Protección para la base de datos CRM de GoldMine utilizando DbDefence

Versión 1.0, 1 junio 2013

Introducción

Representando la columna vertebral de toda empresa digital, las bases de datos son esenciales para el funcionamiento de las organizaciones, sin importar si se trata de enormes entidades corporativas o pequeñas empresas manejadas desde oficinas en casa. Por esta razón, es extremadamente importante que las bases de datos cuenten con protección. Este reporte explicará cómo lograrlo, aún si no está familiarizado con la administración de bases de datos y la programación.

GoldMine es una popular solución de Administración de la Relación con el Cliente (CRM, por sus siglas en inglés) que se utiliza actualmente en el mundo entero, frecuentemente con fines de almacenamiento de datos importantes. Con delitos digitales aumentando año con año, el cifrado de la información nunca había sido tan importante para la protección de sus bases de datos, y por supuesto, de la información contenida en éstas.

Para este reporte utilizamos la versión gratuita de GoldMine que cuenta con un periodo de 30 días de evaluación, la cual incluye datos de demostración para propósitos de prueba, y para permitir a los potenciales clientes examinar el software sin tener que ingresar sus propios datos para lograr saber cómo es su desempeño. También hay una versión gratuita de DbDefence que es capaz de trabajar con bases de datos de hasta 200 MB de tamaño. Por otra parte, la versión de paga de DbDefense puede descargarse del sitio www.dbdefence.com. Si está interesado en nuestro producto, contamos con una amplia gama de opciones de precios, dependiendo del tamaño de su base de datos. Nuestros precios comienzan desde $698 por servidor.

Cifrado Transparente

Si alguien intentara hackear el servidor, tendría problemas leyendo la información contenida en la base de datos, y hasta tendría problemas para robarla por completo, puesto que un contenido con un formato legible y claro únicamente podría ser visualizado adjuntando la base de datos a SQL Server.

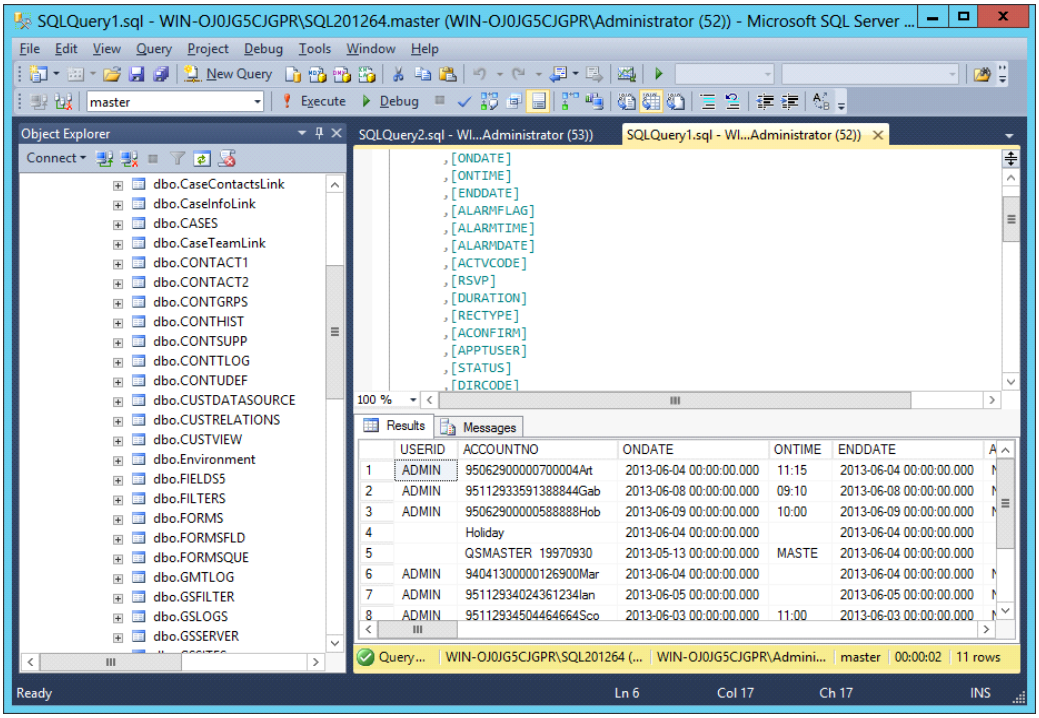

Fig. 1 - Cómo luce una consola de administración de SQL Server cuando se encuentra en el proceso de consulta de datos. Un administrador SQL tiene acceso a todo el contenido en la base de datos.

DbDefence tiene la habilidad de proporcionar características de cifrado transparente para cualquier instancia de SQL Server – incluyendo versiones modernas – sin la necesidad de modificar las aplicaciones que usted utiliza para acceder a dicha base de datos. Este reporte le explicará cómo usar DbDefence para lograr esta tarea.

Hay una característica similar, llamada TDE (Cifrado de Datos Transparente) que está disponible en SQL Server Enterprise Edition, sin embargo, el precio por la Enterprise Edition obviamente resulta una propuesta poco realista para las pequeñas empresas.

Instalación

Para comenzar, necesitará instalar DbDefence [Fig. 2]. Descargue la versión de prueba desde www.dbdefence.com, si aún no lo ha hecho. DbDefence debe estar instalado en la misma computadora desde donde opera SQL Server. La instalación en sí es bastante sencilla, pero lo guiaremos mediante una serie de pasos.

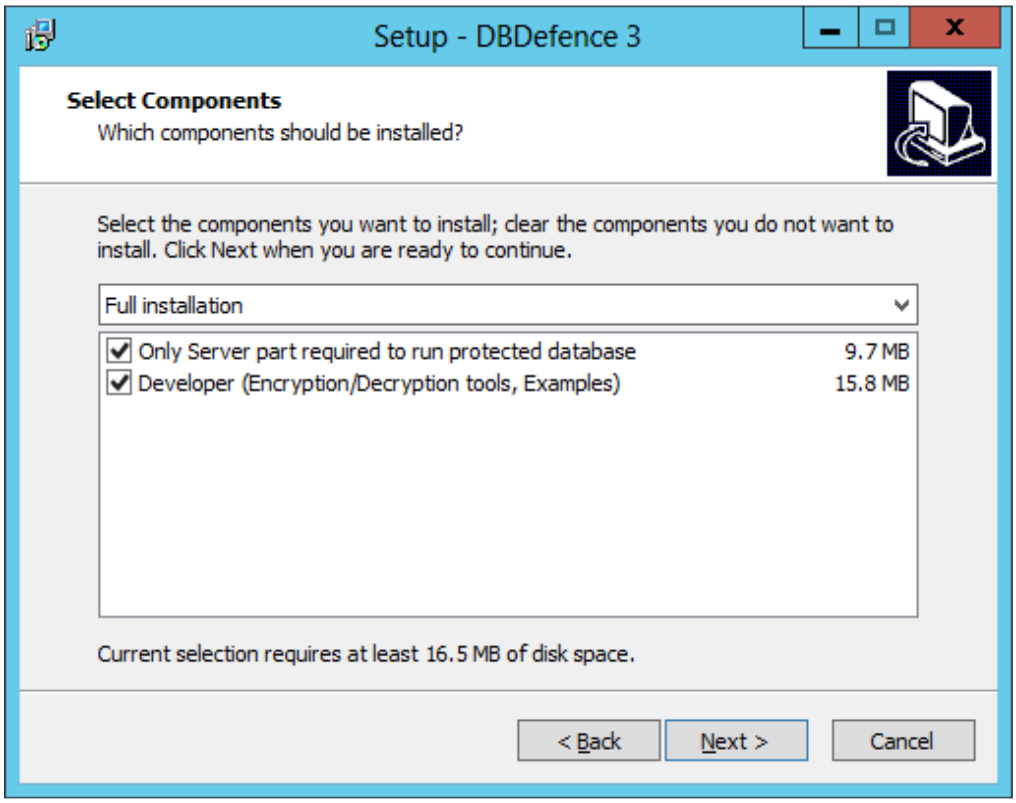

Fig. 2 - Instalación de DbDefence— Pantalla de selección de componentes

La instalación le pedirá que ingrese a SQL Server [Fig. 3], y le proporcionará una lista de instancias de SQL Server instaladas localmente de entre las cuales elegir. Simplemente necesita ingresar la instancia de SQL Server que desea proteger. Debe ingresar como administrador para contar con acceso completo al instalador de DbDefence.

