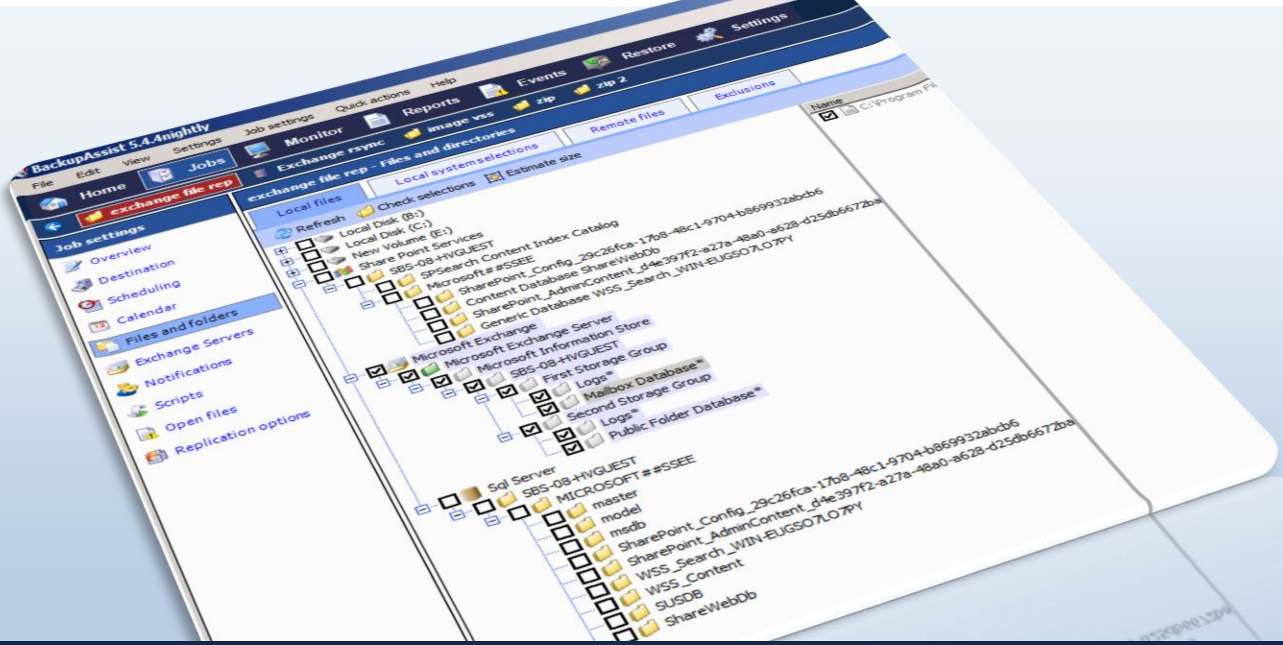


BackupAssist v6 quickstart guide

This guide is intended for users that have upgraded to BackupAssist v6 from a previous version of BackupAssist. A basic understanding of how to use BackupAssist is assumed. If you are new to BackupAssist we recommend that you read the help file that comes with the software, as well as consult the Documentation section of our website. You can also contact our support team at support@backupassist.com for further assistance.

Using the new features in BackupAssist v6

VSS application backup (Exchange, SQL, SharePoint)

File Replication, Zip, Rsync and Windows Imaging

The Microsoft Volume Shadow Copy Service or VSS is used to create point-in-time copies or snapshots of drives where files are in use. In previous versions of BackupAssist, it was possible to back up locally running VSS applications, but it was a manual process that required you to select the relevant files. BackupAssist v6 now includes fully integrated support for local VSS application backup and restore.

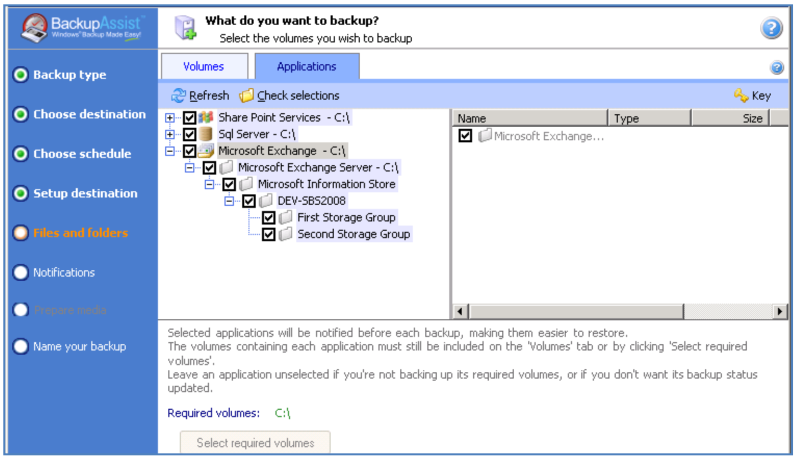
Backing up VSS applications

1. Launch BackupAssist and either choose an existing File Replication, Zip, or Windows Imaging job to edit from the **Edit** menu, or create a new job by going to **File > New backup job**.
2. When creating a new job, select VSS applications to back up during the Files and folders step.

> **Note**: locally installed VSS applications will be automatically detected and listed. If an application is not listed, try re-starting it and then click the **Refresh** button in BackupAssist.
>
> **Note**: BackupAssist cannot be used to back up VSS applications running on remote machines.

Imaging jobs (Server 2008 and REV / rdx drive jobs on Server 2008 R2)

For Imaging jobs running on Windows Server 2008 or jobs to a REV or rdx drive on Windows Server 2008 R2, VSS applications are backed up as part of a full volume snapshot. If you choose a VSS application to back up, the volumes that must be selected will be listed in red. Click the **Select required volumes** button if a required volume is not in your selections.



What do you want to backup?
Select the volumes you wish to backup

☑ Share Point Services - C:\
☑ Sql Server - C:\
☑ Microsoft Exchange - C:\
 ☑ Microsoft Exchange Server - C:\
  ☑ Microsoft Information Store
   ☑ DEV-SBS2008
    ☑ First Storage Group
    ☑ Second Storage Group

☑ Microsoft Exchange...

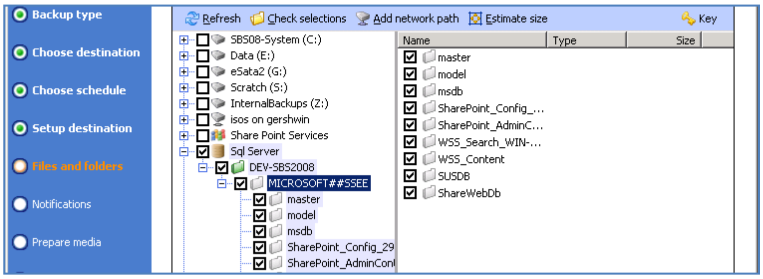
Selected applications will be notified before each backup, making them easier to restore.
The volumes containing each application must still be included on the 'Volumes' tab or by clicking 'Select required volumes'.
Leave an application unselected if you're not backing up its required volumes, or if you don't want its backup status updated.

