TANDBERG DATA

# AccuGuard™ Enterprise for RDX®

# QuikStart Guide V 1.0

TANDBERG DATA
AccuGuard™

P/N 1021249

## Prerequisites

Please check these prerequisites before installing the AccuGuard Enterprise for RDX software!

- All systems which should be backed up by AccuGuard Enterprise for RDX should be included in a domain.
- Identify a Windows 2008 or newer server to use for the software installation of the AccuGuard Enterprise for RDX software. This will be referenced as the Archive Manager server. The Archive Manager server should have access to enough storage for your backup data.
- Join the Archive Manger server to the domain, if it is not already.
  NOTE: If you added the system to the domain, the server must be rebooted before continuing.
- Install .NET 3.5 and Desktop Experience Features. Follow the instructions below for operating system the Archive Manager server is running.
  - On Windows 2008, you must install the 'Desktop Experience' feature before installing this product.
    - Click “Start”, point to “Administrative Tools”, and then click “Server Manager”.
    - In Server Manager, click “Features”, and then in the Server Manager “details pane”, under Features Summary, click “Add Features”. The “Add Features” Wizard starts.
    - In the Features list, select “Desktop Experience”, and then click “Install”.
    - You will need to restart the computer to complete the installation.
  - On Windows 2008 R2, you must install the 'Desktop Experience' and '.NET Framework 3.5.1' features before installing this product.
    - Click Start, point to “Administrative Tools”, and then click “Server Manager”.
    - In Server Manager, click “Features”, and then in the Server Manager “details pane”, under Features Summary, click “Add Features”. The “Add Features” Wizard starts.
    - In the Features list, select “Desktop Experience” and then expand the .Net Framework 3.5.1 Features and select “.Net Framework 3.5.1.” Then click “Install”.
    - You will need to restart the computer to complete the installation.

- On Windows 2012 and 2012 R2, you must install the 'Desktop Experience' and '.NET Framework 3.5' features before installing the product.
  - From the Server Manager, Manage pull-down menu, start the “Add Roles and Features” Wizard.
  - Click “Next” until the Select Features page is displayed.
  - In the Select Features page Features list, select “.NET Framework 3.5 Features”, then expand the User Interfaces and Infrastructure feature and select “Desktop Experience”. Click the “Add Features” button when asked to install the Desktop Experience prerequisites. Click “Next”, and then “Install”.
  - You will need to restart the computer to complete the installation.

- There is a requirement to use a Domain Administrator account for configuring the software, running the protection plans on remote computers, and maintenance tasks for stores. A recommendation is to create a separate backup user account, e.g. ‘backupuser’. The account that you identify or create is referred to as the backup account or ‘run as’ account within the software.
- Log into the server with an account that is a member of the Domain Admins group. This will facilitate setting up protection plans on desktops and servers in your environment.

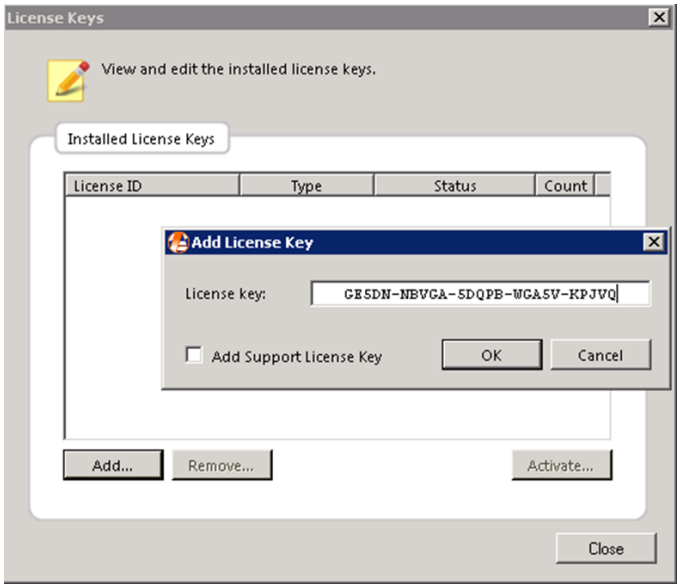
## Install the Software

Install the software on the main backup server by double clicking the AccuGuard setup file, available for download after registration at the Tandberg data web-site (see instructions on the insert card). Follow the instructions on the screen. Once installation is complete, the software opens and prompts for a license or licenses to be added. There are three options to add a license key:

- Add a license key (if you already got one, i.e. sent via email)
- Buy now online (to purchase licenses)
- Register for evaluation (if you participate the 30-days trial)

### Insert license keys

To insert a license key, click the “Add” button. Insert the key into the appropriate field and click “OK”. Hereafter, a new screen appears for activating the key. You can activate either over the internet or telephone. Repeat these steps for further licenses. For inserting support keys, activate the checkbox “Add Support License Key” to get an additional entry-field.




