

Select location

The **Locations** tab of the SQL Safe Backup Policy Wizard allows you to specify the backup location for each operation you include in the backup policy.

What information is on the Locations tab?

For each operation you have included in the backup policy, you can specify the location type, the full path in which to store the backup file, an optional housecleaning schedule for existing disk archives, and the backup file extension.

What types of backup locations can you use?

SQL Safe supports the following location types:

- Backup to a single file on the local computer or a network share.
- Backup to multiple striped files on the local computer or a network share.
- Backup to tape using Tivoli Storage Manager.
- Backup to Data Domain.
- Backup to Amazon S3 Cloud.
- Backup to S3 Compatible Storage.
- Backup to Microsoft Azure Cloud.
- Backup to Tape using Tivoli Storage Manager striped files.

What do you do if you don't have an existing archive?

If you do not specify an existing archive, SQL Safe creates a new backup set with the name you specify. The location entered for each backup type must be valid for all SQL Server instances. You can choose to **Append** or **Overwrite** if the archive already exists.

What accounts can you specify to access the location of the backup files?

Depending on whether you selected to use the SQL Server Agent or the SQL Safe Backup Agent for the scheduling of your policy, in this section you have the option to select between the SQL Server Agent service account/SQL Safe Backup Agent service account respectively, or a Windows account. Click **Account** and select your preferred option.



The account specified must have read and write privileges on the directory selected for your backup file location.

How do you keep my backups running despite network errors?

Select **Enable network resiliency** and then click **Configure** to change the default settings. By default, SQL Safe will retry the backup operation every 10 seconds and then fail after 5 minutes (300 seconds) of continuous errors. Also, over the course of the operation, SQL Safe allows a total of 60 minutes in which to retry the backup before stopping the operation.

This option is not available when backing up to tape using Tivoli Storage Manager.

Can you change the default file locations?

SQL Safe automatically populates the path using several available variables, depending on the location type. You can modify this path to suit your needs, taking advantage of all the available variables.

For a disk backup, browse for or enter the directory in which to store the backup file. You can use the supplied macros in the way best suited to your storage needs. If you want to limit the lifetime of your backup sets created by the policy, you can select the option that removes files older than the specified time.

For a TSM backup, browse for or enter the high level directory for the tape file. You can use the supplied macros in the way best suited to your storage needs. Browse for or enter the location of the TSM configuration file.

 Keep in mind, the filename extension for all backups performed under the SQL Safe format are .safe and for all backups performed under the SQL server format are .bak.

What does removing old files do?

For backups written to a single file or mirrored files, you can choose to remove old files to prevent disk space limitations. When you select to remove files older than the specified time, backup files created with names of the same format will be deleted from that directory. You can configure SQL Safe to delete old backup files from the primary archive as well as from your mirror archives.

For backups written to a TSM Server, you can configure SQL Safe to mark these files as inactive after a specified age.

How do you mirror the backups this policy creates?

Click **Mirror Archives**, and then specify where you want the mirrored files to be stored.

For each mirror, SQL Safe creates a copy of the backup archive set. You can specify up to 2 mirrors for each backup operation.

 Keep in mind that creating mirrors can impact the performance of your backup operation.

If you want to stop the backup operation when the mirror location is unavailable, select **Abort backup if a mirror location reports a failure**.

What do you specify when backing up to a TSM Server?

When a TSM location is selected, you must specify the following settings:

- the location of the TSM Client configuration file that enables generating a password for authorization
- High Level file path

- Low Level file path
- Management Class (optional)

You can also configure SQL Safe to mark these files as inactive after a specified age.

 Note that SQL Safe accepts up to 260 characters for the TSM file path name.

 SQL virtual database is not available when backing up to a TSM Server.

What do you specify when backing up to Amazon S3 Cloud?

When the Amazon S3 Cloud location is selected, you must specify the following settings:

- Access Key
- Secret Key
- Region
- Bucket Name
- Subfolder(s) (optional)
- Filename
- Storage Class
- Part Size

For more information, go to [Amazon Settings](#).

What do you specify when backing up to an S3 Compatible Storage?

When the S3 Compatible Storage location is selected, you must specify the following settings:

- Access Key.
- Secret Key.
- REST Endpoint (IP: Port).
- Bucket Name.
- Subfolder(s) (Optional).
- Filename.
- Part Size.

For more information, go to [S3 Compatible Settings](#).

What do you specify when backing up to Microsoft Azure?

When the Microsoft Azure location is selected, you must specify the following settings:

- Authentication Method
- Azure Storage Account Name
- Azure Access Key
- Sector Type
- Container Name
- Subfolder(s) (optional)
- Filename

- Part Size

For more information, go to [Azure Settings](#).

Once you determine your backup location, click **NEXT** to [configure a schedule](#) for your backup operations.

[IDERA](#) | [Products](#) | [Purchase](#) | [Support](#) | [Community](#) | [Resources](#) | [About Us](#) | [Legal](#)