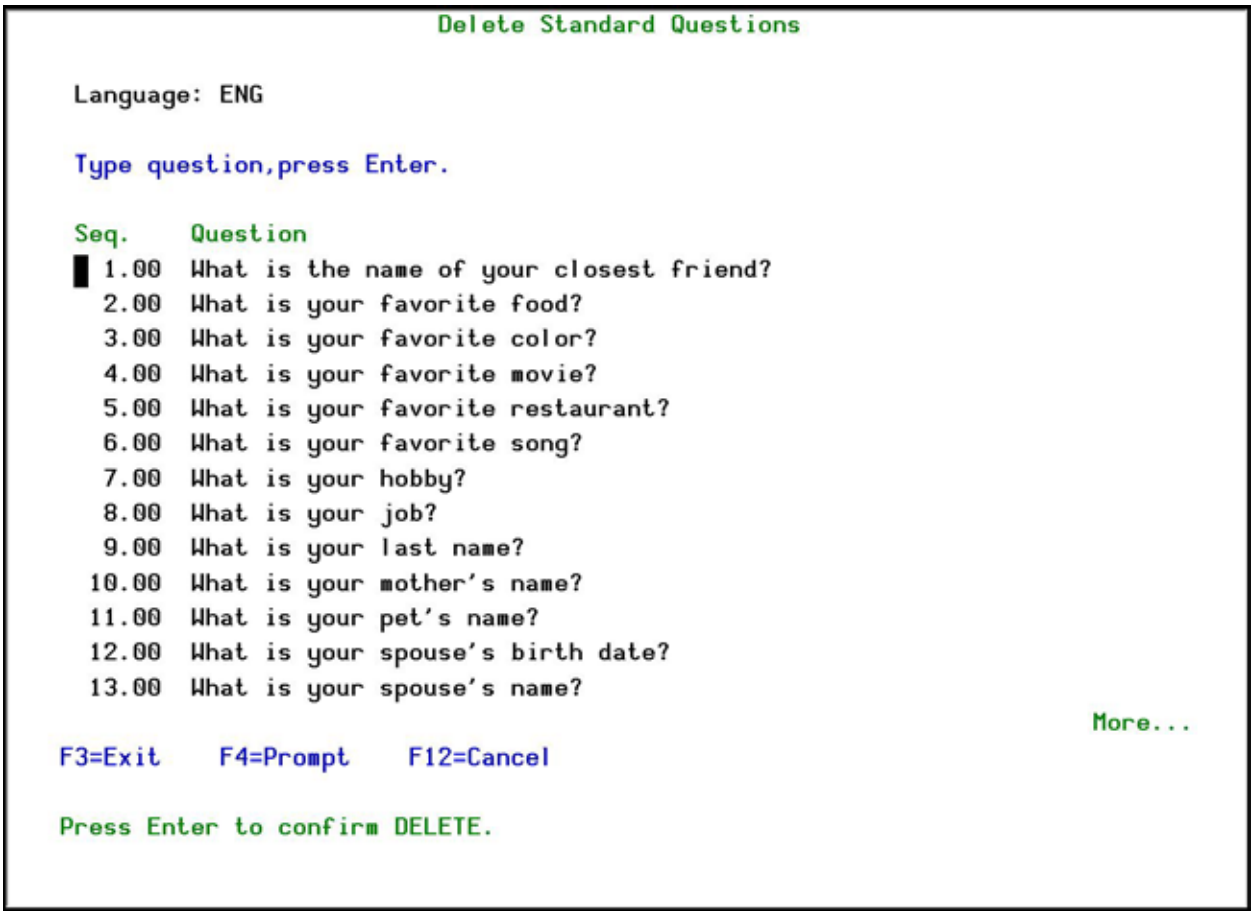
Field/Option/Command Key	Description
From Language	The language from which you are copying (read only).
To New language	The language to which you are copying.

3. Enter the new language and press **Enter**. You are returned to the **Work with Standard Questions** screen. You can modify the actual questions in the **Modify Standard Questions** screen.

Delete Standard Questions

To delete Standard Questions:

1. Select **38. Standard Questions** in the **Password Reset** main menu. The **Work with Standard Questions** screen appears.
2. Select the language which you want to delete from the standard questions and press **4=Delete**. The **Delete Standard Questions** screen appears.



Delete Standard Questions screen

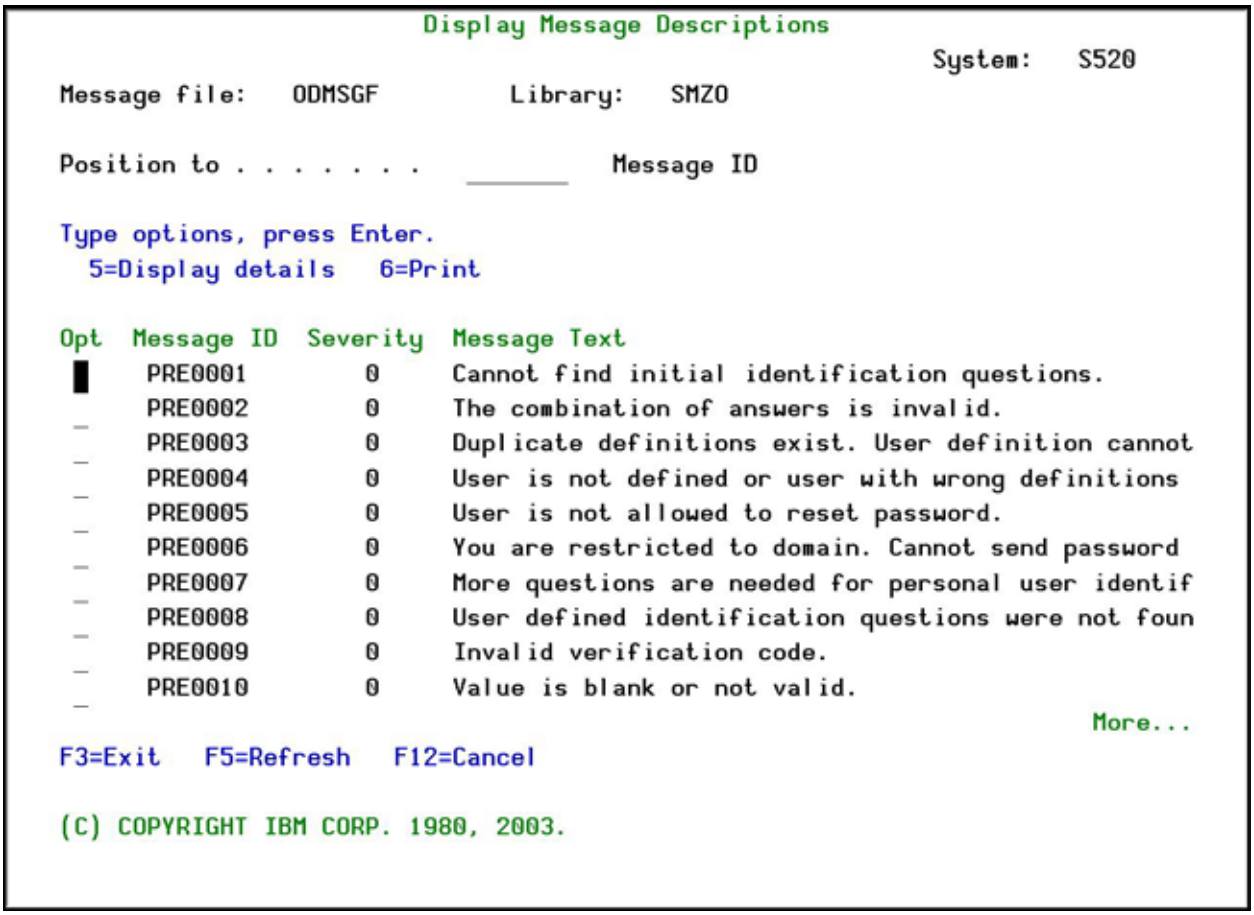
3. Press **Enter**. The updated **Work with Standard Questions** screen appears.

Display Error ID Descriptions

Display the messages that relate to errors received when trying to restore a password. This screen allows the Helpdesk to tell users why their password attempt restore failed.

To display messages:

1. Select **39. Error IDs** in the **Password Reset** main menu. The **Display Message Descriptions** screen appears.



Display Message Descriptions

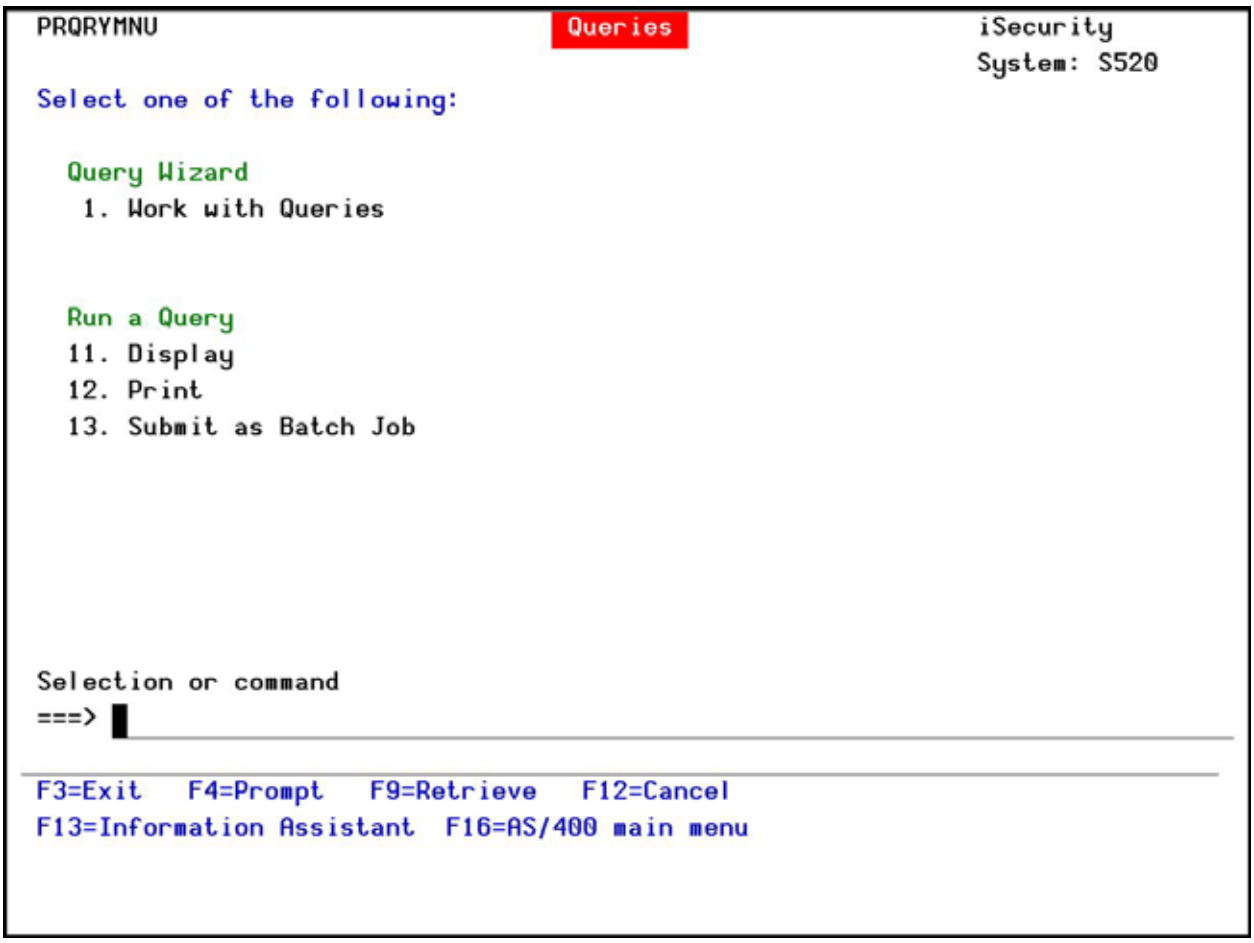
For a description of the fields and options on this screen, please refer to the IBM documentation.

Reporting

Create a New Query

To create a new query:

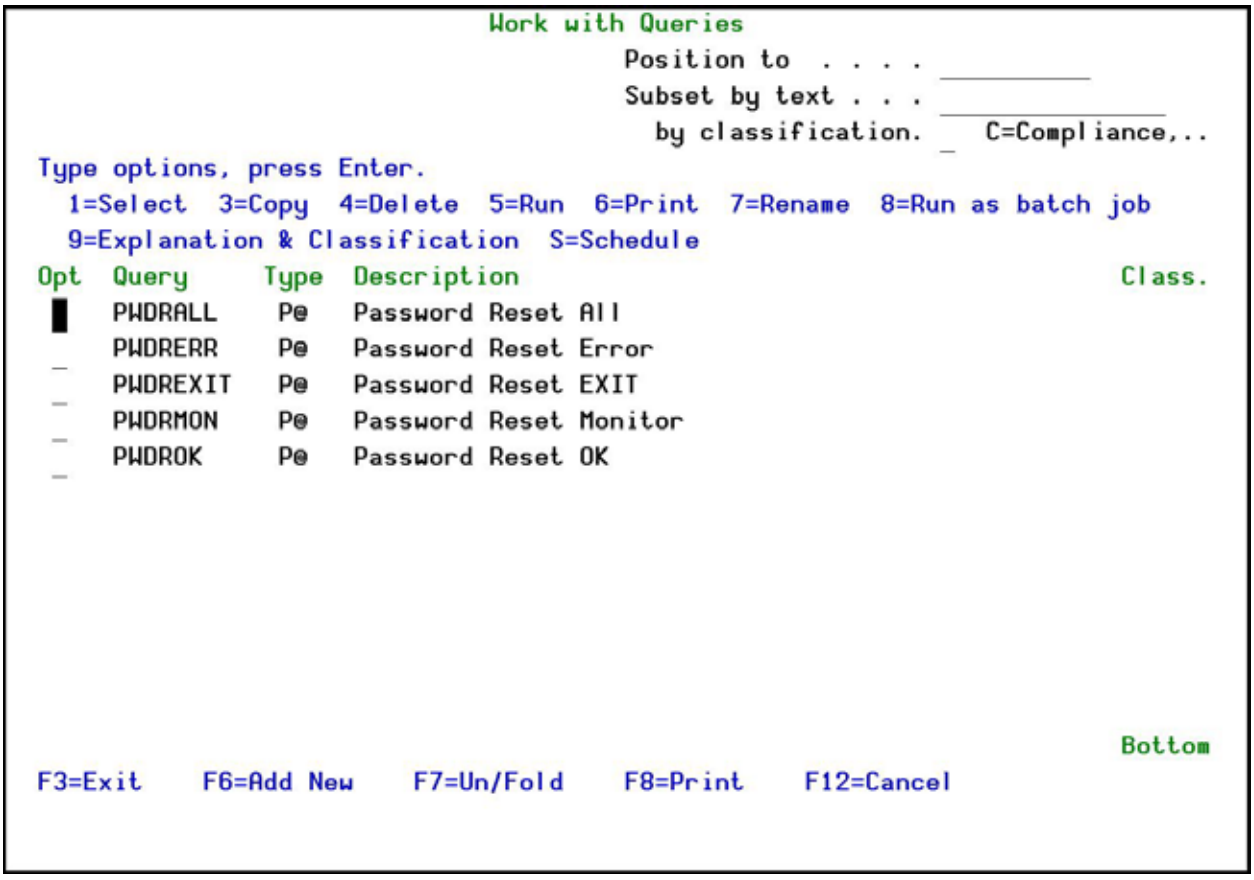
1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.



Queries Menu

Field/Option/Command Key	Description
1. Work with Queries	Opens the **Work with Queries** screen.
11. Display	Opens the **Select Query for DISPLAY** screen.
12. Print	Opens the **Select Query for PRINT** screen.
13. Submit as Batch Job	Opens the **Select Query for SUBMIT** screen.

2. Select **1. Work with Queries** in the **Queries** menu.

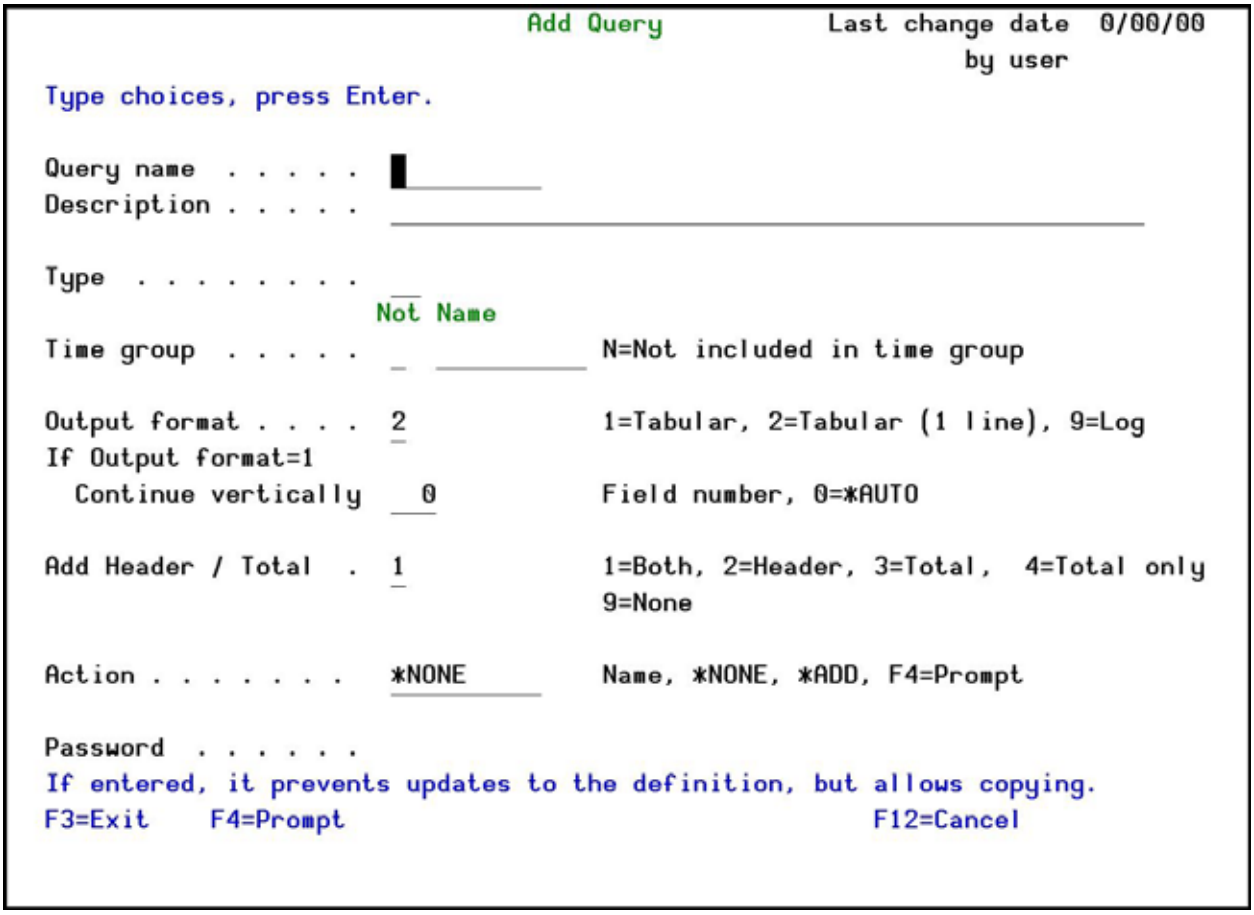


Work with Queries screen

Field/Option/Command Key	Description
1=Select	Opens the **Modify Queries** screen, to allow you to modify the selected query.
3=Copy	Opens the **Copy Queries** screen, to allow you to copy the selected query.
4=Delete	Opens the **Delete Queries** screen, to allow you to delete the selected query.
5=Run	Opens the **Run Queries** screen, to allow you to run the selected query.
6=Print	Opens the **Print Queries** screen, to allow you to print the selected query to a standard output device and file type (***PDF**, ***HTML**, ***CSV**, and so on).
7=Rename	Opens the **Rename Queries** screen, to allow you to rename the selected query.
8=Run as batch job	Opens the **Run a Query as a Batch Job** screen, to allow you to run the selected query in batch mode.
9=Explanation & Classification	Opens the **Explanation and Classification of Queries** screen.
S=Schedule	Opens the **Schedule Queries** screen, to allow you to schedule the selected query to run at a later date or time.
Query	The name of the Query.

Field/Option/Command Key	Description
Type	The type of the Query
Description	The description of the Query
F6=Add New	Opens the **Add Query** screen, to allow you to define a new query.

3. Press **F6=Add New**. The **Add Query** screen appears.



Add Query screen

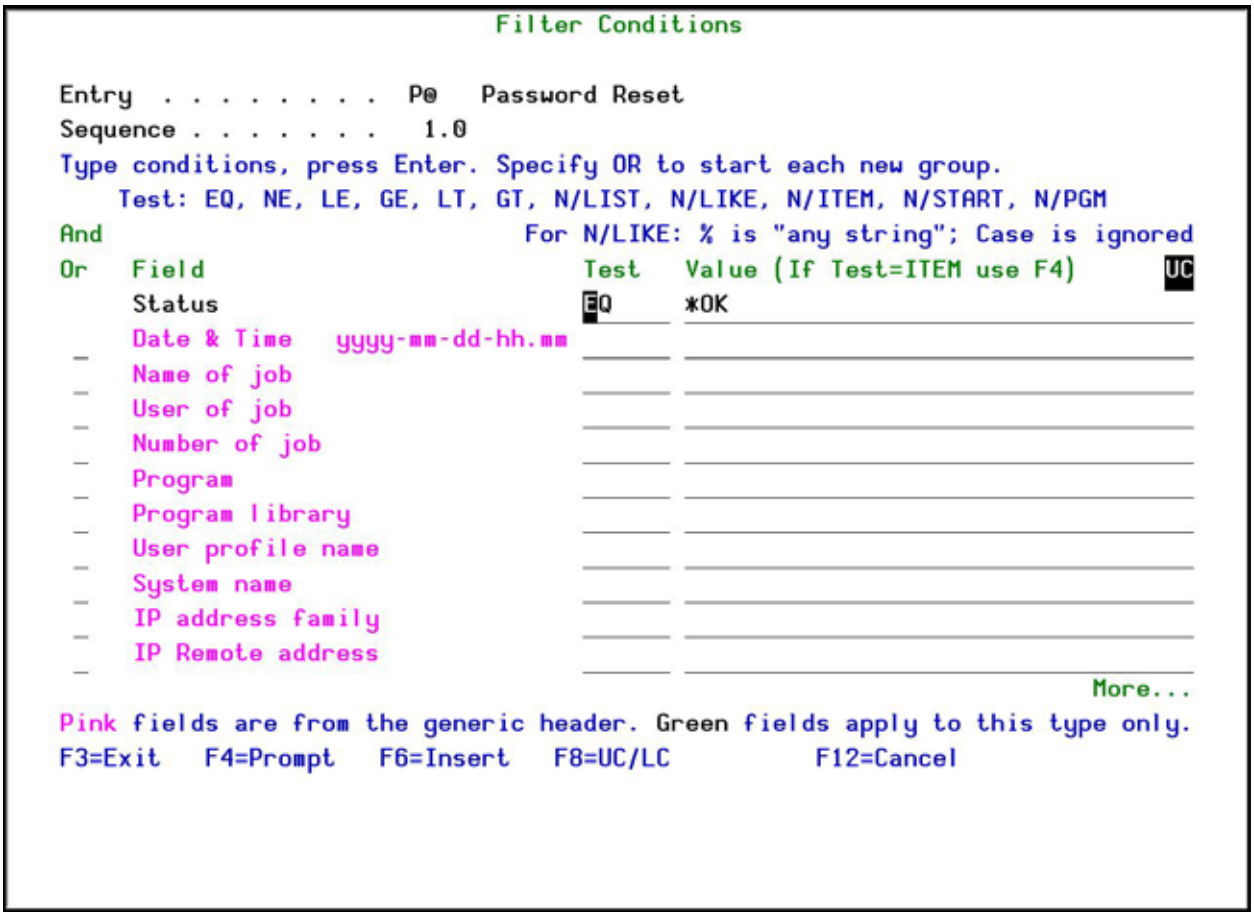
Field/Option/Command Key	Description
Query name	Enter the name of the Query.
Description	Enter a meaningful description for the Query.
Type	Enter the Query Type. Press **F4** for a list of options. For **Password Reset**, the only valid type is **P@**.
Time group	You can define the Query to only run during the times defined in a Time Group. If you enter **N** in the Not field, the Query can only run in the times outside those defined in the Time Group.
Output format	Define the output format: 1=Tabular 2=Tabular (1 line) 9=Log
Continue vertically	If you select tabular output, define the field to continue with

Field/Option/Command Key	Description
Add Header / Total	Define if the Query should show Headers/Totals 1=Both 2=Header 3=Total 4=Total only 9=None
Action	You can define an action to be performed after running the
Password	You can password protect a Query to prevent updates to the Query.

4. Continue with the screens that define the Query, as described below.

Filter Conditions Screen

The Filter Conditions screen appears immediately after you define the basic query parameters for a single audit type query or after you define a filter rule for a multiple audit type query. You can include multiple filter conditions in your definition. Each filter condition consists of a comparison test applied to one of the fields in the history log record.



Filter Conditions screen

Field/Option/Command Key	Description
And/Or	**A** or Blank = And **O** = Or

Field/Option/Command Key	Description
Field	Data field in the history log **Pink** fields are part of the generic header common to all journal types **Green** fields represent data specific to this journal entry type
Test	Comparison test type – see table on the following page for details
Value	Value to be used as the comparison text. Note that this filed is case sensitive.
F4	Displays explanatory information and/or options applicable to the data field on the line where the cursor is located
F6	Select another comparison test from a pop-up window and insert it at the current cursor position
F8	Change Caps Lock from lower to upper case. An indicator appears on the screen.

Filter conditions are optional. If no filter conditions are defined, your query will include all events for the specified audit type or types.

Comparison Test Operators

Several different types of comparison test operators are available as shown in the following table:

Test	Description	Value Field Data
EQ,NE	Equal to, Not equal to	Value
LT, LE	Less than, Less than or equal to	Value
GT, GE	Greater than, Greater than or equal to	Value
LIST, NLIST	Included in list, Not included in list	Values separated by a space
LIKE, NLIKE	Substring search	Value preceded and/or followed by **%**
ITEM/NITEM	Item in a group checks if the value is among the groups' members. The General group is an external value list that can be extended by creating new types.	· ***USER** – Check that the value is a user in a **%GROUP** of users · ***GRPPRF** – Check that the value is a user in an **OS/400 Group Profile** · ***USRGRP** – USER and all user profiles which are members of same user groups as USER · ***ALL** – For both ***GRPPRF** and ***USRGRP** cases · If the **TYPE** is missing, ***USER** or ***USRGRP** is assumed based on the appearance of % sign as the first character in the **GROUP**. · ***SPCAUT** – Check that the value is in the users Special-Authority
START	Starts with	Starting characters of string

And/Or Boolean Operators

You can combine multiple filter conditions in one query using Boolean AND/OR operators. This allows you to create complex queries that produce precise results.

When using 'Or' operators in your filter conditions, the order in which each condition appears in the list conditions is critical. The 'Or' operator allows you to group several conditions together because it includes all 'And' conditions that follow it until the next 'Or' operator or until the end of the list.

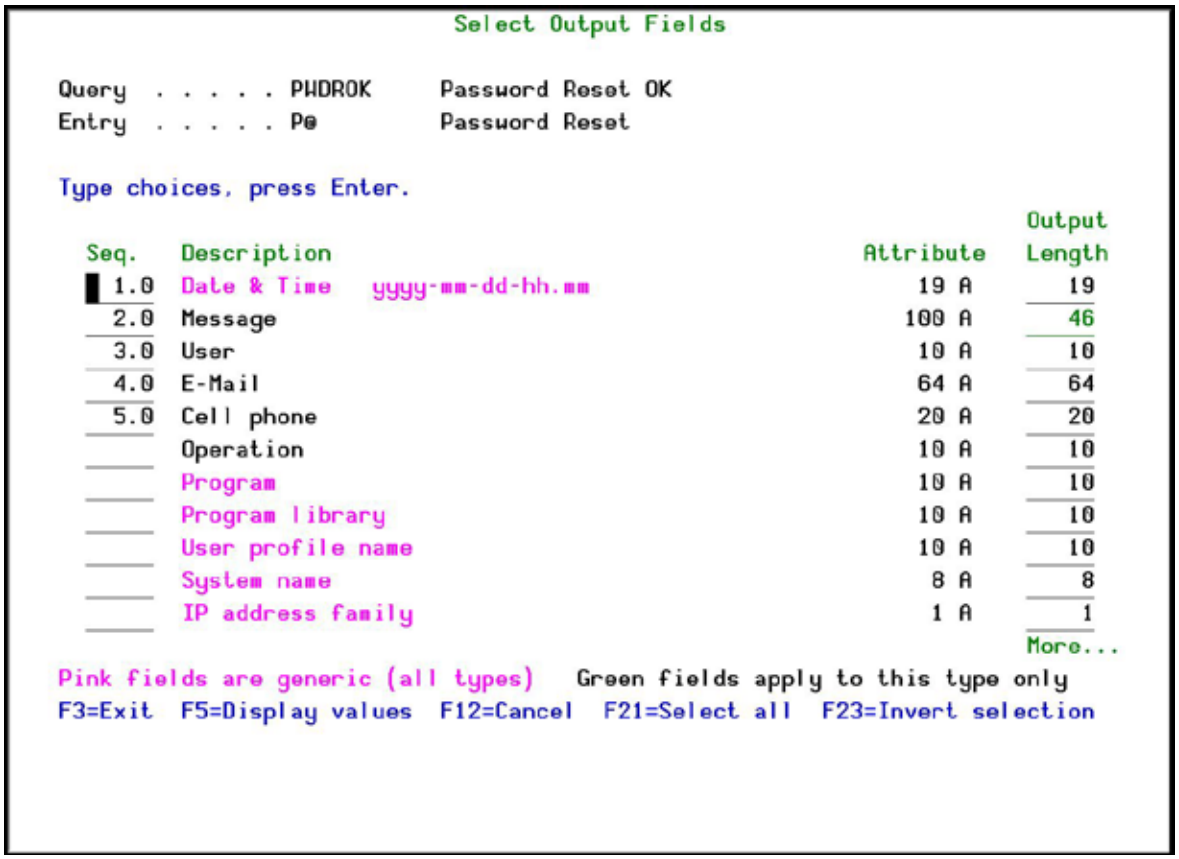
Select Output Fields Screen

The Select Output Fields screen allows you to select those fields from the history log that will appear in the query output and in which order they should appear from left to right. Fields appear in ascending on order the screen, with the top field corresponding to the left-hand field in the query report. The second field corresponds to field the field to the right of the left-hand field, and so on.

You change the order of the fields simply by modifying the sequence numbers. To delete a field from the query report, delete the sequence number. When you press Enter, the new field sequence appears on the screen, with deleted (blank sequence number) fields appearing at the bottom.

You must select at least one field for output.

Fields shown in pink are part of the generic header and are common to the history log record for all audit types. Fields shown in green (on the screen) are specific to the history log record for the currently selected audit type only.



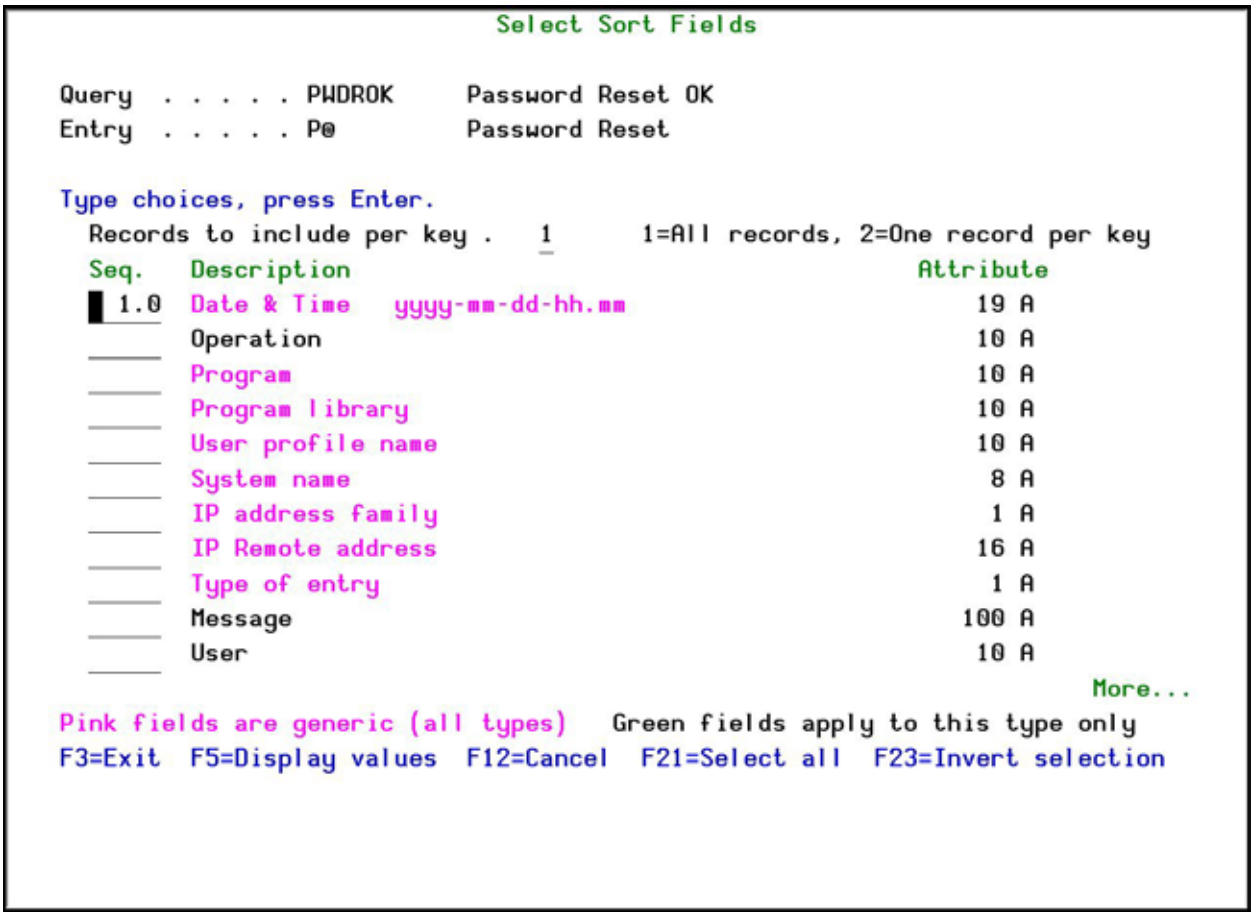
Select Output Fields screen

Field/Option/Command Key	Description
F5	Displays field values
F21	**Select all** – selects all fields
F23	**Invert selection** – All selected items will be deselected and all items that are not selected will become selected. **NOTE**: You might wish to change the sequence numbers after using this command
Seq.	Enter the sequence you wish this field to appear in the query output. Lower numbers appear toward the left of the report and higher numbers appear toward the right.

Select Sort Fields Screen

You can sort records in your query output according to any combinations of fields in the history log record. The lowest sequence number (normally 1.0) represents the primary sort field. The second lowest number (normally 2.0) represents the secondary sort field, and so on.

Fields shown in pink are part of the generic header and are common to the history log record for all audit types. Fields appearing in green (on the screen) are specific to the history log record for the currently selected audit type.

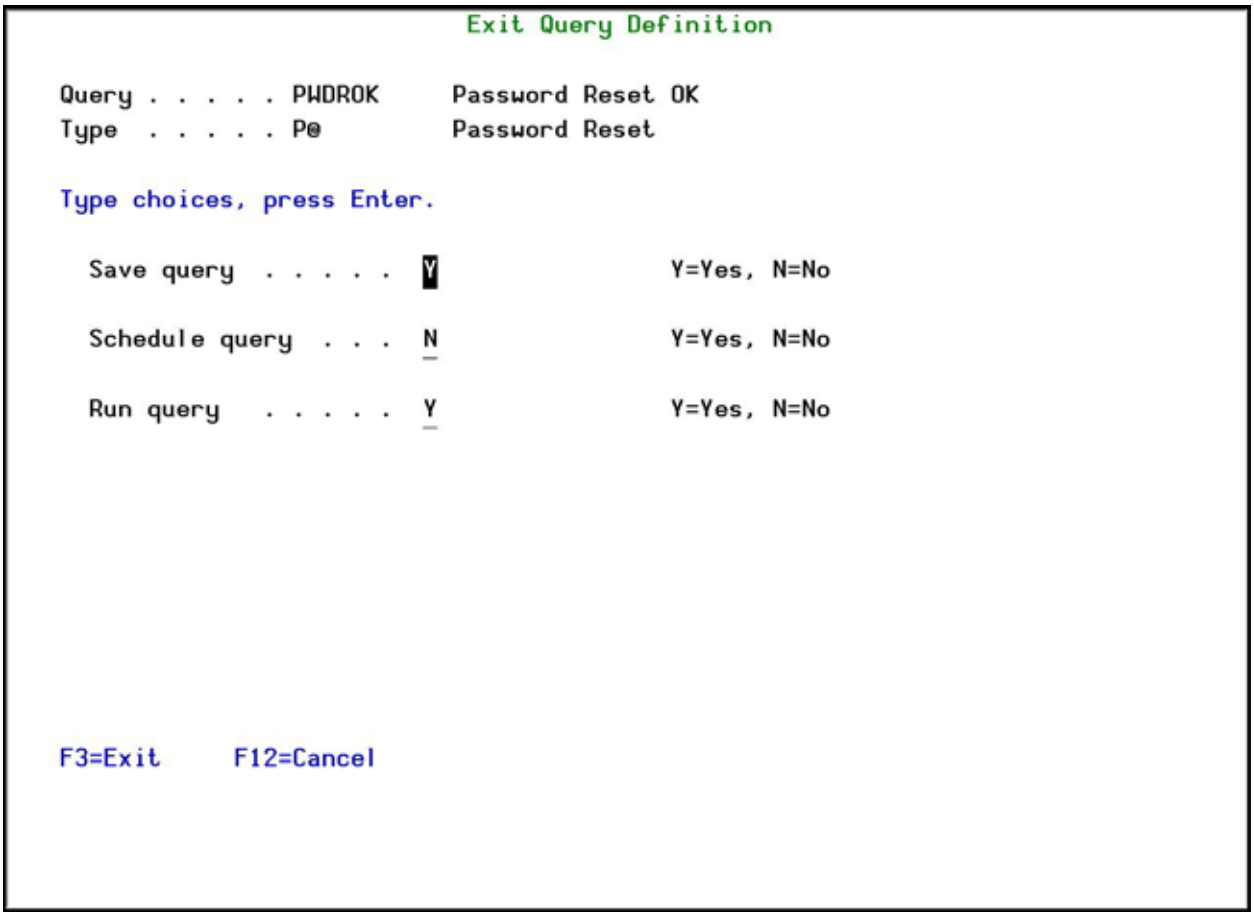


Select Sort Fields screen

Field/Option/Command Key	Description
F5	Displays field values
F21	**Select all –** selects all fields
F23	**Invert selection** – All selected items will be deselected and all items that are not selected will become selected. **NOTE**: You might wish to change the sequence numbers after using this command
Seq.	Enter a number representing the sort sequence.

Exit Query Definition Screen

Upon exiting the query definitions, select to save the query, catalog the report in the report scheduler and whether to run the query now.



