Guía del Usuario IV

Crypto Complete
Encriptación automática directorios y archivos de la IFS

Esta traducción está basada en la versión original de Linoma Software:
"Crypto Complete version: 3.30 Publication date: August 22nd, 2013"

American Top Tools S.L. Tel. +34 933191612 Fax +34 933191755 att@att.es www.att.es

Nota ATT:

La traducción del manual original se ha realizado para facilitar su uso en 4 documentos:

GUIA DEL USUARIO_I_Crypto Complete_Herramienta_de_Encriptación.pdf

GUIA DEL USUARIO_II_Crypto Complete_Encriptación_de_Campos.pdf

GUIA DEL USUARIO_III_Crypto Complete__Backup e IFS encriptados.pdf

GUIA DEL USUARIO_IV_Crypto Complete_Encriptación Automática carpetas IFS.pdf

La primera guía es básica, común y de obligada lectura para la utilización tanto del Módulo de Encriptación de Campos como del Módulo de Encriptación de Backup (de bibliotecas, objetos y archivos de la IFS) como del módulo de Encriptación Automática de carpetas IFS.

Guía del Usuario IV - Encriptación Automática de IFS

1. Introducción

Crypto Complete es una completa herramienta para la protección de los datos sensibles y confidenciales en el System i de IBM (iSeries), a través de una tecnología de encriptación (cifrado) consistente, un sistema de gestión de claves integrado y controles de auditoría.

Crypto Complete se ha diseñado con un principal objetivo: Permitir a las empresas implantar los procesos de encriptación (cifrado), con el máximo grado de protección, de la manera más rápida y sencilla, gracias a pantallas y mandatos intuitivos y de fácil manejo.

Crypto Complete trata de minimizar los cambios en las aplicaciones para agilizar la implantación de un sistema de encriptación a un coste asumible y en el menor tiempo posible.

1.1 Encriptación IFS

Los directorios o carpetas de la IFS pueden ser controlados para que se produzca la encriptación automática de todo lo que se almacene en ellas.

El innovador Registro de Encriptación de las carpetas de la IFS (Sistema Integrado de Archivos) de Crypto Complete permite indicar que directorios encriptar al ser registrados en el Registro de Encriptación de Carpetas de la IFS.

- Cuando se “activan” las entradas de directorios de la IFS en el Registro se produce una encriptación masiva de los archivos y subdirectorios almacenados en ese momento en el directorio seleccionado.
- Desde ese momento, cualquier archivo añadido o modificado en ese directorio o subdirectorio, será automáticamente encriptado.
- La función de encriptación automática del Registro de Encriptación de IFS elimina la necesidad de realizar cambios en sus programas y aplicaciones para encriptar archivos.
- El usuario autorizado para la lectura de un archivo podrá verlo tras ser desencriptado sin cambios en sus programas.
- Si no estuviera autorizado a la lectura, la lectura daría un error con el siguiente mensaje “Object marked as a scan failure”.

1.2 Menú Principal

Los mandatos relacionados con el Crypto Complete son accesibles a través del menú principal y sus menús secundarios. Para acceder al menú principal ejecute el siguiente mandato.

```
GO CRYPTO/CRYPTO
```

Aparecerá la siguiente pantalla, desde la cual accederemos los mandatos relacionados estrictamente con el módulo de encriptación de carpetas de la IFS a través de la opción 7.

```
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 CRYPTO7)
  9. Field Analysis Menu                   (GO CRYPTO9)

 10. Product Information Menu              (GO CRYPTO10)
```

Pantalla del Menú Principal de Crypto Complete

Los mandatos pueden ejecutarse desde el menú introduciendo la opción correspondiente. También puede ejecutarse utilizando el nombre de mandato (en paréntesis) desde la línea de mandatos.

Tras pulsar la opción 7 de acceso al Menú de Encriptación de carpetas de la IFS aparecerá la siguiente pantalla:

```
CRYPTO12        IFS Encryption Menu         CRYPTO COMPLETE
                                            Copyright 2007-2013
                                            Linoma Software
Select one of the following:

  1. Work with IFS Encryption        (WRKIFSENC)
  2. Add IFS Encryption Entry        (ADDIFSENC)
  3. Change IFS Encryption Entry     (CHGIFSENC)
  4. Display IFS Encryption Entry    (DSPIFSENC)
  5. Remove IFS Encryption Entry     (RMVIFSENC)

 10. Activate IFS Encryption         (ACTIFSENC)
 11. Deactivate IFS Encryption       (DCTIFSENC)

 20. IFS Keys Menu                   (GO CRYPTO13)
 21. IFS Utility Menu                (GO CRYPTO14)
```

Pantalla del Menú de Encriptación de Carpetas de la IFS

Presenta tres apartados principales. Los mandatos del 1 al 5 permiten trabajar con el Registro de Encriptación de Claves. Los mandatos del 10 al 11 permiten activar y desactivar la encriptación de las carpetas registradas en el Registro. La opción 20 presenta el menú para asignar las claves DEK de encriptación y desencriptación. Finalmente, la opción 21 presenta el menú y los mandatos para realizar la configuración técnica de este módulo de Encriptación Automática de la IFS.

1.3 Inicio Rápido - Establecer Configuración y Claves

Antes de poder realizar la encriptación de carpetas de la IFS es necesario configurar la el Sistema de Gestión de Claves de Crypto Complete.

a) Configuración particular del módulo de Encriptación de Campos

Utilice las siguientes instrucciones en el orden indicado para configurar rápidamente la Encriptación Automática de la IFS.

Paso 1 – La biblioteca CRYPTO debe añadirse en la lista de bibliotecas del sistema

Nota ATT: Añadir la biblioteca CRYPTO con WRKSYSVAL QSYSLIBL

Paso 2 – Compruebe y modifique, si es necesario, los siguientes Valores del Sistema con WRKSYSVAL:

QSCANFS → *ROOTOPNUD

QSCANFSCTL → *NONE

Los directorios que cree deben tener el atributo "Create Object Scanning for the directory" (Exploración de creación de objetos) → *YES

Los objetos que cree dentro de los directorios deben tener el atributo "Object Scanning" (Exploración de objeto) → *YES

Nota ATT: Estos dos atributos se pueden ver haciendo WRKLNK y la opción 8="Visualizar Atributos" sobre el objeto o el fichero respectivamente.

Paso 3 – Ejecute el mandato ADDIFSEXTP para añadir los Exit Point Programs de Crypto).

Puede acceder a este mandato a través de la opción 3 del menú de Utilidades, al cual se accede directamente con GO CRYPTO 14 o bien, desde el menú de Encriptación de la IFS con la opción 21.

Este mandato añadirá los siguientes Exit Programs al sistema:

QIBM_QPWFS_FILE_SERV
QIBM_QP0L_SCAN_CLOSE
QIBM_QP0L_SCAN_OPEN

Paso 4 – Debe detener y reiniciar cualquier trabajo que accede a los archivos de la IFS.

Existen dos maneras de hacerlo.

1. Hacer una IPL del sistema.

2. Finalizar y reiniciar cualquier trabajo que vaya a utilizar los Exit Programs.

Las siguientes instrucciones le ayudarán a finalizar y reiniciar la mayoría de los servidores. Puede que haya otros que no estén contemplados aquí.

Finalizar procesos:

- ENDTCPSVR *NETSVR
- ENDTCPSVR SERVER(*FTP)
- ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
- ENDHOSTSVR *FILE
- ENDHOSTSVR *DATABASE
- ENDSBS QSERVER
- Finalizar cualquier trabajo Batch que accede a los datos de la IFS.

Reiniciar procesos:

- STRSBS QSERVER
- STRTCPSVR *NETSVR
- STRTCPSVR SERVER(*FTP)
- STRTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
- STRHOSTSVR *FILE
- STRHOSTSVR *DATABASE
- Reiniciar cualquier trabajo batch que accede a los datos de la IFS.

