ULTRABAC

Backup and Disaster Recovery for the Windows Platform

ULTRA**BAC**
SOFTWARE

UltraBac Administrator Guide v9.2.5

The software described in this guide is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Table Of Contents

UltraBac User Manual

Introduction

Minimum System Requirements

O/S (running the latest service pack and hotfixes and Microsoft .NET Framework 2.0 & 3.5):

- Windows 2000 (Professional and Server)
- Windows XP Professional
- Windows Server 2003 / 2003 R2
- Windows Vista (Business and Ultimate Editions)
- Windows Server 2008 / 2008 R2
- Windows 7 (Professional, Enterprise, and Ultimate)

Screen:

- A minimum screen display of 800x600 is required and 1024x768 recommended. 256 color display required and 65536 colors recommended.

Memory:

- Windows 2000 – 512 MB required, 2 GB or greater recommended.
- Windows Server 2003/2003 R2/XP – 512 MB required, 2 GB or greater recommended.
- Windows Server 2008/2008 R2/Vista/Windows 7 – 1024 MB required, 2 GB or greater recommended.
- UBDR Gold – 512 MB required, 1024 MB or greater recommended.

Hard Disk:

- 20GB of free hard disk space required, 50 GB recommended.

Conventions Used In This Manual

Option Name   "   " (Option Name can refer to Menu Items,
                               Choices, Buttons, etc.)
  Convention: "Option Name"
  Example: "Tools"
  Sample: Choose the "Tools" option

Dialog Box Name   "*Italicized*"
  Convention: "*Italicized Dialog Box Name*"
  Example: "*UltraBac Preferences*"
  Sample: Select the "*Operation*" box found in the
                               "New Backup" Screen

Text Box Name   "***Italicized - Bold***"
  Convention: "***Italicized - Text Box Name***"
  Example: "***Restore only SQL table: ...***"
  Sample: Key the table into the "***Restore only SQL table:...***"
                               text box

Text Insertion   <   >
  Convention: <Description of text to be inserted>
  Example: \\<Your Computer Name>\<Share Name>\<File Name>
  Sample: \\CAT\C$\temp

Number Insertion   [   ]
  Convention: [A series of #'s - the quantity of #'s specifies the
                               maximum number of digits]
  Example: Protect Media for [###] days
  Sample: Protect Media for 365 days

An Option Path   "   "/"   "/"   "
  Convention: "Option Name"/"Option Name"/"........
  Example: "Tools"/"Preferences"/"Media"/"Protect Media for
                               [###] days"
  Sample: Select the "Tools" option, then the "Preferences" option, then the
                               "Media" option, followed by the "Protect Media for [###] days"
                               option

Action Insertion   (   )
  Convention: (Action to be Performed)
  Example: "File"/"Open Backup"/"(highlight a set)"
  Sample: Select the "File" option from the main UBUI toolbar and choose the
                               "Open Backups" option. Next, click on the desired backup set to
                               select and highlight the set.

Chapter or   **"Bold Type"**
Section Name
  Convention: **"Chapter or Section Name in Bold Type"**
  Example: **"Backup Group Format"**
  Sample: Refer to the "**Backup Group Format**" section of the "**Creating**

Backup Sets" chapter

File Path	"<u>Underlined</u>"
Convention:	"<u>Underlined File Path</u>"
Example:	"<u>C:\UltraBac\</u>"
Sample:	By default, UltraBac installs into the "<u>C:\UltraBac\</u>" directory

Keyboard Shortcut	"First Alpha Character Underlined"
Convention:	"<u>N</u>ew"
Example:	A keyboard shortcut for creating a new backup is executed by pressing and holding the Ctrl key while pressing the "n" key.
Sample:	"Ctrl" + "n"

Setup and Configuration

Installing UltraBac

The UltraBac Installer allows UltraBac to be installed on either the local system or to remote systems. A full install should be performed on the backup host, then any necessary agents (or a full install) can be installed to the remote systems. Running the full installation on the host machine will allow the backup of remote files, SQL databases, Exchange servers, or a full "Image" backup of the local system.

UltraBac agents can be installed on remote systems to allow the backup of their Active Directory/System State, and Image backups of their physical disks. UltraBac device controls can be installed to allow the use of remote tape devices, including libraries.

> NOTE: During both the installation and uninstallation of UltraBac the system will prompt for the system to be rebooted in order to install/uninstall UltraBac's Locked File driver.
>
> For additional information about files and drivers used by UltraBac, please see the UltraBac Knowledge Base:
>
> **See UBQ000261: Additional File and Driver Details**

To start the install process:

1. Download UltraBac and unzip the contents of the downloaded .zip file to a temporary directory.
2. Double click on the "Launcher.exe" in the temporary directory.

Fig. 1 - Launch screen for the UltraBac Installer.

3. Click "Launch UltraBac Installer."
4. Click "Next" in the "UltraBac Installer" screen.

5. Read the UltraBac Licensing Agreement text, and check "I accept the terms of the licensing agreement."
6. Click "Next" to continue.

Install Types

- Full Install – Select "Full Install" when installing to the backup host. This option can also be used to install all client systems without violating or invalidating UltraBac's license.
- File-by-file and System State – Installs only the agents used to back up files, folders, and the System State, as well as perform Locked File backups.
- Image Backup Only – Installs only the Image Disaster Recovery Agent, UltraBac Management Console, and the backup engine.
- Image Agent Only – Installs only the Image Disaster Recovery Agent.
- Microsoft SQL Agent Only – Installs only the Microsoft SQL Agent.
- Exchange Agent Only – Installs only the Microsoft Exchange Agent.
- Custom Install – Allows the selection of any combination of UltraBac components for install.

Installing UltraBac on the Backup Host

When performing the initial installation of UltraBac on the backup host, all components should be installed using the "Full Install" option.

1. From the UltraBac setup screen, select "Full Install" and click "Next."
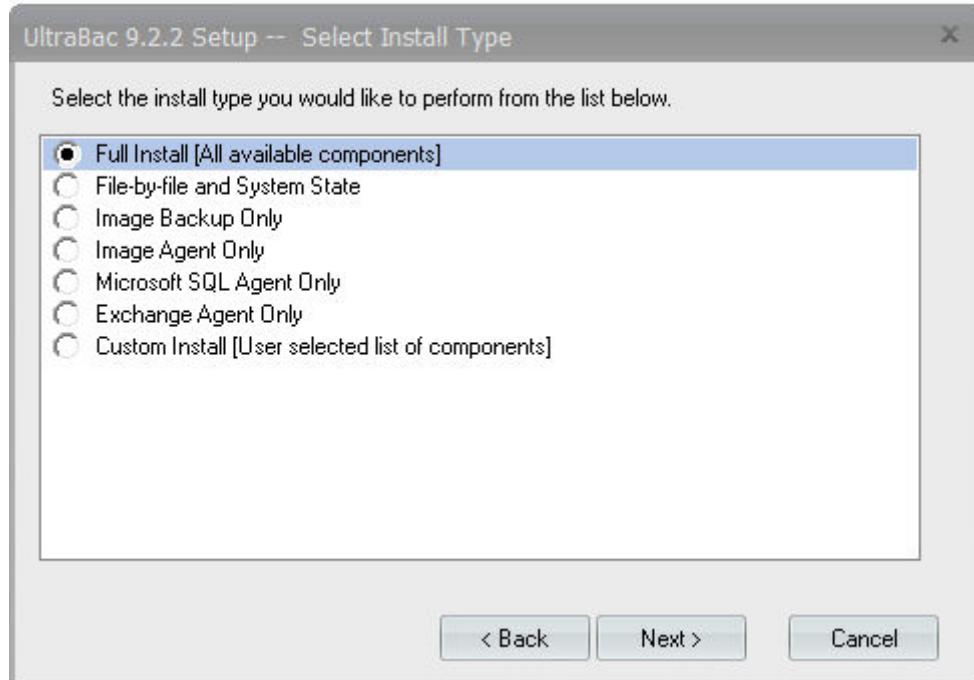
Fig. 2 - Selecting a Full Install.

