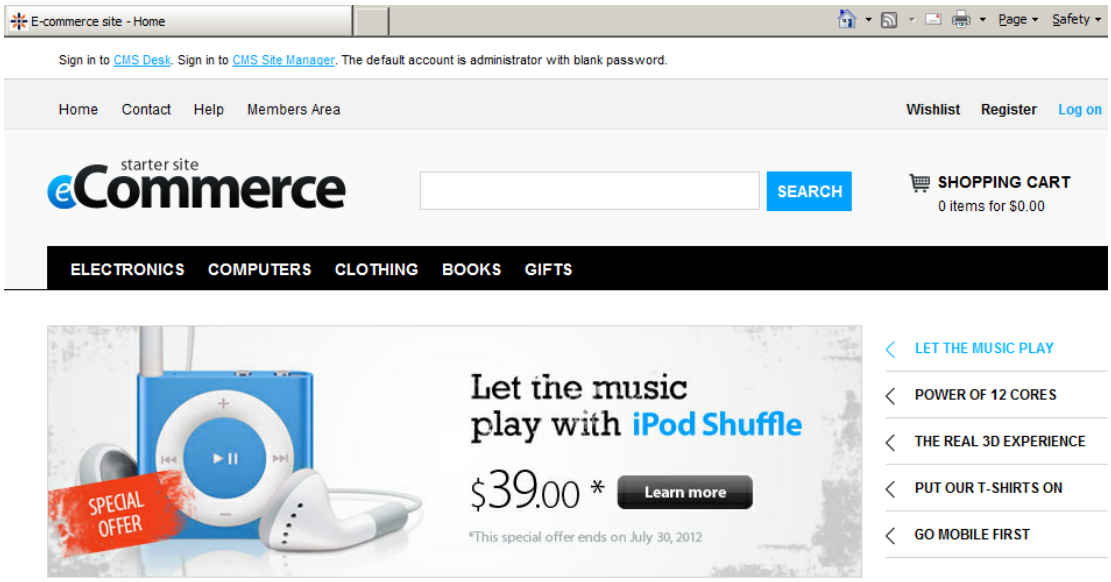
Cifrado de Base de Datos con DbDefence y Aplicaciones Web.

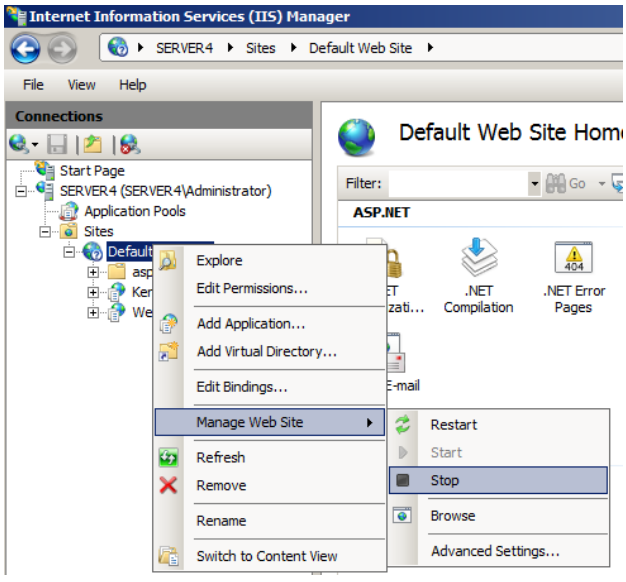
En este artículo le mostraremos cómo cifrar la base de datos, restringir el acceso, y aún así, ¡tener un sitio Web ejecutándose sin escribir una sola línea de código!