**Note**: There must be a RDX drive attached to activate the license keys.

**Note**: There are three or more keys you must activate before you can use the AccuGuard Enterprise for RDX software:

- The Manager key
- Remote Server Computer key
- Remote Desktop Computer key
- Remote Desktop Computer 10-pack key
- Optional Extended Support key

### Launch Software

If software updates are available, the AccuGuard Enterprise for RDX Upgrade wizard opens to update the software. Click “Download” to start the process.

**Note**: You can also verify you have the most current version of the software by clicking the “Check for Updates...” link in the right pane of the AccuGuard Enterprise for RDX interface.

## Setup the Software

There are up to 5 steps to setup AccuGuard Enterprise for RDX:

1. Define Store(s)
2. Define Local Protection Plan(s)
3. Add Remote Computer(s) (Optional)
4. Define Remote Computer Protection Plan(s) (Optional)
5. Define Copy, Expiration, Purge, Verify Tasks (Optional)

### 1. Create a Store

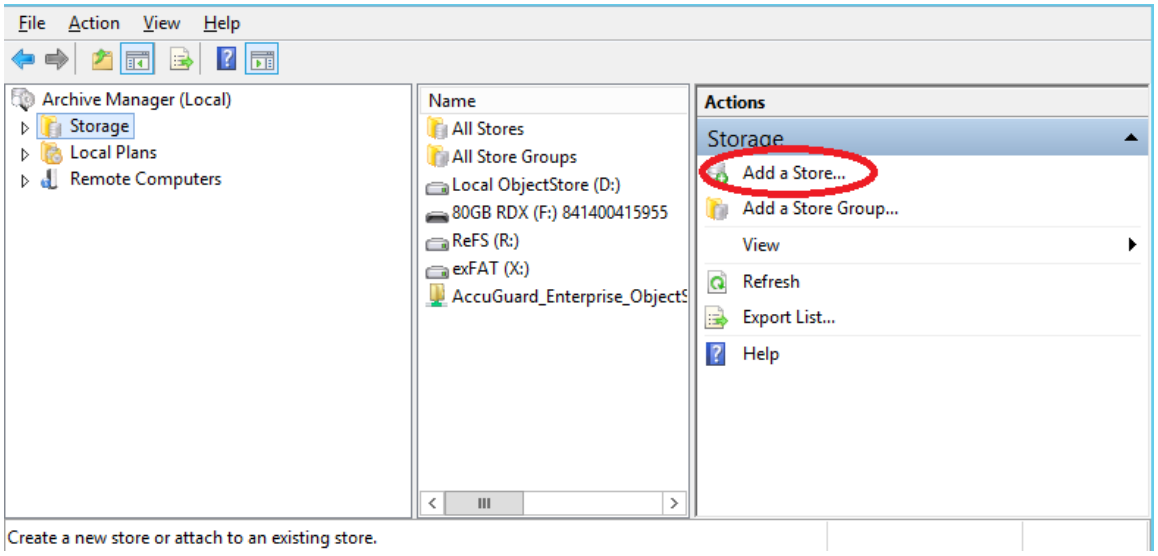
Store Architecture Recommendations:

Multiple stores may be set up to house different kinds of data, or to balance disk space requirements. To achieve maximum performance of maintenance tasks (e.g. copy store tasks, store expiration and purge) proper planning of the number, location, and size of stores is required.