Paso 5 – Ejecute el mandato STRIFSENCJ. Someterá el trabajo de servidor IFS a batch.

Puede acceder a este mandato a través de la opción 1 del menú de Utilidades, al cual se accede directamente con GO CRYPTO 14 o bien, desde el menú de Encriptación de la IFS con la opción 21.

Nota: Este trabajo utiliza la Descripción del Trabajo CRYPTO incluida en la biblioteca CRYPTO. Realice los cambios que desee a esta Descripción del Trabajo de acuerdo con su sistema antes de ejecutar este mandato.

Los siguientes mandatos se encuentran en el menú principal de Crypto Complete y son los relativos a la creación de las claves de encriptación y desencriptación DEK y al almacén de claves que las contendrá. Ver la Guía I - Crypto Complete: Herramienta de Encriptación.

Paso 6 – Cree un almacén de claves con el mandato CRTKEYSTR. Crea un almacén de claves (Key Store) que contendrá las claves DEK (Data Encryption Keys) para la encriptación.

Paso 7 – Cree un almacén de claves con el mandato CRTKEYSTR. Crea un almacén de claves (Key Store) que contendrá las claves DEK (Data Encryption Keys) para la desencriptación.

Paso 8 – Cree una clave DEK de encriptación con el mandato CRTSYMKEY (Create a Data Encryption Key y especifique el Key Store creado en el paso 6 (Almacén de claves para la encriptación).

Paso 9 – Copie la clave DEK creada en el paso 8 con el mandato CPYSYMKEY y sálvela en el Key Store creado en el paso 7 (Almacén de claves para la desencriptación).

Paso 10 – Con el mandato WRKSYMKEY (Opción 10 del Menú de Encriptación de Claves Simétricas) especifique el almacén de la clave de **encriptación** (creado en paso 6) y la biblioteca en que se alojo, para ver la clave de **encriptación** DEK creada en el paso 8. Modifique con la opción 2=Change la clave DEK y cambie el atributo "Decryption allowed with key" a *NO.

Paso 11 – Con el mandato WRKSYMKEY (Opción 10 del Menú de Encriptación de Claves Simétricas) especifique el almacén de la clave de **desencriptación** (creado en paso 6) y la biblioteca en que se alojo, para ver la clave de **desencriptación** DEK creada en el paso 8. Modifique con la opción 2=Change la clave DEK y cambie el atributo "Encryption allowed with key" a *NO.

Paso 12 – Cree una lista de autorización para determinar quién está autorizado a Desencriptar.

Paso 13 – Establezca con el mandato WRKIFSENC una entrada en el Registro de Encriptación de carpetas de la IFS indicando el directorio que desea Encriptar. Más información en el apartado 2.1 de este manual.

Nota: Todo archivo que vaya a ser encriptado tiene que tener el atributo *CRTOBJSCAN en *YES

2. Registro de Encriptación de Carpetas IFS

El Registro de Encriptación de Crypto Complete permite especificar (registrar) que directorios requieren la encriptación.

Hay varias opciones de configuración que puede especificar para cada entrada de directorio añadida al registro. Una de ellas, es hacer que Crypto Complete encripte también todos los archivos que hay en los subdirectorios del directorio indicado en el registro. El Registro, también proporciona un directorio de destino donde los archivos encriptados deberían ser almacenados.

Desde el menú de Encriptación de la IFS **podrá crear nuevas entradas de directorios en el registro, modificarlas, visualizarlas, eliminarlas y trabajar con ellas**.

```
CRYPTO12        IFS Encryption Menu          CRYPTO COMPLETE
                                             Copyright 2007-2013
                                             Linoma Software
Select one of the following:

  1. Work with IFS Encryption         (WRKIFSENC)
  2. Add IFS Encryption Entry         (ADDIFSENC)
  3. Change IFS Encryption Entry      (CHGIFSENC)
  4. Display IFS Encryption Entry     (DSPIFSENC)
  5. Remove IFS Encryption Entry      (RMVIFSENC)

 10. Activate IFS Encryption          (ACTIFSENC)
 11. Deactivate IFS Encryption        (DCTIFSENC)

 20. IFS Keys Menu                    (GO CRYPTO13)
 21. IFS Utility Menu                 (GO CRYPTO14)
```

