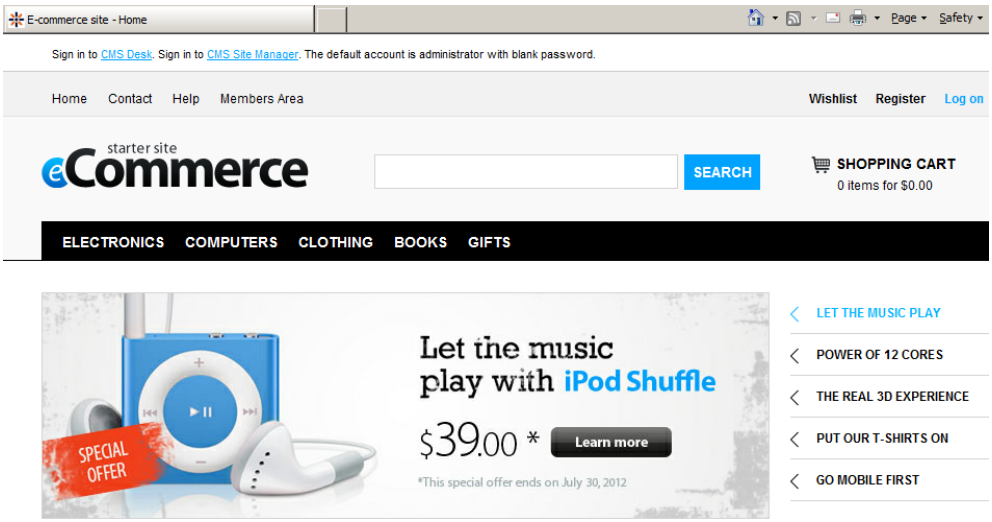
Database Encryption with DbDefence

In this article we will show how to encrypt the database, setup access, but still have a web site running without writing a line of code!

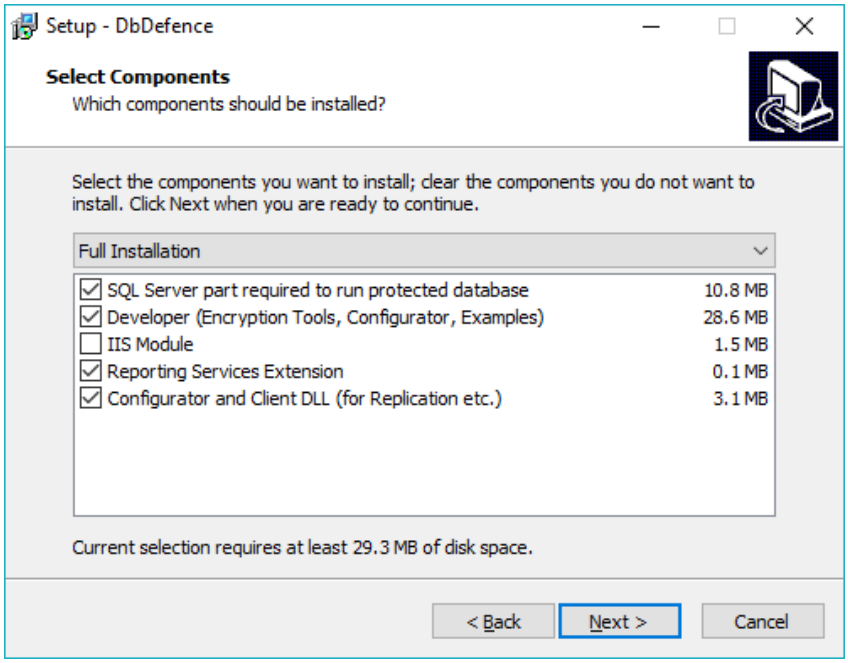
We are going to encrypt a database and show how encryption affects running CMS and other applications.

