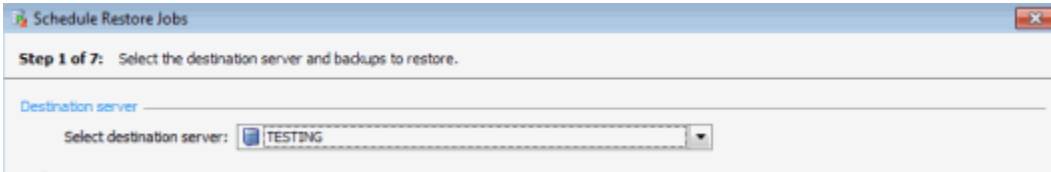


Scheduling restores - select the destination server and backups to restore

[Scheduling restore jobs](#) > **Select destination server and backups to restore** > [Select destination database](#) > [Specify file locations](#) > [Specify verification options](#) > [Configure restore options](#) > [Create restore schedule](#) > [Review summary](#)

On step 1 of the wizard, select the SQL Server you want to restore to and the backup files to use.

Destination server

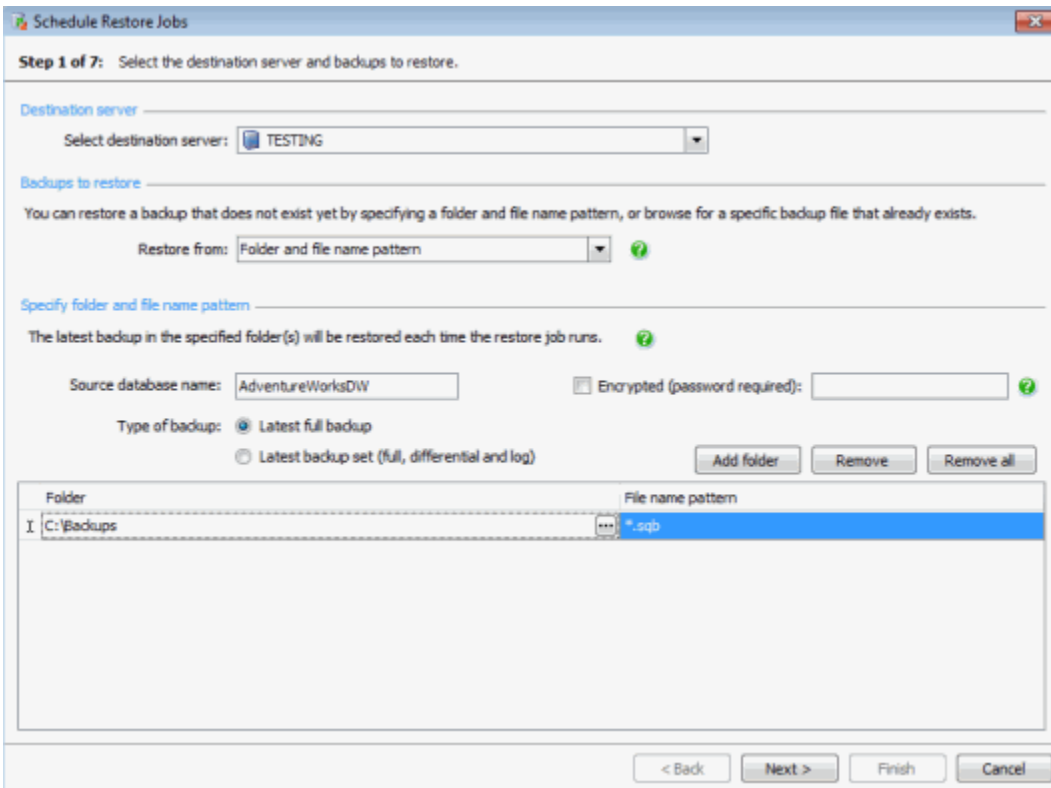


From the **Select destination server** drop-down list, choose the server on which you want to restore the backups. This does not have to be server on which the backups are stored.

If you have launched the wizard from a **reminder**, this option is populated with the server on which the backup job was created. If you change to a different server, you must update the path under **Folder** to refer to the location on the original server.

If the SQL Backup Pro server components are not installed on the selected server, a warning is displayed and you must install the server components to proceed. See [Installing or upgrading on a SQL Server instance](#) for more information.

