iSecurity Password Reset

User Guide
Version 7.05

www.razlee.com

Contents

Contents 2
About this Manual 4
Password Reset Overview 9
Setting Up Password Reset 13
Accessing Password Reset 15
Working with the ZAUTH Subsystem 18
Starting the ZAUTH Subsystem 20
Checking whether the ZAUTH Subsystem is Active 21
Stopping the ZAUTH Subsystem 22
System Configuration 23
Enabling Password Reset 24
Enabling and Controlling Self-Enrollment 26
Setting Initial Process Questions 28
Setting Initial Process Defaults 30
Creating the Special Users for Password Reset 32
Working with Password Reset 33
Working with Classes 34
Modifying Classes 36
Defining Persons 41
Adding a New Person 45
Modifying a Person 48
Setting Up Users for a Person 51
Assigning Users to Persons 54
Managing Private Questions for a Person 55
Sending Keys for a Person 57
Standard Questions 59
Languages 61
Working with Different Languages for Standard Questions 62

Working with Screen Text 64
Adding Screen Text Languages 66
Deleting Screen Text Languages 67
Copying Screen Texts Between Languages 68
Copying One Screen's Texts 69
Working with Email and SMS Text 70
Modifying Email and SMS Text 73
Copying Email and SMS Text 75
Displaying Error ID Descriptions 77
Testing Password Reset 79
Resetting Your Password 83
Resetting Your Password from the Sign-On Screen 84
Resetting Your Password from a Web Browser 87
The Password Reset Web Interface 91
Web interface installation and implementation 92
Password Reset Web Customization 93
Web interface capabilities and best practices 95
Check status of user definition API - SMZO/PRIFEXSTR 96
Configuring the Application Server on IBM i 97

About this Manual

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

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

This user guide, together with the iSecurity Installation Guide, is the only printed documentation necessary for understanding this product. It is available in HTML form as well as in user-friendly PDF format, which may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: http://www.adobe.com/. You can also read and print pages from the manual using any modern web browser.

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

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the- box" security. To learn more about the iSecurity Suite, visit our website at http://www.razlee.com/.

Intended Audience

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

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

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

Native IBM i (OS/400) User Interface

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

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

Conventions Used in the Document

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

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

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

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

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

STRPWDRST **> 81 > 32**

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

Menus

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

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

Data Entry Screens

Data entry screens include many convenient features such as:

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

The following describes the different data entry screens.

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

The following function keys may appear on data entry screens.

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

Legal Notice

This document is provided by Raz-Lee Security for information purposes only and is not a legal binding document.

While Raz-Lee is doing its best to coordinate between this document and Raz-Lee's products, changes might occur. In case a change has been encountered, please inform Raz-Lee. Raz-Lee keeps its right to modify the software or the document as per its sole discretion Usage of this document, and all information (including product information) provided within, are subject to the following terms and conditions, and all

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

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

All registered or unregistered trademarks, product names, logos and other service marks mentioned within this document are the property of Raz-Lee or their respective owners. Nothing contained herein shall be construed as conferring by implication, estoppels, or otherwise any license or right, either express or implied, under any patent or trademark of Raz-Lee or any third party. No use of any trademark may be made without the prior written authorization of Raz-Lee. This document and all of its contents are protected intellectual property of Raz-Lee. Any copying, reprinting, reuse, reproduction, adaptation, distribution or translation without the prior written permission of Raz-Lee is prohibited.

Please check your End User License Agreement (EULA) for terms and Conditions.

2025 © Copyright Raz-Lee Security Inc. All rights reserved.

Manual Revised: Monday, February 10, 2025

Contacts

Raz-Lee Security Inc. www.razlee.com
Marketing: marketing@razlee.com 1-888-RAZLEE-4 (1-888-7295334)
Support: support@razlee.com 1-888-RAZLEE-2 (1-888-7295332)

Password Reset Overview

Resetting passwords is one of the biggest wastes of time for any organization. Surveys suggest that each password reset wastes up to 40 minutes and that password resets make up close to fifty percent of help desk calls.

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

Users, help desk staff, and system administrators can easily use and administer Password Reset. An enterprise can implement it within an organization with minimal overhead, while ensuring that no one other than the user knows the user's password.

Users create their own password profiles and can edit them at any time. They can reset the passwords without additional help or request assistance from the help desk. Users who have forgotten their passwords when trying to log in simply enters "FORGOT" in the User field and "PASSWORD" in the Password field. This triggers the self-authentication process that each user sets up in advance, including case-sensitive personal questions and responses.

Your organization's security policy controls the number and type of challenge questions that the user is asked and how many reset attempts are allowed. Unsuccessful attempts to reset passwords automatically alert relevant security personnel. Challenge questions discourage fraudulent reset requests. Users can set their own default reset password—known only to themselves—which adds another layer of security.

Users can reset their passwords in minutes, without the help desk, saving the company both valuable time and resources.

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).

On systems using Password Reset, users set up a group of personal questions that only they can answer.

When they run Password Reset, they are first asked a set of initial identifying questions, set by the system administrators.

If they answer the questions correctly, they are sent a code via email, SMS, or both.

When they receive the code, they enter it into Password Reset.

They are then asked the personal questions that they had established beforehand.

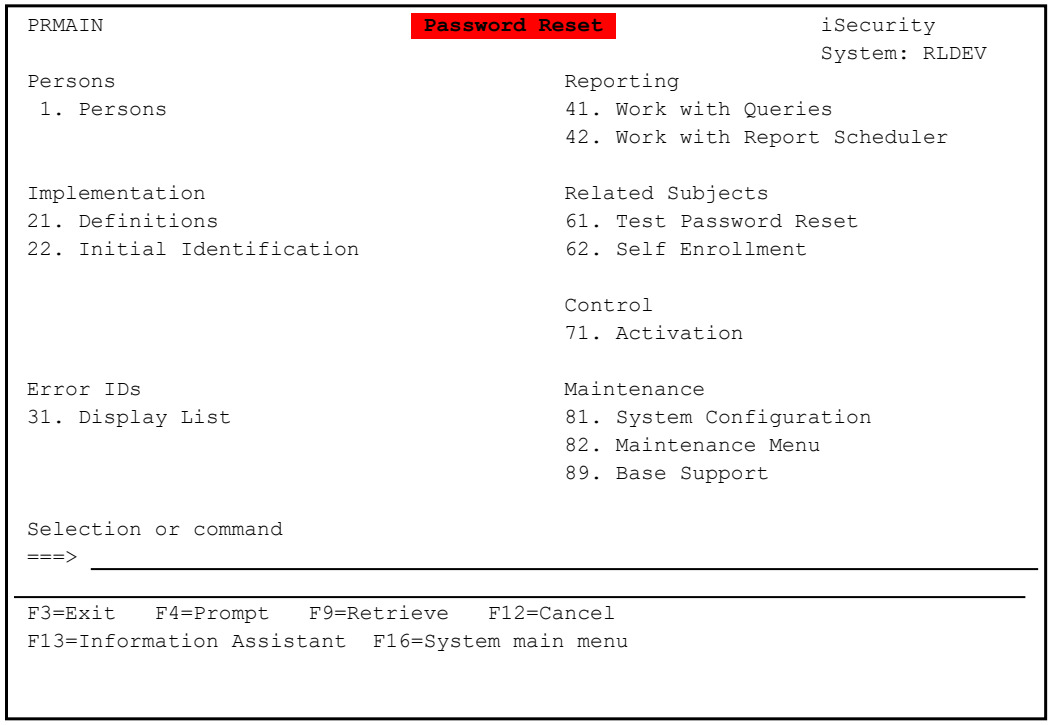
Administrators can set different levels of verification for users, based on a set of user classes defined via the **Work with P-R Classes** screen (shown in "Working with Classes" on page 34).

Setting Up Password Reset

Once you have installed Password Reset (as shown in the iSecurity Installation Manual), you can set it up for your organization via the **Password Reset** menu.

To display it, enter the command ***STRPWDRST*** on the OS/400 command line.

The **Password Reset** screen appears.



Setting up Password Reset involves the following steps:

1. Starting the ZAUTH subsystem (shown in "Working with the ZAUTH Subsystem" on page 18)
2. Enabling and controlling authentication (shown in "Enabling Password Reset" on page 24)
3. Defining classes and roles for users (shown in Classes and Roles)
4. Creating standard questions for users (shown in "Standard Questions" on page 59)
5. Creating special users (shown in "Creating the Special Users for Password Reset" on page 32)

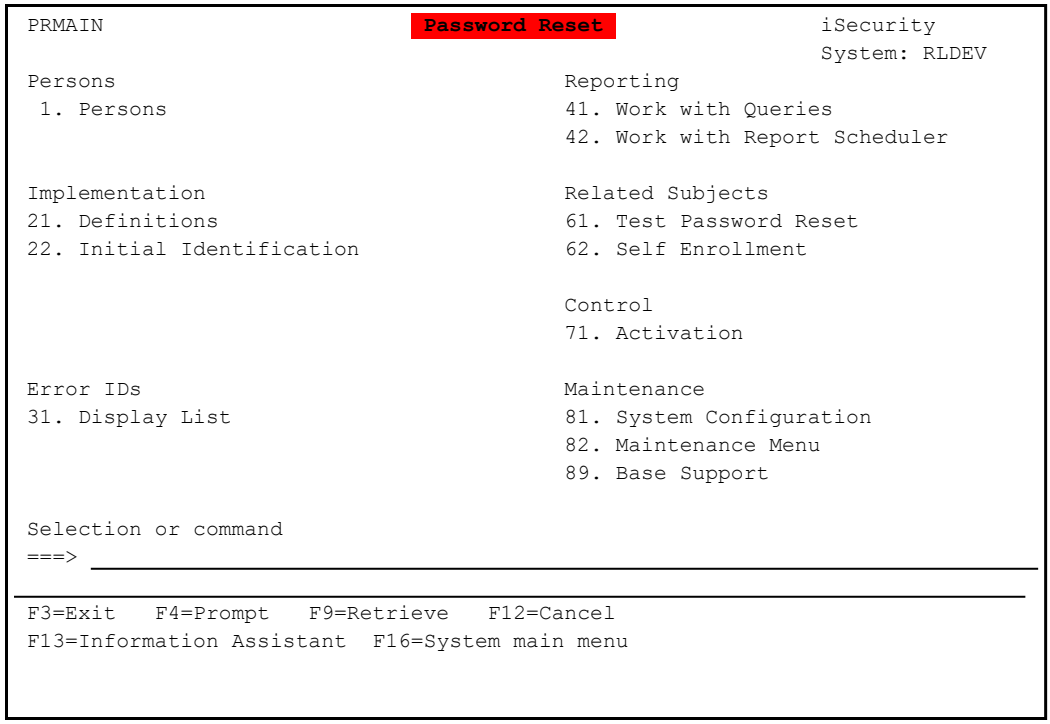
6. Creating text in needed languages for
    1. questions (shown in "Standard Questions" on page 59)
    2. onscreen text (shown in "Working with Screen Text" on page 64)
    3. email and SMS text (shown in "Working with Email and SMS Text" on page 70)
7. Creating persons (shown in Persons)
8. Managing private questions for each person (shown in "Managing Private Questions for a Person" on page 55)
9. Testing Password Reset (shown in "Testing Password Reset" on page 79)

Accessing Password Reset

The Password Reset main menu is the portal to all its functions.

To **display the menu**, type *STRPWDRST* on the command line of any screen and press the **Enter** key.

The **Password Reset Main Menu** appears.



The menu options open the following screens:

1. Persons

Opens the **Persons** menu (shown in Persons), where you define users and modify their settings.

21. Definitions

Opens the **Definitions** screen, where you can define the classes, locations, departments, and positions used in determining a user's role in your organization, as well as the texts that appear in various language on the screen and a suggested set of private questions.

22. Initial Identification

Opens the **Initial ID fields** screen (shown in "Setting Initial Process Questions" on page 28), where you can set the fields used for

initial identification.

31. Display List

Opens the Display Message Descriptions screen (shown in "Displaying Error ID Descriptions" on page 77), where you can define messages shown on the screen.

41. Work with Queries

Opens the Work with Queries screen, where you can define and run the Password Reset queries and reports. These tools are documented in the iSecurity Installation and Base Support manual.

42. Work with Report Scheduler

Opens the Work with Report Scheduler screen, where you can define, schedule, and run Password Reset report groups. These tools are documented in the iSecurity Installation and Base Support manual.

61. Test Password Reset

Opens another Password Reset screen (shown in "Testing Password Reset" on page 79), where you can verify that a given person will be able to use the Reset Password self-service functionality.

62. Self Enrollment

Opens the Self Enrollment of Personal Information screen (shown in Modifying a Person) to allow users to change their own personal attributes and private identification questions.

71. Activation

Opens the Activation menu (shown in "Working with the ZAUTH Subsystem" on page 18), from which you define the circumstances under which the system activates the product.

81. System Configuration

Opens theSystem Configuration menu (shown in "Enabling Password Reset" on page 24), where you can configure Password Reset and its relationship to other iSecurity products.

82. Maintenance Menu

Opens the Maintenance menu, where you can set internal product definitions.

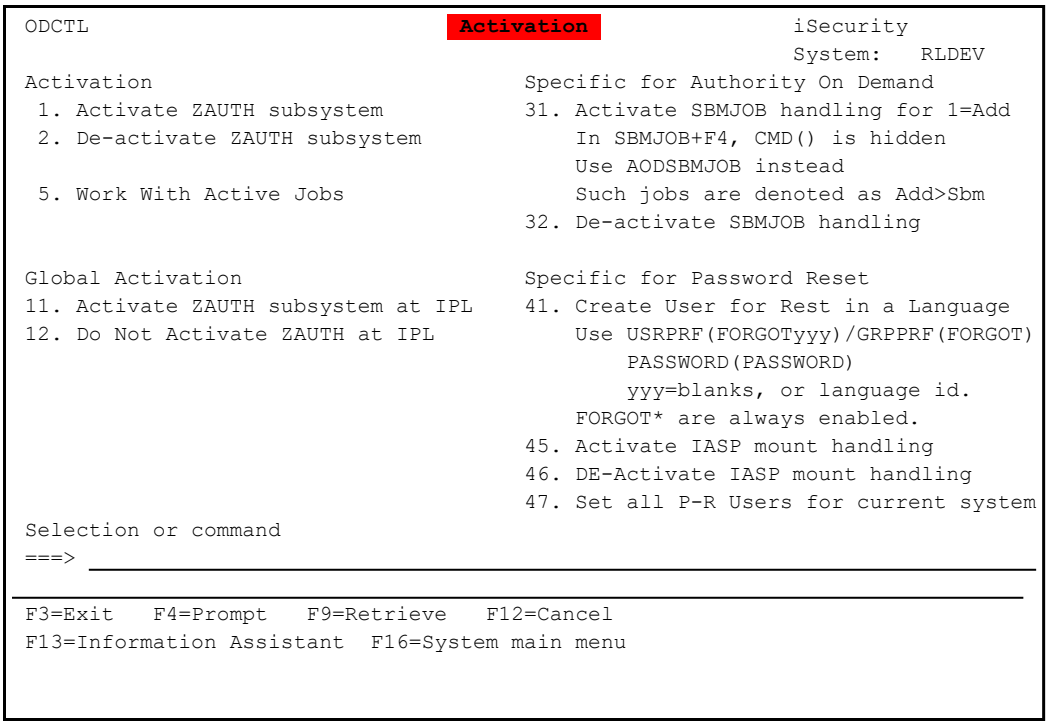
89. BASE Support

Opens the BASE Support menu, where you can configure Password Reset and other iSecurity products..

Working with the ZAUTH Subsystem

The ZAUTH subsystem controls Password Reset as well as the iSecurity Authority on Demand system. It must be running for either to function.

To **work with the ZAUTH subsytem**, select `71. Activation` from the Password Reset main menu. The **Activation** screen appears.



To **activate** the ZAUTH subsystem, select `1. Activate ZAUTH subsystem` from the **Activation** menu. The **Start Real-Time Auth on Demand (STRRTAOD)** screen (shown in "Starting the ZAUTH Subsystem" on page 20) appears.

To **check** that the ZAUTH susystem is active, select `5. Work With Active Jobs` from the **Activation** menu. The **Work with Subsystem Jobs** screen (shown in "Checking whether the ZAUTH Subsystem is Active" on page 21) appears.

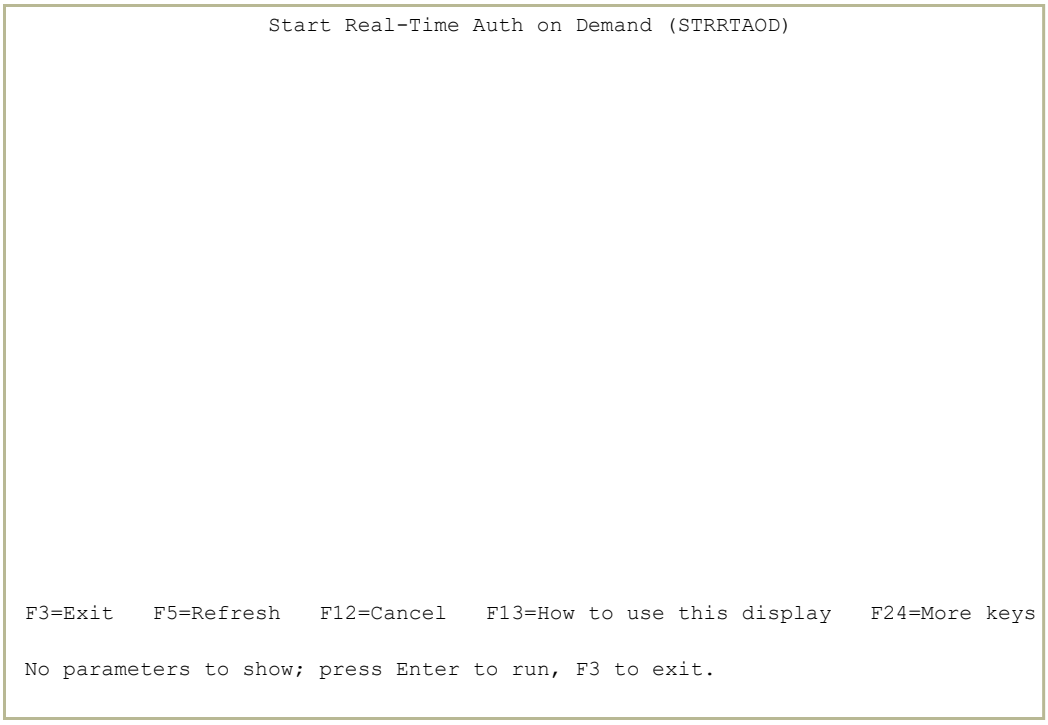
To **de-activate** the ZAUTH subsystem, select `2.De-Activate ZAUTH subsystem` from the **Activation** menu. The **End Real-Time Auth on Demand (STRRTAOD)** screen (shown in "Stopping the ZAUTH Subsystem" on page 22) appears.

To **cause the ZAUTH subsystem to become active each time your system starts**, select `11. Activate ZAUTH subsystem at IPL` from the **Activation** menu. A line at the bottom of the screen appears, saying "`Change effective next time subsystem starts.`"

To **prevent** the ZAUTH subsystem from becoming active each time that your system starts, select `12. De-activate ZAUTH subsystem at IPL` from the **Activation** menu. A line at the bottom of the screen appears, saying "`Change effective next time subsystem starts.`"

Starting the ZAUTH Subsystem

To **activate the ZAUTH subsystem**, select `1. Activate ZAUTH subsystem` from the **Activation** menu (shown in "Working with the ZAUTH Subsystem" on page 18). The **Start Real-Time Auth on Demand (STRRTAOD)** screen appears.

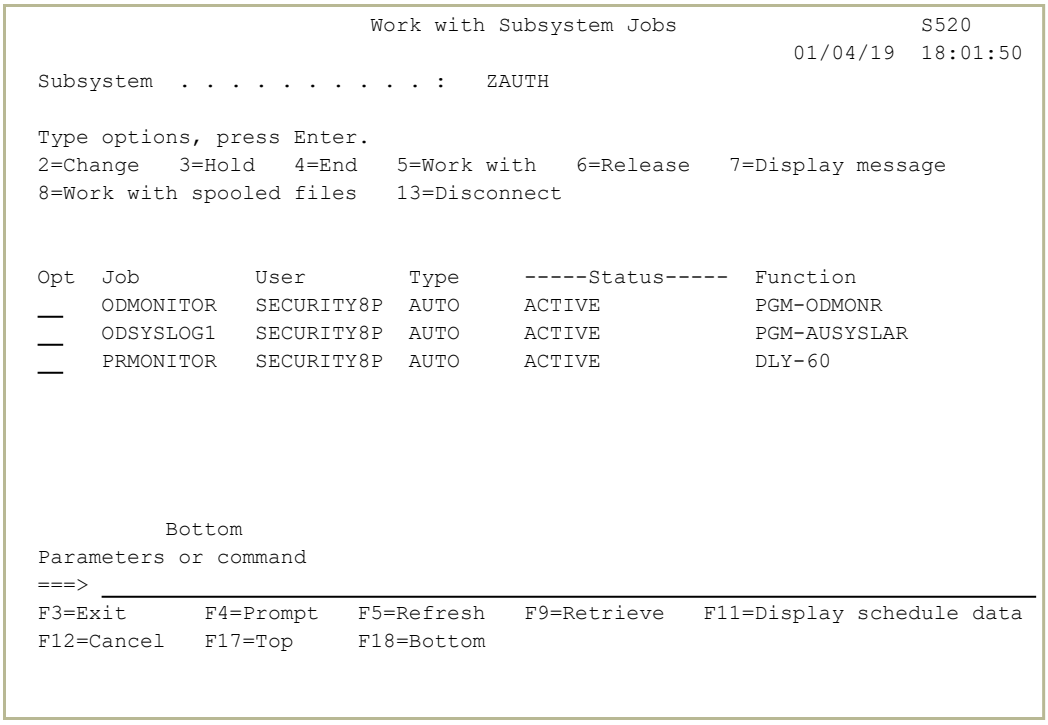


To **confirm** that you want to start the ZAUTH subsystem, press **Enter**. The **Activation** screen appears, with a line at the bottom saying "`Real-Time monitor of Authority on Demand started.`".

To **exit** without starting the ZAUTH subsystem, press the **F12=Cancel** key. The **Activation** screen appears.

Checking whether the ZAUTH Subsystem is Active

To **check that the ZAUTH susystem is active**, select `5. Work With Active Jobs` from the Activation menu (shown in "Working with the ZAUTH Subsystem" on page 18). The **Work with Subsystem Jobs** screen appears.



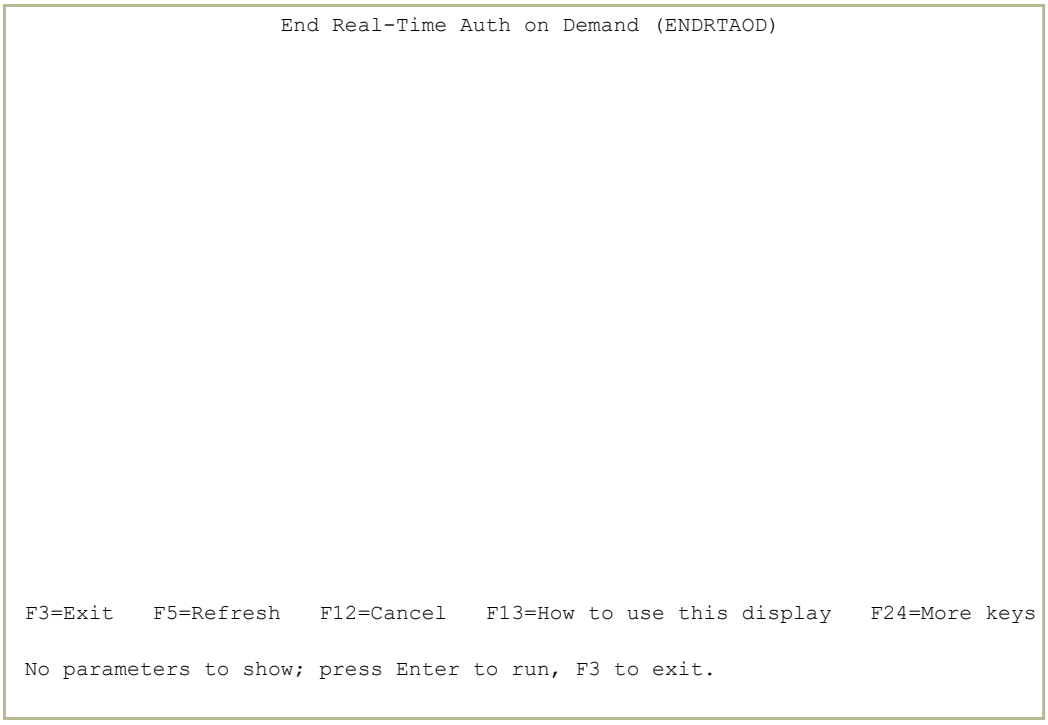
If the ZAUTH subsytem is running, several entries will appear on the screen showing active jobs. The **PRMONITOR** job monitors Password Reset within the ZAUTH subsytem.