Exit Query Definition screen

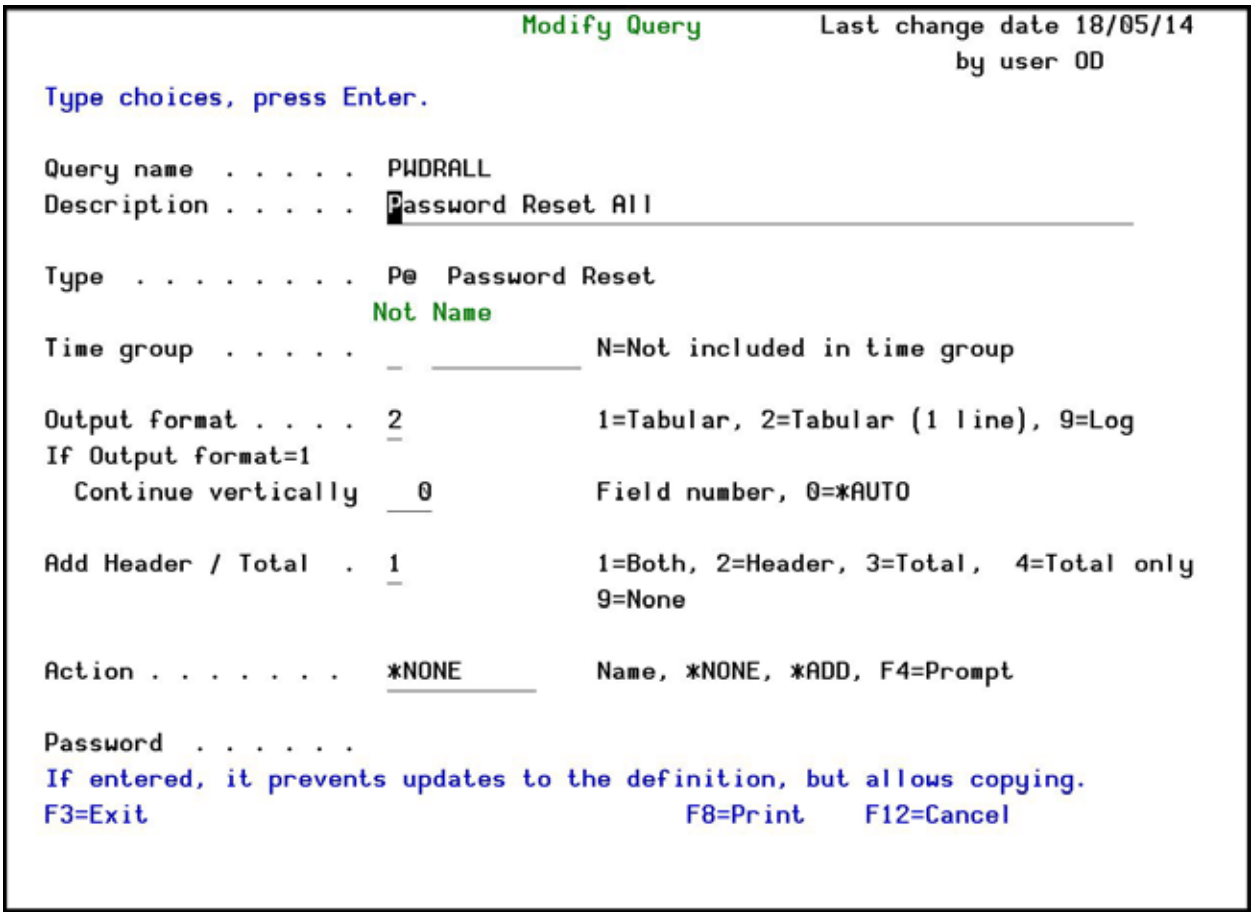
Modify a Query

You may want to fine tune a query, to create your own version of a Raz-Lee query or to create a new query based on an existing query.

To modify a query:

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **1. Work with Queries** in the **Queries** menu. The **Work with Queries** screen appears.

3. Select the Query to copy and press **1=Select**. The **Modify Query** screen appears.



Modify Query screen

Field/Option/Command Key	Description
Query name	The name of the Query (read only).
Description	The description of the Query (read only).
Type	The Query Type (read only).
Time group	You can define the Query to only run during the times defined in a Time Group. If you enter **N** in the Not field, the Query can only run in the times outside those defined in the Time Group.
Output format	Define the output format: **1=Tabular** **2=Tabular (1 line)** **9=Log**
Continue vertically	If you select tabular output, define the field to continue with.
Add Header / Total	Define if the Query should show Headers/Totals **1=Both** **2=Header** **3=Total** **4=Total only** **9=None**

Field/Option/Command Key	Description
Action	You can define an action to be performed after running the Query.
Password	You can password protect a Query to prevent updates to the Query.

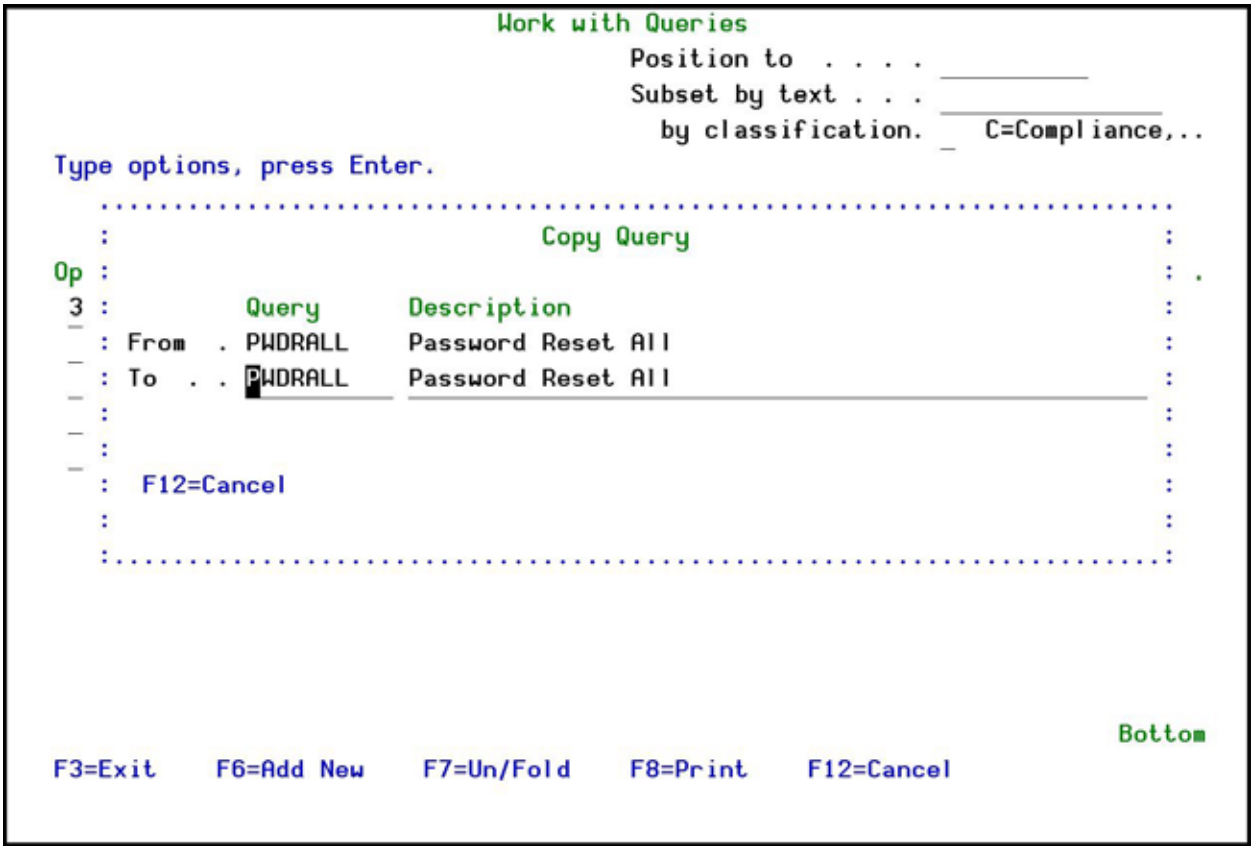
4. Enter your changes and press **Enter**. You should now continue with the rest of the screens as described in the **Create a New Query** procedure.

Copy a Query

You may want to create a new query similar to an existing query. Copy the query to a new name and then you can modify the new query.

To access:

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **1. Work with Queries** in the **Queries** menu. The **Work with Queries** screen appears.
3. Select the Query to copy and press **3=Copy**. The **Copy Query** window opens.



Copy Query screen

Field/Option/Command Key	Description
From	The Query from which you are copying (read only).
To	The Query to which you are copying. You can also change the Query description.

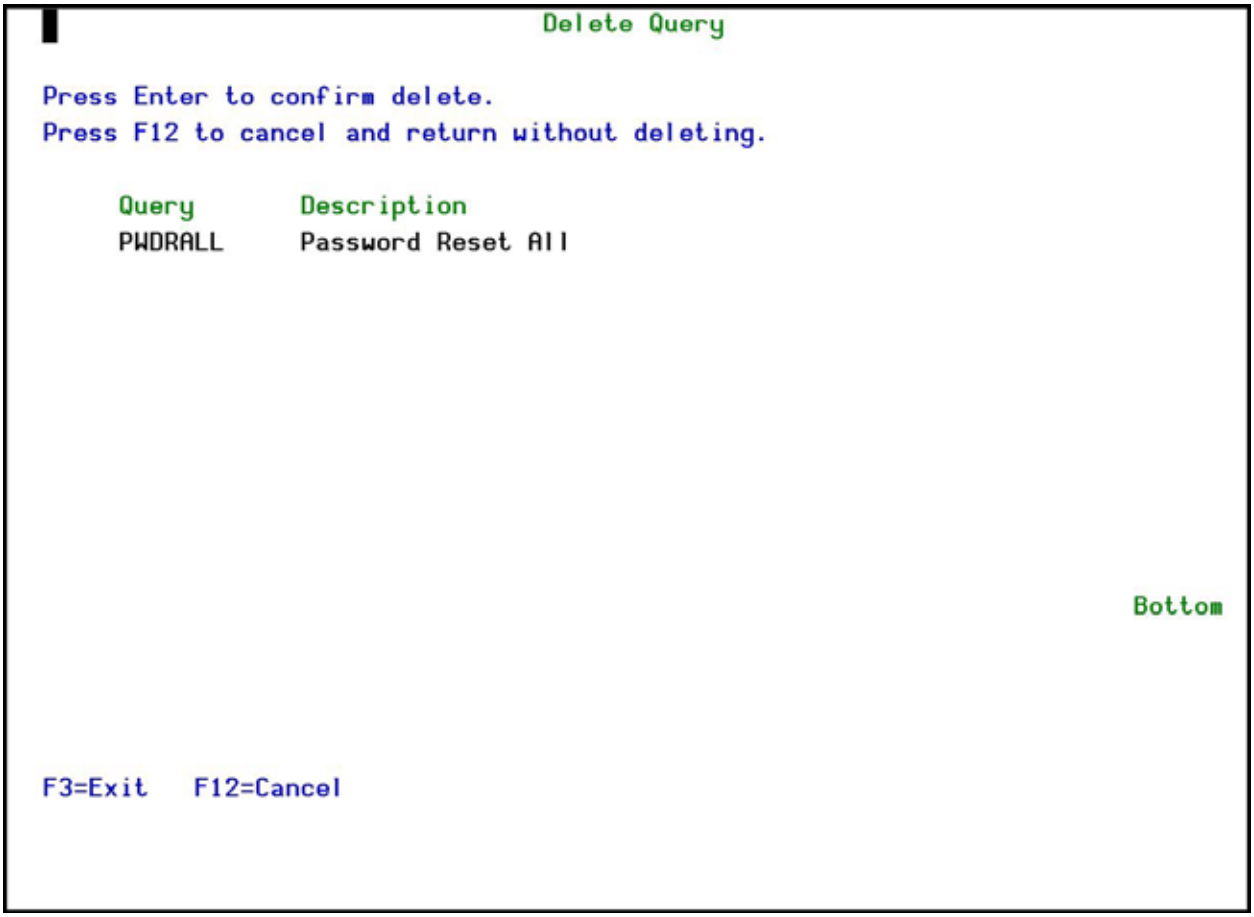
4. Enter the name and description of the new Query and press **Enter**. The updated **Work with Queries** screen appears.
5. Use the **Modify a Query** procedure to make the required changes to the new query.

Delete a Query

You can delete a query that is no longer in use.

To delete a query:

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **1. Work with Queries** in the **Queries** menu. The **Work with Queries** screen appears.
3. Select the Query to delete and press **4=Delete**. The **Delete Query** screen appears.



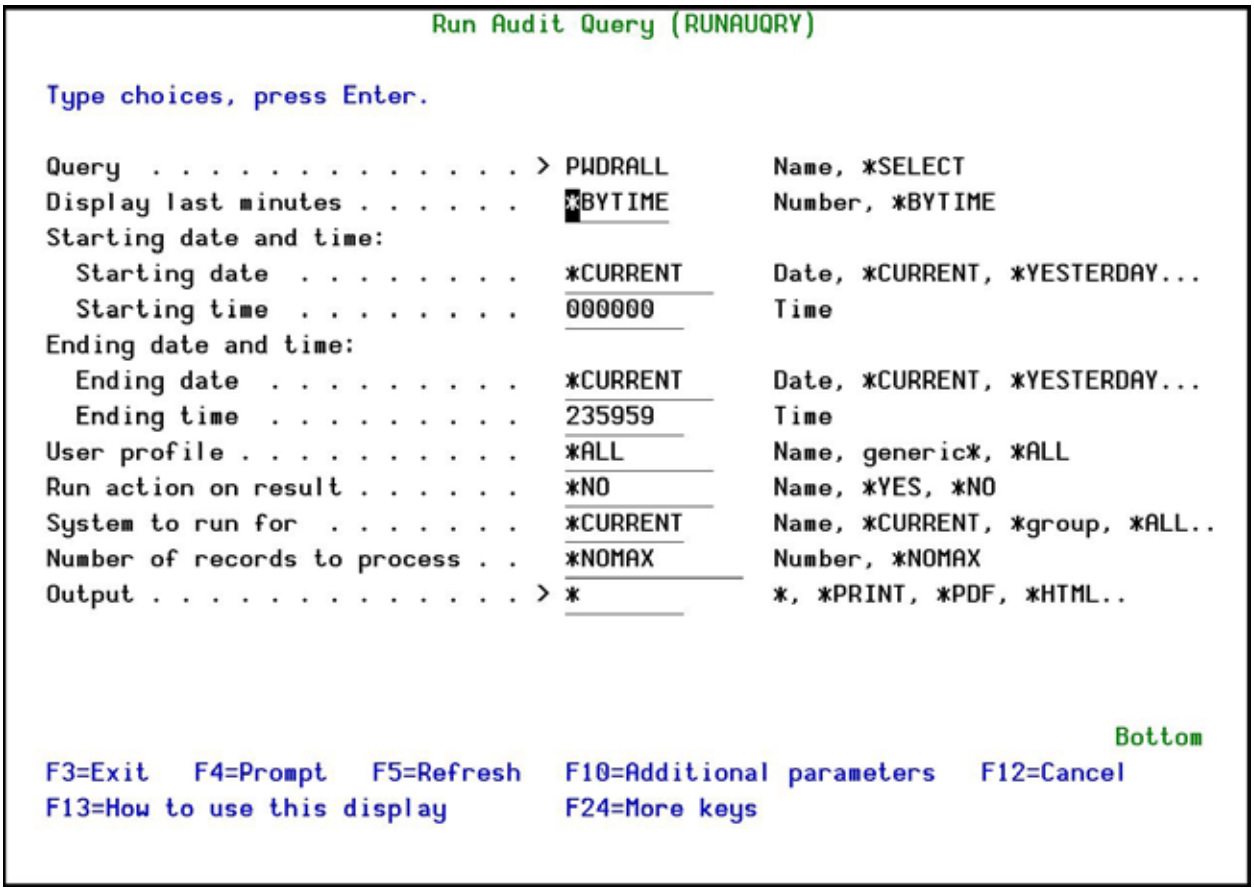
Delete Query screen

4. Press **Enter**. The Query is deleted and the updated **Work with Queries** screen appears.

Run a Query

To run a query:

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **1. Work with Queries** in the **Queries** menu. The **Work with Queries** screen appears.
3. Select the Query to run and press **5=Run**. The **Run Audit Query** screen appears.



Run Audit Query Online screen

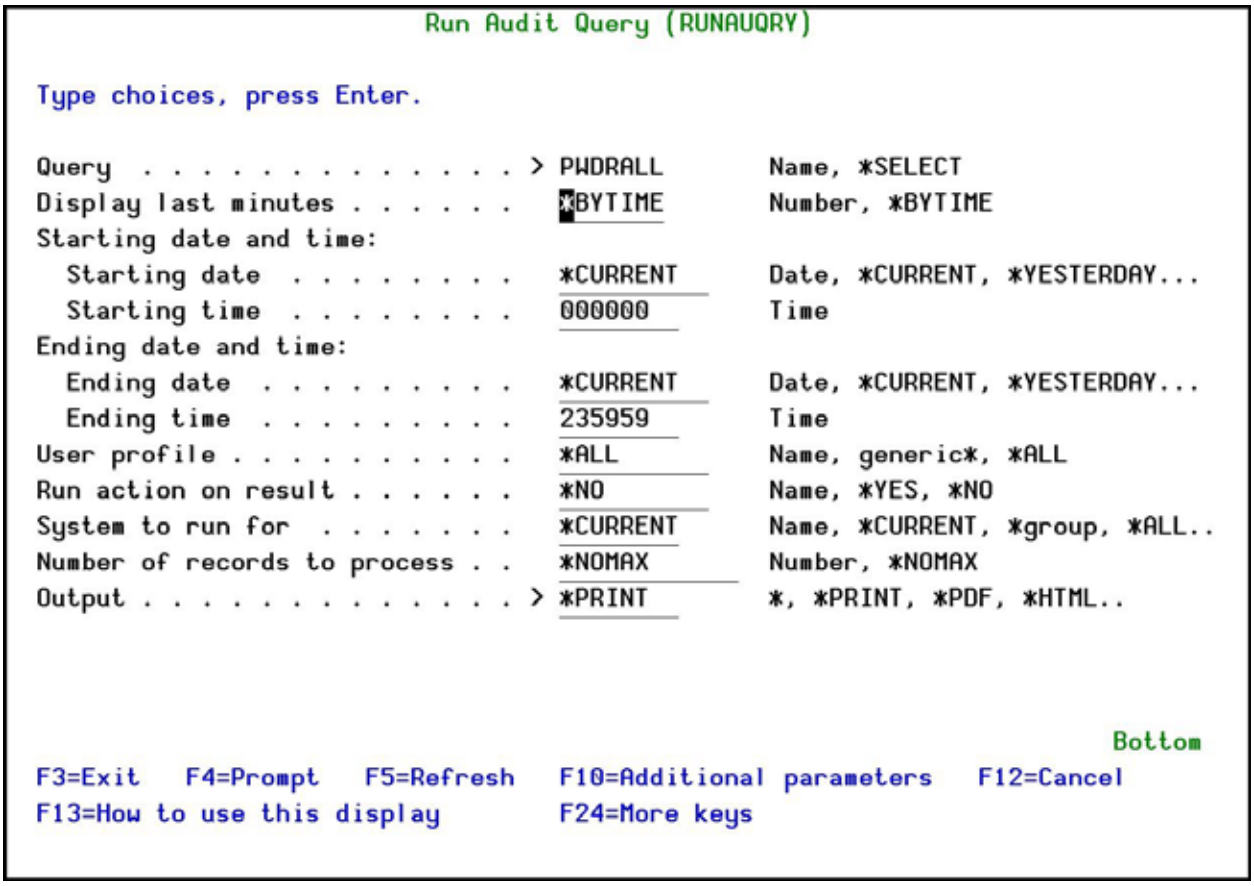
Field/Option/Command Key	Description
Query	**Name** = Name of query ***SELECT** = Select from list at run time
Display Last Minutes	Select only those records occurring within the previous number of minutes as specified by the user **Number** = Number of minutes
Starting Date and Time **Ending Date and Time**	Select only those records occurring within the range specified by the starting and ending time specified below ***CURRENT** = The current date (day the report runs) ***YESTERDAY** = The day before the current date ***WEEKSTR** = Beginning of the current week ***PRVWEEKSTR** = Beginning of the previous week ***MONTHSTR** = Beginning of the current month ***PRVMONTHSTR** = Beginning of the previous month ***YEARSTR** = Beginning of the current year ***PRVYEARSTR** = Beginning of the previous year ***MON - *SUN** = Day of the current (or previous) week **NOTE:** on all Raz-Lee Security queries ($A, $B, and so on), the time-related parameters and "User profile" are not relevant since these are "status" queries and not log (transaction) queries.
User Profile	Selects a subset of records by user profile

Field/Option/Command Key	Description
System to run for	The system to report information from: **SYSTEM** = the system to report information from ***CURRENT** = the current system **Name** = a system name that is defined in the **Work with Network Definitions** option of the **Audit Central Administration** ***Name** = a group of systems as defined in the **Work with Network Definitions** option of the **Audit Central Administration** ***ALL** = all the systems defined in the **Work with Network Definitions** option of the **Audit Central Administration**
Number of Records to Process	Maximum number of records to process ***NOMAX** = No maximum (Default)
Output	***** = Display ***Print** = Printed report ***PDF** = Print report to PDF outfile ***HTML** = Print report to HTML outfile ***CSV** = Print report to CSV outfile ***OUTFILE** = Print report to view from the GUI.
Audit Type	Filter records by audit type ***All** = All audit types as specified in the query definition **F4** = Select OS/400 audit type group from a list
Program Name	Filter records by the name of the program that created the journal record.
Job Name User	Filter records by IBM i (OS/400) job name.
Job Name - Number	Filter records by IBM i (OS/400) job number.
Filter by Time Group – Relationship	***IN** = Include all records in time group ***OUT** = Include all records not in time group ***NONE** = Do not use time group, even if included in query definition ***QRY** = Use time group as specified in query definition
Filter by Time Group – Time Group	**Name** = Name of time group ***SELECT** = Select time group from list at run time

4. Enter your parameters (do ***NOT*** change the **Output** parameter) and press **Enter**. The query is run and the output is displayed on the screen.

Print a Query

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **1. Work with Queries** in the **Queries** menu. The **Work with Queries** screen appears.
3. Select the Query to run and press **6=Run**. The **Run Audit Query** screen appears.



Run Audit Query to Print screen

Field/Option/Command Key	Description
Query	**Name** = Name of query ***SELECT** = Select from list at run time
Display Last Minutes	Select only those records occurring within the previous number of minutes as specified by the user **Number** = Number of minutes
Starting Date and Time **Ending Date and Time**	Select only those records occurring within the range specified by the starting and ending time specified below ***CURRENT** = The current date (day the report runs) ***YESTERDAY** = The day before the current date ***WEEKSTR** = Beginning of the current week ***PRVWEEKSTR** = Beginning of the previous week ***MONTHSTR** = Beginning of the current month ***PRVMONTHSTR** = Beginning of the previous month ***YEARSTR** = Beginning of the current year ***PRVYEARSTR** = Beginning of the previous year ***MON - *SUN** = Day of the current (or previous) week **NOTE:** on all Raz-Lee Security queries ($A, $B, and so on), the time-related parameters and "User profile" are not relevant since these are "status" queries and not log (transaction) queries.
User Profile	Selects a subset of records by user profile

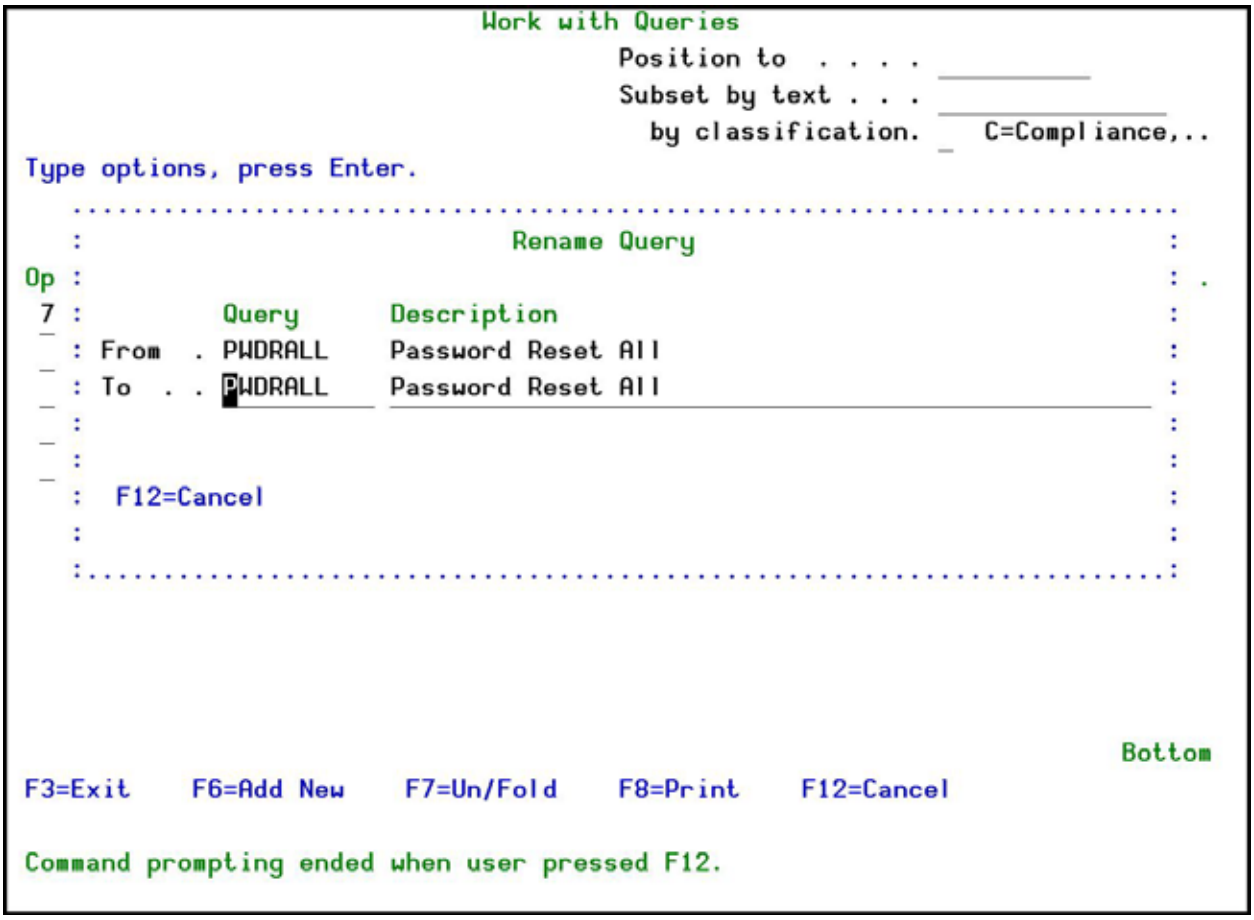
Field/Option/Command Key	Description
System to run for	The system to report information from: **SYSTEM** = the system to report information from ***CURRENT** = the current system **Name** = a system name that is defined in the **Work with Network Definitions** option of the **Audit Central Administration** ***Name** = a group of systems as defined in the **Work with Network Definitions** option of the **Audit Central Administration** ***ALL** = all the systems defined in the **Work with Network Definitions** option of the **Audit Central Administration**
Number of Records to Process	Maximum number of records to process ***NOMAX** = No maximum (Default)
Output	***** = Display ***Print** = Printed report ***PDF** = Print report to PDF outfile ***HTML** = Print report to HTML outfile ***CSV** = Print report to CSV outfile ***OUTFILE** = Print report to view from the GUI.
Audit Type	Filter records by audit type ***All** = All audit types as specified in the query definition **F4** = Select OS/400 audit type group from a list
Program Name	Filter records by the name of the program that created the journal record.
Job Name User	Filter records by IBM i (OS/400) job name.
Job Name - Number	Filter records by IBM i (OS/400) job number.
Filter by Time Group – Relationship	***IN** = Include all records in time group ***OUT** = Include all records not in time group ***NONE** = Do not use time group, even if included in query definition ***QRY** = Use time group as specified in query definition
Filter by Time Group – Time Group	**Name** = Name of time group ***SELECT** = Select time group from list at run time

4. Enter your parameters (do ***NOT*** change the **Output** parameter) and press **Enter**. The query is run and the output is displayed on the screen.

Rename a Query

To rename a query:

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **1. Work with Queries** in the **Queries** menu. The **Work with Queries** screen appears.
3. Select the Query to run and press **7=Rename**. The **Rename Query** window opens.



Rename Query screen

Field/Option/Command Key	Description
From	The current name and description of the Query.
To	The new name and description of the Query.

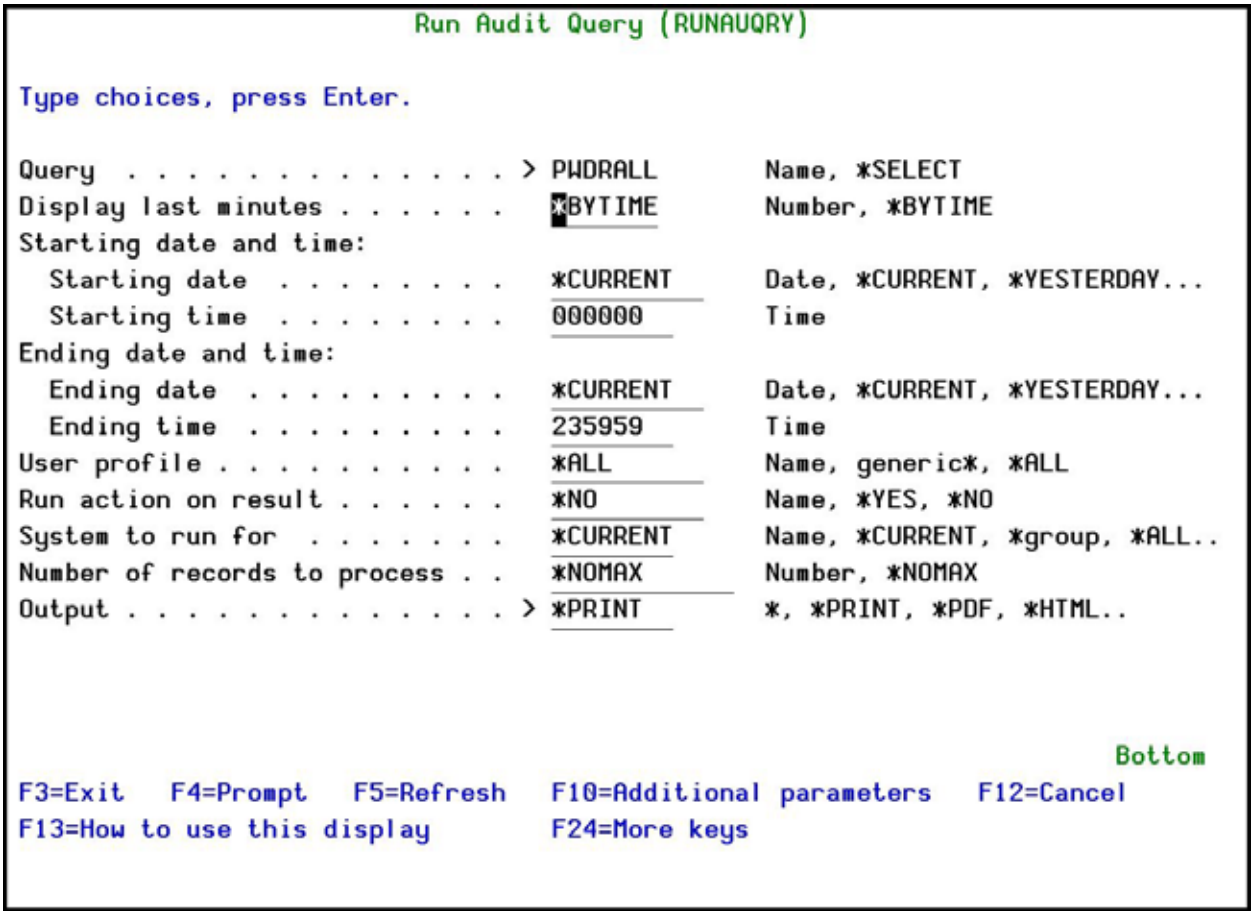
4. Enter the new name and description of the Query and press **Enter**. The updated **Work with Queries** screen appears.

Run a Query as a Batch Job

Running a query in batch mode (from the Job Queue) allows you to continue with other work while the query is running.

To run a query in batch:

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **1. Work with Queries** in the **Queries** menu. The **Work with Queries** screen appears.
3. Select the Query to run and press **8=Run as batch job**. The **Run Audit Query** screen appears.



Run Audit Query in a Batch Job screen

Field/Option/Command Key	Description
Query	**Name** = Name of query ***SELECT** = Select from list at run time
Display Last Minutes	Select only those records occurring within the previous number of minutes as specified by the user **Number** = Number of minutes
Starting Date and Time **Ending Date and Time**	Select only those records occurring within the range specified by the starting and ending time specified below ***CURRENT** = The current date (day the report runs) ***YESTERDAY** = The day before the current date ***WEEKSTR** = Beginning of the current week ***PRVWEEKSTR** = Beginning of the previous week ***MONTHSTR** = Beginning of the current month ***PRVMONTHSTR** = Beginning of the previous month ***YEARSTR** = Beginning of the current year ***PRVYEARSTR** = Beginning of the previous year ***MON - *SUN** = Day of the current (or previous) week **NOTE:** on all Raz-Lee Security queries ($A, $B, and so on), the time-related parameters and "User profile" are not relevant since these are "status" queries and not log (transaction) queries.

Field/Option/Command Key	Description
User Profile	Selects a subset of records by user profile
System to run for	The system to report information from: **SYSTEM** = the system to report information from ***CURRENT** = the current system **Name** = a system name that is defined in the **Work with Network Definitions** option of the **Audit Central Administration** ***Name** = a group of systems as defined in the **Work with Network Definitions** option of the **Audit Central Administration** ***ALL** = all the systems defined in the **Work with Network Definitions** option of the **Audit Central Administration**
Number of Records to Process	Maximum number of records to process ***NOMAX** = No maximum (Default)
Output	***** = Display ***Print** = Printed report ***PDF** = Print report to PDF outfile ***HTML** = Print report to HTML outfile ***CSV** = Print report to CSV outfile ***OUTFILE** = Print report to view from the GUI.
Audit Type	Filter records by audit type ***All** = All audit types as specified in the query definition **F4** = Select OS/400 audit type group from a list
Program Name	Filter records by the name of the program that created the journal record.
Job Name User	Filter records by IBM i (OS/400) job name.
Job Name - Number	Filter records by IBM i (OS/400) job number.
Filter by Time Group – Relationship	***IN** = Include all records in time group ***OUT** = Include all records not in time group ***NONE** = Do not use time group, even if included in query definition ***QRY** = Use time group as specified in query definition
Filter by Time Group – Time Group	**Name** = Name of time group ***SELECT** = Select time group from list at run time

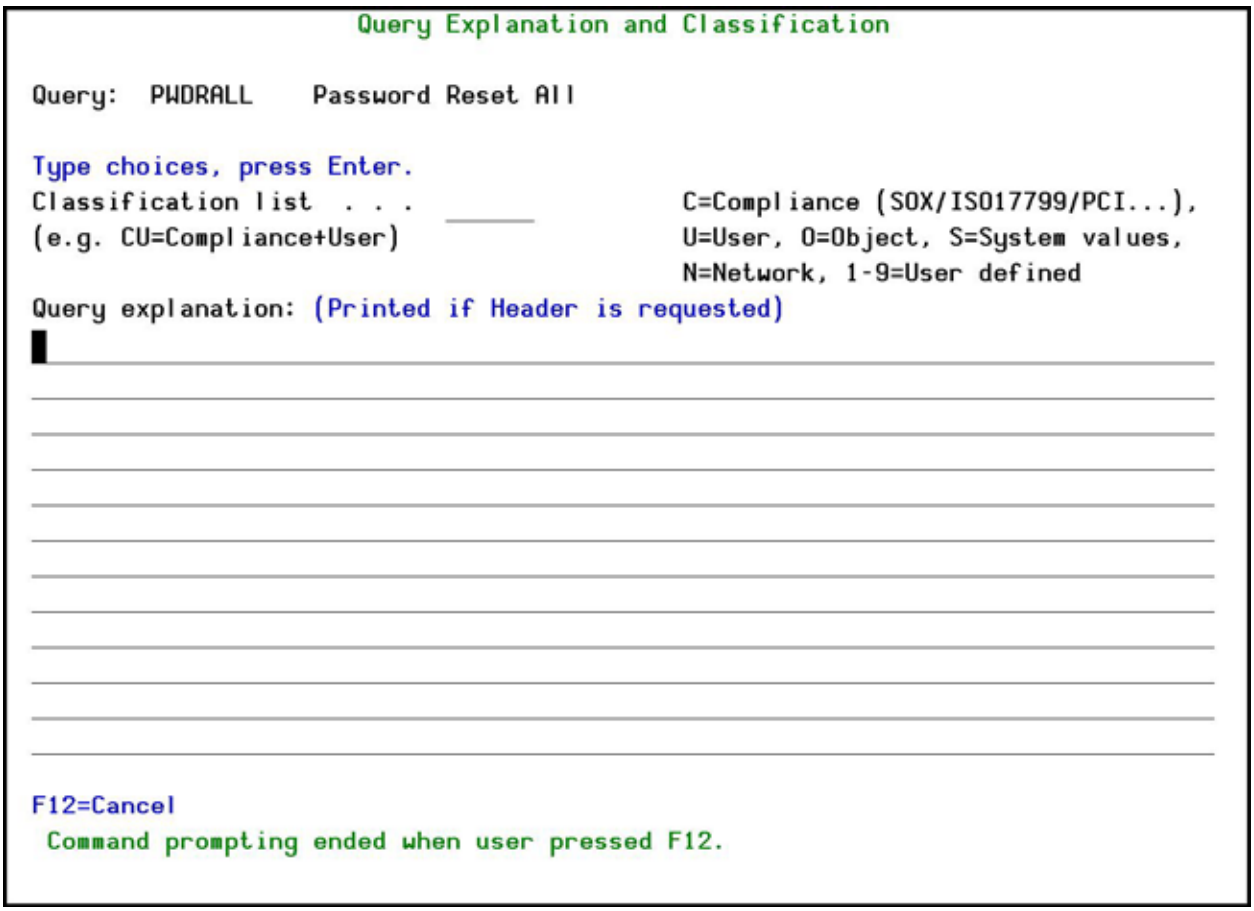
4. Enter your parameters (do ***NOT*** change the **Output** parameter) and press **Enter**. The query is run and the output is displayed on the screen.

Explanation and Classification of a Query

You can classify the Query and also provide a detailed explanation which will be printed on the first page of the report.

To define the classification and explanation of the query:

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **1. Work with Queries** in the **Queries** menu. The **Work with Queries** screen appears.
3. Select the Query to run and press **9=Explanation & Classification**. The **Query Explanation and Classification** screen appears.



Query Explanation and Classification screen

Field/Option/Command Key	Description
Classification list	
Query explanation	

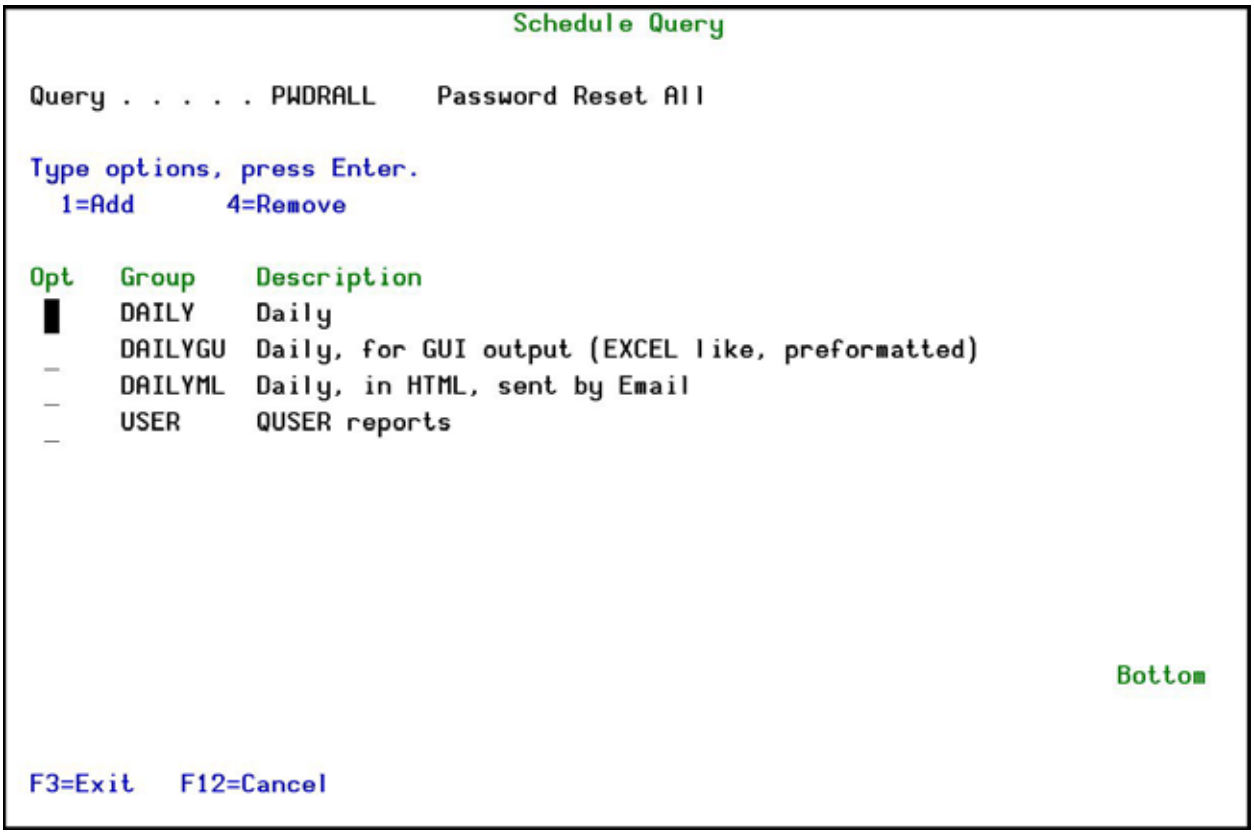
4. Enter your definitions and press **Enter**. You are returned to the **Work with Queries** screen.