Restoring from a folder and file name pattern



You can create a scheduled restore job to restore the latest backup of a database each time the job runs. Restore from a folder and file name pattern if either of the following are true:


- a backup of the database does not already exist
- backups will be created with different file names each time the job runs.

This is useful if you have created a scheduled backup job and opted to name the files automatically using [tags](#) to include the date and time of creation in the file name.

If you have launched the Schedule Restore Jobs wizard from a **reminder**, this option is selected by default and the page is populated with details to identify the latest backup created by the scheduled backup job. The job details, including the password, are populated from the backup job stored on the server, and are not copied elsewhere.

Setting up the folder and file name pattern manually

If you have not launched the Schedule Restore Jobs wizard from a reminder, enter the details to identify the latest backup:

1. From the **Restore from** drop-down list select **Folder and file name pattern**.
2. Specify the name of the backed up database in the **Source database name** box.
3. Choose between restoring the latest full backup of the source database (**Latest full backup**) or the latest set of backups (**Latest backup set**) of the source database.
If you select **Latest backup set**, the latest full backup, the latest subsequent differential backup (if available), and all subsequent log backups (if available) will be restored.
4. Click **Add folder** to specify the folders where the backups will be stored. When the restore job runs, SQL Backup Pro will search the specified folders for the latest backup or set of backups of the source database that matches the specified file name pattern.
You can specify more than one folder and file name pattern. This is useful if you store your backups in multiple locations (for example, separate folders for full, differential and log backups) or split backups into multiple files across different folders. SQL Backup Pro will search all specified folders for the latest full backup or set of backups of the source database using the specified file name pattern.
5. Under **Folder**, specify the folder(s) in which the backup file(s) will be stored when the job runs; SQL Backup Pro will not search subfolders of the specified folder. The default backup location for the destination server is supplied. To edit the path, type or click  to open the **Folder Browser**. If the folder does not exist yet (for example, because it is due to be created by a scheduled backup job), type the path or create the folder from the **Folder Browser**.

Local drives refer to the destination server. Use the **Folder Browser** to view locations on a different server by selecting a different machine from the **Server** drop-down list. If the server you require is not displayed, click **Add Server** and type the server name or IP address. Other servers will only be visible to the local server if it has the appropriate permissions to write to or read from them. The name of the local server you are connected to and your user name are displayed above the **Server** list. This information may explain why some servers cannot be browsed.

6. Under **File name pattern**, specify a file name pattern to search the folder for backups of the source database. By default, the wildcard character * is used to replace the entire file name (*.sqb). SQL Backup Pro will identify the most recent backup in the folder which matches the source database name.

You can combine fixed text with wildcard characters to limit the search to particular files in the folder; SQL Backup Pro will identify the most recent backup of the source database which matches the specified pattern. This is useful if you store backups for two or more databases of the same name in the same folder. For example:

- *(local)_AdventureWorksDW_FULL*.sqb* would match files such as *(local)_AdventureWorksDW_FULL_20120229.sqb* but not *TESTSERV_ER_AdventureWorksDW_FULL_20120228.sqb*
- **Database1_201201*.sqb* would match files such as *FULL_Database1_20120125.sqb* and *DIFF_Database1_20120127.sqb*.

You may find it helpful to set the default backup folder and file name format for the server and select **Name file automatically** when you create scheduled backup jobs using the Schedule Backup Jobs wizard. For more information, see [File management options](#).

