Path to Tape Quick Start Guide

6-67752-02 Rev A, January 2013

Path to Tape Quick Start Guide
6-67752-02 Rev A
January 2013

Path to Tape Quick Start Guide

This document will lead you from installation, to archiving data to tape, to restoring data from tape. (For more information, go to http://www.quantum.com/ServiceandSupport/Index.aspx.) It is designed to give you a quick introduction to the product using default settings. From here you can further your understanding of the product by exploring and referring to the online documentation and the **context-sensitive Help buttons**. It assumes you have the setup program and necessary license keys. Also, the computer that you will install to and the computers you wish to back up must be in the same Windows domain and you should have a domain administrator account dedicated to running this software.

Note: If you are familiar with the product and only want to learn about the new tape support feature you can skip to step 5.

For more information, see 6-67520-XX *DATASTOR Shield Quick Start Guide* for minimum system requirements and details on installing the product.

Step 1) Install the product

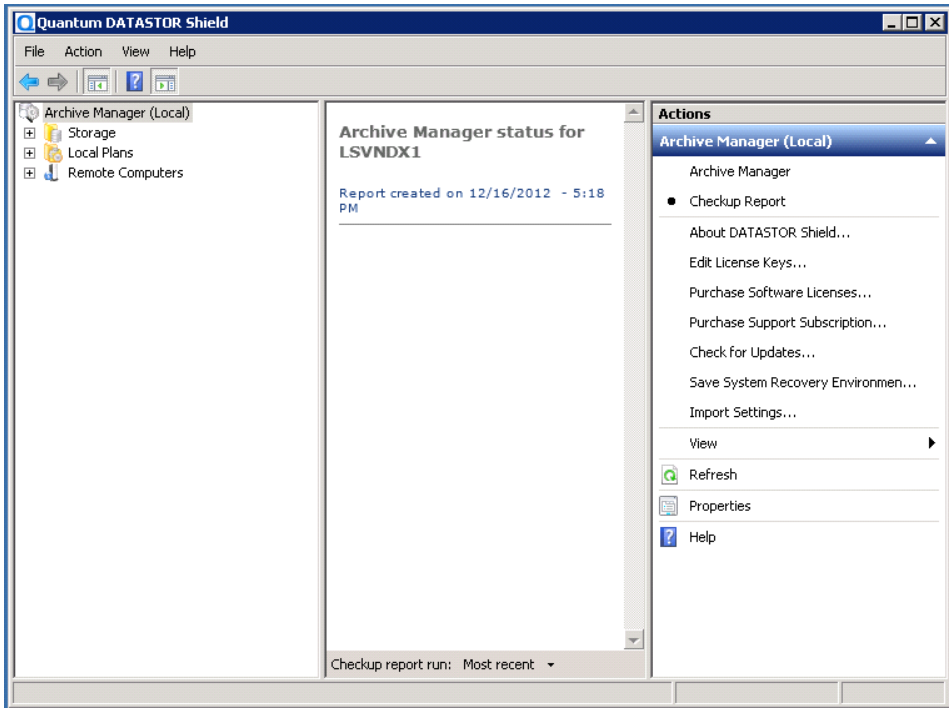
Log onto the computer where you are going to install the product (later referred to as the "Archive Manager server") using the dedicated domain administrator account. Open the setup program Quantum_DATASTOR_Shield_7.x.x.x.exe and follow the prompts to install the program.

When the installation completes, the Archive Manager user interface (later referred to as the "UI") will start up. You will be prompted to add a license key, buy now online, or register for evaluation. Choose Add a License Key and then click Add on the License Keys page. Enter (or paste) your Manager key first and then click Activate Now on the Server Activation page. You should receive a popup message saying the software has been activated. Repeat the Add/Activate steps for each of your keys. In order to complete the steps outlined in this guide you should have a Manager key and possibly a Tape Automation Option key. Some versions of the product automatically include tape library support without requiring a Tape Automation Option key. If you want to archive data from a remote computer you will also need at least one Remote Server key and optionally one Remote Desktop key. Click on the OK button when you have finished entering license keys. Note: You can return to the License Keys page at any time by choosing the Edit License Keys action on the Archive Manager node of the tree view (top node in the left-hand pane of the UI).

After clicking OK on the license keys page the program will start its services and check for program updates. You will be notified if any updates are available.

Step 2) Schedule the Checkup Report

It is important to set up a schedule for the Checkup Report. Setup is accessed by selecting the Properties option under the Archive Manager.

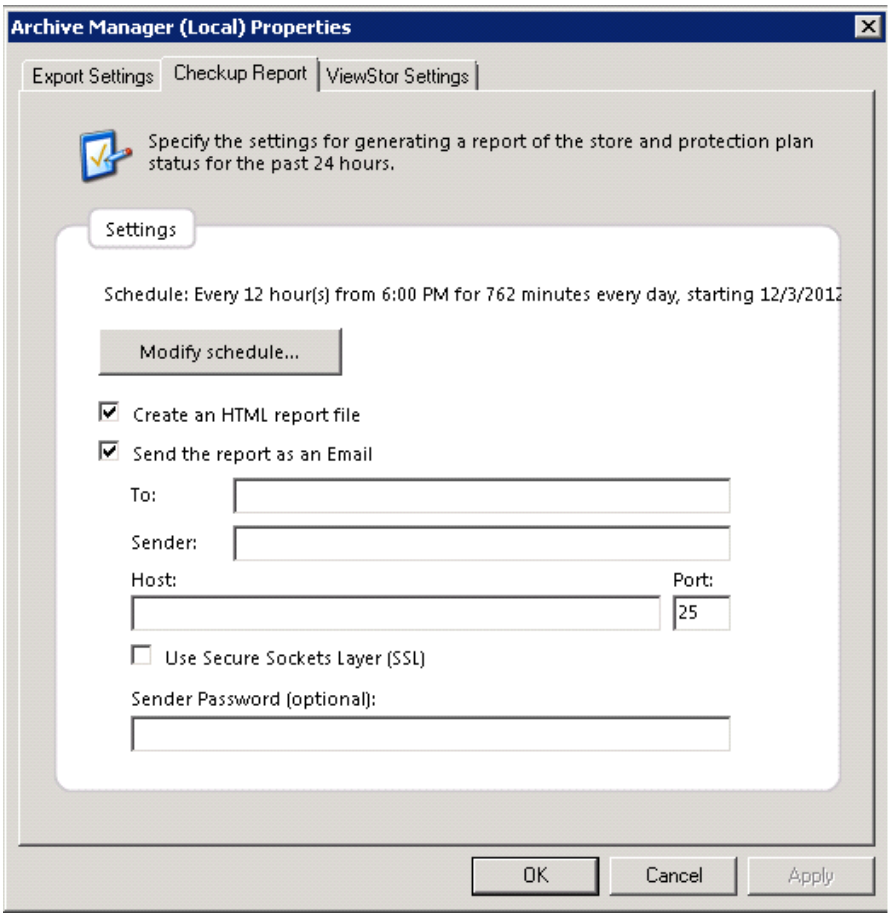


Enter the email address the report should be sent to.

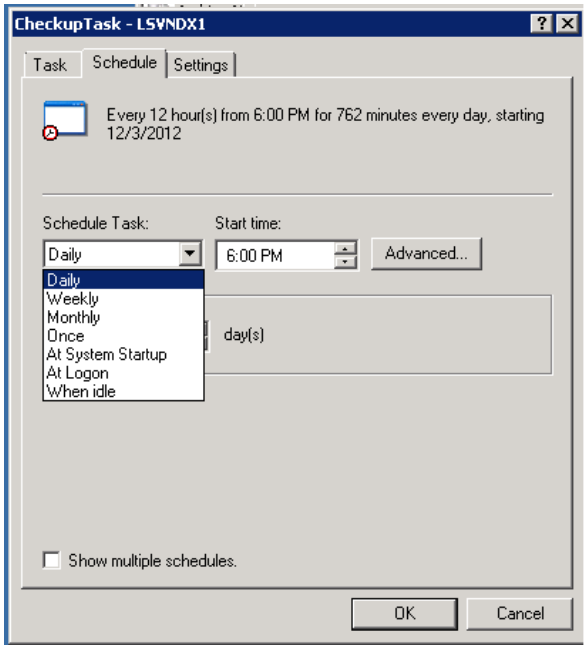
Enter the email address of the sender.

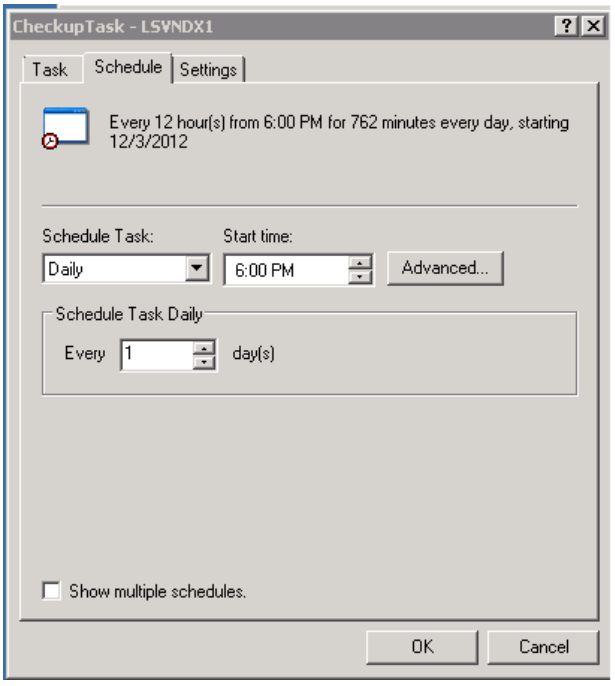
Enter the Host email server's name.

Then select Modify schedule…

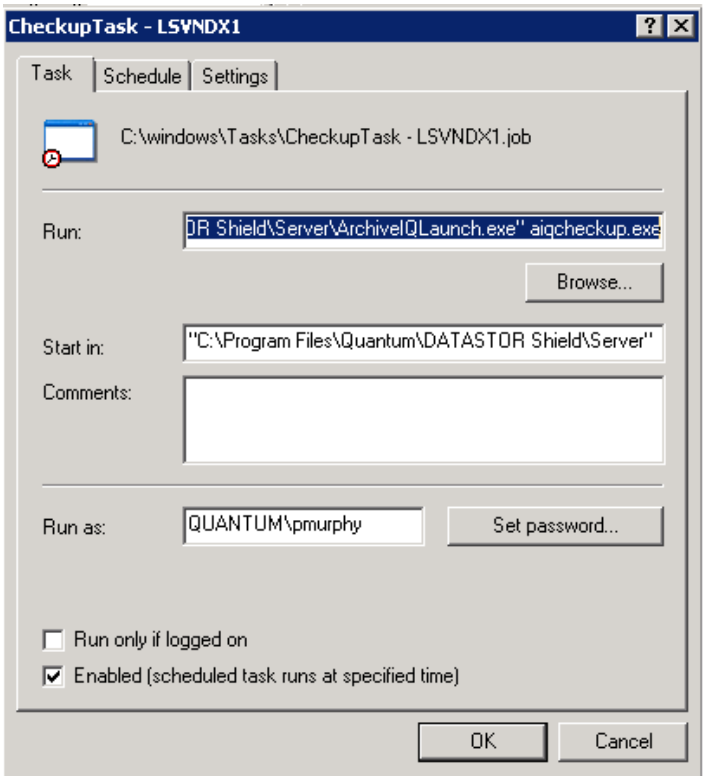


Schedule the task.

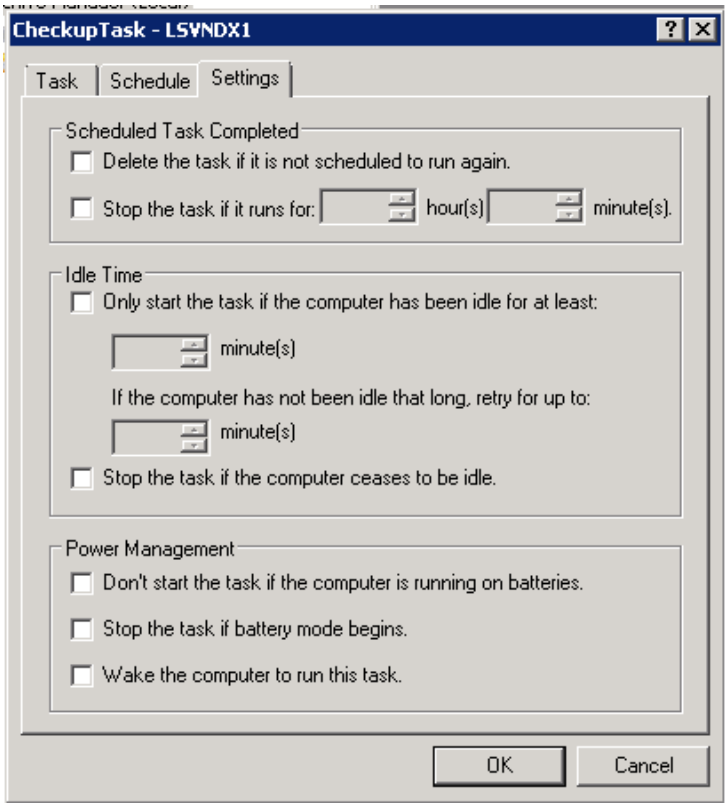




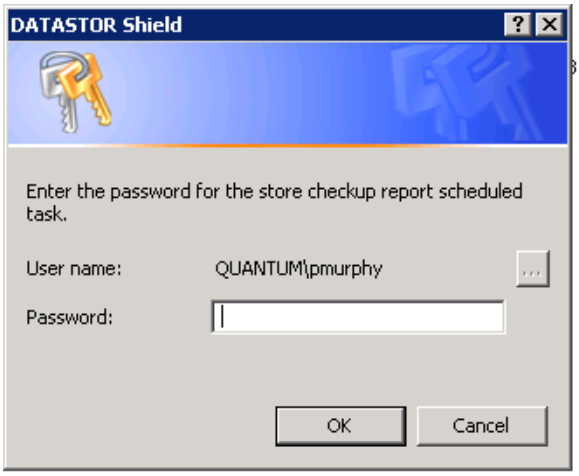
The fields for Run: and Start in: will automatically populate after the schedule is setup.



Select additional settings that are appropriate for your installation.



Finally enter your administrator password to save the scheduled task.



Step 3) Schedule the Export Settings Task

The **Archive Manager** system can automatically create restore points of its configuration files. Archives protected by Store Vaulting Tasks can also be recovered if the vault is available. This section shows how to save and restore the configuration files.

