CRYPTO COMPLETE™

ENCRYPTION SUITE FOR IBM i

Automatic IFS Encryption

Crypto Complete version:	**3.50**
Publication date:	**April 19th, 2016**

LINOMA SOFTWARE

LINOMA SOFTWARE is a division of LINOMA GROUP, Inc.

Table of Contents

Introduction

Crypto Complete is a comprehensive solution for protecting sensitive data through strong encryption technology, integrated key management and audit trails.

The design of *Crypto Complete* allows organizations to implement encryption quickly using intuitive screens and commands, while providing a high degree of protection. Every effort has been made in *Crypto Complete* to minimize the application changes needed, allowing an organization to implement encryption successfully for less time and money.

IFS Encryption

IFS directories can be set up for Automatic encryption.

Crypto Complete's innovative IFS Encryption Registry allows an organization to indicate (register) the directory(s) to encrypt. When IFS directory(s) are "activated" in the Registry, *Crypto Complete* will perform a mass encryption of the current Files in the directory and optionally include subdirectories. *Crypto Complete* can then automatically encrypt the Files in the directory and optionally subdirectories on an ongoing basis as new Files are added or changed.

The automated encryption function in *Crypto Complete's* IFS Encryption Registry will eliminate the need to make changes to your application programs for file encryption. When a user is authorized to view a file, it will be decrypted with no changes to existing programs. When a user is not authorized to view a file, the read will fail with the message "Object marked as a scan failure".

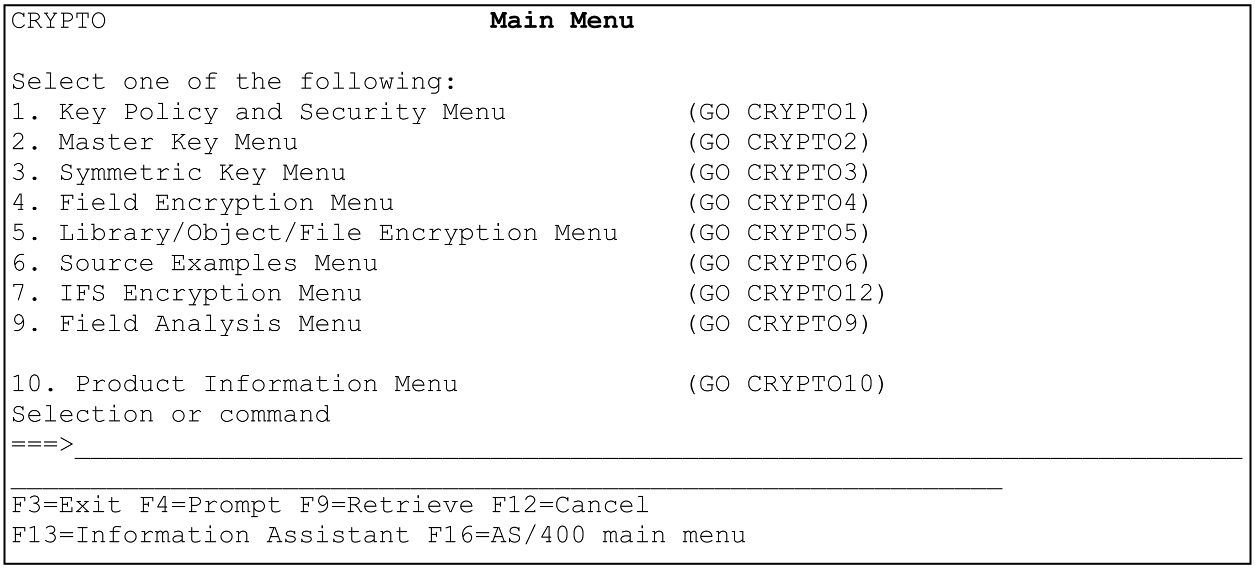
Getting Started

Main Menu

All of the Crypto Complete commands are accessible from a main menu and its sub-menus. To access the main Crypto Complete menu, run the command of:

GO CRYPTO/CRYPTO

The following screen will be displayed:



```
CRYPTO                        Main Menu

Select one of the following:
1. Key Policy and Security Menu           (GO CRYPTO1)
2. Master Key Menu                        (GO CRYPTO2)
3. Symmetric Key Menu                     (GO CRYPTO3)
4. Field Encryption Menu                  (GO CRYPTO4)
5. Library/Object/File Encryption Menu    (GO CRYPTO5)
6. Source Examples Menu                   (GO CRYPTO6)
7. IFS Encryption Menu                    (GO CRYPTO12)
9. Field Analysis Menu                    (GO CRYPTO9)

10. Product Information Menu              (GO CRYPTO10)
Selection or command
===>__________________________________________________________________________
______________________________________________________________
F3=Exit F4=Prompt F9=Retrieve F12=Cancel
F13=Information Assistant F16=AS/400 main menu
```

Commands can be executed from the menu by entering the corresponding menu option. A command can also be executed from the command line using its command name (in parenthesis).

Quick Start

To get started with IFS encryption, you need to first configure Crypto Complete's Key Management settings.

Configure Settings and Keys

Use the commands (in the order listed) below to quickly configure *Crypto Complete's* Automatic IFS Encryption:

Step 1 – Load the Crypto Library into the system Library List

Step 2 – Change System Values #

1. QSCANFS set to *ROOTOPNUD
2. QSCANFSCTL set to *NONE
3. Create Object Scanning for the directory set to *YES
4. Object Scanning set to *YES on the IFS File

Step 3 – Call the ADDIFSEXTP(Adds the Crypto Exit Point Programs) command. This can be found in the IFS Utility Menu (CRYPTO14). This command will add the QIBM_QPWFS_FILE_SERV, QIBM_QP0L_SCAN_CLOSE and QIBM_QP0L_SCAN_OPEN exit programs to the system.

Step 4 – You must stop and restart every Job that will Access the IFS Files. You can do this in two different ways.

1. IPL the system
2. Or end any restart any Job that will be using the exit programs. The instructions below will stop and restart many of the servers. There may be others that are not listed.
    a. End Processes
        i. ENDTCPSVR *NETSVR
        ii. ENDTCPSVR SERVER(*FTP)
        iii. ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
        iv. ENDHOSTSVR *FILE
        v. ENDHOSTSVR *DATABASE
        vi. ENDSBS QSERVER
        vii. End any Batch Jobs that access the IFS Data
    b. Restart processes
        i. STRSBS QSERVER
        ii. STRTCPSVR *NETSVR
        iii. STRTCPSVR SERVER(*FTP)
        iv. STRTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
        v. STRHOSTSVR *FILE
        vi. STRHOSTSVR *DATABASE
        vii. Restart any Batch Jobs that access the IFS Data

Step 5 – Run the STRIFSENCJ Command. This will submit the IFS Server Job to Batch. This command can be found on the IFS Utility Menu (CRYPTO14).

1. This Job uses the CRYPTO Job Description shipped in the CRYPTO Library. Make any changes you want to this Job Description for your system before running the Command.

Step 6 – CRTKEYSTR (Create a Key Store to contain the Data Encryption Keys (DEK)) for Encrypting)

Step 7 – CRTKEYSTR (Create a Key Store to contain the Data Encryption Keys (DEK)) for Decrypting)

Step 8 – CRTSYMKEY (Create a Data Encryption Key (DEK) and save it into the Encryption Key Store)

Step 9 – CPYSYMKEY (Copy the Data Encryption Key (DEK) from the Encryption Key Store into the Decryption Key Store)

Step 10 – In the Encryption Key Store change the Key to only Allow Encryption

Step 11 – In the Decryption Key Store change the Key to only Allow Decryption

Step 12 – Create an Authorization List for Determining who is authorized to Decrypt.

Step 13 – WRKIFSENC (Create an Entry to setup which directory(s) to Encrypt)

* The documentation for these commands (and all other Crypto Complete commands) is contained within this Crypto Complete Manual. All Crypto Complete commands also have on-line help text which can be accessed with the F1 key when a command is prompted.

# Each file that is to be encrypted needs to have the attribute *CRTOBJSCAN set to *YES.

IFS Encryption Registry

Crypto Complete's IFS Encryption Registry allows an organization to specify (register) the directory(s) that require encryption.   There are several configurable options that you can specify for each directory added to the registry.

One option is to have *Crypto Complete* encrypt all files in the subdirectories of the directory entered.

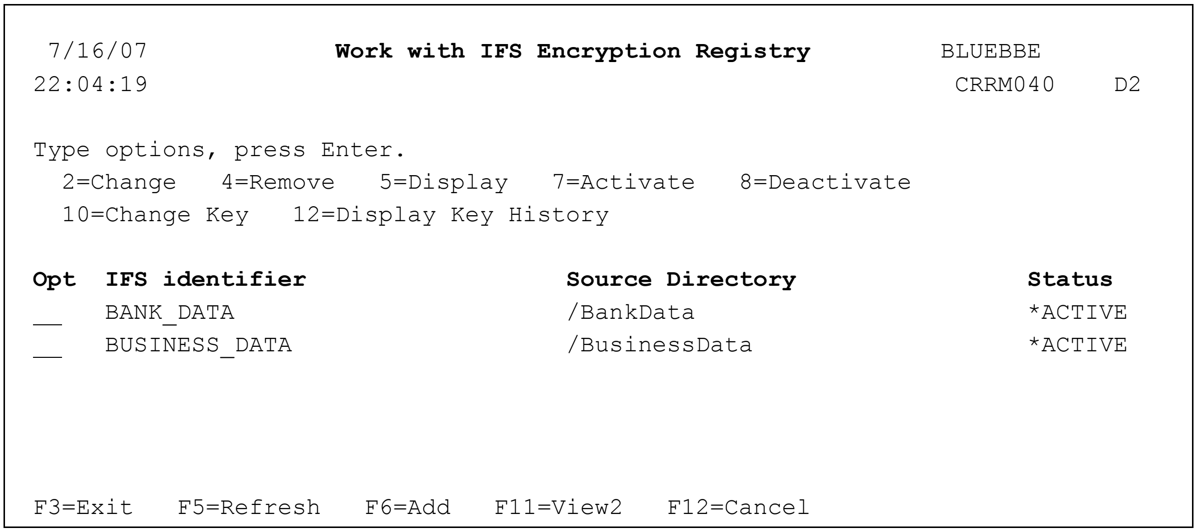
The registry also provides a target directory where the encrypted files should be stored.

