iSecurity Field Encryption

User Guide
Version 1.54

www.razlee.com

Contents

-

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 Field EncryptionUser 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.

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 page 7.

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

STRACT **> 81 > 32**

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

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.

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)

Field Encryption Overview

In today's world, data encryption is an essential element of any effective computer security system. Encryption is the final layer to protect your data from those who somehow managed to get past all your other protection and access your data. Now, even when the data is accessed, it is entirely meaningless. Encryption is also the way to ensure that those who are entitled to access your data, your application users, will see the data in clear text, or masked or not see it at all, as appropriate. PCI-DSS, HPIAA, as well as many other regulatory bodies now require encryption of essential parts of the data. Raz-Lee Security’s iSecurity Encryption solution, part of the iSecurity suite, allows you to fully protect all your sensitive data.

IBM i 7.1 introduced the DB exit program FIELDPROC. The use of this feature for encryption makes it part of the DB capabilities and eliminates use of additional supporting files.

iSecurity Encryption Features

- **Stronger encryption**: Our 192 bit encryption provides the equivalent of regular 256 bit regular encryption.
- **System performance**: A special optimization algorithm that allows the reading and displaying of masked data to be performed with much less degradation in system performance.
- **Stronger keys**: 4 levels of keys: Master key, Organizational Key KEK Key, and Data Key, present a new market standard.
- **Convenience**: Files can be optionally never locked, when encryption keys are modified. This enables the product to support a daily change of the Data Keys.
- **Architecture**: Optionally, the various components of the product can be installed on different LPARs ensuring that obtaining access to a single LPAR will never be sufficient.
- **Practicality**: Centralized key management localizes all key related activity on a single LPAR, which can handle unlimited production LPARs needing encryption.
- **Flexibility**: The Product supports both File Encryption and Tokenization, so you do not have to decide which methodology to use.
- **Using Tokenization**: The Vault can reside on a different LPAR, providing another layer of security.
- A fully comprehensive system is provided to help you discover ALL your sensitive fields. All Database fields are considered and the product offers selection aids based on field: size, name, text, and column headings. This inherently prevents a situation that sensitive data is kept in the clear in a copied version of a file.
- Policy driven security and limitation of capabilities ensures Separation of Duties
- Full proof journaling system guarantees that any change in parameters is logged
- Comprehensive logs are provided to enable tracing of activities

- Uses NIST encryption standards and adheres to both PCI and COBIT standards
- 128-bit, 192-bit, and 256-bit encryption supported
- Several Key Officers may be involved in each manual KEK and Data key update
- Automatic generation of keys provides additional ease of use

Getting Started

This section describes the first steps you need to take when you start working with Field Encryption, as well as listing the standard field names, options and command keys used in the product.

Warnings and Special Considerations

Ensure that you have completed all post-installation steps, as described in the *iSecurity Installation Guide*.

While encryption can be applied to DDS-created physical files, it is well recommended to first convert the physical file to an SQL table definition. This is due to the fact that if the ***Change Physical File*** (***CHGPF***) command is used to apply a new DDS definition to file that is encrypted, ***CHGPF*** will remove the encryption without any prior warning. Also, when the ***CHGPF*** command is used with the SRCFILE parameter to change the field definition of a physical file, the ***CHGPF*** command will remove all registered Field Procedures on that physical file without any warning message.
To prevent such a risk, we recommend considering the following techniques:

- IBM has documented a methodology that allows most physical files to be converted to SQL tables without requiring any application changes or recompiles. This seems to be the best approach. For more information, see this IBM Redbook.
- Avoid using the ***CHGPF*** command.
- Use the iSecurity/COMMAND product to control the use of ***CHGPF*** on encrypted files.

You need to decide whether you will work with encryption, or with tokenization. When you choose an item to be encrypted, the encrypted data replaces the original data in the file. When you choose an item to be tokenized, the encrypted data is written to a token file and a pointer to the token file replaces the original data in the file.

When you work with tokenization, every encrypted field has its own token file. The number of values that can be held in a token file is limited to 1.8 billion. This includes all past values of the field. If your organization wants to use the same token for several fields or for several systems, you should consult with Raz-Lee support staff for implementation and restrictions. The following restrictions will always apply:

- The update of an entry will result with a new Token and will not update the value of the previous token.
- While the current file will show the updated data, other references will refer to the previous value.

Although possible, it is not recommended to encrypt key (index) fields. Accessing with encrypted keys may fail and data will not appear in the order of the clear data. Before you attempt to encrypt key fields, contact Raz-Lee Security support staff.

Basic Workflow

Before you can work with Field Encryption, you must ensure that the, Key Managers, and Token Managers are correctly defined to the product database. After doing this, you can then define which Business Items should be encrypted and how to encrypt them. Use the workflow below to do this.

Before you start this process, you may want to perform some pre-planning, so that the information to enter is readily available.

1. Ensure that the product is installed on each relevant computer/LPAR.
2. Define which users can use the product, as described in Work with Operators.
3. Define Initial Setup: Add Master Key Part, Set Master Key, and Initialize Organizational key.
4. If you are sorting encrypted data according to various LPARs, define those locations on the computer where the Data Manager is located, as described in General Definitions.
5. Define which users will be Key Officers, as described in Key Officers.
6. Define Key Encryption Key (KEK).
7. Define the Data Keys, as described in Data Keys.
8. Define Exception Group (optional).
9. Define authorities for each Business Item and how the Business Items will be displayed, as described in Authorization Groups.
10. If you are separating the Key Manager and the Token Manager locations from the Data Manager location, on the computer where the Key Manager is located, define the location of the Data Manager, as described in Supported Data Manager Systems.
11. If you are separating the Key Manager and the Token Manager locations from the Data Manager location, on the computer where the Token Manager is located, define the location of the Data Manager, as described in Supported Data Managers Systems.
12. (Optional) Let the product help you discover which fields you need to encrypt, as described in Find Fields to Encrypt.

13. Build the Business Items to encrypt and define their occurrences, as described in Field for Encryption.
14. Activate the Encryption subsystem on every relevant computer/LPAR, as described in Activation.
15. Perform the initial encryption, as described in Activate Business Item Occurrences.

NOTE: Depending on the scope of your encryption and the size of your files, the initial encryption may take a very long time. We recommend that you schedule this activity for a time when you have a minimum amount of work on your computer. You may even want to consider performing the initial encryption in incremental stages, file by file, until all files are encrypted. If you have more than one field in a specific file to encrypt, we recommend that you wait until the first field is encrypted before encrypting the second field.

Standard Fields, Options, and Command Keys

Some of the standard fields, options and command keys are described in the table below. Additional options will be provided on particular screens as per the need.

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

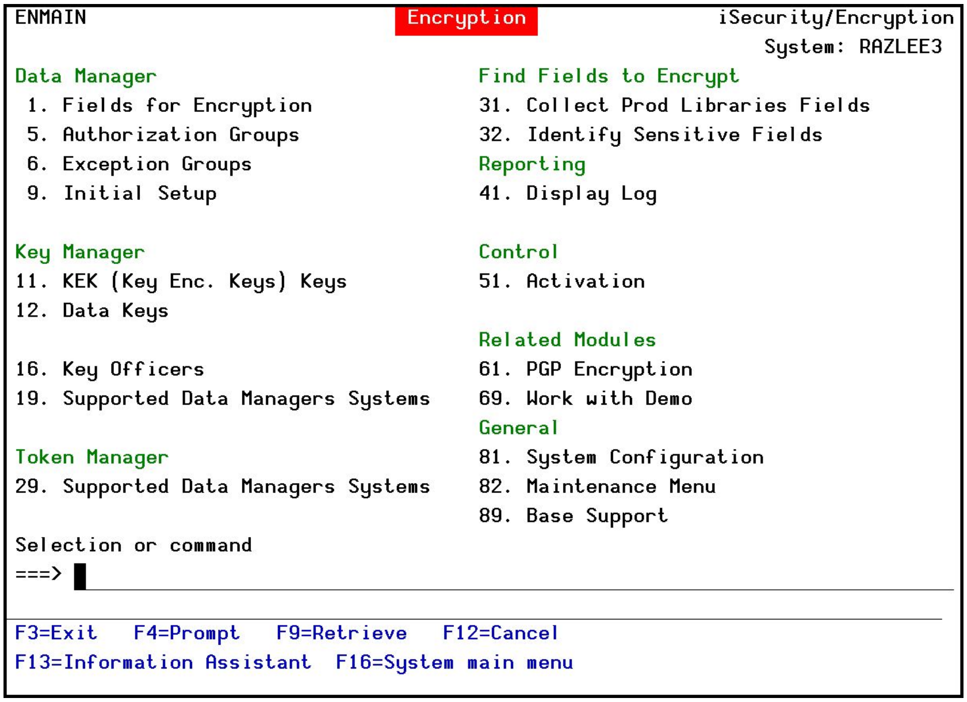
Field/Option/Command Key	Description
3=Copy	Displays a screen that allows you to copy the selected item. You will be able to change the major identifier of the item. You will then the need to select the new item to make all other necessary changes.
4=Delete	Deletes the selected item in a list. You may be asked to confirm your choice before the delete operation is performed.

Accessing Field Encryption

Access all Field Encryption functionality through the Encryption Main menu.

To access the system:

- Type **strenc** in the command line and press **Enter.** The **Encryption** Main menu appears.



```
ENMAIN                           Encryption                iSecurity/Encryption
                                                              System:  RAZLEE3
Data Manager                           Find Fields to Encrypt
 1. Fields for Encryption              31. Collect Prod Libraries Fields
 5. Authorization Groups               32. Identify Sensitive Fields
 6. Exception Groups                   Reporting
 9. Initial Setup                      41. Display Log

Key Manager                            Control
11. KEK (Key Enc. Keys) Keys           51. Activation
12. Data Keys
                                       Related Modules
16. Key Officers                       61. PGP Encryption
19. Supported Data Managers Systems    69. Work with Demo
                                       General
Token Manager                          81. System Configuration
29. Supported Data Managers Systems    82. Maintenance Menu
                                       89. Base Support
Selection or command
===>

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

Figure 1: Encryption Main Menu

Field/Option/Command Key	Description
Data Manager	
1. Fields for Encryption	In the **Work with Business Items** screen, define the fields for encryption
5. Authorization Groups	In the **Work with Authorization Groups** screen, define how encrypted fields can be viewed by different users.
6. Exception Groups	In the **Exception Groups** screen, define the exception views for users.
9. Initial Setup	In the **Initial Setup** screen, add and set Master Keys.
Key Manager	
11. KEK (Key Enc. Keys) Keys	In the **KEK (Key Enc. Keys) Keys**screen, modify/activate and add new KEK keys.
12. Data Keys	In the **Work with Data Keys** screen, define, modify, activate, and remove Data Keys.
16. Key Officers	In the **Work with Key Officers** screen, define Key Officers permissions and actions.
19. Supported Data Managers Systems	In the **Work with Supported Key Data Managers** screen, define the Data Manager environments that the Key Manager can work in.
Token Manager	
29. Supported Data Managers Systems	I the **Work with Supported Token Data Managers** screen, define the Data Manager environments that the Token Manager can work in.
Find Fields to Encrypt	
31. Collect Prod Libraries Fields	In the **Collect Encryption PF Fields** screen, identify possible fields that should be encrypted.
32. Identify Sensitive Fields	In the **Select Encryption PF Fields** screen, select the actual fields to be encrypted from the fields extracted in option 31.

Field/Option/Command Key	Description
Reporting	
41. Display Log	In the **Display Encryption Log Entries** screen, produce Encryption activity log reports.
Control	
51. Activation	In the **Activation** menu, define system activation protocols.
Related Modules	
61. PGP Encryption	Opens the **PGP Encryption** Main menu.
69. Work with Demo	Test how encryption users view data in a supported Demo Environment.
General	
81. System Configuration	In the **System Configuration** menu, configure Encryption.
82. Maintenance Menu	In the **Maintenance** menu, run procedures to update encryption and tokenization. Also, run audit reports from this menu.
89. Base Support	In the **BASE Support** menu, work with various settings that are common for all modules of iSecurity.

Encryption Setup

This section describes all the tasks that you can perform in **Field Encryption**.

Using Master Keys and Data Keys, define user's authorization to work with these keys, and in which systems the Fields for Encryption are accessible.

NOTE: Key Officers must be set first before KEK Keys and Data Keys.

Data Manager

The Data Manager enables you to define the following:

- **Business Item** - The data to encrypt is known as Business Items. The Business Item can be a Credit Card, Phone number, ID number or any alphanumeric field of any sort.
- **Data key** – The encryption method
- **Authorization** – To which group or entity is the encryption authenticated for
- **Data encryption display** – The Group or User View displayed

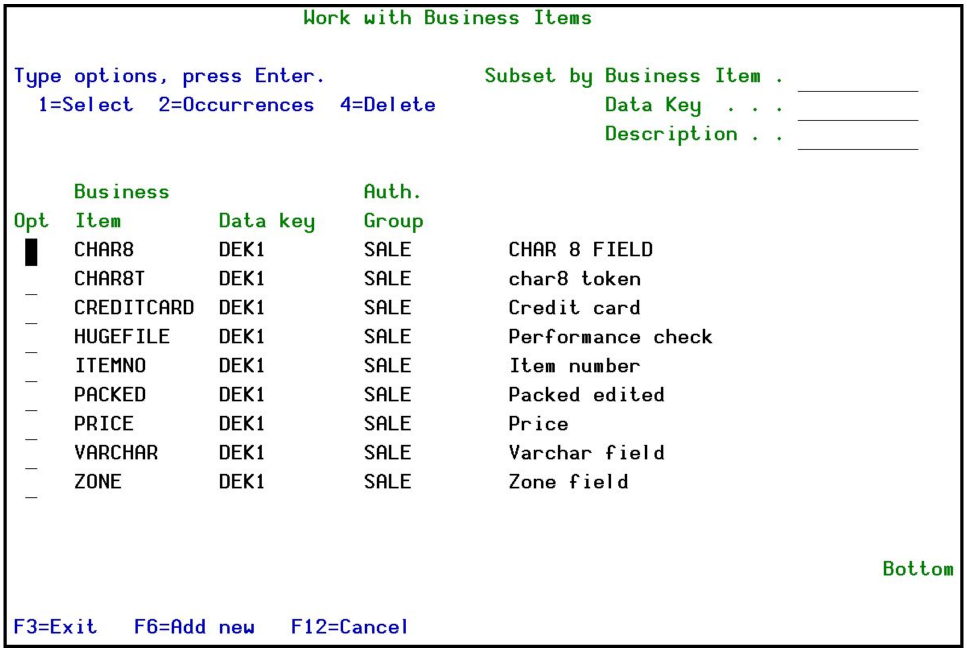
Fields for Encryption

Define the Business Items to be encrypted.

Add Business Items

To add Business Items encryption definitions:

1. Select **1. Fields for Encryption** in the **Encryption** main menu. The **Work with Business Items** screen appears.

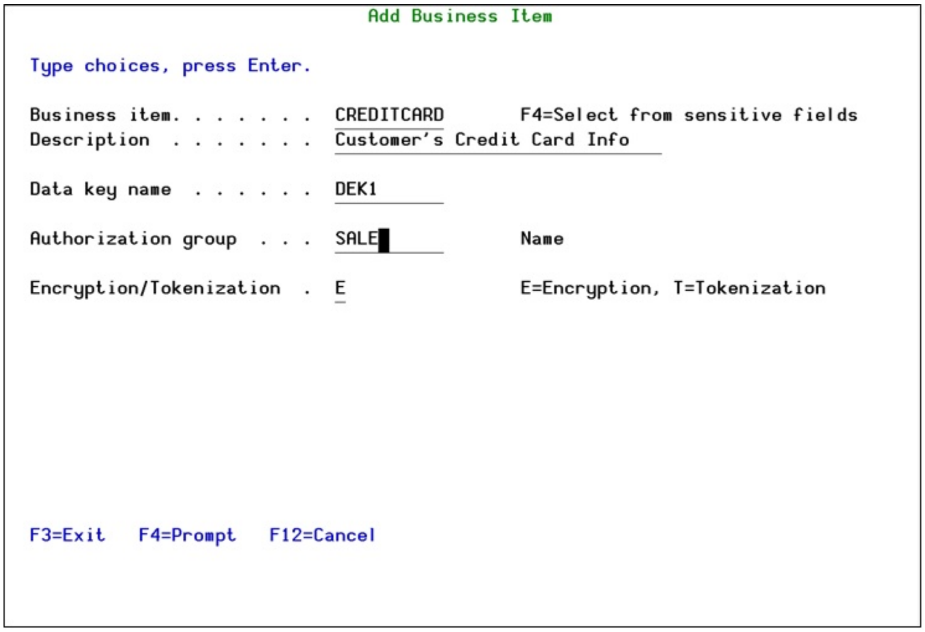


```
                        Work with Business Items

Type options, press Enter.                  Subset by Business Item . ___________
  1=Select  2=Occurrences  4=Delete                   Data Key  . . . ___________
                                                      Description . . ___________

     Business                Auth.
Opt  Item         Data key   Group
 _   CHAR8        DEK1       SALE        CHAR 8 FIELD
 _   CHAR8T       DEK1       SALE        char8 token
 _   CREDITCARD   DEK1       SALE        Credit card
 _   HUGEFILE     DEK1       SALE        Performance check
 _   ITEMNO       DEK1       SALE        Item number
 _   PACKED       DEK1       SALE        Packed edited
 _   PRICE        DEK1       SALE        Price
 _   VARCHAR      DEK1       SALE        Varchar field
 _   ZONE         DEK1       SALE        Zone field

                                                                          Bottom

F3=Exit   F6=Add new   F12=Cancel
```

Figure 2: Work with Business Items screen

Parameter	Description
Option	The options include: **1=Select**; Select an option from the list **2=Occurrences**; The Library/File/Field where the Business Item occurs **4=Delete**; Delete an option from the list
Business Item	The Business Items that can be defined.
Data key	The Data Key linked to the Business Item
Auth. Group	The Authorization Group with which the Business Item is associated.
Description	The description of the Business Item.

2. Press **F6=Add new**. The **Add Business Item** screen appears.



```
                          Add Business Item

 Type choices, press Enter.

 Business item. . . . . . .  CREDITCARD       F4=Select from sensitive fields
 Description  . . . . . . .  Customer's Credit Card Info

 Data key name  . . . . . .  DEK1

 Authorization group  . . .  SALE             Name

 Encryption/Tokenization  .  E                E=Encryption, T=Tokenization






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

Figure 3: Add Business Item screen

Parameter	Description
Business item	Enter a name for the new Business Item or press **F4** to select one of the sensitive items you discovered
Description	Enter a meaningful description for the Business Item
Data Key name	Press **F4** to choose the data key to use for the Business Item Note: If Data key that was defined does not appear in the list, it was not activated after it was created.
Authorization group	Define the Authorization Group for the Business Item. The Authorization Group defines how the Business Item will be viewed by users. **Name** = Enter a name of an Authorization Group. Or press F4 for a list of Authorization Groups.
Encryption/Tokenization	Define whether the Business Item will be encrypted or tokenized **E** = Encryption **T** = Tokenization

3. Enter the Business Item definitions and press **Enter**. The **Work with BI Occurrences** screen appears.

4. Press **Enter**. The new Business Item is added and is displayed in the **Work with Business Items** screen.

Delete Business Items

To delete Business Items encryption definitions:

1. Select **1. Fields for Encryption** in the **Encryption** main menu. The **Work with Business Items** screen appears.
2. Select the Business Item(s) to delete and press **4=Delete**. The **Delete Business Item** screen appears.
3. Press **Enter**. The Business Item is deleted and the updated **Work with Business Items** screen appears.

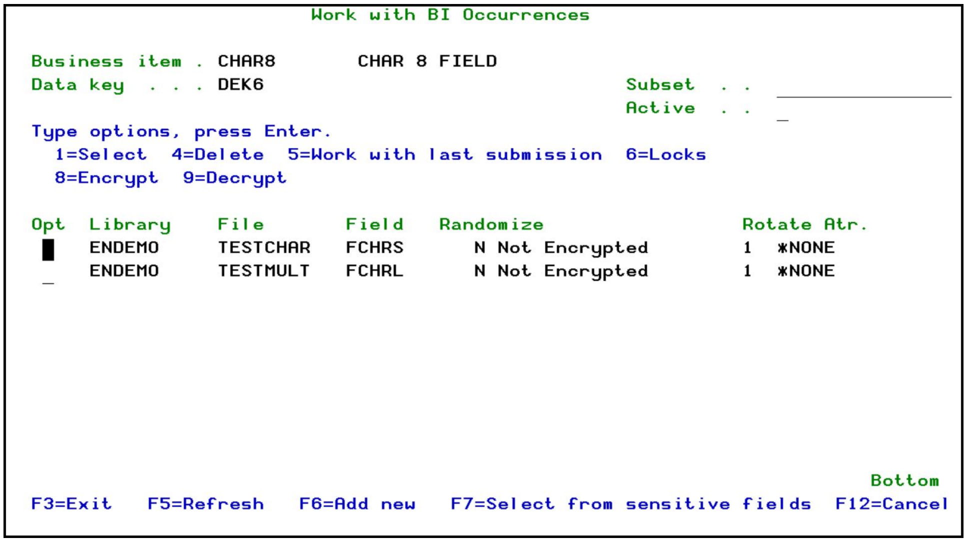
Business Items that are linked to occurrences cannot be deleted. You must first delete the occurrences, as described in Delete Business Item Occurrences.

Add Business Item Occurrences

Map Business Items to actual data per Library/File/Field.

To add Business Items occurrences:

1. Select **1. Fields for Encryption** in the **Encryption** main menu. The **Work with Business Items** screen appears.
2. Select the Business Item for which you want to add occurrences and press **2=Occurrences**. The **Work with BI Occurrences** screen appears.



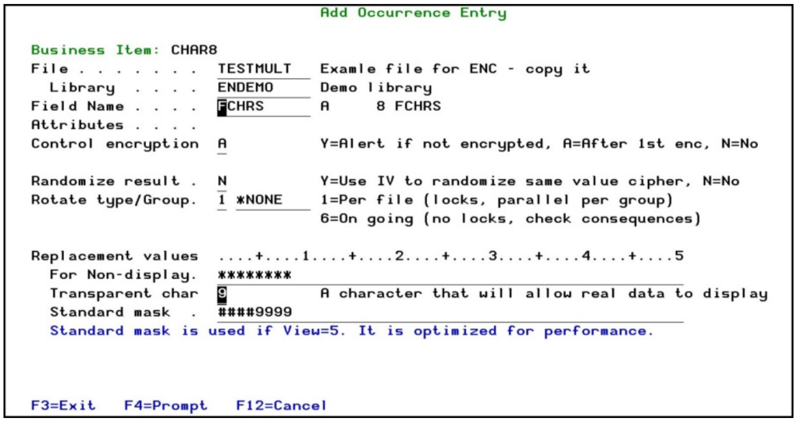
```
                         Work with BI Occurrences

 Business item . CHAR8       CHAR 8 FIELD
 Data key  . . . DEK6                              Subset  . .  _______________
                                                   Active  . .  _
 Type options, press Enter.
   1=Select  4=Delete  5=Work with last submission  6=Locks
   8=Encrypt  9=Decrypt

 Opt  Library    File       Field     Randomize                  Rotate Atr.
  _   ENDEMO     TESTCHAR   FCHRS        N Not Encrypted          1   *NONE
  _   ENDEMO     TESTMULT   FCHRL        N Not Encrypted          1   *NONE








                                                                         Bottom
 F3=Exit   F5=Refresh   F6=Add new   F7=Select from sensitive fields  F12=Cancel
```

Figure 4: Work with BI Occurrences

Parameter	Description
Option	**1=Select**; Select the entry in the relevant row **4=Delete**; Delete the entry in the relevant row **5=Work with last submission**; Work with last entry submitted **6=Locks**; Warning message received if files open in another station **8=Encrypt**; Encrypts the business item **9=Decrypt**; Decrypts the business item
Library	The library where the BI field exists
File	The file where the BI field exists
Field	The field where the Business Item exists
Status	The status of the Business Item can be: Not Encrypted, Pending encryption,*Encrypted*, Pending decryption
Randomized Result	When a short field is encrypted then there is an option to randomize the same value to a different value by means of numeric random number called IV. N – Default. Usually not needed. Y – Choose it when a short field is encrypted to make it difficult reveal the value.
Rotate Type	1 = The field in all the records are encrypted by the same Data Key version. If the Data key version is changed , the encrypted field stays the same until the file is decrypted and encrypted again (which of course locks the file) 6 = Each record in the file may have a different Data key version. When a Data key version is changed a new record is encrypted according to the new key. In this method keys in the file may be Rotated to the new Data Key version for all the records

Parameter	Description
	in parallel to the on-going work without locks. (Option 82 on the main menu and then 21). Note: The Encrypted field Must not be a UNIQUE key Field otherwise the file cannot be decrypted.
F5=Refresh	Refreshes the data displayed after activating or deactivating Business Item links
F7=Select from sensitive fields	Opens the Select Occurrences window that allows you to select Business Items found in the Identify Sensitive Fields process. The name of the Business Item must be Identical to the name of the Field you found on the search
A number of business items can be joined together. **1=Only the Selected** **2=All fields**	

3. Press **F6=Add new**. The **Add Occurrence Entry** screen appears.



```
                                 Add Occurrence Entry

 Business Item:  CHAR8
 File . . . . . . . .   TESTMULT    Examle file for ENC - copy it
   Library  . . . . .   ENDEMO      Demo library
 Field Name . . . . .   FCHRS       A      8 FCHRS
 Attributes . . . . .
 Control encryption     A           Y=Alert if not encrypted, A=After 1st enc, N=No

 Randomize result  .    N           Y=Use IV to randomize same value cipher, N=No
 Rotate type/Group.     1 *NONE     1=Per file (locks, parallel per group)
                                    6=On going (no locks, check consequences)

 Replacement values     ....+....1....+....2....+....3....+....4....+....5
   For Non-display.     ********
   Transparent char     9           A character that will allow real data to display
   Standard mask   .    ####9999
   Standard mask is used if View=5. It is optimized for performance.


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

Figure 5: Add Occurrence Entry

Parameter	Description
File	The file where the linked field exists. F4 may be used to find the file in library
Library	The library where the linked field exists
Field Name	The field linked to the Business Items. F4 may be used to find field in a file
Attributes	The attributes of the field (length, alphameric or numeric, etc.)
Encryption status.	Enter the encryption status of this entry.
Replacement Values	
For Non-display	Enter a value to be used for when the field cannot be displayed (hidden).
Standard mask	Enter a value to be used when the viewer is defined to view a masked field. If no standard mask is defined, the View defined in the Authorization Group is used
Control Encryption	Whether or not to notify the system operator that an encrypted field was decrypted not by the product but by CHGPF. A – The default. Notify only after 1st encryption. Y – Always N – Do not notify
Randomized Result	When a short field is encrypted then there is an option to randomize the same value to a different value by means of numeric random number called IV. N – Default. Usually not needed. Y – Choose it when a short field is encrypted to make it difficult reveal the value.
Rotate Type	1 = The field in all the records are encrypted by the same Data Key version. If the Data key version is the encrypted field stays the same until the file is decrypted and encrypted again (which of course locks the file)

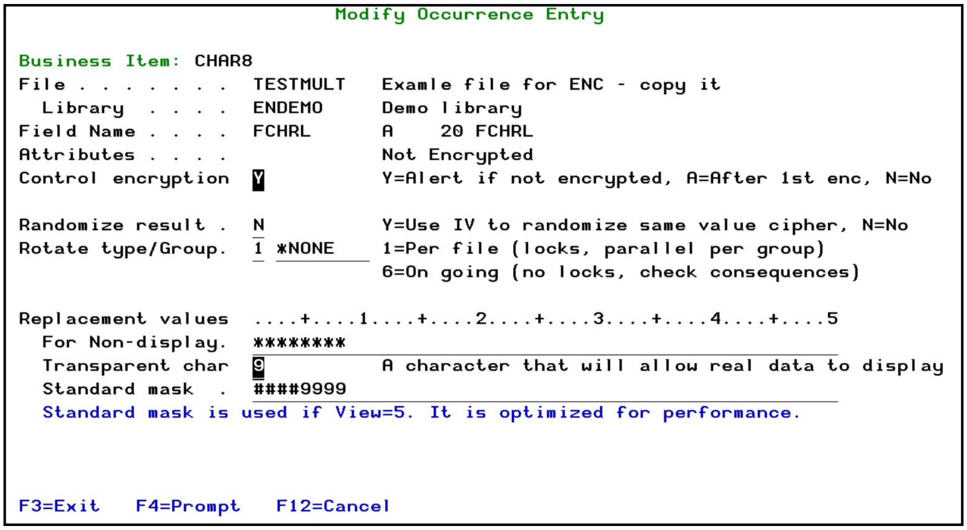
Parameter	Description
	6 = Each record in the file may have a different Data key version. When a Data key version is changed a new record is encrypted according to the new key. In this method keys in the file may be Rotated to the new Data Key version for all the records in parallel to the on-going work without locks. (Option 82 on the main menu and then 21). Note: The Encrypted field Must not be a UNIQUE key Field otherwise It may happen the file cannot be decrypted.
Rotate Group	If a specific value is given it may be used to group together Fields of the same value to run a job that Decrypt and encrypt the files together.

4. Enter the Occurrence Entry definitions and press **Enter**. The new occurrence is added and now appears in the **Work with BI Occurrences** screen.

Modify Business Item Occurrences

To modify Business Items encryption occurrences:

1. Select **1. Fields for Encryption** in the **Encryption** main menu. The **Work with Business Items** screen appears.
2. Select the Business Item for which you want to modify occurrences and press **2=Occurrences**. The **Work with BI Occurrences** screen appears.
3. Select the Occurrence you want to modify and press **1=Select**. The **Occurrence Entry** screen appears.



```
                           Modify Occurrence Entry

Business Item: CHAR8
File . . . . . . .  TESTMULT   Examle file for ENC - copy it
  Library  . . . .  ENDEMO     Demo library
Field Name . . . .  FCHRL      A    20 FCHRL
Attributes . . . .             Not Encrypted
Control encryption  Y          Y=Alert if not encrypted, A=After 1st enc, N=No

Randomize result .  N          Y=Use IV to randomize same value cipher, N=No
Rotate type/Group.  1 *NONE    1=Per file (locks, parallel per group)
                               6=On going (no locks, check consequences)

Replacement values  ....+....1....+....2....+....3....+....4....+....5
  For Non-display.  ********
  Transparent char  9          A character that will allow real data to display
  Standard mask  .  ####9999
  Standard mask is used if View=5. It is optimized for performance.



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

Figure 6: Modify Occurrence Entry

Parameter	Description
File	The file where the linked field exists
Library	The library where the linked field exists
Field Name	The field linked to the Business Items
Attributes	The attributes of the field (length, alphameric or numeric, etc.)
Encryption status.	Enter the encryption status of this entry.
Replacement Values	
For Non-display	Enter a value to be used for when the field cannot be displayed.
Standard mask	Enter a value to be used when the viewer is defined to view a masked field. If no standard mask is defined, the View defined in the Authorization Group is used
Control Encryption	Whether or not to notify the system operator with a message that an encrypted field was decrypted not by the product but by CHGPF. A – The default. Notify only after 1st encryption. Y – Always N – Do not notify
Randomized Result	When a short field is encrypted then there is an option to randomize the same value to a different value by means of a numeric random number called IV. N – Default. Usually not needed. Y – Choose it when a short field is encrypted to make it difficult reveal the value.
Rotate Type	1 = The field in all the records are encrypted by the same Data Key version. If the Data key version is changed , the encrypted field stays the same until the file is decrypted and encrypted again (which of course locks the file). 6 = Each record in the file may have a different Data key version. When a Data key version is

Parameter	Description
	changed a new record is encrypted according to the new key. In this method keys in the file may be Rotated to the new Data Key version for all the records in parallel to the on-going work without locks. (Option 82 on the main menu and then 21). Note: The Encrypted field Must not be a UNIQUE key Field otherwise It may happen the file cannot be decrypted.
Rotate Group	If a specific value is given it may be used to group together Fields of the same value to run a job that Decrypt and encrypt the files together.

4. Enter the Occurrence Entry definitions and press **Enter**. The occurrence is updated and now appears in the **Work with BI Occurrences** screen.

Delete Business Item Occurrences

To delete Business Items encryption occurrences:

1. Select **1. Fields for Encryption** in the **Encryption** main menu. The **Work with Business Items** screen appears.
2. Select the Business Item for which you want to delete occurrences and press **2=Occurrences**. The **Work with BI Occurrences** screen appears.
3. Select the Occurrence you want to delete and press **4=Delete**. The **Delete Occurrence Entry** screen appears.

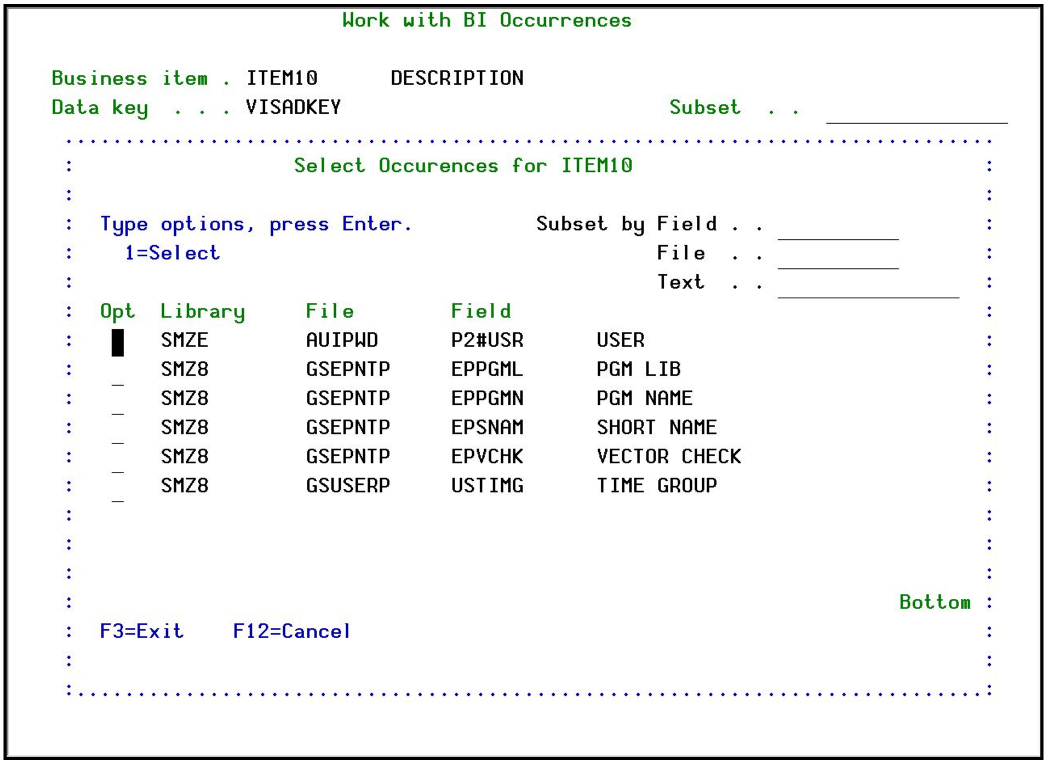
NOTE: Active occurrences cannot be deleted. You must first deactivate the occurrence, as described in Deactivate Business Item Occurrences. However, de-activating an occurrence results in that occurrence being de-encrypted.

4. Press **Enter**. The Occurrence is deleted and the updated **Work with BI Occurrences** screen appears.

Select Business Item Occurrences from Sensitive Fields

To add Business Items encryption occurrences from Sensitive Fields:

1. Select **1. Fields for Encryption** in the **Encryption** main menu. The **Work with Business Items** screen appears.
2. Select the Business Item for which you want to add occurrences and press **2=Occurrences**. The **Work with BI Occurrences** screen appears.
3. Press **F7=Selectfrom sensitive fields**. The **Select Occurrences** window appears.



```
                         Work with BI Occurrences

 Business item . ITEM10      DESCRIPTION
 Data key  . . . VISADKEY                         Subset  . .  _______________
  ..............................................................................
  :                   Select Occurences for ITEM10                             :
  :                                                                            :
  :  Type options, press Enter.          Subset by Field . .  __________       :
  :    1=Select                                    File  . .  __________       :
  :                                                Text  . .  _______________  :
  :  Opt  Library     File        Field                                        :
  :   _   SMZE        AUIPWD      P2#USR      USER                             :
  :   _   SMZ8        GSEPNTP     EPPGML      PGM LIB                          :
  :   _   SMZ8        GSEPNTP     EPPGMN      PGM NAME                         :
  :   _   SMZ8        GSEPNTP     EPSNAM      SHORT NAME                       :
  :   _   SMZ8        GSEPNTP     EPVCHK      VECTOR CHECK                     :
  :   _   SMZ8        GSUSERP     USTIMG      TIME GROUP                       :
  :                                                                            :
  :                                                                            :
  :                                                                            :
  :                                                                    Bottom  :
  :  F3=Exit    F12=Cancel                                                     :
  :                                                                            :
  :............................................................................:
```

Figure 7: Select Occurrences

4. Select one or more Occurrence to link to the Business Item and press **1=Select**. The Occurrence is linked to the Business Item and the updated **Work with BI Occurrences** screen appears.

