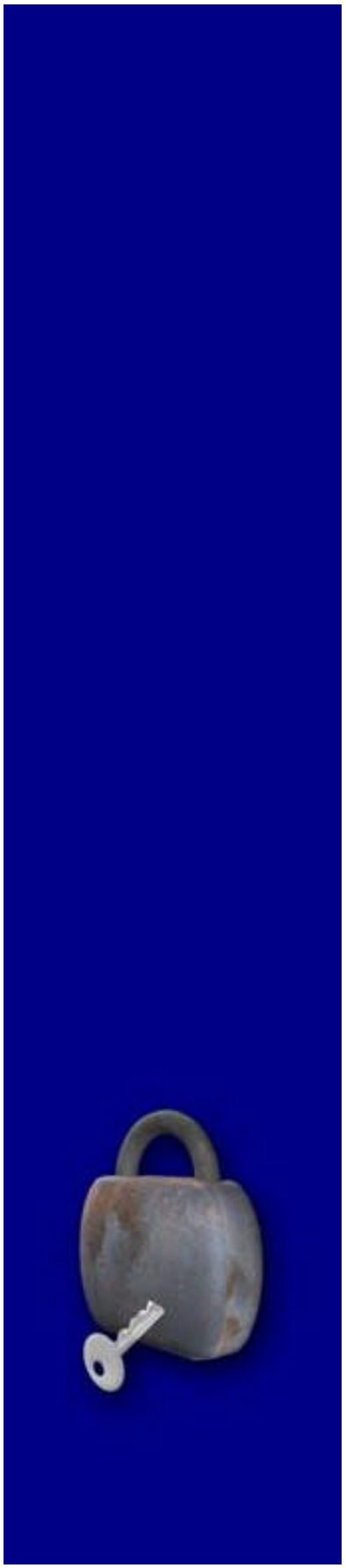


Password Recovery Wizard

Password Recovery Concepts

Passwords are not physically stored in any way inside a SQL Server database. SQL Server uses a mathematical formula known as a SHA1 hashing algorithm to deduce a large number from the password, and stores this number inside the master.mdf data file instead. When a user logs on to SQL Server, the password they enter is once again passed through this SHA1 hashing routine, and the hash resulting from it is compared to the hash stored in SQL Server. If they match, the password is deemed to be correct, and access is granted.

It is theoretically impossible to retrieve a password from an SHA1 hash alone, and the only method that can be used to attempt to find a password is by randomly choosing words, hashing them using the SHA1 algorithm, and comparing the hashes.

The Password Recovery Wizard is designed to be able to retrieve these stored hashes from both an online database (system administrator rights are required) and even from an offline database, using only the master.mdf database file copied from the database server.

Unlike other competitive products, the Password Recovery Wizard does not rely on brute-force password guessing methods alone. The wizard uses combinations of words taken from several dictionaries including Afrikaans, American English, Australian English, Chinese, Croatian, Czech, Danish, Dutch, British English, Finnish, French, German, Hindu, Hungarian, Icelandic, Italian, Japanese, Latin, Norwegian, Polish, Portuguese, Russian, Spanish, Swahili, Swedish, Xhosa, and Zulu to test for passwords, while also using non-standard terms from word lists of computer terminology, literature, movie titles, song titles, people names, religious terms and scientific terms.