For this demo we used Kentico CMS. It is large and complex CMS available for evaluation written on .NET. After installation Kentico in E-commerce mode it looks like a typical e-shop:



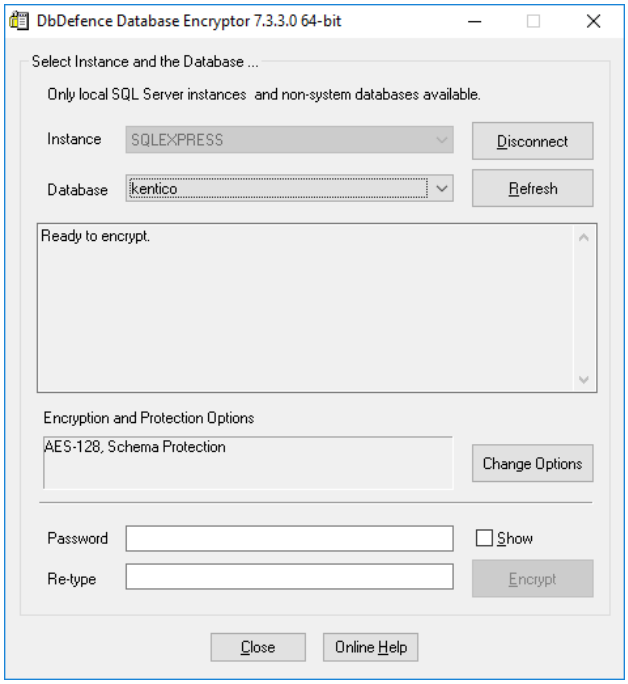
Installation

Install DbDefence on SQL Server computer with the default settings. If IIS Server is on another machine, don't install IIS Module there. The module isn't required in most cases. Encryption will work absolutely transparently.



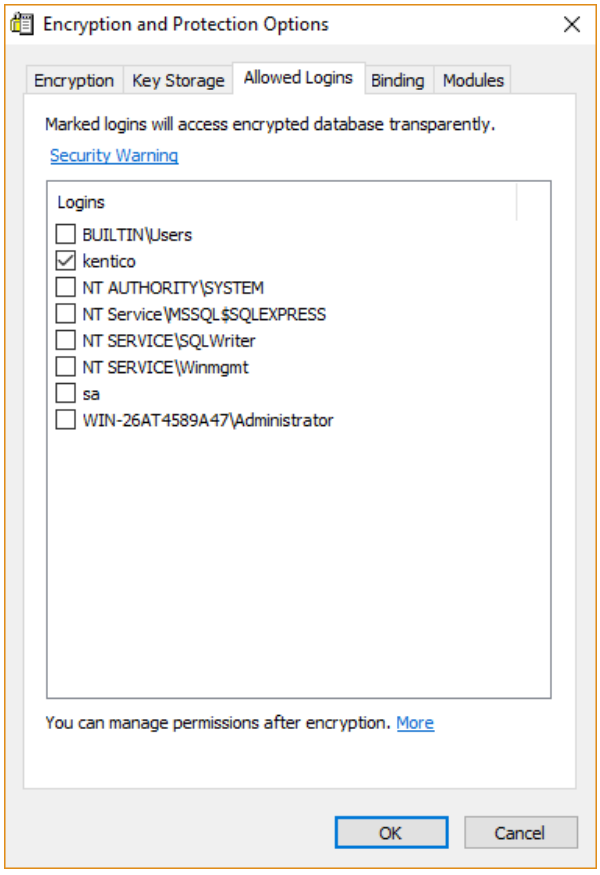
Encryption Settings

Now, run DbDefence Encryptor to encrypt existing Kentico CMS database. Connect to the instance and select the database.



Click *Change Options* to adjust access options. The CMS uses login *kentico*.