2. Review the list of components in the "Setup Summary" and click "Next."

NOTE: UltraBac requires elevated privileges due to the administrative functionality utilized by the backup product. It is recommended that the UBMS account be given Domain Admin privileges for backing up domain systems and services (or local Administrator permissions for non-domain systems). To set up a Backup Account that is not an account with Domain Admin permissions, please see the UltraBac Knowledge Base:

See UBQ000198: Backup Account Permissions

More information:
See UBQ000112: Troubleshooting Permissions Issues

3.   Type the account name to be used for backup in the "Account" field.
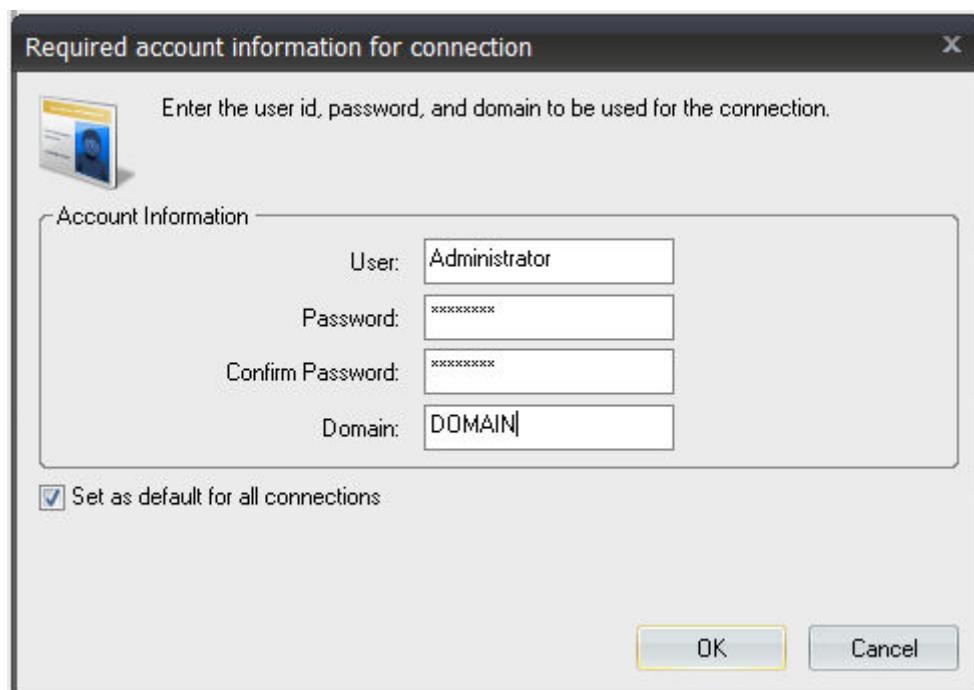
Fig. 3 - Entering account information into UltraBac.

4.   Type the account's domain in the "Domain" field. When installing in a workgroup, leave this field blank.
   5.   Type the password into the "Password" field.
   6.   Re-type the password into the "Confirm Password" field, and click "OK."

Checking "Set as default for other connections" will instruct UltraBac to use the specified account to run the UltraBac Management Service on the local system, and to use that account for backup and restore with the following agents:

   •   Image Disaster Recovery

- File-by-File Local
- File-by-File Network Share
- File-by-File Networked Computer
- Exchange
- Exchange Mailbox
- SQL

Installing UltraBac on a Remote Client

After the initial installation completes, the UltraBac installer will give the option to launch UltraBac, and to launch the Remote Installer. The Remote Installer can also be launched from the Windows Start menu.

To install UltraBac on a client using the Remote Installer:

1. Click "Start"/"Programs"/"UltraBac"/"UltraBac Installer."
2. Select "Install to other machine(s)" and click "Next."
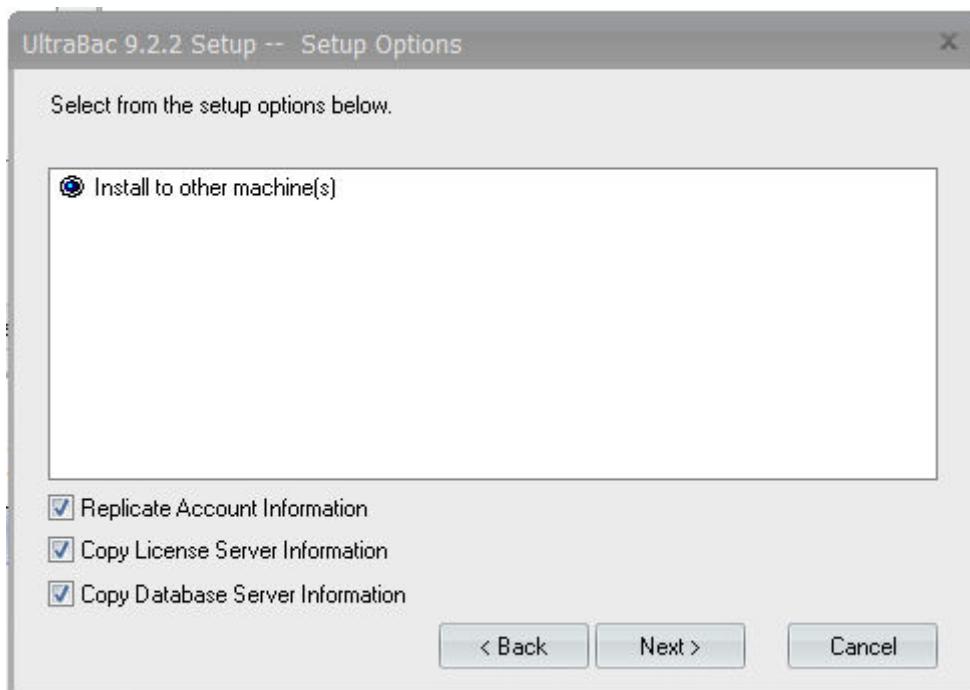
Fig. 4 - Setup options.

3. Click the "Add New" icon, type or browse to the name of the client system(s) to be installed, and after adding all of the systems, click "Next."
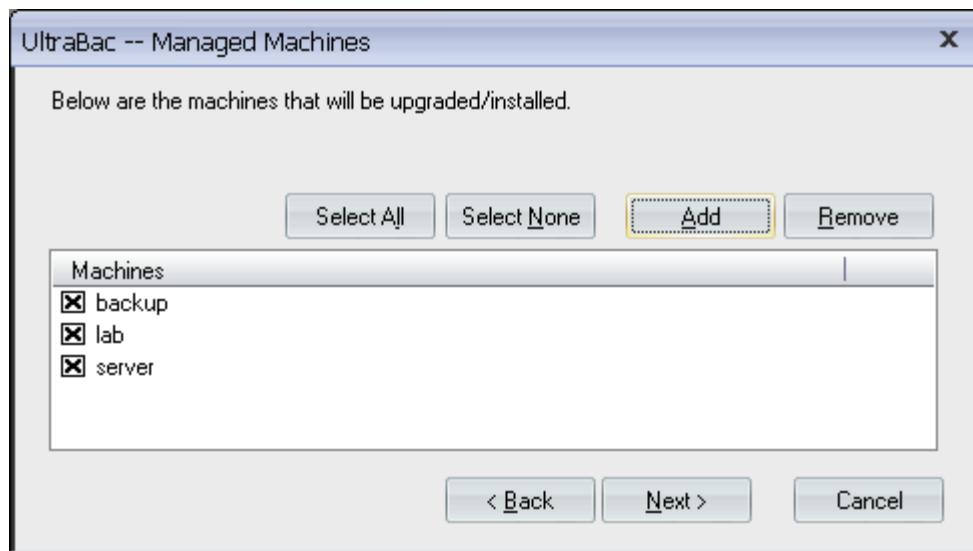
Fig. 5 - Selecting systems for installation.