Pantalla del Menú de Encriptación de Carpetas de la IFS

Todas las opciones de la 1 a la 11, también son accesibles desde la pantalla del mandato WRKIFSENC que accede directamente al Registro de Encriptación de Claves.

```
28/11/13    Work with IFS Encryption Registry     RLR
12:50:48                                          CRRM401  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
     CREDIT_CARD        /creditcard               *INACTIVE



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

Pantalla del Menú de Encriptación de Carpetas de la IFS

2.1 Trabajar con Registro de encriptación de Carpetas

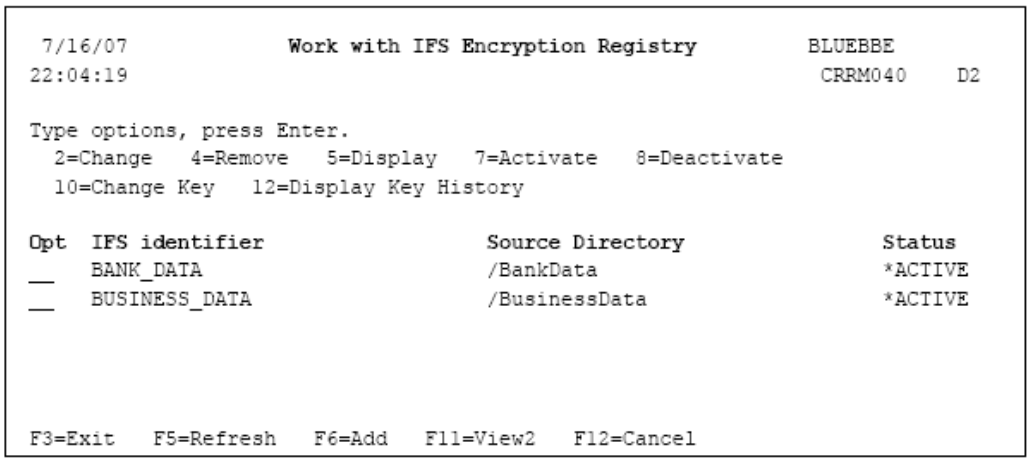
A continuación se presentan los mandatos relacionados con la gestión del Registro de Encriptación de Carpetas de la IFS.

a) Trabajar con Encriptación de IFS (WRKIFSENC)

El mandato **WRKIFSENC** permite a los usuarios autorizados en Crypto Complete a trabajar con las entradas del Registro de Encriptación de IFS. Desde la pantalla de este mandato puede añadir, modificar, activar, desactivar o eliminar las entradas de directorios de la IFS.

Siga los siguientes pasos para trabajar con entradas en el Registro de Encriptación de IFS.

1. Ejecute el mandato **CRYPTO/WRKIFSENC.**
2. Se mostrarán las entradas actuales en el Registro de Encriptación de IFS.



Pantalla del mandato WRKIFSENC

Para cada entrada de directorio IFS listada, la pantalla muestra el identificador de IFS asignado por el usuario, el directorio fuente y el estado. Pulse F11 para ver más información sobre cada entrada: destino, incluir o no subdirectorios y lista de autorización.

Estado:

Estos son los posibles códigos de estado que pueden verse para cada entrada.

Opción	Descripción
*ACTIVE	La entrada de IFS está activa para la encriptación automática.
*INACTIVE	La entrada de IFS no está active para la encriptación automática.
*PROCESS	El proceso de activación/desactivación de la entrada de la IFS está en marcha.
*ERROR	El proceso de activación/desactivación de la entrada de la IFS ha fallado. Contacte con su proveedor.

Opciones de pantalla

Para cada entrada de directorio IFS listada, puede utilizar alguna de las siguientes funciones:

Opción	Descripción
2	Permite cambiar la entrada de la IFS a través del mandato CHGIFSENC.
4	Permite confirmar la eliminación de la entrada IFS del registro a través del mandato RMVIFSENC.
5	Muestra los valores de la entrada IFS a través del mandato DSPIFSENC.
7	Permite activar la encriptación de la entrada de la IFS a través del mandato ACTIFSENC.
8	Permite desactivar la encriptación de la entrada IFS a través del mandato DCTIFSENC.
10	Permite cambiar las claves utilizadas para la encritpación o desencriptación a través del mandato CHGIFSKEY.
12	Permite visualizar el histórico de claves de encriptación y desencriptación de la IFS a través del mandato WRKIFSKEY.

Teclas de función

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

Función	Descripción
F3	Salir de la pantalla WRKIFSENC.
F5	Refrescar la lista de entradas IFS del Registro.
F6	Añadir una entrada IFS al Registro a través del mandato ADDIFSENC.
F11	Mostrar información adicional de la entrada IFS del Registro: directorio que almacena los valores encriptados, la opción de incluir o no los subdirectorios y la lista de autorización de desencriptación.

b) Añadir una entrada IFS (directorio) al Registro (ADDIFSENC)

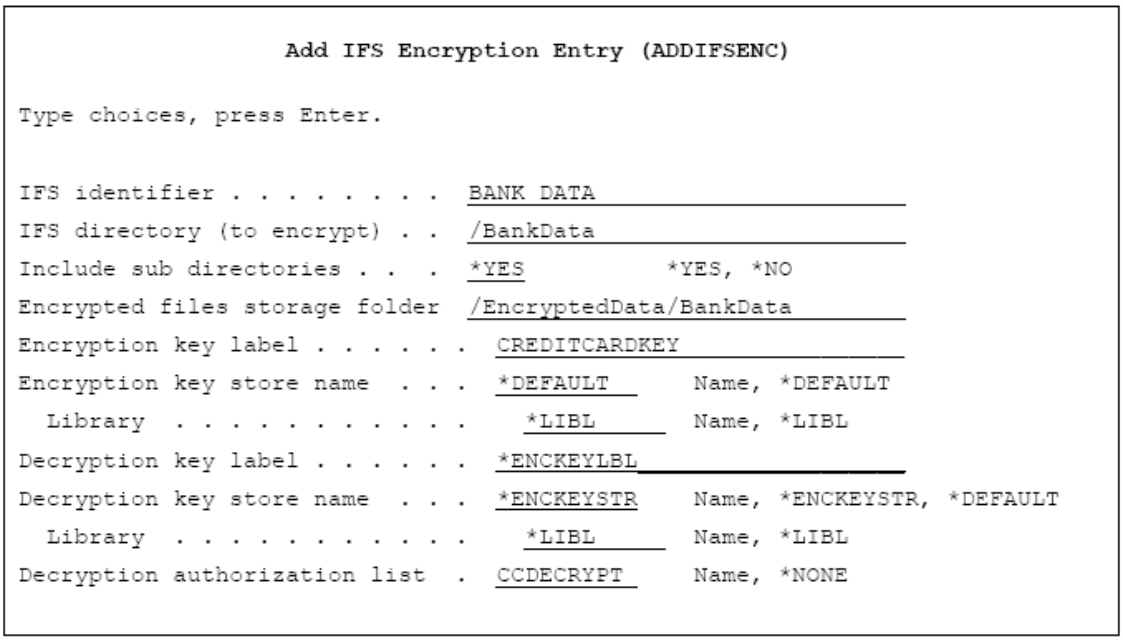
El mandato **ADDIFSENC** permite a los usuarios autorizados añadir una nueva entrada en el Registro de Encriptación de carpetas de la IFS. Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL003, lista de validación *VLDL, el cual contiene el Registro de Encriptación de IFS.

Realice los siguientes pasos para **añadir una nueva entrada en el Registro de Encriptación de carpetas de la IFS:**

1. Introduzca el mandato **CRYPTO/ADDIFSENC** y haga F4
2. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
3. Introduzca los valores de los parámetros y pulse Intro



Pantalla del mandato ADDIFSENC

Note: El mandato ADDIFSENC sólo añade la configuración de la entrada del directorio añadido en el registro. No se producirá ninguna acción sobre los archivos del directorio/s. El directorio de la IFS no se activará para ser encriptado hasta que se utilice el mandato ACTIFSENC (Activate IFS Encryption).

Descripción de los campos del mandato ADDIFSENC:

IFS identifier	Indica el identificador (nombre) único de la entrada de campo: - Máximo de 30 caracteres. - NO permite espacio o caracteres especiales. - SI permite el subrayado bajo (_). - NO es sensible a mayúsculas/minúsculas. Será almacenado en mayúsculas.
IFS directory (to encrypt)	Especifica la ruta del directorio IFS que contiene los archivos a encriptar.
Include subdirectories	Indica si desea incluir o no los subdirectorios del directorio fuente.

Encrypted files storage folder	Indica la ruta del directorio IFS que almacenará las versiones encriptadas de los archivos. Si no existe se creará. Por defecto, creará “Cryptodisk”.
Encryption key label	Indica la etiqueta de la clave DEK que se utilizará inicialmente para encriptar los archivos de la IFS.
Encryption key store name **Library**	Indica el nombre y biblioteca del Almacén de Claves que contiene la clave de encriptación DEK indicada en el campo anterior. Indique *DEFAULT para utilizar el nombre del Almacén de Claves especificado en la Política de Claves del menú principal de Crypto Complete.
Decryption key label	Indica la etiqueta de la clave DEK que se utilizará inicialmente para desencriptar los archivos de la IFS. Indique *ENCKEYLBL para utilizar la misma etiqueta de clave DEK que se introdujo en el campo “Encryption key label.” ATENCIÓN: Si especifica una Etiqueta de la Clave DEK distinta a la Etiqueta especificada para la encriptación, entonces esa clave de desencriptación debería contener el mismo valor de clave que la clave de encriptación. (Ver Nota ATT).
Nota ATT: Para ello, realice una copia de la clave DEK utilizada para encriptar con el mandato CPYSYMKEY asignándole el mismo almacén de claves (cambiar nombre Etiqueta de la Clave DEK) u otro almacén de claves (Podría mantener mismo nombre de Etiqueta de la Clave DEK). De esta manera, el valor de la clave que se usa para encriptar y desencriptar es el mismo.	
Decryption key store name **Library**	Indica el nombre y biblioteca del Almacén de Claves que contiene la Etiqueta de la Clave DEK de desencriptación. Indique *DEFAULT para utilizar el nombre del Almacén de Claves especificado en la política de claves. Indique *ENCKEYSTR para utilizar el mismo valor que se introdujo como Almacén de Claves de encriptación.
Decryption authorization list	Indica la Lista de Autorizaciones del i5/OS que se utilizará por las APIs de desencriptación de la IFS para comprobar los permisos del usuario para poder desencriptar los archivos de la IFS. Especifique *NONE si no quiere utilizar una Lista de autorización. Ver la nota a continuación.

Note: Puede crear una lista de autorización con el mandato CRTAUTL. El perfil de usuario o perfil de grupo de usuarios que necesite acceder a los datos desencriptados debe tener al menos autorización *USE a la Lista de Autorizaciones. Además requieren tener autorización *USE sobre el Almacén de Claves que contiene la clave de desencriptación.

c) Cambiar una entrada IFS en el Registro (CHGIFSENC)

El mandato **CHGIFSENC** permite a los usuarios autorizados modificar la configuración de cualquier entrada del Registro de Encriptación de carpetas de la IFS en estado *INACTIVE.

Los siguientes usuarios pueden emplear este mandato:

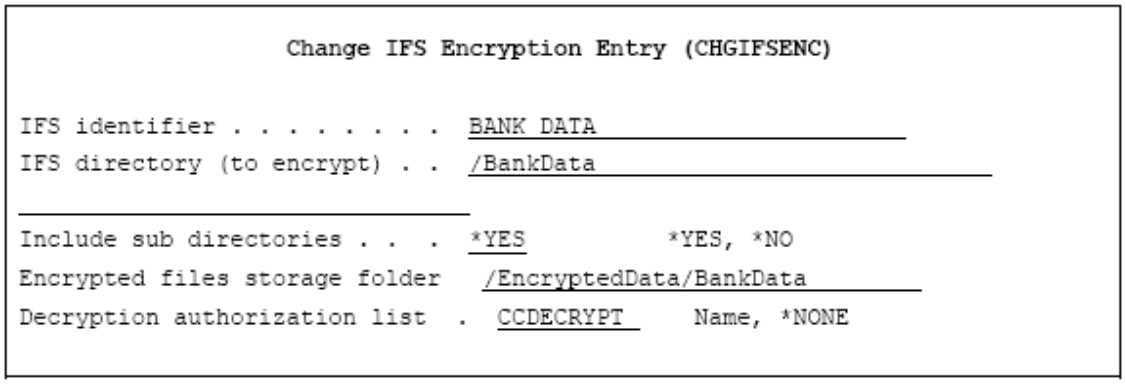
- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL003, lista de validación *VLDL, el cual contiene el Registro de Encriptación de IFS.

Realice los siguientes pasos para **modificar una entrada del Registro de Encriptación de carpetas de la IFS:**

1. Introduzca el mandato **CRYPTO/ CHGIFSENC** y haga F4
2. Introduzca el identificador de entrada IFS a modificar y pulse Intro.
3. Se mostrarán los valores de configuración actuales.
4. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
5. Modifique los valores de los parámetros y pulse Intro

Para más información sobre los parámetros ver el mandato ADDIFSENC.



Pantalla del mandato CHGIFSENC - Modificar una entrada del registro

Note: El mandato CHGIFSENC sólo modifica la configuración de la entrada del directorio modificado en el registro. No se producirá ninguna acción sobre los archivos del directorio/s. El directorio de la IFS no se activará para ser encriptado hasta que se utilice el mandato ACTIFSENC (Activate IFS Encryption).

d) Visualizar una entrada en el Registro (DSPIFSENC)

El mandato **DSPIFSENC** permite a los usuarios autorizados visualizar la configuración de cualquier entrada del Registro de Encriptación de carpetas de la IFS.

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL003, lista de validación *VLDL, el cual contiene el Registro de Encriptación de IFS.

Realice los siguientes pasos para **visualizar una entrada del Registro de Encriptación de carpetas de la IFS:**

1. Introduzca el mandato **CRYPTO/ DSPIFSENC** y haga F4
2. Introduzca el identificador de entrada IFS a visualizar y pulse Intro.
3. Se mostrarán los valores de configuración actuales junto con el timestamp y usuario que realizaron la última adición o modificación.
4. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line

Para más información sobre los parámetros ver el mandato ADDIFSENC.