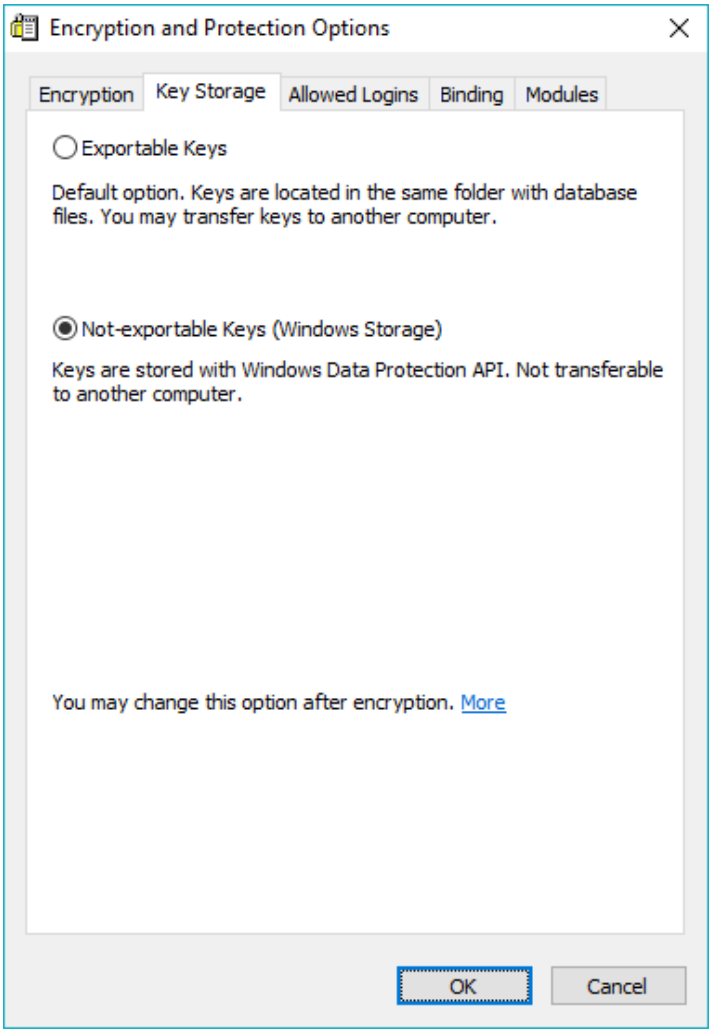
In *Change Options* dialog switch to *Allowed Logins* tab and check *kentico* login.



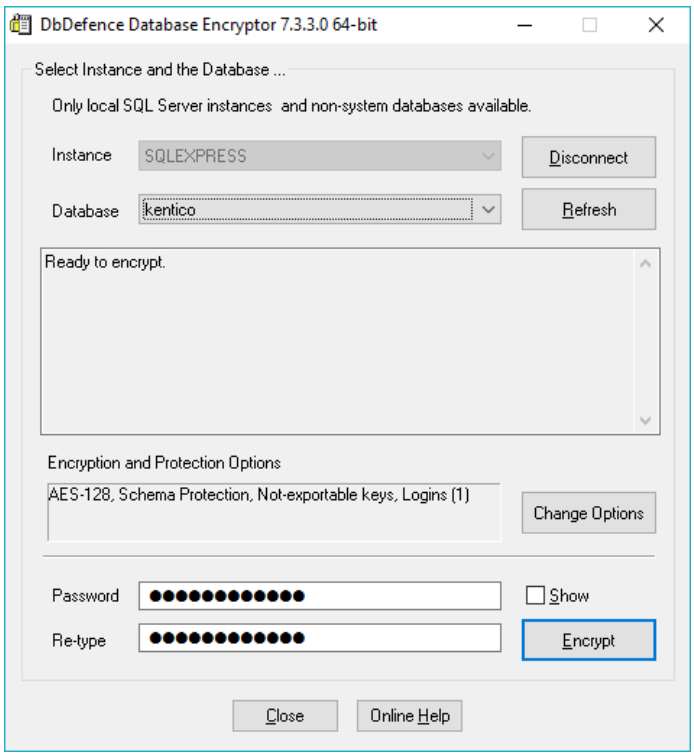
In this example, we check only *kentico* and leave *sa* unchecked. Unchecked logins will not have access; even if they are super users like *sa*. However, you may check as many logins as you need accordingly to your security requirements.

