
# DATASTOR Shield™ Enterprise Protection Server

# Table of contents

# Archive Manager

## Welcome

Congratulations on your purchase of this software!

This backup and restore software is designed for use with hard disk storage. Built on innovative deduplication technology, it virtually eliminates redundant data because unique data is stored only once. The effective storage capacity of the disk is significantly increased, making backup to disk fast, easy and affordable. The software includes additional support for cloud and tape storage for backup redundancy.

Some key features of this software:

- Unique data stored only once (data deduplication)
- Archived data always available on disk
- Data recovery is easy and instantaneous
- Fast backups
- Easy to use interface

Using protection plans, you can easily select data to protect. Each backup contains all of the files in the selected data set as they exist at the time of the protection plan run. There are no cumbersome incremental or differential backups to deal with.

At any time you can see all of the files you have backed up, or archived, using the familiar Windows Explorer interface.

## Features

This software is fully-featured backup and recovery software. It is made up of an Archive Manager server component and optionally, clients, as determined by license keys.

The server component, once configured, is comprised of at least one store for storing archived data, and at least one protection plan. A protection plan defines which data is to be archived, which store to save it in, and when the plan should be run. Additional stores and plans can be added and modified as needed.

The client component allows data on remote computers to be deduplicated prior to being sent to the store. This configuration is ideal for limited-bandwidth situations since only unique data is transferred across the network.

During regular use, you will work with three main features:

- Protection Plans
- Archived Data Viewing
- Archived Data Restoring

### Protection Plans

This software backs up your important data by means of protection plans. A protection plan defines which data is to be archived, which store to save it in, and when the plan runs. Additional stores and plans can be added and modified as needed.

There are four types of protection plans:

- **Files and Folders**

The Files and Folders protection plan protects selected files and folders.

- **SQL Databases** (only available if Microsoft SQL Server is installed on the computer being protected. Proper licensing is required.)

  The SQL Server protection plan lets you protect Microsoft SQL Server databases.

- **Exchange Data** (only available if Microsoft Exchange is installed on the computer being protected. Proper licensing is required.)

  The Exchange Data protection plan lets you protect Microsoft Exchange Storage Groups (for Exchange Server 2003 or Exchange Server 2007) or databases (for all newer versions of Exchange).

- **Computer System** (Proper licensing is required.)

  The Computer System protection plan lets you back up a computer system to enable system and application recovery.

Clicking on a plan type starts the protection plan wizard to guide you through the simple process of creating your plan.

A protection plan keeps track of all the selected items and, after its initial run, will store only new and changed information. At the same time, each plan run creates a *full* restore point.

### Open File Support

Windows Volume Shadow Copy Service (VSS) is used to ensure that open files are properly backed up.

### Items that this software will not archive

This software will not archive these Windows file types:

- Temporary Internet files
- Temp folder
- Digital Rights Management folder
- Recycle Bin
- Power Management files such as the file(s) governing Hibernation
- Memory Page file
- System Volume Information files, System Restore files, Automated System Restore (ASR) files

You can also create your own per-plan exclusion rules. See Excluding File Types for more information.

## Viewing Archived Data

With the exception of purged data, your backup storage contains all versions of your stored files. Every protection plan execution generates a restore point in its archive in the store. The restore point includes every file selected for protection. During plan runtime, the software detects, at a sub-file level, data that has changed between backups and stores only the unique data necessary to protect the versions of the files it encounters. It can reconstruct and restore all versions of files that have been protected.

The **Archive Manager** user interface makes it easy to find each version of a file so you can quickly restore the latest version of the file or a previous version of the file. See Exploring and Restoring Folders and Files for more information.

### Restoring Data

Restoring your data is quick and easy.

To find and restore your data, use one of the following methods:

- Explore a plan's archive restore point to view and restore folders and files as they existed at a specific point in time.
- Restore the entire contents of a plan's archive restore point.

See Exploring and Restoring Folders and Files for more information.

## Overview of User Interface

This section provides a general overview of the **Archive Manager**.

Implemented as a standard Microsoft Management Console (MMC) 3.0 snap-in, the **Archive Manager** is the *control center* for the software. It resides on the **Archive Manager** server, the computer where the software is installed, and defaults to the standard MMC 3-pane view.

The left pane, the *console tree*, provides a hierarchical view of the whole system. By selecting the **Archive Manager** folder at the top of the console tree, you can manage areas that affect the overall system, such as managing license keys and entering user account information used by all plans and store tasks.

Each folder type in the console tree has specific actions defined. Actions can be initiated from the **Actions** (right-hand) console pane, the **Action** drop-down menu on the top menu bar, or by right-clicking the folder and selecting an action from the pop up menu.

The center console pane is the *status* or *results* pane. This is where you see information related to the currently selected folder in the console tree. When actions are available for items in the center pane, they will be available in the actions pane as a sub-group of actions.

When the **Archive Manager** is initially started, **Archive Manager** will be the only folder shown in the console tree, and you will be prompted to activate your software. After activation the console tree can be expanded to show **Archive Manager** (top level), with **Storage**, **Local Plans**, and **Remote Computers** underneath. Click the links below for a brief discussion of each console tree folder.

- Archive Manager
- Storage
- Local Plans
- Remote Computers

### Archive Manager

The top-level category in the console tree is called **Archive Manager**. Actions defined for **Archive Manager** affect the overall system.

Select the **About** action to view product version information. From here you can also gather product logs and history information, useful when working with product support personnel.

Select the **Edit License Keys** action to Add or Remove product license keys.

Select the **Purchase Software Licenses** action to purchase license keys for Archive Managers, Remote Computers and other optional functionality.

Select the **Purchase Support Subscription** action to renew software maintenance for your purchased licenses.

Select the Import Settings action to import saved (exported) Archive Manager configuration files.

Select the **Save System Recovery Environment** action to save a bootable system recovery environment image to USB, CD/DVD or .iso to use as part of a system recovery for systems protected by Computer System protection plans.

The **User Preferences** action lets you set some system-wide preferences. For instance, the **Show Storage** setting, when *false*, hides the store groups and vaulting folders. If your software supports these features but does not use them they can be hidden, thus simplifying the user interface.

Select the **Properties** action to manage export settings for saving Archive Manager configuration files, checkup reporting, ViewStor settings, and User Account information.

### License Keys

The **License Keys** dialog allows you to view, add, remove, and activate your software license keys.

#### Installing License Keys

To add a license key, click the **Edit License Keys** action of the **Archive Manager** folder.

After entering your license key in the edit box and clicking **OK**, you will be prompted for confirmation.

If the license key you entered is a replacement for an existing key (automatically determined by the software), click **Yes** to replace the key, or click **No** or **Cancel** to return to the **License Keys** dialog without replacing the key. After clicking **Yes**, you will be prompted to activate the new key.

### User Account

By specifying backup user account credentials on the **User Account** tab of the **Archive Manager** properties page you avoid being prompted for credentials each time you create or make a change to a protection plan or store task.

### Checkup Report

The software provides a convenient way to monitor the status of your system by generating a report of the store and protection plan status for the past 24 hours. Errors are highlighted in red, and warnings are highlighted in yellow for quick identification of problems.

You can schedule the frequency of reporting and specify email addresses for sending the report. There is a **Send Test Message** button that allows you to quickly test your email settings by sending a short test message.

Configure checkup reporting from the **Checkup Report** tab of the **Archive Manager** properties page.

To configure checkup reporting to save a local copy of the report and display it in the Checkup Report tab in the center pane of Archive Manager, check the box next to **Create an HTML report file**.

To configure email notification, check the box next to **Send the report as an Email**, then fill in the required fields. Below are some common scenarios for configuring the email settings.

- sender is a Microsoft Office 365 account
    - **To:** <*recipient@example.com*>
    - **Sender:** <*sender_name@mycompany.com*>

  - **Host:** <*smtp.office365.com*>
  - **Port:** 587
  - **Use Secure Sockets Layer (SSL)** Check this box.
  - **Sender password:** <*password for sender_name@mycompany.com*>

- sender is a Microsoft Exchange account

  - **To:** <*recipient@example.com*>
  - **Sender:** <*sender_name@mycompany.com*>
  - **Host:** <*exchange.mycompany.com*>
  - **Port:** 25
  - **Use Secure Sockets Layer (SSL)** Leave unchecked.
  - **Sender password:** <*password for sender_name@mycompany.com*>

- sender is a Gmail account

  - **To:** <*recipient@example.com*>
  - **Sender:** <*sender_name@gmail.com*>
  - **Host:** smtp.gmail.com
  - **Port:** 587
  - **Use Secure Sockets Layer (SSL)** Check this box.
  - **Sender password:** <*password for sender_name@gmail.com*>

- sender is a standard SMTP account

  - **To:** <*recipient@example.com*>
  - **Sender:** <*sender_name@domain.com*>
  - **Host:** <*smtp.domain.com*>
  - **Port:** 25
  - **Use Secure Sockets Layer (SSL)** Leave unchecked.
  - **Sender password:** <*password for sender_name@domain.com*>

See KB article How to send the checkup report through your Yahoo! or Google account for information on configuring application specific passwords.

### ViewStor Settings

**ViewStor** is a built-in software service that provides the Point-in-Time Explorer feature of this software. It uses the Microsoft WebClient service to access archives. If the WebClient service is not running, you will not be able to use **Point-in-Time Explorer** to explore for files. In this case, you must restore all files from a restore point by clicking the **Restore** button.

On Windows Vista, Windows 7, and Windows Server 2008 and newer platforms, **ViewStor** is configured to listen on port 8500. On these platforms, you can change the **ViewStor** listening port by checking the box to override the default listening port, then selecting a new port number. You will be prompted to restart the **ViewStor** service for the new setting to take effect.

Note: On Windows Server 2003, the ViewStor service requires port 80 to explore restore points. Only restore functions are available if the **ViewStor** listening port is not port 80.

To change the **ViewStor** settings, open the **ViewStor** tab of the **Archive Manager** properties page.

## Storage

The **Storage** folder shows the storage configured for the software. Folders immediately below the Storage folder include:

- All Stores - This folder shows all of the stores configured for use by the software.

- All Store Groups - All store groups that have been configured are shown here.
- Disk Storage - This is simply another view of the same stores shown in the **All Stores** folder, available to perform recoveries grouped by the disk they are physically located on.
- Cloud Storage* - This folder shows the cloud accounts configured for use by the software and the storage associated with cloud vaulting.
- Tape Storage* - This folder shows the LTO tape devices that have been configured for use by the software and storage associated with tape vaulting.

Actions for **Storage** include:

- **Add a Store**
  The **Add a Store** action launches the **Add Store** wizard for creating a new store or reconnecting to an existing store. After the wizard has completed the store is added to the **All Stores** folder. For more information on adding stores see the Adding Stores topic.
- **Add a Store Group**
  The **Add a Store Group** action launches the **Add Store Group** wizard for creating a store group and assigning stores to the group. For more information on adding store groups see the Adding Store Groups topic.
- **Configure Vaulting***
  The Configure Vaulting action launches the **Configure Vaulting** wizard for configuration of system-wide vaulting settings. See the Store Vaulting topic for more information.

* Vaulting (both cloud and tape vaulting) is not available if this software is installed on a Windows Server 2003 operating system.

### All Stores

A store is a disk storage location targeted by local and remote protection plans for keeping archived data (common content) and associated cataloging information. After a store is created, it will appear in the **All Stores** folder.

From the **All Stores** folder, you can see and manage storage that has been prepared for the software. Information such as the store name, status (**Available** or **Offline**), and the drive designation of the disk are displayed in the status (center) pane.

Part of creating a store is preparing the storage. As part of the store preparation process, the software automatically creates the following folders:

- **Archives** - Archives contain time-stamped catalog entries (restore points) grouped by plan name.
- **Quarantined Items** - Stores can be verified for referential and data integrity. Any data found to be corrupt is moved to this folder. The store will attempt to self-heal on a subsequent plan run by putting a good version of the quarantined item into the store.
- **Recycle Bin** - When an item is expired, its catalog entry is kept in this folder until the item is purged from the system.

See Stores for more information.

### All Store Groups

A store group is a logical collection of **Stores** that allows for creating multiple copies of protected data on different storage devices. Store groups enable automatic fail-over between online media, dynamic rotation of removable media, and round-robin selection of fixed drive media. After a store

group is created, it appears in the **All Store Groups** folder.

Part of creating and maintaining the settings for a store group includes specifying which stores are members of the group and how the software will select available stores when the group is used by Protection Plans and Store Copy Tasks.

From the **All Store Groups** folder, you can see any added group and the stores that are members of the group. Information such as the store name, size of the storage, status (Available or Offline), and the device location are displayed in the status (center) pane.

See Store Groups for more information.

### Disk Storage

The **Disk Storage** folder simply presents another view of the same stores shown in the **All Stores** folder. In this view they are displayed under the disk they are physically located on. The properties of each physical disk can be viewed by choosing its **Properties** action. Shown within each physical disk folder are the stores that reside on that disk. As with the **All Stores** view, each store is shown with its **Archives**, **Quarantined Items** and **Recycle Bin** folders. Actions for these folders are the same as when viewed from the **All Stores** folder.

Archived data can be restored from the **Disk Storage** folder, **All Stores** folder or from the local or remote computer protection plan that archived the data.

### Cloud Storage

From the **Cloud Storage** folder you can view cloud accounts, monitor upload/download activity, create and add a cloud account, and configure cloud upload and download bandwidth throttling.

The **Cloud Storage** folder lists all cloud accounts that have been added to the software and contains an **All Cloud Vaults** folder containing all cloud vaults that currently exist in the software. See Vaulting for more information.

By selecting the **Cloud Storage Upload/Download Status** action you can monitor real-time upload/download activity.

By selecting the **Cloud StorageProperties** action you can configure cloud upload and download bandwidth throttling.

### Tape Storage

Tape devices configured for the software are shown in the **Tape Storage** folder.

If your product is licensed for tape devices and there is at least one LTO-3 or greater tape device (library or standalone drive) attached to the system, the software can be configured to write archived data to tape using a disk-to-disk-to-tape scenario. First the data is deduplicated and written to a Store using a Protection Plan. Then a tape vaulting task reformats the deduplicated data and streams it to tape in the form of a Vault. Because the data remains in its deduplicated state, tape usage is just a fraction of what it would be otherwise.

After adding and activating a tape device license key two new folders will appear under the Tape Storage folder: All Volume Sets and All Tape Vaults.

See Tape Device for more information.

## Local Plans

The **Local Plans** folder contains protection plans configured for protecting local data (versus data on remote computers). From here you can create and manage plans to protect local data.

Actions available for **Local Plans** include:

- **Protection Plans**

  Select the **Protection Plans** action to show all local protection plans for the **Archive Manager** server. From this view, each local plan can be manually run, reconfigured, scheduled, and deleted.

- **History**

  You can see the history for all local plans by selecting the **History** action. Each time a plan runs or is restored, an entry is added to the history list. By selecting an entry from the list, you can click the **View Log** link in the **Result Details** area to view the run log. See also, Protection Plan Results and Log Files.

- **Restore**

  To view local plan restore points, select the **Local Plans** folder, and click the **Restore** action. Days containing restore points are highlighted in bold font in the calendar. Select the restore point you want to restore, and the **Restore** button at the bottom right of the screen becomes active. Click **Restore** and a restore dialog box appears. Refer to Restoring Your Data for more information. If the restore point was from a **Files and Folders or Computer System** type protection plan, the **Explore** button will also become active, and you can explore and restore files as described in Explore a Plan's Archive.

- **Export Plan History**

  See Exporting History to learn about exporting local plan histories.

- **Event Viewer** / **View Log**

  To aid in troubleshooting, this software records its activity in log files and writes significant events to the Windows Application Event Log. See the Log Files topic for more information. Clicking the **Event Viewer** action for local plans opens the Windows Event Viewer for the **Archive Manager** server. Click the **View Log** action for local plans to see the commands that have run for local plans and store tasks.

See the following topics for more information:

- Creating Protection Plans
- Run, Edit, Remove a Plan

## Remote Computers

The **Remote Computers** folder contains the remote computers (clients) section of the console tree. This folder has an All Computers group underneath for adding your remote computers to the software.

Actions for **Remote Computers** include:

- **Add Group**

  For organizational purposes, you can group your remote computers together under a meaningful heading, or group name. For instance, any remote computers you add to the **All Computers** folder are listed in the **All Computers** group. To streamline organization, you could create a specific group for all computers in the sales department. To create a new group, click **Add Group** and enter a name. Any computer you add to your custom group is automatically added to the **All Computers** group. Conversely, any computer you remove from your custom group is *not* automatically removed from the **All Computers** group. The computer is not completely removed until you remove it from the **All Computers** group.