Required volumes: C:\

File Replication, Zip and Imaging[1] jobs

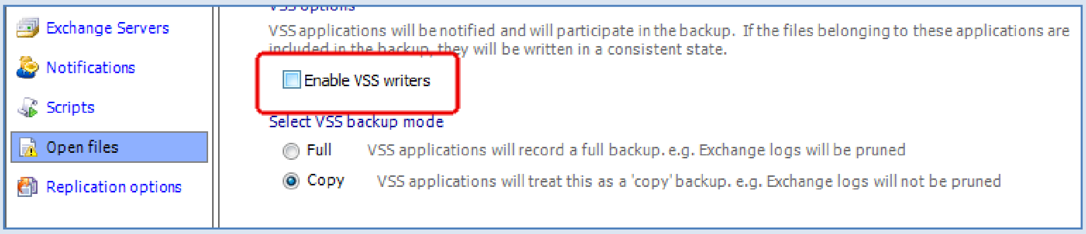
Select either entire VSS applications or drill down and choose individual components:

[1] Imaging jobs running on Windows Server 2008 R2 only (excludes jobs backing up to REV / rdx drives)



3. If you are editing an existing job navigate to **Volume selection** from the left menu for a Windows Imaging job and **Files and folders** from the left menu for a Zip or File Replication job.

> **Note:** if you select VSS applications in the Files and folders tab we recommend disabling the **Enable VSS writers** option in the Open files tab. If the **VSS writers** option is enabled VSS will contact all applications before and after a backup, which can be slow and may cause the VSS application to register that a backup has been completed when it has not.



VSS applications will be notified and will participate in the backup. If the files belonging to these applications are included in the backup, they will be written in a consistent state.

☐ Enable VSS writers

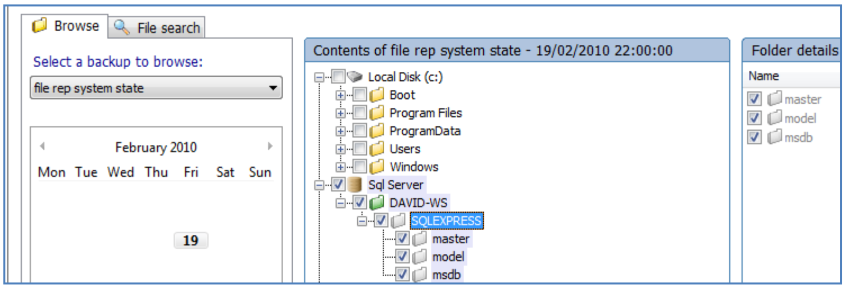
Select VSS backup mode

○ Full VSS applications will record a full backup. e.g. Exchange logs will be pruned

● Copy VSS applications will treat this as a 'copy' backup. e.g. Exchange logs will not be pruned

Restoring VSS applications

1. In BackupAssist, Click **Restore** in the top navigation bar and choose **BackupAssist Restore Console**.
2. Click **Load all known backups** or **Browse** to locate the backup set from which you want to restore.
3. Choose the job that corresponds to the backup from which you want to restore a VSS application.
4. Use the calendar to select the date of the backup from which you want to restore.
5. Use the middle pane to expand the loaded backup set and select the application(s) you want to restore.



6. Click the **Restore to** button located on the bottom right and follow the remaining prompts.

> **How the VSS application restore works**
> VSS supports live application restore, which means that you do not need to stop a running application before recovering a previous version of it from a backup.
>
> If any Windows services need to be stopped and restarted during an application restore this will happen automatically. If, for example, you are recovering an SQL Server and the SQL database being restored is in use, SQL Server will automatically deny access to the database until the restore is complete. Databases that are not part of the restore will not be affected unless the master database is being restored. If the master database is being restored, the entire SQL service will be stopped and restarted after the restore has completed.

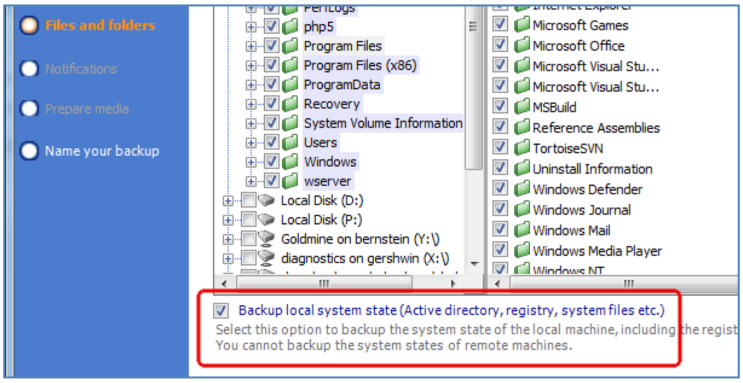
System State backup and restore

File Replication, Zip, and Windows Imaging[3]

With BackupAssist v6 you can schedule 'System State only' backups across all modern Windows operating systems, or back up the System State as part of a larger backup including files and applications, using File Replication, Zip, or Windows Imaging[2]. A System State backup includes important Windows systems settings, such as the Registry, and is crucial for system recovery. System State backups for Windows 7 and Server 2008 are usually between 7GB and 15 GB. For XP and Server 2003, they are much smaller: 200MB to 300 MB.

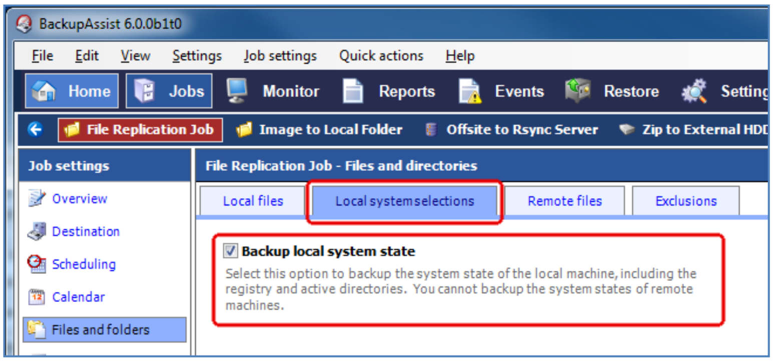
Backing up the System State

1. Launch BackupAssist and either choose an existing File Replication, Zip, or Windows Imaging job to edit from the **Edit** menu, or create a new job by going to **File > New backup job**.
2. When creating a new job check **Backup local system state** during the Files and Folders step:



☑ Backup local system state (Active directory, registry, system files etc.)
Select this option to backup the system state of the local machine, including the regist
You cannot backup the system states of remote machines.

3. If you are editing an existing job select **Files and folders** from the left menu, click the **Local system selections** tab, and then enable the **Backup local system state** option.