Note: *Some customers prefer not to restrict access at all. In this case, switch to Encryption tab and select "Encryption Only"*

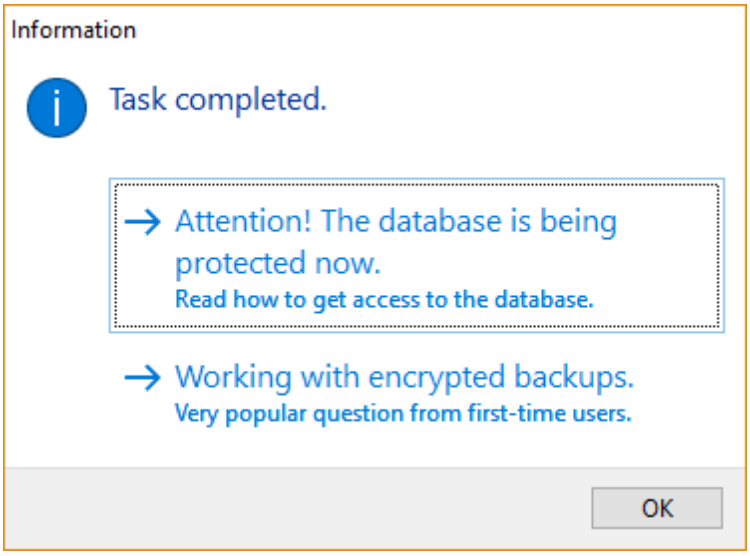
To protect encryption keys and provide better security switch to *Key Storage* tab. Setting "Not-exportable keys" will make the database files and its keys non-transferable to another server.



Enter complex encryption password. Existing password policy in Windows Server OS denies simple passwords. Workstation operating systems like Windows 7,8, or 10 are usually less restrictive. DbDefence does not check the password complexity, but SQL Server does accordingly to Windows policies.



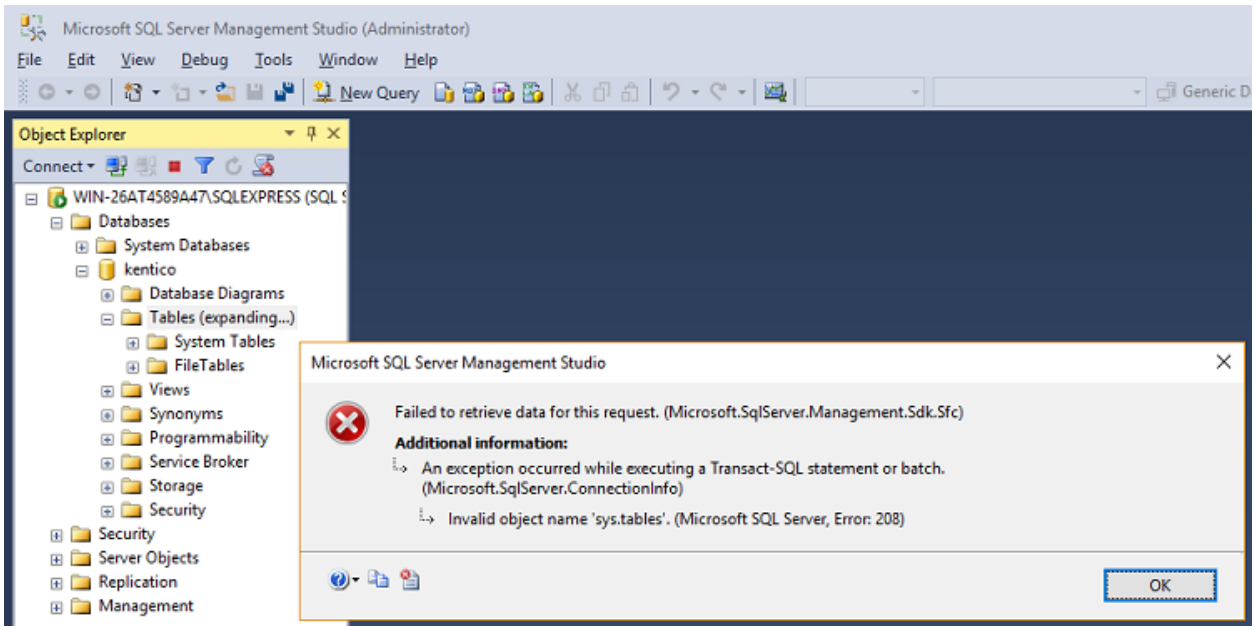
After encryption, Encryptor shows a message box with reminder for the first-time users.