Work with IFS Encryption (WRKIFSENC)

The WRKIFSENC command allows authorized users to work with the entries in the IFS Encryption Registry. This command's screen includes functions to add, change, activate, deactivate and remove IFS entries.

Perform the following steps to work with entries in the IFS Encryption Registry:

1. Execute the command of **CRYPTO/WRKIFSENC**.
2. The current entries within the IFS Encryption Registry will be displayed.



```
 7/16/07             Work with IFS Encryption Registry        BLUEBBE
22:04:19                                                       CRRM040    D2

Type options, press Enter.
  2=Change   4=Remove   5=Display   7=Activate   8=Deactivate
  10=Change Key   12=Display Key History

Opt  IFS identifier                  Source Directory               Status
__   BANK_DATA                       /BankData                      *ACTIVE
__   BUSINESS_DATA                   /BusinessData                  *ACTIVE




F3=Exit   F5=Refresh   F6=Add   F11=View2   F12=Cancel
```

Screen Example: WRKIFSENC Command with Sample Values

For each IFS entry listed, the WRKIFSENC screen will show the user-assigned IFS identifier, the source directory and the status. Press F11 to view more information about each entry.

Status codes:

Listed below are the possible status codes that may be displayed for each entry.

Status	Description
*ACTIVE	The IFS entry is activated for encryption
*INACTIVE	The IFS entry is not activated for encryption
*PROCESS	The IFS entry is currently being processed for activation or deactivation.
*ERROR	The activation or deactivation process failed and requires Linoma Software support

(continued on next page)

Screen Options

For each entry listed on the screen, you can utilize one of the following options.

Option	Description
2	Displays a prompt to change the IFS entry using the CHGIFSENC command
4	Displays a prompt to confirm the removal of the IFS entry using the RMVIFSENC command
5	Displays the values for the IFS entry using the DSPIFSENC command
7	Displays a prompt to activate the IFS entry for encryption using the ACTIFSENC command
8	Displays a prompt to deactivate the IFS entry from encryption using the DCTIFSENC command
10	Displays a prompt to change the IFS entry's encryption/decryption keys using the CHGIFSKEY command.
12	Displays the history of the Keys (used to encrypt/decrypt the IFS entry values) using the WRKIFSKEY command.

Screen Function Keys

Listed below are the function keys you can utilize within the WRKIFSENC screen.

Fnctn	Description
F3	Exits the WRKIFSENC screen
F5	Refreshes the list of IFS entries in the Registry
F6	Displays a prompt to add a new IFS entry in the Registry using the ADDIFSENC command
F11	Additionally shows the IFS entry's directory to store the encrypted values, the include subdirectories value and the Decryption Authorization List
F14	Runs the Verify IFS Encryption (VFYIFSENC) command over the entry which prints out the status of the IFS encryption.
F15	Goes to the Edit Auth List (EDTAUTL) command for the Authorization List in the entry. If an entry does not contain an Authorization List then this will go to the Work with Authorization Lists screen.

Add IFS Encryption Entry (ADDIFSENC)

The ADDIFSENC command allows authorized users to add a new entry into the IFS Encryption Registry.

The following users can utilize the ADDIFSENC command:

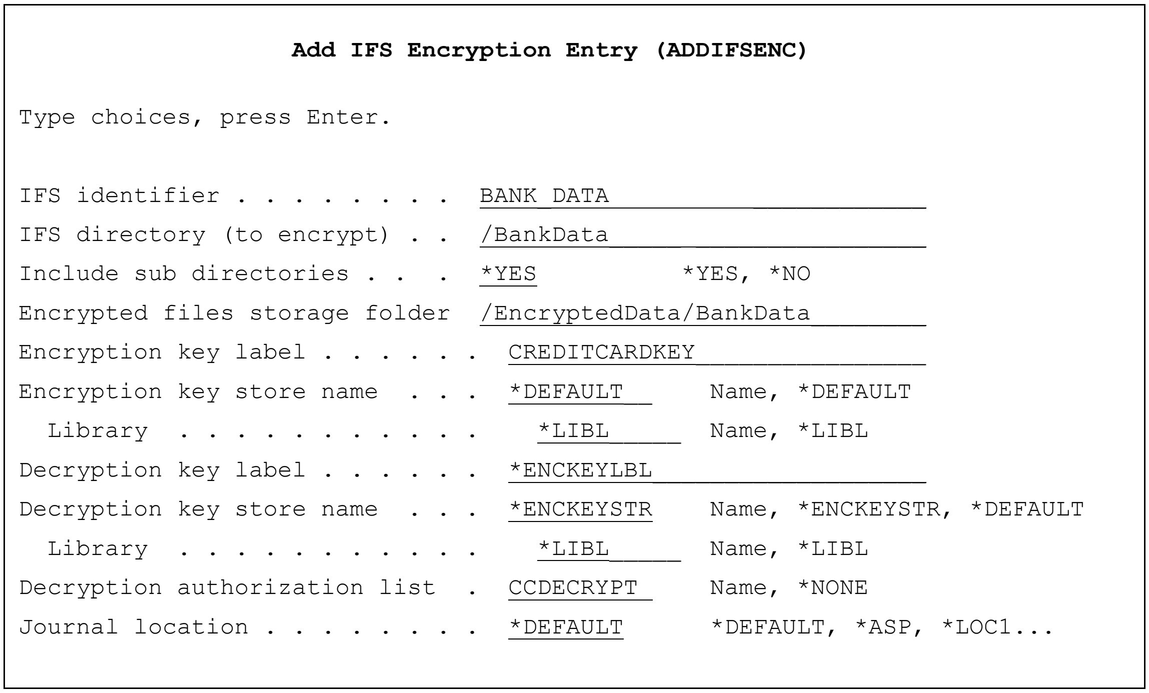
- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the “Maintain IFS Enc. Registry” authority setting

Note: The ADDIFSENC command only adds the IFS entry settings into the registry. It will not cause any action to be performed on the actual files in the directory(s). The IFS will not be activated for encryption until the ACTIFSENC (*Activate IFS Encryption*) command is executed.

This command requires that you have *CHANGE authority to the CRVL003 Validation List (*VLDL) object, which contains the IFS Encryption Registry.

Perform the following steps to add a new entry in the IFS Encryption Registry:

1. Prompt (F4) the command of **CRYPTO/ADDIFSENC**.
2. Press F1 on any parameter for complete on-line help text.
3. Press Enter after the parameter values are entered.



```
                  Add IFS Encryption Entry (ADDIFSENC)

Type choices, press Enter.

IFS identifier . . . . . . . .  BANK_DATA
IFS directory (to encrypt) . .  /BankData
Include sub directories . . .   *YES           *YES, *NO
Encrypted files storage folder  /EncryptedData/BankData
Encryption key label . . . . . .  CREDITCARDKEY
Encryption key store name  . . .  *DEFAULT     Name, *DEFAULT
  Library  . . . . . . . . . . .    *LIBL      Name, *LIBL
Decryption key label . . . . . .  *ENCKEYLBL
Decryption key store name  . . .  *ENCKEYSTR   Name, *ENCKEYSTR, *DEFAULT
  Library  . . . . . . . . . . .    *LIBL      Name, *LIBL
Decryption authorization list  .  CCDECRYPT    Name, *NONE
Journal location . . . . . . . .  *DEFAULT     *DEFAULT, *ASP, *LOC1...
```

Screen Example: ADDIFSENC Command with Sample Values

ADDIFSENC IFS Descriptions:

IFS identifier	Indicate the unique identifier (name) of the entry up to 30 characters. This name cannot contain spaces or certain special characters. Underscore characters can be used in the name (i.e. ACCOUNT_NUMBER). The name is not case sensitive - it will be stored in upper case.
IFS directory (to encrypt)	Specify the path of the IFS directory containing the files to be encrypted.
Include subdirectories	Encrypt files that exist in the subdirectories of the Source directory.
Encrypted files storage folder	Specify the path of the IFS directory to store the encrypted versions of the files.
Encryption key label	Indicate the label of the initial key to use for encrypting the IFS files.
Encryption key store name **Library**	Indicate the name and library of the Key Store which contains the Encryption key label. Specify *DEFAULT to use the default Key Store name specified in the Key Policy.
Decryption key label	Indicate the label of the initial key to use for decrypting the IFS files. Specify *ENCKEYLBL to use the same label name that is entered for the Encryption key label. Caution: If specifying a different key label than the label specified for encryption, then that decryption key should contain the same key value as the encryption key.
Decryption key store name **Library**	Indicate the name and library of the Key Store that contains the Decryption key label. Specify *DEFAULT to use the default key store name specified in the Key Policy. Specify *ENCKEYSTR to use the same value which is entered for the Encryption key store name.
Decryption authorization list	Indicate the i5/OS Authorization List that should be used by the IFS decryption APIs for checking the user's permissions to decrypt for the IFS files. Specify *NONE to not use an Authorization List. * see additional note below
Journal location	Indicate the location of the journal and related objects. Specify *DEFAULT to use the CRYPTO library to store the objects. Specify *IASP to use an IASP library to store the objects. Specify *LOC1 through *LOC5 when an external journal is used to journal the IFS directory and files.

Note: An Authorization List can be created with the CRTAUTL command. The users (or user groups) which need access to the decrypted files will need at least *USE authority to the Authorization List. Additionally the users which need access to the decrypted files are required to have at least *USE authority to the Key Store object which holds the Decryption Key.

Change IFS Encryption Entry (CHGIFSENC)

The CHGIFSENC command allows authorized users to change the settings for an *INACTIVE IFS entry in the Encryption Registry.

> Note: The CHGIFSENC command will only change the settings for an IFS entry in the Encryption Registry. It will not cause any action to be performed on the actual files in the directory(s).

