The Backup Software

User's Guide to the Client

Version: UGC VG4.0

Local and Off-site Data Backup. Anytime, Anywhere Data Access.

Email Retention and Discovery. Mailbox Storage Management.

Table of Contents

Table of Contents (continued)

Table of Contents (continued)

Table of Contents (continued)

1-1 Welcome

Getting Started [**1** 2 3 4 5 6 7 8 9]

Thank you for choosing The Backup Software for your data backup needs.

The purpose of this Getting Started guide is to get your data backups configured and running as quickly as possible. This topic just covers the basic functions and does not include all of the features, benefits and tools available in The Backup Software. The following steps will guide you though the setup process.

You will get a quick overview of the user interface, and then we will walk you through configuring and running your first backup. The entire process should not take more than a few minutes.

This Getting Started guide will walk you through the following steps:

1. Welcome
2. User interface overview
3. Setup your account
4. Create your pass phrase
5. Specify backup data
6. Exclude unwanted data
7. Schedule unattended backups
8. Configure backup options
9. Perform your first backup

Next: Overview of user interface

1-2 User Interface Overview

Getting Started [1 **2** 3 4 5 6 7 8 9]

The The Backup Software program is your starting point for all data backup tasks. You can configure and schedule your backups, manage what to backup, and view detailed information for running and completed backup sessions. There are six administration panels. Activate a panel by clicking on one of the icons on the left:

System Status

Use this panel to monitor backup activity, access log files, and check for software updates. The panel is divided into two pages. Change pages by clicking on one of the tabs across the top:

✓ Backup Status: Start a backup or monitor current activity, view disk usage, and view log files of previous backup and restore sessions.

Online Updates: Check for software updates and view the associated log entries.

Control Panel

Recover or destroy files, access the web portal (manage your account), recover a forgotten pass phrase, and schedule a full backup.

My Account

Configure your backup account and your data encryption settings. Typically you only need to use this panel once because these settings do not usually need changing once configured.

Folders

Manage what data should be backed up. Add, move, and delete root folders. Configure exclusion policies. Visualize! your settings to verify correctness and estimate disk usage.

Schedule

Set when and how often automatic backups should happen.

Options

Customize all aspects of The Backup Software. Configure historical versions. Setup email notifications of backup completion or failure.

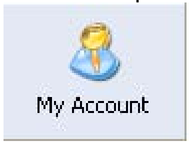
Previous: Welcome
Next: Setup your account

1-3 Setup Your Account

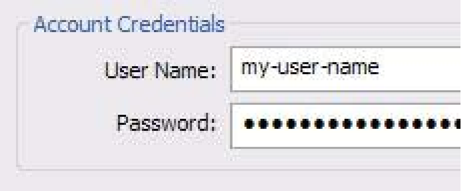
Getting Started [1 2 **3** 4 5 6 7 8 9]

To protect your data from unauthorized access and for billing purposes you must have an account in order to backup data to our servers. If you don't have an account please contact your sales representative.

1. Click the My Account button to navigate to the correct panel:



2. Enter your User Name and Password and press enter to test the connection:



Account Credentials

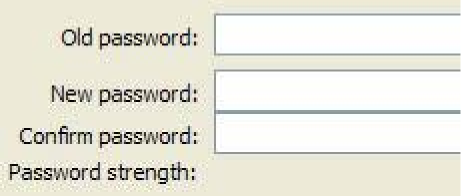
User Name: my-user-name

Password: ••••••••••••••••

If there is difficulty verifying your connection settings please contact technical support.

NOTE: The default server settings for your configuration are shown under the heading of "Destination of Data". These values do not need to be changed as part of the Getting Started process. To learn more about these optional features, reference the topics on Local Disk Backups and Local Server Backups. Please contact your support representative if there are any problems.

3. You will be prompted to change your password. Press OK. The change password dialog will appear.



Old password:

New password:

Confirm password:

Password strength:

Enter your old password, then your new password, and then your new password again (to verify that you typed your password correctly). Do not rush through this step by choosing a weak password. Some thought may be required to create a strong password.

Choosing a strong password is very important. If someone can guess your password then they will be able to destroy data associated with your account, and they will be able to access your account information online. They will not, however, be able to read the contents of your data unless they also guess your pass phrase. To help ensure the security of your password, your password must meet the following criteria:

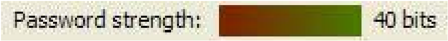
- It must be at least 8 characters long.
- It must contain at least one number or punctuation mark.
- It cannot contain your username.
- It cannot contain a sequence of identical or consecutive digits.

Passwords that meet these criteria are more likely to be strong passwords, but the responsibility of choosing a strong password lies with you. Strong passwords:

- Are long enough such that a computer cannot easily try all possible passwords. %$SHORT_NAME% prevents automated attempts to guess your password by disabling your account if an incorrect password is used too many times consecutively.
- Do not consist mainly of words that can be found in a dictionary (and are not based on words with the vowels replaced by numbers).
- Do not contain other information that is known to or might be easily guessed by an attacker.
- Consist of lower and upper case letters, numbers, and punctuation.

%$SHORT_NAME% will remember your password on your backup computer so that you will not be required to enter it (except when destroying data). However, you will need to memorize your password so you can sign in to your account online and access your data on the web.

The password strength meter at the bottom will help you gauge the strength of your password and will dynamically update as you enter your password.

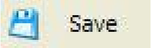


Your password should have an estimated strength of at least 24 bits, and a strong password will have an estimated strength of more than 32 bits. Because your password can be changed and is not used to encrypt your data, your password does not need to be as secure as your pass phrase (discussed next).

For more information on creating strong passwords, click here.

When you have entered the information, press OK. You will be returned to the My Account panel.

4. Click the Save button in the lower right corner:



Previous: User interface overview
Next: Create your pass phrase

1-4 Create Your Pass Phrase

Getting Started [1 2 3 **4** 5 6 7 8 9]

Note: Choosing your pass phrase is the most important step of the setup process. Please do not rush through this section!

Your pass phrase will be used as an encryption key to protect the contents of your data. The security of the encryption used to protect your data depends upon a strong pass phrase. You must remember your pass phrase in order to access the contents of your data.

> Tip: Your pass phrase is different from your account password. Your account password protects access to your online account and billing information, and it also protects the manual destroy data operation in the file manager. Your pass phrase is used as an encryption key

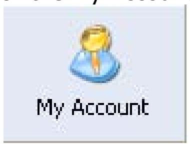
Although a customer service representative can reset your account password if you forget it, they will not be able to 'reset' the pass phrase used to encrypt the data on our servers. You must know the exact pass phrase that was used to encrypt your data in order to decrypt your data.

Because you must not forget your pass phrase, we offer the ability to save your pass phrase in a dually encrypted fashion on our server. No one will be able to read the saved pass phrase without knowing the exact answers to several security questions, which you will choose and answer when saving your pass phrase to our server. For additional information on the security of your saved pass phrase, click here.

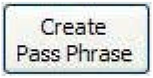
> **WARNING: If you choose not to save your pass phrase to the backup server and you forget your pass phrase, you will be unable to access your data. It is not possible for us to recover your encryption key if you do not save your pass phrase on our server.**
>
> **WARNING: If you do save your pass phrase to the backup server, but you forget the answers to your security questions then we cannot recover your pass phrase, and you will not be able to access your data if you forget your pass phrase.**

Please follow these steps to create your pass phrase:

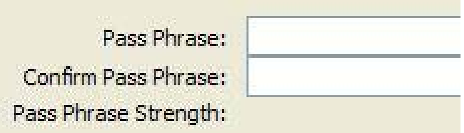
1. If you are not on the My Account panel, click the My Account button on the left:



2. Click the Create Pass Phrase button (if you've already created your pass phrase, click the Change Pass Phrase button):



3. You will be prompted to enter new pass phrase:



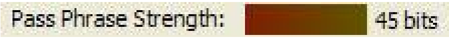
Pass Phrase:
Confirm Pass Phrase:
Pass Phrase Strength:

Enter your pass phrase and then your pass phrase again (to verify that you typed your pass phrase correctly).

Choosing a strong pass phrase is very important. If someone can guess your pass phrase then they will be able to read the data associated with your account (if they know or guess your account password).

A strong pass phrase can be generated by using a string of unrelated words, modifying them in predictable ways, and inserting random numbers and punctuation. The longer and more random your pass phrase is the more secure it is. Using a string of unmodified words found in a dictionary is not secure. You should change characters, insert numbers and punctuation, and use unpredictable capitalization. You should also insert words that consist of random characters (such as a secure password).

The pass phrase strength meter at the bottom will help you gauge the strength of your pass phrase.



Pass Phrase Strength: 45 bits

It is essential to the security of your data that you choose a strong pass phrase. A secure pass phrase will prevent [future] computers from cracking your pass phrase by trying every possible combination.

At the rate technology is currently progressing, a pass phrase with an estimated strength of at least 96 bits should be unbreakable until at least 2015. A pass phrase estimated at 128 bits or more should be unbreakable for an additional 20 years. (More information: Schneier paper, Wikipedia article, and key length calculator)

> Note: The above statements are just estimates and are not providing any guarantees or warranties of security. You are responsible for choosing a strong pass phrase. The strength estimation algorithm is based on Shannon's measure of entropy (more). It measures the degree of predictability of characters within the pass phrase itself.

To help ensure the strength of your pass phrase, your pass phrase must meet the following criteria:

- It must be at least 15 characters long.
- It must contain at least two numbers or punctuation marks.
- It cannot contain your username.
- It cannot contain a sequence of identical or consecutive digits.

Pass phrases that meet these criteria are more likely to be strong passwords, but the responsibility of choosing a strong password lies with you.

For more information on creating a strong pass phrase, please see these articles:

- Article on Wikipedia
- The PGP Passphrase FAQ (Note: Our software uses 256-bit AES encryption, SHA-256 hashing, and follows RFC 2898 PBKDF2 in generating an encryption key from a pass phrase.)

The Backup Software will remember your pass phrase on your backup computer so that you will not be required to enter it. However, you will need to memorize your pass phrase so you can restore your data when offsite or when your computer fails.

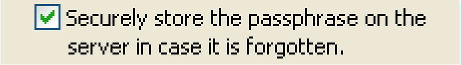
NOTE: Once your pass phrase has been set, you will not be able to change it without first contacting the The Backup Software Technical Support Group so that they will can reset the "pass phrase lock".

4. **Memorize your pass phrase.** The exact pass phrase is required to recover your data. You may want to share pieces of the pass phrase with trusted associates (for example, tell a third of the pass phrase to six people). You should save the pass phrase to the server and also save it to some sort of removable media (see below).

5. If you want to save your pass phrase on the server in a secure fashion, check the box below the confirm pass phrase edit box that says Securely store the pass phrase on the server in case it is forgotten.

> **WARNING: If you choose not to save your pass phrase to the backup server and you forget your pass phrase [and do not have a copy of it in a file], then you will be unable to access your data. It is not possible for us to recover your encryption key if you do not save your pass phrase on our server.**

You should always save the pass phrase on the server. Doing so does not compromise the security of your pass phrase. Click here for more information.



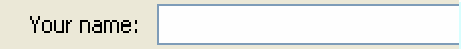
☑ Securely store the passphrase on the server in case it is forgotten.

6. Once you have chosen and entered your pass phrase (twice), press OK.

6a. If you chose to save your pass phrase to the server, the security questions and answers dialog will appear (otherwise skip to 6b). Here you will specify the list of security questions and give answers to these questions. The answers to these questions will be used to protect the pass phrase stored on our server and ensure that only you will be able to recover the pass phrase if it is forgotten.

> **WARNING: If you cannot remember the exact answers to your security questions then we cannot recover your pass phrase, and you will not be able to access your data if you forget your pass phrase.**

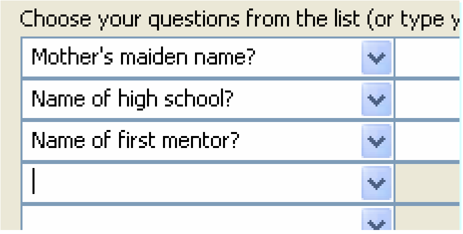
Record the name of the person filling out the security questions in the "Your Name:" box. This way the person using the pass phrase recovery will know who it was that answered the questions. You can also select the level of hints that you want to be provided if you have to use the recovery process. More hints will make it easier to guess your exact answers.



Your name:

During the pass phrase recovery process you will be prompted with the security questions you choose here, and you will have to provide the answers exactly the same as when you type them here (except for capitalization and whitespace). Punctuation is important, so be sure to use a standard format for dates (such as mm/dd/yyyy or Jan 1, 2007).

You specify the questions on the left and give the associated answer in the box to the right of the question. You can either type your own question or choose a predefined question by clicking on the down arrow in the box (⌄).



Choose your questions from the list (or type y

Mother's maiden name?

Name of high school?

Name of first mentor?

The pass phrase will be stored encrypted on the server, and only a few senior level technicians will be able to initiate the recovery process. The answers to your questions provide an additional level of security ensuring that only you have access to your pass phrase. The more questions you answer and the longer and more random your answers, the harder it is to guess or compute the answer. But you should always be able to remember the answers exactly or you will not be able to recover your pass phrase.

You are required to choose and answer at least 3 questions, but answering at least 7 or 8 questions is much more secure (the difficulty becomes exponentially harder as the length of your combined answer increases). You will only have to do so once, so it is better to take the time to choose and answer more questions.

NOTE: This set of security questions is associated with the current pass phrase. It is possible to change the security questions without actually changing your pass phrase. You have to follow the same process as you would to change pass phrase (and again choosing to store the pass phrase on our secure server).

Once you have entered your questions and answers press OK and your pass phrase will be securely stored on the server. Please skip step 6b below to step 7.

6b. If you chose NOT to save your pass phrase to the server a confirmation dialog will appear. Please read the notice and proceed only if you agree. Again, because you have chosen not to store your pass phrase on the server we cannot recover a forgotten pass phrase, and without your pass phrase your data backups will be worthless. To proceed, type YES in the box and click OK.

NOTE: You should always save the pass phrase to a file and place it in a separate and secure location (described in the next step) because the server is not storing your pass phrase, and you must have your pass phrase to recover your data. If you don't save your pass phrase then you run the risk of losing your backup data forever.

7. The software will ask you whether you want to save the pass phrase to a file. Always save the pass phrase to a file and store it on a different computer in a different physical location or other safe place (such as on a CD in a safe deposit box).

Choose yes, and it will prompt you where to save the file (it will save the pass phrase to a text file). You should save the pass phrase to removable media (floppy disk, flash drive, etc.), or save it to your hard disk and then immediately burn a CD. The saved pass phrase file is like a key to your data so protect it accordingly. You may save your pass phrase at any time by choosing the Save Pass Phrase to Disk command from the Tools menu.

Your account is now configured for The Backup Software, and you are ready to specify what data should be backed up.

Previous: Setup your account
Next: Specify backup data

1-5 Specify Backup Data

Getting Started [1 2 3 4 **5** 6 7 8 9]

Next you will specify what content should be backed up. The general strategy is to specify which folders should be backed up (which includes all of its subfolders and files), and then to come back and exclude what you don't need afterward.

> Advanced Feature: Additionally, you can individually list files to backup, but this should only be done for files in folders where you don't want to backup most of the data, and where you don't want to backup files that are created in that directory in the future.

Please follow these steps to specify what data to backup:

1. Click the Folders button to navigate to the correct panel:

2. Click the Add button on the right. The Add Folders dialog window will appear. The folders on your file system will appear on the left, as in Explorer. Folders and files that will be backed up are highlighted in green. The list of folders and files to backup appear on your right.

It will have one or more folders selected by default (what folders it selects depends on your operating system and what data is installed). In general, it will make sure the following items are backed up by default:

- Your user's My Documents, Desktop, Favorites, and Start Menu folders.
- Your user's Application Data folders (often stores email and other application and user specific data).
- Common (Shared) My Documents, Desktop, Favorites, and Start Menu folders.

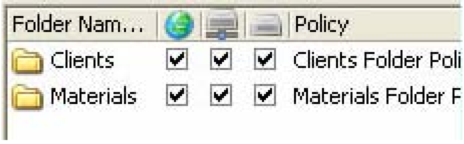
Note: On Windows XP or better all of this data will be contained in a user's profile directory, so only the profile directory for your user and the common user is added. Because this includes subfolders, all of the above data is also mentioned.

3. In the pane on the left select the folders on your file system that you want to backup and then click the Add button in the middle of the dialog (➔), or you can right click and choose Add to backup list. Note that when you add a folder all subfolders will be included in the backup. Don't worry about excluding data here. This will be done in the next step.

> Tip: If you only want to include a folder but not its subfolders then just add the folder now and use exclusions later to exclude the subfolders.

4. When you have specified all of the backup folders click Save. You should be back on the Folders panel.

The folders you selected will be now be listed in the window. The list shows the folder name on the Server, storage mode options, folder policy name, and folder path.

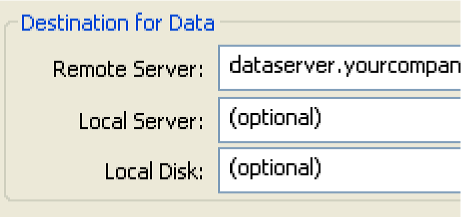


Folder Nam...	🌐	🖥	🖴	Policy
Clients	☑	☑	☑	Clients Folder Poli
Materials	☑	☑	☑	Materials Folder F

The storage mode icons indicate the possible location(s) were the backup for each folder is stored.

Icon	Storage Mode
🌐	Remote Server
🖥	Local Server
🖴	Local Disk

The storage modes are tied to the definitions of storage locations on the My Account page under the heading of Destination for Data.



Destination for Data

Remote Server: dataserver.yourcompan

Local Server: (optional)

Local Disk: (optional)

We recommend that you leave all three mode icons checked (which is the default). This way if you choose to implement a second and/or third storage mode by defining values on the My Account page, the backup will already be set.

5. Click the Save button in the lower right corner: Save

Click here for information on how to backup SQL Server databases.

Previous: Create your pass phrase
Next: Exclude unwanted data

1-6 Exclude Unwanted Data

Getting Started [1 2 3 4 5 **6** 7 8 9]

Next you will exclude data that does not need to be backed up. For example, you may not want to backup mp3 music files. Exclusions are handled via folder policies.

A folder policy is a list of inclusion and exclusion rules. You can exclude (or re-include) files based on several criteria: filenames (via wildcard matching), date/time, and size. A policy can also include rules from other policies. By default each backup folder is associated with its own policy, which includes the rules in the Default Policy.

The Default Policy excludes things such as temporary files, the recycle bin, Internet caches, windows system files, and windows registry files. Advanced users can modify the Default Policy to make system wide exclusions.

> ⚠ **Warning:** Be careful not to exclude data that you really need to backup. Most users will not need to edit policies directly and should use the Visualize! feature instead. After making any changes to a policy you should always use the Visualize! feature to confirm your change is correct.

Please follow these steps to exclude unwanted data:

1. Click the Folders button to navigate to the correct panel:

2. Click the Visualize! button on the right. The Visualize! dialog window will appear. This dialog presents a unified view of all of the data on your file system. You can browse your file system and see exactly what folders and files will be backed up. The files and folders are highlighted with the following colors:

- Green: These items will be backed up.
- Red: These items are excluded from the backup.
- Gray: These items will not be backed up because they are not within any backup folder.

Also, there are three additional columns of information:

- File Size: Size of file. Blank for folders.
- Data to Backup: Amount of data to backup within the folder and all of its subfolders. Blank for files.
- Excluded Data: Amount of data excluded from backup within the folder and all of its subfolders. Blank for files.

At the bottom of the dialog are two information boxes:

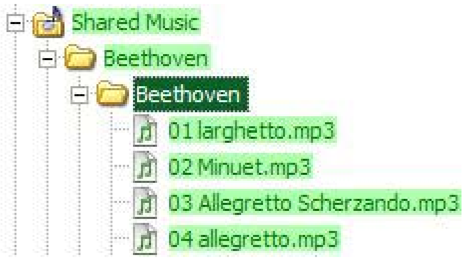
- Top: Displays detailed information about a file or folder: whether it's included in the backup, what backup folders contain the item, whether it's included or excluded, and what rule causes the inclusion or exclusion.

- Bottom: Displays size information for the selected item. It also displays size information for all backup folders in your system, to help you estimate how much data will be backed up.

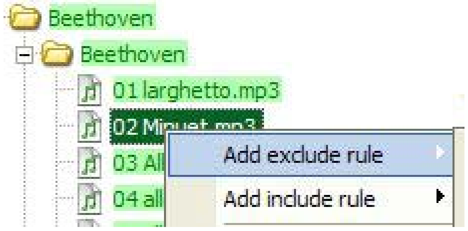
3. You can add exclusion rules (or add inclusion rules to re-include excluded files) by right clicking on a file or folder. If you right click on a folder then you will create a rule that excludes/includes folders (and their subfolder and files). If you right click on a file then you will create a rule that excludes/includes files.

Tip: You can undo and redo any operation. Just right click and select Undo or Redo.

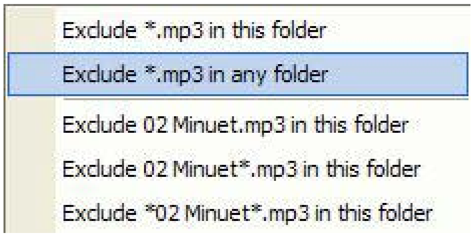
As an example, we will exclude all mp3 files from a backup:



Since we want to exclude a type of file, we will right click on one of the mp3 files:



We choose Add exclude rule from the popup menu:

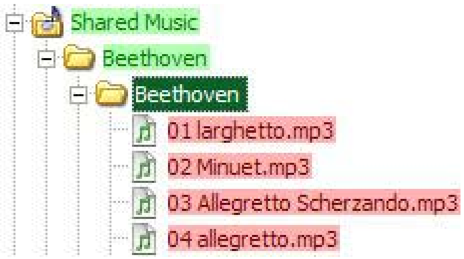

Exclude *.mp3 in this folder
Exclude *.mp3 in any folder
Exclude 02 Minuet.mp3 in this folder
Exclude 02 Minuet*.mp3 in this folder
Exclude *02 Minuet*.mp3 in this folder

Because we want to exclude all mp3 files in any folder and not just the Beethoven folder, we choose Exclude *.mp3 in any folder. The menu lists several other variations that allow you to exclude only that file, mp3 files that begin with 02 Minuet, mp3 files that contain 02 Minute, etc.

