How to verify and change the system administrator password in MSDE or SQL Server 2005 Express Edition

This article was previously published under Q322336

Article ID : 322336
Last Review : December 8, 2005
Revision : 4.0

On This Page

- SUMMARY
  - How to verify if the SA password is blank
  - How to change your SA password
  - How to determine or change your authentication mode
  - Security best practices for a SQL Server installation
- REFERENCES

SUMMARY

This step-by-step article discusses the steps you can use to change the SQL Server **sa** (system administrator) password.

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 conform with the best security practices, you must change the **sa** password to a strong password at the first opportunity.

How to verify if the SA password is blank

1. On the computer that is hosting the instance of MSDE to which you are connecting, open a command prompt window.
2. At the command prompt, type the following command, and then press 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\instancename

   You are now at the following prompt:

   Password:
3. Press ENTER again. This will pass a NULL (blank) password for **sa**.

   If you are now at the following prompt, after you press ENTER, then you do not have a password for the **sa** account:

   1>

   We recommend that you create a non-NULL, strong password to conform with security practices.

   However, if you receive the following error message, you have entered an incorrect password. This error message indicates that a password has been created for the **sa** account:

   > **"Login Failed for user 'sa'."**

   The following error message indicates that the computer that is running SQL Server is set to Windows Authentication only:

   > **Login failed for user 'sa'. Reason: Not associated with a trusted SQL Server connection.**

   You cannot verify your **sa** password while in Windows Authentication mode. However, you can create a **sa** password so that your **sa** account is secure in case your authentication mode is changed to Mixed Mode in the future.

If you receive the following error message, SQL Server may not be running or you may have provided an incorrect name for the named instance of SQL Server that is installed:

> **[Shared Memory]SQL Server does not exist or access denied.**
> **[Shared Memory]ConnectionOpen (Connect()).**

How to change your SA password

1. On the computer that is hosting the instance of MSDE to which you are connecting, open the command prompt window.
2. Type the following command, and then press ENTER:

   osql -U sa

   At the **Password:** prompt, press ENTER if your password is blank or type the current password. This connects you to the local, default instance of MSDE by using the **sa** account. To connect by using Windows authentication, type this command: **use osql -E**

   Note If you are using SQL Server 2005 Express, avoid using the Osql utility, and plan to modify applications that currently use the Osql feature. Use the Sqlcmd utility instead.

   For more information about the Sqlcmd utility, visit the following Microsoft Developer Network (MSDN) Web site:
   http://msdn2.microsoft.com/en-us/library/ms165702.aspx (http://msdn2.microsoft.com/en-us/library/ms165702.aspx)
3. Type the following commands, on separate lines, and then press ENTER:

   ```
   sp_password @old = null, @new = 'complexpwd',  @loginame ='sa'
      go
   ```

   Note Make sure that you replace "complexpwd" with the new strong password. A strong password includes alpha-numeric and special characters, and a combination of upper and lower case characters.

   You will receive the following informational message, which indicates that your password was changed successfully:

   > **Password changed.**

How to determine or change your authentication mode

Important This article contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base:

> 256986 (http://support.microsoft.com/kb/256986/) Description of the Microsoft Windows registry

Warning Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall your operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

If you are not sure how to verify the authentication mode of your MSDE installation, you can check the corresponding registry entry. By default, the value of the Windows **LoginMode** registry subkey is set to 1 for Windows Authentication. When Mixed Mode authentication is enabled, this value is a 2.

- The location of the **LoginMode** subkey depends on whether you installed MSDE as the default MSDE instance or as a named instance. If you installed MSDE as the default instance, the **LoginMode** subkey is located in the following registry subkey:

  HKLM\Software\Microsoft\MSSqlserver\MSSqlServer\LoginMode

  Note If you are using SQL Server 2005, whatever you installed a default instance or a named instance, l ocate the following registry subkey. *MSSQL.x* is a placeholder for the corresponding value for your system:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.x\MSSQLServer

- If you installed MSDE as a named instance, the **LoginMode** subkey is located in the following registry subkey:

  HKLM\Software\Microsoft\Microsoft SQL Server\%InstanceName%\MSSQLServer\LoginMode

Note Before you switch authentication modes, you must set a **sa** password to avoid exposing a potential security hole.

To switch from Mixed Mode to Integrated (Windows) authentication, follow these steps:

1. To stop MSSQLSERVER and all other related services (such as SQLSERVERAgent), open the **Services** applet in Control Panel.
2. Open the Registry Editor. To open the Registry Editor, click **Start**, click **Run**, and then type: **"regedt32" (without the quotation marks)**

   Click **OK**.
3. Locate either of the following subkeys (depending on whether you installed MSDE as the default MSDE instance or as a named instance:

   HKEY_LOCAL_MACHINE\Software\Microsoft\MSSqlserver\MSSqlServer

   or

   HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\<Instance Name>\MSSQLServer\
4. In the right-pane, double-click the **LoginMode** subkey.
5. In the **DWORD Editor** dialog box, set the value of this subkey to 1. Make sure that the **Hex** option is selected, and then click **OK**.
6. Restart the MSSQLSERVER and the SQLSERVERAgent services for this change to take effect.

Security best practices for a SQL Server installation

Each of the items that follow will make your system more secure and they are part of the standard security "best practices" for any SQL Server installation.

- Secure your **sa** login account with a non-NULL password. There are worms that only work if you have no security for your **sa** login account. Therefore, to make sure that the built-in **sa** account has a strong password, you must follow the recommendation provided in the "System Administrator (SA) Login" topic in SQL Server Books Online, even if you never directly use the **sa** account.
- Block port 1433 at your Internet gateways, and then assign SQL Server to listen on an alternate port.
- If port 1433 must be available on your Internet gateways, enable egress and ingress filtering to prevent misuse of the port.
- Run the SQLServer service and SQL Server Agent under a Microsoft Windows NT account, not a Local System account.
- Enable Microsoft Windows NT Authentication, and then enable auditing for successful and failed logins. Then, stop and restart the MSSQLServer service. Configure your clients to use Windows NT Authentication.

REFERENCES

For more information regarding how a blank sa password can be exploited, click the following article number to view the article in the Microsoft Knowledge Base:

> 313418 (http://support.microsoft.com/kb/313418/) PRB: Unsecured SQL Server with blank (NULL) SA password leaves vulnerability to a worm

For more information about a change in behavior with post-SQL Server 2000 Service Pack 1 when the authentication mode changes, click the following article number to view the article in the Microsoft Knowledge Base:

> 274773 (http://support.microsoft.com/kb/274773/) FIX: If you change Windows Security to Windows/SQL Security,

the SA password is blank

APPLIES TO

- Microsoft SQL Server 2000 Desktop Engine (Windows)
- Microsoft SQL Server 2000 64-bit Edition
- Microsoft SQL Server 2005 Express Edition

Keywords: kbhowtomaster KB322336