What to do when the SA account password is lost in SQL Server 2005

<http://blogs.msdn.com/raulga/archive/2007/07/12/disaster-recovery-what-to-do-when-the-sa-account-password-is-lost-in-sql-server-2005.aspx>  |  [Comments](http://blogs.msdn.com/raulga/comments/3841716.aspx)

You may have faced the issue of losing the SQL Server SA password. Perhaps you followed the security best-practice of removing the  builtin\Administrators from the sysadmin server role,  and no one  you can find is in the sysadmin role.   At this point you may think that your only options are to reinstall SQL Server and attach the databases, or to  directly access the master database files, which may potentially damage the data.

SQL Server 2005 provides a better disaster recovery option for this scenario that is non-intrusive for master DB and that will help you preserve any objects and data stored in master DB (such as logins, certificates, Service Master Key, etc.) intact. Members of the Windows Administrators group now have access to SQL Server when SQL Server is in started in single-user mode, also known as “maintenance mode “.

Using the single-user mode, SQL Server 2005 prevents a  Windows Administrator to abuse this privilege to act on behalf of the sysadmin without being noticed. This allows Windows Administrator accounts to perform certain maintenance tasks, such as installing patches.

In order to start SQL Server in single-user mode, you can add the parameter “-m” at the command line. You can also use the *SQL Server Configuration Manager* tool, which provides proper controls for the file access and other privileges. To use the *Configuration Manager* tool to recover your system, use the following steps:

1. Open the *Configuration Manager* tool from the "SQL Server 2005| Configuration" menu

2. Stop the SQL Server Instance you need to recover

3. Navigate to the “Advanced” tab, and in the Properties text box add “;–m” to the end of the list in the “Startup parameters” option

4. Click the “OK” button and restart the SQL Server Instance

**NOTE**: make sure there is no space between “;” and “-m”, the registry parameter parser is sensitive to such typos. You should see an entry in the SQL Server ERRORLOG file that says “SQL Server started in single-user mode.”

5. After the SQL Server Instance starts in single-user mode, the Windows Administrator account is able to connect to SQL Server using the sqlcmd utility using Windows authentication. You can use Transact-SQL commands such as "sp\_addsrvrolemember" to add an existing login (or a newly created one) to the sysadmin server role.

The following example adds the account "Buck" in the "CONTOSO" domain to the SQL Server "sysadmin" role:

EXEC sp\_addsrvrolemember 'CONTOSO\Buck', 'sysadmin';

GO

6. Once the sysadmin access has been recovered, remove the “;-m” from the startup parameters using the Configuration Manager and restart the SQL Server Instance

**Important Security Notes:**

This process should only be used for disaster recovery when no other method to access the system with a privileged (i.e. sysadmin or equivalent) is available.

This process allows a Windows Administrator account to override their privileges within SQL Server. It requires explicit and intrusive actions that can be monitored and detected, including:

         Stop SQL Server and restart it in single use mode

         Connecting to SQL Server using Windows credentials

  Special thanks to Buck Woody (<http://blogs.msdn.com/buckwoody/>) for his help in writing this article.

http://blogs.msdn.com/aggbug.aspx?PostID=3841716