-

Authorization Groups

Authorization Groups define how encrypted fields can be viewed by different users.

Define Views for users or group of users in the system and define by whom a Business Item should be treated viewed or modified.

A View is the Default view authorized per user.

An Exception Group enables Users/Groups to view an alternative presentation under specific conditions.

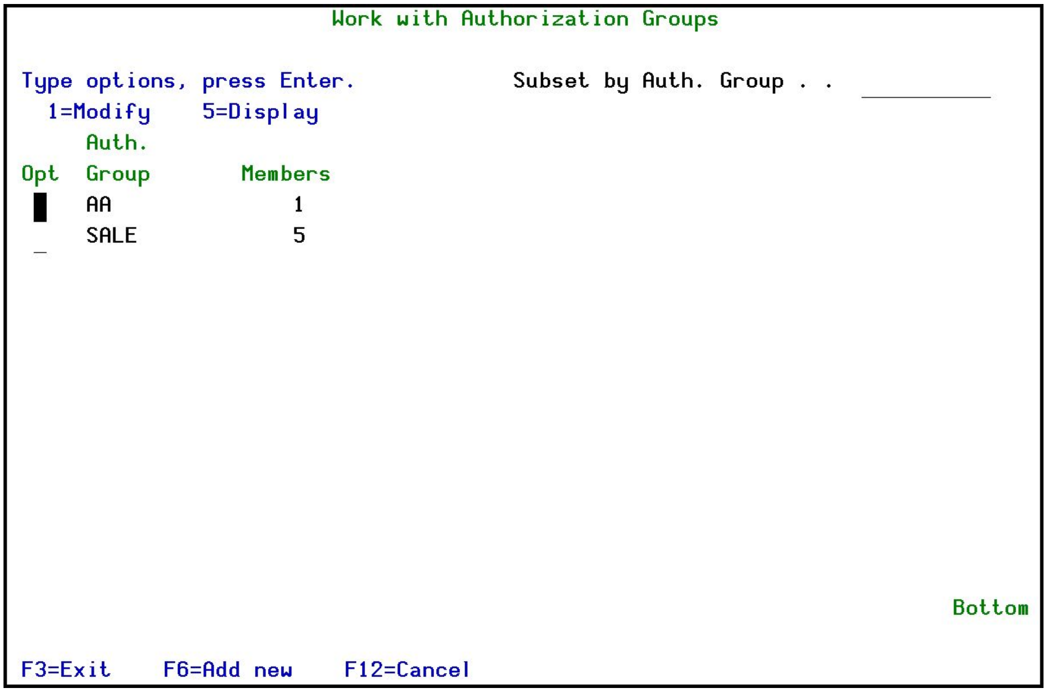
There are three types of Exception Groups:

- **PGM type**: Begins with “PGM” and defines a program or lists of programs that when active (in the program’s stack) during the read or the write of the encrypted field, the default user View is replaced with the new View that is indicated for that program.
- **RCD type**: Begins with “RCD” and defines a Record format of a Display file. If a specific record is active when reading or writing the field that is encrypted, the Default View for the user is replaced with the new View that is indicated for the record format.
- **USR type**: Begin with “USR” and consists of one User Program that will be executed each time the record is written or read and this program will return a new View according to its own specific logic.

Add Authorization Group

To add an Authorization Group:

1. Select **5. Authorization Groups** in the **Encryption** main menu. The **Work with Authorization Groups** screen appears.

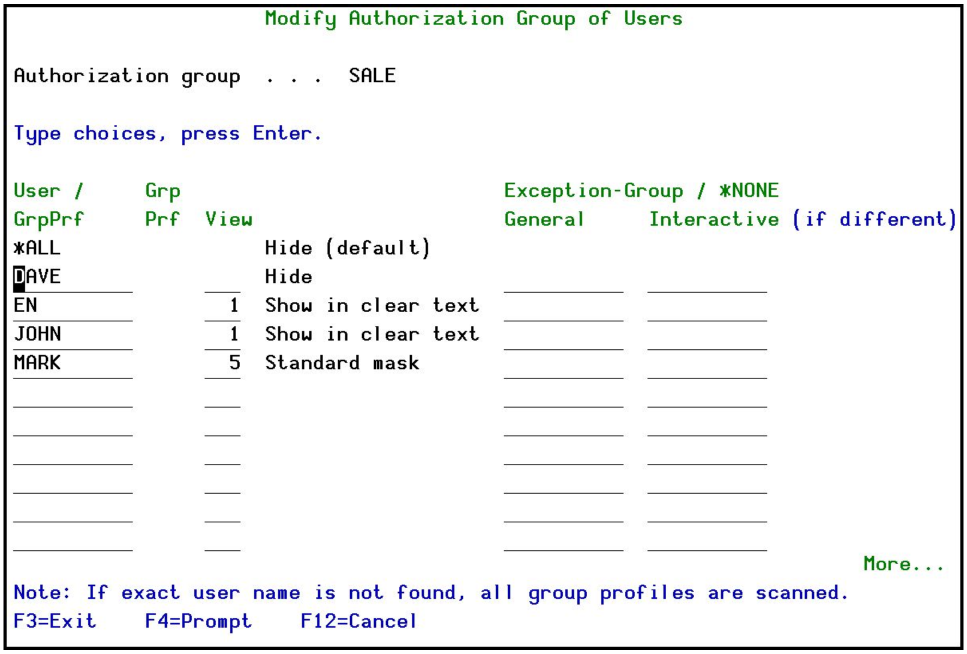


```
                        Work with Authorization Groups

 Type options, press Enter.                 Subset by Auth. Group . .   __________
   1=Modify     5=Display
      Auth.
 Opt  Group         Members
 █    AA                1
 _    SALE              5










                                                                        Bottom

 F3=Exit     F6=Add new     F12=Cancel
```

Figure 8: Work with Authorization Groups

Field/Option/Command Key	Description
Auth. Group	The name of the group
Members	The number of members in this group

2. Select **1=Modify**, the **Modify Authorization Group of Users** screen appears.



```
                     Modify Authorization Group of Users

Authorization group  . . .  SALE

Type choices, press Enter.

User /     Grp                         Exception-Group / *NONE
GrpPrf     Prf  View                   General     Interactive (if different)
*ALL                 Hide (default)
DAVE                 Hide
EN                1  Show in clear text
JOHN              1  Show in clear text
MARK              5  Standard mask






                                                                       More...
Note: If exact user name is not found, all group profiles are scanned.
F3=Exit    F4=Prompt    F12=Cancel
```

Figure 9: Modify Authorization Group of Users

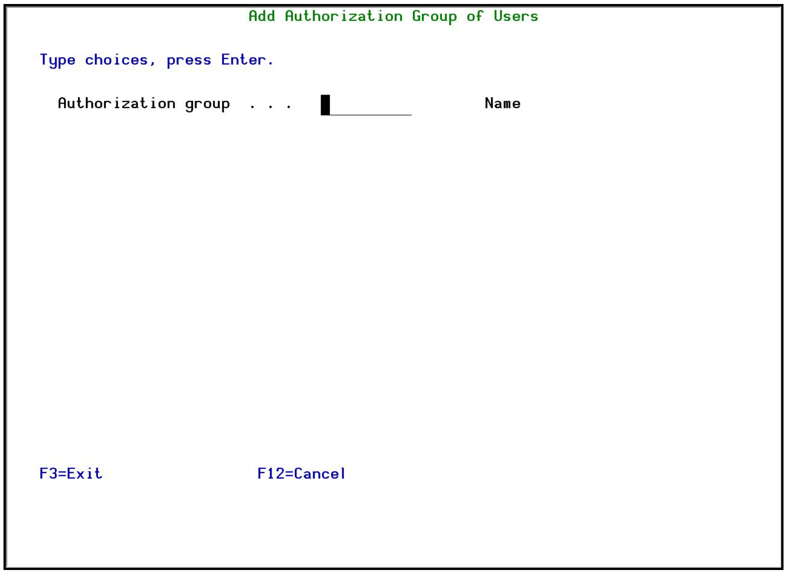
Field/Option/Command Key	Description
User / Grp Prf	The User or Group Profile
Grp Prf	If **Y**, this is a Group Profile
View	The view type associated for this User / Group Profile in this Authorization Group **0 (Blank)** = Hide the value **1** = Value – the actual value is displayed in clear text **5** = Standard mask – display the value using the occurrence's standard mask When Standard mask is displayed the field is not decrypted so it is much faster to view the field. **14** = Last 4 – only the last 4 characters of the Business Item are displayed in clear **16** = Last 6 – only the last 6 characters of the Business Item are displayed in clear **24** = 1-2 and last 4 – only the first 2 and last 4 characters of the Business Item are displayed in clear **26** = 1-2 and last 6 – only the first 2 and last 6 characters of the Business Item are displayed in clear **901** = Scramble (by formula) – displays a numeric representation of the hash value of the clear data **902** = Scramble (random data) – displays a random number with no connection to the clear data
Text	The system description of the User or Group Profile
Exception Group - General	Default exception if interactive exception is not given

Field/Option/Command Key	Description
Exception Group - Interactive	First Priority when a program is interactive (see Exception Groups)

3. Modify the Authorization Group by updating existing users/group profiles, adding new users/group profiles, or deleting users/group profiles and press **Enter**. The Authorization Group is updated and now appears in the **Work with Authorization Groups** screen.

NOTE: When you create a new Authorization Group, you must add at least one user or group profile to the group. If you do not do this, the Authorization Group is not created.

4. Press **F6=Add new**. The **Add Authorization Group of Users** screen appears.



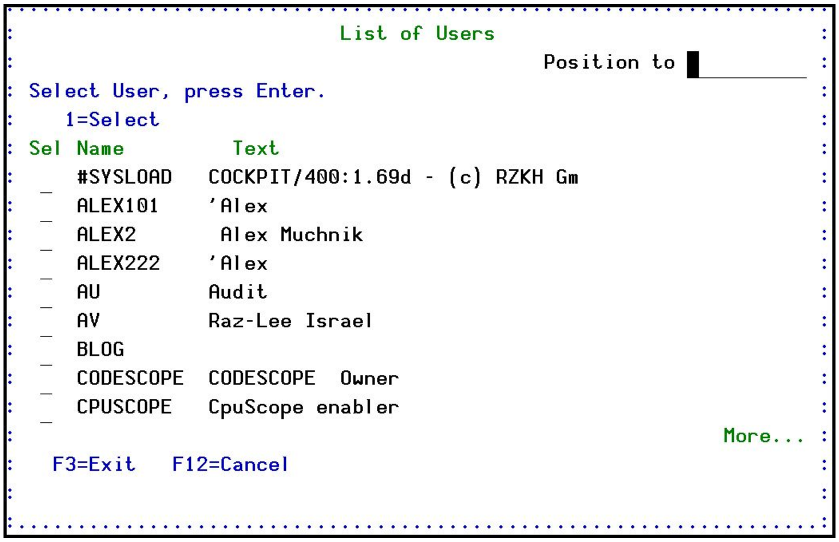
```
                        Add Authorization Group of Users

 Type choices, press Enter.

   Authorization group  . . .  ▌__________          Name








 F3=Exit                   F12=Cancel
```

Figure 10: Add Authorization Group of Users

5. Enter the authorization definitions and press **Enter**. The new authorization is added and now appears in the **Work with Authorization Groups** screen.

To view list of users:

1. In the **Modify Authorization Group of Users** screen, click **F4=Prompt**. The **List of Users** screen appears.



```
                         List of Users
                                          Position to
 Select User, press Enter.
    1=Select
 Sel Name         Text
  _  #SYSLOAD   COCKPIT/400:1.69d - (c) RZKH Gm
  _  ALEX101    'Alex
  _  ALEX2       Alex Muchnik
  _  ALEX222    'Alex
  _  AU         Audit
  _  AV         Raz-Lee Israel
  _  BLOG
  _  CODESCOPE  CODESCOPE  Owner
  _  CPUSCOPE   CpuScope enabler
                                                        More...
   F3=Exit   F12=Cancel
```

Figure 11: List of Users

2. Select an option using **1=Select**, and press **Enter**.

Delete Authorization Groups

To delete Authorization Groups:

1. Select **5. Authorization Group** in the **Encryption** main menu. The **Work with Authorization Groups** screen appears.
2. Select the Authorization Group to delete and press **1=Select**. The **Modify Authorization Group of Users** screen appears.
3. Remove all the members of the group and press **Enter**. The empty Authorization Group is deleted and the updated **Work with Authorization Groups** screen appears.

Delete Authorization Group Members

To delete a member of an Authorization Group:

1. Select **5. Authorization Group** in the **Encryption** main menu. The **Work with Authorization Groups** screen appears.
2. Select the Authorization Group to delete and press **1=Select**. The **Modify Authorization Group of Users** screen appears.
3. Remove the required member from the group and press **Enter**. The Authorization Group is updated and the updated **Work with Authorization Groups** screen appears.

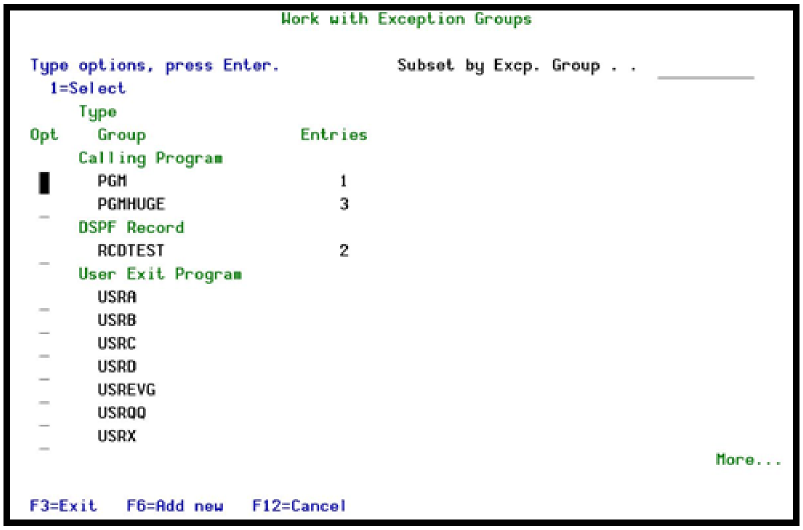
Exception Groups

Exception Groups allow alteration of the View (defined in Authorization Groups), according to:

1. The program that runs when the encrypted field is read or written to the application (PGM type).
2. The Display file Record format that has been used when the encrypted field is read/written. (RCD type).
3. A User Exit Program that runs each time and returns a specific new view (USR type).

To add an Exception Group:

1. Select **6. Exception Groups** in the **Encryption** main menu. The **Work with Exception Groups** screen appears.

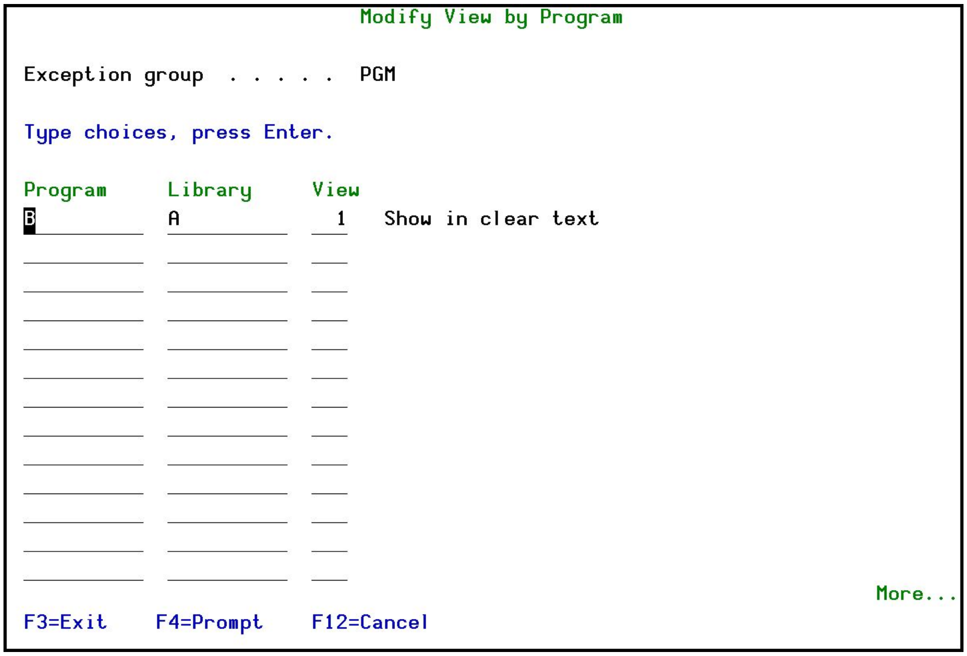


```
                         Work with Exception Groups

 Type options, press Enter.            Subset by Excp. Group . .  __________
   1=Select
      Type
 Opt    Group                  Entries
      Calling Program
 _      PGM                        1
 _      PGMHUGE                    3
      DSPF Record
 _      RCDTEST                    2
      User Exit Program
 _      USRA
 _      USRB
 _      USRC
 _      USRD
 _      USREVG
 _      USRQQ
 _      USRX
                                                                    More...

 F3=Exit   F6=Add new   F12=Cancel
```

Figure 12: Work with Exception Groups

By Program

2. Select an option **Calling Program** with **1=Select** , and then press **Enter** . The **Modify View by Program** screen appears.



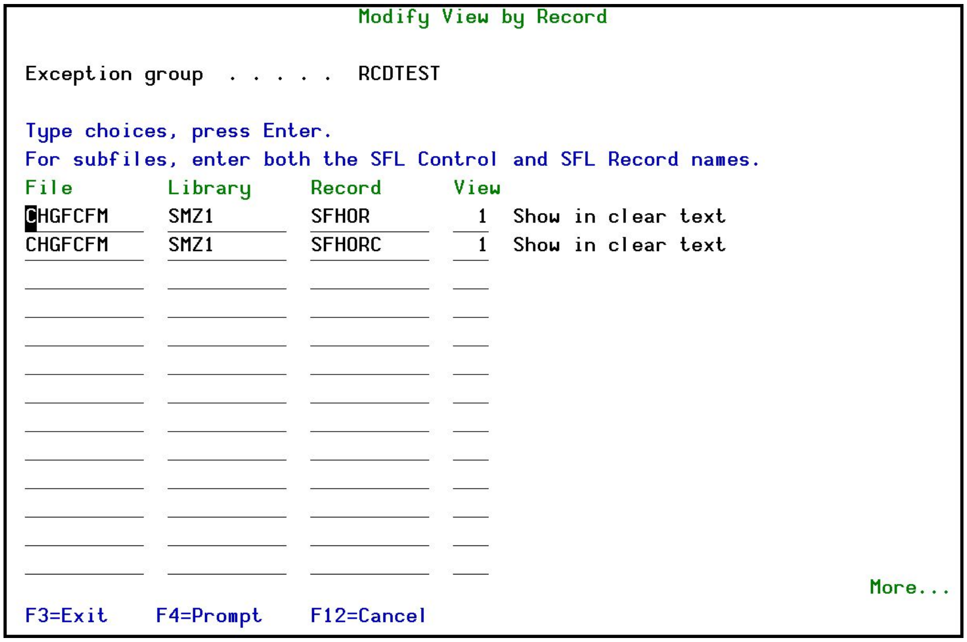
```
                              Modify View by Program

Exception group  . . . . .    PGM

Type choices, press Enter.

Program      Library      View
B            A               1   Show in clear text
















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

Figure 13: Modify View by Program

3. Select **F4=Prompt** , to **Select Program** .

By Record

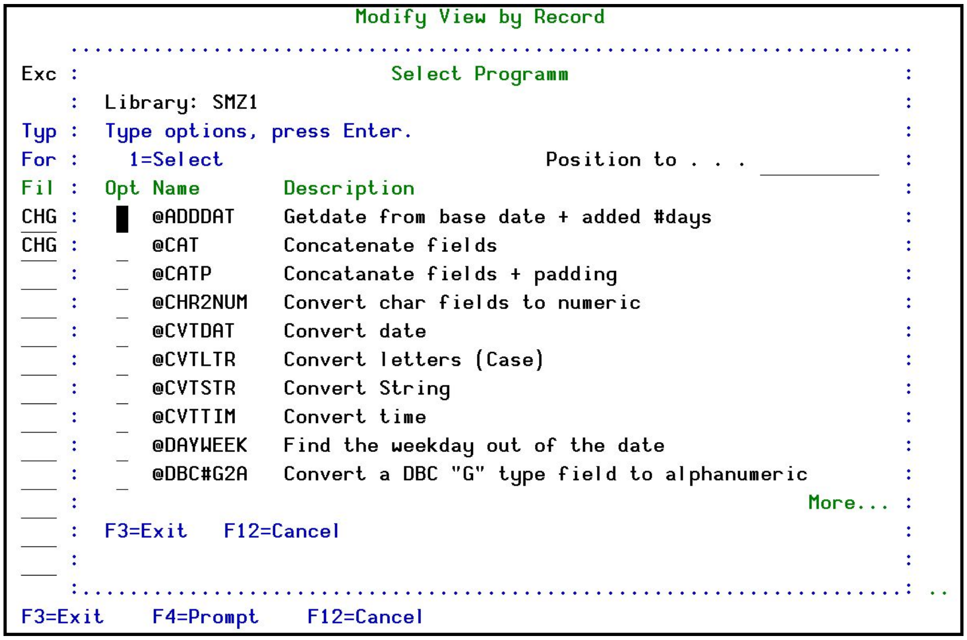
1. Select an option **DSPF Record** with **1=Select** , and then press **Enter** . The **Modify View by Record** screen appears.



```
                          Modify View by Record

 Exception group  . . . . .  RCDTEST

 Type choices, press Enter.
 For subfiles, enter both the SFL Control and SFL Record names.
 File        Library     Record      View
 CHGFCFM     SMZ1        SFHOR          1  Show in clear text
 CHGFCFM     SMZ1        SFHORC         1  Show in clear text
 __________  __________  __________  ___
 __________  __________  __________  ___
 __________  __________  __________  ___
 __________  __________  __________  ___
 __________  __________  __________  ___
 __________  __________  __________  ___
 __________  __________  __________  ___
 __________  __________  __________  ___
 __________  __________  __________  ___
 __________  __________  __________  ___
 __________  __________  __________  ___
                                                                  More...
 F3=Exit    F4=Prompt    F12=Cancel
```

Figure 14: Modify View by Record

2. Select **F4=Prompt** , to **Select Program** .

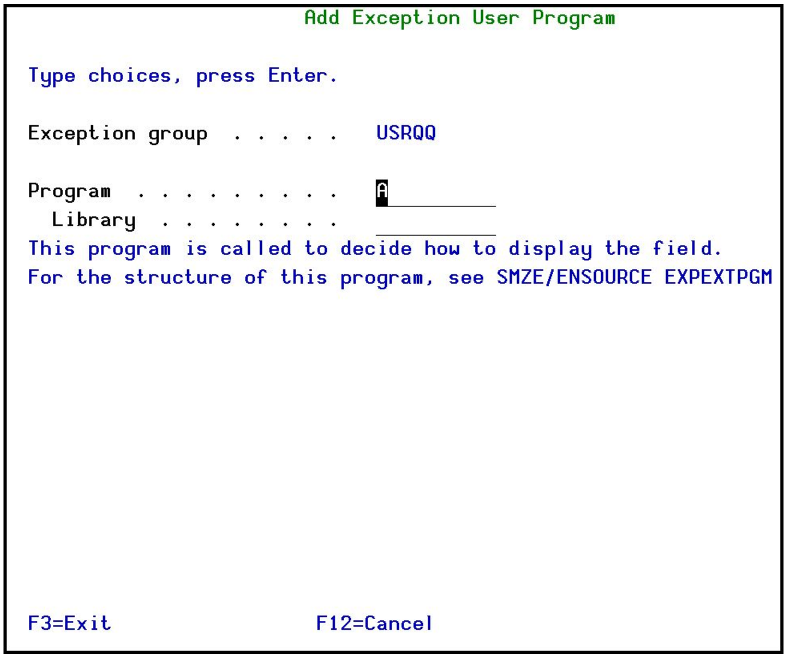


```
                          Modify View by Record
      ..................................................................
 Exc :                        Select Programm                          :
     :  Library: SMZ1                                                  :
 Typ :  Type options, press Enter.                                     :
 For :    1=Select                          Position to . . .  __________ :
 Fil :  Opt Name        Description                                    :
 CHG :      @ADDDAT     Getdate from base date + added #days           :
 CHG :   _  @CAT        Concatenate fields                             :
 ___ :   _  @CATP       Concatanate fields + padding                   :
 ___ :   _  @CHR2NUM    Convert char fields to numeric                 :
 ___ :   _  @CVTDAT     Convert date                                   :
 ___ :   _  @CVTLTR     Convert letters (Case)                         :
 ___ :   _  @CVTSTR     Convert String                                 :
 ___ :   _  @CVTTIM     Convert time                                   :
 ___ :   _  @DAYWEEK    Find the weekday out of the date               :
 ___ :   _  @DBC#G2A    Convert a DBC "G" type field to alphanumeric   :
 ___ :                                                        More...  :
 ___ :  F3=Exit   F12=Cancel                                           :
 ___ :                                                                 :
     :.................................................................: ..
 F3=Exit    F4=Prompt    F12=Cancel
```

Figure 15: Select Program

By User Program

3. Select an option **User Exit Program** with **1=Select** , and then press **Enter** . The **Add Exception user Program** screen appears.



```
                        Add Exception User Program

 Type choices, press Enter.

 Exception group . . . . .    USRQQ

 Program . . . . . . . . .    A_________
   Library . . . . . . . .    __________
 This program is called to decide how to display the field.
 For the structure of this program, see SMZE/ENSOURCE EXPEXTPGM











 F3=Exit                 F12=Cancel
```

Figure 16: Add Exception User Program

4. Type the program and library for field display, and press **Exit** .

-

Initial Setup

The Master Keys are used to encrypt the Organizational key to which it is assigned.

There are up to 8 master keys. You need only one Mater key to encrypt the Organizational key.

Several People can add values to one Master key.

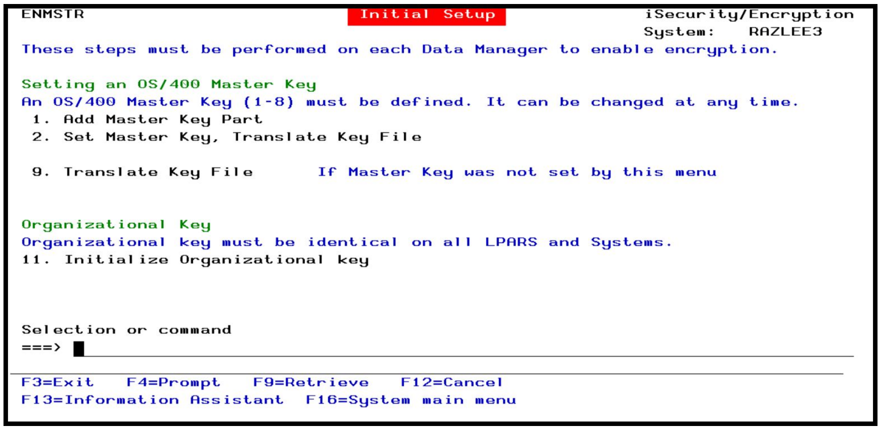
After adding the Master key it must be set by Set Master Key and after that set the Organizational Key only one time for a LPAR.

After the Setting of the Organizational Key once, there is a possibility to add the same Master Key and then set it again to change the Encryption of The Organizational Key.

Add Master Keys

To add Master Keys:

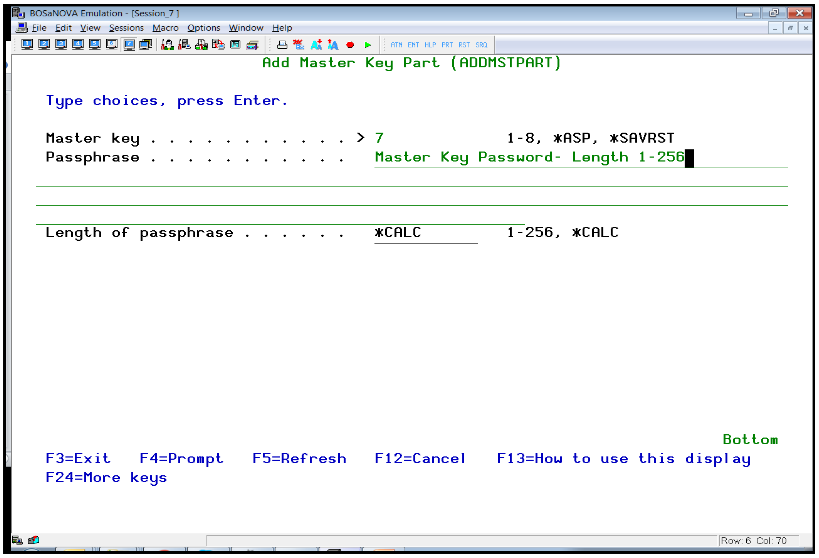
1. Select **9. Initial Setup** in the **Encryption** main menu. The **Initial Setup** screen appears.



```
ENMSTR                          Initial Setup                iSecurity/Encryption
                                                             System:    RAZLEE3
These steps must be performed on each Data Manager to enable encryption.

Setting an OS/400 Master Key
An OS/400 Master Key (1-8) must be defined. It can be changed at any time.
 1. Add Master Key Part
 2. Set Master Key, Translate Key File

 9. Translate Key File       If Master Key was not set by this menu


Organizational Key
Organizational key must be identical on all LPARS and Systems.
11. Initialize Organizational key



Selection or command
===>

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

Figure 17: Initial Setup

2. Select **Add Master Key Part**. The **Master Key Part (ADDMSTPART)** screen appears.


BOSaNOVA Emulation - [Session_7]
File Edit View Sessions Macro Options Window Help
Row: 6 Col: 70

```
                      Add Master Key Part (ADDMSTPART)

 Type choices, press Enter.

 Master key . . . . . . . . . . . > 7            1-8, *ASP, *SAVRST
 Passphrase . . . . . . . . . . .   Master Key Password- Length 1-256



 Length of passphrase . . . . . .   *CALC        1-256, *CALC










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

Figure 18: Add Master Key Part (ADDMSTPART)

Field/Option/Command Key	Description
Master key	Master key 1 or 2 or 3 up to 8.
Passphrase	Type passphrase. Passphrase entries of a number of users are mixed together.
Length of passphrase	1-256 characters may be chosen.

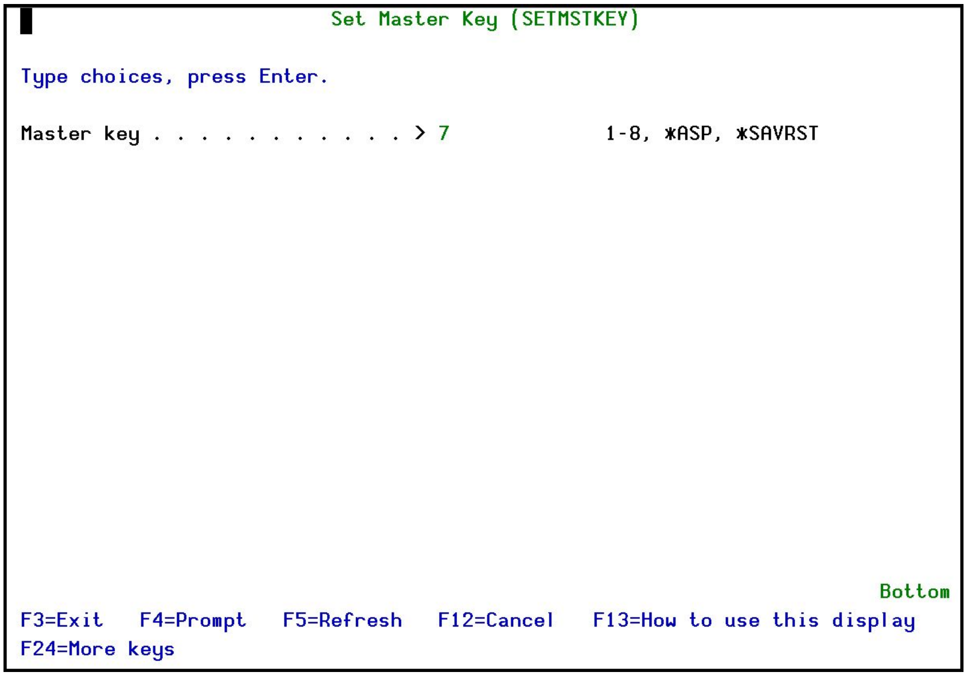
3. Press **F4=Prompt**. The **Specify Value for Parameter MSTKEY** screen appears.

Set Master Key

Setting Master key requires you to select an encryption number between 1-8.

To set Master Key

1. Select **9. Initial Setup** in the **Encryption** main menu. The **Initial Setup** screen appears.
2. Select **Set Master Key**. The **Set Master Key (SETMSTKEY)** screen appears.



```
                          Set Master Key (SETMSTKEY)

Type choices, press Enter.

Master key . . . . . . . . . . . > 7             1-8, *ASP, *SAVRST

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

Figure 19: Set Master Key

1. Type in the number of the Master key that was added before and press **Enter**.

Translate Key File

Translate key file is not to be used regular unless setting of the Master key was done this menu This an option that should not be used regularly because it is included automatically in the option of **Set Master Key** (option 2 of the menu). **Set Master Key** can be done independently (not by option 2) and then complete option 3 of the menu.

To Translate Key File:

3. Select **9. Initial Setup** in the **Encryption** main menu. The **Initial Setup** screen appears.
4. Select **Translate Key File**. The **Translate Key File** screen appears.

Initialize Organizational Key

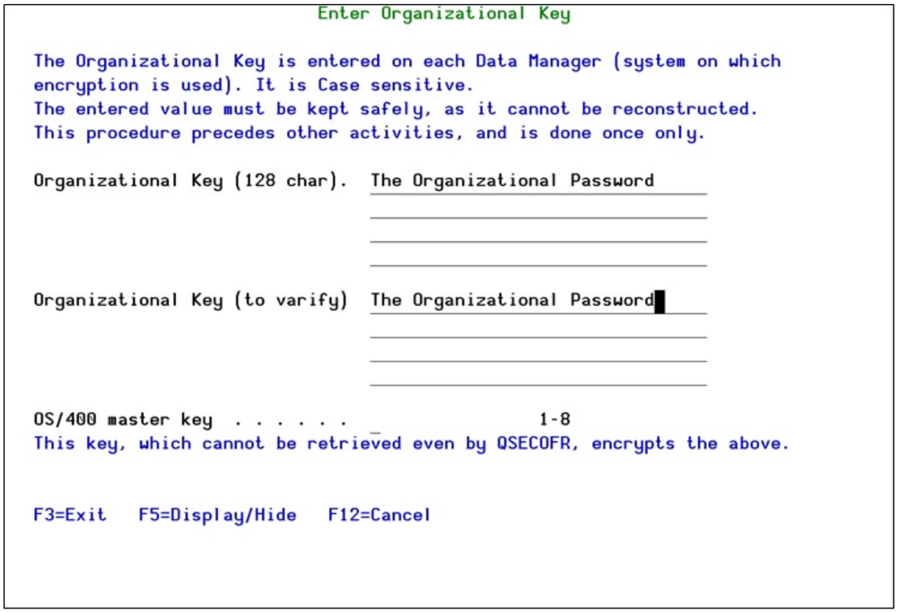
Organizational key must be set for each LPAR that the Encryption runs in (Data and Key LPARs).

The Organizational key MUST BE EXACTLY IDENTICAL in ALL LPARs.

The Master key is used to encrypt the Organization key. The Master key used may be different in one LPAR from another LPAR.