Schedule a Query

You can schedule a query to run in a group of reports.

To add a query to a schedule:

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **1. Work with Queries** in the **Queries** menu. The **Work with Queries** screen appears.
3. Select the Query to run and press **S=Schedule**. The **Schedule Query** screen appears.



Schedule Query screen

Field/Option/Command Key	Description
Group	The name of the report group
Description	Description of the report group

4. Enter **1** next to the group in which you want the query to run and press **Enter**. You are returned to the **Work with Queries** screen.

Unschedule a Query

You can remove a query from running in a group of reports.

To remove a query from a schedule:

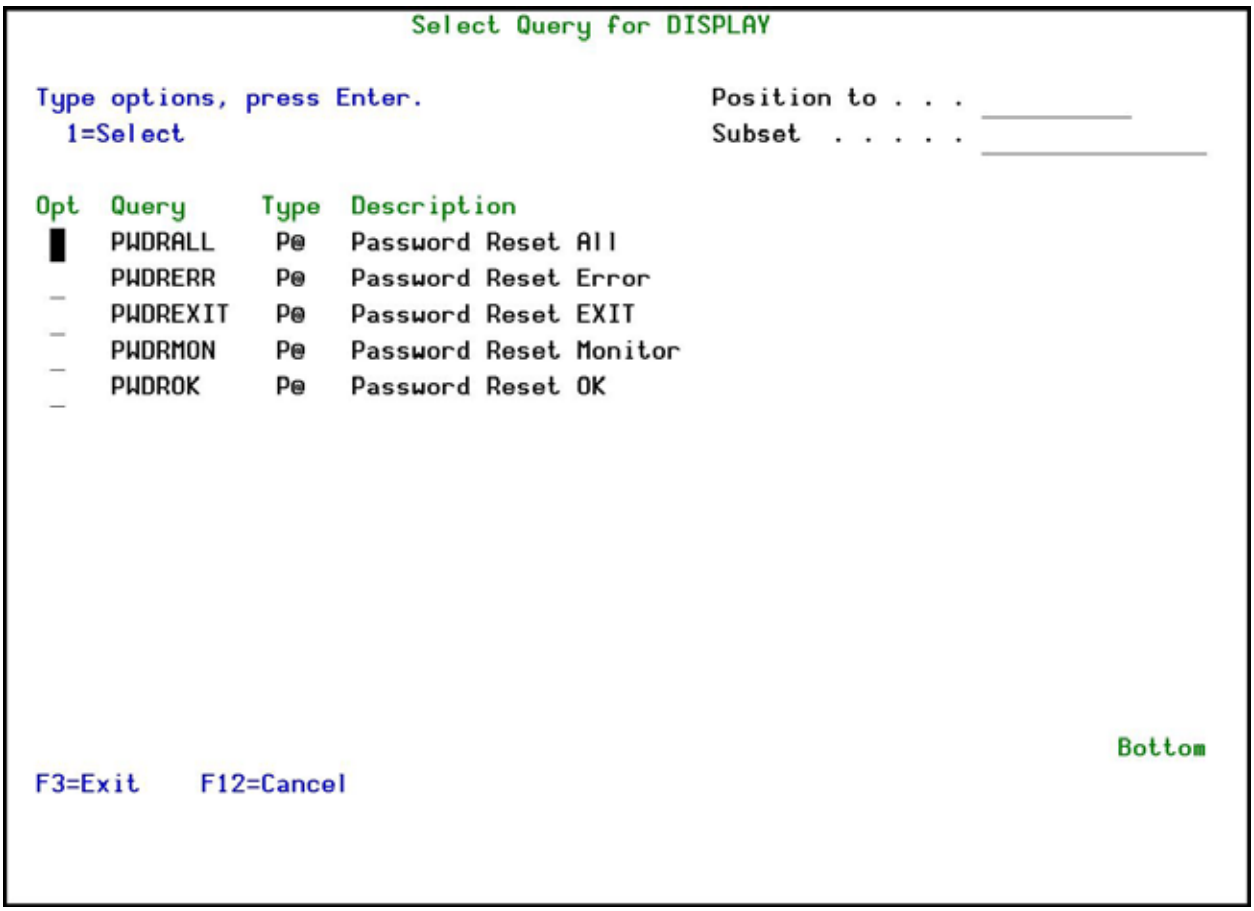
1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **1. Work with Queries** in the **Queries** menu. The **Work with Queries** screen appears.
3. Select the Query to run and press **S=Schedule**. The **Schedule Query** screen appears.
4. Enter **4** next to the group from which you want to remove the query and press **Enter**. You are returned to the **Work with Queries** screen.

Select a Query for DISPLAY

You can run a query and the results are displayed on the screen.

To run a query:

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **11. Display** in the in the **Queries** menu. The **Select Query for Display** screen appears.



Select Query for DISPLAY screen

Field/Option/Command Key	Description
Opt	Enter **1** in the **Opt** field of the Query to display.

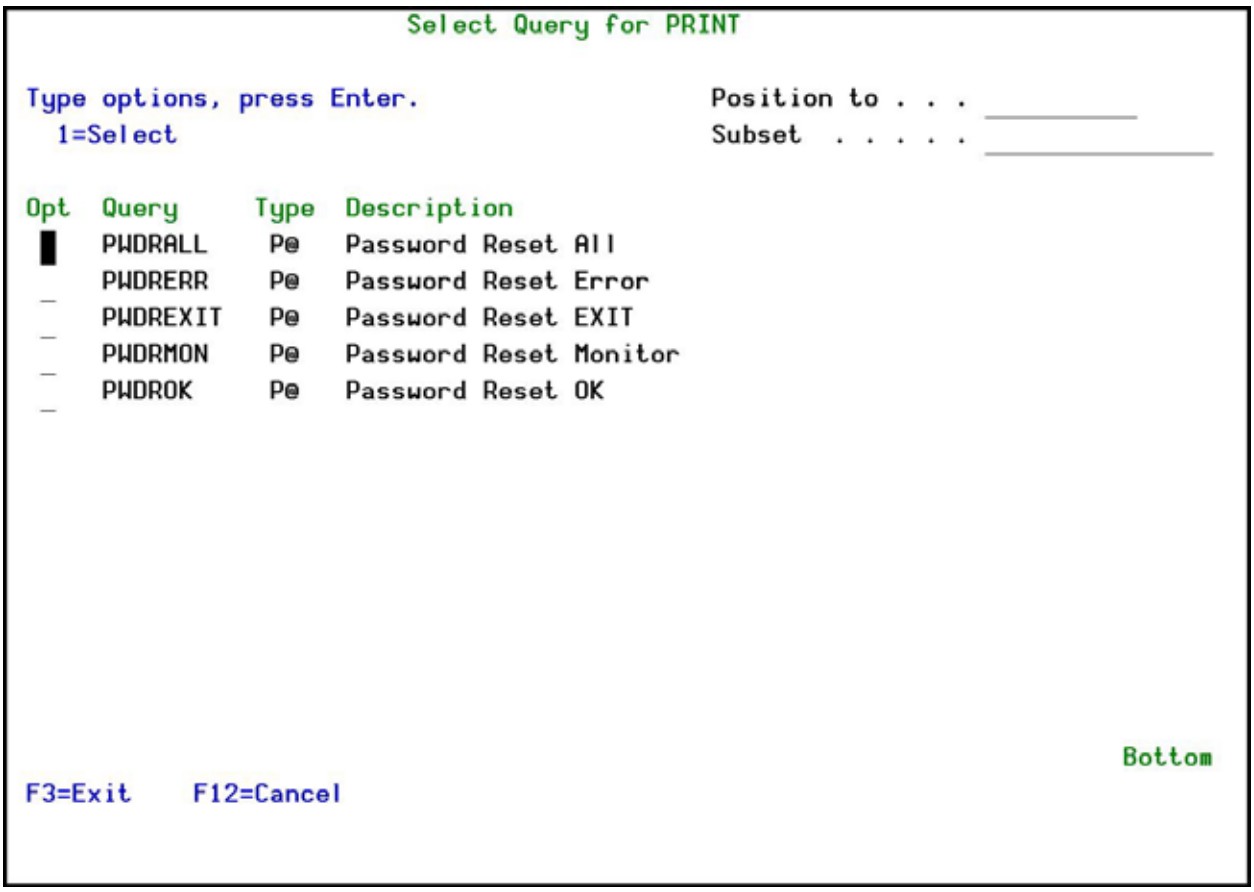
3. Select the Query to run and press **1=Select**. The **Run Audit Query** screen appears.
4. Continue with step **4** of the **Run a Query** procedure.

Select a Query for PRINT

You can run a query and the results are printed.

To print a query:

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **12. Print** in the in the **Queries** menu. The **Select Query for Print** screen appears.



Select Query for PRINT screen

Field/Option/Command Key	Description
Opt	Enter **1** in the **Opt** field of the Query to print.

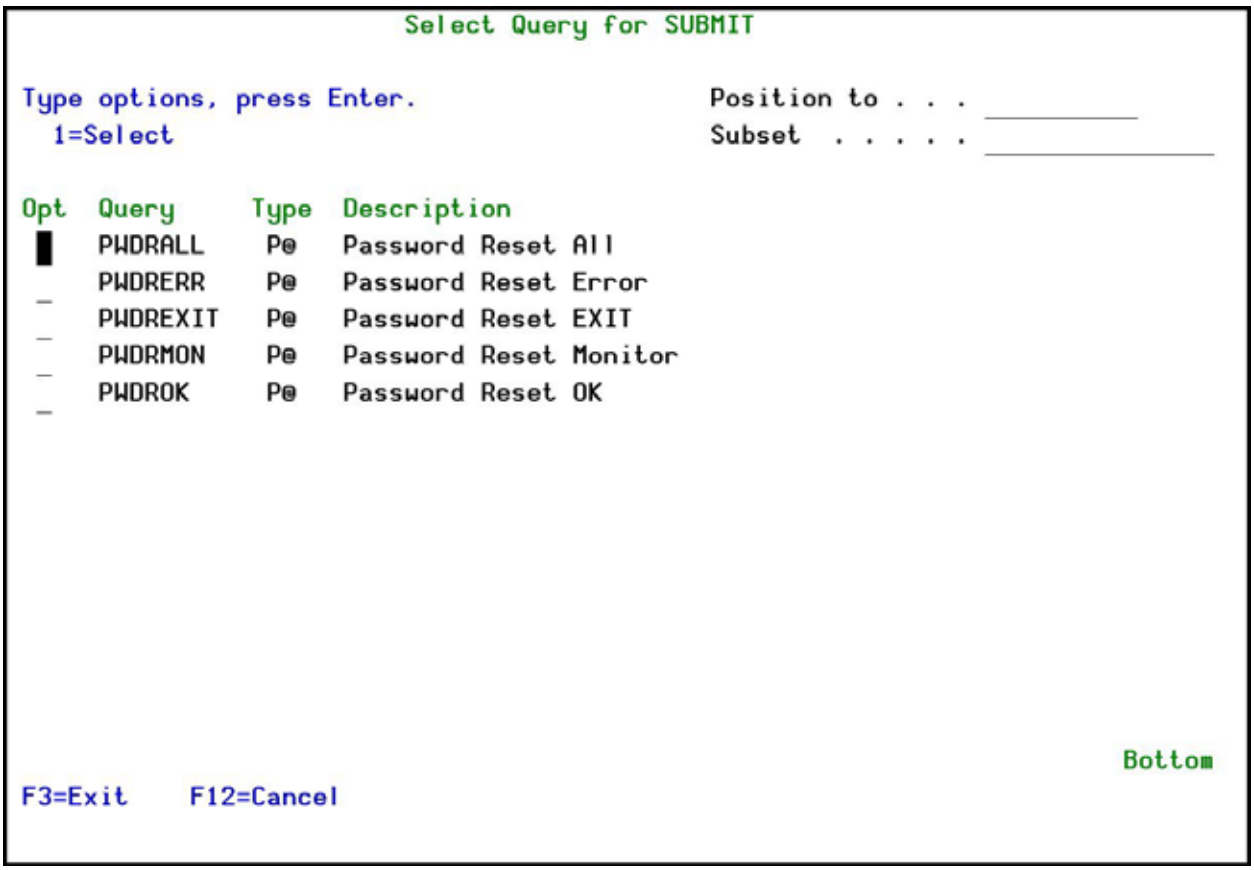
3. Select the Query to run and press **1=Select**. The **Run Audit Query** screen appears.
4. Continue with step **4** of the **Print a Query** procedure.

Select a Query for SUBMIT

You can run a query in batch mode and the results are printed.

To run a query in batch mode:

1. Select **41. Queries and Reports** in the **Password Reset** main menu. The **Queries** menu appears.
2. Select **13. Submit as Batch Job** in the in the **Queries** menu. The **Select Query for Submit** screen appears.



Select Query for SUBMIT screen

Field/Option/Command Key	Description
Opt	Enter **1** in the **Opt** field of the Query to submit to batch.

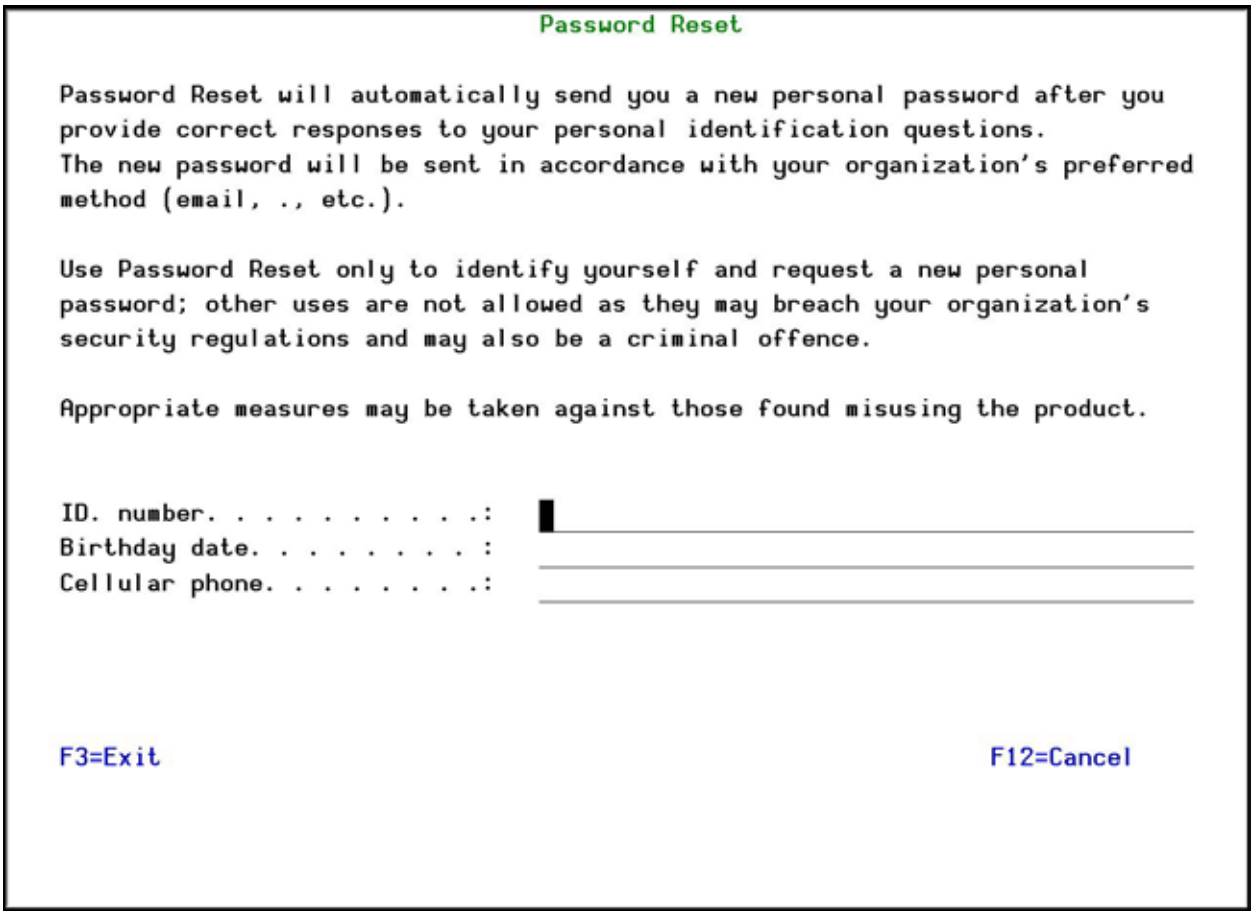
3. Select the Query to run and press **1=Select**. The **Run Audit Query** screen appears.
4. Continue with step **4** of the **Run a Query as a Batch Job** procedure.

Test Password Reset

Use the Test Password Reset functionality to ensure that, if needed, users will be able to reset their passwords without needing to involve the Help Desk.

To test password reset:

1. Select **61. Test Password Reset** in the **Main** menu. The **Password Reset** screen appears.



Test Password Reset screen

Field/Option/Command Key	Description
Questions	The questions displayed here are controlled by the definitions in the **Initial Process Questions**.

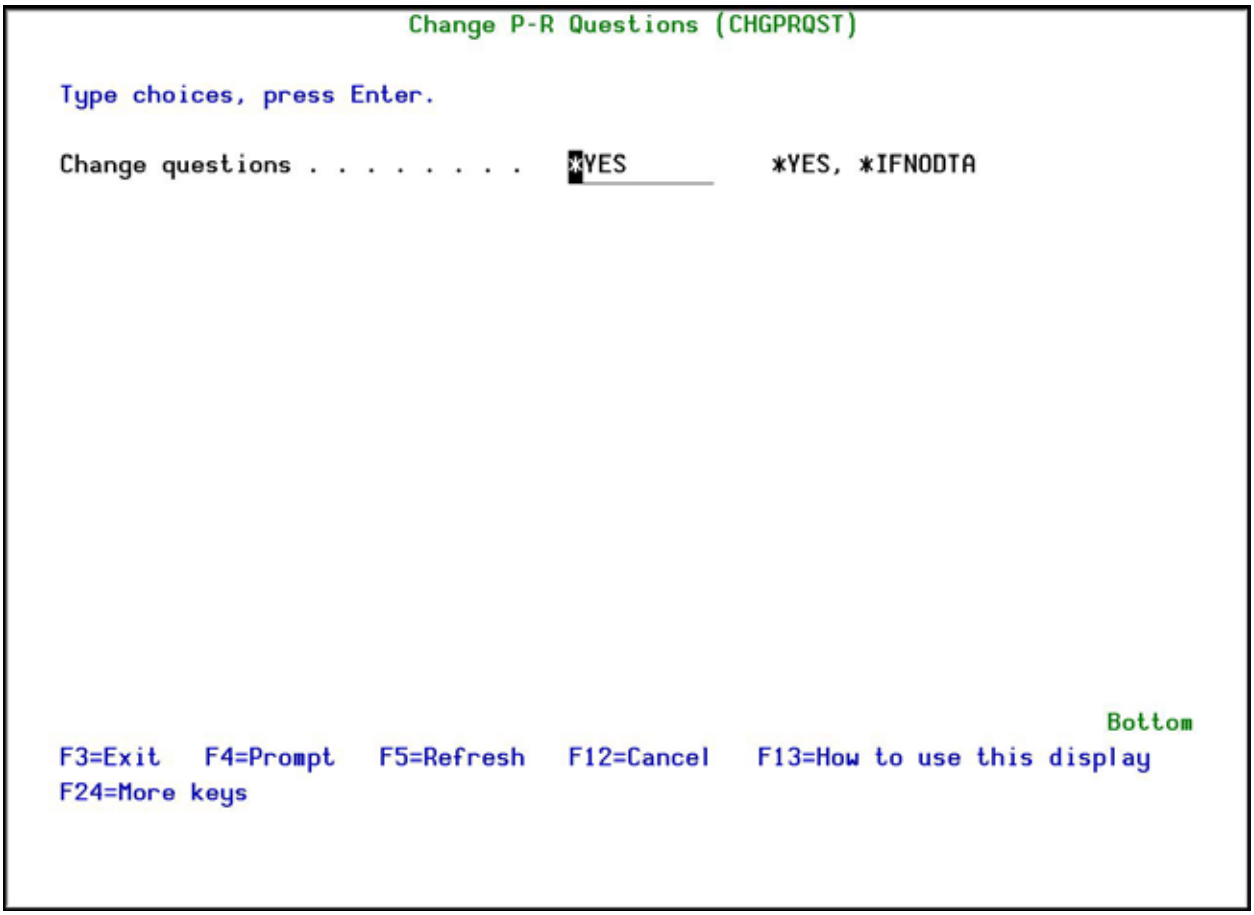
2. Enter the appropriate identification and follow the instructions.

Change Current User Questions

Password Reset enables individual users to set or change their own private questions. This command is only valid if there is a Person associated with the current user.

To set private questions:

1. Select **62. Change Current User Questions** in the **Password Reset** main menu. The **Change P-R Questions** screen appears.

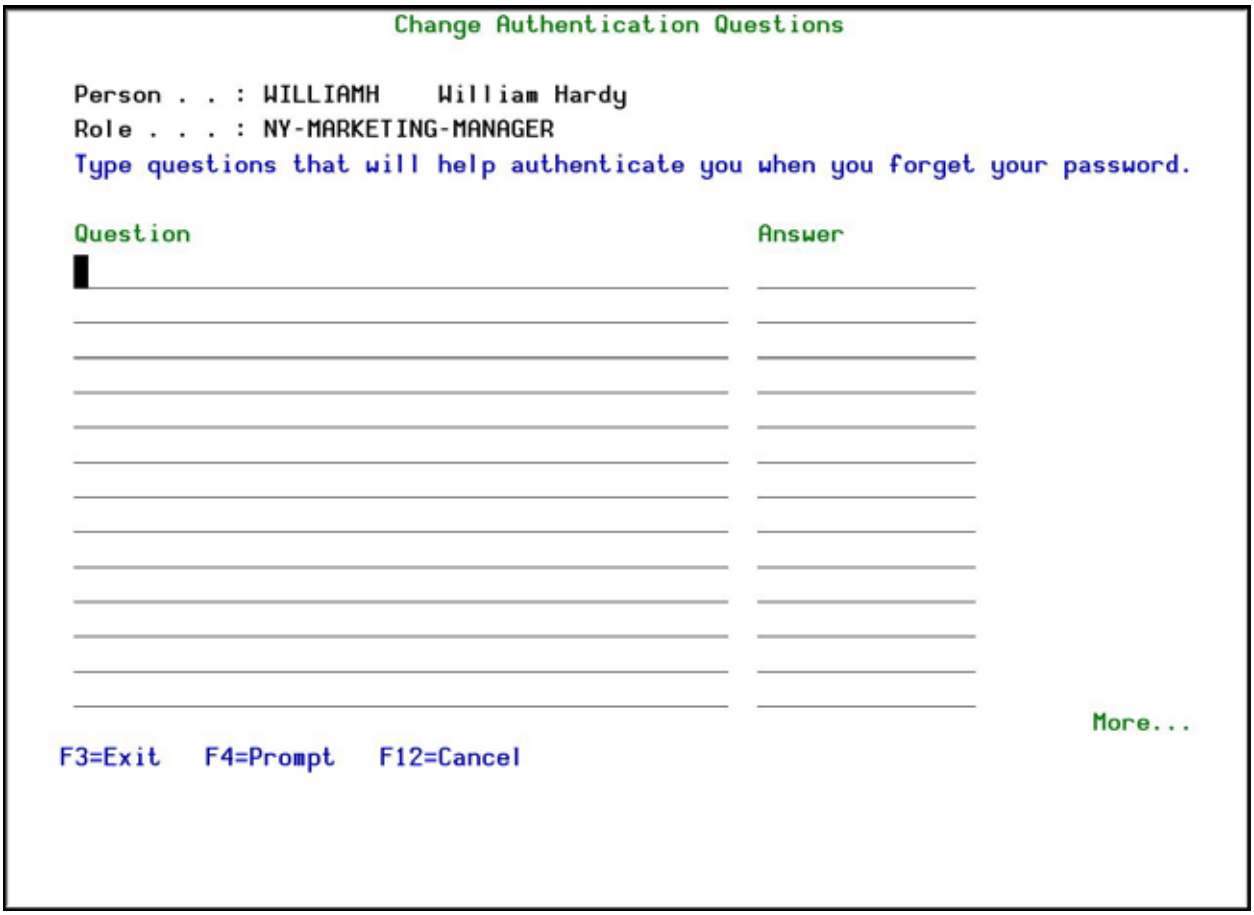


Change P-R Questions

Field/Option/Command Key	Description
Change questions	***YES** = Set or change private questions for the Person. ***IFNODTA** = Set private questions for the person only if currently there are no questions for the person.

2. Enter a value to the parameter and press **Enter**. The **Change Authentication Questions** screen appears, unless there is no person associated with the current user.

Note: The **Change Authentication Questions** screen will only be displayed if the number of current users changing questions does not exceed the number set in the **Control** option of the **System Configuration**. See Authentication Control for more details.



Change Authentication Questions screen

Field/Option/Command Key	Description
Question	Enter the question that will help to uniquely identify the Person. Only the Person should know the answer. Type in any question or use **F4** to select from a list of commonly used questions. You can enter as many questions as you want, but you must enter at least as many questions as will be asked at Password Reset time.
Answer	The answer to the question. Existing answers are shown as asterisks. Remember that the response process when resetting your password is case sensitive. If you use capital letters here, you have to remember to use them when answering the questions in the reset process.

3. Add as many questions and answers as you want. Ensure that there are at least as many questions as required in the **P-R Class** of the person.
4. Press **Enter**. You are returned to the main menu.

Copy HR Data

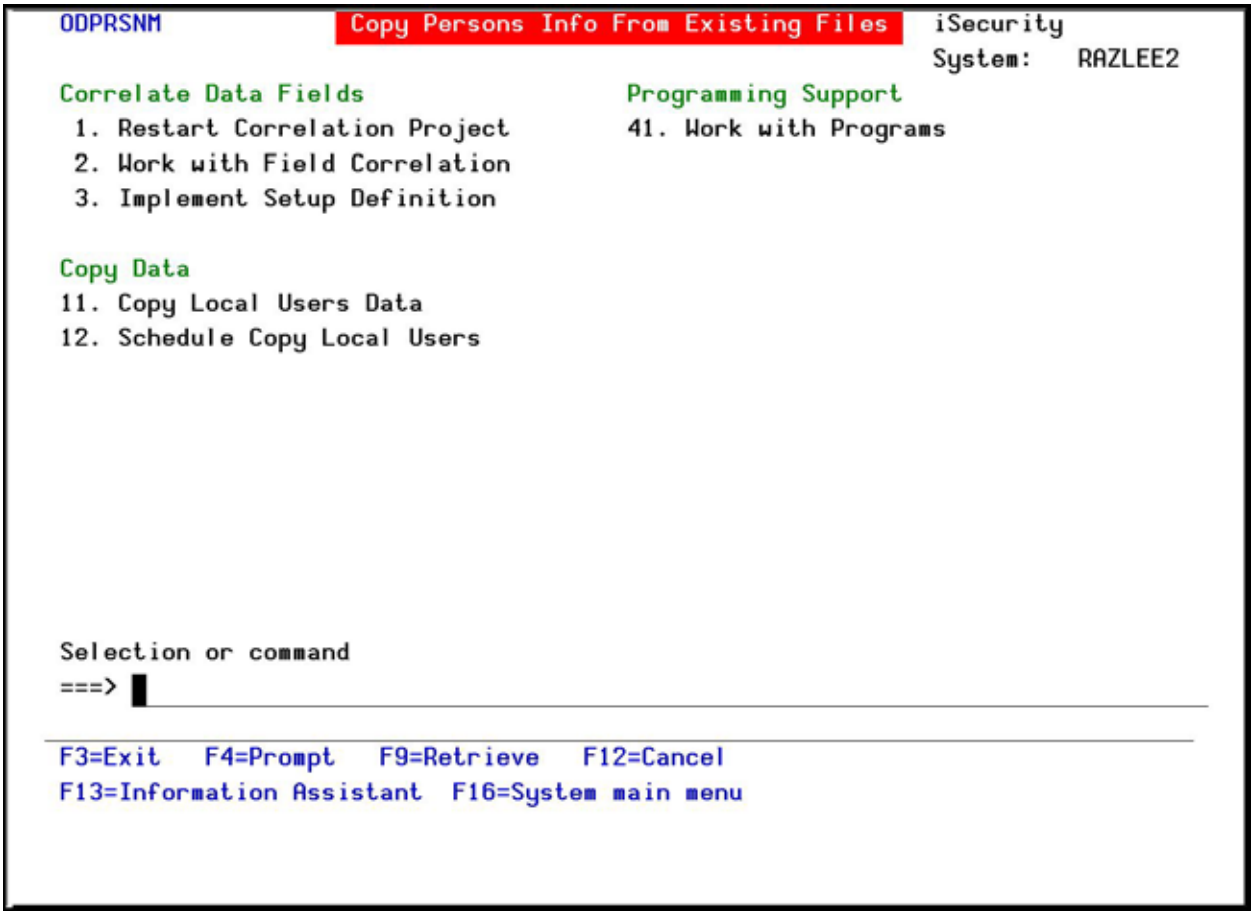
Password Reset enables you to import person information from an external source such as an existing Identity Management system.

Restart Correlation Project

To make changes in the mapping of your organization's files to the **Password Reset** files, you may want to start afresh with the original files with no mapping defined.

To restart the Correlation Project:

1. Select **64. Copy HR Data to Persons File** in the **Password Reset** main menu. The **Copy Person Info From Existing Files** menu appears.

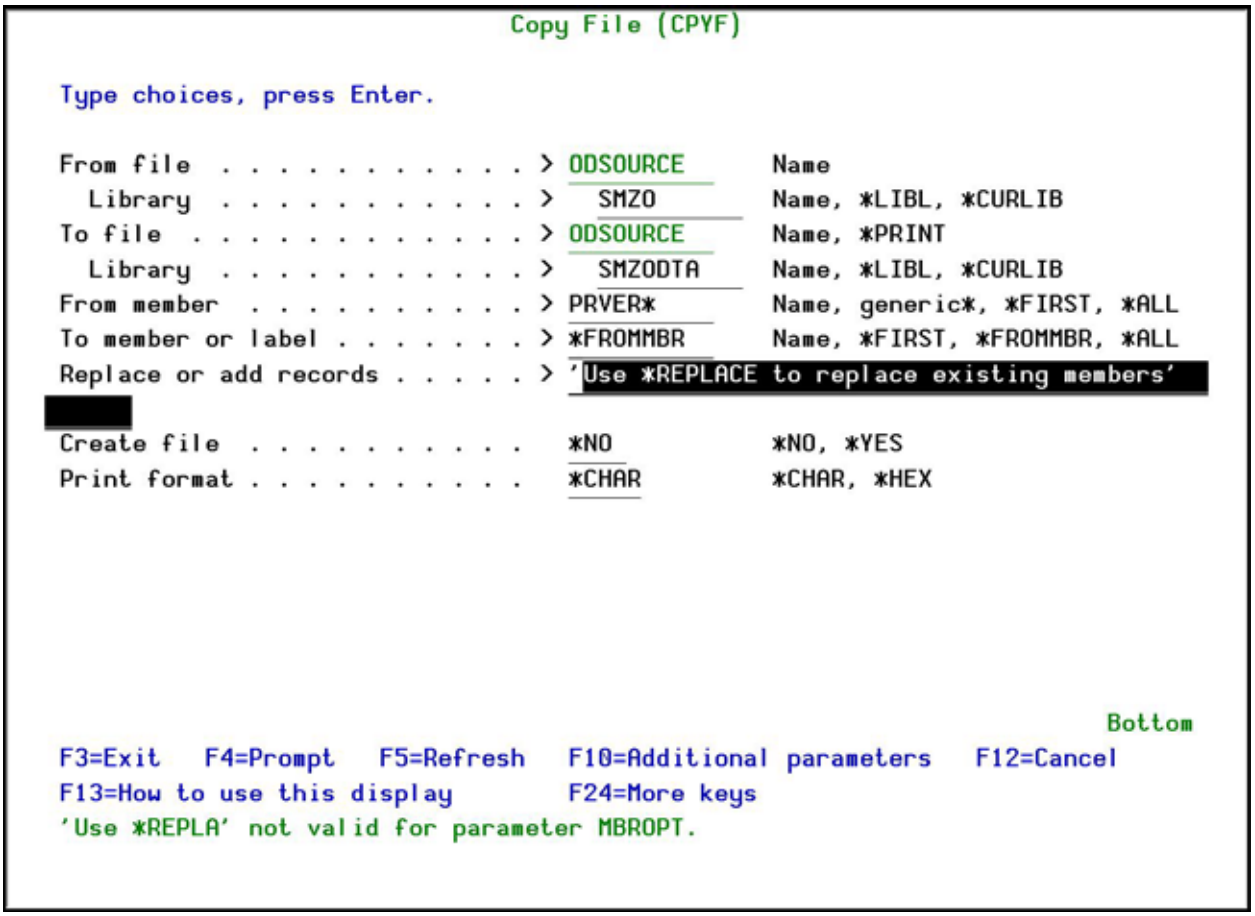


Copy Persons Info From Existing Files Menu

Field/Option/Command Key	Description
1. Restart Correlation Project	Opens a pre-populated **Copy File** screen that allows the user to update the source members that define the organization's person files.
2. Work with Field Correlation	Opens a source edit screen that allows the user to update the source member that defines the organization's person files mapping to the **Password Reset** files.
3. Implement Setup Definition	Opens a pre-populated **Call Program** screen that compiles the source from the **Work with Field Correlation** option.
11. Copy Local Users Data	Opens a pre-populated **Call Program** screen that copies the organization's user data to the **Password Reset** files.

Field/Option/Command Key	Description
12. Schedule Copy Local Users	Opens a Work with Job Schedule Entries screen that allows users to define Jobs that will automatically copy the organization's user data to the **Password Reset** files.
41. Work with Programs	Opens a **Work with Members Using PDM** screen, open to the subset of members that control working with the organization's person files.

2. Select **1. Restart Correlation Project**. The **Copy File** screen appears.



Copy File Screen

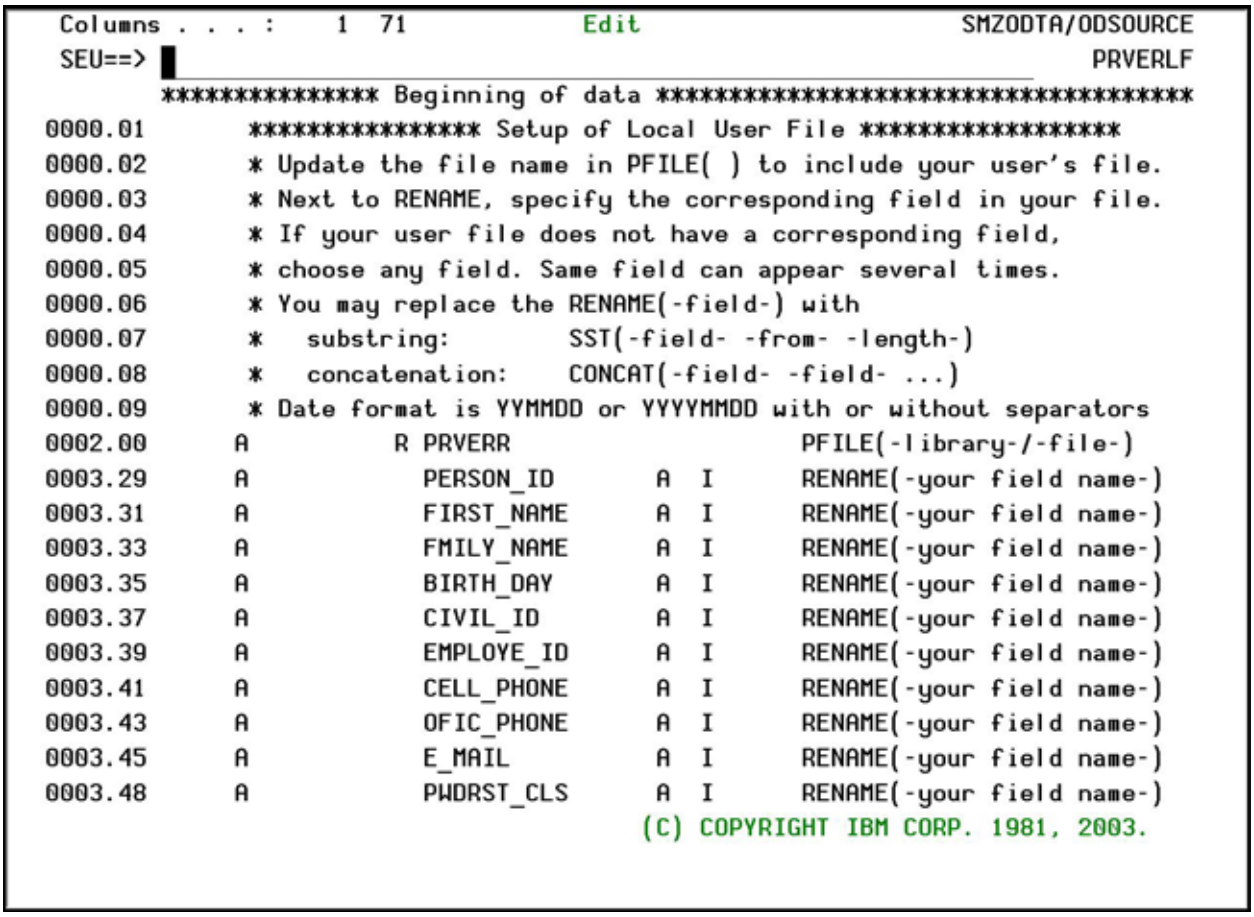
Field/Option/Command Key	Description
From file/library	The file that contains the records to be copied.
To file/library	The file that receives the copied records.
From member	The file-member in the file that is to be copied.
To member or label	The file-member to receive the copied records.
Replace or add records	Defines if the copied records are to be added to the receiving file or to replace the existing file.

3. Enter the appropriate parameters and press **Enter**. The file is copied.

Work with Field Correlation

Edit the source for the file mapping from your organization's file to the **Password Reset** person file.

1. Select **64. Copy HR Data to Persons File** in the **Password Reset** main menu. The **Copy Person Info From Existing Files** menu appears.
2. Select **2. Work with Field Correlation**. The **SEU Edit** screen appears.



SEU Edit Screen

Field/Option/Command Key	Description
PFILE	Replace the current text with the Library/Filename of your organization's file.
PERSON_ID	The unique identifier of the Person.
FIRST_NAME	The first name of the Person.
FMILY_NAME	The family name or surname of the Person.
BIRTH_DAY	The birthday of the Person – can be used for the unique identification of the Person.
CIVIL_ID	The national ID number of the person – can be used for the unique identification of the Person.
EMPLOYE ID	The employee number of the Person within the organization - can be used for the unique identification of the Person.
CELL PHONE	The cell phone number of the Person – can be used for the unique identification of the Person. Can also be used to send notification of a new password.

Field/Option/Command Key	Description
OFIC PHONE	The office phone number of the Person – can be used for the unique identification of the Person.
E_MAIL	The email address of the person - can be used for the unique identification of the Person. Can also be used to send notification of a new password.
PWDRST_CLS	The Password Reset class to which the person belongs.
PRFRD_LNG	Define the language in which this person will receive identity verification questions.
PRFRD_USER	The preferred User ID of the Person.

