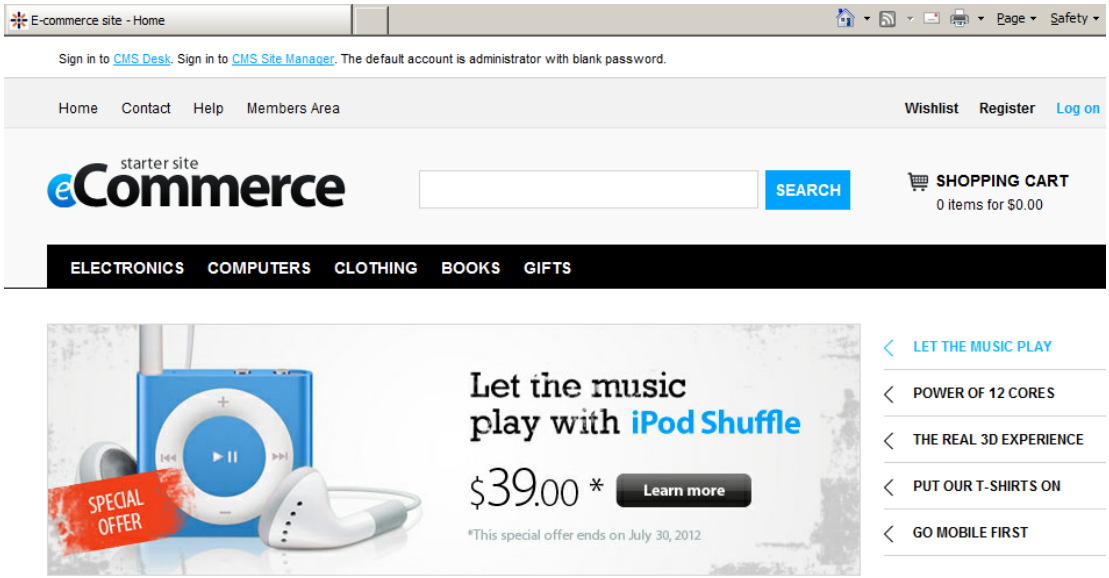
# Datenbank-Verschlüsselung mit DbDefence und Webanwendungen.

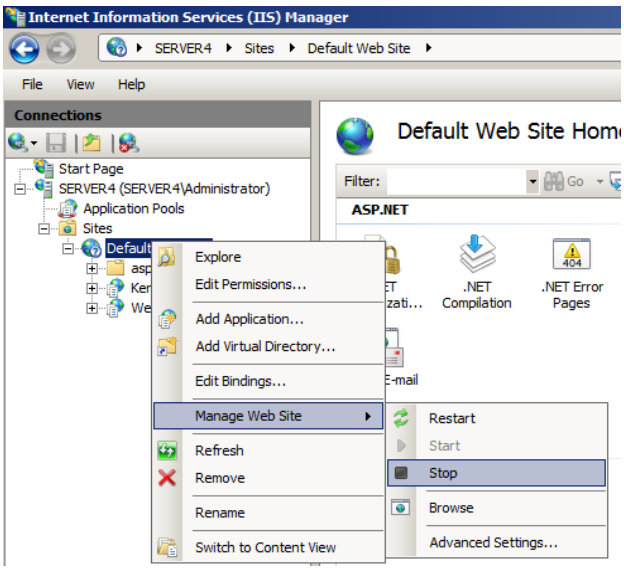
In diesem Artikel werden wir Ihnen zeigen, wie Sie eine Datenbank verschlüsseln können, um den Zugriff einzuschränken, aber trotzdem noch eine funktionierende Website haben, ohne eine einzige Zeile Code zu schreiben!