To enter Organizational Key

1. Select **9. Initial Setup** in the **Encryption** Main menu. The **Initial Setup** screen appears.
2. Select **Enter Organizational Key**. The **Enter Organization Key** screen appears.



```
                          Enter Organizational Key

 The Organizational Key is entered on each Data Manager (system on which
 encryption is used). It is Case sensitive.
 The entered value must be kept safely, as it cannot be reconstructed.
 This procedure precedes other activities, and is done once only.

 Organizational Key (128 char).  The Organizational Password




 Organizational Key (to varify)  The Organizational Password




 OS/400 master key  . . . . . .  _               1-8
 This key, which cannot be retrieved even by QSECOFR, encrypts the above.


 F3=Exit   F5=Display/Hide   F12=Cancel
```

Figure 20: Enter Organizational Key

Key Manager

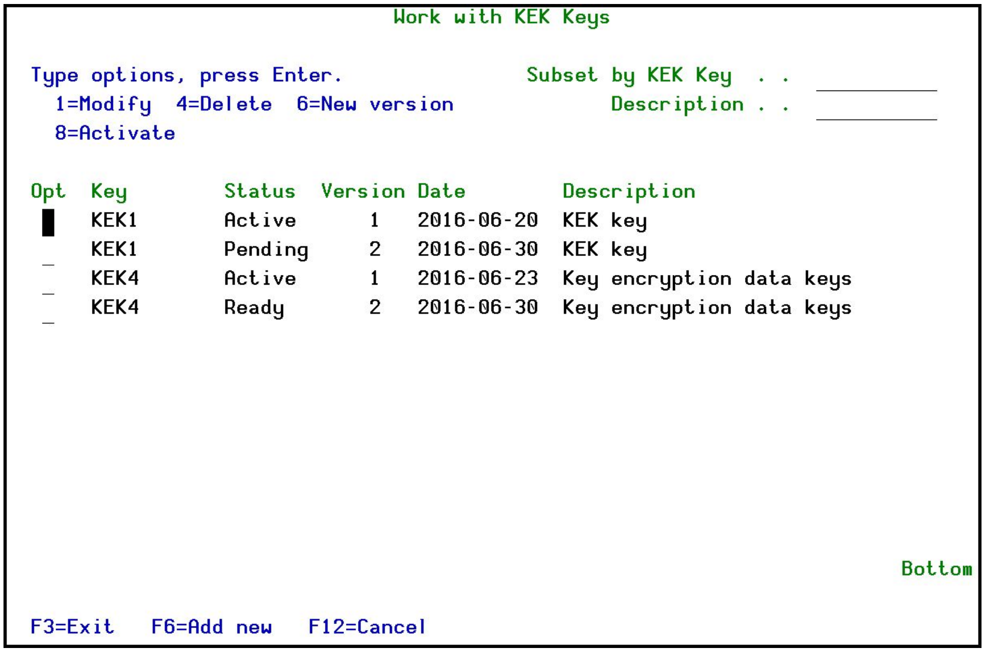
KEK (Key Enc. Keys) Keys

NOTE: Before setting 11. KEK Keys and 12. Data Keys you need to set 16. Key Officers.

Work with KEK Keys

To work with KEK Keys

1. Select **11. KEK (Key Enc. Keys) Keys** in the **Encryption** main menu. The **Work with KEK Keys** screen appears.



```
                                Work with KEK Keys

 Type options, press Enter.                 Subset by KEK Key  . .  __________
   1=Modify  4=Delete  6=New version               Description . .  __________
   8=Activate

 Opt  Key         Status   Version Date        Description
  █   KEK1        Active      1    2016-06-20  KEK key
  _   KEK1        Pending     2    2016-06-30  KEK key
  _   KEK4        Active      1    2016-06-23  Key encryption data keys
  _   KEK4        Ready       2    2016-06-30  Key encryption data keys









                                                                          Bottom

 F3=Exit   F6=Add new   F12=Cancel
```

Figure : Work with KEK Keys

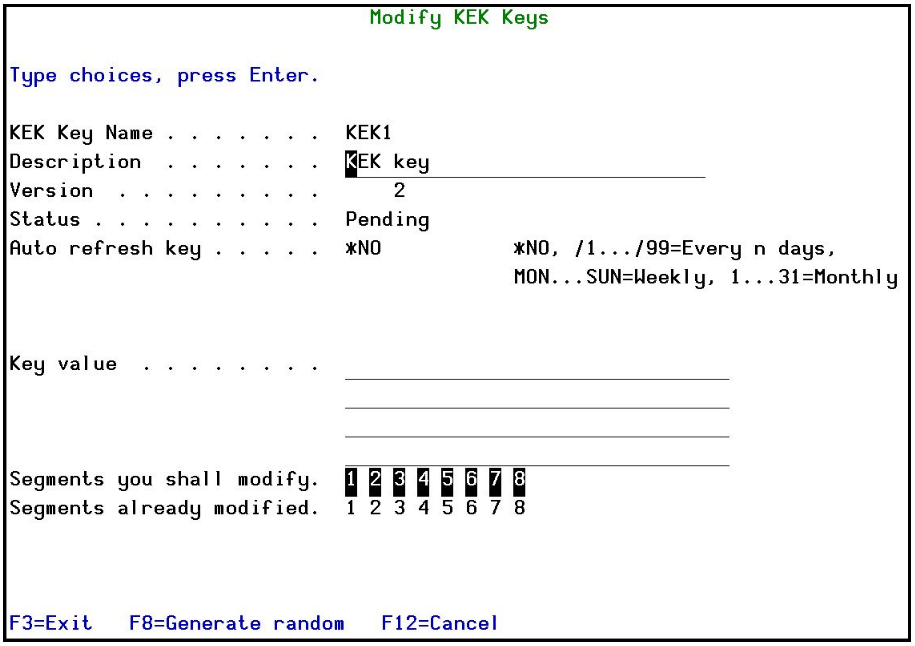
Modify KEK Keys

Warning! When changing the master key, an error may occur indicating that the master key was changed more than once. To overcome this, re-encrypt the Organizational Key by the Master Key, using the following procedure:

1. Delete the file ENLCLKEY in library SMZESYS.
2. Repeat Define Initial Setup: Add Master Key Part, Set Master Key, and Initialize Organizational key.
3. The key must be the exact copy of the original one otherwise all the KEK keys and DATA keys will be lost.

To modify the KEK Keys:

1. Select the KEK Key to modify and press **1=Modify**. The **Modify KEK Keys** screen appears.



```
                              Modify KEK Keys

Type choices, press Enter.

KEK Key Name . . . . . . .   KEK1
Description  . . . . . . .   KEK key
Version  . . . . . . . . .       2
Status . . . . . . . . . .   Pending
Auto refresh key . . . . .   *NO           *NO, /1.../99=Every n days,
                                           MON...SUN=Weekly, 1...31=Monthly


Key value  . . . . . . . .



Segments you shall modify.   1 2 3 4 5 6 7 8
Segments already modified.   1 2 3 4 5 6 7 8



F3=Exit   F8=Generate random   F12=Cancel
```

Figure : Modify KEK Keys

Parameter	Description
KEK Key Name	Name of the KEK Key. It is used to encrypt the Data key. The KEK is encrypted by the Organizational Key
Description	The description of the Key
Version	The version of the KEK key after update/s
Status	The Status of the KEK Key can be Pending before activation.
Auto refresh key	The frequency at which the system is checked for re-encryption. ***NO** = No automatic checking for re-encryption **/1 … /99** = The number of days between checks for re-encryption **MON…SUN** = Check for re-encryption weekly on the given day of the week **1….31** = Check for re-encryption monthly on the given day of the month, but do not use 29, 30, or 31.
Key value	Type in a key-phrase up to 128 alphanumeric characters.
Segments you shall modify. Segments already modified	Each KEK is virtually separated to 8 parts. A key Officer is responsible to fill Up to 8 parts (see defining Key Officer). Here is shown what segments were filled according to the officer's responsibility.
F8=Generate random	Press **F8** to generate random Key values

Only KEK Keys whose status is **Pending** can be modified.

2. Enter the KEK Key definitions and press **Enter**. The KEK Key is updated and appears in the **Work with KEK Keys** screen.

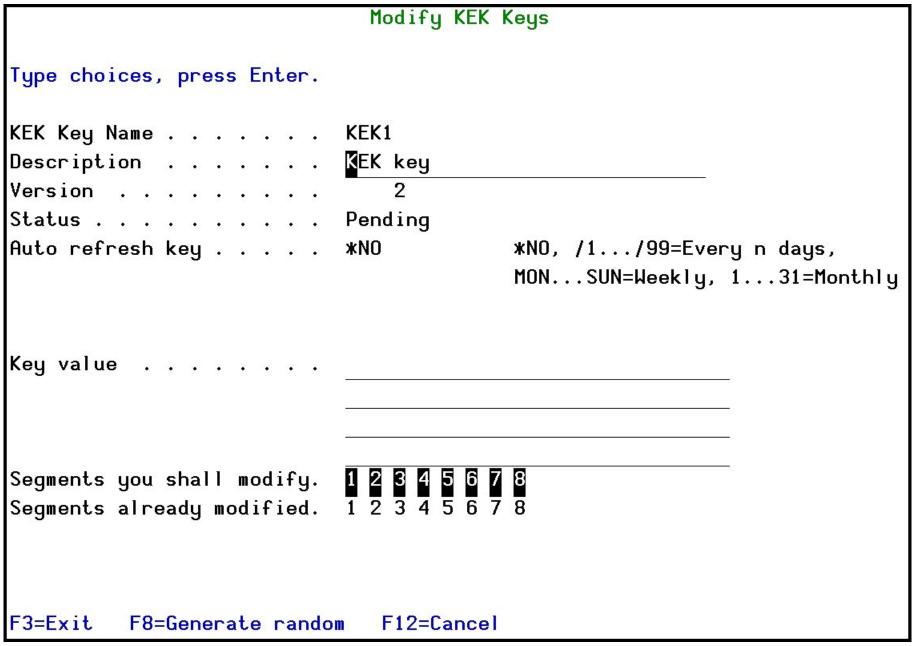
Create a New Version of a KEK Key

You may need to change KEK Keys because of an internal or external compliance requirement. You may also want to change a KEK Key because you feel that it may have become exposed.

You can only create a new version of a KEK Key whose latest version has the **Status** of **Active**.

To create a new version of a KEK Key:

1. Select **11. KEK Keys** in the **Encryption** ain menu. The **Work with KEK Keys** screen appears.
2. Select the **KEK Key** for which you want to create a new version and press **6=New Version**. The **Modify KEK Keys** screen appears with the data for the new version and the **KEK Key** strings unchanged.



```
                              Modify KEK Keys

Type choices, press Enter.

KEK Key Name . . . . . . .  KEK1
Description  . . . . . . .  KEK key
Version  . . . . . . . . .      2
Status . . . . . . . . . .  Pending
Auto refresh key . . . . .  *NO           *NO, /1.../99=Every n days,
                                          MON...SUN=Weekly, 1...31=Monthly


Key value  . . . . . . . .




Segments you shall modify.  1 2 3 4 5 6 7 8
Segments already modified.  1 2 3 4 5 6 7 8



F3=Exit   F8=Generate random   F12=Cancel
```

Figure : Modify KEK Keys

Parameter	Description
KEK Key Name	Name of the KEK Key
Description	The description of the Key
Version	The version of the KEK key after update/s
Status	The Status of the KEK Key can be Pending before activation.
Auto refresh key	The frequency at which the system is checked for re-encryption. ***NO** = No automatic checking for re-encryption **/1 … /99** = The number of days between checks for re-encryption **MON…SUN** = Check for re-encryption weekly on the given day of the week **1….31** = Check for re-encryption monthly on the given day of the month, but do not use 29, 30, or 31.
Key value	Copy from above or delete
Segments you shall modify. **Segments already modified**	Copy from above or delete the description.
F8=Generate random	Press **F8** to generate a random key

3. Enter the new **KEK Key** strings and press **Enter**. The new version of the KEK Key is created with the **Status** of **Pending** and now appears in the **Work with KEK Keys** screen.

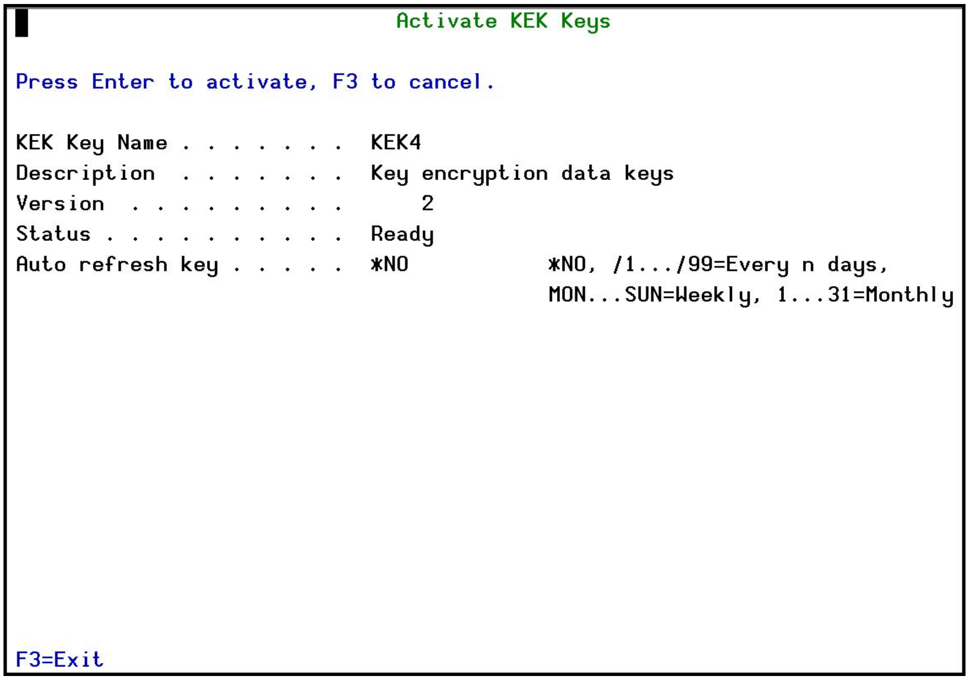
Activate KEK Keys

After you have created a new version of a KEK Key, you must activate it for all associated Data Keys to use it for encryption.

You can only activate a KEK Key with a **Status** of **Ready**.

To activate a KEK Key:

1. Select **11. KEK Keys** in the **Encryption** main menu. The **Work with KEK Keys** screen appears.
2. Select the **KEK Key** for which you want to activate a pending version and press **8=Activate**. The **Activate KEK Keys** screen appears.



```
                               Activate KEK Keys

Press Enter to activate, F3 to cancel.

KEK Key Name . . . . . . .   KEK4
Description  . . . . . . .   Key encryption data keys
Version  . . . . . . . . .       2
Status . . . . . . . . . .   Ready
Auto refresh key . . . . .   *NO           *NO, /1.../99=Every n days,
                                           MON...SUN=Weekly, 1...31=Monthly














F3=Exit
```

Figure : Activate KEK Keys

3. Press **Enter**. The KEK Key version is activated and the updated **Work with KEK Keys** screen appears.

Delete KEK Keys

To delete KEK Keys:

1. Select **11. KEK Keys** in the **Encryption** main menu. The **Work with KEK Keys** screen appears.
2. Select the **KEK Key** to delete and press **4=Delete**. The **Delete KEK Keys** screen appears.
3. Press **Enter**. The **KEK Key** is deleted and the updated **Work with KEK Keys** screen appears.

Only KEK Keys not used by Data Keys can be deleted.

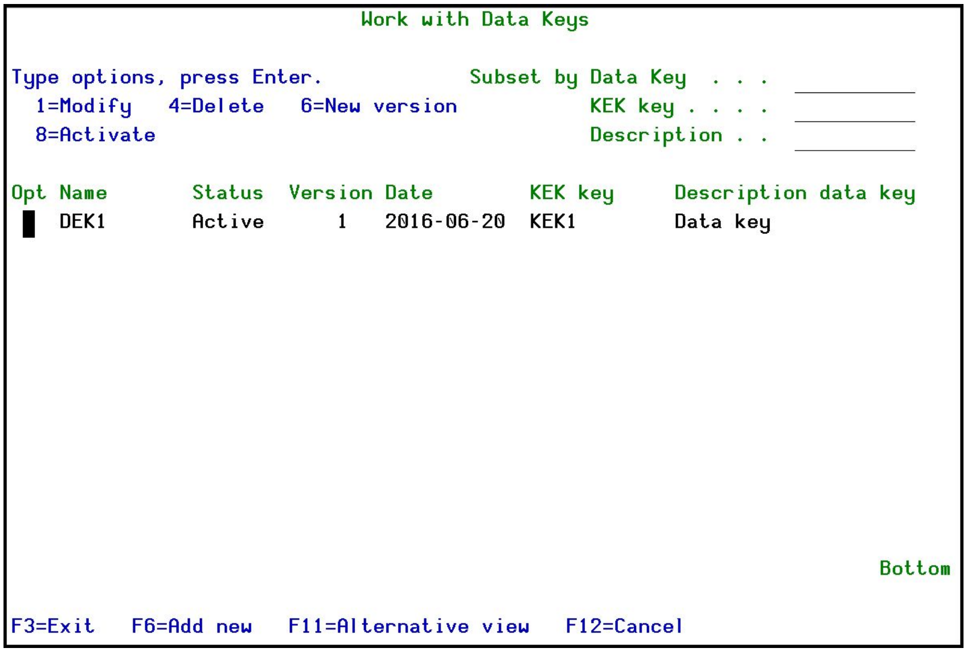
Data Keys

The Data Keys are used to encrypt the Data Fields to which they are assigned. The Data Keys themselves are protected by a KEK Key. You can also require the Data Key to be defined by up to eight different users (see Key Officers for more details).

Add Data Keys

To add Data Keys:

1. Select **12. Data Keys** in the **Encryption** Main menu. The **Work with Data Keys** screen appears.

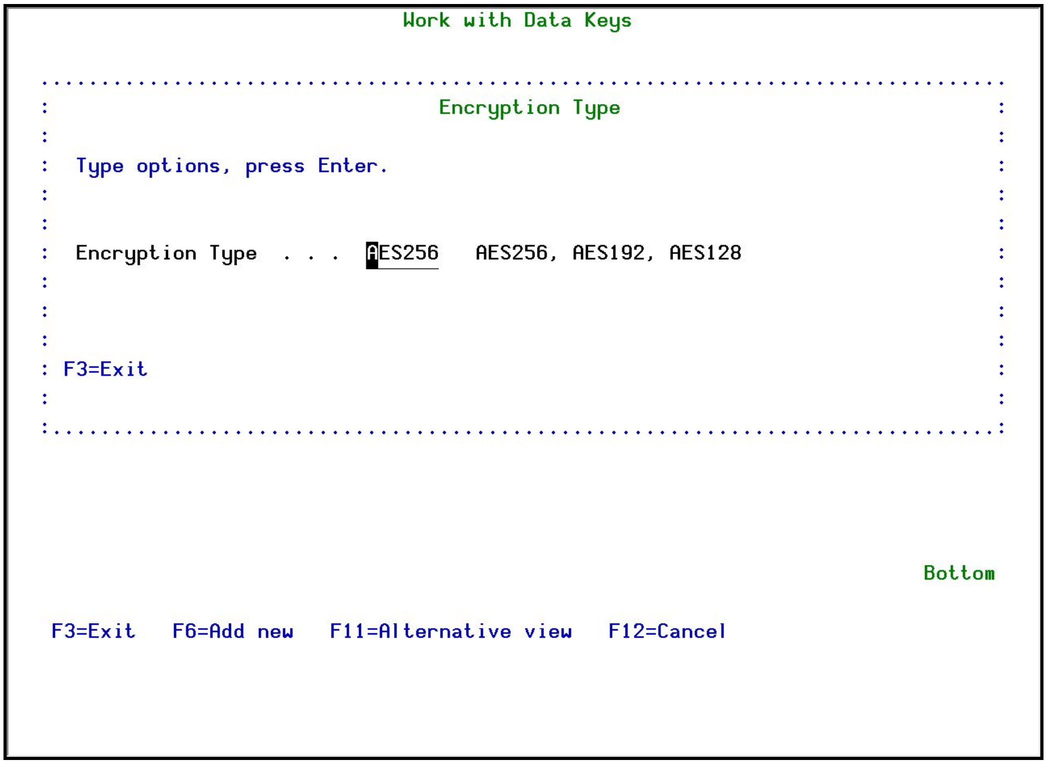


```
                              Work with Data Keys

Type options, press Enter.                  Subset by Data Key  . . .
  1=Modify    4=Delete    6=New version               KEK key . . . .
  8=Activate                                          Description . .

Opt Name         Status   Version Date         KEK key      Description data key
    DEK1         Active         1   2016-06-20 KEK1         Data key








                                                                          Bottom

F3=Exit   F6=Add new   F11=Alternative view   F12=Cancel
```

Figure : Work with Data Keys

Parameter	Description
Opt	Type one of the options to Enter: 1=Modify; Modify fields of the Data Keys in Modify Data Keys screen 4=Delete; Delete Data Keys 6=New Version; Create New Version of Data Keys 8=Activate; Activate Data Keys created
Name	The data key name
Status	The status of data key: Encrypted/Not Encrypted
Version	The version of data key
Date	The date of creation of data key
KEK key	The KEK Key belonging to the current data key selected
Description data key	The description of the data key

2. Press **F6=Add new**. The **Encryption Type** screen appears.

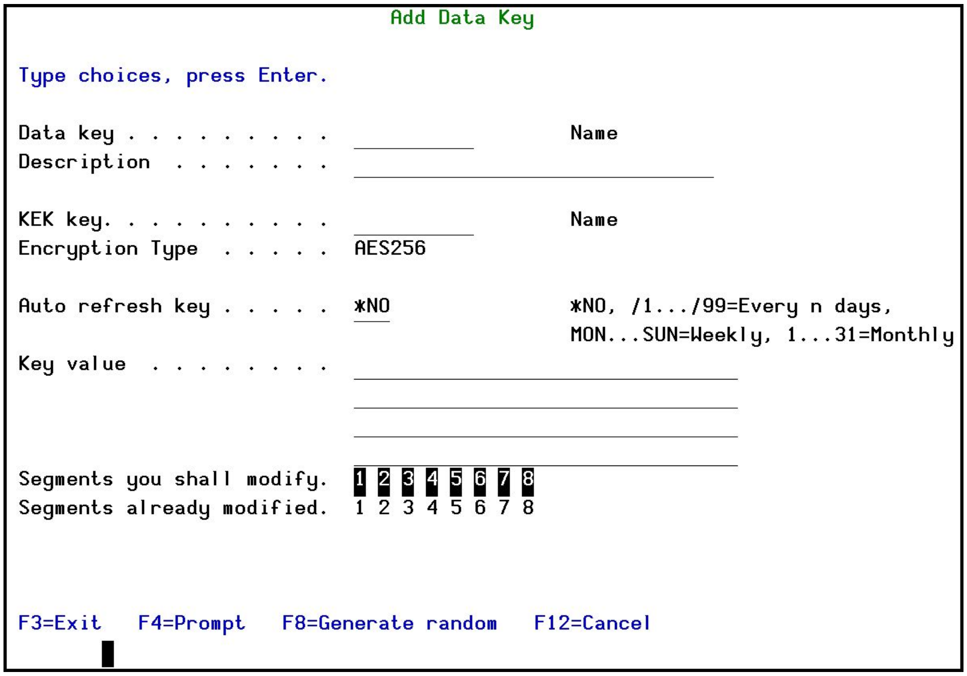


```
                          Work with Data Keys

 ...........................................................................
 :                              Encryption Type                           :
 :                                                                        :
 :  Type options, press Enter.                                            :
 :                                                                        :
 :                                                                        :
 :  Encryption Type  . . .  AES256   AES256, AES192, AES128               :
 :                                                                        :
 :                                                                        :
 :                                                                        :
 : F3=Exit                                                                :
 :                                                                        :
 :........................................................................:




                                                                    Bottom

 F3=Exit   F6=Add new   F11=Alternative view   F12=Cancel
```

Figure : Encryption Type

Parameter	Description
Encryption Type	The encryption type for this key **AES128** - Use the Advanced Field Encryption Standard 128 bit encryption **AES192** - Use the Advanced Field Encryption Standard 192 bit encryption **AES256** - Use the Advanced Field Encryption Standard 256 bit encryption (default)

3. Enter the **Encryption Type** to use and press **Enter**. The **Add Data Key** screen appears.



```
                              Add Data Key

Type choices, press Enter.

Data key . . . . . . . . .   __________        Name
Description  . . . . . . .   ______________________________

KEK key. . . . . . . . . .   __________        Name
Encryption Type  . . . . .   AES256

Auto refresh key . . . . .   *NO               *NO, /1.../99=Every n days,
                                               MON...SUN=Weekly, 1...31=Monthly
Key value  . . . . . . . .   ________________________________
                             ________________________________
                             ________________________________
                             ________________________________
Segments you shall modify.   1 2 3 4 5 6 7 8
Segments already modified.   1 2 3 4 5 6 7 8



F3=Exit   F4=Prompt   F8=Generate random   F12=Cancel
```

Figure : Add Data Key

Parameter	Description
Data Key	The name of the Key
Description	The description of the Key
KEK Key	The KEK Key that is to be used with this Data Key. You can use F4 to choose the KEK. If you don't see a KEK that you defined you probably did not activated it.
Encryption Type	The encryption type for this key
Auto refresh key	The frequency at which the system is checked for re-encryption. ***NO** = No automatic checking for re-encryption **/1 … /99** = The number of days between checks for re-encryption **MON…SUN** = Check for re-encryption weekly on the given day of the week **1….31** = Check for re-encryption monthly on the given day of the month, but do not use 29, 30, or 31.
Key Value	Type a key phrase. The Key phrase is divided virtually to 8 parts.
	Your organization may decide that the definition of the full Data Key will be done by more than one person, up to a maximum of eight. . See Key Officers for more details.
F8=Generate random	Press **F8** to generate a random key

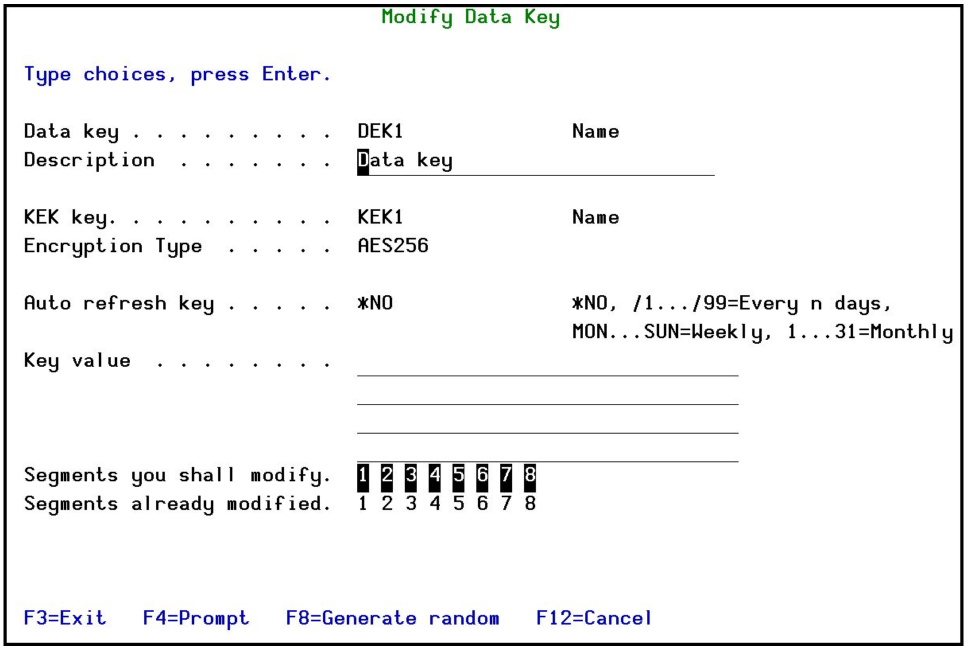
4. Enter the Data Key definitions and press **Enter**. The new Data Key is added and now appears in the **Work with Data Keys** screen.

Modify Data Keys

To modify Data Keys:

Only Data Keys with a **Status** of **Pending** can be modified. A Data Key with a **Status** of **Active** cannot be modified.

1. Select **12. Data Keys** in the **Encryption** main menu. The **Work with Data Keys** screen appears.
2. Select the Data Key to modify and press **1=Modify**. The **Modify Data Key** screen appears.



```
                              Modify Data Key

Type choices, press Enter.

Data key . . . . . . . . .   DEK1                 Name
Description  . . . . . . .   Data key

KEK key. . . . . . . . . .   KEK1                 Name
Encryption Type  . . . . .   AES256

Auto refresh key . . . . .   *NO                  *NO, /1.../99=Every n days,
                                                  MON...SUN=Weekly, 1...31=Monthly
Key value  . . . . . . . .




Segments you shall modify.   1 2 3 4 5 6 7 8
Segments already modified.   1 2 3 4 5 6 7 8



F3=Exit   F4=Prompt   F8=Generate random   F12=Cancel
```

Figure : Modify Data Key

Parameter	Description
Data Key	The name of the Key
Description	The description of the Key
KEK Key	The KEK Key that is to be used with this Data Key
Encryption Type	The encryption type for this key
Auto refresh key	The frequency at which the system is checked for re-encryption. ***NO** = No automatic checking for re-encryption **/1 … /99** = The number of days between checks for re-encryption **MON…SUN** = Check for re-encryption weekly on the given day of the week **1….31** = Check for re-encryption monthly on the given day of the month, but do not use 29, 30, or 31.
Key Value	Copy from above or delete
	Copy from above or delete
F8=Generate random	Press **F8** to generate a random key

3. Enter the Data Key definitions and press **Enter**. The Data Key is updated and now appears in the **Work with Data Keys** screen.

Create a New Version of a Data Key

You may need to change Data Keys because of an internal or external compliance requirement. You may also want to change a Data Key because you feel that it may have become exposed.

You can only update a Data Key whose latest version has the **Status** of **Active**.

To create a new version of a Data Key:

1. Select **12. Data Keys** in the **Encryption** main menu. The **Work with Data Keys** screen appears.
2. Select the Data Key for which you want to create a new version and press **6=New version**. The **Modify Data Key** screen appears.
3. Enter the new **Data Key** strings and press **Enter**. The new version of the Data Key is created with the **Status** of **Pending** and now appears in the **Work with Data Keys** screen.

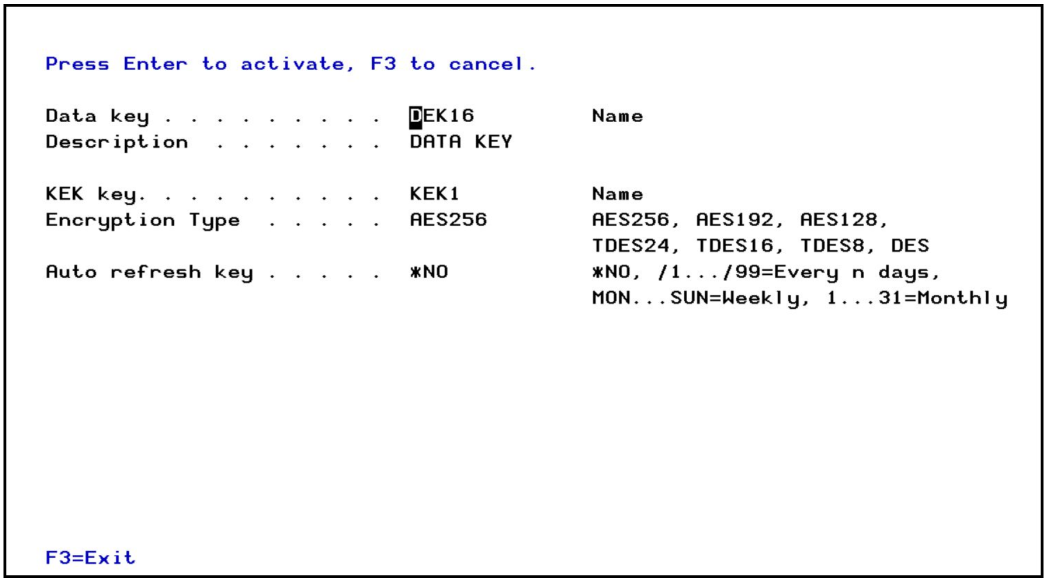
Activate Data Keys

After you have created a new version of a Data Key, you must activate it for all associated fields to use it for encryption. (This option is relevant for Field Rotate Type with a value of 6, in the Add Occurrence screen.)

You can only activate a Data Key with a **Status** of **Pending**.

To activate a Data Key:

1. Select **12. Data Keys** in the **Encryption** main menu. The **Work with Data Keys** screen appears.
2. Select the Data Key for which you want to activate a pending version and press **8=Activate**. The **Activate Data Key** screen appears.



```
Press Enter to activate, F3 to cancel.

Data key . . . . . . . . .   DEK16          Name
Description  . . . . . . .   DATA KEY

KEK key. . . . . . . . . .   KEK1           Name
Encryption Type  . . . . .   AES256         AES256, AES192, AES128,
                                            TDES24, TDES16, TDES8, DES
Auto refresh key . . . . .   *NO            *NO, /1.../99=Every n days,
                                            MON...SUN=Weekly, 1...31=Monthly

F3=Exit
```

Figure : Activate Data Key

3. Press **Enter**. The Data Key version is activated and the updated **Work with Data Keys** screen appears.

Delete Data Keys

To delete Data Keys:

You cannot delete a Data Key that has a later version. You must first delete the later versions. Also, you cannot delete Data Keys that have associated fields.

1. Select **12. Data Keys** in the **Encryption** main menu. The **Work with Data Keys** screen appears.
2. Select the Data Key to delete and press **4=Delete**. The **Delete Data Keys** screen appears.
3. Press **Enter**. The Data Key is deleted and the updated **Work with Data Keys** screen appears.

-

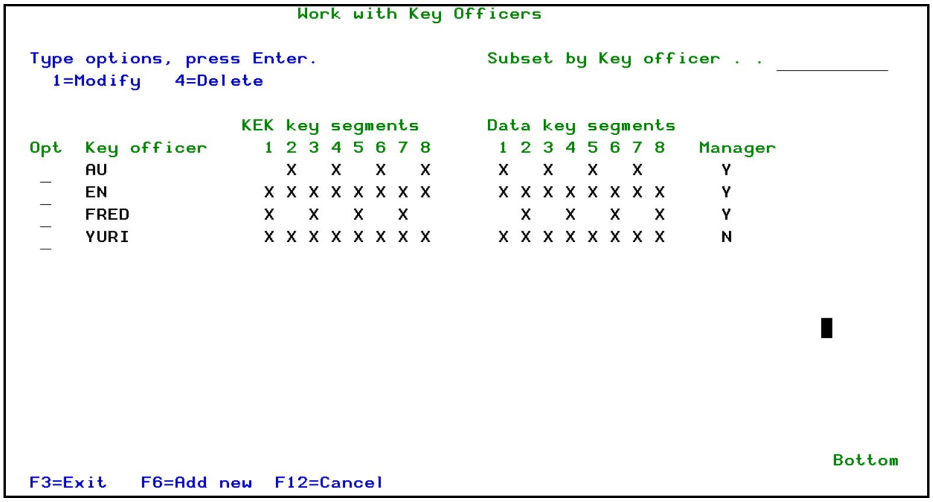
Key Officers

Only Key Officers can administrate KEK Keys, and Data Keys. Define which users can perform these tasks. You can define that users who maintain KEK Keys cannot maintain Data Keys and visa versa. You can also limit users to be able to maintain only part of a key, so that for a new key, more than one user needs authentication.

Add Key Officers

To add Key Officers:

1. Select **16. Key Officers** in the **Encryption** main menu. The **Work with Key Officers** screen appears.

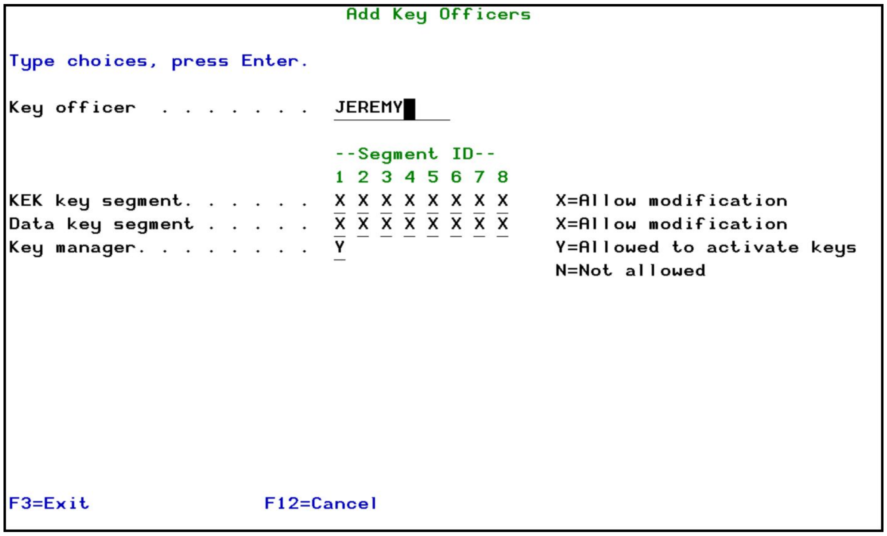


```
                        Work with Key Officers

Type options, press Enter.               Subset by Key officer . .  __________
  1=Modify   4=Delete

                   KEK key segments      Data key segments
Opt  Key officer     1 2 3 4 5 6 7 8      1 2 3 4 5 6 7 8   Manager
 _   AU                X   X   X   X      X   X   X   X       Y
 _   EN              X X X X X X X X      X X X X X X X X     Y
 _   FRED            X   X   X   X          X   X   X   X     Y
 _   YURI            X X X X X X X X      X X X X X X X X     N






                                                                        Bottom
F3=Exit   F6=Add new  F12=Cancel
```

Figure : Work with Key Officers

Parameter	Description
Option	Type one of the options to Enter: 1=Modify; Modify fields of the Data Keys in Modify Data Keys screen 4=Delete; Delete Data Keys
Key officer	The user profiles who are Key Officers
KEK key segments	**X** marks the segments this Key Officer is permitted to enter
Data key segments	**X** marks the segments this Key Officer is permitted to enter
Manager	Indicates if the officer is allowed to activate the key.

