Field Encryption

for IBM i, using Enforcive Enterprise Security

Overview

Enforcive Field Encryption is the simplest and safest way to secure IBM i sensitive data. It is a comprehensive platform for file- and field-level encryption, as well as for masking and scrambling. Field Encryption's management console is a GUI-based module that has been fully integrated into the Enterprise Security product, simplifying operation by using a familiar and intuitive interface. The most remarkable feature is that implementation does not require any source code changes to existing programs in your system as it is application independent encryption.

Features

Field-level Encryption - Within Enforcive Field Encryption, organizations have a large variety of algorithms to choose from to comply with standards such as DES, TDES, or AES. The product provides tools for the encryption of both alphanumeric and numeric fields, and unauthorized users will not be able to see the encrypted data, even when they try to access it through journals.

Security, Masking, and Scrambling - Full or partial masks of fields can be applied on any kind of database field. For numeric fields, Enforcive offers an option to scramble data, which is very beneficial to organizations that need data for developing and testing their applications.

Role-based Key Management - The product offers flexible key management. It is based on two-tier encryption requiring master keys in order to generate data keys, ensuring strict separation between those who generate the keys and those who use them. As an additional measure of security, Enforcive can encrypt each key used to manage the encryption algorithm. Organizations using Enforcive Field Encryption have the option to store the key either on IBM i or on a remote IBM i or other server environment. Encryption keys are assigned to users or groups of users based on roles which can be defined by the organization.

Unlimited Multiple Keys - There's no limit on the number of encryption keys you can use, and a different encryption key can be used for every field.

User-defined Access - Decrypt data at the user group level everywhere on the system, without the need for application level detail.

Control of Object Placement - The automatically generated key files are specified by the administrator who determines the name, library, and authority of the object.

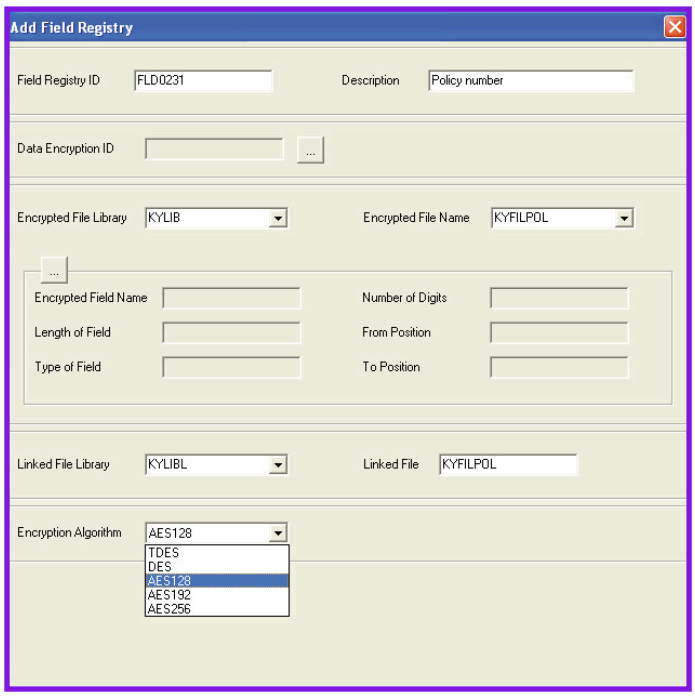

Figure 1: Choosing Encryption Algorithm

Auto-generated Strings - Key strings, the character strings that form the base for the encryption algorithm, can be entered manually or generated automatically so that even the administrator cannot know their value.

High Availability Compatibility - Enforcive Field Encryption works in high availability environments without any special measures being taken. High Availability backup databases will be identical to the production system and will contain the master and data keys needed to encrypt and decrypt the data.

Save File Encryption - In addition to field encryption, security, masking and scrambling, also offered is object encryption for save files, providing the ability to encrypt and save entire libraries as well as individual objects. A series of commands allows easy integration of Enforcive Save File Encryption into backup processes. Organizations backing their data up to tape now have an easy way to make sure the data cannot be read by anyone who is not authorized in case their tapes end up in the wrong hands.

A 5-Step Process of Implementing Encryption

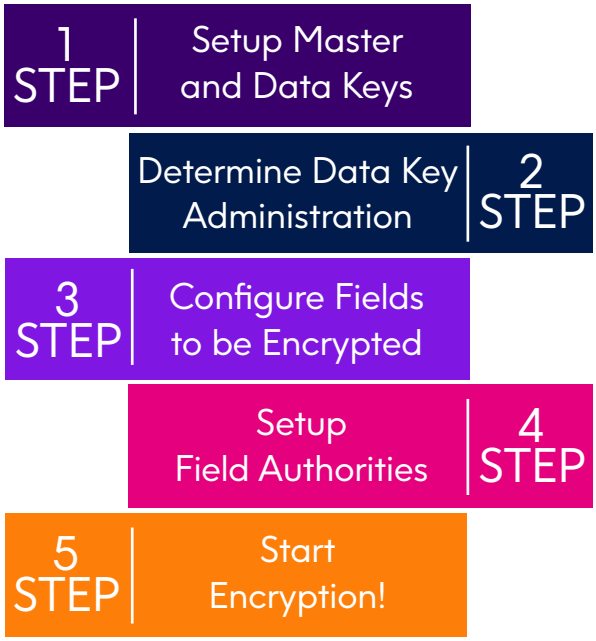

Figure 2: Enforcive Steps to Encryption

Benefits

Data Protection - Encryption adds a vital layer to the security of an organization's sensitive data. Enforcive provides GUI-managed file- and field-level security, preventing even power users from accessing data in fields that require limited access.

Application Independence - Enforcive Field Encryption has been engineered to minimize impact on mission critical applications that could be affected by the encrypting and decrypting processes. Existing database file structures remain unchanged. Organizations will typically not require any program changes.

GUI-based - The product is fully GUI-based allowing security officers who are not necessarily "green screen" experts to easily manage the protection of sensitive data in their organization.

Compliance - Requirements such as the PCI Data Security Standard (requirement 3) specify protection of stored cardholder data. Enforcive Enterprise Security provides the ultimate answer to that requirement by a foolproof encryption and decryption mechanism using universally accepted PCI-approved encryption algorithm standards.

Integration with Enterprise Security Manager - Although Enforcive encryption and masking features can be deployed independently as a standalone solution, the product can be managed seamlessly within the Enterprise Security Suite. From the GUI of Enforcive Field Encryption, users can move easily between modules. The allocation of keys to users is integrated with Enterprise Security's user management. Key creation is integrated with Enterprise Security administration role management. Changes to encryption configurations are logged by Enforcive's Central Audit and can be reported on in Enforcive's Report Generator. With the existing features provided by the Enterprise Security product including Exit Point Management, Object Authority Management and IP Packet Filtering, Enforcive offers the ultimate tool for data protection.