Als Beispiel einer Webanwendung haben wir zur Demonstration das Kentico KMS benutzt. Es ist ein großes und komplexes KMS, welches für Auswertungen zur Verfügung steht. Nach der Installation von Kentico im E-Commerce-Modus sieht es wie ein typischer E-Shop aus:

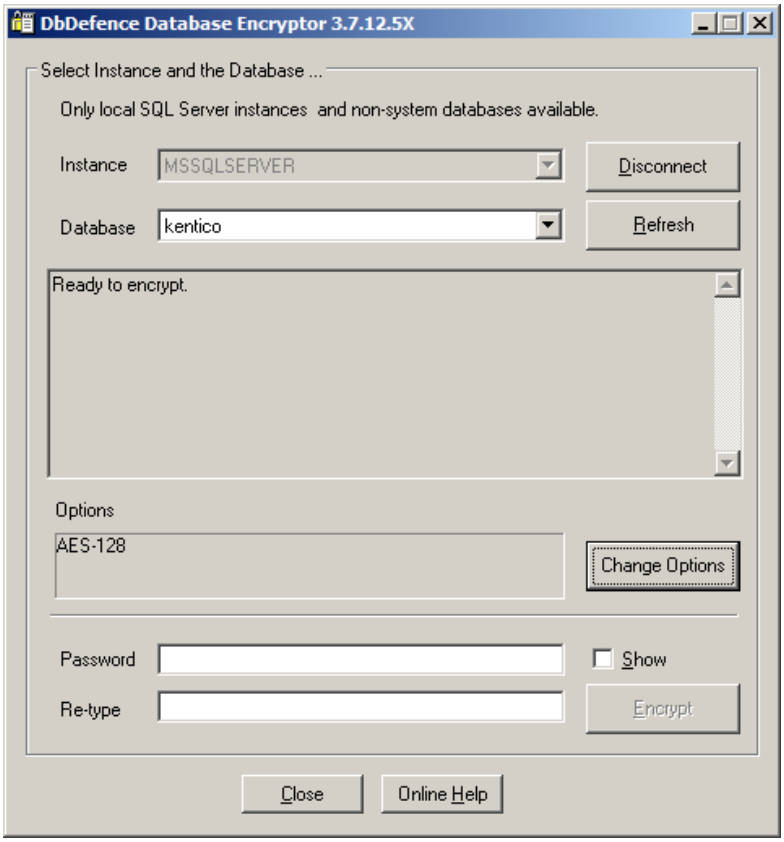



Während der Installation installiert es seine Datenbank auf dem vorhandenen SQL-Server. Wir werden diese verschlüsseln und zeigen, wie das den Ablauf des KMS und anderer Anwendungen beeinflusst.

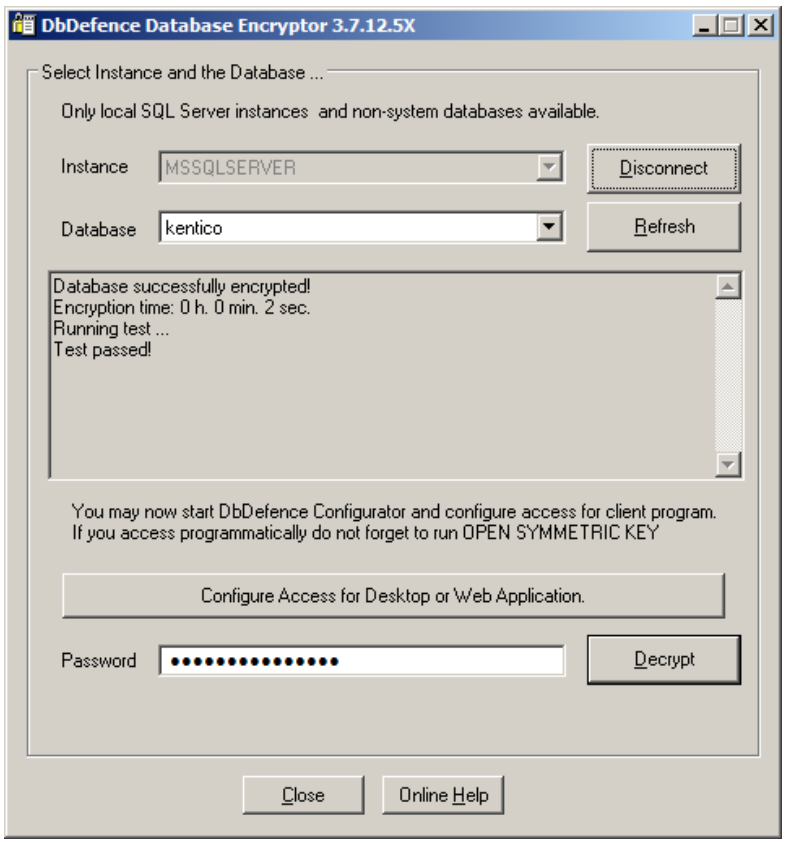
Zuerst müssen Sie den Webserver anhalten, sonst wird die vorhandene Datenbank-Verbindung der Website den Verschlüsseler keine Veränderungen an der Datenbank ausführen lassen. Sie können die Website über den IIS-Manager beenden:




Lassen Sie nun den DbDefence-Verschlüsseler laufen, um die vorhandene Kentico KMS-Datenbank zu verschlüsseln.

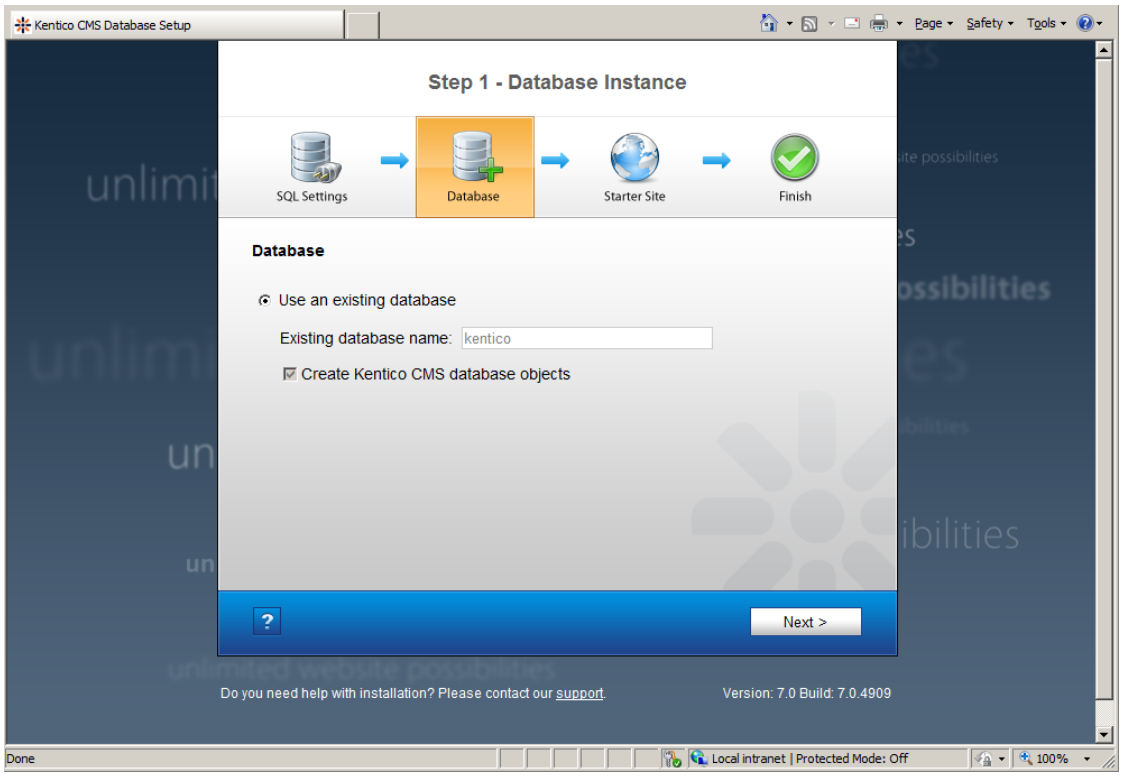



Geben Sie ein komplexes Passwort ein, da die vorhandenen Passwort-Richtlinien einfache Passwörter normalerweise ablehnen.