Usage Scenario

When setting up your Archive Manager computer, Quantum suggests that you schedule an **Export Settings Task** *to archive your settings to a folder location on a removable disk, such as an RDX, or to cloud storage*. This enables you to quickly and easily restore your system and data if your Archive Manager computer dies.

Schedule the Export Settings Task

To configure the system to save configuration settings, open the **Archive Manager Properties** page and choose the **Export Settings** tab.

This feature runs as a scheduled task, called "*ExportSettingsTask - <computername>*." As with Store Tasks and Protection Plans, you can set a schedule for automatically running this task. You can also run the task manually from the Windows Task Scheduler.

To create a new task, select **Modify Schedule** and then click **New** on the **Schedule** tab to create the task.

The settings are exported into a compressed file, which you can use to restore them later. Quantum suggests that you save your settings either to a folder on a removable disk, such as an RDX, or, if you have set up a Cloud Account, to that account.

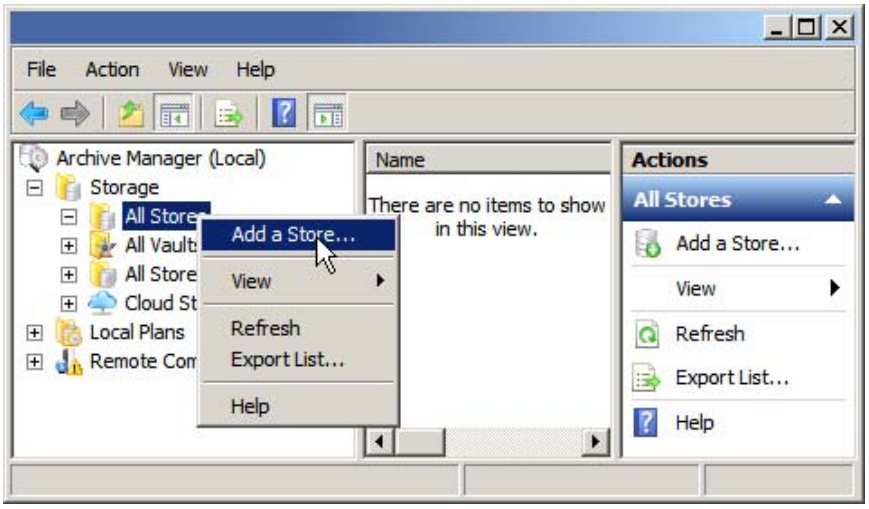
Choose where to save the export file, then specify a number of versions to keep. Oldest versions beyond the number to keep will be deleted. The export file name contains a timestamp indicating when the export was performed, and the computer name of the system that was exported, as follows:

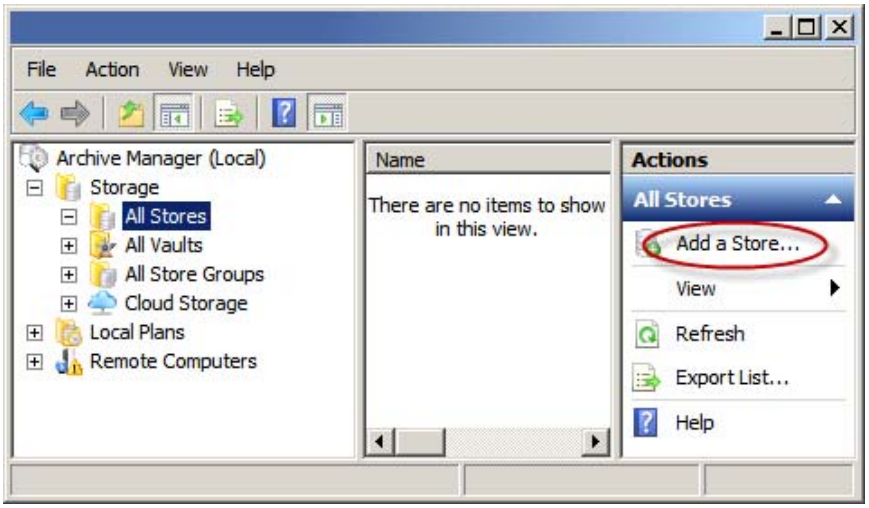
<computer name>.<timestamp>.export.zip.

Note: When you save to a Cloud Account, the exported file will be saved to the default data center specified in the account's Properties page.

Step 4) Create a Store

A store is where your deduplicated data will reside after running a protection plan. Select either the Storage node or the All Stores node and then click its Add a Store action. Note: Actions for a highlighted node can be selected from three locations: right-clicking the node, the Actions pane (right-hand pane of the UI), or the Action drop-down from the menu bar.

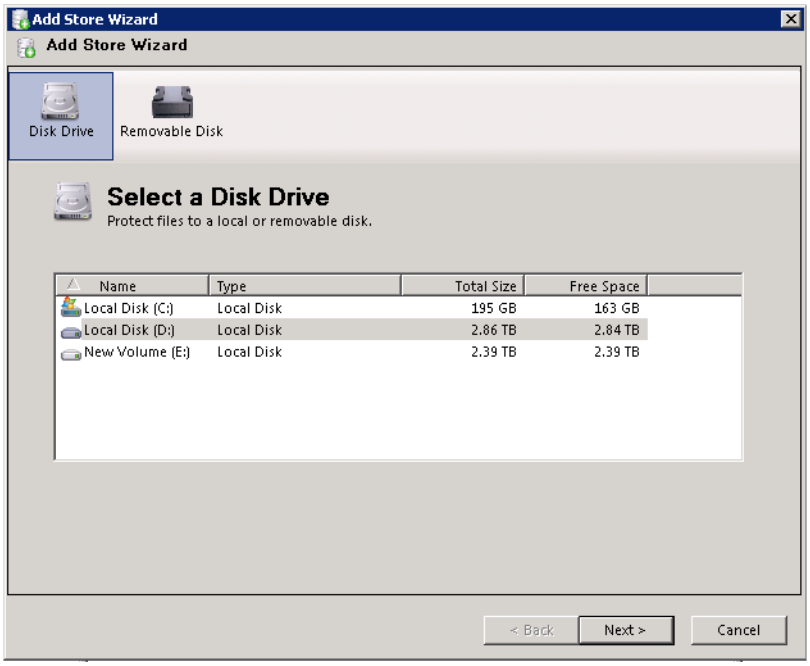




Notice the 'caution' icon on the Remote Computers node in the screenshots above. This is because no Remote Server/Desktop keys have been added. Clicking on the Remote Computers node will prompt you for a license key, or

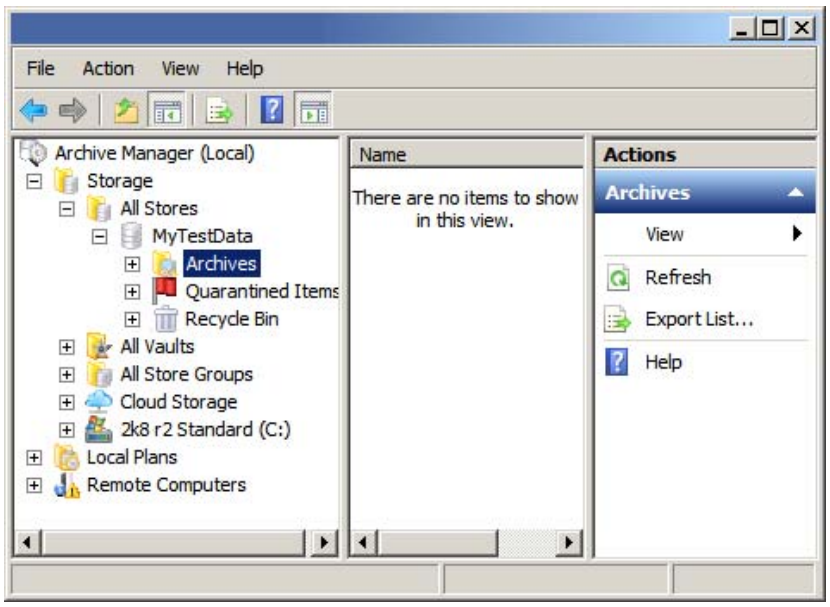
you can highlight the Archive Manager node and choose its Add License Keys action.

Depending on your product version, stores can be on local disks, network drives, removable disks such as RDX, or in Windows folders. You can create as many stores as needed, at any time. The store location you choose should, as a rule of thumb, have as much free space as the data you will be protecting.



For now, choose Disk Drive and then select one from the list, then click Next to go to the Storage Name page.

On the Storage Name page, under Add new, give your store a meaningful name like MyTestData, and then click OK. (This guide assumes you called it MyTestData) The program must 'prepare' the store prior to use. Click the 'Prepare now' button on the Prepare Store page. Click Next when the preparation is complete. Review the information on the Store Added page and then click the Finish button.

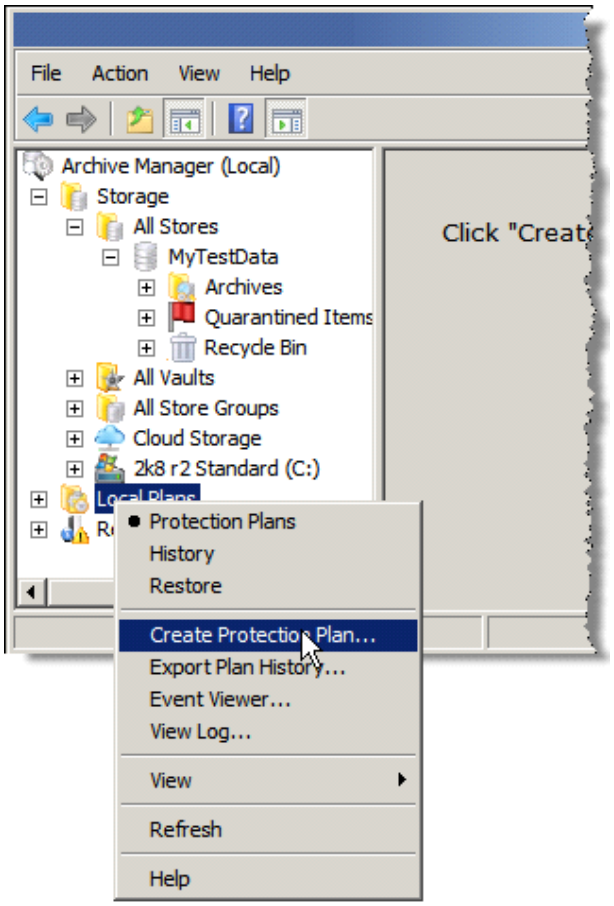


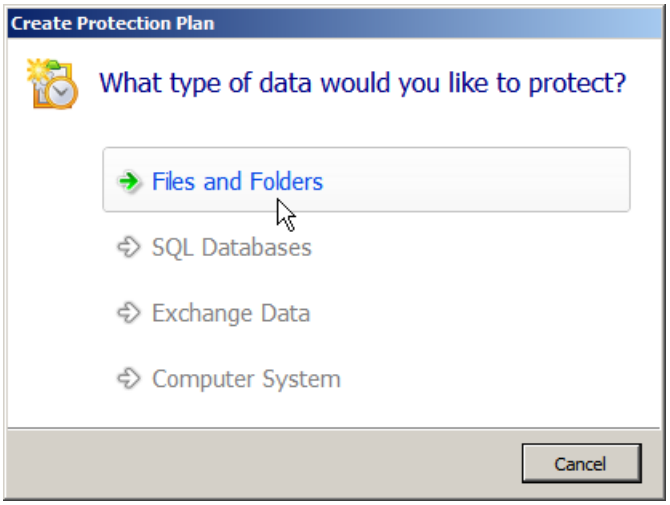
Your new store should appear under the Storage/All Stores node when the All Stores node is expanded (click the '+' to expand). Note: You may need to 'refresh' the view from one of the higher-up nodes. Expand MyTestData and then Archives. Notice there are no archives in the Archives node. We'll get to this later.

Step 5) Create a Protection Plan

A Protection Plan is what archives your data. It runs as a Windows Scheduled Task and contains information like what data to archive and which store to archive it to. Protection plans can be Local Protection Plans which protect data from the Archive Manager server and, if you have added one or more Remote Computers, there can be Remote Protection Plans to protect data from remote computers. Data protected by Remote Protection Plans is deduplicated on the remote computer before it is sent over the network to a store on the Archive Manager server. For this exercise we'll create a local protection plan.

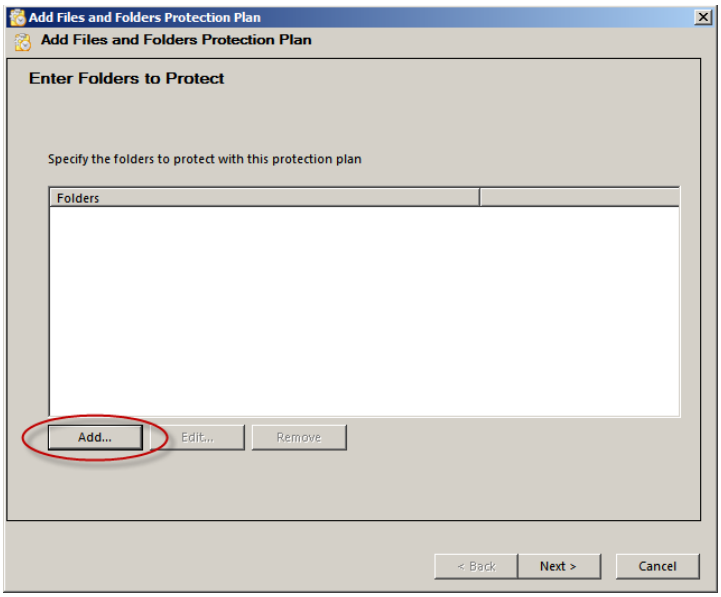
Highlight the Local Plans node by clicking on it. Notice that in the center pane of the UI it says to click "Create Protection Plan" to start protecting your data. Select the Create a Protection Plan action and then choose the type of data you would like to protect. For this example choose Files and Folders. The other types of plans are available based on the existence of the data type (i.e. is SQL installed on the computer?), the product version and installed license keys.