Press the **F3=Exit** key to return to the **Activation** menu.

See IBM documentation for the other functions of this screen.

Stopping the ZAUTH Subsystem

To **de-activate** the ZAUTH subsystem, select `2. De-activate ZAUTH subsystem` from the **Activation** menu (shown in "Working with the ZAUTH Subsystem" on page 18). The **End Real-Time Auth on Demand (ENDRTAOD)** screen appears.

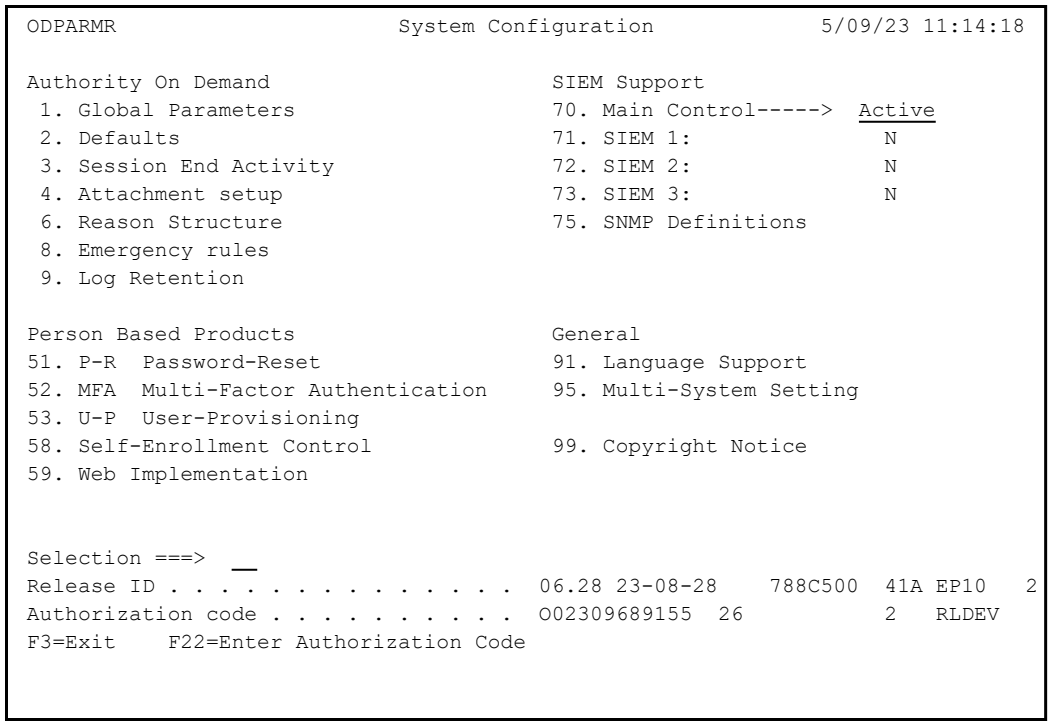


To **confirm** that you want to stop the ZAUTH subsystem, press the **Enter** key. The **Activation** screen appears, with a line at the bottom saying "`Real-Time monitor of Authority on Demand ended.`"

To **exit** without stopping the ZAUTH subsystem, press the **F12=Cancel** key. The **Activation** screen appears.

System Configuration

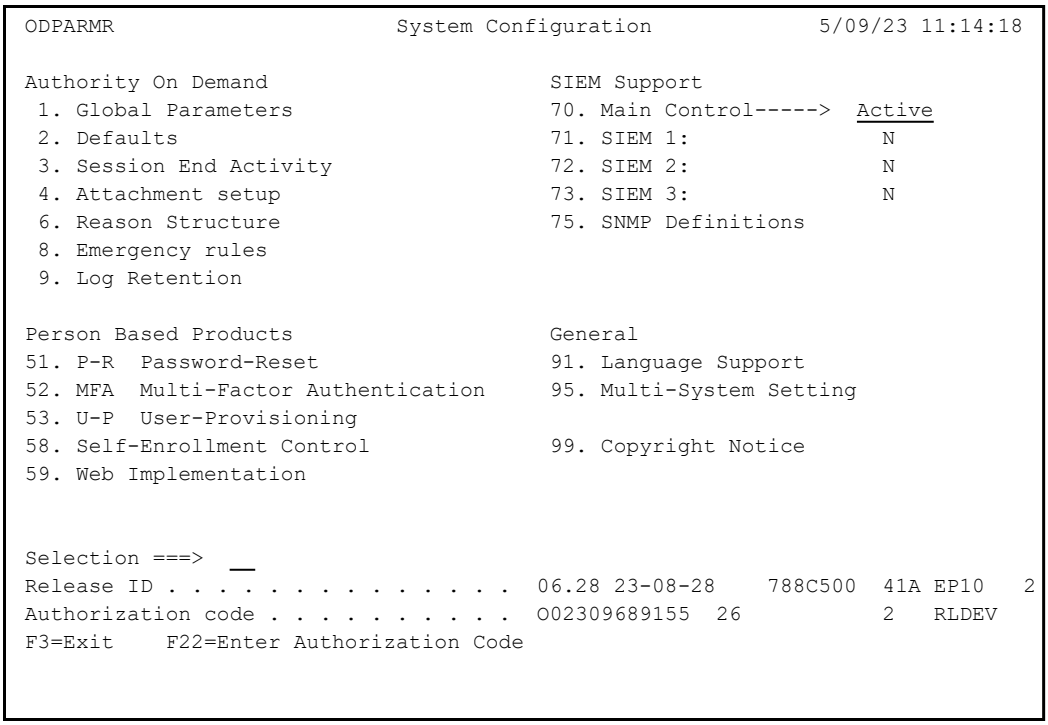
Use the **System Configuration** menu to access the setup processes for Password Reset and to define system parameters.



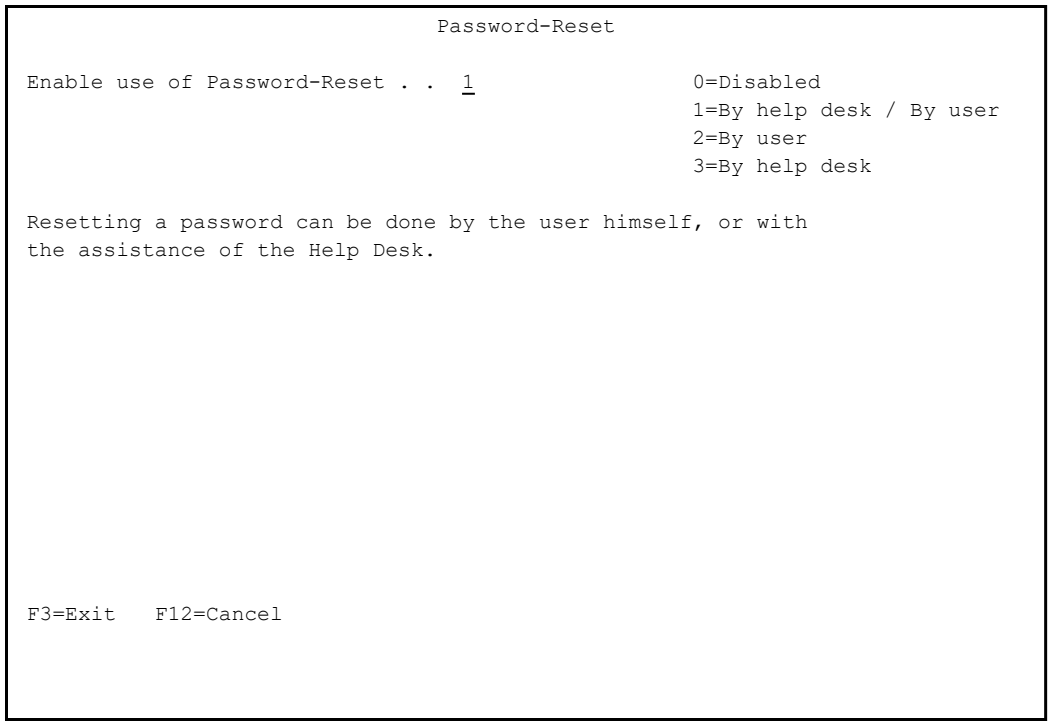
- "Enabling Password Reset" on the next page
- "Enabling and Controlling Self-Enrollment" on page 26
- "Setting Initial Process Questions" on page 28
- "Setting Initial Process Defaults" on page 30
- "Creating the Special Users for Password Reset" on page 32

Enabling Password Reset

To **enable Password Reset**, first select `81. System Configuration` from the Password Reset Main Menu.



To **enable Password Reset,** select **`51. P-R Password Reset`**. The **`Password-Reset`** screen appears.



The screen contains the following fields:

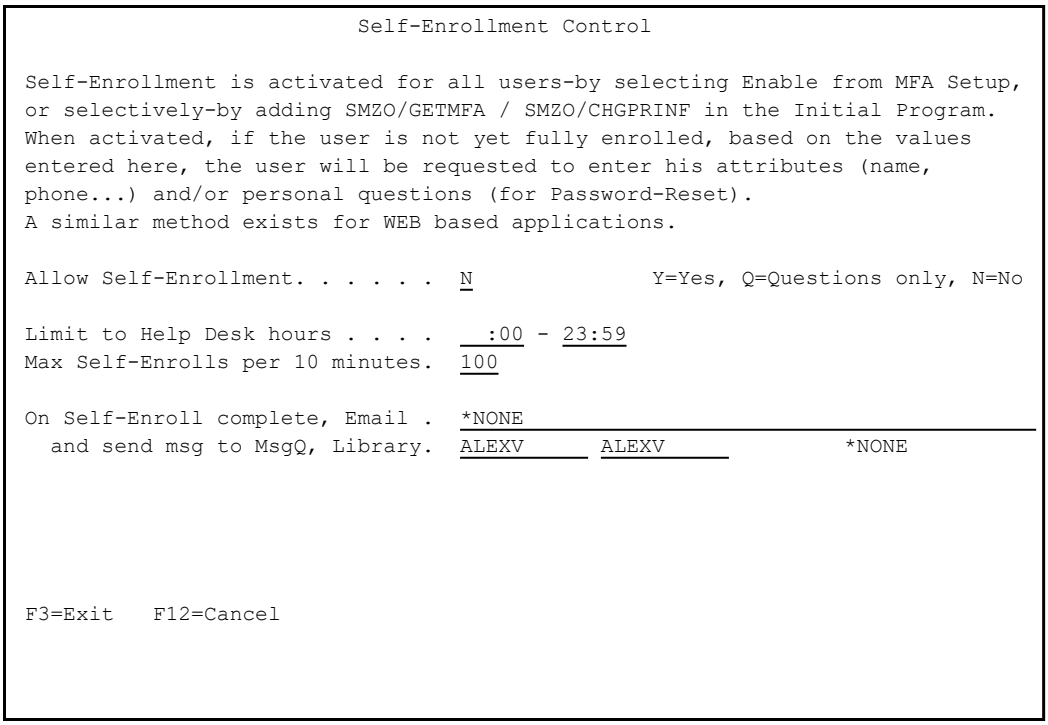
Enable use of Password-Reset

Defines who is allowed to use authentication to reset passwords.

- **0=Disabled.** Password Reset is not available.
- **1=By help desk / By user.** Password Reset can be performed by either the user or the help desk.
- **2=By user.** Password Reset can only be performed by the user.
- **3=By help desk.** Password Reset can only be performed by the help desk.

Enabling and Controlling Self-Enrollment

To **enable and control self-enrollment**, select **`58. Self-Enrollment Control`** from the **System Configuration** menu (*STRPWDRST* **`> 81`**). The **Self-Enrollment Control** menu appears.



`Allow Self Enrollment`

Whether Self-Enrollment is allowed. Possible values are:

Y: Yes

Q: Questions Only

N: No

`Limit to Help Desk hours`

You can choose to permit users to set their personal questions for the first time only during the defined Help Desk hours. This only applies to users setting their questions for the first time, since this is when they are most likely to seek assistance. Enter the starting time in the first field and the closing time in the second.

Max Self-Enrolls per 10 minutes

Defines the maximum number of users who can set their personal questions in a ten-minute period. This only applies to users setting their questions for the first time, since this is when they are most likely to seek assistance.

On Self-Enroll complete, Email

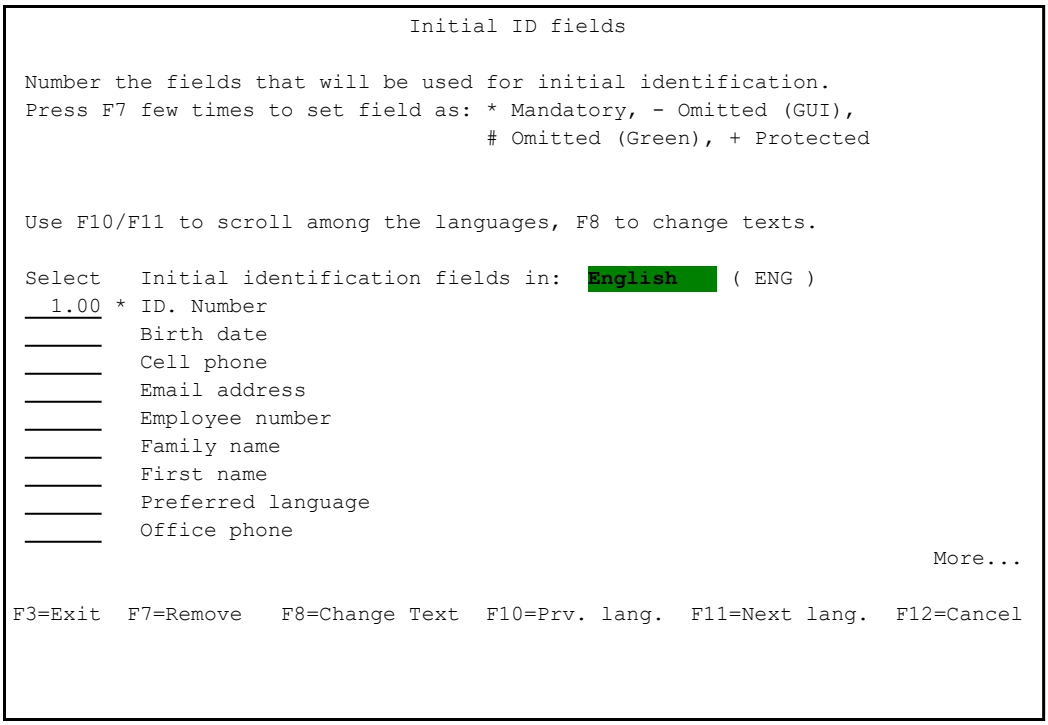
The email addresses to receive notice when users complete entering their personal questions. You can enter multiple addresses, separated by commas.

and send msg to MsgQ, Library

The message queue and library that [[[Undefined variable Raz-Lee-Variables.ProductName]]] is to notify when users enter their personal questions.

Setting Initial Process Questions

To **set the initial questions** asked when a user requests a Password Reset, select **`22. Initial Identification`** in the **Password Reset** main menu. The **Initial ID Fields** menu appears.



With this screen, you can set the questions that a user can be asked in the initial phase of the Password Reset process. You can set the questions for multiple languages and determine which questions must appear and which must not.

To **set the questions** that must appear and the order in which they are asked, enter a number in the **`Select`** field for each question. The numbers determine the order in which the questions are asked. They do not have to be integers. A question numbered "1.5", for example, would appear after a question numbered "1" and before a question numbered "2".

To **remove a question** from the list of possible questions presented on a web interface, place the cursor in the **`Select`** field for the question and press the **F7=Remove** key. A minus sign appears to the right of the field.

To **remove the field** from list of possible questions on the green screen interface as well as the web, press the **F7=Remove** key again. A pound sign ("**#**") replaces the minus sign.

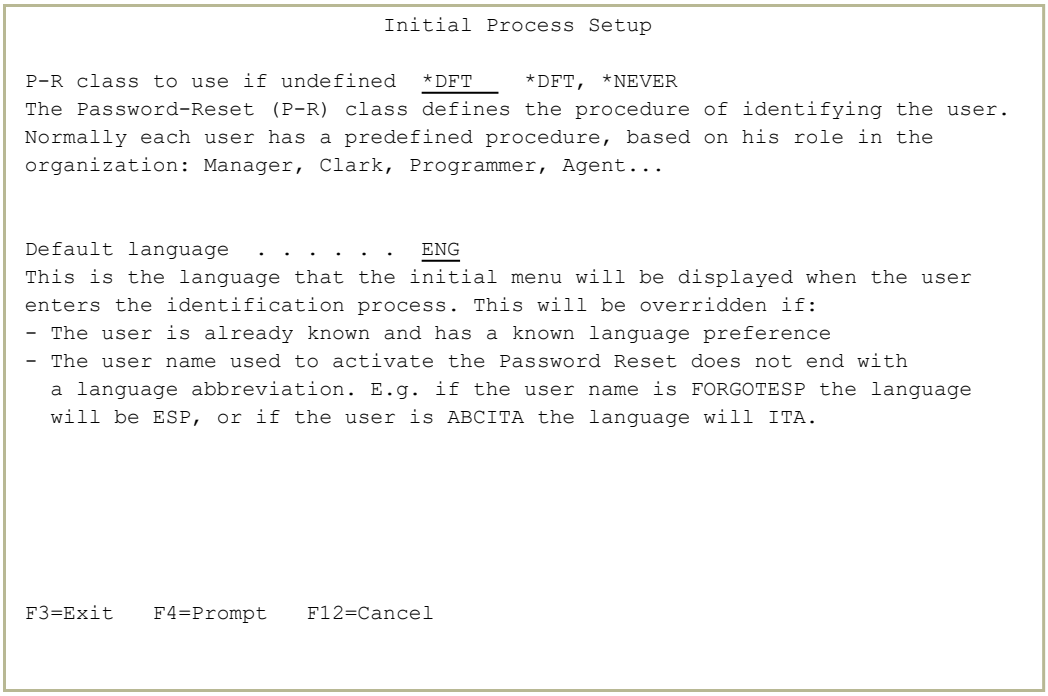
To **remove the pound sign and include the field**, press the **F7=Remove** again.

To **cycle among the languages** in which questions can appear, press the **F10=Prv. lang.** and **F11=Next lang.** keys. The questions appear in the languages defined for the system. To edit the question texts, press the **F8=Change Text** key. You can then enter and change the text of the questions, including further explanations if needed.

When you have finished entering or changing values, press **Enter** to return to the Password Reset screen.

Setting Initial Process Defaults

To **define the default language** in which Password Reset will operate, as well as the Password Reset class to use if the user's role is undefined, , select **21. Definitions** in the **Password Reset** main menu, then select **2. Default Class and Language**, The **Initial Process Setup** screen appears.



To determine the Password Reset**class** to use if the user does not have one, enter a value in the **P-R class to use if undefined** field. The classes are defined on the **Work with P-R Classes** screen (shown in "Working with Classes" on page 34). To set the user to use the system default, enter "***DFT**" in the field. If you do not want to use Password Reset for users for whom a class has not been set, enter "*NEVER" in the field.

To determine **language** in which the Password Reset screens appear by default, enter a value in the **Default Language** field. The text on the screen appears in that language if the user is not known or doesn't have a known language preference, or if the user name used to start the Password Reset process does not end in a three-letter language abbreviation.

To **select the value** from a list of known languages, place the cursor in the field and press the **F4=Prompt** key.

Creating the Special Users for Password Reset

Password Reset uses special users in the process of resetting password. While you can set these to different values, they are often set to the user name "FORGOT" with the password "PASSWORD". Logging in as this user places you in the Password Reset process. You can also create other user names that will start the Password Reset process in other languages.