```
                  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
```

Pantalla del mandato DSPIFSENC - Visualizar entrada del Registro.

e) Eliminar una entrada IFS del Registro (RMVIFSENC)

El mandato **RMVIFSENC** permite a los usuarios autorizados eliminar cualquier entrada del Registro de Encriptación de carpetas de la IFS.

Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL003, lista de validación *VLDL, el cual contiene el Registro de Encriptación de IFS.

Realice los siguientes pasos para **eliminar una entrada del Registro de Encriptación de carpetas de la IFS:**

1. Introduzca el mandato **CRYPTO/ RMVIFSENC** y haga F4
2. Introduzca el identificador de entrada IFS a eliminar y pulse Intro.

```
                  Remove IFS Encryption Entry (RMVIFSENC)

Type choices, press Enter.

IFS identifier . . . . . . . .  BANK_DATA
```

Pantalla del mandato RMVIFSENC - Eliminar una entrada del Registro

Note: El mandato RMVIFSENC sólo elimina la entrada del directorio en el registro. No se producirá ninguna acción sobre los archivos del directorio/s.

f) Activar la encriptación de un directorio de la IFS (ACTIFSENC)

El mandato **ACTIFSENC** permite a los usuarios autorizados activar cualquier entrada del Registro de Encriptación de carpetas de la IFS. Se producirá una encriptación masiva de los archivos actuales en el directorio/s a encriptar. Solo debe ejecutar este mandato cuando ninguna aplicación este utilizando los archivos de la IFS.

Este mandato solo puede utilizarse si el estado de las entradas del registro a activar es *INACTIVE. Se recomienda realizar este mandato en modo batch.

Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL003, lista de validación *VLDL, el cual contiene el Registro de Encriptación de IFS.

Este mandato requiere que el usuario tenga autorización *CHANGE sobre los ficheros CRPRIFS, CRPFIFSL1, CRPFIFSL2, CRPFIFSL3, CRPFIFSL4, CRPFIFS2 y CRPFIFSLOG que serán actualizados durante el proceso.

INSTRUCCIONES ESPECIALES:

Antes de utilizar el mandato ACTIFSENC para encriptar los datos de producción, realice lo siguientes pasos:

1. Asegúrese de tener autorización *ALL al directorio que contiene los archivos a encriptar y a los directorios que almacenan los archivos encriptados.
2. Debería haber probado en un ENTORNO DE PRUEBAS, el mandato ACTIFSENC, y probado el funcionamiento de sus aplicaciones profundamente con los archivos encriptados.
3. Ninguna aplicación o usuario debería estar utilizando en el momento de realizar la encriptación masiva los directorios y archivos que se van a encriptar.
4. El mandato ACTIFSENC realizará una encriptación masiva de los archivos actuales en los directorios IFS. Debería contar con un espacio de tiempo de inactividad suficiente de sus aplicaciones para ejecutar el mandato ACTIFSENC. Los tiempos de ejecución varían según la velocidad del procesador de su sistema, el número de registros en su archivo de base de datos, y otra actividad del sistema. Para poder estimar el tiempo de ejecución del mandato ACTIFSENC, debería ejecutar el mandato ACTIFSENC sobre algunos archivos de prueba.
5. Compruebe la configuración de las entradas del registro IFS con el mandato DSPIFSENC. Especialmente compruebe el nombre del directorio fuente, el directorio de destino y la opción de incluir o no los subdirectorios.

Recomendaciones sobre el mandato ACTIFSENC

- Ejecute el mandato en batch con el mandato SBMJOB
- Especifique *YES en el parámetro "Save Directories" para hacer una copia del directorio a encriptar y sus archivos en un Save File, antes de la activación del proceso. Está opción es importante en caso de emergencia.
- Asegúrese de disponer del espacio suficiente para alojar esas copias.

Realice los siguientes pasos para **activar una entrada en el Registro de Encriptación de carpetas de la IFS:**

1. Introduzca el mandato **CRYPTO/ ACTIFSENC** y haga F4
2. Introduzca el identificador de entrada IFS a activar y pulse Intro.

```
                    Activate IFS Encryption (ACTIFSENC)

Type choices, press Enter.

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

Pantalla del mandato ACTIFSENC para activar la encriptación

Paso a paso del proceso ejecutado por el mandato ACTIFSENC

1. Opcional: Crea un backup de la estructura del directorio de origen y sus archivos en un archivo de salvado llamado BACKUPxxxxx, donde xxxxx es un número secuencial de 1 a 99999. Este archivo se guarda en la biblioteca CRYPTO.
2. Realiza una encriptación masiva de los archivos del IFS en el directorio de origen seleccionado y opcionalmente de los subdirectorios.
3. Se inicia un journal sobre el directorio y si se hubiera incluido a los subdirectorios con la opción *YES en "Include Subdirectories" también lo hará sobre estos.
4. El estado de la entrada de en el Registro de IFS se cambiará a *ACTIVE.