2. Press **F6=Add New**. The **Add Key Officers** screen appears.



```
                                Add Key Officers

Type choices, press Enter.

Key officer  . . . . . . .   JEREMY

                             --Segment ID--
                             1 2 3 4 5 6 7 8
KEK key segment. . . . . .   X X X X X X X X    X=Allow modification
Data key segment . . . . .   X X X X X X X X    X=Allow modification
Key manager. . . . . . . .   Y                  Y=Allowed to activate keys
                                                N=Not allowed








F3=Exit                   F12=Cancel
```

Figure : Add Key Officers

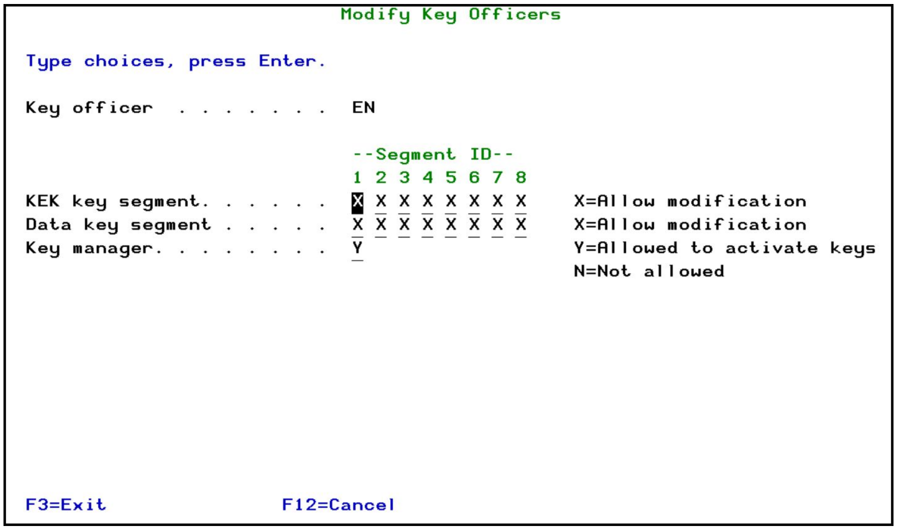
Parameter	Description
Key Officer	Enter a user profile who will be a Key Officer
KEK Key segments	Enter **X** in the segments this Key Officer will be permitted to enter
Data Key segments	Enter **X** in the segments this Key Officer will be permitted to enter
Manager	Indicates if the officer is allowed to activate the key.

3. Enter the Key Officer definitions and press **Enter**. The new Key Officer is added and now appears in the **Work with Key Officers** screen.

Modify Key Officers

To modify Key Officers:

1. Select **16. Key Officers** in the **Encryption** main menu. The **Work with Key Officers** screen appears.
2. Select the **Key Officer** to modify and press **1=Modify**. The **Modify Key Officers** screen appears.



```
                          Modify Key Officers

 Type choices, press Enter.

 Key officer  . . . . . . .   EN

                              --Segment ID--
                              1 2 3 4 5 6 7 8
 KEK key segment. . . . . .   X X X X X X X X    X=Allow modification
 Data key segment . . . . .   X X X X X X X X    X=Allow modification
 Key manager. . . . . . . .   Y                  Y=Allowed to activate keys
                                                 N=Not allowed











 F3=Exit                 F12=Cancel
```

Figure : Modify Key Officers

Parameter	Description
Key Officer	Enter a user profile who will be a Key Officer
KEK Key segments	Enter **X** in the segments this Key Officer will be permitted to enter
Data Key segments	Enter **X** in the segments this Key Officer will be permitted to enter
Manager	Indicates if the officer is allowed to activate the key.

3. Enter the Key Officer definitions and press **Enter**. The Key Officer is updated and now appears in the **Work with Key Officers** screen.

Delete Key Officers

To delete a Key Officer:

1. Select **16. Key Officers** in the **Encryption** main menu. The **Work with Key Officers** screen appears.
2. Select the Key Officer to delete and press **4=Select**. The **Delete Key Officers** screen appears.
3. Press **Enter**. The Key Officer is deleted and the updated **Work with Key Officers** screen appears.

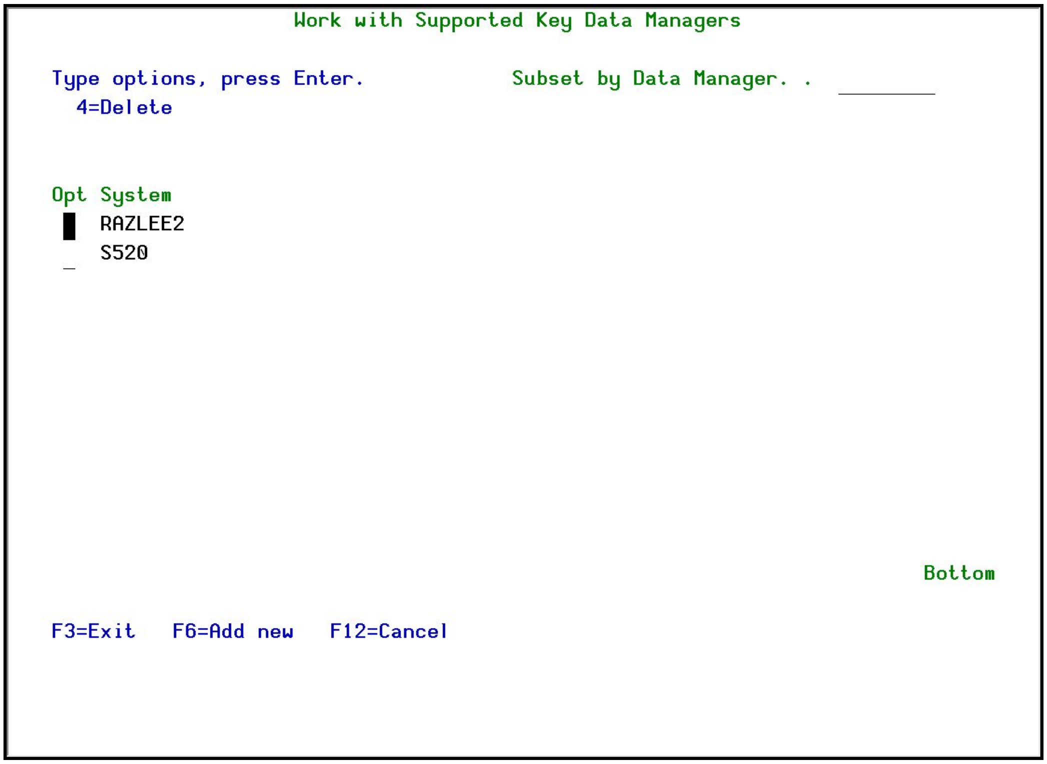
Supported Data Manager Environments

When the Key Manager and the Data Manager are not on the same computer, you must define the Data Manager environments to the Key Manager.

Add Supported Data Manager Systems

To add Data Manager Environments:

1. Select **19. Supported Data Manager Systems** in the **Encryption** main menu. The **Work with Supported Key Data Managers** screen appears.

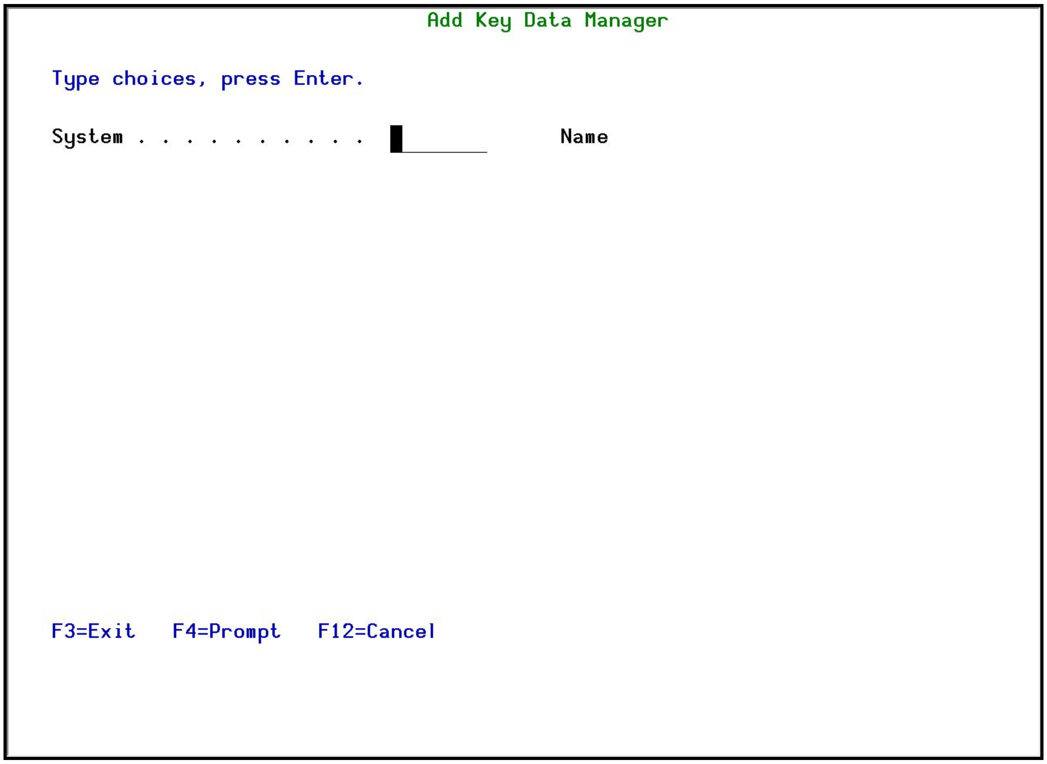


```
                     Work with Supported Key Data Managers

Type options, press Enter.              Subset by Data Manager. .  ________
  4=Delete


Opt System
 _  RAZLEE2
 _  S520








                                                                    Bottom

F3=Exit   F6=Add new   F12=Cancel
```

Figure : Work with Supported Key Data Managers

Parameter	Description
System	The Systems on which the Data Manager is installed.

2. Press **F6=Add New**. The **Add Key Data Manager** screen appears.



```
                              Add Key Data Manager

 Type choices, press Enter.

 System . . . . . . . . . .  _______     Name








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

Figure : Add Key Data Manager

3. Enter the **System** where the Data Manager is installed and press **Enter**. The System is added and now appears in the updated **Work with Supported Key Data Managers** screen.

If you do not know the correct name of the system to add, press **F4=Prompt** and select a system from the displayed list.

Delete Data Manager Environments

To delete Data Manager Environments:

1. Select **19. Data Managers** in the **Encryption** main menu. The **Work with Supported Key Data Managers** screen appears.
2. Select the System to delete and press **4=Select**. The **Delete Key Data Manager** screen appears.
3. Press **Enter**. The System is deleted and the updated **Work with Supported Key Data Managers** screen appears.

Token Manager

The Token Manager enables you to define in which environments the Data Manager is accessible.

The Token Manager can only be worked on if you are working in the specific environment defined for the Token Manager in the **General Definitions** of the Encryption configuration. See Encryption/Tokenization General Definitions for more details.

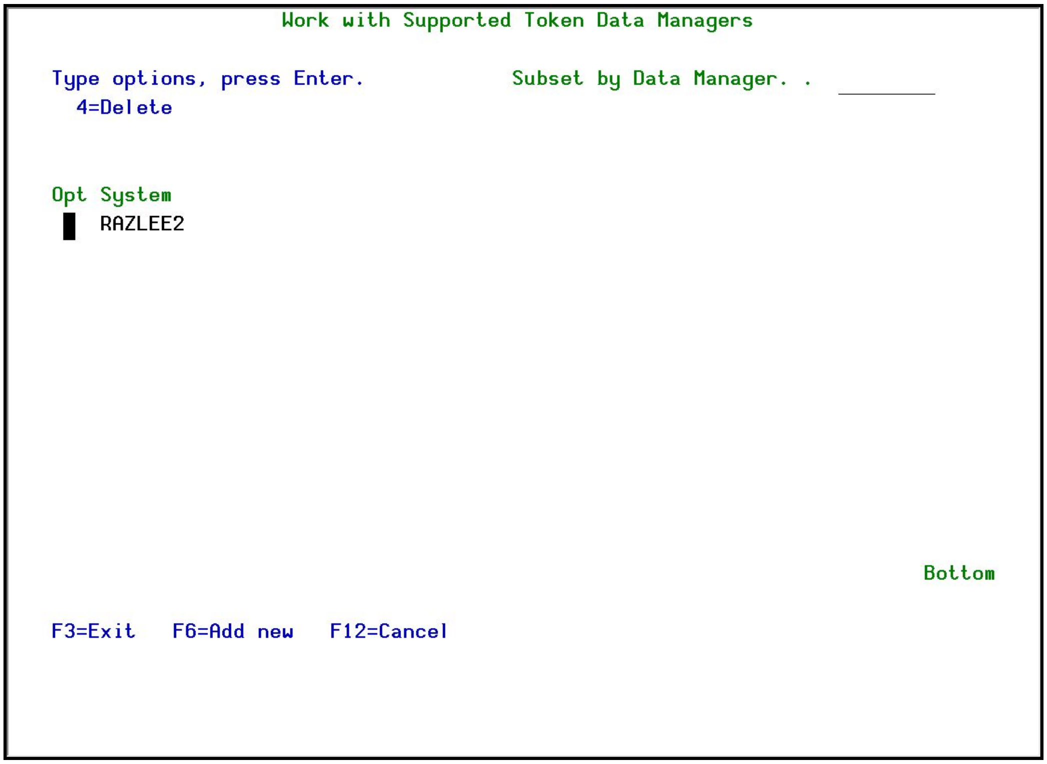
Supported Data Managers

When the Token Manager and the Data Manager are not on the same computer, you must define the Data Manager environments to the Token Manager.

Add Data Manager Environments

To add Data Manager Environments:

1. Select **29. Supported Data Manager Systems** in the **Encryption** main menu. The **Work with Supported Token Data Managers** screen appears.

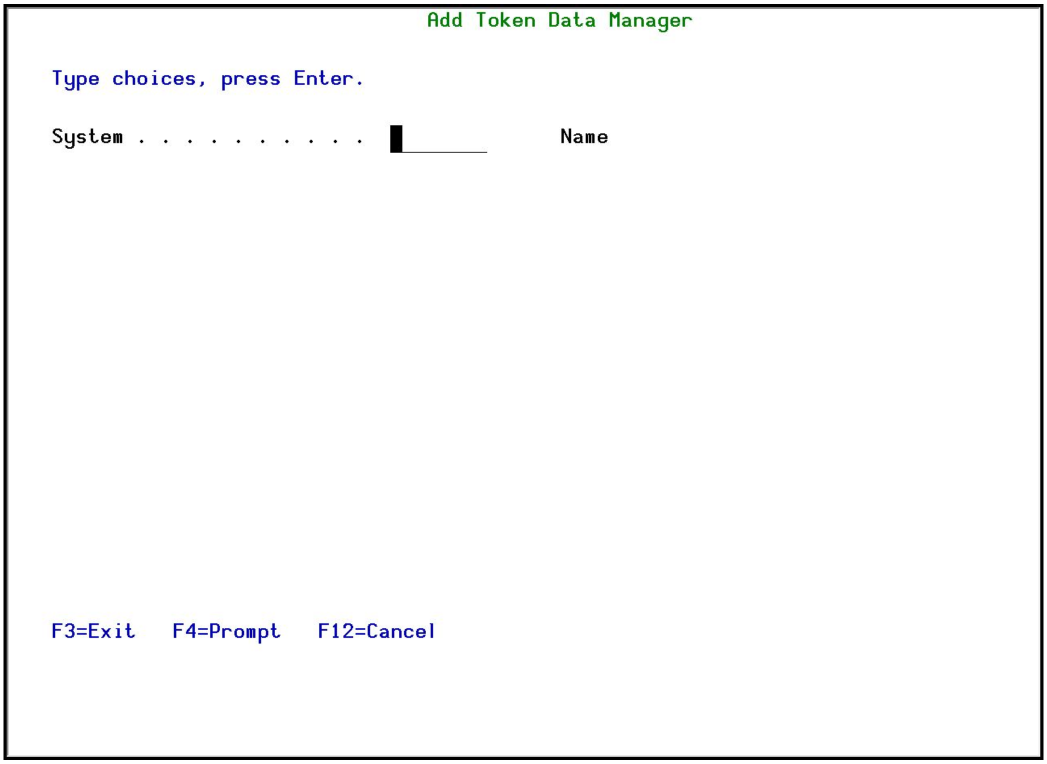


```
                    Work with Supported Token Data Managers

 Type options, press Enter.           Subset by Data Manager. .  ________
   4=Delete


 Opt System
 █   RAZLEE2











                                                                  Bottom

 F3=Exit   F6=Add new   F12=Cancel
```

Figure : Work with Supported Token Data Managers

Parameter	Description
System	The Systems on which the Data Manager is installed.

2. Press **F6=Add New**. The **Add Token Data Manager** screen appears.



```
                               Add Token Data Manager

   Type choices, press Enter.

   System . . . . . . . . . .  _______       Name









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

Figure : Add Token Data Manager

3. Enter the **System** where the Data Manager is installed and press **Enter**. The System is added and now appears in the updated **Work with Supported Token Data Managers** screen.

If you do not know the correct name of the system to add, press **F4=Prompt** and select a system from the displayed list.

Delete Data Manager Environments

To delete Data Manager Environments:

1. Select **29. Data Managers** in the **Encryption** main menu. The **Work with Supported Token Data Managers** screen appears.
2. Select the System to delete and press **4=Select**. The **Delete Data Manager** screen appears.
3. Press **Enter**. The System is deleted and the updated **Work with Supported Token Data Managers** screen appears.

Find Fields to Encrypt

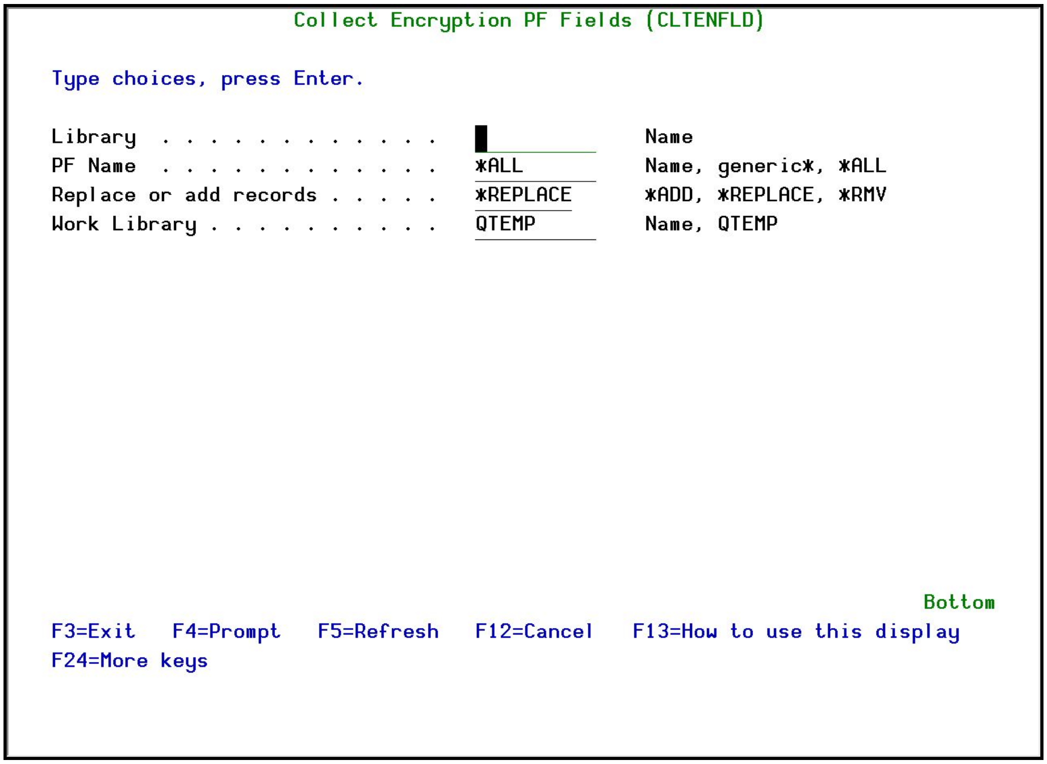
You should ensure that you encrypt all sensitive fields in the system. You do this by first collecting fields from all physical files in the systems in which you want to use Encryption and then within that collection of fields, you can identify the relevant sensitive fields.

Collect Prod Libraries Fields

You must run this option once for every library for which you want to collect fields. The fields you collect will be placed in a work library for further processing. After you have run the option for every library, run the process described in Identify Sensitive Fields.

To collect display file fields from a library:

1. Select **31. Collect Prod Libraries Fields** in the **Encryption** main menu. The **Collect Encryption PF Fields** screen appears.



```
                      Collect Encryption PF Fields (CLTENFLD)

 Type choices, press Enter.

 Library . . . . . . . . . . . .   █            Name
 PF Name . . . . . . . . . . . .   *ALL         Name, generic*, *ALL
 Replace or add records . . . . .  *REPLACE     *ADD, *REPLACE, *RMV
 Work Library . . . . . . . . . .  QTEMP        Name, QTEMP

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

Figure : Collect Encryption PF Fields

Parameter	Description
Library	The name of the library for which you want to collect fields.
PF name	The name of the physical file for which you want to collect fields. **Name** – The name of a specific file **generic*** - A group of files ***ALL** – All the physical files in the library
Replace or add records	Describes what to do with the collected information ***ADD** – Add the records to the Work File ***REPLACE** – Replace all existing records in the Work File relating to the selected Library and File with new records ***RMV** – Remove all records relating to the selected Library and File
Work Library	The name of the library to receive the results. The default is QTEMP. Note that if you work with QTEMP, you must finish the process by running Identify Sensitive Fields before signing off from the session. If you sign off, then all information is lost and you must repeat the collection process again. Also, if you work with QTEMP, you must run the Identify Sensitive Fields option from the same workstation.

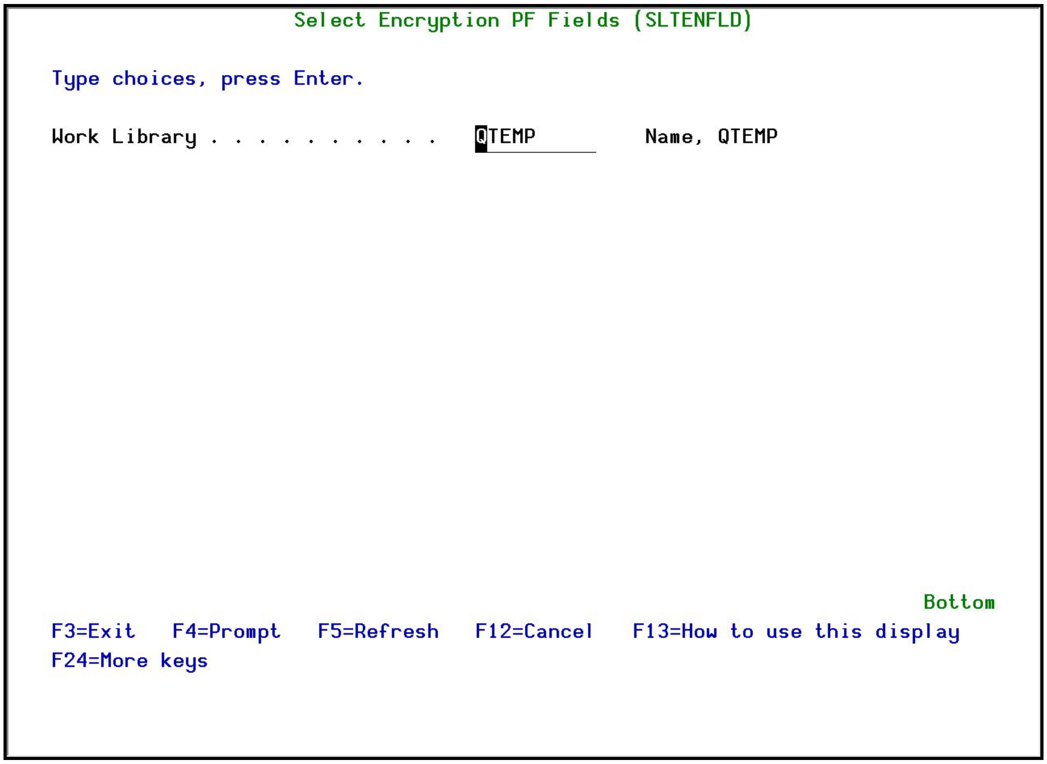
2. Enter your required parameters and press **Enter**. The fields that match the parameter requirements are collected.

Identify Sensitive Fields

Before you identify the Business Items in the display files, you must first prepare the information by running the process described in Collect Prod Libraries Fields .

To identify sensitive fields:

1. Select **32. Identify Sensitive Fields** in the **Encryption** main menu. The **Select Encryption PF Fields** screen appears.

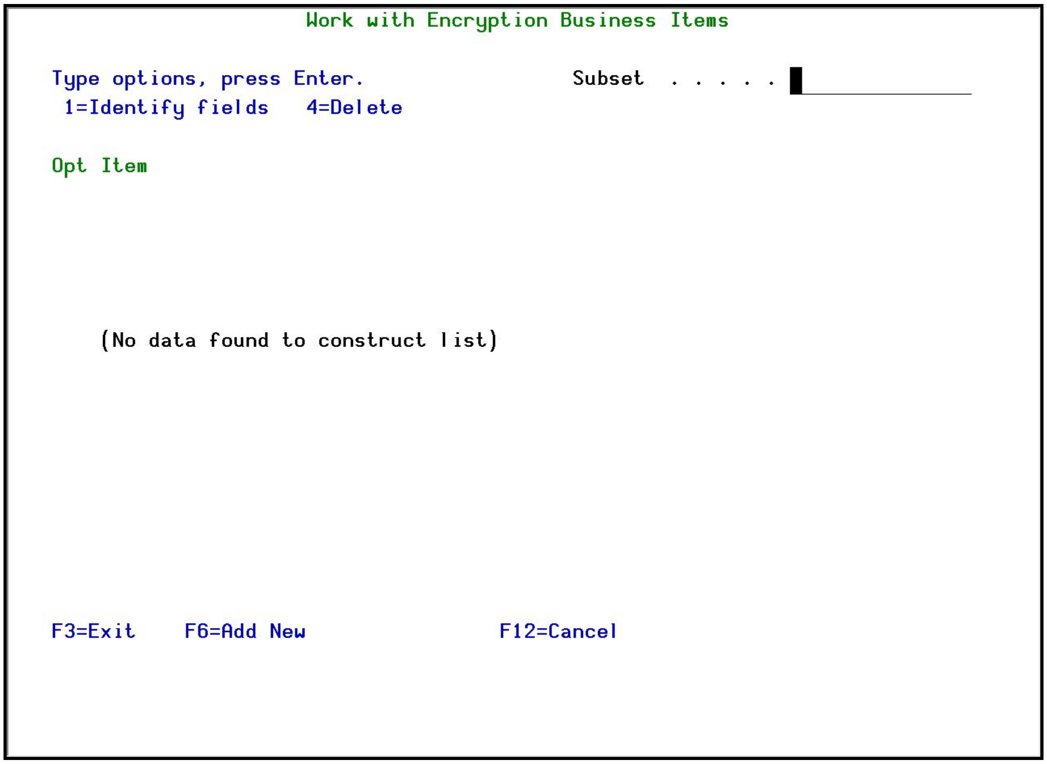


```
                    Select Encryption PF Fields (SLTENFLD)

 Type choices, press Enter.

 Work Library . . . . . . . . . .   QTEMP         Name, QTEMP











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

Figure : Select Encryption PF Fields

2. Enter the **Work Library** you used in the Collect Prod Libraries Fields process and press **Enter**. The **Work with Encryption Business Items** screen appears.

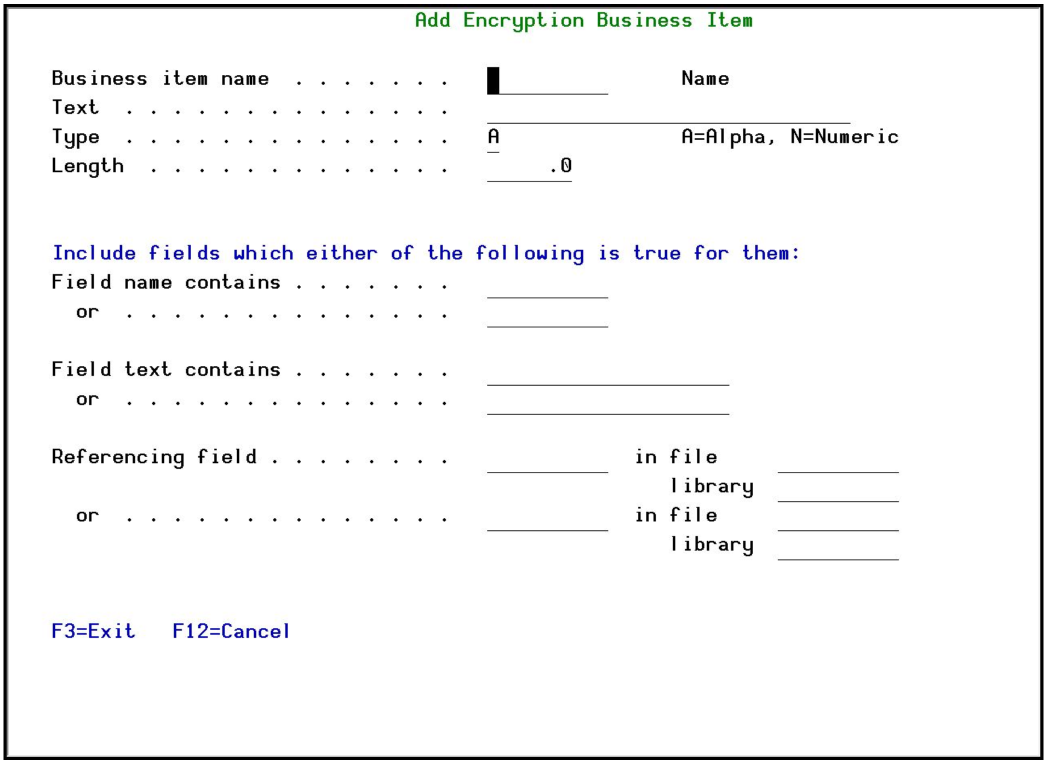
The example shown is how the screen appears the very first time, before any fields have been added.



```
                          Work with Encryption Business Items

  Type options, press Enter.                  Subset . . . . . 
   1=Identify fields   4=Delete

  Opt Item





      (No data found to construct list)








  F3=Exit    F6=Add New                F12=Cancel
```

Figure : Work with Encryption Business Items

3. Press **F6=Add New**. The **Add Encryption Business Item** screen appears.

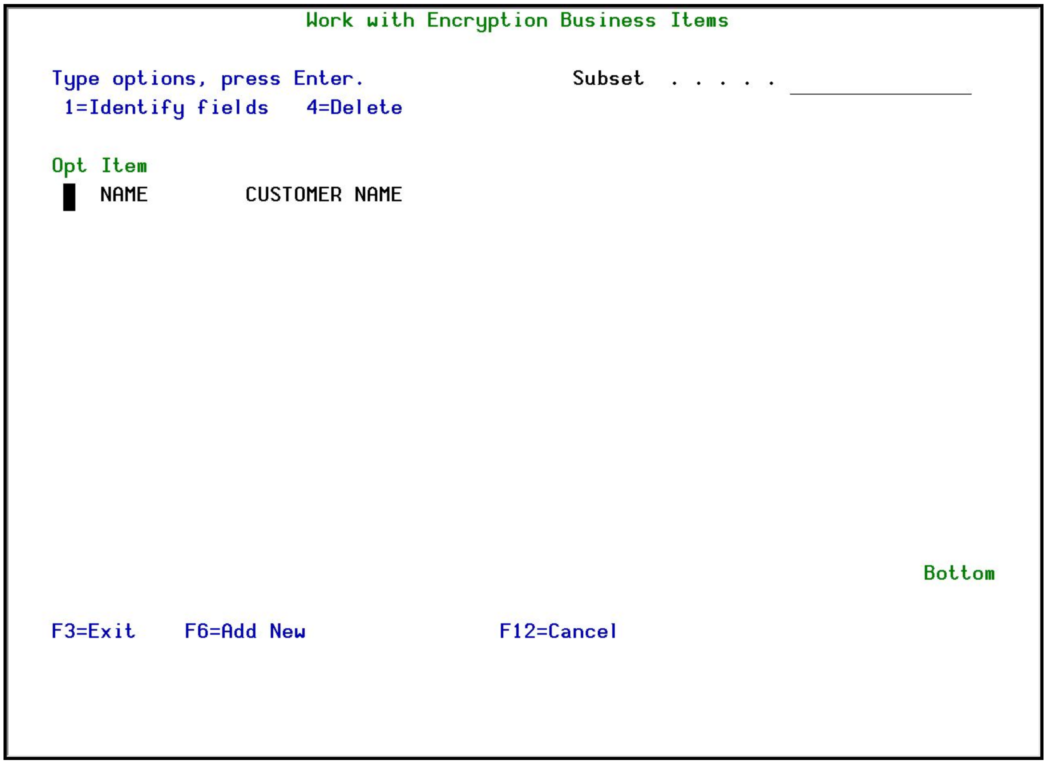


```
                                   Add Encryption Business Item

  Business item name . . . . . . .               Name
  Text . . . . . . . . . . . . . .
  Type . . . . . . . . . . . . . .   A               A=Alpha, N=Numeric
  Length . . . . . . . . . . . . .         .0


  Include fields which either of the following is true for them:
  Field name contains . . . . . . .
    or . . . . . . . . . . . . . .

  Field text contains . . . . . . .
    or . . . . . . . . . . . . . .

  Referencing field . . . . . . .              in file
                                                  library
    or . . . . . . . . . . . . . .             in file
                                                  library


  F3=Exit   F12=Cancel
```

Figure : Add Encryption Business Item screen

Parameters	Description
Business item name	Enter a unique name for the Business Item.
Text	Enter a meaningful description of the Business Item
Type	Type of the fields to be identified **A** = Alphameric **N** = Numeric
Length	Length of fields to be identified. Remember to include the number of decimal places for numeric fields.

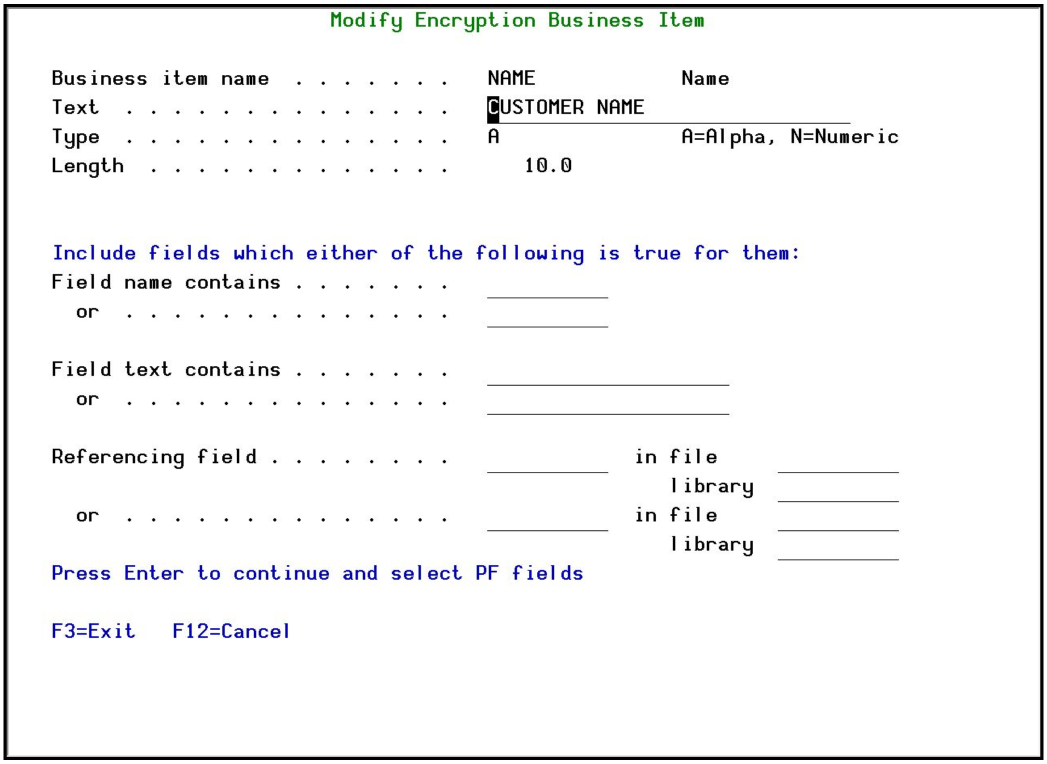
4. In the first four fields, enter the details of the **Business Item** you want to add and press **Enter**. The **Work with Encryption Business Items** screen appears.



```
                    Work with Encryption Business Items

 Type options, press Enter.                   Subset  . . . . .  ____________
   1=Identify fields    4=Delete

 Opt  Item
 █    NAME         CUSTOMER NAME

                                                                      Bottom
 F3=Exit    F6=Add New                F12=Cancel
```

Figure : Work with Encryption Business Items with Data screen

5. Select the Business Item for which you want to identify fields and press **1=Identify Fields**. The **Modify Encryption Business Item** screen appears.