To **create these users**, select `41. Create User` from the **Activation** menu (shown in "Working with the ZAUTH Subsystem" on page 18). The **Create User Profile (CRTUSRPRF)** screen appears.

```
                        Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . . . . . . > FORGOT       Name
User password  . . . . . . . . . > PASSWORD     Character value, *USRPRF...
Current library  . . . . . . . .   *CRTDFT     Name, *CRTDFT
Limit capabilities . . . . . . . > *YES         *NO, *PARTIAL, *YES
Text 'description' . . . . . . . > 'iSecurity Password-Reset (self service)'
_____

                           Additional Parameters

Special authority  . . . . . . . > *NONE        *USRCLS, *NONE, *ALLOBJ...
Group profile  . . . . . . . . . > *NONE        Name, *NONE









                                                                       Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

For the **general Password Reset user**, set the **`User profile`** field to "FORGOT" and the **`User password`** field to "PASSWORD". The text in the user interface will appear in the system's default language.

To **create users for other languages**, set the **User profile** field to "FORGOTyyy" where "yyy" is the three-letter identifier for the language. For example, the user for the Italian language would be "FORGOTITA" and the user for Hebrew would be "FORGOTHEB".

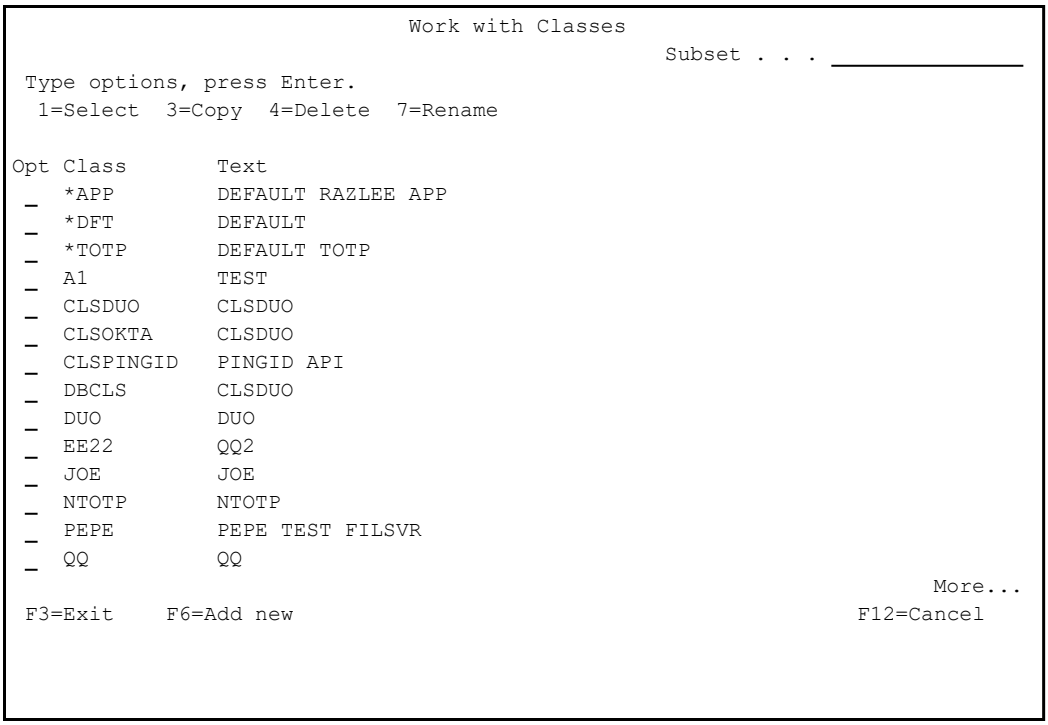
Once you have entered the information for the user, press the **F3=Exit key** to save the entry. The **Activation** screen appears.

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.

Working with Classes

To **add, modify, copy, rename or delete classes**, select **1. Classes** from the **Definitions** screen (STRPWDRST**> 21**). The **Work with Classes** screen appears.



To **modify a class**, enter **1** in the **Opt** field for that class. The **Modify Class** screen appears, as shown in "Modifying Classes" on page 36.

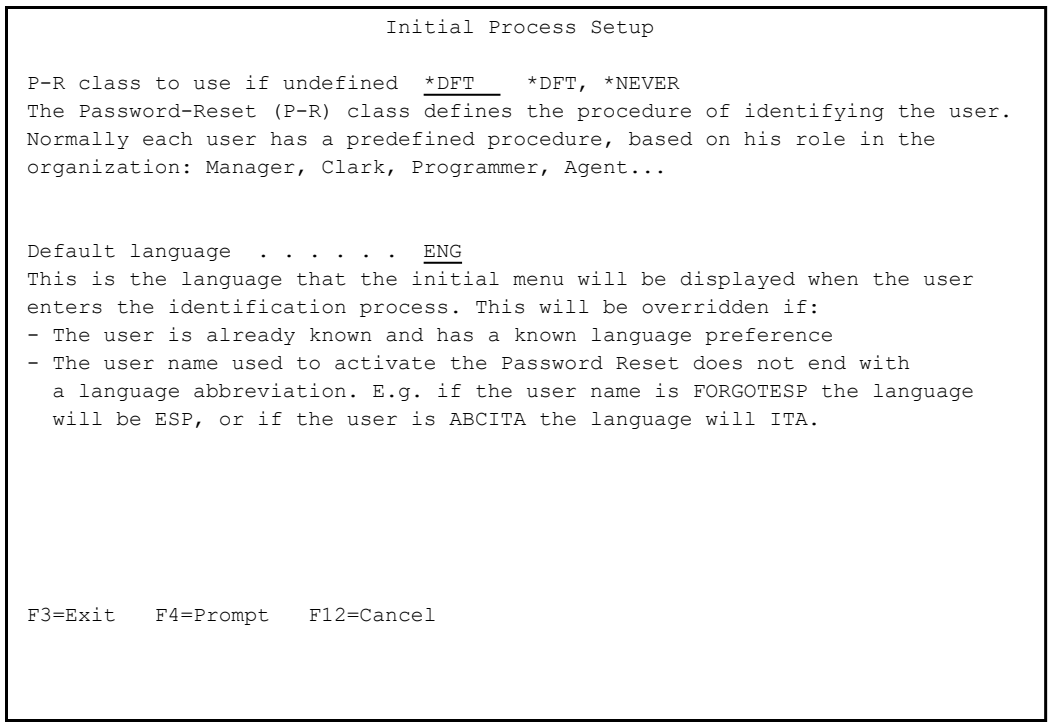
To **copy a class**, enter **3** in the **Opt** field for that class. The **Copy Class** screen appears. Enter the name of the new class in the **New class** field of that screen, then press **Enter**.

To **delete a class**, enter **4** in the **Opt** field for that class. The **Delete Class** screen appears, displaying information about the class. Press **Enter** to delete that class. You can only delete classes that have no Persons as members.

To **rename a class**, enter **7** in the **Opt** field for that class. The **Rename Class** screen appears, displaying information about the class. Type a new name and press **Enter** to rename the class.

To **add a class**, press the **F6** key. The **Add New Class** screen appears, with the same fields as the **Modify Class** screen shown in "Modifying Classes" on the next page.

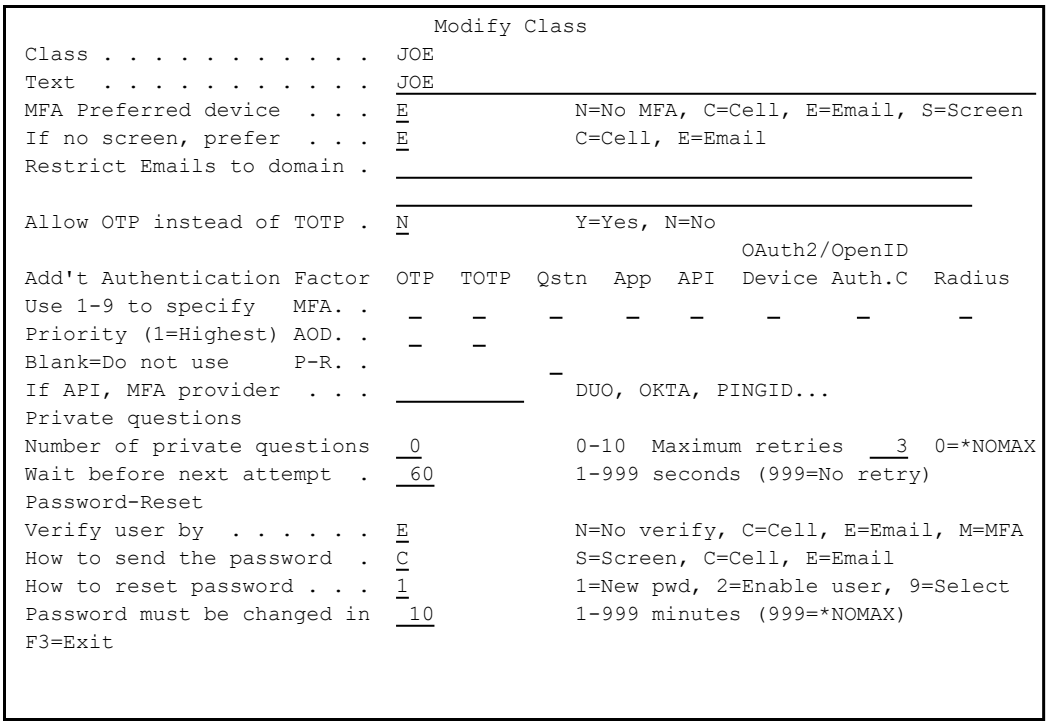
To **set the default class and language** to use, select **2. Default Class and Language** from the **Definitions** menu. The **Initial Process Setup** screen appears:



Enter the values as described on that page.

Modifying Classes

To **modify a class**, enter **1** in the **Opt** field for that class on the **Work with Classes** screen (**STRPWDRST> 21 > 1**). The **Modify Class** screen appears:



The screen contains these fields:

Class

The name of the class. The default class is specified as ***DFT**.

Text

A free-form text description of the class.

MFA Preferred Device

The device to be used for MFA verification. A user who connects to the system and requires MFA is sent a link for confirmation, either via email or via SMS to the user's smartphone.

Values include:

C: Cell phone

E: Email

N: The class does not use MFA.

S: Screen

If no screen, prefer

The destination for messages if the **MFA Preferred Device** is set to Screen but is not available.

Values include:

C: Cell phone

E: Email

Restrict Emails to domain

The domains to which verification codes and new passwords can be sent by email. For example, they might be restricted to domains within the organization. If this field is left empty, the emails can go to any domain.

Allow OTP instead of TOTP

Values include: Y=Yes, N=No

Add't Authentication Factor

The methods that MFA, Authority on Demand, and Password Reset use for additional authentication. When the user signs in using MFA and follows the link sent via email or SMS, the page displays a series of buttons on the lower right. The user can select those buttons to use alternate methods of verification. The values set here determine the order in which the buttons appear onscreen, from left to right. If no value is set for a method here, no button appears for that method.

The three lines show that methods available for MFA, Authority on Demand, and Password Reset.

The methods are:

OTP

A one-time password, sent via email or SMS, as set in the **Preferred Verification Device** field.

TOTP

A temporary one-time password, as shown in an authenticator app, such as the Microsoft Authenticator or

Google Authenticator, installed on the user's smartphone. Users are set up with MFA (as shown in) receive a QR code by email. Scanning this code with an authenticator app connects the app and your MFA system. Users authenticating via TOTP enter the code shown for your system in their app. The codes change every thirty seconds. If a code expires while the user is entering it, they must enter the code that replaced it.

Qstn

A set of personal security questions that the user must answer correctly. The questions for each person are entered on the Modify Person Identification Questions screen (as shown in "Modifying Person Identification Questions" on page 50).

App

The iSecurity authorization App.

API

A relevant API.

OAuth2/OpenID Device

The OAuth 2.0 Device Authorization Grant (formerly known as the Device Flow) is an OAuth 2.0 extension that enables devices with no browser or limited input capability to obtain an access token.

OAuth2/OpenID Auth. C

The authorization code grant type is used to obtain both access tokens and refresh tokens and is optimized for confidential clients. Since this is a redirection-based flow, the client must be capable of interacting with the resource owner's user-agent (typically a web browser) and capable of receiving incoming requests (via redirection) from the authorization server.

RADIUS

RADIUS authentication goes through a separate authentication server to authenticate users.

The two fields under **Private Questions** are relevant if **Qstn** has been selected as an additional authentication option.

Number of private questions

The number of private questions that the user is asked. The value can be between 0 and 10. The default is 0, meaning that Password Reset will skip the personal questions.

Wait before next attempt

The number of seconds that a user must wait after entering the maximum number of failed responses before trying again.

The number can be between **0** and **998**. A value of **999** means that there is no waiting time between failures.

The four fields under **Password Reset** are relevant for Password Reset.

Verify user by

Possible values are:

N: No verification

C: Cell

E: Email

M: MFA

How to send the password

Possible values are:

S: Screen

C: Cell

E: Email

How to reset password

Possible values include:

1: New password

2: Enable user

9: Select

Password must be changed in

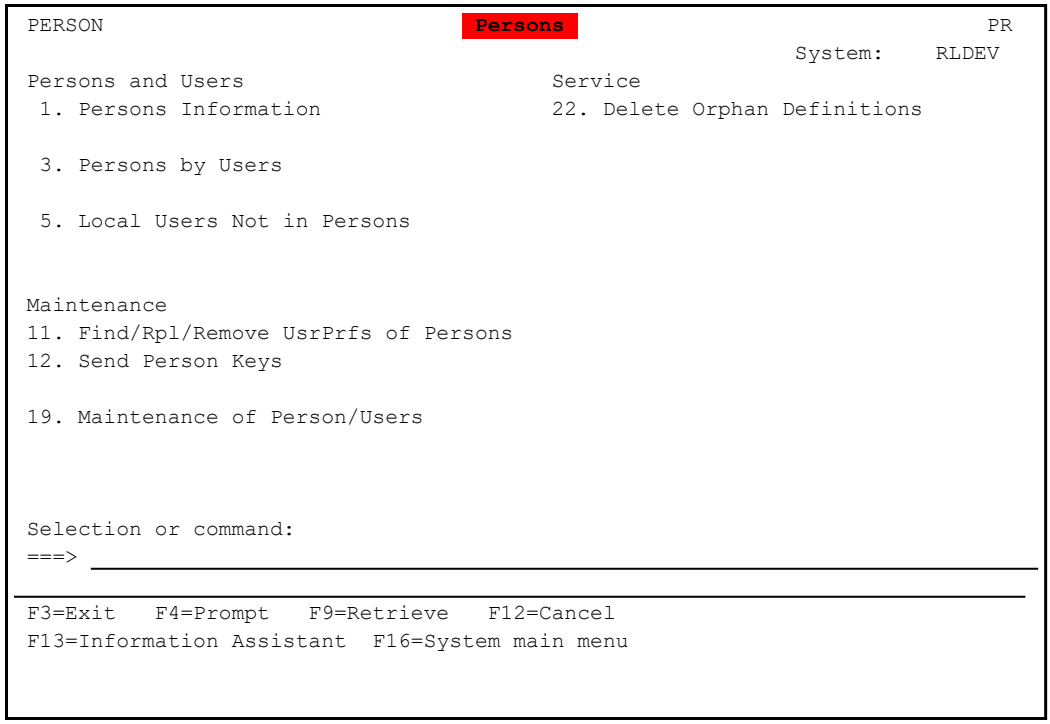
The number of minutes within which the password must be changed. Values are from **1** to **998**, with **999** indicating no

maximum time.

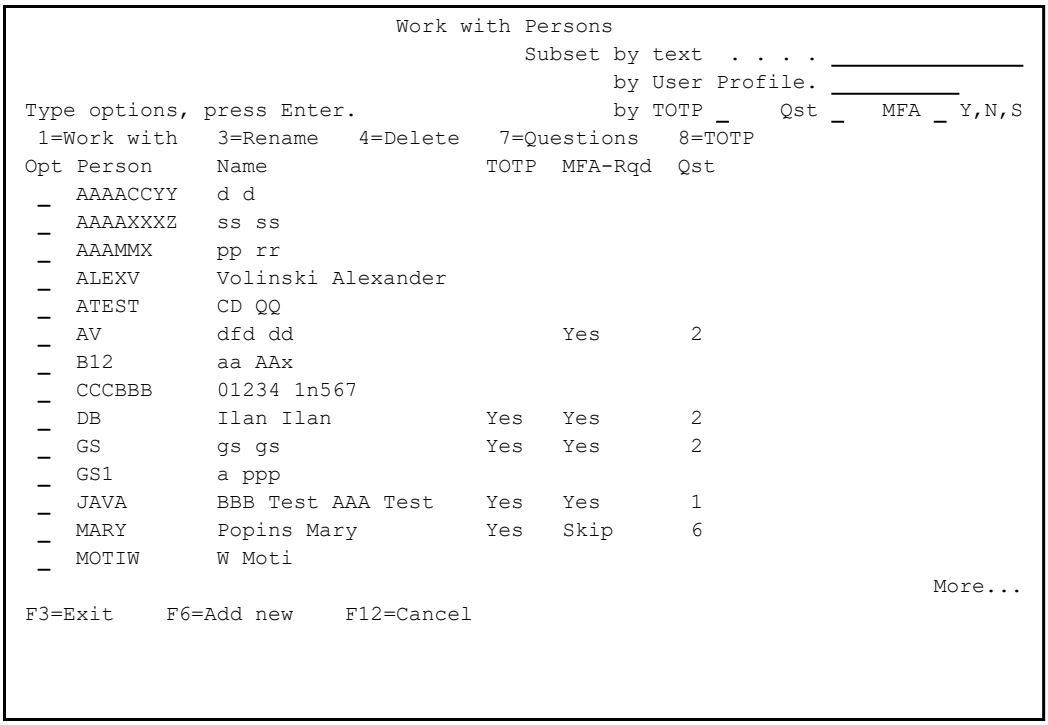
Defining Persons

Multi-Factor Authentication, as well as iSecurity Authority on Demand and Password Reset, manages user information in terms of **Persons**. Since multiple users on multiple system might all be the same person, Password Reset groups them together. Thus, for example, if a person has been successfully authenticated as a particular user on one system, attempts to access related systems by that same person using other user names in a allotted period of time will also be accepted without needing to be authenticated again.

To **define and work with persons**, select **1. Persons** from the **Password Reset** main menu. The **Persons** menu appears.



To **display and enter information concerning each user**, select **1. Person Information** from the **Persons** menu (STRPWDRST**> 1**). The **Work with Persons** screen appears:



The body of the screen contains a line for each user. Each contains the following fields:

Person

A unique identifier for the Person.

Name

The family name and first name of the user.

TOTP

If set to **Yes**, a Temporary One-Time Password for MFA is defined for this person.

MFA-Rqd

Whether MFA is required for this person.

Qst

The number of personal questions and answers defined for this person.

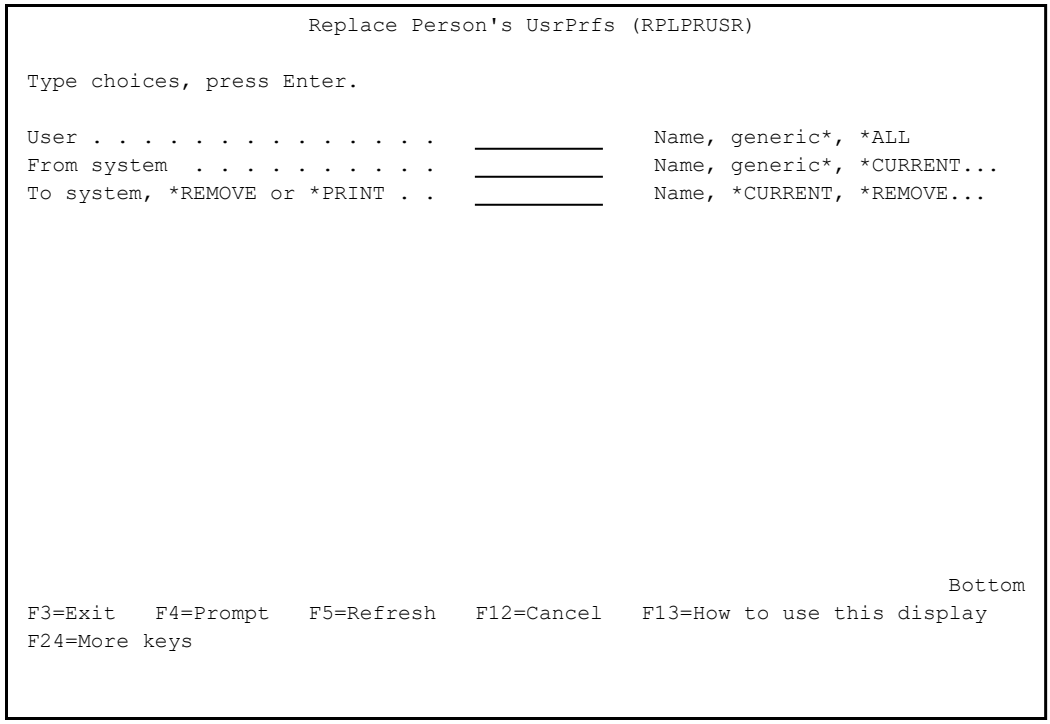
To add a new person, press the F6 key from the Work with Persons screen (*STRPWDRST*> **1 > 1**). The Add New Person screen appears, as shown in "Adding a New Person" on page 45.

To **modify a person**, enter **1** in the **Opt** field for the person on the **Work with Persons** screen (*STRPWDRST*> **1 > 1**). The **Modify Person** screen appears, as shown in "Modifying a Person" on page 48.

To **define a person's private questions** for Password Reset, enter 7 in the **Opt** field for the person on the **Work with Persons** screen (*STRPWDRST*> **1 > 1**). The **Modify Person Identification Questions** screen appears, as shown in "Managing Private Questions for a Person" on page 55.

To **send a person's key** for Temporary One-Time Passwords or Emergency codes to them, select **12. Send Person Keys** from the **Persons** menu (*Password Reset* > **1**). The **Send Person Keys (SNDPRKEY)** screen appears, as shown in "Sending Keys for a Person" on page 57.

To **find, remove, or replace a Person's user profiles**, select **11. Find/Rpl/Remove UsrPrfs of Persons** from the **Persons** menu (*STRPWDRST*> **1**). The **Replace Person's UsrPrfs (RPLPRUSR)** screen appears.



This command could be useful in duplicating a person's user profiles from one system to another.

The body of the screen has three fields:

User

The name of the person or persons. It can be a name, a generic* name, or *ALL.

From system

The system containing the original user profiles. It can be a name, a generic* name, *CURRENT, or *ALL.

To system, *REMOVE or *PRINT

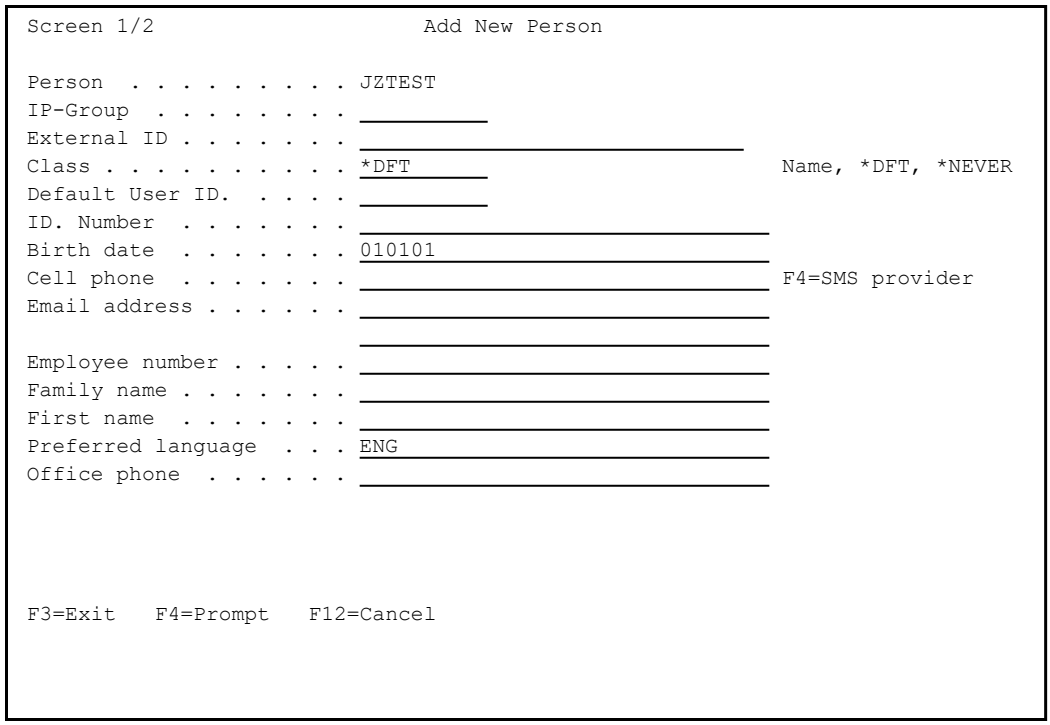
If you are replacing user profiles, the name of the system to which they should be copied from the system in the previous field.

To remove user profiles from the system in the previous field, the string *REMOVE.

To print a listing of user profiles from the system in the previous field.

Adding a New Person

To **add a new person** to the list of users, press the **F6** key on the **Working with Persons** screen (as shown in "Defining Persons" on page 41). The **Add New Person** screen appears.



The body of the screen contains these fields:

Person

A unique identifier for the Person.

IP-Group

The name of an IP Group of which the person is a member, as described in Defining IP Groups.

External ID

A different unique identifier for the Person, if one has been established.

Class

The Password Reset class to which the person belongs. The class determines how the user's identity is verified when resetting passwords. To select the class from a list, press the **F4** key. You can

also enter either "***DFT**" to use default settings or "***NEVER**" to define that the Password Reset class will never be used.

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.

ID. Number

The National ID number of the Person.

Birth date

The Person's birth date in the standard national format as set for the system. In the USA, for example, it would be "MM/DD/YY", so December 31st, 1970 would be "12/31/70". In much of Europe, it would be "DD/MM/YY", so December 31st, 1970 would be "31/12/70".

Cell phone

The cell phone number of the Person. SMS notifications of new passwords would go to this number. To select a mobile phone provider from a list, press the F4 key.

Email address

The email address of the person. Email notifications of new passwords would go to this email address.

Employee number

The employee number of the Person within the organization

Family name

The family name or surname of the Person

First name

The first name of the Person.

Preferred language

The language in which the Person will receive verification questions. To select the language from a list, press the F4 key.

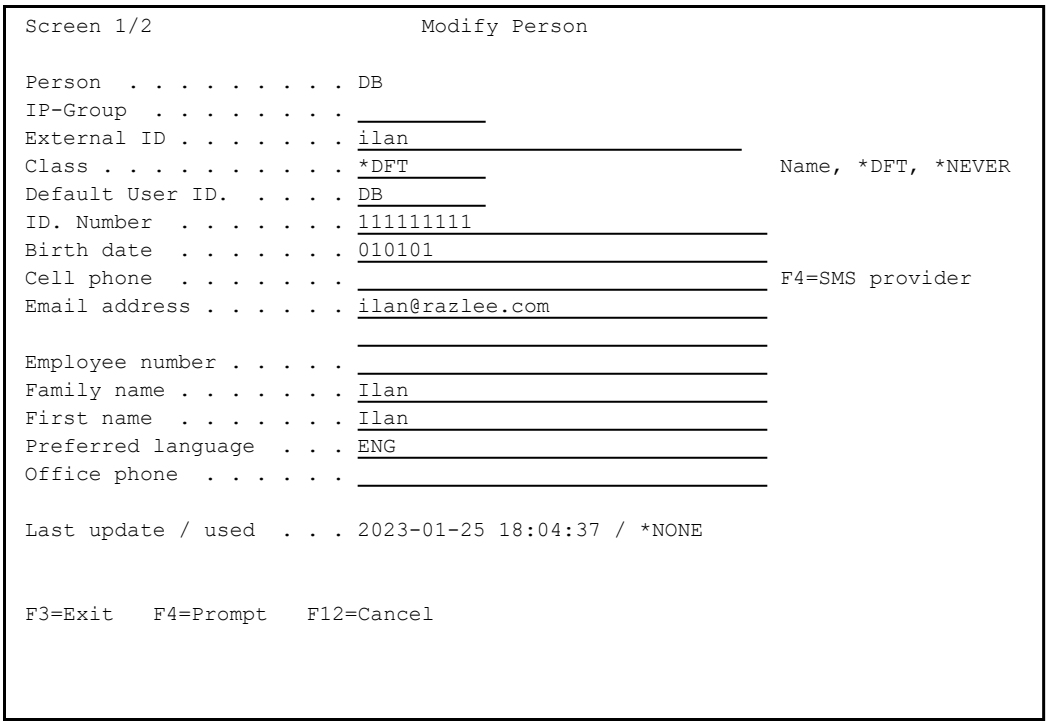
Office phone

The office phone number of the Person

Press **Enter** to complete the entry. The **Work with Users of a Person** screen appears, as shown in "Setting Up Users for a Person" on page 51

Modifying a Person

To **modify a person**, enter **1** in the **Opt** field for the person on the **Working with Persons** screen, as shown in "Defining Persons" on page 41. The **Modify Person** screen appears:



The body of the screen contains these fields:

Person

A unique identifier for the Person.

ID. Number

The National ID number of the Person.

Birth date

The Person's birth date in the standard national format as set for the system. In the USA, for example, it would be "MM/DD/YY", so December 31st, 1970 would be "12/31/70". In much of Europe, it would be "DD/MM/YY", so December 31st, 1970 would be "31/12/70".

Cell phone

The cell phone number of the Person. SMS notifications of new passwords would go to this number. To select a mobile phone provider from a list, press the F4 key.

Email address

The email address of the person. Email notifications of new passwords would go to this email address.

Employee number

The employee number of the Person within the organization

Family name

The family name or surname of the Person

First name

The first name of the Person.

Preferred language

The language in which the Person will receive verification questions. To select the language from a list, press the F4=Prompt key.

Office phone

The office phone number of the Person

Default user ID

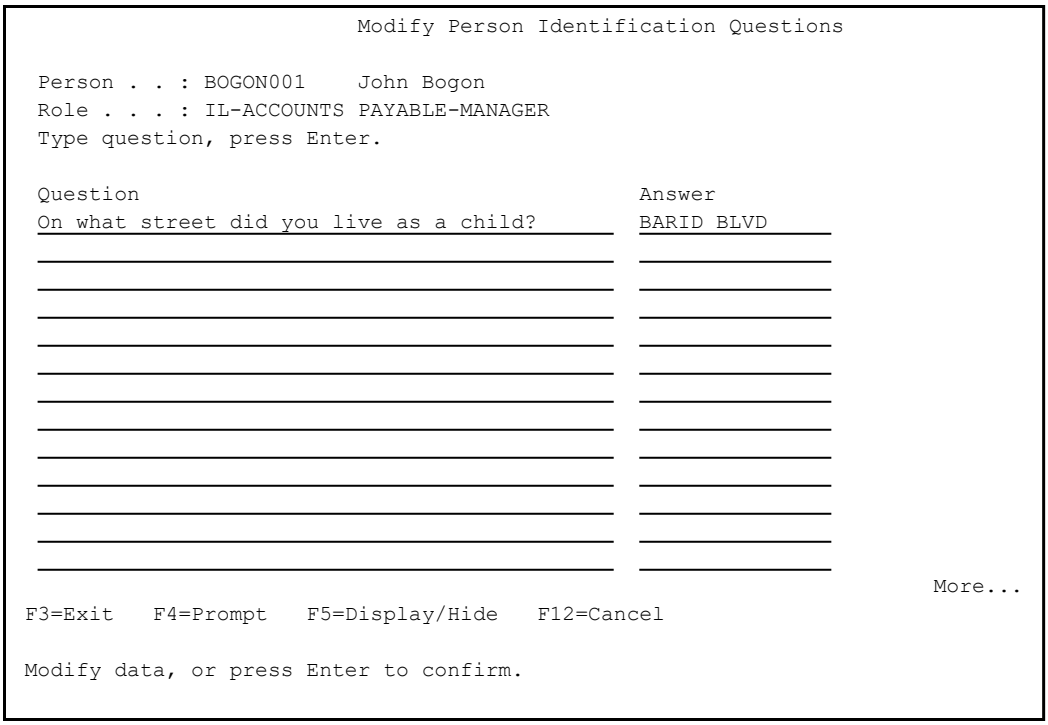
The preferred User ID of the Person on the IBM i. It is used to create the User Profiles for the Person.

Password Reset Class

The Password Reset class to which the person belongs. The class determines how the user's identity is verified when resetting passwords. To select the class from a list, press the F4 key. You can also enter either "***DFT**" to use default settings or "***NEVER**" to define that the Password Reset class will never be used.

Modifying Person Identification Questions

To **set or modify a Person's identification questions and answers**, enter **7** in the **Opt** field for that Person on the **Work with Persons** screen (*STRMFA* **> 1 > 1**). The **Modify Person Identification Questions** screen appears.



The body of the screen contains lines in which you can enter multiple questions, used to identify a Person, and their corresponding answers. The questions can be up to 45 characters long. The answers can be up to 15 characters long.

By default, the answers are hidden. To reveal or hide them press the **F5** key.

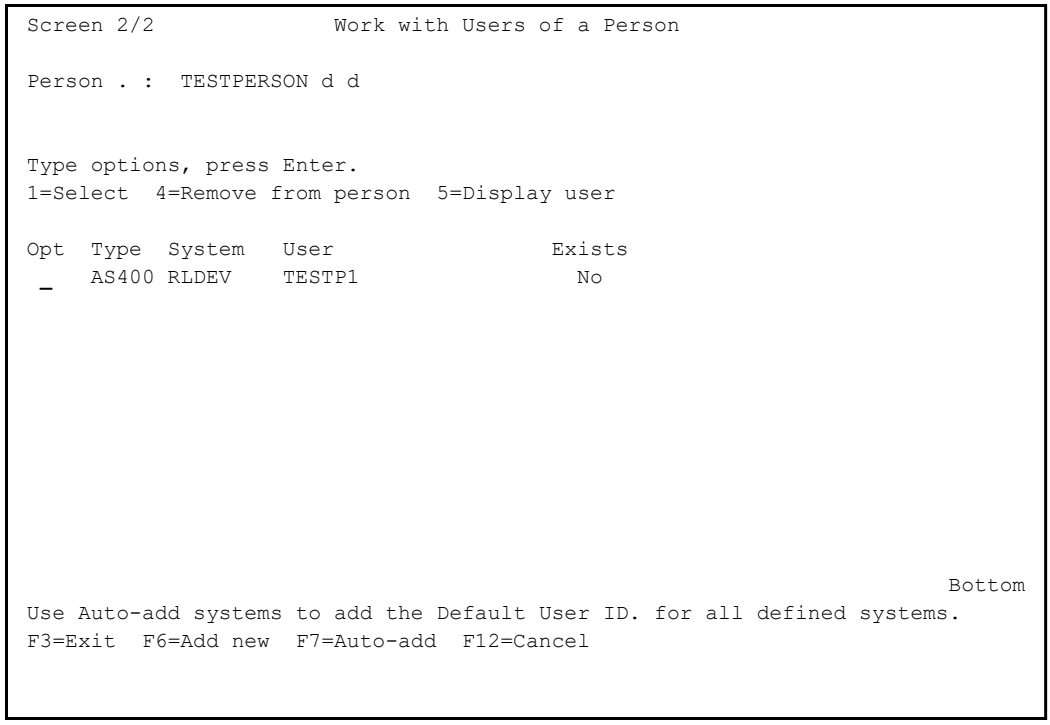
Setting Up Users for a Person

Each Person can correspond to users on multiple systems.

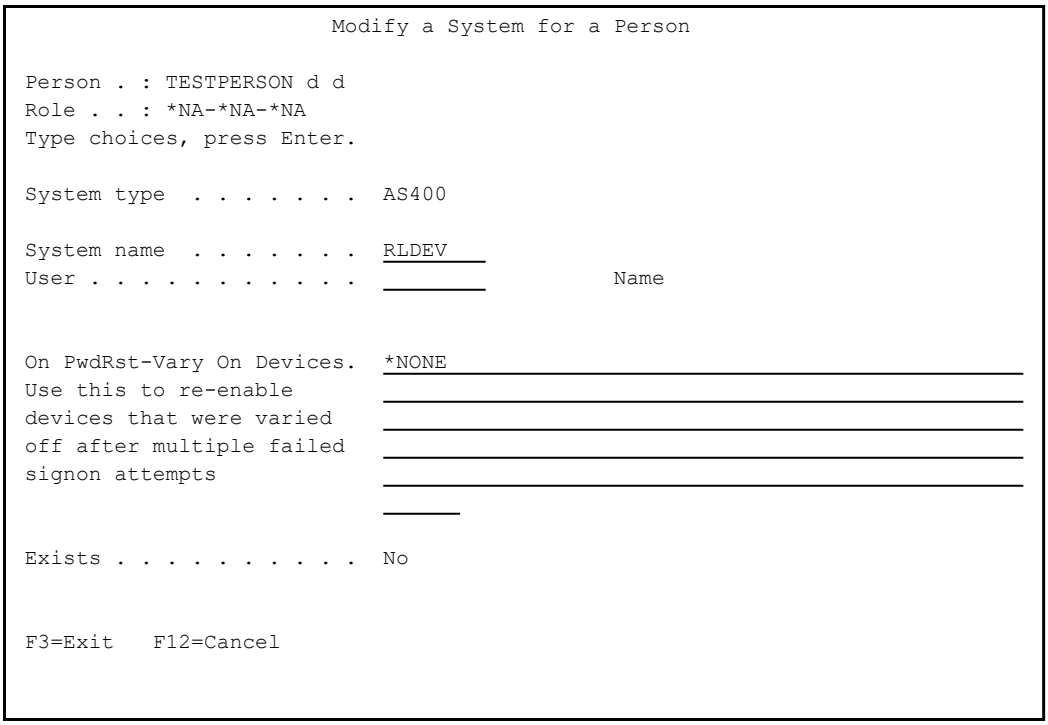
To **add or delete users from a defined Person**, open the **Work with Persons** menu (*STRMFA* **> 1 > 1**).

Enter **1** in the **Opt** field for the Person. The **Modify Person** screen appears.

Press **Enter** again. The **Work with Users of a Person** screen appears.



To **add a user to a person**, press the **F6** key from the **Work with Users for a Person** screen (*STRPWDRST* **> 1 > 1 , 1**).. The **Modify a System for a Person** screen appears.



Enter the name of the system for the user in the **System name** field. By default, this is the system on which you are working,.

Enter the name of the user in the **User** field. Press the **F4** key to display a list of users on the system.

To **automatically add a user to a person**, press the **F7** key from the **Work with Users for a Person** screen (*STRPWDRST* **> 1 > 1, 1**). If a user with the same name of the Person exists on the system, that user is automatically added to the person.

To **modify information about an existing user for the person**, enter **1** in the **Opt** field for the user on the **Work with Users for a Person** screen (*STRPWDRST* **> 1 > 1, 1**). The **Modify a System for a Person** screen appears, as it does for adding a user, with the information for the current user.

To **delete an existing user from a person**, enter **4** in the **Opt** field for the user on the **Work with Users for a Person** screen (*STRPWDRST* **> 1 > 1, 1**). The **Delete a System for a Person** screen appears, with the same fields as the **Modify a System for a Person** screen. Press **Enter** to delete the user, or the **F12** key to cancel the deletion.

To **view detailed information on a user** in a convenient, read-only form, enter **1** in the **Opt** field for the user on the **Work with Persons by Users** screen (*STRPWDRST* **> 1 > 3**). The **Display User** screen appears, showing the information.

To **move a user to another person**, enter **3** in the **Opt** field for the user on the **Work with Persons by Users** screen (*STRPWDRST* **> 1 > 3**). The **Move User to another person** screen appears. Enter the name of the person to whom you are moving the user in the **To person** field.

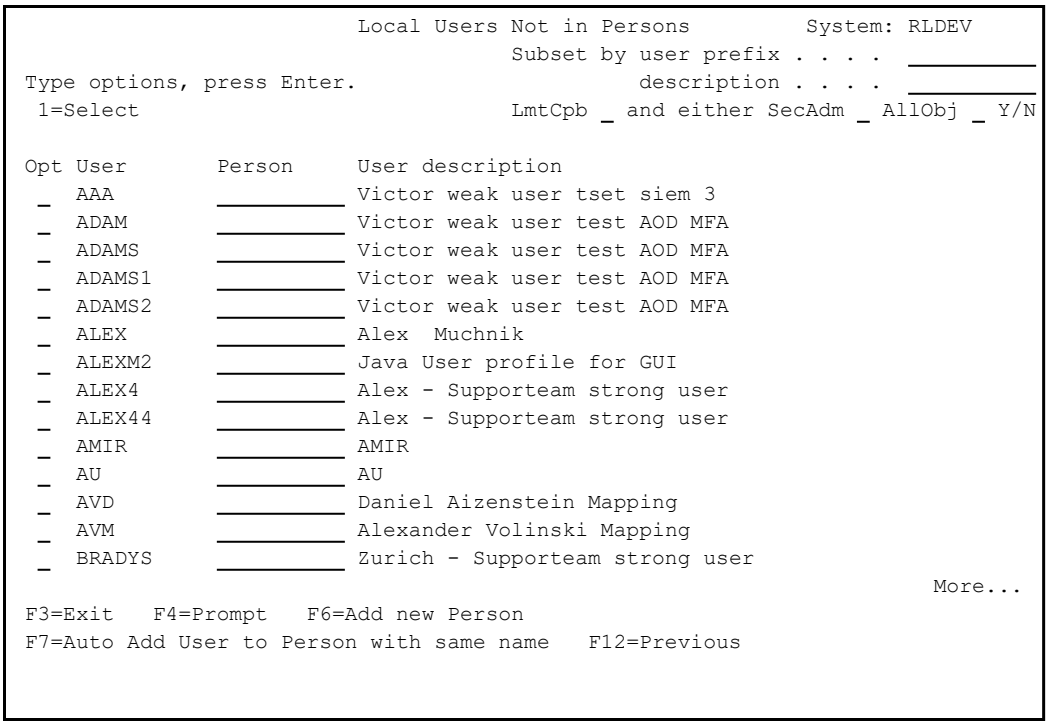
To **remove a user from a person**, enter **4** in the **Opt** field for the user on the **Work with Persons by Users** screen (*STRPWDRST* **> 1 > 3**). The **Remove Users from persons** screen appears, showing the name of the User and System and the Person from whom the user is to be removed. Press **Enter** to remove the user, or the **F12** key to cancel the removal.

To **view users who have not been assigned to persons**, select **5. Local Users Not in Persons** from the **Persons** menu (*STRPWDRST* **> 1**). The **Local Users Not in Persons** screen appears, as shown in "Assigning Users to Persons" on the next page.

To **delete definitions for Persons** who should have been removed in other actions, select **22. Delete Orphan Definitions** from the **Persons** menu (*STRPWDRST* **> 1**). A **Call Program (CALL)** screen appears, which runs the *PRDLTOSR* command from the **SMZO** library.

Assigning Users to Persons

To **view users who have not been assigned to persons**, select **`5. Local Users Not in Persons`** from the **Persons** menu (*STRPWDRST* **>** **`1`**). The **Local Users Not in Persons** screen appears.