4. Select the install type, and click "Next."
5. Review the list of components in the "Setup Summary," and click "Next" to begin the install.

Remote Installer Options

- Install to other machine(s) – Install UltraBac to a system on the network.
- Upgrade managed machine(s) – Upgrade all systems in the Managed Machines set in the Manage tab, under "Managed Machines," to the version installed on the Remote Installer host.
- Replicate Account Information – Replicates all account information set in the Manage tab, under "General"/"Authentication options"/"Accounts," to each system being installed.
- Copy License Server Information – Replicates the licensing server information set in the Manage tab, under "Licensing"/"Set License Server," to each system being installed.
- Copy Database Server Information – Copies the database configuration set in the Manage tab, under "Database"/"Database Wizard," to each system being installed.

Scripted Install

UltraBac can be scripted to perform both local and remote installations, using the following syntax:

setup.exe /installto:server1,server2,exchangesvr

NOTE: For more information on performing a scripted install of UltraBac, please see the UltraBac Knowledge Base:

See UBQ000229: Unattended Installation of UltraBac

Installing UltraBac in a 32/64-bit Environment

When performing the initial installation of UltraBac on the backup host, all components should be installed using the "Full Install" option. This will allow all agents and options to be used and controlled from the backup host. If installing UltraBac into a mixed 32/64-bit environment, check "Install files for other platforms" and check the applicable platforms. This will not install those files, it will make them available for remote installation to other platforms. UltraBac automatically installs the files for the system's platform.
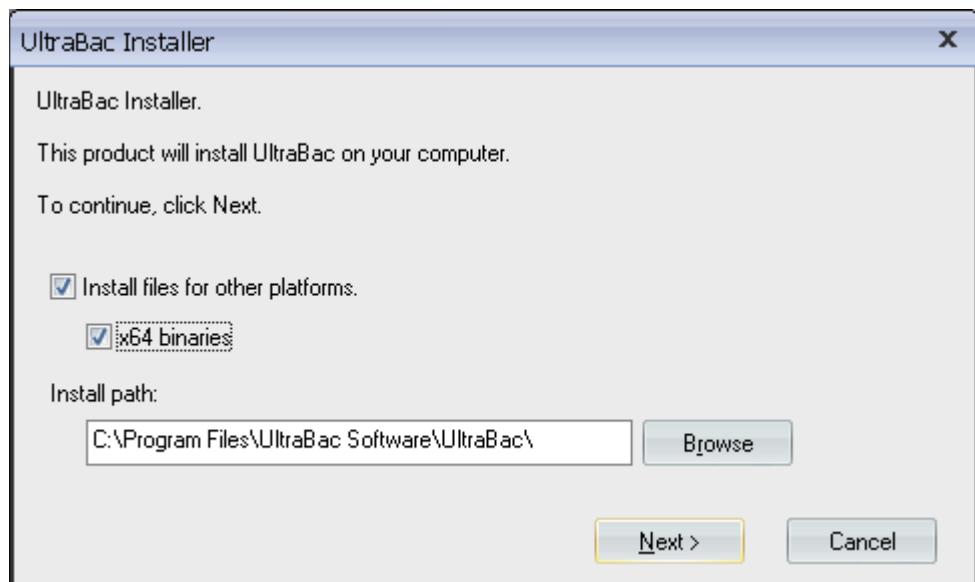
Fig. 6 - Copying 32/64-bit binaries.

Uninstall

Uninstall UltraBac through "Add/Remove Programs" in the Windows Control Panel:

1. Highlight the UltraBac entry in the "Add/Remove Programs" window and click "Change/Remove."
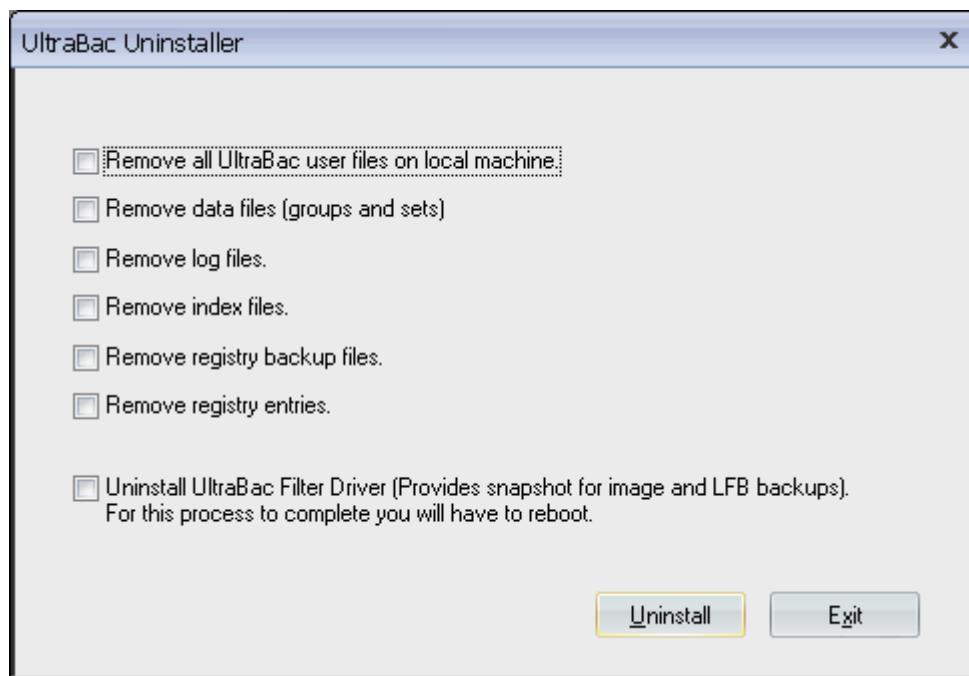
Fig. 7 - Uninstalling UltraBac.

2. Check "Remove all UltraBac user data files on local machine" to completely remove the entire application, including sets, groups, online indexes, registry entries, and ALL other application information.
3. If "Remove all UltraBac user data files" was not selected, open the registry editor and browse to "HKEY_LOCAL_MACHINE"\"SOFTWARE." Delete the "UltraBac Software" key.

NOTE: If the UltraBac Database has been installed, the database files must be removed manually after uninstalling UltraBac. The location of the database files will be dependent on the Database Storage Location; all of the files in the Database Storage Location folder can be removed if they are no longer needed. Please visit the "**UltraBac Database**" section of the User Manual:

UltraBac User Manual: UltraBac Database

UltraBac Preferences

UltraBac allows the configuration of many user preferences in one centralized menu. UltraBac Management Console behavior, the path to backup logs, user accounts, and more can be configured in this menu. The menu can be accessed at any time by selecting the Manage tab, and clicking "General."
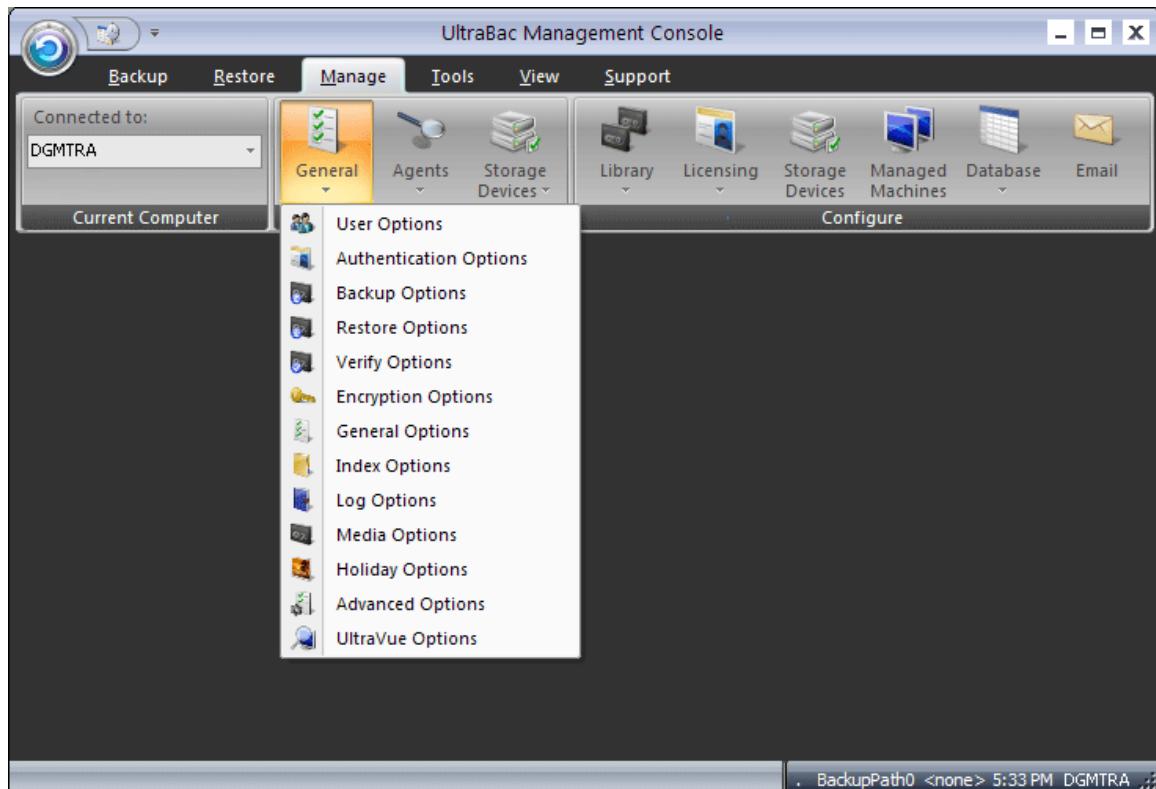
Fig. 1 - Selecting the preferences.

User Options

The User menu modifies the default behavior of the UltraBac user interface.
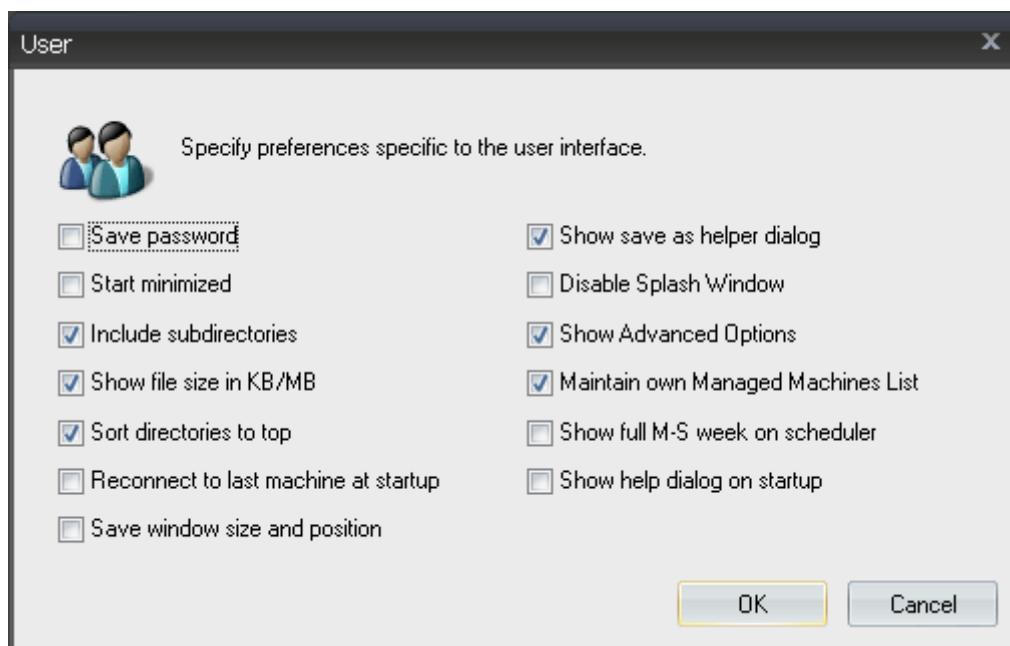
Fig. 2 - User preferences.

User Preferences:

- Save password – If a username and password are entered through the Backup Wizard, the account will automatically be remembered for the next backup set.
- Start minimized – UltraBac will be minimized when launched.
- Include subdirectories – UltraBac will select the entire directory tree by default in all backup sets.
- Express file size in KB/MB – When checked, only data amounts smaller than 1 KB will be expressed as bytes. If unchecked, all data values will be expressed as bytes.
- Sort directories to top – When enumerating a backup set, directories will appear on top of the directory tree.
- Reconnect to last machine at startup – If UltraBac was connected to a remote system when last closed, UltraBac will reconnect at startup.
- Save window size and position – UltraBac will remember its previous window size when opened.
- Show save as helper dialog – Enables the dialog box opened after a set is saved.
- Disable Splash Window – Eliminates the introductory splash screen appearing before the application launches.
- Show Advanced Options – Enables dialog boxes that allow the File-by-File Agent to be run locally or remotely during an ad hoc backup, and during restore.
- Maintain own Managed Machines List – Allows each user to create and maintain a Managed Machines list when logged into the backup host system.
- Show full M-S week on scheduler – Shows the entire 7-day calendar in the UltraBac Scheduler.
- Show help dialog on startup – Enables the helper dialog when the Management Console is launched.

Authentication Options

The Authentication menu allows user accounts to be added for use in UltraBac. Account passwords can also be changed or reset in this menu.
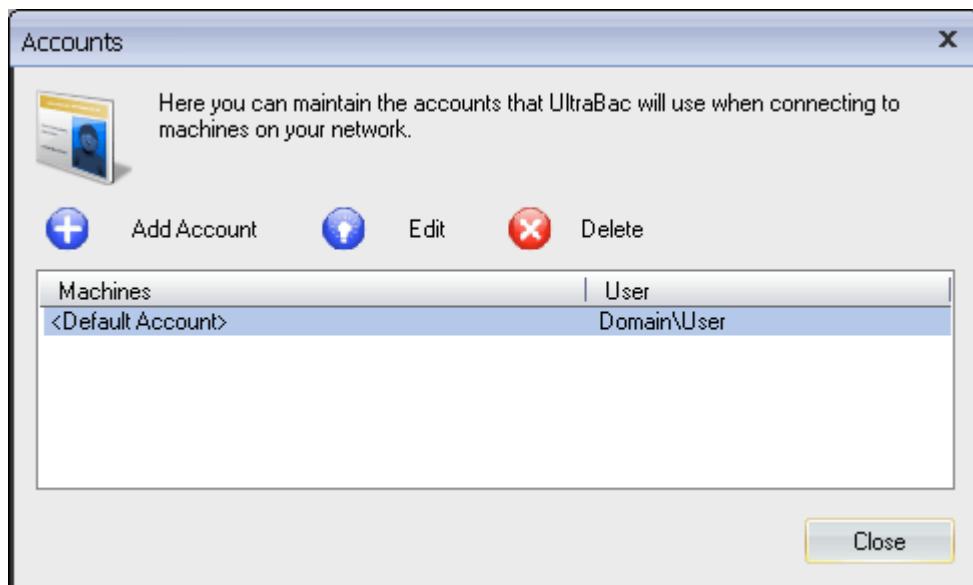
Fig. 3 - User accounts.