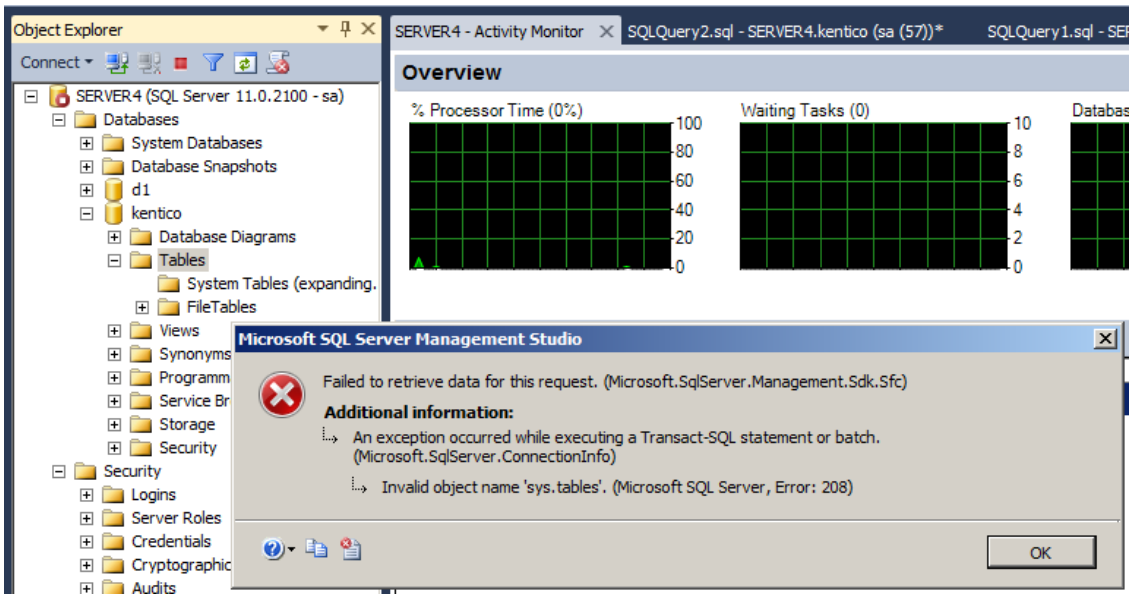

Nachdem wir ein Passwort eingegeben und die Datenbank verschlüsselt haben, bietet der Verschlüsseler an, vorhandene Anwendungen zu konfigurieren, um nur auf die verschlüsselte Datenbank zuzugreifen. Sie können sie auch wieder entschlüsseln, wann immer Sie möchten.

Aber schauen wir uns an, wie die KMS auf die Verschlüsselung der Datenbank reagiert und öffnen die Website wieder:



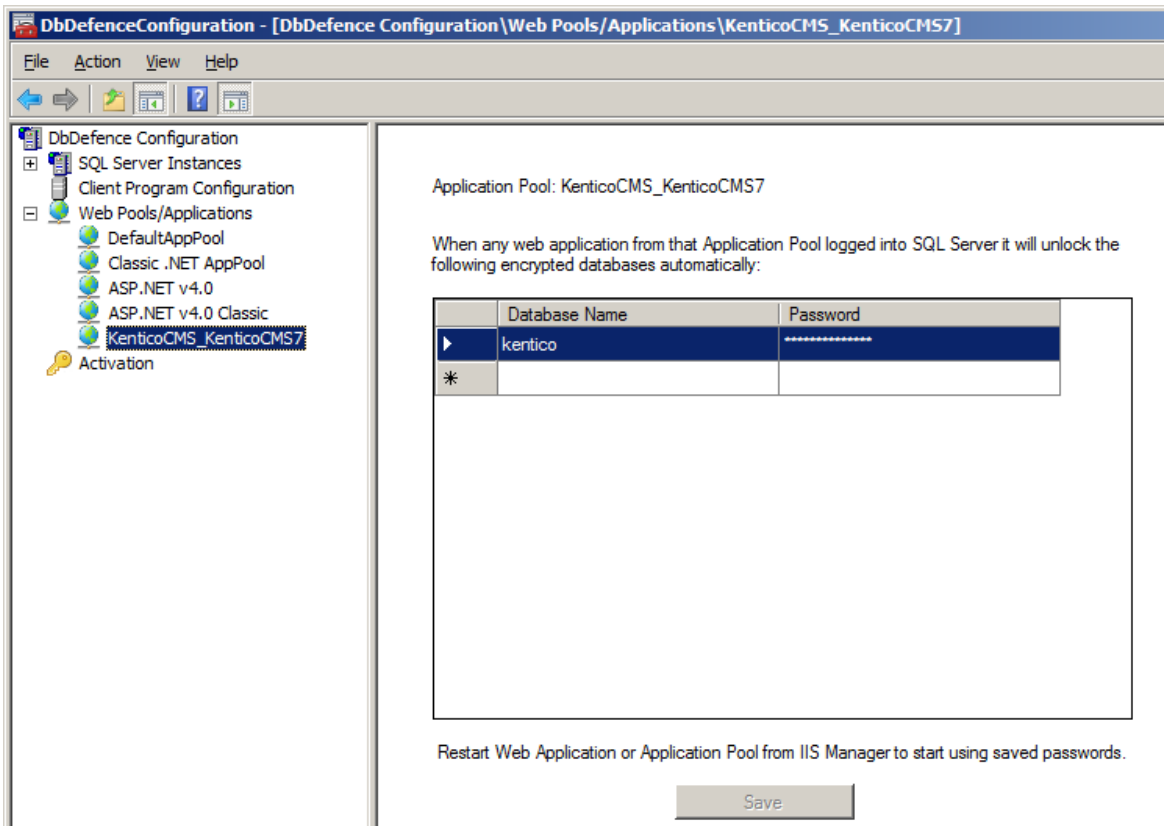
Das KMS kann nicht auf die Datenbank zugreifen, aber die Programmierer behandeln diese Ausnahme professionell und bieten Ihnen an, eine neue Datenbank einzurichten. Wir sehen also, dass die alte Datenbank nicht mehr benutzt werden kann.

Wenn jemand versucht, direkt mit SSMS auf die Kentico-Datenbank zuzugreifen, gibt es keine Tabellen:

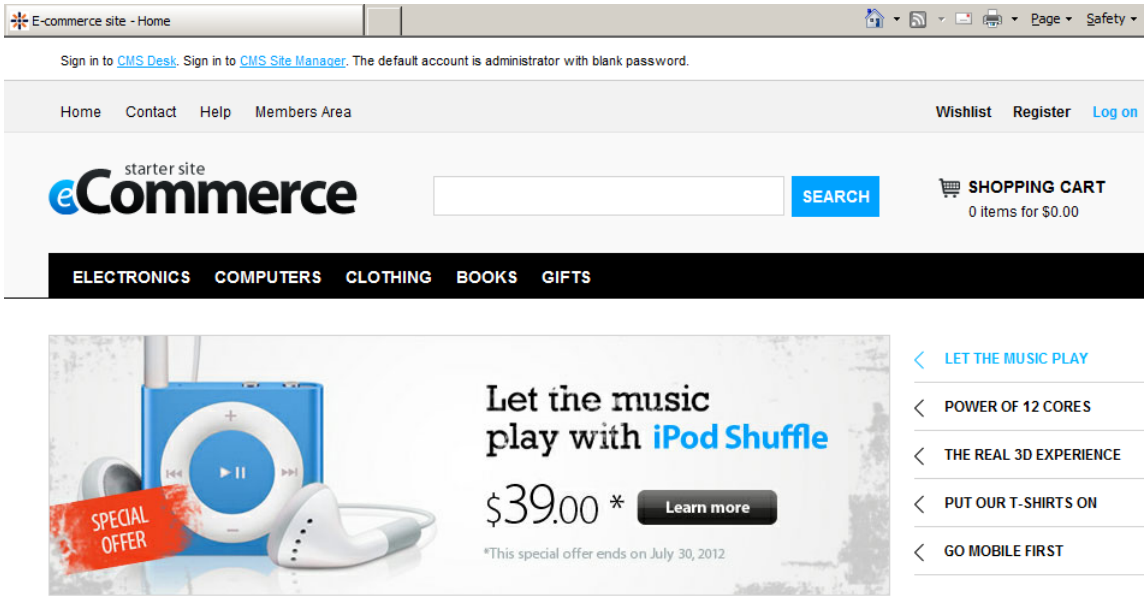



Die Datenbank ist somit für alle nicht autorisierten Anwendungen geschlossen.