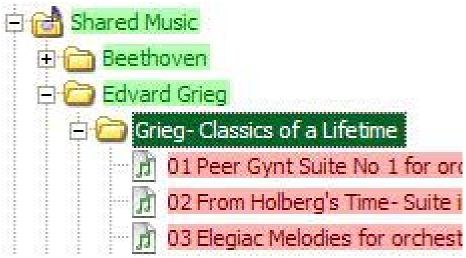
The Create a new filter rule dialog appears after selecting a menu item. This allows you to customize the wildcard before it is created. It also shows you what policies and backup folders will be affected.

A wildcard allows you to use * to match any character any number of times (including zero times) and a ? to match exactly one character.

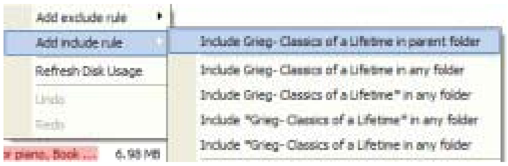
Continuing our example, this is what the screen will look like after adding the rule:



Now all mp3 files have been excluded from our backup of the All Users backup folder. However, let's say that we are a real fan of Edvard Grieg and want to backup our Grieg-Classics of a Lifetime album. Here is what it currently looks like:


Shared Music
Beethoven
Edvard Grieg
Grieg- Classics of a Lifetime
01 Peer Gynt Suite No 1 for orc
02 From Holberg's Time- Suite i
03 Elegiac Melodies for orchest

Now we right click on the Grieg-Classics of a Lifetime folder, choose Add include rule, and then Include Grieg-Classics of a Lifetime in parent folder:


Add exclude rule
Add include rule
Refresh Disk Usage
Undo
Redo
r piano, Book ...
6.98 MB
Include Grieg- Classics of a Lifetime in parent folder
Include Grieg- Classics of a Lifetime in any folder
Include Grieg- Classics of a Lifetime* in any folder
Include *Grieg- Classics of a Lifetime* in any folder
Include *Grieg- Classics of a Lifetime in any folder

Now all files within this folder are included (and will appear green). If you only wanted to include the mp3 files in this folder then you would have right clicked on one of the mp3 files, chosen Add include rule, then Include *.mp3 in this folder (when we added the exclusion rule it was Exclude *.mp3 in any folder)

4. Use the Data to Backup and Excluded Data columns to identify files and folders that need to be excluded (if you see a large amount of data where it's not expected drill down into the subfolders to find out where it comes from, and see if you need to exclude it, etc.).

> Tip: When you exclude or include files the Data to Backup and Excluded Data columns will not update automatically. Right click and choose the Refresh Disk Usage command to refresh the information.

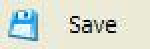
5. When you think you have the filters setup correctly, right click and choose the Refresh Disk Usage command. Wait for all calculations to complete. The disk information box is at the bottom of the dialog. It should include a line of text that begins with Amount to backup in all folders. For example: Amount to backup in all folders: Included=12.856 GB, Excluded=299.56 MB. You may have to use the scroll bar to the right of the box to see this information.

This tells you exactly how much data will be backed up to the server and how much will be excluded. If you are not satisfied create additional rules as described above and repeat this step.

6. Verify that all of your important data will be backed up by traversing your file system and making sure that everything important is highlighted in green.

7. When you are sure everything is correct, click the Save button in the lower right hand corner. You should be back on the Folders panel.

5. Click the Save button in the lower right corner:



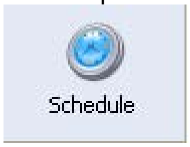
Previous: Specify backup data
Next: Schedule unattended backups

1-7 Schedule Unattended Backups

Getting Started [1 2 3 4 5 6 **7** 8 9]

To ensure a recent copy of your data is always on the backup server you should schedule automated backups.

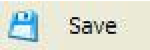
1. Click the Schedule button to navigate to the correct panel:



2. Select Daily and change the starting time and backup frequency (number of times per day) as desired. Backing up your data ensures your work is saved throughout the day, but can also increase the amount of data stored in historical versions. Most users only backup their data once or twice a day.

3. Change other options, as desired. The default settings will work for most users.

4. Click the Save button in the lower right corner:



5. If you are running on a system that requires a password, the Enter Windows Password dialog may appear (Windows 95/98/Me users may skip this step). Enter the password associated with your Windows user account. This is not your backup account password. This is the password you use to logon to Windows.

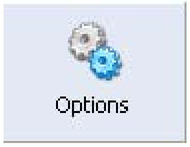
Previous: Exclude unwanted data
Next: Configure backup options

1-8 Configure Backup Options

Getting Started [1 2 3 4 5 6 7 **8** 9]

Finally, before performing your first backup, we need to configure some options.

1. Click the Options button to navigate to the correct panel:



2. There are several options, but most can be left to their default setting. When you click on an option its description will appear at the bottom of the window. The settings that you may want to change include:

Synchronization:

- Number of Days to Keep Historical Versions: Increase this setting if you want previous versions of your data to be available for a longer period of time.
- Minimum Number of Versions to Keep: Increase this setting if you want to always store more versions of files (as a minimum).
- Number of Days to Keep Deleted Files: Increase this setting if you want to keep files that you have deleted locally for a longer period of time.

Notifications:

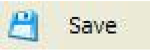
- You may want to change the notification actions when the backup has finished with warnings or errors to Notify me and send me an email. This will help you be alerted when the backup may need help or attention.

Outgoing Email Configuration:

- If you have problems receiving the notification email then you will need to provide an SMTP Server Address (and optionally an SMTP user name and password) in this section. Contact your network administrator for this information.
- To test that notifications are working correctly, go to the system status page, click the Help Me button, and choose to send an email to your desired notification email address. It will indicate whether or not it was successful.

3. Change other options, as desired. The default settings will work for most users.

4. When you are finished, click the Save button:



Previous: Schedule unattended backups
Next: Perform your first backup

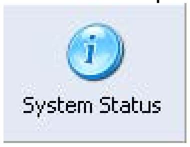
1-9 Perform Your First Backup

Getting Started [1 2 3 4 5 6 7 8 **9**]

You are now ready to perform the initial backup, which may take a long time. You can let the backup run in the background, as The Backup Software will not interfere with other applications. After the initial backup has finished future backups will be much shorter. If you have a large amount of data (more than 50 GB), you may want to use a USB preload. Contact customer service to learn more about how to perform a preload using a USB disk.

To perform the initial backup, follow these steps:

1. Click the System Status button to navigate to the correct panel:



2. Click the Backup Now button. You can monitor the status of the backup in the top part of the window. More detailed information can be obtained by double clicking on the log file on the bottom part of the window.

3. Let the backup run to completion. Double click on the log file to open the log viewer. Use the navigation keys (press F1 in the log viewer for a list of keys) to inspect all of the errors and warnings.

> ⚠ Most errors are caused by files that could not be backed up because another application has exclusively opened or locked the file. When running on Windows XP, Windows Server 2003, or better The Backup Software will use the Volume Shadow Copy service to backup open files. Some applications (including Microsoft Outlook, databases, some business software) will lock files when they are being edited. These applications need to be closed on older operating systems so that these files can be backed up.

You have now successfully configured your remote backups. At this point, you may want to configure and schedule local disk backups or local network backups.

⇦ Previous: Configure backup options

2-1 Overview: Remote Backups

The Backup Software allows you to easily backup a copy of your data to our secure data centers. The Backup Software will encrypt your data using the AES-256 algorithm using an encryption key formed from your pass phrase.

IMPORTANT: Your pass phrase is required in order to restore your data. If you do not have your pass phrase you cannot restore your data. You should keep several different copies of your pass phrase for maximum protection (for example, by printing it and storing the paper copy in a secure location, by using our pass phrase recovery feature, and by keeping a copy of either the pass phrase or your settings profile in a file on a different computer).

As opposed to traditional backup systems, once configured backups are completely automatic. Each time the backup runs it will upload new files to our data center, or if the files were previously uploaded, then it will upload only the changes between the previous version of the file and the new version. Our data center will securely preserve the previous versions of changed files according to your backup settings and policies. Once the first full backup is complete, only changes have to be sent from that point forward.

If you have a lot of data to backup initially, then it is possible to perform a USB Preload to encrypt and save the initial backup data to a USB disk. We then receive and process the USB disk, loading the data into our data center, and return the USB disk back to you. Please contact us to arrange a USB preload.

You can restore data instantly anytime it is needed by using the file manager tool (on this or some other computer), or by logging in to the web portal (found under the Control Panel panel) on any compatible computer and using the Web Access feature to download your data.

2-2 Overview: Local Disk Backups

In addition to backing up your data to the remote server, you can also backup your data to a local filesystem or network share accessible from your computer. This local volume can be another hard drive, external storage such as a USB-attached disk, or a network share (including SAN volumes).

NOTE: If you have more than 10 computers that will be backing up to the same network location, we recommend configuring Local Server Backups instead, as it uses bandwidth more efficiently.

To configure local disk backups, refer to the Setup Instructions.

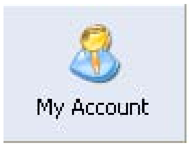
2-3 Setting Up Local Disk Backups

In addition to backing up your data to the remote server, you can also backup your data to a local volume on your computer. This local volume can be another hard drive, external storage such as a USB-attached disk, or a network-mapped drive (including SAN volumes).

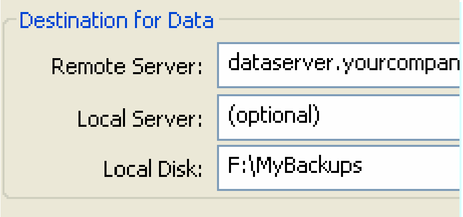
If you want to backup all computers within the same network to a central storage server, then you should use Local Server Backups instead (or in addition to local disk backups).

To configure backups to a local disk:

1. Go to the My Account panel:



2. Change the Local Disk field to be a directory on the local disk where you want to store the backed up data. For example, if you have a USB disk mounted on F:, enter something like F:\MyBackups



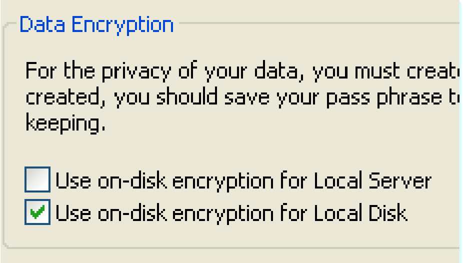
Destination for Data

Remote Server: dataserver.yourcompan

Local Server: (optional)

Local Disk: F:\MyBackups

3. Choose whether or not you want the data stored on the local disk to be encrypted. Encrypting your data is a good idea if the local disk can easily be removed from your computer (such as a USB disk).



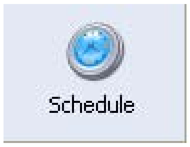
Data Encryption

For the privacy of your data, you must creat
created, you should save your pass phrase t
keeping.

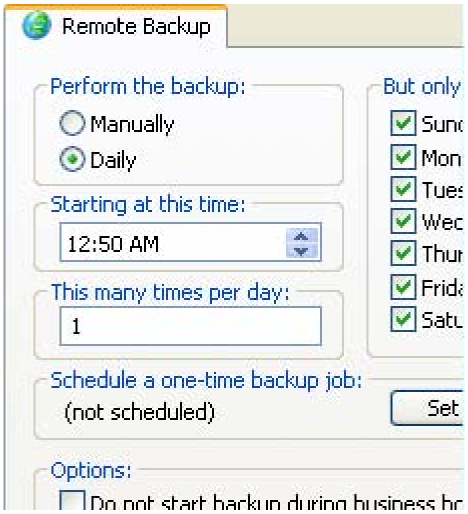
☐ Use on-disk encryption for Local Server
☑ Use on-disk encryption for Local Disk

The advantage of not encrypting your data is that you do not need to know your pass phrase in order to restore the data. If you do encrypt your data, you must know your pass phrase or it will be impossible to restore your data.

4. Go to the Schedule panel:



5. Click the Local Disk Backup tab, choose a time to schedule the backup to local disk, and click Save.



Perform the backup:
○ Manually
● Daily

Starting at this time:
12:50 AM

This many times per day:
1

But only
☑ Sunc
☑ Mon
☑ Tues
☑ Wec
☑ Thur
☑ Frid
☑ Satu

Schedule a one-time backup job:
(not scheduled)

Options:
□ Do not start backup during business hc

On Server 2003 (or better) or Windows Vista (or better) remote backups and local backups can run concurrently. On older operating systems the backups must run at separate times. We recommend starting the local backup first because it will complete faster. If the local backup does not finish on time the remote backup will wait until the local backup finishes before starting.

Once you have configured local disk backups a new tab will appear on the System Status page that will allow you to monitor the status of local disk backups.

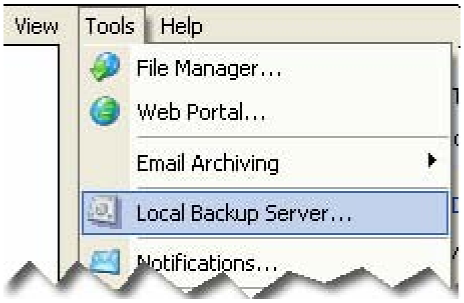
NOTES:

- If you are backing up Microsoft Exchange, change the 'Restrict Concurrent Backups' setting on the Backups tab of the Options page to be checked (Yes). Microsoft Exchange only supports one active backup at one time. If this option is not checked, if one backup starts while another is running, then open file backup will fail and the resulting backup will probably have errors.

2-4 Overview: Local Server Backups

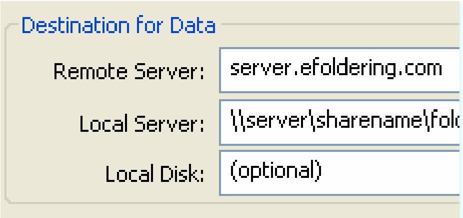
In addition to backing up computers to the remote server, you can also setup a storage server on your local network. To do this, configure the Local Backup Server feature of our software to run on your designated central storage server. Your storage server can then receive backup data from computers within your network. This strategy is especially useful if you have many computers in your network and each computer does not have an extra hard drive or USB-attached storage.

Choose one computer in your network to act as the central storage server. Setup this storage server by using the Local Backup Server Manager feature (access from Tools -> Local Backup Server) of The Backup Software.



The configuration process mainly consists of specifying a backup account authorized to use the Local Backup Server, and also choosing the path of the storage location. It is important that any firewalls on this machine be configured so that the server can accept TCP connections on port 5470.

Once the Local Backup Server feature is configured you will need to set the network hostname of the storage server for each computer in the network that has The Backup Software installed. This is done by supplying the network hostname on the "My Account" page of the The Backup Software in the field "Local Server" for each computer.



Destination for Data

Remote Server: server.efoldering.com

Local Server: \\server\sharename\folc

Local Disk: (optional)

Please see the setup instructions for more information on how to define this strategy.

If you do not want to setup and configure a local backup server, but rather want to perform local backups and store data directly on some filesystem (e.g., USB disk or network share), then you should configure Local Disk Backups.

2-5 Setting Up Local Server Backups

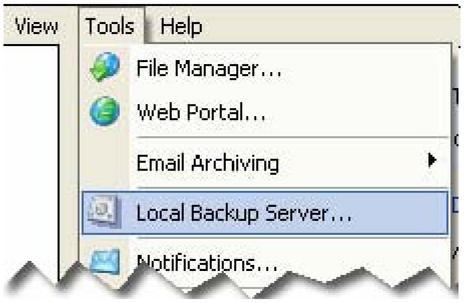
As explained in the Overview, the Local Backup Server feature lets you perform backups on the computers in your network and store the resulting data on your designated central storage server. This central storage server will be running the Local Backup Server feature of our software. This is in contrast to Local Disk Backup feature, which allows you to backup data directly to a local filesystem (such as a USB disk or network share).

To setup local server backups, you first must configure the Local Backup Server feature in our software:

On the computer that you want to use for the central storage server, install The Backup Software.

NOTE: You do not need to configure remote backups on this computer, even though you have installed the software and are operating a storage service on it.

1. Start the Local Backup Server Manager by opening the The Backup Software, opening the Tools menu, and choosing Local Backup Server.



   On the Configure page enter the credentials for a backup account. This account needs to be the parent of all of the accounts for the computers in this network that will be storing data on the local backup server. The local backup server will not store data for accounts that are not related to the backup account configure on this page.

   Using the "Store Path" field, specify the path where data received from local network backups will be stored. This can either be the path of some local drive, RAID volume, or SAN, or you can configure a UNC path.

   NOTE: Do not configure the storage path to be a network mapped drive. Instead, use the UNC path to the network share (e.g., \\server\sharename\folder).

   NOTE: You should specify a subdirectory on the drive and not the root of the drive. For example, use something like F:\LocalBackups and not just F:\ (or \\server\sharename\folder instead of \\server\sharename).

2. When you click Save, it will automatically start the Local Backup Server. You can monitor the status of the local backup server on the "Server Status" page.

If there are any Firewalls on this machine, such as the Windows Firewall, you will need to configure the firewall so that the computer can receive TCP connections on port 5470. (You may want to restrict incoming connections so that they can only come from within the local network.)

NOTE: that the TCP port can be changed on the Options page of the Local Backup Server Manager.

3. If you are backing up to a network location, then in Windows explorer, do start, run, services.msc. Right click the The Backup Software Server service and choose Properties and go to the Log On tab. Change the credentials of the service to use a Windows account that has permission to store data on the network share. Save changes. Right click the service and choose to restart it.

Next, for each machine in the network that has The Backup Software installed you need to perform the following steps to configure it to store data on the local backup server:

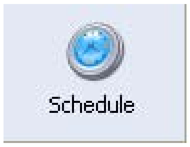
1. Start the The Backup Software and go to the My Account page:

2. In the local server field, enter the network hostname or IP address of the computer on your network that is running the Local Backup Server. If you need to specify a custom TCP port, use the syntax: "hostname:port" (without the quotation marks).

   NOTE: This is not a filesystem path such as F:\ or \\server\sharename.

3. Optionally, go to the Folders page and customize any backup policies for the local backups.

4. Go to the Schedule page:

5. Click the Local Network Backup tab, choose a time to schedule the backup to the local network server, and click Save.

   On Server 2003 (or better) or Windows Vista (or better) remote backups and local backups can run concurrently. On older operating systems the backups must run at separate times. We recommend starting the local backup first because it will complete faster. If the local backup does not finish on time the remote backup will wait until the local backup finishes before starting.

Once you have configured local server backups a new tab will appear on the System Status page that will allow you to monitor the status of local server backups.

Notes:

- If you are backing up Microsoft Exchange, change the 'Restrict Concurrent Backups' setting on the Backups tab of the Options page to be checked (Yes). Microsoft Exchange only supports one active backup at one time. If this option is not checked, if one backup starts while another is running, then open file backup will fail.

2-6 Overview: Email Archiving

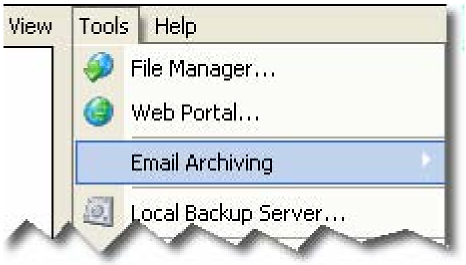
The Backup Software can be used to provide system-wide protection of Microsoft Exchange and other email products. Our email archiving allows you to recover your entire email database if your information store becomes corrupted or is lost. Please refer to our knowledge base for configuration instructions.

Through The Archiving Software we also offer the ability to perform full policy-based email archiving for Microsoft Exchange. Content is copied or moved out of Exchange into a locally stored archive. This archive can optionally be backed up off-site. The use of The Archiving Software offers the following additional advantages:

- Individual messages can be backed up and restored
- Old content can be removed from the Exchange information store and into the archive, increasing the performance of Microsoft Exchange and reducing your Tier 1 storage requirements
  - Content can be removed completely or a small stub can be left behind
  - The stub provides one-click access within Outlook to the original message
  - Content that is removed completely can be instantly searched for and restored
  - Which content to remove is directed by policy -- message age, size, and content
  - Content removal can be automatically triggered to keep mailboxes at a desired percentage of their mailbox quota

- Legal compliance requirements can be satisfied by ensuring retention of all email for the required period of time, after which content can be automatically purged
- Instant search of all email within the archive
- Users can search for and restore messages from the archive within Outlook (no plug-in required)

The Archiving Software is accessed from Tools -> Email Archiving menu from within the The Backup Software.



Configure the system to archive content from Exchange into one or more filesystem locations. This local archive provides instant access to all archived content.

For additional protection and to meet legal compliance requirements, you can then easily backup your email archive by adding the filesystem locations on the Folders page in the The Backup Software.

The Archiving Software Quick Reference topic contains detailed information about this feature. Please refer to the Overview and the Install Guide for The Archiving Software.

3-1 Overview: The Backup Software

The Backup Software program provides the user interface to configure, manage, and monitor remote backups, local backups. It also provides the ability to start other tools, such as the file manager or email archiving.

User Interface:

The main user interface is composed of several pages. You switch to a different page by using the buttons on the left side of the main window. Each page is composed of one or more tabs, which are located across the top.