Notas ACTIFSENC:

Una vez se haya completado el mandato ACTIFSENC: Una vez haya confirmado que sus aplicaciones están funcionando correctamente con los archivos encriptados, puede eliminar el archivo de salvado credo en el paso 1, el cual contiene el backup de la estructura del directorio de origen y sus archivos.

g) Desactivar la encriptación de un directorio de la IFS (DCTIFSENC)

El mandato **DCTIFSENC** permite a los usuarios autorizados desactivar cualquier entrada del Registro de Encriptación de carpetas de la IFS.

Este mandato solo puede utilizarse si el estado de las entradas del registro a activar es *ACTIVE. Se recomienda realizar este mandato en modo batch.

Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL003, lista de validación *VLDL, el cual contiene el Registro de Encriptación de IFS.

Este mandato requiere que el usuario tenga autorización *CHANGE sobre los ficheros CRPRIFS, CRPFIFSL1, CRPFIFSL2, CRPFIFSL3, CRPFIFSL4, CRPFIFS2 y CRPFIFSLOG que serán actualizados durante el proceso.

Instrucciones Especiales:

Antes de utilizar el mandato DCTIFSENC para encriptar los datos de producción, realice lo siguientes pasos:

1. Asegúrese de tener autorización *ALL al directorio que contiene los archivos a desencriptar y a los directorios que almacenan los archivos encriptados.

2. Asegúrese de tener como mínimo autorización *USE sobre el Almacén de Claves que contiene las Claves de Encriptación (DEKs) que se utilizarán para desencriptar los datos. Puede utilizar el mandato WRKFLDKEY para saber que almacenes de claves y claves DEK se están utilizando para desencriptar los datos.
   Si usted es el propietario de una de las claves que creó, entonces debe establecer en *YES el parámetro “DEK Decrypt usage by owner” (se puede ver con DSPKEYPCY), para que pueda utilizarla.

3. Asegúrese de tener al menos autorización *USE a la lista de autorizaciones utilizada para la desencriptación de archivos.

4. Debería haber probado en un ENTORNO DE PRUEBAS, el mandato DCTIFSENC, y probado el funcionamiento de sus aplicaciones profundamente con los archivos encriptados.

5. Ninguna aplicación o usuario debería estar utilizando en el momento de realizar la encriptación masiva los directorios y archivos que se van a encriptar.

6. El mandato DCTIFSENC realizará una desencriptación masiva de los archivos actuales en los directorios IFS. Debería contar con un espacio de tiempo de inactividad suficiente de sus aplicaciones para ejecutar el mandato DCTIFSENC. Los tiempos de ejecución varían según la velocidad del procesador de su sistema, el número de registros en su archivo de base de datos, y otra actividad del sistema. Para poder estimar el tiempo de ejecución del mandato ACTIFSENC, debería ejecutar el mandato DCTIFSENC sobre algunos archivos de prueba.

Recomendaciones sobre el mandato DCTIFSENC

- Ejecute el mandato en batch con el mandato SBMJOB
- Especifique *YES en el parámetro "Save Directories" para hacer copia del directorio de origen y el directorio encriptado y los archivos en un Save File, antes de la activación del proceso. Está opción es importante en caso de emergencia.
- Asegúrese de disponer del espacio suficiente para alojar esas copias.

Realice los siguientes pasos para **activar una entrada en el Registro de Encriptación de carpetas de la IFS:**