```
                          Local Users Not in Persons         System: RLDEV
                                     Subset by user prefix . . . .  __________
Type options, press Enter.                     description . . . .  __________
 1=Select                            LmtCpb _ and either SecAdm _ AllObj _ Y/N

Opt User       Person     User description
 _  AAA        __________ Victor weak user tset siem 3
 _  ADAM       __________ Victor weak user test AOD MFA
 _  ADAMS      __________ Victor weak user test AOD MFA
 _  ADAMS1     __________ Victor weak user test AOD MFA
 _  ADAMS2     __________ Victor weak user test AOD MFA
 _  ALEX       __________ Alex  Muchnik
 _  ALEXM2     __________ Java User profile for GUI
 _  ALEX4      __________ Alex - Supporteam strong user
 _  ALEX44     __________ Alex - Supporteam strong user
 _  AMIR       __________ AMIR
 _  AU         __________ AU
 _  AVD        __________ Daniel Aizenstein Mapping
 _  AVM        __________ Alexander Volinski Mapping
 _  BRADYS     __________ Zurich - Supporteam strong user
                                                                      More...
F3=Exit   F4=Prompt   F6=Add new Person
F7=Auto Add User to Person with same name   F12=Previous
```

The body of the screen contains lines for each user on the current system that does not have a corresponding Person. Each line shows the **`User`** name, a free-text **`User description`**, and an empty **`Person`** field.

To **assign the user to an existing Person**, enter the Person's name in the **`Person`** field and press **Enter**.

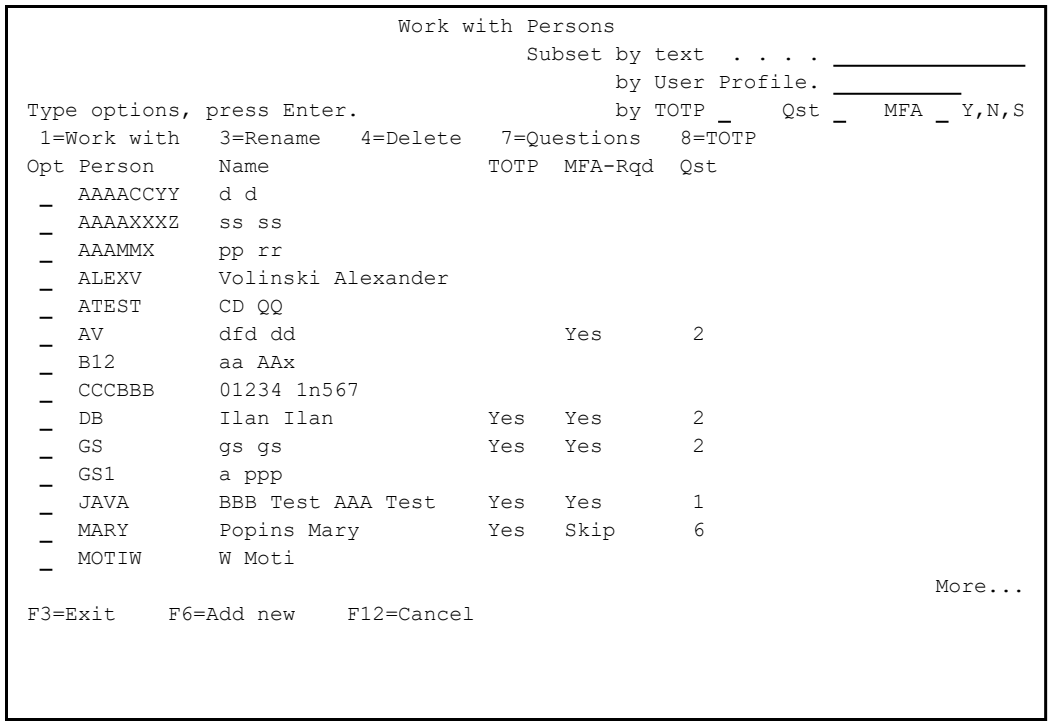
To **select from a list of existing persons**, press the **F4** key.

To **automatically add the user to an existing Person with the same name**, press the **F7** key.

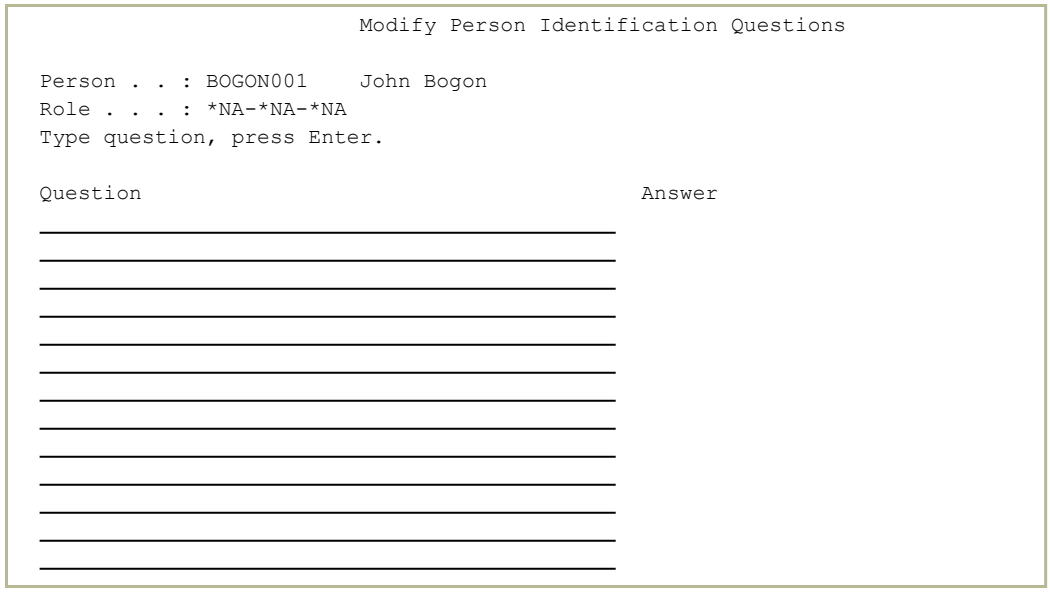
To **create a new Person**, press the **F6** key. The **Add New Person** screen appears, as shown in "Adding a New Person" on page 45.

Managing Private Questions for a Person

To **add, delete, or modify private questions** for a Person, open the **Work with Persons** Screen (shown in Persons).



Type the digit **7** in the **Opt** field for the Person whose questions you wish to manage and press **Enter**. The **Modify Person Identification Questions** screen appears.



```
                                                                    More...
F3=Exit    F4=Prompt    F5=Display/Hide    F12=Cancel
```

To **add a question**, place the cursor in the **Question** field on a blank line and type an identifying question that few people other than you would know. To select from a sample list of questions, press the **F4=Prompt** key.

When you have finished entering the question, press **Enter**. The cursor moves to the **Answer** field for that line.

Type the answer to that question. By default, what you type will not appear on the screen. To display the answers, press the **F5=Display/Hide** key.

Be sure to type exactly the answer you would give later when asked the question. The answers are case-sensitive.

To **modify a question**, edit the question in the **Question** field on that line.

When you have finished entering the question, press the **Enter** key. The cursor moves to the Answer field for that line.

If the answers are not visible, press the **F5=Display/Hide** key to display them.

Be sure to type exactly the answer you would give later when asked the question. The answers are case-sensitive.

To **delete a question**, place the cursor in the **Question** field on the line containing the question and delete the contents of the line.

When you have finished deleting the question, press **Enter**. The cursor moves to the **Answer** field for that line.

If the answers are not visible, press the **F5=DIsplay/Hide** key to display them.

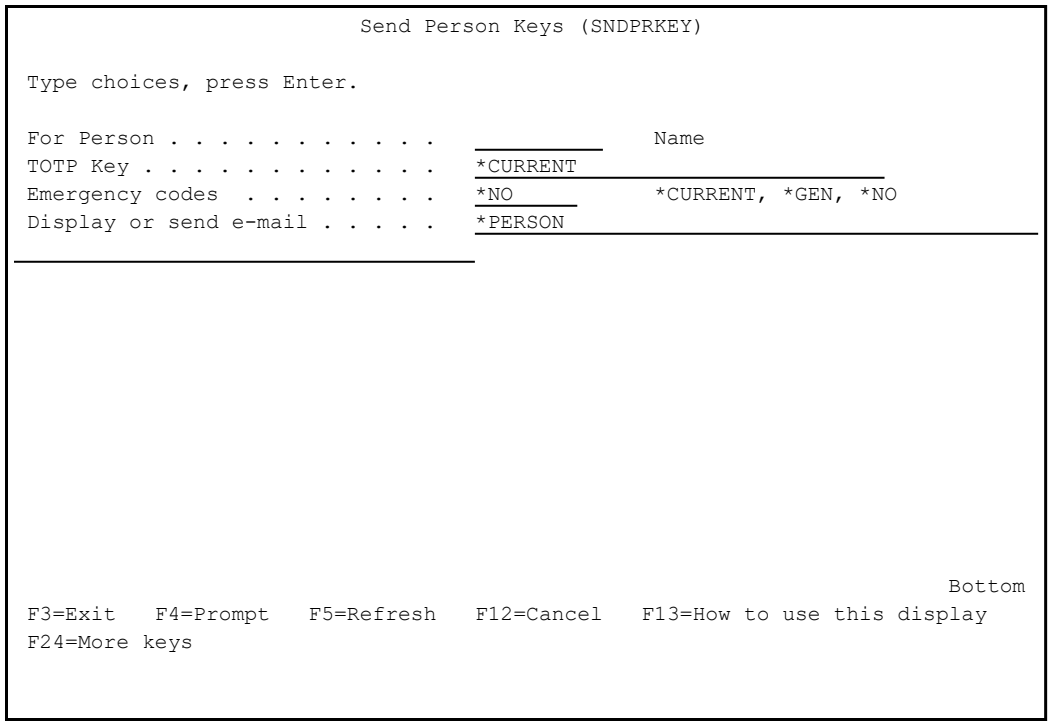
Delete the answer to the question.

Each Person must have at least as many questions as the system asks during the Password Reset process. The Person's Role determines the number of questions, as set on the **Modify Class** screen (shown in "Modifying Classes" on page 36).

When you have finished entering or modifying questions, press **Enter**.

Sending Keys for a Person

To send keys for a person, select **`12. Send Person Keys`** from the Persons menu (*Password Reset* > **`1`**). The Send Person Keys (SNDPRKEY) screen appears:



The screen contains these fields:

`For Person`

The name of the Person for whom the keys are being sent.

`TOTP Key`

Which TOTP (Temporary One-Time Password) key to send for the Person. Values include:

`*CURRENT`

The Person's current TOTP key.

`*GEN`

Generate a new TOTP key.

`*NO`

Do not send a TOTP key.

Emergency Codes

Which emergency codes to send for the Person. Values include:

***CURRENT**

The Person's currentemergency codes.

***GEN**

Generate new emergency codes.

***NO**

Do not send emergency codes.

Display or send email

How to transmit the key. Values include:

***PERSON**

Send email to the Person.

***DSPTXT**

Display the key as text.

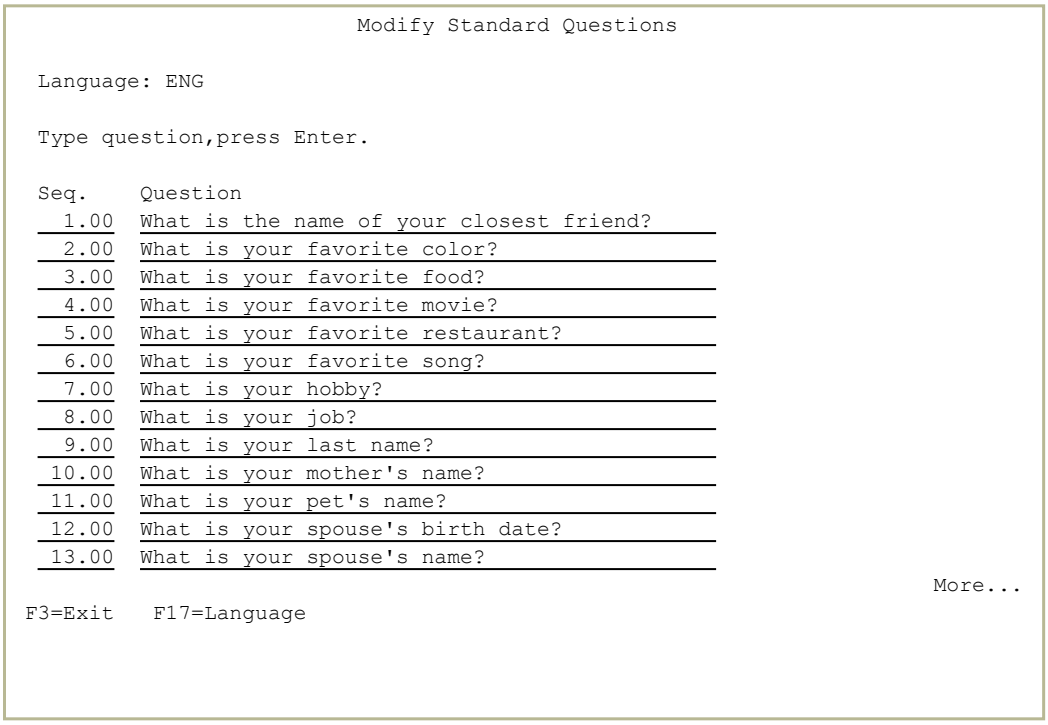
***DSPQR**

Display the QR code for the key in a browser.

Standard Questions

In resetting passwords, Password Reset asks users a set of personal questions to which they had supplied answers earlier. Users can create their own questions or select them from a list of suggested standard questions that you can define for your system in their language.

To work with standard questions, select **15. Suggested Private Questions** from the Definitions screen (*STRPWDRST* **> 21**). The Modify Standard Questions screen appears.