The following topics describe the user interface:

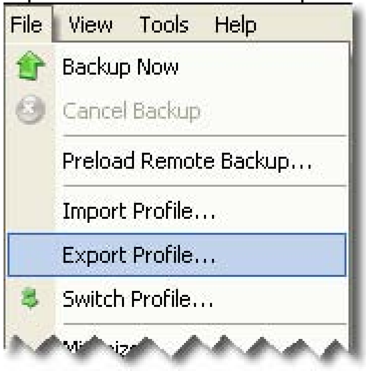
- System Status Page
  - Backup Status Tabs (Remote, Local Server, and Local Disk)
  - Reports Tab
  - Software Updates Tab
- Control Panel Page
- My Account Page
- Folders Page
- Schedule Page
- Options Page
  - Notifications Tab
  - Versioning Tab
  - Backup Tab
  - Bandwidth Tab
  - Advanced Tab

NOTE: To prevent anyone who does not know the account password from changing the backup settings, change the Access Control Level to "Require Account Password" (Page: "Options", Tab: "Advanced", Heading: "Software Security").

3-2 Settings Profiles

All of your backup settings, including your account information, folder list, schedule, and options are included in your settings profile.

The system allows you to export your settings profile to a file. You can then import the settings back into The Backup Software. This process can be very helpful if you are restoring your settings after a crash or to more quickly setup The Backup Software on another computer with similar settings.. To export and import your settings profile, use the File -> Import Profile and File -> Export Profile menu commands.



It is also possible to configure multiple settings profiles on the same machine. This is useful if you want to setup two different service plans on the same machine, or if you want to setup a different backup schedule for part of your data.

The Backup Software only displays settings from one settings profile at a time, which is called the active settings profile. To switch to a different settings profile, use the File -> Switch Profile. . . menu command.

NOTE: The System Status page displays log files for all settings profiles, not just the active settings profile.

The File -> Switch Profile menu command is also used to add a new settings profile. From the Configuration Profiles window, press the green + button to add a new settings profile.

NOTE: An easy way to configure a new settings profile is to copy all of the settings from your first settings profile. Use File -> Export Profile to export your first settings profile. Then switch to the new profile, and use File -> Import Profile to import all of your settings. Then, go to the My Account page and set the user name appropriately. The Schedule will also need to be set again after you import a profile.

3-3 Command Line Switches

In addition to the backup manager user interface, the client Backup Software program also provides functionality for several other specialized commands. These commands are invoked by running the program from the command line (or through the windows task scheduler) and then passing one or more command line arguments.

For example, to reinstall the services, open a command prompt (start, run, cmd) and then enter:

```
cd (directory containing program files)
<client program name>.exe /install
```

The following command line arguments are available to perform some action. These commands do not actually start the user interface, but rather the program will exit as soon as the action indicated by the command line argument has finished.

- /install
  The program will (re)install any required Windows services. It will also check to see if any software dependencies (such as the MSVC 2005 SP1 runtime) is properly installed.

  If you move the location of the installed Program Files, then you should run The Backup Software from the command line with the /install switch (or re-run the setup program) to make sure that all Windows services know the new location of the service executables.

- /uninstall
  This uninstalls all program files. It leaves settings and configuration information intact. Email archiving program files will also be uninstalled if they are present.

- /uninstall-full
  In addition to everything that /uninstall does, this also removes all configuration information and settings (both in the registry and any configuration files).

  WARNING: This will remove all settings and configuration information. If you still need the backup data in your account, then make sure that you know your pass phrase before using this to uninstall everything.

- /start
  This starts the supervisor scheduling service and the local backup server service (this service will only start if you have configured the local backup server; typically this is not configured).

- /stop
  This stops the supervisor scheduling service and the local backup server service.

  WARNING: Scheduled backups may not occur if you stop the services and do not start them before your next scheduled backup.

- /cancelbackup
  This forces any running backups to immediately cancel.

- /startarchiving
  This starts the email archiving service (if it is installed).

- /stoparchiving
  This stops the email archiving service (if it is installed).

  WARNING: Email archiving actions will not be performed when the service is stopped.

- /deduparchives
  By default the software will dedup messages in the email archive(s) once per week on Saturday morning (see the Options page, Backup tab topic). This switch can be used to start a message dedup scan immediately. This is useful if you want to setup a task scheduler task to initiate the dedup scan on a custom schedule, instead of on Saturday mornings.

- /archiving-uninstall-iis
  This uninstalls any email archiving related IIS web applications.

- /archiving-uninstall-app
  This uninstalls any program files that are part of the email archiving engine. This also uninstalls any email archiving related IIS web applications. Note that email archiving settings remain intact.

- /archiving-uninstall-everything
  This uninstalls all email archiving program files, IIS web applications, and settings.

- /exit
  This forces all The Backup Software applications to close immediately. It also stops the supervisor scheduling service and the local server service. Note that it does not stop the email archiving service. You typically will not need to use this switch.

- /upgradenow
  The software will immediately check for any available software updates. If updates are available, it will automatically download and install them without requiring any interaction from the user.

- /schedulemaintenance-all
  /schedulemaintenance-remote
  /schedulemaintenance-localserver
  /schedulemaintenance-localdisk

  These switches are used when you are manually scheduling when the backup should perform account maintenance and optimization. By default this process is automatically performed during a backup every 7 to 10 days. These switches will cause the maintenance to happen during the next backup job. See also the Extra Days Between Maintenance Advanced setting.

  You can also use the "**--profileid=N**" switch (see below) before /schedulemaintenance-... to schedule maintenance for a non-primary settings profile.

In addition to these command line switches, when starting the actual graphical user interface, other switches are available that affect how the user interface starts:

- "**--profileid=N**"
  This switch indicates that a specific settings profile should be loaded by default instead of the primary settings profile. N should be the numeric ID of the settings profile (a listing of all settings profile IDs is in the registry settings for the program). Note that you must include the "** and **" parts of the switch on the command line.

  For example:
  "**--profileid=3**"

- /startup

This switch indicates that the program is starting when you are logging on to Windows. It will suppress any unnecessary dialog prompts when starting in this mode.

- --cmd=viewlog
  Indicates that once the application has started it should immediately start the log viewer for the currently running backup.

- --cmd=viewpage:myaccount
  Indicates that once the application has started it should always show the My Account page initially.

3-4-1 Restoring After a System Crash

Follow the steps described below to restore all of your data after a complete system crash and to resume incremental backups.

These steps are only necessary if your Backup Software program files were lost in the crash (as these files contained the data needed for incremental backups). If you only need to restore files but your Backup Software program files and settings are still intact, then simply use the File Manager Tool to restore the data that you need.

If you still have The Backup Software program files and you only want to move them to a new computer (e.g., because you are upgrading to a new computer), then please see the Upgrading to a New Computer topic.

Restoring data and resuming incremental backups after a complete system crash:

Please follow these instructions precisely. The order of these steps are important. If you have any questions, please contact us.

1. **Reinstall.** Download and install The Backup Software.

2. **Download your settings profile.** Start The Backup Software program. Do not reconfigure the settings. Use the Control Panel page to start the File Manager.

   Use the File Manager to restore all of the files in the @@SoftwareSettings folder to your desktop. Do not restore anything else at this time.

3. **Import your settings profile.** In the Backup Manager, use the File -> Import Profile menu command to import the settings profile file that you restored from step 2. This will re-import all of your settings as they existed during your last backup. Go to the My Account page and re-enter the username that was used to previously back up the data on this computer.

   VERY IMPORTANT: Do not setup a backup schedule and do not start a backup until you have completed the next 2 steps.

4. **Restore your data files.** Open the File Manager again. This time select and restore all of your data files that need restoring.

5. **Rebuild your incremental backup cache.** Once you have restored all of your data, open the File Manager again. On the Data Selection page, select all of the same data that you restored in step 5. Click next to see the Restore Options page. Check the box that says Rebuild incremental backup cache (advanced). Then continue through all steps to complete the wizard. Instead of restoring your data (which you already did in step 5), it will rebuild your incremental backup cache (this process will only take a few minutes), allowing you to resume incremental backups right where you left off.

6. **Reschedule backups.** Use the Schedule page to schedule your backups so that incremental backups will continue from where they left off.

NOTE: If you are restoring from a USB disk (that we shipped to you as part of an emergency restore), then when you are logging in to the File Manager to restore data, be sure to use the Restore from Disk field to select the USB restore disk.

Please contact us if you have any questions. We are here to help make the restore process as smooth as possible for you.

3-4-2 Upgrading to a New Computer

If you are replacing an old computer, need to reload the operating system from scratch, or reformat your hard disk, etc. You may need to move The Backup Software from one computer to another, preserving the account information, pass phrase, and incremental backup cache. This topic will describe how to reliably transfer the backup settings and incremental backup cache.

If you have completely lost The Backup Software program files on your old computer, then please see the Restoring after a Crash topic instead.

Moving The Backup Software, settings, and backup cache to a different computer:

Please follow these instructions precisely. The order of these steps is important. If you have questions about this process, please contact us.

1. **Copy your data files to the new computer.** It is not required, but this process will be easier if the files on the new computer have the exact same location as they did on the old computer.

   NOTE: You can perform steps 2 - 6 while your data files are being copied. Do not continue to step 7 until all of your files have finished copying to the new computer.

2. **Export your settings profile.** On the old computer, open The Backup Software, and use the File -> Export Profile command (see Settings Profiles).

3. **Set backup schedules to manual.** On the old computer, change the backup schedule to manual for all backup destinations.

4. **Download and install The Backup Software on the new computer.**

5. **Move the incremental backup cache to the new computer.** Move all of the incremental backup cache files from the old computer to the new computer. This information is located in the (installed-folder)\folder-cache and (installed-folder)\folder-cache-local folders. Move these folders so that they are in the corresponding location on the new computer.

6. **Import your settings profile on the new computer.** On the new computer, use the File -> Import Profile command to import the settings profile you exported in step 1. Re-enter the username that you were using on the old computer on the My Account page.

   VERY IMPORTANT: Do not setup a backup schedule and do not start a backup until you have completed all of the previous steps and the next two steps (steps 7 and 8).

7. **Update Folder locations.** On the new computer, go to the Folders page. If any of the folders are in a new location on the new computer, highlight the folder and click the Move button to change the location.

   Note that you should select the location that represents the exact same location that was previously selected for your top-level folder. This is very important. If you have questions, please contact us.

8. **Verify your settings are correct using Visualize!** On the Folders page, use the Visualize! button to verify that your backup policies are correct -- anything that you expect to be backed up should be highlighted in green. Anything you do not expect to be backed up should be highlighted in red or grey.

9. **Schedule backups on the new computer.** On the new computer, use the Schedule page to set a new backup schedule.

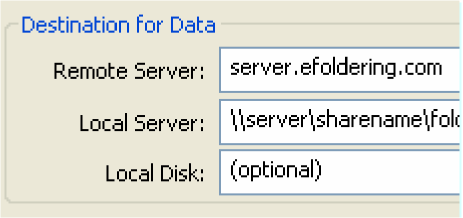
If you have any questions, please contact us. We will be happy to assist you.

IMPORTANT: If the old computer will still be operational, you should remove the account information on the old computer and change the schedule to manual. You can not use the same account for two different computers (doing so can mix your data together and cause other problems). You should always use a new sub-account for the new computer if you will need to continue to backup information on the old computer (in which case you do not need to perform the steps in this article, simply create the new sub-account and then configure the software on the new computer without moving the incremental backup cache).

3-5-1 System Status

The system status page allows you to control and monitor ongoing and previous backups, generate reports, and upgrade the software.

The status of currently running and previously run backups is displayed on one of the Backup Status tabs. You can also start, stop, pause, and resume currently running backups on these pages. Up to three backup status tabs will be visible, one for each possible backup destination. The remote backup status tab will always appear. Additionally, the local server and local disk backup status tabs will appear when you have properly configured these backup destinations on the My Account page.


Destination for Data

Remote Server: server.efoldering.com

Local Server: \\server\sharename\fold

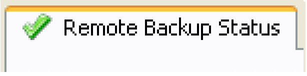
Local Disk: (optional)

The software provides the ability to view, save, email, and print reports showing the change of disk usage over time, a list of backed up files, and other information. All of this is accessible from the Reports tab.

The Software Updates tab provides the current software version information as well as the ability to upgrade the software.

3-5-2 System Status: Backup Status

Each of these tabs provide information about currently running and previously run backup jobs for one backup destination (remote backups, local server backups, or local disk backups). If the local server or local disk backups are not configured, then these tabs will not be visible (the Remote Backups Status tab is always visible).



Backup control and current backup status:

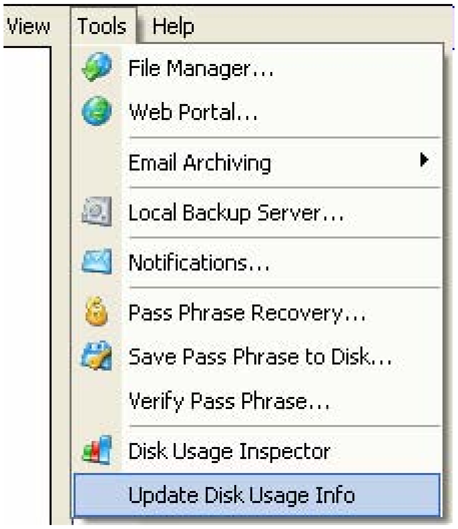
The top section of the page allows you to monitor and control currently running backups. If a backup is not running, then the group title text will indicate when the next backup for this destination is scheduled to run (if applicable). Also, the Backup Now button can be used to immediately start a backup.

If a backup is currently running, then the Backup Now button becomes the View Log button, which starts the log viewer and displays the log file for the currently running backup. Also, if the backup is running, the Interrupt button becomes active. You can click this button to show a menu that will allow you to cancel, pause, or resume the currently running backup.

NOTE: If you start a backup using the Backup Now button, it is safe to logoff and the backup will keep running. However, if you are running Windows 2000 (or earlier) then a backup started in this way will be canceled if you logoff (the software will also warn you about this when the backup begins with a balloon window). One possible workaround is to schedule a one-time backup using the Schedule page, and then to logoff before the one-time backup is scheduled to begin.

Disk usage information:

The middle section of this page displays summary information about the amount of disk storage that is in use for this backup destination for the backup account configured on the My Account page. This information is updated at the end of each backup or at the end of each file manager destroy data session. To force the information to refresh immediately, use the Tools -> Update Disk Usage Info menu command.



The section displays how much data is being used for current data, historical data, and deleted data. Current data represents the space required to store the most recent version of all files that have been backed up. historical data represents the space required to store the historical versions of all files that have been backed up (note that only the changes between versions are stored for historical versions, so you can efficiently store many versions of the same file). Deleted data represents files that were previously backed up, but then were later deleted from your computer, and are now being retained within the backup according to your backup settings (see the Versioning tab on the Options page).

You can reduce the current amount of data by editing your backup policies on the Folders page using Visualize! or the manual policy editor. After editing the policy on the Folders page, right click the folder on the Folders page and choose Destroy Excluded Data. Or you can turn on the Destroy Excluded Data option on the Versioning tab on the Options page.

You can reduce the historical and deleted amount of data by using the file manager to destroy historical versions and/or deleted files.

To view the details of which folders contain the most amount of data, use the disk usage inspector tool.

Backup logs:

The bottom section of this page contains a list of backup logs (and other logs), which contain the results of previously run backups and other operations (such as restoring data and destroying data). The Errors, Warnings, and OK columns summarize the number of error events, warning events, and "OK" events in each log file. An "OK" event is some action that completed successfully during the backup (e.g., a new version of a file was uploaded, a directory was scanned for changes, etc.). The OK column helps you estimate how many actions are required in order to complete a backup (for your configuration).

IMPORTANT: Any backup log with an error or warning in it should be reviewed. Logs with errors or warnings are highlighted in red and orange, respectively. However, if a future backup completes without warnings or errors (and the backup was not canceled), then any previous errors or warnings will have been resolved and you know that you have a good backup.

To view a log, double click the entry in the log list, or alternatively right click the log entry and choose View from the menu that will appear. Doing this will start the log viewer application, which will allow you to easily view, sort, filter, export, copy & paste, and email the contents of log files.

If you need help diagnosing backup problems or have another question, this section of the page provides quick access to our technical support team. The Help Me button on this page will show a dialog that will let you automatically gather any logs with errors or warnings in it and send an email to our technical support team. You should also type in additional information about the problem in the box provided on the Help Me dialog. You can also directly email specific logs by highlighting one or more logs and clicking the Email button.

NOTE: If you have trouble sending emails from this page, check the settings on the Notifications tab on the Options page.

Buttons are also provided to save one or more logs to a text file or for deleting old logs. Note that the software automatically .zips log files older than one week by default. This feature does not prevent the logs from showing up in the log list. Also, the log viewer application can directly open the zipped log files. The automatic zipping of log files is helpful in that it saves a lot of disk space for large log files (by a factor of 50 or more). The software will automatically delete old log files. You can customize log management behavior on the Backup tab of the Options page.

3-5-3 System Status: Reports

The reports tab lets you view, save, print, and email various kinds of backup reports. It also allows you to view on-screen historical disk usage graphs.

Report generation:

To view, print, save, or email a report, first choose the type of report you want to generate, and then choose the period of time for which the report should cover. Two types of reports are currently available:

- **Backup summary report**: This report summarizes your account information and service plan, your current disk usage, and the status of the last backup. It also includes information about your operating system, the software version, the list of folders being backed up, and your backup policies. It also includes a variety of historical disk usage graphs showing how your disk usage changed for the selected report period.
- **Backup details report**: In addition to the information contained in the backup summary report, this report also contains a list of all

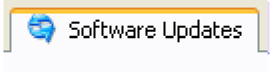
When a report is generated, an HTML file and a set of images is generated and then your default web browser is instruction to open the HTML file. If you are saving or emailing the report, it will .zip all relevant files into a single file. To view the zipped report, unzip the file, and then double click the HTML file to open the report in your web browser.

Disk usage graphs:

You can interactively generate graphs showing disk usage information over time using the lower section of this page. Use the drop down list to select the type of data that you want to graph, and you can customize the time period on the right. If you want to save a picture of the information, either use the top section of this page to generate a report for the same time period, or use a tool to capture a screen shot.

3-5-4 System Status: Software Updates

Our software-as-a-service business model means that you are always entitled to the latest version of the software at no extra charge. The software has the ability to automatically download and install software upgrades. By default, the software will download updates but will wait and ask you once per day whether or not you want to install the new version.



Check for and install new updates:

Use the Check Now button on this page to check for a new version of the software. The current version of the software is displayed in the top left corner of this page, and you can also check using the Help menu, About command.

(installed version is 3.6.2):

View history of updates:

A log is kept of the work performed by the software updater. Note that it is normal to see one or two error messages in the log, as your Internet connection may have been down temporarily when the software performed its daily check for new software versions. If you have problems updating the software, you can email the log to technical support.

Configure updates to automatically install:

If you are not using an Internet security product that restricts access to programs without user approval (e.g., your network is only protected by a perimeter firewall or you are using an inbound only firewall), then it is safe to configure the software to automatically install updates. Use the Advanced tab of the Options page to configure updates to install.

Tip: The reason that you may not want to configure the software to automatically install software updates is that some Internet security products (also called software firewalls) will treat a new version of the program as a completely new program, and will block the program's Internet access until you tell the Internet security product that the new version is allowed to access the Internet. Thus, if you are not aware that there is a new version of the program that needs to be approved in your firewall, your backups may start failing (until you tell your firewall to allow access). If you let the software wait until you confirm to install software updates, then updates will only be installed when you are at the computer. When a new version is installed, the software automatically tries to "ping" the Internet, in order to trigger your software firewall immediately so that you can immediately approve the new software version in your firewall.

3-5-5 Control Panel

The Control Panel page is used to start the most frequently used tools (additional tools are available via the Tools menu at the top of The Backup Software window).

The tools that you can start via this page are:

- **File Manager**: Use the file manager to view, restore, and destroy data located either in our secure data centers (for remote backups) or on your local backup medium (for local backups).

- **Web Portal**: This will open your web browser and allow you to login to our online web portal. The web portal allows you to view and change account information, view backup status reports, and use web access to download your data anywhere you have a compatible browser.

- **Pass Phrase Recovery**: When you configured your pass phrase (see the getting started guide) you can optionally choose to securely save the pass phrase onto the server. We highly recommend that you always keep a copy of your pass phrase printed out in a secure place and/or keep a copy in a file on a different computer (use the File -> Export Profile menu command). However, if you ever need to recover your pass using pass phrase recovery, this is the tool that will help you do it.

  Pass Phrase Recovery consists of two steps. You use this tool to perform both steps. In Step 1 the wizard helps you submit a request to recovery your pass phrase. At this point our senior level staff will be notified, and they will process the request. Once the request is processed, you will receive an email. At this point you can start the recovery wizard again and this time choose Step 2. In this step you will be presented with your security questions. If you can answer your security questions exactly, then you will be able to view and copy your recovered pass phrase.

- **Disk Usage Inspector**: This tool is useful to discover exactly which folders are taking up the most disk space in our data center or on your local backup medium. For each folder you can view how much data is taken up by just that folder, and also for that folder and all of its sub-folders. It also gives a breakdown of the data into current data, historical data, and deleted data. In this way you can quickly drill-down and find the folders that are taking up the most disk space.

Note: If the file manager, pass phrase recovery wizard, or disk usage inspector tools are already running, when you use this page to try and start the tool again it will instead bring the previously running instance of the tool to the foreground.

Tip: If you want to start several instances of the file manager (for example, in order to download several different directories concurrently instead of having them download one after another), then start the tool using the Windows start menu item instead.

3-5-6 My Account

The My Account page allows you to access and modify those variables that make each account unique. The use of the The Backup Software services is authorized through your account.

It's very important that each computer is configured to use a different account (otherwise, data with the same filenames could get mixed together, and backup monitoring and notifications will not work properly). You will receive a parent account for your first computer being backed up, and you will be provided with one additional sub-account for each additional computer you need to backup. New sub-accounts can be created instantly through the Web Portal.

Your data is secured through two distinct things: your account password, and your pass phrase:

- **Account Password**: This is what authorizes you to login to your account and upload or destroy data. The account password can be reset if needed by our support team.