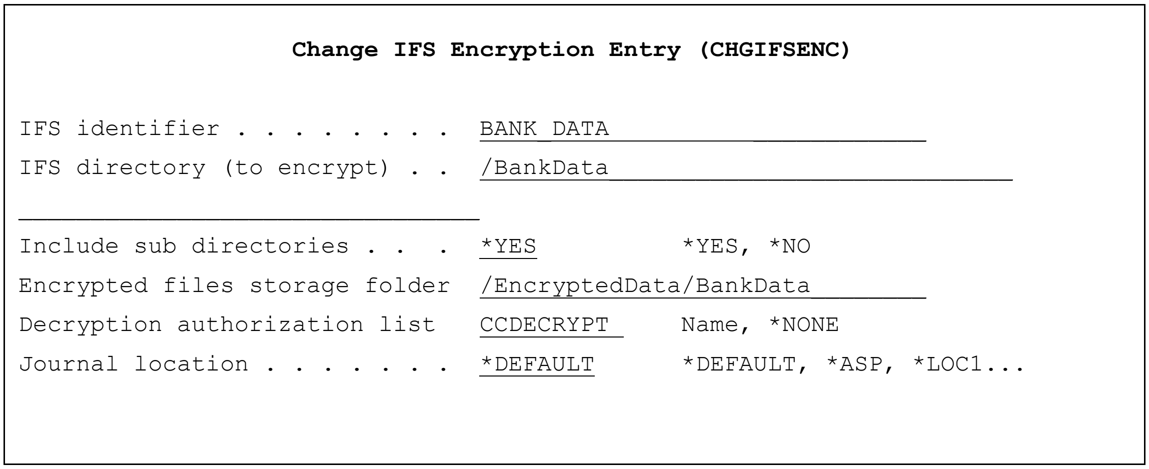
The following users can utilize the CHGIFSENC command:

- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the “Maintain IFS Enc. Registry” authority setting

This command requires that you have *CHANGE authority to the CRVL003 Validation List (*VLDL) object, which contains the IFS Encryption Registry.

Perform the following steps to change an IFS entry in the Encryption Registry:

1. Prompt (F4) the command of **CRYPTO/CHGIFSENC**.
2. Enter the IFS identifier to change, and then press Enter.
3. The current IFS entry settings (parameter values) will be displayed.
4. Press F1 on any parameter for complete on-line help text.
5. Press Enter after the parameter values are changed.
6. For an explanation of the parameters, refer to the documentation for the ADDIFSENC command.



```
                    Change IFS Encryption Entry (CHGIFSENC)

IFS identifier . . . . . . . .  BANK_DATA
IFS directory (to encrypt) . .  /BankData


Include sub directories . .  .  *YES          *YES, *NO
Encrypted files storage folder  /EncryptedData/BankData
Decryption authorization list   CCDECRYPT     Name, *NONE
Journal location . . . . . . .  *DEFAULT      *DEFAULT, *ASP, *LOC1...
```

Screen Example: CHGIFSENC Command with Sample Values

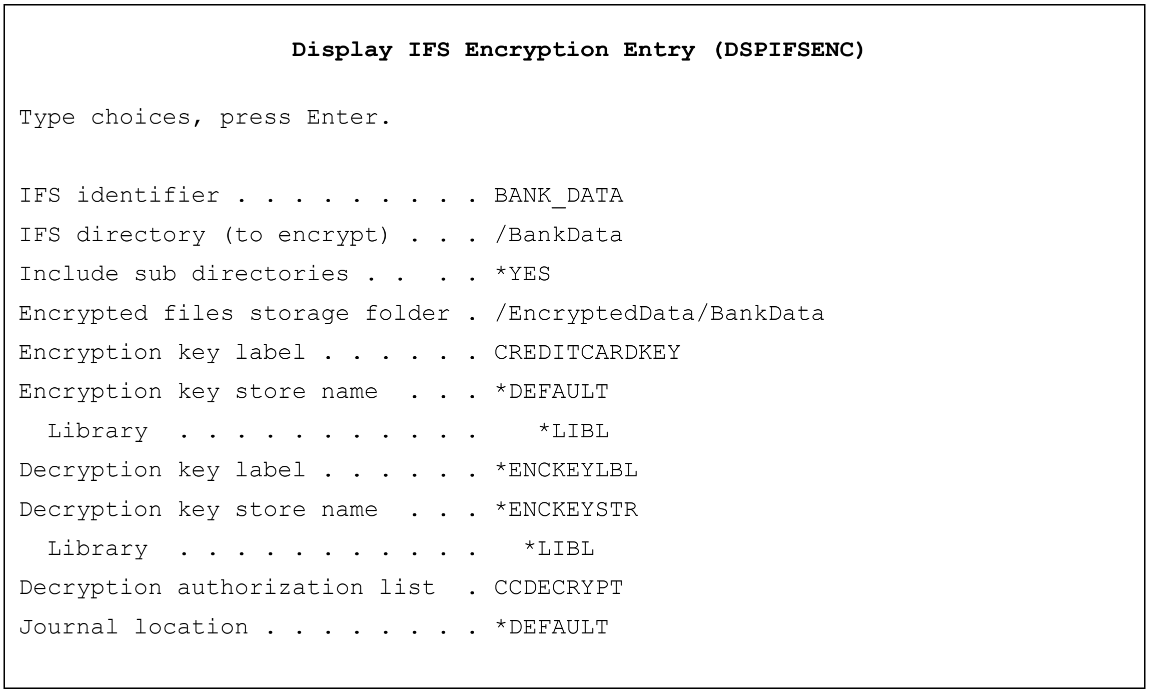
Display IFS Encryption Entry (DSPIFSENC)

The DSPIFSENC command allows authorized users to display an IFS entry's settings within the IFS Encryption Registry.

This command requires that you have *USE authority to the CRVL003 Validation List (*VLDL) object, which contains the IFS Encryption Registry.

Perform the following steps to display an IFS entry's settings within the Encryption Registry:

1. Prompt (F4) the command of **CRYPTO/DSPIFSENC**.
2. Enter the IFS identifier to display, and then press Enter.
3. The current IFS entry settings (parameter values) will be displayed, along with the user and timestamp recorded when the IFS entry was added or last changed.
4. Press F1 on any parameter for complete on-line help text.
5. For an explanation of the parameters, refer to the documentation for the ADDIFSENC command.



```
                    Display IFS Encryption Entry (DSPIFSENC)

Type choices, press Enter.

IFS identifier . . . . . . . . . BANK_DATA
IFS directory (to encrypt) . . . /BankData
Include sub directories . .  . . *YES
Encrypted files storage folder . /EncryptedData/BankData
Encryption key label . . . . . . CREDITCARDKEY
Encryption key store name  . . . *DEFAULT
  Library  . . . . . . . . . . .    *LIBL
Decryption key label . . . . . . *ENCKEYLBL
Decryption key store name  . . . *ENCKEYSTR
  Library  . . . . . . . . . . .   *LIBL
Decryption authorization list  . CCDECRYPT
Journal location . . . . . . . . *DEFAULT
```

Screen Example: DSPIFSENC Command with Sample Values

Activate IFS Encryption (ACTIFSENC)

The ACTIFSENC command allows authorized users to activate an IFS entry in the Encryption Registry.
This command will perform a mass-encryption of the current IFS files in the directory(s) to encrypt. You should only run this command when no applications are currently using the IFS files.

The following users can utilize the ACTIFSENC command:

- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the "Maintain IFS Enc. Registry" authority setting

This command requires that you have *CHANGE authority to the CRVL003 Validation List (*VLDL) object, which contains the IFS Encryption Registry.

This command requires that you have *CHANGE authority to the CRPRIFS, CRPFIFSL1, CRPFIFSL2, CRPFIFSL3, CRPFIFSL4, CRPFIFS2 and CRPFIFSLOG files, which will be updated during this process.

This command can only be used for IFS entries that have an *INACTIVE status.

It is strongly recommended that this command be run in batch mode.

IMPORTANT INSTRUCTIONS:

Before using the ACTIFSENC command to encrypt production data, please make sure you have performed the following steps:

1. Make sure you have *ALL authority to the directory(s) containing the IFS data to encrypt and the directory(s) to store the encrypted file.
2. Within a test environment, you should have tested ACTIFSENC, and tested your applications thoroughly with encrypted values.
3. No applications or users should be currently using the directories containing the IFS files to encrypt.
4. The ACTIFSENC command will perform a mass encryption of the current IFS files in the directory(s). You should allocate enough application downtime for the ACTIFSENC to execute. Execution times will vary depending on the processor speed of your system, the number of files, and other activity running on the system at the time. In order to estimate the execution time for ACTIFSENC, you should run the ACTIFSENC command over some test data first.
5. Check (and double check) the IFS entry settings using the DSPIFSENC command. Especially make sure the Source directory name, Target directory name and include subdirectories settings are correct.

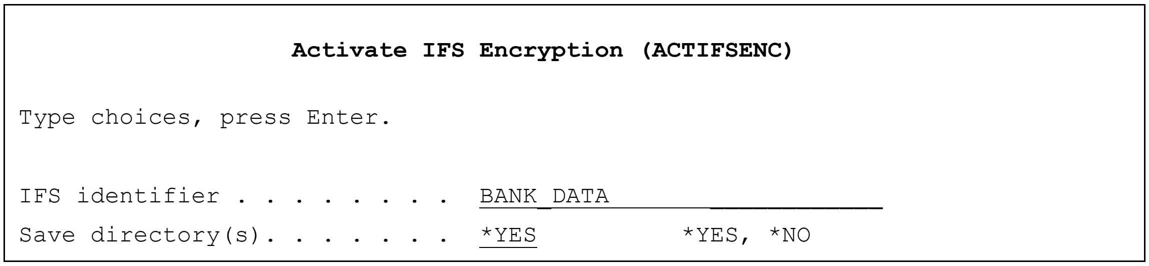
(continue to next page)

Recommendations for ACTIFSENC command:

- Run ACTIFSENC in batch using the SBMJOB command.
- Specify *YES for the “Save directory” parameter to save a copy of the directory(s) to Encrypt and the files into a Save File before the activation process. This option is important for error recovery purposes.
- Ensure that enough disk space is available for a saved copy of the directory and files.

Perform the following steps to activate a IFS entry in the Encryption Registry:

1. Prompt (F4) the command of **CRYPTO/ACTIFSENC**.
2. Type in the IFS identifier to activate and press Enter.



```
                    Activate IFS Encryption (ACTIFSENC)

Type choices, press Enter.

IFS identifier . . . . . . . .  BANK_DATA
Save directory(s). . . . . . .  *YES          *YES, *NO
```

Screen Example: ACTIFSENC Command with Sample Values

The ACTIFSENC command performs the following steps:

1. Optional: Creates a backup of the Source directory structure and files into a Save file named BACKUPxxxxx, where xxxxx is a sequential number from 1 to 99999. This file is placed in the CRYPTO Library.
2. Performs a mass encryption of the current IFS files in the source directory and optionally subdirectories.
3. Journaling will be started over the directory and if Include subdirectories is set to *YES then journaling will be started over the subdirectories as well.
4. The status of the IFS entry will be changed to *ACTIVE.

