Understand encryption levels

SQLsafe allows you to set the encryption level most appropriate for your backup needs. During the initial setup of SQLsafe, you can select a default encryption level. Any time before executing a backup, you can strengthen or lessen the encryption applied to the current backup.

You must have a password in order to restore an encrypted backup. For security reasons, when you generate a T-SQL or CLI script of an encrypted backup, SQLsafe does not write the specified password to the script. To successfully run the script, supply the appropriate password. SQLsafe also does not store encryption passwords and cannot recover lost or forgotten passwords.

> ✓ **Tip**
>
> SQLsafe automatically detects whether the target SQL Server instances require FIPS compliant encryption. When this security setting is detected, SQLsafe uses the FIPS-compliant AES encryption algorithms provided by Microsoft. For more information about FIPS compliance, see Ensure FIPS compliance.

SQLsafe encryption offers you the following encryption methods, allowing you to choose based on your security needs:

None

Provides the fastest execution speed and does not encrypt backed up data.

Advanced Encryption Standard (AES) 128-bit

Provides a strong encryption. The AES algorithm encrypts data in 128-bit blocks using a 128-bit key.

Advanced Encryption Standard (AES) 256-bit

Provides a stronger encryption. The AES algorithm encrypts data in 128-bit blocks using a 256-bit key. This method provides more secure encryption than AES 128-bit.