To add a domain user account in UltraBac:

1. Click the "Show Accounts" button in the Authentication tab.
2. Click the "Add New" icon.
3. Type the domain name for the account to be used in the "Domain" field.
4. Type the account name to be used in the "User Name" field.
5. Type the password for the specified account in the "Password" field.
6. Re-type the password in the "Confirm Password" field.
7. Click "OK" to add the account.
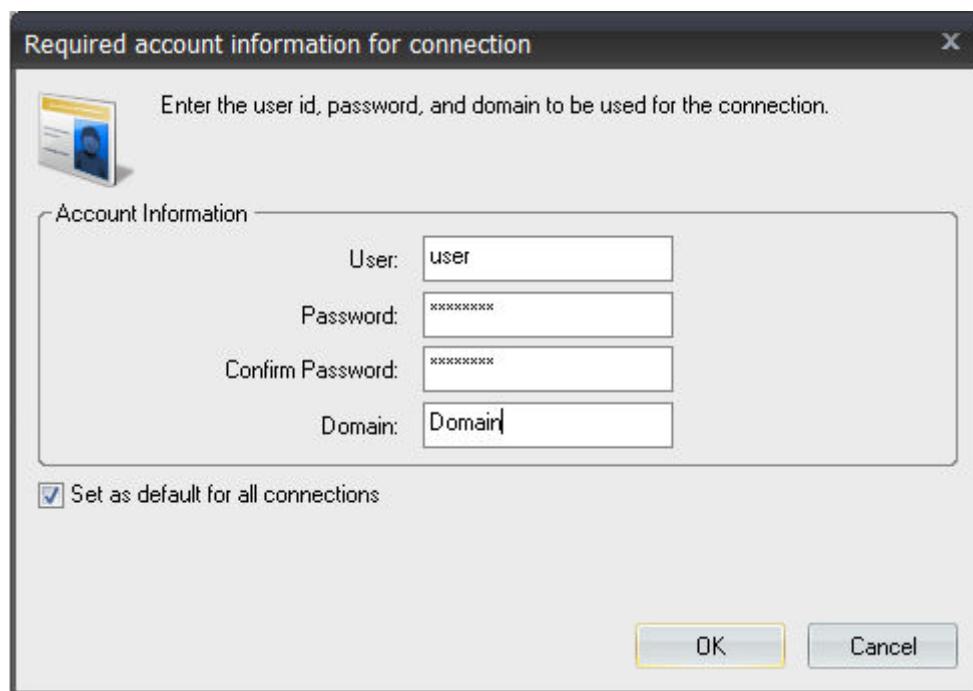
Fig. 4 - Account Information.

Checking "Set as default for all connections" will instruct UltraBac to use the specified account to run the UltraBac Management Service on the local system, and to use that account for backup and restore with the following agents:

- Image Disaster Recovery
- File-by-File Local
- File-by-File Network Share
- File-by-File Networked Computer
- Exchange
- Exchange Mailbox
- SQL

To add a workgroup user account in UltraBac:

1. Click the "Show Accounts" button in the Authentication tab.
2. Click the "Add New" icon.
3. Type the account name to be used in the "User Name" field.
4. Type the password for the specified account in the "Password" field.
5. Re-type the password in the "Confirm Password" field.
6. Click "OK."
7. Type in or browse to the Windows name or IP address of the system to be backed up.
8. Click "OK" to add the account.

NOTE: When specifying an account to be used in a workgroup, do not enter any information into the "Domain" field.

Creating a Secondary Account

When creating a backup of a remote system, it is sometimes necessary to use an account other than the default account for the backup connection. This can be used in cases of backing up a system in a workgroup from a domain, or backing up systems in another domain. The secondary account can target either an individual system or a domain. A workgroup cannot be specified as a target; individual accounts for the systems in that workgroup must be added.

To add a secondary user account in UltraBac:

1. Click the "Show Accounts" button in the Authentication tab.
2. Click the "Add New" icon.
3. Type the domain name for the account to be used in the "Domain" field, if the target system is in a domain. If in a workgroup, leave this field blank.
4. Type the account name to be used in the "User Name" field.
5. Type the password for the specified account in the "Password" field.
6. Re-type the password in the "Confirm Password" field.
7. Click "OK" to add the account.
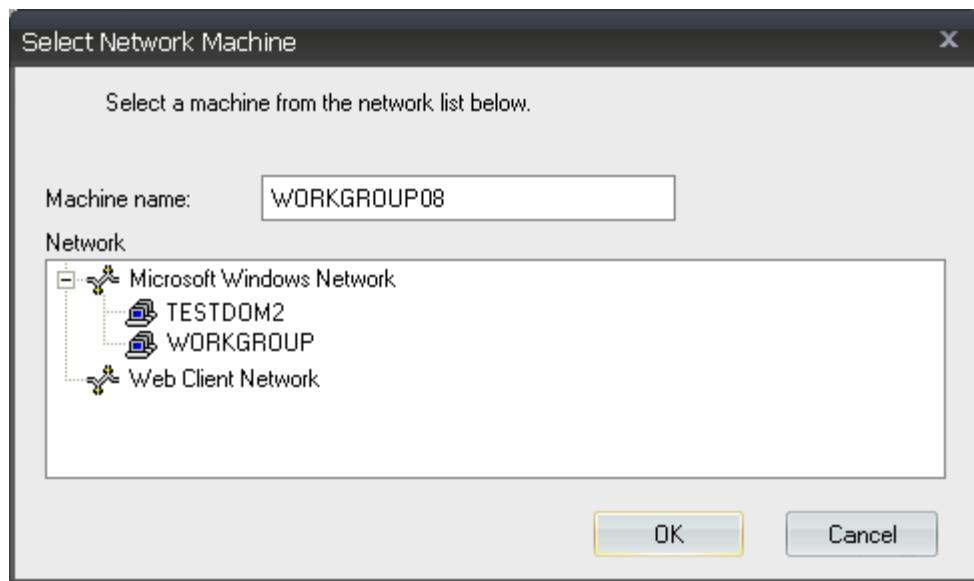
Fig. 4 - Specifying a system in the "Select Network Machine" screen.

8. At the "Select Network Machine" prompt, type or browse to the target machine (or domain) and click "OK."

Deleting an Account

To delete an account from the Authentication menu:

1. Click the "Show Accounts" button in the Authentication tab.
2. Click on the account to be deleted.
3. Click the red "Delete" icon.

To view or modify the properties of an account:

1. Click the "Show Accounts" button in the Authentication tab.
2. Click on the account to be viewed/modified.
3. Click the "Properties" icon.
4. Click "OK" when finished.

Backup Options

The Backup menu can be used to set system usage and other backup specific options.
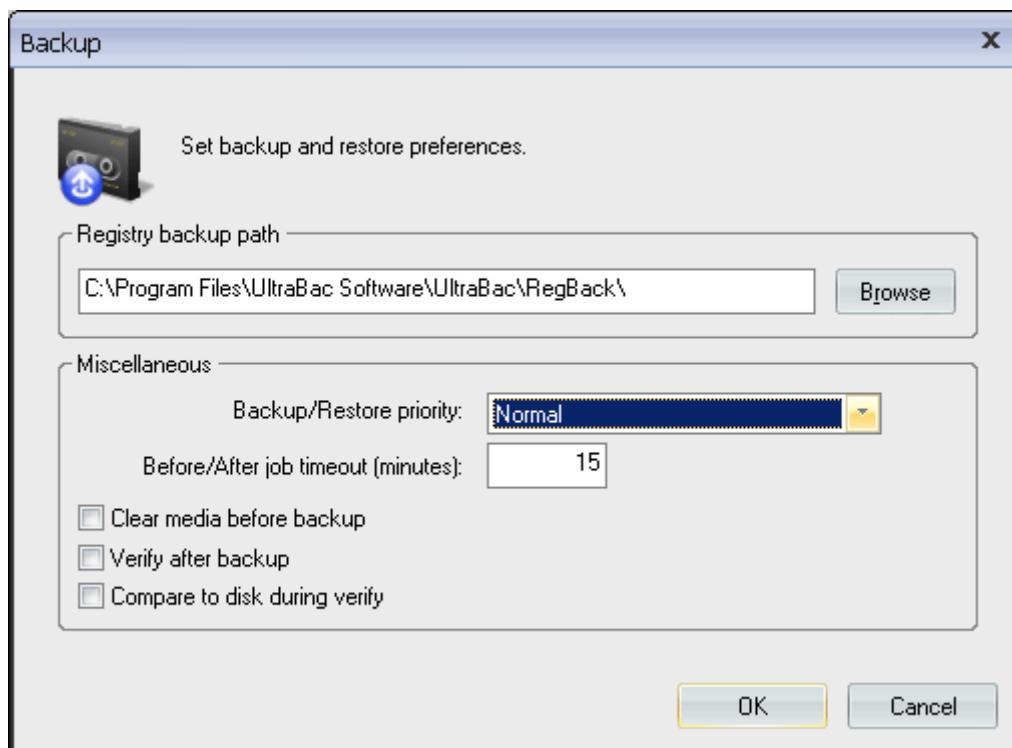
Fig. 5 - Backup preferences.