```
                          Modify Standard Questions

 Language: ENG

 Type question,press Enter.

 Seq.    Question
   1.00  What is the name of your closest friend?
   2.00  What is your favorite color?
   3.00  What is your favorite food?
   4.00  What is your favorite movie?
   5.00  What is your favorite restaurant?
   6.00  What is your favorite song?
   7.00  What is your hobby?
   8.00  What is your job?
   9.00  What is your last name?
  10.00  What is your mother's name?
  11.00  What is your pet's name?
  12.00  What is your spouse's birth date?
  13.00  What is your spouse's name?
                                                                      More...
F3=Exit    F17=Language
```

The screen lists the standard questions for the language shown in the **Language:** field.

You can change, replace, or remove questions already on the list, or add questions at the end.

For each question, the screen shows two fields.

The **Seq.(Sequence)** field determines the order in which Password Reset suggests the questions to the user. These do not have to be integers, or to appear on this screen in that order. For example, a question with the

Seq. value of **4.50** would be shown to the user between questions numbered **4.00** and **5.00**.

The **Question** field holds the question itself.

To change a question, edit the question as it appears in its **Question** field.

To replace a question, type a new question in the **Question** field for the old question.

To remove a question, erase its entries in both the **Question** and **Seq.** fields.

To change to a different language or to copy questions from one language to another, press the F17=Language key. (On keyboards with only twelve function keys, press the Shift+F5 keys.) The Work with Standard Questions screen appears.

To define a particular person's private questions for Password Reset, enter **7** in the **Opt** field for the person on the Work with Persons screen (*STRPWDRST* **> 1 > 1**). The Modify Person Identification Questions screen appears, as shown in "Managing Private Questions for a Person" on page 55.

Languages

In Password Reset, you can set the interface to appear in different languages for different users. This includes the text onscreen, the questions that the user is asked, and the messages sent via email or SMS.

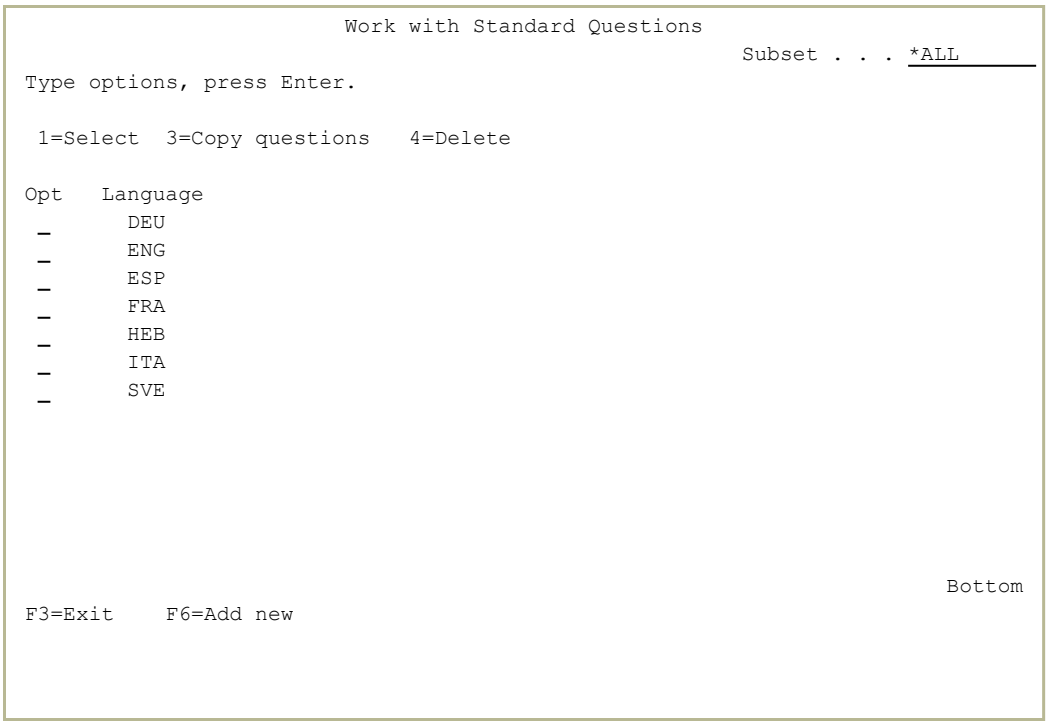
You can work with different languages for:

- Standard Questions (shown in "Working with Different Languages for Standard Questions" on the next page)
- Email and SMS Text (shown in "Working with Email and SMS Text" on page 70)
- Screen Text (shown in "Working with Screen Text" on page 64)

Working with Different Languages for Standard Questions

In resetting passwords, Password Reset asks users a set of personal questions to which they had supplied answers earlier. Users can create their own questions or select them from a list of suggested standard questions that you can define for your system in their language.

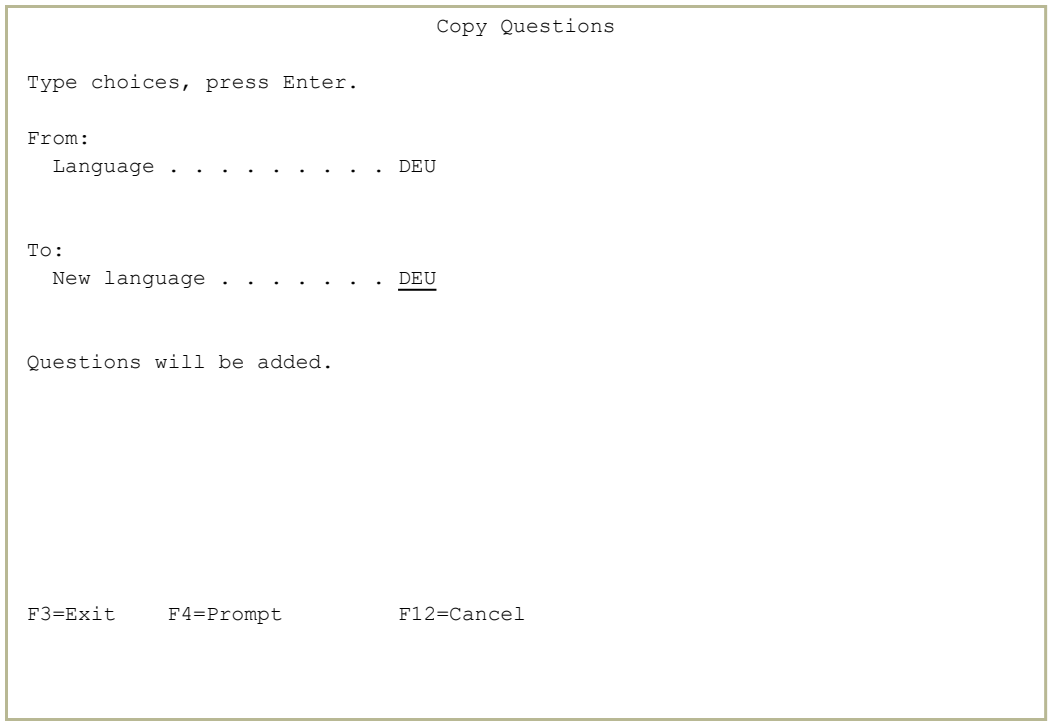
To **change to a different language** or to **copy questions from one language to another**, press the **F17=Language** key from the **Modify Standard Questions** screen (shown in "Standard Questions" on page 59). (On keyboards with only twelve function keys, press the **Shift+F5** keys.) The **Work with Standard Questions** screen appears.



To **change the language in which you are working**, type the digit **1** in the **Opt** field for that language, then press Enter. The **Modify Standard Questions** screen returns with the questions in the selected language.

To **delete the questions for a language**, type the digit **4** in the **Opt** field for that language, then press **Enter**.

To **copy questions to a new language** (if, for example, you want to write question in a second language similar to the first), type the digit **3** in the **Opt** field for the original language, then press **Enter**. The **Copy Questions** screen appears.



Enter the three-letter code for the new language in the **New language** field. To select from a list of available languages, press the **F4=Prompt** key.

Press the **F3=Exit** key to return to the **Modify Standard Questions** screen. The questions for the new language appear in the list.

Working with Screen Text

Each piece of text seen onscreen within Password Reset can be found and changed from the **Work with Screen Text** screen.

To reach that screen, select **`31. Screen Text Translation`** from the **Definitions** screen (*STRPWDRST* **`> 21`**).

```
                          Work with Screen Text
Use this screen to translate text that a user may see. If a screen translation
is missing, the English (ENG) default text will be used.
                                                    Language: FRA   F4=List
Type options, press Enter.                          Screen  : __________
 1=Select  3=Copy                                   Record  : __________
Opt  Lng  Screen      Record      Text
 _   FRA  ATTRIBUTES  WEB         PR-Web field texts
 _   FRA  CHANGEPWD   WEB         PR Change PWD texts for WEB
 _   FRA  PERSONATR   WEB         PR Get person attributes information tex
 _   FRA  PRIQSTFM    CMDLIN      PR-Initial Procedure Questions
 _   FRA  PRIQSTFM    REJECT      PR-Initial Procedure Questions
 _   FRA  PRIQSTFM    REJECT3     PR Password Reset verification
 _   FRA  PRIQSTFM    SFLINC      PR-Initial Procedure Questions
 _   FRA  PRPRVWFM    ALLOPT      PR-Initial Procedure Questions
 _   FRA  PRPRVWFM    ALLOPT2     PR-Initial Procedure Questions
 _   FRA  PRPRVWFM    CMDLIN      PR-Initial Procedure Questions
 _   FRA  PRPRVWFM    CPYUSR      PR-Initial Procedure Questions
 _   FRA  PRPRVWFM    DELLIN      PR User Provisioning
                                                                    More...

F3=Exit   F6=Add New Lang.   F7=Copy Lang.   F9=Delete Lang.   F12=Cancel
```

Each line of the main screen refers to a collection in a particular language of text strings from other screens within Password Reset.

For each collection, it shows:

- **`Lng`**: The three-character code for the language
- **`Screen`**: The name of the screen file containing these strings
- **Record**: The name of the record within the file containing these strings
- **`Text`**: A free description of the collection.

You can **search for a specific collection of texts** using the **`Language`**, **`Screen`**, and **Record** fields at the top right of the screen. To select from a list of known languages, place the cursor in the **`Language`** field and press the **F4=List** key.

To **add a new language**, press the **F6=Add New Lang.** key. The **Add Screen Texts** screen (shown in "Adding Screen Text Languages" on the next page) appears.

To **delete a language**, press the **F9=Delete Lang.** key. The **Delete Screen Texts screen** (shown in "Deleting Screen Text Languages" on page 67) appears.

To **copy texts from one language to another**, press the **F7=Copy Lang.** key. The **Copy All Screen Texts** screen (shown in "Copying Screen Texts Between Languages" on page 68) appears.

To **copy one collection of text strings to another language or record**, type the digit **1** in the **Opt** field for that collection and press the **Enter** key. The**Copy One Screen Texts** (shown in "Copying One Screen's Texts" on page 69) screen appears.

Adding Screen Text Languages

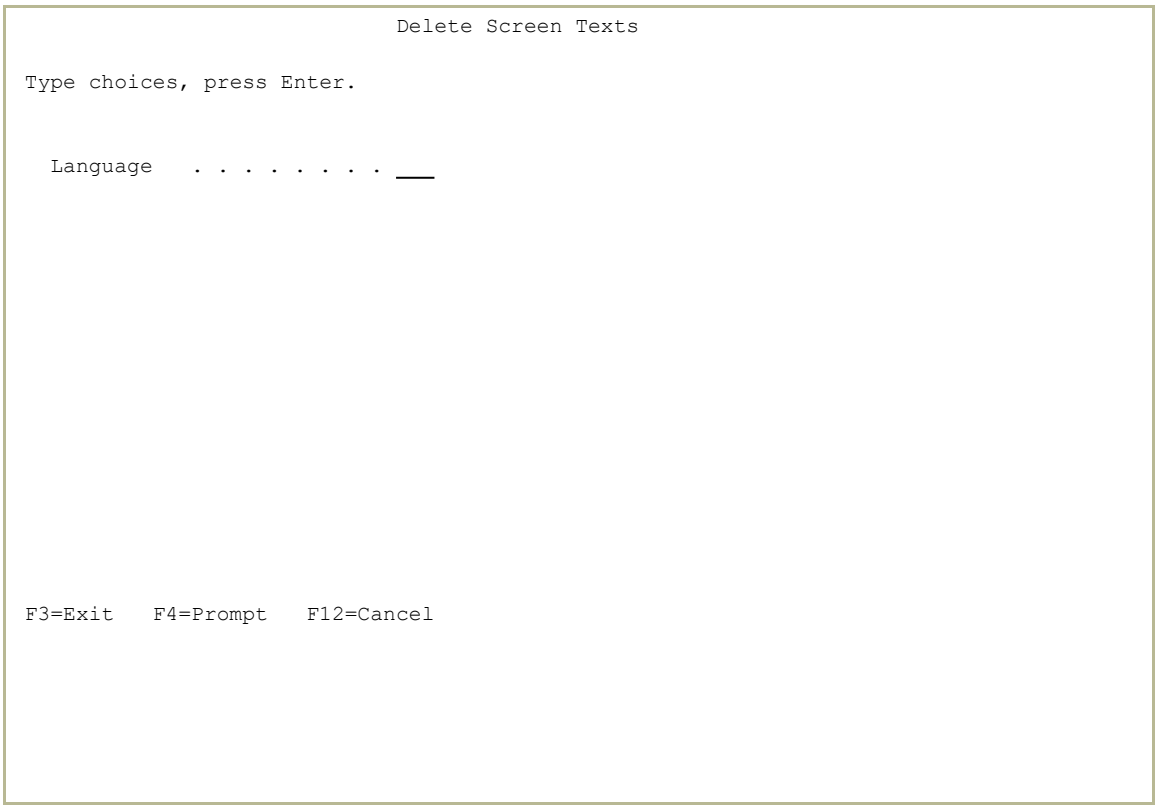
To **add a new language**, press the **F6=Add New Lang.** key from the **Work with Screen Text** screen (shown in "Working with Screen Text" on page 64). The **Add Screen Texts** screen appears.

To **add a new language**, type the three-character identifier for the language in the New language field then press **Enter**.

To **select from a list of known languages**, press the **F4=Prompt** key.

Deleting Screen Text Languages

To **delete the screen texts for a language**, press the **F9=Delete Lang.** key from the **Work with Screen Text** screen (shown in "Working with Screen Text" on page 64). The **Delete Screen Texts** screen appears.



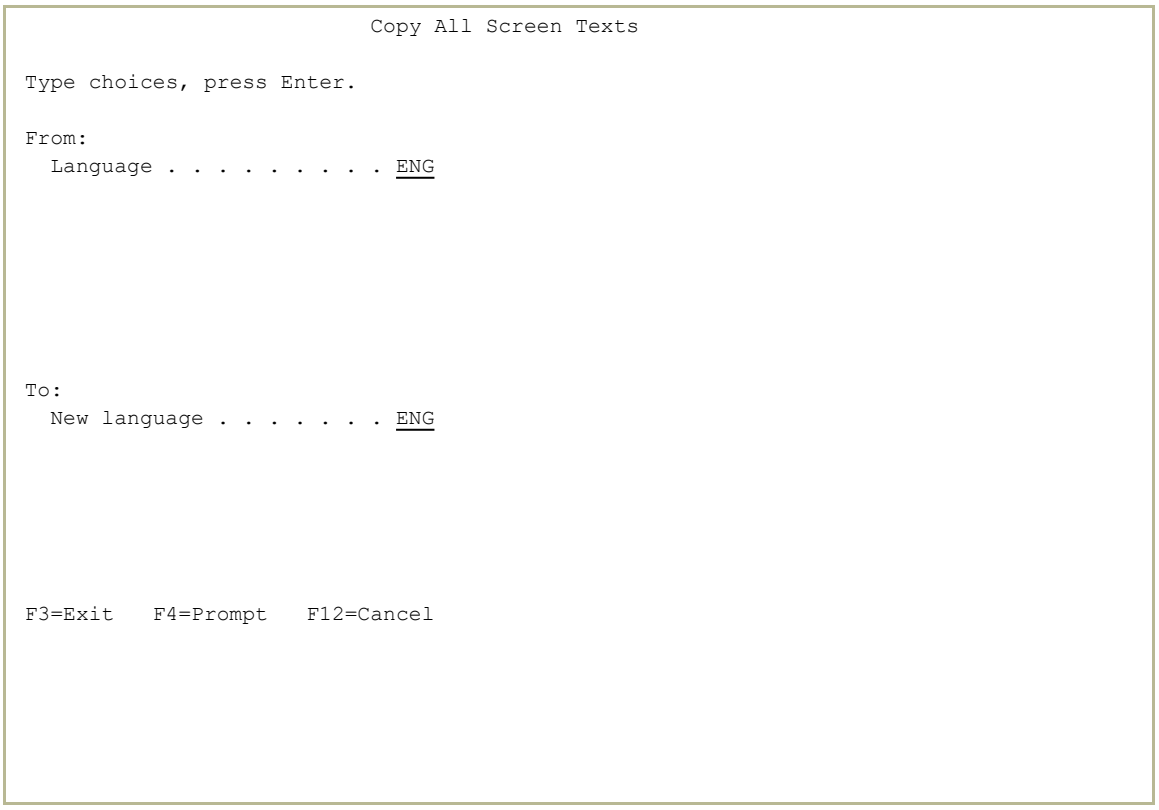
To **delete a language**, type the three-character identifier for the language in the Language field then press **Enter**. To select from a list of known languages, press the **F4=Prompt** key.

A user set to the deleted language will see the default English-language texts.

The Work with Screen Text screen reappears.

Copying Screen Texts Between Languages

To **copy texts from one language to another**, press the **F7=Copy Lang.** key from the **Work with Screen Text** screen (shown in "Working with Screen Text" on page 64). The **Copy All Screen Texts** screen appears.



The screen includes two fields.

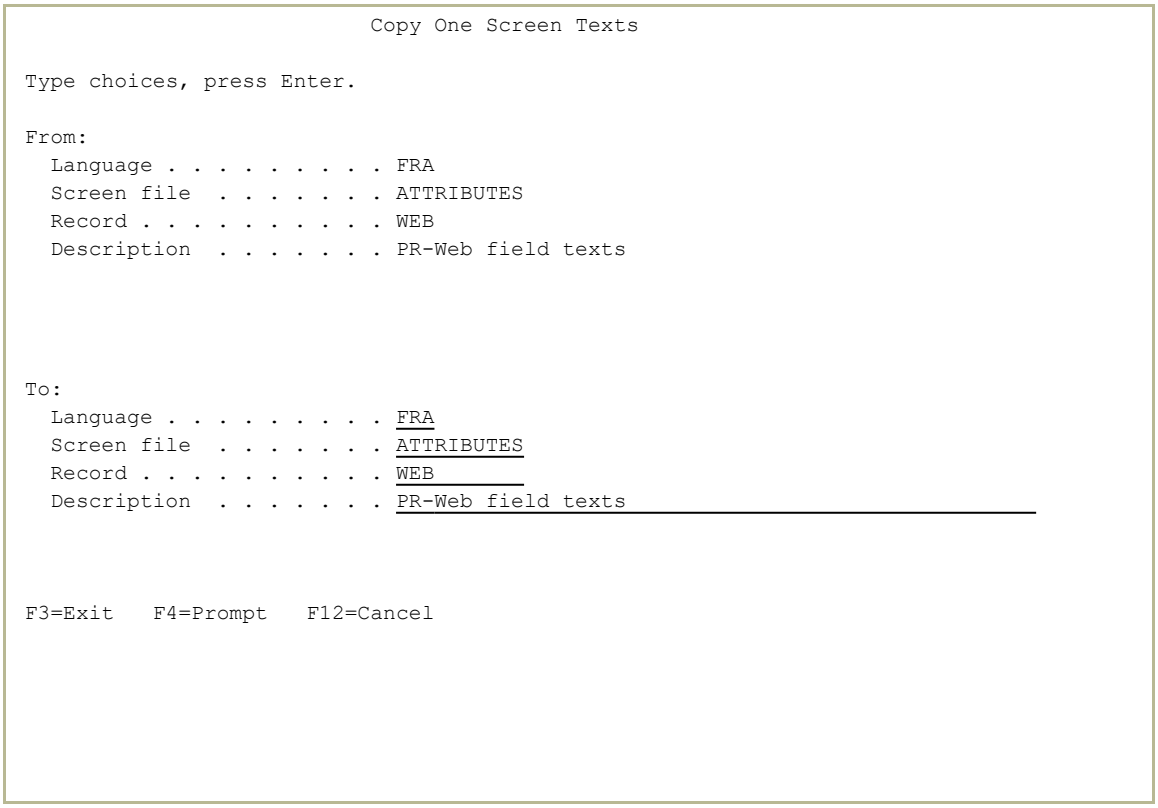
To indicate the language **from** which you are copying the texts, type the three-character identifier for the language in the **Language** field. To select from a list of known languages, press the **F4=Prompt** key.

To indicate the language **to** which you are copying the texts, type the three-character identifier for the language in the **New Language** field. To select from a list of known languages, press the **F4=Prompt** key.

To copy the texts, press the **Enter** key or the **F3=Exit** key. The Work with Screen Text screen reappears.

Copying One Screen's Texts

To **copy one collection of text strings to another language or record**, type the digit **3** in the Opt field for that collection on the **Work with Screen Text** (shown in "Working with Screen Text" on page 64) screen and press **Enter**. The **Copy One Screen Texts** screen appears.



The screen contains two sets of fields, labeled **From:** and **To:**, respectively. Each set contains the fields:

- **Language**: The three-character code for the language. To select from a list of known languages, place the cursor in this field and press the **F4=Prompt** key.
- **Screen File**: The name of the screen file containing these strings
- **Record**: The name of the record within the file containing these strings
- **Description**: A free description of the collection.

Enter the values for the collections from which and to which you want to copy the text strings. To copy the texts, press **Enter** or the **F3=Exit key**. The Work with Screen Text screen reappears.

Working with Email and SMS Text

Password Reset can display different texts in the emal and SMS messages that it sends, depending on the user's language preference. The messages can contain the current values of relevant variables, represented by placeholders in the message text.

To **work with these messages**, select `1. Email/SMS Text` from the **Definitions** screen (*STRPWDRST* > 21). The **Work with Email/SMS Text** screen appears.