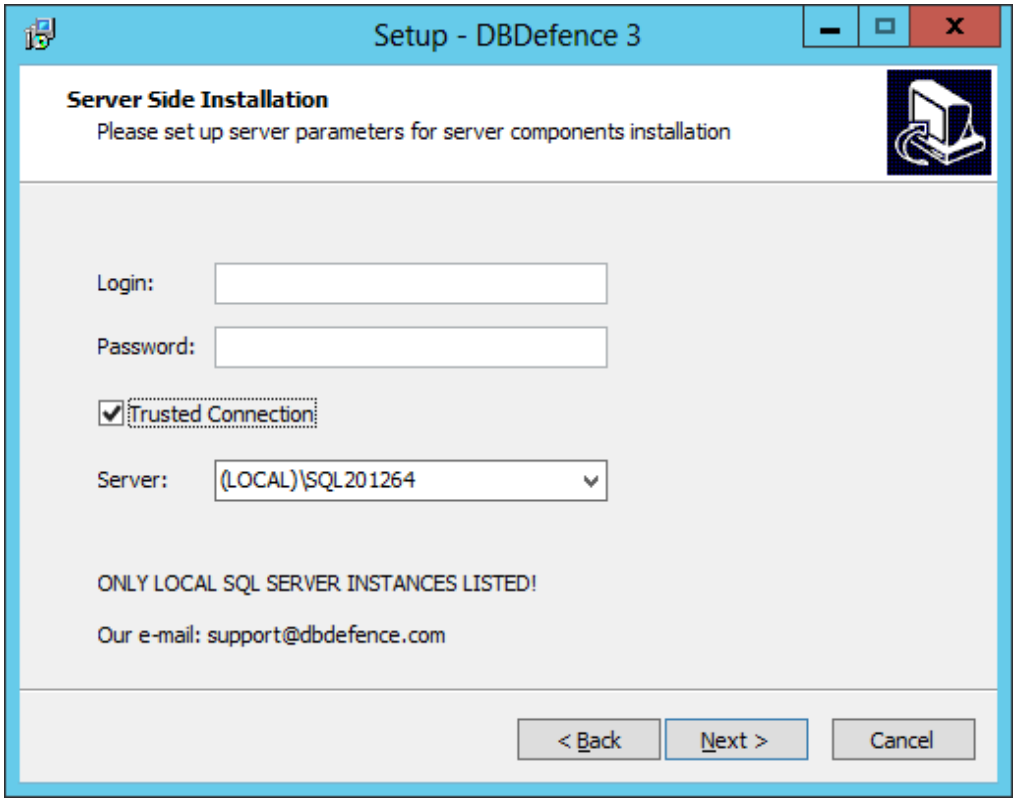

Fig. 3 - DbDefence Installation—Logging in to target SQL Server

Después de que haya ingresado al Servidor SQL deseado, no es necesaria ninguna configuración posterior en el proceso de instalación. Simplemente haga clic en Next, y la instalación continuará. Una vez que finalice, podrá ver una pantalla final [Fig. 4], informándole que la instalación ha sido completada (en esta pantalla también se le notificará si la instalación falló). Tan sólo haga clic en Finish para cerrar el instalador.

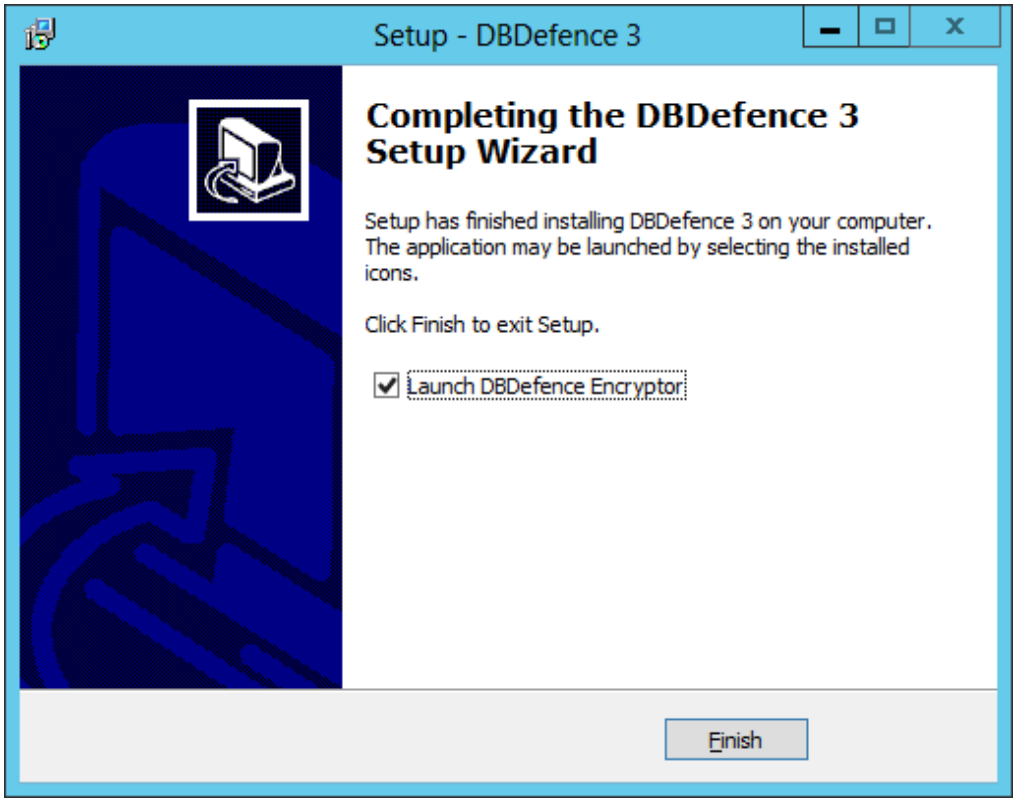

Fig. 4 - Instalación de DbDefence— Pantalla final. Puede elegir abrir DbDefence inmediatamente después de que el instalador se cierre, seleccionando la casilla indicada.

Una vez que la instalación se haya completado, necesitará ejecutar DbDefence Encryptor. Si eligió “Launch DbDefence Encryptor” [Fig. 4] en la última pantalla del proceso de instalación, el software se abrirá por sí mismo cuando el instalador se cierre. De otra manera, simplemente localice el acceso directo en el menú de Inicio.

Cifrado y Descifrado

Una vez que DbDefence Encryptor se está ejecutando, conéctese a la instancia de SQL Server con la que desea trabajar, podrá observar una ventana con información [Fig. 5]. Recuérdelo, la versión gratuita de DbDefence Encryptor tan sólo trabaja con bases de datos de hasta 200 MB de tamaño, pero, puesto que este reporte tiene como objetivo llevarlo de la mano a lo largo del proceso, es recomendable que utilice bases de datos pequeñas de ejemplo para comenzar. El proceso es sencillo, y no requiere de mucho tiempo, así que será fácil repetir los pasos a continuación en la base de datos que desee utilizar.