- Backup/Restore priority – This setting designates the priority of the system's resources when UltraBac is running:
  - Normal
  - High
  - Realtime
  - Idle
- Registry Backup Path – The directory used to store the registry dump created during backup.
- Before/After job timeout (minutes) – Through either the set level or scheduled backup group level, UltraBac has a function available to execute batch files, or previously written scripts, to run before the backup begins or after the backup finishes. This time interval specifies how many minutes UltraBac should wait before it stops trying to run the script.
- Clear media before backup – Sets a global preference to check the "Clear storage media" option when creating scheduled backup groups. "Clear storage media" can be unchecked in the scheduled group.
- Verify after backup – Sets a global preference to check the "Verify after backup" option when creating scheduled backup groups. "Verify after backup" can be unchecked in the scheduled group.
- Compare to disk during verify – Sets a global preference to compare all files to their original source files during verify. With this option unchecked, only a CRC verify is performed.

Restore Options

The Restore Options menu is used to set two restore options.
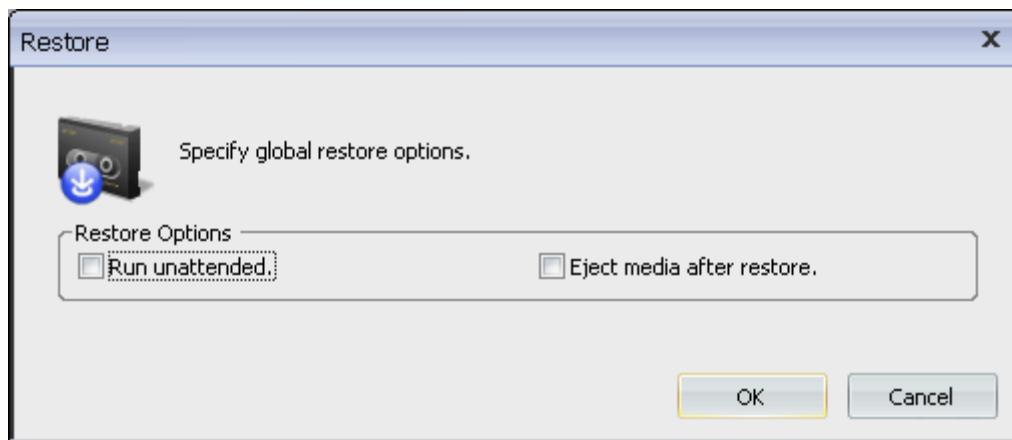
Fig. 6 - Restore preferences.

Restore Options:
- Run unattended – Do not prompt the user during ad hoc backups.
- Eject media after restore – Eject removable media after ad hoc backup.

Verify Options

The Verify Options menu is used to set two restore options.
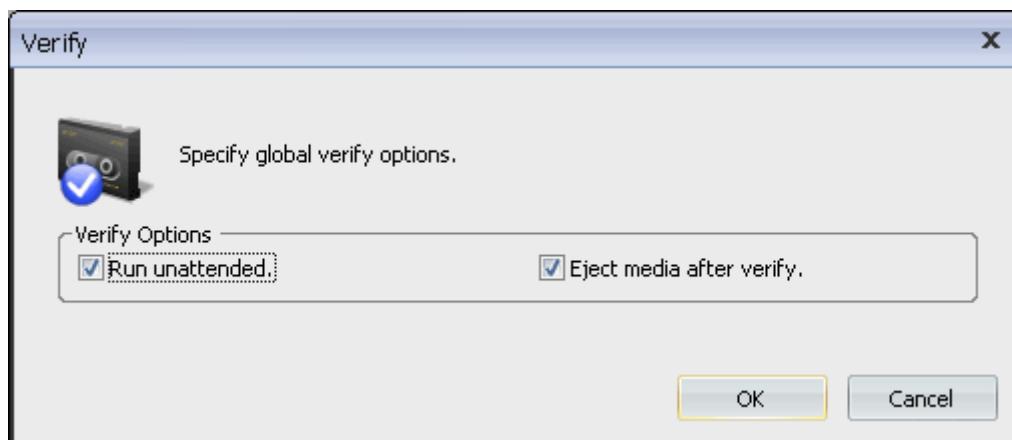
Fig. 7 - Verify preferences.

Restore Options:
- Run unattended – Do not prompt the user during ad hoc backups.
- Eject media after restore – Eject removable media after ad hoc backup.

Encryption Options

The Encryption Options menu sets the global options for using AES encryption during backup. When AES is enabled, it functions on the device level, and encrypts all data written to the backup media.
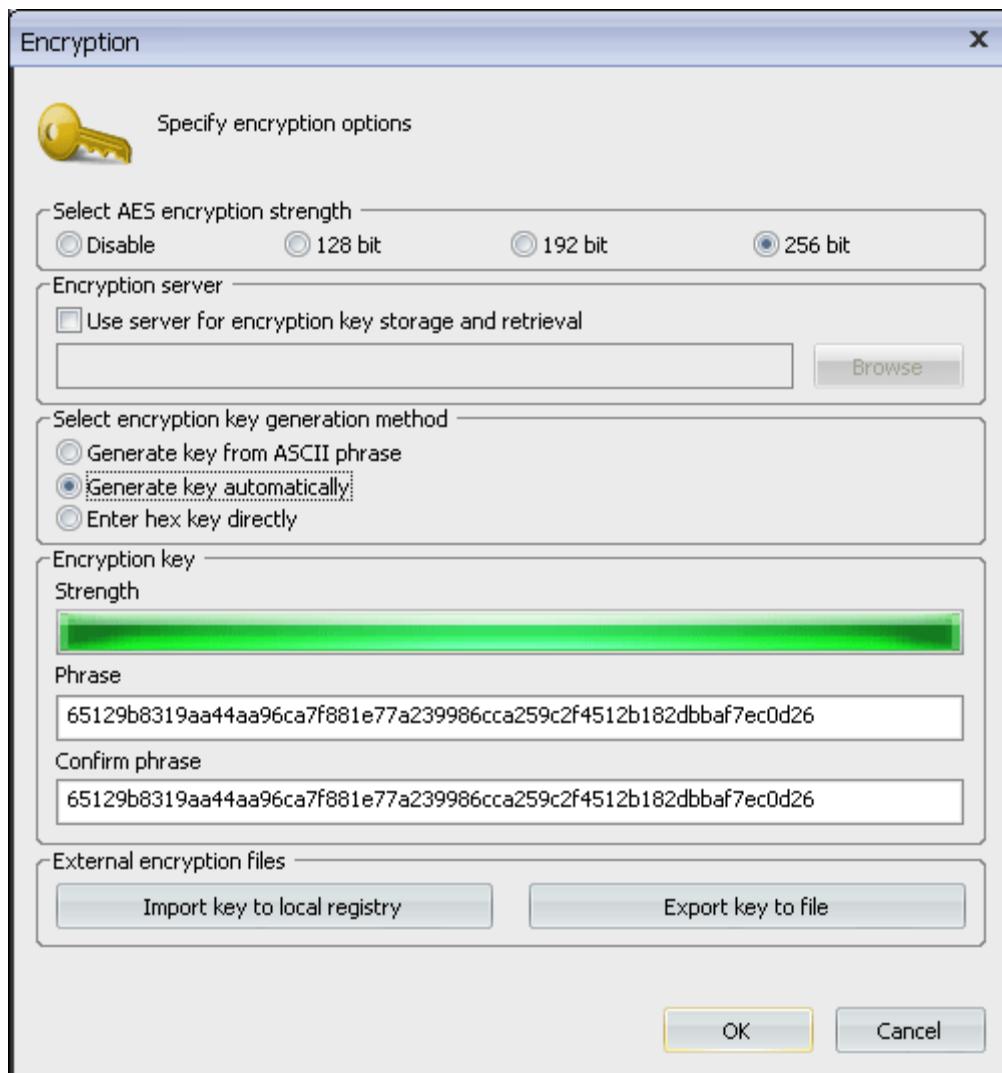
Fig. 8 - AES encryption options.