Para la versión de muestra de Aplicaciones Web utilizamos Kentico CMS. Es un CMS extenso y complejo disponible para evaluación. Después de la instalación, Kentico en modo E-commerce luce como una e-shop normal:

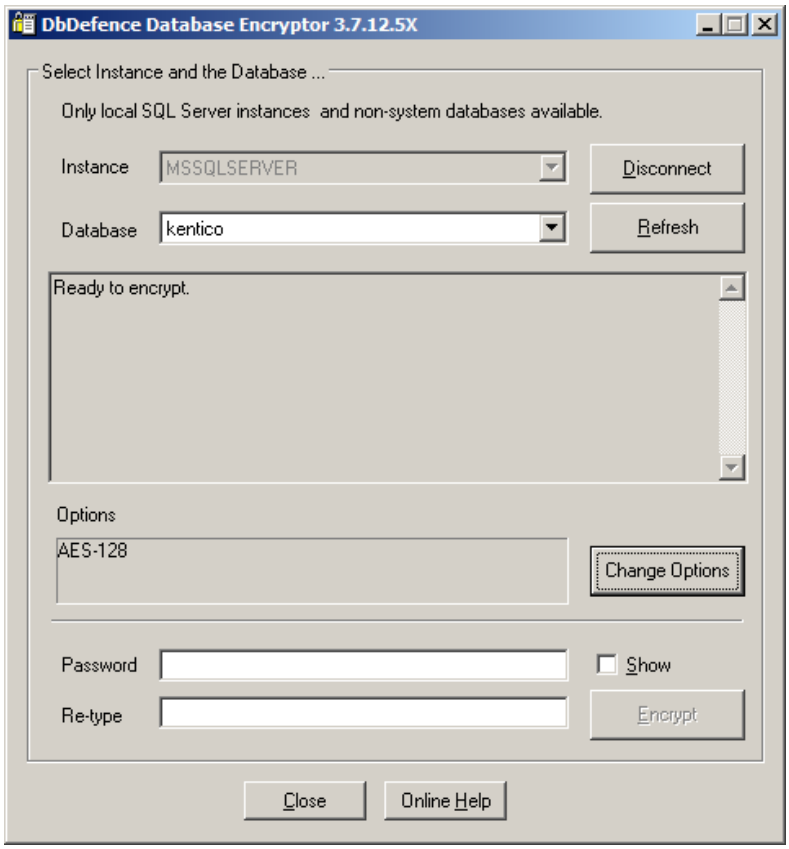


Durante la instalación, instala su base de datos en un SQL Server existente. Vamos a cifrarla y demostrar su comportamiento en la ejecución de un CMS y otros clientes.

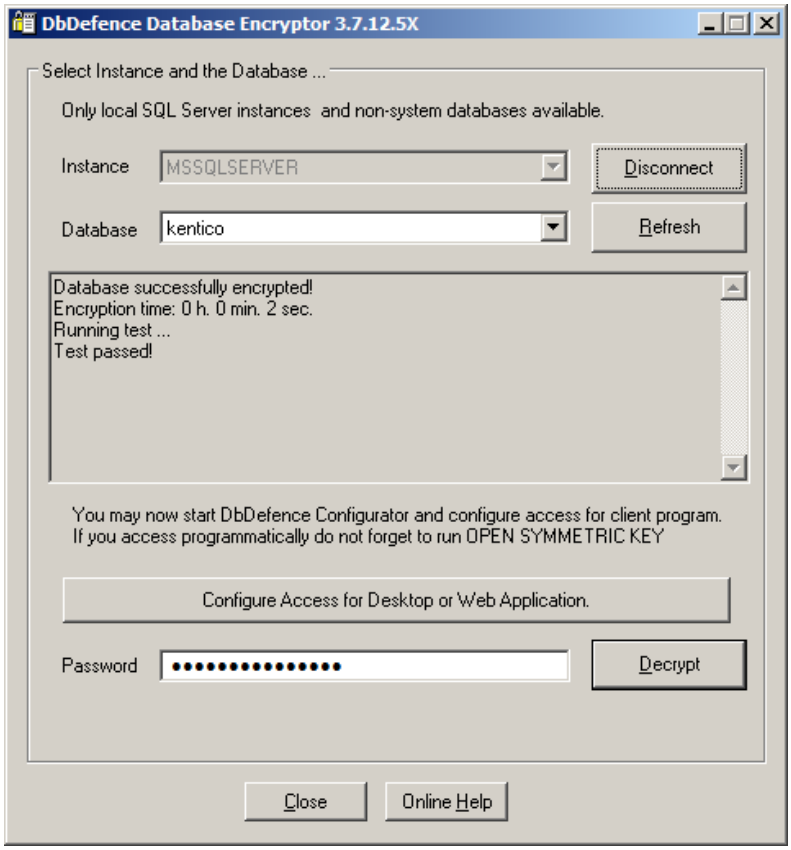
Primero que nada, necesita detener el servidor Web, de otra manera la conexión existente de la base de datos desde el sitio Web no le permitirá a Encryptor realizar operaciones en la base de datos. Puede detener el sitio Web desde IIS Manager:



Ahora, ejecute DbDefence Encryptor para cifrar la base de datos existente de Kentico CMS.

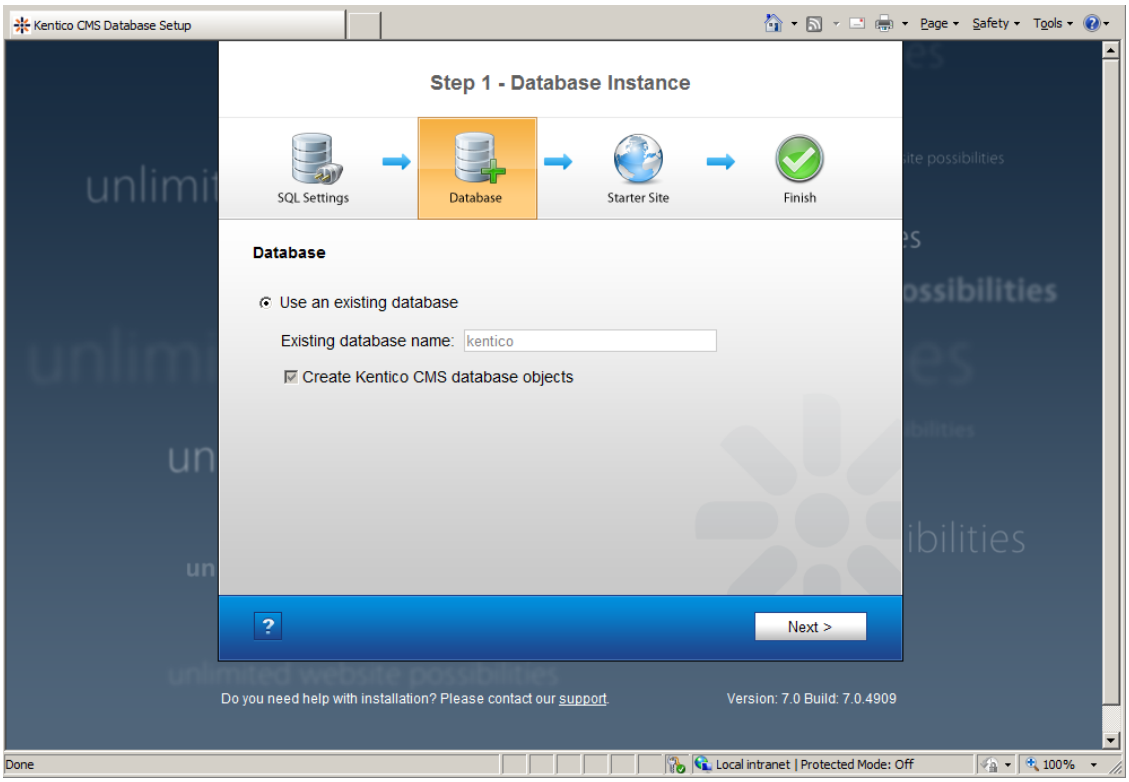


Ingrese una contraseña compleja, ya que por lo general las políticas referentes a contraseñas niegan contraseñas sencillas.



