



Guidance for Backing Up Your Accrivia System(s)

A reliable backup strategy is critical for all businesses and organisations. We strongly recommend you use a reputable third party backup solution, and implement and follow a rigid backup policy, including regularly testing the validity of any backups to minimise any potential losses. Your IT vendor is likely your best source of recommendations and assistance when considering specific products and in implementing a solution. You may want to share this document with them.

This document covers our general advice for backup strategies and the data that must be backed up to protect your Accrivia system from loss:

1. Backups **must** include these critical sources of data:

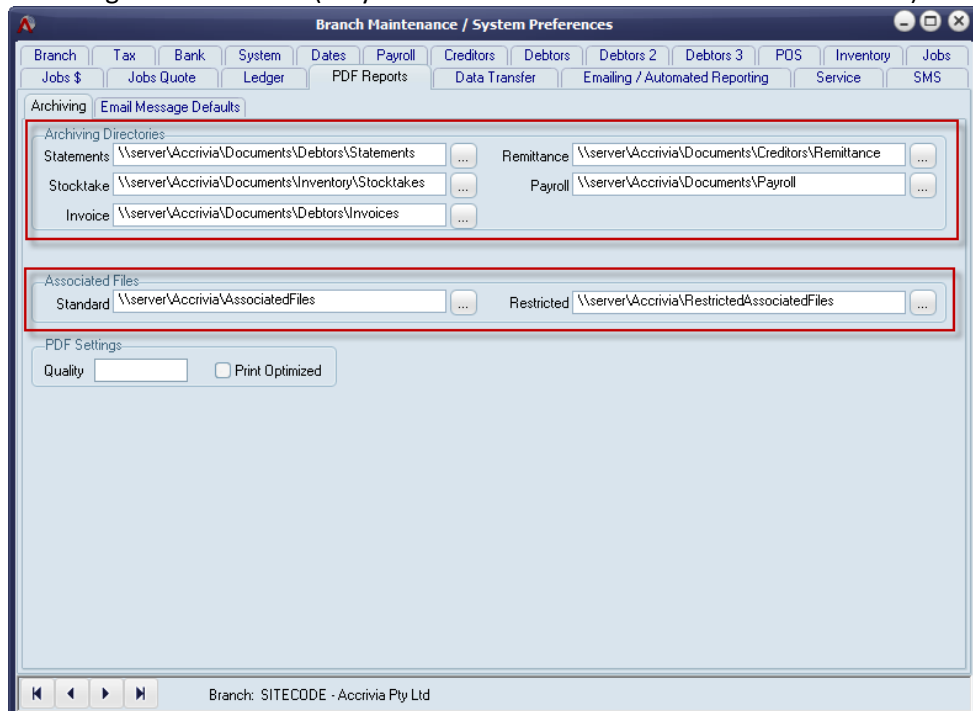
For each database / Accrivia system in use, you must backup the following set of folders. All data sources described here must be backed up if you require a full restore of your system.

a. Database

The Accrivia database is generally found in the db folder of your server's Accrivia share. If you run more than one database, and need assistance identifying the live databases, please contact the Accrivia Help Desk.

b. PDF Folders

Go to File – System – Settings – PDF Reports, and include each folder listed in the Archiving Directories box (may include additional folders to the ones shown).