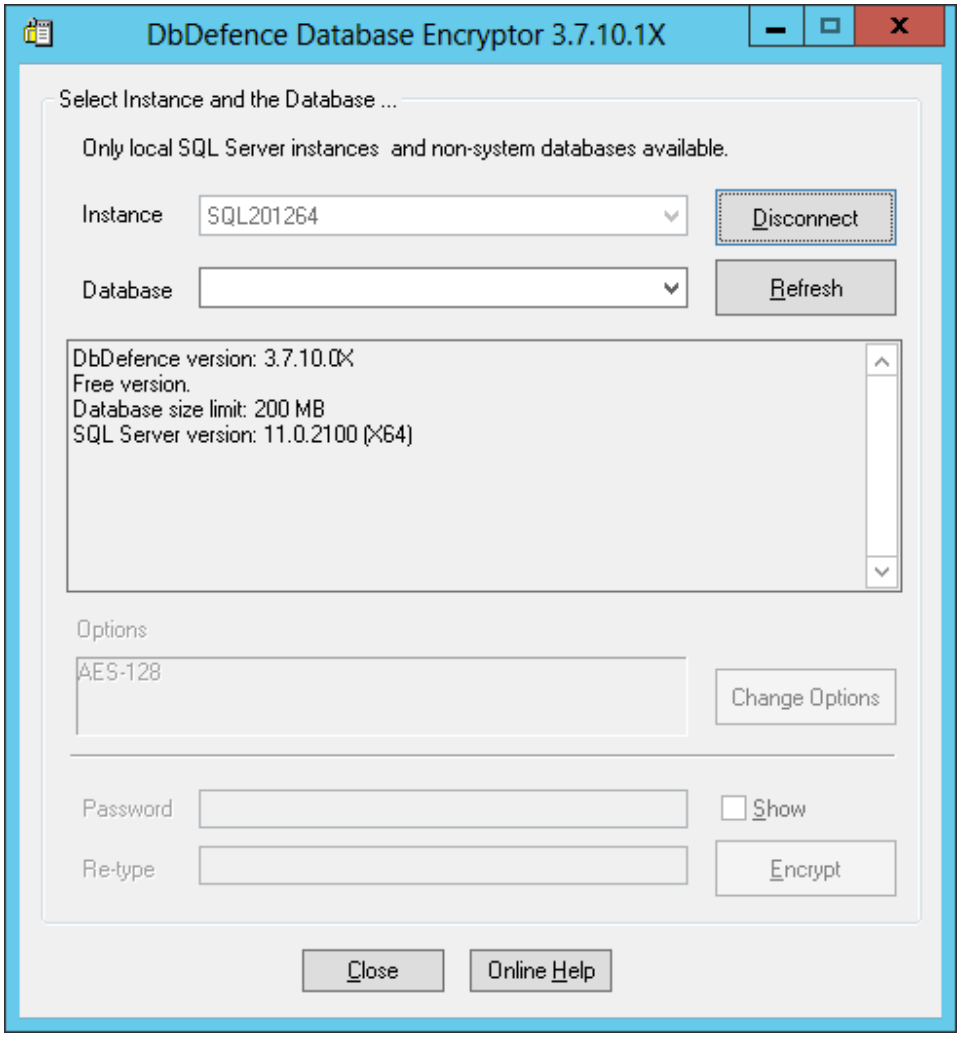

Fig. 5 - Pantalla de selección de instancia de DbDefence Encryptor. Aquí tendrá que seleccionar la instancia de la base de datos con la que desea trabajar. (La base de datos debe ser menor de 200 MB en la versión gratuita)

Una vez que haya seleccionado la instancia apropiada de SQL Server que desea cifrar, necesitará seleccionar la base de datos en la casilla desplegable correspondiente, la cual se localiza debajo de la casilla desplegable donde seleccionó la instancia de SQL Server [Fig. 6]. El método de cifrado predeterminado es AES 128-bit, AES es el método de cifrado predeterminado en EUA y el mundo entero. Las letras son las iniciales de Advanced Encryption Standard. Para la mayoría de los casos, un cifrado de 128-bit es suficiente. Sin embargo, si se necesita un cifrado mayor, también puede trabajar con 256-bit. Puede cambiar la forma de cifrado haciendo clic en el botón Change Options, el cual se localiza justo debajo de la casilla de información [Fig. 6]. Esto abrirá la ventana de diálogo de Opciones de Cifrado (128-bit y 256-bit). Simplemente seleccione el cifrado que desea utilizar y haga clic en OK. Hay más opciones en esta ventana de diálogo, pero hablaremos de éstas posteriormente.

Finalmente, necesita ingresar una contraseña. Esta contraseña es la clave para acceder a la base de datos una vez que haya sido cifrada, así que es importante que memorice su contraseña – no hay disponible una característica de “Reestablecimiento de contraseña” en el proceso de cifrado. También es importante que ingrese una contraseña segura, no solamente para propósitos de seguridad, también porque las políticas de

SQL Server (depende del sistema operativo) pueden rechazar aceptar contraseñas que se consideren muy débiles. Una contraseña segura debe contener caracteres en mayúsculas y minúsculas, así como al menos un número y un símbolo.

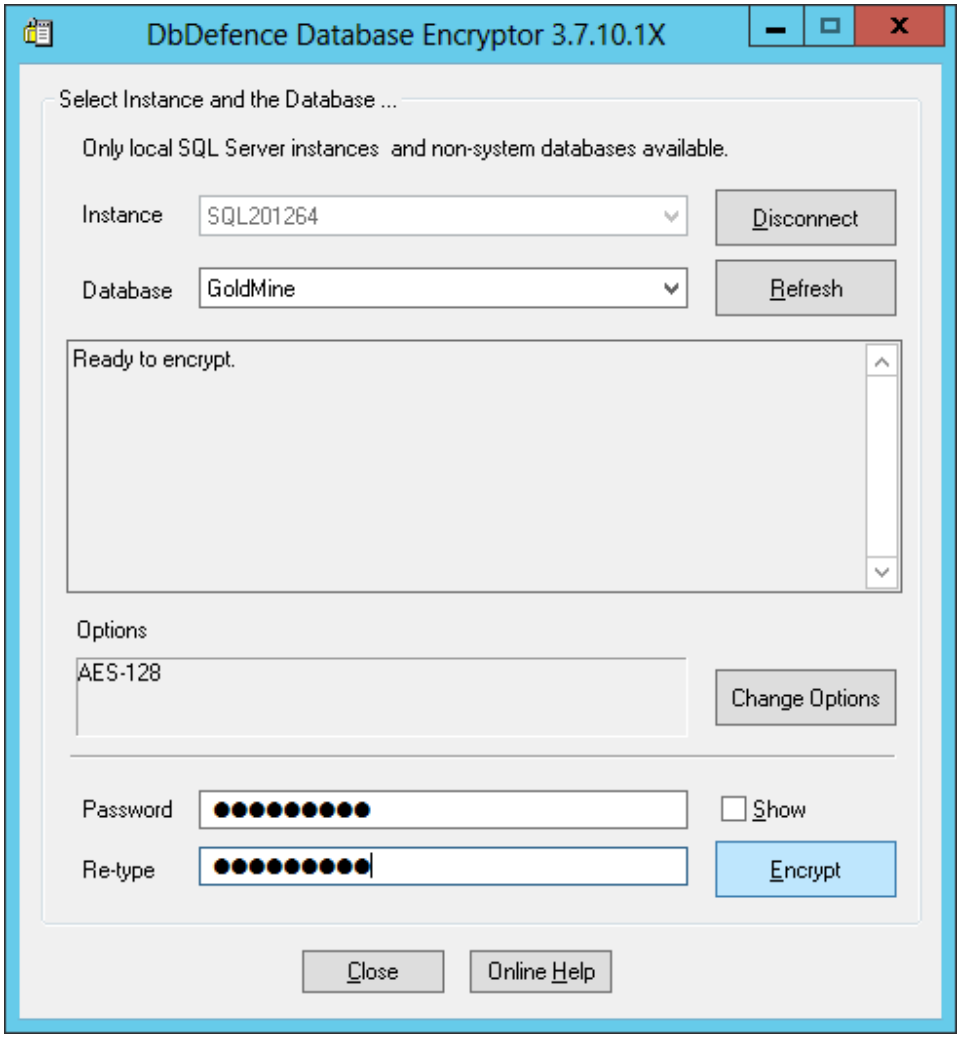

Fig. 6 - Nuevamente, la pantalla de selección de instancia, esta vez con toda la información requerida.