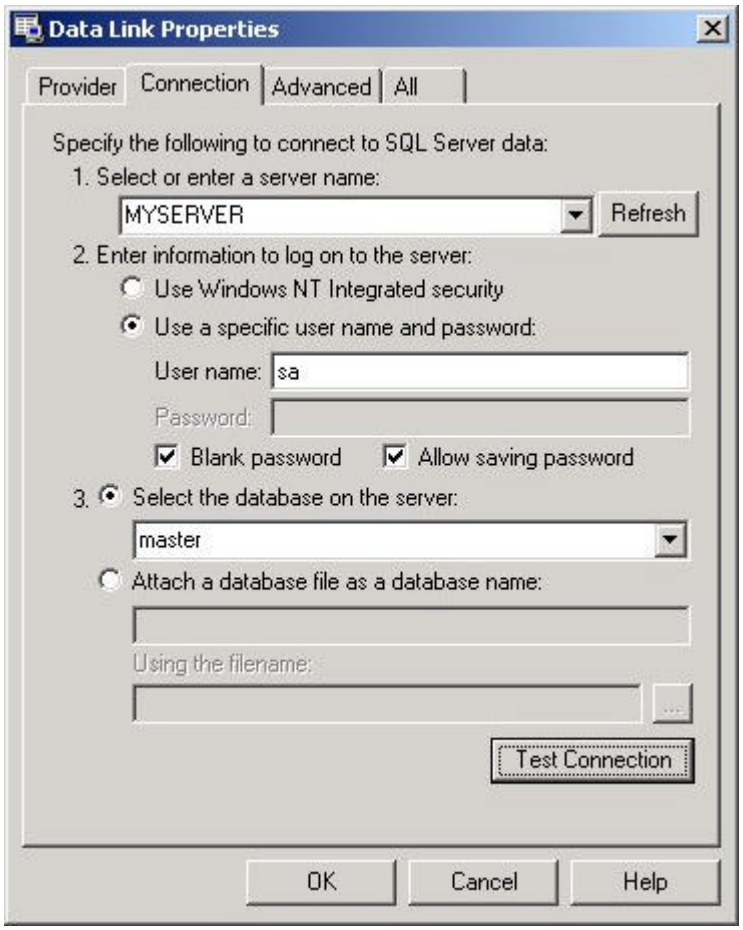
Using these dictionaries results in a much faster method of operation when users use common, easy to remember words, as is most often the case.

Should no password be retrieved using these supplied dictionaries, the Password Recovery Wizard will automatically switch over to using a more traditional brute-force method of password recovery.

Recovering a Password from an Online Server

To recover a password from an online SQL Server database, start the Password Recovery Wizard and select the **Recover Password from an online Master database option**. Click the **Next** button to continue.

Click on the **Connect** button to select the server, database and logon credentials to use to connect to the SQL Server database.



The Password Recovery Wizard will connect to SQL Server and retrieve a list of available user names from the master database. Select the user name for which to recover the password and click on the **Next** button.

The Password Recovery Wizard will start the analysis process, first using its built-in dictionaries and word-lists, and then using brute-force if necessary.

This process could take several minutes and even several hours to complete, depending on the length and complexity of the password.

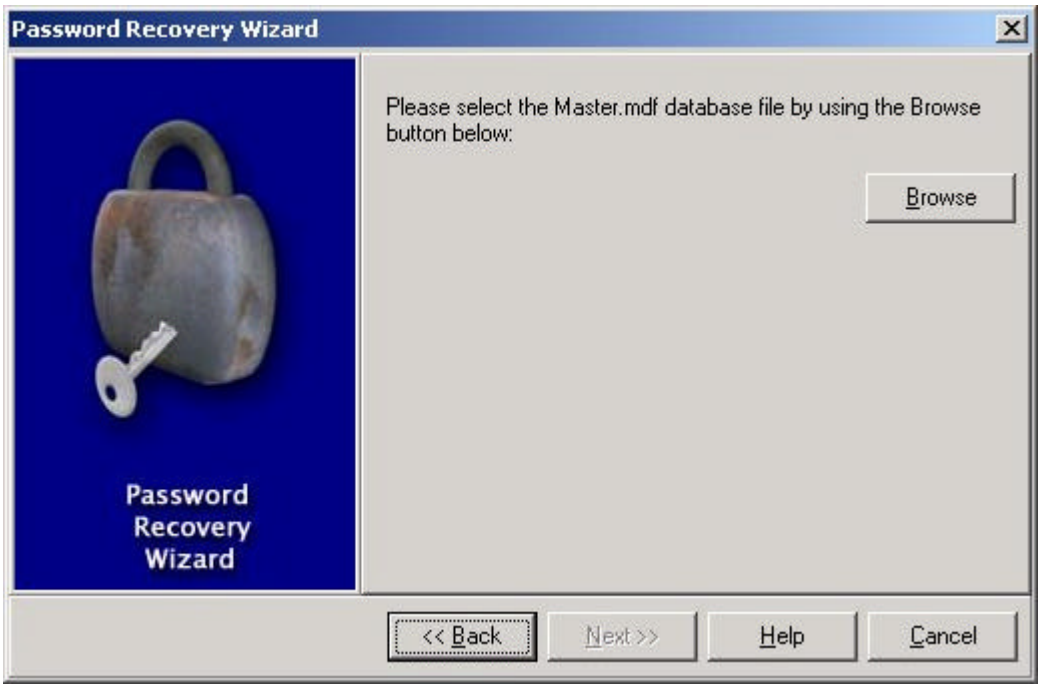
Once the password has been recovered, it will be displayed on-screen.