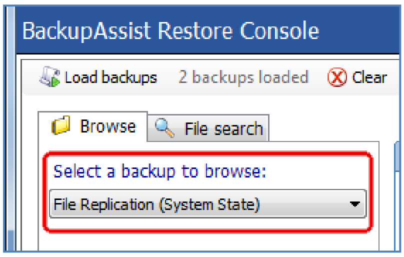
☑ **Backup local system state**
Select this option to backup the system state of the local machine, including the registry and active directories. You cannot backup the system states of remote machines.

Restoring the System State

Note: you cannot restore the System State from an Image backup using the BackupAssist Restore Console. You must use the built-in Windows tool, **wbadmin**. Visit wbadmin.info for instructions.

1. In BackupAssist, Click **Restore** in the top navigation bar and choose **BackupAssist Restore Console**.
2. Click **Load all known backups** or use **Browse** to locate the backup set from which you want to restore.
3. Choose the job that corresponds to the backup from which you want to restore the System State:

[2] Individual System State backup with Windows Imaging only on Server 2008 R2 where the destination is not rdx/REV or NAS.

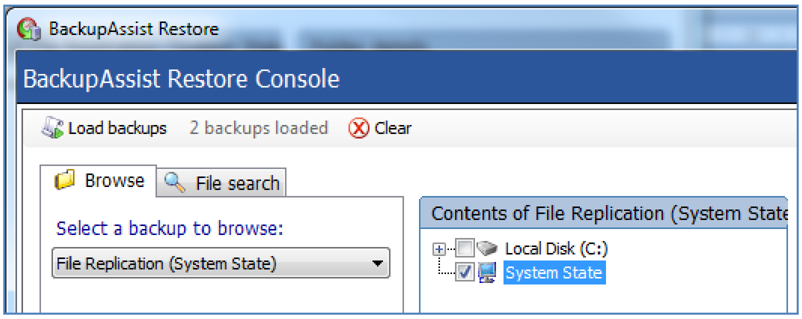


Select a backup to browse: File Replication (System State)

4. Use the calendar to select the date of the backup from which you wish to restore.

> **Note**: dates for which backups are available are marked in **bold** on the calendar.

5. Use the middle pane to expand the loaded backup set and select the System State to restore.

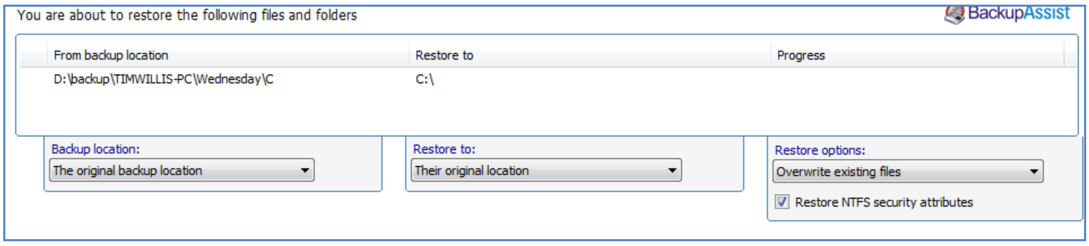


Select a backup to browse: File Replication (System State)

☐ Local Disk (C:)
☑ System State

> **Note:** you may see files located on the Windows system drive (C: drive in the example above) available for restore. These files are associated with the System State. If you choose to restore individual files from this list and not the System State, the System State will not be restored, and the files themselves may not restore correctly. If you want to perform a full restore we recommend selecting **both** the System State and all other files listed.

6. Once you have made your selections click the **Restore to** button on the bottom right of the window.
7. The restore confirmation screen will then load:



You are about to restore the following files and folders

From backup location	Restore to	Progress
D:\backup\TIMWILLIS-PC\Wednesday\C	C:\	

Backup location: The original backup location

Restore to: Their original location

Restore options: Overwrite existing files

☑ Restore NTFS security attributes

You can choose to restore the System State either to its original location or to an alternate location of your choosing. If you select an alternate location click **[...]** to set an alternate restore path.

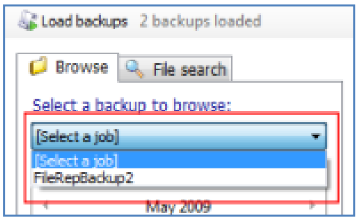
8. Once you have selected where to restore the System State to, click **OK** to perform the restore.

> **Note**: if you are restoring the System State to a machine that hosts Directory Services, you will be prompted to reboot into the Directory Services Restore Mode.
>
> **Note:** Before the restore starts, BackupAssist will take a VSS snapshot of the volumes to be restored, so you can roll back to a pre-restore state, if necessary, using Windows' previous versions feature.

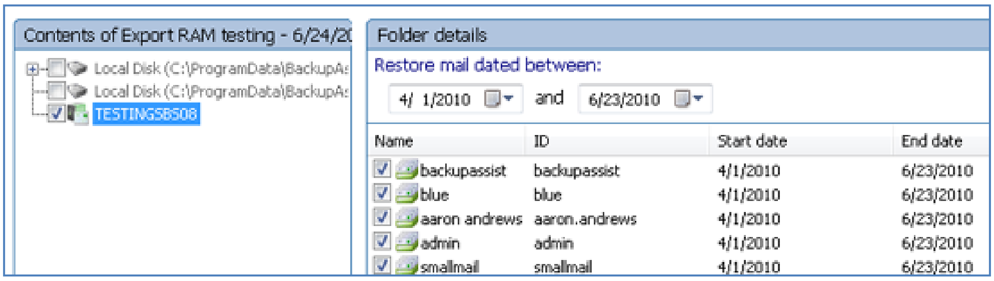
Exchange mailbox and public folder restore

Using the BackupAssist v6 Restore Console you can easily restore Exchange mailboxes and public folders either directly back into the Exchange Server or to an alternate Exchange Server of your choosing.

1. In BackupAssist, Click **Restore** in the top navigation bar and choose **BackupAssist Restore Console**.
2. Click **Load all known backups** or **Browse** to locate the backup set from which you want to restore.
3. Choose the job that corresponds to the backup from which you want to restore mailboxes:



4. Use the calendar to select the date of the backup from which you wish to restore.
5. If any mailbox or public folder backups are included in the loaded backup set, named Exchange Server(s) will be listed in the middle pane. If you select an Exchange Server a list of mailboxes available for restore will appear to the right. Choose which mailboxes to restore, as well as the date range of the mail items you want to recover (e.g. you might want to retrieve all of jan.doe's mail data from July 2010).