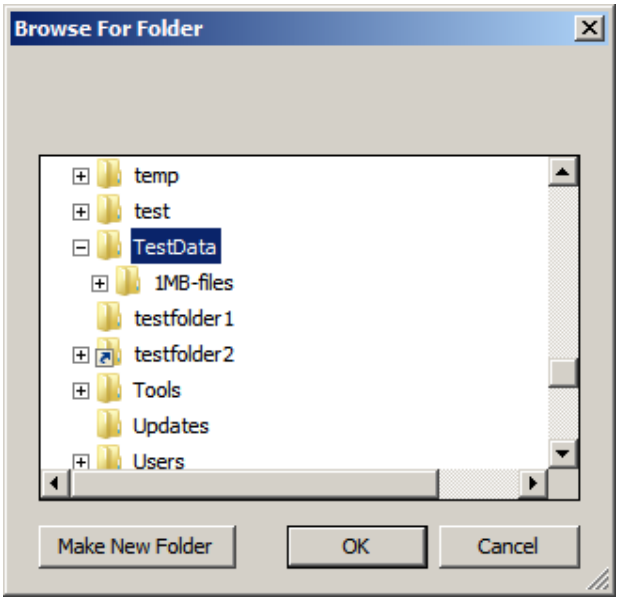


There may or may not be a Plan Configuration page. If there is, click Next to create a new configuration for this plan.

On the Enter Folders to Protect page click the Add button to open the Browse For Folder dialog.

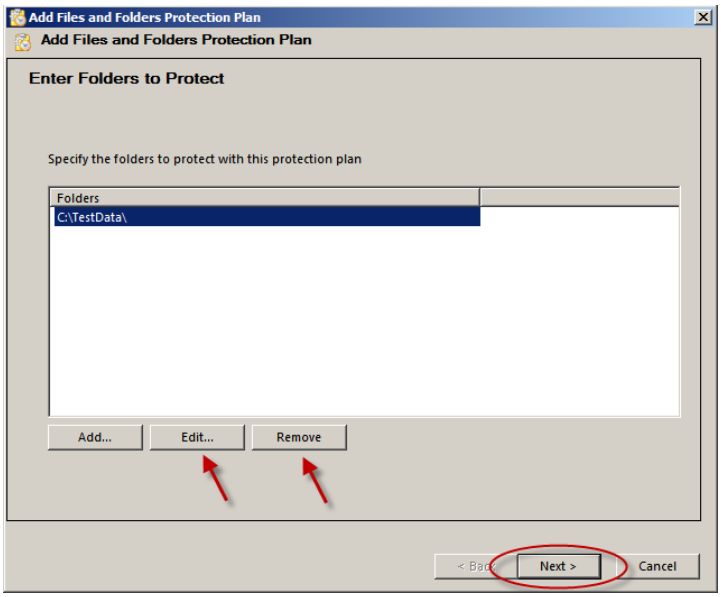


Browse for folders you wish to protect with this protection plan. Highlight the folder you wish to protect, and then click OK.

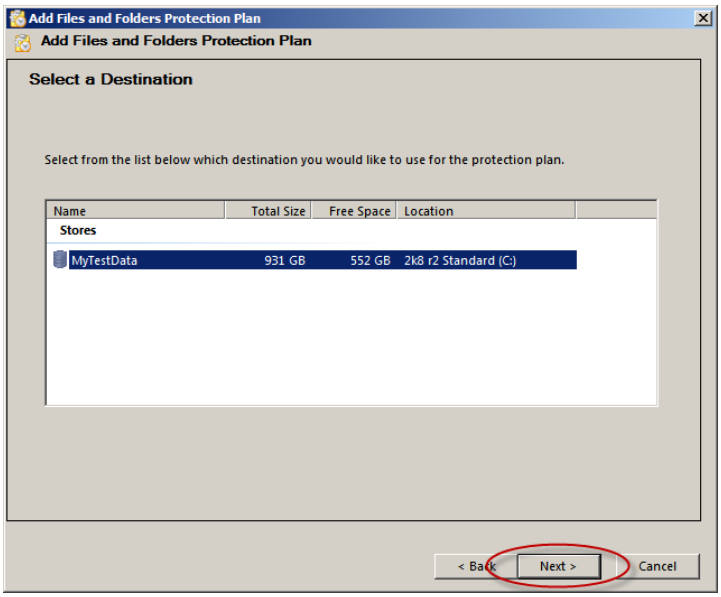


Notice that when your folder selection is highlighted in the Enter Folders to Protect screen, you can Edit or Remove the selection. If you choose Edit you can further refine the selection by adding inclusion and exclusion rules. You can also click Add again to add more folders to protect. You can make these changes later by clicking the protection plan's Plan Settings action.

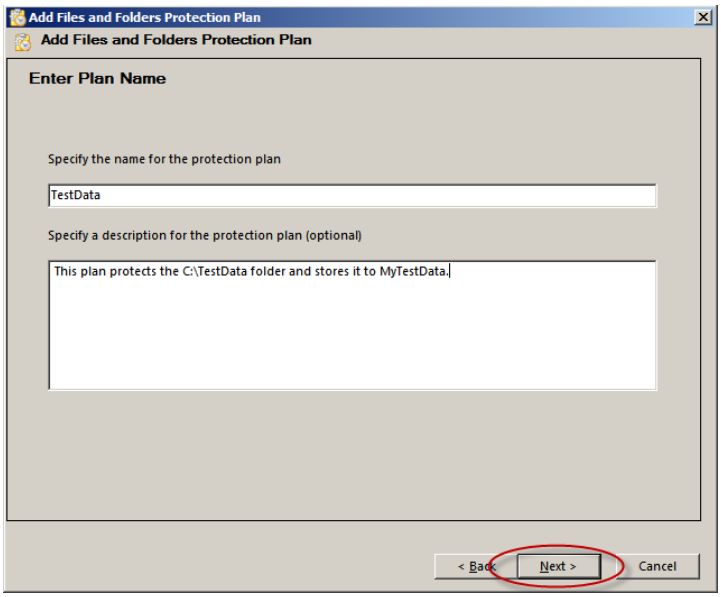
In this case, the folder TestData and all of its folders/files will be protected by the plan.



Click Next to continue to the Select a Destination screen. Here you will choose the Store where you want to keep your deduplicated data. Since we only created one store the choice is easy. Highlight the store and click Next.

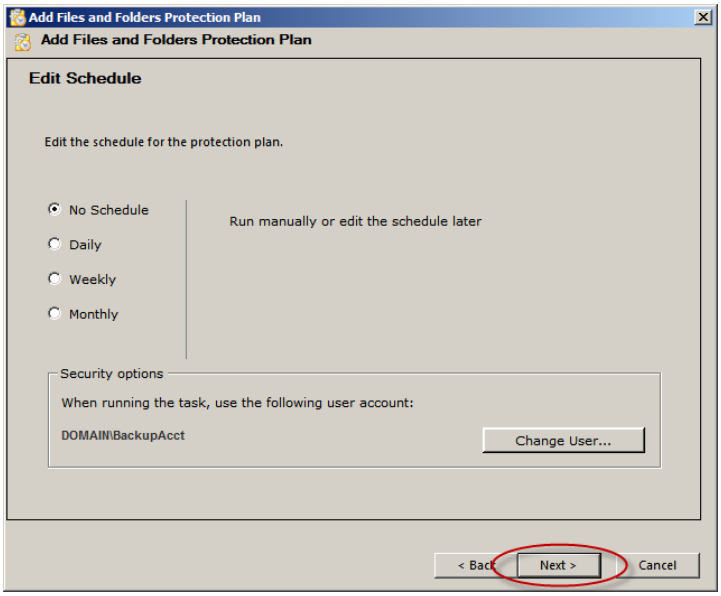


On the Enter Plan Name screen give your plan a meaningful name. For this example we'll call it TestData. You can optionally give it a description. Click Next to continue to the Edit Schedule screen.

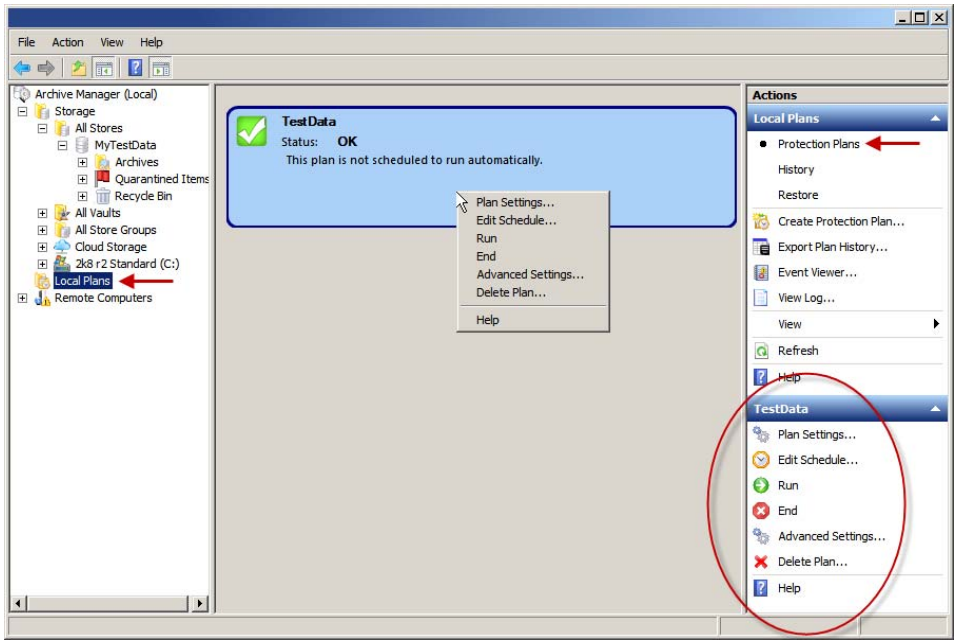


On the Edit Schedule screen you can configure a schedule for automatically running the Protection Plan. By default the plan will not have a schedule and will run as the currently-logged-on user. You can change who the plan runs as by clicking the Change User button and you can configure a schedule by changing the selected radio button. You can also make these changes later by clicking the plan's Edit Schedule action. Regardless of the schedule settings, you can run the plan at any time by clicking its Run action.

For this example let's just accept the defaults: no schedule and run as currently-logged-on user. Click Next to continue.

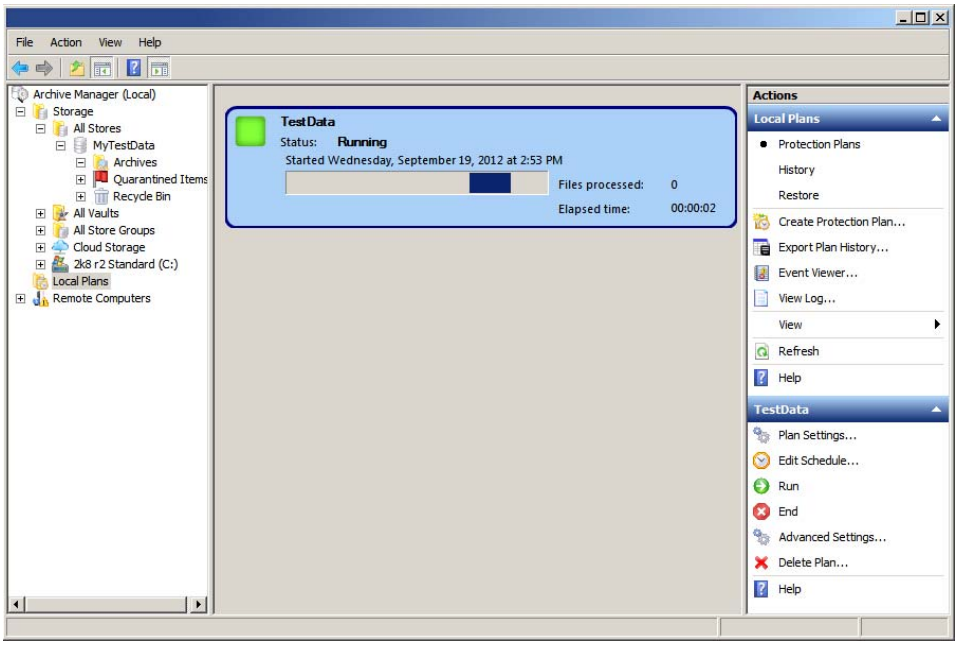


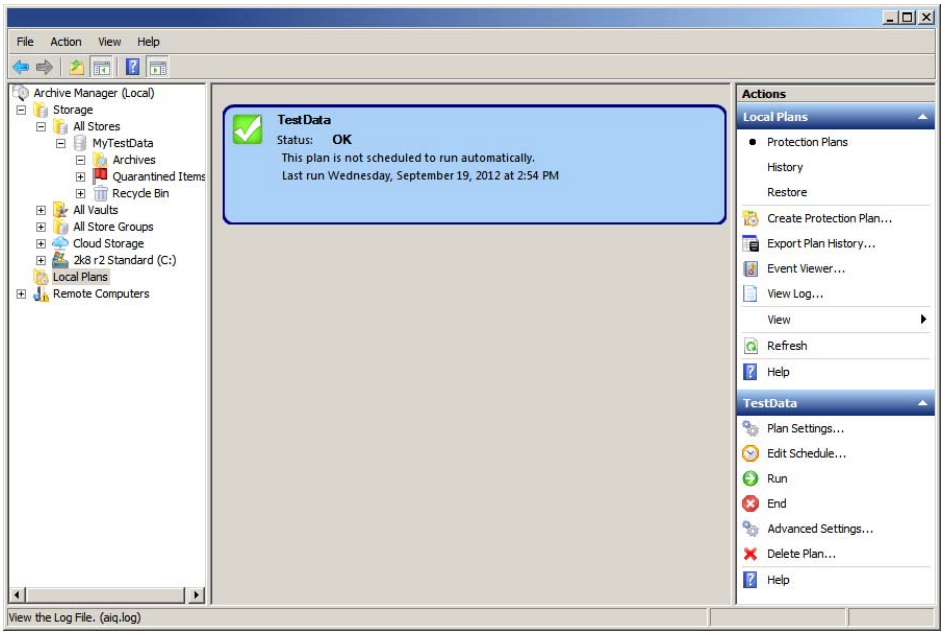
Review the summary on the Completing the Add Files and Folders Protection Plan wizard and click the Back button to make any adjustments. Click Finish to accept the settings and exit the wizard. Enter the password for running the scheduled task when prompted. The new protection plan will now appear in the middle pane of the UI when the Local Plans node is highlighted and its Protection Plans action is selected.