Recovering a Password from an Offline Server

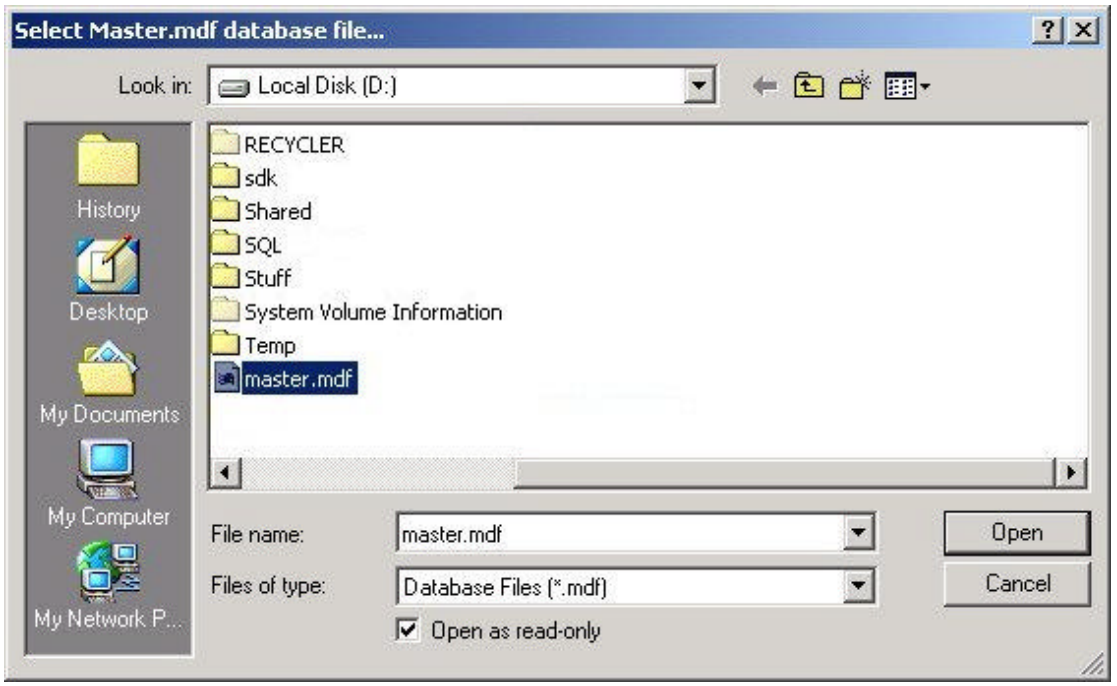
To recover a password from an offline SQL Server database, start the Password Recovery Wizard and select the **Recover Password from an offline Master.mdf database file** option. Ensure that the SQL Server Service is stopped. This process cannot extract the information from the master.mdf file while the SQL Server service is running, as the master.mdf file is then exclusively locked.

To continue, click the **Next** button.

Select the **Browse** button from the next screen to select the master.mdf file from the server.



The Password Recovery Wizard will scan through the master.mdf file and extract the user names and password hashes directly from the data pages.



Once this process is complete, a list of available user names will be displayed. Select the user name for which to recover the password and click on the **Next** button.

The Password Recovery Wizard will start the analysis process, first using its built-in dictionaries and word-lists, and then using brute-force if necessary.

This process could take several minutes and even several hours to complete, depending on the length and complexity of the password.

Once the password has been recovered, it will be displayed on-screen.