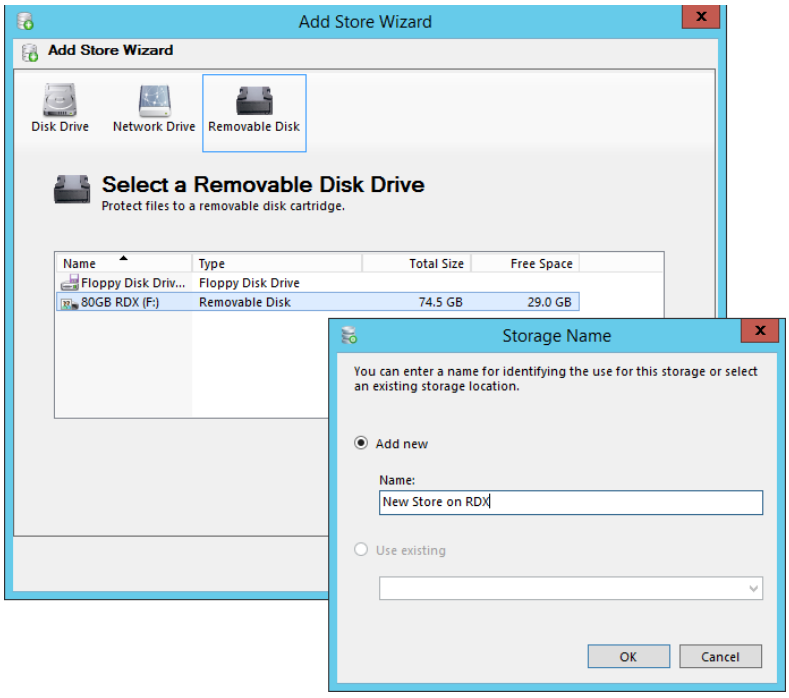
- Multiple Stores may be created within AccuGuard Enterprise for RDX. Consider creating at least two stores. One for backup data and one for backup databases and exchange. Files have a greater probability to match across servers, so the optimum deduplication could be achieved. This improves the store expiration and validation time windows.
- The Single Instance Storage capability of AccuGuard Enterprise ensures that equal files and blocks across different computers and servers, are only stored once in the backup target (store). So, target the backup jobs of your computers and servers with the highest level of identical data to the same store.

To create a store:

- Click on “Storage” on the left side of the screen, select “Add Store” on the right pane.




- Choose the store location on your storage device and name the store, click “OK”.

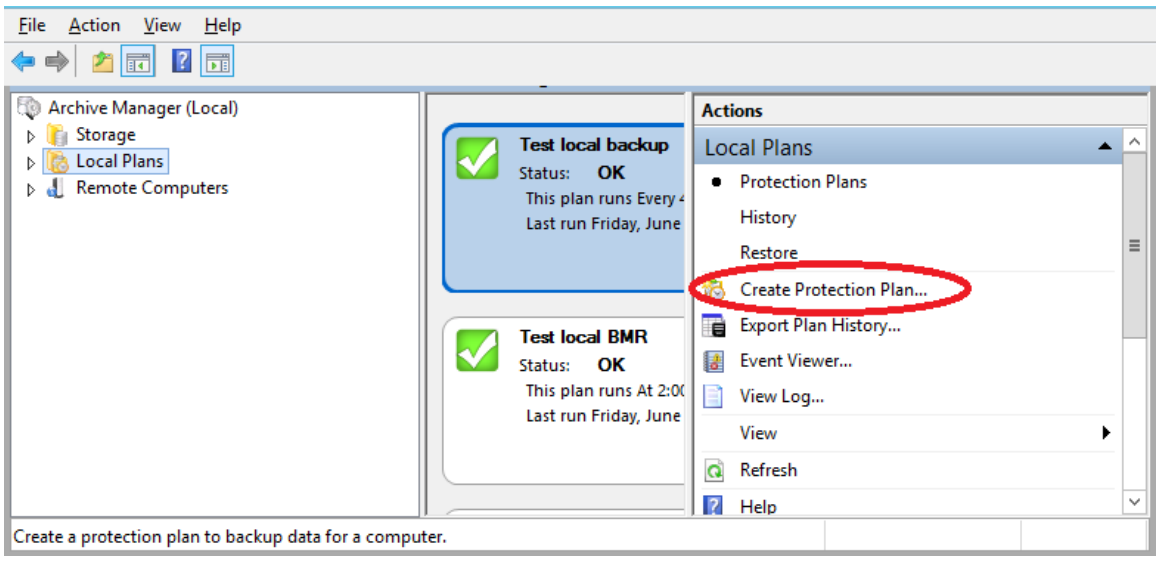



- Click “Prepare Store”, your store is now ready to use. Repeat for further stores.

## 2. Define Local Protection Plans

The local protection plan is a backup job for the AccuGuard Enterprise for RDX server itself. Consider to create different protection plans for your entire system and for your data, as different schedules could be established dependent on importance of the data.

- Click “Create Protection Plan” from the Actions Pane (right pane).