To enable encryption:

1. From the main UltraBac toolbar, click "Tools"/Options"/"General"/"Backup."
2. Click the button marked "Global Encryption Options."
3. *S*et the AES encryption strength:
    o Disable – Turns off all AES usage.
    o 128-bit – Sets AES to use a 128-bit key.
    o 192-bit – Sets AES to use a 192-bit key.
    o 256-bit – Sets AES to use a 256-bit key.
4. Select the method for generating the encryption key:

    o Generate key from ASCII phrase – Creates an encryption key using any ASCII characters, of the specified encryption strength.
    o Generate key automatically – Creates a random encryption key using HEX characters, of the specified encryption strength.
    o Enter hex key directly – Allows a user to create a specific encryption key using HEX characters, of 32, 48, or 64 characters.

5. Click "OK" to set the encryption options as specified.

NOTE: For more information on using AES encryption, please see the UltraBac Knowledge Base:

See UBQ000251: Encrypting Backup Data with AES

General Options

UltraBac stores all backup sets and groups in the path specified under "Default path for UltraBac data files."
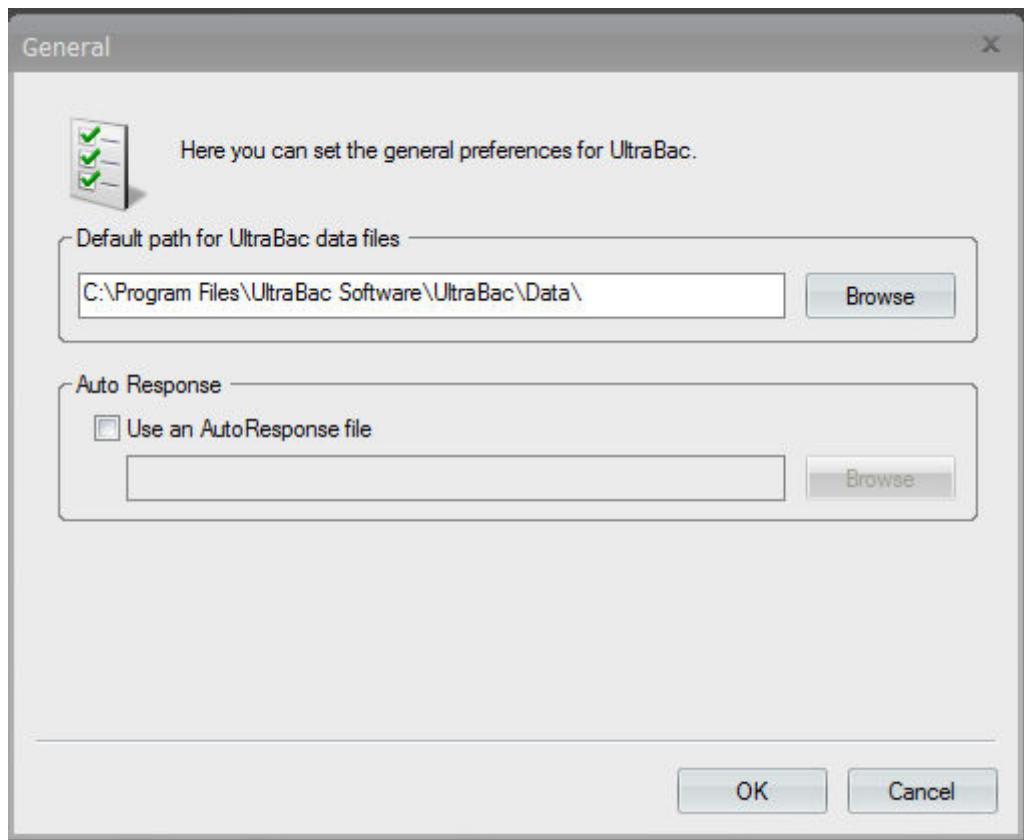
Fig. 9 - General preferences.

To change the default data file path:

1. Type in or browse to the folder to be used to store the UltraBac sets and groups.
2. Click "OK."

Index Options

The Index menu can be used to set the location of both backup and express indexes, and the amount of time those indexes are to be stored.
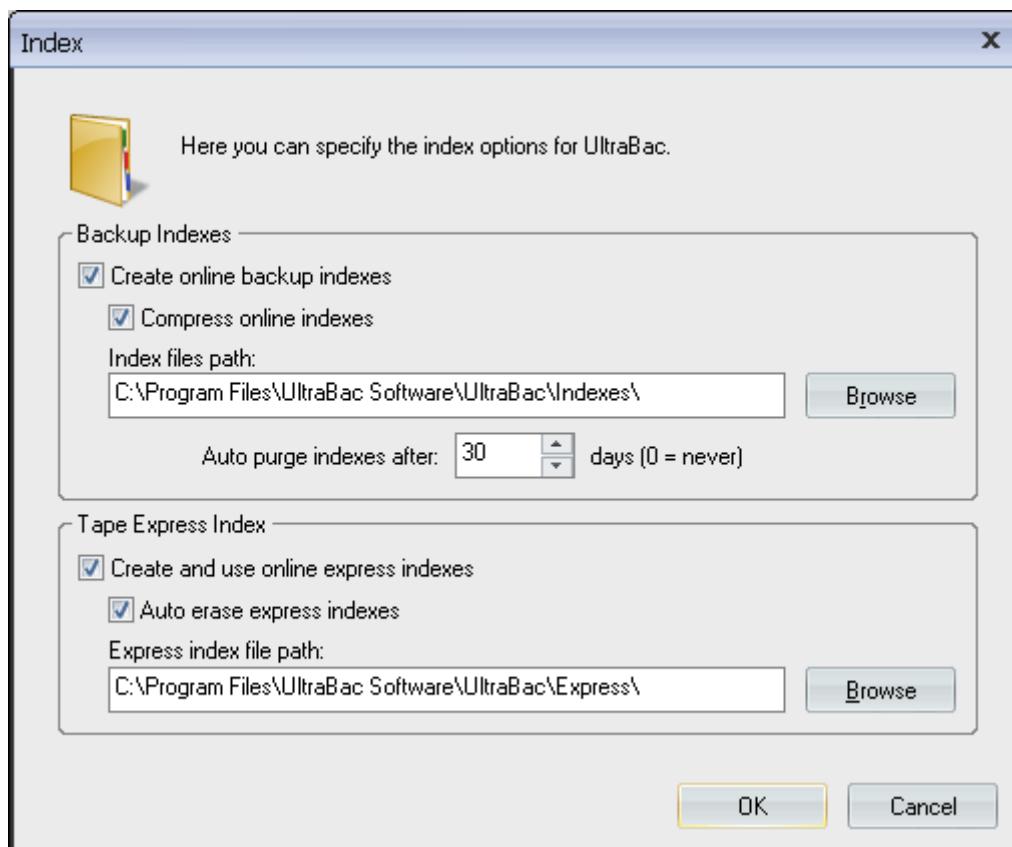
Fig. 10 - Backup index preferences.