3. Enter the mapping information for your organization's file and press **Enter** twice.

Note: If there is not a direct one to one relationship from your organization's fields with the Password Reset fields, instead of replacing the field name in the RENAME(-field-) phrase, you can replace it completely with either a substring of a field (SST(-field- -from- -length-)) or by concatenating two fields (CONCAT(-field- -field- ...)).

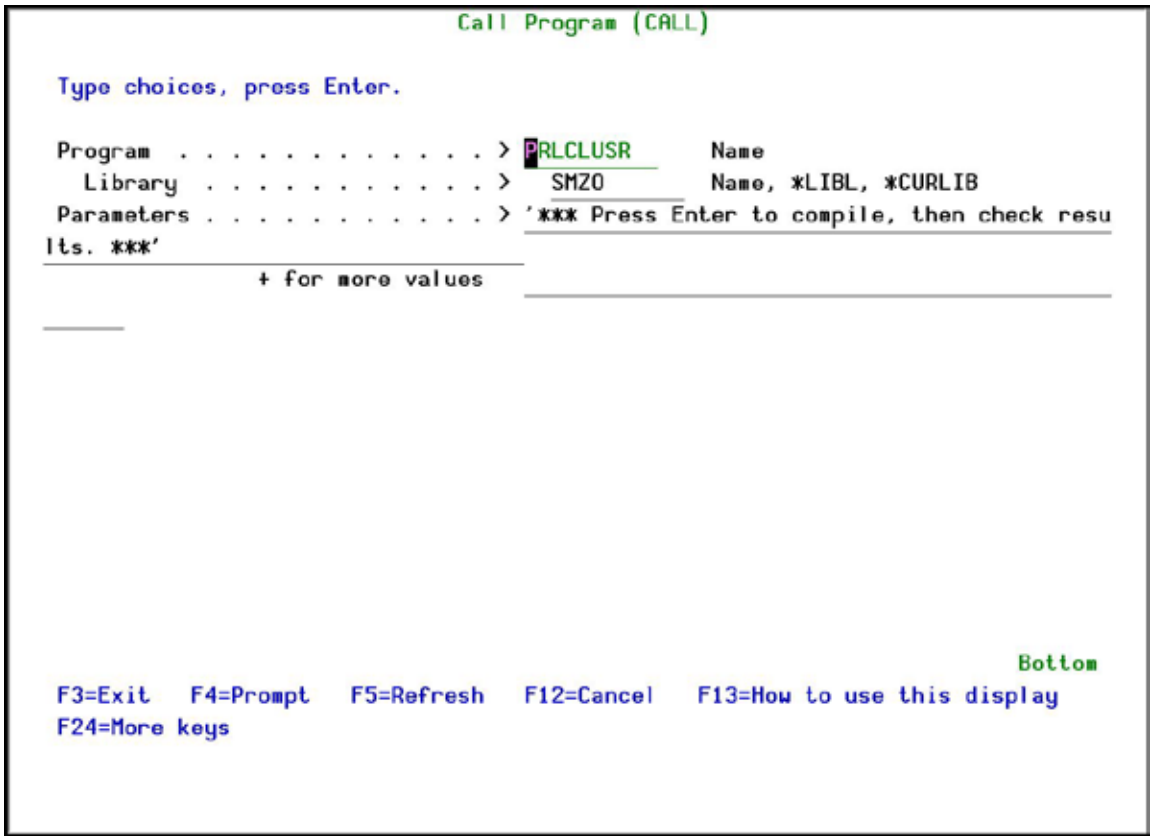
4. You should now continue by compiling the file, as described in *Implement Setup Definition*.

Implement Setup Definition

After you have setup the source files, you must compile the program.

To compile the program:

1. Select **64. Copy HR Data to Persons File** in the **Password Reset** main menu. The **Copy Person Info From Existing Files** menu appears.
2. Select **3. Implement Setup Definition** in the **Copy Person Info From Existing Files** menu. The **Call Program** screen appears.



Call Program

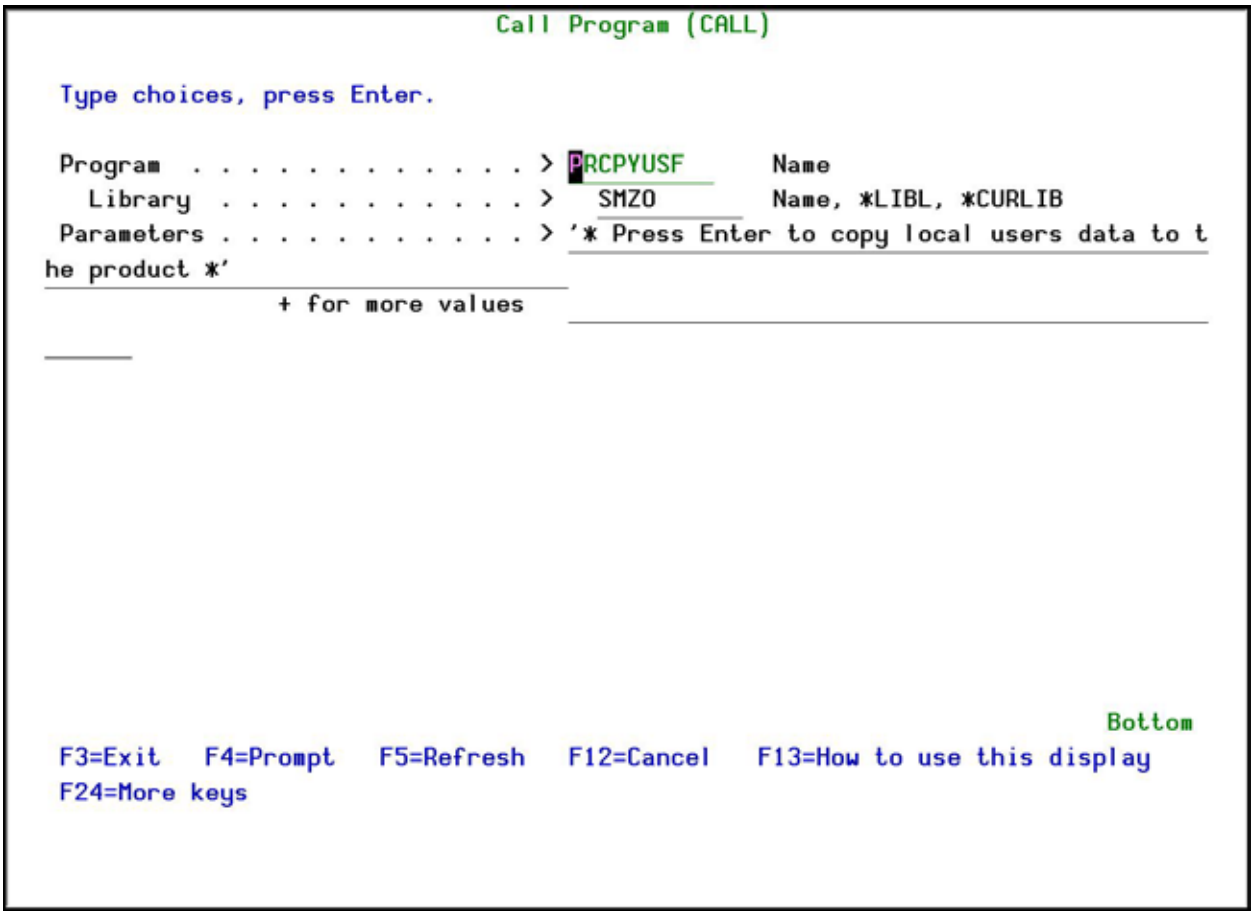
3. Press **Enter** and check the results.

Copy Local Users Data

When you have set up the product to work with your files, you must copy the data

To copy the data:

1. Select **64. Copy HR Data to Persons File** in the **Password Reset** main menu. The **Copy Person Info From Existing Files** menu appears.
2. Select **11. Copy Local Users Data** in the **Copy Person Info From Existing Files** menu. The **Call Program** screen appears.



Call Program

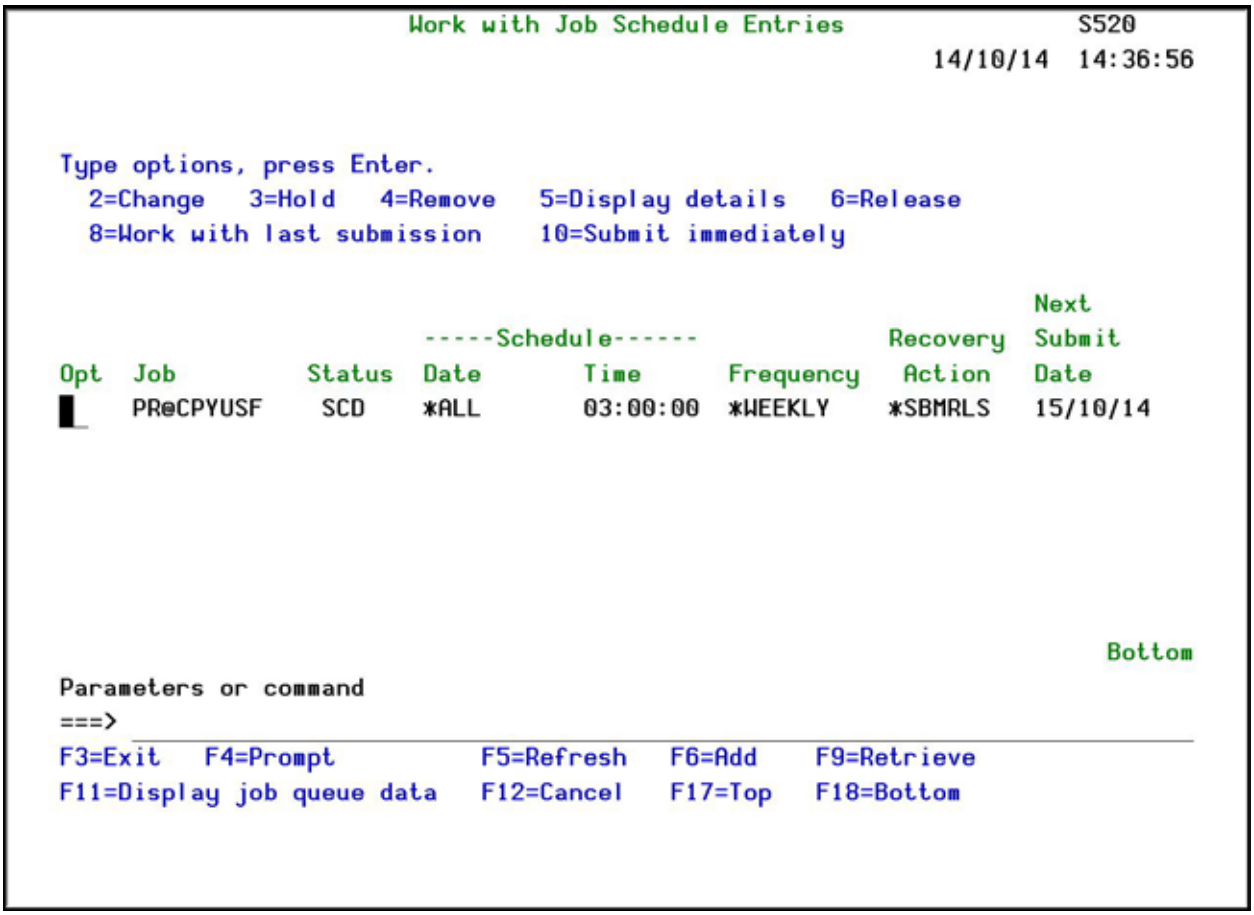
3. Press **Enter**. The data is copied.

Schedule Copy Local Users

It is important to keep your User data and the product user data synchronized. You can schedule a job to run periodically to do this.

To schedule user data synchronization:

1. Select **64. Copy HR Data to Persons File** in the **Password Reset** main menu. The **Copy Person Info From Existing Files** menu appears.
2. Select **12. Schedule Copy Local Users** in the **Copy Person Info From Existing Files** menu. The **Work with Job Schedule Entries** screen appears.



Work with Job Schedule Entries

3. The job is set to run weekly at 03:00. Use option **2=Change** to update this.

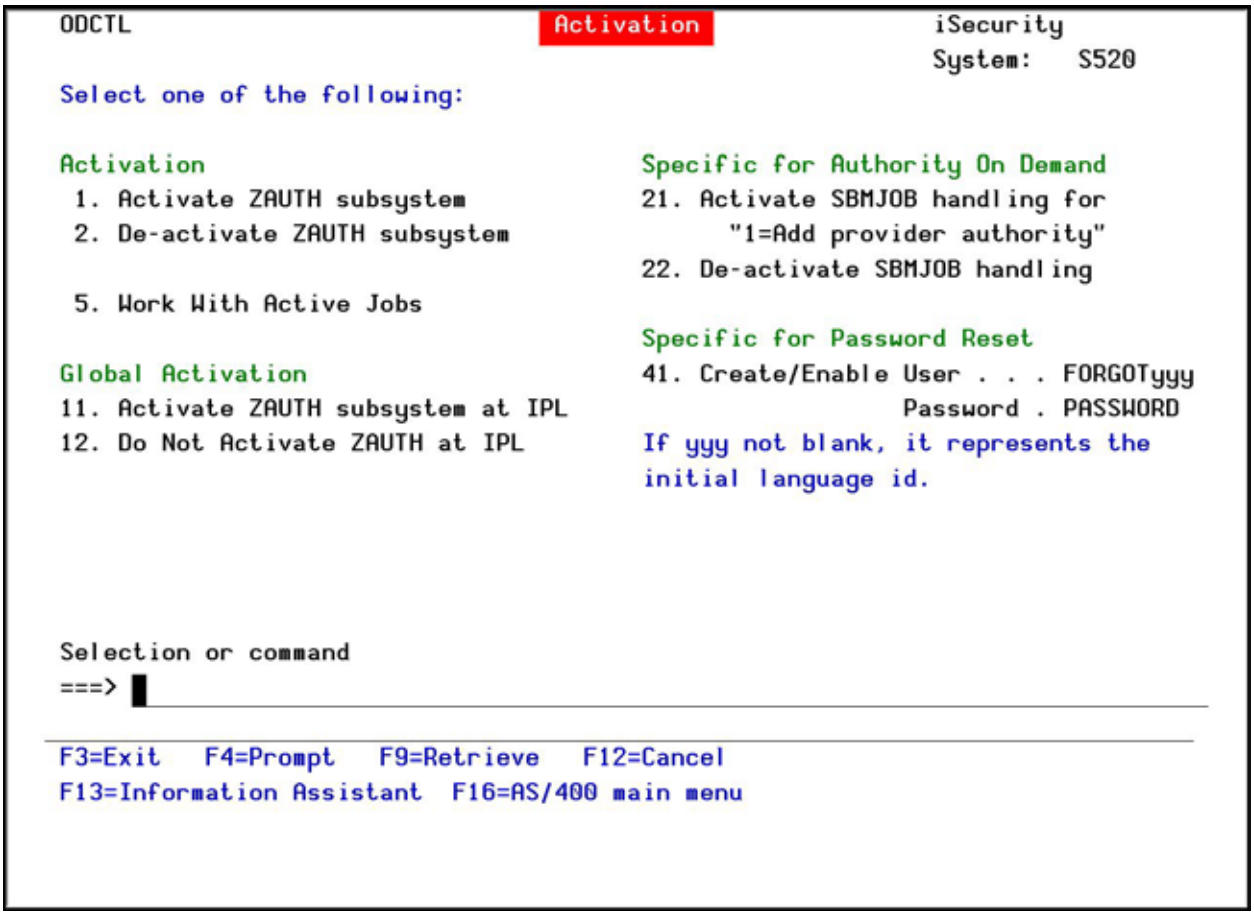
Control

Activation

Before using Password Reset, you must activate the ZAUTH subsystem. You also need to create the special user to be used for resetting passwords.

To activate the sub-system:

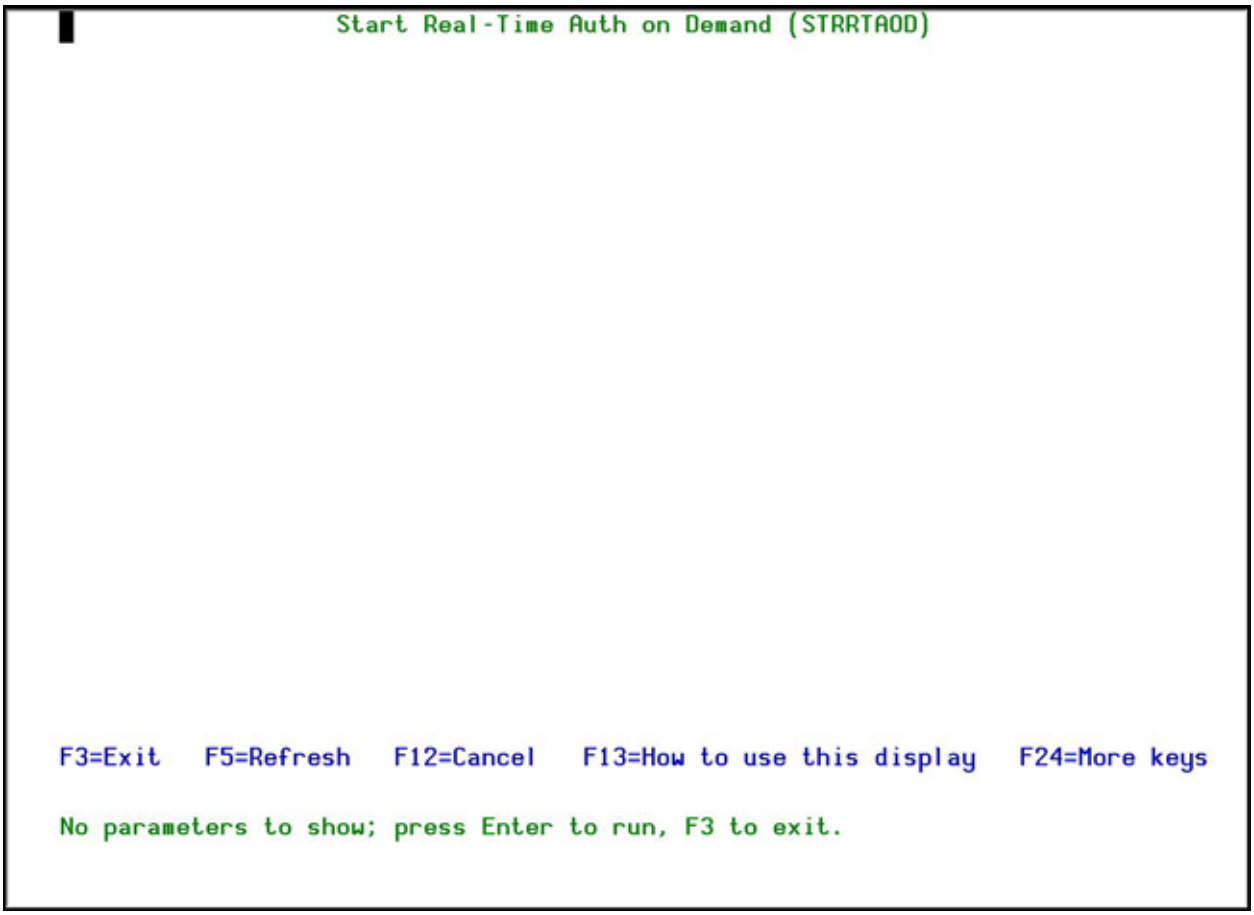
1. Select **71. Activation** in the **Password Reset** main menu. The **Activation** menu appears.



Activation Menu

Field/Option/Command Key	Description
1. Activate ZAUTH subsytem	Opens the **Start Real Time Auth on Demand** screen.
2. De-activate ZAUTH subsytem	Opens the **End Real Time Auth on Demand** screen.
5. Work with Active Jobs	Opens the **Work with Subsystem Jobs** screen.
41. Create/Enable User FORGOTyyy	Opens the **Create User Profile** to enable you to create the special user for resetting passwords.

2. Select **1. Activate ZAUTH subsystem** in the **Activation** menu. The **Start Real Time Auth on Demand** screen appears.



Start Real-Time Auth on Demand screen

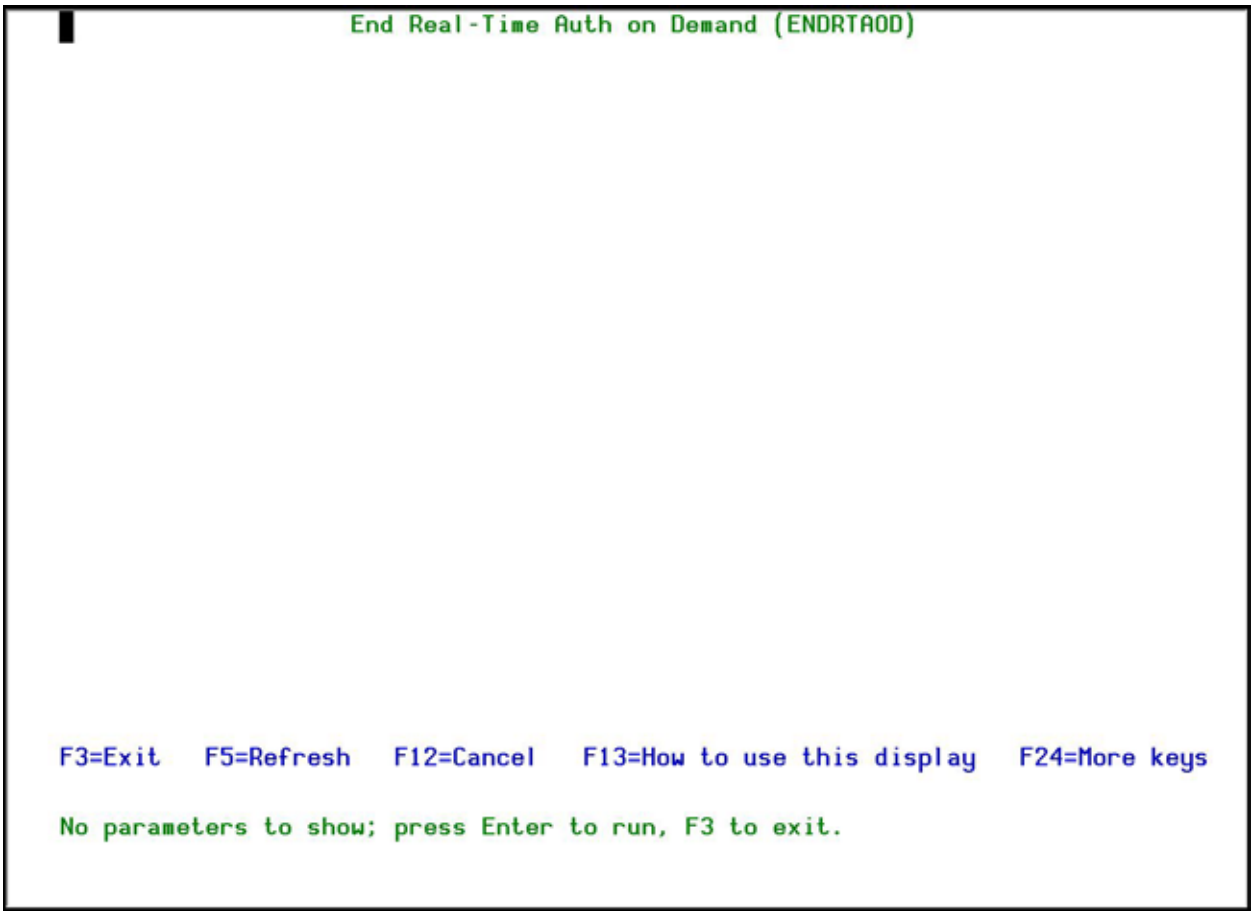
3. Press **Enter**. The subsystem is started.

End Real Time Auth on Demand Screen

For certain system activities to be performed, you may need to de-activate the ZAUTH subsystem.

To de-activate the sub-system:

1. Select **71. Activation** in the **Password Reset** main menu. The **Activation** menu appears.
2. Select **2. De-activate ZAUTH subsystem** in the **Activation** menu. The **End Real Time Auth on Demand** screen appears.



End Real-Time Auth on Demand screen

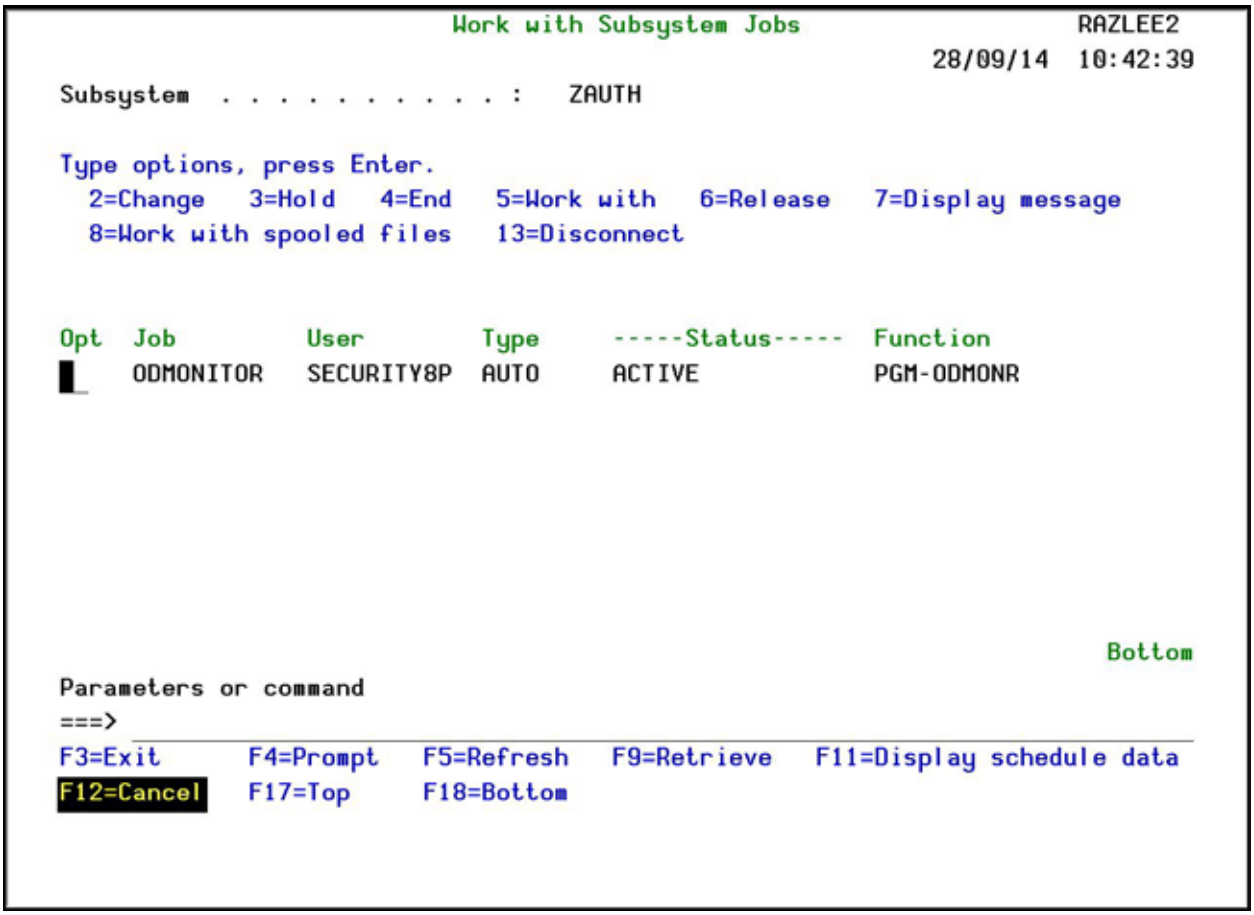
3. Press **Enter**. The subsystem is ended.

Work with Subsystems

You can check that the subsystem is active

To check:

1. Select **71. Activation** in the **Password Reset** main menu. The **Activation** menu appears.
2. Select **5. Work with Active Jobs** in the **Activation** menu. The **Work with Subsystem Jobs** screen appears.



Work with Subsystem Jobs screen

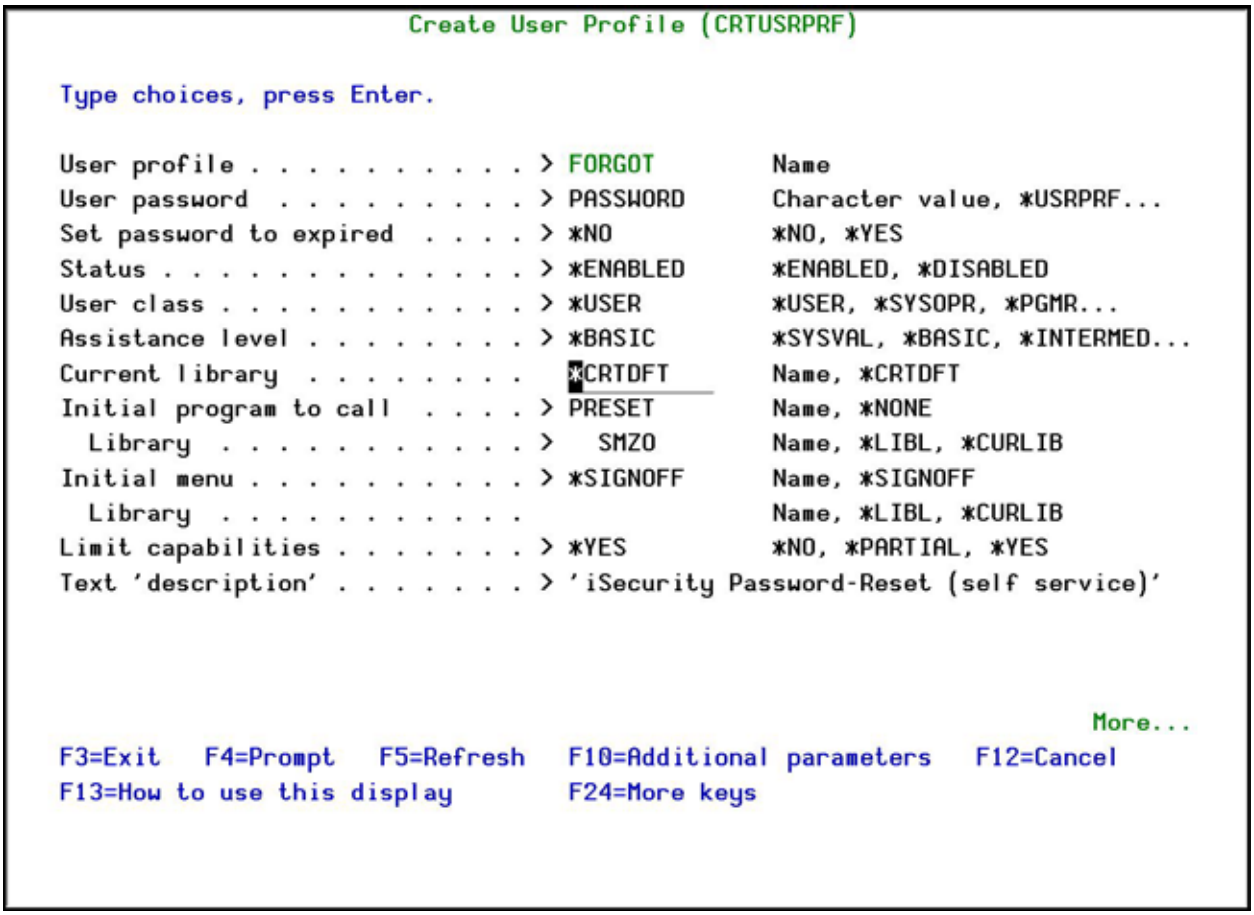
See the IBM documentation for a description of the fields, options, and command keys available in this screen.

Create Special User FORGOTyyy

You need to create and enable the special user FORGOT to allow users to reset their passwords.

To create/enable the special user:

1. Select **71. Activation** in the **Password Reset** main menu. The **Activation** menu appears.
2. Select **41. Create/Enable** in the **Activation** menu. The **Create User Profile** screen appears.



Work with Subsystem Jobs screen

3. Press **Enter**. The user is created/enabled.

System Configuration

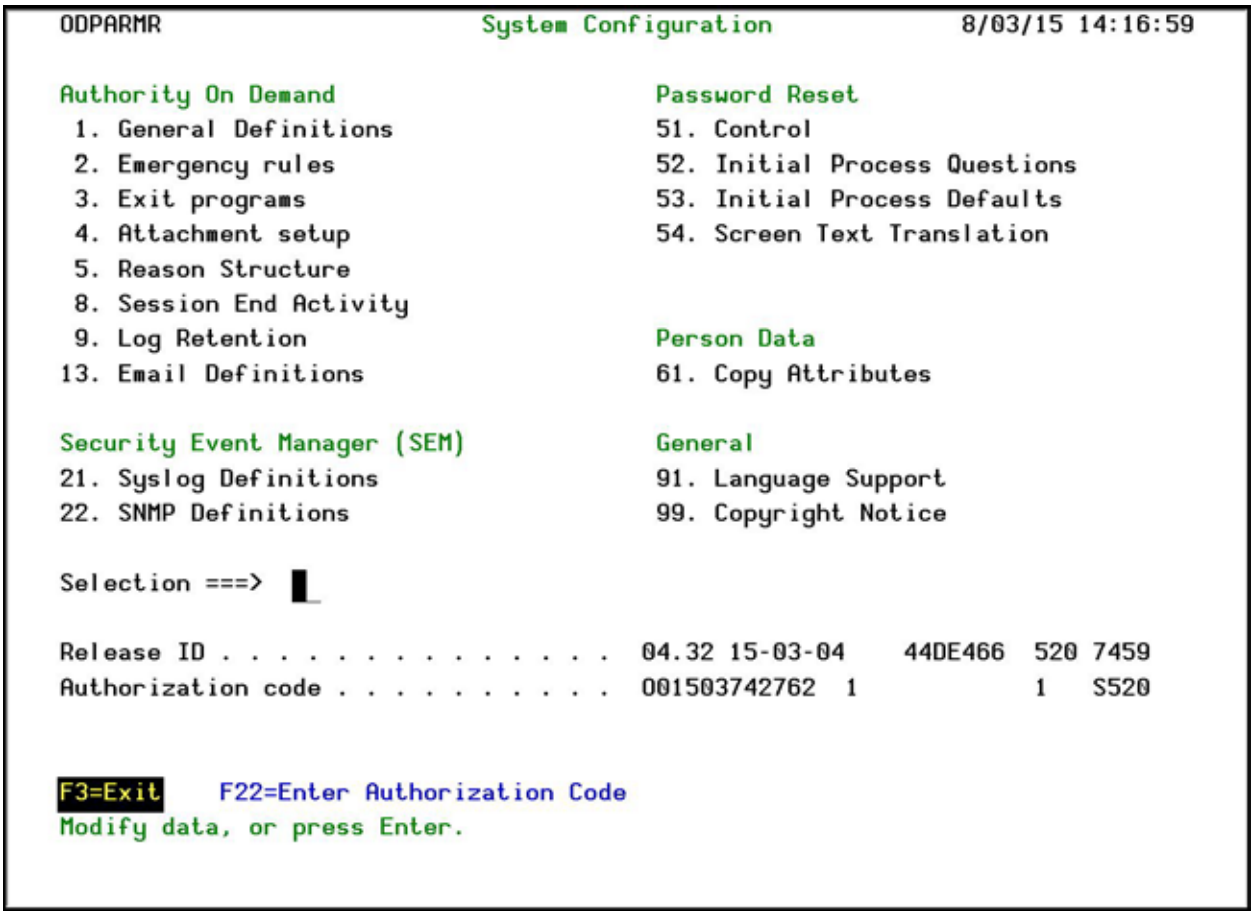
Use the System Configuration menu to access the setup processes for Password Reset and to define system parameters.

Authentication Control

Define the level of control you want to provide for password reset.

To define field defaults:

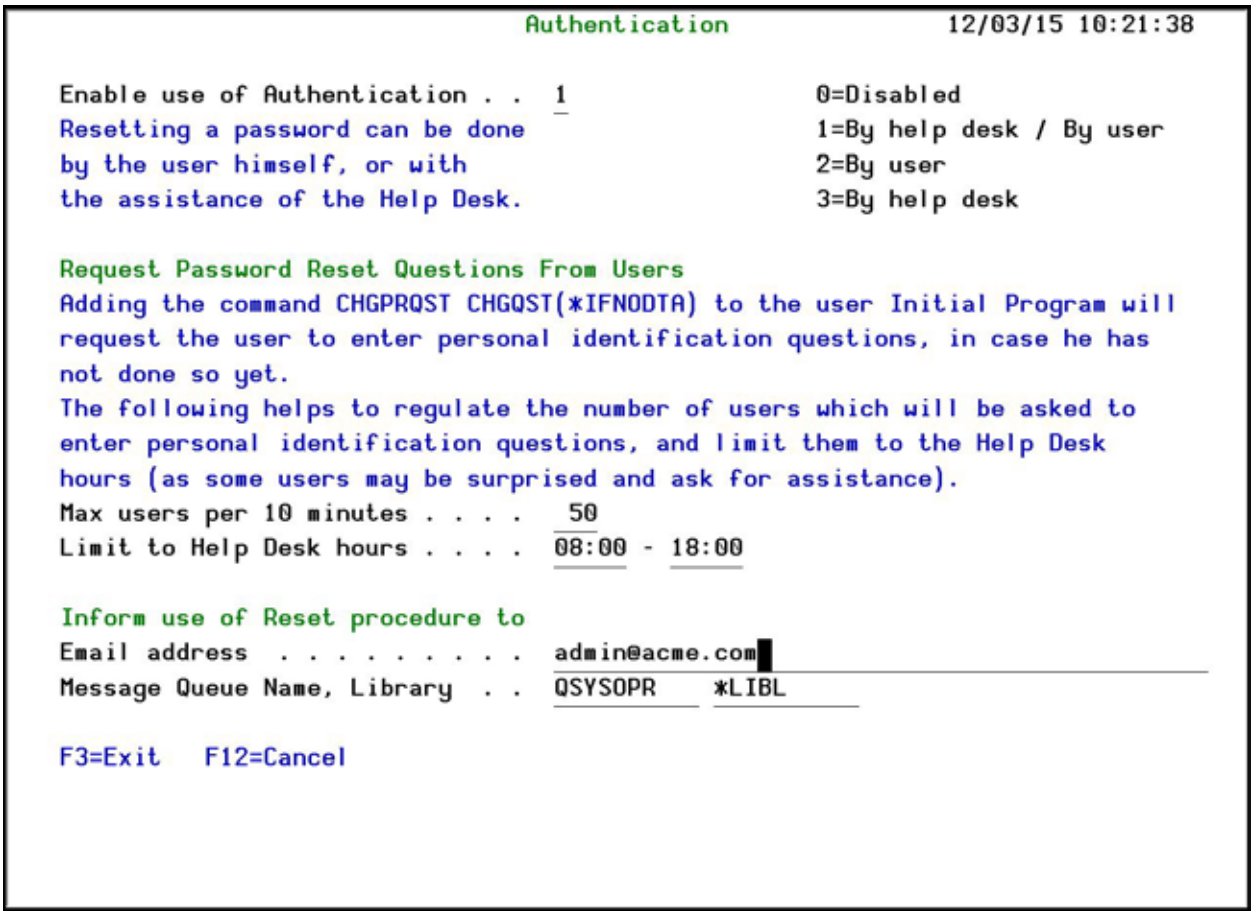
1. Select **81. System Configuration** in the **Password Reset** main menu. The **System Configuration** menu appears.



System Configuration screen

Field/Option/Command Key	Description
51. Control	Opens the **Authentication** screen, where you define the controls for resetting passwords.
52. Initial Process Questions	Opens the **Initial Process Questions** screen, where you define and modify the questions to be asked when resetting a User's password.
53. Initial Process Setup	Opens the **Initial Process Setup** screen, where you define and modify the Password Reset system parameters.
54 Screen Text Translation	Opens the **Work with Screen Text** screen, where you can customize the messages to be shown during the Password Reset process.

2. Select **51. Control** in the **System Configuration** menu. The **Authentication** screen appears.



Authentication screen

Field/Option/Command Key	Description
Enable use of Authentication	Define who is allowed to use authentication to reset passwords. **0=Disabled** No authentication is permitted **1=By help desk / By user** Authentication can be performed by either the user or the help desk. **2=By user** Authentication can only be performed by the user. **3=By help desk** Authentication can only be performed by the help desk.
Max users per 10 minutes	Defines the maximum number of users who can set their personal questions in a 10 minute period. This is only checked if the users are setting their questions for the first time, as this is when they may request assistance.
Limit to Help Desk hours	You can limit the ability of users to set their personal questions to be permitted only during the defined Help Desk hours. This is only checked if the users are setting their questions for the first time, as this is when they may request assistance.
E-Mail address	The email address to receive notice when users reset their passwords.
Message Queue Name, Library	The message queue to receive notice when users reset their passwords.

