Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

MSDE Password Management for ISA Server 2006

Abstract

In this article, I will show you how to configure ISA Server 2006 MSDE logging features to assign a custom password to the SA account for the MSFW database instance which ISA server 2006 uses by default for logging purposes.

The problem

You can configure Microsoft SQL Server 2005 Express, Microsoft SQL Server Desktop Engine (MSDE) versions 2000, or earlier versions of Microsoft SQL Server to run in mixed authentication mode. The SA account is created during the installation process and the SA account has full rights in the SQL Server environment. By default, the SA password is blank (NULL), unless you change the password when you run the MSDE Setup program. To establish additional security for your ISA Server environment it is best practice to change the SA password to a very strong password as a first method in your line of defence. A much better approach is to use only Windows Authentication, because Windows Authentication uses Kerberos as the athentication protocol and provides strong password enforcements methods.

The dangerous SA account?

In the past and sometimes today, the SA Account was the dangerous thing in Microsoft SQL Server deployments. The SA account is used by Microsoft SQL Server, MSDE (Microsoft SQL Server Desktop Engine) and Microsoft SQL Server Express. In some versions and under some circumstances, the password for the SA account is blank (NULL) and a possible attacker can use this account to get full access to the SQL Server configuration and databases. So it is very important to assign a secure password to the SA account which is under your own control.

SQL Authentication modes

Microsoft SQL Server databases and its small brother MSDE, can use different types of Authentication methods.

You can use the following authentication methods:

- Mixed Mode
- Windows Authentication Mode

Mixed Mode

In Mixed Mode, Administrators can use Windows Authentication or SQL Server Authentication. When you use SQL Server Authentication you will need an account, created with the SQL Management tools like the Microsoft SQL Server Enterprise Manager. You can also use the built In SQL Server Administration account called SA.

Windows Authentication Mode

Windows Authentication mode is the securest Authentication Mode, because it uses Kerberos as the security protocol. Windows Authentication also provides Account lockout features, password policy enforcement in terms of the password complexity. Windows Authentication also supports password expirations, while Standard SQL authentication provides this feature not. If you select Windows Authentication, Setup creates an SA account that is disabled by default. To utilize Mixed Mode Authentication you must activate the SA account after Setup is completed.

Strong Password Guidelines

Strong passwords are not easy to establish. Passwords that are to strong are not easy to remember; weak passwords are easy to remember but are very insecure. Make your own decision which type of passwords you want to use. Strong passwords cannot use prohibited conditions or terms, including:

A blank or NULL password
"Password"
"Admin"
"Administrator"
"sa"
"sysadmin"

A strong password should be consist of more than 8 characters in length and satisfy at least three of the following four criteria:

- It must contain uppercase letters.
- It must contain lowercase letters.
- It must contain numbers.
- It must contain non-alphanumeric characters; for example, #, %, or ^.

Maximum password length

Microsoft SQL Server passwords can be between 1 and 128 characters in length, including combination of letters, symbols and numbers.

ISA Server MSDE logging

Per Default ISA Server 2004/2006 setups installs the Advanced Logging for ISA Server Firewall services and for Webproxy Logging. That means that theses services logs per default into a MSDE database. You can change the Log storage format after ISA Server installation from MSDE to Microsoft SQL Server or classic file format.

In large environments it could be necessary to change the logging format from MSDE to text file because of Security reasons. You will find more information about ISA Server logging and performance in the following article.

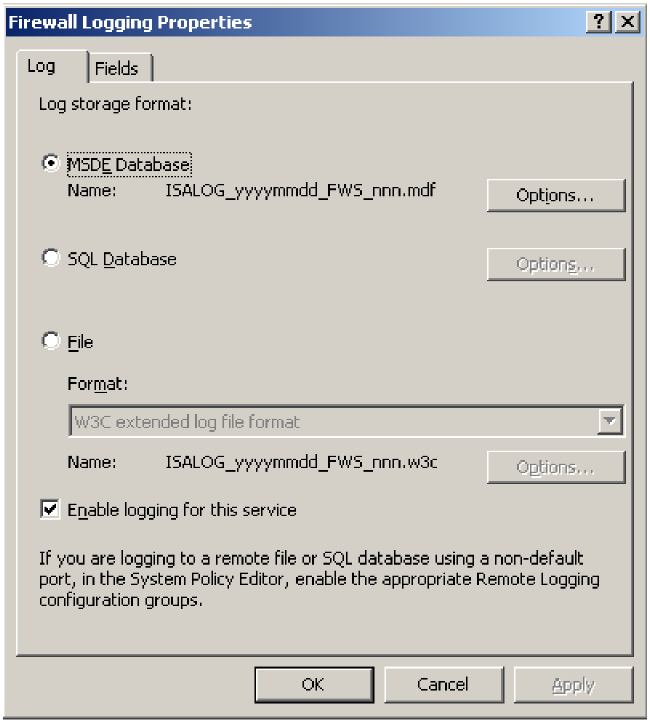

Figure 1: ISA Server log storage format

How to verify if the SA password is blank

On the ISA Server that is using the instance of the MSDE or SQL Express, open the command prompt and enter