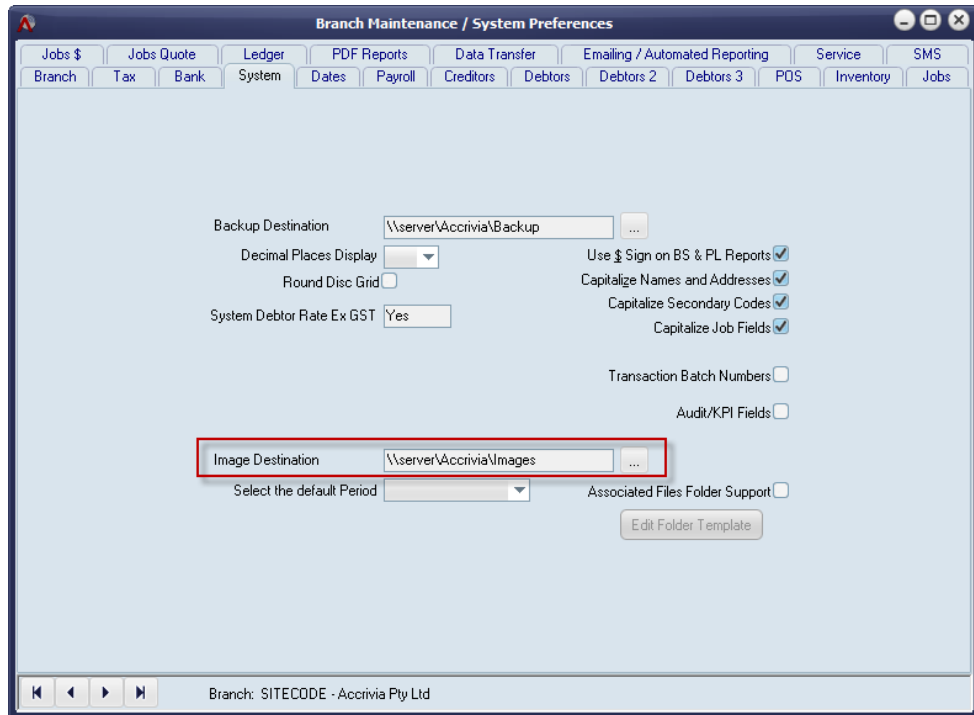


c. Associated Files Folders

Go to File – System – Settings – PDF Reports, and include the folders listed in the Associated Files (both Standard and Restricted) box.

d. Image Folder

If you use images in your Accrivia system (usually available in Inventory / Jobs systems), go to File – System – Settings – System, and identify the Images folder listed under Image Destination. If this field is not filled in you do not have an Images folder.



2. Backups need to be run regularly, preferably daily

A carefully planned system of full and incremental (i.e. only what has changed since the last full backup) backups can be efficient and provide a very good solution. To determine how frequently you should be completing a backup, answer the question – “How much data can you afford to lose if something happened?” A days worth? A weeks worth? This will guide how frequently you need to backup.

3. Your backup strategy should include separate periodic and offsite backups

To protect against threats such as hardware and backup media failure, dormant viruses, data corruption, physical risks (fire, theft) etc., full and separate backups that aren’t overwritten for a number of weeks and months, including secure off-site backups must be made. A sample backup strategy of an Accrivia system is included below to illustrate this.

4. Ensure backups are valid and are able to be restored

From time to time you need to test that you can restore your backups successfully to a separate location – if you discover that your backup system has failed in some way when you need it, it will be too late!

A Sample Backup Strategy

This sample backup strategy could be used as a basis to create your own backup schedule, and should be adjusted as necessary to meet your individual needs.

	<i>Floating</i>	Mon	Tues	Wed	Thurs	Fri
1 st of Month	Full <i>(plus test restore function)</i>					
Week 1		Incremental	Incremental	Incremental	Incremental	Full
Week 2		Incremental	Incremental	Incremental	Incremental	Full
Week 3		Incremental	Incremental	Incremental	Incremental	Full
Week 4		Incremental	Incremental	Incremental	Incremental	Full
Week 5		Incremental	Incremental	Incremental	Incremental	Full

Definitions:

Full: Full backup completed on 1st of Month and each Friday, includes a full backup of the Accrivia data (refer to list of critical data sources)

Incremental: Includes all changed files since the last full Friday backup of the of the Accrivia data (refer to list of critical data sources)

Other Notes:

- At least 12 months of historical monthly backups are retained at any given time
- Monthly, and Week 1, 2, 3, 4, and 5 (if relevant) backups are kept on separate physical backup media
- Backups are removed to the secure offsite fire-proof safe. The previous weeks backups may remain on-site for accessibility (e.g. in Week 3, the backups of Week 2 will be left onsite).
- Each month, a full Accrivia backup is restored, using a combination of a Thursday and Friday backup from a nominated week (to a separate location).

Legal Statement

The advice provided here is general in nature. We advise you to seek specific advice from a suitably qualified IT vendor to assess and implement your backup and security needs.

While the scope of Accrivia data required for a full backup is accurate at the time of producing this document, this may change from time to time, and we will update our published advice. You accept full responsibility to make yourself aware of any changes or additions to data sources that require backup.

We take no responsibility, financially or otherwise, for any loss or consequential damage associated with backup failures or loss of data of your system, and You hereby release us from any liability of whatsoever nature or howsoever arising which you may suffer as a result.