- **Add VMware Group**

  This action starts the **Add VMware Computer Group Wizard** for protecting VMware virtual machines. Click the wizard's **Browse** button to select a vCenter server or VMware host to find virtual machines to include in the group. After virtual machines have been added to the group they can be protected like any other computer in the Remote Computers section. All virtual machines included in the group are protected with a default policy.

- **View Log**

  Click the **View Log** action for remote computers to see the commands that have run for remote computer plans. See the Log Files topic for more information.

Actions available for remote computers in the **Remote Computers** section include:

- **Protection Plans**

  Select the **Protection Plans** action to show all protection plans for the selected remote computer. From this view, each plan can be manually run, reconfigured, scheduled, and deleted.

- **History**

  You can see the history for all plans for a remote computer by selecting the **History** action. Each time a plan runs or is restored, an entry is added to the history list. To view the run log for a given plan, select an entry from the history list. Next, click the **View Log** link located in the **Result Details** area. The run log for the selected entry appears. See also, Protection Plan Results and Log Files.

- **Restore**

  All restore points for a remote computer can be seen by selecting the remote computer, and then clicking the **Restore** action. If the desired protection plan has been deleted from the computer, you may still be able to access restore points from the Archives folder in the store. Days that contain restore points are highlighted in bold font in the calendar. To restore a restore point, select it from the list. Click the **Restore** button in the lower-right area of the screen. A restore dialog box appears. Refer to Restoring Your Data for more information. If the restore point was from a **Files and Folders or Computer System** type protection plan, you can also click the **Explore** button to restore files. See Explore a Plan's Archive for more information.

- **Export Plan History**

  See Exporting History to learn about exporting remote plan histories.

- **Event Viewer**

  To aid in troubleshooting, this software records its activity in log files and writes significant events to the Windows Application Event Log. Clicking the **Event Viewer** action for a remote computer opens the Windows Event Viewer for the remote computer.

See Adding Remote Computers for additional information.

## Adding Remote Computers

A remote computer refers to a computer protected by this software that is not the **Archive Manager** server.

Note: For best results, you should use the same domain administrator account to schedule plans for

your remote computers as for administering your **Archive Manager** server.

To add a remote computer, select the desired computer group under the Remote Computers folder (or just select the All Computers group if you haven't added additional groups) and then select its **Add Computer** action. This will open a screen where you can specify the computer by either browsing the network (not supported on Windows Server 2003), searching the Active Directory if applicable, or typing in the computer name.

After adding a remote computer and selecting it, you can choose its **Create Protection Plan** action to begin the protection plan wizard. See Creating Protection Plans for more information.

## Protection Plans

Protection plans specify which data to protect and where to keep the protected data (which store to use). You can optionally set up a schedule to automatically run the plan. See the following topics for more information:

- Creating Protection Plans
- Scheduling Protection Plans
- Run, Edit, Remove a Plan
- Protection Plan Results

### Creating Protection Plans

This software allows you to create and save protection plans to store your data on storage prepared for use by the software. A protection plan is made up of a plan type, selections relevant to the type, the store or store group to use, and a schedule specifying when the plan runs. Local plans are protection plans that run on the local server and protect local data. Remote protection plans are plans that run on, and protect data on, remote computers (clients), where the protected data is deduplicated prior to being sent to a store for archiving.

If Microsoft SQL Server and proper licensing are installed on the computer you are protecting, a protection plan type for protecting SQL Server databases will be enabled.

If Microsoft Exchange and proper licensing are installed on the computer you are protecting, a protection plan type for protecting Microsoft Exchange Storage Groups (for Exchange Server 2003 or Exchange Server 2007) or databases (for all newer versions of Exchange) will be enabled.

If your product is licensed for system recovery and the operating system is supported on the computer you are protecting, a protection plan type called **Computer System** will be enabled.

Note: Prior to creating a protection plan, you will need to create a store or store group for storing your archived data. See Stores and Store Groups for more information.

To create a protection plan, open **Archive Manager**. In the console tree, select either the **Local Plans** folder or a remote computer, depending on where the data resides that you want to protect. Click the **Create Protection Plan** action and choose a plan type (**Files and Folders**, **Exchange Data**, **SQL Databases**, or **Computer System**) to start the protection plan wizard.

Provide the following information to complete the protection plan wizard:

- folders, Exchange Storage Groups or databases, SQL Server databases, or Computer System drives to protect
- store to use
- a name for the plan
- a scheduling option and the administrator account credentials needed to run the plan

When a protection plan is highlighted in the results (center) pane of the **Archive Manager**, the

**Actions** pane will contain actions applicable to that plan. From the **Actions** pane, you can run a plan, view its results, view the history of a plan, and modify a plan.

See Run, Edit, Remove a Plan for information about using protection plans.

See the following topics for more information about creating protection plans:

- Add Files and Folders Protection Plan
- Add Exchange Protection Plan
- Add SQL Server Protection Plan
- Add Computer System Protection Plan

### Add Files and Folders Protection Plan

Note: Prior to creating a protection plan, you will need to create a store for keeping your archived data. See Stores and Store Groups for more information.

To create a protection plan for files and folders, select **Create Protection Plan** from either the **Local Plans** folder or from a remote computer located within the **Remote Computers** folder. Next, choose **Files and Folders** to begin the protection plan wizard for protecting files and folders.

Note: The **Files and Folders** plan type is not recommended for protecting Exchange and SQL. Instead, choose the **Exchange Storage Groups** or **SQL Databases** plan types.

The first step in creating a **Files and Folders** protection plan is to specify the folders to protect. Click the **Add** button on the **Enter Folders to Protect** screen and then use the Windows Explorer-like controls to expand the disks and folders that you want to protect. Click **OK** to protect the selected disk/folder and sub-folders. Click **Add** again to add another path to be protected by this plan. Repeat as needed.

Note: Once you've created a plan, you can refine your selection down to the file level via the **Plan Settings** action. You can also specify exclusions within the selected data. For instance, you could exclude all files with the .exe file extension. Excluding certain file types, such as images, audio, and video files, can significantly reduce the amount of data that is stored on your target storage device, and speed up execution of your protection plan. See Editing a Plan for more information.

Click **Next** on the **Enter Folders to Protect** screen to continue with the **Add Files and Folders Protection Plan** wizard. This step takes you to the **Select a Destination** screen to select a store or store group; the target location for your archived data. Highlight a store, then click **Next** to continue to the **Enter Plan Name** screen.

Give the plan a descriptive name, then click **Next** to continue to the **Scheduled Task** screen to set up a schedule for automatically running the plan. You can also specify a different user account for running the plan. See Scheduling Protection Plans for more information. Click **Next** to go to the final screen where you can review the settings. Click the **Back** button to change settings, or click **Finish** to close the protection plan wizard and create the plan. You will be prompted for the password of the account specified for running the plan.

See Run, Edit, Remove a Plan for information about using protection plans.

### Add Exchange Data Protection Plan

The software detects Microsoft Exchange 2003 or newer versions on the computer you are protecting. With proper licensing, if Exchange is installed the protection plan type **Exchange Data** is enabled.

An **Exchange Data** protection plan protects all of the required Exchange files for each storage group selected (for Exchange Server 2003 or Exchange Server 2007) or Exchange database

selected (for all newer versions of Exchange). The software queries Exchange for their location; there is no need to specify folders for protection. Each plan run truncates all eligible log files.

To create a protection plan for Exchange, select **Create Protection Plan** from either the **Local Plans** folder or from a remote computer located within the **Remote Computers** folder. Next, choose **Exchange Data** to begin the **Add Exchange Protection Plan** wizard.

The first screen, **Select Exchange Data** lists the available Exchange Storage Groups or databases. Check the box for each storage group or database to protect, then click **Next** to continue to the **Select a Destination** screen.

Highlight the store or store group where you want the protected data to reside. A store in this context refers to the storage within the **Archive Manager** server, and not Exchange. Click **Next** to continue to the **Enter Plan Name** screen.

Give your plan a descriptive name, then click **Next** to continue to the **Scheduled Task** screen where you can set up a schedule to automatically run the plan. You can also specify a different user account to run the plan. See Scheduling Protection Plans for more information. Click **Next** to go to the final screen where you can review the settings. Click the **Back** button to change settings, or click **Finish** to close the **Add Exchange Protection Plan** wizard and create the plan. If you have not entered account information on the User Account tab of Archive Manager Properties, you will be prompted for the password of the account specified to run the plan.

See Run, Edit, Remove a Plan for information about using protection plans.

Note: This software uses Microsoft Exchange VSS Writer to create a snapshot of Microsoft Exchange Storage Groups or databases. Verify Microsoft Exchange VSS Writer is present on the Microsoft Exchange Server by running `VSSADMIN LIST WRITERS` at a command prompt on the server being protected.

### Add SQL Server Protection Plan

The software detects if Microsoft SQL Server 2005 or newer is installed on the computer you are protecting. If so, the protection plan type **SQL Databases** is enabled if proper licensing is installed.

A **SQL Databases** protection plan specifies which SQL Server databases to protect and where to keep the protected data. At the launch of the protection plan, the software queries SQL for the required database and log file locations; there is no need to set up specific folders for protection. During the **Add SQL Server Protection Plan** wizard, you can specify whether the transaction logs on databases configured in the **Full** recovery model will be truncated at the end of a protection plan run. The truncation of logs will not shrink the size of a transaction log file, but instead clear space within the transaction log file for the creation of new log records.

To create a protection plan for SQL, select **Create Protection Plan** from either the **Local Plans** folder or from a remote computer located within the Remote Computers folder, then choose **SQL Databases** to begin the **Add SQL Server Protection Plan** wizard.

The wizard will display a list of all databases grouped by their instance names, as well as each database operational state and recovery model. Place a checkmark next to each database to protect. To have the software truncate the database transaction logs, thereby allowing SQL to continue logging without growing the transaction log file size, place a checkmark in the checkbox **Truncate logs of Full Recovery Model databases**. Note: The **Truncate logs of Full Recovery Model databases** switch is ignored on protected databases configured for the **Simple** recovery model. Click **Next** to continue to the **Select a Destination** screen.

Highlight the store where you want the protected data to reside, then click **Next** to continue to the **Enter Plan Name** screen.

Give your plan a descriptive name, then click **Next** to continue to the **Scheduled Task** screen where you can set up a schedule to automatically run the plan. You can also specify a different user account to run the plan. See Scheduling Protection Plans for more information. Click **Next** to go to

the final screen where you can review the settings. Click the **Back** button to change settings, or click **Finish** to close the **Add SQL Server Protection Plan** wizard and create the plan. You will be prompted for the password of the account specified to run the plan.

See Run, Edit, Remove a Plan for information about using protection plans.

Note: This software uses Microsoft SQL VSS Writer to create a snapshot of SQL. Verify **Microsoft SQL VSS Writer** is present on the SQL server by running `VSSADMIN LIST WRITERS` at a command prompt on the server being protected. In addition, the SQL server you are protecting requires Microsoft CLR Types and Microsoft SQL Management Objects for SQL 2012. If not present, these components are installed automatically the first time a SQL protection plan runs.

### Add Computer System Protection Plan

A Computer System protection plan will create a complete backup of your system, suitable for recovering complete computer systems (also known as "bare metal" restore). With proper licensing, this plan type is available for local and remote computers.

There are two basic elements for protecting and recovering complete computer systems using this product. The first element is creating and running a Computer System Protection plan. The second element is the System Recovery Environment (SRE). When recovering a complete system, the computer needs to use a bootable device to bootstrap the recovery process. The System Recovery Environment is a custom Microsoft Windows 7 Pre-installation Environment image that can run from a CD/DVD drive, bootable USB drive and, in the case of a virtual machine recovery, mounted as an ISO formatted bootable CD/DVD. Once the computer has been booted with the SRE, the process of recovering the system is only a few steps away.

To start the Add a System Protection Plan wizard click **Create Protection Plan** from the actions for a Local Plan or a Remote Computer you have added to the system. Then, choose **Computer System** from the enabled plan types. First, the **Add a System Protection Plan** wizard displays the disk drives to select for protection by the plan. There are three elements to choose in this view: System Recovery Information, system drives and data drives. When the System Recovery Information is checked all system drives must be checked as well. A system drive will be indicated with an icon of a disk with a Windows Logo overlaid in the upper left of the icon. The data drives are not required to be selected as part of the plan, where it may be preferable to protect data on those drives with a different plan type. For example the data on a data drive might contain database and/or log files for Microsoft Exchange, and in this case an Exchange Data Protection Plan would be a better candidate for protection of the data on this data drive, since only an Exchange Data plan-type truncates Exchange logs.

Next, select a store for the system plan to use for storing the backup data and catalogs. A good practice would be to use a store created specifically for Computer System-type protection plans, as deduplication of data across servers is a big benefit when backing up several Windows computers.

Next, provide a name for the protection plan. Protection plan names must be unique throughout the Archive Manager system. A good practice for a Computer System Protection Plan is to use the computer name as part of the plan name, for example "Denver1 System Plan", where Denver1 is the computer being protected.

Next, select a schedule for running the protection plan. A typical schedule for a system protection plan is to run daily or weekly after business hours. The security options section specifies a user account to use to run the plan. A good practice is to create a single domain administrator account to run all of the protection plans in the environment. See Scheduling Protection Plans for more information.

Finally, click **Finish** to complete the wizard or **Back** to review or change any of the plan settings before saving the plan. Note: You will be prompted for a password for the plan "run as" user before the plan is saved to the system. Enter the password and click **OK** to save the plan.

After the plan is saved a dialog box appears asking if you would like to save the System Recovery Environment to media. This dialog serves as a reminder to save the SRE before it is needed; it is

not necessary to save the SRE each time you create a Computer System protection plan. Two separate recovery environments are downloadable from within the product. Some versions of the product also have the SRE environments bundled into the installation program. One System Recover Environment is for BIOS-bootable systems. Most computers today are of this type. The other is for newer UEFI-bootable systems. If you click **Yes** to save the SRE and the SRE is not already on your system it will be downloaded from the Internet. In addition to saving the SRE to the location you specify, it will be saved in <installation directory>\SRE if not already there. Note: You can download/save the SRE(s) at any time by selecting the **Save System Recovery Environment** action of the **Archive Manager** folder in the console tree of the Archive Manager user interface. See Saving the System Recovery Environment to Media for more information.

After the plan is created you can choose one of the following actions to review or modify how and when the plan runs: **Plan Settings**, **Edit Schedule**, **Run**, **End**, **Advanced Settings** or **Delete Plan**. See Run, Edit, Remove a Plan for more information.

To restore a computer system protected by a Computer System protection plan please refer to Saving the System Recovery Environment to Media and Restoring a Computer System.

### Saving the System Recovery Environment to Media

Recovering a computer system starts by booting into the System Recovery Environment (SRE). The SRE must be saved to bootable media prior to a system recovery. Save the SRE using the **Save System Recovery Environment** dialog launched either at the end of creating a Computer System protection plan or from the **Save System Recovery Environment** action on the **Archive Manager** folder of the console.

Note: It is not necessary to save the SRE each time you create a Computer System protection plan.

You can save the SRE to different types of media: USB, ISO formatted file, or CD/DVD.

Two separate recovery environments are provided by the software. One is for BIOS boot systems and uses a 32-bit Windows 7 Pre-installation Environment (Windows PE). The other is for newer UEFI boot systems and uses a 64-bit version of Windows PE. **The Save System Recovery Environment** dialog has a checkbox in the lower left corner to save the SRE for systems that boot using UEFI.

You should verify that you can boot the recovery environment by booting a system with the saved SRE media attached.

#### Copy to USB

Selecting **Copy to a USB** drive allows you to copy the image file to one of the USB drives connected to the system. Only the first partition on a USB drive can be used. IMPORTANT: The partition should be set to active using Windows Disk Management or the DISKPART utility. This enables the USB drive to boot the SRE.

Note: When copying to a USB drive, existing data is preserved - the drive is not formatted.

Click **Copy** when you are ready to copy the information to the target drive. When the copy completes click **Cancel** to close the dialog.

#### Copy SRE .iso file

Selecting **Copy SRE .iso file** presents a **Browse For Folder** chooser dialog allowing you to specify a location to save the SRE .iso file. You can choose a folder on a local or mapped drive. Once you choose a folder and click **OK** the copy starts with a progress bar.