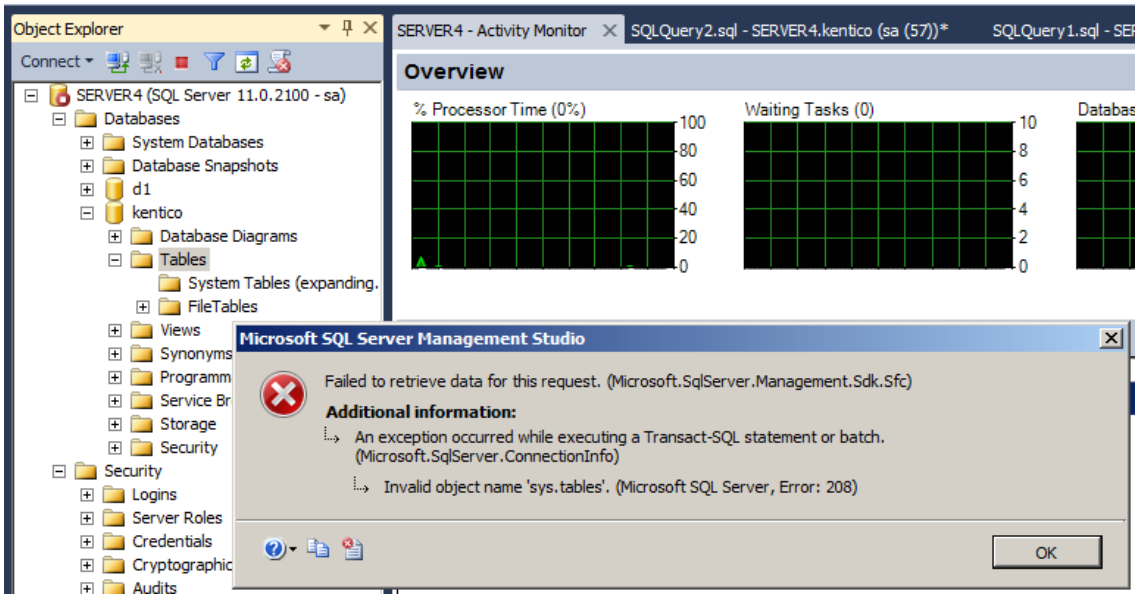
Después de que ingresamos una contraseña y ciframos la base de datos, Encryptor ofrece configurar las aplicaciones existentes para acceder sólo a la base de datos cifrada. También puede descifrarla cuando lo considere necesario.

Pero veamos cómo reacciona el CMS en la base de datos cifrada y abramos una página Web nuevamente:



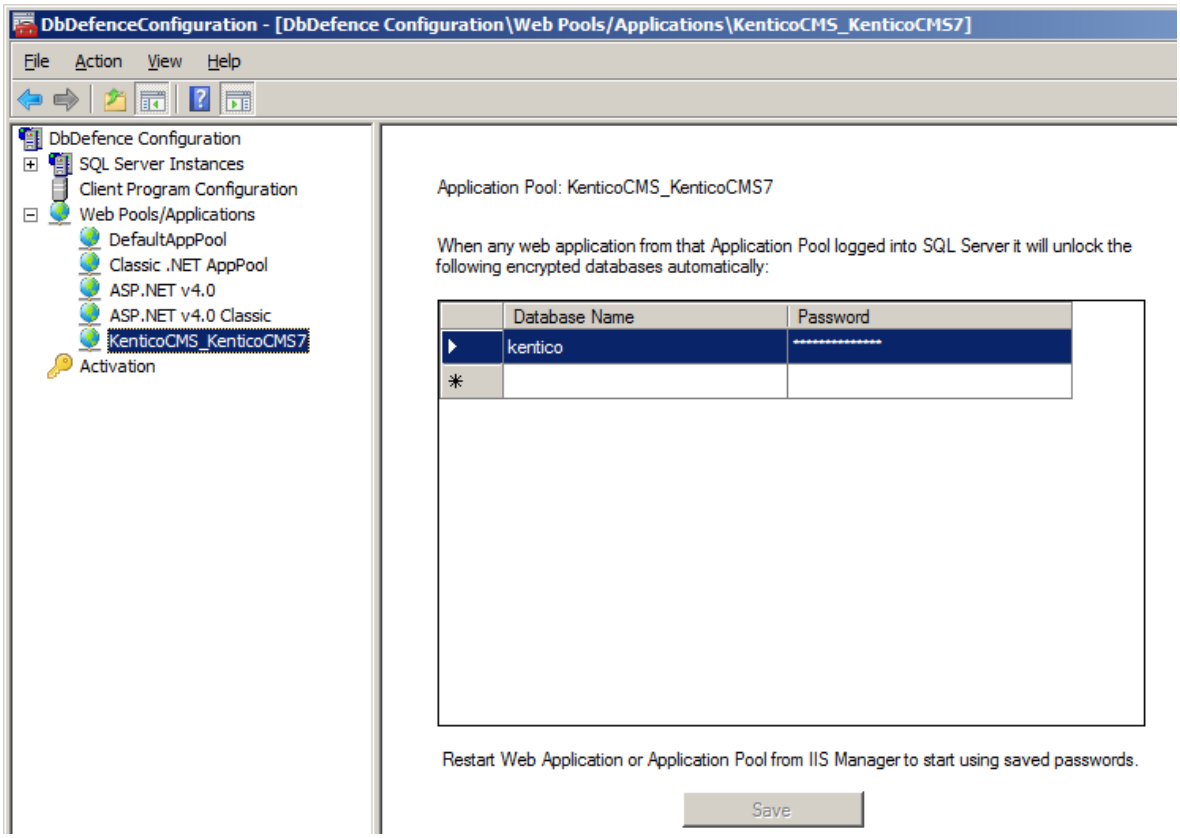
El CMS no puede acceder a la base de datos, aunque los programadores pueden lidiar con esa excepción de manera profesional y ofrecer la configuración de una nueva base de datos. Así que observamos que esa vieja base de datos no puede utilizarse más.

Cuando alguien intenta acceder a la base de datos de Kentico directamente con SSMS no hay tablas:

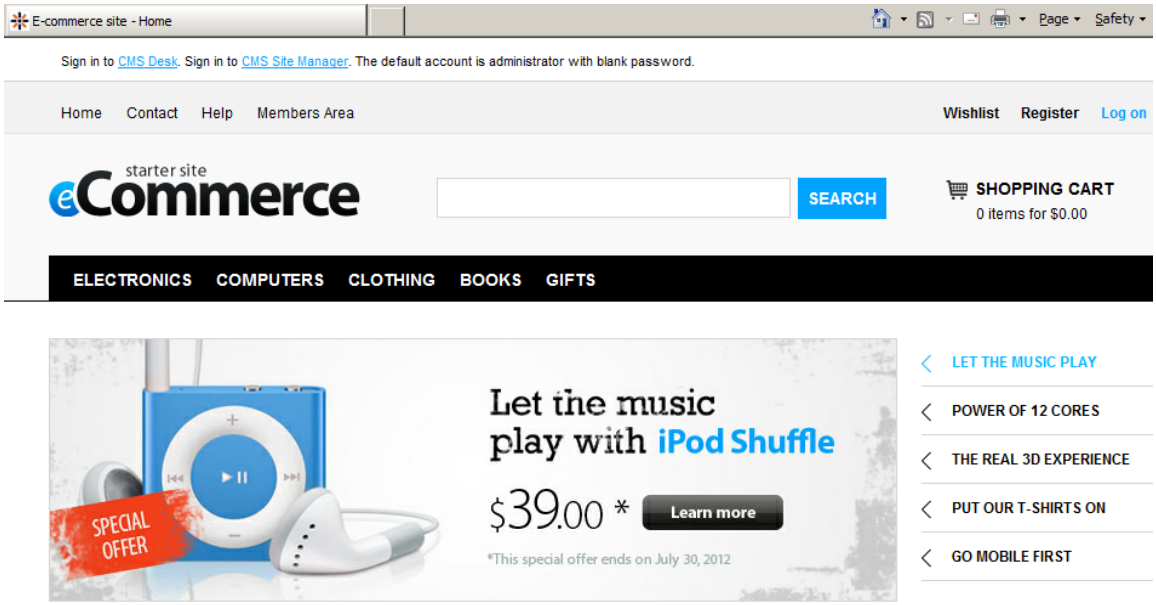


Así que la base de datos está cerrada para todas las aplicaciones sin autorización.