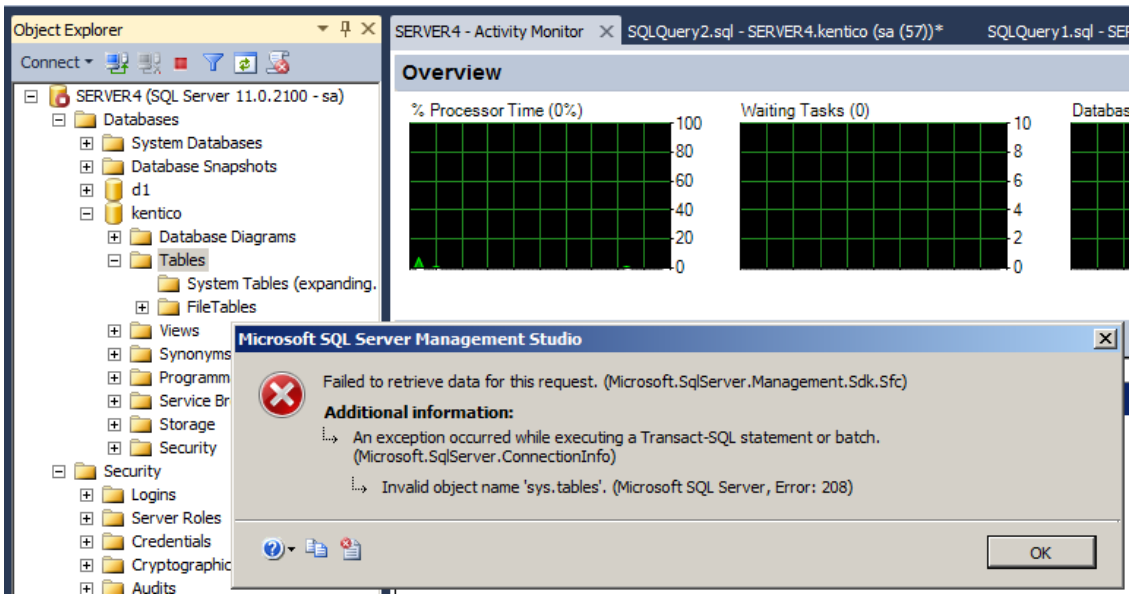
Lassen Sie uns nun das KMS autorisieren, um die gesperrte Datenbank verwenden zu können. Wir müssen den DbDefence-Konfigurator aufrufen und den Namen der Datenbank und das Passwort, welches wir für die bisherige Verschlüsselung benutzt haben, eingeben. Der Konfigurator zeigt die vorhandenen Datenbanken an. Glücklicherweise erstellt Kentico seinen Namen automatisch, so dass wir nicht raten müssen, mit welchem Programm wir es zu tun haben. Geben Sie den Namen der Datenbank und das Passwort ein, und drücken Sie „Speichern“.




Starten Sie die Website vom IIS-Manager aus, und öffnen Sie die Kentico-Website erneut. Wie Sie sehen, läuft sie jetzt, als wäre nichts geschehen.



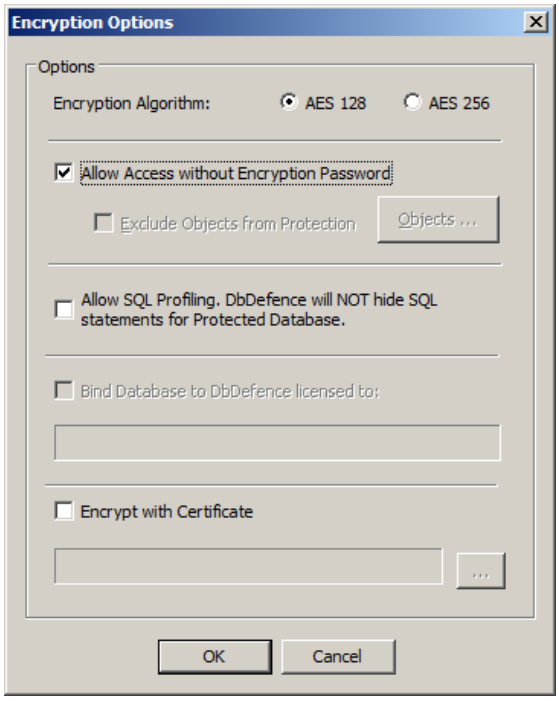

Der Versuch, zur gleichen Zeit mit SSMS auf die Datenbank zuzugreifen, wird uns immer noch eine Fehlermeldung anzeigen:



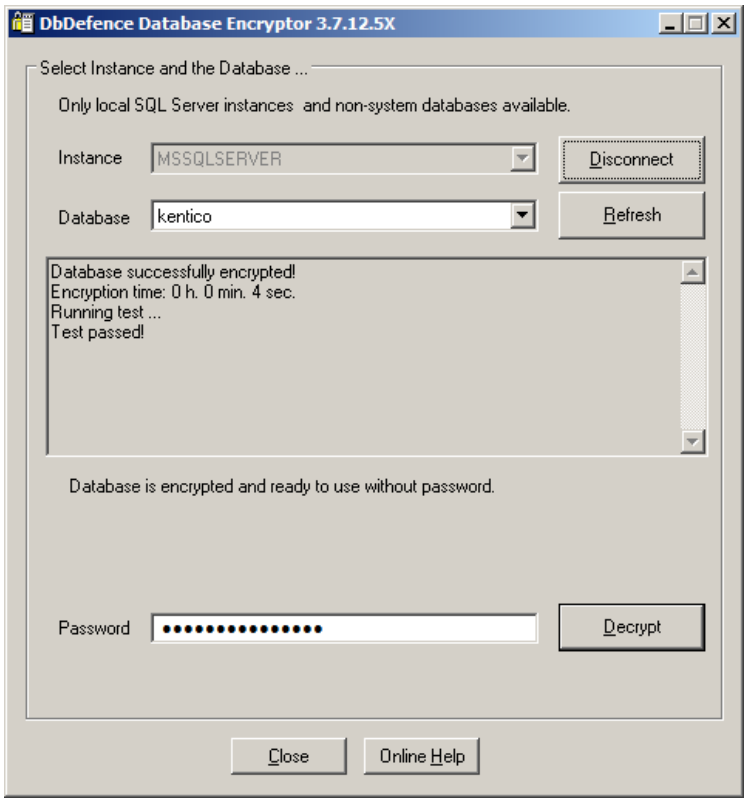

Wenn Sie möchten, dass SSMS im „ungesperrten“ Modus auch läuft, müssen Sie im Konfigurator im Abschnitt „Kunde Programm-Konfiguration“ die ssms.exe hinzufügen (im Hauptordner der SSMS-Anwendung zu finden) und auf die gleiche Weise die Datenbank und das Passwort zuweisen.

ALTERNATIV, wenn Sie nur Dateien verschlüsseln aber NICHT DEN ZUGRIFF AUF ANWENDUNGEN BESCHRÄNKEN möchten, müssen Sie vor der Verschlüsselung eine spezielle Option einrichten.

Drücken Sie vor dem Verschlüsseln einer Datenbank „Optionen ändern“, und markieren Sie die Box „Zugriff ohne Verschlüsselungspasswort erlauben". Darüber hinaus können Sie den Verschlüsselungsalgorithmus auf AES-256 verstärken.




Nachdem Sie die Datenbank mit dem „Zugriff erlauben“-Parameter verschlüsselt haben, wird der Verschlüsseler Ihnen die Zugriffskonfiguration nicht anbieten, da es keine Änderungen der Zugriffsberechtigungen gab.




Das heißt, Sie müssen keine Daten eingeben, um das Kentico KMS und SSMS laufen zu lassen, aber die Dateien bleiben verschlüsselt. Um das zu überprüfen, sollten Sie zunächst eine Sicherheitskopie der Datenbank anfertigen und auf einem anderen Server speichern.

Das ist alles, wir wünschen Ihnen einen schönen Tag!

Wenn Sie Fragen haben, wenden Sie sich bitte an support@dbdefence.com