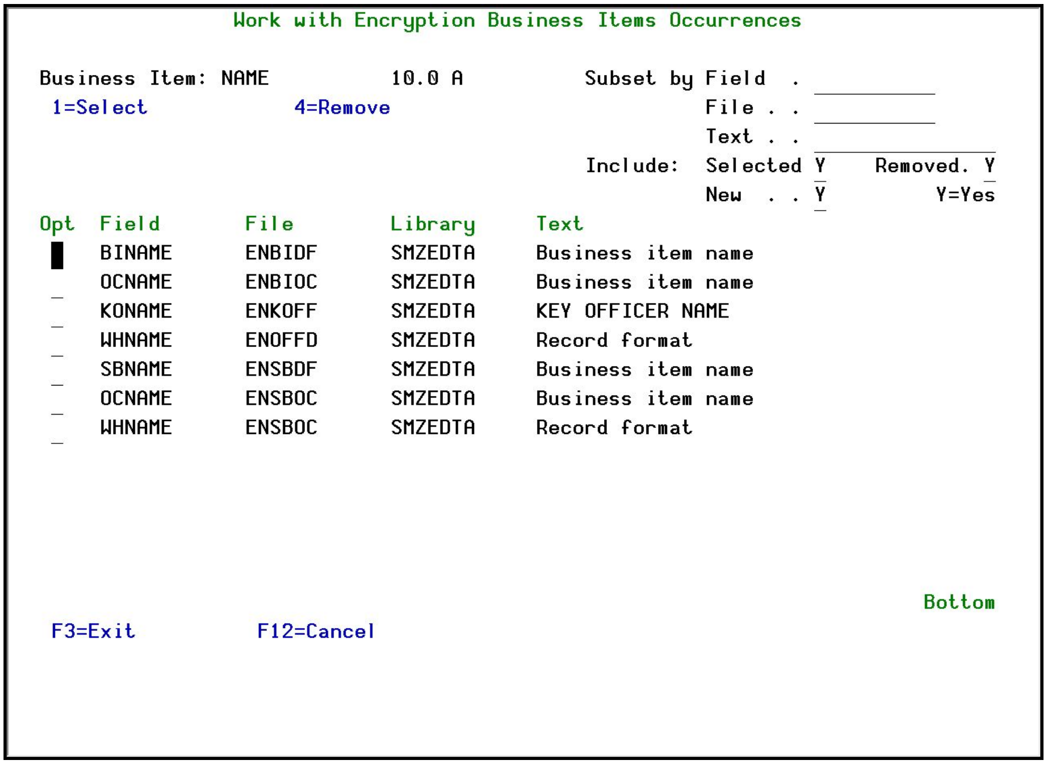


```
                        Modify Encryption Business Item

   Business item name . . . . . . .   NAME            Name
   Text . . . . . . . . . . . . . .   CUSTOMER NAME
   Type . . . . . . . . . . . . . .   A               A=Alpha, N=Numeric
   Length . . . . . . . . . . . . .      10.0


   Include fields which either of the following is true for them:
   Field name contains . . . . . . .   __________
     or . . . . . . . . . . . . . .   __________

   Field text contains . . . . . . .   ____________________
     or . . . . . . . . . . . . . .   ____________________

   Referencing field . . . . . . . .   __________   in file    __________
                                                       library __________
     or . . . . . . . . . . . . . .   __________   in file    __________
                                                       library __________
   Press Enter to continue and select PF fields

   F3=Exit   F12=Cancel
```

Figure : Modify Encryption Business Item screen

Parameters	Description
Business item name	A unique name for the Business Item.
Text	A meaningful description of the Business Item
Type	Type of the fields to be identified **A** = Alphameric **N** = Numeric
Length	Length of fields to be identified.
Field name contains	The field name must contain this text
Field text contains	The field description must contain this text
Referencing field name, file, and library	The field must be referenced from the given field, file and library.

6. Enter a list of filters (if required) and press **Enter**. The **Work with Encryption Business Items Occurrences** screen appears with a list of all fields that satisfy at least one of the filters. If no filters are entered, all fields that match the field type and length are displayed.



```
                   Work with Encryption Business Items Occurrences

  Business Item: NAME          10.0 A         Subset by Field  . __________
   1=Select            4=Remove                         File . . __________
                                                        Text . . _______________
                                              Include:  Selected Y    Removed. Y
                                                        New   . . Y         Y=Yes
  Opt  Field       File        Library     Text
   _   BINAME      ENBIDF      SMZEDTA     Business item name
   _   OCNAME      ENBIOC      SMZEDTA     Business item name
   _   KONAME      ENKOFF      SMZEDTA     KEY OFFICER NAME
   _   WHNAME      ENOFFD      SMZEDTA     Record format
   _   SBNAME      ENSBDF      SMZEDTA     Business item name
   _   OCNAME      ENSBOC      SMZEDTA     Business item name
   _   WHNAME      ENSBOC      SMZEDTA     Record format




                                                                          Bottom
   F3=Exit          F12=Cancel
```

Figure : Work with Encryption Business Items Occurrences screen

7. Select a field to be linked to the Business Item and press **1=Select**. Repeat this until all required fields are selected.

Previously selected fields are designated with **>**.

8. Press **Enter** to return to the **Modify Encryption Business Item** screen and then press **F3**.

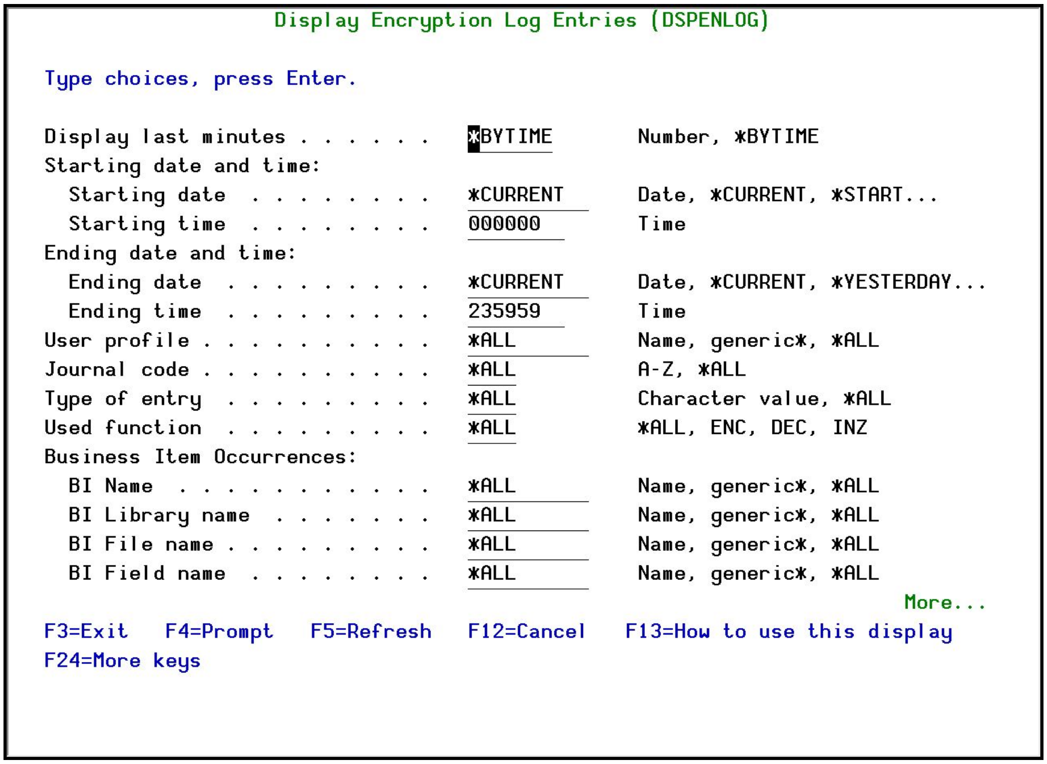
The sensitive fields are now available to be selected for encryption definition. See Data to Encrypt for details.

Reporting

Display the Encryption Log

To display the Encryption Log:

1. Select **41. Display Log** in the **Encryption** main menu. The **Display Encryption Log Entries** screen appears.



```
                    Display Encryption Log Entries (DSPENLOG)

 Type choices, press Enter.

 Display last minutes . . . . . .   *BYTIME       Number, *BYTIME
 Starting date and time:
   Starting date  . . . . . . . .   *CURRENT      Date, *CURRENT, *START...
   Starting time  . . . . . . . .   000000        Time
 Ending date and time:
   Ending date  . . . . . . . . .   *CURRENT      Date, *CURRENT, *YESTERDAY...
   Ending time  . . . . . . . . .   235959        Time
 User profile . . . . . . . . . .   *ALL          Name, generic*, *ALL
 Journal code . . . . . . . . . .   *ALL          A-Z, *ALL
 Type of entry  . . . . . . . . .   *ALL          Character value, *ALL
 Used function  . . . . . . . . .   *ALL          *ALL, ENC, DEC, INZ
 Business Item Occurrences:
   BI Name  . . . . . . . . . . .   *ALL          Name, generic*, *ALL
   BI Library name  . . . . . . .   *ALL          Name, generic*, *ALL
   BI File name . . . . . . . . .   *ALL          Name, generic*, *ALL
   BI Field name  . . . . . . . .   *ALL          Name, generic*, *ALL
                                                                     More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Figure : Display Encryption Log Entries screen

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

-

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

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

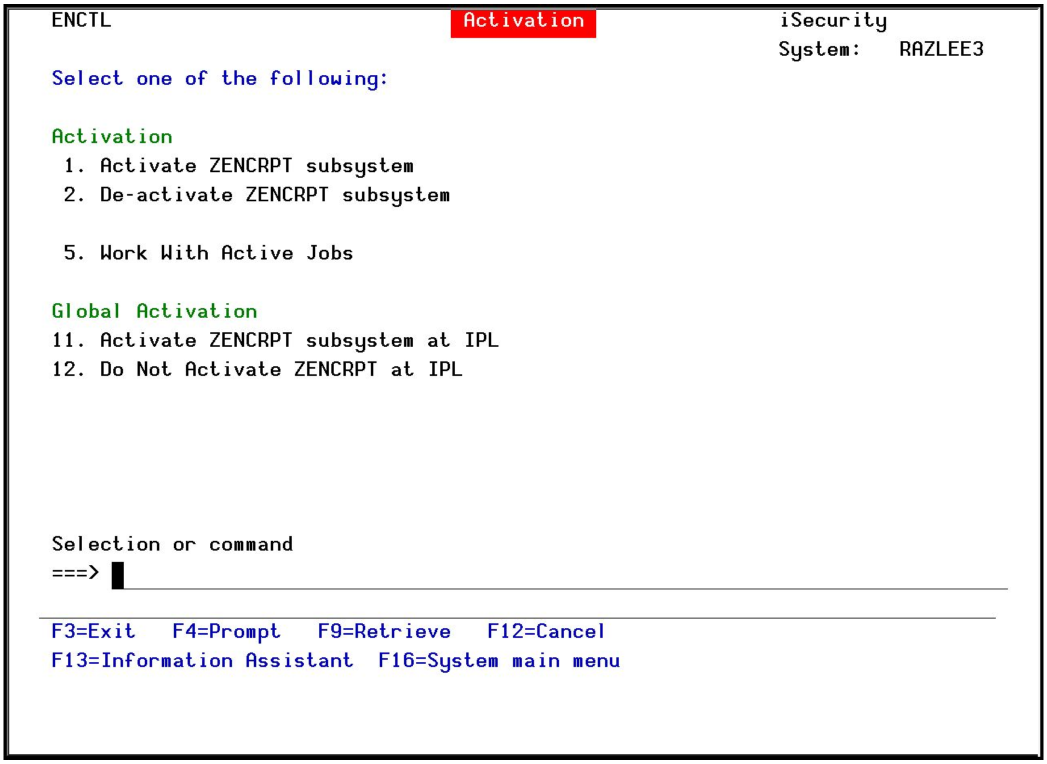
Control

Activation

Before using Encryption, you must activate the ZENCRPT subsystem, especially before running forced encryption or tokenization (see Recent Key Usage Enforcement for more details).

To activate the sub-system:

1. Select **51. Activation** in the Encryption main menu. The **Activation** menu appears.

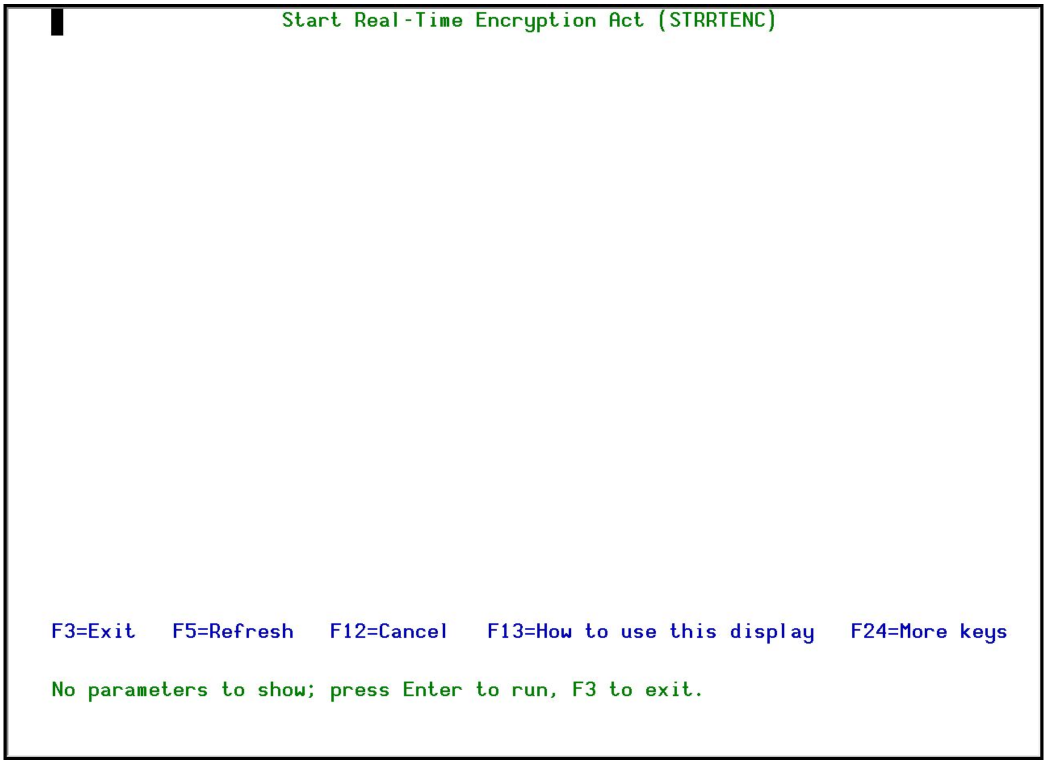


```
ENCTL                         Activation                    iSecurity
                                                            System:    RAZLEE3
Select one of the following:

Activation
 1. Activate ZENCRPT subsystem
 2. De-activate ZENCRPT subsystem

 5. Work With Active Jobs

Global Activation
11. Activate ZENCRPT subsystem at IPL
12. Do Not Activate ZENCRPT at IPL




Selection or command
===>

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

Figure : Activation Menu

Parameters	Description
1. Activate ZAUTH subsytem	Opens the **Start Real Time Auth on Demand** screen.
2. De-activate ZAUTH subsystem	Opens the **End Real Time Auth on Demand** screen.
5. Work with Active Jobs	Opens the **Work with Subsystem Jobs** screen.

2. Select **1. Activate ZENCRPT subsystem** in the **Activation** menu. The **Start Real-Time Encryption Act** screen appears.



```
                    Start Real-Time Encryption Act (STRRTENC)

F3=Exit   F5=Refresh   F12=Cancel   F13=How to use this display   F24=More keys

No parameters to show; press Enter to run, F3 to exit.
```

Figure : Start Real-Time Encryption Act screen

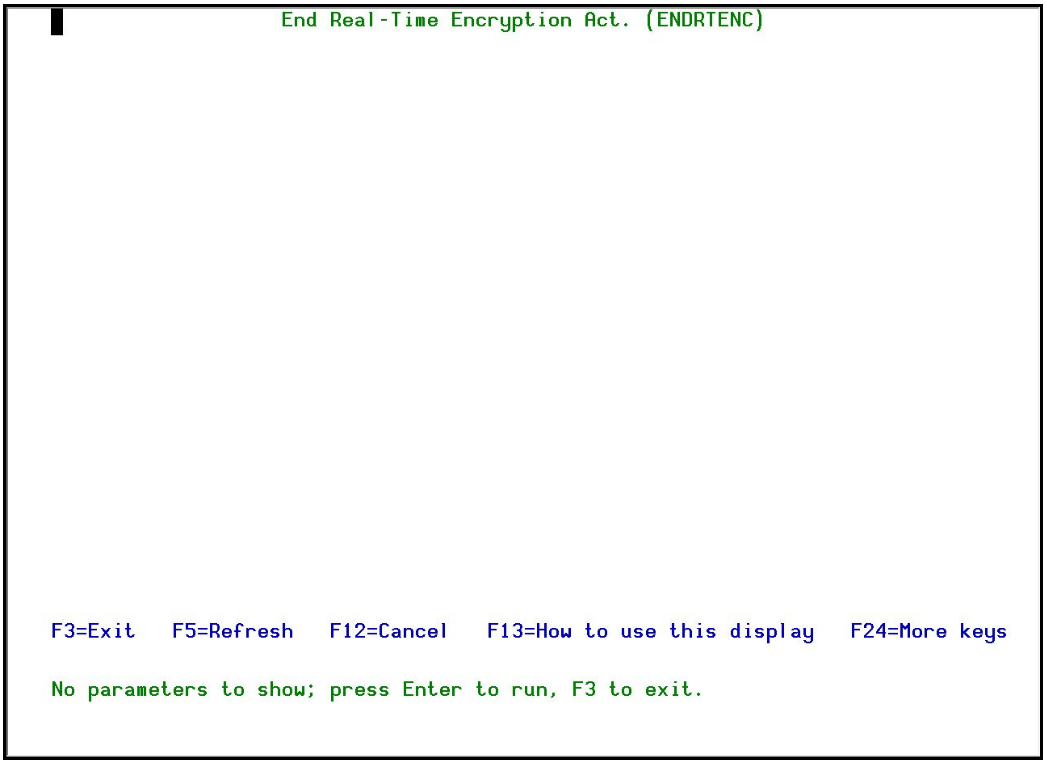
3. Press **Enter**. The subsystem is started.

End Real Time Encryption

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

To de-activate the sub-system:

1. Select **51. Activation** in the Encryption main menu. The **Activation** menu appears.
2. Select **2. De-activate ZENCRPT subsystem** in the Activation menu. The **End Real Time Encryption Act** screen appears.



```
                     End Real-Time Encryption Act. (ENDRTENC)

F3=Exit   F5=Refresh   F12=Cancel   F13=How to use this display   F24=More keys

No parameters to show; press Enter to run, F3 to exit.
```

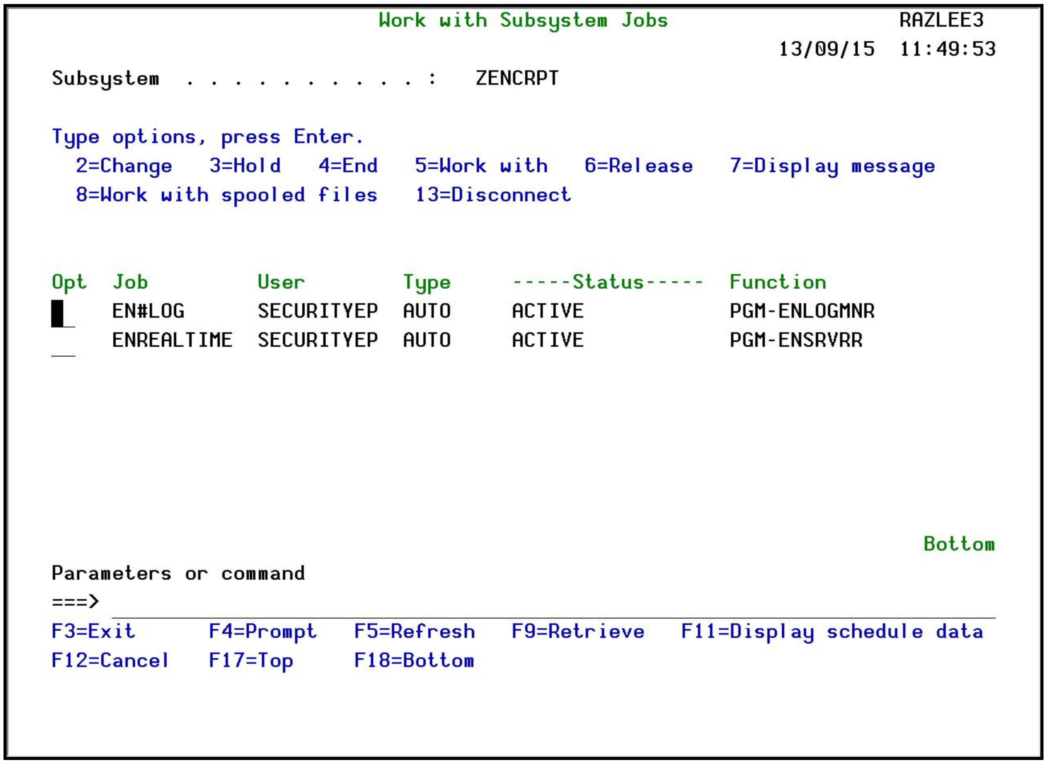
Figure : End Real-Time Encryption Act screen

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

Work with Subsystems

To check that a subsystem is active:

1. Select **51. Activation** in the Encryption main menu. The Activation menu appears.
2. Select **5. Work with Active Jobs** in the Activation menu. The **Work with Subsystem Jobs** screen appears.



```
                         Work with Subsystem Jobs                     RAZLEE3
                                                           13/09/15  11:49:53
Subsystem  . . . . . . . . . . :   ZENCRPT

Type options, press Enter.
  2=Change   3=Hold   4=End   5=Work with   6=Release   7=Display message
  8=Work with spooled files   13=Disconnect


Opt  Job         User        Type     -----Status-----  Function
 _   EN#LOG      SECURITYEP  AUTO     ACTIVE            PGM-ENLOGMNR
 _   ENREALTIME  SECURITYEP  AUTO     ACTIVE            PGM-ENSRVRR







                                                                       Bottom
Parameters or command
===> ________________________________________________________________________
F3=Exit       F4=Prompt     F5=Refresh    F9=Retrieve   F11=Display schedule data
F12=Cancel    F17=Top       F18=Bottom
```

Figure : Work with Subsystem Jobs screen

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

System Configuration

Use the System Configuration menu to set the general definitions and log retention definitions for **Field Encryption**.

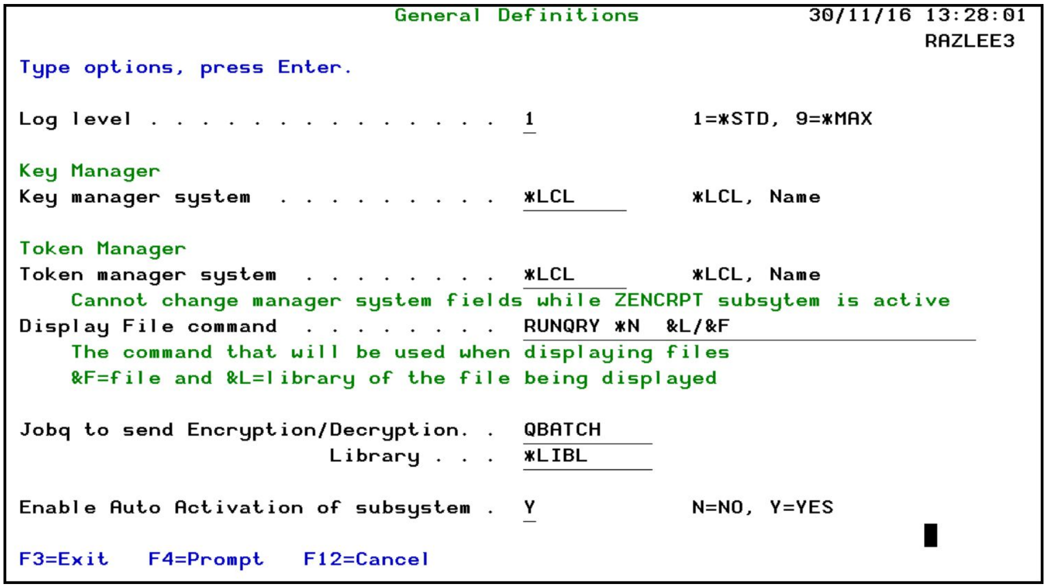
Encryption/Tokenization

General Definitions

Before running this option, you should ensure that the Encryption subsystem ZENCRPT is not active. See Work with Subsystems and End Real Time Encryption for further details. After you have finished using this option, re-activate the subsystem as described in Activation.

To set the **Field Encryption** general definitions:

1. Select 81. System Configuration in the Encryption main menu. The System Configuration menu appears.
2. Select 1. General Definitions in the System Configuration menu. The General Definitions screen appears.



```
                                General Definitions                30/11/16 13:28:01
                                                                           RAZLEE3
Type options, press Enter.

Log level . . . . . . . . . . . . . .  1            1=*STD, 9=*MAX

Key Manager
Key manager system  . . . . . . . . .  *LCL         *LCL, Name

Token Manager
Token manager system  . . . . . . . .  *LCL         *LCL, Name
    Cannot change manager system fields while ZENCRPT subsytem is active
Display File command  . . . . . . . .  RUNQRY *N  &L/&F
    The command that will be used when displaying files
    &F=file and &L=library of the file being displayed

Jobq to send Encryption/Decryption. .  QBATCH
                        Library . . .  *LIBL

Enable Auto Activation of subsystem .  Y            N=NO, Y=YES

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

Figure : General Definitions screen

Parameters	Description
Log level	**1=*STD** – Record only basic encryption transactions **9=*MAX** – Record all encryption transactions.
Key manager system	The system where the Key Manager will reside. ***LCL** = the current system **Name** = the name of the system The Key Manager can only be worked on from the system on which it is installed. Users who try to work on the Key Manager from another system will receive an error message. If the Key Manager is not on the *LCL system, then on the system where the Key Manager resides, you must define the system(s) where the Data Manager resides. See Supported Data Managers for more details.
Token manager system	The system where the Token Manager will reside. ***LCL** = the current system **Name** = the name of the system The Token Manager can only be worked on from the system on which it is installed. Users who try to work on the Token Manager from another system will receive an error message. If the Token Manager is not on the *LCL system, then on the system where the Key Manager resides, you must define the system (s) where the Data Manager resides. See Supported Data Managers for more details.
Display file command	The command that will be used when displaying files
Jobq to send Encryption/Decryption.	Default value is QBATCH in library *LIBL
Enable Auto Activation	If the Encryption Subsystem is not activated

Parameters	Description
of subsystem	when a file is read/written it is automatically activated to prevent a suspension of the activities.

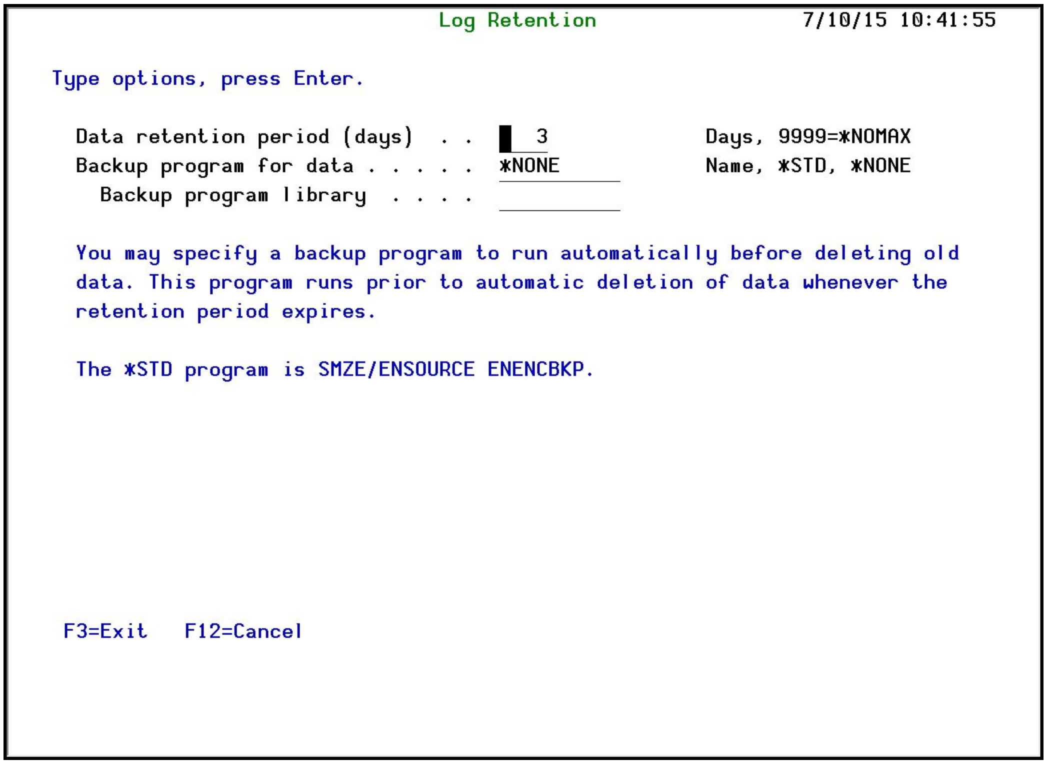
3. Enter your setup definitions and press Enter. You are returned to the System Configuration menu.

Log Retention

You can keep log file indefinitely on the system or you can choose to delete them after a specified period of time. You can also define a backup program to run immediately before deletion. The backup program stores the logs offline to allow for reports to be run against historical data. The system comes with a built in backup program, ENENCBKP. The backup program source is stored in file ENSOURCE in library SMZE.

To set the Field Encryption log retention definitions:

1. **Select 81. System Configuration in the Encryption main menu. The System Configuration menu appears.**
2. **Select 9. Log retention in the System Configuration menu. The Log Retention screen appears.**



```
                                Log Retention                 7/10/15 10:41:55

   Type options, press Enter.

     Data retention period (days)  . .    3             Days, 9999=*NOMAX
     Backup program for data . . . . .  *NONE           Name, *STD, *NONE
       Backup program library  . . . .

     You may specify a backup program to run automatically before deleting old
     data. This program runs prior to automatic deletion of data whenever the
     retention period expires.

     The *STD program is SMZE/ENSOURCE ENENCBKP.




    F3=Exit   F12=Cancel
```

Figure : Log Retention screen

Parameters	Description
Data Retention period (days)	The length of time (in days) to retain the log files. **9999=*NOMAX** – the log files are never deleted.
Backup program for data	**Name** = The name of your in-house program that will save the logs before deletion. If you enter a name, you must also specify the library where the program is stored. ***STD** = Use the Raz-Lee provided backup program. ***NONE** = Do not backup log files before deleting them.
Backup program library	The library where the backup program is stored.

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

Maintenance

Use this menu to manually run procedures to update encryption and tokenization. You can also run audit reports from this menu.

Recent Key Usage Enforcement

There may be occasions when you need to re-encrypt or re-tokenize fields immediately after updating their Data Keys or Tokens, instead of waiting for the scheduled procedures to run. These options should only be run on the computer/LPAR where the Data Manager is situated, as defined in General Definitions.

Before running these options, you should ensure that the Encryption subsystem ZENCRPT is active. See Work with Subsystems and Activation for further details.

Force Encryption Rotation

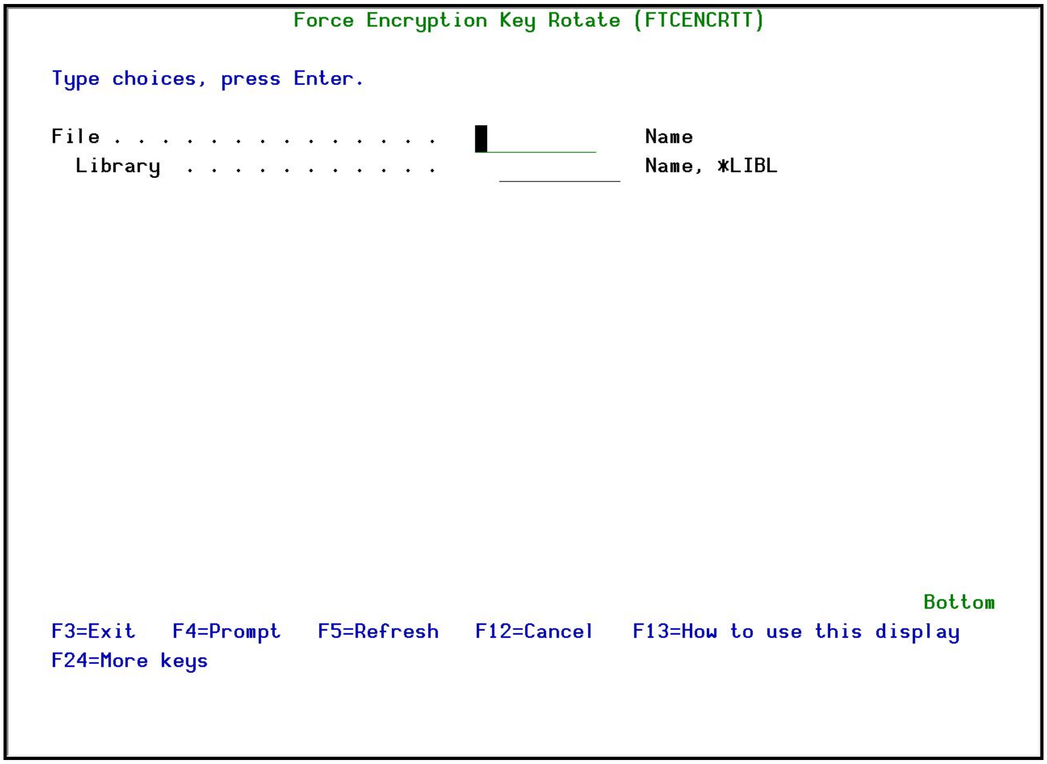
This procedure should be run for every file that contains data whose encryption Data Keys have been updated.

(This option is relevant for Field Rotate Type with a value of 6, in the Add Occurrence screen.)

NOTE: This function can only be performed by a user who has authorization to see all encrypted Business Items in the file as clear data.

To re-encrypt fields:

1. Select **82. Maintenance Menu** in the **Encryption** main menu. The **Maintenance** menu appears.
2. Select **21. Force Encryption Rotation** from the **Maintenance Menu**. The **Force Encryption Key Rotate** screen appears.



```
                    Force Encryption Key Rotate (FTCENCRTT)

 Type choices, press Enter.

 File . . . . . . . . . . . . . .   ▌_________     Name
   Library  . . . . . . . . . . .     __________   Name, *LIBL

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

Figure : Force Encryption Key Rotate screen

Parameters	Description
File	The name of the file that contains fields that must be re-encrypted.
Library	The name of the library that contains the file object.

3. Enter information about the file to be re-encrypted and press **Enter** . You are returned to the **Maintenance** menu and the file is re-encrypted.

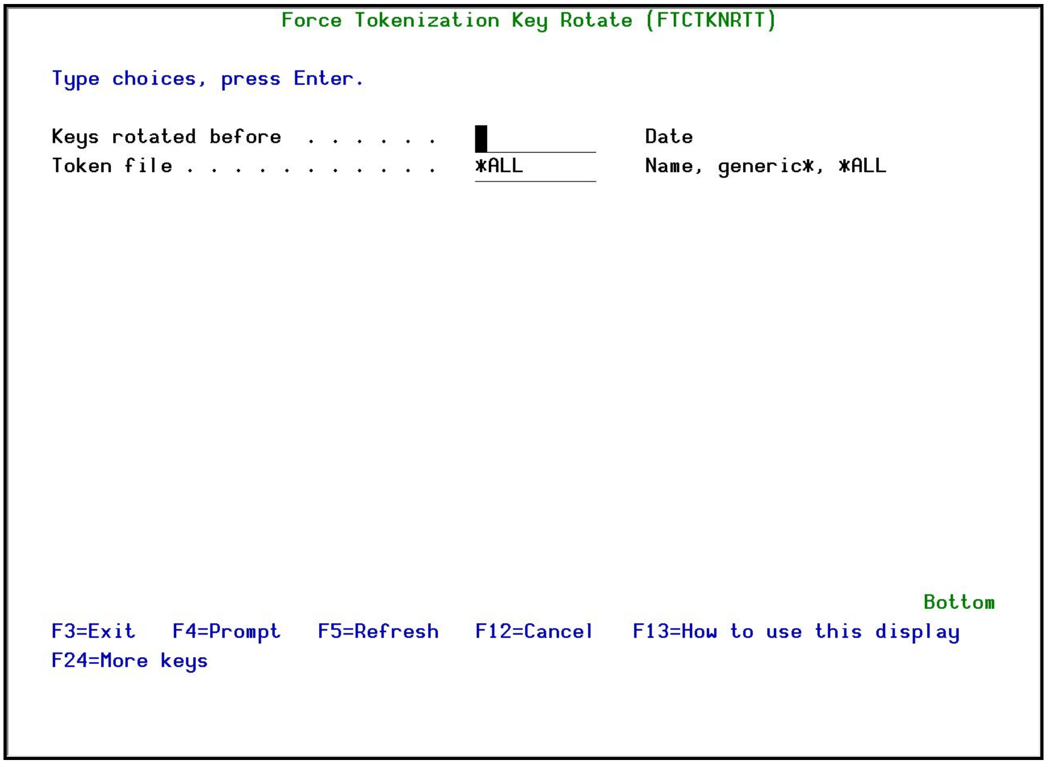
Force Tokenization Rotation

This procedure should be run for to force re-encryption of every tokenized file that has not been re-encrypted since a certain date.