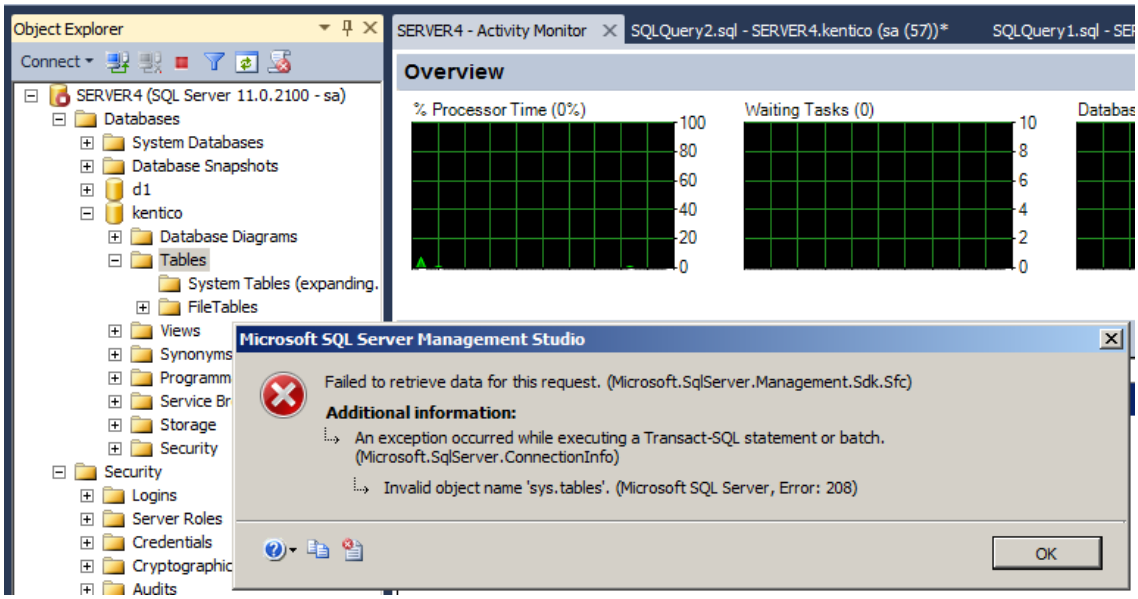
Vamos a darle autorización al CMS para que utilice la base de datos restringida. Necesitamos iniciar el Configurador de DbDefence e ingresar el nombre de la base de datos y la contraseña que utilizamos previamente para el cifrado. El configurador enlista los nombres de agrupaciones existentes. Por fortuna, Kentico crea su propio nombre de agrupación y no tenemos que adivinar cuál es. Ingrese el nombre de la base de datos, la contraseña y presione Save.



Inicie el sitio Web desde IIS Manager y abra la página Web Kentico nuevamente. Allí está. Ejecutándose como si nada hubiera pasado.