1. Introduzca el mandato **CRYPTO/ DCTIFSENC** y haga F4
2. Introduzca el identificador de entrada IFS a desactivar y pulse Intro.

```
                  Deactivate IFS Encryption (DCTIFSENC)

Type choices, press Enter.

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

Pantalla del mandato DCTIFSENC para desactivar una entrada del Registro

Paso a paso del proceso ejecutado por el mandato DCTIFSENC

1. Opcional: Crea un backup del directorio IFS y subdirectorios si el parámetro INCSUBDIR es *YES (contiene los archivos fuente) en un archivo de salvado llamado BACKUPxxxxx, donde xxxxx es un número secuencial de 1 a 99999.
2. Opcional: Crea un backup del directorio IFS y subdirectorios si el parámetro INCSUBDIR es *YES (contiene los archivos encriptados) en un archivo de salvado llamado BACKUPxxxxx, donde xxxxx es un número secuencial de 1 a 99999.

3. Se finaliza el journal sobre los directorios.
4. Realiza una desencriptación masiva de los archivos de los directorios IFS.
5. El estado de la entrada en el registro IFS se cambiará a *INACTIVE.

Notas DCTIFSENC:

Una vez se haya completado el mandato DCTIFSENC: Una vez haya confirmado que sus aplicaciones están funcionando correctamente con los archivos desencriptados, puede eliminar los archivos de salvado creados en el paso 1 y 2, los cuales contienen el backup de la estructura del directorio de origen y sus archivos.

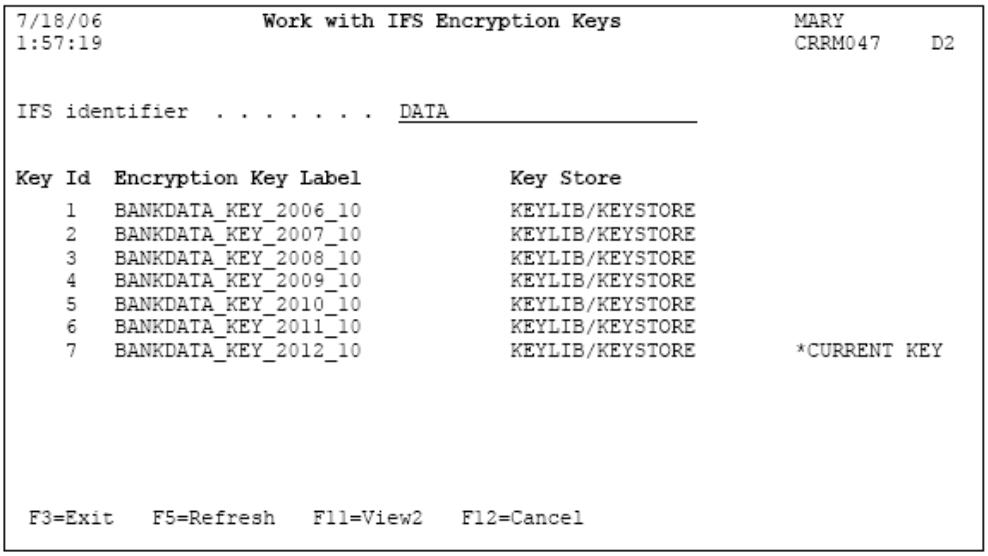
2.2 Trabajar con claves de encriptación

a) Trabajar con claves de encriptación de IFS (WRKIFSKEY)

El mandato **WRKIFSKEY** permite a los usuarios autorizados ver la clave actual, así como el histórico de claves DEK utilizadas para encriptar y desencriptar datos para una entrada del Registro de Encriptación de carpetas de la IFS.

Realice los siguientes pasos para **ver las claves para una entrada en el Registro de Encriptación de carpetas de la IFS:**

1. Introduzca el mandato **CRYPTO/ WRKIFSKEY** y haga F4
2. Introduzca el identificador de entrada IFS y pulse Intro.
3. Se mostrarán las claves DEK para la entrada IFS seleccionada.



Pantalla WRKIFSKEY Command with Sample Values

La clave mostrada con el comentario *CURRENT KEY es el id de Clave que se está utilizando actualmente para encriptar archivos de la IFS. El archivo será desencriptado utilizando la Etiqueta de Clave DEK y Almacén de Claves que se salvan junto el archivo encriptado.

Teclas de función

Función	Descripción
F3	Salir de la pantalla WRKIFSKEY.
F5	Refrescar la lista de claves IFS del Registro.
F11	Mostrar información sobre la Etiqueta de Clave DEK y el Almacén de Claves. También muestra el usuario y timestamp de la última modificación de la clave.

b) Cambiar Clave de Encriptación IFS (CHGIFSKEY)

El mandato **CHGIFSKEY** permite a los usuarios autorizados cambiar (rotar) las claves utilizadas para encriptar y desencriptar una entrada del Registro de Encriptación de carpetas de la IFS. Se pueden rotar hasta 99.999 claves para una misma entrada de IFS.

Este mandato puede utilizarse cuando las entradas del Registro de Encriptación de carpetas de la IFS sea tanto *INACTIVE como *ACTIVE. Todos los archivos encriptados utilizarán la clave original (valor de clave) que fue utilizada para su encriptación en el momento de la desencriptación.

Los siguientes usuarios pueden emplear este mandato:

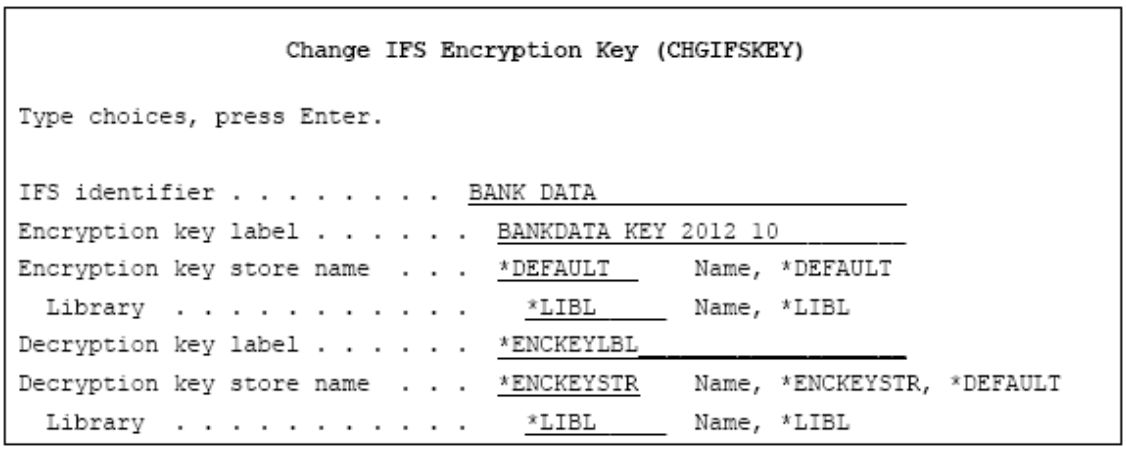
- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL003, lista de validación *VLDL, el cual contiene el Registro de Encriptación de IFS.

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el fichero CRPFIFS2 que será actualizado durante el proceso.

Realice los siguientes pasos para **cambiar las claves para una entrada en el Registro de Encriptación de carpetas de la IFS:**

1. Introduzca el mandato **CRYPTO/ CHGIFSKEY** y haga F4
2. Pulse F1 sobre cualquier parámetro para obtener ayuda on-line
3. Modifique los valores de los parámetros y pulse Intro



Pantalla del mandato CHGIFSKEY para cambiar las claves en una entrada ya definida

Descripción de los campos del mandato CHGIFSKEY:

IFS identifier	Indica el identificador (nombre) único de la entrada de campo: - Máximo de 30 caracteres. - NO permite espacio o caracteres especiales. - SI permite el subrayado bajo (_). - NO es sensible a mayúsculas/minúsculas. Será almacenado en mayúsculas.
Encryption key label	Indica la etiqueta de la clave DEK que se utilizará inicialmente para encriptar los archivos de la IFS.
Encryption key store name **Library**	Indica el nombre y biblioteca del Almacén de Claves que contiene la clave de encriptación DEK indicada en el campo anterior. Indique *DEFAULT para utilizar el nombre del Almacén de Claves especificado en la Política de Claves del menú principal de Crypto Complete.
Decryption key label	Indica la etiqueta de la clave DEK que se utilizará inicialmente para desencriptar los archivos de la IFS. Indique *ENCKEYLBL para utilizar la misma etiqueta de clave DEK que se introdujo en el campo "Encryption key label." ATENCIÓN: Si especifica una Etiqueta de la Clave DEK distinta a la Etiqueta especificada para la encriptación, entonces esa clave de desencriptación debería contener el mismo valor de clave que la clave de encriptación. (Ver Nota ATT).
Nota ATT: Para ello, realice una copia de la clave DEK utilizada para encriptar con el mandato CPYSYMKEY asignándole el mismo almacén de claves (cambiar nombre Etiqueta de la Clave DEK) u otro almacén de claves (Podría mantener mismo nombre de Etiqueta de la Clave DEK). De esta manera, el valor de la clave que se usa para encriptar y desencriptar es el mismo.	
Decryption key store name **Library**	Indica el nombre y biblioteca del Almacén de Claves que contiene la Etiqueta de la Clave DEK de desencriptación. Indique *DEFAULT para utilizar el nombre del Almacén de Claves especificado en la política de claves. Indique *ENCKEYSTR para utilizar el mismo valor que se introdujo como Almacén de Claves de encriptación.

La Etiqueta de Clave DEK de Desencriptación (Decrypiton Key Label), el almacén de claves (Key Store Name) y su biblioteca se guardan en el archivo encriptado y se utilizarán para desencriptar el archivo.

Cuando se modifica las Etiquetas de Clave con el mandato CHGIFSKEY, la nueva información de la clave se utilizará en los archivos que se encripten a partir de entonces. Ahora bien, la información de la clave permanece igual para los archivos de IFS ya encriptados, lo que permite a Crypto Complete desencriptar esos valores utilizando las etiquetas de claves anteriores. Está técnica permite la rotación de claves sin tener que reencriptar inmediatamente todos los archivos existentes en la IFS.

2.3 Menú de Utilidades

a) Arrancar el trabajo del servidor IFS (STRIFSENCJ)

El mandato **STRIFSENCJ** somete el trabajo de servidor a batch. Este trabajo se encarga de monitorear los el registro de journals producidos cuando se acceda a un archivo y ejecutar procesos cuando se ha accedido a un archivo.

Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

Este mandato utiliza la descripción de trabajo “CRYPTO Job Description” tal y como se envía con la biblioteca CRYPTO Library cuando se somete el trabajo de servidor (IFSENCJOB) a Batch. Puede modificar esta Descripción de Trabajo para ejecutar el trabajo IFSENCJOB donde y como usted prefiera.

```
                  Start IFS Encryption Job (STRIFSENCJ)

Type choices, press Enter.