Notes on ACTIFSENC:

- After the ACTIFSENC command completes: Once you have determined that your applications are working properly with the encrypted files, you can remove the Save file (created in step 1 above) containing a backup of the Source directory structure and Files.
- To activate an iASP entry you should be run this command while in the iASP.

Change IFS Encryption Key (CHGIFSKEY)

The CHGIFSKEY command allows authorized users to change (rotate) the keys used to encrypt and decrypt data for an IFS entry in the Encryption Registry.   Up to 99,999 keys can be rotated for an IFS entry.

This command can be used for *INACTIVE IFS entries, as well as *ACTIVE IFS entries. All Encrypted files will use the original Key that was used to encrypt them when they are Decrypted.

The following users can utilize the CHGIFSKEY command:

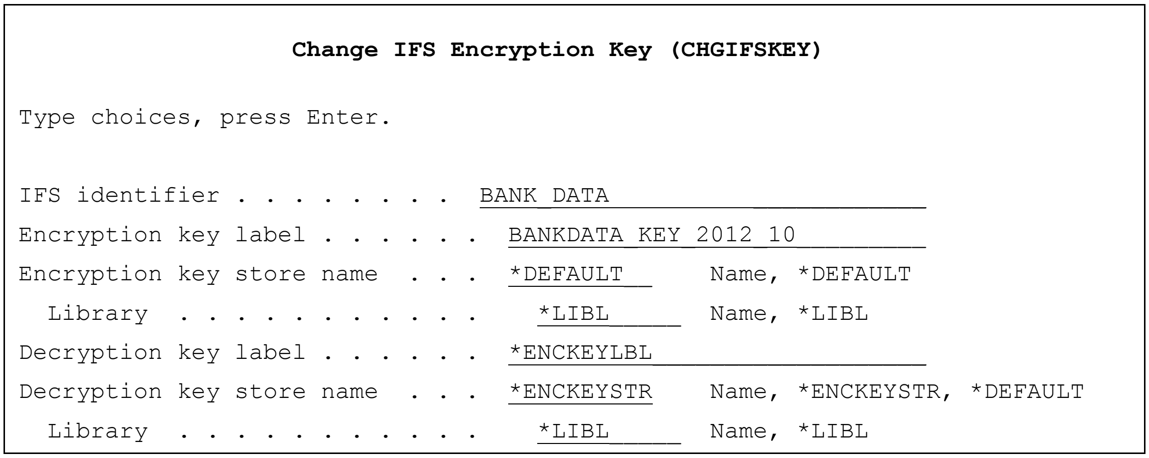
- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the “Maintain IFS Enc. Registry” authority setting

This command requires that you have *CHANGE authority to the CRVL003 Validation List (*VLDL) object, which contains the IFS Encryption Registry.

This command requires that you have *CHANGE authority to the CRPFIFS2 file which will be updated during this process.

Perform the following steps to change the keys for a IFS entry in the Encryption Registry:

1. Prompt (F4) the command of **CRYPTO/CHGIFSKEY**.
2. Press F1 on any parameter for complete on-line help text.
3. Press Enter after the parameter values are specified.



```
                    Change IFS Encryption Key (CHGIFSKEY)

Type choices, press Enter.

IFS identifier . . . . . . . .  BANK_DATA
Encryption key label . . . . . .  BANKDATA_KEY_2012_10
Encryption key store name  . . .  *DEFAULT      Name, *DEFAULT
  Library  . . . . . . . . . . .    *LIBL       Name, *LIBL
Decryption key label . . . . . .  *ENCKEYLBL
Decryption key store name  . . .  *ENCKEYSTR    Name, *ENCKEYSTR, *DEFAULT
  Library  . . . . . . . . . . .    *LIBL       Name, *LIBL
```

Screen Example: CHGIFSKEY Command with Sample Values

IFS descriptions:

IFS identifier	Indicate the unique identifier of the IFS entry in the encryption registry.
Encryption key label	Indicate the label of the key to use for encrypting the IFS values.
Encryption key store name **Library**	Indicate the name and library of the Key Store that contains the Encryption key label. Specify *DEFAULT to use the default Key Store name specified in the Key Policy.
Decryption key label	Indicate the label of the key to use for decrypting the IFS values. Specify *ENCKEYLBL to use the same value which is entered for the Encryption key label. Caution: If specifying a different key label than the label specified for encryption, then that decryption key should contain the same key value as the encryption key.
Decryption key store name **Library**	Indicate the name and library of the Key Store that contains the Decryption key label. Specify *DEFAULT to use the default Key Store name specified in the Key Policy. Specify *ENCKEYSTR to use the same value which is entered for the Encryption key store name.

The Decryption Key Label, Key Store Name and Library are stored in the Encrypted File and are used to Decrypt the file.

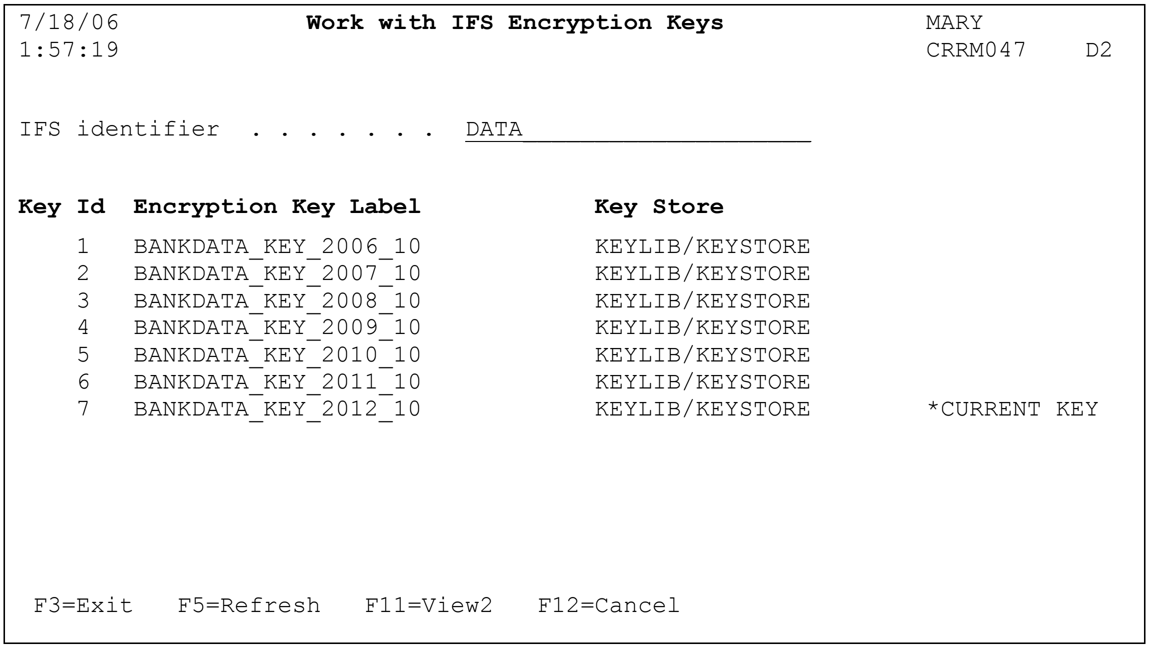
When Key Labels are changed with the CHGIFSKEY command, the new Key information is saved in any newly encrypted IFS file. However the Key Information remains the same for any existing encrypted IFS files, which will allow *Crypto Complete* to decrypt those IFS values using the prior Key Labels. This technique allows you to rotate the keys frequently without having to immediately re-encrypt existing IFS files.

Work with IFS Encryption Keys (WRKIFSKEY)

The WRKIFSKEY command allows authorized users to view the current key, as well as the history of keys used to encrypt and decrypt data for an IFS entry in the Encryption Registry.

Perform the following steps to view the keys for an IFS entry in the Encryption Registry:

1. Prompt (F4) the command of **CRYPTO/WRKIFSKEY**.
2. Specify the IFS identifier and press enter.
3. The keys for the IFS entry will be displayed



```
7/18/06              Work with IFS Encryption Keys              MARY
1:57:19                                                         CRRM047     D2


IFS identifier  . . . . . . .  DATA________________________


Key Id  Encryption Key Label             Key Store
    1   BANKDATA_KEY_2006_10             KEYLIB/KEYSTORE
    2   BANKDATA_KEY_2007_10             KEYLIB/KEYSTORE
    3   BANKDATA_KEY_2008_10             KEYLIB/KEYSTORE
    4   BANKDATA_KEY_2009_10             KEYLIB/KEYSTORE
    5   BANKDATA_KEY_2010_10             KEYLIB/KEYSTORE
    6   BANKDATA_KEY_2011_10             KEYLIB/KEYSTORE
    7   BANKDATA_KEY_2012_10             KEYLIB/KEYSTORE        *CURRENT KEY







 F3=Exit   F5=Refresh   F11=View2   F12=Cancel
```

Screen Example: WRKIFSKEY Command with Sample Values

The key shown with the value of "*CURRENT KEY" is the current Key id used to encrypt IFS files. The file will be decrypted using the Key Label and Key Store that is saved in the Encrypted file.

Screen Function Keys

Listed below are the function keys you can utilize within the WRKIFSKEY screen.

Fnctn	Description
F3	Exits the WRKIFSKEY screen
F5	Refreshes the list of keys for the IFS entry
F11	Additionally shows the decryption key label and Key Store, as well as the user/timestamp recorded when the key was changed.

Deactivate IFS Encryption (DCTIFSENC)

The DCTIFSENC command allows authorized users to deactivate an IFS entry in the Encryption Registry.

The following users can utilize the DCTIFSENC command:

- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the "Maintain IFS Enc. Registry" authority setting

This command can only be used for IFS entries that have an *ACTIVE status.

It is strongly recommended to submit this command to batch.

This command requires that you have *CHANGE authority to the CRVL003 Validation List (*VLDL) object, which contains the IFS Encryption Registry.

This command requires that you have *CHANGE authority to the CRPRIFS, CRPFIFSL1, CRPFIFSL2, CRPFIFSL3, CRPFIFSL4, CRPFIFS2 and CRPFIFSLOG files, which will be updated during this process.