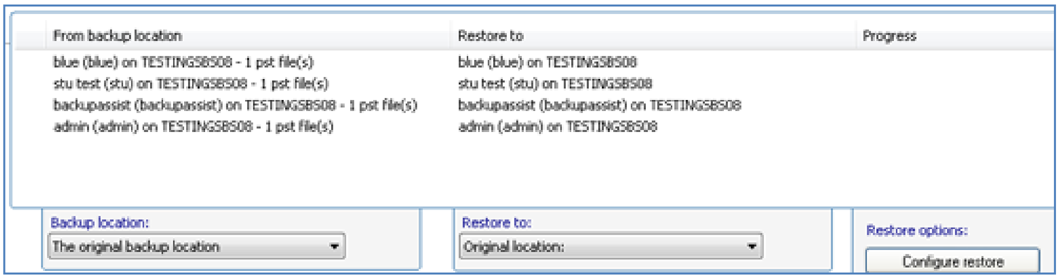

Contents of Export RAM testing - 6/24/20
Local Disk (C:\ProgramData\BackupAs
Local Disk (C:\ProgramData\BackupAs
TESTINGSBS08
Folder details

Restore mail dated between: 4/ 1/2010 and 6/23/2010

Name	ID	Start date	End date
☑ backupassist	backupassist	4/1/2010	6/23/2010
☑ blue	blue	4/1/2010	6/23/2010
☑ aaron andrews	aaron.andrews	4/1/2010	6/23/2010
☑ admin	admin	4/1/2010	6/23/2010
☑ smallmail	smallmail	4/1/2010	6/23/2010

Please note: mailboxes must be restored separately to other data. If you need to restore files, applications or the System State, you will need to complete this as a separate restore task.

6. Once you have made your selections click the **Restore to** button to be taken to the confirmation screen.



From backup location	Restore to	Progress
blue (blue) on TESTINGSBS08 - 1 pst file(s)	blue (blue) on TESTINGSBS08	
stu test (stu) on TESTINGSBS08 - 1 pst file(s)	stu test (stu) on TESTINGSBS08	
backupassist (backupassist) on TESTINGSBS08 - 1 pst file(s)	backupassist (backupassist) on TESTINGSBS08	
admin (admin) on TESTINGSBS08 - 1 pst file(s)	admin (admin) on TESTINGSBS08	

Backup location: The original backup location

Restore to: Original location:

7. In the middle drop-down menu choose where you want to restore your mailbox and public folders to:
   1. **Original location**: mailboxes will be copied directly back to the original Exchange Server.
   2. **Alternate server:** mailboxes will be copied to an alternate Exchange Server of your choosing. Click the **Select** button to choose an alternate server.
   3. **Alternate path:** mailboxes will be restored as separate PST files to a single folder. You can then open up any of the PST files extracted with Outlook and drag-and-drop the required mail items back to a the user's live mailbox. This option is useful if your PST backups are distributed across multiple folders (e.g. you used a grouping period).

If you choose to restore your mailboxes to either their original location or an alternate server, you can click the **Configure restore** button located under 'Restore options' to change how mailboxes are restored. Here you can individually specify which mailbox each backup should overwrite in your Exchange Server. This is useful if an Exchange Server mailbox has been renamed since being backed up, or if you want to overwrite one mailbox with another.

8. Click **OK** to perform the restore.

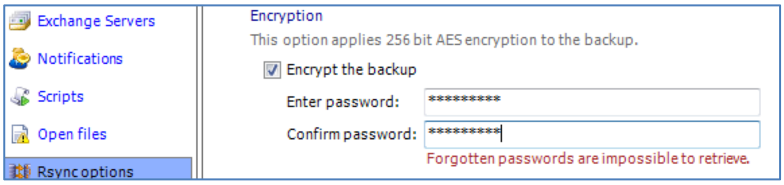
‘Cloud’ ready Internet backup features

Requires BackupAssist for Rsync (Standalone or Add-on)[3]

Enabling AES-256 encryption

BackupAssist for Rsync now provides data encryption at the Server using AES-256 bit encryption in an Rsync friendly format. File names and directory names are also obfuscated so data on the host cannot be read.

1. Select **Edit** from the top file menu and choose an appropriate Rsync backup job.
2. Click **Rsync options** on the left menu and check **Encrypt the backup** and enter your password.



Encryption

This option applies 256 bit AES encryption to the backup.

☑ Encrypt the backup

Enter password: *********

Confirm password: *********

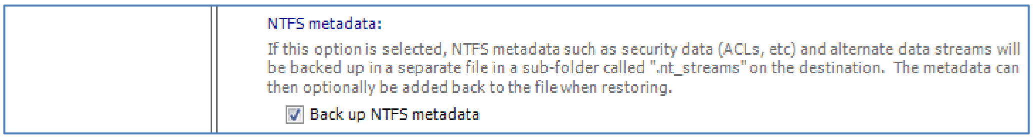
Forgotten passwords are impossible to retrieve.

Note: if you enable or disable encryption for your Rsync job, BackupAssist will need to "re-seed" your backup to the Rsync backup destination with a full set of data (i.e. the next backup will be a full backup regardless of how many files have changed).

Backing up NTFS metadata

With the **NTFS metadata** option enabled, NTFS streams, such as alternate data streams and security data will be saved to a separate file on the Rsync backup destination and then added back to the file as part of the restore process when data is restored using the BackupAssist Restore Console.

1. Select **Edit** from the top file menu and choose an appropriate Rsync backup job.
2. Click **Rsync options** on the left menu and check **Back up NTFS metadata**.



NTFS metadata:

If this option is selected, NTFS metadata such as security data (ACLs, etc) and alternate data streams will be backed up in a separate file in a sub-folder called ".nt_streams" on the destination. The metadata can then optionally be added back to the file when restoring.

☑ Back up NTFS metadata

Hyper-V backup and restore capabilities

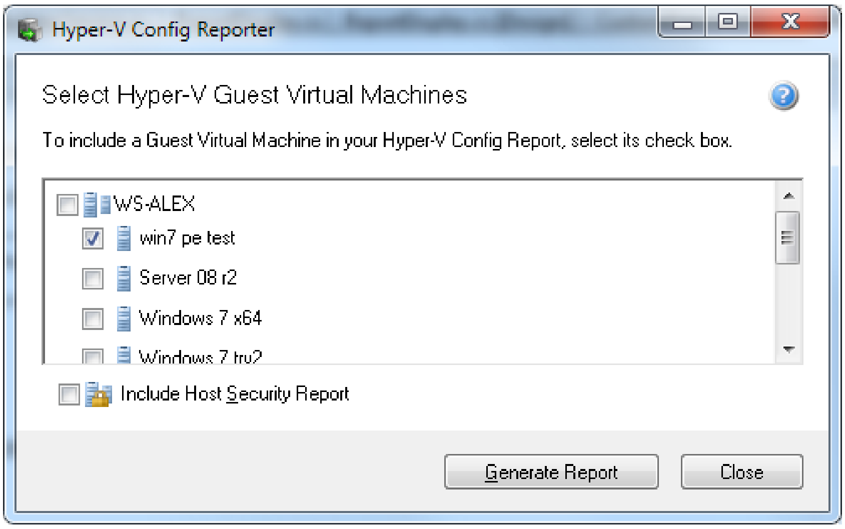
The BackupAssist VM Granular Restore Console Add-on

The Hyper-V Config Reporter

The BackupAssist VM Granular Restore Console Add-on now includes the Hyper-V Config Reporter, which automates the tasks of documenting your Hyper-V configuration settings. You can generate a HTML report of your Hyper-V Host and Guest Virtual Machine settings, making it easy to recreate an existing VM on a new Host.