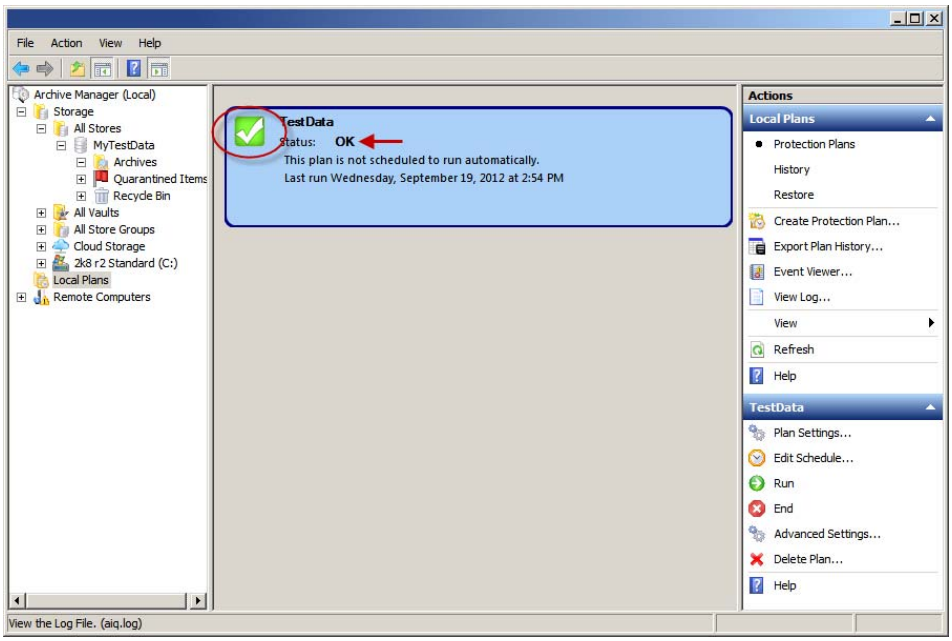
Step 6) Run the Protection Plan

Click the plan's Run action to run the plan.

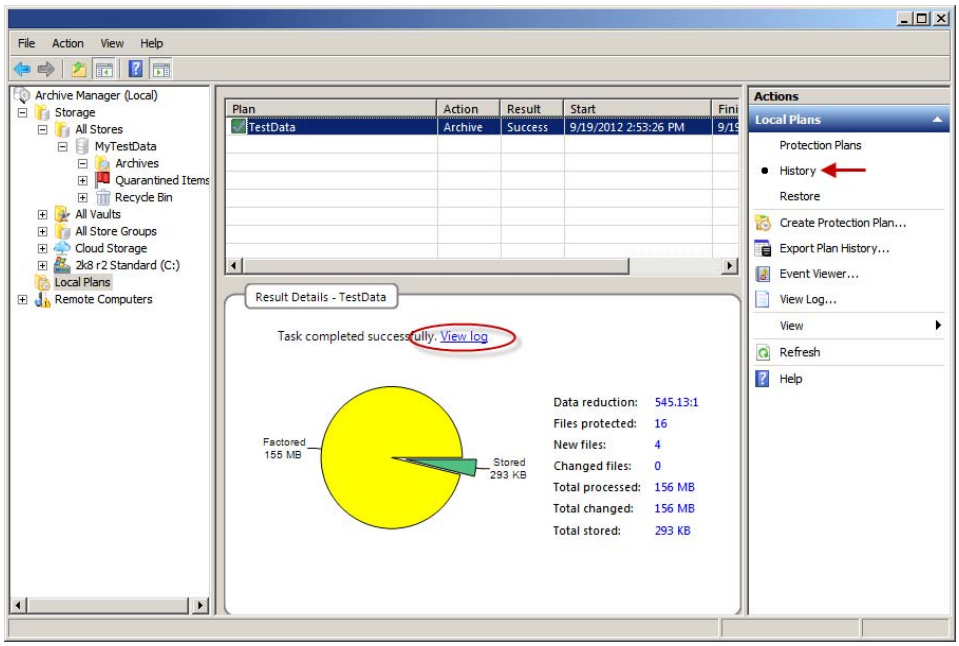




When the plan has finished running the completion status will be indicated by the icon and on the status line. In this case the plan ran successfully as indicated by the green icon with checkmark and Status: OK.

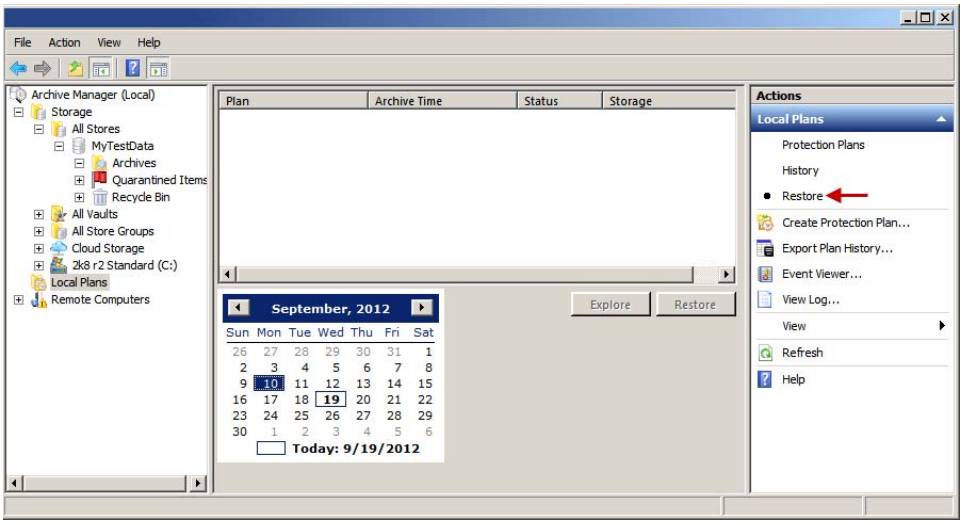


You can review the statistics for the plan run by choosing the Local Plans History action. Then, with the particular run highlighted, click on the View Log link to see the log file. The most recent logging information is at the end of the file.

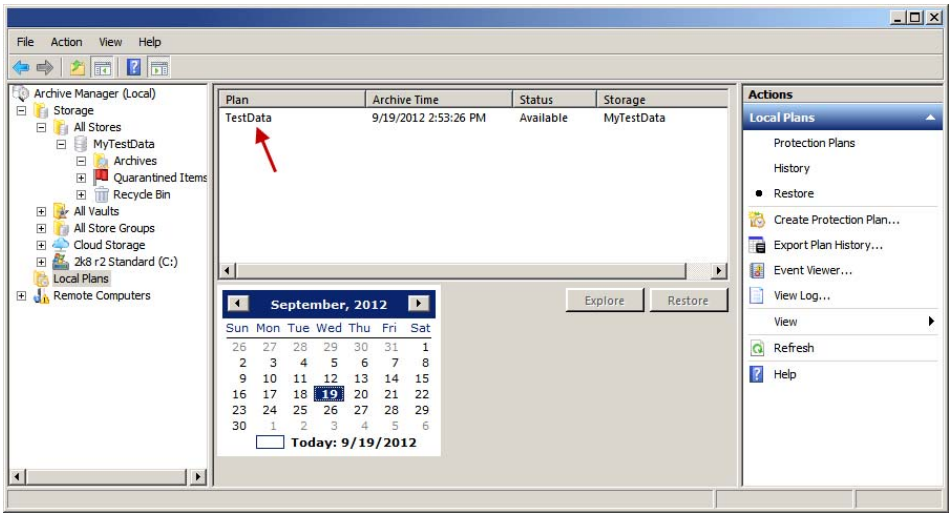


By default, protection plans run with multiple processes. The main (parent) process and the plan run's overall statistics are shown. The first time a plan is run it typically has to archive all data to set a 'baseline'. This run achieves reduction primarily through single-instance deduplication (i.e. if two files are the same only one is stored) and compression. A reduction of 2:1 is common. Subsequent runs are much quicker and only store changed unique data.

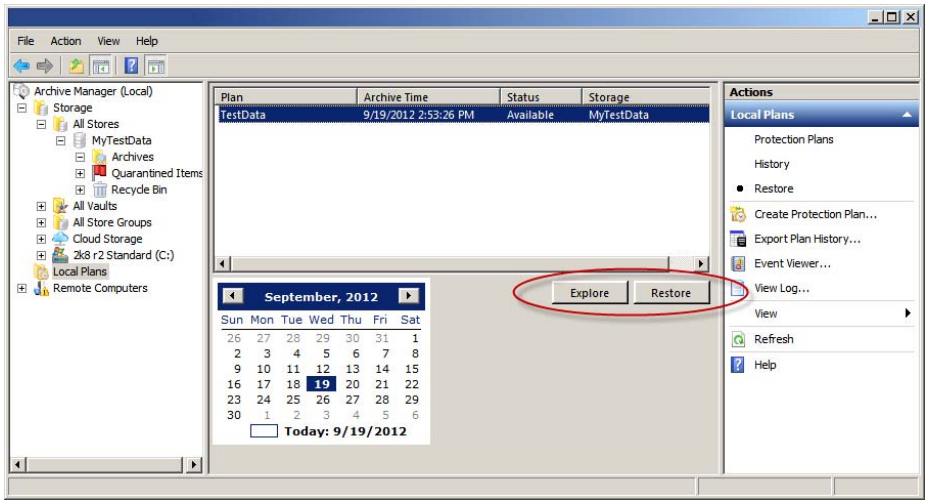
To restore data click on the Local Plans Restore action. Notice in the screenshot below that there is nothing shown to restore. That's because there were no protection plans run on September 10th, the date selected on the calendar.



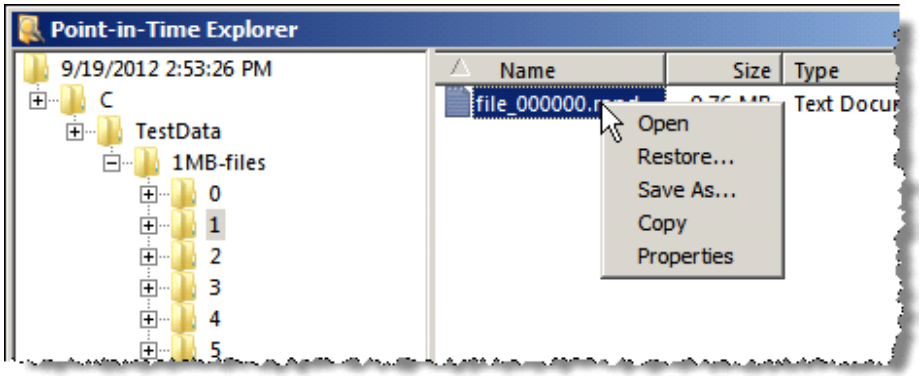
Dates that had protection plan runs are shown in bold print. September 10th (also the current date, as indicated by the box around it) is bold so let's select it.



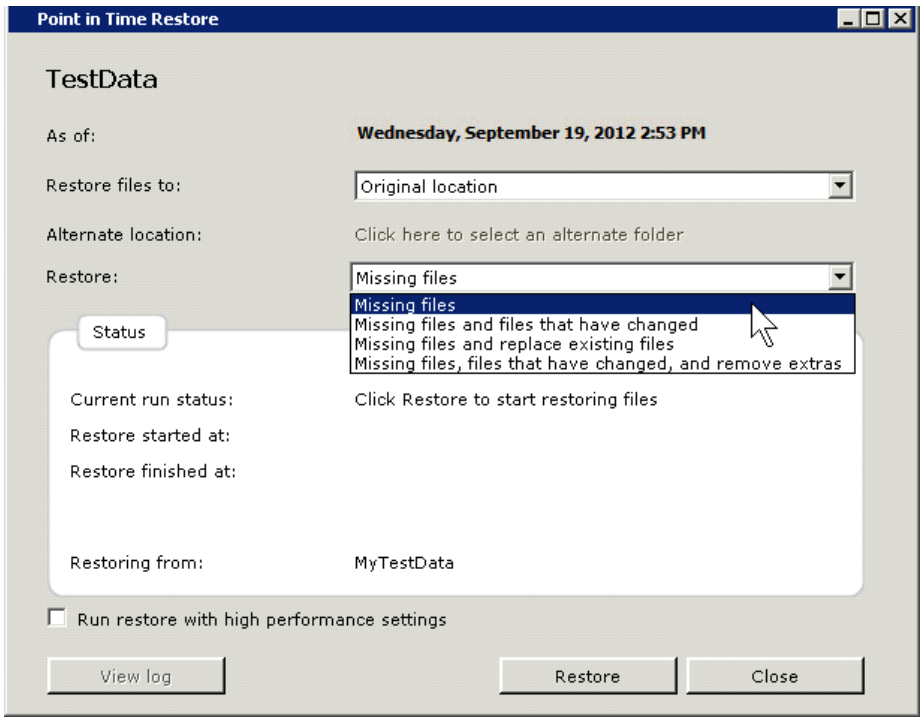
There's our plan run, or 'point-in-time' capture of the data. We need to highlight it before the Explore and Restore buttons are enabled.



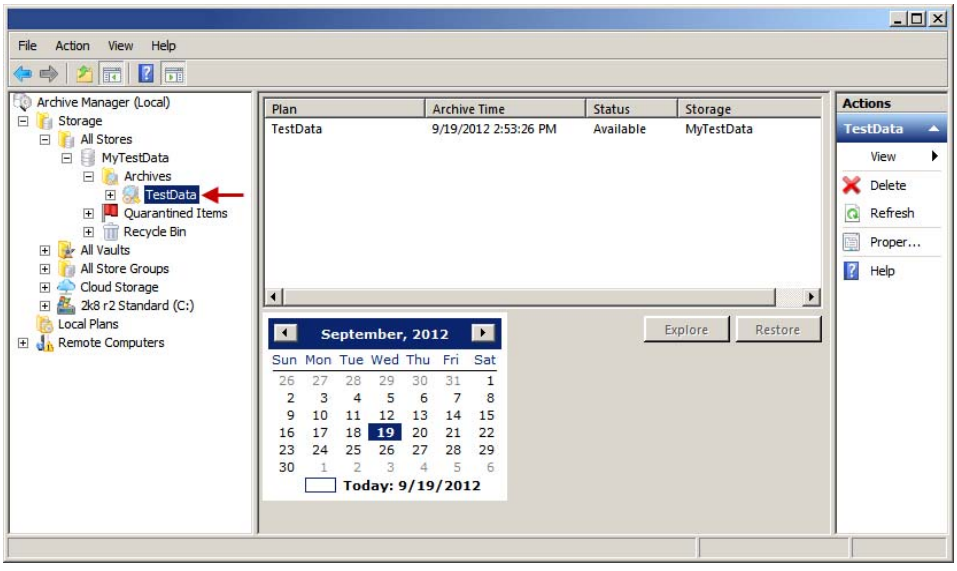
Choosing Explore lets you browse the point-in-time just like in Windows Explorer. By right-clicking an item in the Point-in-Time Explorer you can open it, drag-n-drop it from the archive to the desktop or Windows Explorer, Save As, and Copy/Paste.