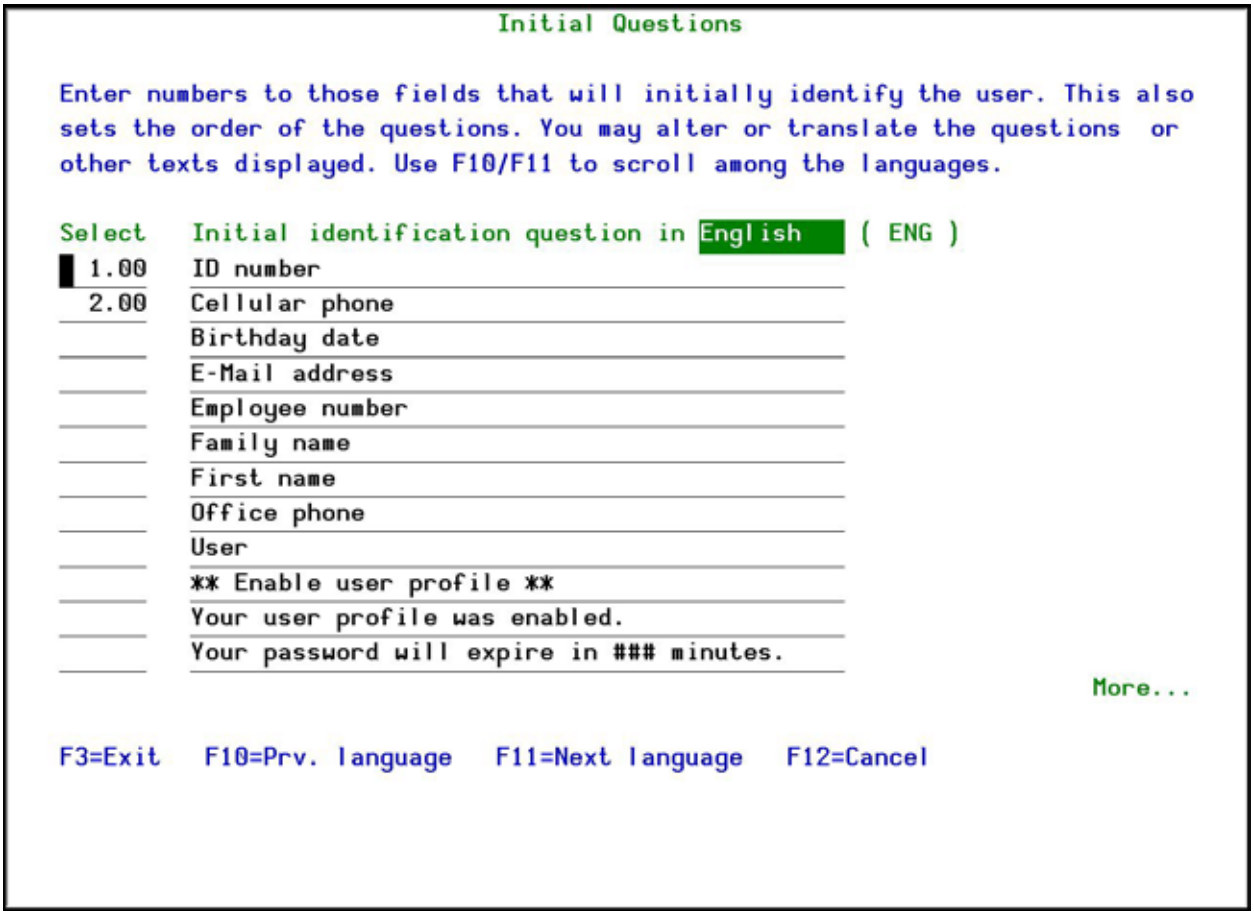
3. Enter your setup definitions and press **Enter**. You are returned to the **System Configuration** menu.

Initial Process Questions

Set up the initial Identification Questions that will be used for Password Reset.

To set up the questions:

1. Select **81. System Configuration** in the **Password Reset** main menu. The **System Configuration** menu appears.
2. Select **52. Initial Process Questions** in the **System Configuration** menu. The **Initial Questions** screen appears.



Initial Questions screen

Field/Option/Command Key	Description
Select	For each question you want to use in the initial identification process, put a number. The questions will be asked in the order you define here. Make sure that you choose a combination of questions that will guarantee a unique identification. For example, choosing just a date of birth may not be sufficient.
Question	The text for the questions that are used for the initial identification process. You can add explanations to the text if necessary. For example, you might add the required date format to the Birthday date text.
F10/F11	Use **F10** and **F11** to scroll from language to language.

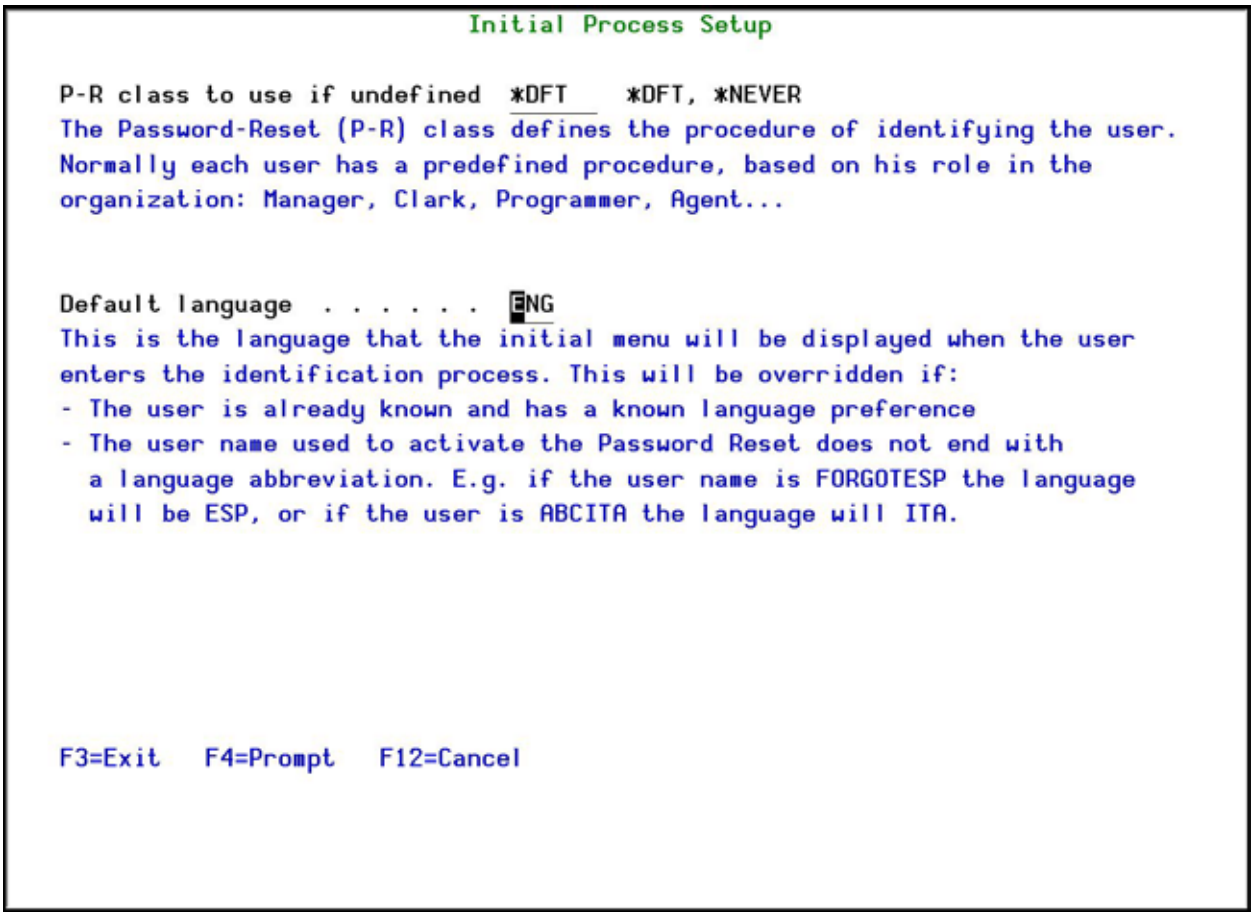
3. Enter your setup definitions and press **Enter**. You are returned to the **System Configuration** menu.

Initial Process Defaults

You must define the environment in which **Password Reset** will work.

To define the **Password Reset** environment:

1. Select **81. System Configuration** in the **Password Reset** main menu. The **System Configuration** menu appears.
2. Select **53. Initial Process Defaults** in the **System Configuration** menu. The **Initial Process Setup** screen appears.



Initial Process Setup screen

Field/Option/Command Key	Description
P-R class to use if undefined	Define the default P-R class to be used for resetting passwords for users who do not have a P-R Class defined. ***DFT**(Default). ***NEVER**

Field/Option/Command Key	Description
Default language	Enter a default language for the Password Reset questions. This is the language in which the initial menu will be displayed when the user enters the identification process. Press **F4** to select from a list of available languages. If the language you require does not appear in the list, there are two non-defined languages (LN1 and LN2) that you can use.

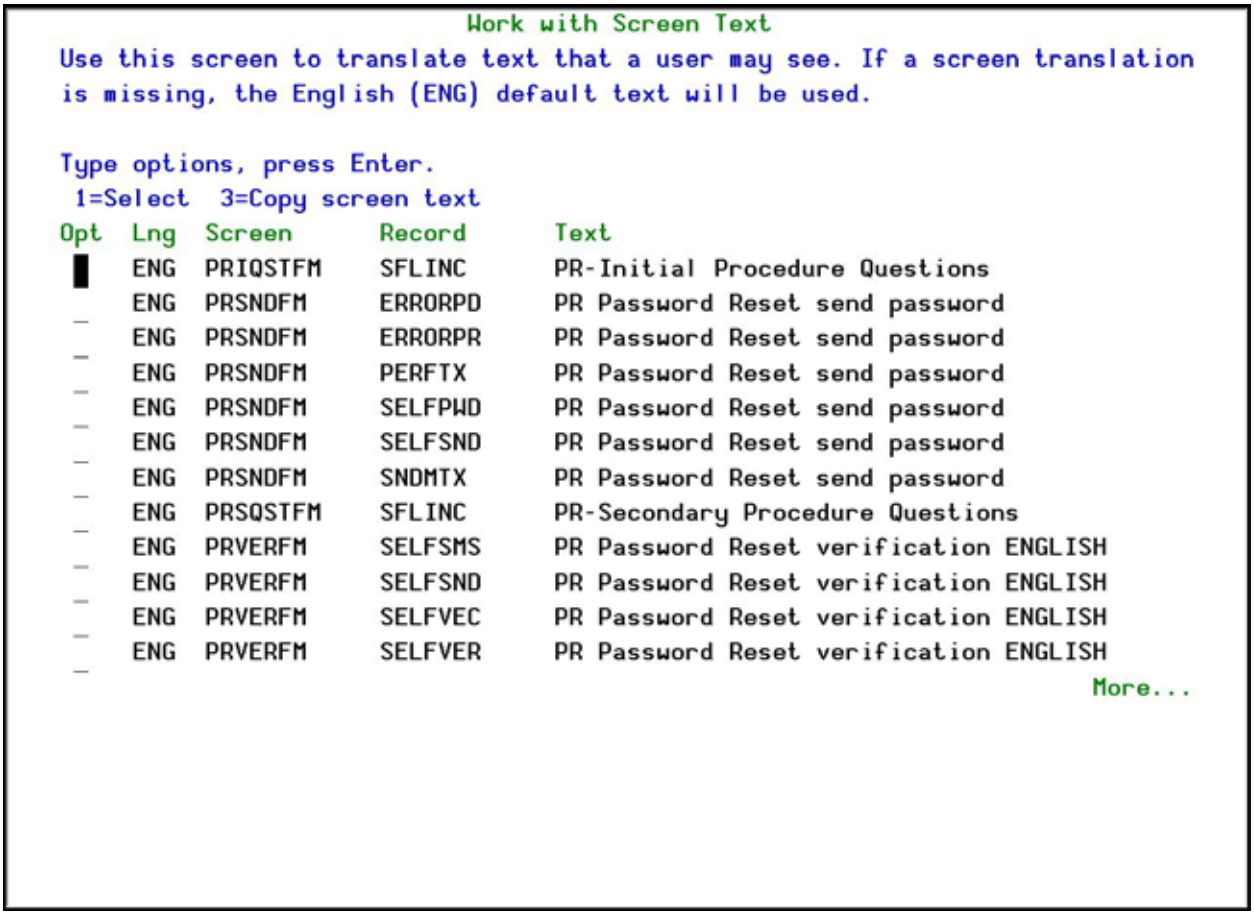
3. Enter your setup definitions and press **Enter**. You are returned to the **System Configuration** menu.

Customize Password Reset Messages

You can customize the messages to be shown during the **Password Reset** process

To customize messages:

1. Select **81. System Configuration** in the **Password Reset** main menu. The **System Configuration** menu appears.
2. Select **54. Screen Text Translation** in the **System Configuration** menu. The **Work with Screen Text** screen appears.

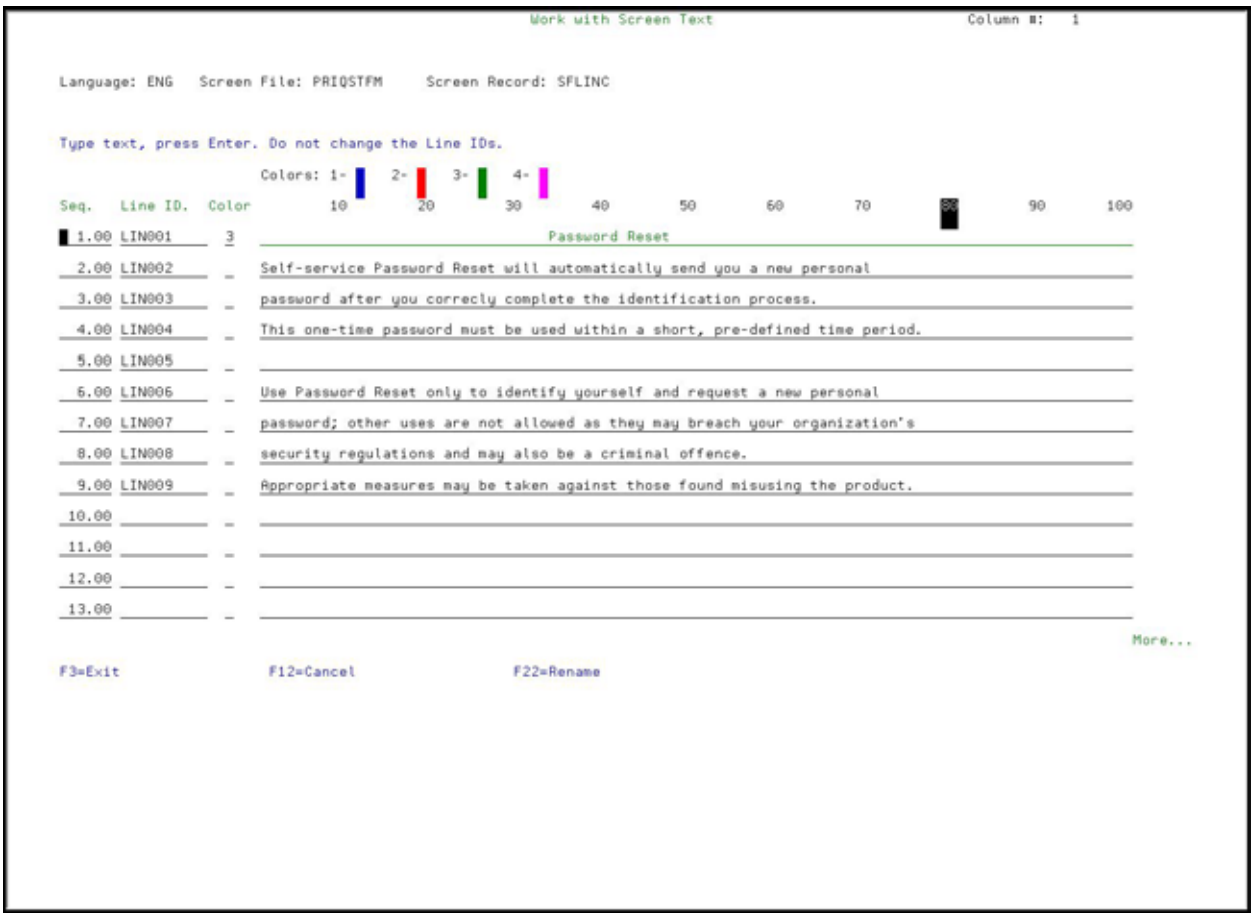


Work with Screen Text screen

Field/Option/Command Key	Description
1=Select	Work with the selected screen.

Field/Option/Command Key	Description
3=Copy screen text	Copy the selected screen to a new screen or a new language.
Language	The language the screen uses
Screen	The name of the screen file
Record	The name of the record in the screen file

3. Select the screen to edit and press **1=Select**.



Screen Text Editing screen

Field/Option/Command Key	Description
Seq	The order the screen lines appear
Line ID	The ID of the line.
Color	The color the of the line when displayed on the screen
Text	The message text to be displayed.

4. Make your changes and press **Enter** twice. You are returned to the **Work with Screen Text** screen.

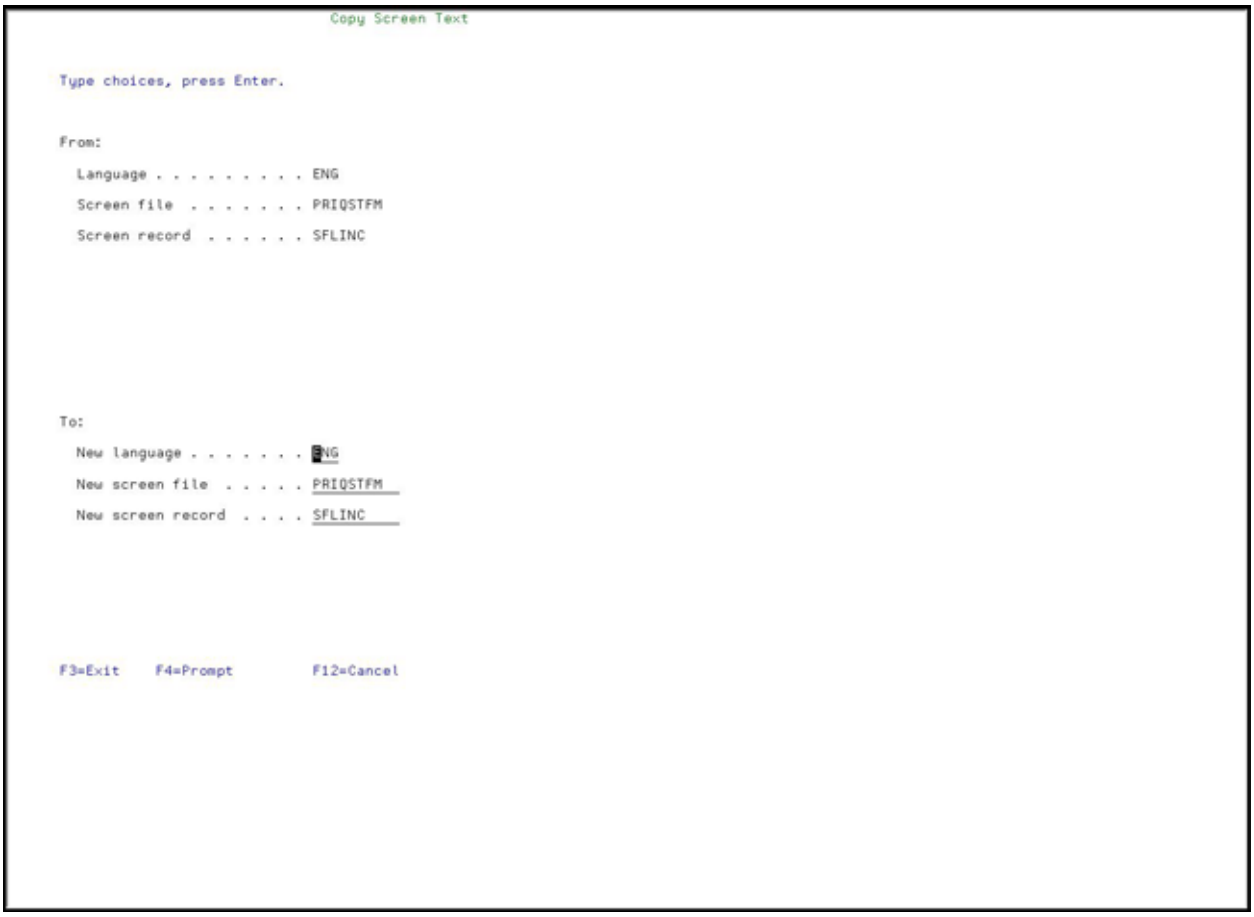
Copy Screen Text Screen

Copy screen text to a new screen file/record or to a new language.

To copy text:

1. Select **81. System Configuration** in the **Password Reset** main menu. The **System Configuration** menu appears.

2. Select **53. Screen Text Editing** in the **System Configuration** menu. The **Work with Screen Text** screen appears.
3. Select the screen to copy and press **3=Copy**. The **Copy Screen Text** screen appears.



Copy Screen Text screen

Field/Option/Command Key	Description
From	
Language	The language of the current text
Screen file	The file to be copied
Screen record	The record to be copied
To	
Language	The language of the new text
Screen file	The new file name
Screen record	The new record

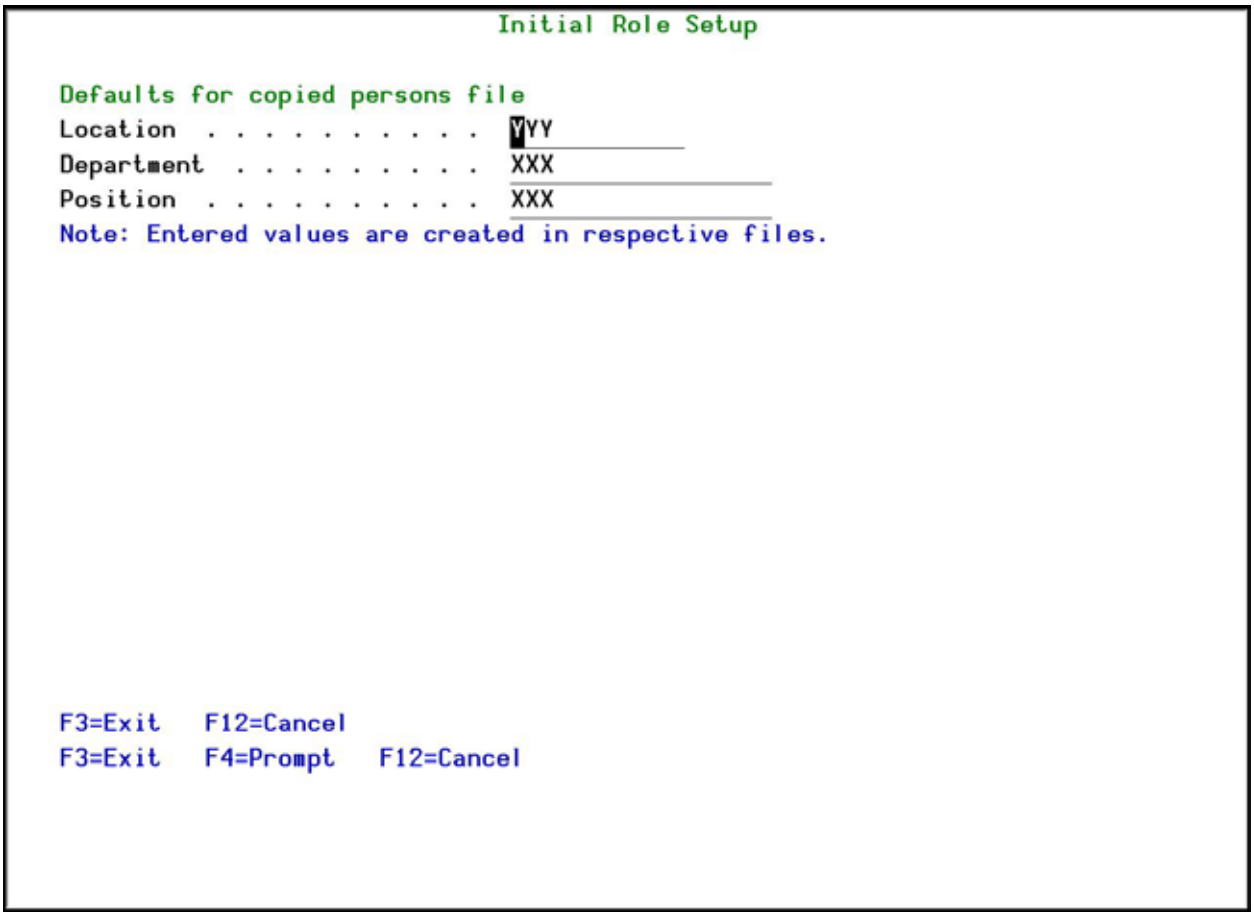
4. Make your changes and press **Enter** twice. You are returned to the **Work with Screen Text** screen.

Copy Attributes

The fields that together make up the role are not mapped when copying data from your organization's files to the **Password Reset** Persons file. You can define defaults for these fields that will be used in the records created when the mapping is run.

To define field defaults:

1. Select **81. System Configuration** in the **Password Reset** main menu. The **System Configuration** menu appears.
2. Select **61. Copy Attributes** in the **System Configuration** menu. The **Initial Role Setup** screen appears.



Initial Role Setup screen

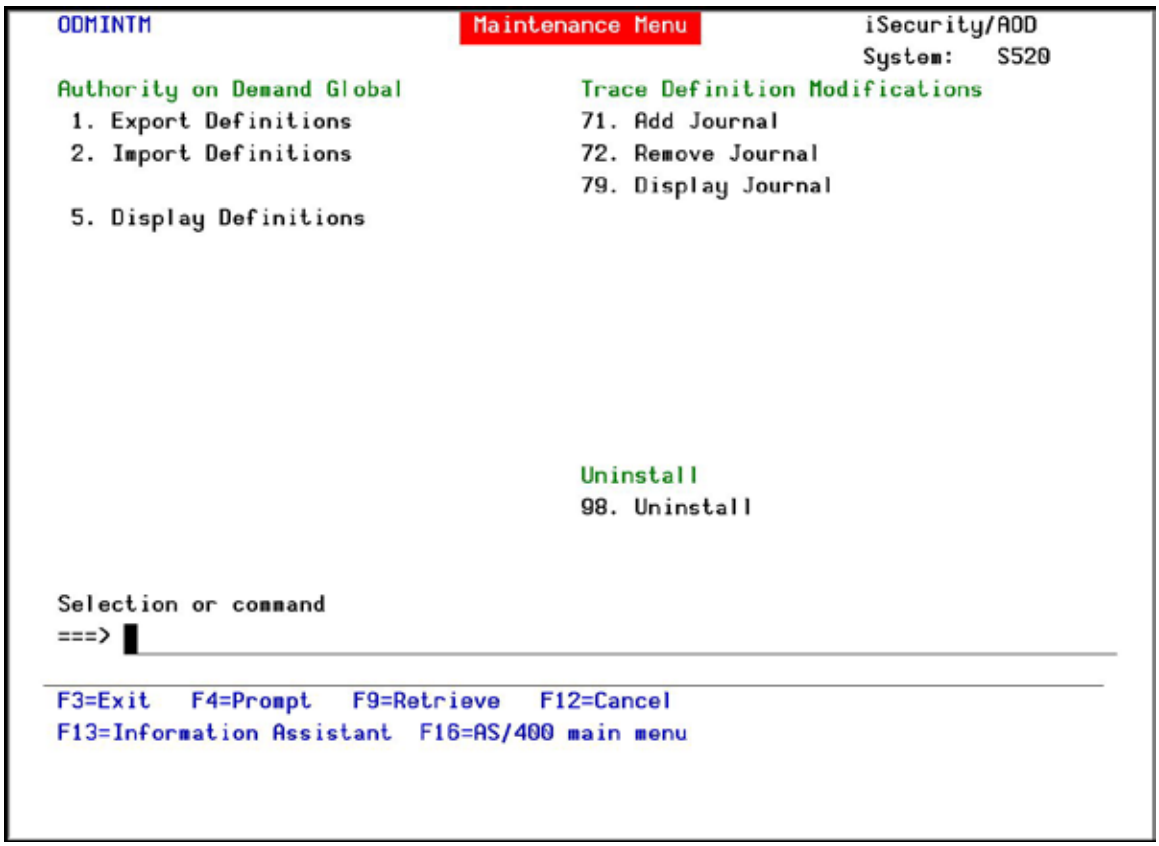
Field/Option/Command Key	Description
Location	A default location
Department	A default department
Position	A default position

3. Enter your setup definitions and press **Enter**. You are returned to the **System Configuration** menu.

Note: The entered values are used to create records in the respective files for each of the three fields.

Maintenance Menu

The **Maintenance Menu** enables you to set and display global definitions for **Password Reset**. To access the **Maintenance Menu**, select **82. Maintenance Menu** from the main menu.

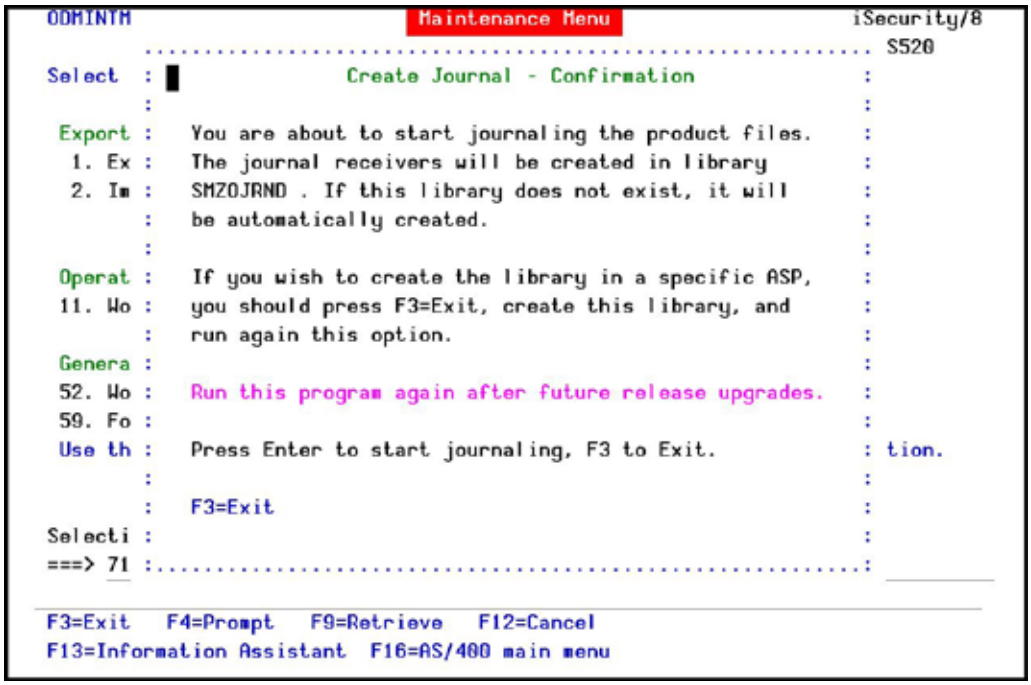


Maintenance Menu

Trace Definition Modifications

Add Journal

1. Select **71. Add Journal** from the **Maintenance Menu**. The **Create Journal – Confirmation** screen appears.



Create Journal - Confirmation

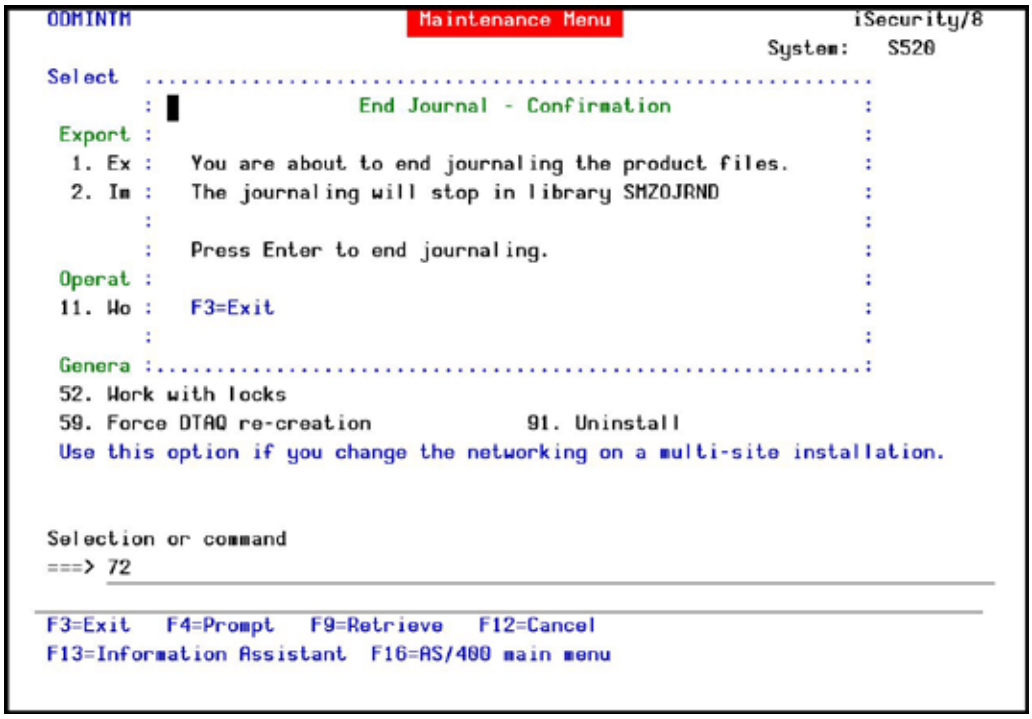
2. Press **Enter** to confirm. The process of journaling the product files begins. The journal receivers will be created in library **SMZ0JRND**. If this library does not exist, it will be automatically created.

Note: If you wish to create the library in a different ASP, press **F3=Exit**, create the library and run this option again.

You must re-run this option after every release upgrade.

Remove Journal

1. Select **72. Remove Journal** from the **Maintenance Menu**. The **End Journal – Confirmation** screen appears.

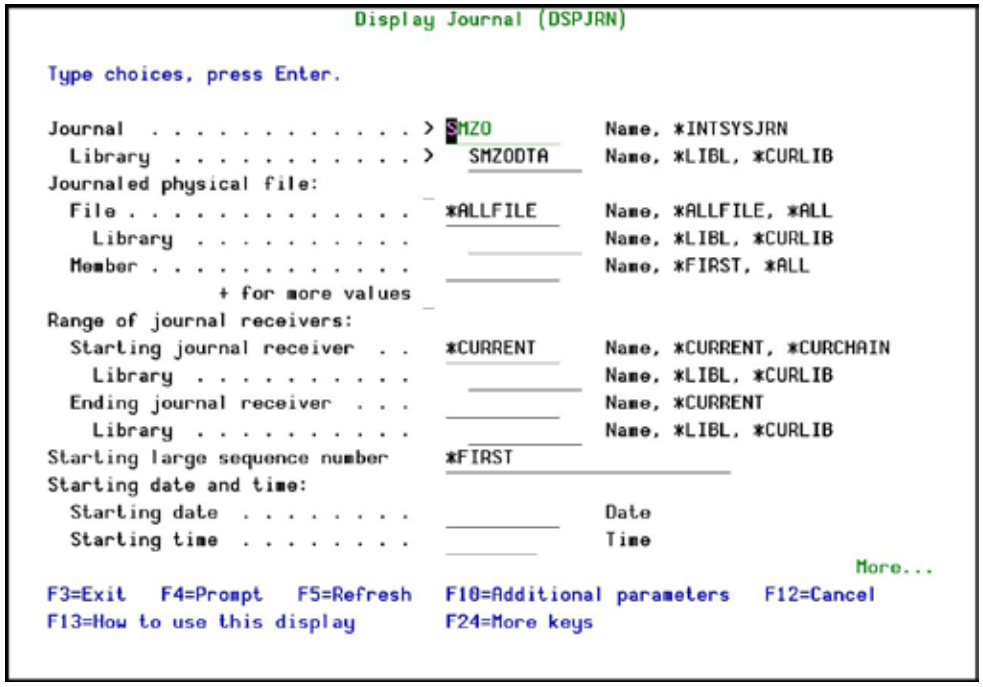


End Journal - Confirmation

2. Press **Enter** to confirm.

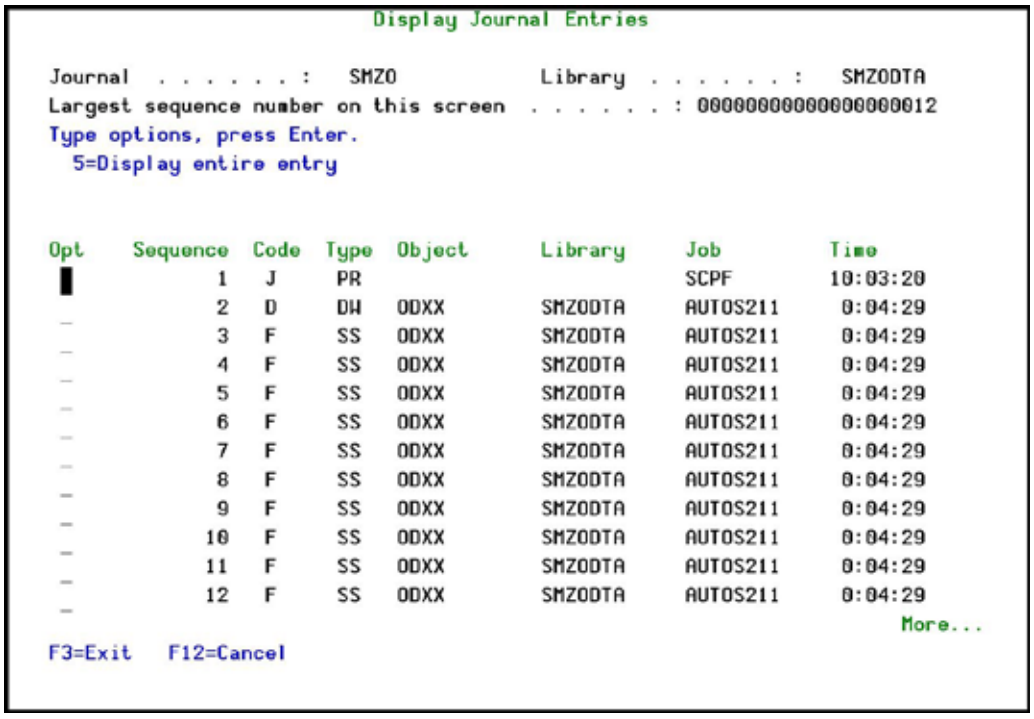
Display Journal

1. Select **79. Display Journal** from the **Maintenance Menu**. The **Display Journal (DSPJRN)** screen appears with preset filter parameters entered for you.