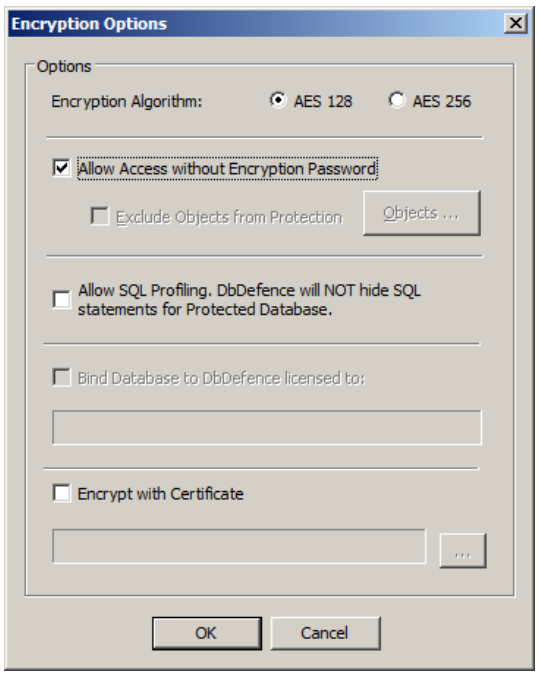
A la par, al intentar acceder a la base de datos con SSMS aún obtenemos un error:



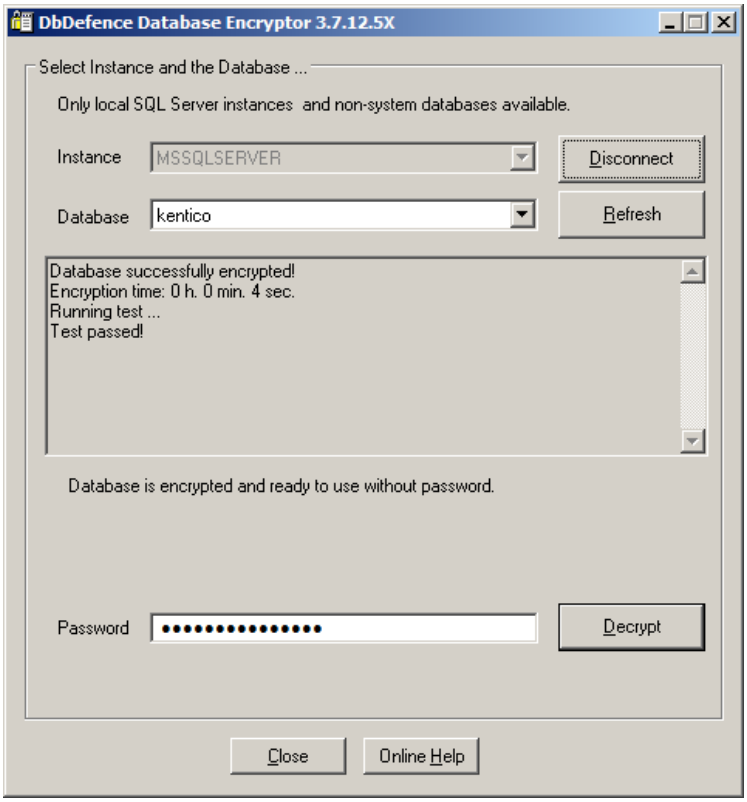
Si quiere que SSMS se ejecute en "modo desbloqueado" también, necesita agregar ssms.exe (el archivo de aplicación principal de SSMS) en el Configurador en la Sección Client Program Configuration y asignar la base de datos/contraseña de la misma manera.

DE MANERA ALTERNATIVA, si únicamente quiere cifrar los archivos y NO RESTRINGIR el acceso de las aplicaciones, necesita configurar una opción especial antes del cifrado.

Antes de cifrar una base de datos, presione "Change Options" y marque la casilla "Allow Access without Encryption Password". De manera adicional, puede cambiar el algoritmo de cifrado a uno AES-256 más fuerte.



Después de que haya cifrado la base de datos con el parámetro “permitir acceso”, la interfaz gráfica de usuario de Encryptor no ofrece la posibilidad de configurar el acceso puesto que no hay cambios en los permisos de acceso.



Esto significa que no necesita ingresar ningún dato para ejecutar Kentico CMS y SSMS, aunque los archivos permanecen cifrados. Para verificar eso, intente hacer un respaldo de la base de datos y restáurelo en un servidor diferente.

Eso es todo, ¡tenga un buen día!

Si tiene alguna pregunta, no dude en contactarnos en support@dbdefence.com.