osql -U sa

This connects you to the local, default instance of MSDE by using the sa account. To connect to a named instance installed on your computer type:

osql -U sa -S servername\MSFW

You will see the following prompt:

Password:

Press *ENTER* again. This will use a blank password for the SA account.

If you see the prompt *1*>, you are successfully logged on without a password.
Change SQL Authentication mode

Change MSDE Authentication mode

By default MSDE on ISA Server 2004/2006 uses Windows Authentication, so you must change the Authentication mode to mixed mode Authentication. This is done by patching the Registry.

Before you start patching the Registry, you must stop the Microsoft SQL Server service. This is done through the SQL Server Service Manager as you can see in the following picture.

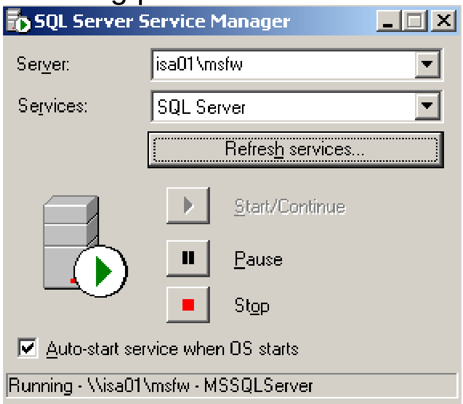

Figure 2 SQL Server Service Manager

Tip:

Have you ever wondered on your own ISA Server that the SQL Server Service Manager entry for Servername and services is empty, but all services working as expected?
Simply enter the servername and the name of the MSDE instance for ISA in the Server field – as an example *ISA01\MSFW*. And click the *Refresh services* button.

Next, navigate to *HKLM\Software\Microsoft\Microsoft SQL Server\MSFW\MSSQLServer.*