[3] BackupAssist for Rsync can be purchased as an add-on or as a standalone product.

1. Run the Hyper-V Config Reporter from the Windows Start Menu (**Start > Programs > BackupAssist v6 > Hyper-V Config Reporter**) on the Hyper-V Host machine.
    - ○ Alternatively, run **Hyper-V Config Reporter.exe** from the HyperVConfigReporter folder located in the BackupAssist installation directory (e.g. C:\Program Files (x86)\BackupAssist v6).
2. The Hyper-V Config Reporter will display a list of Guests VMs that are configured on the Hyper-V Host.



Hyper-V Config Reporter

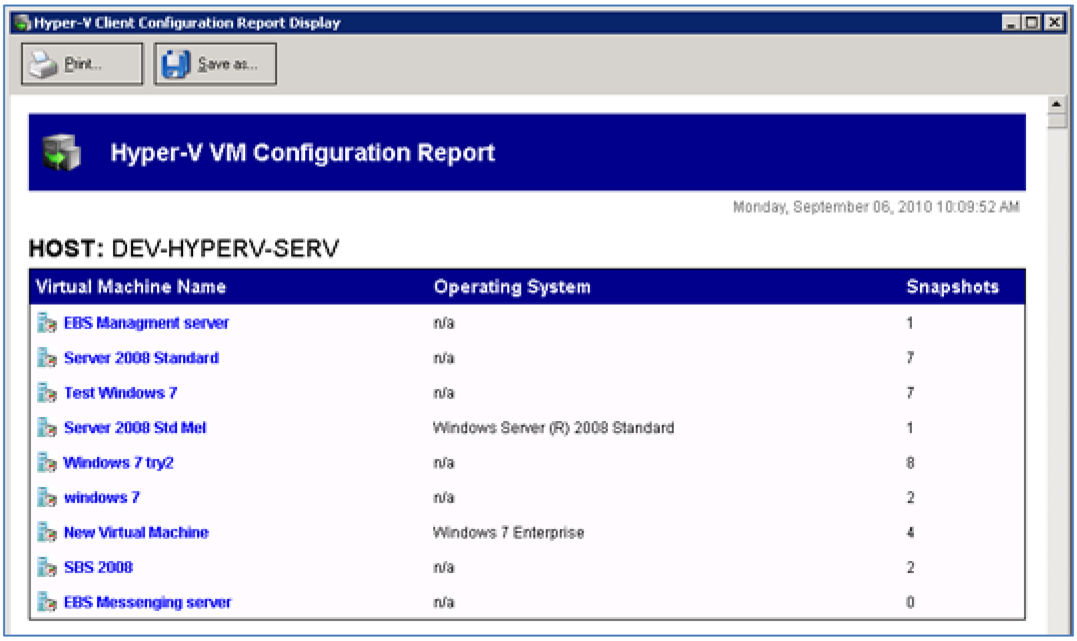
Select Hyper-V Guest Virtual Machines

To include a Guest Virtual Machine in your Hyper-V Config Report, select its check box.

- □ WS-ALEX
    - ☑ win7 pe test
    - □ Server 08 r2
    - □ Windows 7 x64
    - □ Windows 7 try2

□ Include Host Security Report

3. Select Guest VMs from the list and click **Generate Report**.
    - ○ **[Optional]** Check **Include Host Security Report** to include security and access settings configured on the Hyper-V Host in your report.
4. A HTML report will then be created and displayed in a new window.



Hyper-V Client Configuration Report Display

Hyper-V VM Configuration Report

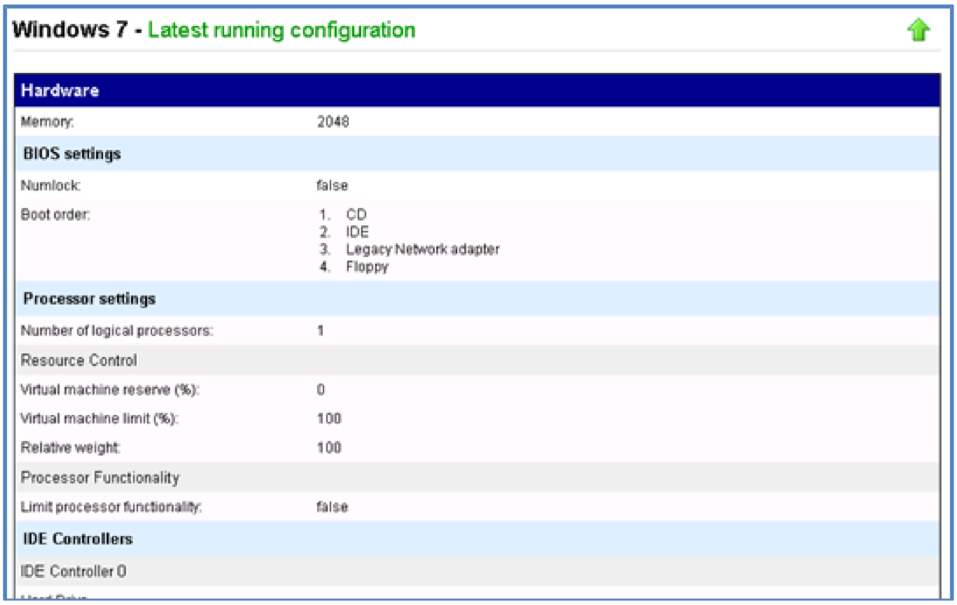
Monday, September 06, 2010 10:09:52 AM

HOST: DEV-HYPERV-SERV

Virtual Machine Name	Operating System	Snapshots
EBS Managment server	n/a	1
Server 2008 Standard	n/a	7
Test Windows 7	n/a	7
Server 2008 Std Mel	Windows Server (R) 2008 Standard	1
Windows 7 try2	n/a	8
windows 7	n/a	2
New Virtual Machine	Windows 7 Enterprise	4
SBS 2008	n/a	2
EBS Messenging server	n/a	0

5. At the top of the report is a list of all the Guest VMs selected. If you click the Virtual Machine Name link of any Guest VM you will be taken to a list of settings for the latest running configuration for that VM.
6. Below this is an additional list of each VM along with its associated snapshots. You can click the link for any snapshot to view settings for that snapshot.