Access

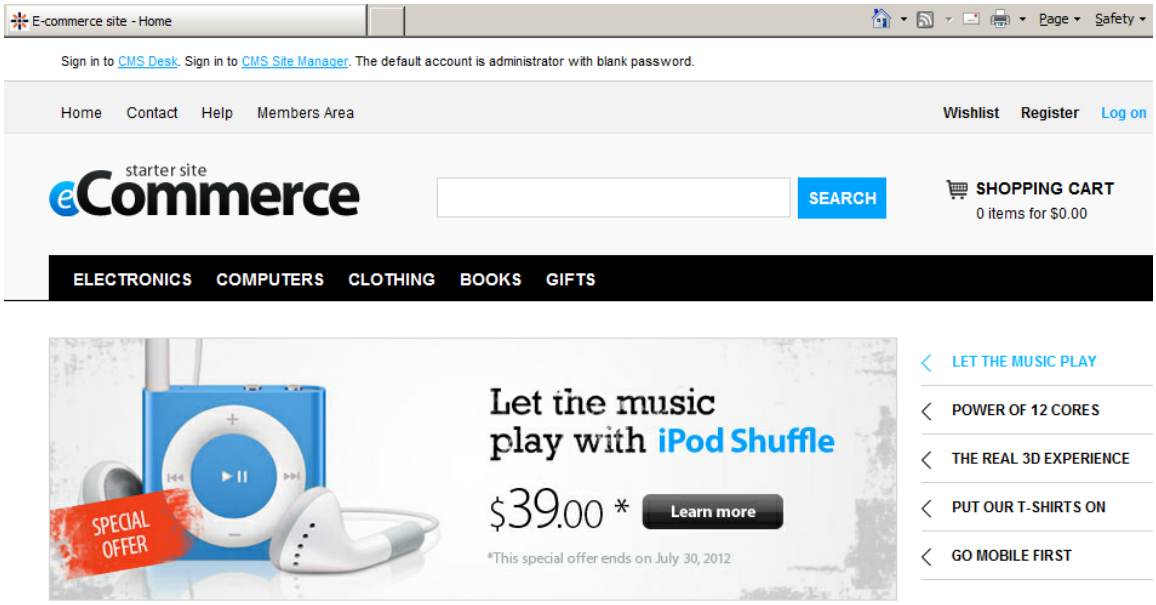
Let's see how SSMS with *sa* login reacts on the database encryption. When *sa* tries to access Kentico database directly with SSMS there is an error.

Typical error message:



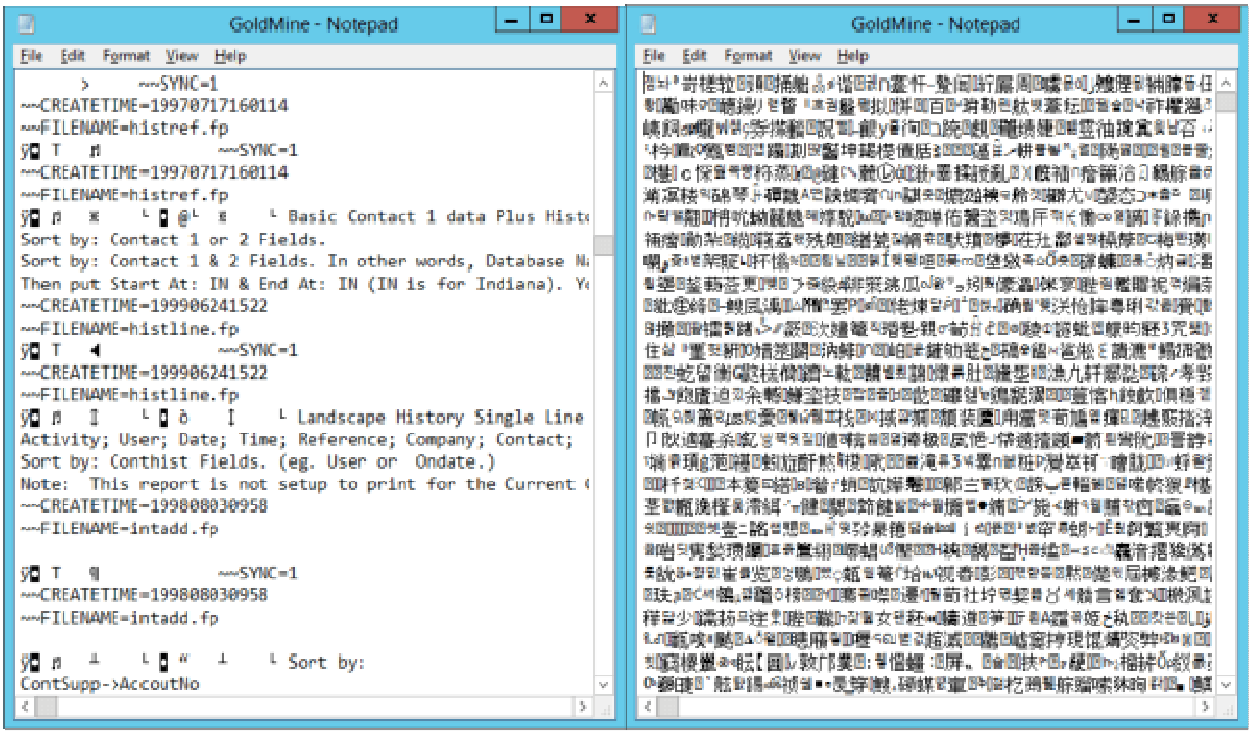
In this way DbDefence denies access to the database for all logins except those ones marked on *Allowed Logins* tab.

Open CMS web page again. Here it is. Running like nothing happened to the database. The website works absolutely transparently and with no changes.



Finally, very popular question: **How can I see that database is encrypted?**

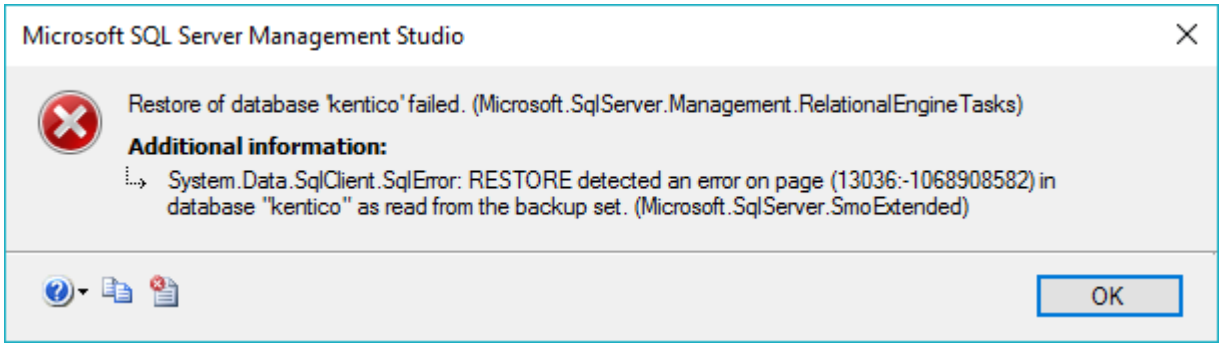
With small databases you can use Notepad to open database files (MDF and LDF). In general, the database file looks like on the left side of the picture below. It is full of structured data and clear text. The right side of the picture is encrypted database file.



Backup/Restore

After the encryption, you can't easily restore the backup (made out of encrypted database) on another server. Encrypted backup can be restored only to the database encrypted with the same password.

Typical error when someone tries to restore an encrypted backup to unencrypted database.



For customers with specific needs we can provide more information on used algorithms, FIPS-140-2 and PKCS#11 modules.

If you have any questions, do not hesitate to contact support@activecrypt.com.