- **Pass Phrase**: The pass phrase is used to define the encryption key that encrypts your data (we use the PBKDF2 algorithm to convert the pass phrase into a 256-bit encryption key). You configure the pass phrase only one time when you initially configure your backups. Once the pass phrase has been configured, it should not be changed. (If you change your pass phrase, all of your data must be backed up again.)

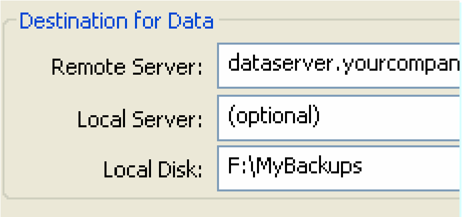
  It is very important that you know your exact pass phrase. Without your pass phrase you will not be able to recover your data. Once you have configured your pass phrase, you can use this page to export your pass phrase to a file or securely re-save it to our data center.

This page allows you to configure your where the data is backed up to, configure your account credentials, and set or save your pass phrase.

Configure Data Destination:

If you are only performing remote backups, then normally this section does not need to be customized. The remote backup server name is the network hostname or IP address. If you need to route remote backup traffic on a different TCP port other than 443, then you can add ':5470' to the end of the remote backup server name and it will try to connect on port 5470 instead of 443. The system will only use ports 443 and 5470.

This section can also be used to configure local server or local disk backups. Local disk backups can be used to also backup your data directly to some filesystem location (such as a USB disk or network share). Local server backups are useful for more complex environments where you need to securely route local backup traffic over your IP network using our custom network protocol.


Destination for Data

Remote Server: dataserver.yourcompan

Local Server: (optional)

Local Disk: F:\MyBackups

The local server field accepts a network hostname or IP address or a computer that is configured to run the local backup server. The local disk field accepts a filesystem path (such as F:\MyBackup or \\server\sharename\folder). Once you have something configured in the local server or local disk backup fields and you save your changes, then additional tabs will appear on the Schedule page and System Status page.

NOTE: If you configure local backups, be sure to choose whether or not you want to encrypt local backup data at the bottom of this page.

Configure Account Credentials:

In the middle section of this page you enter your username and password. If your password is a temporary password, then it will ask you to change your password. You can also use the Change Password button to change your password. If you have forgotten your password, our support team can reset it for you.

IMPORTANT: Each computer (or settings profile) should be configured with a different username. Otherwise, data with the same filenames could be mixed together, and backup monitoring and notifications won't work correctly.

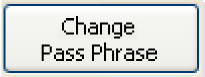
Set, Save or Change your Pass Phrase:

In the bottom section of the page you can create, export, and verify your pass phrase. You also choose whether or not you want to encrypt data that is backed up to the local server or local disk.

Configuring your pass phrase is the most important part of the configuration process. Please see our getting started guide for a walkthrough of how to properly configure your pass phrase.

Once data has been uploaded under a given pass phrase, you will not be allowed to use a different pass phrase on that account until our support department has reset the "pass phrase lock" on your account. This feature provides protection against accidental or malicious changing of the pass phrase without the account owner's knowledge. It avoids the situation where you have to restore your data only to find out that someone else changed your pass phrase without your knowledge.

If you want to intentionally change your pass phrase, please contact us to have the change of pass phrases approved. Once the change has been approved, you can use the Change Pass Phrase button to change to a new pass phrase. Note that this will schedule a full backup so that all of your data will be uploaded with the new pass phrase. To avoid keeping two copies of your data, we recommend first destroying all of your data before changing your pass phrase (or you can ask support to create a new account for you and delete your old one).



If you have already configured your pass phrase and want to securely save it to the server again (for example so you can setup different security questions for pass phrase recovery), then click Change Pass Phrase but then enter your current pass phrase. (You may want to use the Verify button to verify that you know your existing pass phrase correctly before you do this.) If you enter your same pass phrase correctly, the software will not warn you that you are changing your pass phrase, but instead will proceed directly to the security questions and answers dialog. When you re-save your pass phrase to the server in this way it will not interrupt your incremental backups (a new full backup is not required).

Use the Verify button to check that you know your exact pass phrase at any time. This button will show a dialog that lets you type in a pass phrase. It will automatically highlight in green or red whether or not the pass phrase that was typed in matches the pass phrase that is being used to backup your data.

If you want to save your pass phrase to a file for safe keeping, this can be done in two ways: first, you can use the Save button on the bottom section of this page to save your pass phrase to a text file. Note that this text file will only contain the binary form of your pass phrase (see note below). Alternatively, you can use the File -> Export Profile menu command to save your pass phrase and all of your settings to a file.

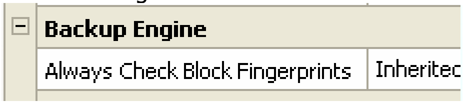
NOTE: The actual text of your pass phrase is not stored in the software settings. Rather, the software stores the "binary" form of your pass phrase (it stores a cryptographic hash of your pass phrase). This ensures that if you used any sensitive information in your pass phrase (such as your social security number) that information will not be stored on your hard disk somewhere. The binary form cannot be converted back into the text of the pass phrase, so any sensitive information is not exposed. For details, please search the Internet for information about the PBKDF2 standard.

3-5-7 Folders

The folders page is where you configure what you want to backup.

The Backup Software operates by taking each top-level folder in the folders list and scanning all files and in the directory specified by that folder's path (as well as in all of its subdirectories). The backup policy for that top-level folder determines if each scanned file is included or excluded in the backup. If any file that the policy includes in the backup set has changed since the last backup, then the software will upload and store the changes to that file.

IMPORTANT: The Backup Software uses the modification date and time of the file to determine if the file has changed since the last backup. Certain server software packages, such as Microsoft Exchange and SQL server, do not update the modification date of the file even though they are writing data to the file. In general this is true for any application that will keep a file open without re-opening it for days, weeks, or even months. If you are going to backup this kind of data, you need to turn on the Always Check Block Fingerprints option in the properties for the folder(s) that contain this kind of data (right click the folder, choose Properties). Note that our software will normally detect automatically when to use this technique for Exchange and SQL server, but for other types of data that keeps files open all the time you will need to turn this on manually. Please refer to our knowledge base for more information.

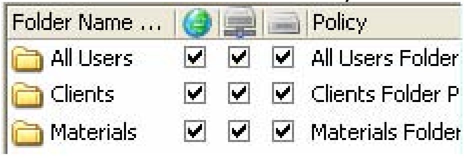


⊟ Backup Engine	
Always Check Block Fingerprints	Inheritec

Folder list:

The main feature of the Folders page is the folder list. This contains a list of all top-level folders in your backup. For each top-level folder the list displays the name of the folder on the remote server, the backup policy assigned to that folder, and the path of the directory where The Backup Software will start to look for data to place into this folder on the remote server.

The list also contains three columns that each contain a checkbox -- one column for each data destination (the columns are in the following order: remote backups, local server backups, local disk backups). You can easily exclude a top level folder from a particular backup destination by unchecking the appropriate box for that particular folder. Please note that Visualize! is not affected by the state of these checkboxes.



Folder Name ...				Policy
All Users	☑	☑	☑	All Users Folder
Clients	☑	☑	☑	Clients Folder P
Materials	☑	☑	☑	Materials Folder

Backup policies:

Each folder is assigned its own backup policy. A backup policy is a set of rules that either exclude or include a file based on its filename, filesize, or modification date. There are also rules that apply to another policy. Each policy also includes a rule to apply the default policy, so if you want to add an exclusion that applies to all folders, you should edit the default policy. Policies can also be used to customize versioning settings and other properties for individual files or files that match a policy rule. See below for more details on how to edit policies.

If you have local backups configured in addition to remote backups, then you can easily add rules to a policy that are specific to remote backups, local server backups, or local disk backups. This is accomplished through sub-policies. A sub-policy first includes the main policy it is associated with, and then it contains a list of additional rules that should be applied. Each policy contains three sub-policies (one for each backup destination). When local backups are configured, when you choose to edit a policy or you Visualize!, then it will show a menu so that you can choose to edit the main policy for all backup destinations, or whether you want to edit the sub-policy for a specific destination.

Strategies for data selection:

There are a few strategies for determining which top-level folders to add to the Folders page. One strategy is to just add the root of each drive (e.g., X:\) or network share (e.g., \\server\sharename) and then use Visualize! or the policy editor to exclude those folders and files that you don't want to include.

Another strategy is to add only those top-level folders that include just the data you are interested in backing up. For example, if all of your documents for all of your users were located in subdirectories off of the C:\Users folder, then you would add C:\Users as a top-level folder. Or for example, if you want to backup a Microsoft Exchange information store, then you would add the MDBDATA folder as a top-level folder. This has the advantage that it is easier to customize versioning settings for a given set of data, and also it is easier to move the location of a top-level folder if that is ever necessary.

The strategy where you add the root of a drive or network share has the advantage that it is easy to setup policy rules to backup based on file type (e.g., search-based backup). However, the disadvantages are that if certain subfolders on the drive have to be moved to a different drive (e.g., X:\Users is moving to Y:\Users but everything else on X:\ is remaining the same) then the data will have to be backed up again, because you can only move the locations of top-level folders but you cannot move the locations of subdirectories within a top-level folder.

In general, the second strategy is preferred over the first strategy, as it provides more flexibility and greater efficiency.

Adding folders:

You can either use the Add button or the Visualize! button to add new top-level folders to the list. When you click Add the software will display a dialog showing your filesystem in the left pane and the folder list on the right pane. In the left pane any files currently in the backup set will be highlighted in green. Note that in this dialog, the coloring will not be red if you have excluded a file or folder (to see this, use Visualize! instead of Add). You can also use the edit box in the lower left-hand corner to manually type the path of the folder you want to add (this is the easiest way to add a UNC network path).

TIP: If you have setup email archiving, then when you click the Add button instead of showing the dialog immediately, you will be presented with a menu, where you can choose to add a normal folder (which will show the add dialog as usual) or you can choose to add one of your email archives. This is the best way to add your email archives to the folder list, as it will automatically edit the backup policy of the archive to exclude duplicate messages.

Alternatively, you can use the Visualize! feature to add folders to your list -- start Visualize! and then simply check the top-level folder that you want to add.

Customizing properties for folders:

You can customize settings that affect the backup (such as file versioning settings) for a particular folder by right clicking on the folder and choosing Properties. This will display the properties editor window. The left pane of this window shows you which set of properties that you are editing. By default when you open the window you will be editing the set of properties for the folder that you had selected. You can also change this to be editing the properties of the policy or the global properties (which you can also changes on the Options page).

Properties are inherited and can be refined for a particular policy or folder. For example, all folders by default will have all of their properties set to Inherit. This means that the actual value of the property is the value of the next-higher property set in the chain of properties (the order from highest to lowest goes: Global, Policy, Folder).

For example, if you wanted to keep 2 years worth of versions for all of your data, but then only keep 14 days of versions for your Exchange server information store, you could right click the folder containing your Exchange information store, choose Properties, and change the Numbers of Days to Keep Historical Versions from Inherit to 14.

In the properties editor if you want to change the value back to Inherit then:

- For textboxes, delete all of the characters from the box and press TAB.
- For checkboxes, keep clicking the box until it changes to Inherit.
- For dropdown listboxes, choose Inherit from the list of choices.

If you have local backups configured, then you can choose to customize the properties of a folder for a particular backup destination. For example, you could choose to store two years worth of historical versions for all backup destinations, but then customize the remote backup destination so that it only retained 14 days worth of historical versions. This allows you to store more copies of your data on less expensive local storage, while only what is necessary remotely.

Visually editing backup policies (Visualize!):

You can graphically see and edit your backup policies using the Visualize! button. Visualize! is useful for three tasks:

- For excluding certain folders or filetypes from your backup
- For tallying up the total amount of current data that is in the backup set
- For quickly verifying that any manual changes to a backup policy are correct

When you press the Visualize! button it brings up a dialog showing an explorer-type view of your filesystem, as well as an informational pane at the bottom of the window. Within the view of your filesystem, each folder or file will take on one of three colors:

- Gray: This color indicates that the folder or file is not included in any of your top-level folders. You can check the box to the left of a gray folder to add it to your list of top-level folders.
- Green: This color indicates that the folder or file is included in your backups.
- Red: This color indicates that the folder or file is included in one of your top-level folders, but it is excluded from the backup because of a policy rule.

To include an excluded file or include an excluded file, right click the file of interest and use the appropriate include or exclude commands from the popup menu. It will present you with different rules that you could add based on different possible patterns derived from the filename of the file that you right click (for example if you right clicked a file named classic.mp3, then it would let you add a rule to exclude just classic.mp3, *.mp3 (all mp3 files), classic*.mp3, etc. Also, the rule can either be just for that folder (e.g., only for that one directory that contains the file that you right clicked and not any of its subdirectories or parent directories) or for all folders (in which case the rule will apply to all directories within the top-level folder that contains that file). It will also allow you to add a custom rule, in which case it will bring up a window allowing you to edit the new policy rule.

You can also include/exclude files by checking or unchecking a file or folder. When you do this the software will bring up a window allowing you to customize the policy rule that it is going to add. If you only want to quickly exclude the one file or directory that you check or uncheck, then you can hold down the ctrl key while you click and it will skip the rule customization dialog.

TIP: If you want to exclude or include certain files or kinds of files in all top-level folders, then you should use the manual policy editor to edit the default policy (see below). Also, if you need to exclude or include certain files based on criteria other than the filename, you will need to use the manual policy editor.

Visualize! also provides for unlimited undo and redo -- if you make a mistake, right click the window and choose Undo to undo the last change. Likewise the Redo command will re-apply the last change that you undid. You can Undo and Redo an unlimited number of times. This allows you to experiment with tricky policy rules until you get exactly what you want.

The bottom part of the window displays detailed information about the currently selected folder or file, indicating which top-level folder(s) contain the folder or file, as well as which policy rule caused the file to be included or excluded. If you are having trouble determining why a file is included or excluded, left click the file to select it, and then look to see which policy rule is affecting that file.

The bottom part of the window is also used to display an estimate of the total amount of current data that is in the backup set. This is calculated in the background while the window is open. As this background process discovers information it will populate the Data to Backup and Excluded Data columns in the list.

TIP: If you include or exclude files after you open the Visualize! dialog, then you will need to tell the software to recalculate the disk usage amounts once you are finished making changes. You do this by right clicking the window and choosing the Refresh Disk Usage command. This will update the grand totals as well as the individual totals in the Data to Backup and Excluded Data columns.

NOTE: The Visualize! dialog does not display how much data is actually stored on the remote server. It does help you understand how much data will need to be uploaded for the initial backup, and once your initial backup has finished, the total amount of data in Visualize! should closely match the amount of current data in your account. The actual amount of data that is stored on the server can be understood by using the Reports tab of the System Status page, as well as the disk usage inspector tool.

Manually editing backup policies:

The manual policy editor is the most powerful way to configure policies but it is also the most complex. To edit a policy, right click a folder and choose Edit policy. If you have local backups configured, this menu will let you choose whether you want to edit the main policy for all backup destinations, or whether you want to edit a sub-policy for one specific destination.

TIP: To edit the default policy, right click and Folder and choose Edit policy, then highlight the Apply Default Policy rule, and click the Edit Default Policy button in the lower-right hand side of the window.

The policy editor window has the functionality to edit, export, and import the backup policy for a particular top-level folder. The top-level folder that you are editing is displayed at the very top. Immediately below this is a dropdown list indicating which policy should be used when backing up the top-level folder. Normally, each top-level folder is assigned it's own backup policy. Buttons to the right of the policy list allow you to add a new policy, delete a policy, rename the policy, export the policy to a file, or import a policy from a file.

The main portion of the window is composed of the rule list on the left and the rule editor on the right. The rule editor allows you to edit the currently selected rule in the rule list.

When a policy is applied in order to determine whether a file or folder should be backed up, the rules are applied from top to bottom. This means that rules at the bottom of the list will override rules at the top of the list. So if you wanted to exclude all music files (*.mp3) but then include all MP3s in the Recordings folder, then you would want to put the include rule for the Recordings folder below the exclude rule for *.mp3.

There are two types of rules: wildcard rules and apply policy rules. Wildcard rules are used to exclude or include files or folders based on a file's name, size, or modification date and time. Apply policy rules are used to apply all of the other rules in another policy. By default every policy will also apply the Default

Policy, allowing you to easily exclude certain files from all top-level folders by editing the default policy.

After you edit your policy, we strongly recommend using Visualize! to verify that your policy rules are working as expected.

Wildcard rules:

A wildcard rule is used to either include or exclude files and folders matching certain criteria. Use the dropdown at the top of the rule editor to change whether the rule will include or exclude files and folders. The dropdown list to the immediate right of the include/exclude dropdown indicates whether the rule will apply to both files and folders, just folders, or just files.

Wildcard rules match on either the relative path or absolute path of a file or folder. The absolute path is simply the filesystem path you would normally use to open a file. The relative path is the remaining path after the path of the top-level folder is excluded.

For example, say that you had a top-level folder "Users" that was backing up the C:\Users folder, and you wanted to add a rule that excluded the C:\Users\MusicFan\My Music folder. The absolute path would be C:\Users\MusicFan\My Music. The relative path would be \MusicFan\My Music since this is the part of the path that comes after the path of the top-level folder (C:\Users).

Visualize! will usually add wildcard rules that use relative paths. Relative paths are more robust because if the location of the top-level folder changes the policy rule will not need to be changed (this is not true for absolute paths). Note that if you are creating a rule that will apply to files in any folder (e.g., "*.mp3") then it does not matter whether you use an absolute path or a relative path.

The textbox on the third line of the rule is where you actually type the wildcard pattern. The * character matches any number of any characters. The ? characters matches exactly one of any character. The * and ? can also be used in conjunction with the directory separator character (either \ or /) to create powerful and precise patterns. Here are some guidelines and examples (in the example, c:\Users is the path of the top-level directory):

- The pattern "abc*" will match files or directories that start with abc and that have any file extension.

- The pattern "*.txt" will match all files or directories that have a file extension of "txt"

- The pattern "*.*txt" will match all files or directories that have a file extension that ends with "txt"

- The pattern "abc*.*txt" will match all files or directories that start with abc and have a file extension that ends with "txt"

- The pattern "*20??.dat" would match "abc-2000.dat" and "abc-2010.dat" but it would not match "abc-20100.dat"

- A pattern that starts with "*\" or that contains "*\" will match any number of directories (one or more levels of directories). For example, "*\My Music" will match files in any My Music directory no matter how deeply nested it is (e.g., it would match all of the following: C:\Users\My Music, C:\Users\MusicFan\My Music, C:\Users\MusicFan\My Documents\My Music, etc.).

  As another example, "*\Classical*\Beethoven" would match both:
  "C:\Users\MusicFan\My Music\Classical\1800-Favorites\Personal\Beethoven" as well as
  "C:\Users\MusicFan\My Music\Classical\1800-Archive\Beethoven"

- If you have one or more non-star characters, followed by a * and then a directory separator (or you have a * followed by one or more non-star characters followed by a directory separator), this will match exactly one directory level. For example, "*\Classical\1800-*\Beethoven" would match
  "C:\Users\MusicFan\My Music\Classical\1800-Archive\Beethoven"
  "C:\Users\MusicFan\My Music\Classical\1800-Favorites\Beethoven"

but it would not match
"C:\Users\MusicFan\My Music\Classical\1800-Favorites\Personal\Beethoven"

- This principle also applies to the use of the ? character. If you want to include any directory name but you only want it to match one directory and no subdirectories, then use "\?*\".

  For example, "*\Classical\?*\Beethoven" would match:
  "C:\Users\MusicFan\My Music\Classical\1800-Archive\Beethoven"
  "C:\Users\MusicFan\My Music\Classical\1800-Favorites\Beethoven"
  but it would not match
  "C:\Users\MusicFan\My Music\Classical\1800-Favorites\Personal\Beethoven"

We highly recommend testing complex rules using the Visualize! feature before backing up to make sure that they are worked as you would expect them to.

In addition to specifying a wildcard pattern, you can also use matching criteria based on a file's modification date and time (either relative to the current date and time when the backup is being processed or an absolute date and time).

If you are adding an exclude rule in order to exclude files that were backed up previously and you no longer want to back them up, then you should check the Destroy files excluded by this rule option. This indicates that any files that were previously backed up but are now excluded by this rule should be removed from the backup. You can turn this option on for all policy rules by using the Versioning tab of the Options page or by editing the folder properties.

If you are confident that a particular folder will never contain any files that need to be backed up, then you can increase the efficiency of the backup by adding an exclude rule and turning on the Rule cannot be overridden option. This indicates that if this rule matches a file or folder, and rules below this rule in the rule list will be ignored. If you use this to exclude a directory, then the backup will not even check inside the directory for files and folders that might be part of the backup -- it will immediately skip the directory instead.

Use the Rule cannot be overridden feature with caution. For example, if you exclude the C:\Users\Archive folder and enable this option for that rule, but then add an include rule for *.doc, any *.doc files in the C:\Users\Archive folder will not be backed up because the exclude rule for the Archive folder cannot be overridden.

Finally, if this wildcard rule is an include rule, then the Change Backup Settings for Rule will be active. This is used to customize the backup properties for files matching this wildcard rule. See more details about this feature below.

Apply policy rules:

An "Apply policy" rule is used to include all of the other rules in some other policy in this policy. This is used by default to include all of the rules from the Default Policy in each top-level folder's backup policy. Note that it does not include the first rule from the referenced policy if the rule is "include *.*" or "exclude *.*". For example, even though the first rule of the default policy is "Include *.*" this rule is ignored and it will not affect any exclude rules you have before the "Apply Default Policy" rule.

You can use the Edit ... Policy button to actually edit the rules of the referenced policy. The easiest way to edit the default policy is to therefore edit any policy, highlight the 'Apply Default Policy' rule, and then click this button.

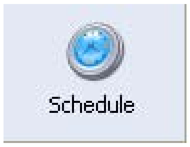
As an advanced option, you can choose to only include the exclude wildcard rules or the include wildcard rules from the referenced policy. Also, you can indicate that you want to invert the meaning of these rules (meaning exclude rules become include rules and vice versa). These options are advanced and should not normally be changed.