Choosing Restore opens the Point-in-Time Restore screen. You can restore back to the original location or an alternate location. You can restore just files that are missing and files that have changed, files that are missing and replace all existing files, or files that are missing and files that have changed and remove any files or folders from the restore location that are not in the restore point-in-time.



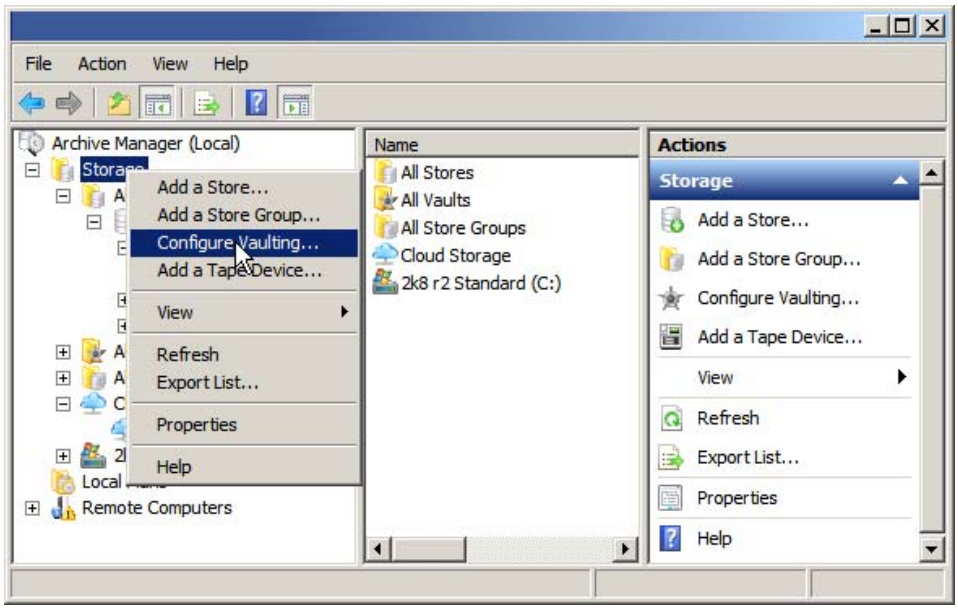
To run the restore job with multiple processes check the 'Run restore with high performance settings' option.



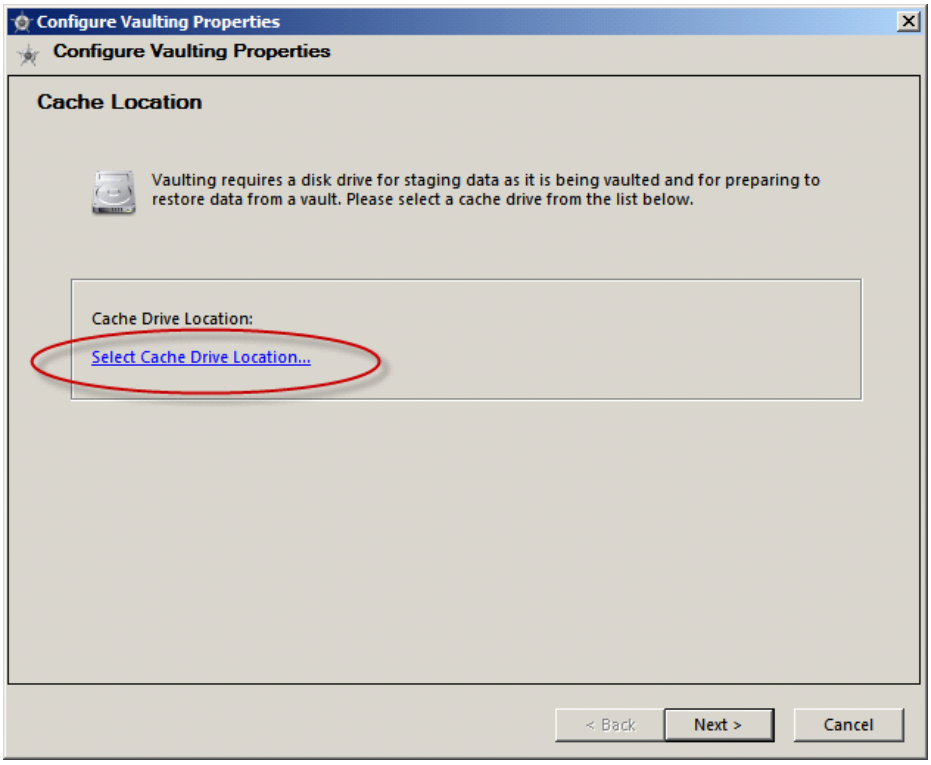
Notice also that after running the plan there is an Archive in the store called TestData (the protection plan's name). You can also Explore and Restore from here.

Step 7) Configure Vaulting

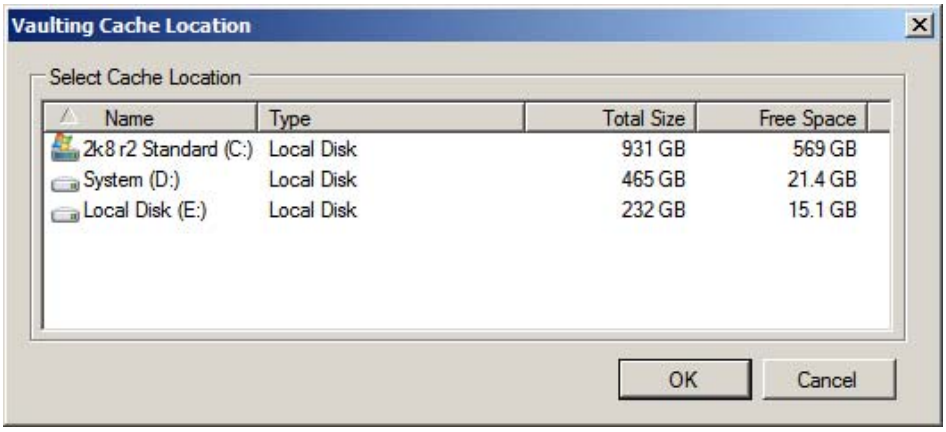
Before you can archive data to cloud or tape you must configure the system for vaulting. Note: You should only need to configure vaulting one time for the life of the system.



Click the Configure Vaulting action of the Storage node to begin the Configure Vaulting wizard.

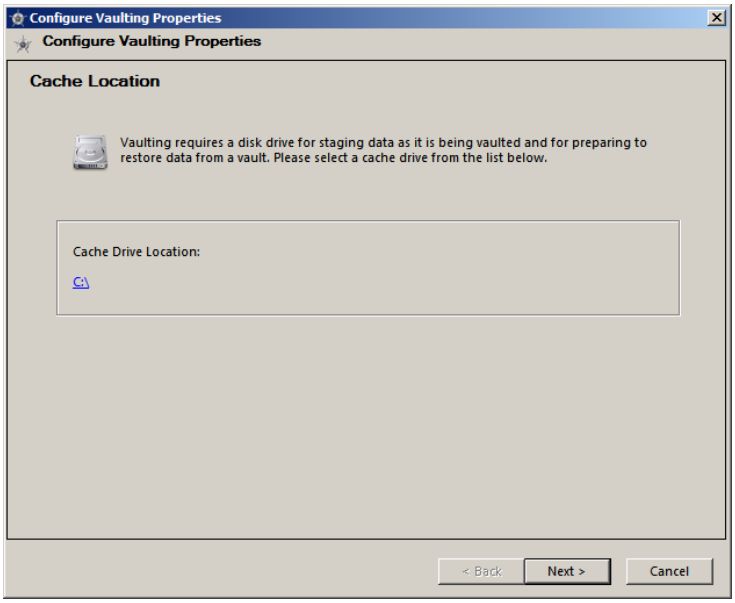


On the Cache Location screen click the 'Select Cache Drive Location' link to select a drive for staging data as it is being vaulted and for preparing to restore data from a vault.

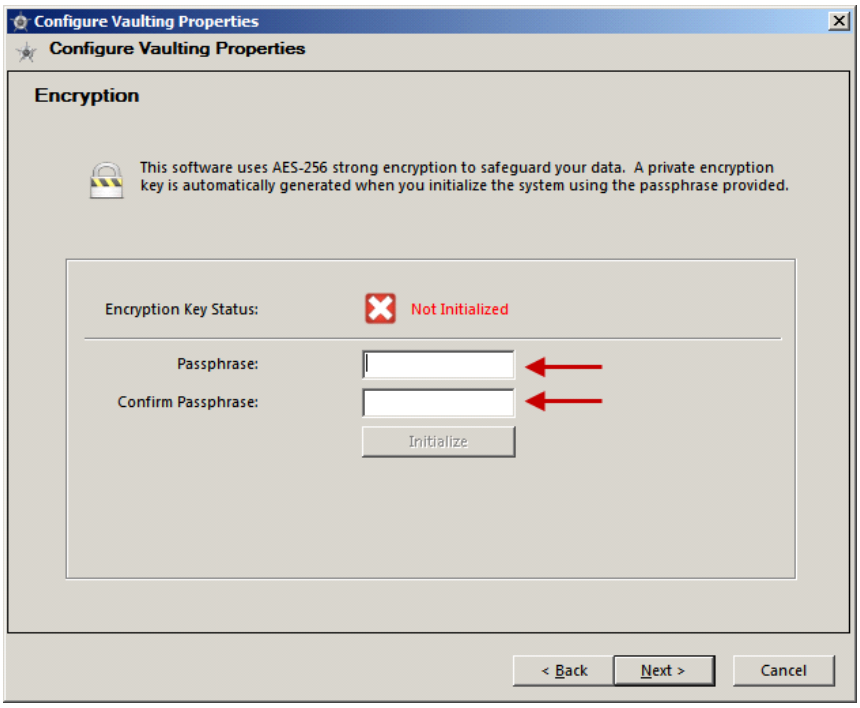


Select a drive and then click the OK button to close the Vaulting Cache Location screen and return to the Cache Location screen.

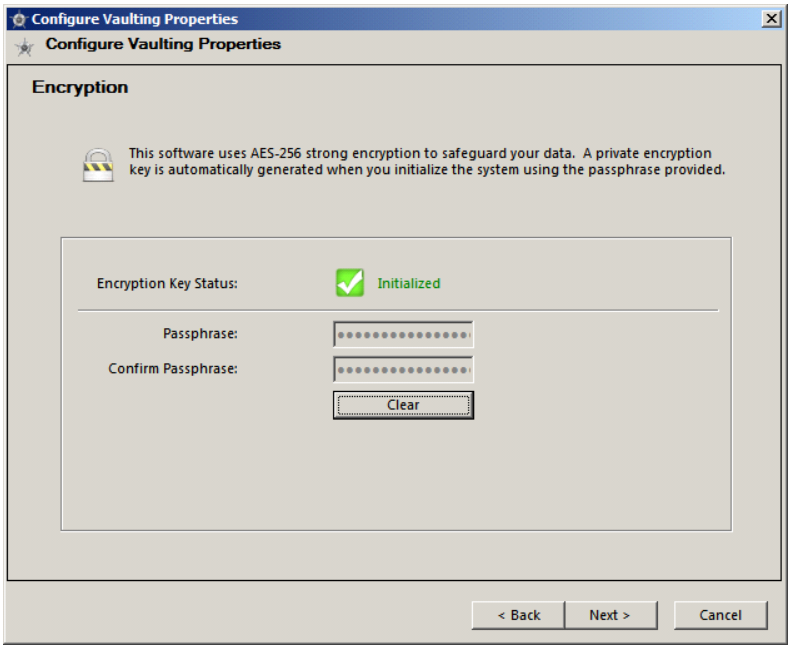
Note: Do not use the partition containing the OS for the cache location.



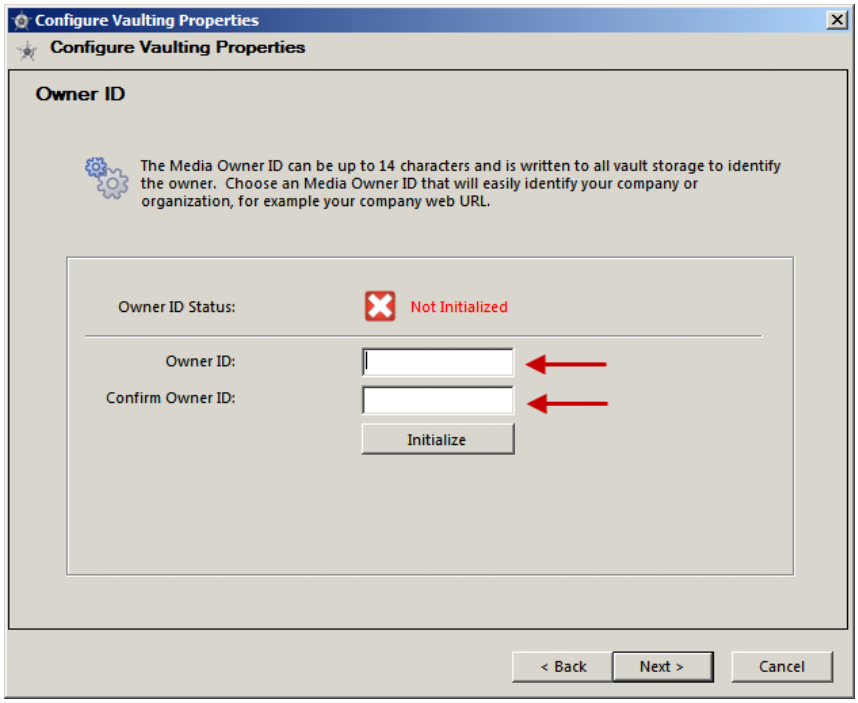
Click the Cache Drive Location link again if you want to change your selection or Click Next to continue to the Encryption screen.