The SRE .iso file is an ISO formatted file that can be used for booting virtual machines. Most virtual machine hypervisors allow a user to configure a virtual machine to boot from CD/DVD devices or ISO formatted files.

### Burn to CD or DVD

Selecting **Burn to CD or DVD** presents the Windows Disc Image Burner dialog box allowing you to burn a bootable CD or DVD using one of the installed CD or DVD burners on your computer. This option is only available if the program Windows Disc Image Burner (isoburn.exe) is installed on your computer. Isoburn.exe is installed by default on Windows 7 and newer desktop systems and on Windows Server 2008 R2 and newer server systems that have the Desktop Experience feature installed.

See Restoring a Computer System to learn about restoring from a Computer System protection plan.

## Scheduling Protection Plans

Protection plans run on the computer as Windows Scheduled Tasks. When the **Edit Schedule** action for a plan is clicked, the standard Windows Task Scheduler is opened with some pre-filled settings for the plan.

The **Edit Schedule** action allows you to run a protection plan as an alternate user. That is, a user account that is different from the user which is currently logged in to the computer where the software is installed.

The **Edit Schedule** action also allows you to create a schedule to automatically run your protection plan.

A protection plan's Windows Scheduled Task will be configured to match that computer's Windows operating system. The task properties tabs below reference Windows Server 2003 tasks; for Windows Server 2008 and newer operating systems the tasks will instead use the General tab (for account information) and Triggers tab (for scheduling) to achieve the same settings.

### Run as

From the **Task** tab of the Windows Task Scheduler, you can change the account information required for running the plan. By default, the **Run as** account is the user account of the currently logged in user.

Enter the user account you want to be effective when the plan runs and enter the password for that user account. When using this option, the **Run only if logged on** scheduling option is normally left unchecked.

You might change **Run as** account information for a task if it needs access to network mapped drives that are available under a different user account than the one currently logged on. In a Windows domain, use an account with Domain Admins and Backup Operators Group membership.

See User Account for more information.

### Schedule

Click the **New** button on the **Schedule** tab to edit the various scheduling fields.

Use the **Show multiple schedules** option to set up multiple run times for the protection plan. You can create a single schedule for a plan that covers multiple days, times, and frequency of plan executions.

The field **Schedule Task** specifies how often the scheduled task (your protection plan) runs. Options are:

- **Daily**
- **Weekly**
- **Monthly**
- **Once**
- **At System Startup**
- **At Logon**
- **When Idle**

The field **Start Time** specifies the starting time of the protection plan if the plan is scheduled for **Daily**, **Weekly**, **Monthly**, or only **Once**.

The field **Schedule Task Daily** (or **Weekly**) specifies how often, in days or weeks, the plan runs.

### Advanced Schedule Options

An additional set of options to create enhanced schedules is available by clicking the **Advanced** button of the **Schedule** tab.

The **Start Date** field allows you to choose the starting day for the plan to run.

The **End Date** field allows you to choose the date that the plan will stop running. This field is optional and does not need to be set.

The **Repeat task** field allows you to set a plan to run repeatedly at the interval specified in the **Every** fields.

## Run, Edit, Remove a Plan

Click on the links below for details on running, editing, and removing protection plans.

- Running Protection Plans
- Editing Protection Plans
- Removing Protection Plans

### Running a Plan

After creating a protection plan, the plan name and scheduling behavior that you specified is displayed in the **Archive Manager**.

You can configure protection plans to run either as *unscheduled* or *scheduled*. An *unscheduled* plan can only be executed by clicking its **Run** action. A *scheduled* plan can be executed by waiting for the scheduled day and time to start the plan, or by clicking its **Run** action.

See Scheduling Protection Plans for information on creating and modifying protection plan schedules.

### Editing a Plan

You can edit a protection plan at any time; however, if the plan is running at that time, your changes will not take effect until the next time the plan runs. To edit a plan, click its **Plan Settings** action.

To change the store that the plan uses for archiving, click the **Change** button on the **Settings** tab and select from the list of available stores.

Click the **Apply** button at any time to save changes made so far. Click the OK button to save any changes and return to the protection plan page. Click the **Cancel** button to return to the protection plan page without saving any changes.

The following describes settings you can change specific to plan type.

### Files and Folders Protection Plans

From the **Plan Settings** page of a **Files and Folders** protection plan, you can:

- change the store that the plan uses for archiving
- add more folders/files to be protected
- remove folders/files to be protected
- exclude certain folders/files
- exclude predefined file types
- change the temporary file storage location

To change which folders and files are protected by the plan, choose the plan settings **Folders** tab, then click **Add** to add **Include** or **Exclude** rules. Exclude rules always override include rules. For instance, if you include *.tmp and also exclude *.tmp, all .tmp files will be excluded. See Excluding File Types for information about excluding predefined file types from a Files and Folders protection plan.

### Exchange Protection Plans

From the **Plan Settings** page of an Exchange protection plan, you can:

- change the store that the plan uses for archiving
- select/deselect Exchange Storage Groups or databases to be protected
- change the temporary file storage location

### SQL Server Protection Plans

From the **Plan Settings** page of an SQL Server protection plan, you can:

- change the store that the plan uses for archiving
- select/deselect SQL databases to be protected
- select/deselect log truncation per database

  Note: The **Truncate logs of Full Recovery Model databases** switch is ignored on protected databases configured for the *simple* recovery model.

- change the temporary file storage location

### Computer System Protection Plans

From the **Plan Settings** page of a Computer System protection plan, you can:

- change the store that the plan uses for archiving
- select/deselect drives to be protected
- change the temporary file storage location

#### Excluding File Types

Your computer contains many types of files. The types of files may range from simple text files to word processing, spreadsheet, picture, project, music, video, and so on.

When a protection plan runs for the first time, the software performs data compression and data deduplication on all the files specified by the protection plan and builds an index so that the current and subsequent plan runs will achieve the best data reduction possible.

Some file formats do not compress well. The contents of these files are static, that is, the files themselves probably will not change. Examples of these kinds of files are music and audio files, video files, photographs and images (pictures, etc.), and compressed files. This software will protect all of these files and ensure that these files are only archived once (assuming the file does not change), but these files could take up a significant amount of space on your storage disk. If you have collections of music, video, or photos that are multiple gigabytes in size, you may want to protect these files by using a second store on a second disk and use your primary storage for your important business type data.

While editing a protection plan from its **Plan Settings** page, you can easily exclude file types from your plan. In the **Folders** tab click the **Exclude file types** button to display a list of predefined file types that can be excluded. There are several categories of file types that you can exclude from a protection plan. To expand these categories, click the plus sign. Select the file types you want to exclude by checking the appropriate boxes.

The **Folders** tab then updates with the file types that are excluded.

### Changing a Protection Plan Schedule

You can change a protection plan run schedule by clicking on its **Edit Schedule** action. See Scheduling Protection Plans for information about scheduling protection plans.

### Removing a Plan

A protection plan can be removed by clicking its **Delete Plan** action.

After clicking **Delete Plan**, you will be asked to confirm the action. From the confirmation dialog box, you can choose to delete the associated configuration file (this is checked by default) and the associated archive (this is not checked by default).

If you do not delete the associated archive, you can still restore data by clicking the **Restore** action of the archive under its parent store in the **Stores** folder. If you delete the associated archive, it will be moved to the **Recycle Bin** of the store with a timestamp added to its name indicating when it was deleted. The archive remains in the recycle bin until deleted by the **Delete** action or the store purge task. While the deleted archive is in the recycle bin, you can open it and restore individual point-in-time catalogs back to the archive by clicking the **Restore** action. After a point-in-time catalog is restored from the recycle bin, it can be explored and its contents restored as if it had never been deleted.

See Store Expiration and Store Purge for more information.

## Protection Plan Results

To quickly determine the results of a local protection plan run, select Local Plans, then the Protection Plans action. Look at the plan **Status** field in the center pane when the run is complete. After a plan run, the **Status** line displays one of the following states: **OK**, **Cancelled**, **Error**, or **Warnings**. For a remote computer protection plan, select the remote computer name under the Remote Computers folder, then the Protection Plans action.

See also: Checkup Report.

To see **Result Details**, click on the **History** action, then select the plan run result for which you are interested in viewing. Each plan run result has a **Result**, **Start** and **Finish** time to help you identify which result you may want to view. The **Result Details** view displays both text and a graph which includes:

- the data reduction ratio for this run of the plan
- how many files were protected by the plan
- how many new and changed files were encountered since the last run of the plan
- the amount of data processed by the plan
- the amount of data that was changed since the last run of the plan
- the amount of data that was stored on the backup disk

On the first plan run, the **New files** count equals the **Files protected** count, and the number of **Changed files** is zero. Also, in this case the **Total changed** bytes count equals the **Total processed** bytes count. The green color in the graph depicts the amount of data that is stored on the backup disk during this plan run. The yellow color in the graph depicts the amount of data that the software has reduced or factored during this plan run.

When the **View Log** link is opened, you will see a log file containing more detail.

The log file includes statistics that require a couple of definitions:

- "Data reduction" - the ratio of "New and changed" data to the "Total stored" (total amount of data written to the disk for this run of the plan)
- "CCF Ratio" - the ratio of the "Protected data" (all of the data protected by the plan) to the "Total stored" (total amount of data written to the disk for this run of the plan)

Looking at the **Result Details** for a plan that has run after some changes have taken place in the data and the plan has been run again, you will see the amount of **Total processed** data stays about the same. The software scans all of the files selected in the plan but identifies data that is new or changed.

The graph depicts the amount of unchanged data in blue and with the label **Unchanged**. The new and changed data, which the software reduced or **Factored**, is shown again in yellow, and the amount of data actually **Stored** to the disk is shown again in green.

## Restoring Your Data

Click on one of the following topics for help with restoring your data. You can restore data from an archive, **Local Plans** folder, or protection plans configured for a remote computer by selecting the **Restore** action.

- Exploring and Restoring Folders and Files
- Restoring Exchange Data
- Restoring SQL Server Databases
- Restoring Data from a Vault

### Finding a Plan's Archive Restore Point

When you click on the protection plan (or archive) **Restore** action, you will be presented with a calendar showing the current day of the current month. Dates of the month that are in **bold** font are days when the protection plan has been run. Clicking on one of those dates will show the restore points that are available for that day.

The Status column shows **Available** or **Offline**. The Status **Available** means that the restore point can be viewed and explored or restored because the storage containing that restore time is currently online and available. The Status **Offline** means that the storage containing that time is not available.

### Exploring and Restoring Folders and Files

This software provides instant access to the data you have archived by taking advantage of random access storage. The process of finding and restoring your data is easy because the software can display your data using a familiar Windows Explorer interface that you use every day.

You can restore your entire protection plan or even restore single files using a drag-and-drop (or copy-and-paste) method.

#### Explore a Plan's Archive

You can explore archived data from the **Local Plans** folder with the **Restore** action selected, or from a remote computer in the **Remote Computers** group folder with the **Restore** action selected, by then selecting a date on the calendar and a restore point that is listed as **Available** in the **Status** column, and then clicking the **Explore** button. A Windows Explorer view of the archive restore point appears.

Click on the folder in the window just like you would in any Windows Explorer view and see your individual files.

You can open any of the files by double-clicking on the file and using the appropriate application to view the file. When viewing a file, the file will be opened as a read-only file. You can restore a file by using the copy-and-paste or drag-and-drop method, or by right-clicking a file or folder and selecting **Restore** from the menu.

If you select **Restore**, see Step 2 of Restoring Files and Folders.

### Drag and Drop Restore

You can restore a single file or groups of files using the same standard drag-and-drop or copy-and-paste methods that you use when transferring your files within Microsoft Windows Explorer.

Restoring a file begins with finding the plan's archive restore point you want to explore. Refer to Finding a Plan's Archive Restore Point.

Click on a restore point and the **Explore** and **Restore** buttons will become active.

Click **Explore** and in a few moments the Windows Explorer view will open. You can now navigate the data you archived.

You can restore by using your mouse to drag files to a folder location, or even just to your desktop. You can also restore by right-clicking the files and clicking **Copy** in the menu, then open the folder where you want to copy the files and right-click **Paste**.

### Restoring Files and Folders

#### Step 1 - Find the protection plan restore time

In addition to restoring an individual file or a group of files, the software can restore an entire archive at a given point in time. Generally, you only need to restore an entire archive in the case of moving files, accidental deletion, restoring a system after a disk change or crash, etc.

The process of restoring an entire archive begins with finding the restore point for the archive you want to restore. Refer to Finding a Plan's Archive Restore Point.

Select the restore point you want to restore and the **Explore** and **Restore** buttons in the lower-right portion of the screen become active. Click **Restore**, and a **Point-in-Time Restore** dialog box appears.

#### Step 2 - Choose how to restore

There are three basic questions to answer when restoring a **Files and Folders** protection plan:

- What location, or folder, should I choose to restore my files?
- Should I replace existing files?
- Should I remove extra files from the restore location?

**Restore Location**:

- **Original location** - Your files can be restored to their original folder from which they were archived. This is the default operation. If the folder which contained the files at the time the

files were archived no longer exists the software will create the folder.

- **Alternate location** - You can restore your files to an alternate folder, that is, a folder different from the one(s) from which you archived the files. This option will preserve the folder structure of the archived data. That is, all folders and subfolders that existed when the protection plan archived the data will appear in the alternate folder you choose.

To restore to an alternate folder, click the **Restore files to** drop-down feature and click **Alternate Location**. When this action is done, the text next to **Alternate location** becomes active and is displayed as a blue link.

When the link **Click here to select an alternate folder** is clicked, a dialog window opens where you can choose a folder to restore the files.

### Restore Options:

There are four options to choose from when replacing the files.

- Choose **Missing files** if you do not want the restore operation to copy over files that are already in the restore location. This option only restores files that are not present in the folder where you have chosen to restore the files. You might choose this option to only copy files you believe are missing from a folder. If you have chosen to restore the archive to an alternate folder, then it is possible that all files will be restored since the alternate folder may not contain any of the files in the archive.

- Choose **Missing files and files that have changed** if you want the restore operation to restore files that no longer exist in the folder (missing) and files that that have a different Last Modified Time than those in the restore point. You might choose this option to replace a file on your hard disk with a different version from the restore point. If you have chosen to restore to an alternate folder, then it is possible that all files will be restored since the alternate folder might not contain any of the files in the archive.

- Choose **Missing files and replace existing files** if you want the restore operation to restore files that no longer exist in the folder (missing) and to replace all files in the restore location regardless of whether the archived files are newer or older. You might choose this option if you are rebuilding a particular area of your hard disk.

- Choose **Missing files, files that have changed, and remove extras** if you want the restore operation to restore files that no longer exist in the folder (missing) and files that have a different Last Modified Time than those in the restore point, and remove all files and folders from the restore location that do not exist in the restore point. You might choose this option to replace a file on your hard disk with a different version from the restore point and remove any files that were created since this restore time. If you have chosen to restore to an alternate folder, then it is possible that all files will be restored since the alternate folder might not contain any of the files in the archive.

After choosing the options, click **Restore**, and the software will begin to restore the files. After the restore is complete you can view the log file for the restore by clicking **View Log**. A record of the restore will also appear in the results page under the corresponding protection plan name. You can view the record of the restore by clicking the **History** action. In the **Action** column, will be the word **Restore** and the date and time of the restore.

## Restoring Exchange Data

An Exchange protection plan backs up Microsoft Exchange databases and log files for each Microsoft Exchange Storage Group selected. After the plan runs, eligible logs are truncated. This page discusses the process of restoring and recovering Exchange databases.

The software protects Microsoft Exchange using the Microsoft Exchange Writer for VSS included with newer versions of Windows. When a Microsoft Exchange Storage Group is backed up by the

software, the VSS Writer is invoked and the files that compose the databases, log files, and ancillary meta files are backed up in an open state (while the mailbox stores are mounted). Email transactions and new log files are deferred in memory while the existing files are backed up. Because databases are protected in an open, or victimized state, recovery steps are necessary before restored databases can be remounted in Exchange.

When restoring one or more Microsoft Exchange Storage Groups (for Exchange Server 2003 or Exchange Server 2007) or databases (for all newer versions of Exchange) from an Exchange protection plan, all files composing the Microsoft Exchange Storage Group or database are restored to an alternate location of your choosing. The software never restores the database files back to their original location, due to the potential of corrupting running mailbox databases. After restoring all files from your protection plan, you must run an Exchange recover command using the Microsoft utility ESEUtil.exe, included with Exchange, before the individual databases can be used again by Exchange. You may replace an existing damaged Exchange database, or simply recover data from a mailbox by mounting the database in an Exchange Recovery Storage Group (for Exchange Server 2003 or Exchange Server 2007) or recovery database (for all newer versions of Exchange).