NOTE: This function can only be performed by a user who has authorization to see all encrypted Business Items as clear data.

To re-encrypt fields:

1. Select **82. Maintenance Menu** in the **Encryption** main menu. The **Maintenance** menu appears.
2. Select **22. Force Tokenization Rotation** from the **Maintenance Menu**. The **Force Encryption Key Rotate** screen appears.



```
                     Force Tokenization Key Rotate (FTCTKNRTT)

 Type choices, press Enter.

 Keys rotated before  . . . . . .  █              Date
 Token file . . . . . . . . . . .  *ALL           Name, generic*, *ALL

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

Figure : Force Encryption Key Rotate screen

Parameters	Description
Keys rotated before	Enter a cutoff date in Job Date format. All records in the files that meet the second parameter with an encryption date before this date will be re-encrypted.
Token file	The name of the file(s) to be re-encrypted. **Name** – The name of a specific token file **generic*** - A group of token files ***ALL** – All token files

3. Enter information about the file to be re-encrypted and press **Enter** . You are returned to the **Maintenance** menu and the file is re-encrypted.

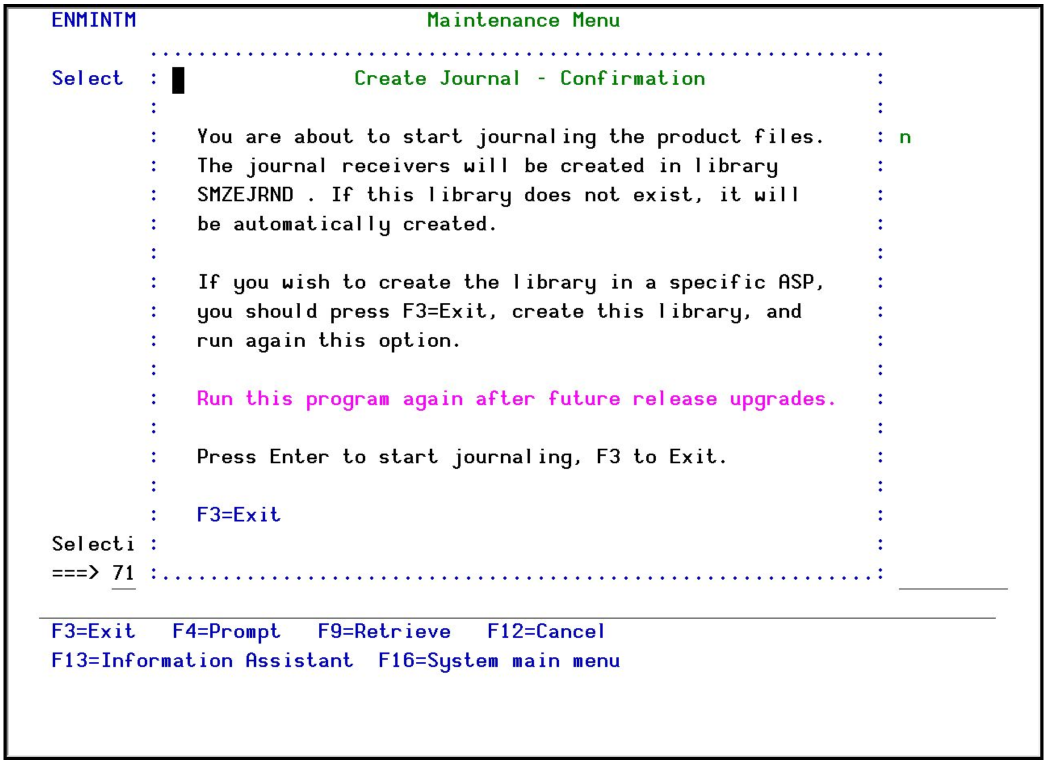
To find the name of a specific token file or a group of token files, run the command
DSPOBJD OBJ(SMZETKN/*ALL) OBJTYPE(*FILE) DETAIL(*BASIC) on the computer where the Token Manager is located. The name of the file to which each Token File is associated is contained in the text description of the Token File.

Trace Definition Modifications

These options allow you to run audit reports on the changes that were made to your encryption definitions.

Add Journal

1. Select **82. Maintenance Menu** in the **Encryption** main menu. The M **aintenance** menu appears.
2. Select **71. Add Journal** from the **Maintenance Menu**. The **Create Journal – Confirmation** screen appears.



```
ENMINTM                               Maintenance Menu

              ...........................................................
Select     : █               Create Journal - Confirmation             :
           :                                                           :
           :   You are about to start journaling the product files.    : n
           :   The journal receivers will be created in library        :
           :   SMZEJRND . If this library does not exist, it will      :
           :   be automatically created.                               :
           :                                                           :
           :   If you wish to create the library in a specific ASP,    :
           :   you should press F3=Exit, create this library, and      :
           :   run again this option.                                  :
           :                                                           :
           :   Run this program again after future release upgrades.   :
           :                                                           :
           :   Press Enter to start journaling, F3 to Exit.            :
           :                                                           :
           :   F3=Exit                                                 :
Selecti    :                                                           :
===> 71    :...........................................................:

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

Figure : Create Journal – Confirmation window

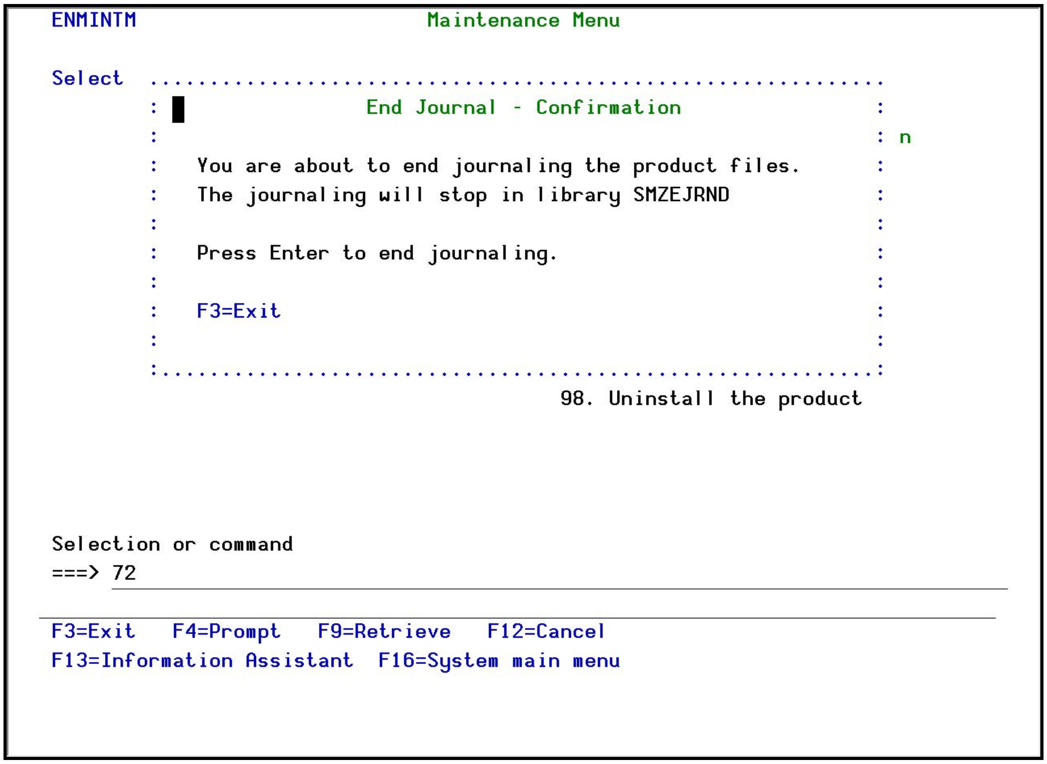
3. Press **Enter** to confirm. The process of journaling the product files begins. The journal receivers will be created in library **SMZEJRND**. If this library does not exist, it will be automatically created.

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

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

Remove Journal

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



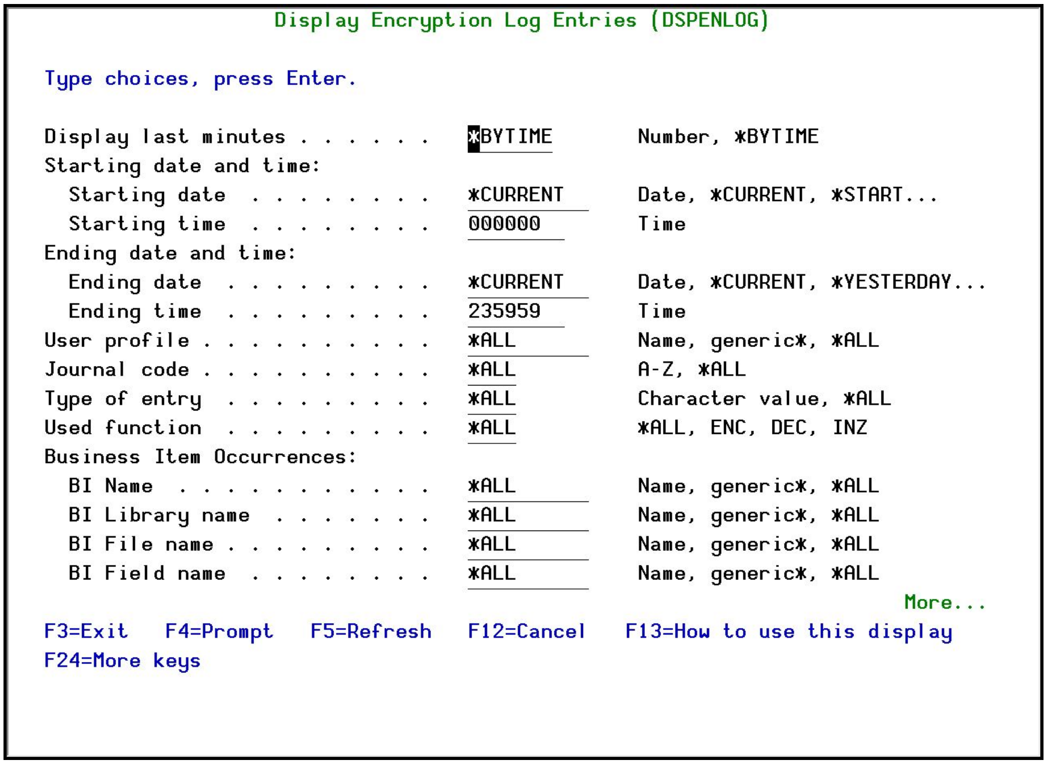
```
ENMINTM                        Maintenance Menu

Select  ............................................................
        : █                End Journal - Confirmation              :
        :                                                          : n
        :   You are about to end journaling the product files.     :
        :   The journaling will stop in library SMZEJRND           :
        :                                                          :
        :   Press Enter to end journaling.                         :
        :                                                          :
        :   F3=Exit                                                :
        :                                                          :
        :..........................................................:
                                        98. Uninstall the product




Selection or command
===> 72

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

Figure : End Journal – Confirmation window

2. Press **Enter** to confirm.

Display Journal

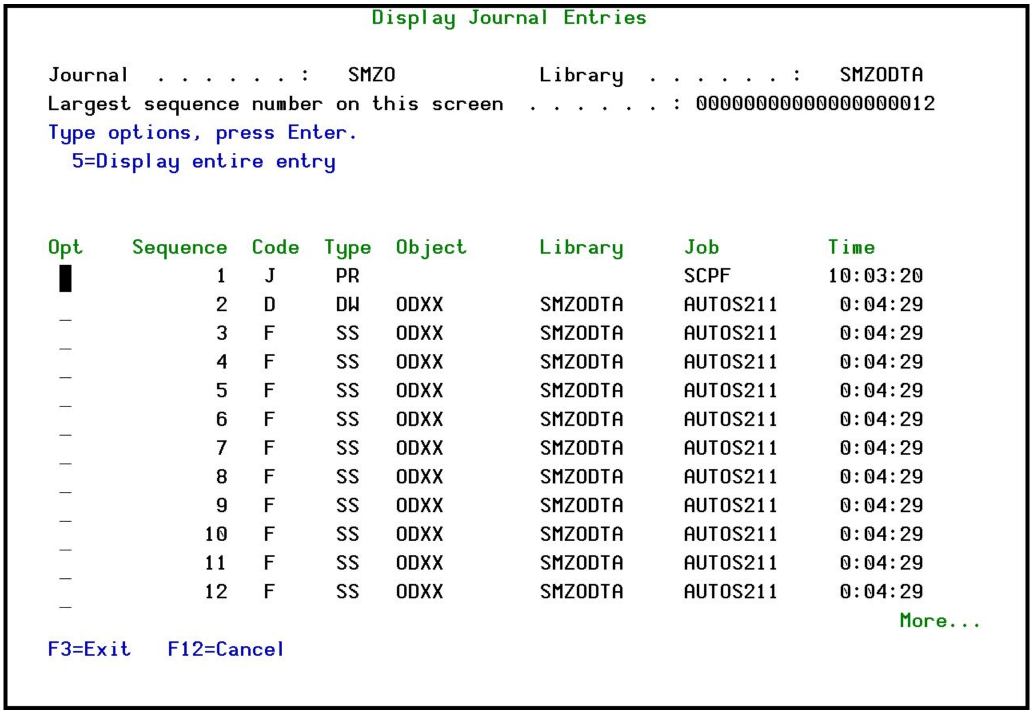
1. Select **79. Display Journal** from the **Maintenance Menu**. The **Display APP Current Journal (DSPAPCRJ)** screen appears with preset filter parameters entered for you.



```
                    Display Encryption Log Entries (DSPENLOG)

 Type choices, press Enter.

 Display last minutes . . . . . .   *BYTIME       Number, *BYTIME
 Starting date and time:
   Starting date  . . . . . . . .   *CURRENT      Date, *CURRENT, *START...
   Starting time  . . . . . . . .   000000        Time
 Ending date and time:
   Ending date  . . . . . . . . .   *CURRENT      Date, *CURRENT, *YESTERDAY...
   Ending time  . . . . . . . . .   235959        Time
 User profile . . . . . . . . . .   *ALL          Name, generic*, *ALL
 Journal code . . . . . . . . . .   *ALL          A-Z, *ALL
 Type of entry  . . . . . . . . .   *ALL          Character value, *ALL
 Used function  . . . . . . . . .   *ALL          *ALL, ENC, DEC, INZ
 Business Item Occurrences:
   BI Name  . . . . . . . . . . .   *ALL          Name, generic*, *ALL
   BI Library name  . . . . . . .   *ALL          Name, generic*, *ALL
   BI File name . . . . . . . . .   *ALL          Name, generic*, *ALL
   BI Field name  . . . . . . . .   *ALL          Name, generic*, *ALL
                                                                      More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Figure : Display Encryption Log Entries (DSPENLOG) screen

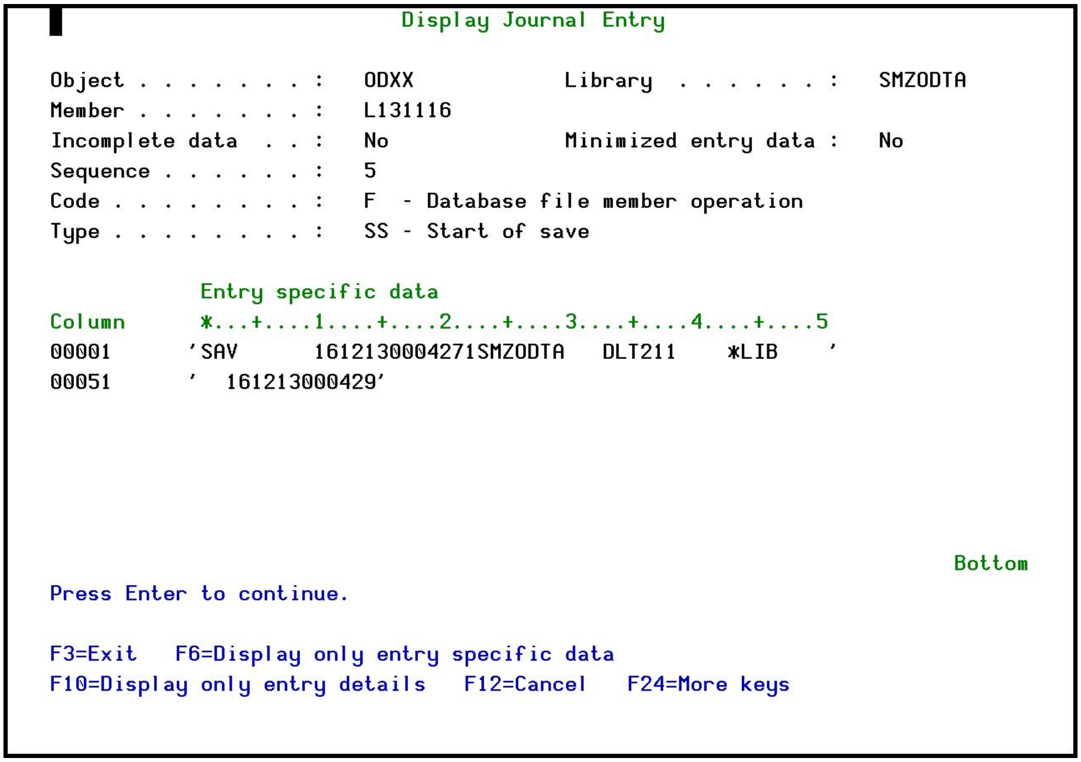
2. Press **Enter**. The **Display Journal Entries** screen appears.



```
                              Display Journal Entries

 Journal  . . . . . . :   SMZO            Library  . . . . . . :   SMZODTA
 Largest sequence number on this screen  . . . . . . : 00000000000000000012
 Type options, press Enter.
   5=Display entire entry


 Opt    Sequence  Code  Type  Object      Library     Job         Time
  _            1   J     PR                           SCPF        10:03:20
  _            2   D     DW   ODXX        SMZODTA     AUTOS211     0:04:29
  _            3   F     SS   ODXX        SMZODTA     AUTOS211     0:04:29
  _            4   F     SS   ODXX        SMZODTA     AUTOS211     0:04:29
  _            5   F     SS   ODXX        SMZODTA     AUTOS211     0:04:29
  _            6   F     SS   ODXX        SMZODTA     AUTOS211     0:04:29
  _            7   F     SS   ODXX        SMZODTA     AUTOS211     0:04:29
  _            8   F     SS   ODXX        SMZODTA     AUTOS211     0:04:29
  _            9   F     SS   ODXX        SMZODTA     AUTOS211     0:04:29
  _           10   F     SS   ODXX        SMZODTA     AUTOS211     0:04:29
  _           11   F     SS   ODXX        SMZODTA     AUTOS211     0:04:29
  _           12   F     SS   ODXX        SMZODTA     AUTOS211     0:04:29
                                                                        More...
 F3=Exit   F12=Cancel
```

Figure : Display Journal Entries screen

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

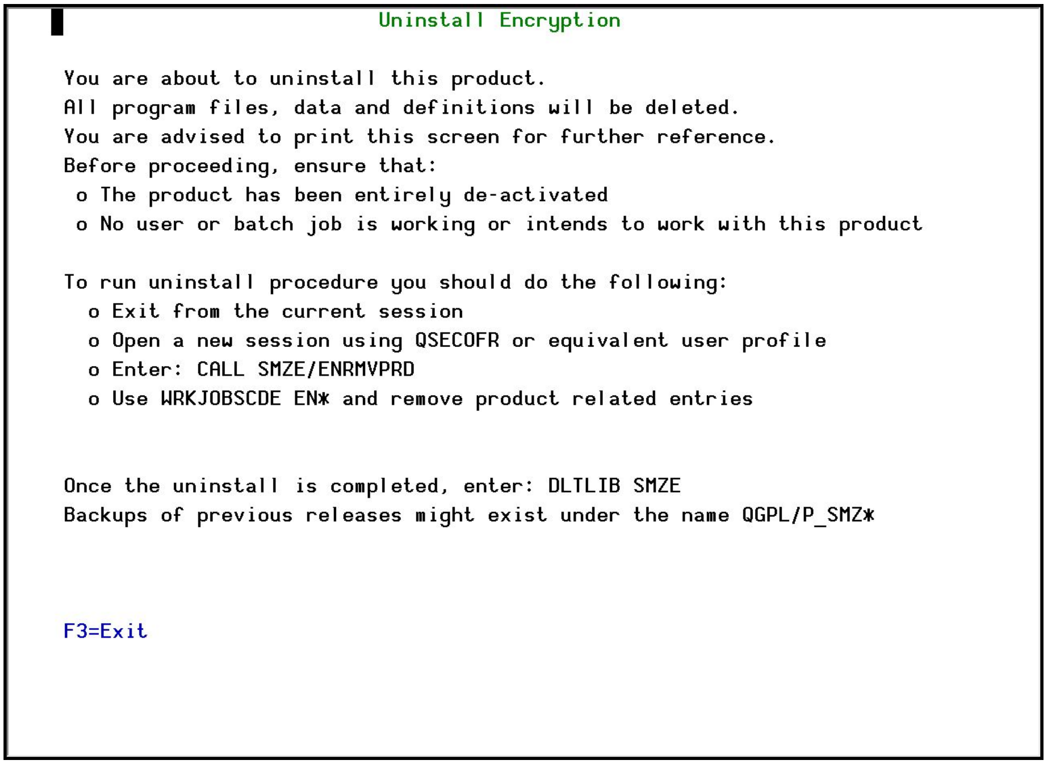


```
                              Display Journal Entry

 Object . . . . . . . :   ODXX            Library  . . . . . . :   SMZODTA
 Member . . . . . . . :   L131116
 Incomplete data  . . :   No              Minimized entry data :   No
 Sequence . . . . . . :   5
 Code . . . . . . . . :   F  - Database file member operation
 Type . . . . . . . . :   SS - Start of save

             Entry specific data
 Column      *...+....1....+....2....+....3....+....4....+....5
 00001      'SAV      1612130004271SMZODTA   DLT211    *LIB    '
 00051      '  161213000429'






                                                                        Bottom
 Press Enter to continue.

 F3=Exit   F6=Display only entry specific data
 F10=Display only entry details   F12=Cancel   F24=More keys
```

Figure : Display Journal Entry screen

Uninstall

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

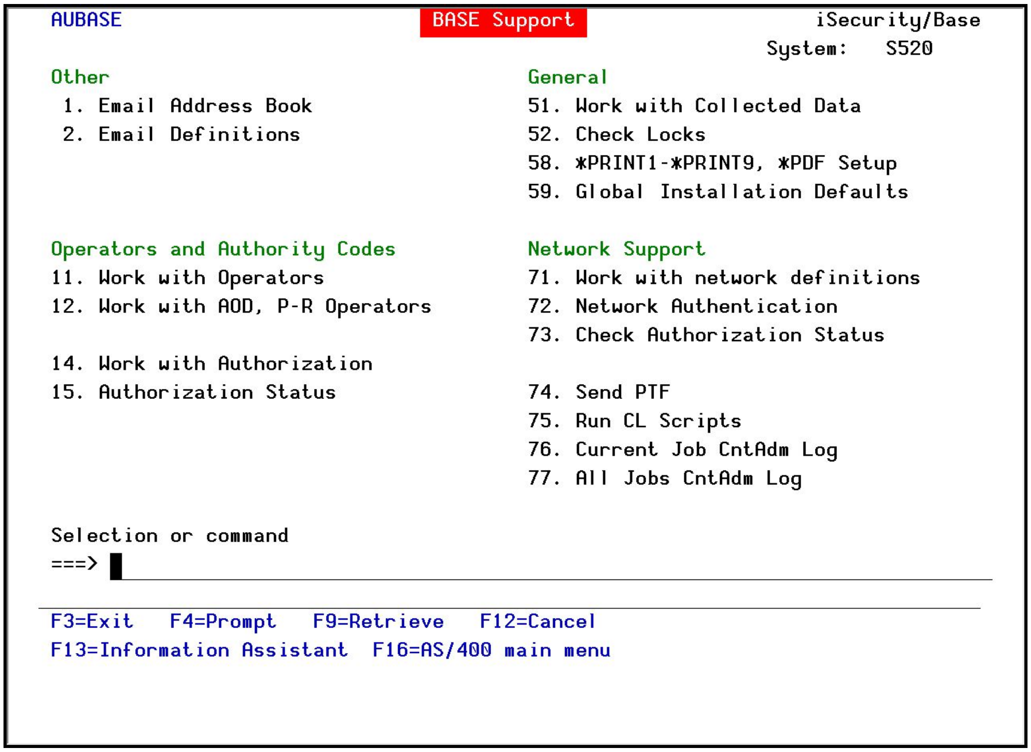


```
                              Uninstall Encryption

 You are about to uninstall this product.
 All program files, data and definitions will be deleted.
 You are advised to print this screen for further reference.
 Before proceeding, ensure that:
  o The product has been entirely de-activated
  o No user or batch job is working or intends to work with this product

 To run uninstall procedure you should do the following:
   o Exit from the current session
   o Open a new session using QSECOFR or equivalent user profile
   o Enter: CALL SMZE/ENRMVPRD
   o Use WRKJOBSCDE EN* and remove product related entries


 Once the uninstall is completed, enter: DLTLIB SMZE
 Backups of previous releases might exist under the name QGPL/P_SMZ*



 F3=Exit
```

Figure : Uninstall Encryption screen

BASE Support

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



```
AUBASE                              BASE Support                        iSecurity/Base
                                                                     System:    S520
Other                                       General
 1. Email Address Book                      51. Work with Collected Data
 2. Email Definitions                       52. Check Locks
                                            58. *PRINT1-*PRINT9, *PDF Setup
                                            59. Global Installation Defaults

Operators and Authority Codes               Network Support
11. Work with Operators                     71. Work with network definitions
12. Work with AOD, P-R Operators            72. Network Authentication
                                            73. Check Authorization Status
14. Work with Authorization
15. Authorization Status                    74. Send PTF
                                            75. Run CL Scripts
                                            76. Current Job CntAdm Log
                                            77. All Jobs CntAdm Log

Selection or command
===>

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

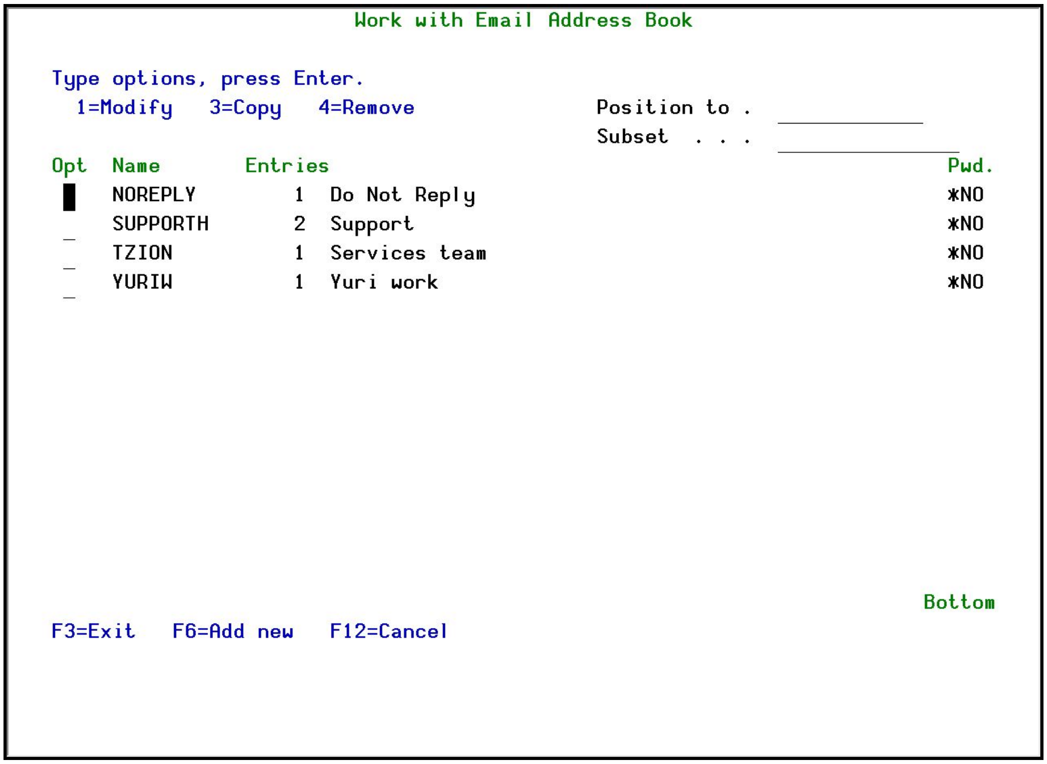
Figure : BASE Support menu

Other

Email Address Book

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

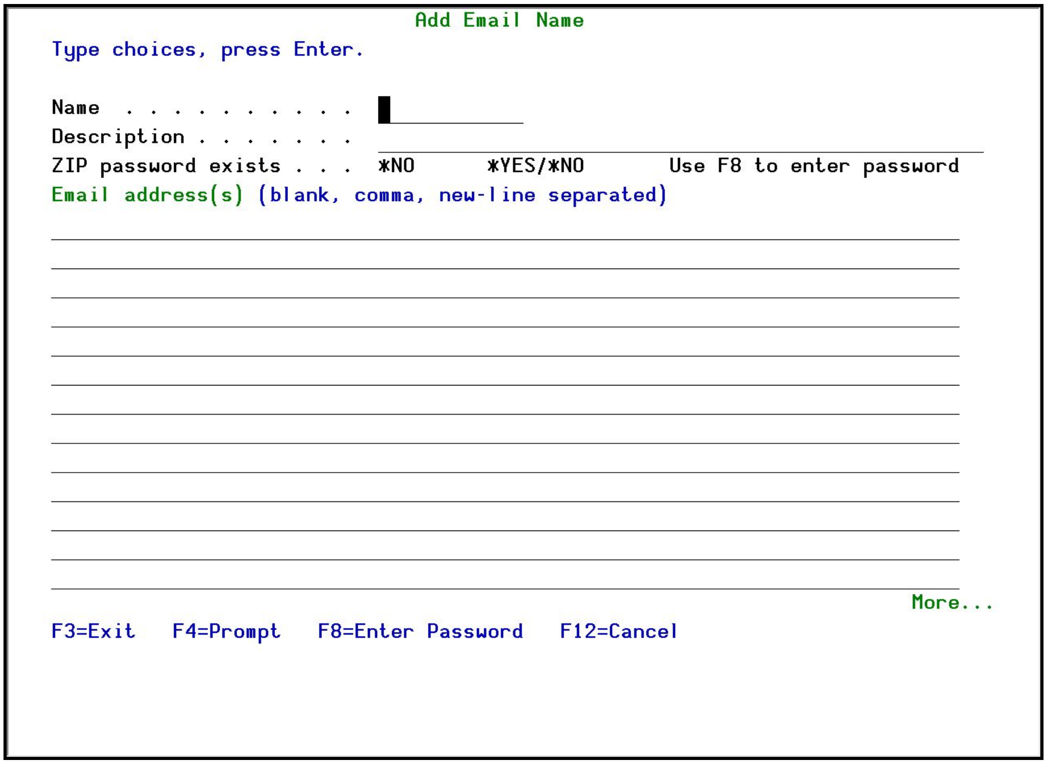
1. Select **1. Email Address Book** from the **BASE Support** menu. The **Work with Email Address Book** screen appears.



```
                         Work with Email Address Book

 Type options, press Enter.
   1=Modify   3=Copy   4=Remove                Position to .  __________
                                               Subset  . . .  ____________
 Opt  Name       Entries                                              Pwd.
 █    NOREPLY        1  Do Not Reply                                  *NO
 _    SUPPORTH       2  Support                                       *NO
 _    TZION          1  Services team                                 *NO
 _    YURIW          1  Yuri work                                     *NO











                                                                   Bottom
 F3=Exit   F6=Add new   F12=Cancel
```

Figure : Work with Email Address Book screen

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



```
                                    Add Email Name
 Type choices, press Enter.

 Name  . . . . . . . . . .  ________
 Description . . . . . . .  __________________________________
 ZIP password exists . . .  *NO       *YES/*NO       Use F8 to enter password
 Email address(s) (blank, comma, new-line separated)

                                                                      More...
 F3=Exit   F4=Prompt   F8=Enter Password   F12=Cancel
```

Figure : Add Email Name screen

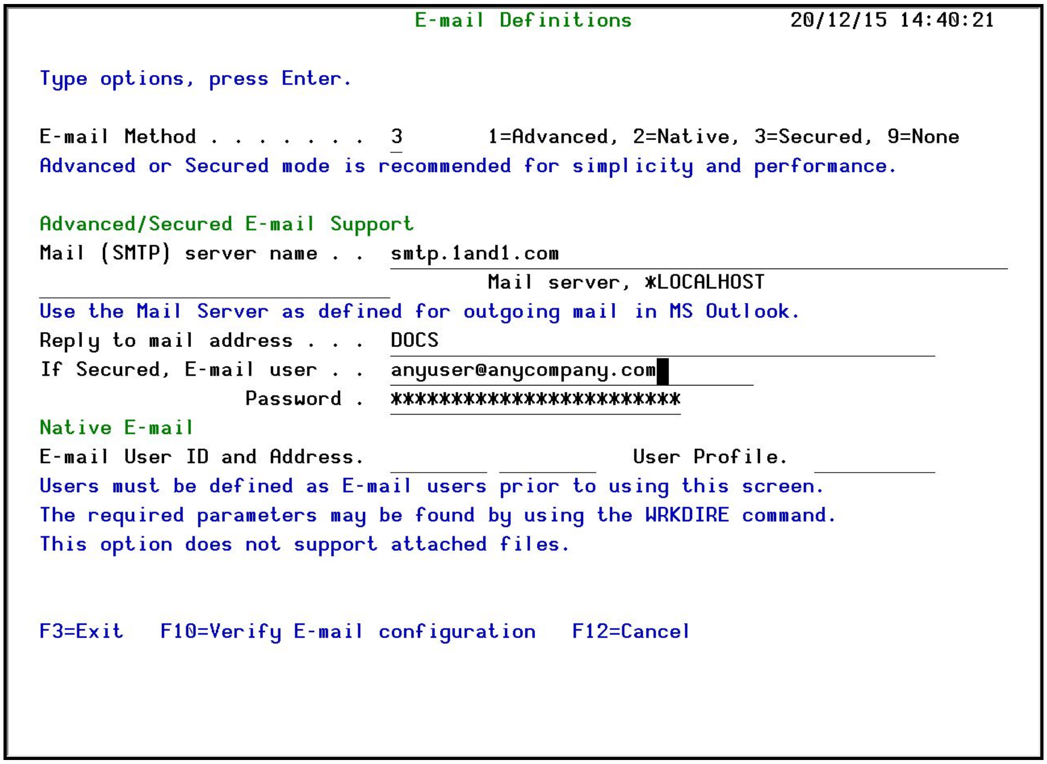
3. Enter a **Name**, **Description**, and all the associated email addresses and press **Enter**.

You can also use **F8** to add a password to protect any ZIP files that will be sent by this user.

Email Definitions

Field Encryption can send out automatic emails every time a temporary authority is used.

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



```
                                E-mail Definitions           20/12/15 14:40:21

 Type options, press Enter.

 E-mail Method . . . . . . .  3       1=Advanced, 2=Native, 3=Secured, 9=None
 Advanced or Secured mode is recommended for simplicity and performance.

 Advanced/Secured E-mail Support
 Mail (SMTP) server name . .  smtp.1and1.com
                                      Mail server, *LOCALHOST
 Use the Mail Server as defined for outgoing mail in MS Outlook.
 Reply to mail address . . .  DOCS
 If Secured, E-mail user . .  anyuser@anycompany.com
                  Password .  ************************
 Native E-mail
 E-mail User ID and Address.                       User Profile.
 Users must be defined as E-mail users prior to using this screen.
 The required parameters may be found by using the WRKDIRE command.
 This option does not support attached files.