Customizing properties for files matching a policy rule:

Wildcard rules can also be used to override folder properties (such as versioning settings). This is accomplished by adding an include wildcard rule matching the folders and files that need the customized properties, and then by clicking the Change Backup Settings for Rule button at the bottom of the rule editor (if the button does not appear, please move your mouse over the area and/or resize the window -- sometimes the controls do not refresh correctly and the button is not visible until you move your mouse over it). Clicking this button will bring up the properties editor window, allowing you to override the folder properties for files matching this include rule. Note that the button is disabled for exclude rules, because the properties only affect files that are backed up.

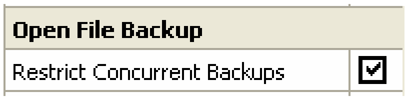
3-5-8 Schedule

This page is used to set the backup schedule for remote backups, local server backups, and local disk backups.



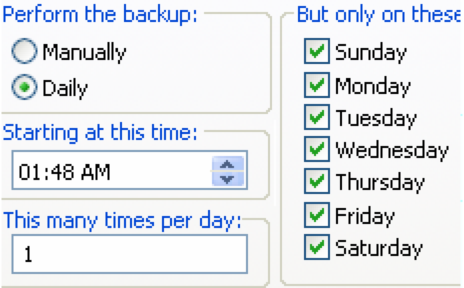
There is one tab across the top for each backup destination. If a particular destination is not yet configured on the My Account page, then the tab for it will be hidden.

If you are performing both local backups and remote backups, then we recommend scheduling the local backup to start one to three hours before the remote backup is scheduled to start. Certain operating systems (Windows 2003 or better and Windows Vista or better) do allow you to backup remotely and concurrently at the same time; however, we recommend that in most cases it is better to have the local backup run first. If you are backing up Microsoft Exchange, then the backups must not run concurrently. To enforce this, change the Restrict Concurrent Backups option on the Backup tab of the Options page to be set to checked (Yes).



Open File Backup	
Restrict Concurrent Backups	☑

Scheduled backups can be disabled by changing the setting to backing up Manually. Otherwise, use the Weekly option to backup one or more times per week (the default is to backup every day). Unless you have good reasons for not backing up every day, we recommend daily backups, as the backup is able to best optimize for performance on a daily schedule. The first time you come to this page for a particular backup destination it will suggest a random time for daily backups between 7pm and 5am.



Perform the backup:
○ Manually
● Daily

Starting at this time: 01:48 AM

This many times per day: 1

But only on these
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

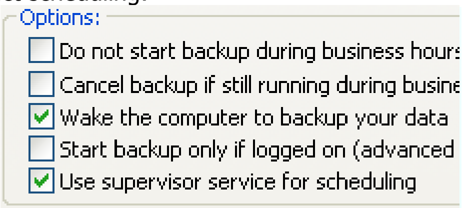
You can indicate how many times who would like to backup every day. If this is more than 1, then it will evenly divide 24 hours by the number of times to backup, and then schedule a backup that often starting at the backup time. For example, if you indicate to backup 3 times per day starting at 6:30pm, then it will schedule backups for 6:30pm, 2:30am, and 10:30am.

Note: If you are backing up individual files that are individually larger than 10 GB, we recommend only backing up once or twice per day, with the best time to start the backup being in the early evening hours.

If you need to schedule a backup to start on a particular date and time in the future, then you can use the

Set and Clear buttons in the Schedule a one time backup control group to do this.

There are three options that affect scheduling:



Options:

- ☐ Do not start backup during business hours
- ☐ Cancel backup if still running during busine
- ☑ Wake the computer to backup your data
- ☐ Start backup only if logged on (advanced
- ☑ Use supervisor service for scheduling

- Wake the computer to backup your data: If this option is checked, then a Windows task scheduler task will be created that will be triggered at the appropriate times to ensure that your computer wakes up from standby, if necessary. Note that if your computer has been put into hibernation it will not be able to wake up your computer. If your computer is always on (e.g., because it's a server) we recommend leaving this unchecked.

- Start backup only if logged on: If a Windows task scheduler task is needed in order to schedule the backup (either because you are waking up the computer to backup your data or you are not using the supervisor service for scheduling), then normally it will ask you for your Windows password so that the Windows task scheduler can log you on if you are not logged on when the backup needs to begin. However, if you don't have a Windows password, or you don't want to enter your password, then check this option. It will allow you to continue without entering a password, but when it's checked it also means that the backup will not be able to start if you are not logged in.

- Use supervisor service for scheduling: If this is checked, then %$CLIENT_NAME% will use a Windows service instead of the Windows task scheduler to actually start the scheduled backup. In general we have found that the Windows service is more reliable than the Windows task scheduler in starting backups. However, if you are running a version of Windows older than Windows 2000 or you have specialized scheduling needs, then it may be necessary to rely solely on the Windows task scheduler for starting scheduled backups.

3-5-9 Options

This page allows you to configure options that affect all backup destinations (remote, local server, and local disk backups).

Navigate to different categories of options by using the tabs across the top. The following option categories are available:

- Notifications
- Versioning
- Backup
- Bandwidth
- Advanced

3-5-10 Options: Notifications

The Notifications page configures when you should receive backup-related email notifications, to whom the emails should be sent, and how the emails should be sent.

Normally you only need to configure the Notifications sub-category. However, if the software has trouble sending email, you may need to configure the SMTP server settings in the Outgoing Email Configuration subcategory.

- **Notifications**

  - Email Address:
    Where notifications should be sent. Separate multiple addresses with a semicolon (;). Normally you can leave this blank, in which case it will use the email address associated with your account in the web portal. This has the advantage that the notification email address can be updated from the web without having to change the settings in the backup client.

  - Email Format:
    If your email reader supports HTML, choose one of the email formats. If your email reader does not support HTML or you prefer smaller emails, choose the plain text format.

  - Action on Start of Backup:
    What to do when a backup starts. For this setting and the other action settings, this can be one of the following:

    Do nothing -- you will not be notified

    Notify me with a balloon window -- a small window will appear for a few seconds by the tray area of your taskbar informing you of the event

    Notify me and send me an email -- in addition to showing the balloon window, it will send you an email, but it will not attach the actual backup log

    Notify me and send me an email with logs -- the same as the above, but it will also attach the full backup log (possibly zipped)

  - Action on Successful Finish:
    What to do when the backup ends with 0 warnings and 0 errors.

  - Action on Finished with Warnings:
    What to do when the backup ends with some warnings and 0 errors.

  - Action on Finished with Errors:
    What do do when the backup ends with some errors.

  - Last Backup Quick Alert:

After you unlock your computer or your screen saver is deactivated the backup manager can show a quick alert balloon window showing the status of your last backup. It can be configured to only show this alert once per completed backup, not at all, or every time you unlock your computer or deactivate your screen saver.

- Balloon Window Duration:
  How long balloon windows should remain visible (in seconds).

- **Outgoing Email Configuration**

  - Minimum Zip Size:
    When sending emails, if any attached backup logs are larger than this amount (in KB) then it will automatically .zip the log file before attaching it.

  - Send via local SMTP Server:
    Enable this option if you want to send via your own mail delivery server (SMTP server).

    - SMTP Server Address:
      The network hostname of the SMTP server to use. If you need to use a TCP port other than port 25, use the syntax: hostname:port

      For example: smtp.myisp.com:465

    - SMTP User Name:
      If your SMTP server requires authentication, specify your SMTP username.

    - SMTP Password:
      The password associated with the user in the SMTP User Name field.

    - SMTP Connection Security:
      Certain SMTP servers require network communication to be encrypted (through TLS or SSL). In most cases the Automatic setting is best. This determines what type of connection security to use:

      Automatic -- If you connect to port 25, it will not use TLS/SSL. If you connect to port 465, it will immediately start a TLS/SSL connection. If you connect to some other port, it will negotiate for a TLS/SSL connection using the STARTTLS command.

      Normal -- It will never try to form a TLS/SSL connection.

      Secure connection -- Same behavior as Automatic, except that it requires a TLS/SSL connection on port 25 through the STARTTLS command.

      Force immediate TLS/SSL -- Upon connecting it will immediately attempt to start a TLS/SSL connection.

      Force negotiation of TLS/SSL -- It will require a TLS/SSL connection through the use of the STARTTLS command.

    - POP3 authenticate before SMTP:
      Instead of requiring a username and password, some SMTP servers require that you login to a related POP3 server immediately before using the SMTP server.

      - POP3 Server Address:
        The network hostname of the POP3 server. If you need to connect on a TCP port other than 110, use the syntax: hostname:port.

      - POP3 User Name:

        The username to login with. Typically this is your email address (or just the first part of it).

    - POP3 Password:
      The password associated with the POP3 User Name.

    - POP3 Connection Security:
      Similar to the SMTP Connection Security setting, except that port 110 is the 'unencrypted' port instead of port 25 for the Automatic setting.

- Send via Direct SMTP:
  If this is enabled, the software will try to connect directly to the destination mail server of each recipient and deliver the mail directly. Normally this method is successful, although some mail servers will mark the mail message as spam if you have a dynamic IP address.

- Send via MAPI:
  These options are strictly for backwards compatibility and should normally not be used. Most MAPI compatible mail clients will not allow programs to send email without first confirming each message with you every time a message is sent.

    - MAPI Profile Name: See your email software vendor for the appropriate value.
    - MAPI Profile Password: The password associated with your MAPI profile.

3-5-11 Options: Versioning

The Versioning page is used to configure how much historical and deleted data is retained. It also determines whether or not files that were previously backed up (but are now excluded) are automatically destroyed.

The settings here can be overridden for a particular folder, file type, or file on the Folders page.

- Limit Number of Versions to Store:
  If this is checked, then The Backup Software will automatically destroy older historical versions that should not longer be retained. If this is unchecked, then all historical versions will be kept forever.

  - Number of Days to Keep Historical Versions:
    This indicates that all historical versions generated within the last N days should be retained. For example, if this set to 365 and a file changed once per week, it would retain no more than 52 historical versions of that file. Normally this setting is the only setting that needs to be adjusted in this section.

  - Minimum Number of Versions to Keep:
    This indicates that this number of historical versions for each file should always be retained even if the historical version is older than what the Number of Days to Keep Historical Versions allows for. For example, if you were keeping 365 days of versions, and a file changed twice per year, then normally there would be only 2 historical versions retained for that file. If you wanted to ensure that no matter what there were always at least 4 historical versions retained for any file, then you would set this setting to be 5 (4 historical versions + the current version). This is an advanced setting and typically does not need to be changed.

  - Maximum Number of Versions to Keep:
    This setting overrides the previous two settings. It indicates that for each file there should never be no more than N versions of the file (including the current version). If this is set to -1 (the default), then when to destroy old versions of a file is determined solely by the Number of Days to Keep Historical Versions setting.

    Caution: If this setting is not -1, then it may not be possible to restore some files to a point in time in the past, even if that point in time is more recent than the point in time window dictated by the Number of Days to Keep Historical Versions setting. This is because historical versions of a file may be destroyed sooner than they would otherwise be because the file is changing too frequently and thus exceeds the maximum number of allowed versions before it exceeds the time limit imposed by the Number of Days to Keep Historical Versions setting.

    This is an advanced setting and typically should be left at -1. It is normally only used on folders that contain data that changes on a regular basis, for example a folder where all files in the folder change once per day, etc.

- Destroy Deleted Files:

This indicates how often the software should check for deleted files that are too old (according to the setting below) and should be permanently removed from the backup. We recommend leaving this set to Weekly.

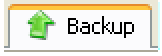
  - Number of Days to Keep Deleted Files:
    This is how long files that are backed up and then deleted off of your local computer should be retained for. The software will automatically synchronize this setting with the Number of Days to Keep Historical Versions setting. Keeping this setting synchronized ensures that you can do a true point-in-time restore and restore to any point N days in the past (where N is the value of both of these settings), because files that were deleted less than N days ago are still able to be restored at the point in time more than N days ago. Only change this setting manually if you are sure you want to retain deleted files for a shorter period of time.

    Typically you only change this setting for specific folders by editing the properties for a specific folder on the Folders page.

- Destroy Excluded Files:
  Indicates whether or not files that were previously backed up but are now excluded from the backup (because of a rule in the backup policy) should automatically be destroyed on the remote server. Turn this setting on if you want to automatically remove from the backup any data that is shown in red on the Visualize! dialog. We recommend using Visualize! to double-check your backup policies before turning this on.

3-5-12 Options: Backup

The settings of the Backup page allow you to adjust the behavior of the backup engine.



Use these settings to fine tune performance, configure open file backup (VSS enabled) advanced settings, configured actions to happen before and after the backup (or before and after the volume snapshots are taken), and to adjust the management of log files.

- **Shutdown/Restart Behavior:**
  - Backup on Logoff or Shutdown:
    If this is checked, if you try to logoff or shutdown the computer and the The Backup Software is running then it will cancel the logoff or shutdown, run a backup, and then re-initiate the logoff or shutdown.
  - Delay Shutdown to Finish Backup:
    Whether or not to delay a shutdown or reboot of the computer. If this is set to Yes then if the backup is running when the system tries to logoff, shutdown, or reboot, it will delay this until the backup finishes. If this is set to No or Auto then the backup will instead be immediately canceled and it will automatically schedule a one-time backup job 10 minutes in the future, so that the backup can continue where it left off as soon as the system is back to a normal state.
- **Email Archiving:**

  NOTE: These category will only appear if you have installed email archiving and you are switched to the primary settings profile (the first profile that appears in the list in the switch profile dialog).

  - Deduplication Schedule:
    How frequently duplicate messages in the email archive(s) should be scanned for and deduped. The deduplication process will always initiate on a Saturday morning. If you would like to setup a custom schedule, set this to Never and then use the Windows task manager to start the backup software program with the /deduparchives command line switch.
- **Exchange Server:**
  - Full Path to eseutil.exe:
    If you are backing up Exchange information stores then The Backup Software can use the eseutil Exchange program to verify the integrity of your information store before it backs it up. (This is recommended by Microsoft and is helpful in catching silent data corruption on your local hard disk.) Normally the location of eseutil.exe can be found automatically, but sometimes you have to manually specify where it can be found.

    If you don't see the Verify Database Files option on the folder properties page, then you need to manually specify the path to eseutil.exe using this setting.

- **ShadowProtect:**

    - Full Path to sbrun.exe:
      If you are backing up StorageCraft ShadowProtect bare-metal backup images, The Backup Software can verify the correctness, integrity, and completeness of these backups. To do this, it needs to know where ShadowProtect is installed. If you have installed it within a standard location, it will be automatically detected. Otherwise, you will need to use this setting to indicate the directory that contains the sbrun.exe file that is installed as part of ShadowProtect. Once the location of ShadowProtect is identified, new integration options will become available in the properties for folders on the Folders page.

- **Backup Session:**

    - Number of Retries for Entire Operation:
      If a transient error (such as a network failure) is experienced during the backup, the backup will continue to try up to this many times before giving up and logging a failure. In this way, the backup jobs will do their best to overcome any temporary conditions and always complete a fully successful backup.

    - Number of Retries for Individual Files:
      This is the number of times an operation should be retried for transient errors that are specific to individual files (such as an open or locked file when not using open file backup).

    - Number of Resume Retries:
      This is the number of times that the backup will attempt to resume an operation after experiencing a transient error in the middle of backing up a file. If you are backing up really large files, we recommend setting this value to be the same as the Number of Retries for Entire Operation setting.

    - Delay Between Retry Attempts:
      After a transient failure (network failure, etc.), the software will wait this many seconds before retrying the last command.

    - Worker Thread Priority:
      This is the process priority that should be used for backup jobs. We highly recommend keeping this set to Below Normal or Low, as it does not significantly affect backup performance but it does help with system responsiveness.

    - Use Low Priority I/O:
      On Vista (or better) and Server 2008 (or better) the OS can treat IO from different processes with different levels of priority. If you are using a laptop and prefer system responsiveness instead of maximum backup speed, try enabling this option.

- **Open File Backup:**

    - Restrict Concurrent Backups:
      If this option is checked, if a remote backup starts while a local backup is running (or vice versa), then the backup that started second will wait until the backup that was already running to finish before processing. You must enable this option if you are backing up a Microsoft Exchange information store to more than one destination, because Exchange only supports one backup at a time.

    - Volume Shadow Copy Mode:
      Supported values for this option are either Off or Auto. If you are having trouble with VSS (Volume Shadow Copy Services) or do not need to use open file backup then you can disable the use of VSS with this option.

    - Volume Shadow Backup Type:

The Backup Software works as a VSS requestor and cooperates with the VSS writers on your system (such as the Exchange VSS writer and the SQL Server VSS writer) in order to capture a good snapshot of your server applications, as well as to perform routine maintenance at the end of a good backup.

If you do not want The Backup Software to rotate/cleanup transaction logs (such as Exchange transaction logs) at the end of the backup (e.g., because some other backup is relying on them), then change this setting to Copy and The Backup Software will not ask the VSS writers to cleanup transaction logs.

- Volume Shadow Copy Exclusions:
  If you do not need to use open file backup on certain volumes, then you can list the drive letters of these volumes here, separated by commas. (e.g., C:, D:)

- Volume Shadow Copy Writer Exclusions:
  The Backup Software automatically determines which VSS writers to involve in the backup by examining the set of files in your backup set. If you want to explicitly exclude a VSS writer from the backup, you may list them in this setting. Separate multiple writers by commas.

  To get a list of VSS writers on your system, run the 'vssadmin list writers' command inside of a command prompt.

- Volume Shadow Copy Provider:
  VSS providers are responsible for cooperating with your disk and filesystem drivers in actually taking a snapshot of your volumes. All systems come with the default Microsoft provider. Certain SAN vendors may provide a special provider that works with hardware snapshots on the SAN. Also, certain 3rd party backup vendors will also install a custom VSS provider.

  Use this setting to customize which VSS provider should be used for taking snapshots of particular volumes. Specify the names or GUIDs of the VSS providers that should be used, separated by commas. Each provider should have the volume name (or *) followed by an equal sign, followed by the partial name of the provider to use.

  For example:

  ```
  *=Microsoft, D:=EqualLogic
  ```

  This example indicates that the Microsoft provider should be used by default, except that for D: the EqualLogic VSS provider should be used.

- Volume Shadow Copy Logging:
  Change this at the direction of technical support in order to diagnose rare VSS issues.

  Most VSS issues can be diagnosed by looking for vss, volsnap, and other events in the Windows application and system event log. Also, make sure that the Volume Shadow Copy service is running, as well as the MS Shadow Copy Provider service. It is also helpful to run the following commands at the command prompt to see if they run successfully:

  ```
  vssadmin list providers
  vssadmin list writers
  ```

  If these commands fail, search the Microsoft knowledge base for information about the failure. Rebooting often fixes the problem.

  Please contact us if you have trouble diagnosing and resolving issues with Volume Shadow Copy Services on your system and we will be glad to assist you.

- **Scripted Actions:**

- Action Trigger:
  The backup can be configured to run commands and stop/start services either before and after the entire backup or before and after the volume snapshots are taken.

  This can be useful to backup certain legacy applications that either don't support being backed up while in an open state or have offline backup procedures.

  This setting determines when the services and scripts in this settings sub-category are stopped and started -- either when the backup itself begins and ends, or right before and after the VSS volume snapshot is taken. This is called the trigger action.

- Preinit Stop Scripts:
  At the start of the backup or right before the VSS snapshot, The Backup Software will execute this set of scripts and programs. You can list .bat files (batch files) here. Separate multiple scripts with semicolons.

- Preinit Stop Services:
  At the start of the backup or right before the VSS snapshot, these Windows services will be stopped. Separate multiple services with semicolons.

- Preinit Fail Action:
  If the backup fails to start some of the scripts of stop some of the services listed above, this determines how the backup should proceed (either fail immediately or warn and continue).

- Postinit Start Services:
  After the end of the backup or after the VSS snapshot is taken, these Windows services will be started. Separate multiple services with semicolons.

- Postinit Start Scripts:
  After the end of the backup or after the VSS snapshot is taken, this set of scripts and programs will be executed. You can list .bat files (batch files) here. Separate multiple scripts with semicolons.

- **Logging:**

  - Number of Days Before Zipping Log Files:
    All log files are stored in the Logs subdirectory of the directory where the program was installed. To save space, log files older than this number of days will automatically be zipped. Zipped log files are recognized as valid log files on the System Status page, and the log viewer is also able to open zip files directly.

    For these reasons, there is no disadvantage to zipping log files after a few days, and it can save you a lot of disk space, especially for backups that scan millions of files.

  - Number of Days to Retain Log Files:
    Log files older than this number of days will automatically be placed into the Windows recycle bin.

  - Diagnostics Logging:
    Technical support may direct you to change this setting to aid in diagnosing and resolving errors in your backups.

  - Performance Logging:
    If local backups are performing slowly, enable this setting to help technical support understand the cause.

  - Slow Event Timer:
    If performance logging is enabled, then any internal process that takes longer than this

many milliseconds will be logged. Normally you would set it to a value close to 10000 (10 seconds).

3-5-13 Options: Bandwidth

Bandwidth used by the backups can be throttled for both remote and local backups.

The week is divided up into Off Hours and Business Hours. By default business hours are between 7am and 7pm Monday through Friday. You can specify different bandwidth limits for Off Hours and Business Hours, ensuring that your backups won't affect your business operations if run during the day, while still maximizing performance when possible.

Tip: You can change these settings while the backup is running. Changes will take effect immediately. You do not need to restart the backup for the changes to take effect.

- **Bandwidth Usage:**
  - Usage Mode During Off Hours:
    For convenience, three bandwidth rates are defined: High, Medium, and Low. You can choose to use one of these modes or set this to Max, which indicates that bandwidth should not be throttled.