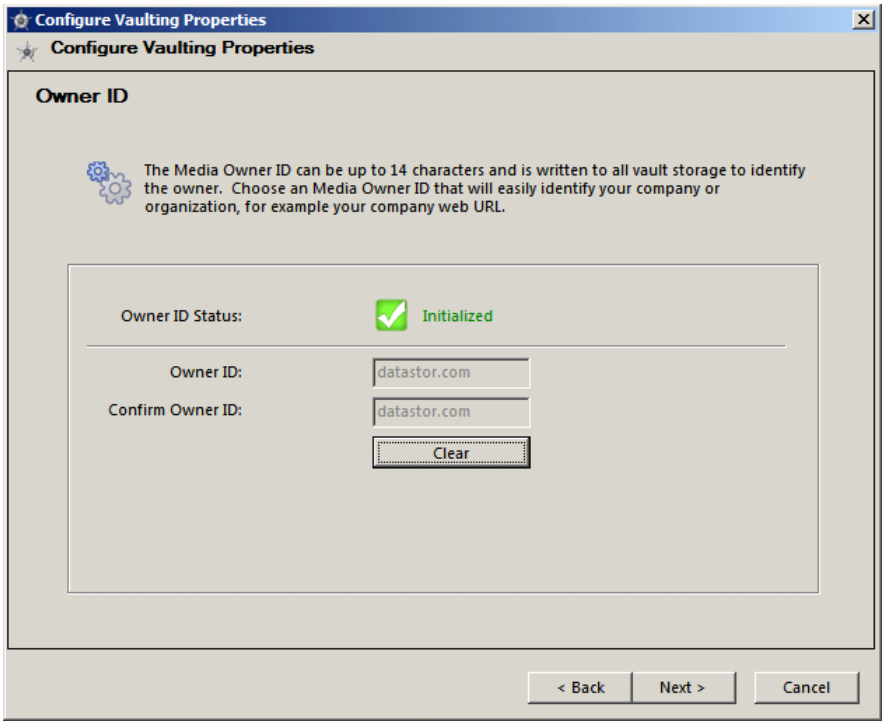
Your data is encrypted with AES 256 encryption prior to archiving to the cloud. Encryption is optional when archiving to tape. Enter an encryption passphrase to generate a private encryption key. You should record and safeguard this passphrase. Click the Initialize button to configure the product with this encryption passphrase.



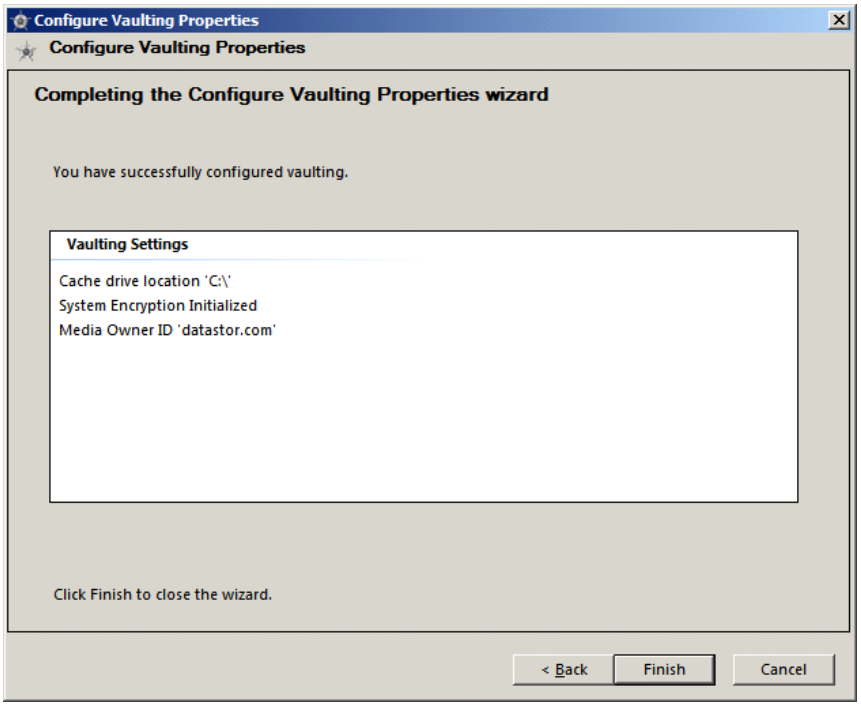
Click the Clear button if you want to change the passphrase, otherwise click Next to continue to the OwnerID page.



Enter an Owner ID that will identify the cloud and tape media as yours. For this example we'll enter datastor.com. Click the Initialize button to configure the product with this OwnerID.



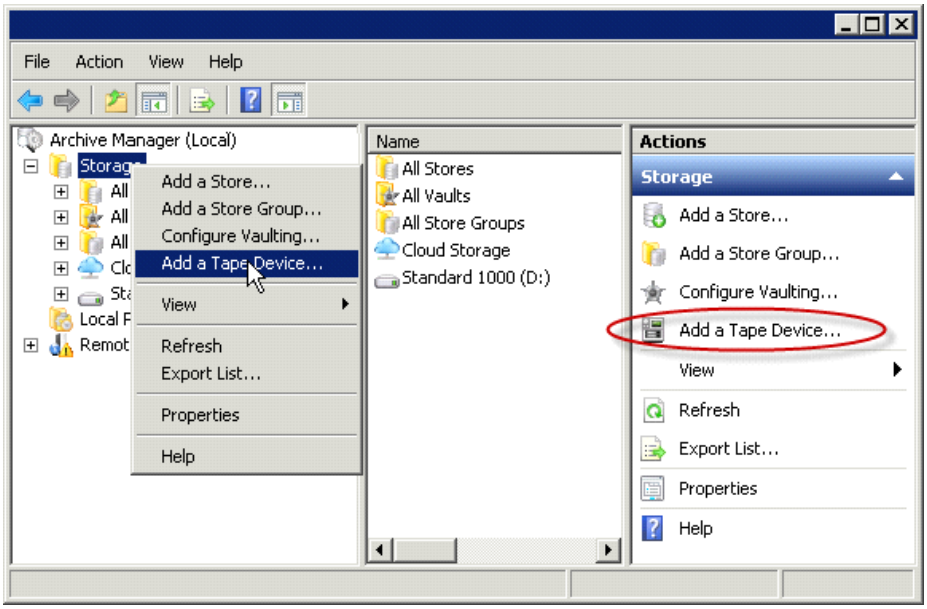
Click the Clear button if you want to change the Owner ID, otherwise click Next to continue to the summary page.

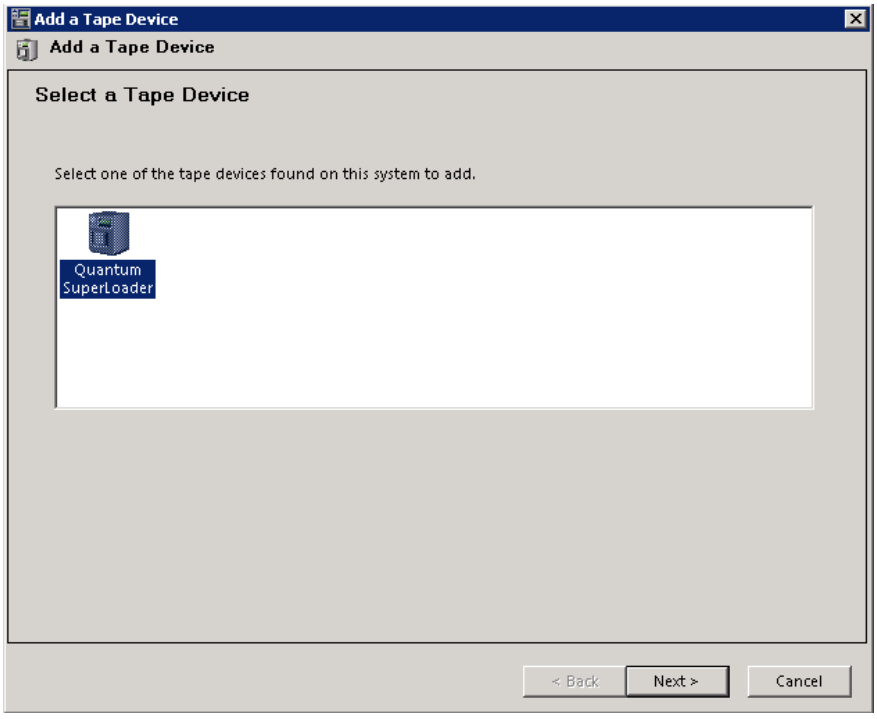


Review the vaulting settings and click Back if you want to change something, otherwise click Finish to close the wizard.

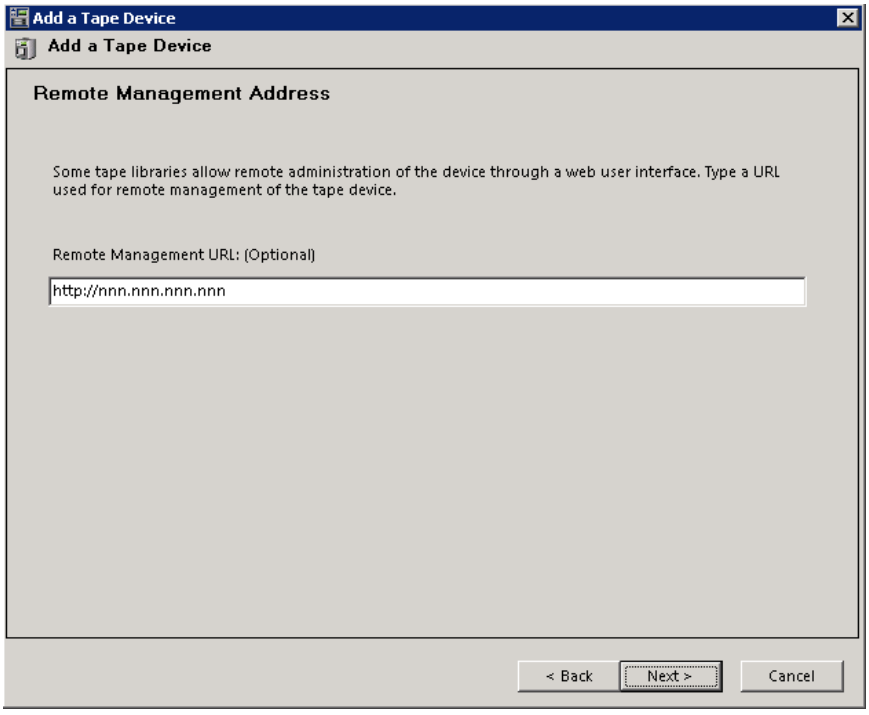
Step 8) Add a Tape Device to the product

To add a tape device to the system, select the Storage node and then choose its Add a Tape Device action.

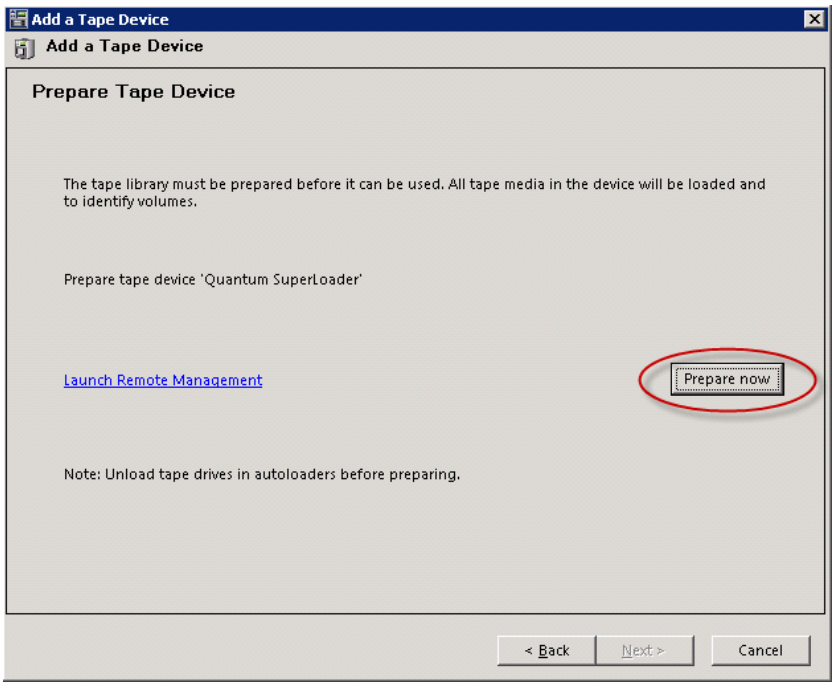




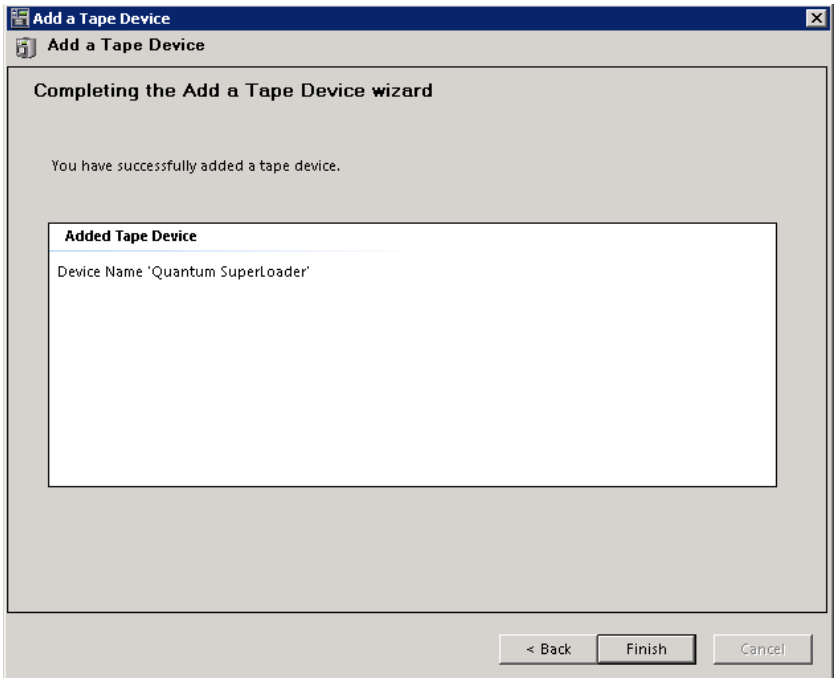
Select the device and then click Next to continue.



You can optionally add the address of the device's remote administration interface, if applicable. Click Next to continue.