The process of restoring a protection plan begins with finding the restore point for the plan you want to restore in the **Archive Manager** software. Refer to Finding a Plan's Archive Restore Point.

Select the restore point you want to restore and the **Restore** button in the lower-right portion of the screen becomes active. Click **Restore** and a **Storage Group Restore** dialog box appears. Choose a volume or directory with enough space to save all log files and all databases for the Microsoft Exchange Storage Group.

To use the restored database files with Exchange, they must be recovered and reattached to the Exchange Server. For information on recovering and attaching databases to an Exchange Server please refer to the following links:

- Exchange 2003/2007

  http://technet.microsoft.com/library/aa998848(EXCHG.80).aspx

  http://support.microsoft.com/default.aspx/kb/824126

  http://technet.microsoft.com/library/aa996168(EXCHG.65).aspx

- Exchange 2010/2013

  http://technet.microsoft.com/library/dd876954.aspx

  http://technet.microsoft.com/library/ee332321.aspx

  http://technet.microsoft.com/library/ee332351.aspx

## Restoring SQL Server Databases

A SQL Server protection plan backs up all required files for each SQL Server database selected. This page discusses the process of restoring and recovering SQL Server databases.

In addition to restoring an individual database or a group of databases, the software can restore the entire protection plan. Generally, you only need to restore an entire protection plan in the case of accidental deletion, or restoring a system after a disk change or crash.

This software protects Microsoft SQL databases using the Microsoft SQL VSS Writer included with newer versions of Windows. When a database is backed up by the software, the VSS Writer is invoked and the files that compose the database are backed up in an open state (while databases are mounted). New transactions are deferred in memory while the existing database and Transaction Log files are backed up. The databases are left in an open state in the store targeted by the protection plan.

The software does not allow you to restore the database files to the original location. You must always choose an alternate location for restoring. The software never restores the database files back to their original location due to the potential of corrupting running databases. After restoring, you will need to reattach the database to the SQL Server. Whether the goal is to replace an existing damaged database, or simply to recover data from a table or tables, will determine if you should move the restored files to the original location of the database files, or leave them in their restored location. Never overwrite your original database files. Rename them and later delete them when your recovery is complete.

The process of restoring a protection plan begins with finding the restore point in the **Archive Manager** software for the plan you want to restore. Refer to Finding a Plan's Archive Restore Point.

Select the restore point you want to restore and the **Restore** button in the lower-right portion of the screen becomes active. Click **Restore** and a **Database Restore** dialog box appears.

After restoring, you simply need to reattach the database files to the SQL Server instance. Please refer to http://msdn.microsoft.com/en-us/library/ms190209.aspx for information on attaching databases to SQL Server instances.

## Restoring Data from a Vault

There are three steps to restoring data from a vault:

- Locate
- Prepare
- Restore

### Locate

Locate the vault's restore point to restore or restore from.

From either the **All Cloud Vaults** folder or the **All Tape Vaults** folder, open the vault to restore from and then open its **Archives** folder. When you click on the archive you want to restore from you will be presented with a calendar showing the current day of the current month. Dates of the month that are in **bold** font are days when the store vaulting task has been run. Clicking on one of those dates will show the restore points that are available for that day.

The Status column shows 'Available, Vaulted' or 'Offline, Vaulted'. The status 'Available, Vaulted' means that the restore point can be viewed and explored or restored because the storage containing that restore point is currently online and available. The Status 'Offline, Vaulted' means that the storage containing that restore point is not available.

### Prepare

Prepare the restore point for restoring.

The restore point that is presented is from the cache. (See Configure Vaulting.) Although you can explore it in the cache by clicking the **Explore** button, the actual data is not available until it has been restored from the vault to the cache by clicking the **Prepare** button.

Note: If you do try restoring before it has been prepared, the restore job will fail with errors like 'The content store is not consistent' and 'The system cannot find the file specified' logged in the log file.

Note: If you try opening a file through the Point-in-Time Explorer (**Explore** button) before the point in time has been prepared you will see a message like 'The file cannot be accessed by the system'.

### Restore

Restore the data.

After preparing the point in time for restoring, you can restore as you would from a store. See Restoring Your Data for more information.

## Restoring a Computer System

The Computer System protection plan stores all of the system information to needed to restore a computer, and optionally any attached data disk volumes. You can also restore individual files and folders using the **Explore** and **Restore** actions. See Restoring Files and Folders. You must use the System Recovery Environment to restore an entire system.

Assuming you have run a Computer System protection plan for the system to be restored and have saved the System Recovery Environment to media, you can restore the computer system as follows:

### Booting a Computer for Recovery

The System Recovery Environment (SRE) is used to boot a computer for recovery. Most computer systems can boot from CD/DVD or USB drives. Check your computer specifications and BIOS support for booting from CD/DVD or USB drives. You may have to select the boot drive from a boot menu at startup or adjust the BIOS to boot from a CD/DVD or USB drive.

Virtual machine (VM) hosts allow guest virtual machines to boot from physical CD/DVD drives or ISO image files. To recover the VM, first configure it to boot the SRE.

Once you boot the SRE you are presented with the SRE Launch screen. This screen allows you to restore a system by following a step-by-step wizard. From the SRE Launch screen you can open a command prompt, shut down or restart the computer.

Most system restores can be performed without requiring the use of the command prompt, however there are several reasons you may need to use the command prompt. For example, you may need to set an IP address for a network adapter using the netsh command, if a DHCP server does not automatically provide one.

### Restoring your Computer System

From the SRE Launch screen, select **Restore your computer** and follow the step-by-step wizard.

The first step is to identify the storage that contains recovery points created by Computer System protection plans. There are two locations the wizard can search to find recovery points: local disks and network locations.

Note: To search network locations the SRE needs to bind to a network adapter. At boot time the SRE searches all of the network drivers to find a match for your hardware. If a network driver is available for your system it is loaded and attempts to obtain an IP address using DHCP. If a network driver cannot be loaded by the SRE you can click **Load Driver** to browse for a 32-bit (or 64-bit if using the SRE for systems that boot using UEFI) network adapter driver compatible with your system. Once the network driver is loaded, the driver attempts to obtain an IP address using DHCP.

If you click **Search local disks**, the disk drives are scanned for systems to recover.

If you click **Search network locations** you are prompted to map a network drive letter to a network location or UNC path. If your storage device is connected to another computer, you will need to share the drive before you can connect to the device over the network. Enter the credentials for the user account when prompted and then click **OK**. Note: Use the same account for accessing the storage through a network folder that you used for your Computer System protection

plan. Once connected, the disk drive is scanned for systems to recover.

Next, choose the system to recover and a recovery point. Each system that has recovery points available is displayed showing the system name, OS version and build number. Select the recovery point you would like to use and click **Next**.

Next, configure the volume-to-drive mapping for the restore. The original volumes that were backed up by the protection plan are displayed with the original drive letter, label, capacity and file system type. Check the first drive you would like to restore. The **Map To** column will automatically choose the first disk drive attached to the system. If this is not the desired mapping you can change the disk from the drop-down menu in the **Map To** column. You can change the size of the volume that will be created on the drive by selecting the ... button in the Restore Size column. If the volume mapping you have specified is smaller than the original capacity, the mapping will have a warning icon; otherwise, it will have a checkmark icon.

Note: If a drive is missing for a volume mapping you may need to install a driver for a storage controller. To install a driver click **Load Driver** and browse to a location containing a compatible 32-bit driver (or 64-bit driver if using the SRE for systems that boot using UEFI). Once the driver is installed, click **Rescan** to scan for drives to map to volumes.

Once you are satisfied with your mappings click **Next** to go to the final page.

On final page there are two options:

- **Restore saved boot information (Recommended)** - repairs the boot records used to initialize the recovered operating system. After restoring the file data, the SRE will display a command window prompting you to repair the boot records for any operating systems that it finds on the restored computer. If you do not repair the boot records of the recovered operating system, it may not boot. If you do not restore the saved boot information, you will need to manually repair the boot records using other tools from within the SRE or use the Windows Recovery Environment (WinRE).
- **Run restore with high performance settings** - uses multiple processors to accelerate restore.

When you are ready to recover the system, click **Recover**. You will be warned that the data on the existing volumes will be destroyed. Click **Yes** to continue or **No** to return and change your settings.

While the restore is running you can monitor the throughput and an estimate for when the restore will finish.

After the recovery completes you can view the restore log or click **Finish** to return to the SRE Launch screen.

Once back at the launch screen, you can choose to restart the computer and boot into the recovered OS. Note: You may need to adjust your BIOS boot menu if you changed it during the recovery process.

## Stores

The **All Stores** folder shows the current availability of archive storage and available free space.

After adding a store, the status in the **center console** pane of the **Archive Manager** shows the new store and its status. To change the settings for a store, select the store and click **Properties**.

The store architecture has changed beginning with version 9 of the software. This new architecture provides significant performance improvements for store tasks and protection plans. To take advantage of these improvements with stores created in versions of the software prior to version 9, simply select the store's **Properties** page and click the **Improve storage performance** button to begin the conversion process. This button is only visible for stores that have not been converted. As noted on the **Convert Store** page (shown after clicking the Improve storage performance button), all stores associated with this store through **Store Copy** tasks must also be converted. This includes stores located on other Archive Manager servers. That means these remote servers must also be

running version 9 or newer in order to convert their stores.

The **Status** column shows the availability status of the storage media. If the status is **Available**, then this media is available for use. An **Offline** status means that the media is currently not available.

The **Capacity** column displays the native capacity of the storage.

The **Free Space** column displays the native free space of the storage.

After highlighting a store in the tree pane, you can display its **Details**, **Usage History**, **Store Tasks**, and **Task History** by clicking on the appropriate action in the **Actions** pane.

Please refer to the following topics for more information:

- Adding Storage
- Removing Storage
- Store Tasks
- Store Actions
- Store Properties

## Adding Stores

A new installation of the software will not have any storage assigned to it. Highlight the **Storage** folder in the console tree and click the **Add a Store** action to start the **Add Store** wizard.

There are four categories of storage to choose from. Click on a topic below for more information.

- Disk Drive Storage
- Network Drive Storage
- Removable Disk
- LTFS Drive
- File Folder Storage

### Disk Drive

Choose **Disk Drive** if you want to create a store on a locally-attached hard disk. This option creates a store at the root of the disk that you select in the **Add Store** wizard. Choose a disk, then click the **Next** button.

If there are stores already at the root of this disk (perhaps from a previous installation of this software), you can reattach by choosing the **Use existing** option and selecting a store from the drop-down list. See Use Existing Store for more information. If no stores exist at the root of the disk, this option will be disabled.

To create a new store, choose **Add new** and enter a descriptive name for your new store. After the store has been created, this name is displayed in the **Archive Manager** tree pane under the **All Stores** folder.

If this is an existing store, the **Prepare Store** screen will have a **Reconnect** button. Otherwise, it will have a **Prepare now** button. Preparing a store creates the file and folder structure used by the software to store and track your protected data. Preparing a store does not destroy any data already

on the disk.

Click the **Prepare now** (or **Reconnect**) button. When the prepare or reconnect process is complete, the progress indicator will show **Preparation Complete** and the **Next** button will be enabled. Click **Next** to continue to the **Store Added** screen.

The **Store Added** screen shows a high-level summary of the store configuration. Notice the **Storage location** value is <*drive letter*>:\ObjectStore{...}. This is a hidden system folder. The store name you entered is used within the **Archive Manager**. After clicking **Finish**, the new store is added to the **All Stores** folder and can be used by protection plans.

### Network Drive

Choose **Network Drive** if you want to use network-attached storage (NAS). This option creates a store at the root of the network storage share you select in the **Add Store** wizard. Choose a network drive, then click **Next**. If your network storage isn't listed, you will need to make it known to your computer by either mapping a drive or adding a network location:

- On Windows XP and Windows Server 2003 operating systems, click the **Map network drive** link to launch the **Windows Map Network Drive** wizard. When mapping the NAS, it is recommended to select the **Reconnect at logon** option to ensure availability of the storage.
- On other Windows operating systems, you can either map a drive as described above, or you can add a network location. To launch the **Add Network Location** wizard click the **Add a network location** link.

If there are stores already on this NAS (perhaps from a previous installation of this software), you can reattach to them by choosing the **Use existing** option and selecting a store from the drop-down list. See Use Existing Store for more information. If no stores exist on the NAS, this option will be disabled.

To create a new store, choose **Add new** and enter a descriptive name for your new store. After the store has been created, this name will be displayed in the **Archive Manager** tree pane under the **Stores** folder.

If this is an existing store, the **Prepare Store** screen will have a **Reconnect** button. Otherwise, it will have a **Prepare now** button. Preparing a store creates the file and folder structure used by the software to store and track your protected data.

Click the **Prepare now** (or **Reconnect**) button. When the prepare or reconnect process completes, the progress indicator will show **Preparation Complete**, and the **Next** button is enabled. Click **Next** to continue to the **Store Added** screen.

The **Store Added** screen shows a high-level summary of the store configuration. Notice the **Storage location** value is \\<NAS n*ame*>\<*share name*>\ObjectStore{...}. This is a hidden system folder. The name you entered is used within the **Archive Manager**. After clicking **Finish**, the new store is added to the **Stores** folder and can be used by protection plans.

### Removable Disk

Choose **Removable Disk** if you want to use a removable disk drive. This option creates a store at the root of the drive that you select on the **Add Storage** screen. Choose a removable disk drive, then click the **OK** button.

If there are stores already on this disk (perhaps from a previous installation of this software), you can reattach by choosing the **Use existing** option and selecting a storage location from the drop-down list. See Use Existing Store for more information. If no storage locations exist on the drive, this option will be disabled.

To create a new store, choose **Add new** and enter a descriptive name for your new store. After the store has been created, this name is displayed in the **Archive Manager** tree pane under the **Stores**

folder.

If this is an existing store, the **Prepare Store** screen will have a **Reconnect** button. Otherwise, it will have a **Prepare now** button. Preparing a store creates the file and folder structure used by the software to store and track your protected data.

Click the **Prepare now** (or **Reconnect**) button. When the prepare or reconnect process is complete, the progress indicator will show **Preparation Complete**, and the **Next** button is enabled. Click **Next** to continue to the **Store Added** screen.

The **Store Added** screen shows a high-level summary of the store configuration. Notice the **Storage location** value is <*drive letter*>:\ObjectStore{...}. This is a hidden system folder. The name that you entered is used within the **Archive Manager**. After clicking **Finish**, the new store is added to the **Stores** folder and can be used by protection plans.

### LTFS Drive

LTO generation 5 and newer tapes can be formatted with the Linear Tape File System (LTFS) available from third-party vendors. LTFS allows an LTO tape to be used like a hard disk. This software recognizes an LTFS-formatted tape and allows its use as a store or archive restore task target.

Certain precautions must be taken when using LTFS. See your LTFS vendor documentation for full details. In particular, you should never shut down the computer while an LTFS tape is mounted, and you should only eject the tape from the Windows Explorer view (right-click-Eject). The LTFS software disables the unload button on the tape drive, and this software disables the load/unload actions for LTFS tapes.

### File Folder

Note: This option is provided primarily for legacy purposes. In earlier versions of the software, stores were normally created at the folder level. Choosing this option allows you to reconnect to those stores.

Choose **File Folder** if you want to create or reconnect to a store in a folder on a locally-attached disk drive. Select the folder via the link **Click here to select a folder**. If this is a new store, you will be prompted to give it a name. Enter a descriptive name for your new store. After the store has been created, this name is displayed in the **Archive Manager** tree pane under the **Stores** folder. Click **Next** to continue with the **Add Store** wizard.

If the folder is an existing store (perhaps from a previous installation of the software), the **Prepare Store** screen will have a **Reconnect** button. Otherwise, it will have a **Prepare now** button. Preparing a store creates the file and folder structure used by the software to store and track your protected data.

Click the **Prepare now** (or **Reconnect**) button. When the prepare or reconnect process is complete, the progress indicator will show **Preparation Complete**, and the **Next** button is enabled. Click **Next** to continue to the **Store Added** screen.

The **Store Added** screen shows a high-level summary of the store configuration. After clicking **Finish**, the new store is added to the **Stores** folder and can be used by protection plans.

### Use Existing Store

You can reattach a store to this software if it had been removed with the **Keep the data on the media for future use** option. See Storage Remove for more information. You can also add existing stores from another system in the same manner.

To use an existing store, first click the **Add a Store** action, then choose the physical storage containing the existing store.