    You can customize the actual rates for the High, Medium, and Low modes using the other settings below.
  - Usage Mode During Business Hours:
    Similar to the previous setting, except that it determines bandwidth throttling during business hours.
  - High Bandwidth Usage (Kbits/sec):
    The maximum bandwidth to use for the High mode. 1 Megabit/sec is about 1000 Kbit/sec. A T1 provides about 1400 Kbit/sec. Cable modems usually provide around 700 to 2000 Kbit/sec. DSLs typically provide between 250 Kbit and 2000 Kbit/sec. Fiber connections can provide up to 20,000 Kbit/sec.
  - Medium Bandwidth Usage (Kbits/sec):
    The maximum bandwidth to use for the Medium mode.
  - Low Bandwidth Usage (Kbits/sec):
    The maximum bandwidth to use for the Low mode.
  - Local Server Bandwidth Multiplier:
    When local server backups are running, the same bandwidth throttling settings are used as for remote backups above, except that the rate for the active mode is also multiplied by this number. If this is equal to -1.0 then it disables bandwidth throttling for this backup destination.
  - Local Disk Bandwidth Multiplier:
    Similar to the previous setting, except that it affects local disk backups instead of local server backups.

  - Local Disk Max Disk Bandwidth (KB/sec):
    Local disk backups perform additional copying of data during the incremental backups of large files. This setting regulates the rate of all forms of data copying during the local disk backup operation. If your local disk backups are failing with temporary file system errors, the USB disk or network volume is temporarily dropping out, or other similar errors, try setting this to 5000. If problems persist, contact technical support.

- **Business Hours:**

  - Starting Weekday:
    The day of the week when business hours should start to become applicable.

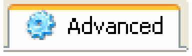
  - Ending Weekday:
    The last day of the week when business hours are applicable.

  - Starting Time:
    The time when business hours begin on a weekday.

  - Ending Time:
    The time when business hours end on a weekday.

3-5-14 Options: Advanced

The Advanced options affect the overall operation of the software.



Backup options that normally do not need to be changed are also located on this tab.

- **Software Updates:**

  - Check for New Versions:
    How frequently the software should check for newer software versions.

  - Automatically Install Updates:
    If this is checked, then after each backup (or when the backup manager is running) it will automatically download and install software updates. If this is unchecked, updates will automatically be downloaded, but you will be asked if you want to install the update before it proceeds.

    You probably do not want to turn this option on if you are using a software firewall or Internet security product that restricts outbound Internet access only to approved applications. This is because if the software is continually changing, your security software will treat the backup program as a new program and will block its Internet access until you manually tell your firewall to approve access. If you always allow outbound traffic on port 443 (or port 5470 if you are configured to use that port instead), then it is safe to turn on this option.

  - Treat Minor Versions as Major Versions:
    Software updates are classified by our development team as either minor or major. Minor updates are more frequent and contain minor feature updates or specific bugfixes. If this is set to No then it will only automatically install major versions (if you have automatic installs of updates enabled). You may always use the software updates tab on the system status page to check for a new version (minor or major) at any time.

- **Software Security:**

  - Access Control Level:
    You can prevent users who do not know your account password from changing your backup settings (even if they are an administrator on this machine). If you change this option to Require Account Password then your settings will be locked and cannot be changed until they are unlocked.

    There is a button in the lower-left hand corner of the window that can be used to unlock the settings. Settings will remain unlocked for 30 minutes, or until you re-lock the settings using the button, or until the program exits (whichever comes first).

  - Access Control User List:
    If the Access Control Level is set to Require Account Password then normally it will ask for the password of the account currently configured on the My Account page in the software

before allowing settings to be changed. This setting forces the software to only allow changes if the correct password is typed for one of the accounts listed in this setting.

This setting can be used to lock down the software so that the settings can only be changed by someone who knows the password for a specific account. This setting should contain the list of usernames of the users authorized to change the backup settings. Multiple users can be specified by separating usernames with commas.

  - Start Backup Manager at Logon:
    If enabled, the backup manager will automatically start when the current Windows user logs in to Windows.

- **Windows Registry:**

  - Registry Storage Location:
    The software can either store its settings in either a machine-specific location (HKEY_LOCAL_MACHINE) or a user-specific location (HKEY_CURRENT_USER). This is an advanced setting. Normally you should always store the settings in a machine-specific location.

  - Use Secure ACLs:
    If this option is enabled it uses Windows security features to restrict non-administrators from reading or modifying the configuration of the software in the Windows registry. It should always be left on in almost all circumstances.

- **Backup Engine:**

  - Number of Concurrent Connections:
    Large data sets may backup faster if more than one file is backed up at the same time. This setting determines how many files can be backed up concurrently.

  - Maintenance Mode:
    Every 7 to 14 days, extra work is performed on the account, such as checking for old deleted files to purge and to verify all data that should be stored in the backup is actually stored in the backup. This process can take quite a while if there are hundreds of thousands of directories. Set the maintenance mode to Background to have this work be performed in the background and not during the main backup job. This ensures that backup jobs do not take longer than normal. The maintenance running in the background will not interfere with backup jobs running at the same time.

  - Extra Days Between Maintenance:
    Accounts with millions of directories in the backup set may want to run account maintenance work once a month instead of once every 7 to 14 days. Change this setting to 24 to enable such a strategy. We also recommend setting the Maintenance Mode to Background for accounts this large.

  - Directory Cache Size:
    For performance, during backups while changed files are being uploaded in the foreground, a background process is scanning the directories in the backup set to determine which files have changed. This determines how "far ahead" this background process can get. Increasing this value has the potential to increase performance for accounts with millions of directories, but does require more memory. Typically the default setting of 10,000 is a good balance.

  - Always Check Block Fingerprints:
    The Backup Software uses the modification date and time and size of a file in order to quickly determine if the file has changed since the last time it was backed up. For certain types of files, this technique is not sufficient to detect all changes.

For example, Microsoft Exchange and SQL server can write data to a file for several days or even weeks without causing the modification date on the file to change. In general, any application that will keep a file open for days, weeks, or even months without re-opening the file will need to have the file contents scanned in order to detect changes.

Turning this option on tells the backup engine that it must scan the contents of files in order to determine whether or not they have changed. Typically you do not turn this option on for all folders here, but rather you turn it on only for the specific top-level folders that contain the data that needs the more thorough change-detection technique (such as Exchange and SQL server data). Please see our knowledge base for more information.

Note that The Backup Software will always scan the contents of the following file types to detect changes: .chk, .edb, .stm, .mdb, .ldb, .mdf, .ldf, .ndf, .db, .vhd, .vmdk, .vdi.

WARNING: Do not change this setting to Disabled without contacting technical support.

- **Local Backup Engine:**

  - Synchronous File Updates:
    Whether or not to force the flushing of the target medium's physical write buffers after backing up each file for local disk backups. (For remote backups this is always enabled.)

  - Periodically Flush Buffered Writes:
    Certain file systems or NAS devices may have trouble if the local disk backup is too fast and the target storage device has a very large write cache. Enabling this option will cause the write buffer to be flushed every 5 MB, and may help improve backup stability if the backup target medium is heavily loaded or stalls out periodically.

4-1 Overview: File Manager

The file manager is used to view, restore, and destroy data.

When restoring, you can either restore the current version of the data or you can restore data as it existed at an earlier point in time. You can select to restore just one file, a set of files, or everything. Likewise, you can use the file manager to destroy all versions of your data, destroy old historical versions, or to destroy only "deleted" files. (Deleted files are files that were backed up and then later deleted off of your computer, which are being retained according to your versioning settings).

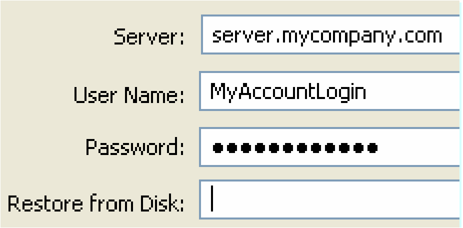
To use the file manager, you first login with your account credentials and then choose which task you want to perform: restoring data or deleting data. Each task will take you through a wizard follows this pattern:

1. You select which data to either restore or destroy (a single file, many files, or everything)
2. You configure options related to restoring or destroying
3. The file manager builds a list of all files and versions that will be restored or destroyed. You will be presented with a report explaining exactly what is about to happen. When you confirm that you are ready to proceed, the restore or destroy process will continue.
4. Finally, the data is either restored or destroyed.

NOTE: Normally only one instance of the file manager can be running at one time. However, if you want to start several instances of the file manager tool (e.g., to restore different sets of files at the same time), then use the Windows start menu to start the additional instances of the application. When you start the tool from the Windows start menu, it will allow the other instances to start. If you use the File Manager button on the Control Panel page in the backup manager to start the tool, then if you are already running the file manager it will bring that window to the foreground instead of starting a new instance.

4-2-1 Login Page

The Login Page allows you to login and connect to the remote server or to your local backup storage. If you have configured local backups, the server drop down list will also contain selections for the local server or local disk backup destinations. Additionally, you can also select a different filesystem path that contains backup data by using the restore from disk field.



Server: server.mycompany.com
User Name: MyAccountLogin
Password: ●●●●●●●●●●●●●
Restore from Disk:

If you are performing an emergency restore from a USB disk that our data center shipped to you, use the Restore from Disk field to browse to the directory on the USB disk that contains your account's data (the root of the USB disk should contain a text file indicating the proper location).

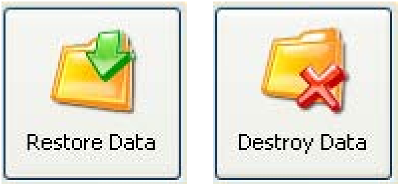
NOTE: You do not need your credentials to restore data from local backups. This means that once you have backed up your data locally, you will always be able to use that backup, even if you no longer have service with us. To restore data without your credentials, use the browse button (...) next to the Restore from Disk field to select the directory containing your local backup data. After you do this, click Next and you will be able to choose the Restore command without valid account credentials.

To complete this page, click Next, and if successful you will be taken to the Task Selection page.

4-2-2 Task Selection

From the Task Selection page you to choose what you would like to do with the backup data.

You can choose to either restore data or to destroy data.



If you choose to destroy data, you will be required to enter the account password again if you logged in with a saved password on the login page. This is to ensure that the user operating the program knows the account password before being allowed to destroy data.

NOTE: When you destroy data it immediately reduces the disk usage in your account. There is no delay between when you destroy the data and when the disk usage in your account is reduced.

4-3-1 Restoring Data: Data Selection

The Restore Data page lets you select which folders and files you want to restore. You check off the data you want to restore and click Next when you're ready to choose your restore options.

The pane on the left is the folder pane and contains the list of folders. When you first enter this page the folder list will automatically download. Once downloaded, you can browse all of the folders that are on the server and use the checkboxes to select or unselect particular folders.

The pane on the right is the file list pane and shows the files that are inside the currently selected folder on the folder pane.

TIP: If you want to check or uncheck many files at the same time (but you do not want to check/uncheck all of the files in that directory), then use shift-click and ctrl-click to highlight the files of interest in the file list pane, then right click one of those files and choose either Select or Unselect.

NOTE: If you only want to restore a single file, find the file on this page, right click it, and choose Versions... A dialog will appear that shows the list of all versions that can be restored for this file. You can then choose to download a specific version, or to destroy one particular version (and all older versions). Note that the Size column in the versions dialog indicates the size the file when it was uploaded to create that version (the size of the delta required to actually store the data for each version is not displayed).

4-3-2 Restoring Data: Options

Once you select the data to restore, the wizard helps you choose where you want to place the restored data, which point in time to use, and what to do if the files you are restoring already exist.

The options are split across two pages. Once you have finished changing the first page of options, click Next to get to the second options page. Once you have finished with the second page of options, click Next to get to the action confirmation page.

Location to place restored folders and files (page 1):

You can choose to either place the restored files back into the same place that they were in when they were backed up, or you can choose to restore to a different folder of your choosing. If you are restoring a historical version of your data instead of the current version, you probably want to choose to restore the data to an alternate location.

Version control (page 1):

This group of options controls whether you restore the most recent version of your data or some historical version. How many historical versions will be available to restore depend on what your versioning settings were when you backed up your data.

TIP: If you just want to restore your files exactly as they existed at a certain date and time, use the Data as it existed at or before choice and leave the other options set to their default settings.

There are three different methods to choose from to control which versions to restore:

- Most recent data: The most recent version of your data will be restored.
- Data as it existed at or before: Use this option to perform a point-in-time restore. A point-in-time restore is where you restore your files as they would have existed at some particular point in time. With this option, the most recent version that is before the indicated date and time will be restored.
- Data matching date nearest to: This is an advanced setting and typically should not be used. It indicates that the version of the file that is closest to the indicated date and time should be restored. With this option it is possible that the version that will be restored will be past the indicated point in time.

There are three options that adjust how deleted files are treated. Deleted files are files that were backed up and then later deleted from your local computer, and are now being retained in the backup according to your versioning settings. The three options are:

- Include deleted files in search checkbox: If this box is not checked, then deleted files will not be restored (even if they were selected on the data selection page).
- However, exclude deleted files not matching point in time checkbox: This option is only relevant if the Include deleted files in search option is checked. If this box is checked, then any files that did not actually exist on your computer at the date and time indicated in the version control settings will not be restored. In other words, any files that were deleted after the date and time will not be

restored.

For example, say that a file named 'report.docx' was backed up on July 1st, 2000, and then it was later deleted from your computer on August 15th, 2000. If you performed a point-in-time restore for July 20th, 2000, then the 'report.docx' file would be restored, whether or not this option was checked. However, if you performed a point-in-time restore for August 20th, 2000, then this file would only be restored if this option was not checked.

To perform a point-in-time restore, you normally want to leave this option checked. This will ensure that any files that were deleted from your local system at the given date and time will not be restored.

- Include the deleted date and time in the restored filename checkbox: If this option is checked, then any deleted files that are restored will be restored using a modified filename that appends the following to the name of the file: [Deleted Month, Day Year]

Finally, the Include the version date and time in the restored filename option can be used to include the restored version's timestamp in the restored file's filename. For example, if you are restoring a historical file named 'report.docx' that was uploaded on July 1st, 2000, then it will actually restore the data to a file named 'report [historical version July 1st, 2000].docx.' This option is useful if you want to restore the historical versions of certain files back into their original locations, but you do not want to overwrite the current versions of those files.

Incremental backup cache (page 1):

If you check this option, then the data will not actually be restored. Instead, the software will rebuild the incremental backup cache. This is useful if you are resuming incremental backups after a complete system crash (see Restoring After a System Crash).

How existing files should be treated (page 2):

This determines how files that already exist in the restore location that have the same name as a file being restored should be treated. You can choose from the following options:

- Prompt for action: Every time a conflict occurs, a dialog box will be shown presenting the details of each file (the file already on your computer and the file being restored) asking what you want to do.

- Overwrite without asking: Files with the same name that already exist on your computer will be overwritten with the data restored from the backup without asking you for confirmation.

- Skip without asking: Files with the same name that already exist on your computer will not be restored.

- Move to this folder: Files with the same name that already exist on your computer will be moved to a different folder (that you specify) before the file is restored from the backup.

Subdirectory creation options (page 2):

These options determine how the directory structure within the alternate restore location should be re-created. These options are not applicable if you are restoring the files to their original locations. There are three ways to choose from:

- Flat: All files that you are restoring from any folder will be placed into the same directory. No subdirectories will be created, and any files with the same filename will be renamed to avoid conflicts. Typically you would not want to select this option.

- Minimalized: This indicates that any common parent directories in the list of directories you have selected for restore will not be created (only the subdirectories needed to differentiate the files being restored will be created). This concept is best illustrated with an example.

Say that you had selected the following three folders for restoring:

Users\Analyst\My Documents
Users\Analyst\My Documents\My Pictures
Users\Analyst\My Documents\My Music

Also, say that you had chosen to restore the files to C:\Restored.

Since "Users\Analyst\My Documents" was a common parent directory of all of the folders, if the data was restored with this option then it would restore files in ...\My Documents into C:\Restored, restore files in ...\My Documents\My Pictures into C:\Restored\My Pictures, and restore files in ...\My Documents\My Music into C:\Restored\My Music.

Typically, this is the option that you want to select.

- Full reconstruction: This option will cause all subdirectories to be recreated. Continuing the example above, if this option was selected, in the example the data would be restored to:

  C:\Restored\Users\Analyst\My Documents
  C:\Restored\Users\Analyst\My Documents\My Pictures
  C:\Restored\Users\Analyst\My Documents\My Music

4-3-3 Restoring Data: Action Confirmation

Clicking Next on the second restore options page brings you to this page. This page will download a list of all versions of files that should be restored based on the choices you have made so far. Once it has built a list of a versions that will be restored, it will present a detailed report showing what is about to happen. You can use this information to confirm that you have configured your restore options correctly.

If you are ready to proceed to start restoring your data, click the Restore button in the lower-right hand corner. Once the restore process begins, you will not be able to change the restore options without canceling and starting over. Clicking Restore will take you to the action page.

TIP: This page does not restore any data. It is only building a list of files that it is going to be restored during the next step. You still need to click the Restore button after it has finished building the file list in order for the restore process to begin.

4-3-4 Restoring Data: Action

At this point it will download and restore all of your data according to your data selection and restore options.

NOTE: If you checked the rebuild incremental backup cache option, this step will not actually restore any data but rather will rebuild the incremental backup cache for the selected files.

This page will display the current download rate, as well a log of the activity so far.

When all of the selected files have been restored, the action results page will automatically appear.

4-3-5 Restoring Data: Action Results

This is the final step of the wizard where the software presents a summary of what happened during the restore process, as well as a detailed log showing all of the details. The detailed restore log will also appear on the System Status page in The Backup Software.

At this point you can choose to either exit the program or you can start over if you want to perform another task.

4-4-1 Destroying Data: Data Selection

The Destroy Data page lets you select which folders and files you want to destroy. You check off the data you want to destroy and click Next when you're ready to choose your destroy options.

The user interface on this page is identical in function to the Restoring Data: Data Selection Page.

4-4-2 Destroying Data: Options

Once you select the data to destroy, the wizard helps you choose the strategy that should be followed when choosing which versions of each file should be destroyed.

There is only one page of destroy options. Once you have finished changing the destroy options, click Next to get to the action confirmation page.

Version control:

This group of options controls whether you destroy all versions of the data you have selected, or whether only certain historical versions are destroyed.

Tip: The options are set by default to only destroy historical versions of files that do not match your global data retention policy as set in your versioning settings. If you completed a destroy process but did not see your disk usage decrease, then please double-check that you chose to destroy all versions of your data (if that is what you are trying to do).

There are three different methods to choose from to control which versions to destroy:

- Destroy all data: All versions of each selected file will be destroyed.
- Destroy versions with data older than (date and time): Use this option to destroy all historical versions that are older than a particular point in time. This is useful if you recently changed your versioning settings to keep fewer days of historical versions, and now you want to immediately destroy any versions that do not match your new retention policy. There are three checkboxes that affect the behavior of this method:
  - Allow current version to be included in search for versions to destroy:
    If this is checked, then it will be possible to destroy all versions of a file if that file was uploaded before the indicated date and time. If you are only trying to trim unwanted historical versions, do not check this option.
  - However, keep at least ___ version(s), including the current version:
    If this is checked, then even if a historical version is older than the indicated date and time, it will not be destroyed if it would cause the file to have fewer than N versions. For example, if you set this to 3, then it would never destroy the current version and would never destroy the two most recent historical versions.
  - But allow no more than ___ version(s), including the current version:
    If this is checked, then it will make sure that each file has no more than N versions. For example, if you set this to 3, then it would destroy any versions older than the 2nd historical version, even if those versions were more recent than the date and time indicated above.

    TIP: It does not make sense to set this to a value that is less than the value of the previous setting.

    TIP: If you set this to 0, then all versions of each file will be destroyed, including the current version.

- Destroy versions that are at least ___ step(s) away from the current version: This is useful if you want to destroy historical versions not based on a date and time, but rather based solely on how many historical versions there are for a file. For example, if you set this to 3, then it will make sure that each file has no more than the current version and the two most recent historical versions (any other older historical versions would be destroyed).

In addition to choosing how to select which version to destroy, the Consider only deleted files option makes it easy to destroy only deleted files. Deleted files are files that were backed up and later were deleted from your computer, and are still in the backup according to your versioning settings. If this option is checked, then any files that were selected on the data selection page that are not "deleted" will not be destroyed.

4-4-3 Destroying Data: Action Confirmation

Clicking Next on the destroy options page brings you to this page. This page will download a list of all versions of files that should be destroyed based on the choices you have made so far. Once it has built a list of a versions that will be destroyed, it will present a detailed report showing what is about to happen. You can use this information to confirm that you have configured your destroy options correctly.

If you are ready to proceed to start destroying your data, click the Destroy button in the lower-right hand corner. Once the destroy process begins, you will not be able to change the destroy options without canceling and starting over. Clicking Destroy will take you to the action page.

TIP: This page does not actually destroy any data. It is only building a list of files that it is going to be destroyed during the next step. You still need to click the Destroy button after it has finished building the file list in order for the destroy process to begin.

4-4-4 Destroying Data: Action

At this point it will download and destroy all of your data according to your data selection and destroy options.

This page will display a summary of progress, as well as a log of the files destroy so far.

When all of the selected versions of files have been destroyed, the action results page will automatically appear.

4-4-5 Destroying Data: Action Results

This is the final step of the wizard where it presents a summary of what happened during the destroy process, as well as a detailed log showing all of the details. The detailed destroy log will also appear on the System Status page in The Backup Software.

At this point you can choose to either exit the program or you can start over if you want to perform another task.

5-1 Overview: Disk Usage Inspector

The disk usage inspector tool is designed to help you understand which directories are contributing the most towards your current, historical, and deleted disk usage.

You can start the tool by using the Control Panel page of the The Backup Software.

The first page of the wizard displays the login page. If you have configured local backups, the server drop down list will also contain selections for the local server or local disk backup destinations. Additionally, you can also select a different filesystem path that contains backup data by using the restore from disk field.

The next page of the wizard displays the disk usage information. This page first downloads the list of all folders contained on the server. Once downloaded, it will display the folders along with several columns of information.