Hoy en día, las máquinas modernas llevan a cabo eficientemente las rutinas de cifrado, las cuales están optimizadas para procesadores modernos, y esto significa que dichas rutinas se ejecutan muy rápidamente en las nuevas computadoras. Una base de datos de 40 GB, por ejemplo, puede cifrarse en aproximadamente siete minutos. Al concluir, la base de datos estará completamente cifrada incluyendo el archivo de registro. A partir de este punto, el acceso a la base de datos sin la contraseña de cifrado es prácticamente imposible (es posible violar el cifrado, pero es muy, muy difícil, y requiere de mucho tiempo y recursos).

A través de la misma ventana de diálogo que utilizó para cifrar su base de datos, cuando se ha seleccionado una base de datos que ya ha sido cifrada, se le proporcionará la opción de descifrar dicha base de datos, lo cual puede realizar fácilmente. Simplemente ingrese la contraseña que estableció en el paso anterior y haga clic en Decrypt [Fig. 7]. DbDefence descifrará la base de datos, restaurándola a su estado previo.

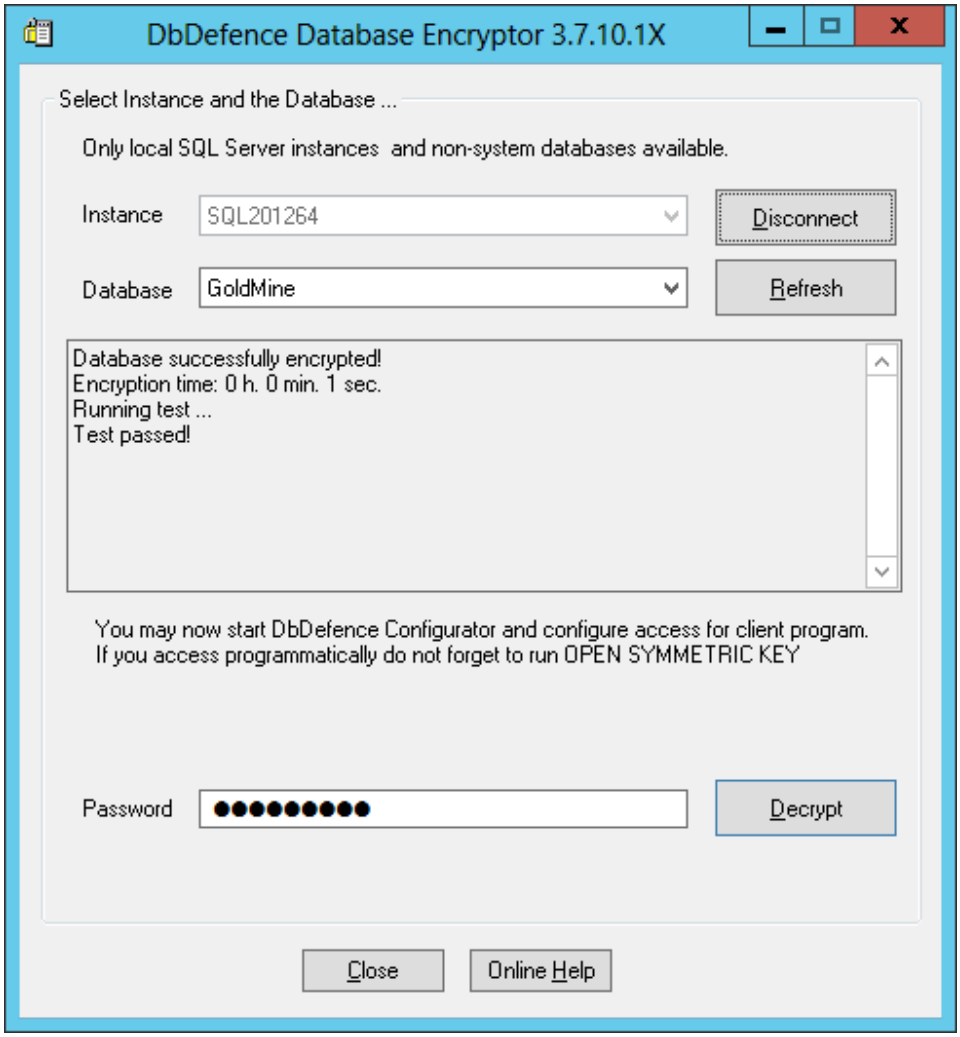

Fig. 7 - DbDefence mostrando que la basa de datos ha sido cifrada correctamente.

Utilización de una base de datos cifrada y protegida

Ahora que su base de datos ha sido cifrada, el acceso queda restringido únicamente a aquellas aplicaciones y servicios que puedan proporcionar la contraseña correcta. Esto incluye cualquier aplicación que intente acceder a la base de datos, y también a los administradores de la base de datos. Abrir el archivo de base de datos tal cual se encuentra, únicamente revelará una serie de códigos indescifrables e ilegibles. Intentar

visualizar el contenido de la base de datos sin la contraseña correcta hará que se muestre un mensaje de error [Fig 8].

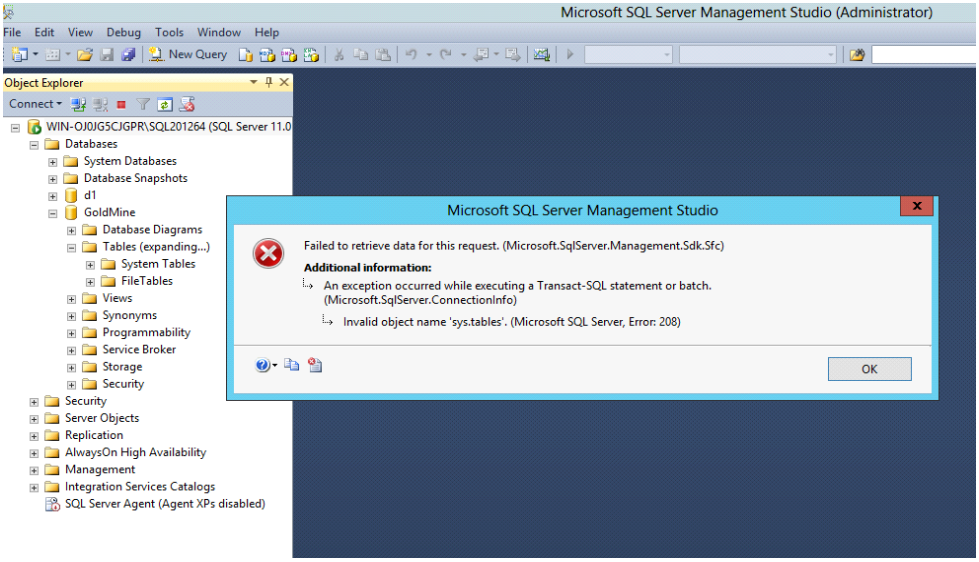

Fig. 8 – Un error generado al intentar visualizar el contenido de una base de datos cifrada sin la contraseña correcta.