- Select one of the following: Files and Folders, SQL Databases, or Exchange Data, Computer System.

**Note**: The options to select SQL Databases or Exchange Data only apply if the computer has SQL or Exchange installed.

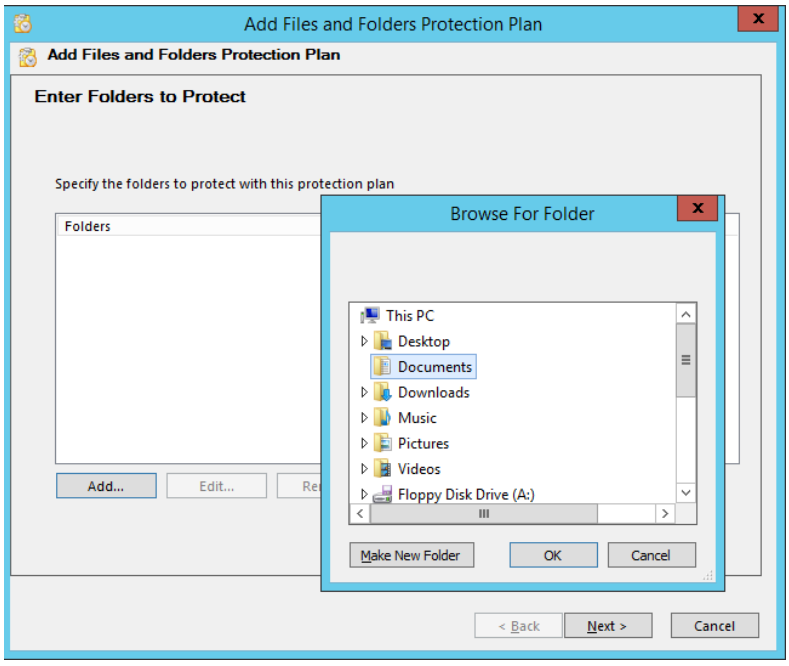
Follow the Plan wizard to create a plan:

- Choose the data to protect (files and folders, computer systems, databases).
- Select a store.
- Type a plan name. A best practice is to use a naming convention of <server>-<data>, e.g. myfs1-d drive.
- Set a backup schedule. Under Security Options, enter an account with Domain Admins group membership. Enter the backup service account discussed above if you prepared one.
- Click Next
- Click finish

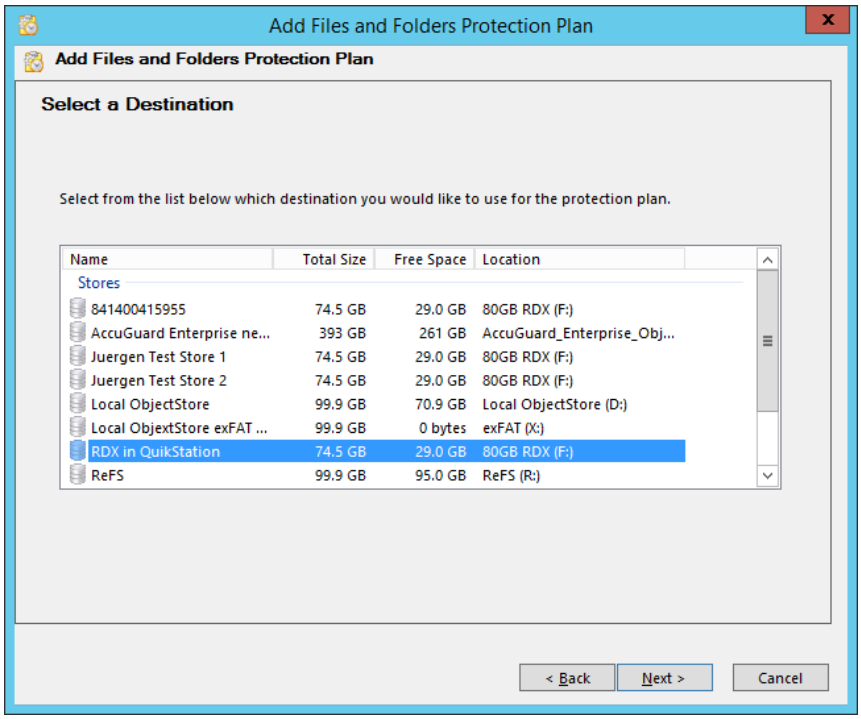
Type the requested administrator password for the computer. Click “OK”.