The software will detect that there are stores already on the physical storage and will enable the **Use existing** option. Choose **Use existing** and select a store from the drop-down list. If no stores exist on the storage media, this option will be disabled.

After clicking the **OK** button, the store appears under the **Stores** folder and archived data in this store may now be explored and restored; however, you cannot add any new data.

### Removing Storage

You can remove stores from this software. You might remove a store if you want to set the storage aside for just restoring data. This action helps reduce the number of stores you are viewing in the store status panel to just the current ones being used by your protection plans. Note that removing storage is an optional procedure. The storage can be used for restoring data, or used by protection plans for storing data (assuming it is not full) by adding it back to the software via the **Add a Store** action.

To remove a store, choose the store to remove from the software, then click its **Remove Store** action to open the **Remove Store** dialog.

Note: You cannot remove a store that is being used by protection plans or is used by any store copy task.

You must decide whether or not to delete the data on the media.

- Keep the data on the media for future use

  When storage is removed from the software, the stored data is not removed or deleted. However, you will be unable to restore files in the removed store. If you want to use the storage again to archive protection plans or restore files, you must perform the Add a Store action. See Use Existing Store for more information.

  When **Cancel** is clicked, the **Remove Store** dialog box closes, and the software will take no action.

  When **Continue** is clicked, the software removes the storage. The following actions will take place:

  - the selected store is removed from the **Storage** area in the console tree
  - all restore points for archives associated with the storage are removed from the **Explore** page

- Permanently delete the data on media

  When storage is permanently deleted from the software, the stored data is destroyed. You can reuse the media for new storage, but you will not be able to access any old data.

  When **Cancel** is clicked the **Remove Store** dialog will close and the software will take no action.

  When **Continue** is clicked, the software will ask for confirmation.

  Click **No** to return to the **Remove Store** dialog without removing the storage. Click **Yes** to remove the storage. The following actions will take place:

  - the selected store is removed from the **Storage** area in the console tree
  - all restore points for archives associated with the storage are removed from the **Explore** page
  - data is completely destroyed for the selected store

### Store Tasks

Store tasks are tasks that operate at the store level. You can create tasks for copying stores, vaulting data in its deduplicated state from a store to either cloud or LTO tape, verifying data in a store, expiring data in a store, purging expired data from a store, and restoring store archives to an alternate location.

Please refer to the following links for more information:

- Store Copy
- Store Vaulting
- Store Verify
- Store Expiration
- Store Purge
- Archive Restore

## Store Copy

Store copy tasks allow you to copy a selection of archives from one store to another. You can copy archives between stores within the same **Archive Manager** system , or you can copy archives to or from a store on another **Archive Manager** system .

Before you create a store copy task, both stores, source and destination, must exist. They must also be of the same generation.

The store copy task is associated with the store it is created from. This store can be the source store or the destination store. Initially it will be the source store, but this can be changed before the task is actually created.

When copying stores to or from a different **Archive Manager** system, performance is generally better when *pushing* data rather than *pulling* it. Beginning with version 9.0 the software performs a verification of the latest restore points prior to copying data. Because this verification is quickest when performed on the source store it is better to *push* the data from the source store rather than *pull* it from the destination store. Just the opposite was true with earlier versions of the software where pulling was the recommended method. If stores have recently been converted to the version 9.0 generation, new store copy tasks should be created on the source stores, if they do not already exist, so that data is being pushed to the destination store.

Note: The source and target stores must be of the same generation. For example, if you want to copy an older *legacy* store that was created with a version of the software prior to version 9, you would need a target store of the same generation. If one of the stores is a new (version 9) generation the older store must be converted. If you are targeting a single store and it is not compatible a message box will pop up telling you to first convert the store and then create the task. If you are targeting a **Store Group** no message popup will occur and the task will fail when it is run. In this case the task history log will indicate the problem. See Store Generations for more information.

### Creating a Store Copy Task

Assuming both a source and destination store exist, select the store from the **Archive Manager** console tree that you want the store copy task to be associated with and then click the **Create Store Task** action, then select Create Store Copy Task. This action opens the **Create Store Copy Task** wizard with the selected store shown in the **Source Store** window of the **Create Store Copy Task** screen. Other stores configured for this **Archive Manager** server are listed in the **Destination Store** window. Click the **Browse** button to select a store on another **Archive Manager** server.

You can reverse the source and destination lists by clicking the double-ended arrow button. You would do this if you wanted the store listed in the **Source Store** window to actually be the destination store.

Select your destination store from the **Destination Store** window. Contents of the highlighted store in the **Source Store** window are copied to the highlighted store in the **Destination Store** window. Click **Next** to continue.

If there is more than one archive in this store (for example, more than one protection plan is writing to this store), you can copy all archives or a subset of archives. Click **Next** to continue.

On the **Configure Restore Points to Copy** screen, you can choose to copy all restore points or copy only the most recent restore point. Make your choice, then click **Next** to continue.

Enter a meaningful name for this task on the **Copy Task Name** screen, then click **Next** to continue to the **Schedule Copy Task** screen.

You can schedule this task to run automatically or click **Next** to accept the **No Schedule** default. The task runs as the currently-logged-on user unless you change the **Run as** account information on the **Task** tab of the task scheduler.

Review the store copy task settings shown on the **Completing the Add Store Copy Task** wizard screen. If you need to make changes, navigate back via the **Back** button. When you are satisfied with the settings, click the **Finish** button. If you have not entered account information on the User Account tab of Archive Manager Properties, you will be prompted for the password of the account specified to run the plan. After you enter the password, the task is created, the **Create Store Copy Task** wizard closes, and the new task appears in the store tasks results of the store where the task was created.

## Common usage scenarios for the Store Copy task

### Copy local drive store to store on removable storage

A good backup plan often includes taking the backup media to an off-site location. You could set up a store copy task to run, for instance, once a week, and only copy the most recent restore point from each archive, thereby allowing for many weekly backups on removable disk or USB storage.

### Copy a store from one Archive Manger server to another Archive Manager server

As mentioned above, performance is better when *pushing* data rather than *pulling* it. For best performance, you should create the store copy task on the **Archive Manager** server that you are copying the data from and set the store to be the source store.

### Seeding a store from a remote site

This software employs source-based deduplication, in which data processing is distributed across a network of servers and only the deduplicated data is moved across a LAN or WAN to a store. If a large amount of deduplicated data has to travel across a slow WAN link during the baseline run of a system in a remote office, the baseline run time may be unacceptably long due to the bandwidth bottleneck. Once the baseline run has completed, however, subsequent runs will skip items already in the store and only process new and changed data. Only the deduplicated versions of active data moves across the WAN and into the store, greatly reducing the backup window and making protection of remote systems across the WAN feasible. To facilitate the baseline run of a system in a remote office, the deduplicated data may be saved to a removable storage device plugged directly into the remote system, and then shipped to the location of the **Archive Manager** server for synchronization, thus *seeding* the store for future runs.

Follow these steps for seeding a store from a remote site:

1. Configure storage at the remote site for the plan to use.

   Attach a removable storage device to the remote computer that you want to protect. If USB connected, make sure the server supports at least USB 2.0. It will appear in the Computer window with a local drive letter, for example, H:. Share the root of the drive and allow *Full NTFS* permissions to the Domain Admins Group. You can configure a NAS device with a share instead, as long as the share is accessible to **Archive Manager**.

2. Add a store to the share at the remote site.

   In **Archive Manager**, click the **Stores** folder and choose the **Add a Store** action. In the **Add Store** wizard, select **Network Drive**, click the link to map a network drive (or add a network location). Map a drive to the share on the removable storage device, choosing a drive letter for the mapped drive and entering the UNC path to the share, e.g. \\<*remote computer name*>\<*share name*>. Once mapped, the share appears in the **Select a Network Drive** window. Select the share and click **Next**. Name the store with a unique name (for example, the permanent store name plus "_temp"). Click **Next**. Prepare the store by clicking **Prepare Now** and complete the **Add Store** wizard.

3. Add a protection plan for the remote computer.

   In **Archive Manager**, expand the **Remote Computers** folder, select the **All Computers** group, right-click and select **Add Computer**. Add the remote computer by machine name or IP address. (Note: Exchange and SQL require the machine name.) Click on the newly-added computer. In the **Actions** pane, select **Create Protection Plan**. Step through the protection plan wizard. Give the plan its permanent name. The plan name will not change. Add the folders to be protected and select to use the store created in step two.

4. Run the plan one time. The baseline is generated and stored.

5. Run the plan at least two more times so items in the store are verified.

6. Set the plan to run to the permanent store.

   Once the protection plan completes, in **Archive Manager**, under **Remote Computers**, **All Computers**, select the remote computer. The plan appears in the center pane. Highlight the plan. In the **Actions** pane, select **Plan Settings**. On the **Settings** tab, click the **Change** button. Choose the permanent (seeded) store from the list of available stores. Click **OK**. Click **OK** again.

7. Remove the USB device properly with the Safely Remove Hardware icon in the system tray. This action will flush buffers prior to removal. Ship the USB device and connect to the **Archive Manager** server.

8. From the **Archive Manager** list of stores, remove the store on the removable media, since it has an incorrect device path now.

   In **Archive Manager**, select the store. In the **Actions** pane, select **Remove Store**. Accept the default to keep the data on the media for future use. Click **Continue**.

9. Reconnect **Archive Manager** to the store.

   In **Archive Manager**, select **Stores**. In the **Actions** pane, select **Add a Store**. If the store is located at the root of a removable USB device, in the **Add Store** wizard, select **Disk Drive**, then select the drive letter of the USB device. Click **Next**. In the **Storage Name** window, select the **Use existing** radio button. The field becomes active, and you can then select the store on the USB device. Click **OK**. Click **Next**, then click the **Reconnect** button, then click **Finish**. If the store is located in a folder on the USB device, do not select **Disk Drive**, select **File Folder** and click the link to select a folder. Browse to the folder on the USB device that contains the store, then finish reconnecting to the store. If the store resides on a NAS share, in the **Add Store** wizard select **Network Drive**, browse to the folder that contains the store, then finish reconnecting to the store.

10. Create a store copy task to synchronize the store on the removable device with a permanent store. (If you have not created the permanent store yet, do so now.)

    In **Archive Manager**, select the store on the removable media. In the **Actions** pane, select **Create Store Task**. In the dialog box that opens, choose **Create Store Copy Task**. Select the source and destination stores. The source store is the store on the removable media. Select the

destination store from the list of available stores. The destination store is the permanent store that the plan will use in the future. Click **Next**. Keep the default selection to copy all archives. Click **Next**. Choose the default selection to copy all restore points. Click **Next**. Accept the default name for the store copy task and enter proper credentials for the task to use when it runs.

11. Run the store copy task.

    In **Archive Manager**, with the store on the removable media selected, click **Store Tasks** in the **Actions** pane. In the center pane, highlight the store copy task. Right-click the store copy task and select **Run**.

12. Run the plan to the new store. Configure a schedule for the plan (optional).

13. You may remove the store on the removable device from **Archive Manager** once you are satisfied the new configuration is working properly.

    In **Archive Manager**, select the store on the removable device. In the **Actions** pane, select **Remove Store**. Accept the default to keep the data on the media for future use or delete the contents permanently. Make sure you are deleting the correct store or permanent protection plan data loss may result. Click **Continue**.

## Store Vaulting

Store vaulting tasks copy selected archives to 'vaults' for longer-term storage. Vaults can be in the cloud or on tape, and they are created automatically when the store vaulting task is created.

Prior to creating a Store Vaulting Task vaulting needs to be configured. See Configure Vaulting.

If you haven't already done so, you can set up a cloud account for vaulting to cloud and you can add tape volume sets during the creation of a **Store Vaulting Task**.

### Creating a Store Vaulting Task

To create a **Store Vaulting Task**, select the store to vault and choose its **Create Store Task** action. On the **Create Store Task** screen choose "*Create Store Vaulting Task*" to begin the **Create Store Vaulting Task** wizard. Select either **Cloud Account** or **Tape Device**. If you are vaulting to cloud, you can sign up for a cloud account and add it to the Archive Manager system from here. If vaulting to tape, you can add a tape device here.

Note: If you know there is a tape library attached to the system but it is not showing up, check the device to make sure there is not a tape loaded into the drive.

Once you have chosen a cloud account or tape device for your vault, choose to vault all archives from the store or select individual archives to vault.

On the **Configure Restore Points to Copy** screen choose to copy all restore points, a range of restore points, or only the most recent restore point.

On the **Copy Task Name** screen, choose a name for the task and a name for the vault, then click **Next** to continue to the **Schedule Copy Task** screen.

You can schedule this task to run automatically or click **Next** to accept the **No Schedule** default. The task runs as the currently-logged-on user unless you change the **Run as** account information on the **Task** tab of the task scheduler.

Review the store copy task settings shown on the **Completing the Create Store Vaulting Task** wizard screen. If you need to make changes, navigate back via the **Back** button. When you are satisfied with the settings, click the **Finish** button. If you have not entered account information on the User Account tab of Archive Manager Properties, you will be prompted for the password of the account specified to run the plan. After you enter the password, the task is created, the **Create Store Vaulting Task** wizard closes, and the new task appears in the store tasks of the store where the task was created. The new vault will appear either in the **All Cloud Vaults** folder or the **All Tape Vaults** folder, depending on whether the vaulting task is for cloud or tape.

## Store Verify

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. A quarantined item is no longer available from the store, but if the data is available on primary storage, it will automatically be replaced (repaired) in the store during the next protection plan run. Each item listed in the **Quarantined Items** folder has either a red flag indicating that the item has not yet been repaired, or a green check indicating that the item has successfully been repaired. Items with green checks can be deleted safely from the **Quarantined Items** folder.

Note: Do *not* attempt to manually repair quarantined items. Instead, please contact Technical Support for assistance.

Verification can be accomplished in one of three ways, with the third option being a full verification of all links to content and data signature checks on every item in the store. Because this third option can take a long time to run it should only be used when disk corruption is suspected. In fact, it is not even offered as an option when creating a verification task.

When creating a Store Verify task you must choose one of these two options:

- **Check integrity of the latest restore point in each archive and verify data signature of new and changed files.**

This option is the default. It will insure that the newest restore points have been recorded successfully. Content and links of the latest restore points are verified, insuring that your latest backups are recoverable.

- **Check integrity of all restore points in each archive and verify all links to content are valid.**

Choose this option to check the entire store for missing content and bad links. Actual file content is not verified when using this option.

To create a store verify task, highlight the store in the **Stores** folder and then select the **Create Store Task** action. In the **Create Store Task** screen, choose **Create Store Verify Task** to open the **Create Store Verify Task** wizard. Enter a name that describes the purpose for this verify task. Click **Next**. Choose whether to verify the entire store contents or to perform random sample verification with each run of the task. Click **Next**. Configure a schedule for automatically running the task (optional). Click **Next**. Review the settings, then click **Finish** to create the task, enter a password for running the task and exit the **Create Store Verify Task** wizard.

You can manually run the task from the **Archive Manager** at any time by selecting the store in the **Stores** folder, then selecting the verify task in the center pane and selecting **Run** in the **Actions** pane.

To modify a store verify task, highlight the task and then select its **Task Settings** action. In addition to the two options described above is a third option:

- **Check integrity of all restore points in each archive, verify all links to content are valid, and verify data signature of all files (this can take a long time - use only if disk corruption is suspected).**

As noted in the option text, this option can take a long time to run and should only be used if disk corruption is suspected.

## Store Expiration

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.

Once the task is created, you can edit the retention settings from the store **Properties** action. To change the retention settings, select the store in the **Stores** folder of the **Archive Manager** tree console, then click the **Properties** action to open the **Properties** page. Click the **Expiration** tab to edit the expiration settings.

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**. The expired restore points are no longer exposed, but their data is still in the store.

Note: As a safety precaution, the most recent ten restore points in an **Archive** will *not* expire even though they may meet the expiration criteria. You can change this setting from the **Edit Settings** action, but the minimum value allowed is one. To remove *all* restore points from an archive, you must delete the archive.

Expired items can be removed (purged) from the recycle bin with a Store Purge task.

To create a store expiration task, select the store from the **Stores** folder in the **Archive Manager** console tree, then click **Create Store Task** from the **Actions** pane. Choose **Create Store Expiration Task** on the **Create Store Task** screen, then enter a meaningful name for the expiration task. Next, optionally set up a schedule for automatically running the task. Note: Regardless of schedule, you can always run the task manually at any time. Finally, review the task settings, then click **Finish** to create the task and exit the **Create Store Expiration Task** wizard. If you have not entered account information on the User Account tab of Archive Manager Properties, you will be prompted for the password of the account specified to run the plan.