```
                        Work with Email/SMS Text
                                                Subset Lang. FRA     F4=List
Type options, press Enter.                        Text . . . *ALL
 1=Select  3=Copy  4=Delete

Opt  MsgID   Target   Description
 _     01     EMAIL    Enable subject
 _     01     SMS      Enable subject
 _     02     EMAIL    Enable text
 _     02     SMS      Enable text
 _     03     EMAIL    Information about use of P-R. Subject.
 _     03     SMS      Information about use of P-R. Subject.
 _     04     EMAIL    Information about use of P-R. Text.
 _     04     SMS      Information about use of P-R. Text.
 _     05     EMAIL    Additional text at the end.
 _     05     SMS      Additional text at the end.
 _     06     EMAIL    Password expiration text.
 _     06     SMS      Password expiration text.
 _     07     EMAIL    Password message subject.
 _     07     SMS      Password message subject.
                                                                      More...
F3=Exit   F6=Add new   F11=Un/Fold   F17=Language
```

The **`Subset Lang.`** field at the top of screen shows the language with which you are currently working. To change languages, enter the three-letter abbreviation for the new language in that field. To select the language from a list, press the **F17=Language(Shift+F5)** key or place the cursor in that field and press the **F4=List** key.

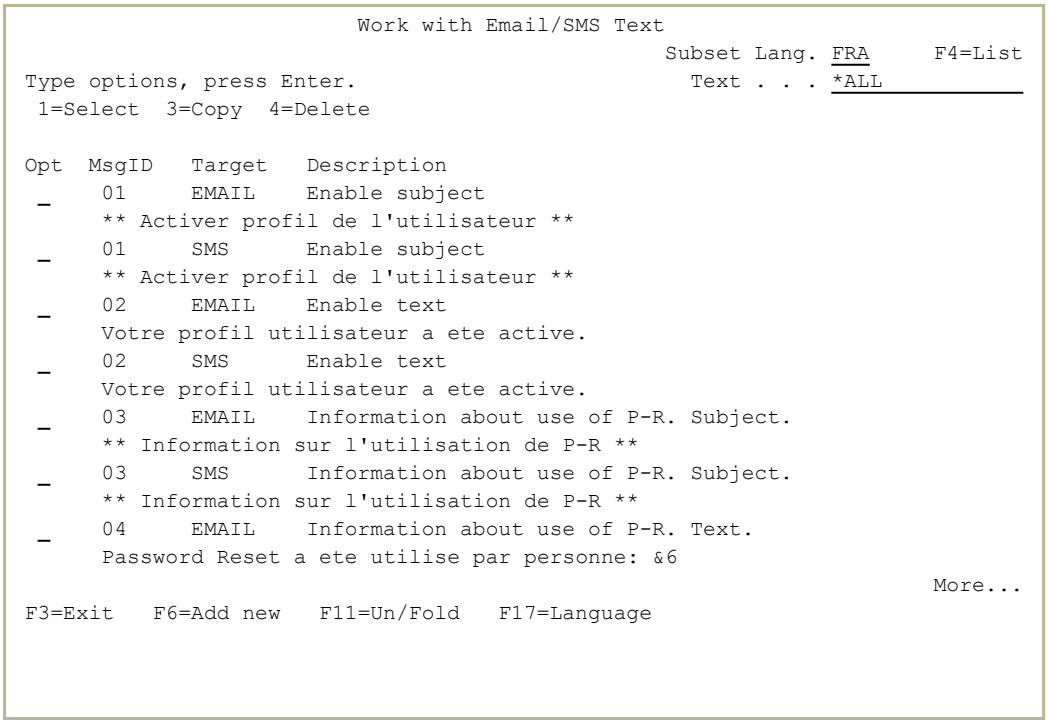
For each message, the screen shows

- a numeric **`MsgID`**
- a **`Target`** field showing whether the message is for Email, SMS, or Screen, and
- a **`Description`**.

The messages are

1. Enable subject
2. Enable text
3. Information about the use of Password Reset. Subject
4. Information about the use of Password Reset. Text.
5. Additional text at the end.
6. Password expiration text.
7. Password message text.
8. Password message text.
9. Verification subject.
10. Verification code text.
11. Left part of verification message.
12. Right part of verification code.

To **see the messages for the current language**, press the **F11=Un/Fold** key. Each message appears below its description. Pressing the **F11** key again hides the message text.



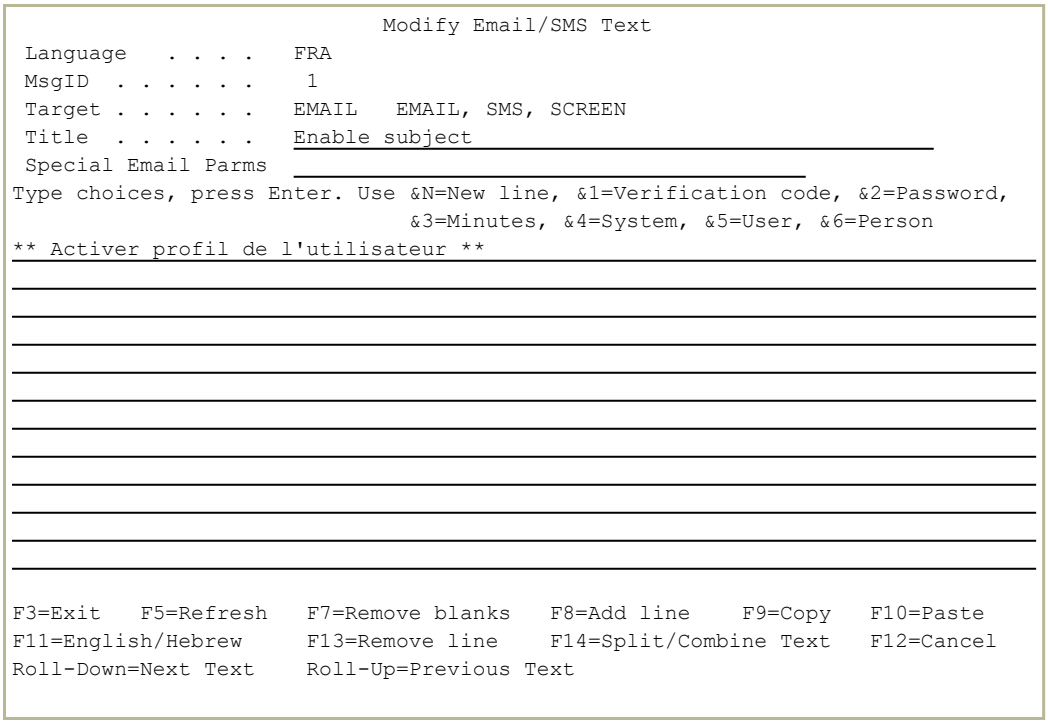
To **modify a message**, type the digit **1** in the **Opt** field for that message and press **Enter**. The**Modify Email/SMS Text** screen (shown in "Modifying Email and SMS Text" on page 73) appears.

To **copy a message from one language, message type, or target to another**, type the digit **3** in the **Opt** field for that message and press the **Enter** key. The **Copy Email/SMS Text** screen (shown in "Copying Email and SMS Text" on page 75) appears.

Modifying Email and SMS Text

Password Reset can display different texts in the emal and SMS messages that it sends, depending on the user's language preference. The messages can contain the current values of relevant variables, represented by placeholders in the message text.

To **modify a message**, type the digit **1** in the **Opt** field for that message on the **Work with Email/SMS Text** screen (shown in "Working with Email and SMS Text" on page 70) and press **Enter**. The **Modify Email/SMS Text** screen appears.



The four fields at the top of the screen correspond to fields on the previous screen:

- **Language**: The language of the current message
- **MsgID**: The message ID for that type of message
- **Target**: Whether the message is used for EMAIL, SMS, or SCREEN
- **Title**: The type of message

The remaining blank lines on the screen are for the message itself. Most of these will usually be empty. The current message begins on the first line.

To **modify the text on a line**, type over it.

To **revert to the previous text**, press the **F5=Refresh** key.

To **remove a line**, place the cursor on that line and type to **F13=Remove Line (Shift+F1)** key. The contents of the lines below that line move up.

To **add a blank line**, place a cursor on the line above it and press the **F8=Add Line** key. The contents of that line and those below it move down by one line.

To **join the contents of a line with those of the line above it**, place the cursor after the last character on the upper line and press the **F14=Split/Combine(Shift+F2)** key. The contents of the lower line appear on the upper line, starting at the cursor position. Lines below that rise by one line.

To **split the contents of a line**, place the cursor on the character at which you want to split the line and press the **F14=Split/Combine(Shift+F2)** key. The contents of that line, beginning with the character at the cursor, move down to the start of the next line. The contents of the lines below it each move down by one line.

To **copy text**, select the text and press the **F9=Copy** key.

To **paste text copied from another screen**, place the curson at the point that you want to paste it and press the **F10=Paste** key.

To **toggle between Left-to-Right text entry** (for languages such as English and French) and Right-to-Left entry (for languages such as Arabic and Hebrew), press the **F11=English/Hebrew** key.

To **save your changes and move to the next message**, press the **PageDown** key.

To **save your changes and move to the previous message**, press the **PageUp** key.

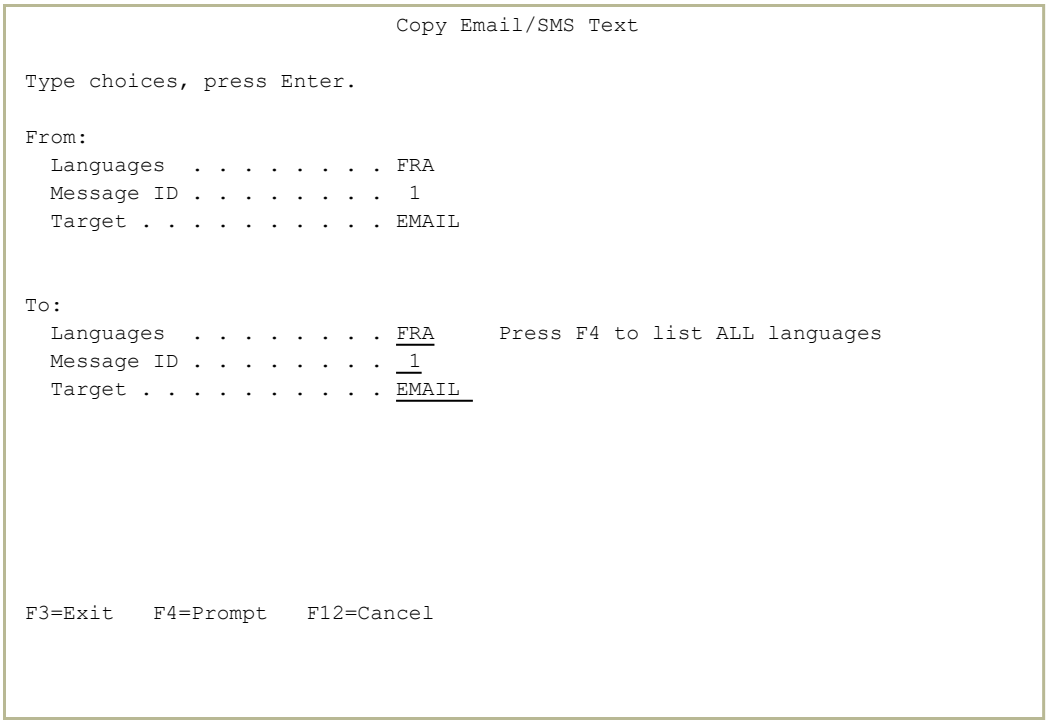
To **cancel your changes**, press the **F12=Cancel** key. The changes are discarded and the **Work with Email/SMS Text** screen reappears.

To **complete your changes**, press the **F3=Exit** key. The changes are saved and the **Work with Email/SMS Text** screen reappears.

Copying Email and SMS Text

Password Reset can display different texts in the email and SMS messages that it sends, depending on the user's language preference. The messages can contain the current values of relevant variables, represented by placeholders in the message text.

To **copy a message from one language, message type, or target to another**, type the digit **3** in the **Opt** field for that message on the **Work with Email/SMS Text** screen (shown in "Working with Email and SMS Text" on page 70) and press **Enter**. The **Copy Email/SMS Text** screen appears.



The screen consists of two sets of fields, labeled **From:** and **To:**. Each has three subfields:

- **Languages**: The language of the message
- **Message ID**: The type of message.
- **Target**: Whether the message is intended for Email or SMS messages or onscreen.

The **Message ID** types are:

1. Enable subject
2. Enable text

3. Information about the use of Password Reset. Subject
4. Information about the use of Password Reset. Text.
5. Additional text at the end.
6. Password expiration text.
7. Password message text.
8. Password message text.
9. Verification subject.
10. Verification code text.
11. Left part of verification message.
12. Right part of verification code.

The **From:** values are read-only.

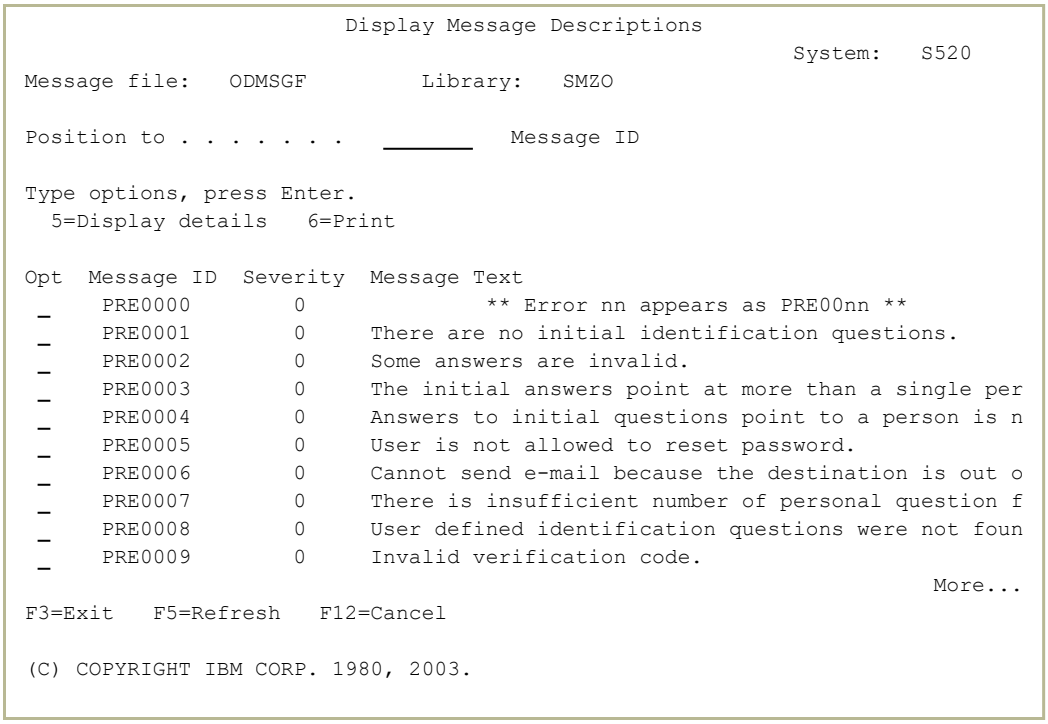
Change the **To:** values as needed. To see a list of available languages, place the cursor in the **To:** group's **Languages** field and press the F4=Prompt key.

When you have made the changes, press the Enter key. The Work with Email/SMS Textscreen reappears.

Displaying Error ID Descriptions

If a user encounters errors when attempting to reset a password, Password Reset may display a message containing an error ID code. The **Display Message Descriptions**screen can assist the Helpdesk in understanding these codes.

To **display these message descriptions**, select **`31. Display List`** in the **Password Reset** main menu. The **Display Message Descriptions** screen appears.



```
                        Display Message Descriptions
                                                              System:   S520
Message file:   ODMSGF         Library:   SMZO

Position to . . . . . .   _______   Message ID

Type options, press Enter.
  5=Display details   6=Print

Opt  Message ID  Severity  Message Text
 _     PRE0000        0              ** Error nn appears as PRE00nn **
 _     PRE0001        0     There are no initial identification questions.
 _     PRE0002        0     Some answers are invalid.
 _     PRE0003        0     The initial answers point at more than a single per
 _     PRE0004        0     Answers to initial questions point to a person is n
 _     PRE0005        0     User is not allowed to reset password.
 _     PRE0006        0     Cannot send e-mail because the destination is out o
 _     PRE0007        0     There is insufficient number of personal question f
 _     PRE0008        0     User defined identification questions were not foun
 _     PRE0009        0     Invalid verification code.
                                                                        More...
F3=Exit   F5=Refresh   F12=Cancel

(C) COPYRIGHT IBM CORP. 1980, 2003.
```

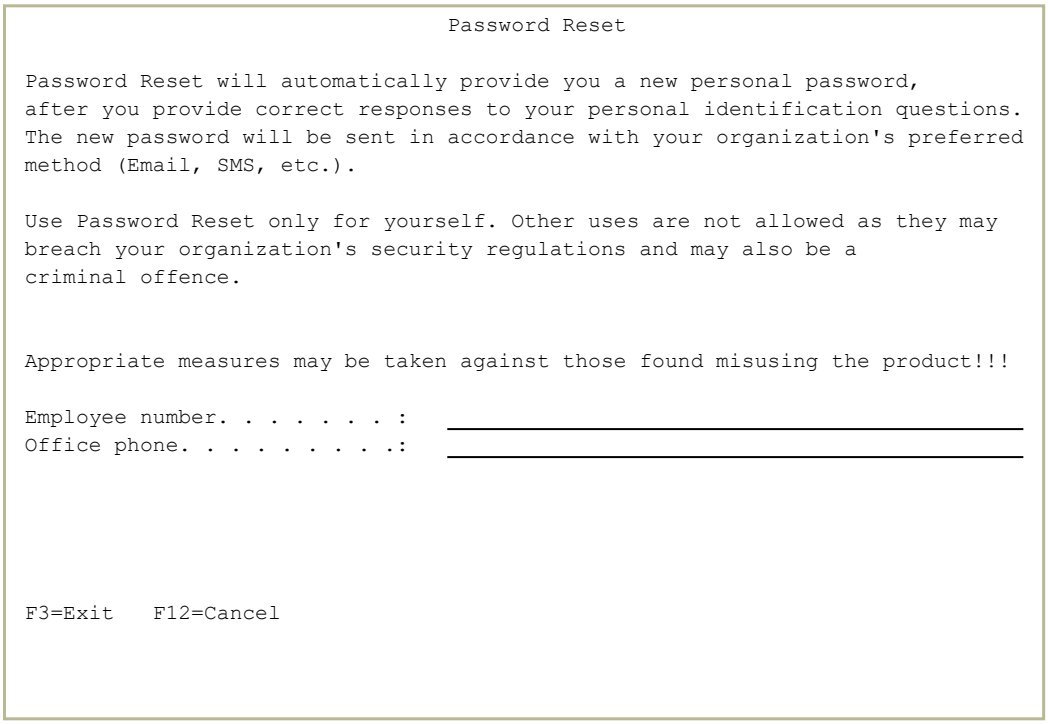
To **scroll to a specific error**, enter the error ID in the **`Position to`** field.

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

Testing Password Reset

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

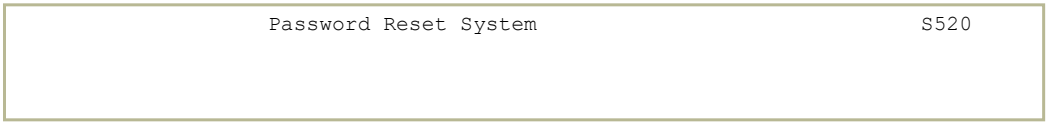
To test password reset, select **61. Test Password Reset** from the main menu. The **Password Reset** screen appears.



Password Reset asks questions from the set defined on the **Initial Questions** screen (shown in "Setting Initial Process Questions" on page 28).

Enter the answers that you set earlier for that user name via the **Modify Questions** screen (shown in "Managing Private Questions for a Person" on page 55).

If the information is correct, a screen appears, telling you that a verification string has been sent by email or SMS and prompting you to enter the code once it is received.



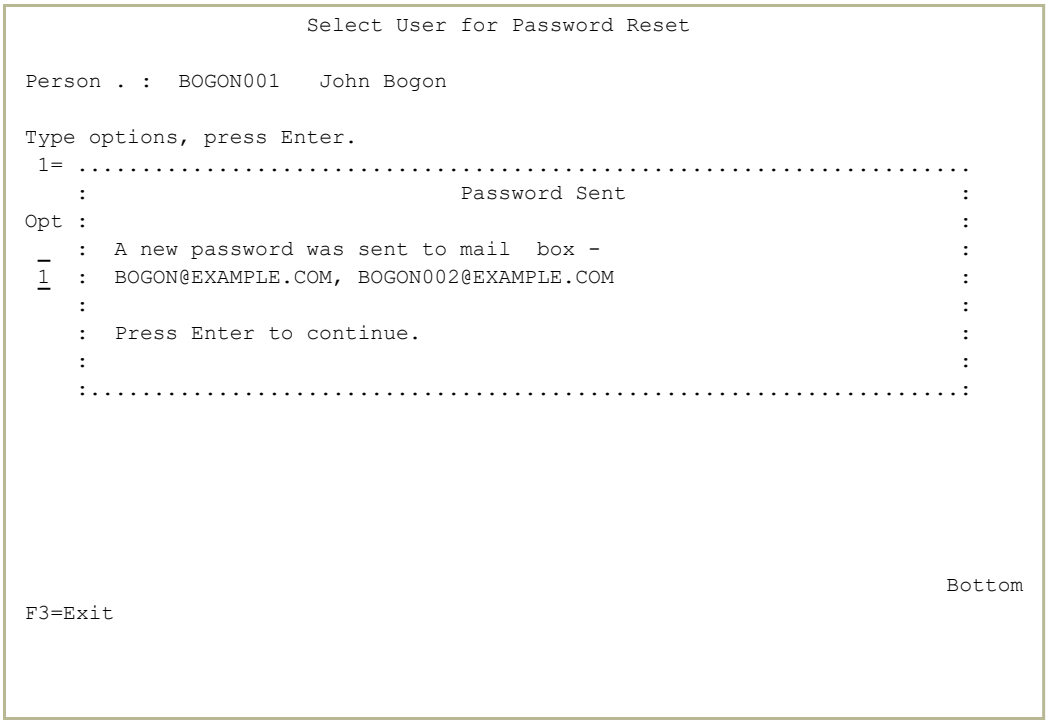
```
Your user. . : BOGON001
Date & Time. : 31/03/19 15:31:08

An E-mail has been sent to you, containing a verification code.
Please copy the verification string from message to the field below.

Verification code. .:  ______
Copy the verification code from message, press Enter.

F3=Exit
```

If you enter the code correctly, the **Select User for Password Reset** screen appears, showing a list of system users associated with that Person.