Columns of information:

- Size: The amount of current data in just this directory.
- Total Size: The amount of current data in this directory and all of its subdirectories.
- Deleted Size: The amount of deleted data in this directory and all of its subdirectories.
- Size of Versions: The amount of historical data in this directory and all of its subdirectories.

Types of data:

Current data is information required to store the current versions of all of your files. The results of the estimated disk usage on the Visualize! dialog on the Folders page of The Backup Software should roughly match the amount of current data shown on this screen.

Historical data is information required to store the previous versions of files that still exist on your computer. Only the changes between versions are stored. Files that change frequently or large files that are rewritten often (such as very large .zip files) can contribute towards high levels of historical disk usage. Use this tool to quickly identify which directories contain files with the largest historical deltas. You can then customize your backup policies for just these folders or files to store less historical information, if desired.

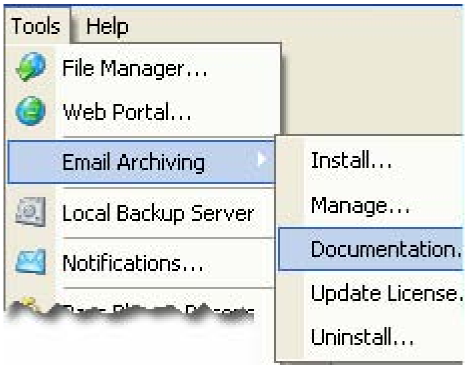
Deleted data is information required to store the current and historical versions of files that were once backed up but then were subsequently deleted from your computer. The Backup Software retains these deleted files in the backup for as long as you have configured it to do so according to the versioning settings on the Options page.

6-1 Overview: The Archiving Software

The Archiving Software can be used to provide message-level backup and restore as well as active archiving of content out of Microsoft Exchange mailboxes (to optimize space and performance). See the email archiving feature overview for more details on its capabilities.

The product works by copying information out of Exchange mailboxes into a locally stored archive. The local archive can be stored on any local filesystem. Additionally, The Archiving Software can also remove archived content out of mailboxes, either leaving behind a stub or removing the content completely. Optionally, you can configure The Backup Software to remotely backup your local email archive by adding your archive locations on the Folders page in the The Backup Software.

The topics in this quick reference guide will help you install The Archiving Software. Once installed, more detailed documentation is available that will help you configure and manage email archiving and perform archiving tasks. To view the detailed product documentation without installing, open the The Backup Software, and use the Tools ->Email Archiving-> Documentation menu command.



To install The Archiving Software, first review the system requirements, and then follow the steps in the install guide.

6-2 System Requirements for The Archiving Software

The Archiving Software is intended for use with Microsoft Exchange. The computer performing the email archiving process must meet the following requirements:

- Windows 2000, XP Professional, Vista, Windows 7, Server 2003, Server 2008 (or better)
- .NET Framework v2.0 (will be installed automatically if not yet installed)
- Microsoft Internet Information Server 5.0 (or better)
- Exchange 5.5, 2000, 2003, 2007 (or better)
- Outlook 2000 (or better; only needed if not installed onto the Exchange server)
- 40MB for the program files and log files
- Local disk storage for the archive data (any accessible directory, including network shares, is supported)

Exchange end-users who need to access archive content for their Exchange mailboxes from within Outlook should be using Outlook 2000 or better (other Exchange-compatible email clients should also be compatible).

NOTE: An extra plugin installation on each Exchange client computer is not required. Outlook Web Access is also supported.

Refer to the Install Guide for detailed installation instructions.

6-3-1 Overview: The Archiving Software Installation

The Archiving Software Install Guide [**1** 2 3 4 5 6 7 8 9]

The Archiving Software is composed of two separately installable components:

- **Service component**: This component has three pieces:
  - A management console application to graphically configure email archiving.
  - A Windows service to perform the archiving work in your Exchange information stores.
  - A backend web service IIS application that processes requests from the Web component.

  NOTE: These components must be installed onto a computer is part of the same domain as the Exchange server, and also has IIS running in 32-bit mode. This means that the Service component cannot be installed onto an Exchange 2007 server (because Exchange 2007 requires IIS to be running in 64-bit mode). Please follow the flowchart in this guide carefully. A future software version will allow you to install this component onto a computer with IIS in 64-bit mode.

- **Web component**: This is a Microsoft IIS web application (ASP.NET v2.0) that allows Outlook and Outlook Web Access users to search for and restore messages from the email archive. It also provides the original message data when a user clicks a message stub link. It communicates with the backend web service (part of the Service component) over your local network.

  NOTE: This component can be installed to run as either a 32-bit or 64-bit IIS application. Use this guide to determine which version of the component (x86 or x64) should be installed.

Depending on your requirements, each component can be installed onto the same computer or a different computer.

Another choice is whether to install the components onto the Exchange server or onto a different computer (either workstation or server) that has Outlook installed onto it.

This guide is composed of the following topics:

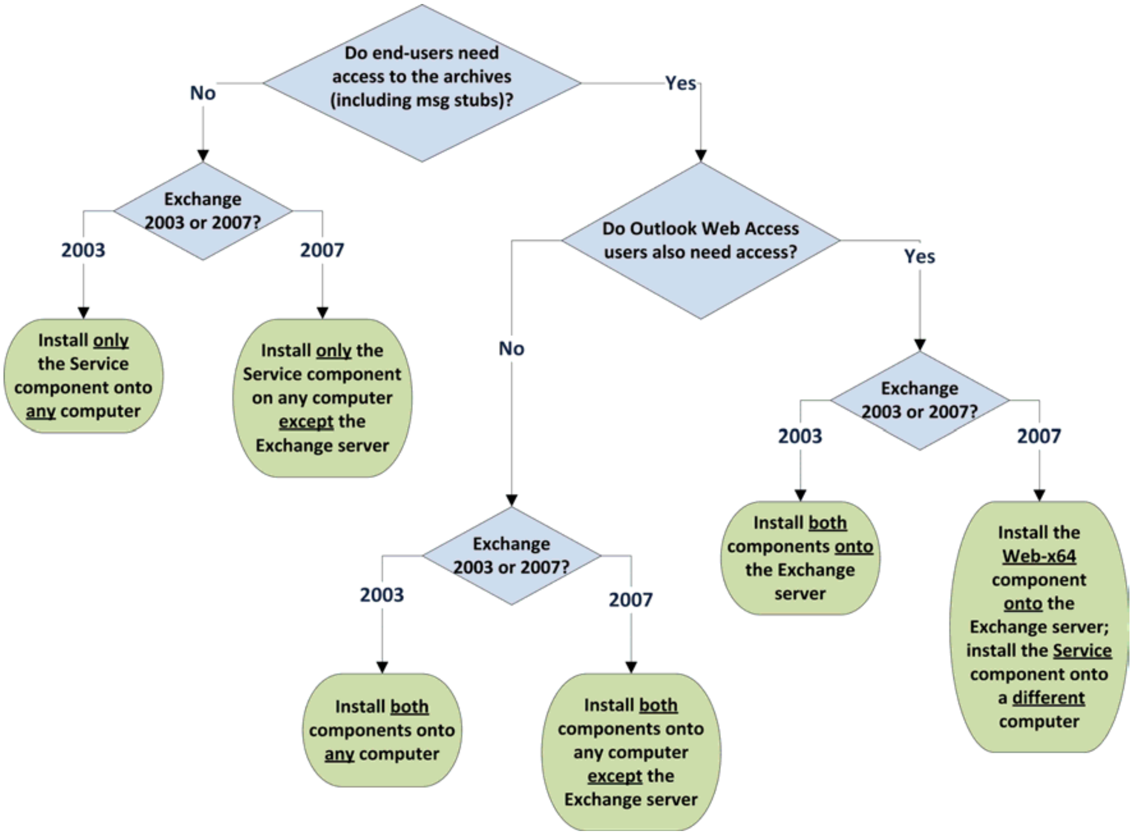
Please contact us if you have any questions about the install process.

➡ Next: Choose components and install location

6-3-2 Choose Components and Location

The Archiving Software Install Guide [1 **2** 3 4 5 6 7 8 9]

Use the following flowchart to decide where the install the Service component, whether you need to install the Web component, and where the Web component should be installed (refer to the overview for a description of the components).


Do end-users need access to the archives (including msg stubs)?
No
Yes
Exchange 2003 or 2007?
2003
2007
Install only the Service component onto any computer
Install only the Service component on any computer except the Exchange server
Do Outlook Web Access users also need access?
No
Yes
Exchange 2003 or 2007?
2003
2007
Install both components onto the Exchange server
Install the Web-x64 component onto the Exchange server; install the Service component onto a different computer
Exchange 2003 or 2007?
2003
2007
Install both components onto any computer
Install both components onto any computer except the Exchange server

Previous: Overview
Next: Windows security setup

6-3-3 Windows Security Setup

The Archiving Software Install Guide [1 2 **3** 4 5 6 7 8 9]

Now that you know where each of The Archiving Software components will be installed, Windows security must be adjusted.

Each component can be assigned to operate with the credentials of two different Windows users or to operate with the same Windows user.

Each component has requirements to different parts of your domain and Exchange server:

Service component:

We highly recommend that you create an additional Windows user in active directory that is dedicated to running The Archiving Software Service component. Domain administrators are denied access to mailboxes within Exchange information stores by default. It is easier to add a new Windows user (the user does not need to have an Exchange mailbox associated with it). The exception is if you are installing the Service component onto a domain controller or Small Business Server. In that case, you must use a user that is domain administrator, and you must follow the steps in Microsoft KB article 821897 (see below).

The Windows user that the service component uses to access your domain must:

- Have local administrative privileges on the computer where the Service component is installed.

  To give a Windows user local administrative privileges, logon to the computer, right click My Computer, and choose Manage. Then go to Local Users and Groups, and open Groups. Right click Administrators and choose Properties. Click the Add button to add the Windows user to the group.

  TIP: Do not add the user to the Domain Admins or Enterprise Admins group. While this will give the user administrative permissions on the computer, it will also deny that user access to the Exchange information stores (see note below).

- Have permission to read and write to any directory where you want to store your email archive data.

- Have permission to read and write to all mailboxes in your Exchange information store(s).

  IMPORTANT: Any member of the Domain Admins or Enterprise Admins user groups are explicitly denied access to mailboxes in Exchange Information stores by default. We highly recommend creating an additional Windows user in active directory dedicated to running The Archiving Software Service component.

  However, if you are installing the Service component onto a domain controller (including a Small Business Server), or if you do not want to add a dedicated Windows user, then you must follow the steps in Microsoft KB article 821897 to allow Domain Admins access to the mailboxes in your Exchange information store.

  To grant permissions to access Exchange mailboxes to a Windows user that is not a domain or enterprise admin, follow these steps:

1. Start the Exchange System Manager.
2. Expand the Servers group, expand the relevant server and storage group, and then right click on the appropriate information store (e.g. Mailbox Store) and choose Properties.
3. Click the Security tab. Click Add.
4. Type in the name of the user or click Advanced to search for the appropriate user. Click OK when finished.
5. Highlight the user in the list and make sure they have Full Control.
6. Save all changes. If you are already install the Service component, then make sure to restart The Archiving Software Windows service.

Web component:

The only requirement for the Windows user that the Web component uses for credentials is that the user must have local administrative privileges on the machine where the Web component is installed. This can either be an account that is a domain administrator or another Windows user that has been given local administrative privileges (see note on granting local administrative privileges in the previous section).

Next steps:

Now that you have configured Windows security to grant the components the necessary privileges to perform email archiving, you can proceed to configure your The Backup Software account credentials.

Previous: Choose components and install location
Next: Configure Account Credentials

6-3-4 Configure Account Credentials

The Archiving Software Install Guide [1 2 3 **4** 5 6 7 8 9]

The Archiving Software relies on your Backup Software account credentials for licensing and web-based status monitoring and reporting. Before you install email archiving, you must first configure a username and password for a Backup Software account that is licensed to use The Archiving Software. The Archiving Software is licensed per mailbox, so a certain number of mailboxes will be activated for your Backup Software account. To activate email archiving features for your account, please contact customer service.

NOTE: If you plan to archive information out of an Exchange journaling mailbox, you must be licensed for at least as many mailboxes as are in the Exchange information store(s) that contains the journaling mailbox(es) that you will be archiving information from. Please see the end-user license agreement for more information.

Once email archiving has been activated for your account, follow these steps on each computer where you need to install email archiving components:

1. Download and install The Backup Software.

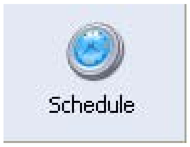
2. Open the The Backup Software and go to the My Account page.

3. Enter the username and password of your Backup Software account for which email archiving has been activated.

4. If you plan on backing up your archive remotely, then you should also configure your pass phrase (otherwise skip this step).

   TIP: If you are installing the Service component and Web component on different computers and you want to backup your archive(s) remotely, then you only need to configure the pass phrase on the computer where the Service component is being installed.

5. If you will be installing the Service component on this computer, go to the Schedule page and setup a daily schedule.



   Even if you have not configured any data to backup on the Folders page, this is a required step. Each day The Archiving Software will update licensing information as well as update your email archiving status reports in the web portal.

Tip: If you are installing only the Web component on this computer, then you do not need to set a schedule.

Once you have configured your account credentials, you are ready to download and install the The Archiving Software components.

Previous: Windows security setup
Next: Download and install components

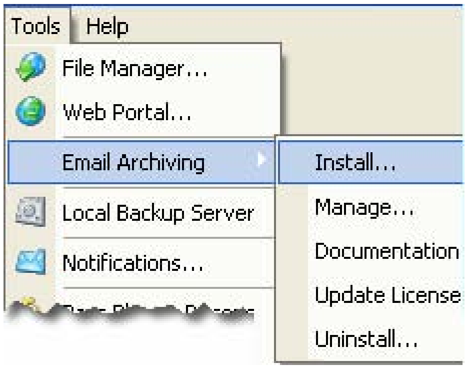
6-3-5 Download and Install Components

The Archiving Software Install Guide [1 2 3 4 **5** 6 7 8 9]

Once you have configured your account credentials, the next step is to download and install The Archiving Software components on each computer where the components should be installed (refer to the flowchart for guidance).

If you are installing the components onto separate computers, then you should install the software onto the computer that needs the Service component first, and then install the software onto the computer that needs the Web component.

To install one or more components onto a computer, open The Backup Software and use the Tools -> Email Archiving ->Install menu command.



This will start the install wizard process. This wizard takes you through a number of steps:

1. It checks that your Backup Software account has email archiving features activated.

2. It checks for, and automatically downloads and installs (if necessary) any dependent system runtime libraries, including the .NET framework v1.1, the .NET framework v2.0, the MSVC 2005 SP1 Runtime, and the MSVC 2008 Runtime.

3. It also checks to make sure you have installed Microsoft Internet Information Server v5.0 or later.

   TIP: If you are using IIS 7.0 (e.g., on Vista or Server 2008), you need to make sure that the IIS 6.0 management compatibility component is installed.

4. It helps you choose which components to install. It will ask you a series of questions, which are the same questions on the flowchart. After you answer the questions, it will ask which components you want to install onto this computer.

5. Based on your choices in the previous step, it automatically downloads and installs the appropriate files.

6. Finally, it runs the configuration wizard for the component(s) that you chose to install.

The next two steps will help you complete the configuration wizard for each component.

Previous: Configure account credentials
Next: Configuration wizard: service component

6-3-6 Configuration Wizard: Service Component

The Archiving Software Install Guide [1 2 3 4 5 **6** 7 8 9]

At the end of the component install process (initiated by the Tools -> Email Archiving -> Install menu command in The Backup Software), the configuration wizard will start for any component(s) that you chose to install. Which pages of the wizard that will be displayed depend on which components you chose to install.

If you installed the Service component, then the configuration wizard will show the The Archiving Software Service Account page.

This page asks you to enter the credentials of the Windows account that you want to use for the Service component. (See windows security setup for details on the permissions that this Windows user must have and configuration instructions.

NOTE: Domain admins and enterprise admins do not have sufficient privileges in a default Microsoft Exchange configuration.)

The username should either have the form domain\username or username@domain.

To proceed with the install, complete the Web component configuration wizard on the computer where you installed the Web component. If you installed the Web component on the same computer as the Service component, then clicking Next in the configuration wizard on the Service Account wizard page will take you to this step.

Previous: Download and install components
Next: Configuration wizard: Web component

6-3-7 Configuration Wizard: Web Component

The Archiving Software Install Guide [1 2 3 4 5 6 **7** 8 9]

At the end of the component install process (initiated by the Tools menu, Email Archiving, Install command in The Backup Software), the configuration wizard will start for any component(s) that you chose to install. Which pages of the wizard that will be displayed depend on which components you chose to install.

If you installed the Web component, then the configuration wizard will show The Archiving Software Web Service Account page.

This page asks you to enter the credentials of the Windows account that you want to use for the Web component. (See windows security setup for details on the permissions that this Windows user must have and configuration instructions.) This Windows account must have local administrative privileges on this computer.

The username should either have the form domain\username or username@domain.

If you did not install the Service component on this computer, then the configuration wizard will also show The Archiving Software Console Computer page. This page will ask you for the hostname or IP address of the computer that is running the Service component.

Once you have completed the configuration wizard for both the Service component and the Web component, you can use The Archiving Software management console to start configuring your email archiving policies.

⇦ Previous: Configuration wizard: Service component
⇨ Next: Configure archiving policies and settings

6-3-8 Configure Archiving Policies and Settings

The Archiving Software Install Guide [1 2 3 4 5 6 7 **8** 9]

When the configuration wizard completes on the computer where you installed the Service component, you will be given the option of starting the management console, and also starting The Archiving Software reference manual (which provides detailed help on all aspects of the management console).

This topic will give an overview of how you should use the management console to configure email archiving. For detailed instructions about a particular step, please consult the relevant topic in The Archiving Software reference manual, which can be started from within The Backup Software by using the Tools menu, Email Archiving, Documentation command.

Use the management console to perform the following tasks:

1. Use the Archive Locations page to add one or more filesystem locations where you want to store archive data. If you want to store to a network share or NAS, add a location using a UNC path (\\server\share\folder, etc.).

2. Use the User Groups page to add the Exchange mailboxes that need to use email archiving. If you want to automatically activate email archiving for any Exchange mailboxes matching certain criteria, use the Automation page to setup a Query active directory for mailboxes process.

3. If you want to archive information within Exchange public folders, add the relevant folders using the Public Folders page.

4. Use the Policies page to configure one or more archiving policies (there is no limit). An archiving policy determines (a) what information should be copied (based on message age, size, sender, subject, etc.), (b) whether or not the information should be left in the mailbox, replaced with a stub, or removed completely, and (c) when the archiving should be performed.

   Which policies to create depends on what you want to accomplish. Here are some common ways to configure and use The Archiving Software:

   Message-level backup + removal of old content: This scenario is relevant if you want to protect all email content for some or all of your Exchange mailboxes and you also want to remove old information out of Exchange to optimize Exchange performance.

   To implement this scenario, create two policies: one to capture all messages without removing content, and another policy to move older content out of Exchange and into the archive (leaving either a stub behind or removing it completely according to your preference). For details on how to configure each policy, see the instructions for the next two scenarios.

   The system is efficient such that once a message has already been stored in the archive, it will not be stored in the archive again if another policy matches the message at a later point in time. Thus, you can use one policy to copy everything into the archive (providing message-level backup), and then have another policy that comes back later and stubs or removes old content (or content matching other criteria).

Message-level backup only: This scenario is relevant if you want to protect all email content for all or only some of your Exchange mailboxes and you do not want to remove any information from the Exchange mailboxes. To implement this scenario, configure a new policy as follows: On the Message Types tab, check all boxes. On the Action tab, choose Leave the original message in the mailbox and turn on indexing. On the Conditions tab, choose Capture all messages. Then assign your policy to all of your users.

Tip: Message-level backup is typically not a suitable replacement for an information-store wide backup of Exchange. In general, after a complete loss of the information store it will be much faster to perform an information-store wide restore, rather than performing a message-level restore. Thus, we recommend that you also backup your store files (.chk, .edb, .stm, .log) directly in addition to performing message-level backup.

Removal of old content: This scenario is relevant if you only want to use The Archiving Software to optimize the performance of your Exchange information stores by moving old content (such as large attachments) out of Exchange and into the archive. Since you will not be using The Archiving Software to archive all message content, you should have a suitable Exchange backup solution in place that complements The Archiving Software.

Legal compliance: This scenario is relevant if you are using The Archiving Software to assist with email retention regulations and you need to capture all email, even email that was deleted by recipients as soon as they received it. To implement this scenario, configure Exchange journaling for your information stores. Then, create a policy that archives all message content, and be sure to check the This policy applies to Journal mailboxes checkbox in the General policy options tab. Finally, activate the policy for the user that corresponds to the Exchange journaling mailbox.

Tip: This scenario can be combined with any of the other scenarios. First, complete the configuration for the other scenario, and then add another policy to archive information out of just the Exchange journaling mailbox.

Note: If you are archiving information in a journaling mailbox, then you must be licensed for at least as many mailboxes as there are in your Exchange information store.

Category-based archiving: If desired, users can be given the ability to use Outlook categories to indicate when messages should be archived (stubbed) or restored (unstubbed). Rather than using policies this is actually a property of users (set on the Users page). Category scanning also has to be enabled on the Local Service page. Users should create two Outlook categories: *Archive Message and *Restore Message and then mark messages as appropriate to have messages archived and restored.

5. Once you have configured your policies, you need to assign users to each policy, so that each policy knows which users and public folders this policy should apply to (to do this, right click a policy, choose View Users for this Policy, and then click the add toolbar button (second from the left) to select and add the users).

   If you want to automatically assign users matching certain criteria to a specific policy, use the Automation page to setup a Set policy based on active directory process.

6. Finally, use the Local Service page to schedule routine archive maintenance. We recommend the following settings:

   - Enable Debug Logging: Unchecked
   - Folder Maintenance: Checked and scheduled once per day
   - Scan User Categories: Unchecked
   - Archive Maintenance: Checked and scheduled once per 7 days

- Stub Maintenance: Checked and scheduled once per 28 days
- Stub Maintenance Safe Delete: Checked
- Backup Duplicate Messages: Checked -- This only affects whether or not duplicate messages are stored in the local archive. When you remotely backup your archive, duplicate messages are not backed up. If you want to save space in your local archive as well, then uncheck this setting.