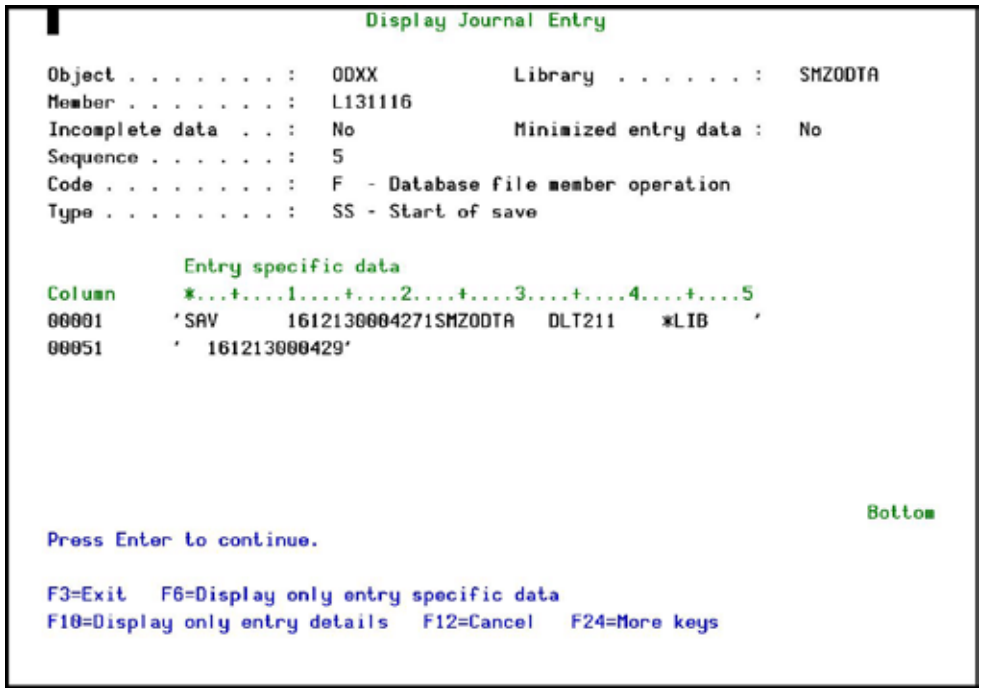
Display Journal (DSPJRN) screen

2. Press **Enter**. The **Display Journal Entries** screen appears.



Display Journal Entries screen

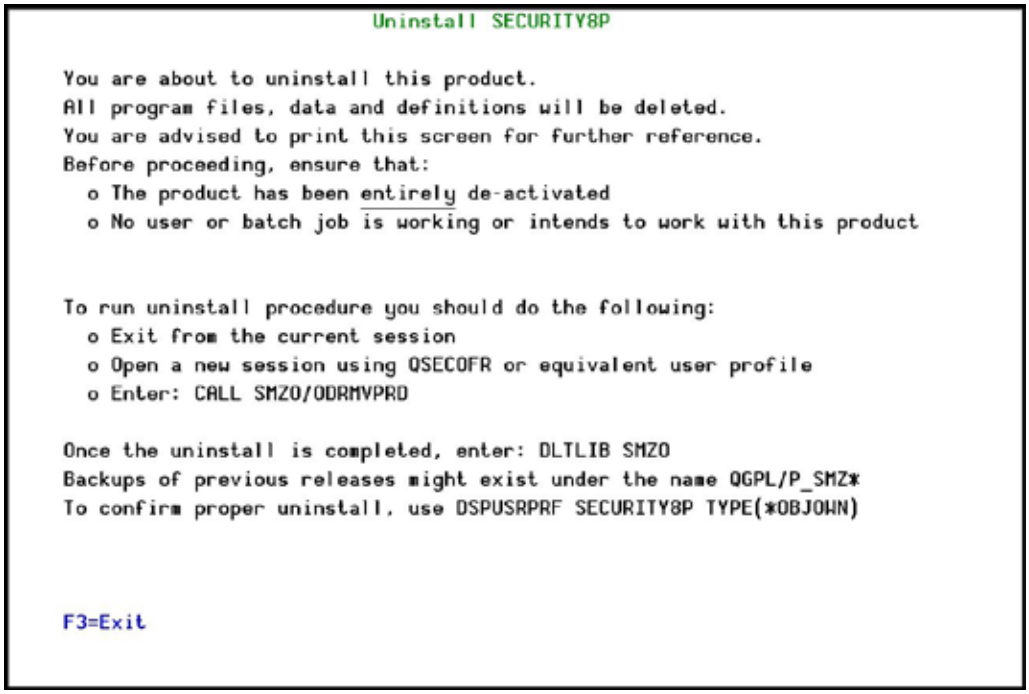
3. To display a specific entry, type **5** by that entry and press **Enter**. The **Display Journal Entry** screen appears.



Display Journal Entry screen

Uninstall

To uninstall the product, select **98. Uninstall Product** from the **Maintenance Menu**, and follow the directions on the screen.

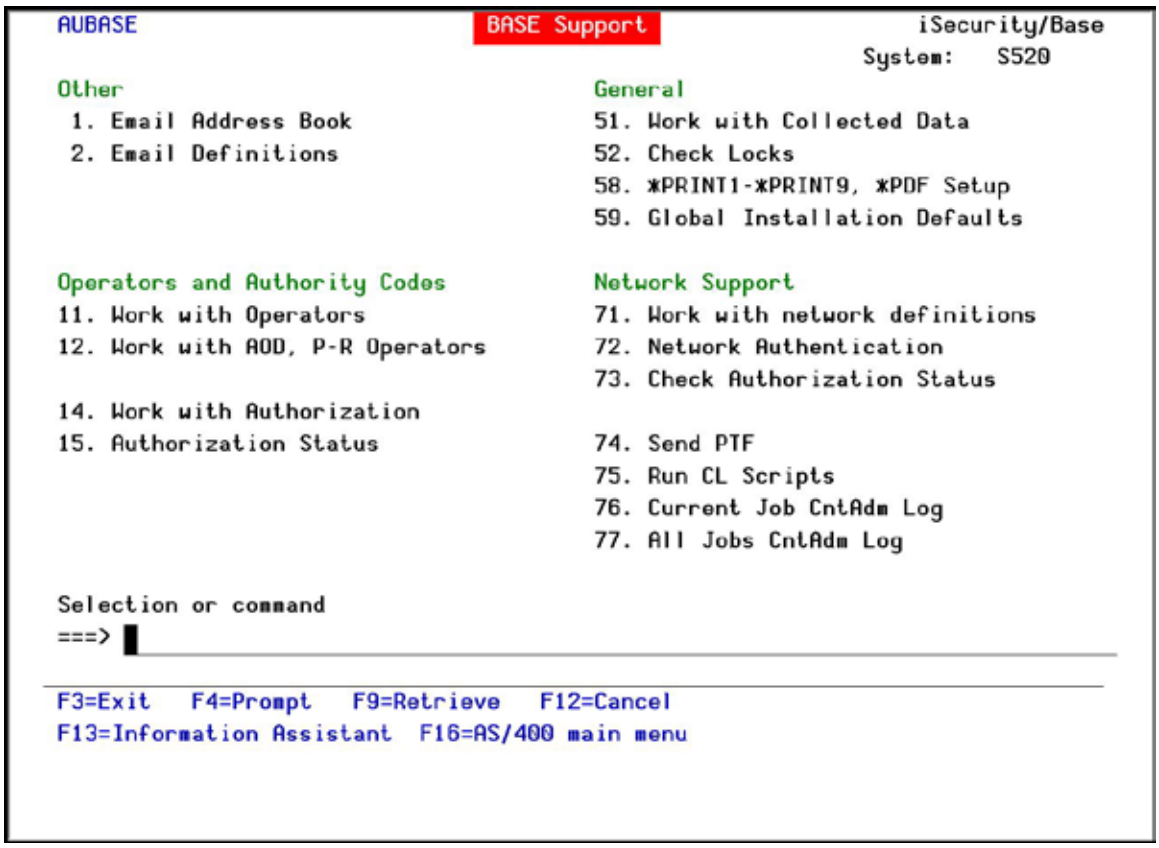


Uninstall SECURITY8P screen

Note: Running this option will uninstall not just **Password Reset**, but also **Authority on Demand**.

BASE Support

The **BASE Support** menu enables you to work with various settings that are common for all modules of iSecurity. This menu, with all its options, is in all iSecurity major modules. To access the **BASE Support** menu, select **89. BASE Support** from the **Password Reset** main menu.



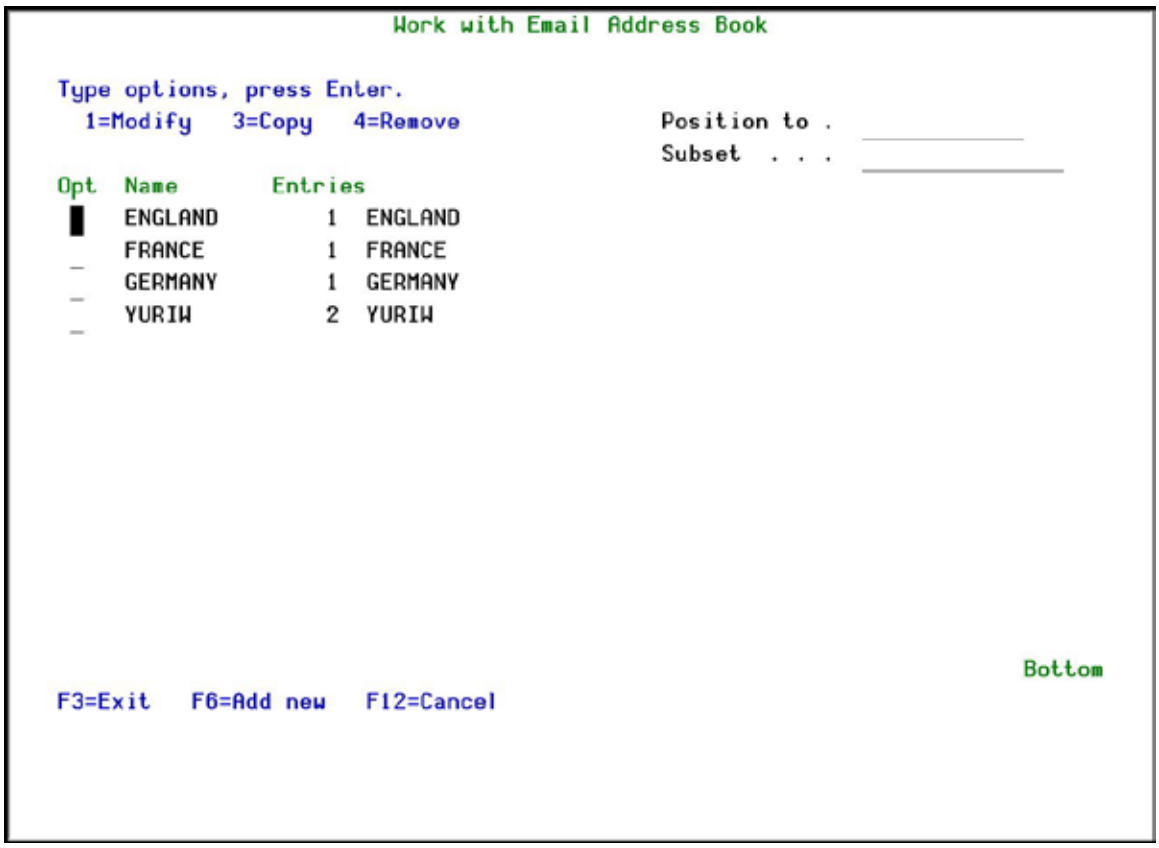
BASE Support

Other

Email Address Book

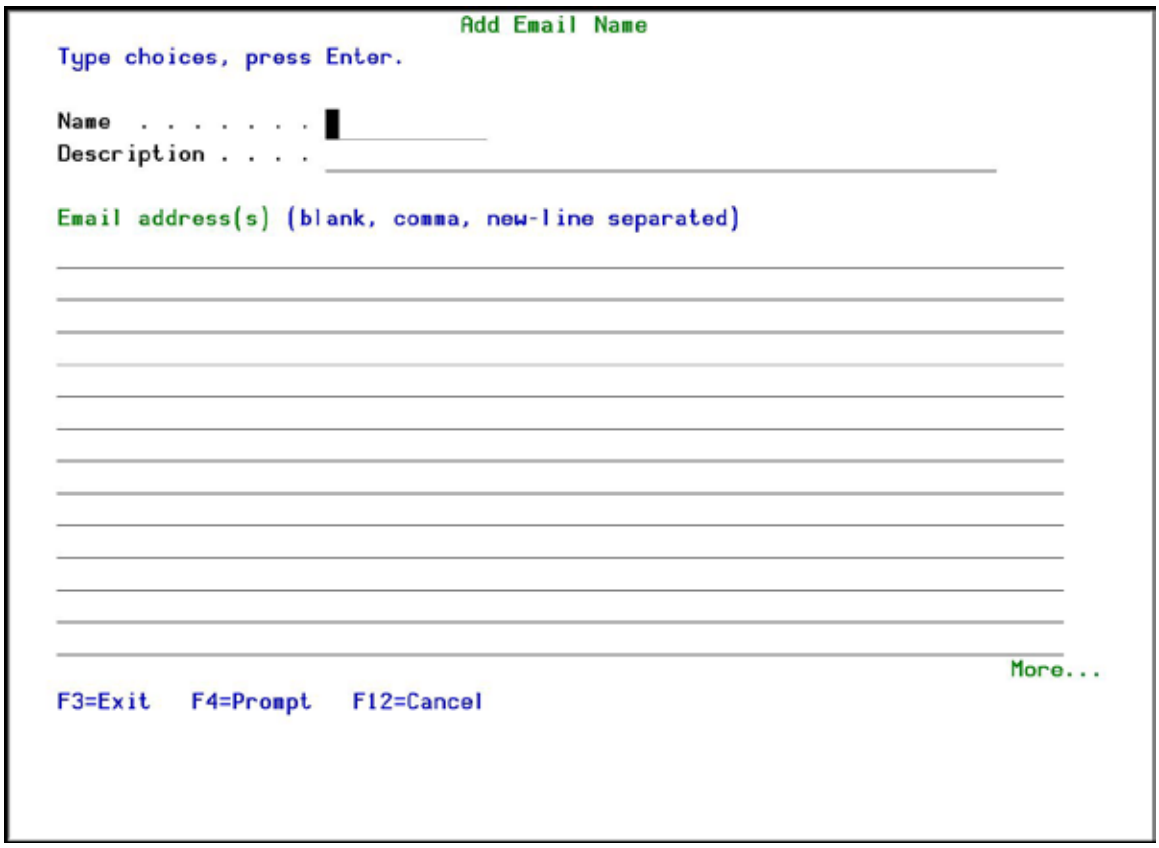
You can define the email address to be used for each user profile. You can also use this option to define an email group, with multiple addresses.

1. Select **1. Email Address Book** from the **BASE Support** menu. The **Work with Email Address Book** screen appears.



Work with Email Address Book

2. Press **F6** to add a new address entry (or type **1** next to a name to modify it). The **Add Email Name** screen appears.



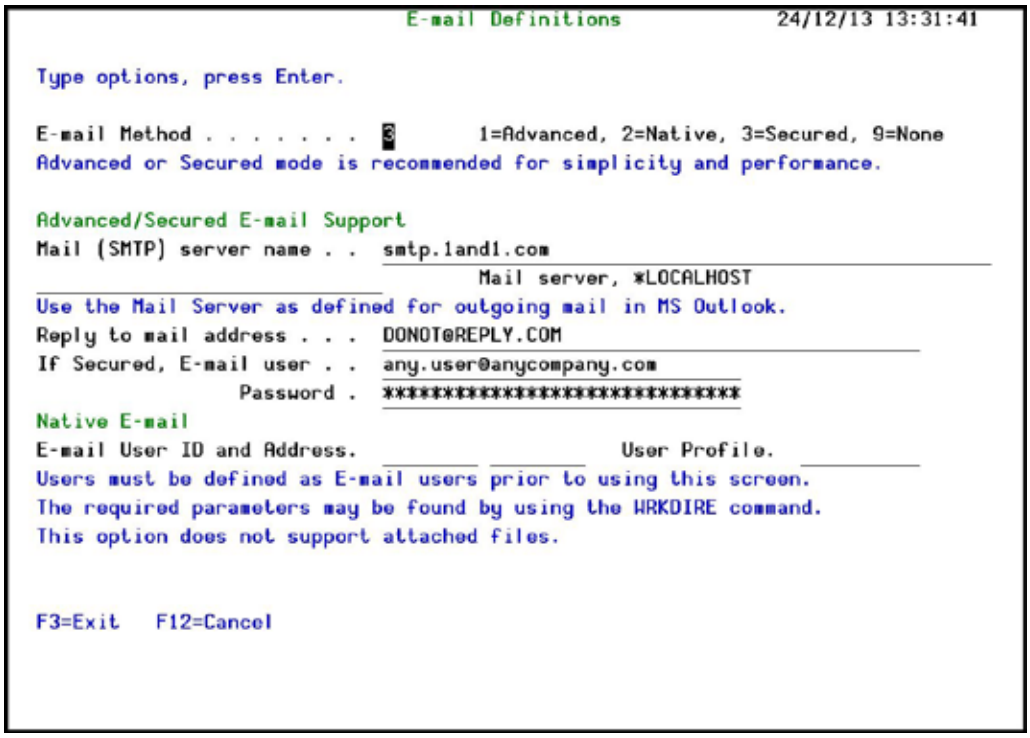
Add Email Name

3. Enter a **Name**, **Description**, and all the associated email addresses and press **Enter**.

Email Definitions

Password Reset can send out automatic emails every time a temporary authority is used.

1. Select **2. Email Definitions** from the **BASE Support** menu. The **E-mail Definitions** screen appears.



E-mail Definitions

2. Enter the required fields as defined below and press **Enter**.

Parameter	Description
E-mail Method	**1**=Advanced **2**=Native **3**=Secured **9**=None Advanced or Secured mode is recommended for simplicity and performance. **Note**: If using **2**=native, Users must be defined as E-mail users prior to using this screen. The required parameters may be found by using the WRKDIRE command. This option does not support attached files.
Mail (SMTP) server name	The name of the STMP server or *LOCALHOST
Reply to mail address	The e-mail address to receive replies.
If secured, E-mail user and Password	If you chose **1**=Advanced or **3**=Secured for the E-mail method, enter the email user that will be used to send the emails and the password of that user
E-mail User ID and Address	If you chose **2**=Native for the E-mail method, enter the user ID and address that will be used to send the emails.
User Profile	If you chose **2**=Native for the E-mail method, enter the user profile that will be used to send the emails.

Operators and Authority Codes

Work with Operators

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

There are three default groups:

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

iSecurity related objects are secured automatically by product authorization lists (named **security1P**). This strengthens the internal security of the product. It is essential that you use **Work with Operators** to define all users who have ***SECADM**, ***AUDIT** or ***AUD#SECAD** privileges, but do not have all object authority. The **Work with Operators** screen has Usr (user management) and Adm for all activities related to starting, stopping subsystems, jobs, import/export and so on. **iSecurity** automatically adds all users listed in **Work with Operators** to the appropriate product authorization list.

Users may add more operators, delete them, and give them authorities and passwords according to their own judgment. Users can even make the new operators' definitions apply to all their systems; therefore, upon import, they will work on every system.

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

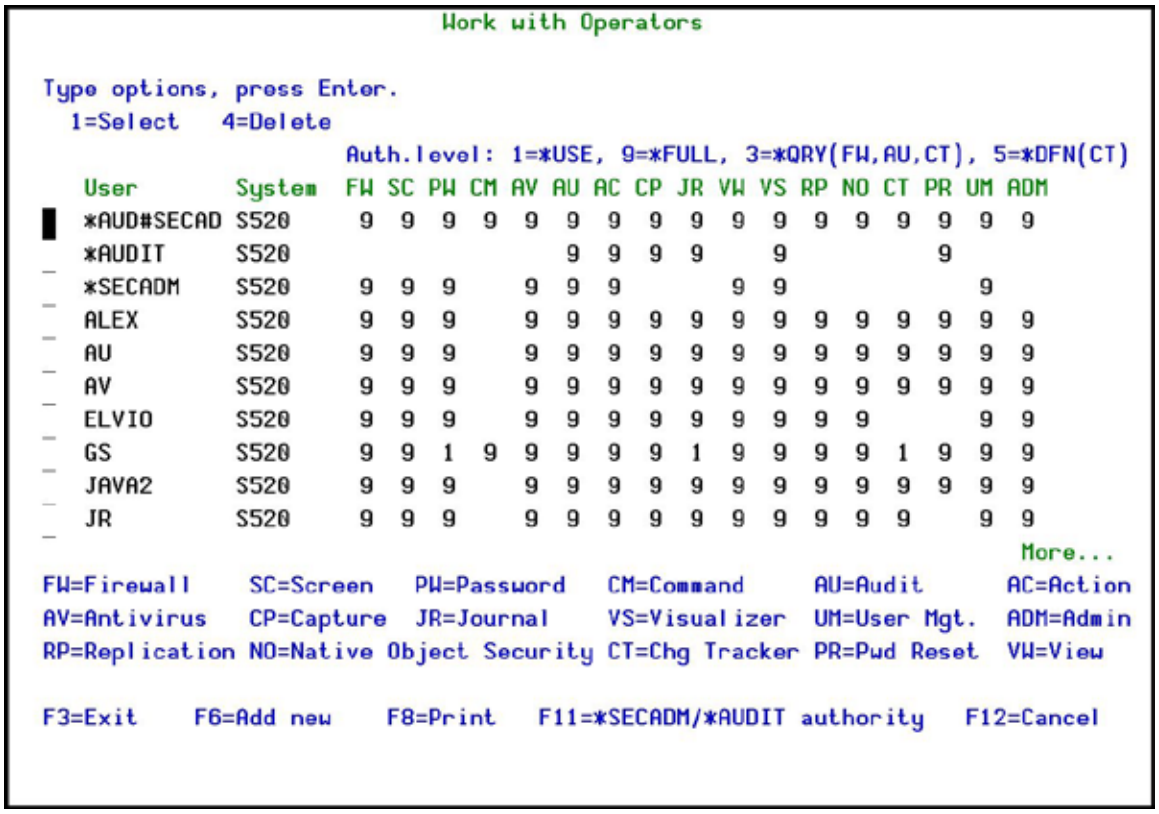
If your organization wants the default to be *BLANK, then the following command must be used:
`CRTDTAARA SMZTMPC/DFTPWD *char 10`

This command creates a data area called DFTPWD in library SMZTMPC. The data area is 10 bytes long and is blank.

NOTE: When installing **iSecurity** for the first time, certain user(s) might not have access according to the new authority method. Therefore, the first step you need to take after installing is to edit those authorities.

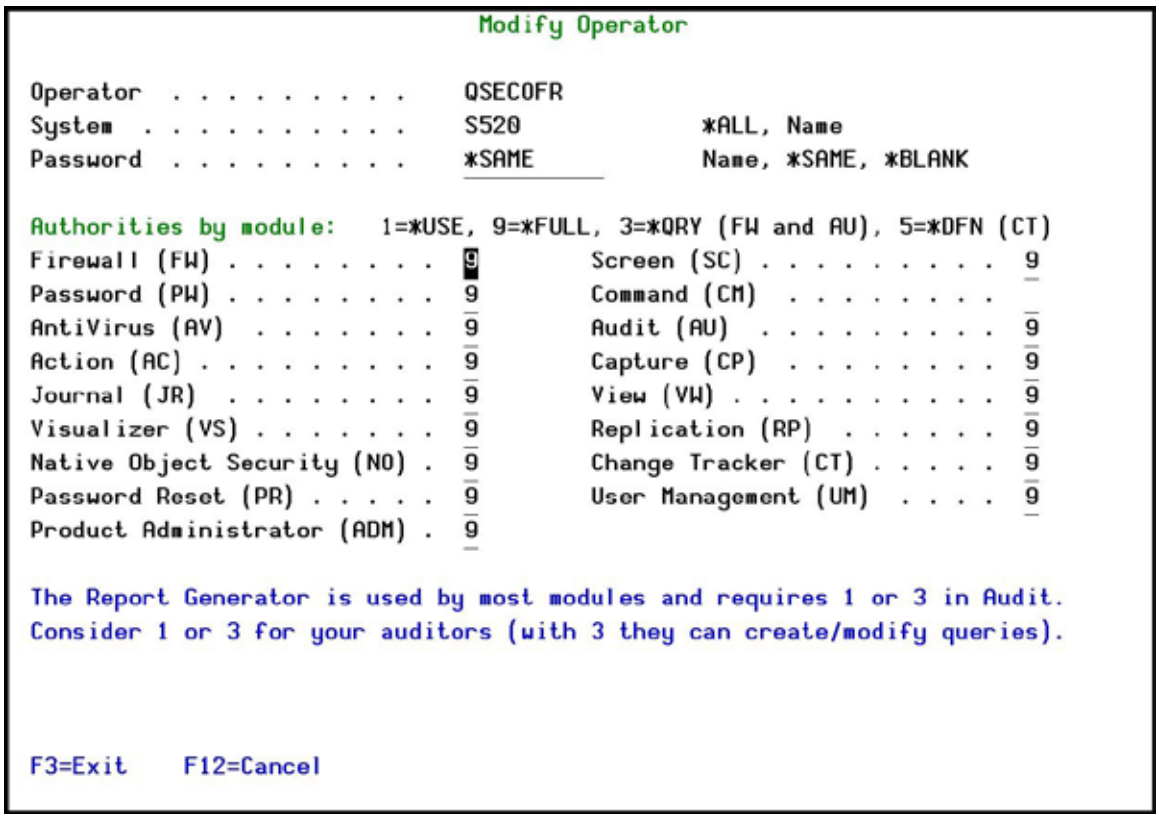
To modify operators' authorities:

1. Select **11. Work with Operators** from the **BASE Support** menu. The **Work with Operators** screen appears.



Work with Operators

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



Modify Operator

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

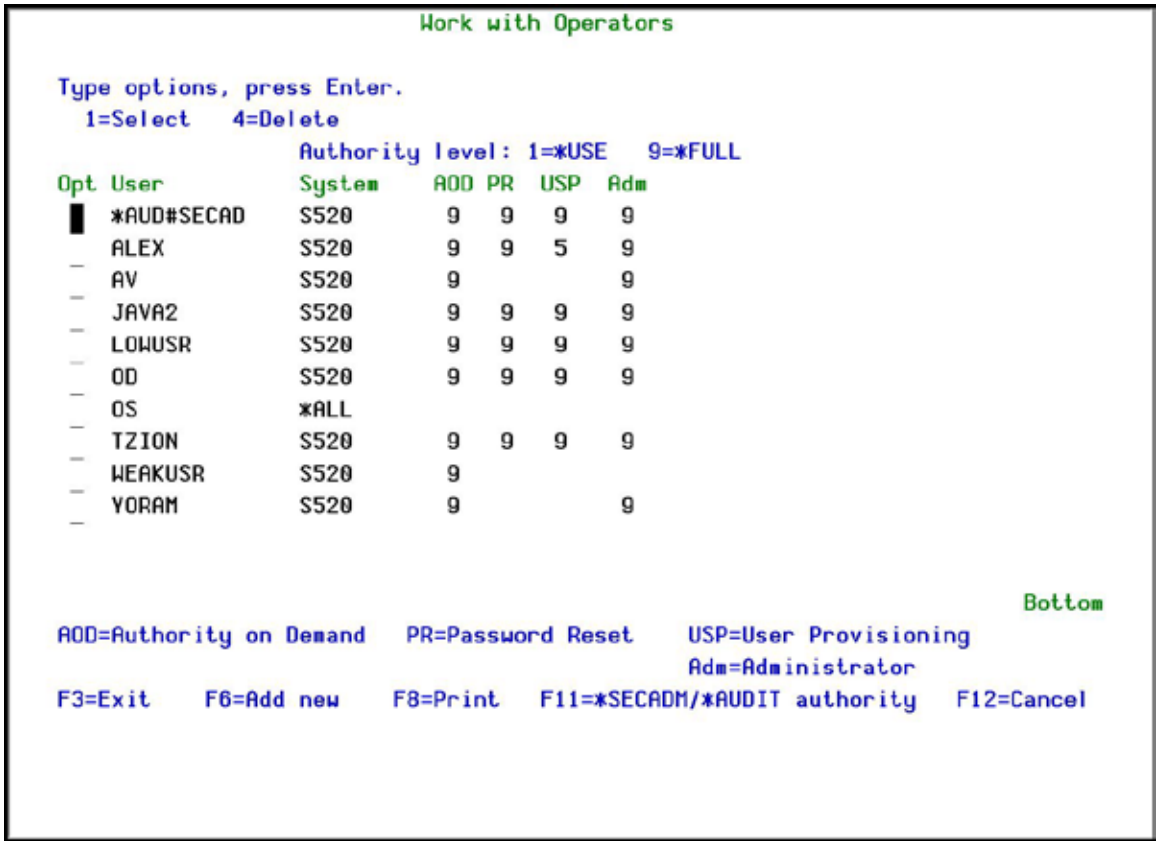
Most modules use the Report Generator, which requires access to the Audit module. For all users who will use the Report Generator, you should define their access to the Audit module as either 1 or 3. Option 1 should be used for users who will only be running queries. Use option 3 for all users who will also be creating/modifying queries.

3. Set authorities and press **Enter**. A message appears to inform that the user being added/modified was added to the Authority list that secures the product's objects; the user carries Authority *CHANGE and will be granted Object operational authority. The Authority list is created in the installation/release upgrade process. The SECURITY_P user profile is granted Authority *ALL whilst the *PUBLIC is granted Authority *EXCLUDE. All objects in the libraries of the product (except some restricted special cases) are secured via the Authority list.

Work with AOD, P-R Operators

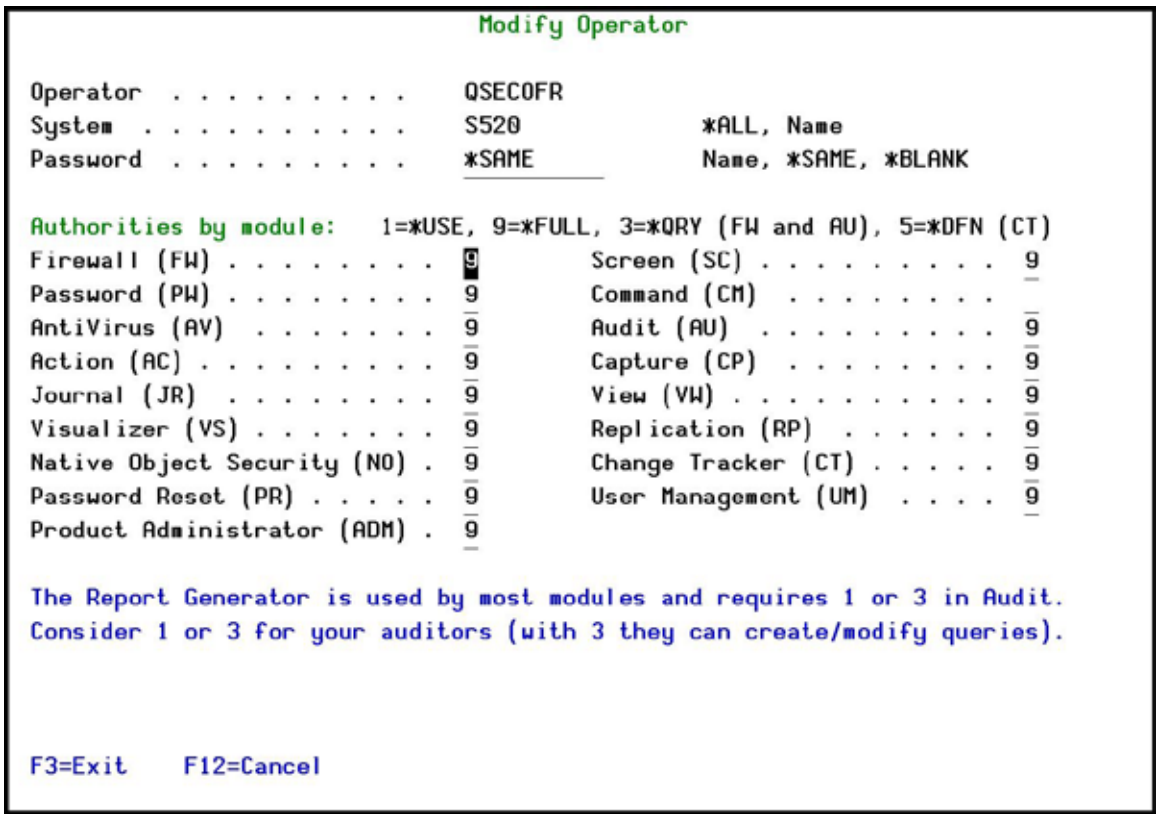
To modify operators' authorities:

1. Select **12. Work with AOD, P-R Operators** from the **BASE Support** menu. The **Work with Operators** screen appears.



Work with Operators

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



Modify Operator

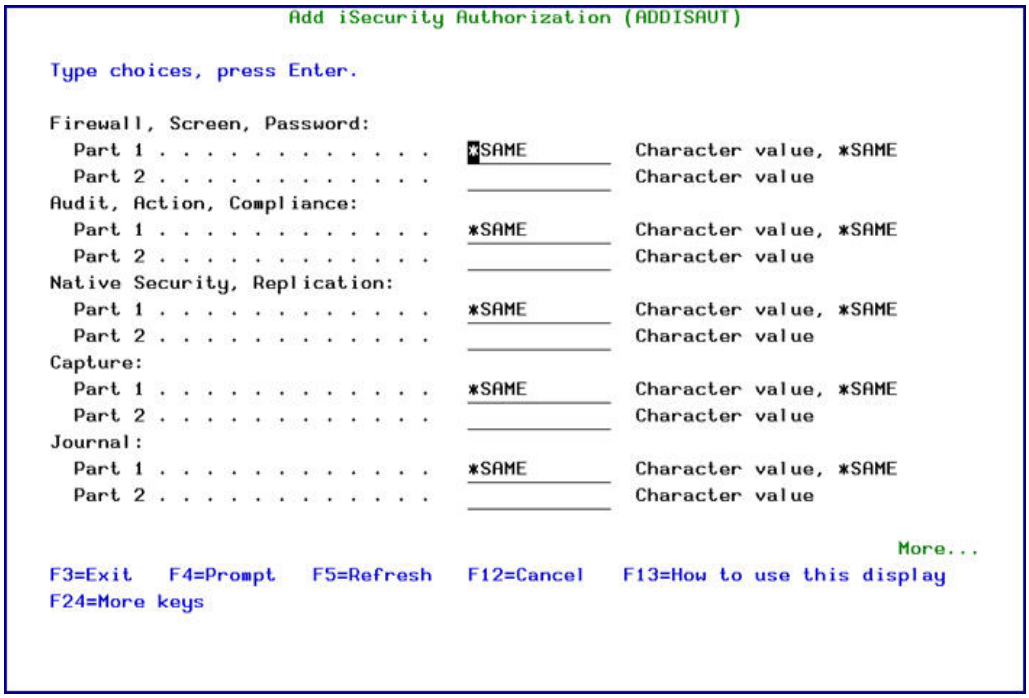
Option	Description
Password	**Name** = Password ***Same** = Same as previous password when edited ***Blank** = No password
1 = *USE	Read authority only
9 = *FULL	Read and Write authority
3 = *QRY	Run Queries. For auditor use.
5 = *DFN	For Change Tracker use.

3. Set authorities and press **Enter**. A message appears to inform that the user being added/modified was added to the Authority list that secures the product's objects; the user carries Authority *CHANGE and will be granted Object operational authority. The Authority list is created in the installation/release upgrade process. The SECURITY_P user profile is granted Authority *ALL whilst the *PUBLIC is granted Authority *EXCLUDE. All objects in the libraries of the product (except some restricted special cases) are secured via the Authority list.

Work with Authorization

You can insert license keys for multiple products on the computer using one screen.

1. Select **14. Work with Authorization** from the **BASE Support** menu. The **Add iSecurity Authorization** screen appears.



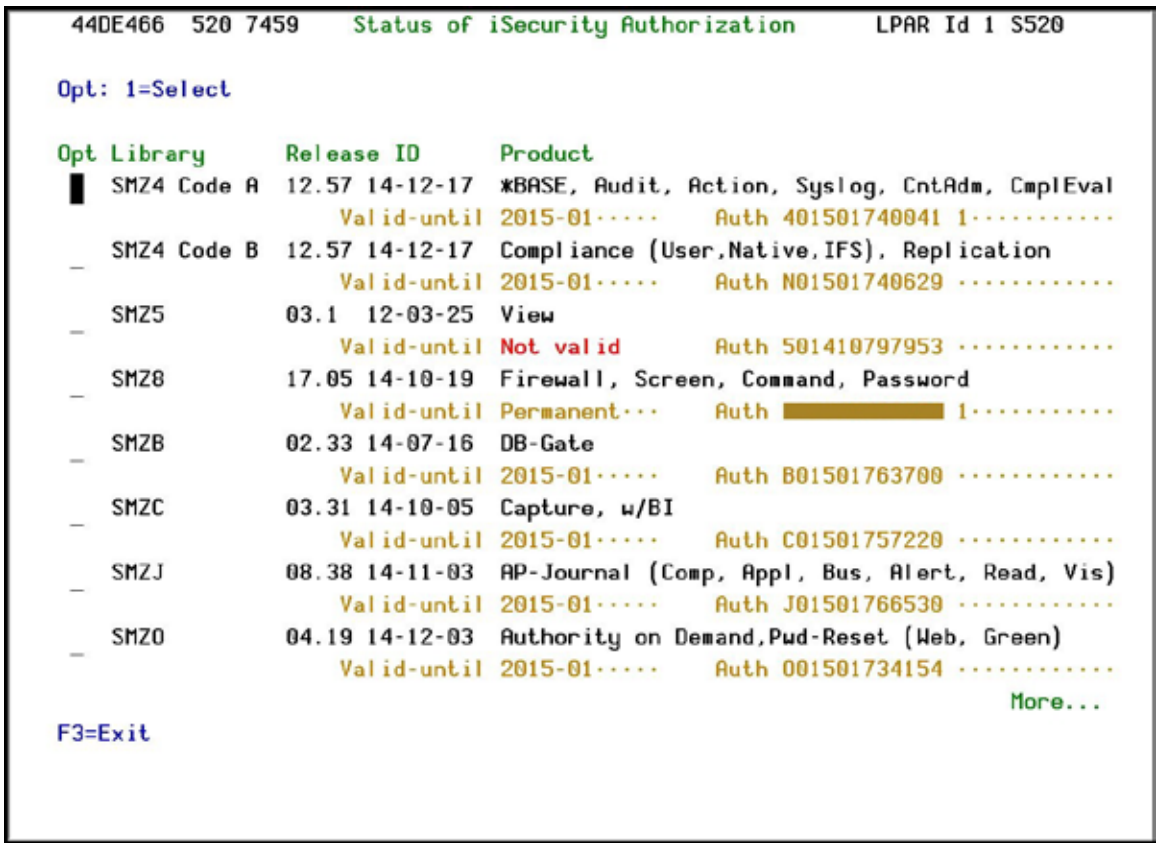
Add iSecurity Authorization (ADDISAUT)

2. Enter the required parameters and press **Enter**.

Display Authorization Status

You can display the current authorization status of all installed iSecurity products on the local system.

1. Select **15. Authorization Status** from the **BASE Support** menu. The **Status of iSecurity Authorization** screen appears.



Status of iSecurity Authority Codes

2. Select a specific line and type **1** in the **Opt** field to see the authority details of one specific product.

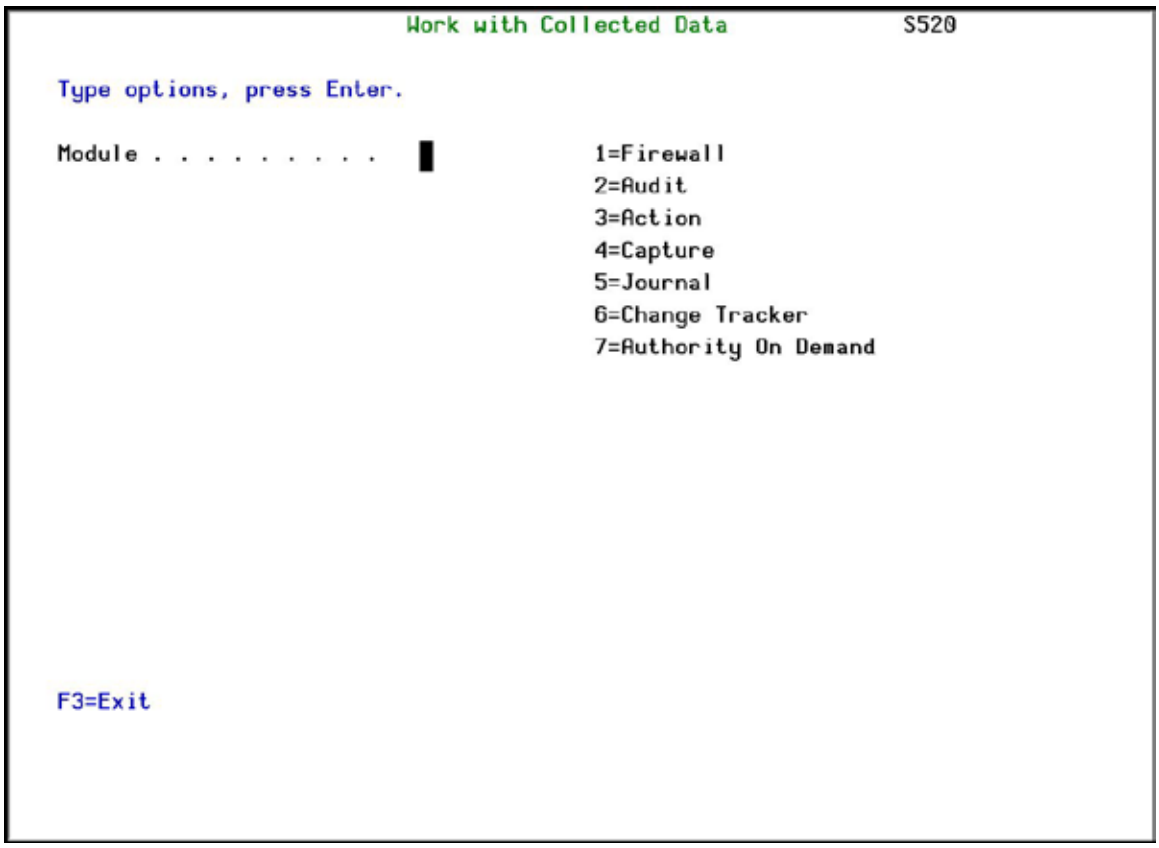
NOTE: Codes that will expire in less than 14 days appear in pink
Permanent codes have deliberately been hidden in this screenshot.