Una vez que la base de datos haya sido cifrada, si inicia GoldMine como siempre lo hace, deberá recibir un mensaje de error que le indicará que el inicio de sesión no pudo completarse debido a que la tabla de USUARIOS está vacía [Fig. 9]. Esto se debe a que, sin la contraseña de cifrado, GoldMine no puede interpretar los datos que observa.

Fig. 9 – Mensaje de error de GoldMine generado al intentar ingresar después de cifrar la base de datos.

No obstante, la base de datos aún se encuentra en un estado completamente funcional, y las aplicaciones autorizadas funcionarán correctamente con la base de datos, aunque DbDefence necesita saber qué aplicaciones tienen permiso para poder descifrar la base de datos para dichas aplicaciones.

Ahora necesitaremos “aprobar” la aplicación GoldMine para que pueda acceder a los datos dentro de la base de datos cifrada. Si usted es un programador, llevar a cabo esto no requiere más que de un solo argumento SQL en su código. Sin embargo, debido a que este reporte ha sido escrito para personas sin conocimiento en programación que podrían estar utilizando una aplicación (como GoldMine), daremos por hecho que usted no es un programador.

Requerimiento de Contraseña

Primero, inicie la Configuración de DbDefence. En el panel de la izquierda, localice *Client Program Configuration*, y haga clic encima. En el menú contextual que aparece, elija “Add Program” [Fig. 10], desde allí, se puede agregar cualquier programa de escritorio, pero utilizaremos a GoldMine para nuestro ejemplo.

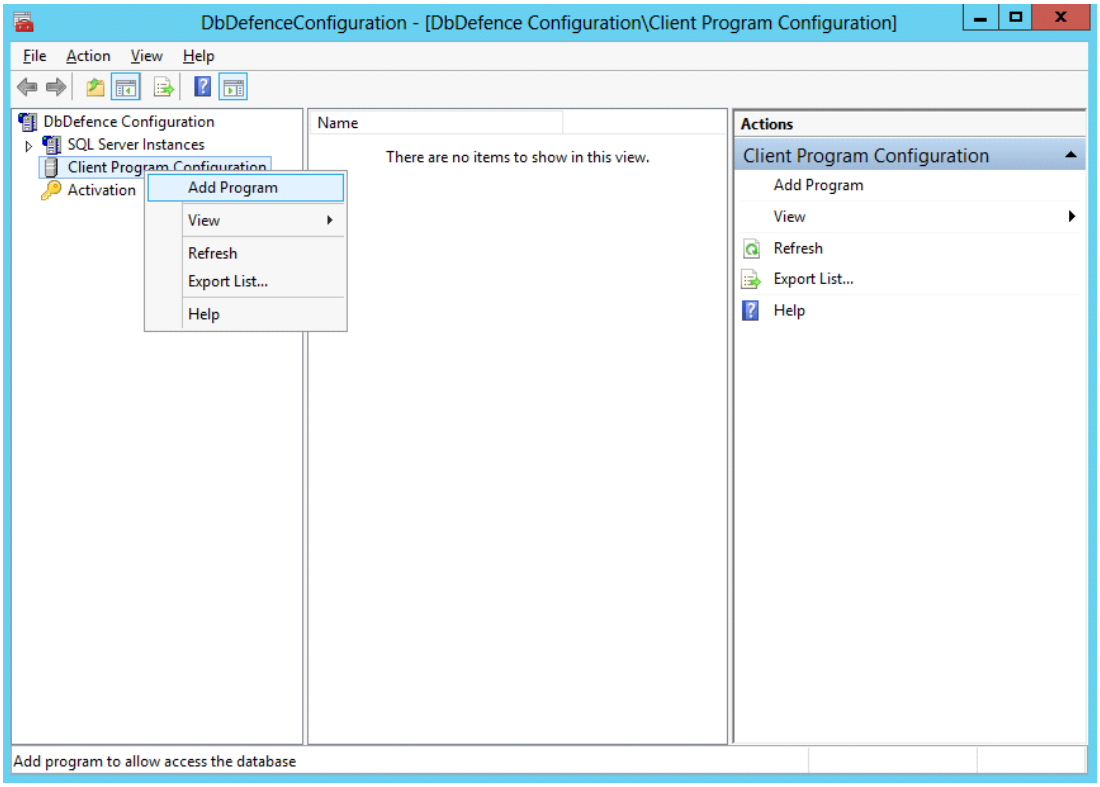

Fig. 10 – Ventana de configuración de DbDefence. Haga clic derecho en “Client Program Configuration”, y posteriormente en “Add Program”

En la ventana *Open*, navegue hacia la carpeta de instalación de GoldMine. Aquí es donde han sido instalados los archivos de programa de GoldMine. La dirección debe lucir similar a "C:\Archivos de Programa\GoldMine\". Una vez allí, debe observar un archivo llamado *gmw.* Seleccione ese archivo. Se trata del archivo ejecutable principal de la aplicación GoldMine. Cuando lo haya seleccionado, haga clic en Abrir.

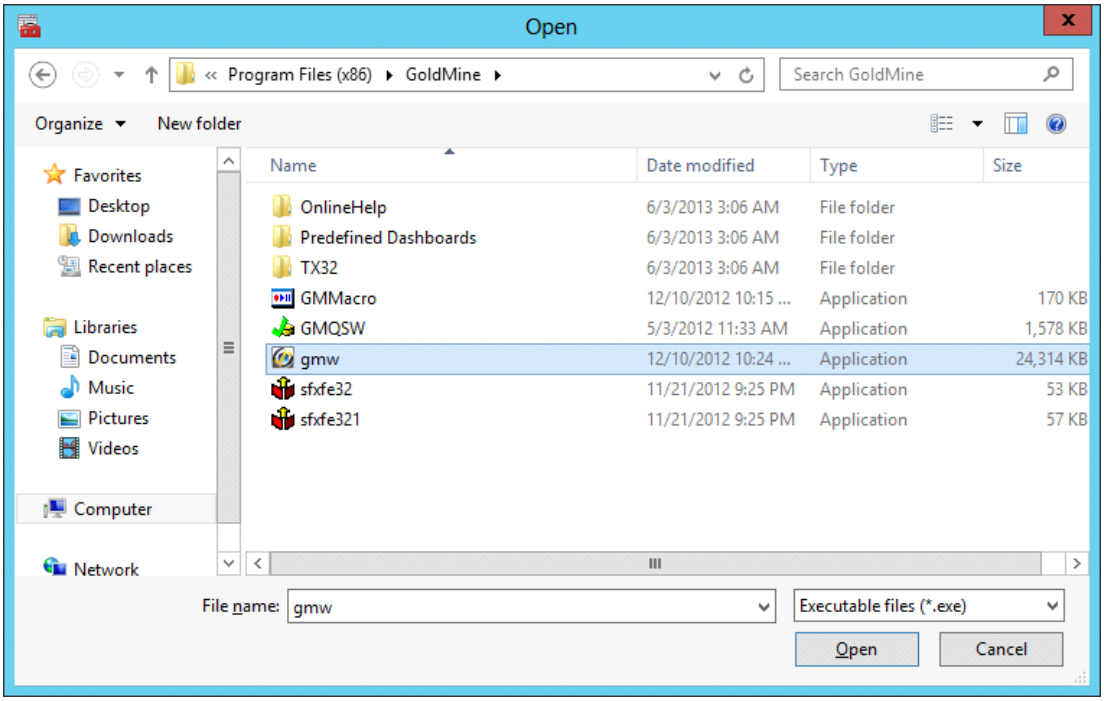

Fig. 11 – La ventana *Open*, con el archivo ejecutable de GoldMine seleccionado.