### Store Purge

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 create a store purge task, select the store from the **Stores** folder in the **Archive Manager** console tree and then click **Create Store Task** from the **Actions** pane. Choose **Create Store Purge Task** on the **Create Store Task** screen, then enter a name for the purge task. Next, set up a schedule for automatically running the task (optional). Note: Regardless of schedule you can always run the task manually at any time. Finally, review the task settings, then click **Finish** to create the task and exit the **Create Store Purge Task** wizard. If you have not entered account information on the User Account tab of Archive Manager Properties, you will be prompted for the password of the account specified to run the plan.

See Store Expiration for more information.

### Archive Restore

Using slipstream™ technology, an **Archive Restore Task** restores archives from the selected store to an alternate location on local disk, RDX media or LTFS volume. This feature allows for keeping archival copies of data in native (original) format.

By configuring this task to restore the latest (most recent) restore point and scheduling it to run periodically, the restore location would always contain a copy of the latest backed up data in its original format. Consider, for instance, a restore task that restores a virtual machine file (VHD). The restore location would always contain the latest version of the virtual machine readily available for disaster recovery.

#### Creating an Archive Restore Task

To create an **Archive Restore Task**, select the store and choose its **Create Store Task** action. On the **Create Store Task** screen choose **Create Archive Restore Task** to begin the **Create Archive**

**Restore Task** wizard.

First choose the type of media to restore to: local disk file folder, RDX media or LTFS volume by clicking the appropriate icon at the top of the page. Note that LTFS currently does not support compression nor does it support access control lists (ACL). Files with the compression attribute set will be restored uncompressed and files with ACLs will be restored without security information.

- File Folder

Select a folder or click **Make New Folder** to create a new folder.

- RDX Media/LTFS Volume

When restoring to RDX or LTFS media, the cartridge/tape in the dock/drive at the time the task runs is the one that will be written to.

When restoring with the Archive Restore task, the software creates a path in the restore location as follows:
<server name>\<archive name>\<display name>\

where:
server name = name of computer containing the original files that were backed up

archive name = name of protection plan that backed up the files

display name = <drive label> (Drive <drive letter>) on '<computer name>'

The display name can be configured as a mount point to a stand-by virtual machine, for example, along with the **As a Mirror Image** restore option to facilitate disaster recovery or disaster recovery practice drills.

After you have chosen where to restore the archives, click **Next** to choose which archives to restore. Pick individual archives or choose to restore all archives. If **Restore all archives from the selected store** is chosen, new archives created from new protection plans running to the store will automatically be included.

After choosing which archives to restore, click **Next** to configure the restore points to restore.

Select **Only the most recent restore point** to always have the most recent data in the restore location.

If you choose **Restore restore points within a date range** you can choose a start date, end date, or both.

Select **Restore all restore Points** to restore every restore point in each of the selected archives.

Click **Next** to continue to the **Restore Options** page.

On the **Restore Options** page choose a restore file option from the text box drop-down. Then choose additional options as desired by checking the appropriate checkboxes. Not all additional options are available for all restore file options and will be enabled/disabled accordingly.

Restore options for an **Archive Restore Task** are as follows:

- **Only Missing Files and Folders**
- **All Files and Folders**
- **As a Mirror Image**

The restore location will mirror the backed up location. Files added to the restore location since the

backup was taken will be removed.

For improved restore performance, this option will merge in the changed portions of an existing file rather than restoring the complete file, unless the **Force an overwrite of existing files** modifier is checked.

- **Only Security for Files and Folders**

Restores security information for the backed up files that exist in the restore location. This option will have no effect if the destination does not support ACLs.
You can review the settings before finishing the **Create Archive Restore Task** wizard, then click **Finish** to complete the wizard.

## Store Actions

When a store is highlighted in the **Stores** folder of the console tree the actions available include:

- **Usage History**

  The **Usage History** action lists tasks that have been run against the store. Statistics such as *start and stop times* and *results* are shown for each task.

  Below the task list is a graph depicting the **Free Space Trend** for the store. The graph line begins at the left by showing the space available when the store was created. Then as the line moves to the right, it typically indicates a drop in free space available as protection plans are run to the store. Assuming only one large data set (one protection plan) is archived to the store several times, the line drops for the first run of the protection plan, indicating space used for the baseline run (typically a 2:1 data reduction). The line then flattens out to a gradual downward slope, indicating storage of only the changed, *deduplicated* data.

- **Store Tasks**

  This view shows all **Store Tasks** that have been created for the store. You can readily see last run status, schedule, and last run time for each task.

  Actions for the currently-selected task in the list are shown as *sub-actions* in the **Actions** pane. These actions allow you to edit the task settings and schedule, run the task manually, and delete the task.

  See Store Tasks for more information.

- **Task History**

  Selecting **Task History** brings up a list showing each time a store task was run. As with **Usage History**, start and stop times and results are shown for each store task run. Unlike **Usage History**, you can select a run time from the list and then click the **View Log** link at the bottom to view the run log.

- **Create Store Task**

  See Store Tasks for more information.

## Store Properties

From a store property page you can control data retention settings, sharing and bandwidth throttling.

- **Expiration**

  The default setting is to retain archived data indefinitely. This setting can be overridden from the **Expiration** tab of the store property page by changing the selected radio button from

**Infinite Retention** to **Number of days to keep restore points**. Choose the number of days you want to retain archived data and optionally change the **Minimum number of restore points to keep** value. The default setting is to keep ten restore points regardless of age. You can increase or decrease this setting, but the software will always keep at least one restore point.

The store expiration settings will have no effect until a **Create Store Expiration Task** is created and run, at which time the software scans the store for restore points older than the retention days setting. Restore points older than the retention days setting, excluding the minimum number to keep, are moved to the **Recycle Bin** of the store. A catalog for a restore point remains in the recycle bin until it is either restored back to the original archive via the **Restore** action or it is deleted by running the store purge task.

Note: Individual archives have their own properties page where you can override the store expiration settings. Refer to Archives for more information.

See Store Expiration and Store Purge for more information.

- **Sharing**

  Protection plans for remote computers archive the files to a store through a shared folder. You can edit the share settings and create additional shares from the **Sharing** tab on the store property page.

  If there is more than one share for the store, you can select which one a remote computer protection plan uses when you are creating the plan on the **Select a Destination** page of the protection plan wizard. Existing remote computer protection plans can be changed to use a different share by clicking the **Plan Settings** action and then clicking the **Change** button of the **Settings** tab.

- **Bandwidth**

  You can control bandwidth utilization from the **Bandwidth** tab on the store property page.

  To enable and configure bandwidth throttling for a remote computer, click **Add**, then enter the computer name or IP address of the remote computer. In the **Bandwidth Throttling** window, check **Enable bandwidth throttling**, then adjust the speed, date and time settings.

  Click **Apply** to save your settings , then click **Add** to add another computer, or just click **OK** to save your settings and close the store property page.

## Archives

When a protection plan runs for the first time, an archive is created in the store that is targeted by the plan. This archive appears in the **Archive Manager** console tree as a sub-folder of the **Archives** folder of the store, and it is given the same name as the protection plan. A restore point is also created for exploring and restoring this point in time. Each subsequent run of the plan adds another restore point to the archive.

When an archive is protected by a Store Vaulting Task, the archive will also appear in the vault under the **All Vaults** folder and the tape device or cloud account folder where the vault resides. Refer to Restoring Data from a Vault for information about restoring from an archive in a vault.

Actions available for an archive in a store include:

- **Restore**

  To view restore points, select the archive and then click its **Restore** action. Days containing restore points are highlighted in bold font in the calendar. Select the restore point you want to restore, and the **Restore** button at the bottom right of the screen will become active. Click **Restore** and a restore dialog box appears. Refer to Restoring Your Data for more information.

If the restore point was from a **Files and Folders** protection plan, the **Explore** button will also become active, and you can explore and restore files as described in Explore a Plan's Archive.

- **Properties**

  From the **Properties** action, you can define expiration settings for the archive that override the expiration settings of the parent store. See the Store Expiration section in the Store Properties topic for information about expiring data from a store.

### Store Generations

Starting with version 9, the store architecture provides significant performance improvements for archiving and store task execution. Storage efficiency is also improved. The software supports both types of stores but the performance improvement will only be realized when using the new architecture. Older stores are not compatible with the new store architecture. This means that store copy tasks won't be able to copy from one generation to the other. Fortunately, conversion of older stores to the new architecture is a simple process.

To convert a store to the new version 9 architecture open its **Properties** page and click the **Improve storage performance** button. Note: The Improve storage performance button will only be available if the store has not yet been converted. Clicking the button will open the **Store Conversion Wizard**. To convert the store simply click the **Convert now** button.

For more information regarding store copy tasks and store generations see Store Copy.

## Store Groups

A store group is a logical collection of Stores that facilitates creating multiple copies of protected data on different storage devices. Store groups enable automatic fail-over between online media, dynamic rotation of removable media, and round-robin selection of fixed drive media.

- Automatic fail-over between online media

The first available store will be used in the priority order specified. With this option if the primary store fills up or fails (goes offline), a secondary store in the group is automatically selected allowing backup jobs to run uninterrupted.

- Dynamic rotation of removable media

The most recently used and available store in the group is used until the store is either offline, or unavailable for normal use. With this option, media can be easily rotated offsite and back onsite without any interaction with the software. Stores are selected automatically by the software based on which stores are currently available.

- Round-robin selection of fixed drive media

The least recently used and available store in the group is always used. Stores are selected in circular order creating copies of data on multiple stores. With this option copies of data are maintained independently by continuously rotating to different stores, eliminating any single point of secondary storage failure.

After a store group is created, it appears in the All Store Groups folder. Creating and maintaining the settings for a store group includes specifying which stores are members of the group and how the software will select available member stores when the group is used by Protection Plans and Store Copy Tasks.

See the following topics for more information about store groups:

- Adding Store Groups
- Store Group Properties

## Adding Store Groups

A **Store Group** is a logical grouping of stores. Store groups are used to configure a Protection Plan or Store Copy Task to use media in a rotation scheme. Using a store group with removable media is a good practice for getting data off premise, providing an offsite copy in case of a site wide disaster.

To create a new store group, right-click either the **Storage** folder or **All Store Groups** folder and then select the **Add a Store Group** action. The **Add Store Group** wizard starts by prompting you to name the store group. Choose a meaningful store group name. For example, if you are backing up data to a new group of stores in media rotation each quarter of the year, your first store group could be called "Q1 Backups Group".

After you have named the group, click **Next** and select which stores will be members of the group. Check each store you would like to have in the group. You can change the priority of the stores within the group using the up or down arrows to the right of the list. Store priority is one method of selecting a store. See "Store selection preference" below.

When you have finished choosing the stores you would like to have as members of the group, click **Next** and choose a "*Store selection preference*".

When a Protection Plan or Store Copy Task is configured to target a store group, the stores in the group are analyzed and a determination is made to use an available store based on the store selection preference setting for the group.

If you choose "*Selects the first available store in the order specified*", the first available store will be used in priority order specified in the list. A store is considered unavailable if it is offline, read-only or has less than the minimum free space required. Choose this setting for automatic fail-over between online media.

If you choose "*Selects the most recently used available store*", the most recently used and available store in the group will be used for subsequent plan or copy task runs until the store is either offline, read-only or has less than the minimum free space required. Choose this setting for dynamic rotation of removable media.

If you choose "*Selects the least recently used available store*", the least recently used and available store in the group will be used for the next plan or copy task run. Stores are selected in circular order creating copies of data on multiple stores. Choose this setting for round-robin selection of fixed drive media.

After you have selected the stores to include in the group and a selection preference, click **Next**. You can review the store group settings before finishing the **Add Store Group** wizard.

## Store Group Properties

From a store group property page, you can add or remove stores as members, order the stores within the group to change their priority, and change the store selection preference setting.

All stores are listed in the store group property page. To include a store in the group, check the box next to the store you would like to add. To remove a store from the group, uncheck the box.

The order of checked stores from top to bottom in the list is important to the store selection preference setting. To order the stores in the box use the up and down arrows to switch the position of the selected store.

When a Protection Plan or Store Copy Task is configured to target a store group, the stores in the group are analyzed and a determination is made to use an available store based on the store selection preference setting for the group.

If you choose "*Selects the first available store in the order specified*", the first available store will be used in priority order specified in the list. A store is considered unavailable if it is offline, read-only

or has less than the minimum free space required. Choose this setting for automatic fail-over between online media.

If you choose "*Selects the most recently used available store*", the most recently used and available store in the group will be used for subsequent plan or copy task runs until the store is either offline, read-only or has less than the minimum free space required. Choose this setting for dynamic rotation of removable media.

If you choose "*Selects the least recently used available store*", the least recently used and available store in the group will be used for the next plan or copy task run. Stores are selected in circular order creating copies of data on multiple stores. Choose this setting for round-robin selection of fixed drive media.

See Adding Store Groups for more information.

## Vaults

A vault is a storage location on cloud or tape storage targeted by a store vaulting task and is created automatically when the store vaulting task is created. After a vault is created, it will appear in the **All Cloud Vaults** or **All Tape Vaults** folder. Underneath the new vault will be an empty **Archives** folder for holding archive restore points grouped by protection plan name.

You can explore and restore vaulted data, although before you can restore data the vaulted point in time must be transferred from either cloud or tape to a local (cache) store.

See Vaulting for more information.

### Vaulting

Vaults and stores are both created and used by the software to store data. A store is a storage location on disk targeted by local and remote protection plans. A vault is a storage location on cloud or tape storage targeted by store vaulting tasks.

Whereas a store is a container for data storage designed for random access devices, a vault is a container for longer-term data storage, designed for cloud and tape. The vault design allows for fast streaming of data to and from the cloud/tape device. It does not, however, allow for direct restoring of files.

Instead of archiving data directly to a vault, data to be archived is first deduplicated and written to a store using a Protection Plan. Then a Store Vaulting Task "copies" the data from the store to the vault. A cache drive is required for staging the data as it is being vaulted and for preparing data to be restored from a vault.

Vaults are created automatically when a store vaulting task is created. The default vault name is the store name plus " Vault" and the location for staging the data is at the root of the cache drive specified in the Configure Vaulting wizard.

See the following for more information about vaulting:

- Configure Vaulting
- Store Vaulting Task
- Restoring Vaulted Data

#### Configure Vaulting

Before you can create a Store Vaulting Task or run the Archive Manager Import Settings action, you need to configure vaulting. Vaulting only needs to be configured one time.

Select the **Storage** folder in the **Archive Manager** console tree and then choose its **Configure Vaulting** action to launch the **Configure Vaulting Properties** wizard. The settings you specify here apply to both cloud and tape vaulting. The wizard will guide you in configuring the following settings:

- **Cache Location**

  Vaulting requires a disk drive for staging data as it is being vaulted and for preparing to restore data from a vault. Click the "*Select Cache Drive Location*" link, then select a drive from the list provided, then click **Next** to proceed to the **Encryption** page.

- **Encryption**

  The software uses AES-256 strong encryption to safeguard your data. A private encryption key is automatically generated when you initialize the system using the passphrase provided. Enter a passphrase, then initialize by pressing the Initialize button. The status should change from red "*not initialized*" to green "*initialized*." Click **Next** to proceed to the **Owner ID** page.

  Note: If you later change the passphrase, vaulted data encrypted with the original passphrase will not be accessible for restoring until you change the passphrase back to the original.

  Note: Encryption is required when vaulting to cloud storage but is optional when vaulting to tape. This allows you to take advantage of hardware encryption, if available, without also requiring software encryption.

- **Owner ID**

  Enter an Owner ID to be used for identifying the owner of the media, and then click Initialize. The status should change from red "*not initialized*" to green "*initialized*." Click **Next** to go to the **Finish** page. Review the summary, revise as necessary using the **Back** buttons, then click **Finish** to close the wizard.

## Store Vaulting

Store vaulting tasks copy selected archives to 'vaults' for longer-term storage. Vaults can be in the cloud or on tape, and they are created automatically when the store vaulting task is created.

Prior to creating a Store Vaulting Task vaulting needs to be configured. See Configure Vaulting.

If you haven't already done so, you can set up a cloud account for vaulting to cloud and you can add tape volume sets during the creation of a **Store Vaulting Task**.