**Note**: A best practice is to create a backup user account in the domain that is a member of the domain administrators group.

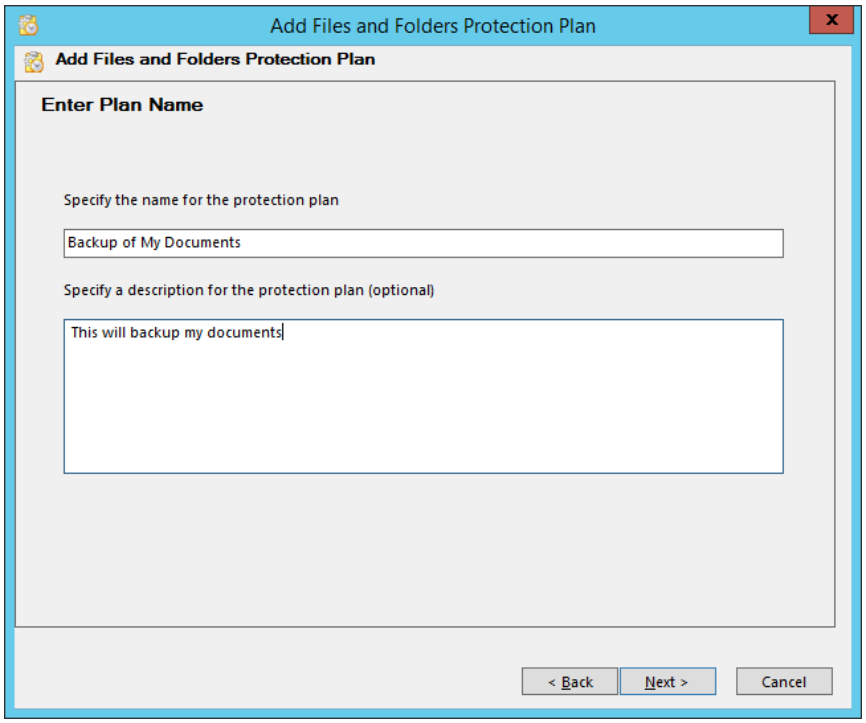
See screenshot examples of creating a protection plan:



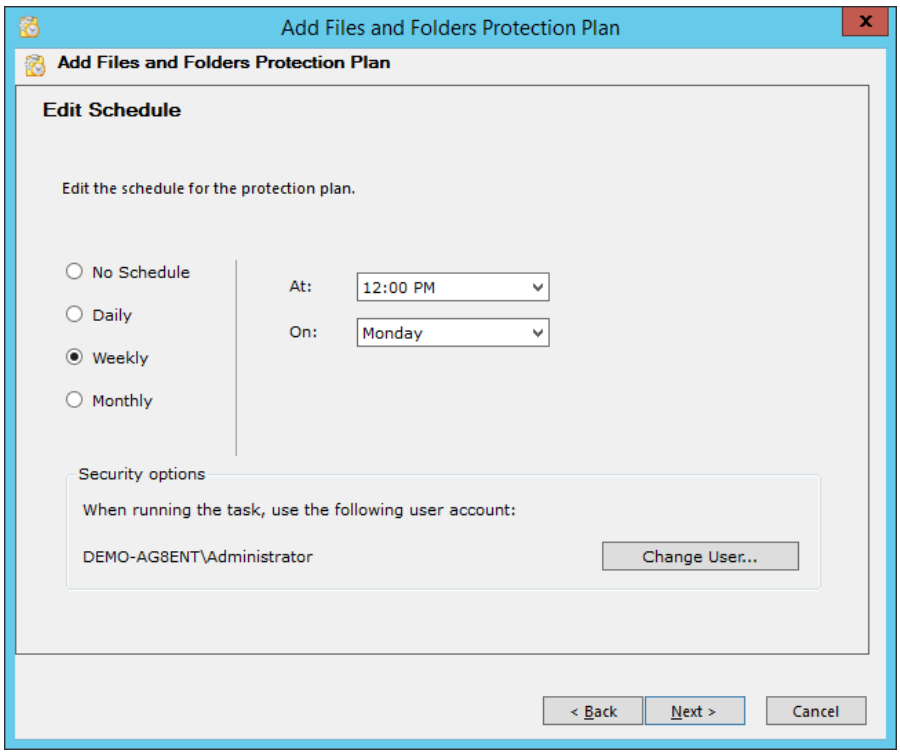

1. Select a folder




2. Select a store




3. Enter a plan name




4. Choose a schedule

### 3. Add remote computer

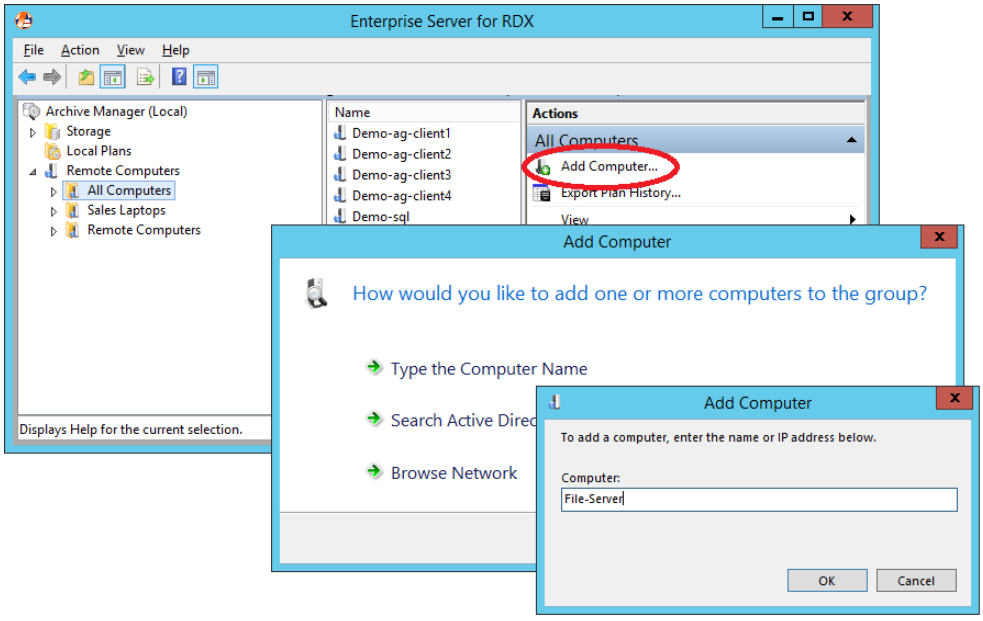
AccuGuard Enterprise for RDX is able to protect additional servers and desktops beside the Archive Manager Server. Therefore, additional remote computers can be added to the software.

**Note**: Additional licenses have to be obtained.

**Note**: All remote computers should be in the same domain and an equal backup-user should be created on each system.

The following steps have to be performed:

- Expand “Remote Computers” in the left pane of the AccuGuard Enterprise Shield interface.
- Click “All Computers” from the left pane.
- Click “Add Computer...” from the right pane.
- Select one of the methods listed (browse network, search active directory, or type computer name) to add a computer.
- Click OK.
- Repeat the process to add more remote computer clients.



### 4. Define Remote Computer Protection Plan(s) (Optional)

The remote computer protection plan is a backup job for the remote servers or desktops added above. The procedure is the same as for the local computer. The entire remote computer has to be selected first:

- Expand “Remote Computers” in the left pane of the AccuGuard Enterprise Shield interface.
- Click “All Computers” from the left pane.
- Select the remote computer you want to create the protection plan.
- Click “Create Protection Plan...” from the right pane.
- Refer to “Define Local Protection Plans” in this manual

### 5. Define Copy, Expiration, Purge, Verify Tasks (Optional)

In addition to the backup plan, tasks can be performed on stores. Therefore, the relationship between backup jobs and stores should be considered. The following tasks are available:

- Store copy tasks allow you to copy the contents of one store to another, i.e. to create a second backup for off-site vaulting. You can copy stores within the same AccuGuard Enterprise system, or you can copy stores to or from another system.
- By default, all data is retained indefinitely in a store. A store expiration task lets you set the number of days that data is retained in a store and how often to expire the data. Only one store expiration task is allowed per store. The expiration process looks at each archive within the store to determine what is eligible for expiration and moves those point-in-time catalogs (restore points) to the store Recycle Bin folder.
- Expired items can be removed (purged) from the Recycle Bin with a store purge task. Purging also scans the entire store for data no longer referenced. Unreferenced data is then deleted and the integrity of the store is verified before the purge process is completed.
- To maintain store integrity, the software can verify the contents of a store and identify corrupt files sometimes caused by disk corruptions. If a corrupt file is found, it is moved to the store Quarantined Items folder.

For further information please refer to the “Store Tasks” section of the user manual.