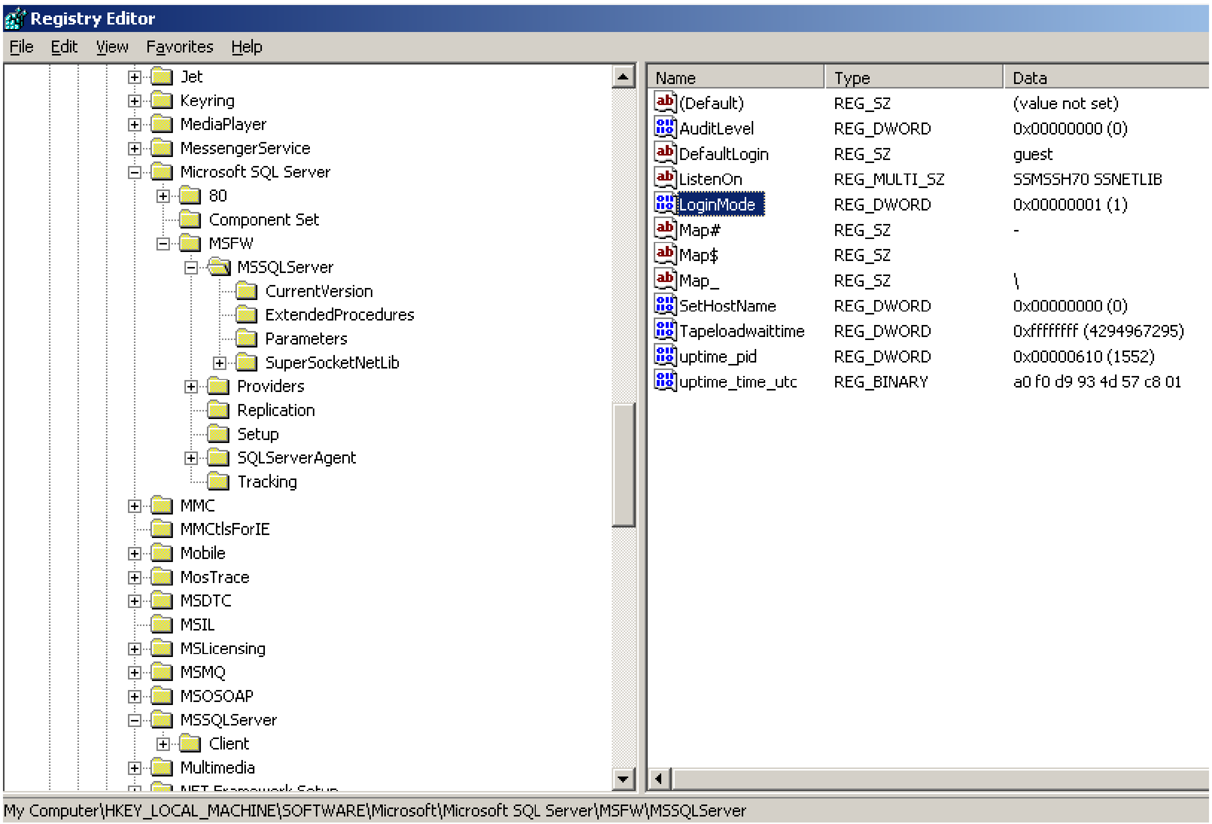

Figure 3: Registry settings for SQL Authentication mode

Change the *LoginMode* entry from *1* to *2*.

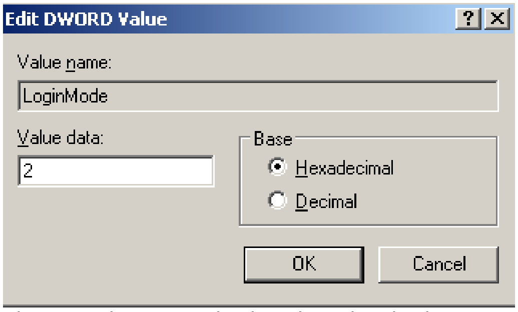

Figure 4: Change to mixed mode authentication

Restart the Microsoft SQL Server service.
Open a command prompt and enter the following command to establish a connection to the MSDE:

OSQL –E –S ISA01\MSFW

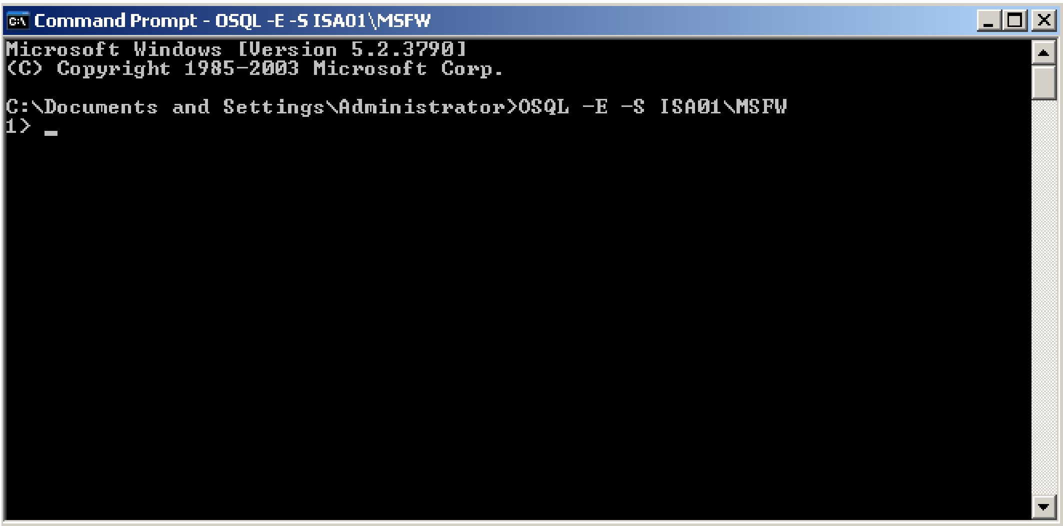

Figure 5: Log on to the MSDE instance for ISA Server

At this OSQL command prompt, enter the following commands shown in the following picture:

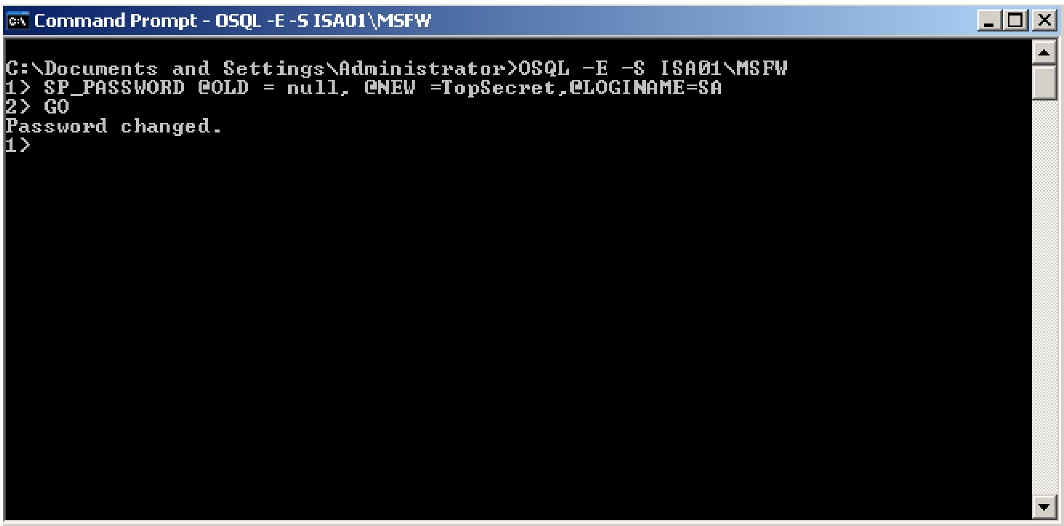

Figure 6: Change the password of the SA account for the instance

The password has successfully changed.
Explanation of the syntax:

SP_password @old = null - The old password
@new = TopSecret – TopSecret is the new password
@loginname – The account for which you want to change the password
GO – Executes the OSQL command

You can now use the SA account and the new password to logon to the database.

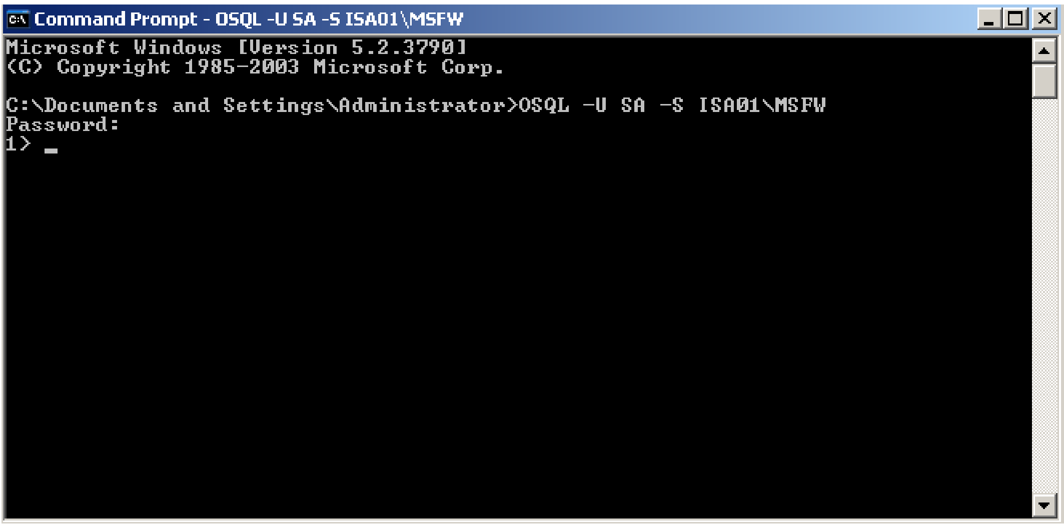

Figure 7: Logon with new credentials

Don't forget to change the SQL Server authentication mode if you don't want to use mixed Mode Authentication in the future. Microsoft recommends using only Windows Authentication. If you change the authentication method back to Windows Authentication, you have to restart the Microsoft SQL Server service.

Conclusion

This article showed you how to manage passwords for the SA account in the Microsoft SQL Server Desktop Engine and how to use mixed mode authentication instead of Windows Authentication only.

Related links

How to verify and change the system administrator password in MSDE or SQL Server 2005 Express Edition
http://support.microsoft.com/kb/322336/en-us
Windows Authentication mode is the default security mode after a typical installation of SQL Server 2000 or of SQL Server 2005
http://support.microsoft.com/kb/269587/en-us
How to setup SQL Logging in ISA Server
http://www.isaserver.org/tutorials/How_to_setup_SQL_Logging_in_ISA_Server.html
How to configure ISA Server 2004 and ISA Server 2006 to log data to an SQL Server database
http://support.microsoft.com/kb/838710/en-us