General

Work with Collected Data

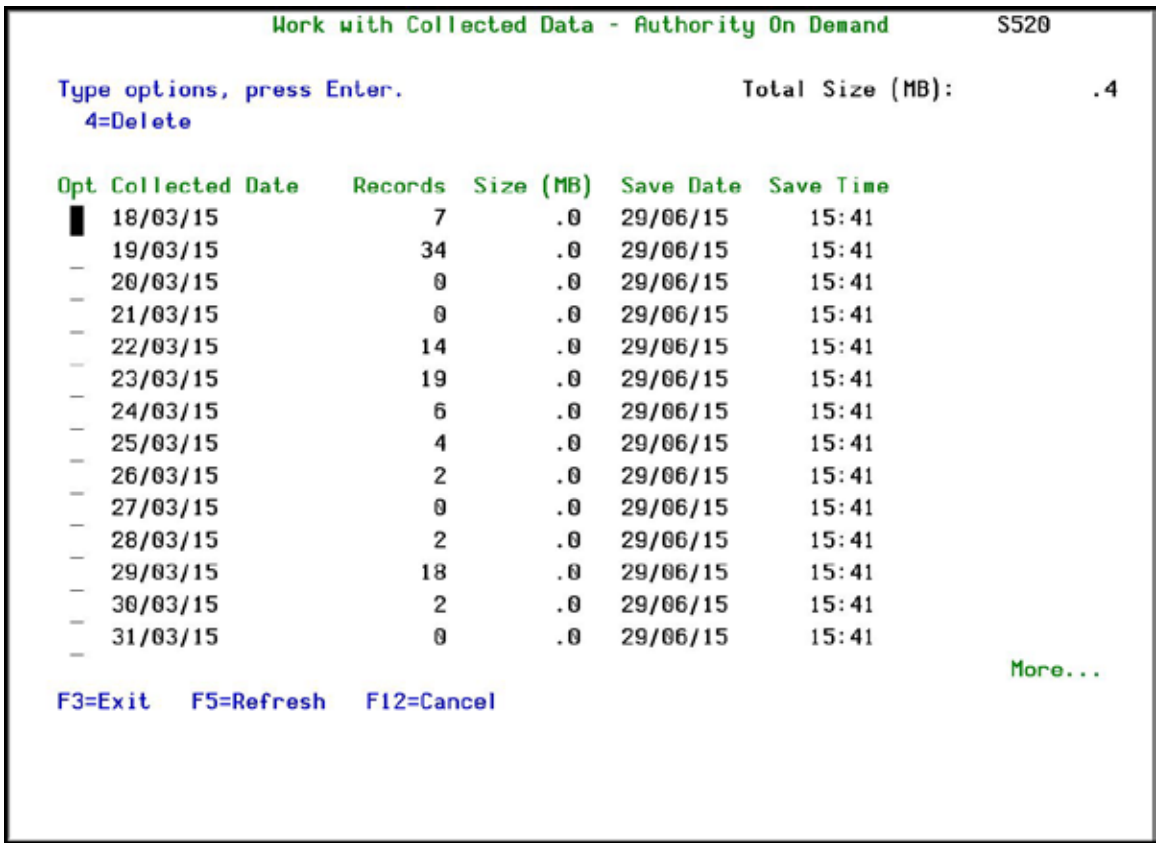
Administrators can view summaries of journal contents of various products by day, showing the number of entries for each day together with the amount of disk space occupied. Administrators can optionally delete individual days to conserve disk space.

1. Select **51. Work with Collected Data** from the **BASE Support** menu. The **Work with Collected Data** screen appears.



Work with Collected Data

2. Enter **7** (Authority On Demand) and press **Enter**. The **Work with Collected Data – Authority On Demand** screen appears.



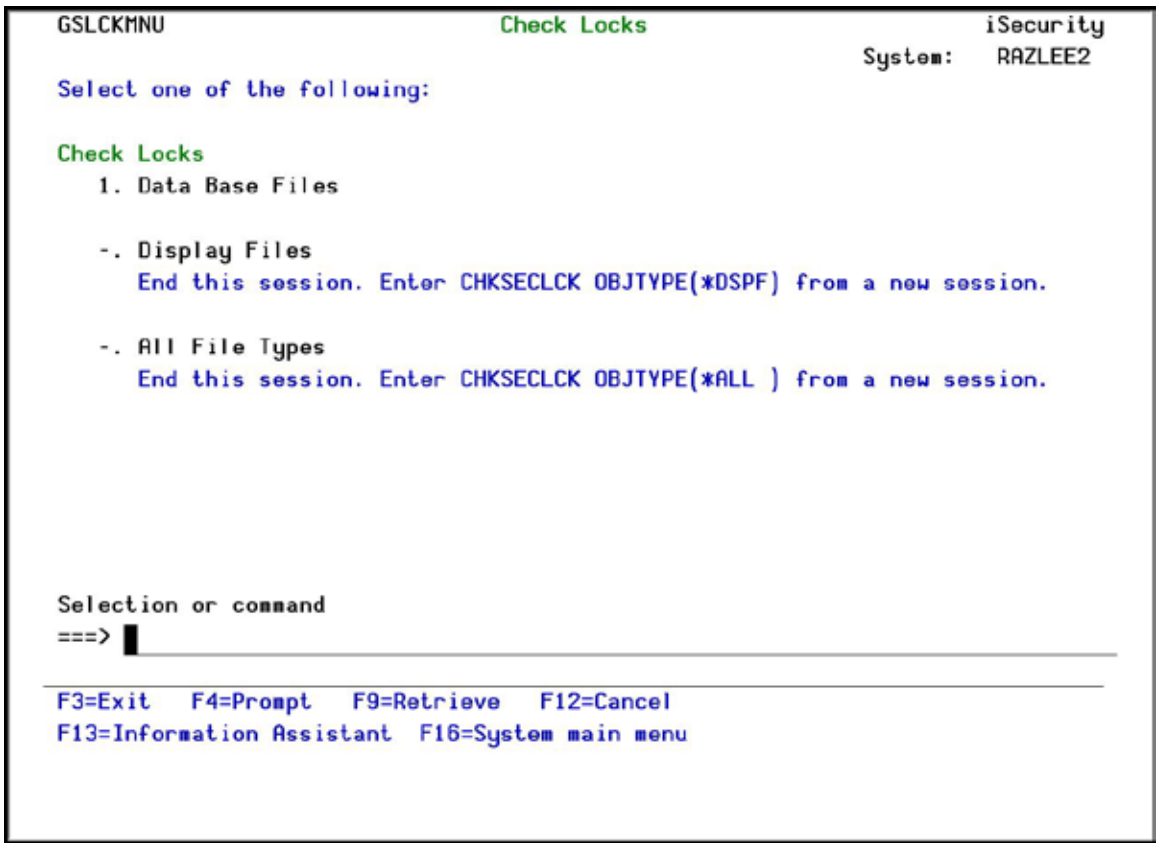
Work with Collected Data – Authority On Demand

3. Select **4** to delete data from specific date(s) and press **Enter**.

Check Locks

You need to run this option before you upgrade your system to check if any of the AOD files are being used. If they are, you must ensure that they are not in use before you run the upgrade.

1. Select **52. Check Locks** from the **BASE Support** menu. The **Check Locks** screen appears.



Check Locks

2. Select one of the commands that appear on the screen.

*PRINT1-*PRINT9 Setup

Password Reset allows you to define up to nine specific printers to which you can send printed output. These may be local or remote printers. ***PRINT1-*PRINT9** are special values which you can enter in the **OUTPUT** parameter of any commands or options that support printed output.

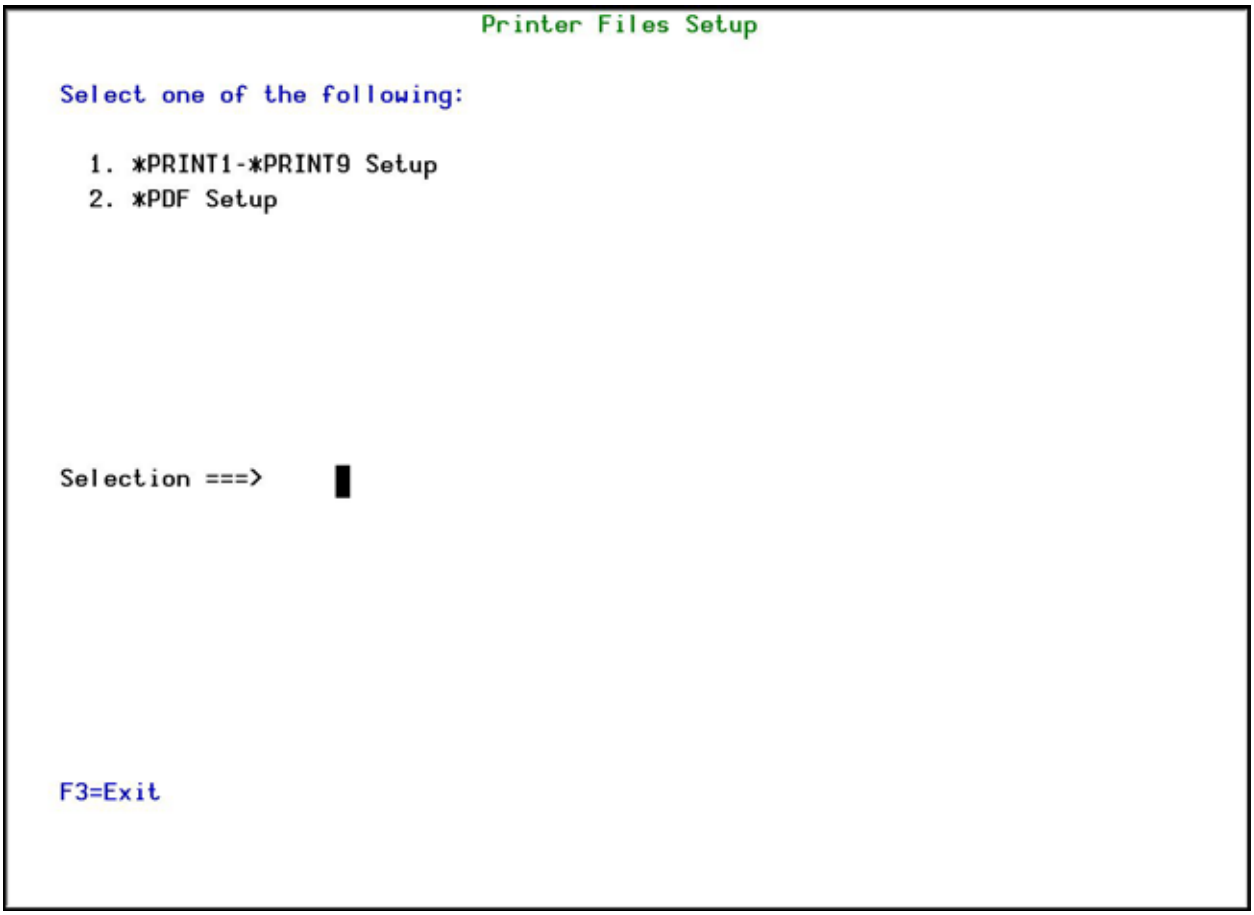
Output to one of the nine remote printers is directed to a special output queue specified on the ***PRINT1-*PRINT9 User Parameters** screen, which, in turn, directs the output to a print queue on the remote system. You use the CHGOUTQ command to specify the IP address of the designated remote location and the name of the remote output queue.

By default, two remote printers are predefined. ***PRINT1** is set to print at a remote location (such as the home office). *PRINT2 is set to print at a remote location in addition to the local printer. In addition:

- *PRINT3 creates an excel file.
- *PRINT3-9 are user modifiable

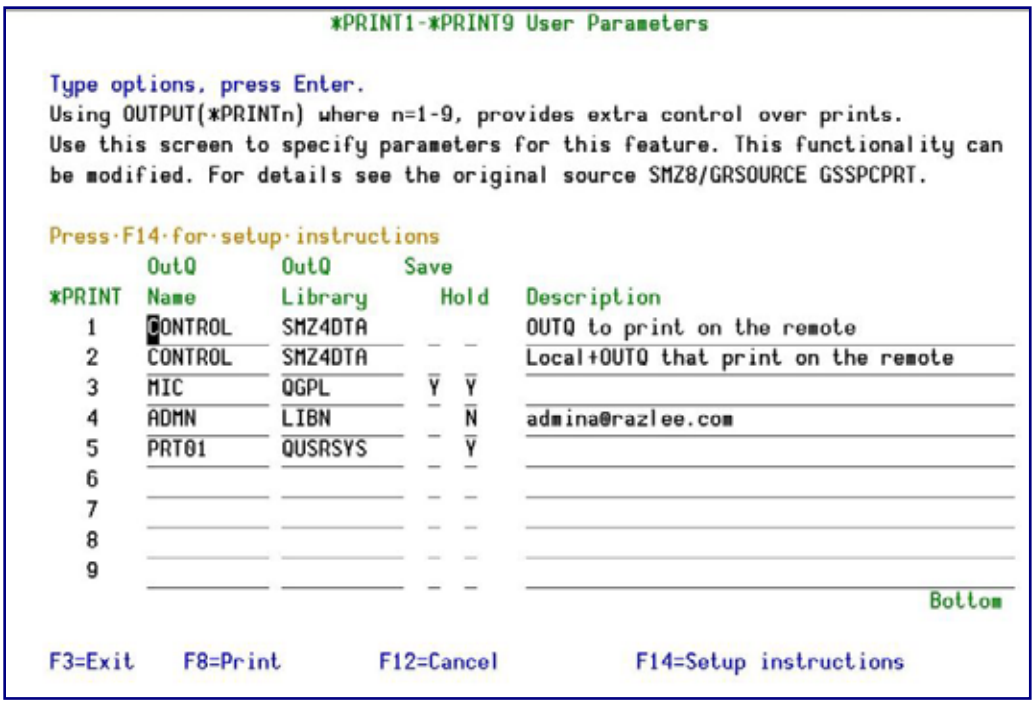
To define remote printers:

1. Select **58. *PRINT1 - *PRINT9, PDF Setup** from the **BASE Support** menu. The **Printer Files Setup** screen appears.



Printer Files Setup

2. Enter **1** and press **Enter**. The ***PRINT1 - *PRINT9 Setup** screen appears.



PRINT1-*PRINT9 User Parameters

3. Enter the name of the local output queue and library as shown in the above example. You can optionally enter a description.

Parameter	Description
User Parameter	Name of the local output queue and its library
Description	Optional text description

4. Enter the following command on any command line to direct output to the remote printer. This assumes that the designated output queue has already been defined.

```
CHGOUTQ       OUTQ('local       outq/library')       RMTSYS(*INTNETADR)
+         RMTPRTQ('outq   on   remote')   AUTOSTRWTR(1)   CNNTYPE(*IP)
TRANSFORM(*NO)
+   INTNETADR('IP of remote')
```

Parameter	Description
QUTQ()	Name of the local output queue
RMTPRTQ()	Name of the remote print queue
INTNETADR()	IP address of the remote system

If the desired output queue has not yet been defined, use the CRTOUTQ command to create it. The command parameters remain the same.

For example, ***PRINT1** in the above screen, the following command would send output to the output queue '**MYOUTQ**' on a remote system with the IP address '**1.1.1.100'** as follows:

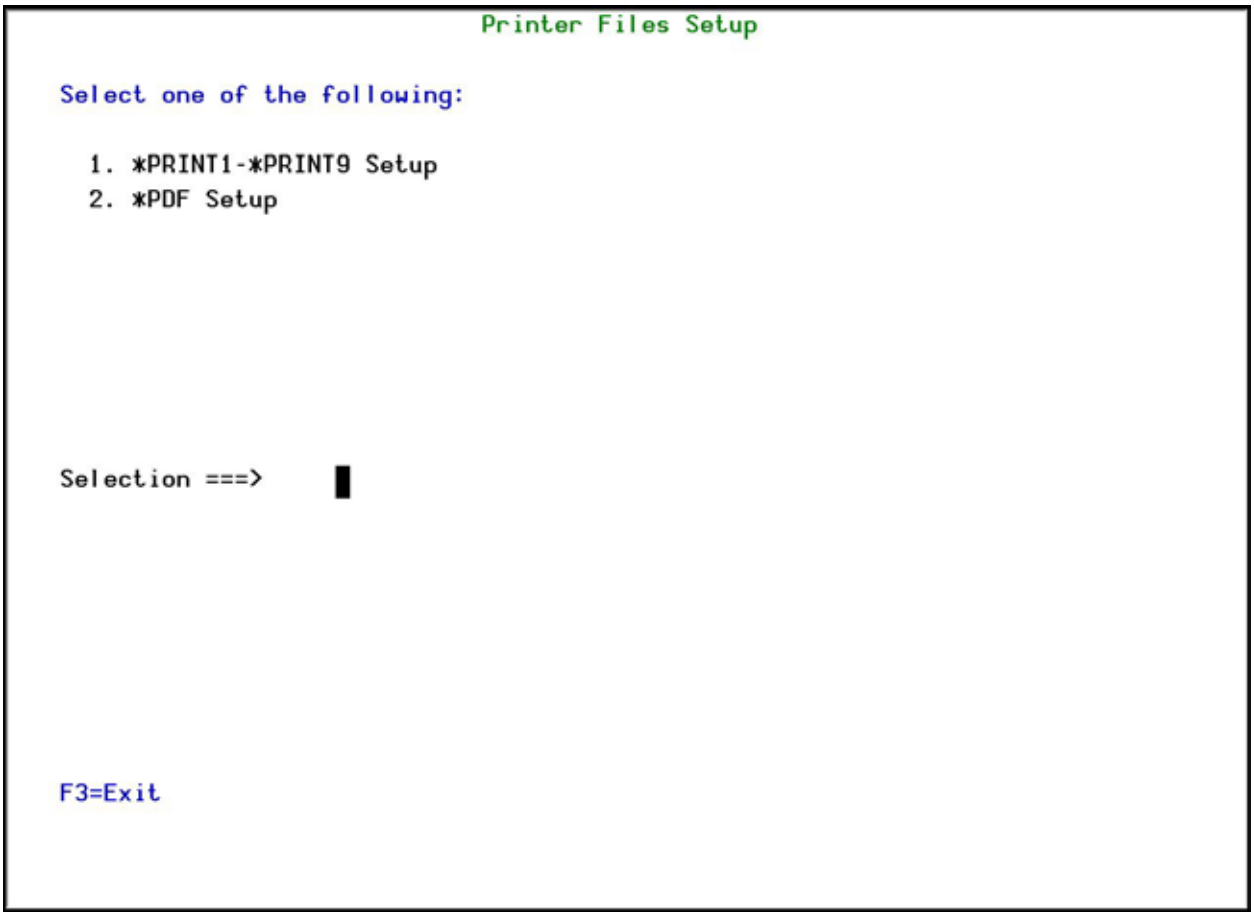
```
CHGOUTQ            OUTQ(CONTROL/SMZTMPA)            RMTSYS(*INTNETADR)
+       RMTPRTQ(MYOUTQ)   AUTOSTRWTR(1)   CNNTYPE(*IP)   TRANSFORM(*NO)
+   INTNETADR(1.1.1.100)
```

*PDF Setup

The operating system, from release 6.1, directly produces *PDF prints. In the absence of such support a standard *PDF is printed by other means.

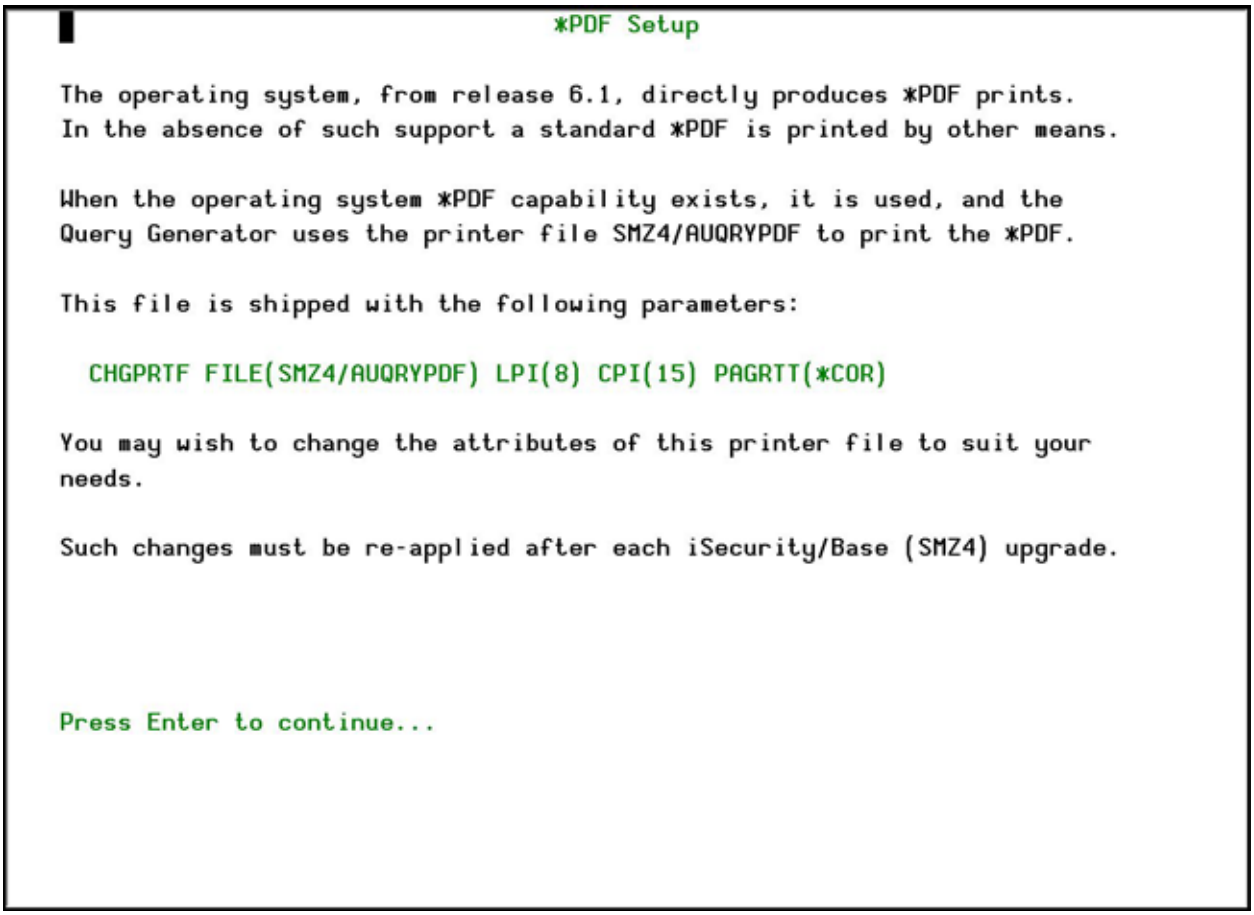
To define PDF printers:

1. Select **58. *PRINT1 - *PRINT9, PDF Setup** from the **BASE Support** menu. The **Printer Files Setup** screen appears.



Printer Files Setup

2. Enter **2** and press **Enter**. The ***PDF Setup** screen appears.



***PDF Setup**

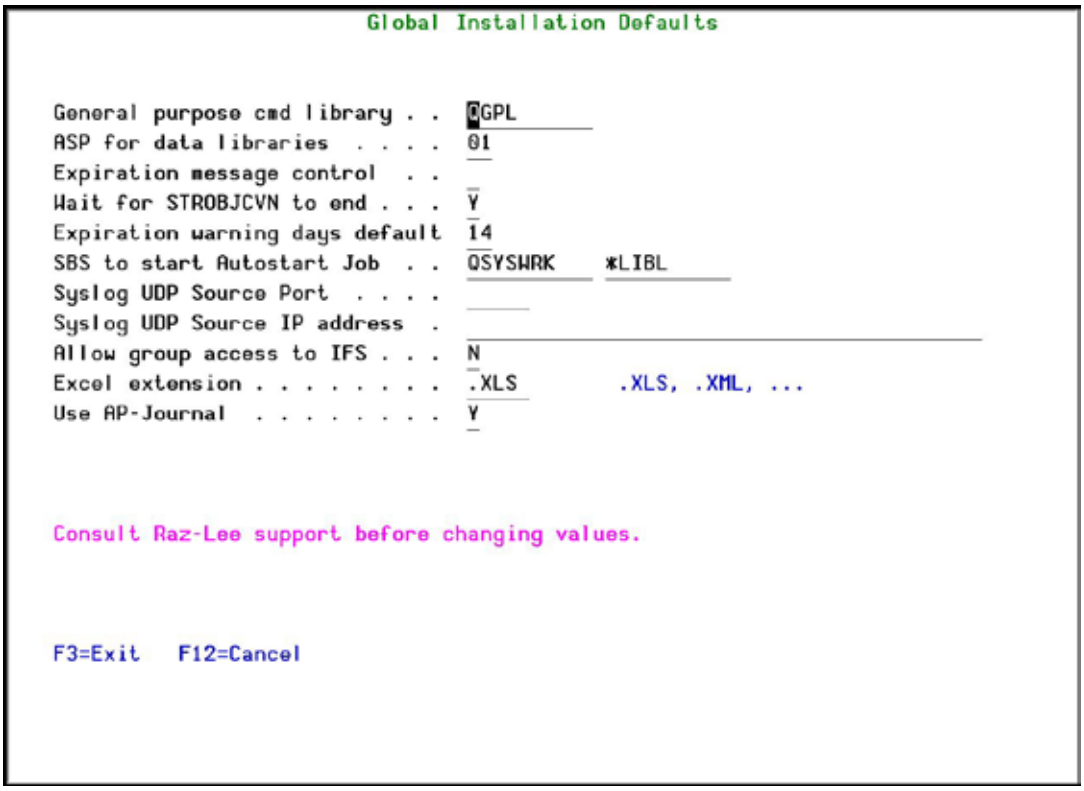
3. Follow the instruction on the screen.

NOTE: You must re-perform this task after every upgrade of **Password Reset**.

Global Installation Defaults

You can set the parameters that iSecurity uses to control the Installation and upgrade processes.

1. Select **59. Global Installation Defaults** from the **BASE Support** menu. The **Global Installation Defaults** screen appears.



Global Installation Defaults

Parameter	Description
General purpose cmd library	An alternative library to QGPL from which all **STR***, **RUN***, and ***INIT** commands will be run.
ASP for data libraries	Products being installed for the first time will be installed to this ASP. This refers to the product library and data library (for example, SMZ4, SMZ4DTA) In some products such as APJournal, other libraries are created. For example, in the AP-Journal a library is created per application. When created you are prompted with the CRTLIB (Create Library) so that you can set the ASP number. Change the current ASP of the library. All future upgrades will use this ASP. •All products will try to preserve the current ASP at upgrade time. Due to its sensitivity, you should check it.
Expiration message control	**Y**=Yes **N**=No
Wait for STROBJCVN to end	**Y**=Yes **N**=No When installing the product on an OS400 version which is not the one that it was created for, objects require conversion and this is normally done in a batch job sent to work parallel to the installation. If you want the conversion to run inline, (wait until it ends), this field should be set to Y.

Parameter	Description
Expiration warning days default	All products whose authorization expires in less than this number of days are reported as an exception. Enter a number between 01 and 99. The default is **14** days.
SBS to start Autostart Job	The Subsystem name and library to use for the Autostart Job.
Syslog UDP Source Port	The source port for Syslog UDP.
Syslog UDP Source IP Address	The source IP address for Syslog UDP
Allow group access to IFS	**Y**=Yes **N**=No Allow access to IFS from group profiles.
Excel extension	The extension to be used when creating Excel files: **.XLS** **.XML**
Use AP-Journal	**Y**=Yes **N**=No If you want to use the self-journaling option that will allow you to trace all changes made to iSecurity products, enter **Y**.

2. Enter your required parameters and press **Enter**.

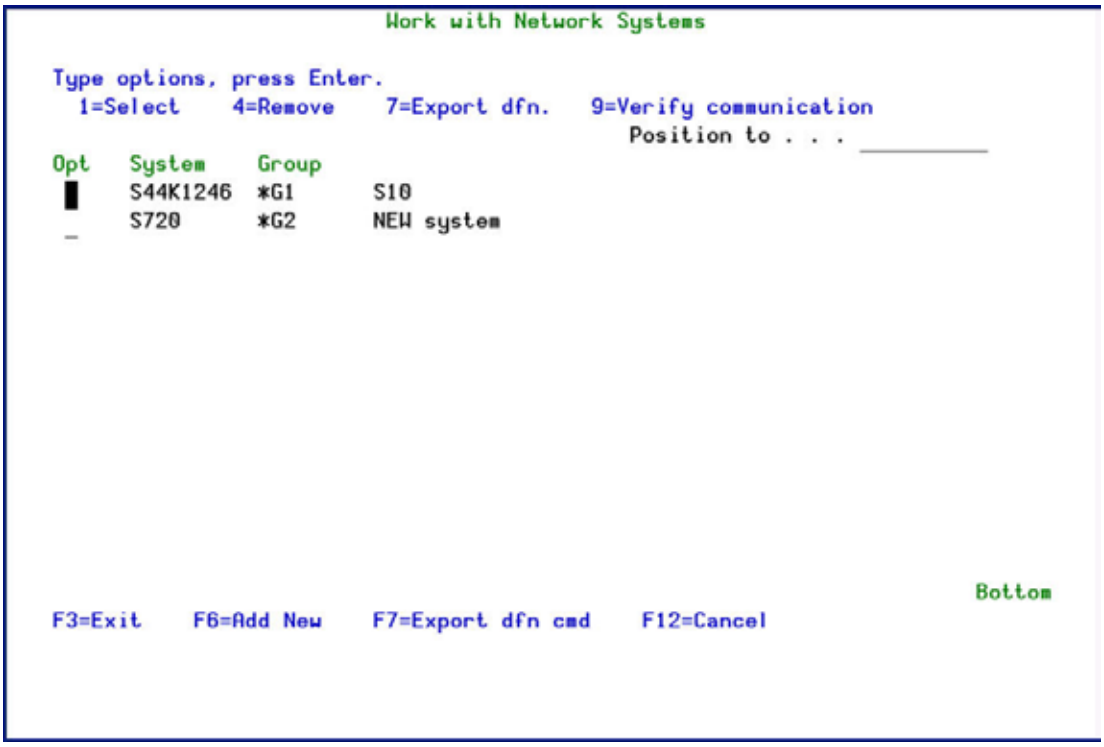
NOTE: You should not change any of the values in this screen without first consulting with Raz-Lee support staff at support@razlee.com.

Network Support

Work with network definitions

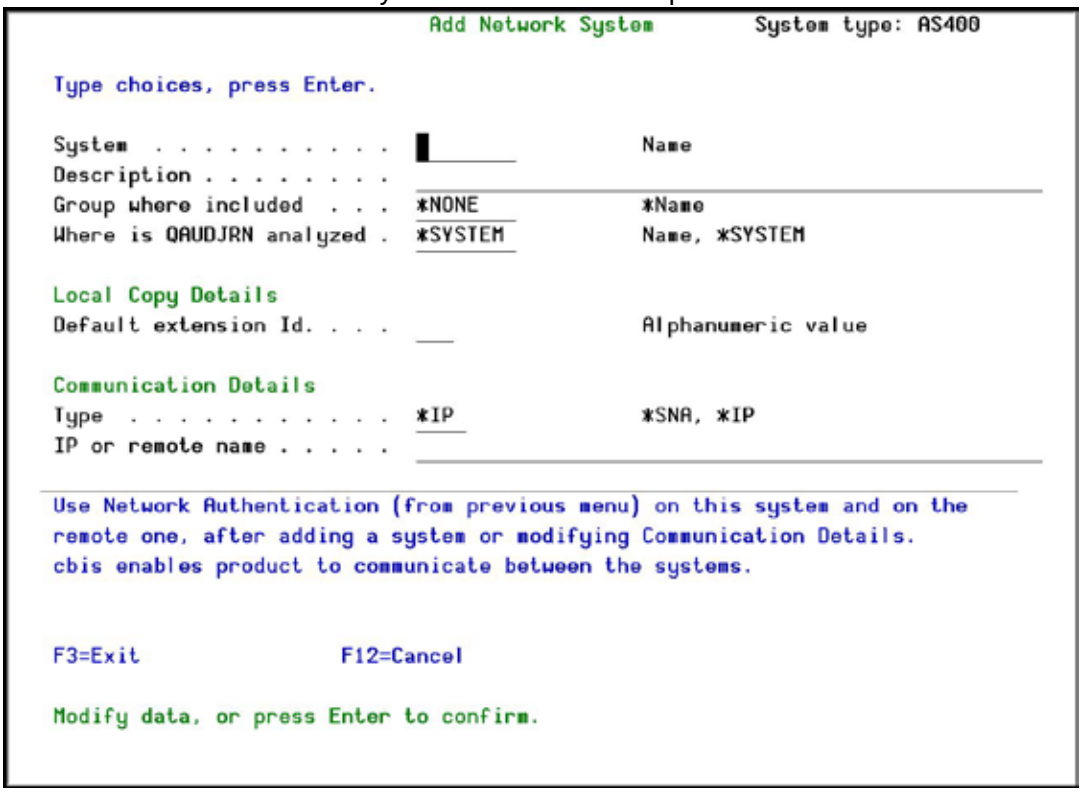
To get current information from existing report or query. Adjusting the system parameters only, to collect information from all the groups in the system to output files that can be sent via email.

1. Select **71. Work with network definitions** from the **BASE Support** menu. The **Work with Network Systems** screen appears.



Work with Network Systems

2. Press **F6** to define a new network system to work with and press **Enter** to confirm.



Add Network System

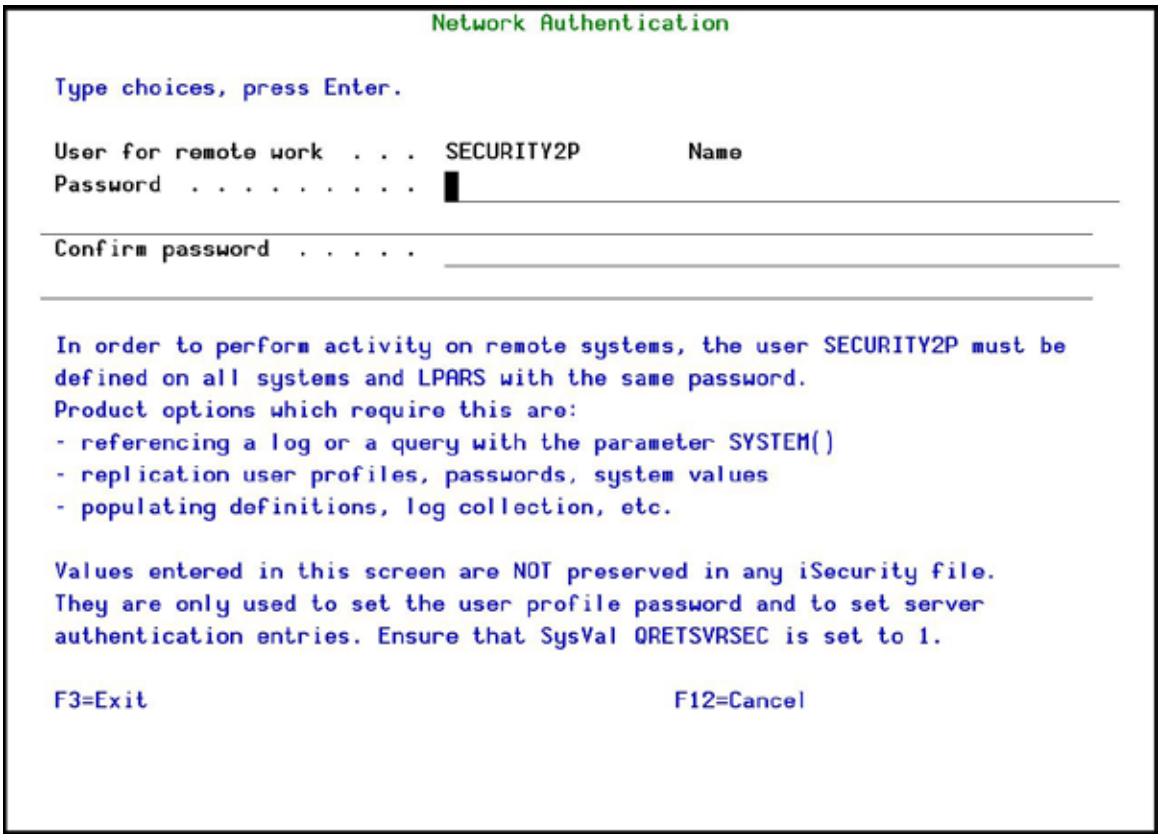
Parameter	Description
System	The name of the system
Description	A meaningful description of the system
Group where included	Enter the name of the group to which the system is assigned
Where is QAUDJRN analyzed	Give the name of the System where QAUDJRN is analyzed. Enter *SYSTEM if it is analyzed locally.
Default extension Id	Enter the extension ID for local copy details
Type	The type of communication this system uses ***SNA** ***IP**
IP or Remote Name	Enter the IP address or SNA Name, depending on the **Type** of communication you defined.

3. Enter your required definitions and press **Enter** to confirm.

Network Authentication

To perform activity on remote systems, you must define the user SECURITY2P with the same password on all systems and LPARS with the same password.

1. Select **72. Network Authentication** from the **BASE Support** menu. The **Network Authentication** screen appears.



Work with Network Systems

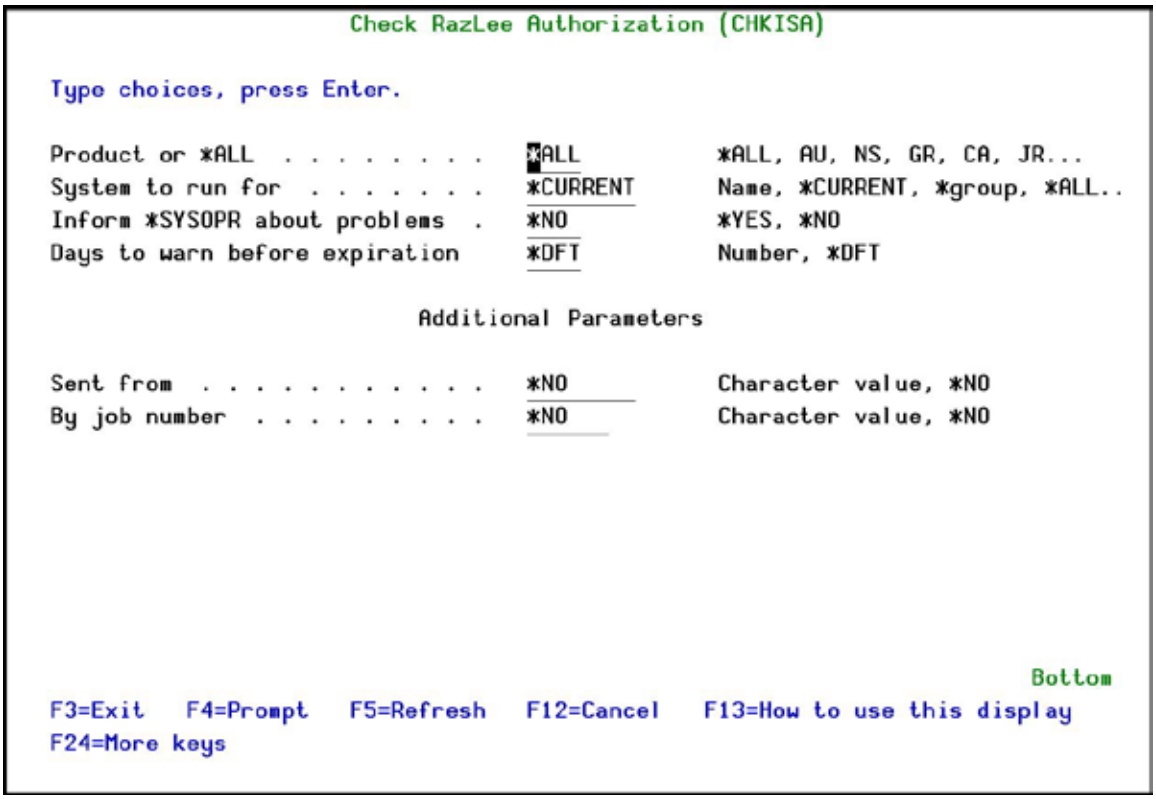
2. Enter the SECURITY2P user password twice and press **Enter**.