Encrypted backups

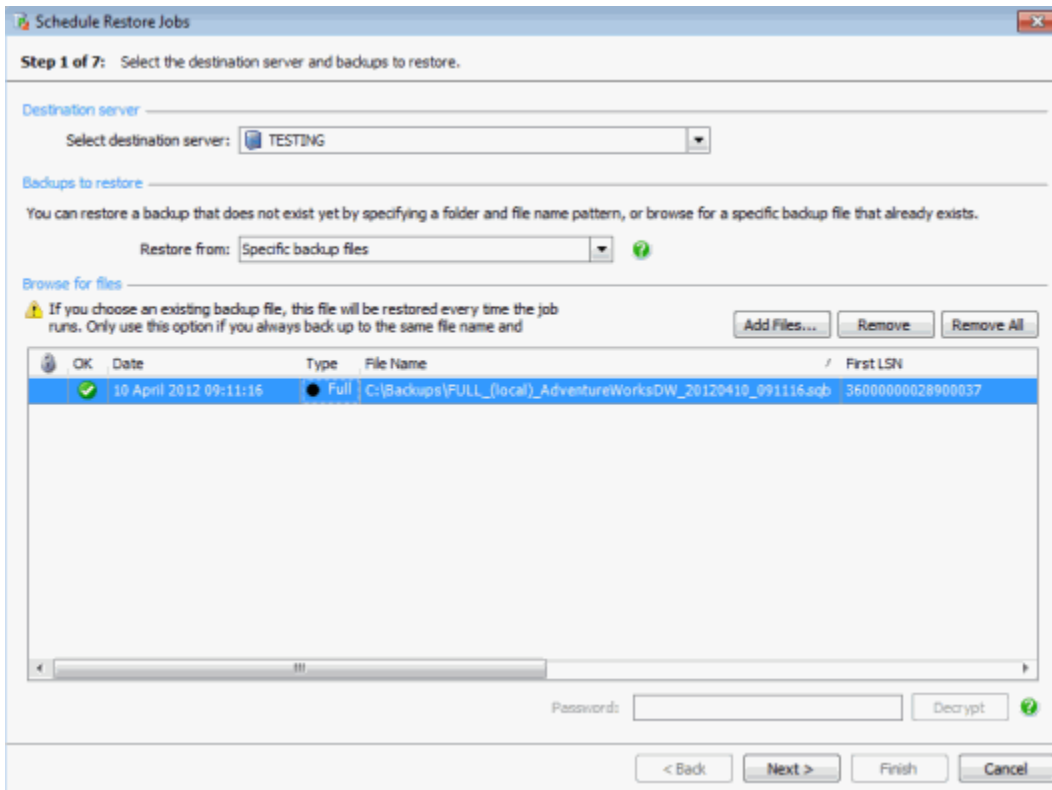
You must supply the password for any backups that will be encrypted. If you have selected **Latest backup set**, the same password will be applied to all encrypted backups. Any backups in the set which are not encrypted will also be included in the restore job.

If any of the backups have been encrypted with a different password, they will *not* be identified as part of the set and will *not* be included in the restore job. However, the restore will only fail if there are subsequent backups in the set which depend on the backup that has not been decrypted. If the last backups in the set have been encrypted with a different password, they will not be identified as part of the set and no error will be returned.




The plain text password will be stored in the job script. This is to prevent the obfuscated password from a backup script being used to restore an encrypted backup. You are recommended to secure the destination server (on which the restore job is created and stored) to prevent unauthorized access to your data.



Restoring from specific backup files



You can schedule a restore job for specific backup files which already exist. The file of that exact name will be restored every time the job runs. You may wish to select this option if you always back up to the same file name, for example *TestDB_FullBackup.sqb*, and store the file in the same location.

1. From the **Restore from** drop-down list, select **Specific backup files**.
2. Click **Add files** to display the File Browser. The backup files in the destination server's default backup location are displayed. To view files on a different server, select a different machine from the **Server** drop-down list. If the server you require is not displayed, click **Add Server** and type the server name or IP address. Other servers will only be visible to the local server if it has the appropriate permissions to write to or read from them. The name of the local server you are connected to and your user name are displayed above the **Server** list. This information may explain why some servers cannot be browsed.
3. You can restore only one database at a time; you can select either one full backup or a full backup, a subsequent differential backup and/or subsequent transaction log backups of the same database. If a backup is split into multiple files, you must select all the files which form the backup. Note that it is not possible to restore a differential backup or transaction log backup without a corresponding full backup.
4. If there is a problem with a backup file,  is displayed. Move your mouse pointer over the icon to see details of the error.

Encrypted backups

 is displayed next to encrypted backups. Type the password into **Password** and click **Decrypt**.  is displayed next to all backups to which the password applies. The selected backups must be decrypted before you can move on to the next step of the wizard.

SQL Backup Pro requires the plain text password to restore an encrypted backup. This is to prevent the possibility of an obfuscated password from a backup script being used to restore a database from an encrypted backup.



The plain text password will be stored in the restore job script. You are recommended to secure the destination server (on which the restore job is created and stored) to prevent unauthorized access to your data.

Next: [select the destination database](#)