IMPORTANT INSTRUCTIONS:

Before using the DCTIFSENC command to decrypt production data, please make sure you have performed the following steps:

1. Make sure you have *ALL authority to the Source and Target directories containing the IFS files to decrypt.
2. Make sure you have at least *USE authority to the Key Store(s) which hold the Data Encryption Keys (DEKs) that will be used to decrypt the data. You can use the WRKIFSKEY command to find out which Key Store(s) and DEKs are used to decrypt the IFS values. If you created any of these DEKs yourself, in which you are considered the owner of these DEK(s), then the "DEK decrypt usage by owner" setting (viewable in the DSPKEYPCY command) must be a *YES.
3. Make sure you have at least *USE authority to the Authorization List used to allow for decryption of the data.
4. Within a test environment, you should have tested DCTIFSENC and tested your applications thoroughly with decrypted values.
5. No applications or users should be currently using the directory containing the IFS files to decrypt.
6. The DCTIFSENC command will perform a mass decryption of the current IFS files. You should allocate enough downtime for the DCTIFSENC to execute. Execution times will vary depending on the processor speed of your system, the number of files, and other activity running on the system at the time. In order to estimate the execution time for DCTIFSENC, you should run the DCTIFSENC command over some test data first.

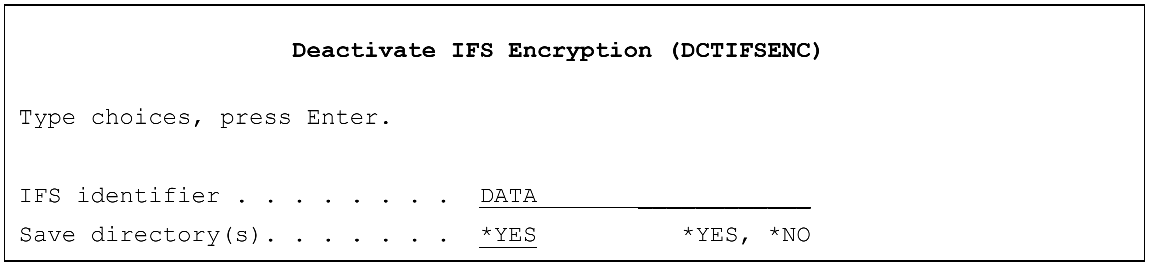
(continue to next page)

Recommendations for DCTIFSENC command:

- Run DCTIFSENC in batch using the SBMJOB command.
- Specify *YES for the “Save directories” parameter to save a copy of the source directory structure and files and the target directory structure and files into a Save File before the deactivation process. This option is important for error recovery purposes.
- Ensure that enough disk space is available for a saved copy of the directory structures.

Perform the following steps to deactivate an IFS entry in the Encryption Registry:

1. Prompt (F4) the **CRYPTO/DCTIFSENC** command.
2. Enter the IFS identifier to deactivate, and then press Enter.



```
                     Deactivate IFS Encryption (DCTIFSENC)

Type choices, press Enter.

IFS identifier . . . . . . . .   DATA
Save directory(s). . . . . . .   *YES          *YES, *NO
```

Screen Example: DCTIFSENC Command with Sample Values

The DCTIFSENC command performs the following steps:

1. Optional: Creates a backup of the IFS directory and subdirectories if INCSUBDIR is *YES (containing the source files) into a Save File named BACKUPxxxxx, where xxxxx is a sequential number from 1 to 99999.
2. Optional: Creates a backup of the IFS directory and subdirectories if INCSUBDIR is *YES ((containing the encrypted files) into a Save File named BACKUPxxxxx, where xxxxx is a sequential number from 1 to 99999.
3. Journaling will be stopped for the directory(s).
4. Performs a mass Decryption of IFS files in the directory(s).
5. The status of the IFS entry will be changed to *INACTIVE.

Notes on DCTIFSENC:

- After the DCTIFSENC command completes: Once you have determined that your applications are working properly with the decrypted values, you can remove the Save files (created in steps 1 and 2 above) containing the backup of the directory(s) containing the source files and the directory(s) containing the encrypted files.
- To deactivate an iASP entry you should be run this command while in the iASP.

Remove IFS Encryption Entry (RMVIFSENC)

The RMVIFSENC command allows authorized users to remove an *INACTIVE IFS entry from the Encryption Registry.

Note: The RMVIFSENC command will only remove the IFS entry from the Encryption Registry. It will not cause any action to be performed on the IFS files in the directory(s).

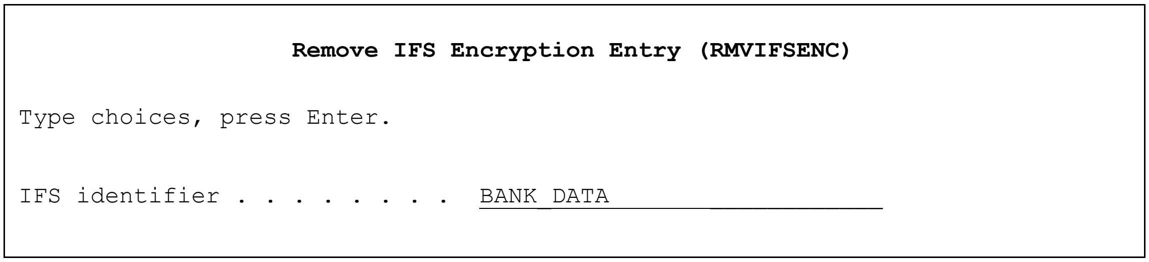
The following users can utilize the RMVIFSENC command:

- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the “Maintain IFS Enc. Registry” authority setting

This command requires that you have *CHANGE authority to the CRVL003 Validation List (*VLDL) object, which contains the IFS Encryption Registry.

Perform the following steps to remove an IFS entry from the Encryption Registry:

1. Prompt (F4) the command of **CRYPTO/RMVIFSENC**.
2. Enter the IFS identifier to remove, and then press Enter.



```
                    Remove IFS Encryption Entry (RMVIFSENC)

Type choices, press Enter.

IFS identifier . . . . . . . .   BANK DATA
```

Screen Example: RMVIFSENC Command with Sample Value

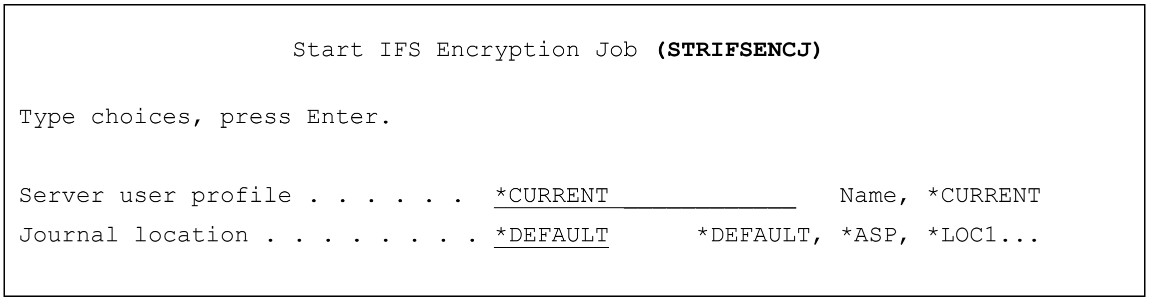
Start IFS Server Job (STRIFSENCJ)

The STRIFSENCJ command submits the server job to batch. This job will monitor the journal records created when files are accessed and run processes after a file has been accessed.

The following users can utilize the STRIFSENCJ command:

- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the “Maintain IFS Enc. Registry” authority setting

This command uses the CRYPTO Job Description that is shipped in the CRYPTO Library when submitting the Server Job (IFSENCJOB) to Batch. You can change this Job Description to run the IFSENCJOB where and how you want.



```
                    Start IFS Encryption Job (STRIFSENCJ)

Type choices, press Enter.

Server user profile . . . . . .  *CURRENT____________   Name, *CURRENT
Journal location . . . . . . . . *DEFAULT      *DEFAULT, *ASP, *LOC1...
```

Screen Example: STRIFSENCJ Command

The Journal Location parameter will determine which journal to monitor. The job names used will be IFSENCJOB(*DEFAULT), IFSENCJOBA(*IASP), IFSENCJOB1(*LOC1), IFSENCJOB2(*LOC2), IFSENCJOB3(*LOC3), IFSENCJOB4(*LOC4) or IFSENCJOB5(*LOC5)

The Server User Profile must have the following authorities:

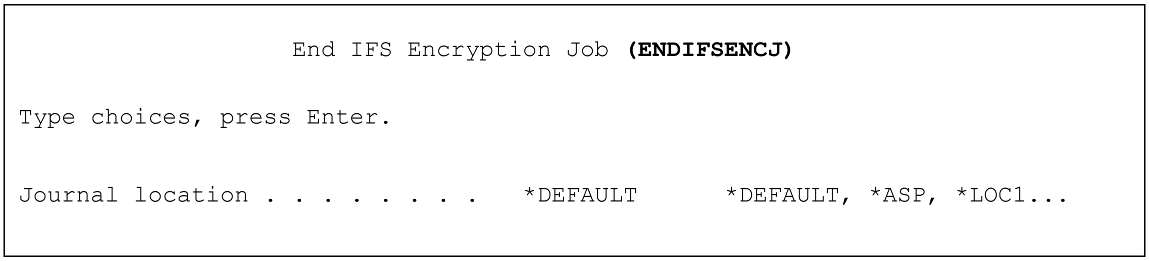
- ALL authority to the Directory(s) to encrypt and all the files in the directory(s).
- ALL authority to the Directory(s) that hold the encrypted files and the files in the directory(s).
- CHANGE authority to the CRPFIFS, CRPFIFSL1, CRPFIFSL2, CRPFIFSL3, CRPFIFSL4, CRPFIFS2, CRPFIFSLOG Files.
- CHANGE authority to the CRDEBUG, CRLSTSEQ and CRSRVRUN Data Areas.
- USE authority to the CRJNI001 Journal and all Journal Receivers.
- USE authority to the CRCL414 and CRRP040 programs in the CRYPTO Library.

End IFS Server Job (ENDIFSENCJ)

The ENDIFSENCJ command sends a message to stop the Server Job (IFSENCJOB).

The following users can utilize the ENDIFSENCJ command:

- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the “Maintain IFS Enc. Registry” authority setting



```
                    End IFS Encryption Job (ENDIFSENCJ)

Type choices, press Enter.

Journal location . . . . . . . .   *DEFAULT      *DEFAULT, *ASP, *LOC1...
```

Screen Example: ENDIFSENCJ Command

The Journal Location parameter will determine which server job to end. The job eneded will be IFSENCJOB(*DEFAULT), IFSENCJOBA(*IASP), IFSENCJOB1(*LOC1), IFSENCJOB2(*LOC2), IFSENCJOB3(*LOC3), IFSENCJOB4(*LOC4) or IFSENCJOB5(*LOC5)

Add Exit Programs (ADDIFSEXTP)

The ADDIFSEXTP command will add the QIBM_QPWFS_FILE_SERV, QIBM_QP0L_SCAN_CLOSE and QIBM_QP0L_SCAN_OPEN exit programs to the system.