You can also use the Archive Web URLs tab, Status button to see if the Web component is properly installed and running.

Now that archiving has been configured and scheduled, you can optionally choose to remotely backup your archives for backup and disaster recovery purposes.

Previous: Configuration wizard: Web component
Next: Configure remote backups

6-3-9 Configure Remote Backups

The Archiving Software Install Guide [1 2 3 4 5 6 7 8 **9**]

Optionally, you can choose to enable remote backups of your email archives. You can also use the local backup features to make encrypted local backups of your email archive.

To backup your archives:

1. On the My Account page in The Backup Software, make sure that you have configured a pass phrase.

2. On the Folders page, click the Add button. Now that you have configured one or more Archive locations within The Archiving Software, a popup menu will appear with a list of your archive locations. Select one of the archive locations to add it to your folder list (or there is a menu item to proceed to the normal add folder dialog, if you wish).

You should have already have scheduled a time for backups to begin when your configured your account credentials.

We recommend scheduling remote backups so that they start after The Archiving Software has finished the archiving process for the day. How long the archiving process will take depends on the size of your Exchange database and the memory and speed of your computer(s).

For smaller Exchange servers, schedule the remote backup to begin 1 or 2 hours after the email archiving work is scheduled to begin. For larger Exchange servers, we recommend examining the daily processing log from within The Archiving Software to estimate how much time email archiving will require on average. If necessary, use the Schedule page to adjust your backup schedule.

TIP: If you are also backing up your Exchange information store from this computer, then if you have a large Exchange information store (larger than 20GB) you may want to consider using two settings profiles on this machine -- one to backup the Exchange information store, and the other to backup your email archive.

Conclusion:

At this point email archiving is fully installed and configured. Archiving will automatically happen according to the schedules you have assigned to your policies.

Previous: Configure archiving policies and settings

6-4-1 General Tips

Whenever you have an issue with The Archiving Software, a good place to start is to look at the various logs and look for error conditions highlighted in red. The following logs are available from within the management console of The Archiving Software:

- **Console**: This logs all actions performed from within the management console user interface.
- **Service**: This logs the startup and shutdown of the Windows service that performs the actual email archiving. If you start tasks with the management console interface, but no processing tasks appear to start, use these logs to understand if the service is running and if something is preventing it from finding and queuing tasks.
- **Processing**: These logs contain a detailed record of what happened while a particular task was being performed. If a processing task appeared to run, but the results were not what you expected (e.g., messages aren't appearing in your archive), then check the processing log for errors.

You can also use the Help Me button on the System Status page of The Backup Software to package all of the recent Archiving Software logs to send to technical support for analysis.

6-4-2 Check Stub Messages Setup

This topic will help you troubleshoot problems accessing stub messages.

Retrieval of messages in the archive via message stubs (from within Outlook and OWA) uses a web service running in IIS (on the computer where the Web component has been installed). Errors encountered accessing message content can usually be attributed to configuration or permission based issues in IIS. Although The Archiving Software setup wizard attempts to detect and resolve these configuration issues, manual configuration may be necessary.

Please follow these steps to troubleshoot:

1. On the computer where you installed the Web component, check that the aaWeb IIS application exists in the Default Web Site. If the application is not there, follow these instructions to create it.

2. On the computer where you installed the Service component, check that the aaWebService IIS application exists within the Default Web Site. If the application is not there, follow these instructions to create it.

3. Launch a web browser and enter the following URL:
   http://SERVER/aaWeb/default.aspx
   where SERVER is the hostname or IP address of the computer where you installed the Web component.

   If successful, you should see a screen that says Configured AA Services and shows a listbox with one entry, indicating one service in an Idle state.

   If you do not see a screen like this, please refresh the page and try one more time. If the page does appear, then please try clicking on the message stub link again. If an error still occurs, please continue with the troubleshooting process.

4. If you are using IIS 6.0 (or later), check that the status of the ASP.NET v2.0 web extension is set to Allowed. To verify this, launch IIS manager from within Administrative Tools from within the Windows control panel, and look in the Web Service Extensions list.

5. Open the IIS manager on the computer(s) where the Web component and Service component are installed, right click either aaWeb or aaWebService, click the ASP.NET tab, and verify that the ASP version is set to 2.0.

6. If you are using IIS 6.0 (or later), on the computer where the Web component was installed, start the IIS manager and click the MIME Types list. If .msg is missing from the list of MIME types, add a new MIME type with an extension of .msg (including the period) and a MIME type of application/outlook.

7. On the computer where the Web component was installed, start IIS manager, right click aaWeb, and choose Properties. Click the Documents tab. Make sure Enable default content page is checked and make sure that default.aspx is in the list.

8. On the computer where the Web component was installed, start IIS manager, right click Default

Web Site and choose Properties. Click the Web Site tab. Check that the TCP port is set to 80.

9. On the computer where the Service component was installed, start IIS manager, right click aaWebService, and choose Properties. Click the Directory Security tab. Click the Edit button in the Authentication and access control group. Make sure that it is set to use the Windows user that meets all of the requirements listed in the windows security setup for the Service component.

Please contact technical support if these steps do not resolve your issue.

6-4-3 Archiving fails with MAPI_E_UNKOWN_FLAGS

This topic will help you resolve an error where you have archiving policies configured and they appear to run, but no messages appear in your archive, and where your processing log contains an error message with MAPI_E_UNKNOWN_FLAGS in the error text.

This error is caused when the Service component is installed onto an Exchange 2003 server or a computer that has Outlook 2000 on it (instead of Outlook 2003 or better). The version of MAPI provided by Microsoft with these application versions do not support the Unicode message format.

To resolve this issue, you must change the archiving format to ASCII instead of Unicode (which is the default). Follow these steps to do this:

1. Open The Archiving Software management console, and go to the User Groups page.
2. For each user group, select all users, right click, and choose Edit user settings (this will edit the properties of all users in the user group at the same time).
3. Change the MSG Format in the lower-left hand corner of the page to ASCII.
4. Save all changes.

Future versions of the software will allow setting a default message format for all users. If the error continues to happen after making this change, please contact technical support.

6-5-1 Checking the System Path

The Archiving Software requires that its executables be in the system path for proper operation. Normally, the setup wizard is able to automatically modify your system path. If the setup wizard encounters an error, you will need to manually add the appropriate directory to your system path.

The following location is the installation directory and should be in your system path:

```
(program files)\(location of <The Backup Software>)\email-archiving-exch
```

To check if the directory is in the path or to add it to the path, follow these steps:

1. In Windows explorer, right click on My Computer and choose Properties.
2. Click the Advanced tab.
3. Click the Environment Variables button.
4. In the System Variables list, find and highlight the Path entry and click Edit.
5. If you do not see the installation directory listed anywhere within the variable value, then add a semicolon (;) to the end, followed by the full path of the installation directory.

6-5-2 Creating the Web IIS Application

The setup wizard for The Archiving Software will automatically create an IIS application called aaWeb on the computer where you chose to install the Web component. If the setup wizard encounters an error, you will need to manually add the IIS application using the IIS management console.

To configure the aaWeb IIS application, follow these steps on the computer where you installed the Web component:

1. Navigate to the Windows control panel, and start the Administrative Tools.
2. Launch the Internet Information Service (IIS) management application.
3. Navigate to the root of the Default Web Site and expand it to see the list of configured web applications.
4. If aaWeb is not present, then right click Default Web Site and choose New Virtual Directory.
5. Complete the Virtual Directory Creation Wizard using the following settings
   - Name: aaWeb
   - Directory: `(program files)\(<The Backup Software>)\email-archiving-exch\WebSite`
   - Make sure the Read and Run Scripts permissions are checked.
6. Right click on the aaWeb application and choose Properties.
7. Click the Directory Service tab. Click the Edit button in the Authentication and access control settings group.
8. Make sure that the Enable anonymous access is checked, and that you configure it to use a Windows account that has local administrative privileges on the machine. Click OK to close the Authentication Methods dialog.
9. Back on the Properties page, click the ASP.NET tab. Make sure that version 2.0 is selected. Click OK to save all changes.

The IIS web application that hosts the logic for the Web component has now been configured.

6-5-3 Creating the Web Service IIS Application

The setup wizard for The Archiving Software will automatically create an IIS application called aaWebService on the computer where you chose to install the Service component. If the setup wizard encounters an error, you will need to manually add the IIS application using the IIS management console.

These instructions are very similar to those for configuring the IIS web application for the Web component. The main differences are that the virtual directory path is different, and the Windows user you should select needs to be the Windows user that you configured for the Service component.

To configure the aaWebService IIS application, follow these steps on the computer where you installed the Service component:

1. Navigate to the Windows control panel, and start the Administrative Tools.
2. Launch the Internet Information Service (IIS) management application.
3. Navigate to the root of the Default Web Site and expand it to see the list of configured web applications.
4. If aaWebService is not present, then right click Default Web Site and choose New Virtual Directory.
5. Complete the Virtual Directory Creation Wizard using the following settings
   - Name: aaWebService
   - Directory: `(program files)\(<The Backup Software>)\email-archiving-exch\WebService`
   - Make sure the Read and Run Scripts permissions are checked.
6. Right click on the aaWebService application and choose Properties.
7. Click the Directory Service tab. Click the Edit button in the Authentication and access control settings group.
8. Make sure that the Enable anonymous access is checked, and that you configure it to use the Windows account that you setup for the Service component (see windows security setup for details).
9. Back on the Properties page, click the ASP.NET tab. Make sure that version 2.0 is selected. Click OK to save all changes.

The IIS web application that hosts the logic for the Service component has now been configured.

7-1-1 Why can't I see options for open file backup?

Open file backup requires Windows XP, Windows 2003 Server, or better. If you have an older version of Microsoft Windows then the options for open file backup will not be displayed (it is automatically disabled). If you are running a version of Microsoft Windows that supports Volume Shadow Copy but the options are not displayed then please contact technical support.

7-1-2 Why does open file backup fail with error 8000fff (E_UNEXPECTED)?

This error can be caused by the Volume Shadow Copy service having a startup type of Disabled. To resolve this error, follow these steps:

1. Start the Services task within Administrative Tasks. Alternatively, run services.msc
2. Locate the Volume Shadow Copy service in the list.
3. Right click on the service and choose Properties.
4. Change the Startup Type to Manual.
5. Click OK to apply your changes.

7-1-3 Why does open file backup fail with error80042306 (VSS_E_PROVIDER_VETO)?

This error usually indicates one of the following conditions:

- Insufficient disk space. Volume shadow copy requires at least 100MB of free disk space for each volume (drive) in the snapshot set.
- All volumes were formatted with the FAT32 format. This is common if you upgraded from Windows 95/98/Me and chose not to convert your volumes to NTFS format. Volume Shadow Copy requires at least one NTFS partition to function correctly. You should either add a new hard disk and format it with NTFS or you should convert one of your FAT32 partitions to NTFS (backup your data first; please see here and here for more information).

It can also indicate an extremely high volume of I/O operations causing the snapshot creation operation to fail. Please inspect your system log (use the Event Viewer administrative tool or run eventvwr.msc) for VSS or VOLSNAP entries, and email these to our Technical Support Department.

7-1-4 Why does open file backup fail with error 800423f4?

This error can be caused by the SQL Server (MSDE) volume shadow copy writer when the SQL Server database recovery model is not set to simple.

To resolve this error, please change your SQL Server database recovery model to simple. The Backup Software automatically performs incremental backups, so the more complicated recovery models should not be used, as they interfere with the backup process and create redundant data. Please see here and here for more information.

Procedure to change the database recovery model to simple:

1. Start SQL Server Enterprise Manager.
2. Navigate to each database that you are backing up.
3. Right-click each database and choose Properties.
4. Click the Options tab.
5. Under Recovery, set the model to Simple.

This error can also be caused when the SQL Server (or MSDE) startup service is running under a startup account with the format .\UserName.

To resolve this error, configure the startup account of the SQL Server service to use the LocalSystem account. Alternatively, use a fully qualified user name: Domain\UserName. Please see here for more information.

Procedure to change the startup account of the SQL Server service:

1. Start the Services task within Administrative Tasks. Alternatively, run services.msc
2. Locate the MSSQLSERVER service in the list.
3. Right click on the service and choose Properties.
4. Click the Log On tab.
5. Change Log on as to be the Local System account. Alternatively, click This account and specify an account located within a domain.

7-2-1 What will I need to recover a forgotten pass phrase?

To recover a forgotten pass phrase you will need:

- A computer that has the client software installed on it
- Your account username and password
- The exact answers to your security questions.

However, you will not need to remember the security questions themselves.

7-2-2 Why is the pass phrase stored on your server secure?

Ensuring your privacy and security is our number one priority. Your pass phrase is encrypted twice before it is stored on the server to prevent anyone but you from recovering the stored pass phrase. The system is designed so that recovering a pass phrase requires action from two people: the person that created the key and a senior level server technician. Neither person can recover the pass phrase without the cooperation of the other person. The system is also designed so that only the creator of the pass phrase can view the pass phrase once it is recovered.

Is this secure? Will someone be able to access my data?

Using 2 layers of encryption around the stored pass phrase offers a very high level of protection. The outer layer requires our 3072-bit private key to decrypt. This private key is encrypted by our master pass phrase recovery password, which is never written down and is known by only a few people (it is a closely guarded secret). Even those who know the master pass phrase recovery password cannot view your pass phrase because of the inner layer of encryption protecting your pass phrase.

Decrypting the inner layer of encryption requires knowing the answers to your security questions. The security questions themselves are only protected by the outer layer of encryption (anyone with the private key has access to your security questions). Thus, you should choose questions that are difficult for another person to answer (and yet will be something you will never forget). The more questions you use the harder it is to break the inner layer of encryption. Each additional question makes it exponentially more difficult. We recommend using at least four security questions to protect your pass phrase. The answers to your security questions are only used to encrypt the pass phrase and are never sent across the Internet, stored on the server, or remembered by the client software.

Technical Details

When your pass phrase is stored on the server it is secured by following this process:

1. You select a series of questions that only you should know the answer to and then provide the answers. You should use enough questions such that you are sure that only you will have the answers to all of the questions.
2. The answers to the questions are used to generate a 256-bit encryption key by following the standard described in RFC2898 (using SHA-256 for the hash function).
3. The pass phrase is encrypted using the Advanced Encryption Standard (AES) algorithm and the encryption key derived from the answers to your security questions.
4. A random 256-bit file encryption key is generated and is used to encrypt your encrypted pass phrase and your list of security questions (but not their answers) using the AES-256 algorithm. The dually encrypted pass phrase and the encrypted list of security questions is called a pass phrase envelope.
5. The random 256-bit file key is encrypted using our 3072-bit public key. Only someone with the matching private key can decrypt this data. We are the only ones with access to the private key.
6. The encrypted 256-bit file key along with the pass phrase envelope is sent via SSL (an encrypted Internet connection) to our server, where it is stored. The permissions on the stored file are narrowed such that only a senior level server technician can access the data.

When you need to recover your pass phrase it is secured by the following process:

1. You use the client software to request that your pass phrase be recovered. The software generates a new 3072-bit public/private key pair (this is your request key).
2. The public request key and the details of your request are sent via SSL to our server, where it is stored.
3. A senior level server technician will use the master pass phrase recovery program to decrypt the outer layer of your stored pass phrase envelope. This requires that the operator to enter the master pass phrase recovery password, which decrypts our 3072-bit private key.
4. At this point your pass phrase is still encrypted with the 256-bit encryption key that was generated by the answers to your questions. As the technician does not know the answers to your security questions your pass phrase is still private.
5. The recovery program generates a new 256-bit file key and encrypts the pass phrase envelope. The pass phrase envelope is now fully encrypted again. The new 256-bit file key is encrypted with your request public key. Now only the person that can decrypt the pass phrase envelope is the person with the request private key (the person that submitted the request).
6. The newly encrypted pass phrase envelope is stored on the server. The technician emails you notifying you that your request has been handled.
7. You use the client software to connect to our server and download the response over an SSL connection.
8. The client software uses the request private key to decrypt the outer layer of the pass phrase envelope.
9. The client software presents your security questions. If you correctly answer these questions then it will be able to decrypt the final encryption layer protecting your pass phrase, and your pass phrase will be recovered.

7-3-1 How can I backup SQL server databases?

The answer can be summarized as follows:

- Create a sub-account for each database server.
- Login to each database server as a user that has rights to read the database files.
- Install and configure The Backup Software on each database server.
- Add the folder containing your database files (*.mdf and *.ldf) to the backup.
- Change the database recovery model to Simple. More information on why this is required is available here.
- With the database recovery model set to Simple you do not need to use the backup functionality of SQL Server, as long as The Backup Software is successfully backing up your database on a regular basis.

The Backup Software will automatically perform differential, hot backups of your database. If using the Simple recovery model does not meet your needs then you should configure The Backup Software to backup the directory where SQL Server places its backup files. More information on SQL Server recovery models is available here.

Procedure to change the database recovery model to simple:

1. Start SQL Server Enterprise Manager.
2. Navigate to each database that you are backing up.
3. Right-click each database and choose Properties.
4. Click the Options tab.
5. Under Recovery, set the model to Simple.

7-3-2 How can I restore an SQL Server database?

The procedure depends on whether you were backing up your database using the simple recovery model or another recovery model. If you were using the simple recovery model and volume shadow copy service (the default database backup procedure for The Backup Software) then follow these procedures:

1. Use the file manager to select the database files (*.mdf and *.ldf) you want to restore.
2. On the Restore Data: Options screen, choose to restore the files to a folder that is different from the folder containing your existing database files. Please choose a location that is on a local hard disk (SQL Server will not attach databases on network storage)
3. Be sure not to overwrite any existing files when performing the restore.
4. Follow the steps in the wizard to finish the restore process.
5. Login as the database administrator and open a SQL command window.
6. For each database your need to restore, perform the following SQL commands:

```
use master
go
sp_detach_db 'databasename'
go
sp_attach_db 'databasename' 'path to mdf file' 'path to ldf file'
go
```

7. After you have verified all data was restored successfully, you may delete the old mdf and ldf files.

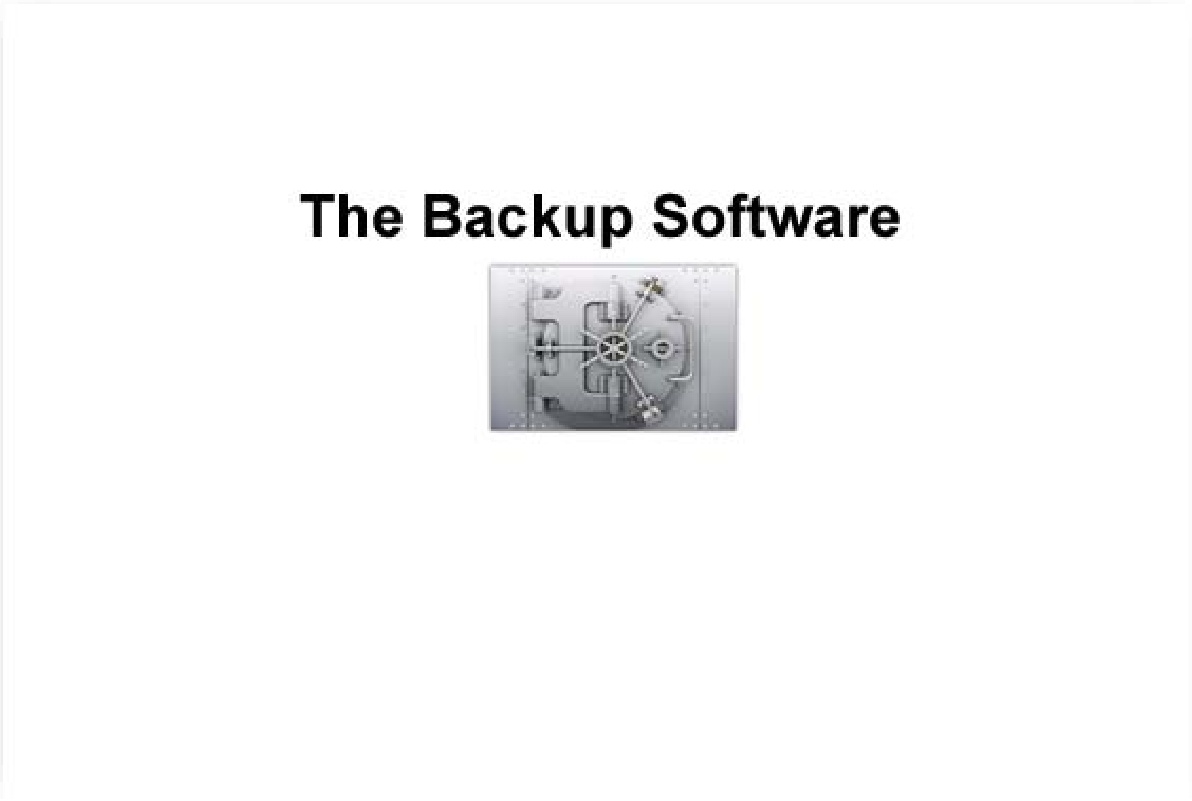
If you only need to perform partial recovery of a database, then follow this procedure:

1. Restore the mdf and ldf files following steps 1 - 4 from above.
2. Login as the database administrator and open a SQL command window.
3. For each database you need to extract information from, perform the following SQL commands:

```
use master
go
sp_attach_db 'temp_databasename' 'path to mdf file' 'path to ldf file'
go
        (use SQL commands or other tools to copy data you want to restore
        from temp_databasename to the live database)
sp_detach_db 'temp_databasename'
go
```

4. After you have restored all the data you need you may delete the downloaded mdf and ldf files.

If The Backup Software was not backing up the mdf and ldf files directly but was rather backing up SQL Server backup files, then please restore the SQL Server backup files and follow the restore procedures found here.



The Backup Software