 F3=Exit   F10=Verify E-mail configuration   F12=Cancel
```

Figure : E-mail Definitions screen

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

Parameter	Description
E-mail Method	**1**=Advanced **2**=Native **3**=Secured **9**=None Advanced or Secured mode is recommended for simplicity and performance. **NOTE:** If using **2**=native, Users must be defined as E-mail users prior to using this screen. The required parameters may be found by using the WRKDIRE command. This option does not support attached files.
Mail (SMTP) server name	The name of the STMP server or *LOCALHOST
Reply to mail address	The e-mail address to receive replies.
If secured, E-mail user and Password	If you chose **1**=Advanced or **3**=Secured for the E-mail method, enter the email user that will be used to send the emails and the password of that user
E-mail User ID and Address	If you chose **2**=Native for the E-mail method, enter the user ID and address that will be used to send the emails.
User Profile	If you chose **2**=Native for the E-mail method, enter the user profile that will be used to send the emails.
F10=Verify E-mail configuration	Press **F10** to open a dialog that allows you to confirm the change to email definitions and sends a confirmation email to the **Reply to mail address**. You should check that the confirmation email is received. If it is not received, there is a problem with your email definitions.

Operators and Authority Codes

Work with Operators

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

There are three default groups:

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

iSecurity related objects are secured automatically by product authorization lists (named **security1P** . This strengthens the internal security of the product. It is essential that you use **Work with Operators** to define all users who have ***SECADM**, ***AUDIT**or ***AUD#SECAD** privileges, but have all object authority. The **Work with Operators** screen has Usr (user management) and Adm for all activities related to starting, stopping subsystems, jobs, import/export and so on.iSecurity automatically adds all users listed in **Work with Operators** to the appropriate product authorization list.

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

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

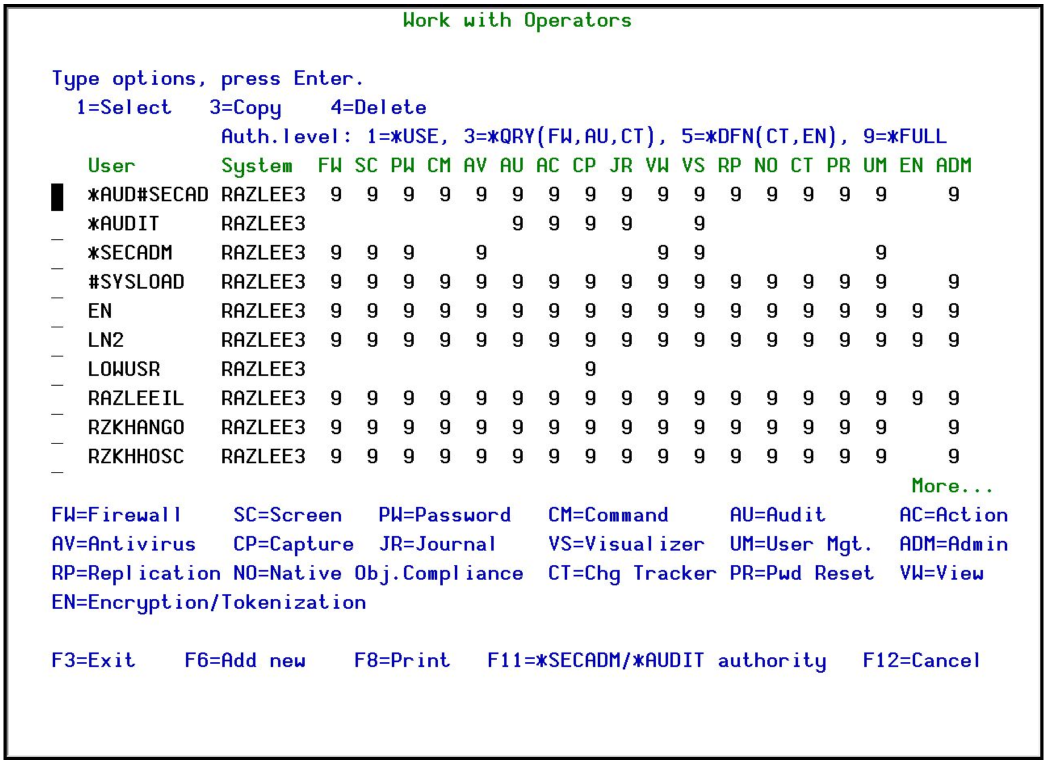
If your organization wants the default to be *BLANK, then the following command must be used:
CRTDTAARA SMZTMPC/DFTPWD *char 10

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

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

To modify operators’ authorities:

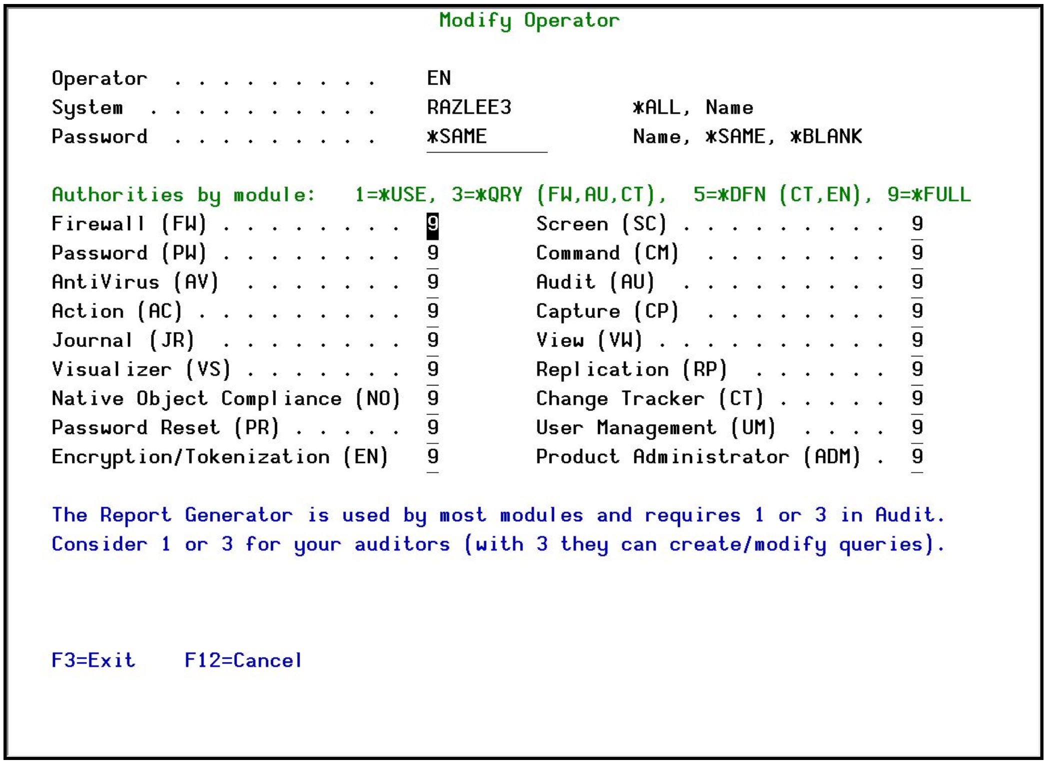
1. Select **11. Work with Operators** from the **BASE Support** menu. The **Work with Operators** screen appears.



```
                             Work with Operators

Type options, press Enter.
  1=Select   3=Copy    4=Delete
              Auth.level: 1=*USE, 3=*QRY(FW,AU,CT), 5=*DFN(CT,EN), 9=*FULL
   User       System  FW SC PW CM AV AU AC CP JR VW VS RP NO CT PR UM EN ADM
_  *AUD#SECAD RAZLEE3  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9     9
_  *AUDIT     RAZLEE3                 9  9  9  9     9
_  *SECADM    RAZLEE3  9  9  9     9              9  9              9
_  #SYSLOAD   RAZLEE3  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9     9
_  EN         RAZLEE3  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9
_  LN2        RAZLEE3  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9
_  LOWUSR     RAZLEE3                       9
_  RAZLEEIL   RAZLEE3  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9
_  RZKHANGO   RAZLEE3  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9     9
_  RZKHHOSC   RAZLEE3  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9     9
                                                                       More...
FW=Firewall    SC=Screen   PW=Password   CM=Command     AU=Audit      AC=Action
AV=Antivirus   CP=Capture  JR=Journal    VS=Visualizer  UM=User Mgt.   ADM=Admin
RP=Replication NO=Native Obj.Compliance  CT=Chg Tracker PR=Pwd Reset  VW=View
EN=Encryption/Tokenization

F3=Exit    F6=Add new    F8=Print   F11=*SECADM/*AUDIT authority   F12=Cancel
```

Figure : Work with Operators screen

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



```
                           Modify Operator

  Operator  . . . . . . . . .    EN
  System  . . . . . . . . . .    RAZLEE3          *ALL, Name
  Password  . . . . . . . . .    *SAME            Name, *SAME, *BLANK

  Authorities by module:   1=*USE, 3=*QRY (FW,AU,CT),  5=*DFN (CT,EN), 9=*FULL
  Firewall (FW) . . . . . . .    9       Screen (SC) . . . . . . . . .   9
  Password (PW) . . . . . . .    9       Command (CM)  . . . . . . . .   9
  AntiVirus (AV)  . . . . . .    9       Audit (AU)  . . . . . . . . .   9
  Action (AC) . . . . . . . .    9       Capture (CP)  . . . . . . . .   9
  Journal (JR)  . . . . . . .    9       View (VW) . . . . . . . . . .   9
  Visualizer (VS) . . . . . .    9       Replication (RP)  . . . . . .   9
  Native Object Compliance (NO)  9       Change Tracker (CT) . . . . .   9
  Password Reset (PR) . . . .    9       User Management (UM)  . . . .   9
  Encryption/Tokenization (EN)   9       Product Administrator (ADM) .   9

  The Report Generator is used by most modules and requires 1 or 3 in Audit.
  Consider 1 or 3 for your auditors (with 3 they can create/modify queries).



  F3=Exit    F12=Cancel
```

Figure : Modify Operator screen

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

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

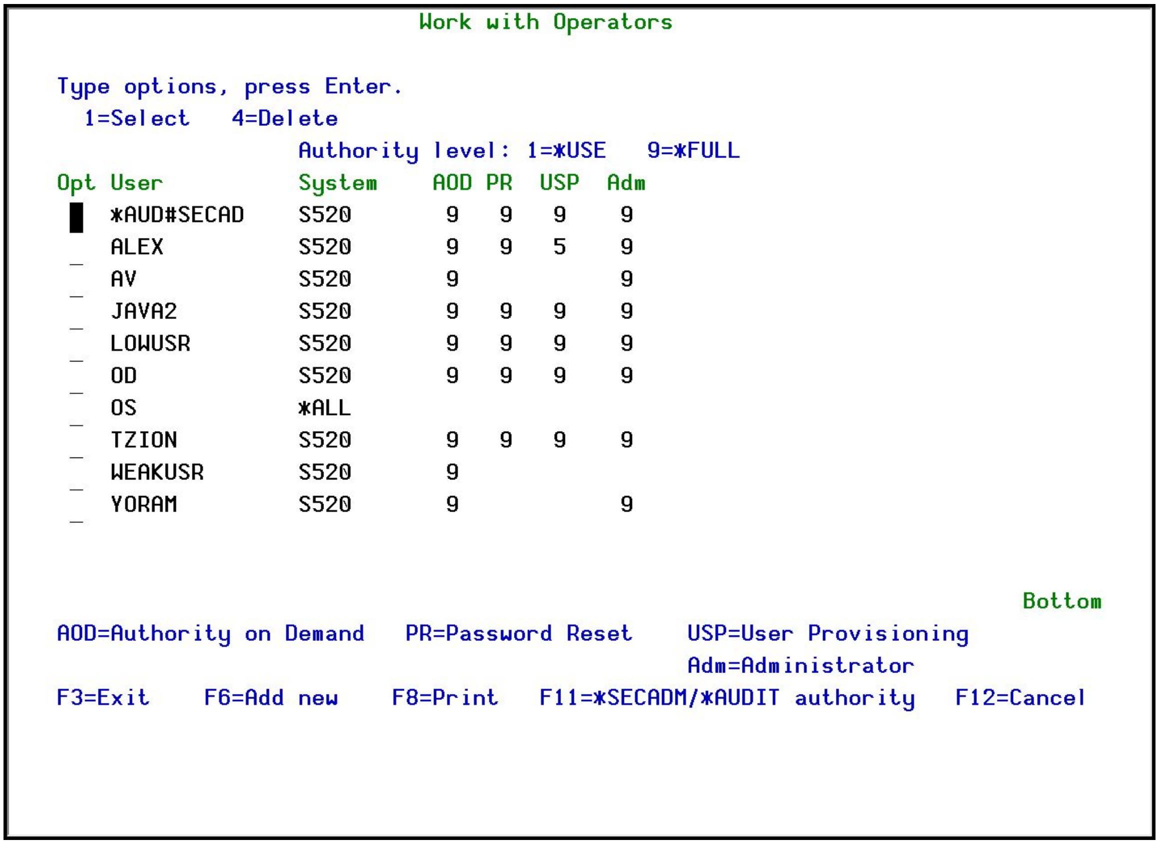
3. Set authorities and press **Enter**. A message appears to inform that the user being added/modified was added to the Authority list that secures the product's objects; the user carries Authority *CHANGE and will be granted Object operational authority. The Authority list is created in the installation/release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

All users of **Encryption** should be added with an authority level of **9** for both **Encryption** and **Product Administrator**.

Work with AOD, P-R Operators

To modify operators' authorities:

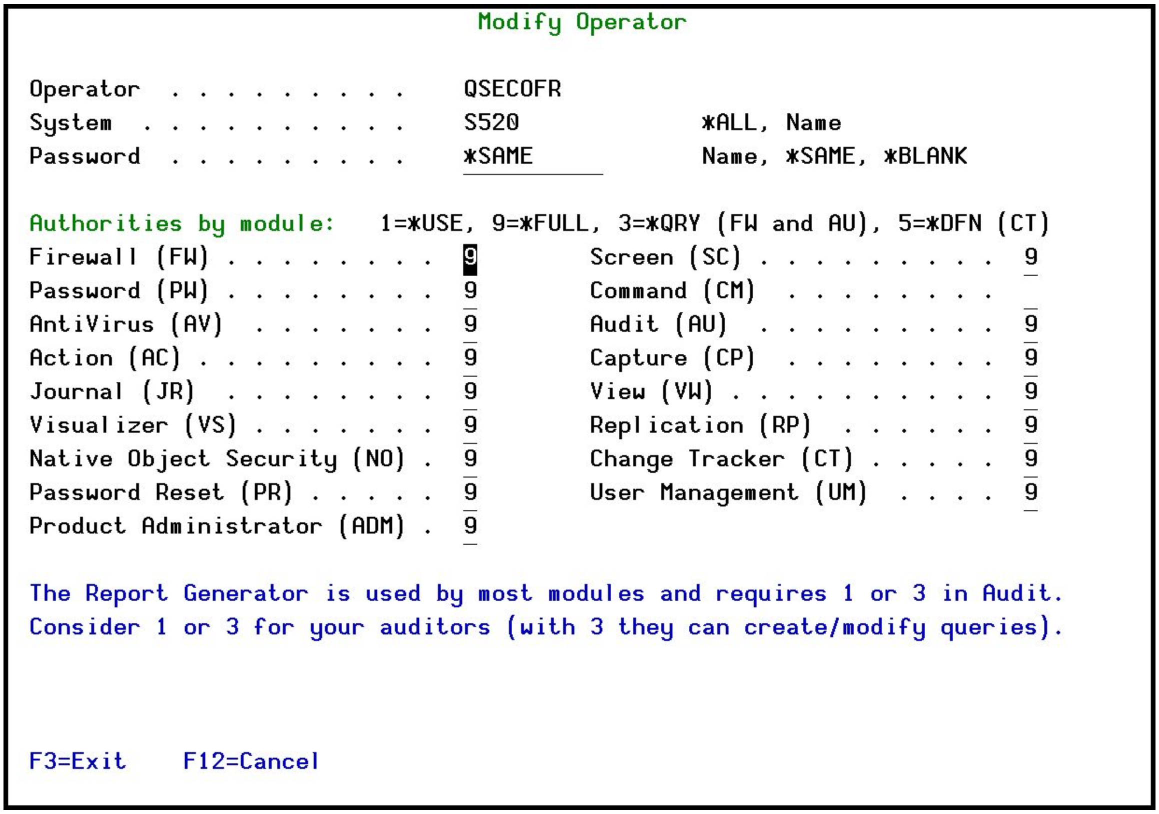
1. Select **12. Work with AOD, P-R Operators** from the **BASE Support** menu. The **Work with Operators** screen appears.



```
                              Work with Operators

   Type options, press Enter.
     1=Select   4=Delete
                     Authority level: 1=*USE   9=*FULL
   Opt User           System     AOD PR  USP  Adm
       *AUD#SECAD     S520        9   9   9    9
    _  ALEX           S520        9   9   5    9
    _  AV             S520        9            9
    _  JAVA2          S520        9   9   9    9
    _  LOWUSR         S520        9   9   9    9
    _  OD             S520        9   9   9    9
    _  OS             *ALL
    _  TZION          S520        9   9   9    9
    _  WEAKUSR        S520        9
    _  YORAM          S520        9            9
    _

                                                                    Bottom
   AOD=Authority on Demand   PR=Password Reset    USP=User Provisioning
                                                  Adm=Administrator
   F3=Exit    F6=Add new    F8=Print   F11=*SECADM/*AUDIT authority   F12=Cancel
```

Figure : Work with Operators screen

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



```
                              Modify Operator

Operator  . . . . . . . . .    QSECOFR
System  . . . . . . . . . .    S520            *ALL, Name
Password  . . . . . . . . .    *SAME           Name, *SAME, *BLANK

Authorities by module:   1=*USE, 9=*FULL, 3=*QRY (FW and AU), 5=*DFN (CT)
Firewall (FW) . . . . . . . .  9       Screen (SC) . . . . . . . . .  9
Password (PW) . . . . . . . .  9       Command (CM)  . . . . . . . .  _
AntiVirus (AV)  . . . . . . .  9       Audit (AU)  . . . . . . . . .  9
Action (AC) . . . . . . . . .  9       Capture (CP)  . . . . . . . .  9
Journal (JR)  . . . . . . . .  9       View (VW) . . . . . . . . . .  9
Visualizer (VS) . . . . . . .  9       Replication (RP)  . . . . . .  9
Native Object Security (NO) .  9       Change Tracker (CT) . . . . .  9
Password Reset (PR) . . . . .  9       User Management (UM)  . . . .  9
Product Administrator (ADM) .  9

The Report Generator is used by most modules and requires 1 or 3 in Audit.
Consider 1 or 3 for your auditors (with 3 they can create/modify queries).



F3=Exit    F12=Cancel
```

Figure : Modify Operator screen

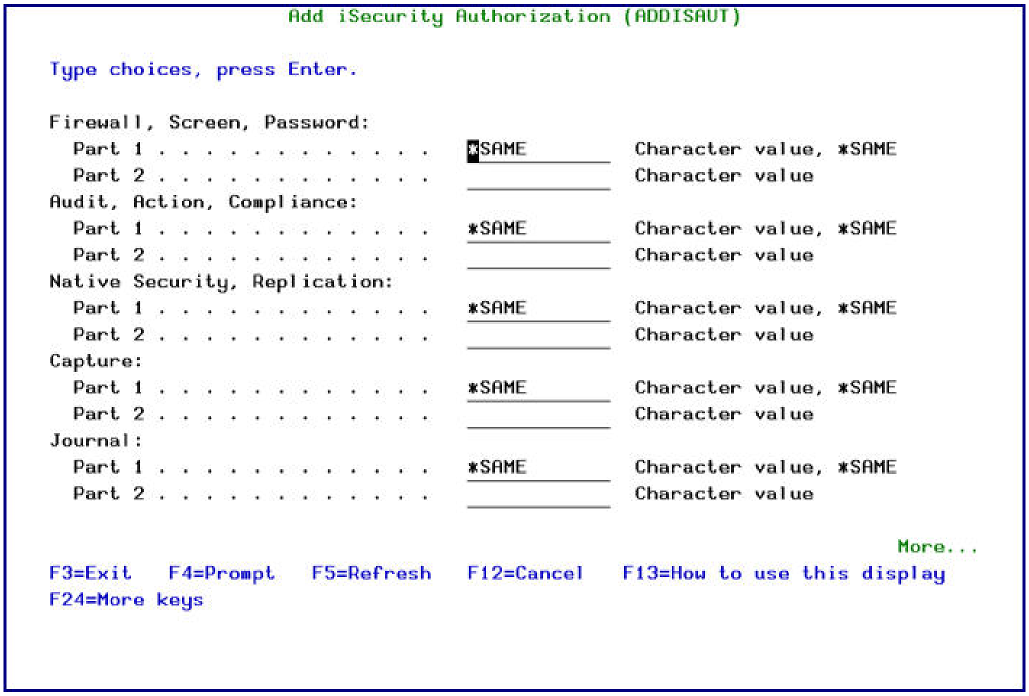
	Description
Password	**Name** = Password ***Same** = Same as previous password when edited ***Blank** = No password
1 = *USE	Read authority only
9 = *FULL	Read and Write authority
3 = *QRY	Run Queries. For auditor use.
5 = *DFN	For Change Tracker use.

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

Work with Authorization

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

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



```
                    Add iSecurity Authorization (ADDISAUT)

 Type choices, press Enter.

 Firewall, Screen, Password:
   Part 1 . . . . . . . . . . . .   *SAME         Character value, *SAME
   Part 2 . . . . . . . . . . . .                 Character value
 Audit, Action, Compliance:
   Part 1 . . . . . . . . . . . .   *SAME         Character value, *SAME
   Part 2 . . . . . . . . . . . .                 Character value
 Native Security, Replication:
   Part 1 . . . . . . . . . . . .   *SAME         Character value, *SAME
   Part 2 . . . . . . . . . . . .                 Character value
 Capture:
   Part 1 . . . . . . . . . . . .   *SAME         Character value, *SAME
   Part 2 . . . . . . . . . . . .                 Character value
 Journal:
   Part 1 . . . . . . . . . . . .   *SAME         Character value, *SAME
   Part 2 . . . . . . . . . . . .                 Character value

                                                                 More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

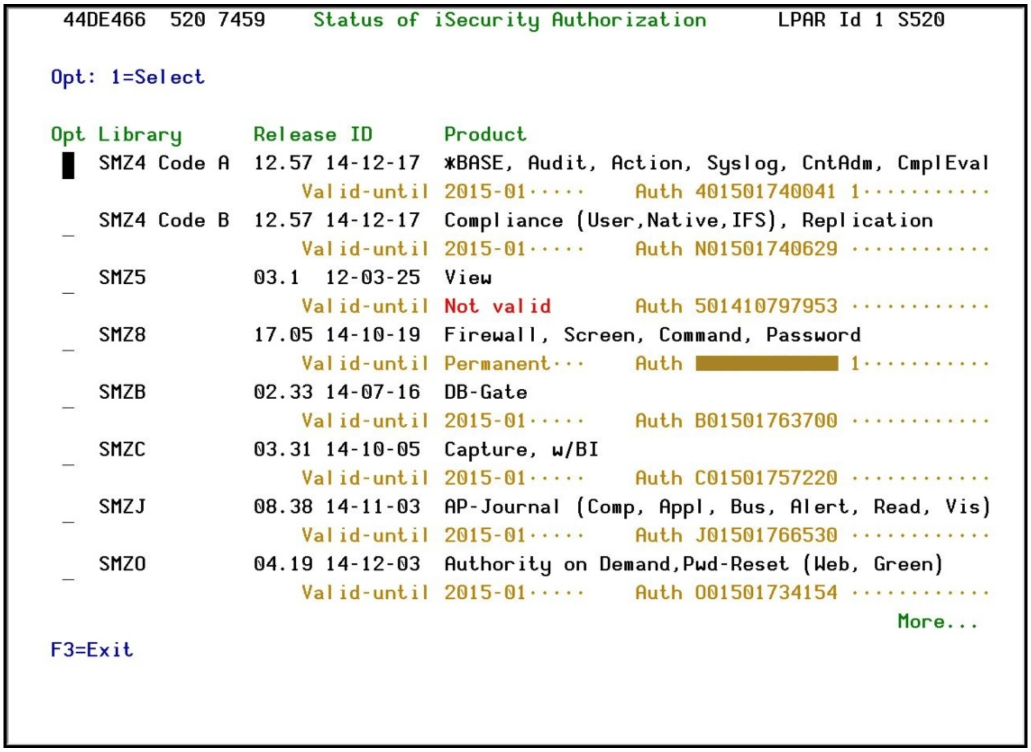
Figure : Add iSecurity Authorization (ADDISAUT) screen

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

Display Authorization Status

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

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



```
 44DE466  520 7459    Status of iSecurity Authorization      LPAR Id 1 S520

Opt: 1=Select

Opt Library      Release ID      Product
    SMZ4 Code A  12.57 14-12-17  *BASE, Audit, Action, Syslog, CntAdm, CmplEval
                     Valid-until 2015-01·····     Auth 401501740041 1···········
 _  SMZ4 Code B  12.57 14-12-17  Compliance (User,Native,IFS), Replication
                     Valid-until 2015-01·····     Auth N01501740629 ············
 _  SMZ5         03.1  12-03-25  View
                     Valid-until Not valid        Auth 501410797953 ············
 _  SMZ8         17.05 14-10-19  Firewall, Screen, Command, Password
                     Valid-until Permanent···     Auth [redacted] 1···········
 _  SMZB         02.33 14-07-16  DB-Gate
                     Valid-until 2015-01·····     Auth B01501763700 ············
 _  SMZC         03.31 14-10-05  Capture, w/BI
                     Valid-until 2015-01·····     Auth C01501757220 ············
 _  SMZJ         08.38 14-11-03  AP-Journal (Comp, Appl, Bus, Alert, Read, Vis)
                     Valid-until 2015-01·····     Auth J01501766530 ············
 _  SMZO         04.19 14-12-03  Authority on Demand,Pwd-Reset (Web, Green)
                     Valid-until 2015-01·····     Auth 001501734154 ············
                                                                       More...
F3=Exit
```

Figure : Status of iSecurity Authority Codes screen

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

Codes that will expire in less than 14 days appear in pink

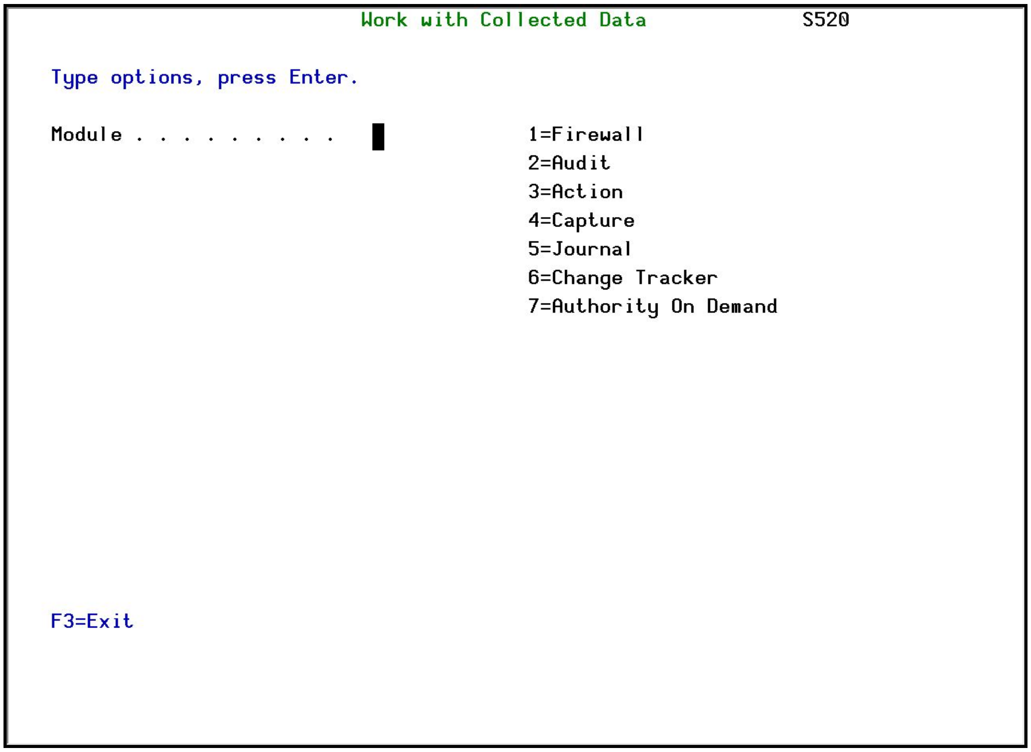
Permanent codes have deliberately been hidden in this screenshot.

General

Work with Collected Data

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

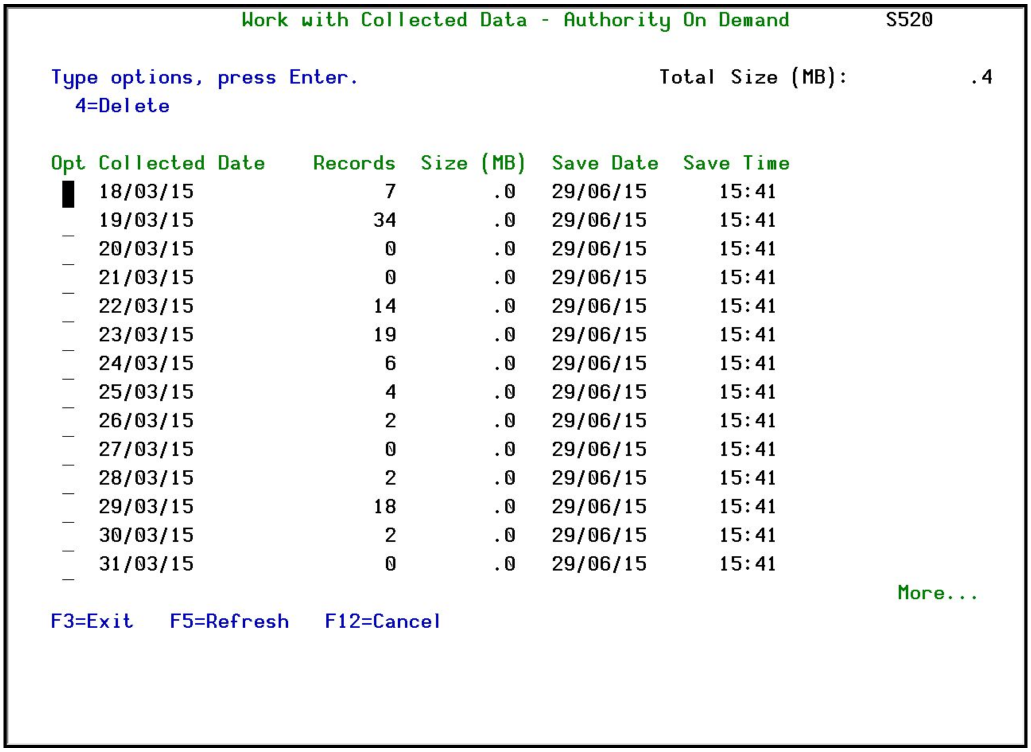
1. Select **51. Work with Collected Data** from the **BASE Support** menu. The **Work with Collected Data** screen appears.



```
                          Work with Collected Data                 S520

 Type options, press Enter.

 Module . . . . . . . . .                  1=Firewall
                                           2=Audit
                                           3=Action
                                           4=Capture
                                           5=Journal
                                           6=Change Tracker
                                           7=Authority On Demand









 F3=Exit
```

Figure : Work with Collected Data screen

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



```
                    Work with Collected Data - Authority On Demand        S520

   Type options, press Enter.                             Total Size (MB):         .4
     4=Delete

   Opt Collected Date    Records  Size (MB)  Save Date  Save Time
   █   18/03/15                7        .0   29/06/15      15:41
   _   19/03/15               34        .0   29/06/15      15:41
   _   20/03/15                0        .0   29/06/15      15:41
   _   21/03/15                0        .0   29/06/15      15:41
   _   22/03/15               14        .0   29/06/15      15:41
   _   23/03/15               19        .0   29/06/15      15:41
   _   24/03/15                6        .0   29/06/15      15:41
   _   25/03/15                4        .0   29/06/15      15:41
   _   26/03/15                2        .0   29/06/15      15:41
   _   27/03/15                0        .0   29/06/15      15:41
   _   28/03/15                2        .0   29/06/15      15:41
   _   29/03/15               18        .0   29/06/15      15:41
   _   30/03/15                2        .0   29/06/15      15:41
   _   31/03/15                0        .0   29/06/15      15:41
   _                                                                    More...
   F3=Exit   F5=Refresh   F12=Cancel
```

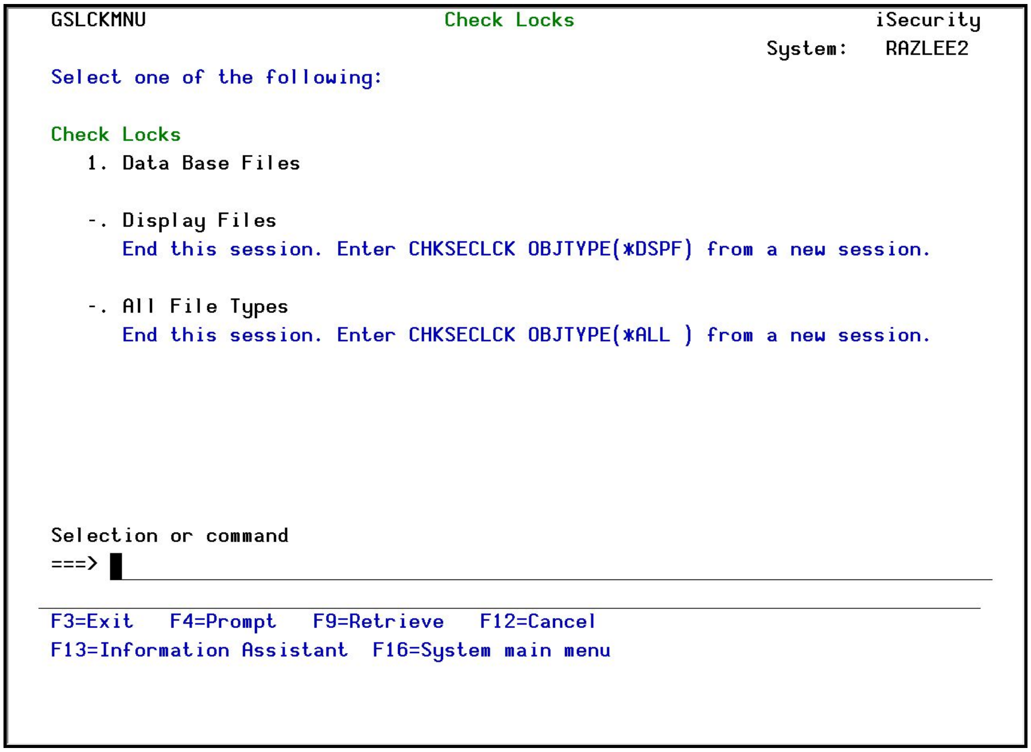
Figure : Work with Collected Data – Authority On Demand screen

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

Check Locks

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

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



```
GSLCKMNU                         Check Locks                         iSecurity
                                                            System:   RAZLEE2
Select one of the following:

Check Locks
   1. Data Base Files

   -. Display Files
      End this session. Enter CHKSECLCK OBJTYPE(*DSPF) from a new session.

   -. All File Types
      End this session. Enter CHKSECLCK OBJTYPE(*ALL ) from a new session.





Selection or command
===>

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

Figure : Check Locks screen

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

*PRINT1-*PRINT9 Setup

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

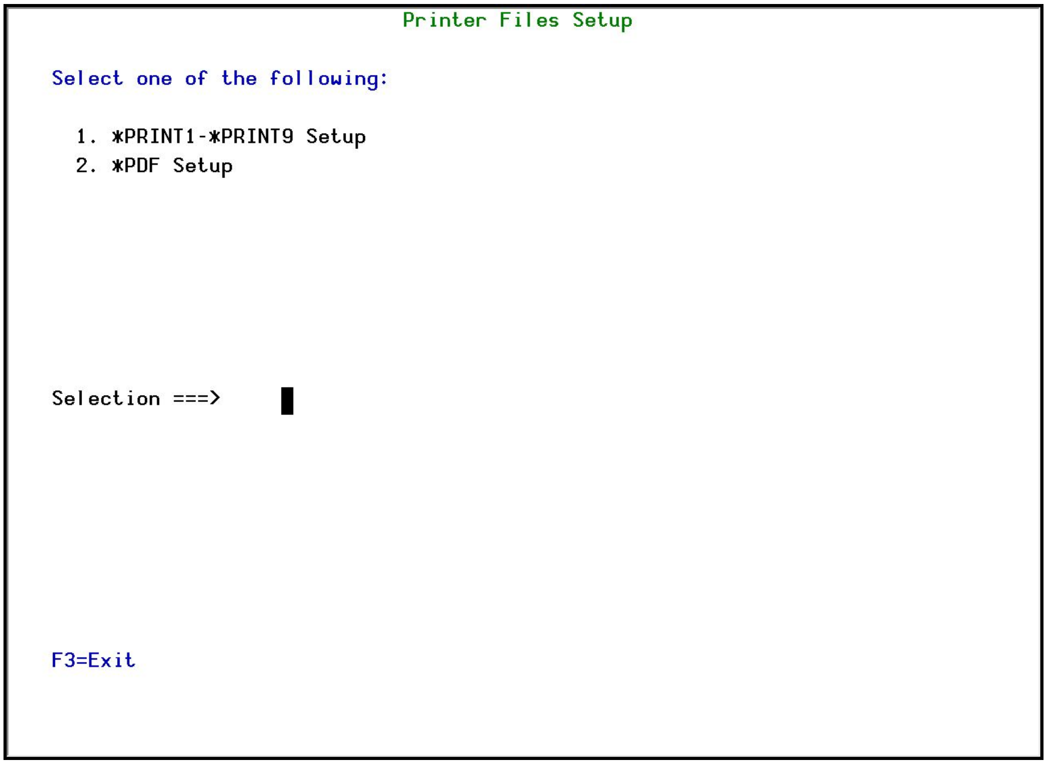
Output to one of the nine remote printers is directed to a special output queue specified on the ***PRINT1-*PRINT9 User Parameters** screen, which, in turn, directs the output to a print queue on the remote system. You use the ***CHGOUTQ*** command to specify the IP address of the designated remote location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

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

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

To define remote printers:

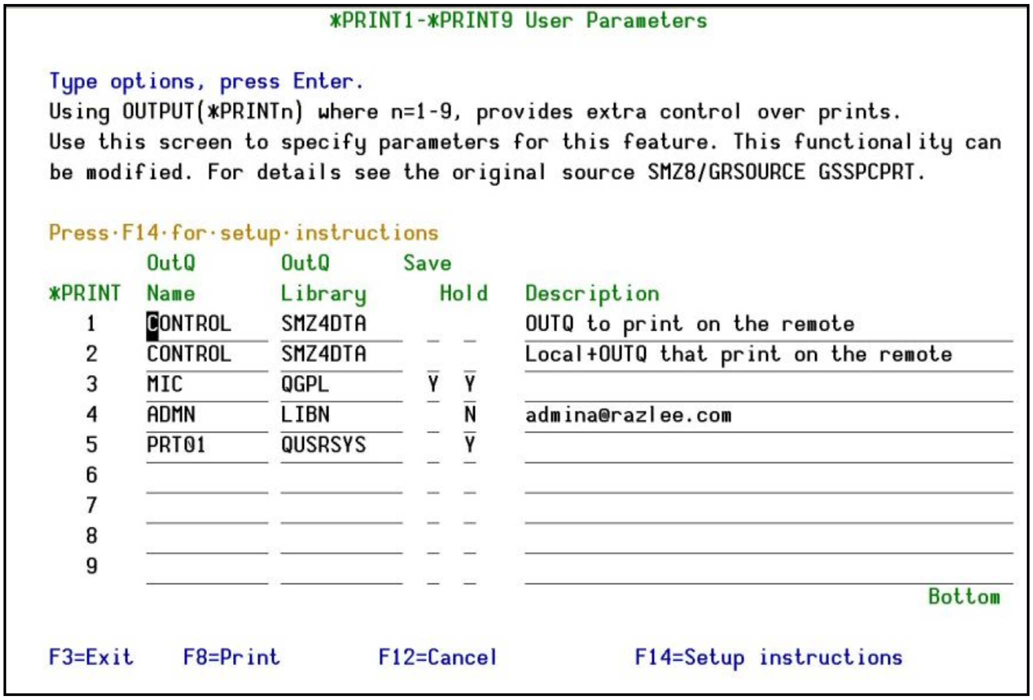
1. Select **58. *PRINT1 - *PRINT9, PDF Setup** from the **BASE Support** menu. The **Printer Files Setup** screen appears.