### Creating a Store Vaulting Task

To create a **Store Vaulting Task**, select the store to vault and choose its **Create Store Task** action. On the **Create Store Task** screen choose "*Create Store Vaulting Task*" to begin the **Create Store Vaulting Task** wizard. Select either **Cloud Account** or **Tape Device**. If you are vaulting to cloud, you can sign up for a cloud account and add it to the Archive Manager system from here. If vaulting to tape, you can add a tape device here.

Note: If you know there is a tape library attached to the system but it is not showing up, check the device to make sure there is not a tape loaded into the drive.

Once you have chosen a cloud account or tape device for your vault, choose to vault all archives from the store or select individual archives to vault.

On the **Configure Restore Points to Copy** screen choose to copy all restore points, a range of restore points, or only the most recent restore point.

On the **Copy Task Name** screen, choose a name for the task and a name for the vault, then click

**Next** to continue to the **Schedule Copy Task** screen.

You can schedule this task to run automatically or click **Next** to accept the **No Schedule** default. The task runs as the currently-logged-on user unless you change the **Run as** account information on the **Task** tab of the task scheduler.

Review the store copy task settings shown on the **Completing the Create Store Vaulting Task** wizard screen. If you need to make changes, navigate back via the **Back** button. When you are satisfied with the settings, click the **Finish** button. If you have not entered account information on the User Account tab of Archive Manager Properties, you will be prompted for the password of the account specified to run the plan. After you enter the password, the task is created, the **Create Store Vaulting Task** wizard closes, and the new task appears in the store tasks of the store where the task was created. The new vault will appear either in the **All Cloud Vaults** folder or the **All Tape Vaults** folder, depending on whether the vaulting task is for cloud or tape.

### Cloud Storage

Vaults and stores are both created and used by the software to store data. A store is a storage location targeted by local and remote protection plans. A vault is a storage location targeted by store vaulting tasks.

Whereas a store is a container for data storage designed for random access devices, a vault is a container for longer-term data storage, designed for tape and cloud. The vault design allows for fast streaming of data to and from the cloud/tape device. It does not, however, allow for direct restoring of files.

Instead of archiving data directly to a vault, data to be archived is first deduplicated and written to a store using a Protection Plan. Then a Store Vaulting Task "copies" the data from the store to the vault. A cache drive is required for staging the data as it is being vaulted and for preparing data to be restored from a vault.

Vaults are created automatically when a store vaulting task is created. The default vault name is the store name plus " Vault" and the location for staging the data is at the root of the cache drive specified in the Configure Vaulting wizard.

See the following for more information about vaulting:

- Configure Vaulting
- Store Vaulting Task
- Restoring Vaulted Data

### Cloud Accounts

Before you can store data to the cloud you need to create a Cloud Account. To create a cloud account, right-click the Cloud Storage folder and select the **Add Cloud Account** action to open the **Cloud Accounts** screen. Note: You can also create a cloud account as part of creating a Store Vaulting Task. Click the link at the bottom of the **Cloud Accounts** screen to open the Amazon "Sign In or Create an AWS Account" web page. Enter your email address and select "I am a new user" to sign up for an account. If you've already signed up but need to get a fresh activation key, choose "I am a returning user and my password is:" In either case, enter a password to get your activation key. This key will be valid for 1 hour. Highlight and copy the activation key to your clipboard.

Return to the **Cloud Accounts** screen and click **Add** to register your account with the Archive Manager server. Paste your activation key into the "*Activation key*" text box. Enter a descriptive name for your account in the "*Display name*" text box and choose a default data center. The default data center is where export files will be kept if this cloud account is selected when creating an Export Settings Task. You can override the default data center when creating Store Vaulting Tasks. Even though your data is encrypted by the software, you can still select "Use SSL" if you want to transfer your data over a Secure Sockets Layer. Now click the "*Test Connection*" button to make sure everything is working. You will either get a "*Connection failed*" message or a "*Connection success*" message. Assuming it was successful, click **OK** to add the account and **Close** to return to the **Archive Manager**. Your new cloud account should appear in the **Cloud Storage** folder and will be available as a target for Export Settings and Store Vaulting tasks.

Properties of a cloud account show the account's details and its usage statistics.

### Tape Storage

Vaults and stores are both created and used by the software to store data. A store is a storage location on disk targeted by local and remote protection plans. A vault is a storage location on cloud or tape storage targeted by store vaulting tasks.

Whereas a store is a container for data storage designed for random access devices, a vault is a container for longer-term data storage, designed for cloud and tape. The vault design allows for fast streaming of data to and from the cloud/tape device. It does not, however, allow for direct restoring of files.

Instead of archiving data directly to a vault, data to be archived is first deduplicated and written to a store using a **Protection Plan**. Then a **Store Vaulting Task** "copies" the data from the store to the vault. A cache drive is required for staging the data as it is being vaulted and for preparing data to be restored from a vault.

Vaults are created automatically when a store vaulting task is created. The default vault name is the store name plus " Vault" and the location for staging the data is at the root of the cache drive specified in the **Configure Vaulting** wizard.

See the following for more information about vaulting:

- Configure Vaulting
- Store Vaulting Task
- Restoring Vaulted Data

### Volume Sets

A Volume is another term for a tape. A Volume Set is a logical grouping of Volumes, or tapes. A volume set is the destination for store vaulting tasks that target tape. When creating a vaulting task for tape you must choose a volume set as its destination. A volume set can be created by right-clicking the **All Volume Sets** folder and clicking its **Add Volume Set** action or by clicking the **Add volume set** button when creating a tape vaulting task, or it can be created when labeling a tape in a standalone drive. Blank unassigned tapes (volumes) are automatically added to a volume set as needed and are drawn from configured tape libraries. After a volume set is created, it appears in the **All Volume Sets** folder of the **Tape Storage** node.

Multiple tape vaulting tasks can write to the same volume set, and a tape vault can span more than one volume in a volume set.

A volume will be appended to until it becomes full or is unavailable, at which time the next available volume in the volume set will be used. If there are no more volumes in the volume set the software will automatically assign a blank, unassigned volume from a configured library, if available. If no volumes are available the vaulting task will fail with an indication that no usable media was available.

## Tape Rotation

A tape rotation scheme can be configured by having two tape vaulting tasks, each writing to a different volume set. One task, for instance, runs on Mondays, Wednesdays and Fridays to one volume set and the other task runs on Tuesdays, Thursdays and Saturdays to the other volume set. A particular tape in the volume set will be written to every other day until it becomes full, at which time it can be removed from the library. If a tape that was just written to is removed, the next run of the vaulting task will use the next available tape in the volume set. If there are no available tapes in the volume set a new blank unassigned tape will automatically be assigned to the volume set. If no tapes are available the vaulting task will fail with an error indicating that no media is available.

If using a standalone tape drive, setting the **Eject** option (available from the **Advanced Settings** of a tape vaulting task) to *True* will cause the tape to be ejected upon completion of the task. Each day one tape can be taken off-site and one from the other volume set inserted into the drive.

If using a tape library, tapes in one magazine can be assigned to one volume set and tapes in another magazine can be assigned to the other volume set. The magazines can be rotated daily with one magazine taken off-site and the other inserted into the library.

## Removing volume sets

A volume set cannot be removed until all vaults in the set have been removed. To remove a vault you must first delete the associated vaulting task. Once a volume set is removed, all of the tapes in that volume set are marked 'erase pending'. Tapes in the erase pending state can be erased by using the **Erase** action from the **Volumes** folder view.

## Tape Device

testBefore data can be stored to tape a tape device must be added to the software. Assuming the device has been attached to the computer and necessary drivers loaded, select the **Tape Storage** folder and choose its **Configure Tape Devices** action to launch the Configure Tape Devices wizard. After completing the wizard the tape devices will appear in the Tape Storage folder as a <device name> sub-folder.

The tape device folder will contain one or more tape drives, and a Volumes folder that shows each volume (tape) and its status. Standalone tape drives will have the same name for the tape device folder and the tape drive sub-folder.

Barcodes are required for tapes in libraries and are optional but recommended for standalone drives in case a library is added at some point in the future. Tapes in libraries are automatically labeled by the software using the barcode label of the tape. Tapes in standalone drives should be labeled to match the barcode using the barcode format of 6 alpha-numeric characters plus the LTO generation of the tape, for example 123456L6 or DEV001L5. To label a tape click its **Label and Assign** action from the standalone device's **Volumes** folder. See Label and Assign for more information.

Actions for a tape device include:

- **Synchronize Library Inventory** - This action launches a library inventory command to synchronize the software with the current state of the library. Because the media will be mounted and read, this action can take several minutes.
- **Device Properties** - This action opens the Windows properties for the device.

## Tape Drives

A tape library will contain one or more tape drives that are automatically added to the software when the library is added. The drives will be shown grouped with their respective library and each has its own **Device Properties** action for displaying its properties.

## Tape Volumes

### Tape library

Volumes (tapes) that are in a library are automatically labeled using the volume's barcode when the software first writes to them.

Each volume and its status is shown in the library's **Volumes** folder. To update the status of all volumes, run the autoloader's **Synchronize Library Inventory** action. Actions for an individual volume or multi-selected volumes include:

- **Assign** - This action allows you to assign media to a particular volume set. Once the media has been written to you cannot change its assignment.
- **Unassign** - This action allows you to unassign media from a volume set, making it available for assignment to another volume set. Once the media has been written to you cannot change its assignment.
- **Erase** - This action will erase the media. You cannot erase media that is being used by the system.
- **Identify** - This action identifies the media by reading its on-media-label.

### Standalone tape drives

Volumes for standalone tape drives must be labeled manually using the volume's **Label and Assign** action. See Label and Assign for more information.

The **Volumes** folder shows the status of the currently-loaded volume. To update the status of the volume, run the drive's **Synchronize Library Inventory** action. Actions for an individual volume include:

- **Label and Assign** - This action allows you to label and assign media to a particular volume set.

Once the media has been written to you cannot change its assignment.
- **Unassign** - This action allows you to unassign media from a volume set, making it available for assignment to another volume set. Once the media has been written to you cannot change its assignment.
- **Erase** - This action will erase the media. You cannot erase media that is being used by the system.
- **Identify** - This action identifies the media by reading its header information.

### Label and Assign

Barcodes are required for tapes in libraries and are optional but recommended for standalone drives in case a library is added at some point in the future. Tapes in libraries are automatically labeled by the software using the barcode label of the tape. Tapes in standalone drives should be labeled to match the barcode using the barcode format of 6 alpha-numeric characters plus the LTO generation of the tape, for example 123456L6 or DEV001L5. To label a tape click its **Label and Assign** action from the standalone device's **Volumes** folder.

The **Label and Assign** dialog lets you label a tape and assign it to a **Volume Set**. Optionally, you can create a new volume set by clicking the **Add Volume Set** button. Note: Volume sets can also be created from the **Add Volume Set** action of the **All Volume Sets** folder or during creation of a Store Vaulting task that is targeting tape (vs. cloud). See Volume Sets for more information.

## Exporting History

You can export store usage, and store task and protection plan histories into the Excel spreadsheet (.xls) format. After choosing an export action, you will be presented with a very powerful tool for organizing the history data prior to exporting.

The **Export Plan History** action is available from several places in the **Archive Manager** console tree:

- store - exports all plan histories that run to the currently selected store
- **Local Plans** folder - exports all local plan histories
- remote computers group folder - exports all plan histories for all computers in the currently selected group
- remote computer - exports all plan histories for the currently selected computer

In addition to exporting plan histories, when you select a store in the console tree, you can export task histories using the **Export Task History** action, and you can export the store usage history with the **Export Usage History** action.

### Organizing the exported data

After clicking an export history action, the data is displayed using some default format settings. You can customize the format in several ways. A few are described below.

To hide a column, right-click anywhere in that column and choose **Hide Column**. To show a hidden column, right-click anywhere in any column and select **Column Chooser**, then double-click the column you want to show.

Columns can be re-sized by dragging the column separator left or right, or moved by dragging the column header to another location.

Results can be filtered by clicking the funnel icon of a column and selecting from the list of available filters.

Results can be grouped by dragging a column heading to the bar just above the column headings. For example, to group data by computer name you would drag the **Computer** column heading to

the bar just above the column headings row. You can create subgroups by dragging another column heading up above the row of column headings. To restore the view, click the 'X' in the heading or just drag the heading back down.

To export the formatted data to an Excel spreadsheet, click the **Export** button in the upper-right corner of the history page, specify a location and filename, then click **Save**.

## Best Practices

Click on the links below for suggestions that will help you obtain the best experience from this software.

- Getting the most from this software
- User Account
- Protecting Your Archive Manager System

### Getting the most from this software

#### Introduction

This software contains an advanced technology called data **deduplication** or **capacity optimization**. This technology reduces standard business data by as much as a twentieth of the original size of the data during backup to disk. It achieves this level of optimization by removing all redundant data from the files being archived and storing only the unique data over time while allowing virtually instant point-in-time restore of the data. Additionally, the software enhances data reduction by performing LZ data compression.

#### Dynamic files and fixed files

Files on a computer may be classified generally as either fixed or dynamic. Fixed files are files whose content is created and never, or rarely, changes. Files such as video, music, images (pictures), and the like are examples of fixed content files. Files such as word processing documents, spreadsheets, presentations, projects, and the like are examples of dynamic content files because they may be opened and edited.

As noted above, this software reduces the size of your backups dramatically. This dramatic reduction occurs because during each plan run, the software finds the changed bytes and metadata of each file and stores only those changes to the disk. Therefore, by creating a protection plan that targets the largest number of dynamic files that are most likely to change over time, you will enable the software to achieve the greatest data reduction.

#### Backup scenarios

This software offers you the flexibility to create backup processes that fit your needs.

You can choose exactly which folders to back up, and you can run protection plans as often as needed, even more than once per day.

The software allows you to designate specific storage for specific protection plans.

When determining how you want to store your data by using this software, it may help to think about what files you might need to recover most often, or which files are most important, and schedule the protection plans that protect those files to run most often.

### User Account

Windows denies or grants access to its resources by means of user accounts. When running this

software in a domain, create a domain user account solely for use by this software. Add the account to the Domain Admins and Backup Operators Group, thereby allowing the account access to required resources. Specify this account from the Create Protection Plan (or store task) wizard schedule page, or in the Run as field of the scheduled task of each protection plan.

By specifying backup user account credentials on the **User Account** tab of the **Archive Manager** properties page you avoid being prompted for credentials each time you create or make a change to a protection plan or store task.

If the **Archive Manager** server or the remote computer is in a workgroup, not a domain, then a matching user account and password must be created for the **Archive Manager** server and each remote computer. This user account must be a member of the local **Administrators** group. You will also need to add the following registry setting to each remote computer if it is not already there. Windows User Account Control (UAC) treats local administrator accounts as standard accounts when accessing the computer using a remote administrative connection. To disable this restriction add a DWORD value to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System called LocalAccountTokenFilterPolicy and set its data to 1. Refer to http://support.microsoft.com/kb/951016 for more information. Log on to the **Archive Manager** server with this account. When creating remote computer protection plans, specify the account for the remote computer in the **Run as** field of the scheduled task. This configuration will allow credentials to pass through to the other computer for access to necessary resources.

Do not use administrator accounts with blank passwords.

## Protecting Your Archive Manager System

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.

### Usage Scenario

Let's assume that you have been periodically running an Export Settings Task to archive your settings to a folder or cloud storage (recommended). Then one day your **Archive Manager** computer dies. No problem; you can quickly and easily restore your system and data as follows:

Install the **Archive Manager** software and license keys on a new computer. If you have the media containing your stores, attach it to the new computer. If you were vaulting to cloud then add your Cloud Account to the **Archive Manager** system.

Run the **Archive Manager Import Settings** action to start the import settings wizard and choose an export file to restore. When you click Finish and enter credentials the task will run and the settings will be imported to your new system. Stores attached to the new computer will be discovered and reconnected. Vaults will be shown in the **Archive Manager** but you will need to recover the vault information for each vault by running its **Restore Vault Information** action. At this point the vaults will contain restore points that you can restore data from. See Restoring Data from a Vault for more information.

### Creating an 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 the task. You can also run the task manually from the Windows Task Scheduler. Choose Modify Schedule and then click "*New*" on the Schedule tab to create a new task.

The settings are exported into a compressed file that can be saved to either a folder location or, if a

cloud account has been set up, to a Cloud Account. Note: When saving to a cloud account, the export file will be saved to the default data center specified in the cloud account's **Properties** page. 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."

### Importing Settings

Prior to importing settings, you must install the software and activate your license keys. Add your Cloud Accounts if applicable. Add your tape libraries and removable disks to the computer if applicable. If you have backups of your stores, attach them to the new computer.