Check Authorization Status

You can set up the system so that the local *SYSOPR will get messages for all network wide authority problems.

Before you run this command, you must allow the system to run network commands and scripts. See Run CL Scripts for more details.

1. Select **73. Check Network Authority Status** from the **BASE Support** menu. The **Check Razlee Authorization** screen appears.



Check Razlee Authorization

Parameters or Options	Description
Product or *ALL	***ALL** = report on all products **AU** = Audit **NS** = Native Object Security **GR** = Firewall **CA** = Capture **JR** = AP-Journal **OD** = Authority On Demand **AV** = Anti-Virus **CT** = Change Tracker **DB** = DB-Gate **VW** = View

Parameters or Options	Description
System to run for	The system to run the authorization check for: **Name** = The name of a specific system in the network ***CURRENT** = The current system ***group** = The name of a group of systems ***ALL** = All systems in the network
Inform *SYSOPR about problem	***YES** = ***NO** =
Days to warn before expiration	Number = Any system whose expiry date is less than this number of days will be reported. The default number of days is 14. ***DFT**
Sent from	Value ***NO**
By job number	Value ***NO**

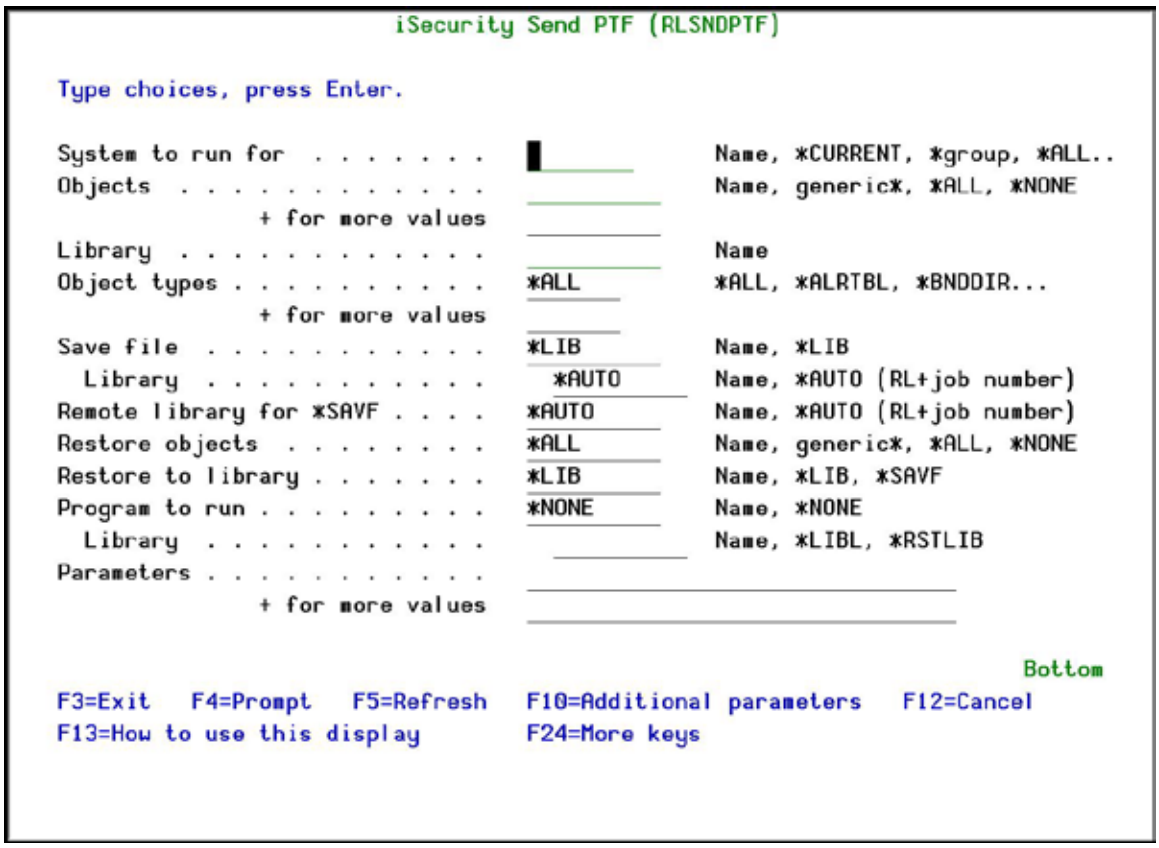
2. Select the correct options and press **Enter**.

Send PTF

This option allows you to run of a set of commands that will send objects as a PTF. This option is restricted to iSecurity products only. If you need to send PTFs for other products, please contact RazLee Support.

Before you can use this option, ensure that you define the entire network, as described in Work with network definitions, and that you define user SECURITY2P on all nodes, using the same password, as described in Network Authentication.

1. Select **74. Send PTF** from the **BASE Support** menu. The **iSecurity Send PTF (RLSNDPTF)** screen appears.



iSecurity Send PTF

Parameter	Description
System to run for	**Name** = The specific name of the system ***CURRENT** = The current system ***group** = All systems in the group ***ALL** = All systems on the network
Objects	The objects you want to send. You can enter multiple values **Name** = A specific object **generic*** = A group of objects with the same prefix ***ALL**= All the objects ***NONE**= No objects need to be extracted, the SAVF has already been prepared
Library	The name of the library that contains the objects
Object types	The object types to be sent
Save file / Library	The name and library of the SAVF to contain the objects. If you enter ***LIB** for the file name, the name of the library containing the objects will be used. If you enter ***AUTO** as a name for the library, a library will be created with the name of RL<jobnumber>
Remote library for SAVF	The name of the remote library to receive the SAVF to contain the objects. If you enter ***AUTO** as a name for the library, a library will be created with the name of RL<*jobnumber*>

Parameter	Description
Restore objects	The objects to be restored **Name** = A specific object **generic*** = A group of objects with the same prefix ***ALL**= Restore all objects ***NONE**= Do not restore any objects
Restore to library	The name of the library to receive the restored objects **Name** = A specific library ***LIB** = the name of the original library containing the objects will be used. ***SAVF**= the same name as the SAVF
Program to run / Library	The name and library of a program to run after the objects have been restored.
Parameters	The parameters for the program that runs after the restore.

2. Select the correct options and press **Enter**.

Run CL Scripts

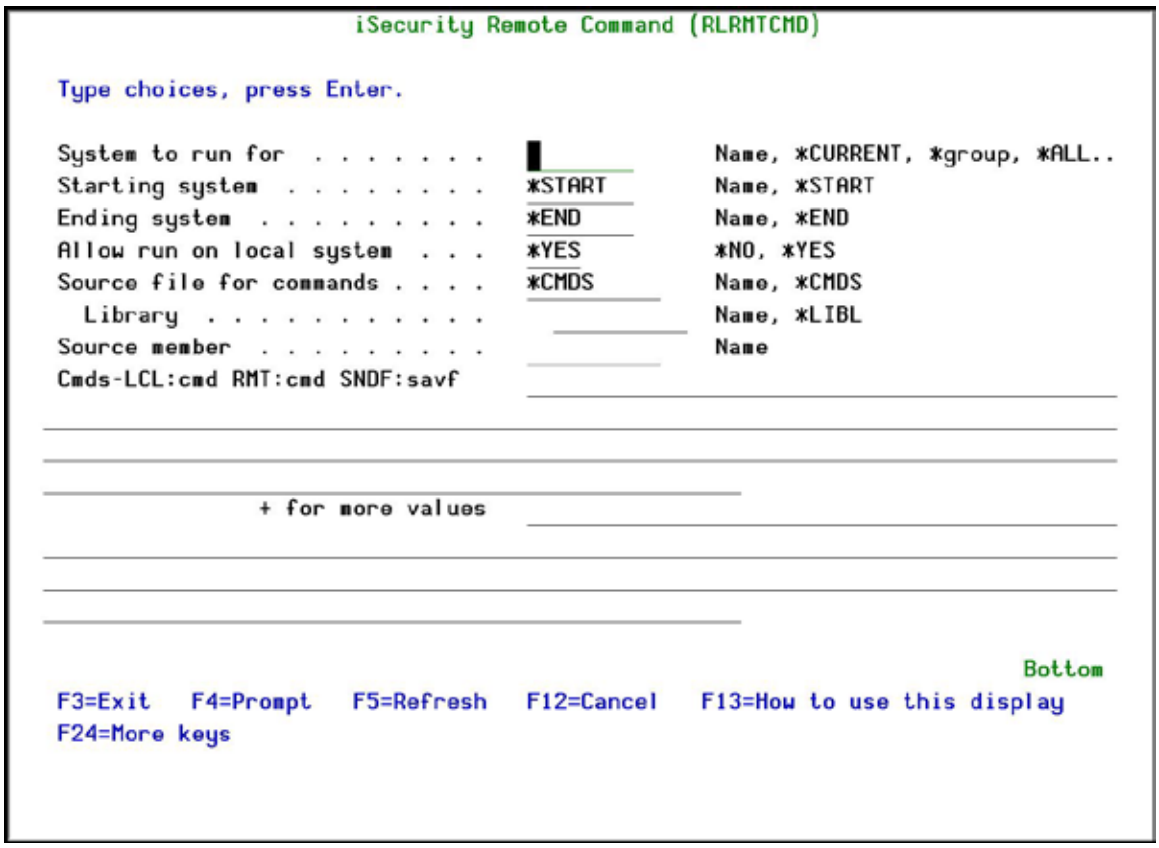
This option allows you to run of a set of commands either from a file or by entering specific commands as parameters. Each command must be preceded by a label:

- LCL: Run the following command on the local system
- RMT: Run the following command on the remote system
- SNDF: Send the save file (format: library/file) to RLxxxxxxxx/file (xxxxxxxx is the local system name)

You can use this option to define the commands to run to check system authorities, as described in Check Authorization Status.

Before you can use this option, ensure that you define the entire network, as described in Work with network definitions, and that you define user SECURITY2P on all nodes, using the same password, as described in Network Authentication.

1. Select **75. Run CL Scripts** from the **BASE Support** menu. The **iSecurity Remote Command (RLRMTCMD)** screen appears.



iSecurity Remote Command

Parameter	Description
System to run for	**Name** = The specific name of the system ***CURRENT** = The current system ***group** = All systems in the group ***ALL** = All systems on the network
Starting system	Use to define a the start of a subset within ***group** or ***ALL** This is useful if you want to rerun a command that previously failed
Ending system	Use to define a the end of a subset within ***group** or ***ALL** This is useful if you want to rerun a command that previously failed
Allow run on local system	***YES** = The remote command can run on the local system ***NO** = The remote command cannot run on the local system
Source file for commands	**Name** = The file where the commands to run are stored. ***CMDS** = Use the commands entered below
Library	**Name** = The library that contains the commands source file ***LIBL** =
Source member	**Name** = The member that contains the commands

Parameter	Description
Cmds –LCL:cmd RMT:cmd SNDF:savf	The commands that can be run (if the Source file for commands parameter is ***CMDS**): **LCL:cmd** = A command that will be run on the local computer **RMT:cmd** = A command that will be run on a remote computer **SNDF:savf** =

2. Select the correct options and press **Enter**.

Current Job Central Administration Messages

Select **76. Current Job CntAdm Messages** from the **BASE Support** menu to display the current job log.

All Jobs Central Administration Messages

Select **77. All Jobs CntAdm Messages** from the **BASE Support** menu to display the job log for all jobs.

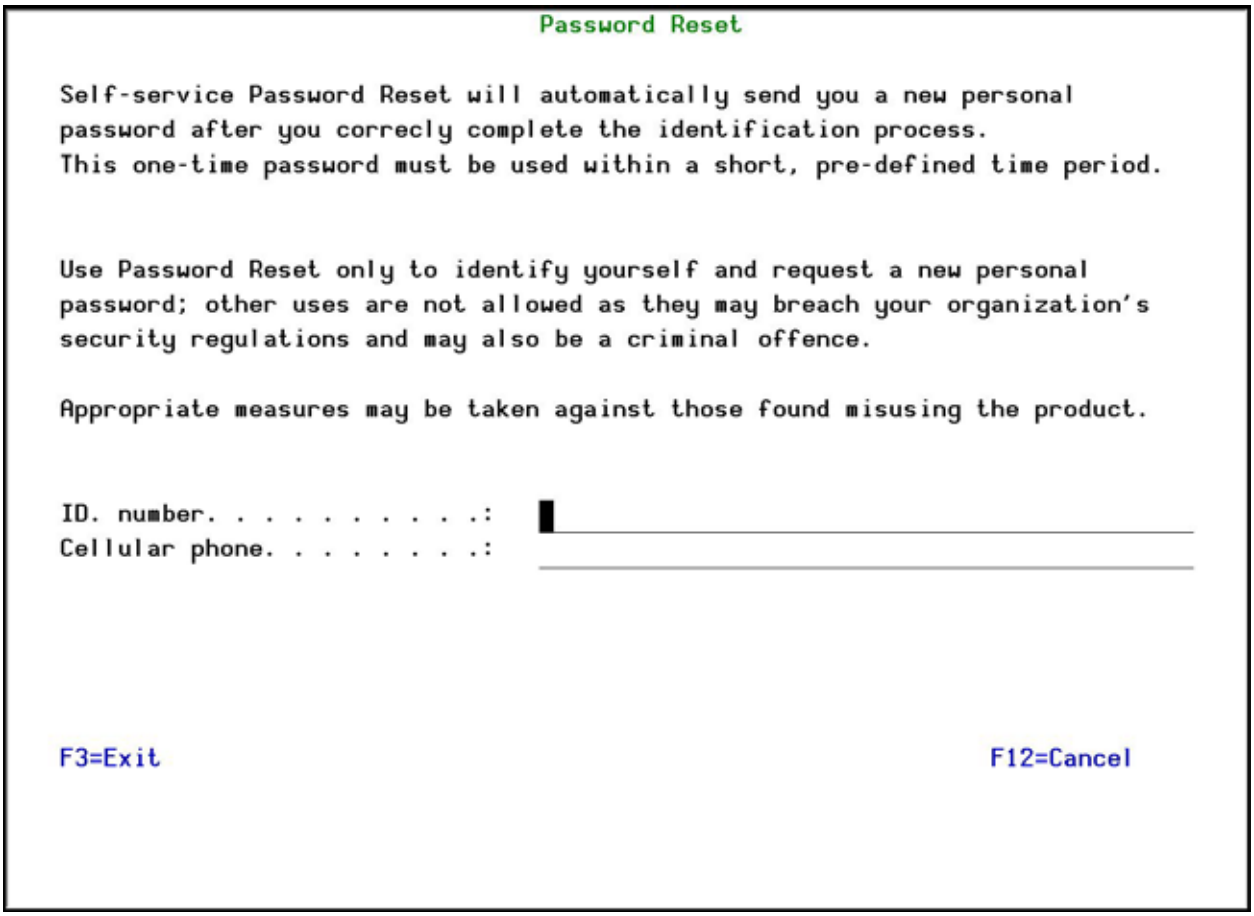
Resetting Your Password

The procedures shown below are generic procedures which describe the general method of resetting a password both from the System i Sign On screen and from a web browser. Your organization's procedures may differ from the procedures shown below, but the general principles and the initial screen are the same. The procedure is governed by the Password Reset Class of the person who is performing the Password Reset (see Add P-R Classes for more details).

Resetting From the Sign On Screen

To reset your password in the System i:

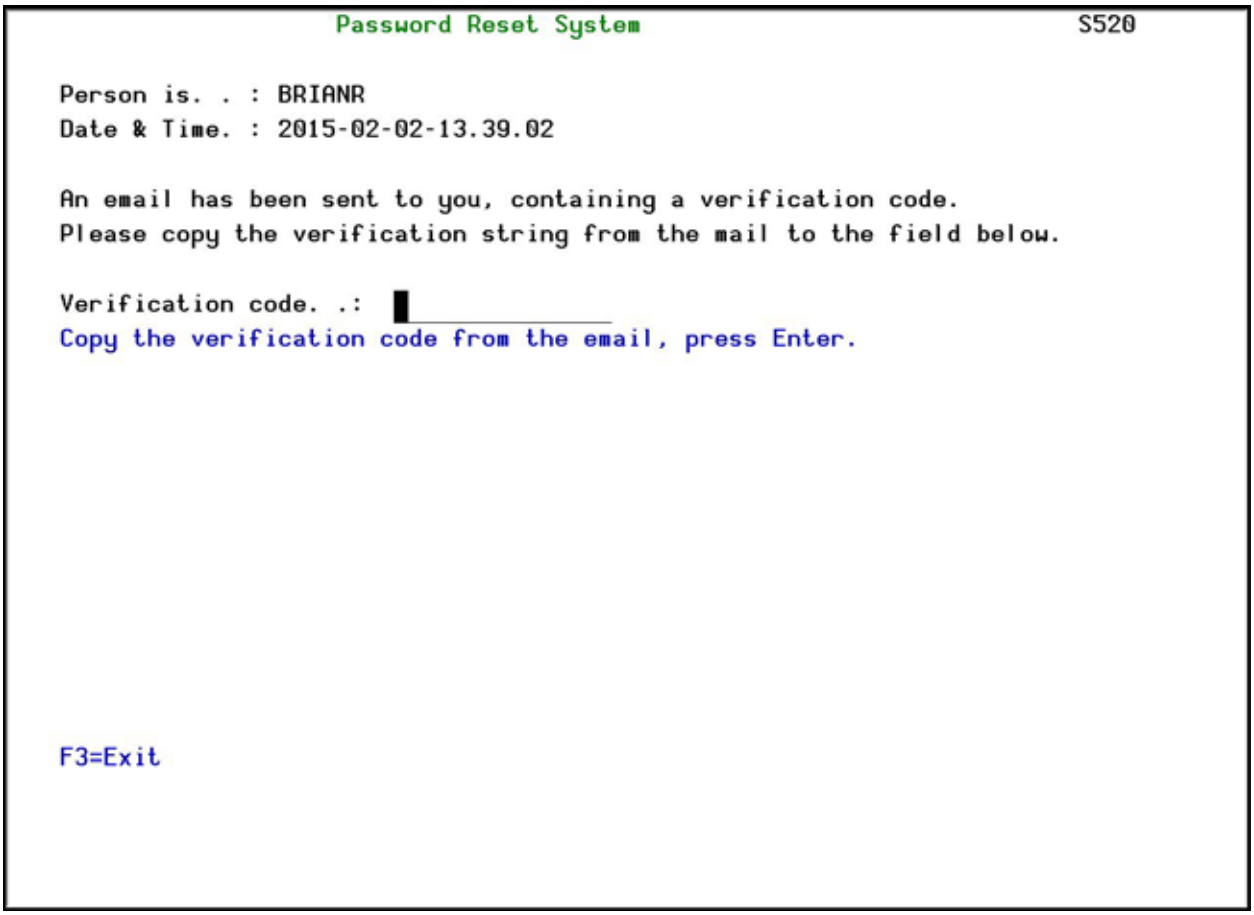
1. In the sign on screen, sign on with User FORGOT and Password PASSWORD. The **Password Reset** screen appears.



Password Reset

2. Enter the requested identification information and press **Enter**. The **Password Reset System** screen appears.

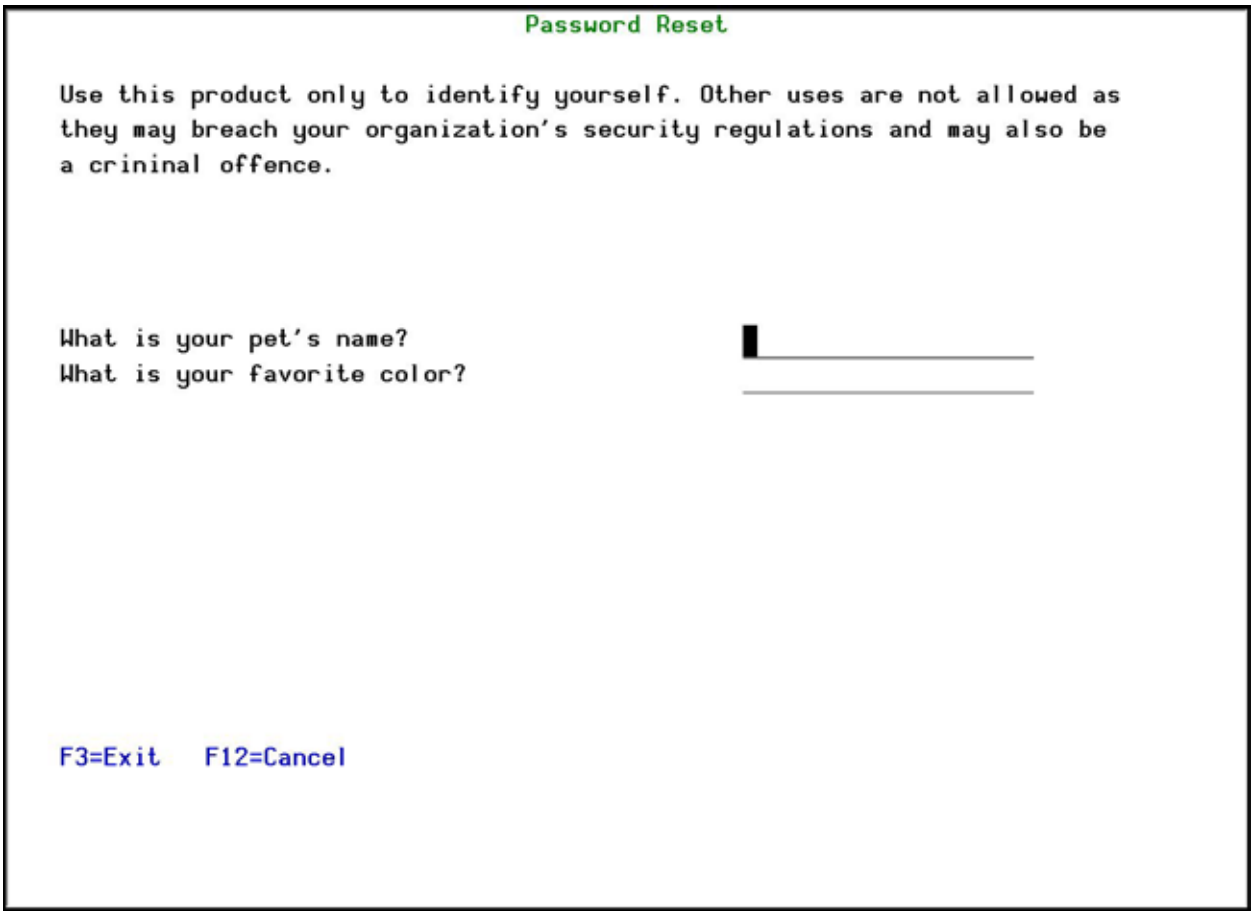
Note: Remember that the responses are case-sensitive.



Password Reset System

3. Enter the **Verification Code** and press **Enter**. The **Personal Questions** screen appears.

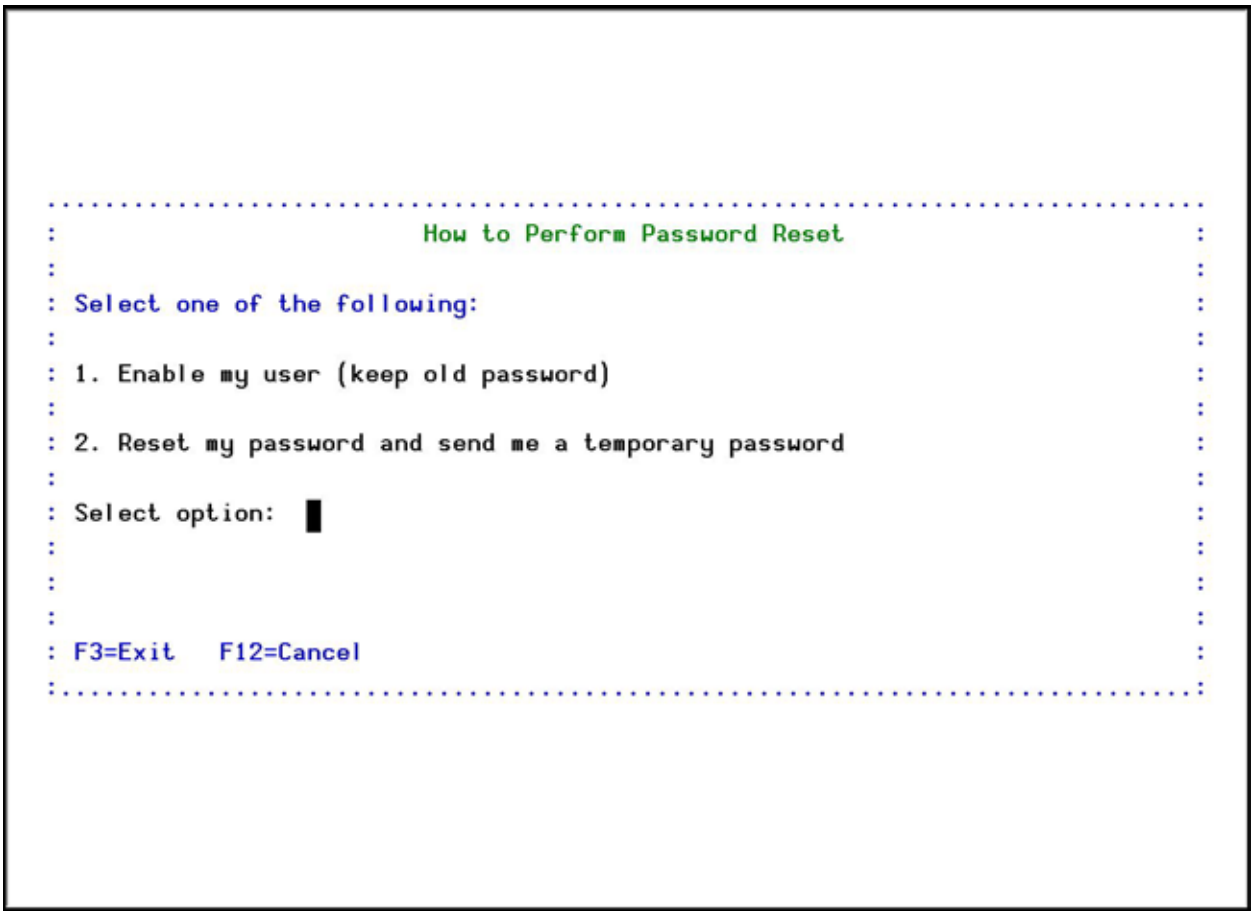
Note: If you do not find the email in your Inbox folder, check in the Junk/Spam/Other folders.



Personal Questions

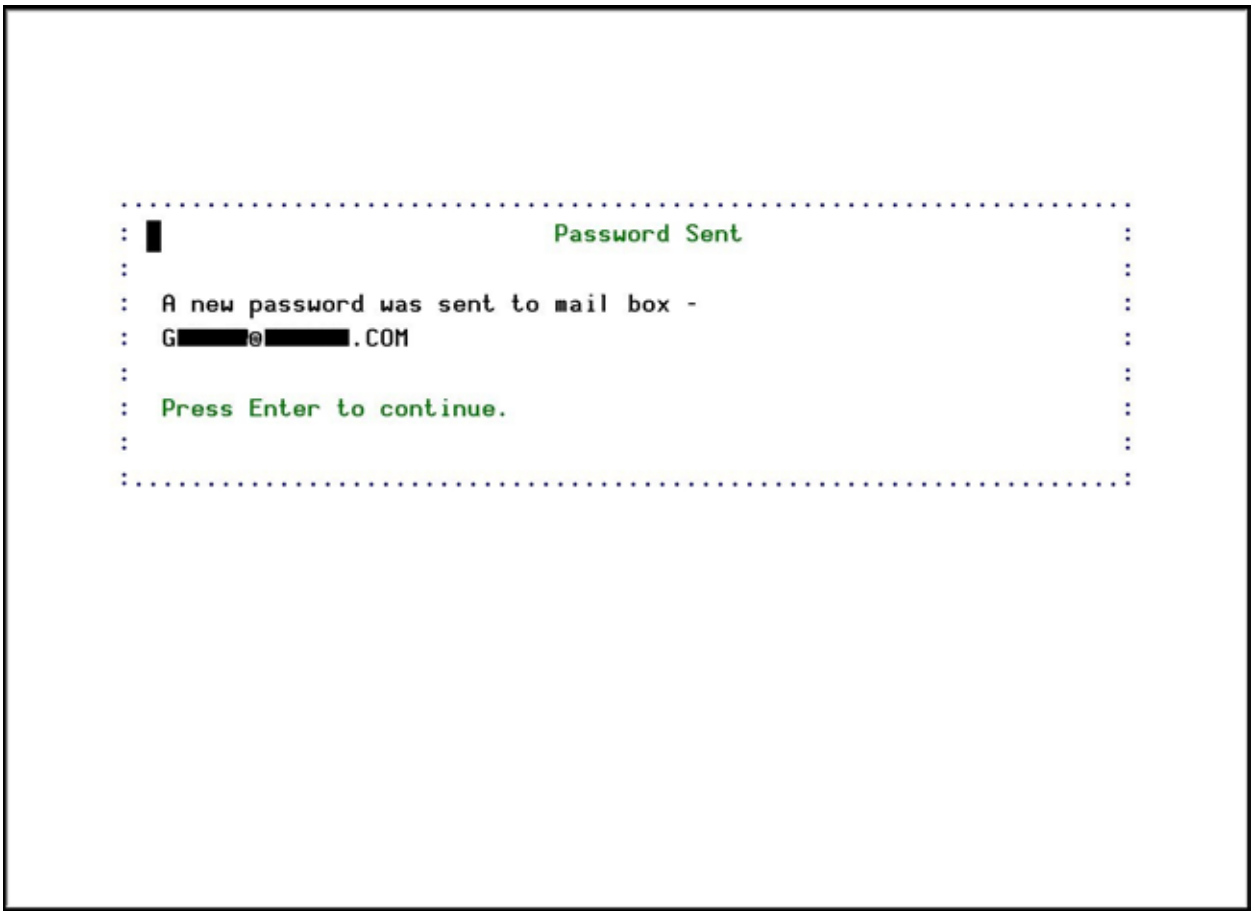
4. Enter your answers and press **Enter**. The **How to Perform Password Reset** screen appears.

Note: Remember that the responses are case-sensitive.



How to Perform Password Reset

5. Select **2** to reset your password. The **Password Sent** screen appears.



Password Sent

6. Press **Enter**. You must now sign on within the time limit set by your System Administrator.

The password you receive is defined as expired. The first time you sign on with it, you will be prompted to change it.

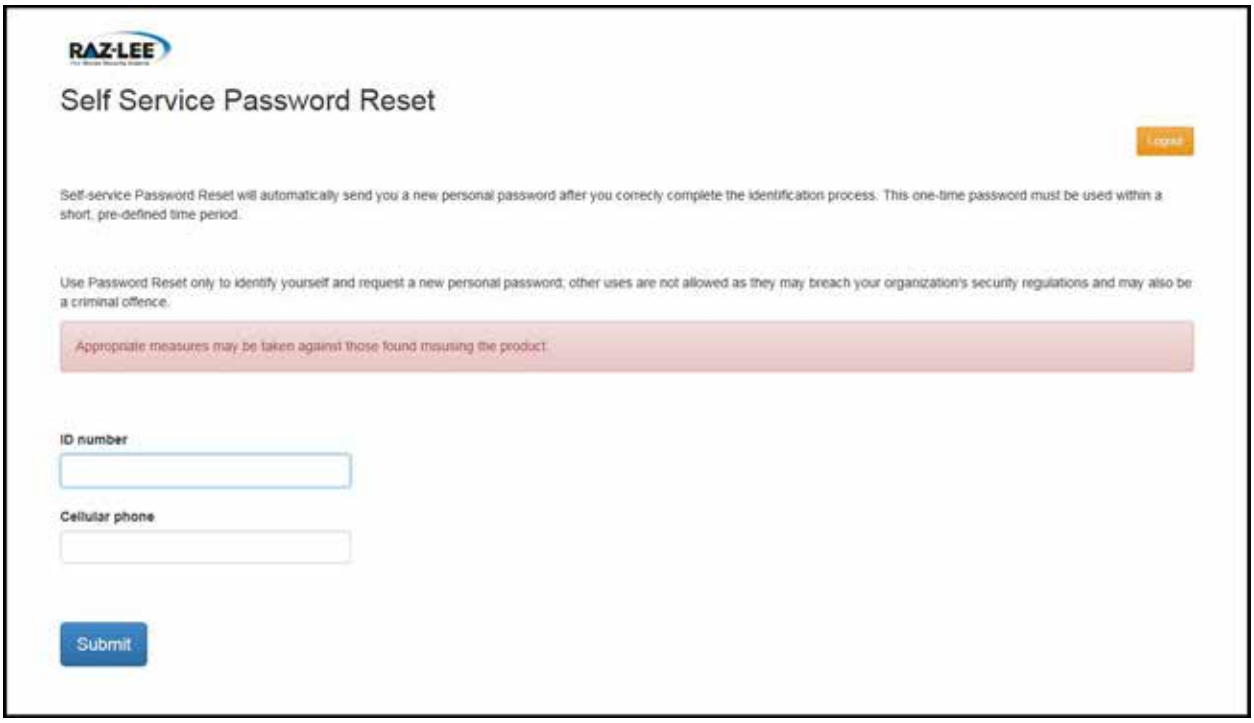
Note: If you do not find the email in your Inbox folder, check in the Junk/Spam/Other folders.

Resetting From a Web Browser

If your organization has installed a special program, you can reset your password in a web browser, even when you do not have access to the System i.

To reset your password in a web browser:

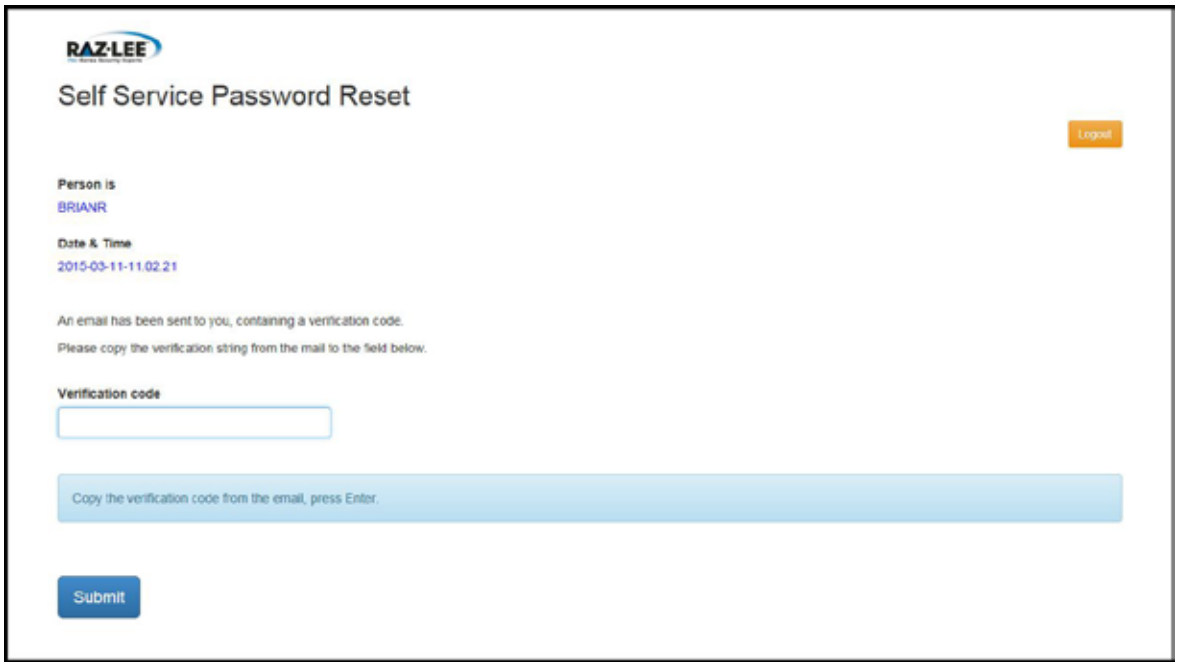
1. In a web browser, enter the URL you received from your System Administrator. The **Self Service Password Reset** page appears.



Password Reset System

2. Enter the requested identification information and press **Enter**. The **Verification Code** screen appears.

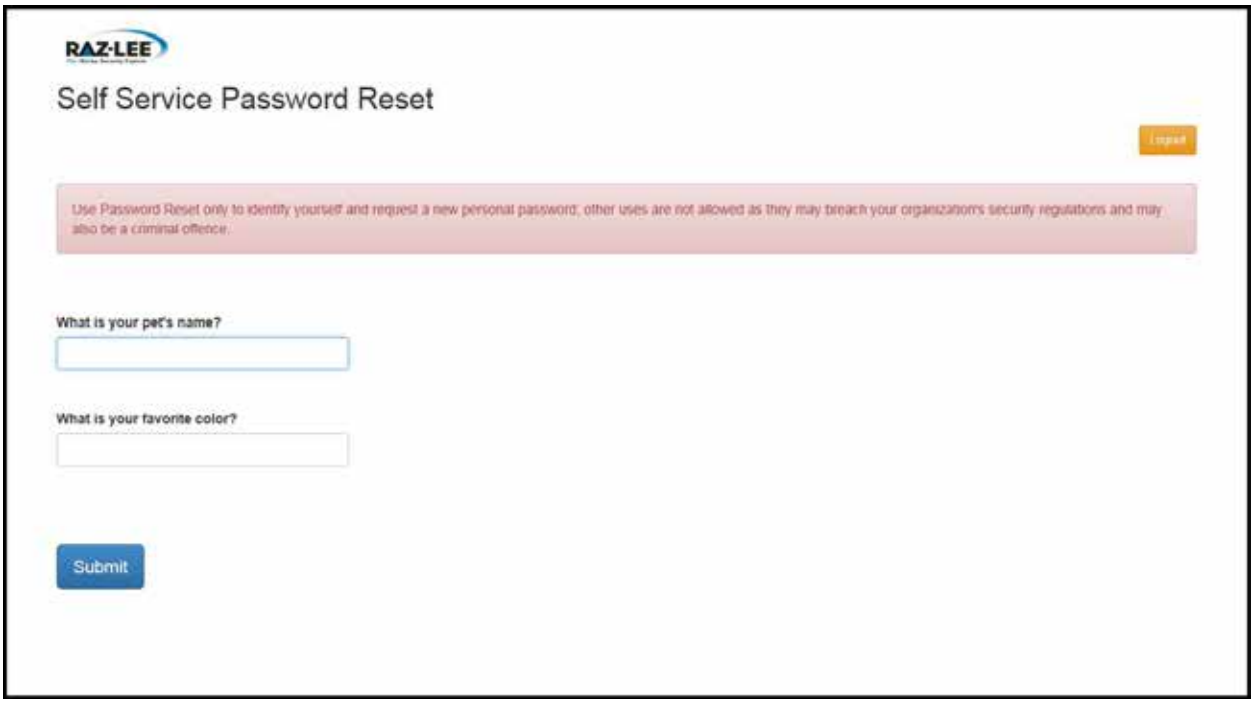
Note: Remember that the responses are case-sensitive.



Verification

3. Enter the **Verification Code** and press **Enter**. The **Personal Questions** screen appears.

Note: If you do not find the email in your Inbox folder, check in the Junk/Spam/Other folders.



Personal Questions

4. Enter your answers and press **Enter**. The **How to Perform Password Reset** screen appears.

Note: Remember that the responses are case-sensitive.

Personal Questions

5. Select **2** to reset your password. The **Password Sent** screen appears.

Password Sent

6. Press **Enter**. You must now sign on within the time limit set by your System Administrator.

The password you receive is defined as expired. The first time you sign on with it, you will be prompted to change it.

Note: If you do not find the email in your Inbox folder, check in the Junk/Spam/Other folders.

Comments

We hope you found this user manual informative; your comments are important to us!

Raz-Lee Security wants its user manuals to be as helpful as possible; please send your comments about this user manual to docs@razlee.com.