```
                              Printer Files Setup

   Select one of the following:

     1. *PRINT1-*PRINT9 Setup
     2. *PDF Setup






   Selection ===>









   F3=Exit
```

Figure : Printer Files Setup screen

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



```
                        *PRINT1-*PRINT9 User Parameters

Type options, press Enter.
Using OUTPUT(*PRINTn) where n=1-9, provides extra control over prints.
Use this screen to specify parameters for this feature. This functionality can
be modified. For details see the original source SMZ8/GRSOURCE GSSPCPRT.

Press·F14·for·setup·instructions
        OutQ        OutQ       Save
*PRINT  Name        Library       Hold  Description
   1    CONTROL     SMZ4DTA             OUTQ to print on the remote
   2    CONTROL     SMZ4DTA     _  _    Local+OUTQ that print on the remote
   3    MIC         QGPL        Y  Y
   4    ADMN        LIBN        _  N    admina@razlee.com
   5    PRT01       QUSRSYS     _  Y
   6                            _  _
   7                            _  _
   8                            _  _
   9                            _  _
                                                                         Bottom

F3=Exit    F8=Print        F12=Cancel          F14=Setup instructions
```

Figure : PRINT1-*PRINT9 User Parameters screen

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

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

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

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

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

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

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

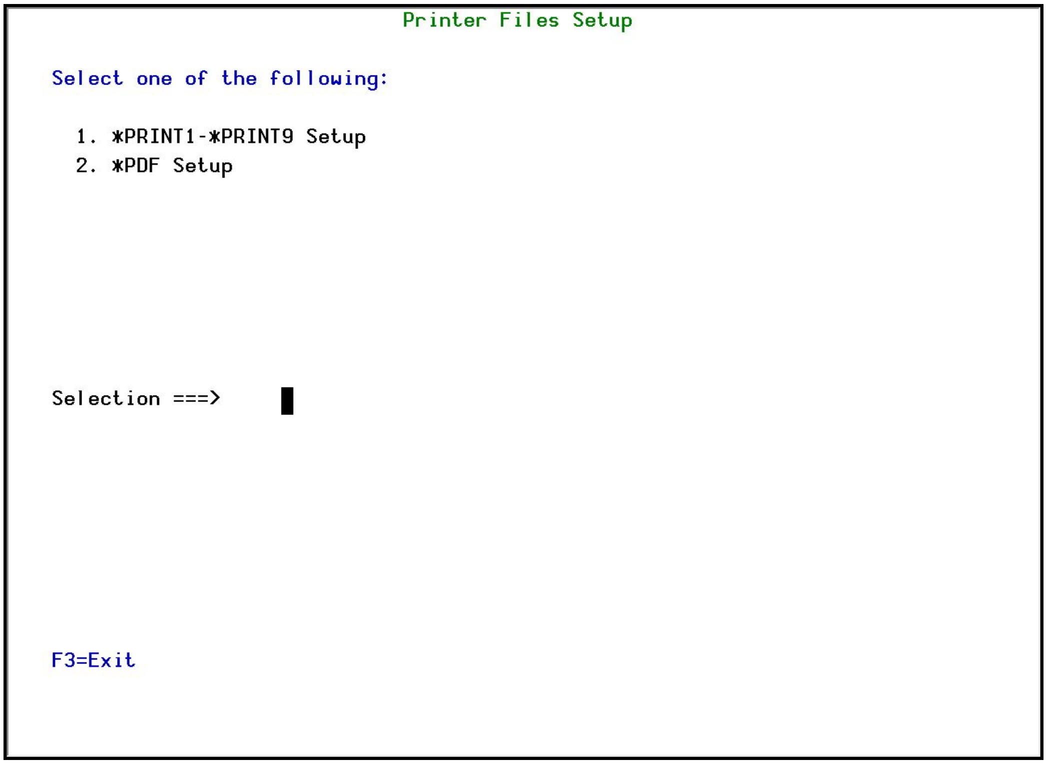
```
CHGOUTQ OUTQ(CONTROL/SMZTMPA) RMTSYS(*INTNETADR)
+   RMTPRTQ(MYOUTQ) AUTOSTRWTR(1) CNNTYPE(*IP) TRANSFORM(*NO)
+   INTNETADR(1.1.1.100)
```

*PDF Setup

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

To define PDF printers:

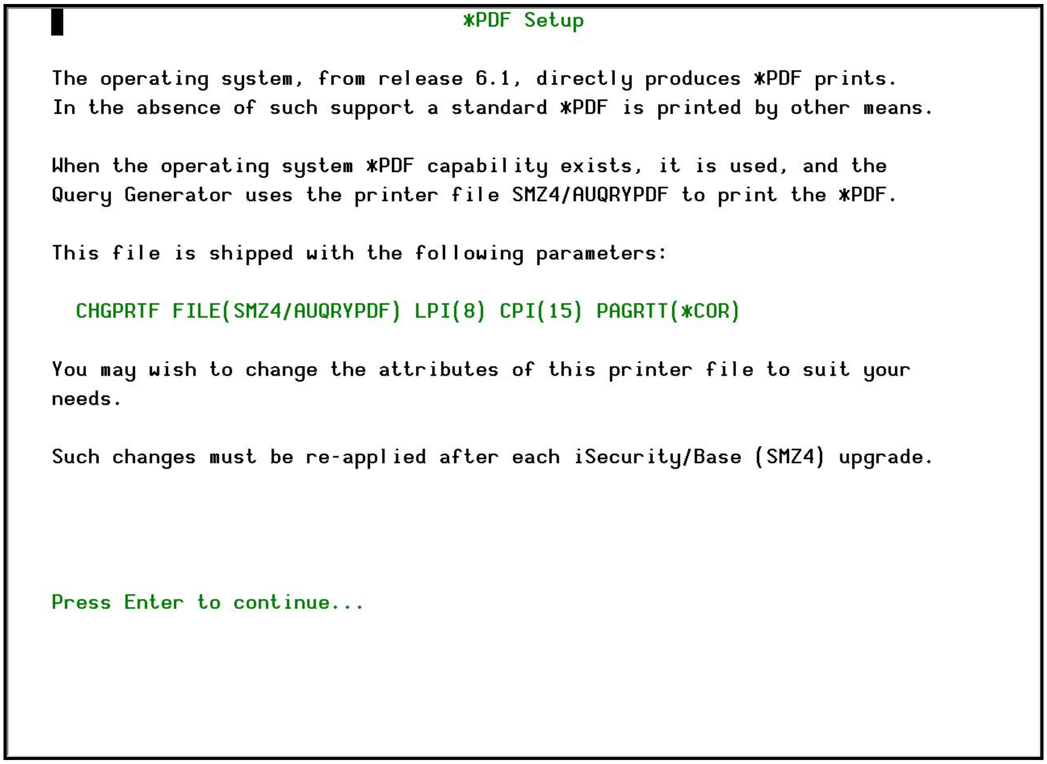
1. Select **58. *PRINT1 - *PRINT9, PDF Setup** from the **BASE Support** menu. The **Printer Files Setup** screen appears.



```
                              Printer Files Setup

  Select one of the following:

    1. *PRINT1-*PRINT9 Setup
    2. *PDF Setup









  Selection ===>










  F3=Exit
```

Figure : Printer Files Setup screen

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



```
                              *PDF Setup

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

When the operating system *PDF capability exists, it is used, and the
Query Generator uses the printer file SMZ4/AUQRYPDF to print the *PDF.

This file is shipped with the following parameters:

  CHGPRTF FILE(SMZ4/AUQRYPDF) LPI(8) CPI(15) PAGRTT(*COR)

You may wish to change the attributes of this printer file to suit your
needs.

Such changes must be re-applied after each iSecurity/Base (SMZ4) upgrade.




Press Enter to continue...
```

Figure : *PDF Setup screen

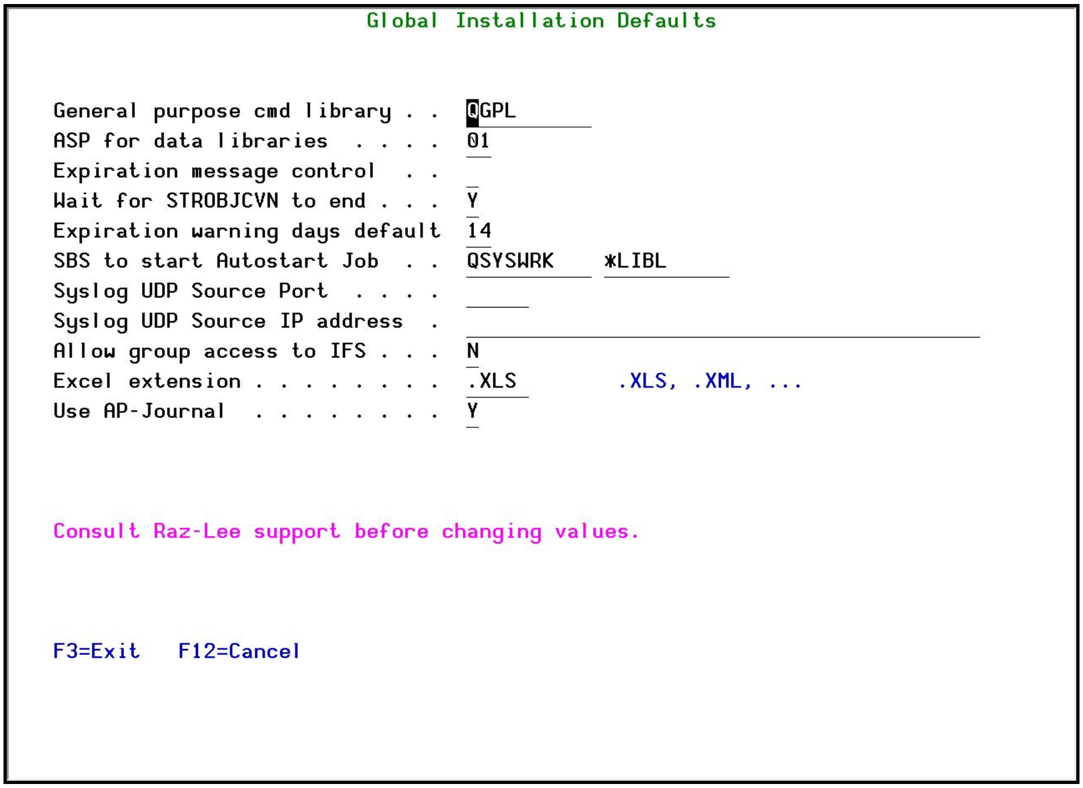
3. Follow the instruction on the screen.

You must re-perform this task after every upgrade of **Field Encryption**.

Global Installation Defaults

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

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



```
                           Global Installation Defaults


   General purpose cmd library . .  QGPL
   ASP for data libraries  . . . .  01
   Expiration message control  . .  _
   Wait for STROBJCVN to end . . .  Y
   Expiration warning days default  14
   SBS to start Autostart Job  . .  QSYSWRK    *LIBL
   Syslog UDP Source Port  . . . .  _____
   Syslog UDP Source IP address  .  ________________________________________
   Allow group access to IFS . . .  N
   Excel extension . . . . . . . .  .XLS        .XLS, .XML, ...
   Use AP-Journal  . . . . . . . .  Y




   Consult Raz-Lee support before changing values.




   F3=Exit   F12=Cancel
```

Figure : Global Installation Defaults screen

Parameter	Description
General purpose cmd library	An alternative library to QGPL from which all **STR***, **RUN***, and ***INIT** commands will be run.
ASP for data libraries	Products being installed for the first time will be installed to this ASP. This refers to the product library and data library (for example, SMZ4, SMZ4DTA) In some products such as AP-Journal, other libraries are created. For example, in the AP-Journal a library is created per application. When created you are prompted with the CRTLIB (Create Library) so that you can set the ASP number. Change the current ASP of the library. All future upgrades will use this ASP. •All products will try to preserve the current ASP at upgrade time. Due to its sensitivity, you should check it.
Expiration message control	**Y**=Yes **N**=No
Wait for STROBJCVN to end	**Y**=Yes **N**=No When installing the product on an OS400 version which is not the one that it was created for, objects require conversion and this is normally done in a batch job sent to work parallel to the installation. If you want the conversion to run inline, (wait until it ends), this field should be set to **Y**.
Expiration warning days default	All products whose authorization expires in less than this number of days are reported as an exception. Enter a number between 01 and 99. The default is **14** days.

Parameter	Description
SBS to start Autostart Job	The Subsystem name and library to use for the Autostart Job.
Syslog UDP Source Port	The source port for Syslog UDP.
Syslog UDP Source IP Address	The source IP address for Syslog UDP
Allow group access to IFS	**Y**=Yes **N**=No Allow access to IFS from group profiles.
Excel extension	**The extension to be used when creating Excel files:** **.XLS** **.XML**
Use AP-Journal	**Y**=Yes **N**=No If you want to use the self-journaling option that will allow you to trace all changes made to iSecurity products, enter **Y**.

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

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

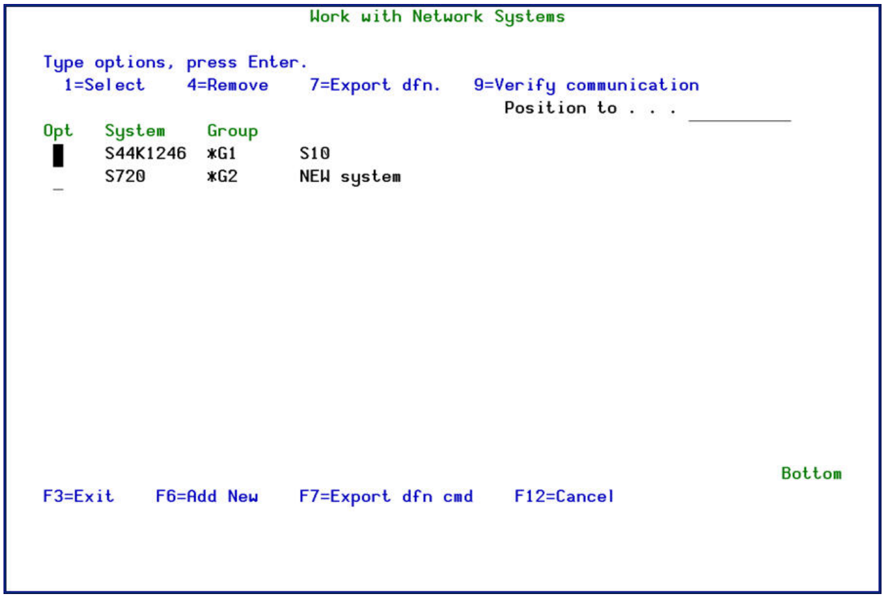
Network Support

-

Work with Network Definitions

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

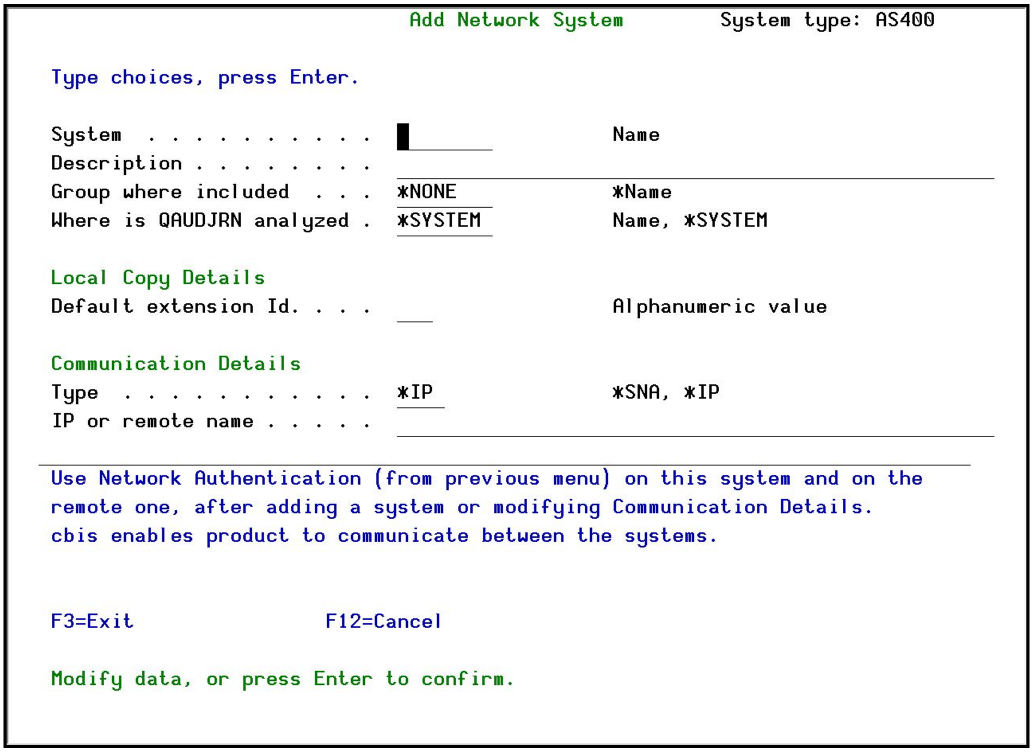
1. Select **71. Work with network definitions**from the **BASE Support** menu. The **Work with Network Systems** screen appears.



```
                              Work with Network Systems

 Type options, press Enter.
   1=Select     4=Remove     7=Export dfn.    9=Verify communication
                                                Position to . . .  __________
 Opt   System     Group
 █     S44K1246   *G1       S10
 _     S720       *G2       NEW system





                                                                        Bottom
 F3=Exit     F6=Add New     F7=Export dfn cmd     F12=Cancel
```

Figure : Work with Network Systems screen

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



```
                              Add Network System         System type: AS400

   Type choices, press Enter.

   System  . . . . . . . . . .                   Name
   Description . . . . . . . .
   Group where included  . . .  *NONE            *Name
   Where is QAUDJRN analyzed .  *SYSTEM          Name, *SYSTEM

   Local Copy Details
   Default extension Id. . . .                   Alphanumeric value

   Communication Details
   Type  . . . . . . . . . . .  *IP              *SNA, *IP
   IP or remote name . . . . .

   Use Network Authentication (from previous menu) on this system and on the
   remote one, after adding a system or modifying Communication Details.
   cbis enables product to communicate between the systems.


   F3=Exit                 F12=Cancel

   Modify data, or press Enter to confirm.
```

Figure : Add Network System screen

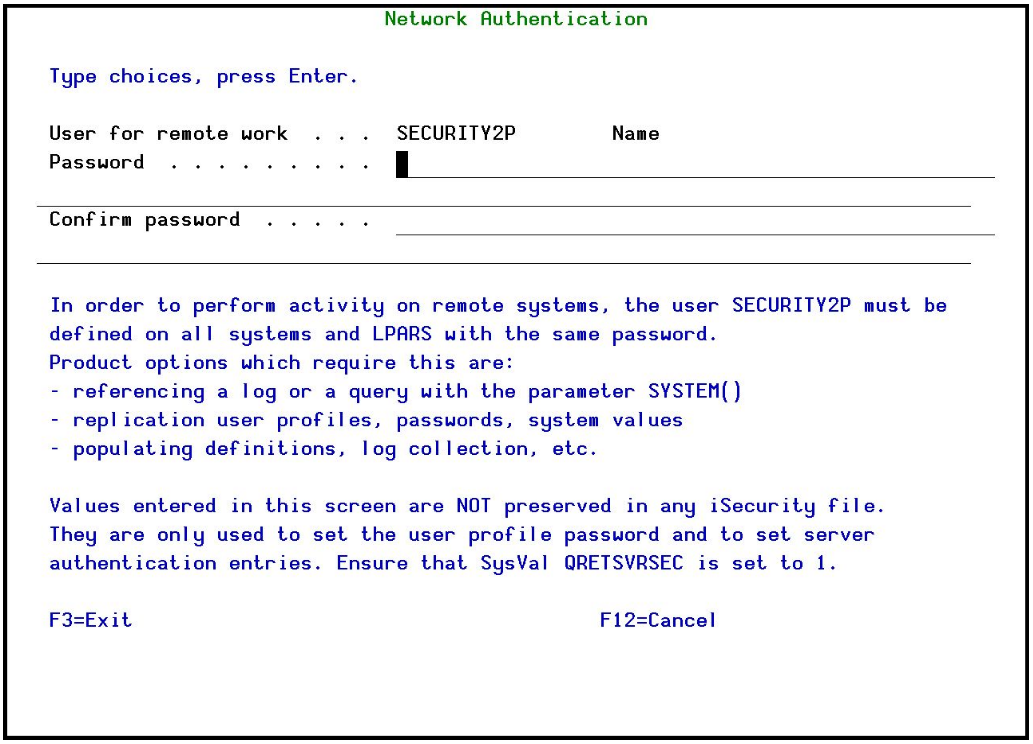
Parameter	Description
System	The name of the system
Description	A meaningful description of the system
Group where included	Enter the name of the group to which the system is assigned
Where is QAUDJRN analyzed	Give the name of the System where QAUDJRN is analyzed. Enter *SYSTEM if it is analyzed locally.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

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

Network Authentication

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

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



```
                          Network Authentication

 Type choices, press Enter.

 User for remote work  . . .  SECURITY2P       Name
 Password  . . . . . . . . .

 Confirm password  . . . . .

 In order to perform activity on remote systems, the user SECURITY2P must be
 defined on all systems and LPARS with the same password.
 Product options which require this are:
 - referencing a log or a query with the parameter SYSTEM()
 - replication user profiles, passwords, system values
 - populating definitions, log collection, etc.

 Values entered in this screen are NOT preserved in any iSecurity file.
 They are only used to set the user profile password and to set server
 authentication entries. Ensure that SysVal QRETSVRSEC is set to 1.

 F3=Exit                                        F12=Cancel
```

Figure : Work with Network Systems screen

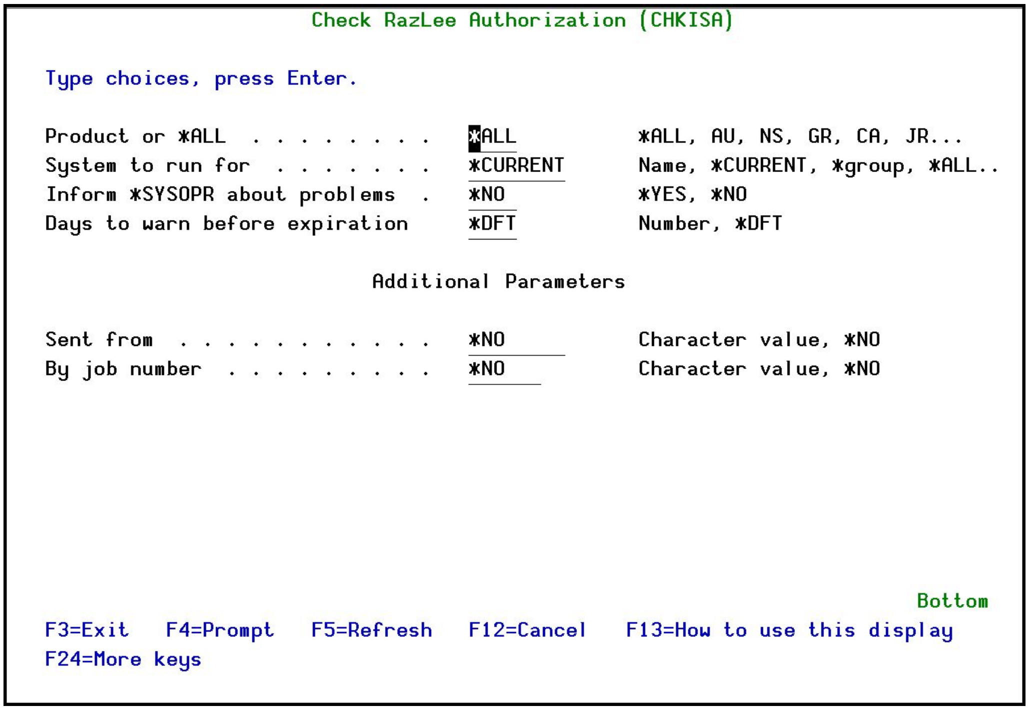
2. Enter the SECURITY2P user password twice and press **Enter**.

Check Authorization Status

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

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

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



```
                        Check RazLee Authorization (CHKISA)

 Type choices, press Enter.

 Product or *ALL  . . . . . . . .   *ALL          *ALL, AU, NS, GR, CA, JR...
 System to run for  . . . . . . .   *CURRENT      Name, *CURRENT, *group, *ALL..
 Inform *SYSOPR about problems  .   *NO           *YES, *NO
 Days to warn before expiration     *DFT          Number, *DFT

                             Additional Parameters

 Sent from  . . . . . . . . . . .   *NO           Character value, *NO
 By job number  . . . . . . . . .   *NO           Character value, *NO







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

Figure : Check Razlee Authorization screen

Parameters or Options	Description
Product or *ALL	***ALL** = report on all products **AU** = Audit **NS** = Native Object Security **GR** = Firewall **CA** = Capture **JR** = AP-Journal **OD** = Authority On Demand **AV** = Anti-Virus **CT** = Change Tracker **DB** = DB-Gate **VW** = View
System to run for	The system to run the authorization check for: **Name** = The name of a specific system in the network ***CURRENT** = The current system ***group** = The name of a group of systems ***ALL** = All systems in the network
Inform *SYSOPR about problem	***YES** = ***NO** =
Days to warn before expiration	**Number** = Any system whose expiry date is less than this number of days will be reported. The default number of days is 14. ***DFT**
Sent from	Value ***NO**
By job number	Value ***NO**

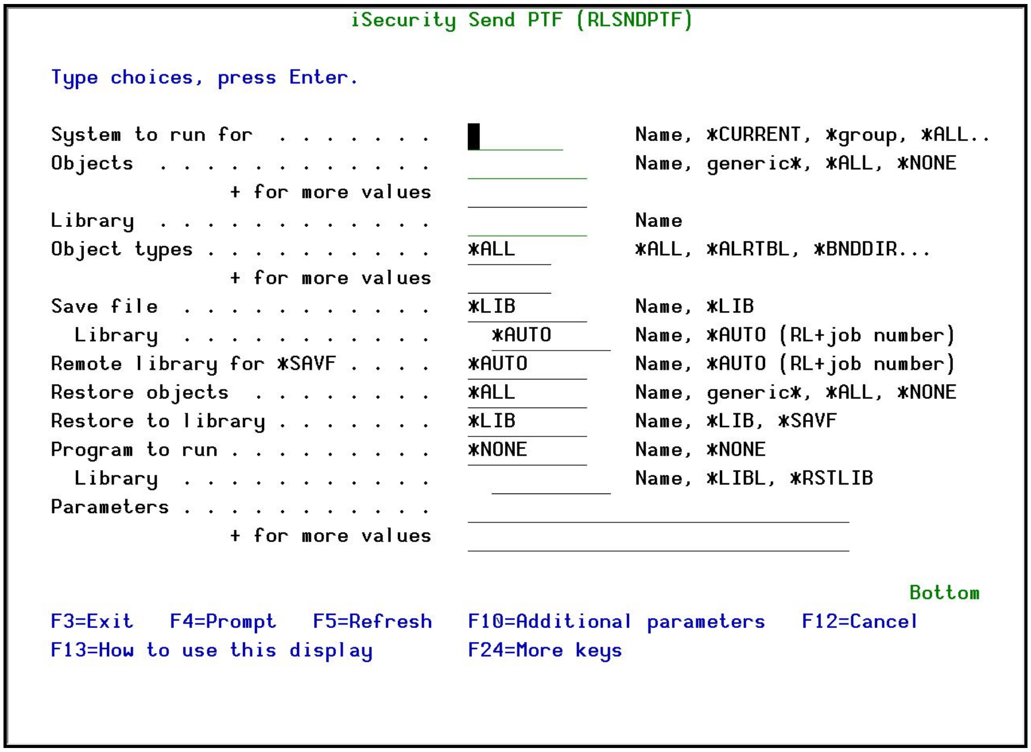
2. Select the correct options and press **Enter**.

Send PTF

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

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

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



```
                          iSecurity Send PTF (RLSNDPTF)

 Type choices, press Enter.

 System to run for  . . . . . . .   _            Name, *CURRENT, *group, *ALL..
 Objects  . . . . . . . . . . . .                Name, generic*, *ALL, *NONE
                + for more values
 Library  . . . . . . . . . . . .                Name
 Object types . . . . . . . . . .   *ALL         *ALL, *ALRTBL, *BNDDIR...
                + for more values
 Save file  . . . . . . . . . . .   *LIB         Name, *LIB
   Library  . . . . . . . . . . .     *AUTO      Name, *AUTO (RL+job number)
 Remote library for *SAVF . . . .   *AUTO        Name, *AUTO (RL+job number)
 Restore objects  . . . . . . . .   *ALL         Name, generic*, *ALL, *NONE
 Restore to library . . . . . . .   *LIB         Name, *LIB, *SAVF
 Program to run . . . . . . . . .   *NONE        Name, *NONE
   Library  . . . . . . . . . . .                Name, *LIBL, *RSTLIB
 Parameters . . . . . . . . . . .
                + for more values

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

Figure : iSecurity Send PTF screen

Parameter	Description
System to run for	**Name** = The specific name of the system ***CURRENT** = The current system ***group** = All systems in the group ***ALL** = All systems on the network
Objects	The objects you want to send. You can enter multiple values **Name** = A specific object **generic*** = A group of objects with the same prefix ***ALL**= All the objects ***NONE**= No objects need to be extracted, the SAVF has already been prepared
Library	The name of the library that contains the objects
Object types	The object types to be sent
Save file / Library	The name and library of the SAVF to contain the objects. If you enter ***LIB** for the file name, the name of the library containing the objects will be used. If you enter ***AUTO** as a name for the library, a library will be created with the name of RL<jobnumber>
Remote library for SAVF	The name of the remote library to receive the SAVF to contain the objects. If you enter ***AUTO** as a name for the library, a library will be created with the name of RL<jobnumber>
Restore objects	The objects to be restored **Name** = A specific object **generic*** = A group of objects with the same prefix ***ALL**= Restore all objects ***NONE**= Do not restore any objects

Parameter	Description
Restore to library	The name of the library to receive the restored objects **Name** = A specific library ***LIB** = the name of the original library containing the objects will be used. ***SAVF**= the same name as the SAVF
Program to run / Library	The name and library of a program to run after the objects have been restored.
Parameters	The parameters for the program that runs after the restore.

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

Run CL Scripts

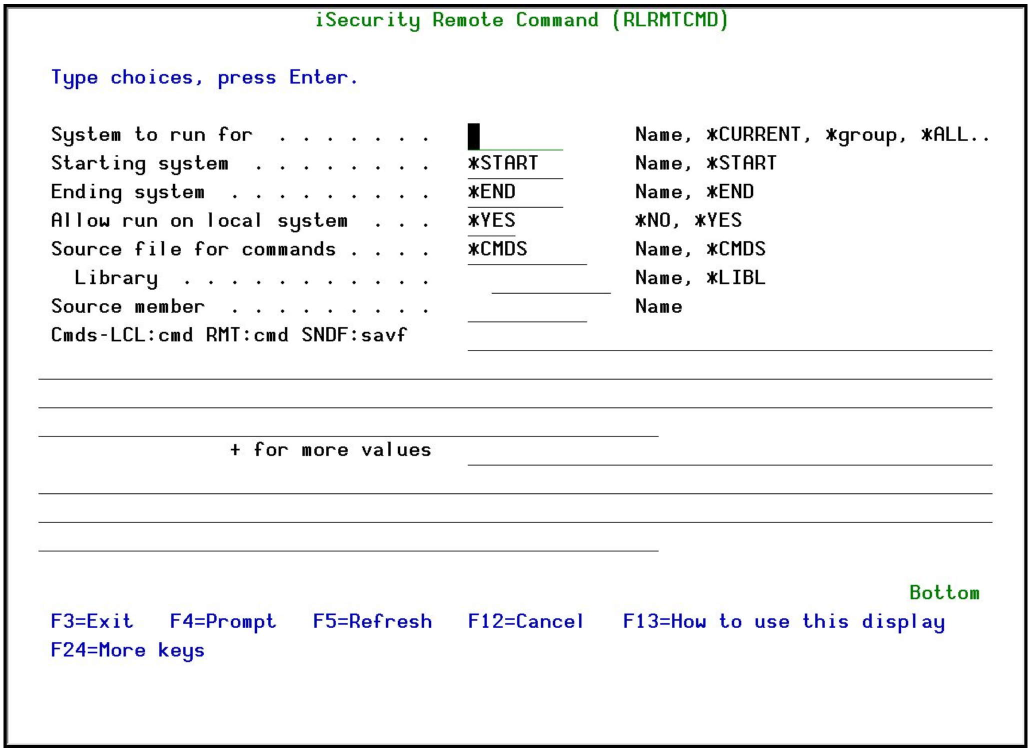
This option allows you to run of a set of commands either from a file or by entering specific commands as parameters. Each command must be preceded by a label:

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

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

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

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



```
                     iSecurity Remote Command (RLRMTCMD)

 Type choices, press Enter.

 System to run for  . . . . . . .                Name, *CURRENT, *group, *ALL..
 Starting system  . . . . . . . .   *START      Name, *START
 Ending system  . . . . . . . . .   *END        Name, *END
 Allow run on local system  . . .   *YES        *NO, *YES
 Source file for commands . . . .   *CMDS       Name, *CMDS
   Library  . . . . . . . . . . .               Name, *LIBL
 Source member  . . . . . . . . .               Name
 Cmds-LCL:cmd RMT:cmd SNDF:savf



                + for more values




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

Figure : iSecurity Remote Command screen

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

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

Current Job Central Administration Messages

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