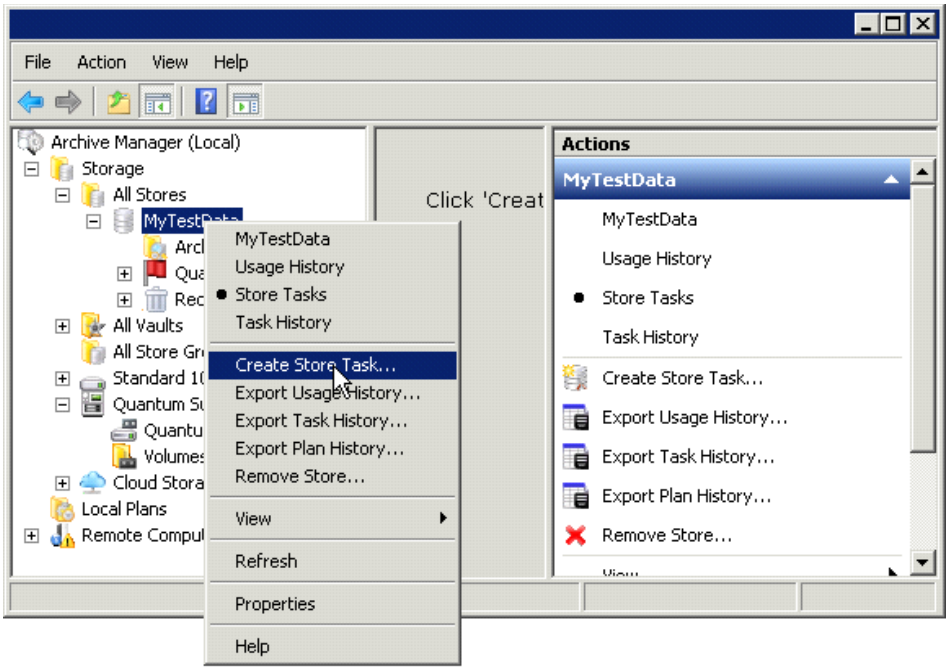
Before the device can be used by the software it must be inventoried. If there are tapes in any drives of the library, unload them before proceeding. Note: Inventorying the library may take a long time since each tape must be loaded and read by the software. Make sure no tapes are loaded in the drive(s) and then click Prepare now to begin the inventory. When complete, the Next button will be enabled. Click Next to continue to the summary screen.



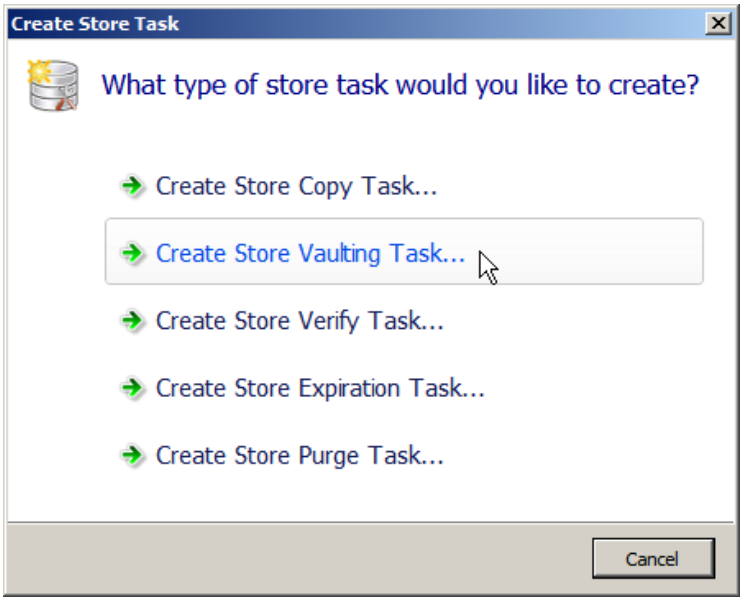
Click Finish to complete the Add a Tape Device wizard.

Step 9) Create a Store Vaulting Task

To archive data to the cloud or to tape you need to create a Store Vaulting Task. This task copies a whole 'Store' to a tape or cloud 'Vault'.



Create a Store Vaulting Task by highlighting the store and choosing its Create Store Task action.



While we're here, notice the other types of store tasks you can create. Store Copy Tasks can replicate stores within this Archive Manager system or even to another Archive Manager system across a network.

A Store Verify Task verifies the integrity of a store, including data and catalogs. Corrupt data will be moved to the store's Quarantined Items folder and flagged

'red'. Subsequent runs of a protection plan will attempt to repair (replace) the corrupt data. When successful, the quarantined item will get a 'green' flag. Green-flagged quarantined items may be safely deleted.

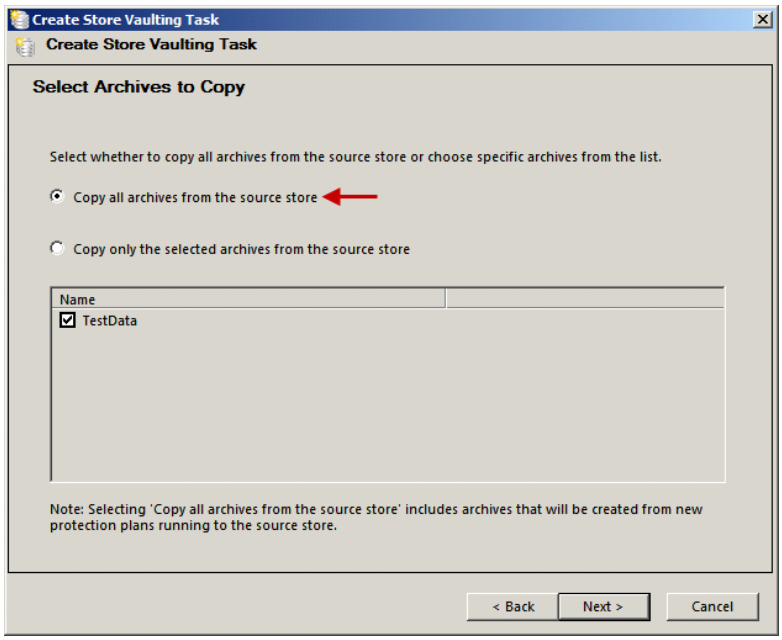
A Store Expiration Task will expire data from a store by moving it to the store's Recycle Bin. The expiration criteria can be set through the store's Property page. The default retention setting is 'indefinite'.

A Store Purge Task removes unreferenced and expired data from the Archive Manager system.

Click 'Create Store Vaulting Task' and then select Tape Device.

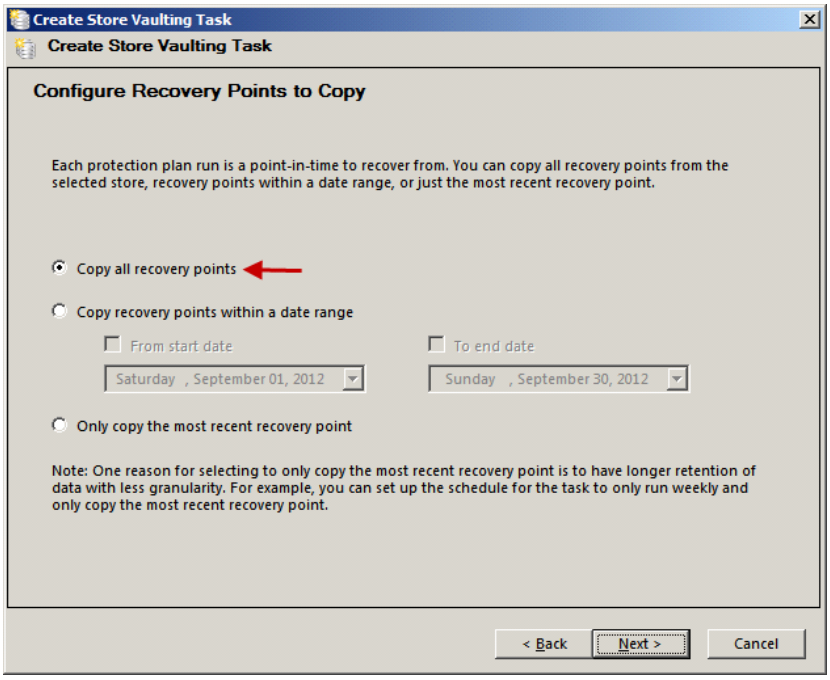
Select the device you wish to vault to and then click Next to continue.

WARNING: When attempting to perform the vaulting task ensure non-write protected media is selected.

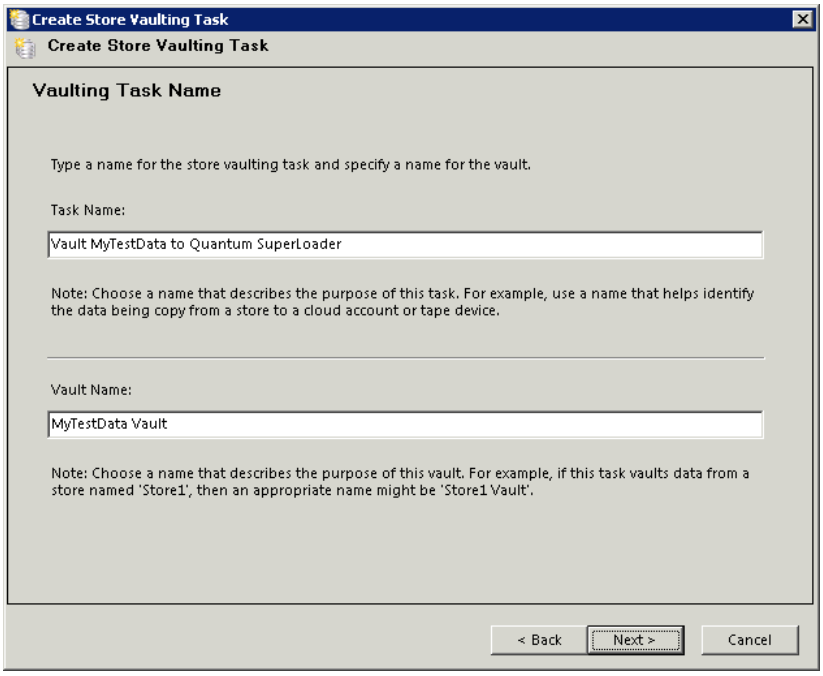


You can copy all archives (all data from all protection plans writing to this store) or you can select to copy only certain ones. We'll take the default of copying all archives. Click Next to continue.

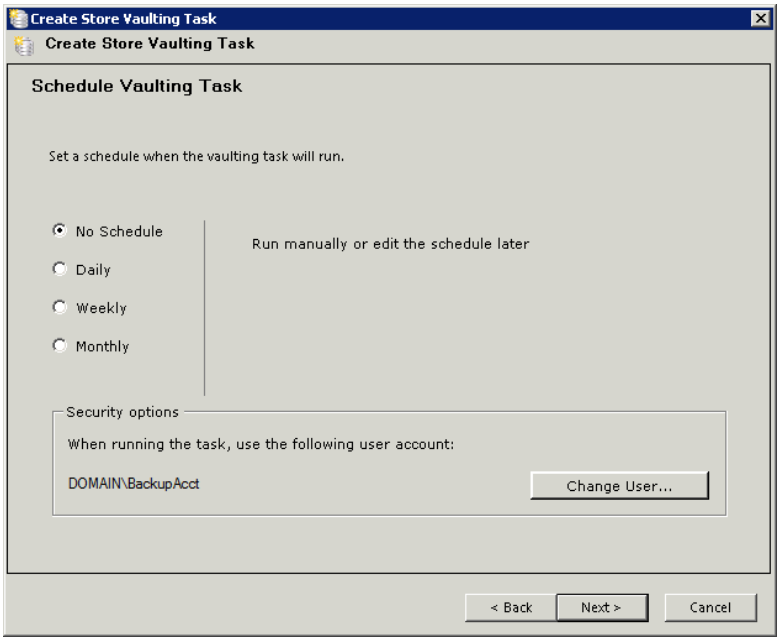
Each protection plan run is a point-in-time to recover from. You can copy all recovery points into the selected vault, copy a range of recovery points, or copy only the most recent recovery point. Again, we'll take the default of copying all recovery points.



When the Store Vaulting Task first runs it creates the Vault. On the Copy Task Name screen you can give the task a name and you can also give the vault a name. Again, we'll take the defaults. Click Next to continue.



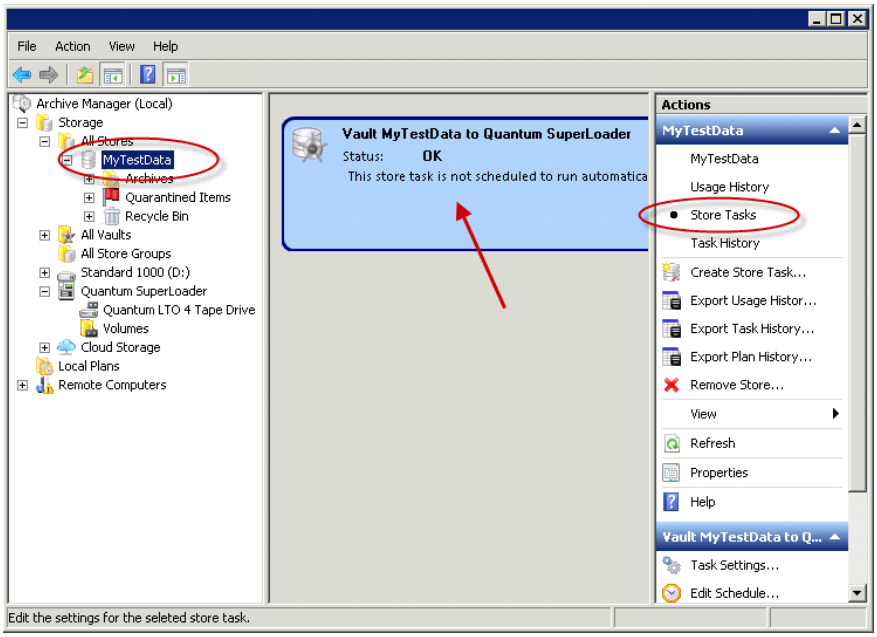
As with protection plans, Store Vaulting Tasks can be scheduled. In fact, all store tasks can be scheduled. For this example we won't schedule the task but instead just run it manually. Click Next on the Edit Schedule screen to continue.