The following users can utilize the ADDIFSEXTP command:

- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the "Maintain IFS Enc. Registry" authority setting

Note: The ADDIFSEXTP command will add the exit programs to the Registry however any job that was active at the time will need to be restarted.

IMPORTANT INSTRUCTIONS:

The Add Exit Programs (ADDIFSEXTP) command will just register the exit programs in the system. Any Job that needs to use those exit programs will need to be restarted. There are a couple of ways of doing this.

1. IPL the System.
2. Or end any restart any Job that will be using the exit programs. The instructions below will stop and restart many of the servers. There may be others that are not listed.
    a. End Processes
        i. ENDTCPSVR *NETSVR
        ii. ENDTCPSVR SERVER(*FTP)
        iii. ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
        iv. ENDHOSTSVR *FILE
        v. ENDHOSTSVR *DATABASE
        vi. ENDSBS QSERVER
        vii. End any Batch Jobs that access the IFS Data
    b. Restart processes
        i. STRSBS QSERVER
        ii. STRTCPSVR *NETSVR
        iii. STRTCPSVR SERVER(*FTP)
        iv. STRTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
        v. STRHOSTSVR *FILE
        vi. STRHOSTSVR *DATABASE
        vii. Restart any Batch Jobs that access the IFS Data

The user profile must have the following authorities:

1. *USE authority to the CRRP041 exit program in the CRYPTO Library.
2. *EXECUTE authority to the CRYPTO library.
3. *ALL authority to the Directory(s) to encrypt and all the files in the directory(s).
4. *ALL authority to the Directory(s) that hold the encrypted files and the files in the directory(s).
5. *CHANGE authority to the CRPFIFS, CRPFIFSL1, CRPFIFSL2, CRPFIFSL3, CRPFIFSL4, CRPFIFS2, CRPFIFSLOG Files.
6. *CHANGE authority to the CRDEBUG, CRLSTSEQ and CRSRVRUN Data Areas.
7. *Use Authority to the CRJNI001 Journal and all Journal Receivers.

WARNING: If the user profile is not valid or accessible at the time the exit program is called, the action on the IFS file will be ignored, which may cause the file to NOT be encrypted or decrypted at the appropriate time.

Remove IFS Exit Point Programs (RMVIFSEXTP)

The RMVIFSEXTP command will remove the QIBM_QPWFS_FILE_SERV, QIBM_QP0L_SCAN_CLOSE and QIBM_QP0L_SCAN_OPEN exit programs from the system.

Note: The RMIFSVEXTP command will remove the exit programs from the Registry however any job that was active at the time will need to be restarted.

The following users can utilize the RMVIFSEXTP command:

- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the “Maintain IFS Enc. Registry” authority setting

IMPORTANT INSTRUCTIONS:

The Remove IFS Exit Programs (RMVIFSEXTP) command will remove the IFS Exit Programs from the Registry. Any Jobs that are using the exit programs will need to be restarted. There are a couple of ways of doing this.

1. IPL the System.
2. Or end any restart any Job that will be using the exit programs. The instructions below will stop and restart many of the servers. There may be others that are not listed.
    a. End Processes
        i. ENDTCPSVR *NETSVR
        ii. ENDTCPSVR SERVER(*FTP)
        iii. ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
        iv. ENDHOSTSVR *FILE
        v. ENDHOSTSVR *DATABASE
        vi. ENDSBS QSERVER
        vii. End any Batch Jobs that access the IFS Data
    b. Restart processes
        i. STRSBS QSERVER
        ii. STRTCPSVR *NETSVR
        iii. STRTCPSVR SERVER(*FTP)
        iv. STRTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
        v. STRHOSTSVR *FILE
        vi. STRHOSTSVR *DATABASE
        viii. Restart any Batch Jobs that access the IFS Data

Display IFS Debug Mode (DSPIFSDBG)

The DSPIFSDBG command allows users to view the Debug Mode.   .

This command requires that you have *USE authority to the CRDEBUG Data Area.

Change IFS Debug Mode (CHGIFSDBG)

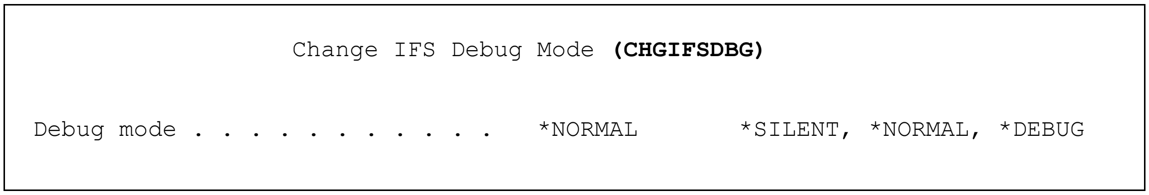
The CHGIFSDBG command allows authorized users to change the Debug Mode.
.

The following users can utilize the CHGIFSDBG command:

- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the “Maintain IFS Enc. Registry” authority setting

This command requires that you have *CHANGE authority to the CRDEBUG Data Area.

This command requires that you have *CHANGE authority to the CRPFIFS2 File.



```
                   Change IFS Debug Mode (CHGIFSDBG)


Debug mode . . . . . . . . . . .   *NORMAL       *SILENT, *NORMAL, *DEBUG
```

Screen Example: CHGIFSDBG Command

Clear IFS Debug Log (CLRIFSLOG)

The CLRIFSLOG command will clear all debug records from the CRPFIFSLOG file.

The following users can utilize the CLRIFSLOG command:

- QSECOFR user profile (unless excluded in the Key Officer settings)
- A user profile with *SECADM authority (unless excluded in the Key Officer settings)
- A Key Officer that has a *YES specified for the “Maintain IFS Enc. Registry” authority setting

This command requires that you have *USE authority to the CRVL003 Validation List (*VLDL) object which contains the IFS Encryption Registry.

This command requires that you have *CHANGE authority to the CRPFIFSLOG File.

IFS Registry Authorization List

Within your applications, you may want to control if IFS files are available for each user to access, based on their authorities. You can control this application-level security through i5/OS Authorization Lists and *Crypto Complete's* IFS Encryption Registry.

Listed below is an example of the steps needed to create Authorization Lists and then associate them to a IFS in the IFS Encryption Registry:

1. Create an i5/OS Authorization List to control authority to DECRYPT values for IFS files. Example:

   > **CRTAUTL AUTL(CCFULL) TEXT('Auth. List of Users allowed to decrypt')**

2. For the CCDATA Authorization List, grant *USE authority only to those users (or user groups) that should have access to decrypt the values. Example:

   > **EDTAUTL AUTL(CCDATA)**

Audit Trails

Entry Type	Description	Command Issued
60	IFS Encryption Registry – Entry added	ADDIFSENC
61	IFS Encryption Registry – Encryption Key changed	CHGIFSKEY
62	IFS Encryption Registry – Entry removed	RMVIFSENC
63	IFS Encryption Registry – Entry activated	ACTIFSENC
64	IFS Encryption Registry – Entry changed	CHGIFSENC
65	IFS Encryption Registry – Entry deactivated	DCTIFSENC
66	IFS Encryption Registry – Unable to Activate Entry	
67	IFS Encryption Registry – Unable to Deactivate Entry	
68	IFS Encryption Failed	
69	IFS Decryption Failed	
70	IFS Error	
71	Add Exit Point Program	
72	Remove Exit Point Program	
73	IFS Server Program Started	
74	IFS Server Program Stopped	
75	Debug Mode was changed	
76	Debug File was cleared	
77	Config File record was added	
78	Config File record was changed	

IFS Encryption Processes and Notes

The IFS Encryption process works in the following way:

When an IFS Entry is activated, the following processes will occur for all files in the directory(s):

1. When SAVDTA is set to *YES a backup of the directory and optionally subdirectories is created.
2. Journaling is started for the directory(s) and all files in the directory(s).
3. If the file is not zero bytes,
    a. the file is Encrypted into the Target directory
    b. The file is cleared and set to zero bytes.
    c. A record is added in the CRPFIFS File.

Note: A record is added to the CRPFIFS file for every directory encrypted.

When an IFS Entry is Deactivated, the process will do the following to every file found in the directory(s):

1. When SAVDTA is set to *YES a backup of the directory and optionally subdirectories is created and a backup of the target directory is created.
2. Journaling is stopped for the file.
3. If the file has an entry in the CRPFIFS file and is zero bytes the file is Decrypted
4. The Target Encrypted File is deleted.
5. The record is removed from the CRPFIFS File.

Note: The directory records are removed from the CRPFIFS.

For an Activated IFS Entry, when a user attempts to Open a file and the QIBM_QP0L_SCAN_OPEN exit point program is called then the following processes occur:

1. The User Authority is checked for the Decrypt Key Store
2. If an Authorization List has been entered the User Authority is checked on the Authorization List.
3. If the User is Authorized to read the file the file will be Decrypted back into the directory and the process will be allowed to continue.

4. If the User is NOT authorized to view the file, then the file is locked and the Open Process will fail. The IBM Message put out when the Open Fails is “Object marked as a scan failure”.
5. The file will remain locked until the IFS Server Job unlocks the file. If the Server Job is not running the File will remain locked.

For an Activated IFS Entry, when a File is Closed and the QIBM_QP0L_SCAN_CLOSE exit point program is called then the following processes occur:

1. If the file is not zero bytes then the following occurs:
    a. Check if a record exists in the CRPFIFS file.
        i. If a record does not exist.
            1. Check if the Target directory exists. If not then create it.
            2. Encrypt the file.
            3. Start Journaling
            4. Add a record to the CRPFIFS File
        ii. If the record exists
            1. Encrypt the file.
            2. Update the record in the CRPFIFS

Note: when a file or directory is copied or moved, a File Open or Close may not be called. When this occurs then the QIBM_QP0L_SCAN_OPEN or QIBM_QP0L_SCAN_CLOSE exit point programs would not be called. When these operations are performed a journal may be created that allows the IFSENCJOB Server program to be alerted that the file or directory was copied or moved.

There are some processes that you need to be aware of when using the IFS Encryption Process.

1. When a user tries to open a file to read and they are not authorized. The file is locked on the system. The file will remain locked until the Server Program (IFSENCJOB) Opens and Clears the file. This process will unlock the file. Depending on how backed up the Server program (IFSENCJOB) is, this may not happen immediately.