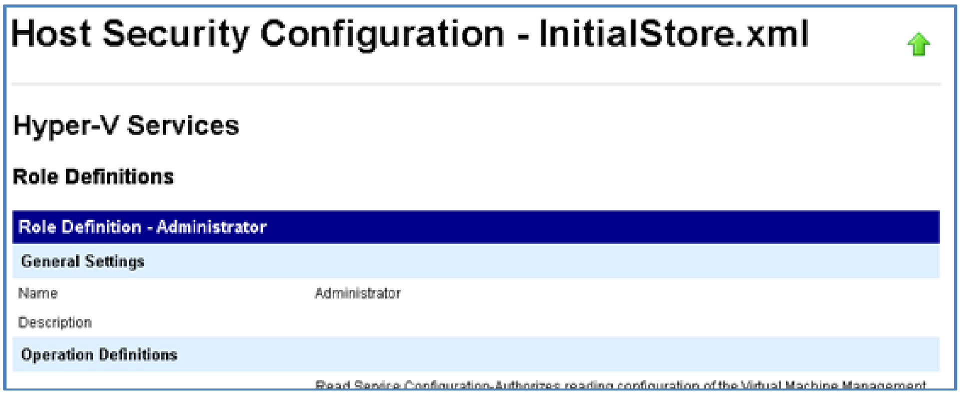
7. Each VM included in the report contains a full list of the VM settings for the latest running configuration at the top, and then a list of any additional snapshots underneath, in date order.



Windows 7 - Latest running configuration

Hardware	
Memory:	2048
BIOS settings	
Numlock:	false
Boot order:	1. CD 2. IDE 3. Legacy Network adapter 4. Floppy
Processor settings	
Number of logical processors:	1
Resource Control	
Virtual machine reserve (%):	0
Virtual machine limit (%):	100
Relative weight:	100
Processor Functionality	
Limit processor functionality:	false
IDE Controllers	
IDE Controller 0	
Hard Drive	

8. The Host Security Report will be located at the very bottom of the overall report:



Host Security Configuration - InitialStore.xml

Hyper-V Services

Role Definitions

Role Definition - Administrator	
General Settings	
Name	Administrator
Description	
Operation Definitions	
	Read Service Configuration-Authorizes reading configuration of the Virtual Machine Management

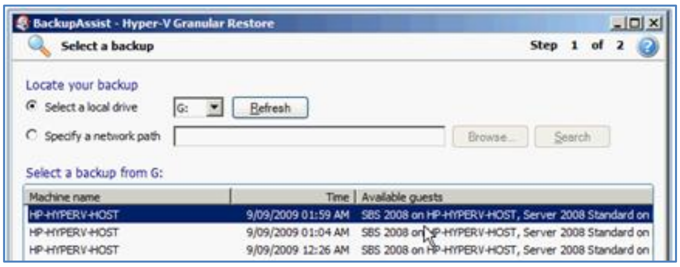
9. You can use the buttons at the top of the Hyper-V Config Reporter window to print a copy of the report, save it to a HTML file that can be opened with a web browser, or close the report window.

Exporting Guest VM drive volumes to .vhd files

You can use the BackupAssist VM Granular Restore Console to export a Guest VM drive volume to a .vhd file so you can easily rebuild a virtual machine in the event of a major disaster scenario:

1. Click **Restore** in the top navigation bar and then click **Hyper-V Granular Restore**.

2. BackupAssist will attempt to detect and list Hyper-V backups located on local drives. Each Hyper-V backup will display a list of Guest VMs that are available for restore under the **Available guests** column.



BackupAssist - Hyper-V Granular Restore

Select a backup — Step 1 of 2

Locate your backup

● Select a local drive: G:

○ Specify a network path

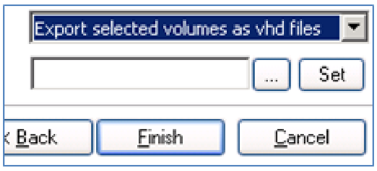
Select a backup from G:

Machine name	Time	Available guests
HP-HYPERV-HOST	9/09/2009 01:59 AM	SBS 2008 on HP-HYPERV-HOST, Server 2008 Standard on
HP-HYPERV-HOST	9/09/2009 01:04 AM	SBS 2008 on HP-HYPERV-HOST, Server 2008 Standard on
HP-HYPERV-HOST	9/09/2009 12:26 AM	SBS 2008 on HP-HYPERV-HOST, Server 2008 Standard on

- If no backups are listed, either connect your backup device to the machine (e.g. external USB HDD) and click **Refresh**, or browse to a network path where Hyper-V Image backups are located by selecting the **Specify a network path** radio button and clicking **Browse**.

3. Select a backup set to restore from and click **Next**.

4. Set the drop-down menu in the bottom right corner to **Export selected volumes as vhd files:**



5. Use the **Mount drives from Hyper-V guest** drop-down menu to select a Guest machine on the Host to restore from. A list of volumes associated with the Guest that can be restored from will appear below.

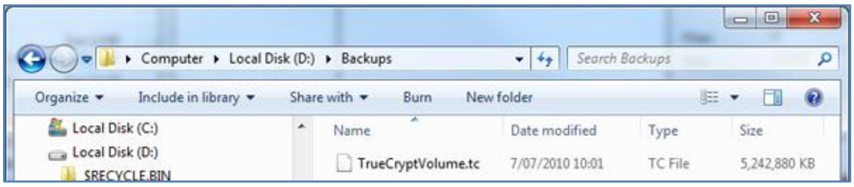
6. Check the drive letters you would like to export as separate vhd files.

7. Set the location that you would like to export the vhd files to in the field location in the bottom right hand corner of the window and then click **Finish** to export the selected volumes.

TrueCrypt-compatible encryption

File Replication and NTBackup

With TrueCrypt-compatible encryption enabled a password encrypted file is created on your backup destination, which contains a virtual encrypted volume that is used to store backups. Encryption occurs on the fly as BackupAssist copies data to the encrypted volume. Anyone browsing the backup destination will see a single TrueCrypt-compatible container file, **TrueCryptVolume.tc**, making the contents of your backups safe:



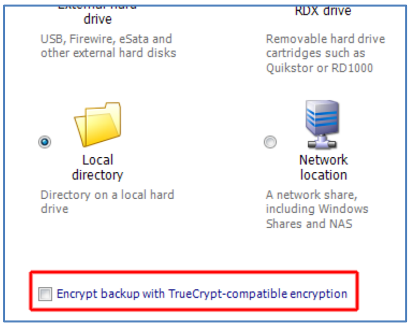
Name	Date modified	Type	Size
TrueCryptVolume.tc	7/07/2010 10:01	TC File	5,242,880 KB

To enable TrueCrypt-compatible encryption on an existing job use the "Select new destination..." button at the top of the destination settings window for a job. To create a job with TrueCrypt-compatible encryption:

1. Go to **File > New backup job** from the file menu.

2. Choose **File Replication** or **NTBackup** as your backup method.

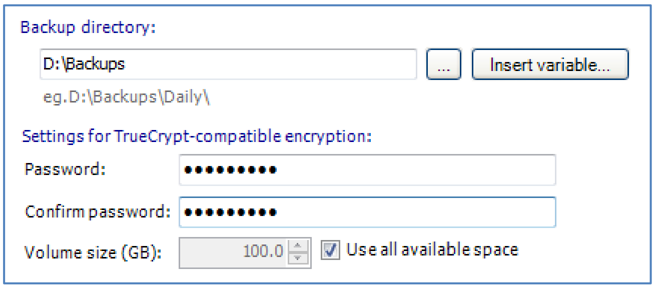
3. Choose your backup destination and check the **Encrypt backup with TrueCrypt-compatible encryption** option located at the bottom-left corner of the window:


External hard drive
USB, Firewire, eSata and other external hard disks
RDX drive
Removable hard drive cartridges such as Quikstor or RD1000
● Local directory
Directory on a local hard drive
○ Network location
A network share, including Windows Shares and NAS
□ Encrypt backup with TrueCrypt-compatible encryption

4. Click **Next** to download and install the TrueCrypt-compatible software if it is not already available.

> The encryption software is designed to run without it needing to be fully installed (for example, it can run from a USB flash drive). We recommend that you do not install another version of TrueCrypt on the same machine as it may interfere with the encryption software that BackupAssist uses.

5. During the **Setup destination** step you will be asked to supply a password for your TrueCrypt-compatible container file. We recommend using a strong password containing a combinations of letters, numbers and punctuation symbols.



Backup directory:
D:\Backups

eg.D:\Backups\Daily\
Settings for TrueCrypt-compatible encryption:
Password: ●●●●●●●●●
Confirm password: ●●●●●●●●●
Volume size (GB): 100.0 ☑ Use all available space

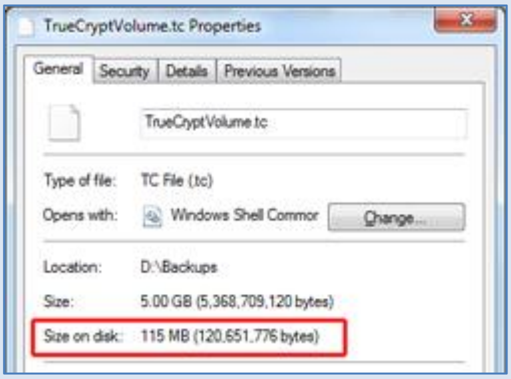
6. Specify the size of the encrypted container file used to store your backup sets.

> BackupAssist will create a dynamically sized encrypted container file that will grow as new backups are added to it up to the maximum size you specify.
>
> If you enable the "**Use all available space**" option, the maximum size of the container file will be equal to the amount of space available on the drive you are backing up to. If you enable this option we recommend that the backup directory be located on a drive dedicated to backups; otherwise the container file may not be able to grow to the maximum size specified when it was created.

7. If you selected the **Most recent full** as your schedule type, you can specify how disk space will be managed on the TrueCrypt-compatible volume. We recommend choosing the **Use all available space** option, which will automatically delete old backups as the disk space used approaches the maximum size of the TrueCrypt-compatible container file.

8. When your job first runs a TrueCrypt-compatible container file will be created on the backup directory. If you are using a portable device, such as a USB hard drive, each time a new drive is connected for a backup, a new container file will be created on the drive if one is not already present:

> **Note**: the size of the TrueCrypt-compatible container file will be reported by Windows as its maximum size. To determine the physical size of the container file (i.e. the actual disk space it is using), right-click it in a Windows Explorer window, select **Properties** and refer to the **Size on disk** value.



TrueCryptVolume.tc
Type of file: TC File (.tc)
Opens with: Windows Shell Commor
Location: D:\Backups
Size: 5.00 GB (5,368,709,120 bytes)
Size on disk: 115 MB (120,651,776 bytes)

Exporting and importing BackupAssist settings

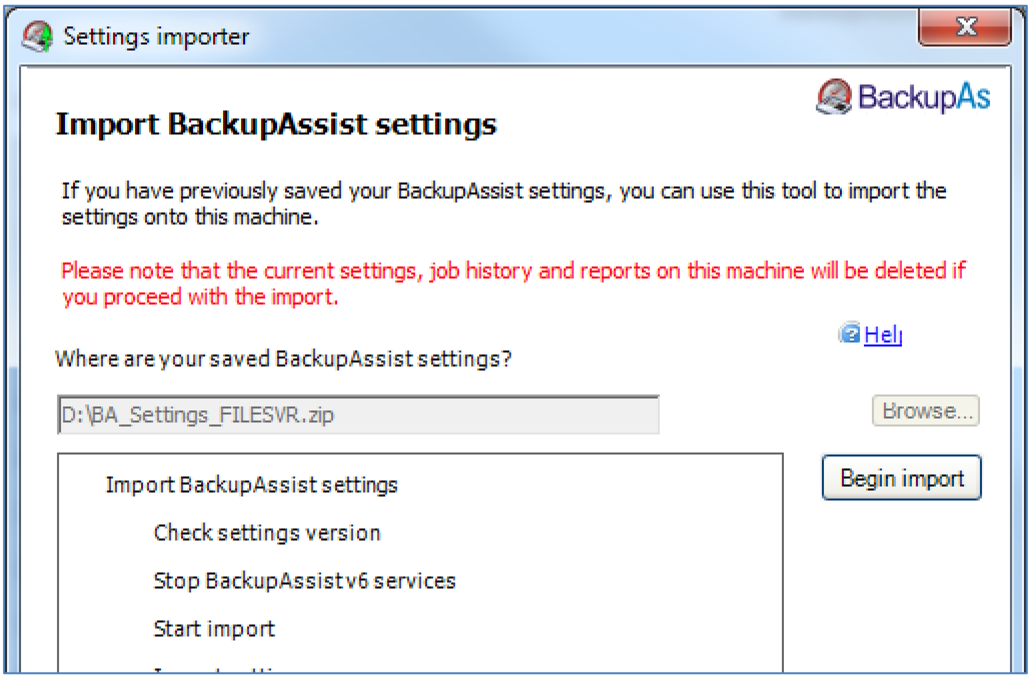
You can export BackupAssist settings to a file that can be imported into to any BackupAssist v6 installation. BackupAssist settings that can be exported include: job settings, mail server settings, backup user identity settings, the global email address list, and the global printers list. To export BackupAssist settings:

1. Run BackupAssist and go to **File > Export settings** from the file menu.
2. Click the **Browse** button to specify where to export your settings.
3. Browse to the directory you want to export to and input the name of the settings file.
4. Click **Save** and the **OK** to export your settings.

To import BackupAssist settings:

> **Note:** importing BackupAssist settings from a saved file will overwrite your current settings. Job history and backup reports will also be removed as part of the import process.

1. Run BackupAssist and go to **File > Import settings** from the file menu. Browse to the location of your exported settings file and then click **OK** to start the settings import wizard.