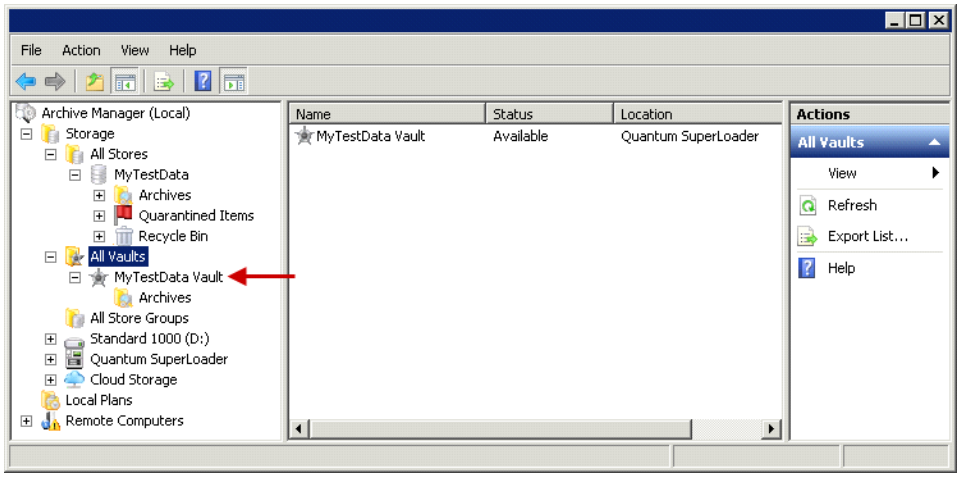


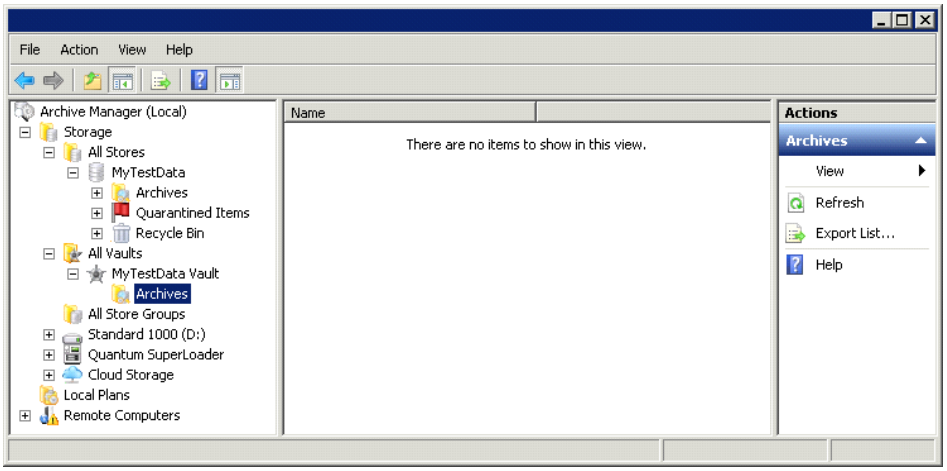
Review the summary on the Completing the Create Store Vaulting Task wizard and click the Back button to make any adjustments. Click Finish to accept the settings and exit the wizard. Enter the password for running the scheduled task when prompted. The new Vault will automatically be created and the new Store Vaulting Task will appear in the middle pane of the UI when the particular store node is highlighted and its Store Tasks action is selected. The Vault will appear

under the All Vaults node. The vault's Archives folder will be empty until the Store Vaulting Task has been run.

Note: This is the location where data will be cached before being written to tape.

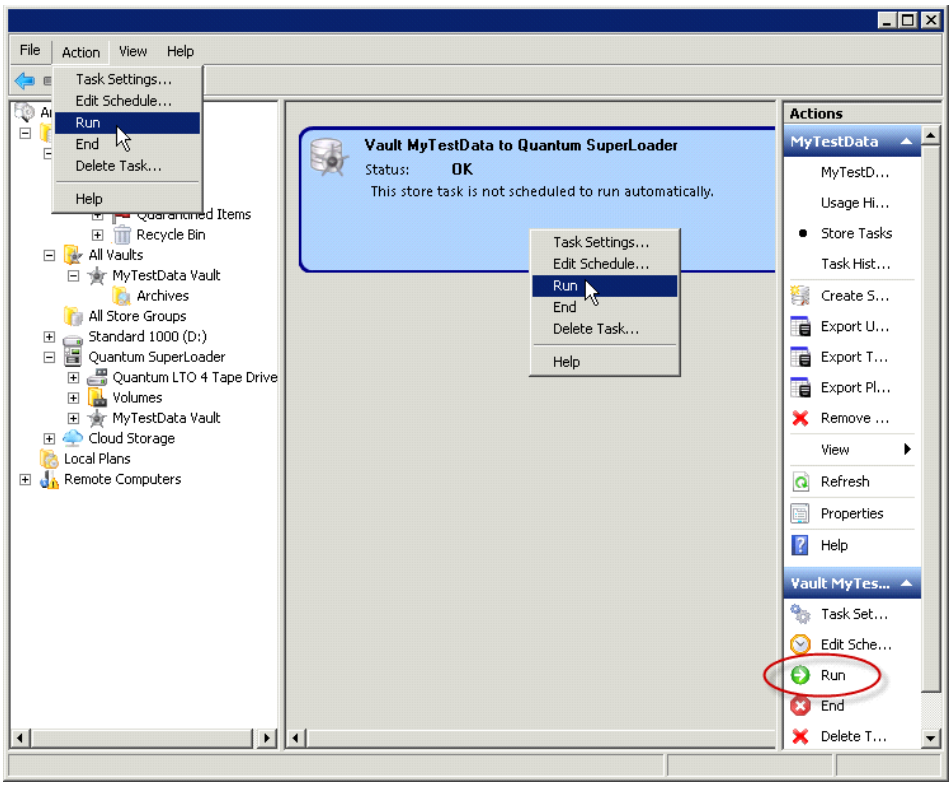


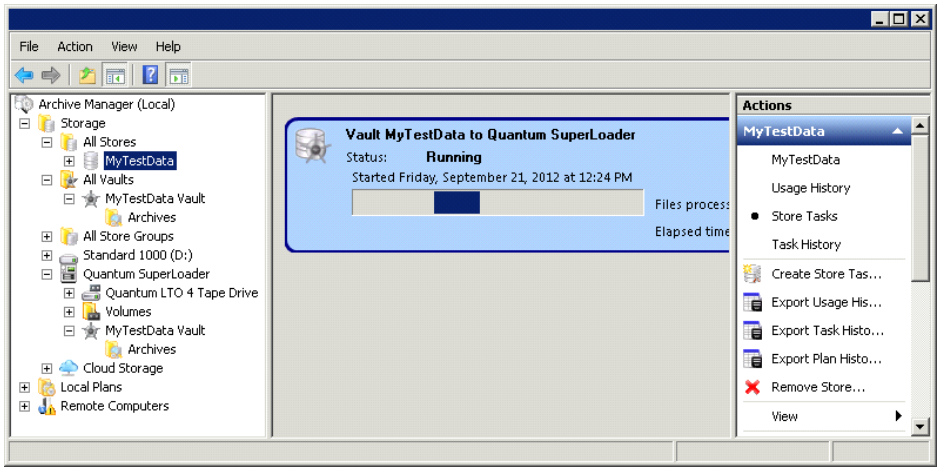


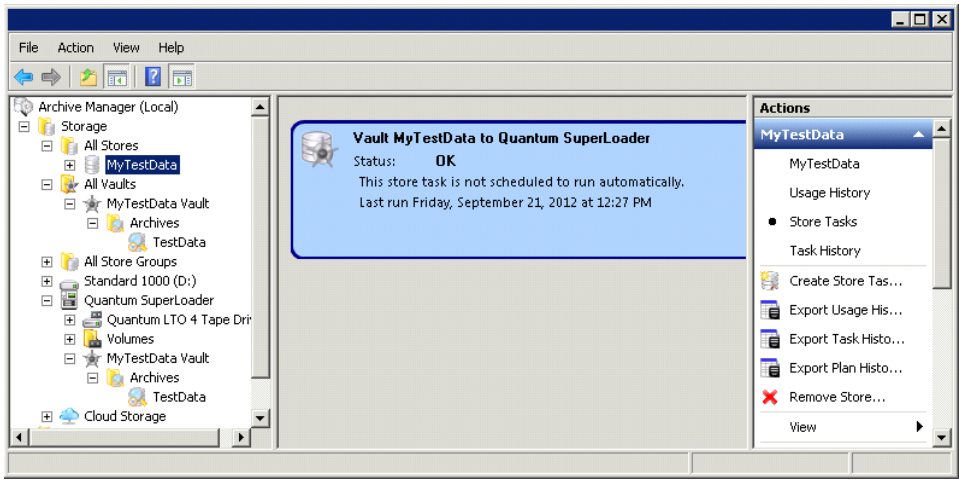


Step 10) Run the Store Vaulting Task

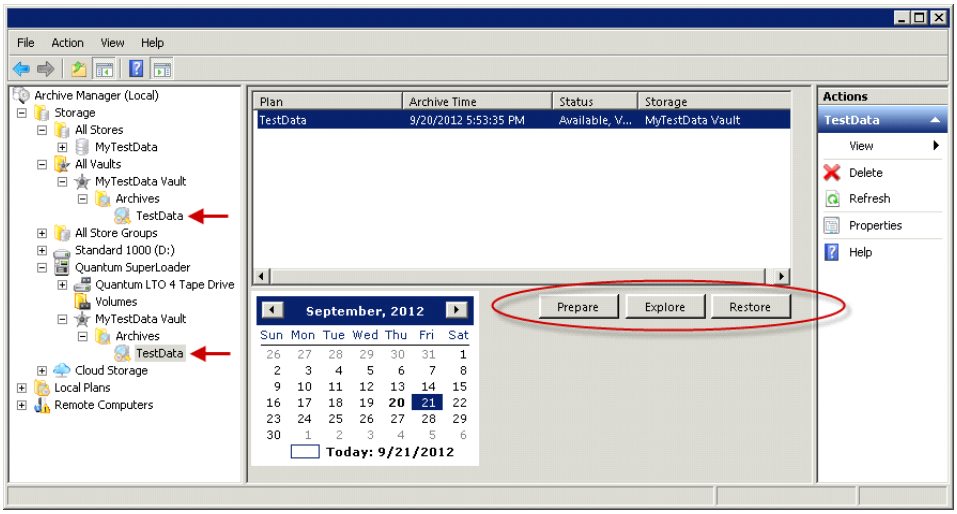
Run the Store Vaulting Task by clicking its Run action.







Running the store vaulting task for the first time automatically creates the archive in the vault defined by the vaulting task. You can explore and restore the data from the vault after running the 'Prepare' step (pressing the Prepare button).



Although you can explore the recovery point without running Prepare, the actual data is not reachable and you will see error messages like "The file cannot be accessed by the system" or "The system cannot find the file specified" if you try opening a file or restoring. The prepare step transfers the data from the tape into the recovery point-in-time on the local system. After preparing the recovery point you can explore and restore normally, either by exploring to a folder or file, right-clicking it and choosing an action or by clicking the Restore button to restore the whole point-in-time.

Summary

This completes the quick start exercise. We've gone from installing the product, to archiving data to tape, to restoring data from tape. To learn more about the product please refer to the online context-sensitive help and the User Guide.

Tape Statuses

This article explains the various tape statuses as reported by the DATASTOR Shield software. There are three sections:

- Statuses - A listing and description of each status
- Refreshing the Status - How you can update the status after a change
- Adding / Removing / Rotating Tapes - How to update the software after adding or removing tapes

Statuses

The possible statuses of a tape are listed below.

- Foreign

  The tape contains data, but the data is from another software application. The DATASTOR Shield software will not use this tape, but the tape can be erased through the Erase action.

- Unidentified

  The tape is either unknown to the software or could not be read. It will not be used by the software until it can be successfully identified. The tape may be erased through the Erase action or Identified through the Identify action.

- Blank

  The tape is available for use by any vaulting task that targets this library. The tape can be assigned to a specific vault by selecting it from the Volumes folder and selecting the Assign action.

- Full

  The tape is considered full when the free space is less than 7% of the reported capacity. It will not be written to, but might be needed for restores. A Full status can be reported, regardless of the application that has been using the tape.

  Note: DATASTOR Shield attempts to reserve up to 7% of a tape's free space for media error correction.

- Cleaning

  The tape is a cleaning tape. This tape will not be used by the software.

- Assigned

  The tape is assigned to a vault.

- Appendable

  The tape can be written to by a store vaulting task it has been assigned to.

- Read Only

  The tape will not be written to by the software, possibly because the tape's write-protect tab is on.

  Note: Media of type WORM will not have a Read Only status. Rather, it will show Appendable until it is full, taking into account that up to 7% free space is reserved for media correction by the software.

- Online

  The tape is physically present and its location will be shown in the Location column of the Volumes folder.

  Note: The software identifies a tape by its bar code label.

- Offline

  The tape is not physically present and its location will be shown as N/A in the Location column of the Volumes folder.

  Note: The software identifies a tape by its bar code label.

- Erase Pending

  The tape was assigned to a vault that has been removed.

Note: You can remove a vault with the tape media online or offline. The tapes must be erased and transitioned to Blank before they are used by the software again (see the "Refreshing the Status" section, below). A tape's Erase action is available for online tapes.

Refreshing the Status

Full Inventory

A full inventory mounts and attempts to read every tape in the library to identify it, so this process may take a long time. A full inventory is performed as part of adding a tape library with the Add Tape Device wizard when you click the Prepare button. A full inventory can also be performed later by using the library folder Synchronize Library Inventory action.

Possible statuses for tapes discovered during the inventory are:

- Blank
- Foreign
- Unidentified
- Full
- Assigned
- Appendable

Note: The Assigned and Appendable statuses may be from another installation of the software on another computer.

Lightweight Inventory

When you refresh the Volumes folder, selected volumes in the Volumes folder, or a tape drive folder, a "lightweight" inventory is performed. This inventory quickly scans the device to reconcile tape bar codes.

- Possible statuses for tapes discovered during the inventory are:
- Offline
- Online
- Unidentified

Identify

To identify a tape that has an Unidentified or Foreign status, you can select it from the Volumes folder and click the Identify action. This causes the tape to be mounted and read as in the Full Inventory. You can also multi-select tapes to identify.

Possible statuses after an Identify has been attempted are:

- Blank
- Foreign
- Unidentified

- Full
- Assigned
- Appendable

Note: The Assigned and Appendable statuses may be from another installation of the software on another computer.

Note: Incorrect Error Message: When performing a "quick inventory" media is listed as foreign. If the user right clicks on the media and selects "Identify", an error message will be generated "An error occurred. Review the Application log for more information". In the Application log the media is shown as "write protected", this error message is incorrect. The media is foreign and has been used by a different application. The user must decide if they want to erase the data and use the media with the DATASTOR SW or not. If the user does want to erase the media they should right click on the media and select "Erase". The media will then be blank.

Adding / Removing / Rotating Tapes

When tapes are removed from or added to a library, perhaps due to a tape rotation, the software needs to be made aware of the changes.

Perform one of the following actions:

- Full Inventory

Run the Synchronize Library Inventory action from the library folder to mount and read every tape.

- Lightweight Inventory
- Refresh the Volumes folder to update it. This action will scan the barcode database. Select a tape (or multi-select tapes) from the Volumes folder and then click the Identify action to mount and read the selected tape(s).