To import saved configuration settings, select the **Archive Manager** folder and then choose the **Import Settings** action to launch the Archive Manager Import Settings wizard. You will be prompted for a user name and password of the Scheduled Task's "Run as" user account for running protection plans. All imported tasks will be saved with this "Run as" user account.

After importing the Archive Manager settings, close and reopen the Archive Manager user interface to refresh the Archive Manager system.

## Troubleshooting

To aid in troubleshooting, this software records its activity in log files and writes significant events to the Windows Application Event Log. See the Log Files topic for more information.

See Remote Computer Connection Issues for help with adding protection plans to remote computers. If your Archive Manager server is in a workgroup you should start with this topic: Use Administrator Level Account and then continue with the Remote Computer Connection Issues topic.

### Log Files

The software logs information that is useful for troubleshooting and historical purposes. Two types of logs are used by this software, *internal component logs* and *protection plan logs*.

Note: By default only summary information is written to a protection plan log file. You can change the configuration **LogLevel** setting for a protection plan to record more or less information.

#### Internal component Logs

These logs are specific to internal components of the software and are located in the installation directory as *<internal component name>.log*.

Two of these logs, *aiq.log* and *aiqRemote.log*, can be viewed from within the **Archive Manager**. The aiq log contains information pertaining to local plan execution. The aiqRemote log contains information pertaining to remote computer plan execution. To view the aiq log, select **Local Plans**, then choose its **View Log** action. To view the aiqRemote log, select **Remote Computers**, then choose its **View Log** action.

#### Plan logs

Each time a plan is run, its results are appended to a log file: *<installation directory>\Logs\<plan name>.log*. The most recent logging information can be found at the end of the file. By default only summary information is logged, but you can change the configuration **LogLevel** setting to record more or less information.

If a plan fails or completes with warnings, you should check its log file for details. For this reason, **LogLevel**=**none** is not recommended.

To view a protection plan log file, select the **History** action, then click the **View Log** link in the **Result Details** section.

The following statistics are written to the log file for each run of a folder and files protection plan:

- "Total transfer time" - the amount of time it took to write the updated archive information to the store
- "Directories processed" - the total number of directories processed by the protection plan
- "Protected items" - the total number and size (in bytes) of files processed by the current run of the protection plan
- "Protected data" - the total amount of data protected by the plan
- "New files" - the number of new files since the last run of the protection plan
- "Changed files" - the number of files that changed since the last run of the protection plan
- "New and changed" - the amount (and percentage) of protected data that changed since the last run of the protection plan
- "Factored" - the amount of data that was reduced in size by Adaptive Content Factoring
- "Total stored" - the amount of data written to the Store for this run of the protection plan
- "Data reduction" - the ratio of the total amount of new and changed data ("New and changed") to the total amount of data written to the Store ("Total stored") by the current run of the protection plan
- "CCF ratio" - the ratio of all the data protected by the plan ("Protected data") to the total amount for data written to the Store ("Total stored") for this run of the protection plan
- "Doubling time" - an estimated number of protection plan runs possible before the archived data becomes twice as large as the original dataset
- "Common content" - the amount (and percentage) of common data subject to data deduplication
- "Elapsed time" - the amount of time for the entire archive operation, including the total transfer time

## Remote Computer Connection Issues

This topic addresses the following scenario:

In **Archive Manager**, you add a remote computer that is a member of the domain. You are logged on to the **Archive Manager** server with an account that has permission to connect to the remote computer from the network. After the remote computer is added, you click it and wait for communication to be established. Eventually, a yellow triangle appears in the remote computer icon. An error briefly appears at the bottom of the **Archive Manager** stating that the network path is not found, or the RPC Server is unavailable. (Note: To view the error again, right-click the computer and refresh.) You do not receive an option in the **Actions** pane to create a protection plan.

The most likely causes are:

- Remote Registry service is not running. The Remote Registry service startup type should be set to **Automatic** and the service should be started. This service is needed to remotely administer the system.
- Windows firewall may be preventing communication with the **Archive Manager** server.
- Other services needed for remote administration of the remote computer may not be running or have proper permissions.

To verify that the Remote Registry service startup type is set to **Automatic** and the service is running, follow these steps:

1. Click **Start** (or the **Start** icon), right-click **My Computer** (or **Computer**), and select **Manage**.

2. When **Computer Management** opens, select and expand the **Services** section.

3. Scroll to the **Remote Registry** service and observe its status (should be **Started**) and **Startup Type** (should be **Automatic**). If necessary, double-click the **Remote Registry** service and set startup type to **Automatic**. Click the **Start** button.

4. Try to establish communication with the remote computer from **Archive Manager** again. Right-click the remote computer and select **Refresh**. If the **Create Protection Plan** action appears in the **Actions** pane, start the **Create Protection Plan** wizard. Otherwise, continue below.

Verify that the firewall is not preventing remote administration of the computer by allowing exceptions.

1. On the remote computer, click **Start**, **Control Panel**.

2. Add the following exceptions to the firewall. Note: Some of these may not be listed for your firewall because this list was compiled from several different Windows operating systems. If the exception is listed on your computer, then add it as an exception to the firewall. If it is not listed, just continue to the next exception in the list below.

   - File and Printer Sharing
   - Remote Administration
   - Windows Management Instrumentation (WMI)
   - Core Networking

   Note: These may be set at the group policy level. For example, in Group Policy Management select a group policy, right-click and select **Edit**. Navigate to **Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile**. Enable **Allow remote administration exception** for **localsubnet**. Do the same for **Allow file and printer sharing exception**. After the policy updates, close and open **Archive Manager** and attempt to connect again. You can force group policy update with the `gpupdate` command on both the domain controller and the remote computer. You may manually set the exceptions from the remote computer, as well. File and Printer Sharing is available on the exceptions tab of the firewall settings, unless disabled in group policy. At a command prompt on the remote computer, an administrator may set the Remote Administration exception with: `Netsh firewall set service type=remoteadmin mode=enable scope=all profile=all`.

3. Try to establish communication with the remote computer from **Archive Manager** again. Right-click the remote computer and select **Refresh**. If the **Create Protection Plan** action does not appear in the **Actions** pane, continue with the next step.

4. **Archive Manager** uses the credentials of the currently-logged-on account to connect to the remote computer. So, make sure you are logged on with a domain administrator account, and that the remote computer is in the domain.

5. If still having trouble, you may need to check local group policy settings on the remote computer for **log on locally**, **log on as batch job**, and **log on as a service**.

6. On the remote computer, verify the following services are started: Remote Procedure Call, Remote registry, and COM. Click **Start**, **Run**, type `services.msc` and click **OK**. Search for the services and verify they are started.

7. Test the WMI remote connection with WMI Tester. On the **Archive Manager** server, click **Start**, **Run**, then type `WBEMTEST` and try to connect to the remote computer by UNC path to the namespace, e.g. \\<*computer name*>\root\cimv2 and click **Connect**. If you receive an error message, check that DCOM is running on the remote computer and check DCOM permissions with DCOMCNFG. Go to **Start**/**Run** and type `dcomcnfg` and click **OK**. In dcomcnfg, navigate to **My Computer**/**Properties**/**Default Properties** and verify DCOM is enabled with **Connect** and

**Identify** set (any changes require a reboot). Go to **COM Security** tab and verify **Launch** and **Activation** permissions. The account logged in to the **Archive Manager** server must have **Remote Launch** and **Remote Activation** permissions. Add the account and check the permissions, if needed.

## Trademarks and Notices



## Glossary

### Alerts
This software uses alerts for update/upgrade notification and certain other conditions that require attention. When an Alert occurs the software will create a popup from the Windows notification area (also known as "system tray"). The popup will be visible for 7 seconds. Additionally, the Alerts tab of the Archive Manager folder will contain the Alert. The Alerts tab will change from "Alerts (0)" to "Alerts (1)". If more than one Alert is active the display of the number of Alerts will change from 1 to 2 and so on.

### Archive
An archive is the result of running a protection plan, and contains protected data as the data exists at each protection plan runtime. Each time a protection plan executes, a new restore point is added to the archive associated with the plan. When a protection plan runs for the first time, an archive is created in the store that is targeted by the plan. This archive appears in the Archive Manager console tree as a sub-folder of the Archives folder of the store, and it is given the same name as the protection plan. A restore point is also created for exploring and restoring the archive at this point in time. Each subsequent run of the plan adds another restore point to the archive.

### Archive Manager
The user interface is called the Archive Manager. It is the "control console" for the software and runs on the computer where the software is installed.

### Archive Manager Service
This is a Windows software service that provides the core functionality of the product.

### Archive Restore Task
An Archive Restore Task restores archives from the selected store to an alternate location on local disk, RDX media or LTFS volume. This feature allows for keeping archival copies of data in native (original) format.

### ArchiveIQ
ArchiveIQ is a trademarked term for the deduplication technology used by the software.

### BMR
Bare Metal Restore (BMR) is a term used to describe restoring a computer operating system and its data volumes in their entirety. It allows for restoring a backed up system to the same or similarly configured piece of hardware. The Computer System protection plan type provides BMR capability.

### Checkup Report
The Checkup Report is a convenient way to monitor the status of your system by generating a report of the store and protection plan status for the past 24 hours. Any plan or store task errors are highlighted in red, and warnings are highlighted in yellow for quick identification of problems.

### Cloud Gateway Service
This is a Windows software service that provides the bridge between this software and cloud storage.

### Cloud Storage
The term Cloud Storage is used by this software to describe networked online storage.

### Cloud Vaulting
Cloud vaulting is the term used to describe storing backed up data to the cloud.

### Copy Task
Short for Store Copy Task, a store copy task copies selected archives from one store to another.

### Expire Task
A store can be configured to expire older restore points based on daily, weekly, monthly, quarterly and yearly age. Expire tasks evaluate a store's current restore points and moves expired catalogs to the store's recycle bin.

### Local Plans
Local Plans are protection plans that protect data stored on the server where the software in installed.

### Log File
The software writes output to files called log files.

### LTFS
LTO generation 5 and newer tapes can be formatted with the Linear Tape File System (LTFS), available from third-party vendors. LTFS allows an LTO tape to be used like a hard disk.

### Plan
Plan is an abbreviation of the term Protection Plan.

### Point-in-Time Explorer
The Point-in-Time Explorer is a Windows Explorer-like interface for viewing a backed up set of data at a specific point in time. Data can be restored back to disk through copy and paste functionality or a Point-in-Time Restore action.

### Protection Plan
A Protection Plan is the set of parameters used by the ArchiveIQ engine to protect data on a given computer. It defines which data is to be archived, which store to save it in, and when it should run. Each remote computer requires at least one protection plan. There are four protection plan types available: Files and Folders, Computer System, Exchange Data and SQL Databases. Protection plans initiate snapshots of computer systems and generate archives of data in targeted stores.

### Purge Task
A Purge Task is a store task that recovers disk space from expired or deleted restore points.

### Quarantined Items
If the software encounters a problem file in the stored content it will move the item to the store's Quarantined Items folder, and update plan indexes to reflect the quarantine. The store is then prepared to auto-heal during a subsequent protection plan execution. The software verifies a store's contents for corrupt and missing files through Store Verify Tasks and automatically during plan runtime, or as part of other operations like Store Copy and Store Purge tasks. When an item is quarantined it is marked with a red flag icon. The software will rewrite the data into the store if it comes across the item again during a Protection Plan run. If it successfully "repairs" the item, the

red flag on the item in the Quarantined Items folder is changed to a green flag, at which time it can safely be deleted from the folder.

### Recover
This term is used to describe the act of recovering a computer system.

### Recovery Point
A Recovery Point is the result of running a Computer System plan type. Each time a Computer System Protection Plan executes it creates a Recovery Point that can be used to recover the entire computer system, or individual files within it.

### Recycle Bin
Each Store has its own recycle bin where expired catalogs are kept until purged by a store Purge task.

### Remote Computers
Networked computers protected by the software are called Remote Computers. Each remote computer is listed and managed by its network computer name under the Remote Computers folder in Archive Manager. The computer that the software is installed on is called the Local computer, or sometimes the Archive Manager server.

### Restore
The Restore action initiates data recovery as the data existed at a point in time. Data is restored by choosing a particular restore point from a particular archive in a store. Files can be restored to their original location or to an alternate location of your choice. The original directory structure and permissions are also restored.

### Restore Point
A restore point is an archive of selected data as it exists at protection plan runtime. The plan initiates volume shadow copies for consistent and application-aware restore points. Each time a Protection Plan is executed a new restore point is created corresponding to that particular point in time.

### Search Service
The Search Service is a Windows software service for performing file lookups within stores. Search is not compatible with all editions of the software.

### Service
This is a Windows computer program that runs in the background.

### SRE
The System Recovery Environment (SRE) is a bootable pre-installation environment used in the process of recovering a computer system that has been protected with a Computer System plan type. An SRE ISO image can be downloaded and burned to media using the Save System Recovery Environment action in Archive Manager. It contains a lightweight Windows operating system and an interface for configuring the new hardware and choosing a recovery point.

### Storage
The term Storage refers to disk, cloud and tape storage used by the software. It is sometimes used to describe a store or set of stores used by the software.

### Store
A store is a disk storage location targeted by local and remote protection plans for keeping archived data. Protected file content originating from all associated computers is deduplicated and stored in a common content location within the store. Information specific to each protection plan (metadata) is abstracted and tracked in individual store archives.

### Store Group
Store Groups facilitate running a protection plan using rotating media and allow for taking media off-site. Copy Tasks can also select a destination store group instead of a specific destination store to

enable media rotation. When stores have been created on multiple storage devices, stores can be grouped together into a Store Group. Protection Plans can then target a Store Group instead of targeting a specific store.. At plan startup time, the plan selects a store in the store group based on the Store Group settings. Stores can also be added or removed from the group without affecting the plan configuration.

### Store Task
Store tasks are tasks that operate at the store level and run processes on the Archive Manager server. Types of store tasks are: Vaulting, Copy, Verify, Expire, Purge and Archive Restore.

### System Recovery Environment
The System Recovery Environment (SRE) is a bootable pre-installation environment used in the process of recovering a computer system that has been protected with a Computer System plan type. An SRE ISO image can be downloaded and burned to media using the Save System Recovery Environment action in Archive Manager. It contains a lightweight Windows operating system and an interface for configuring the new hardware and choosing a recovery point.

### Tape
This software can store data on LTO tapes for long-term retention. Primarily, tape is used by a vault task to write to tape selected archives that already exist in a store on disk. A Store Vaulting Task reformats a store's deduplicated data into a form called a Vault, suitable for high-speed streaming. In addition, LTO generation 5 and newer tapes can be formatted with the Linear Tape File System (LTFS). LTFS tapes can be used as a Store location and Archive Restore Task targets.

### Tape Storage
Tape Storage is a folder of the Archive Manager user interface that contains all of the tape-related items. Here you will find Volume Sets, Tape Vaults and Tape Devices, for instance.

### Tape Vaulting
The process of backing up selected archive data to tape is called Tape Vaulting. Deduplicated data is reformatted from the store into a Vault, suitable for high-speed streaming to tape for long-term retention.

### Task
Tasks are configurable commands that may be scheduled or run on demand. Tasks are stored and executed as Windows Scheduled Tasks. Task types consist of Protection Plans and Store Tasks.

### User Account
Windows denies or grants access to its resources by means of user accounts. For best results, a user account should be created for exclusive use by this software. Plans and tasks should run using this account to avoid conflicts. The Properties page of the Archive Manager folder in the user interface contains a tab called User Account. Here you can specify account credentials that will automatically be used when creating or editing tasks. This avoids being frequently prompted for user account credentials.

### Vault
A vault is a cloud or tape storage location targeted by a store vaulting task and is created automatically when the store vaulting task is created. After a vault is created, it will appear in the All Cloud Vaults or All Tape Vaults folder.

### Vaulting
Vaulting is the process of storing previously archived, deduplicated data to cloud or tape for long-term retention.

### Vaulting Task
A Vaulting Task is a store task for saving data in its deduplicated state either to cloud or tape for long-term retention.

### Verify Task
A Verify Task is a store task for verifying store consistency.

### ViewStor Service
The ViewStor Service is a Windows service for viewing the contents of an archive restore point in the point-in-time explorer window.

### Volume
A Volume is another term for a tape.

### Volume Set
A Volume Set is a logical grouping of Volumes, or tapes. A Vaulting Task targets a Volume Set. A Vault can span Volumes within a Volume Set. Multiple Vaulting Tasks can target the same Volume Set, as well. A single volume, therefore, can contain zero or more vaults or partial vaults.