Import BackupAssist settings

If you have previously saved your BackupAssist settings, you can use this tool to import the settings onto this machine.

Please note that the current settings, job history and reports on this machine will be deleted if you proceed with the import.

Where are your saved BackupAssist settings?

D:\BA_Settings_FILESVR.zip

Import BackupAssist settings
Check settings version
Stop BackupAssist v6 services
Start import

2. Click **Begin import** to import settings from a saved file. The progress window will display the import result of the import.

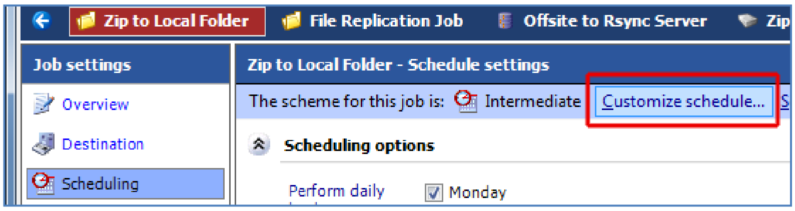
Full, incremental, differential, and copy backups with the Zip Engine

Zip jobs can be configured to run full, incremental, differential and copy backups. This new capability is available for all Zip hardware destinations, including tape drives[4]. You can also restore from a differential, incremental or copy Zip backup using the BackupAssist Restore Console.

[4] Requires the BackupAssist Zip-To-Tape Add-on.

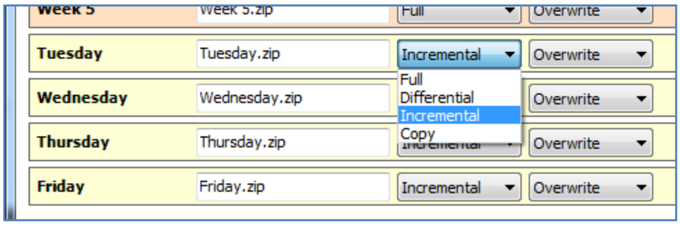
1. Launch BackupAssist and either choose an existing Zip job to edit from the **Edit** menu, or create a new job by going to **File > New backup job**.

2. Once you have created a new Zip job or chosen an existing job, select **Scheduling** from the left menu and click the **Customize schedule...** link near the top of the 'Scheduling settings' window.



The scheme for this job is: Intermediate

3. To change the backup method for a single media item use the drop-down menu in the **Method** column.



Week 5	Week 5.zip	Full	Overwrite
Tuesday	Tuesday.zip	Incremental	Overwrite
Wednesday	Wednesday.zip		Overwrite
Thursday	Thursday.zip	Incremental	Overwrite
Friday	Friday.zip	Incremental	Overwrite

Note: each file in Windows has an attribute known as the "archive bit". You can view this attribute by right-clicking a file, choosing **Properties** and clicking **Advanced**. Here you will see a check box with the label "file is ready for archiving".

When a full backup runs, this attribute is cleared, indicating that the file has been backed up. When a file is modified, the archive bit is turned on. When an incremental backup runs, only files that have the archive bit checked are backed up (i.e. files that have been modified since the last backup).

If you are running other backup software or have configured other BackupAssist jobs to run differential or incremental backups, this may interfere with your Zip job.

- **Full**: all data selected is backed up and each file is marked as having been backed up (the archive bit is cleared). To restore all your data you only need the most recent full backup.
- **Differential**: only data that has changed since the last full backup is copied to the backup device. Files are not marked as having been backed up (the archive bit is not cleared). You will require the last full backup and the last differential backup to restore all your data.
- **Incremental**: only data that has changed since the last backup (any type) is copied to the backup device. Files are marked as having been backed up (the archive bit is cleared). You will require the last full backup and all the incremental backups since the last full backup to perform a complete restore.
- **Copy**: the same as a full backup except that files are not marked as having been backed up (the archive bit is not cleared). Copy backups are useful if you have multiple jobs and need to back up certain files between full and incremental backup runs.

4. Once you have customized your schedule click **OK** and then click **Apply changes**.

5. Select **Calendar** from the left menu to verify that your schedule is configured correctly.

File and folder restore from Image backups

With the BackupAssist v6 Restore Console you can easily restore files from any Windows Image backup either by browsing its contents, or by using the 'free search' facility to find a specific file across all Image backup sets.

1. In BackupAssist, click **Restore** in the top navigation bar and choose **BackupAssist Restore Console**.
2. Click **Load all known backups** or **Browse** to locate the backup set from which you want to restore.
3. Once your backup catalogues have loaded you can choose to either **Browse** your Image backups and select data to restore, or **Search** through your Image backups for specific files to restore.

Embedding Mailbox / Public Folder backups in a backup job[5]

File Replication, NTBackup, Zip, Windows Imaging and Rsync

In BackupAssist v6 you can embed Exchange Mailbox and Public Folder backups to PST[6] in all BackupAssist jobs via the 'Exchange Servers' tab. Mailbox and Public Folder backups are executed as part of a backup run, and included in your main file selections, which are written to your backup destination in the specified format.

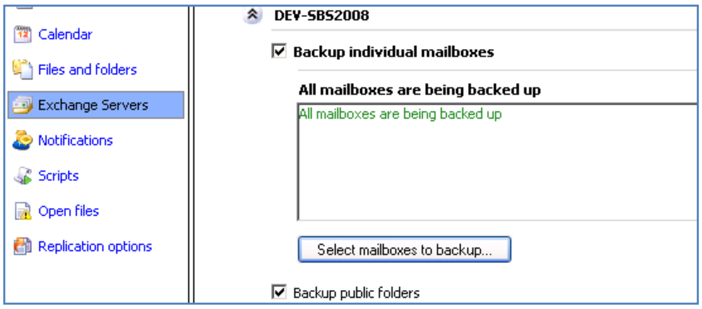
1. Launch BackupAssist and either choose an existing job to edit from the **Edit** menu, or create a new job by going to **File > New backup job**.
2. While editing a job select **Exchange Servers** from the left menu.
3. Click the **Add Exchange Server** button to backup Mailboxes and Public Folders.

> **Note:** you can add as many Exchange Servers as required, and each can be configured separately.

4. BackupAssist will now attempt to detect Exchange Servers running on your domain. Click **Add** to add the selected Exchange Servers and make them available for Mailbox and Public Folder backup.

> If your Exchange Server is located on a different domain, enter the computer name of an Exchange Server or a domain controller in the **Search for Exchange Servers on other domains field**.

5. Check the **Backup individual mailboxes** and **Backup public folders** options.



☑ Backup individual mailboxes

All mailboxes are being backed up

All mailboxes are being backed up

☑ Backup public folders

6. By default BackupAssist will back up all mailboxes on the Exchange Server. To specify which mailboxes to backup click the **Select mailboxes to backup** button.

[5] Requires BackupAssist Exchange Mailbox Add-on
[6] Requires the BackupAssist Exchange Mailbox Add-on