

Field Encryption para IBM i, utilizando Enforcive Enterprise Security

Enforcive Field Encryption es la forma más sencilla y segura de proteger los datos confidenciales de IBM i. Es una plataforma completa para el cifrado a nivel de archivo y campo, así como para enmascaramiento y codificación. La consola de gestión de Field Encryption es un módulo basado en GUI que se ha integrado completamente en el producto Enterprise Security, simplificando la operación mediante una interfaz familiar e intuitiva. La característica más notable es que la implementación no requiere ningún cambio en el código fuente de los programas existentes en su sistema, ya que es un cifrado independiente de la aplicación.

CARACTERÍSTICAS

Cifrado a nivel de campo: dentro del Cifrado de campo de Enforcive, las organizaciones tienen una gran variedad de algoritmos para elegir para cumplir con los estándares tales como DES, TDES o AES. El producto proporciona herramientas para el cifrado de los campos alfanuméricos y numéricos, y los usuarios no autorizados no podrán ver los datos cifrados, incluso cuando intenten acceder a ellos a través de diarios.

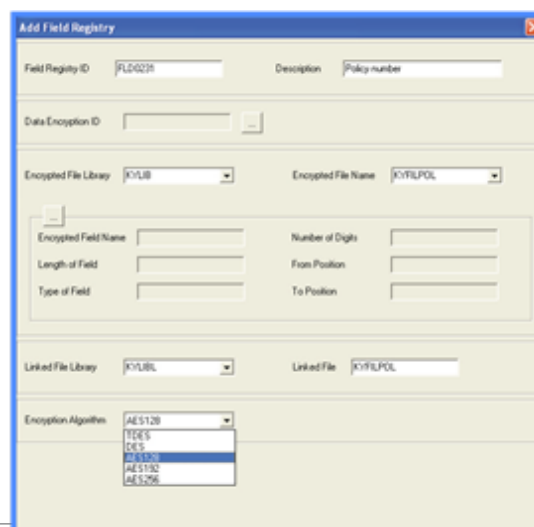
Seguridad, enmascaramiento y aleatorización: se pueden aplicar máscaras completas o parciales de campos en cualquier tipo de campo de base de datos. Para los campos numéricos, Enforcive ofrece una opción para mezclar datos, lo cual es muy beneficioso para las organizaciones que necesitan datos para desarrollar y probar sus aplicaciones.

Gestión de claves basada en roles: el producto ofrece una gestión de claves flexible. Se basa en un cifrado de dos niveles que requiere claves maestras para generar claves

de datos, lo que garantiza una separación estricta entre quienes generan las claves y los que los usan. Como medida adicional de seguridad, Enforcive puede cifrar cada clave utilizada para administrar el algoritmo de cifrado. Las organizaciones que utilizan Enforcive Field Encryption tienen la opción de almacenar la clave en IBM i o en un IBM i remoto u otro entorno de servidor. Las claves de cifrado se asignan a usuarios o grupos de usuarios según los roles que puede definir la organización.

Llaves múltiples ilimitadas: no hay límite en el número de claves de encriptación que puede usar, y se puede usar una clave de encriptación diferente para cada campo. **Acceso definido por el usuario:** descifre datos a nivel de grupo de usuarios en todo el sistema, sin la necesidad de detalles de nivel de aplicación.

Control de ubicación de objetos: los archivos de claves generados automáticamente son especificados por el administrador que



determina el nombre, la biblioteca y la autoridad del objeto.

Figura 1: Selección del algoritmo de cifrado

Cadenas generadas automáticamente: las cadenas clave, las cadenas de caracteres que forman la base para el algoritmo de cifrado, pueden ingresarse manualmente o generarse automáticamente para que incluso el administrador no pueda conocer su valor.

Compatibilidad de alta disponibilidad: Enforcive Field Encryption funciona en entornos de alta disponibilidad sin que se tomen medidas especiales. Las bases de datos de respaldo de alta disponibilidad serán idénticas al sistema de producción y contendrán las claves maestras y de datos necesarias para cifrar y descifrar los datos.

Guardar cifrado de archivos: además del cifrado de campos, la seguridad, el enmascaramiento y la codificación, también se ofrece el cifrado de objetos para guardar archivos, que brinda la capacidad de cifrar y guardar bibliotecas completas, así como objetos individuales. Una serie de comandos permite la integración fácil de Enforcive Save File Encryption en los procesos de respaldo. Las organizaciones que hacen copias de seguridad de sus datos ahora tienen una forma fácil de asegurarse de que nadie que no esté autorizado pueda leer los datos en caso de que sus cintas terminen en las manos equivocadas.

BENEFICIOS

Protección de datos: el cifrado agrega una capa vital a la seguridad de los datos confidenciales de una organización. Enforcive proporciona seguridad de nivel de campo y archivo administrada por GUI, lo que evita que incluso los usuarios avanzados accedan a los datos en campos que requieren acceso limitado.

Independencia de la aplicación: el cifrado de campo de Enforcive se ha diseñado para minimizar el impacto en las aplicaciones de misión crítica que podrían verse afectadas por los procesos de cifrado y descifrado. Las estructuras de archivos de bases de datos existentes permanecen sin cambios. Las organizaciones normalmente no requerirán ningún cambio de programa.

Basado en GUI: el producto está totalmente basado en GUI, lo que permite a los responsables de seguridad que no son necesariamente expertos en "pantalla verde" Para gestionar fácilmente la protección de datos sensibles en su organización.

Cumplimiento: requisitos tales como el estándar de seguridad de datos PCI (requisito 3) especifican la protección de los datos almacenados del titular de la tarjeta. Enforcive Enterprise Security proporciona la respuesta definitiva a ese requisito mediante un mecanismo de cifrado y descifrado infalible que utiliza estándares de algoritmo de cifrado aprobados por PCI universalmente aceptados.

Integración con Enterprise Security Manager: aunque las funciones de encriptación y enmascaramiento de Enforcive se pueden implementar de forma independiente como una solución independiente, el producto se puede administrar sin problemas dentro de Enterprise Security Suite.

Desde la GUI de Enforcive Field Encryption, los usuarios pueden moverse fácilmente entre los módulos. La asignación de claves a los usuarios se integra con la administración de usuarios de Enterprise Security. La creación de claves está integrada con la administración de roles de administración de Enterprise Security. Los cambios en las configuraciones de cifrado se registran en la Auditoría Central de Enforcive y se pueden informar en el

Generador de informes de Enforcive. Con las funciones existentes proporcionadas por el producto Enterprise Security, incluida la gestión de puntos de salida, la gestión de la autoridad de objetos y el filtrado de paquetes IP, Enforcive ofrece la herramienta definitiva para la protección de datos.