

ENCRYPTIONIZER FOR SQL SERVER

Securing sensitive data or meeting the new compliance standards (HIPAA Omnibus, PCI, FIPS 140-2) on SQL Server, Encryptionizer, is an easy-to-use and deploy, flexible architecture securing data in physical, virtual and cloud infrastructures. It requires no administrative overhead while increasing ROI through enhanced protection of customer data and your own IP.

Encryptionizer offers the following capabilities for SQL Server Encryption:

- Automatic Transparent Whole Data Encryption (TDE)
Automatic Transparent Column Encryption
- File/Folder Encryption

As a cost effective alternative (to upgrading to SQL Server 2008 Enterprise or later) for Transparent Data Encryption, Encryptionizer is well suited to transparently protecting applications which are based on the SQL Server Platform such as Microsoft Sharepoint and Dynamics, with virtually no impact on performance.



ENCRYPTIONIZER FOR SQL SERVER

Automatic Transparent Whole Data Encryption (TDE) For SQL Server Encryption

- ❖ Supports all versions from SQL Server 2000 to SQL Server 2016.
 - ❖ Supports all editions of SQL Server, Express to Enterprise.
 - ❖ Deploys quickly and easily with point-and-click GUIs. No programming or ongoing administration required.
 - ❖ Protect all your intellectual property while making them seamlessly accessible through your application or website, including:
 - ◆ SQL databases,
 - ◆ System databases (Master, TempDB, etc)
 - ◆ Backups,
 - ◆ FileStreams,
 - ◆ Attachments (PDFs, Documents, image and media files, Access databases, etc)
 - ❖ Deploys quickly. Maintenance-free. Minimal ongoing administration.
 - ❖ No programming required. No changes to applications, schemas, queries, etc.
 - ❖ Fast – less than 1% performance impact on a properly sized server.
 - ❖ Optional Enterprise Manager for deployment on multiple servers from one location.
 - ❖ Optional, powerful API set.
 - ❖ Developer friendly: easy to bundle into existing SQL-based applications with no reprogramming.
- Encryptionizer's SQL Server Encryption provides an additional layer of security on top of Windows security and SQL Server security, in case perimeter defenses are breached. It secures data on servers

as well as on backup media. Combined with Encryptionizer for SQL Express, Encryptionizer secures distributed databases all the way down to the workstation or laptop. It is also a cost effective alternative to MS SQL TDE without having to upgrade to SQL Server Enterprise Edition.

Automatic Transparent Column Encryption

- ❖ Provides additional granularity on top of, or instead of TDE.
- ❖ Control access to columns by User, Group and/or Role.
- ❖ Unmask all or part of a column based on access. for example, show only last four digits of social security number.
- ❖ Supports all versions from SQL Server 2000 to SQL Server 2016.
- ❖ Supports all editions from SQL Server Express to SQL Server Enterprise.
- ❖ Simple Point and click interface.
- ❖ Deploys quickly. Maintenance-free.
- ❖ No programming required. No changes to applications, schemas, queries, etc.
- ❖ Optionally audit access to protected columns.
- ❖ Optional, powerful API set.

Column encryption (Col-E) can be deployed in combination with (or depending on your requirements, instead of) transparent database encryption. Encryptionizer with Col-E protects specific columns from users/groups who normally need access to the underlying table.

Col-E Manager – utilizes a point-and-click interface that allows you to quickly set up column encryption that in most cases can be transparent to exist-



ENCRYPTIONIZER FOR SQL SERVER

ting applications. The Col-E Manager allows you to encrypt a column and specify the groups of users that are allowed to view the encrypted data through the use of database roles.

File/Folder Encryption

The Advanced Version of NEP allows you to automatically encrypt any files copied to or created in designated folders and subfolders, even on a remote drive. You can also optionally audit access to encrypted files and folders to a SQL database. This feature is useful for data that may be imported or exported to your protected SQL Server, keeping all data encrypted at all times. As an example, you might have an FTP server which receives data into a folder. Encryptionizer can automatically encrypt all received data in that folder until it is ready to be imported into SQL.

API's

The APIs can be used in combination with (or depending on your requirements, instead of) whole file encryption. They allow programmable access to the "Encryptionizer engine." They allow a greater level of flexibility and "granularity" than whole database encryption.

The main purpose of the APIs is to protect certain columns, fields, and/or records from authorized users who must have access to other columns in a table. For example, you might want to give only certain users the ability to see a column containing credit card numbers. You can even use them to encrypt SQL Server columns.

Besides column encryption, there are various APIs for encrypting and decrypting files. These are useful if you are planning to distribute encrypted

databases, files, or other digital content to workstations, laptops, or other servers (e.g., connected by LAN, over the internet, or via removable media.).



contact@exsystemusa.com
+1 (786) 352-8109
3785 NW 82 Ave Suite 309
Miami, FL 33166. USA.