```
                      Select User for Password Reset

Person . :  BOGON001   John Bogon

Type options, press Enter.
 1=Select      (Select only ONE user from the list)

Opt  User               System
 _   DB          AS400  S520
 _   MUFIN       AS400  S520

                                                                  Bottom
F3=Exit
```

To select the user whose password you want to change, type the digit **1** in the **Opt** field for that user and press the **Enter** key.

A dialog appears confirming that Password Reset has sent the user a new, temporary password.



Log in again with that user name and the temporary password. A screen appears requiring you to set a new password. Press Enter to dismiss that message.

A second screen appears with which you can set a new password.

In the **Current password**field, type or paste the temporary password that you had received.

In the **New password** and **Repeat New Password** fields, enter a new password, which must meet your system's security standards, then press the Enter key.

Your password is set to the new value and the OS/400 Main Menu appears.

Resetting Your Password

With Password Reset, you can reset your password from either the native IBM i sign-on screen or through a web browser. You must have already set your questions and information for the reset process.

The procedures shown below are generic procedures which describe the general method of resetting a password both from the IBM 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 "Modifying Classes" on page 36 for more details.

- "Resetting Your Password from the Sign-On Screen" on the next page
- "Resetting Your Password from a Web Browser" on page 87

Resetting Your Password from the Sign-On Screen

You can reset your password from the native IBM i sign-on screen.

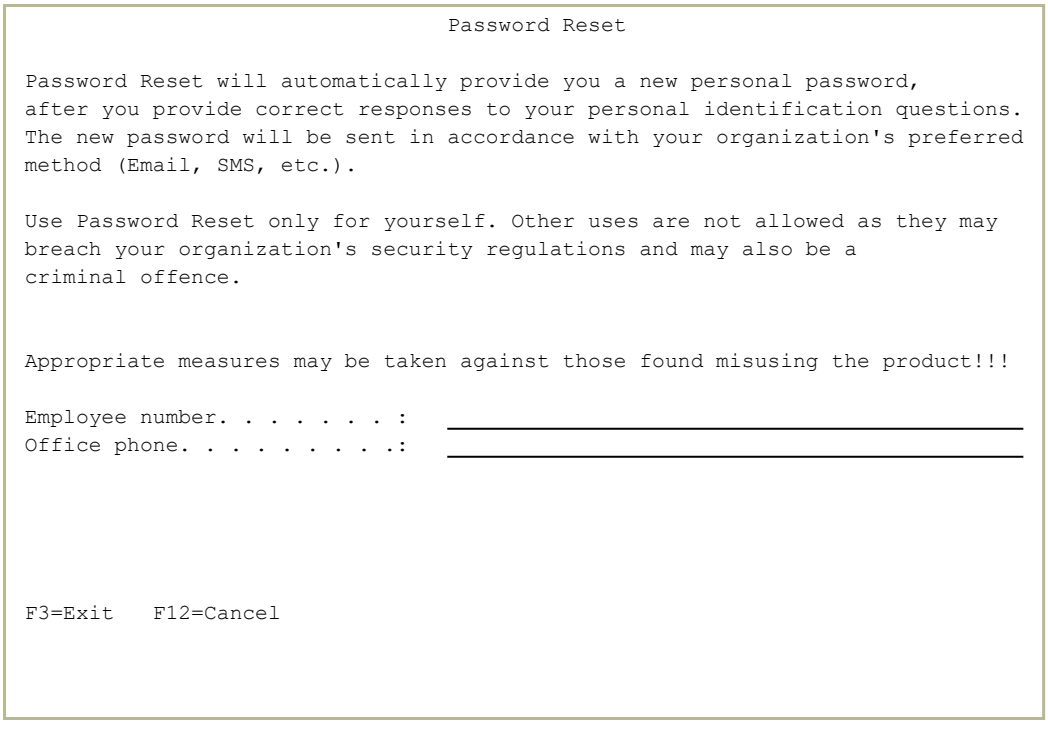
To work with Password Reset in **your system's default language**, log in as the user "FORGOT" and the password "PASSWORD".

To work with Password Reset in **another supported language**, log in as the user "FORGOTyyy" and the password "PASSWORD", where "yyy" represents the three-character code for your language. The languages include:

- **ARA**: Arabic
- **DEU**: German
- **ENG**: English
- **ESP**: Spanish
- **FRA**: French
- **HEB**: Hebrew
- **ITA**: Italian
- **SVE**: Swedish

For example, to work with Password Reset in Swedish, for example, you would log in as the user "FORGOTSVE".

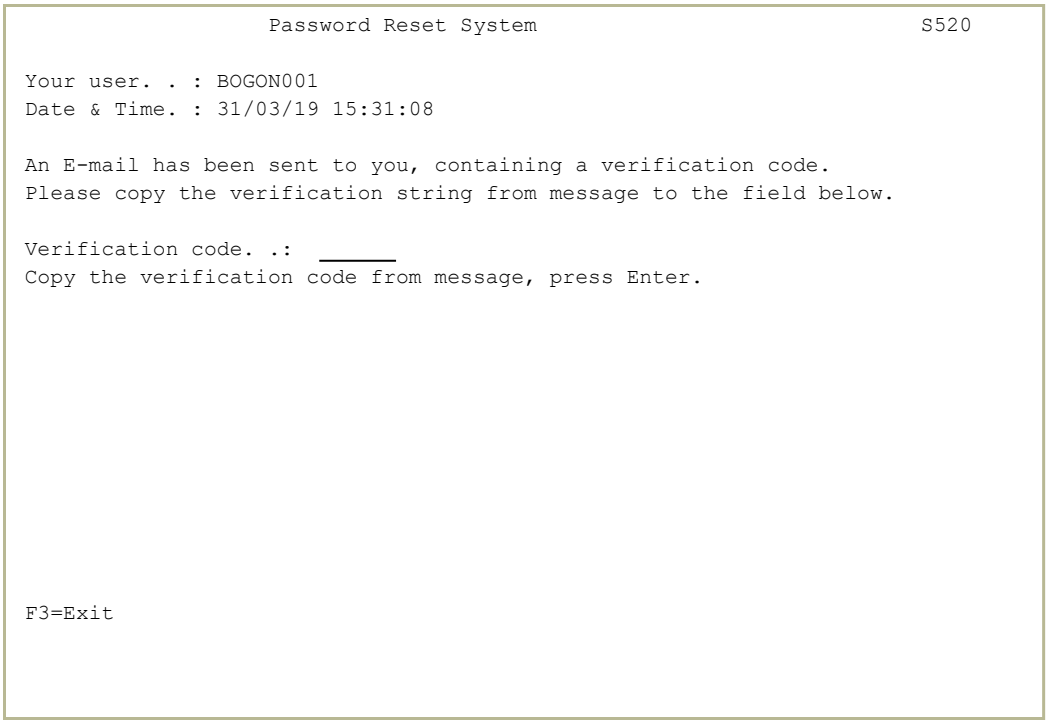
The**Password Reset** screen appears.



Password Reset asks questions from the set defined on the **Initial Questions** screen (shown in "Setting Initial Process Questions" on page 28).

Enter the answers that you set earlier for that user name via the **Modify Questions** screen (shown in Modifying a Person).

If the information is correct, a screen appears, telling you that a verification string has been sent by email or SMS and prompting you to enter the code once it is received.



If you enter the code correctly, a dialog appears confirming that Password Reset has sent you a new, temporary password.

Log in again with that user name and the temporary password. A screen appears requiring you to set a new password. Press Enter to dismiss that message.

A second screen appears with which you can set a new password.

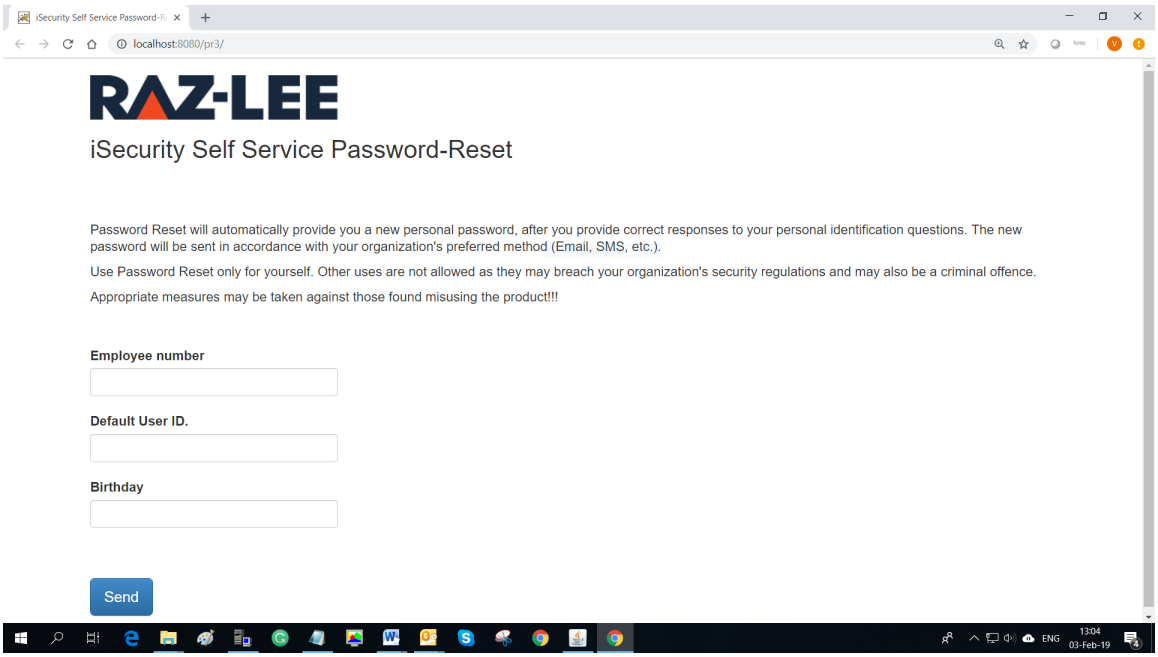
In the **Current password** field, type or paste the temporary password that you had received.

In the **New password** and **Repeat New Password** fields, enter a new password, which must meet your system's security standards, then press the Enter key.

Your password is set to the new value and the OS/400 Main Menu appears.

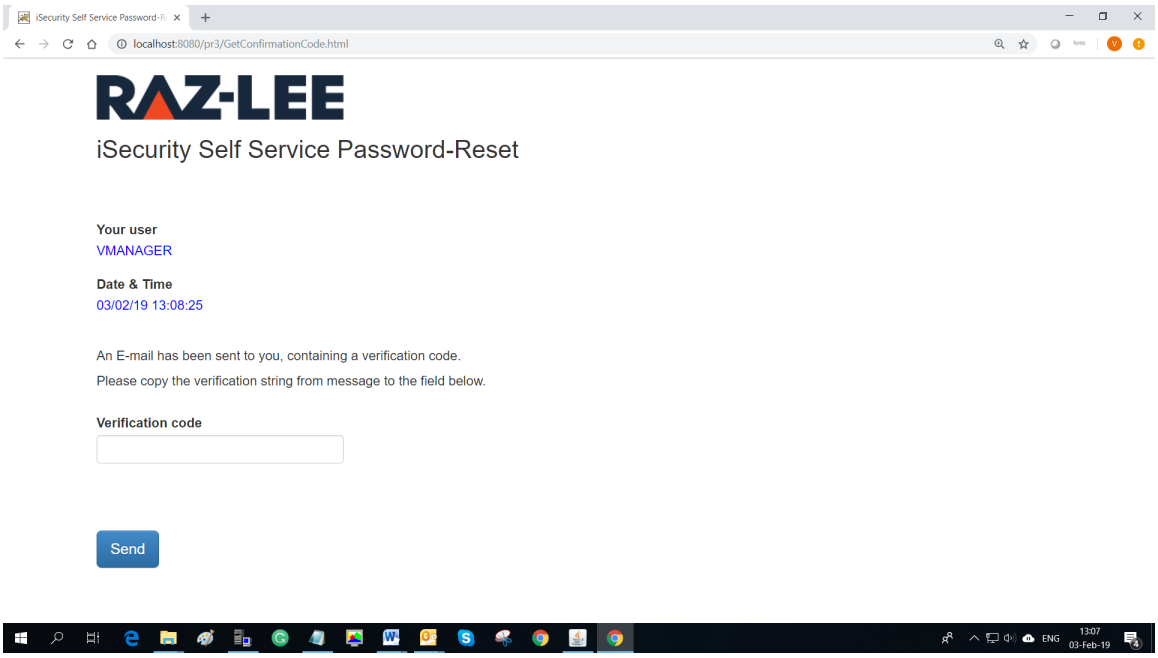
Resetting Your Password from a Web Browser

If your organization has set up their web server to support Password Reset, you can reset your password or re-enable a disabled password via a web browser. Ask your help desk for the web address to your Password Reset page.

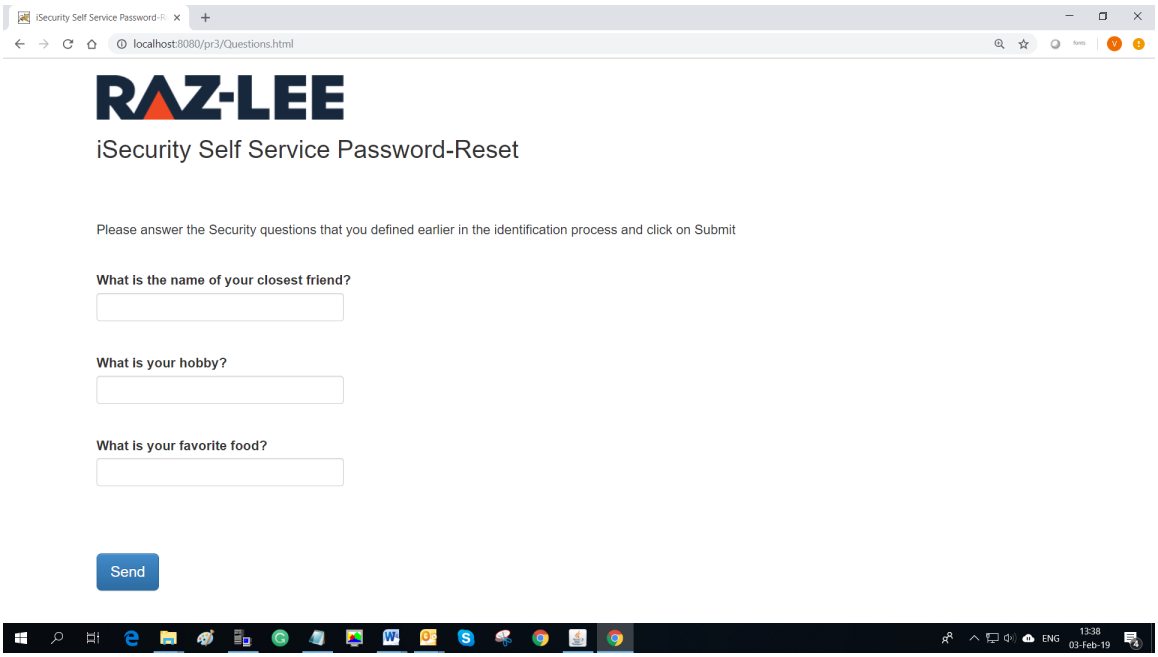


Enter the answers that you had set earlier via the **Modify Questions** screen (shown in Modifying a Person).

If the information is correct, a screen appears, telling you that a verification string has been sent by email or SMS and prompting you to enter the code once it is received.

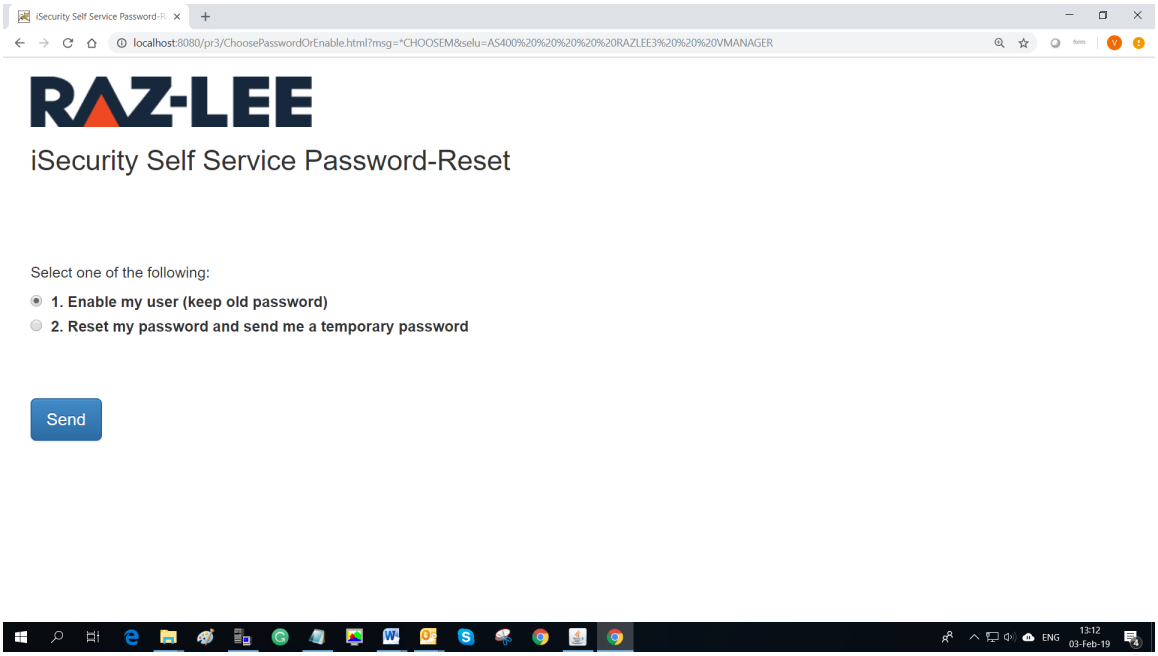


If you enter the verification code correctly, Password Reset displays a screen with some of the personal questions that you had supplied earlier:



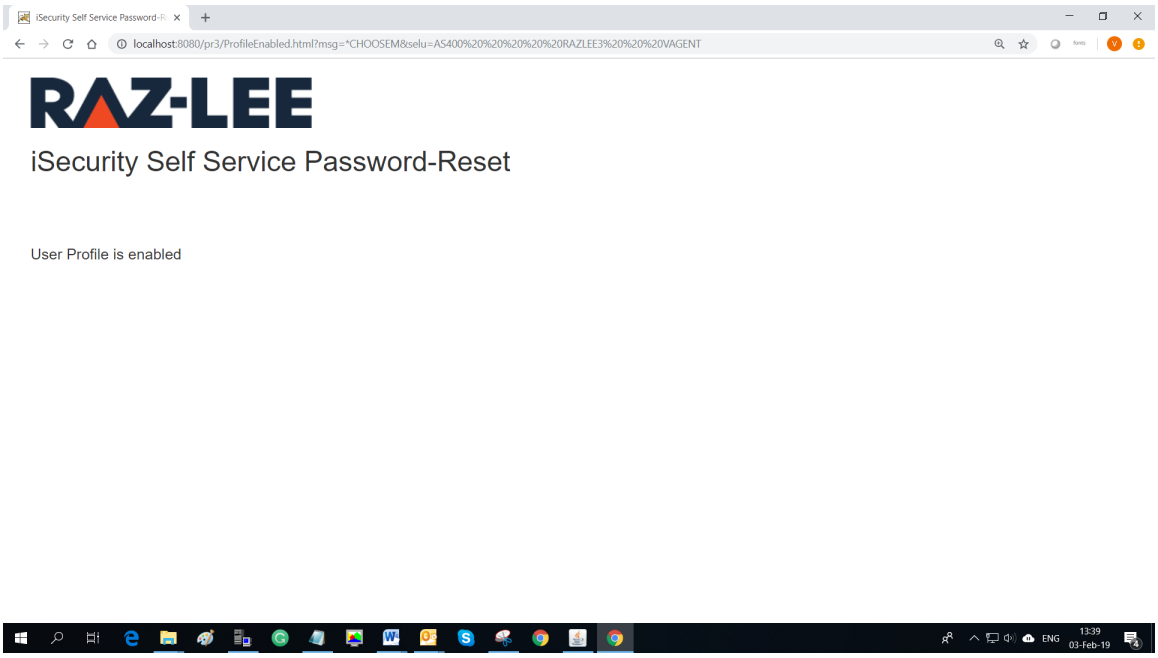
Enter the answers to the questions. The answers are case-sensitive and must match the answers that you had supplied earlier precisely.

Password Reset displays a screen asking whether you want to re-enable a disable password or set a new one.



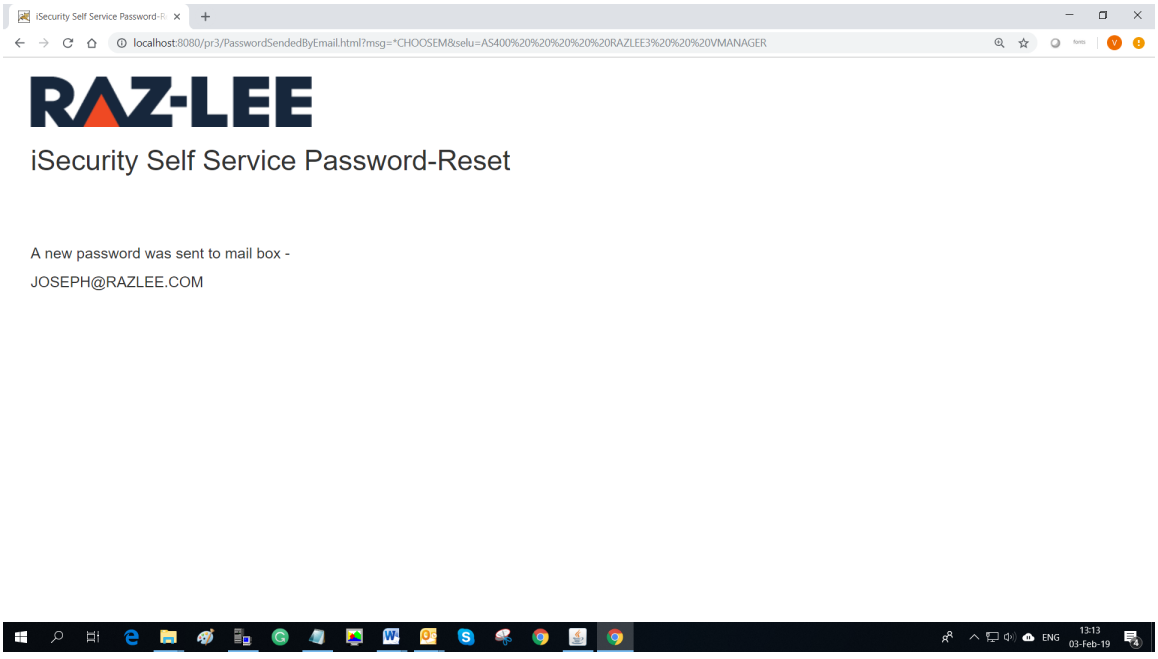
To re-enable a disabled password, click option **1** then the **Send** button.

Password Reset displays a screen confirming that your password has been re-enabled.



To reset your password once you have answered the personal questions correctly, click option **2** then the **Send** button.

Password Reset displays a screen confirming that it has sent a new password to you.



Log in to the IBM i with the new password that you have received.

Password Reset prompts you there to enter a new password, then changes your password to that value.

The Password Reset Web Interface

Password Reset can be used by either a web interface or a green screen interface. Both interfaces use the same definitions and have similar capabilities.

This document describes:

- Web interface installation and implementation
- Web interface capabilities and best practices

Web interface installation and implementation

The Password Reset Web Interface comes as a Java servlet. It can be run by any Servlet Container. A reasonable choice is Tomcat (but any other compatible web server will work as well). You can choose to run it on the IBM i or on any other platform.

The following describes how to install and use the Web interface with Tomcat as the server of choice and refers to its installation and usage on an IBM i.

Since IBM i release 6.1, Tomcat has not been part of OS400. It has to be installed by the client. The IBM document Running your IBM i web solution on ASF Tomcat is a good source of details about installation and deployment.

