

By Steven Warren, MCSE, MCDBA

1. **Create a strong “sa” password** – It is very important to make sure that SQL Server has a very strong “sa” (administrator) password with a combination of letters, numbers, and symbols. This reduces the possibility of a password being guessed or hacked. I can’t begin to tell you how many people choose “password” or “sa” – or worse, use a blank (null) password. Avoid those mistakes at all costs.
2. **If at all possible, use Windows Authentication mode for SQL Server** – Requiring Windows Authentication for SQL Server will help prevent Internet attacks because it is much more secure than mixed mode authentication.
3. **Take advantage of the Microsoft Baseline Security Analyzer (MBSA)** – At any given point-in-time, the Microsoft Baseline Security Analyzer can provide a good summary of the security of the Windows server that you’re running SQL Server on. You can run it locally or on the network. [Download](#) the tool and start using it.
4. **Install the most recent SQL Server service pack** – By keeping up to date on your SQL Server service packs, you can make sure the latest security vulnerabilities and system bugs are being addressed. You can download the latest SQL Server service packs [here](#).
5. **Install the latest SQL Server security updates** – In addition to the latest SQL Server service pack, Microsoft puts out SQL Server security updates that can be downloaded. You need to combine the latest SQL Server service pack and the latest security updates to keep your system fully patched. You can search for updates that apply to SQL Server at [this Microsoft TechNet site](#).
6. **Run the service accounts with domain user permissions** – When you install SQL Server, two service accounts are created: MSSQLSERVER and SQLSERVERAGENT. By running these accounts as domain user accounts, you limit the destruction that can result if they are compromised.
7. **Get info from the SQL Server 2000 Operations Guide** – Download Microsoft's [SQL Server 2000 Operations Guide](#) and make note of the security recommendations that are listed. This document covers security, monitoring, change control, and a host of other topics that will help you lock down a SQL Server, especially SQL Server 2000.
8. **Implement Encrypting File System (EFS)** – Windows 2000 is prepackaged with EFS to allow you to encrypt files. Using EFS with SQL Server can encrypt the client/server data to keep companies' most valuable asset (your private data) secure. [This article](#) shows how to use EFS with SQL Server.
9. **Block firewall ports 1433 and 1434** – When you install a default installation of SQL Server, ports 1433 and 1434 are the basic ports in use. A best practice is to explicitly filter out packets addressed to these ports on your firewall (and log any attempts to access them). This will help keep your SQL Server from being compromised by outside attackers.
10. **Encrypt and secure your backups** – The default installation of SQL Server does not encrypt or compress backups. You can place a password on your backups, but any text editor can compromise a backup, even with a password. Use software such as [LiteSpeed for SQL Server](#) to handle your encryption.



Steven S. Warren is an IT consultant with expertise in administering Microsoft networks, especially Microsoft SQL Server. He is also a freelance technical writer who has been a long-time contributor to TechRepublic. He also has a forthcoming book on VMware Workstation. Steven holds the following certifications: MCDBA, MCSE, MCSA, CCA, CIW-SA, CIW-MA, Network+, and i-Net+. He has also been honored with the Microsoft Most Valuable Professional (MVP) award.

Additional resources

- Sign up for the [SQL Server newsletter](#), delivered on Tuesdays
- Sign up for the [Security Solutions newsletter](#), delivered on Fridays
- See all of [TechRepublic's newsletter offerings](#)
- "[Microsoft SQL Server Security Configuration Assessment](#)" (TechRepublic download)
- "[TechRepublic SQL Server QuickStart](#)" (TechRepublic download)
- "[Five SQL Server scripts for novice DBAs](#)" (TechRepublic download)

Version history

- **Version:** 1.0
- **Published:** March 9, 2005

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team