2. When Encrypting or Decrypting large files, files 10 MB or larger, the process of opening or closing a file may take a little longer than you are used to. The process has to decrypt the file before you access the file and encrypt the file when the file closes.

3. If a user has a file decrypted and in edit mode, the file will stay decrypted until the file is closed by that user.
    a. If an unauthorized user tries to open the file to read it, the file will be locked.
    b. Also if another user tries to move that file out of the directory to another unencrypted directory, they will get the decrypted version of the file.

4. If a user moves a file into or out of an Encrypted directory, our processes may not know about it until the IFS Server Program retrieves the Journal after the process has occurred. No immediate Encrypting or Decrypting may take place. If the QIBM_QP0L_SCAN_OPEN or QIBM_QP0L_SCAN_CLOSE exit programs are not called then no Authority checking will take place.
    a. When the server program (IFSENCJOB) encounters a Journal record showing a file or directory was copied or moved out of an Encrypted directory, the following process is ran.
        i. Check to see if a record exists in the CRPFIFS file for the Source file or directory. If the record does not exist we ignore the file or directory.
        ii. If the source record still exists in the CRPFIFS file we
            1. Check to see if the user was authorized to Copy or Move the file.
            2. If they were not authorized and the process was a move we recreate the directory structure and zero byte files for the source.
            3. If the user was authorized to move the files we decrypt the files into the destination directories and then remove the source Encrypted files and directories and then remove the CRPFIFS records.

5. When a user tries to Decrypt a file thru a mapped drive, the default user that is used is QUSER. Crypto Complete will use the exit point QIBM_QPWFS_FILE_SERV to retrieve the User Id that the user signed in as. This user Id will be used to check for authority to Decrypt the File. When the exit point QIBM_QP0L_SCAN_OPEN is called to Decrypt the file, the user QUSER must be authorized to the Decrypt Key Store to be able to Decrypt the file.
    a. If you want all operations to be authorized from a mapped drive you can also give QUSER authority to the Authorization List.

b. If you only want certain users to have authority to Decrypt when using a mapped Drive then you need giver those users or groups *USE Authority to the Authorization List

License agreement and limited warranty

READ CAREFULLY BEFORE USING

The *Crypto Complete* software ('CRYPTO COMPLETE') is a proprietary product of Linoma Software ('LINOMA SOFTWARE') and is protected by this Agreement, copyright laws and international treaties. This is a legal agreement (the 'Agreement') between you, the user, and LINOMA SOFTWARE. Clicking on the license agreement acceptance button (if you are downloading CRYPTO COMPLETE), opening the package (if you have acquired a copy of CRYPTO COMPLETE on physical media) or loading or using CRYPTO COMPLETE on your system indicates your acceptance of the terms of this Agreement. If you do not wish to agree to the terms of this Agreement, you should promptly notify LINOMA SOFTWARE and immediately remove CRYPTO COMPLETE from your system and cease use of CRYPTO COMPLETE.

A. LINOMA SOFTWARE grants you the right to use CRYPTO COMPLETE on your computer system. If you have a trial version of CRYPTO COMPLETE, your license is limited to use only during the trial period and only for evaluation purposes.

B. You may not alter, modify, decompile, disassemble or reverse engineer CRYPTO COMPLETE, or otherwise attempt to reproduce the source code thereof.

C. You acknowledge that CRYPTO COMPLETE is provided pursuant to a license and all title and ownership to CRYPTO COMPLETE shall remain with LINOMA SOFTWARE or its licensors.

D. You may use CRYPTO COMPLETE only for your own internal business purposes and may not use CRYPTO COMPLETE in a service bureau (or similar) environment unless your customers have also purchased a license to CRYPTO COMPLETE or a special licensing arrangement has been arranged with LINOMA SOFTWARE.

TERM

This license is effective until terminated. You may terminate it at any time by destroying CRYPTO COMPLETE together with all copies and merged portions in any form. It will also terminate upon conditions set forth elsewhere in this Agreement, or if you fail to comply with any term or condition of this Agreement.

LIMITED WARRANTY

YOU HEREBY ACKNOWLEDGE AND AGREE THAT CRYPTO COMPLETE IS PROVIDED BY LINOMA SOFTWARE ON AN "AS IS" BASIS, AND YOUR ACCESS TO AND/OR USE OF CRYPTO COMPLETE IS AT YOUR SOLE RISK. LINOMA SOFTWARE EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THOSE OF MERCHANTABILITY, SATISFACTORY QUALITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. LINOMA SOFTWARE MAKES NO WARRANTY THAT CRYPTO COMPLETE WILL MEET YOUR REQUIREMENTS OR THAT YOUR USE OF CRYPTO COMPLETE WILL BE UNINTERRUPTED, TIMELY OR ERROR-FREE, NOR DOES LINOMA SOFTWARE MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF CRYPTO COMPLETE OR THAT ANY DEFECTS WILL BE CORRECTED. YOU UNDERSTAND AND AGREE THAT THE USE OF CRYPTO COMPLETE IS DONE AT YOUR SOLE RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR SYSTEM OR LOSS OF DATA. NO INFORMATION OR ADVICE, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM LINOMA SOFTWARE OR THROUGH CRYPTO COMPLETE SHALL CREATE ANY WARRANTY NOT EXPRESSLY MADE HEREIN. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, SO SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU.

IN NO EVENT WILL LINOMA SOFTWARE BE LIABLE TO YOU FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING BUT NOT LIMITED TO ANY LOST PROFITS, LOST SAVINGS, LOST DATA OR LOST BUSINESS OPPORTUNITIES ARISING OUT OF THE USE OR INABILITY TO USE CRYPTO COMPLETE EVEN IF LINOMA SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Circumstances may arise where, because of a default on LINOMA SOFTWARE's part or other liability, you are entitled to recover damages from LINOMA SOFTWARE. In each such instance, regardless of the basis on which you may be entitled to claim damages from LINOMA SOFTWARE, (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), LINOMA SOFTWARE is liable for no more than the amount you paid for CRYPTO COMPLETE.

This limited warranty gives you specific legal rights. Some states provide other rights, and some states do not allow excluding or limiting implied warranties or limiting liability for incidental or consequential damages. As a result, the above limitations and or exclusions may not apply to you. Furthermore, some jurisdictions have statutory consumer product provisions which may supersede these provisions of the Agreement.

GENERAL

If any provision of this Agreement shall be unlawful, void or for any reason unenforceable, then that provision shall be deemed severable from this Agreement and shall not affect the validity and enforceability of the remaining provisions of this Agreement. This Agreement will be governed by the laws of the State of Nebraska including the applicable provisions of the Uniform Electronic Transactions Act, as adopted in the State of Nebraska.

Purchasing a License

For *Crypto Complete* pricing information, please contact sales@linomasoftware.com or call our office at (402) 944-4242 or 1-800-949-4696 (in the US).

How to Order

You will need to provide the following information when placing an order for *Crypto Complete*:

- The IBM i Serial number(s) to be licensed and their corresponding Processor groups
- Your Name
- E-mail address
- Voice phone number
- Fax number
- Organization name
- Country
- Address
- Where you heard about the Toolbox

Use one of the following methods to place your order:

- **Fax:** Purchase orders can be faxed to (402) 944-4243.
- **Phone:** Call (402) 944-4242 or 1-800-949-4696 (in the US) and order using a credit card.
- **Mail:** Send the proper payment amount to Linoma Software, 1409 Silver St., Ashland NE 68003
- **Wire Transfer:** Bank wire transfers are also accepted. Call us for details.

Upon receipt of a valid payment, we will e-mail or fax you the permanent license key(s) for *Crypto Complete*.

Contacting Linoma Software

The Company

Founded in 1994, Linoma Software provides innovative technologies for protecting sensitive data and automating data movement. Linoma Software has a diverse install base of over 3,000 customers around the world including Fortune 500 companies, non-profit organizations and government entities.

Linoma's success has been built on being very responsive to our customer's requirements. So if you have suggestions on how we can improve our products to better serve your organization, please let us know.

How to Contact Linoma Software

Electronic

Sales	sales@linomasoftware.com
Support	support@linomasoftware.com
Website	www.linomasoftware.com

Phone Numbers

Toll-free:	1-800-949-4696
Outside USA:	(402) 944-4242
Fax:	(402) 944-4243

Address

Linoma Software
1409 Silver Street
Ashland, NE 68003 USA

Remove IFS Encryption from the system

Use the commands (in the order listed) below to remove Crypto Complete's IFS Encryption*:*

Step 1 – DCTIFSENCJ (Deactivate all files in the encrypted Directory(s)).
Run this for all Activated IFS IDs

Step 2 – ENDIFSENCJ (This will end the IFS Server Job)

Step 3 – RMVEXTPGMS(Remove the Crypto Exit Point Programs)

Step 4 – You must stop and restart every Job that will Access the IFS Files.
You can do one of two things

1. IPL the system
2. Or end any restart any Job that will be using the exit programs. The instructions below will stop and restart many of the servers. There may be others that are not listed.
   a. End Processes
      i. ENDTCPSVR *NETSVR
      ii. ENDTCPSVR SERVER(*FTP)
      iii. ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
      iv. ENDHOSTSVR *FILE
      v. ENDHOSTSVR *DATABASE
      vi. ENDSBS QSERVER
      vii. End any Batch Jobs that access the IFS Data
   b. Restart Processes
      i. STRSBS QSERVER
      ii. STRTCPSVR *NETSVR
      iii. ENDTCPSVR SERVER(*FTP)
      iv. ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
      v. STRHOSTSVR *FILE
      vi. STRHOSTSVR *DATABASE
      vii. Restart any Batch Jobs that access the IFS Data

Config File Quick Start

When using the new CRCONFIG file to set up the IFS encryption, you need to use the following steps to setup and run the IFS Encryption processes.

In all cases the CRCONFIG file must be in the CRYPTO library. When the file is not found or a setting is not found then the default settings are used.

The WRKCONFIG command allows you to change the settings in the CRCONFIG file. In the new version the WRKCONFIG command will be located on the “Product information” menu.