NOTE: During installation, you will be required to define a Manager-GUI Role, which is actually a user and password for the Tomcat manager.

Password Reset Web Customization

1. Copy the **/iSecurity/PRWEB/pr.war** file from the IFS to your PC.
2. Open the **pr.war** file. A **.war** file is similar to a **.zip** file. Opening the file presents a set of folders.
3. Modify the **/WEB-INF/web.xml** file.
4. To customize the interface:
    a. Replace the image file **/assets/img/logo.png** with the logo of your own brand
    b. Change the text font and size, logo size, and related parameters by editing the **/assets/img/style.css** file.
5. If the web server is not on the IBM i, edit these values in the **/WEB-INF/web.xml** file:
    a. Change the **IBMi-Name** value from LOCALHOST to the IP or host name
    b. Change the **IBMi-User** value from *CURRENT to the user name
    c. Change the **IBMi-Password** value from *CURRENT to the user password
6. Close the **pr.war** file.
7. If your web server is on the local IBM i, copy the **pr.war** file back to **/iSecurity/PRWEB/pr.war** . The **pr-bkp.war** file in that folder is a backup of the original **pr.war** file.
8. Start the Web server
9. If you web server is on the IBM i, enter the command **QSHELL** or **QSH** as a powerful user.
10. To start Tomcat, enter: /*Tomcat-installation-location*/**bin/star-tup.sh** (e.g. **/home/tomcat/apache-tomcat-7.0.28/bin/startup.s-h**)

Deploying

Access the Tomcat manager from a browser on your PC at **`http://`***your-IBM-i-IP-or-URL*`:8080/manager`.

Navigate to the location where the **`.war`** file exists and select Deploy.

By default, the WAR file is placed in the IBM i IFS at **`/iSecurity/PRWEB/pr.war`**

Web interface capabilities and best practices

To support web implementation, Password Reset provides an API with which you can:

- Check if the Password Reset system is available and the status of a user in the Password Reset system
- Obtaining a token for the duration of the process. This token hides the actual user identity.

A user web interface should perform on entry the following steps:

1. Identify the IBM i user profile.
2. Call the API with 'GETSTATUS'
3. If the answer is that there are missing attributes for the user in the Password Reset system, call the API with 'GETTOKEN'
4. Run the Password Reset Web using the Token

In addition, the organization portal may provide an option to enable the user to update his details at will.

The web application may ask the user to provide the details by running the Password Reset web interface at either of the following URLs:

To activate entry of person Attributes, run:

localhost:8080/pr/ChangeQuestions.html?screen_mode=attributes&token=XXXXXX

Note that this URL will automatically activate the following one after its entry has been satisfied.

To activate entry of personal questions, run:

localhost:8080/pr/ChangeQuestions.html?screen_mode=questions&token=XXXXXXX

Check status of user definition API - SMZO/PRIFEXSTR

Operation	10A (i)	'GETSTATUS', 'GETTOKEN'
Type	10A (i)	Should include ‘USER’
Value	10A (i)	Name of user
Return code	10A	See list below
Seconds	5A	Number of seconds that token is valid
NoOfUses	5A	Number of uses the token is valid
Token	10A	Token to call the process

A call with GETTOKEN disables any existing token for the specified user.

Possible Return codes are:

- General

OK	All is OK
NOTACTIVE	Password-Reset is not active (see option 81)
NOTALW	Password-Reset does not allow self-operations (see option 81)
ERROR	Any other error

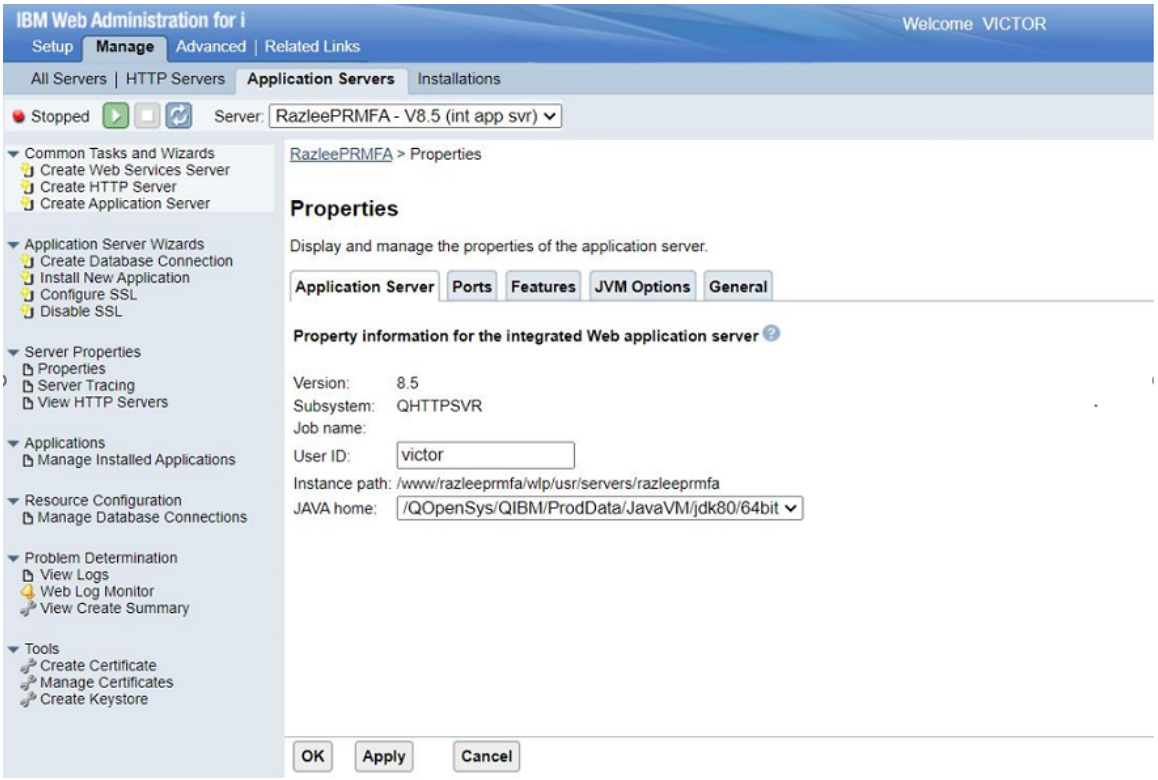
- For GETSTATUS

ERPARMUSER	Parameter Type does not contain 'USER'
NOATR	User specified does not exist in Password-Reset
NOQST	Missing question (as per needed: entirely or partially)
NOATR+WAIT	NOATR + Time is not convenient to ask for it now
NOQST+WAIT	MISQST + Time is not convenient to ask for it now is text and replace it with your own content.

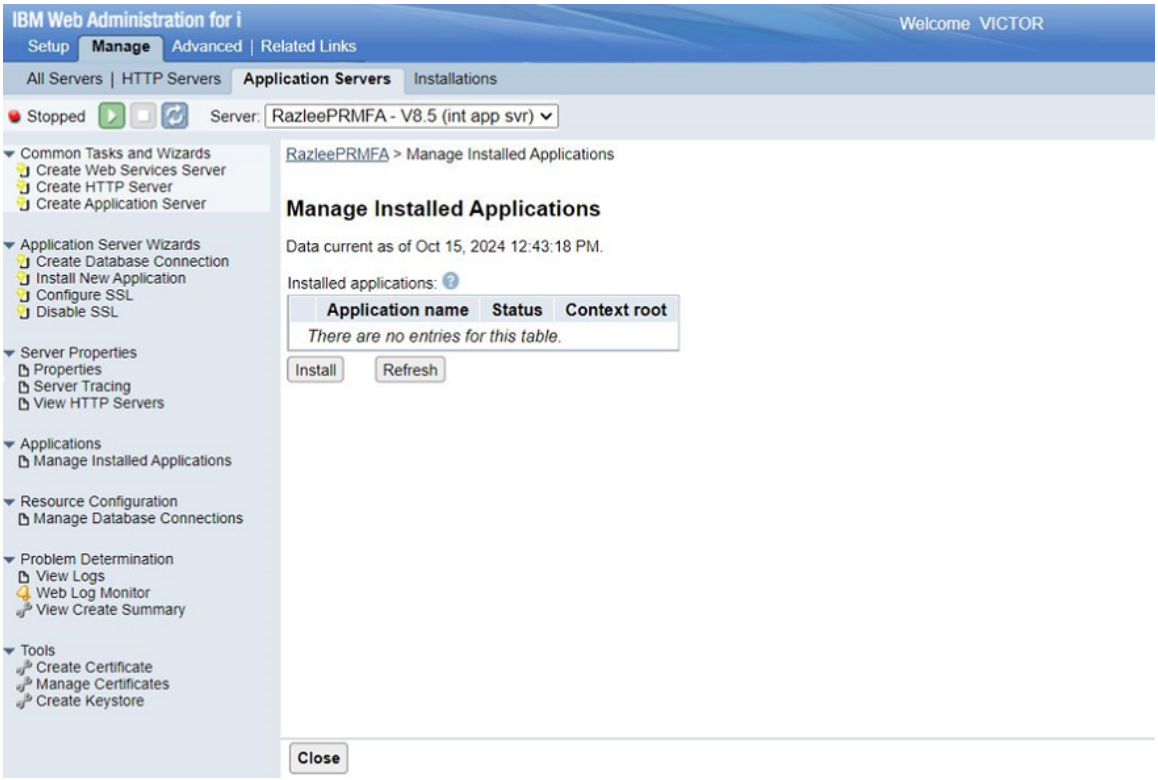
Configuring the Application Server on IBM i

To configure Password Reset and Multi Factor Authentication applications in IBMi WebSphere, follow these steps:

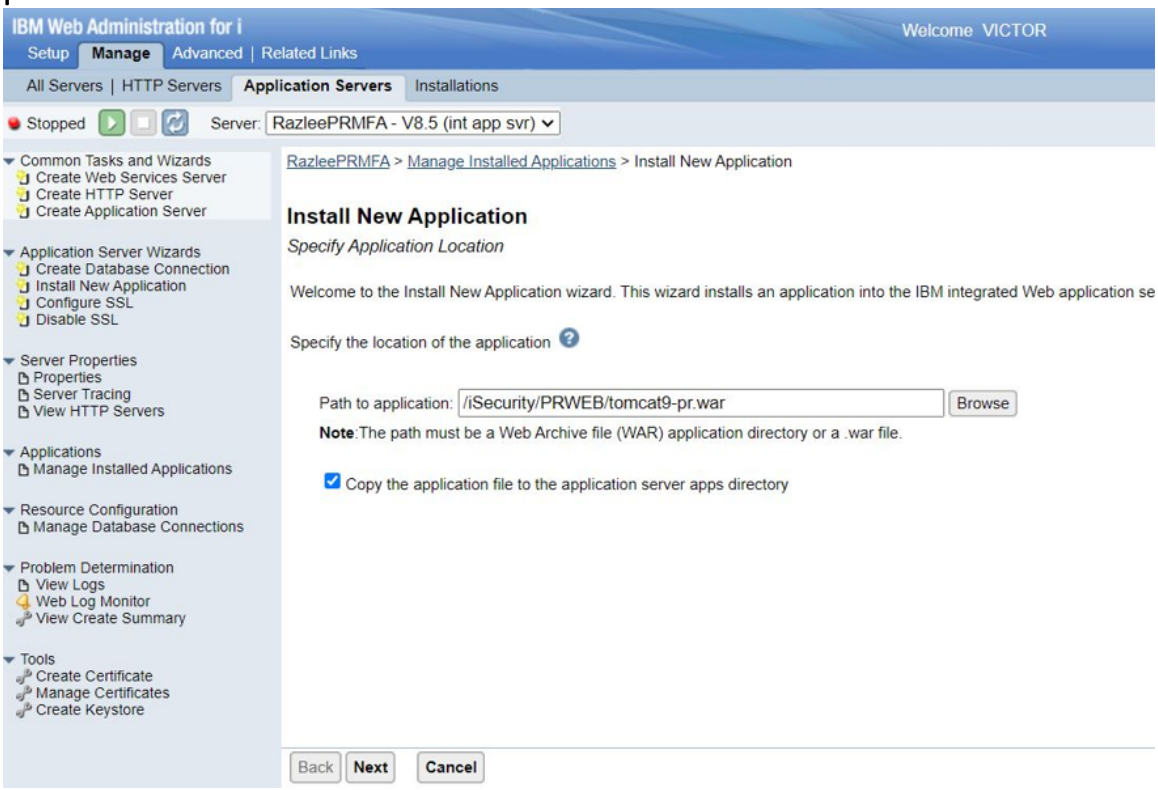
1. In your web browser, navigate to **`http://`***IBMi-IP*`:2001/HTTPAdmin`** where *IBMi-IP* is the IP address of your IBM i.
2. Sign on with **`QSECOFR`** or similar profile with enough special authorities.
3. Click on **Create Application Server** located in **Manage > Application Servers > Common Tasks and Wizards > Create Application Server**.
4. Select V8.5. and specify **Application Server Name**, for example, RazleePRMFA.
5. Enter a **User ID** to be fixed for this server. This should be a power user with a valid password and ***SIGNOFF** special authority. In the following screen, it's "victor".



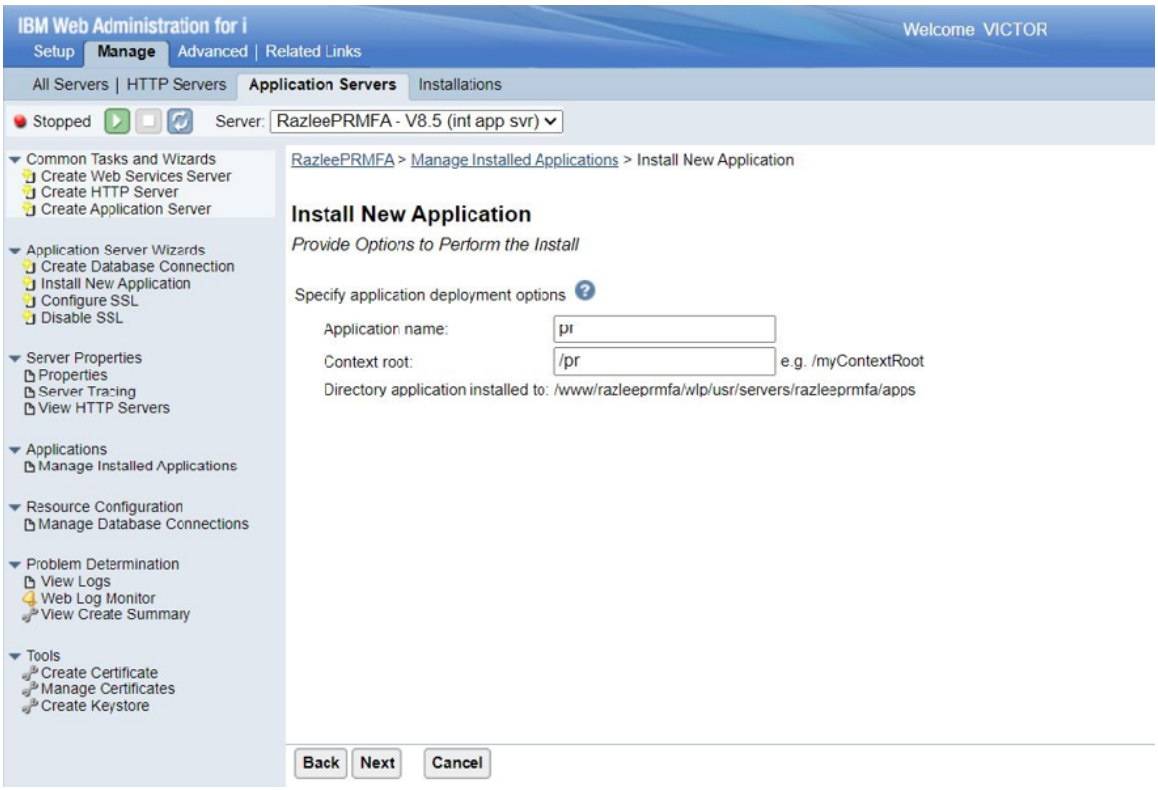
6. Click on **Manage Installed Applications** located in **Applications** and click **Install**.



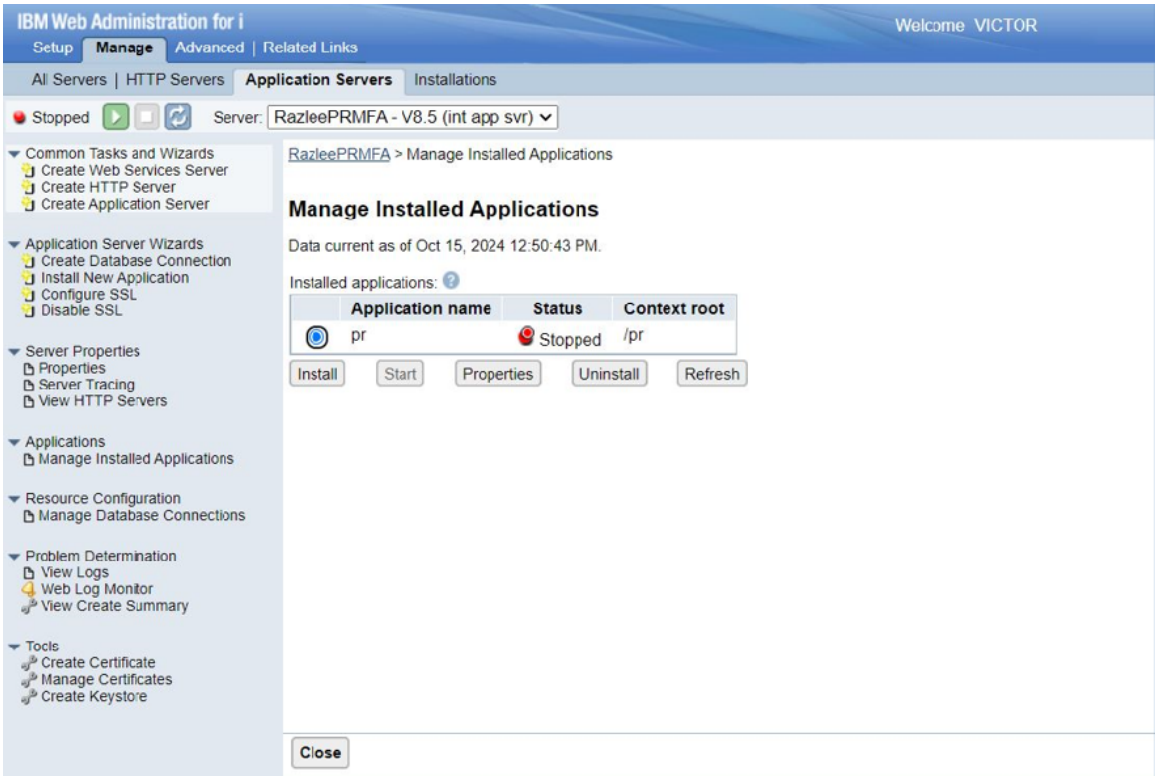
7. In **Path to application**, click **Browse** , select **/iSecurity/PRWEB/tomcat9-pr.war** and click **Next.**



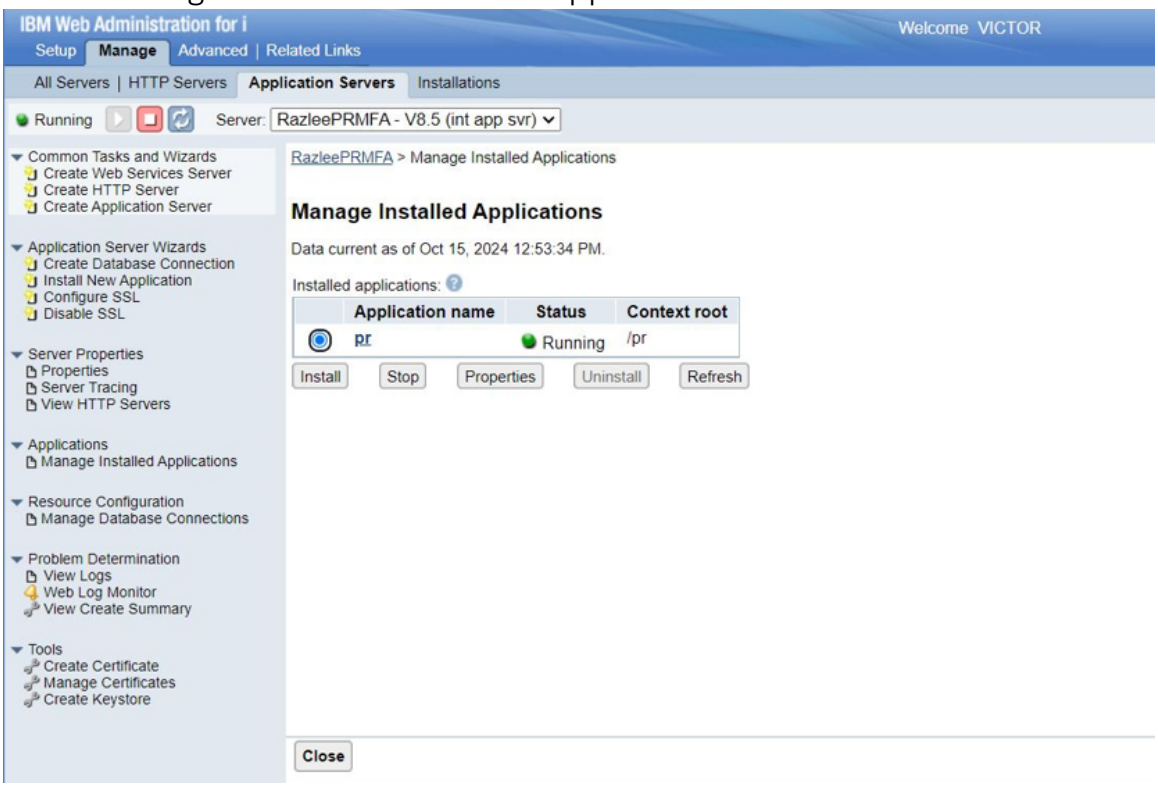
8. Change the **Application name** from **tomcat9-pr** to **pr** and the **Context root** from **/tomcat9-pr** to **/pr**. Click **Next**. Click **Finish**.



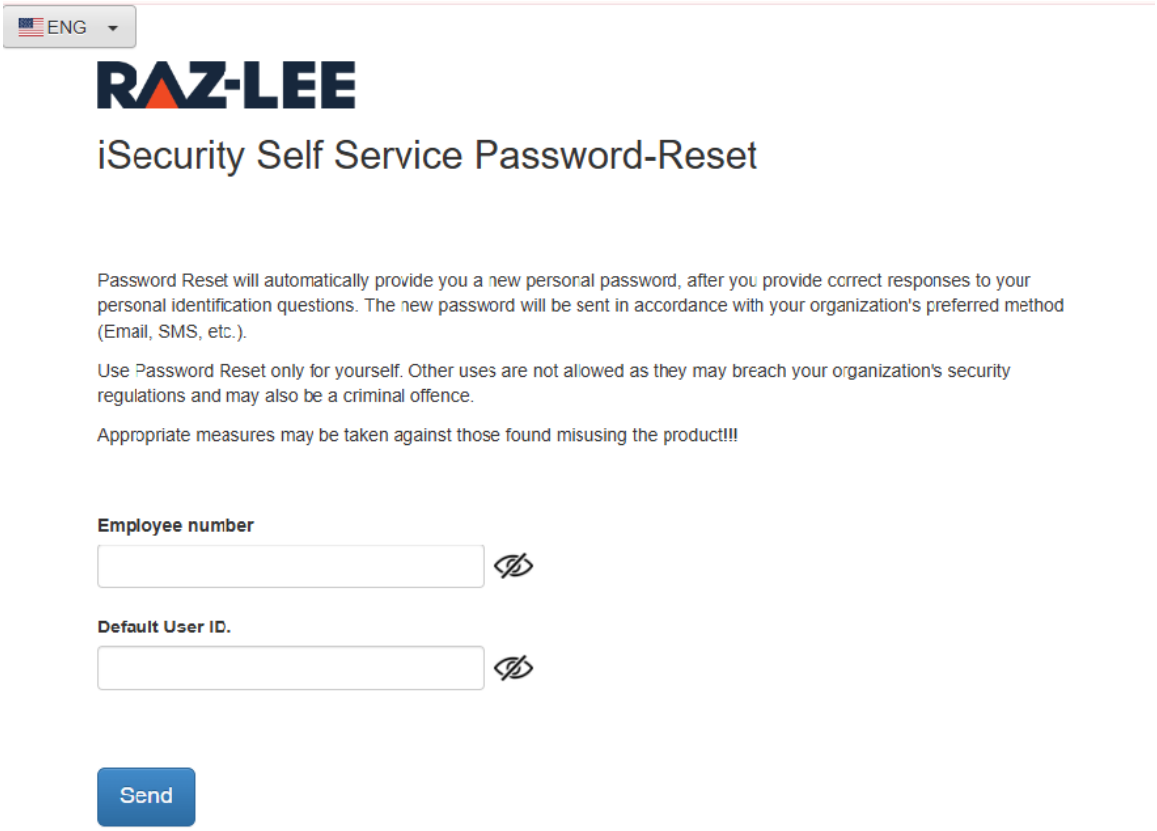
9. To start the server, click on the **Start** button on the left top.



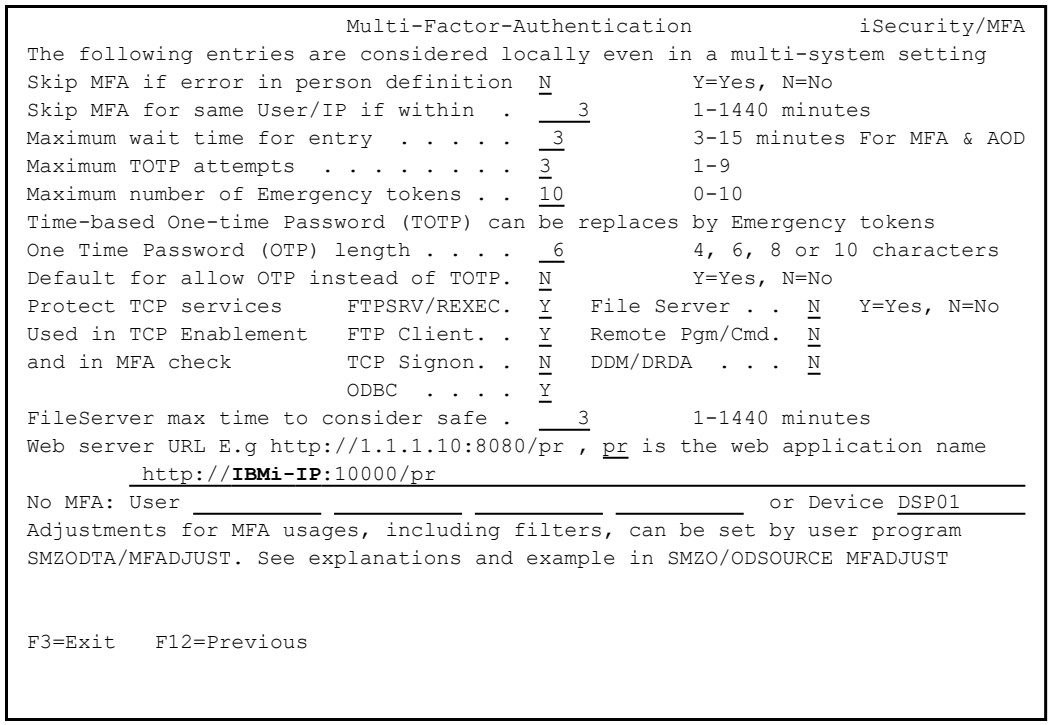
The following screen shows that the application is now active.



To check that Password Reset application is working, navigate in your web browser to **`http://IBMi-IP:10000/pr/`**, where **IBMi-IP** is the IP address of your IBM i.

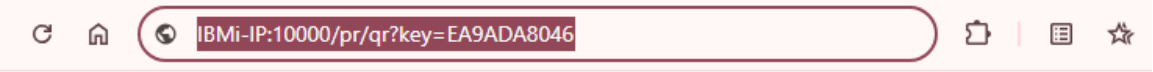


To check Multi-Factor Authentication enter the command **`STRMFA > 81 > 52`**.



Then Enter the command **STRMFA > 1 > 1** and enter **8** in the **Opt** field for the Person.

To create TOTP Secret Key, select 1. Create/Replace TOTP Secret Key and then 4. Display QR code.



iSecurity by RAZ-LEE · MFA
Multi-Factor Authentication

Scan QR code with your phone camera

Emergency Tokens

DA272C C2CAC2 D2C24A C4252A C4252C A7C2C4 A57242 A2ACA4 DACD24