Server user profile . . . . . *CURRENT _____________   Name, *CURRENT
```

Screen Example: STRIFSENCJ Command

El Perfil de Usuario del Servidor debe tener las siguientes autorizaciones:

• ALL sobre el directorio y archivos y subdirectorios a encriptar.

• ALL sobre el directorio que contiene los directorios y archivos encriptados.

• CHANGE sobre los archivos CRPFIFS, CRPFIFSL1, CRPFIFSL2, CRPFIFSL3, CRPFIFSL4, CRPFIFS2, CRPFIFSLOG.

• CHANGE sobre las aéreas de datos CRDEBUG, CRLSTSEQ y CRSRVRUN.

• USE sobre el journal CRJNI001 y TODOS los receptores de journal.

• USE sobre los programas CRCL414 y CRRP040 en la biblioteca CRYPTO.

b) Finalizar el trabajo de servidor IFS (ENDIFSENCJ)

El mandato **ENDIFSENCJ** envía un mensaje para finalizar el trabajo de servidor (IFSENCJOB).

Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

c) Añadir IFS Exit Point Programs (ADDIFSEXTP)

El mandato **ADDIFSEXTP** añadirá los siguientes exit programs al Registro del sistema:

QIBM_QPWFS_FILE_SERV
QIBM_QP0L_SCAN_CLOSE
QIBM_QP0L_SCAN_OPEN

Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

Nota: El mandato ADDIFSEXTP añadirá los exit programs al Registro del sistema (ver con WRKREGINF) si bien cualquier trabajo que estuviera activo en ese momento tendrá que ser reiniciado.

INSTRUCCIONES IMORTANTES:

El mandato (ADDIFSEXTP) sólo registra los exit programs en el sistema. Cualquier trabajo que necesite usar estos exit programs tendrá que ser reiniciado.

Debe detener y reiniciar cualquier trabajo que accede a los archivos de la IFS.

Existen dos maneras de hacerlo.

1. Hacer una IPL del sistema.

2. Finalizar y reiniciar cualquier trabajo que vaya a utilizar los Exit Programs.

Las siguientes instrucciones le ayudarán a finalizar y reiniciar la mayoría de los servidores. Puede que haya otros que no estén listados aquí.

Finalizar procesos:

- ENDTCPSVR *NETSVR
- ENDTCPSVR SERVER(*FTP)
- ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
- ENDHOSTSVR *FILE
- ENDHOSTSVR *DATABASE
- ENDSBS QSERVER
- Finalizar cualquier trabajo Batch que accede a los datos de la IFS.

Reiniciar procesos:

- STRSBS QSERVER
- STRTCPSVR *NETSVR
- STRTCPSVR SERVER(*FTP)
- STRTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
- STRHOSTSVR *FILE
- STRHOSTSVR *DATABASE
- Reiniciar cualquier trabajo batch que accede a los datos de la IFS.

El Perfil de Usuario debe tener las siguientes autorizaciones:

- *USE sobre el exit program CRRP041 de la bibliotecaCRYPTO Library.
- *EXECUTE sobre la biblioteca CRYPTO.
- *ALL sobre el directorio y archivos y subdirectorios a encriptar.
- *ALL sobre el directorio que contiene los directorios y archivos encriptados.
- *CHANGE sobre los archivos CRPFIFS, CRPFIFSL1, CRPFIFSL2, CRPFIFSL3, CRPFIFSL4, CRPFIFS2, CRPFIFSLOG.

- *CHANGE sobre las aéreas de datos CRDEBUG, CRLSTSEQ y CRSRVRUN.
- *USE sobre el journal CRJNI001 y TODOS los receptores de journal.

Importante: Si el perfil de usuario no es válido o accesible en el momento que se llama al exit program la acción sobre el archivo de la IFS será ignorada, lo que hará que el archivo no se encripte/desencripte en el momento deseado.

d) Eliminar IFS Exit Point Programs (RMVIFSEXTP)

El mandato **RMVIFSEXTP** eliminará los exit programs añadidos en el sistema para el funcionamiento de este modulo de encriptación de IFS.

QIBM_QPWFS_FILE_SERV
QIBM_QP0L_SCAN_CLOSE
QIBM_QP0L_SCAN_OPEN

Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

INSTRUCCIONES IMORTANTES:

El mandato RMVIFSEXTP sólo elimina los exit programs del Registro del sistema. Cualquier trabajo que necesite usar estos exit programs tendrá que ser reiniciado.

Existen dos maneras de hacerlo.

1. Hacer una IPL del sistema.

2. Finalizar y reiniciar cualquier trabajo que vaya a utilizar los Exit Programs.

Las siguientes instrucciones le ayudarán a finalizar y reiniciar la mayoría de los servidores. Puede que haya otros que no estén listados aquí.

Finalizar procesos:

- ENDTCPSVR *NETSVR
- ENDTCPSVR SERVER(*FTP)
- ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
- ENDHOSTSVR *FILE

- ENDHOSTSVR *DATABASE
- ENDSBS QSERVER
- Finalizar cualquier trabajo Batch que accede a los datos de la IFS.

Reiniciar procesos:

- STRSBS QSERVER
- STRTCPSVR *NETSVR
- STRTCPSVR SERVER(*FTP)
- STRTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
- STRHOSTSVR *FILE
- STRHOSTSVR *DATABASE
- Reiniciar cualquier trabajo batch que accede a los datos de la IFS.

Nota: El mandato RMVIFSEXTP eliminará los exit programs del Registro del sistema (ver con WRKREGINF) si bien cualquier trabajo que estuviera activo en ese momento tendrá que ser reiniciado.

e) Visualizar IFS Debug Mode (DSPIFSDBG)

El mandato **DSPIFSDBG** permite a los usuarios ver el modo Debug.

El usuario tiene que tener autorización *USE al área de datos CRDEBUG.

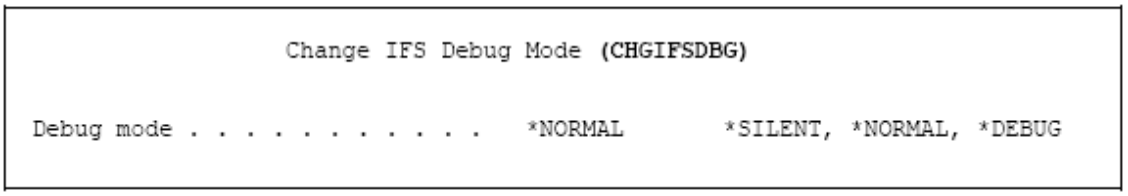
f) Cambiar IFS Debug Mode (CHGIFSDBG)

El mandato **CHGIFSDBG** permite a los usuarios cambiar el modo Debug.

Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

Requiere autorización *CHANGE al área de datos CRDEBUG y al archivo CRPFIFS2.



Pantalla del mandato CHGIFSDBG

f) Limpiar el log - IFS Debug Log (CLRIFSDBG)

El mandato **CLRIFSLOG** limpiará los registros del modo debug del archivo CRPFIFSLOG.

Los siguientes usuarios pueden emplear este mandato:

- Perfil de usuario QSECOFR (si no está excluido en Key Officer Settings)
- Usuarios con autorización *SECADM (si no está excluido en Key Officer Settings)
- Un oficial de claves cuya configuración de autorizaciones “Maintain IFS Enc.Registry” (Mantener Registro de Encriptación de IFS) está establecida en *YES

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el objeto CRVL003, lista de validación *VLDL, el cual contiene el Registro de Encriptación de IFS.

Este mandato requiere que el usuario tenga autorización *CHANGE sobre el fichero CRPFIFSLOG.

3. Lista de Autorizaciones del Registro de IFS

Dentro de sus aplicaciones quizá quiera controlar que archivos de los directorios controlados por el Registro de Encriptación de directorios IFS están disponibles y accesibles para cada usuario en función de sus autorizaciones.

Puede controlar esta seguridad a nivel de aplicación a través de las Listas de Autorización del sistema i5/OS y el Registro de Encriptación de carpetas de la IFS de Crypto Complete.

A continuación, se muestra un ejemplo de los pasos necesarios para añadir una Lista de Autorización y luego asociarla a una entrada de IFS en el Registro de Encriptación de carpetas de la IFS.

1. Cree una Lista de Autorización del sistema para controlar quién puede ver los archivos de la IFS DESENCRIPTADOS.

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

2. En la lista de autorizaciones CCFULL, confiera autorización *USE solo a aquellos usuarios o grupos de usuarios que deben tener acceso al valor desencriptado.

EDTAUTL AUTL(CCFULL)

3. Pulse F6 para añadir nuevos usuarios a la lista.

4. Auditoría - 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	

5. Procesos de Encriptación de la IFS y Notas

5.1 Procesos de Encriptación.

Activación de una entrada del Registro de Encriptación

Todos los archivos en el directorio pasarán estos procesos:

1. Si SAVDTA está en *YES se realiza un backup del directorio a encriptar y opcionalmente de los subdirectorios.
2. Se arranca el Journaling sobre el directorio y archivos.