Una vez que ha seleccionado y abierto *gmw.exe*, podrá observar un nuevo panel de diálogo dentro de la ventana de Configuración de DbDefence [Fig. 12]. Allí puede establecer los parámetros de manera que GoldMine ingrese automáticamente la contraseña de cifrado siempre que intente acceder a la base de datos, ingresando el nombre de la base de datos y la contraseña en los campos apropiados, un procedimiento que explicaremos posteriormente en este documento. Sin embargo, para los propósitos de este ejercicio, ignore ese aspecto, y simplemente seleccione la casilla "Show Password Dialog", y posteriormente presione *Start !* para ejecutar GoldMine.

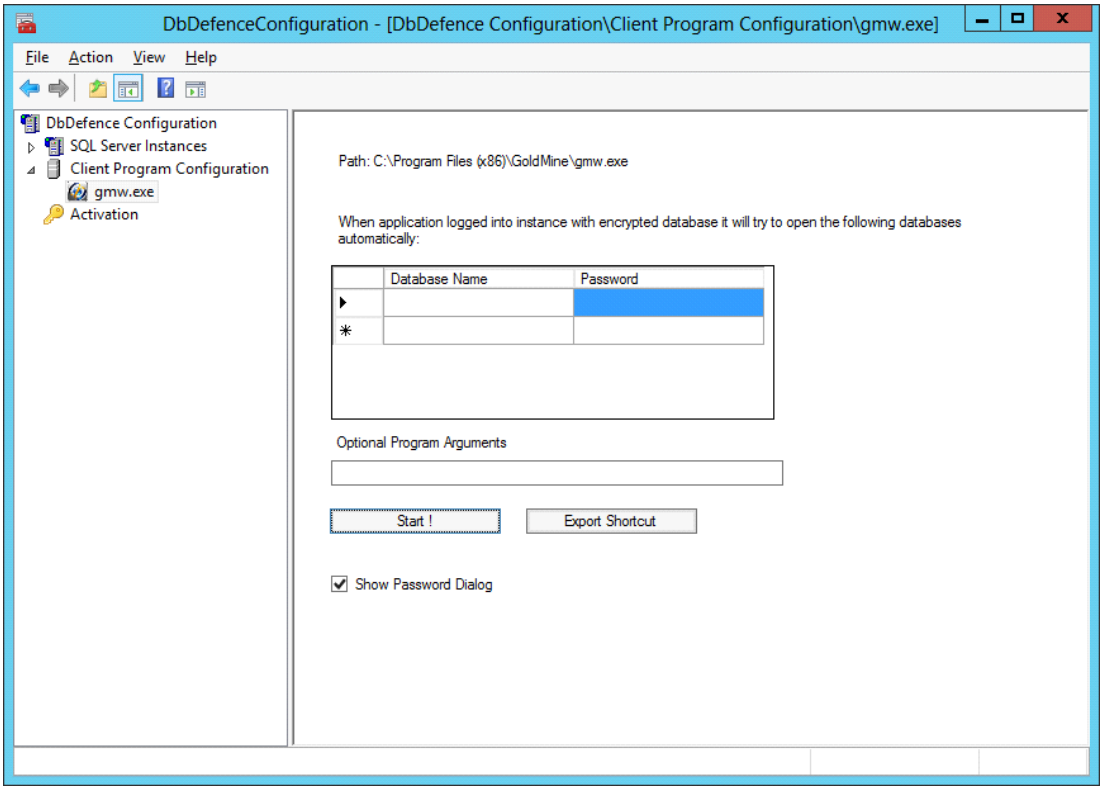

Fig. 12 – Elija la manera como GoldMine accederá a la base de datos cifrada – automáticamente o con confirmación.

Ahora, cuando se abra GoldMine, e intente establecer una conexión con su base de datos cifrada, se mostrará una caja de diálogo de DbDefence requiriendo una contraseña [Fig. 13]. Asegúrese de seleccionar la base de datos correcta para desbloquear, e ingresar la contraseña en el campo debajo de la casilla desplegable.

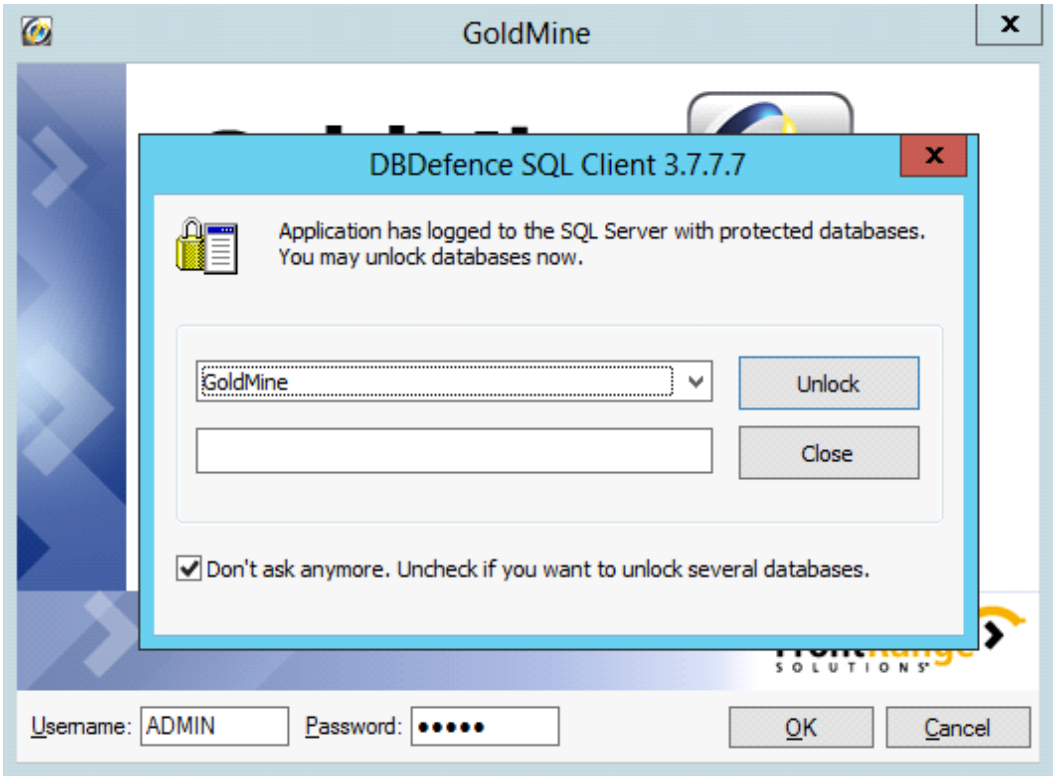

Fig. 13 – Una vez que GoldMine tiene aprobación, aparecerá la caja de contraseña de DbDefence cuando GoldMine intente acceder a la base de datos.

Seleccionando la base de datos correcta e ingresando la contraseña correcta, haga clic en Unlock. Ahora que GoldMine cuenta con autorización, cargará la base de datos de manera normal, mostrando su contenido como si estuviera trabajando con una base de datos sin ningún tipo de cifrado [Fig. 14]. Mientras tanto, si intentamos acceder a la base de datos con SQL Server Management Console, recibiremos un mensaje de error de acceso denegado [Fig. 15], ya que SSMS no cuenta con acceso asignado en DbDefence para ingresar a la base de datos.