Below are the default settings in the file when installed.

```
Opt  Name                                                Value
     Default Settings
     EXTFILE_USECMTCTRL                                  YES
     IFS_ASPNAME                                         ______
     IASP Settings
     IFS_IASP_CRYPTO_OBJECTS_LIBRARY                     CRYPTO
     IFS_IASP_FILES_JOURNALLED_BY_THIRD_PARTY            NO
     IFS_IASP_JOURNAL_LIBRARY                            CRYPTO
     IFS_IASP_JOURNAL_NAME                               CRJNI001
     LOC1 Settings
     IFS_LOC1_CRYPTO_OBJECTS_LIBRARY                     CRYPTO
     IFS_LOC1_FILES_JOURNALLED_BY_THIRD_PARTY            NO
     IFS_LOC1_JOURNAL_LIBRARY                            CRYPTO
     IFS_LOC1_JOURNAL_NAME                               CRJNI001
     LOC2 Settings
     IFS_LOC2_CRYPTO_OBJECTS_LIBRARY                     CRYPTO
     IFS_LOC2_FILES_JOURNALLED_BY_THIRD_PARTY            NO
     IFS_LOC2_JOURNAL_LIBRARY                            CRYPTO
     IFS_LOC2_JOURNAL_NAME                               CRJNI001
     LOC3 Settings
     IFS_LOC3_CRYPTO_OBJECTS_LIBRARY                     CRYPTO
     IFS_LOC3_FILES_JOURNALLED_BY_THIRD_PARTY            NO
     IFS_LOC3_JOURNAL_LIBRARY                            CRYPTO
     IFS_LOC3_JOURNAL_NAME                               CRJNI001
     LOC4 Settings
     IFS_LOC4_CRYPTO_OBJECTS_LIBRARY                     CRYPTO
     IFS_LOC4_FILES_JOURNALLED_BY_THIRD_PARTY            NO
     IFS_LOC4_JOURNAL_LIBRARY                            CRYPTO
     IFS_LOC4_JOURNAL_NAME                               CRJNI001
     LOC5 Settings
     IFS_LOC5_CRYPTO_OBJECTS_LIBRARY                     CRYPTO
     IFS_LOC5_FILES_JOURNALLED_BY_THIRD_PARTY            NO
     IFS_LOC5_JOURNAL_LIBRARY                            CRYPTO
     IFS_LOC5_JOURNAL_NAME                               CRJNI001
```

Configuration Settings when in the IFS Encryption Registry the Journal Location (JRNLOC) field is set to *DEFAULT

This is used for all normal IFS Encryption. *ASP is used for IASP replication. *LOCx are used when a third party Journal is being used to journal a directory you want to encrypt.

1. When the Journal Location for a field is *DEFAULT then no records need to be added to the CRCONFIG file. Use the WRKCONFIG command to enter or change the objects.

The following objects will already exist in the CRYPTO library and must stay there.

1.	CRVL003	*VLDL	IFS Encryption Registry
2.	CRPFIFS	*PF	IFS Encryption Information
3.	CRPFIFSL1	*LF	
4.	CRPFIFSL2	*LF	
5.	CRPFIFSL3	*LF	
6.	CRPFIFSL4	*LF	
7.	CRPFIFS2	*PF	IFS Encryption Changes File
8.	CRJNI001	*JRN	Journal
9.	CRJRI001	*JRNRCV	Journal Receiver
10.	CRLSTSEQ	*DTAARA	Keeps track of the Last Receiver and Seq Number
11.	CRSRVRUN	*DTAARA	Used to let the server program know to End.

Configuration Settings when in the IFS Encryption Registry the Journal Location (JRNLOC) field is set to *IASP

*IASP is used for IASP replication is used on a system. The default objects will still exist in the CRYPTO library.

When the Journal Location for a field is *IASP then the following setup needs to be done.

1. Create or designate an IASP library to hold the Crypto objects created below that need to be copied from the CRYPTO library.

2. All of the objects below must exist in the IASP Library. These objects should only hold information about the IASP files.
    a. CRPFIFS
    b. CRPFIFSL1
    c. CRPFIFSL2
    d. CRPFIFSL3
    e. CRPFIFSL4
    f. Journal Receiver. Use the following command CRTJRNRCV JRNRCV(IASPLIB/CRJRI001)
    g. Journal. Use the following command CRTJRN JRN(IASPLIB/CRJNI001) JRNRCV(IASPLIB/CRJRI001)
    h. CRLSTSEQ
    i. CRSRVRUN

3. Create a DDM file in the CRYPTO library called CRPFIFSA over the CRPFIFS file in the CRASP library. For example if my IASP name is IASP1 and my library in the IASP I am using is CRASP then use the following command.
    a. CRTDDMF FILE(CRYPTO/CRPFIFSA) RMTFILE(CRASP/CRPFIFS) RMTLOCNAME(*RDB) RDB(IASP1)

4. The CRCONFIG file in library CRYPTO must have the following records added and set. Use the WRKCONFIG command to enter or change the records.
    a. IFS_IASP_CRYPTO_ OBJECTS_LIBRARY
        i. The value must be the library that holds the new objects created above. This must not be CRYPTO.
    b. IFS_IASP_FILES_JOURNALLED_BY_THIRD_PARTY → *NO
    c. IFS_IASP_JOURNAL_LIBRARY
        i. The value must be the library that holds the journal. This must not be CRYPTO.
    d. IFS_IASP_JOURNAL_NAME

5. The authorities for these objects should be the same as for the ones in the CRYPTO Library.

6. The CRPFIFS file must be empty.

7. The CRLSTSEQ Data Area holds the current Journal receiver name in the first 10 characters. This should be changed to the current Journal Receiver for the journal that is journaling the directory.

   a. 'CRJRI001 000000000000001'

8. The CRLSTSEQ Data Area holds the last sequence number read in the current Journal receiver in the last 15 characters. This should be changed to the last sequence number in the Current Journal Receiver for the journal that is journaling the directory.

9. The CRSRVRUN Data Area should be set to “N”.

10. Create an IFS Encryption Registry Entry in the (CRVL003) located in the CRYPTO library and set the JRNLOC value to *IASP.

11. Start the IFSENCJOBA by using the following command.
    a. STRIFSENCJ JRNLOC(*IASP)

12. Activate the Entry. This process will make sure that the IASP Library is available to the job. If the library is not then the SETASPGRP command will be ran. If the command fails then the Activate will fail.

IFS_IASP_CRYPTO_OBJECTS_LIBRARY	The IASP Library that holds the copied objects from the CRYPTO Library. 1. CRPFIFS 2. CRPFIFSL1 3. CRPFIFSL2 4. CRPFIFSL3 5. CRPFIFSL4 6. Journal object. If you are using the same naming convention as Crypto does then the name would be CRJNI001 7. Journal Receiver objects. If you are using the same naming convention as Crypto does then the name would be CRJRI001 8. CRLSTSEQ 9. CRSRVRUN
IFS_IASP_FILES_JOURNALLED_BY_THIRD_PARTY	Value should be NO when encrypting an IASP directory
IFS_IASP_JOURNAL_LIBRARY	The IASP Library that holds the Journal to be used.
IFS_IASP_JOURNAL_NAME	The Journal name .

Configuration Settings when in the IFS Encryption Registry the Journal Location (JRNLOC) field is set to *LOC1 through *LOC5

*LOCx is used when a directory is already being journaled by a third party journal.

When the Journal Location (JRNLOC) for a field is *LOC1, *LOC2, *LOC3, *LOC4 or *LOC5, then the following setup needs to be done.

1. Check that the directory and all files in the directory are being journaled by using the following:

2. WRKLNK '/DirectoryName'
   - a. Enter option 8 next to the directory and the files to make sure they are journaled. The Directory and the files must be journaled. The journal information will be on the 4th or 5th page. Take note of the journal Library and Name.

3. Once you know the Journal Library and Journal Name use the command WRKJRN to view the Journal Information.
   - a. Take option 8 to get the Attached receiver. Make note of the receiver name.
   - b. Press F17 from there to get the Last sequence number.

4. Create or designate a library to hold the Crypto objects created in the next step below. These objects can be copied from the CRYPTO library. Make sure the CRPFIFS file is empty in the new library.

5. All of the objects below must be copied to the new Library designated above.

a.	CRPFIFS	Physical File
b.	CRPFIFSL1	Logical File over CRPFIFS
c.	CRPFIFSL2	Logical File over CRPFIFS
d.	CRPFIFSL3	Logical File over CRPFIFS
e.	CRPFIFSL4	Logical File over CRPFIFS
f.	CRLSTSEQ	Data Area
g.	CRSRVRUN	Data Area

6. The authorities for these objects should be the same as for the ones in the CRYPTO Library.

7. The CRPFIFS file must be empty.

8. The CRLSTSEQ Data Area holds the current Journal receiver name in the first 10 characters and the last 15 characters holds the Last Sequence Number of the current Journal. For example. 'CRJRI010 000000000000235'
   - a. Change the first 10 characters to hold the current Journal receiver name found above.
   - b. Change the last 15 characters to hold Last Sequence Number of the current Journal found above. Be sure to include the leading zeros.

9. The CRSRVRUN Data Area should be set to "N".

10. The CRCONFIG file must have the following records added. Use the WRKCONFIG command to enter or change the objects.
    a. IFS_LOCx_CRYPTO_ OBJECTS_LIBRARY
        i. The value must be the library that holds the new objects created above. This must not be Crypto.
    b. IFS_LOCx_FILES_JOURNALLED_BY_THIRD_PARTY
    c. IFS_LOCx_JOURNAL_LIBRARY
        i. The value must be the library that holds the journal. This must not be Crypto.
    d. IFS_LOCx_JOURNAL_NAME

11. Create an IFS Encryption Registry Entry in the (CRVL003) located in the CRYPTO library and set the JRNLOC value to the appropriate value. Either *LOC1, *LOC2, *LOC3, *LOC4 or *LOC5.

12. Start the IFSENCJOBx (where x is 1 thru 5) by using the following command.
    a. STRIFSENCJ JRNLOC(*LOCx)

13. Activate the Entry in the IFS Registry.

IFS_LOCx_CRYPTO_OBJECTS_LIBRARY	The Library that holds the copied objects from the CRYPTO Library. 1. CRPFIFS 2. CRPFIFSL1 3. CRPFIFSL2 4. CRPFIFSL3 5. CRPFIFSL4 6. Journal object. 7. Journal Receiver object 8. CRLSTSEQ 9. CRSRVRUN
IFS_LOCx_FILES_JOURNALLED_BY_THIRD_PARTY	Value should be YES when using these options.
IFS_LOCx_JOURNAL_LIBRARY	The Library that holds the Journal to be used.
IFS_LOCx_JOURNAL_NAME	The Journal name .