3. Si el archivo No tiene “cero bytes”:
    i. El archivo se encripta y almacena en el directorio de destino indicado.
    ii. El archivo original se vacía y establece en “cero bytes”.
    iii. Se añade un registro en el archivo CRPFIFS

Nota: Se añade un registro en el archivo CRPFIFS por cada directorio encriptado.

Desactivación de una entrada del Registro de Encriptación

Todos los archivos en el directorio pasarán estos procesos:

1. Si SAVDTA está en *YES se realiza un backup del directorio a encriptar y opcionalmente de los subdirectorios. También un backup del directorio de destino.
2. Se finaliza el Journaling sobre el archivo.
3. Si el archivo tiene una entrada en el archivo CRPFIFS y está es “cero bytes” el archivo se desencripta.
4. El archivo encriptado del destino es eliminado.
5. Se elimina el registro del archivo CRPFIFS.

Nota: Los registros del directorios son eliminados del CRPFIFS.

Intento de Apertura de un archivo cuando la entrada del Registro IFS está en *ACTIVE

Se llama al exit point program QIBM_QP0L_SCAN_OPEN:

1. Se comprueba la “User Authority” sobre el almacén de claves que contiene la clave de desencritpación (Decrypt Key Store).
2. Si existe una Lista de Autorizaciones también se comprueba la “User Authority” en esa lista.
3. Si el usuario está autorizado a leer el archivo se desencriptará en el directorio original y el proceso puede continuar.

4. Si el usuario NO está autorizado a leer el archivo, este se bloquea y falla el proceso de apertura. El sistema lanzará un mensaje de fallo de apertura: “Object marked as a scan failure”.
5. El archivo permanecerá bloqueado hasta que el trabajo de servidor IFS desbloquee el archivo. Si el trabajo de servidor no está siendo ejecutado el archivo permanecerá bloqueado.

Intento de Cierre de un archivo cuando la entrada del Registro IFS está en *ACTIVE

Se llama al exit point program QIBM_QP0L_SCAN_CLOSE:

Si el archivo No tiene “cero bytes”, comprobar si un registro existe en el archivo CRPFIFS. A continuación,

A. Si No Existe un registro:
   i. Comprobar si el directorio de destino existe. Si no existe, lo crea.
   ii. Encripta el archivo.
   iii. Inicia el Journaling.
   iv. Añade un registro en el archivo CRPFIFS.
B. Si el registro Si Existe
   i. Encripta el archivo.
   ii. Actualiza el registro CRPFIFS.

Nota: Cuando un fichero o directorio es copiado o movido, no siempre se llamará a un File Open o File Close. Cuando esto ocurra, los exit point programs QIBM_QP0L_SCAN_OPEN o QIBM_QP0L_SCAN_CLOSE no serán llamados. Cuando estas operaciones se realizan puede crearse un journal que permita al programa del servidor IFSENCJOB ser alertado de que el archivo o directorio fue copiado o movido.

5.2 Notas a tener en cuenta

Existen toda una serie de procesos que necesita tener en cuenta cuando utilice el proceso de Encriptación de la IFS.

1. Cuando un usuario intenta abrir un archivo para leer y no están autorizados.

El archivo se bloquea en el sistema. Permanecerá bloqueado hasta que el Programa de Servidor IFSENCJOB lo abra y vacía el fichero. Este proceso desbloquea el archivo. Este proceso puede que no ocurra inmediatamente según la configuración del programa de servidor IFSENCJOB.

2. Encriptar/Desencriptar archivos de tamaño de más de 10MB

El proceso de abrir o cerrar un fichero puede llevar más tiempo del que está habituado. El proceso tiene que desencriptar el archivo antes de poder acceder a él y encriptarlo cuando lo cierra.

3. Un usuario tiene un archivo desencriptado y en modo de edición.

El archivo permanece desencriptado hasta que el usuario lo cierre.

a. Si un usuario autorizado intenta abrirlo mientras está abierto y en modo edición el fichero se bloqueará.

b. Si otro usuario intenta mover ese fichero fuera del directorio a otro directorio no encriptado, obtendrán la versión encriptada del archivo.

4. Si un usuario mueve un archivo a o fuera de un directorio (destino) encriptado.

Puede que nuestros procesos no sean conscientes de ello hasta que el programa de servidor IFS recupere el journal una vez el proceso haya sucedido. No se puede producir ninguna encriptación o desencriptación inmediata.

Si los exit programs QIBM_QP0L_SCAN_OPEN o QIBM_QP0L_SCAN_CLOSE no son llamados no se produce la comprobación de autorización.

Si el programa servidor IFSENCJOB encuentra un registro en el Journal que muestra que un archivo o directorio fue copiado o movido fuera de un directorio Encriptado se produce el siguiente proceso:

1 - Comprobar si el registro existe en el archivo CRPFIFS para el directorio o archivo de origen. Si el directorio No existe, ignoramos el archivo o directorio.

2 - Si el registro original todavía existe en el archivo CRPFIFS:

a. Comprueba si el usuario está autorizado a copiar o mover el archivo.

b. Si NO está autorizado y el proceso era un “Mover”, se recrea la estructura del directorio y cero bytes para el origen.

c. Si el usuario SI está autorizado a mover los archivos, se desencriptan los archivos en los directorios a donde se desea mover y se eliminan los archivos encriptados y directorios originales y luego se eliminan los registros del archivo CRPFIFS.

5. Desencriptar un archivo a través de una unidad de red

El usuario por defecto utilizado es QUSER.

Crypto Complete utilizará el exit point QIBM_QPWFS_FILE_SERV para recuperar el Id de Usuario con el que el usuario entro o se logueo. Este Id de usuario se utilizará para realizar la comprobación de autorización para desencriptar el archivo.

Cuando se llama al exit point QIBM_QP0L_SCAN_OPEN para desencriptar el archivo. el usuario QUSER debe tener autorización sobre el almacén de claves que contiene la clave de desencriptación (Decrypt Key Store) para poder desencriptar el archivo.

A. Si desea que todas las operaciones estén autorizadas desde una unidad de red puede añadir al usuario QUSER a la Lista de Autorizaciones.

B. Si solo desea que ciertos usuarios tengan acceso a través de la unidad de red tiene que dar autorización *USE a esos usuarios o grupos de usuarios en la Lista de Autorizaciones.

6. Eliminar la Encriptación Automática de la IFS del sistema

Siga los siguientes pasos y en este orden, para eliminar la Encriptación de la IFS:

Paso 1 - DCTIFSENCJ - Desactive todos las entradas activas del Registro de Encriptación.

Paso 2 - ENDIFSENCJ - Finalizar el trabajo de servidor IFS

Paso 3 - RMVEXTPGMS - Eliminar los Exit Point Programs añadidos por Crypto.

Paso 4 - Debe detener y reiniciar cualquier trabajo que tuviera acceso a los archivos de la IFS.

Cualquier trabajo que necesite usar estos exit programs tendrá que ser reiniciado.

Existen dos maneras de hacerlo.

1. Hacer una IPL del sistema.

2. Finalizar y reiniciar cualquier trabajo que vaya a utilizar los Exit Programs.

Las siguientes instrucciones le ayudarán a finalizar y reiniciar la mayoría de los servidores. Puede que haya otros que no estén listados aquí.

Finalizar procesos:

- ENDTCPSVR *NETSVR
- ENDTCPSVR SERVER(*FTP)
- ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
- ENDHOSTSVR *FILE
- ENDHOSTSVR *DATABASE
- ENDSBS QSERVER
- Finalizar cualquier trabajo Batch que accede a los datos de la IFS.

Reiniciar procesos:

- STRSBS QSERVER
- STRTCPSVR *NETSVR
- STRTCPSVR SERVER(*FTP)
- STRTCPSVR SERVER(*HTTP) HTTPSVR(*ALL)
- STRHOSTSVR *FILE
- STRHOSTSVR *DATABASE
- Reiniciar cualquier trabajo batch que accede a los datos de la IFS.