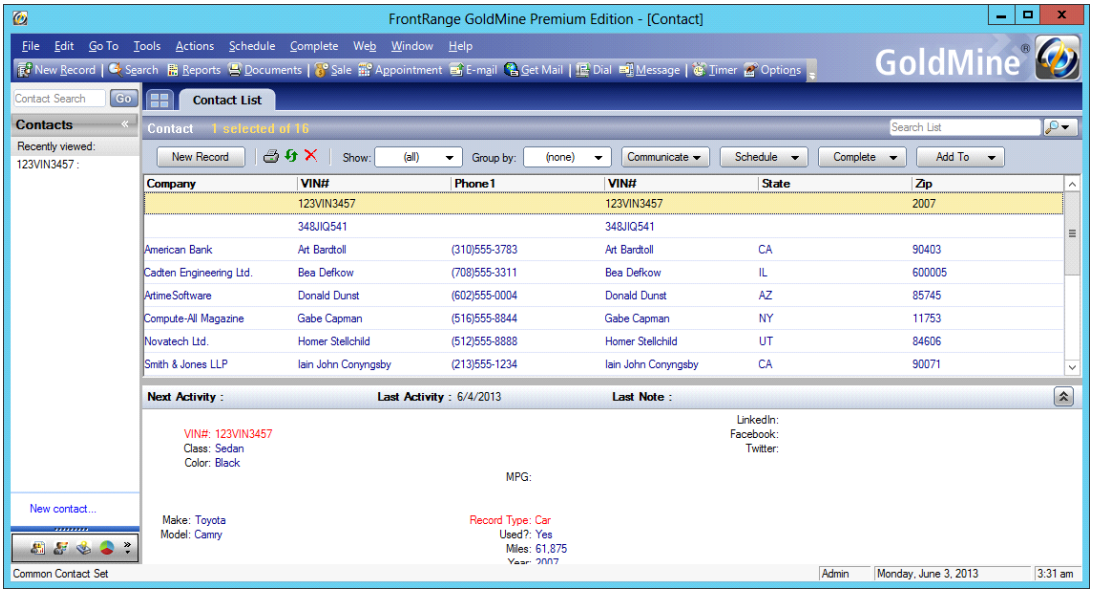

Fig. 14 - GoldMine funcionando de manera normal con la base de datos contando con cifrado.

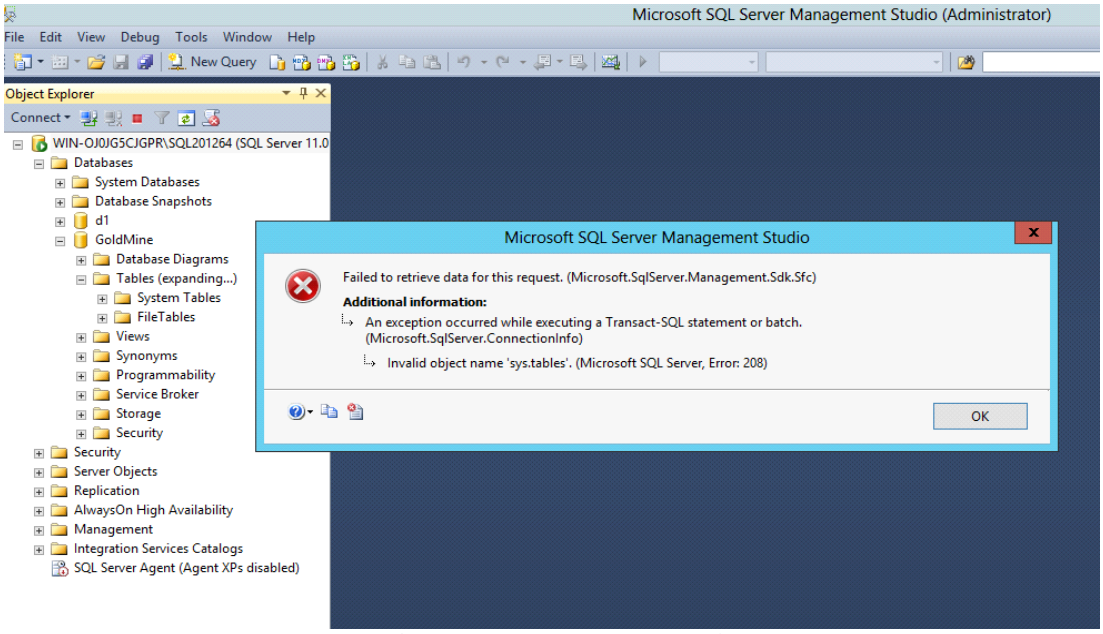

Fig. 15 -Mientras que GoldMine está accediendo a la base de datos cifrada, SQL DBA no lo puede lograr.

Ingreso Automático

Si usted está trabajando desde un sistema seguro, quizá le parezca una molestia innecesaria tener que ingresar su contraseña cada vez que quiere acceder a la base de datos. Por fortuna, como lo mencionamos anteriormente, puede hacer que DbDefence reconozca ciertas aplicaciones e ingrese la contraseña de manera automática cualquier número de veces para acceder a la base de datos cifrada.

Para llevar a cabo esto, necesitará regresar a la Configuración de DbDefence, y, en el panel a la izquierda, localice Client Program Configuration. *gmw.exe* debe encontrarse justo debajo. Si no puede observar a gmw.exe, haga clic en Client Program Configuration para expandir el menú. Ahora debe estar observando la misma pantalla que veía al comienzo de esta sección, únicamente que esta vez, no necesita localizar y agregar a *gmw.exe* a la lista, porque esto ya lo ha realizado.

Esta vez, vamos a agregar las credenciales de acceso en los campos apropiados de la tabla en el centro del panel a la derecha [Fig. 16]. Tendrá que ingresar el nombre de la base de datos (probablemente GoldMine), y su contraseña de cifrado. En los casos cuando tiene múltiples bases de datos cifradas a las que desea permitir acceso, puede ingresar múltiples nombres de bases de datos y contraseñas en este recuadro. Una vez que lo haya realizado, desmarque la casilla “Show Password Dialog” para que no sea necesario ingresar una contraseña la próxima vez que intente acceder a la base de datos mediante GoldMine.

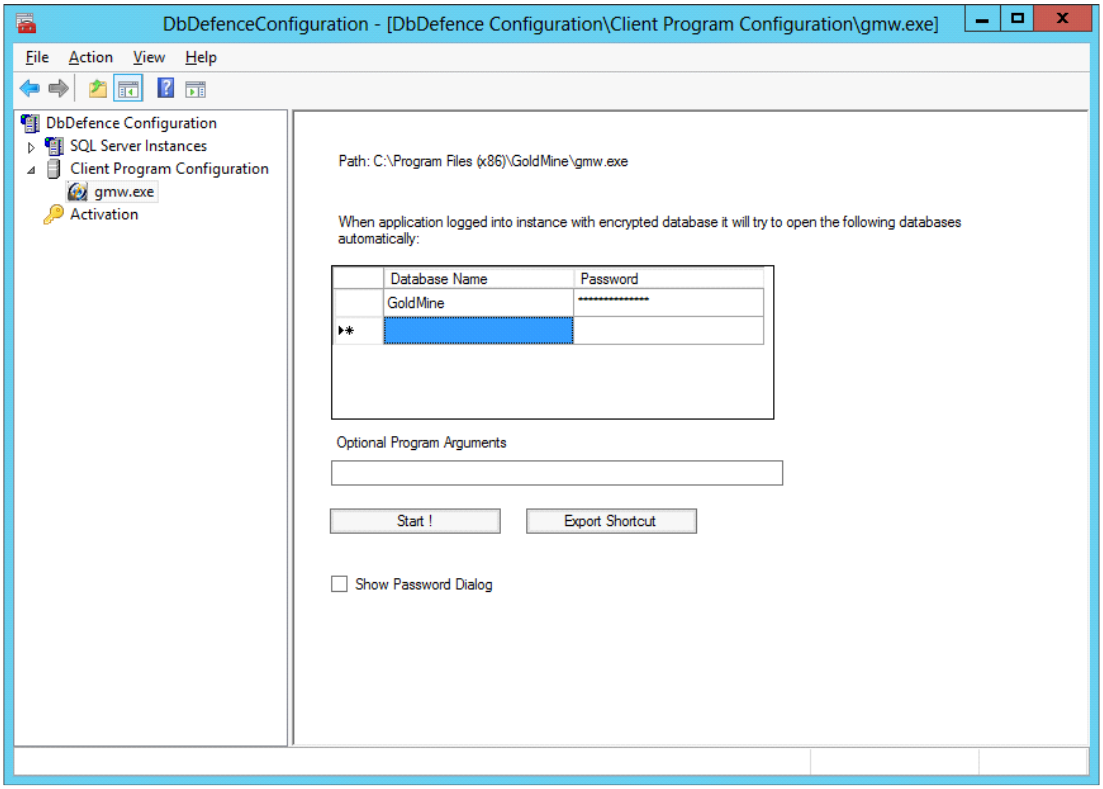

Fig. 16 - Ingreso de la contraseña para que las aplicaciones puedan tener acceso automático a la base de datos.

Ahora, si abre GoldMine haciendo clic en *Start !* en la ventana de configuración, se iniciará de manera normal, sin la necesidad de ingresar la contraseña para obtener acceso.

Creación de Acceso Directo

Si prefiriera no tener que abrir la Configuración de DbDefence cada vez que quiere acceder a su base de datos cifrada, puede crear un acceso directo [Fig. 17] que puede colocar en su escritorio. Sin embargo, al realizar esto, su contraseña quedará expuesta, pero este aspecto de esta opción será mejorado en versiones posteriores. Así que es importante asegurarse de que la ubicación del acceso directo sea un lugar seguro en cuanto al acceso de otros usuarios. Si coloca el acceso directo a su base de datos en el escritorio de una computadora compartida que también es utilizada por aquellas personas que quiere que *no* tengan acceso a la base de datos, sería suficiente tan sólo hacer clic en el acceso directo para que pudieran ingresar. Asegúrese de que su acceso directo por lo menos esté en su propia área de usuario protegida con contraseña, si es que no está en un sistema seguro que únicamente usted utiliza.

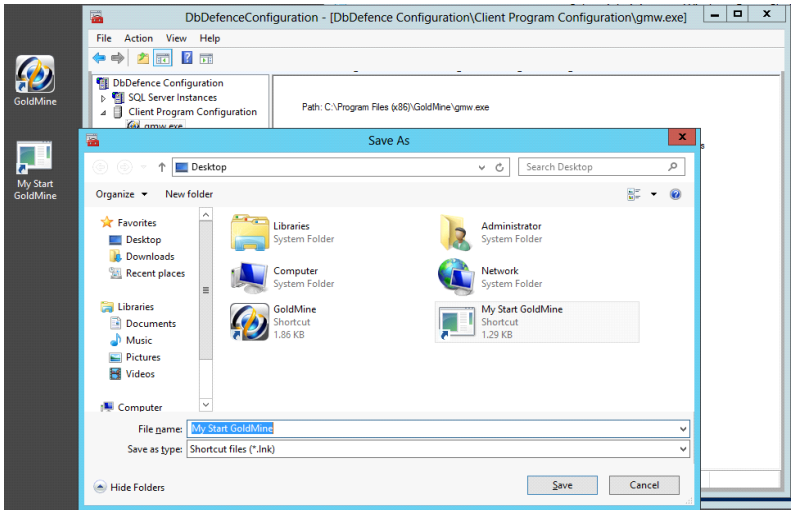

Fig 17 - Exportación de un acceso directo al escritorio para evitar tener que abrir DbDefence cada vez que se requiere acceder a la base de datos cifrada.

Acceder a su base de datos cifrada de esta manera es igual que acceder mediante la Configuración de DbDefence, sin la molestia de tener que abrir la Configuración de DbDefense. Este proceso es completamente transparente para la aplicación (GoldMine, en este caso).

Agregar una aplicación distinta a GoldMine es igual de sencillo, todo lo que necesita saber es el nombre y la ubicación del archivo ejecutable principal. Posteriormente hay que repetir los pasos descritos previamente, reemplazando *gmw.exe* con el archivo ejecutable de la aplicación que desea agregar. SQL Server Management Studio de SQL Server 2012 usualmente se localiza en "C:\Archivos de Programa (x86)\Microsoft SQL Server\110\Tools\Binn\ManagementStudio\ssms.exe" y SQL Server Management Studio de SQL Server 2008 en "C:\Archivos de Programa (x86)\Microsoft SQL Server\100\Tools\Binn\VSShell\Common7\IDE\ssms.exe"

Cifrado de bases de datos sin protección

Hay ocasiones en las que podría requerir cifrar archivos de bases de datos, sin que sea necesario restringir el acceso de o a través de ninguna aplicación o servicio Web. Afortunadamente, hay una característica en DbDefence que puede llevar a cabo esta tarea.

Al utilizar esta característica, puede especificar qué partes de la base de datos tienen permiso de acceder sin la contraseña de cifrado. Esto se realiza antes de que la base de datos sea cifrada, mediante la misma ventana de diálogo mencionada casi al principio de este documento, la cual utiliza para elegir entre un método de cifrado de 128-bit y uno de 256-bit.

En la ventana de selección de instancia [Fig. 6], haga clic en el botón *Change Options*. Esto le mostrará el cuadro de diálogo de Encryption Options [Fig. 18]. En el cuadro de diálogo de Encryption Options, marque la casilla *"Allow Access without Encryption Password"*.

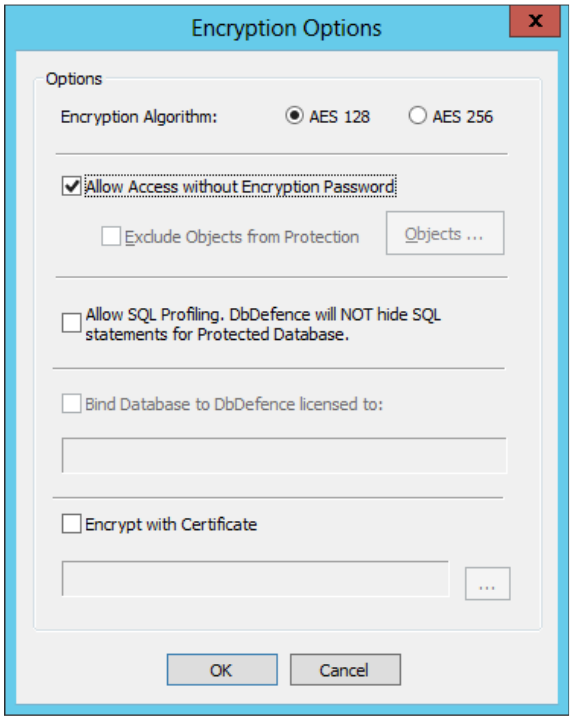

Fig. 18 – Cuadro de diálogo de Encryption Options.

Una vez que haya cifrado su base de datos con esta opción, será posible que cualquier aplicación acceda a la base de datos sin la contraseña de cifrado. Sin embargo, el archivo de base de datos *será* cifrado, lo que significa que si alguien (por ejemplo, un hacker) intentara descubrir el contenido de la base de datos con tan solo ver el archivo tal cual se encuentra, sería imposible sin la contraseña de cifrado.

Conclusión

La importancia de proteger sus datos no puede subestimarse en la actualidad, cuando el valor de la información, cualquiera sea la forma en la que se encuentre, se incrementa exponencialmente, aunque eso no significa que tenga que ser difícil proteger su valiosa información. Con nuestro software, puede asegurarse de que su base de datos (o la de su compañía) se encuentra completamente segura, sin la necesidad de contar con años de experiencia técnica y/o habilidades de programación.

Si está interesado en nuestro producto, contamos con diversas opciones de precios, dependiendo del tamaño de su base de datos. Los precios comienzan desde $698 por servidor.

Esperamos que este reporte haya sido de utilidad. *¡Gracias por su tiempo!*