Backup Indexes

- Create online backup indexes – Must be checked to create an online disk index for every set backed up.
- Compress online indexes – Uses up to 65% less storage space than uncompressed online indexes, while requiring minimal compression/decompression time.
- Index files path – Path where all online disk indexes are stored. Online disk indexes can be stored locally or on a network path.
- Auto purge indexes after [###] days – Number of days before online disk indexes are purged. When set to "0," index entries are not purged by UltraBac. Valid entries are "0" through "999."

Tape Express Index

- Create and use online express indexes – Enables express indexes.
- Auto erase express indexes – Automatically deletes the express index when the corresponding storage media is cleared by UltraBac.
- Express index file path – Path where all express indexes are stored. Express indexes can be stored locally or on a network path.

Logs

The Logs menu can be used to set the location of backup, verify and restore logs, and define the amount of time those logs are to be stored.
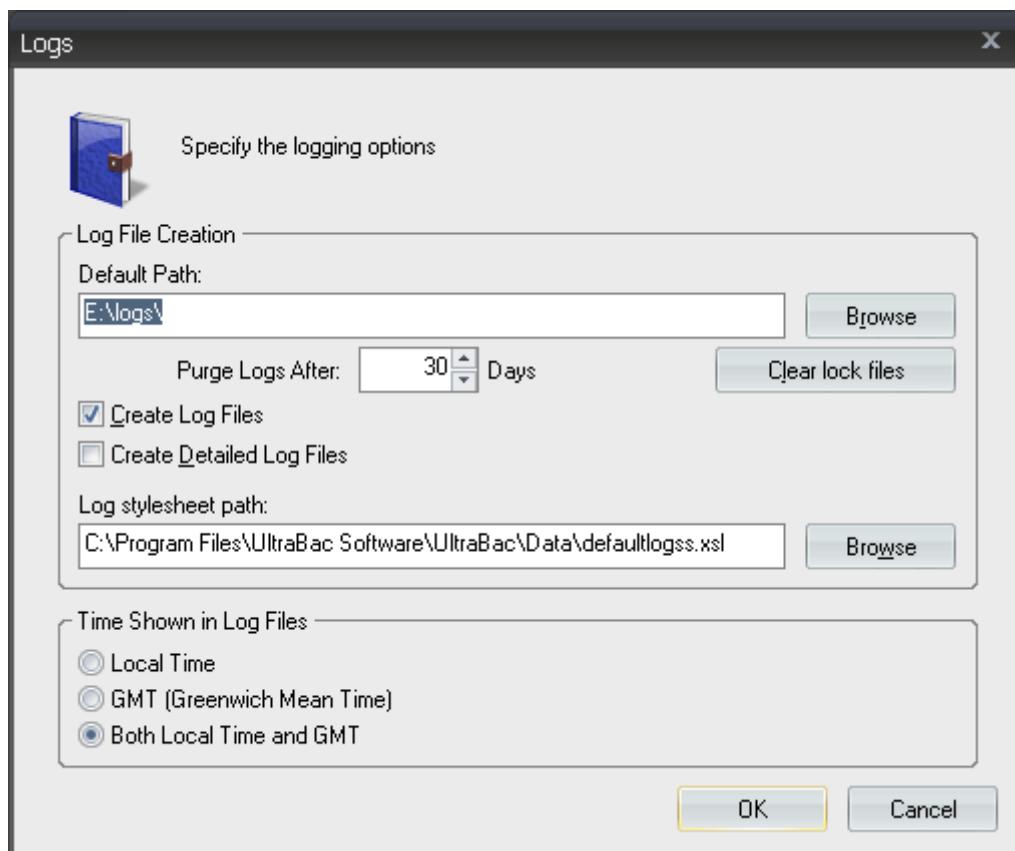
Fig. 11 - Log file preferences.

Log File Options

The default location and other log file options are handled by the preferences selected. The log file time can be set to use the time zone specified in the Windows clock on the backup host, or GMT, or both.

Log File Creation:

- Default path for Log Files – Path where all UltraBac log files are stored. Log files can be stored locally or on a network path.
- Purge Logs After [###] Days – Number of days before log files are purged. When set to "0," log files are not purged by UltraBac. Valid entries are "0" through "999."
- Clear lock files – Deletes all .lck files from the logs directory.
- Create Log Files – Enables the creation of backup, verify, and restore logs.
- Create Detailed Log Files – Backup logs will show all files handled during backup, verify, and restore operations.
- Log stylesheet path – Specifies the path to the stylesheet to use for displaying all UltraBac logs in the UltraBac File Viewer.

NOTE: For further information on the Centralized Reporting Console, including installation of a web based Centralized Reporting Console, please see the UltraBac Knowledge Base:

See UBQ000157: Configuring Centralized Reporting

Time Shown in Log Files:

- Local Time
- GMT (Greenwich Mean Time)
- Both Local Time and GMT

Media Options

The Media menu is used to set the default values for the media protection and compression options available in UltraBac.
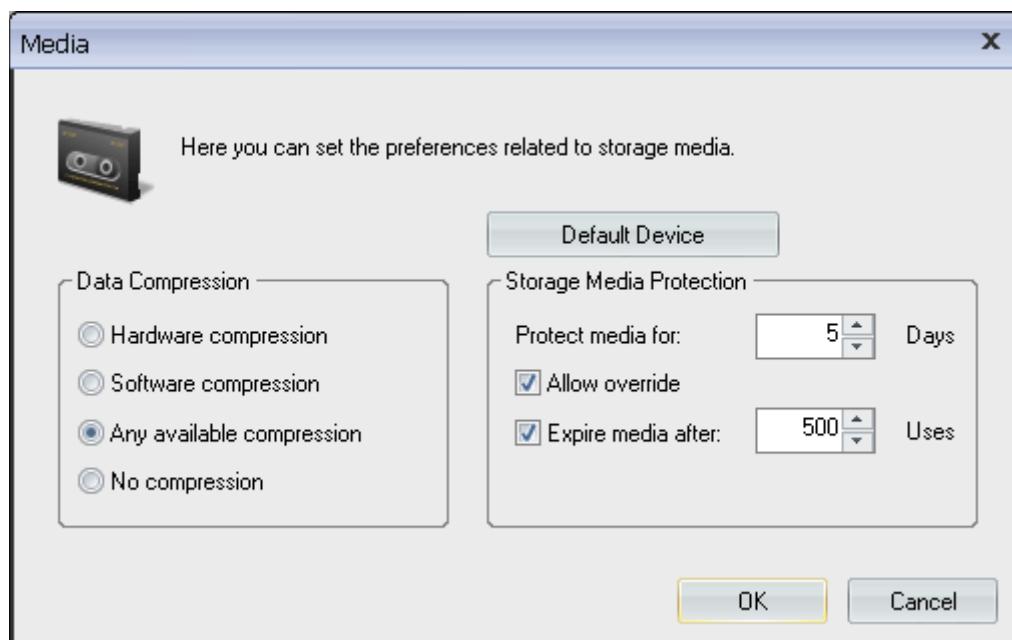
Fig 12 - Media options.

Default Device – Opens the UltraBac Storage Device Manager.

NOTE: For more information on using the UltraBac Storage Device Manager, please visit the "**Storage Device Manager**" section of the User Manual:

UltraBac User Manual: Storage Device Manager

Data Compression

Data compression options are set globally and cannot be overridden in the scheduled backup groups:

- Hardware compression – Compression is controlled by the storage media.
- Software compression – Compression is controlled by UltraBac, and is reported in the backup log.
- Any available compression – Software compression is used if hardware compression is not available.
- No compression – Disables the use of compression in all backups.

Storage Media Protection

- Protect media for: [###] Days – Protects the storage media from being overwritten by UltraBac for the number of days specified. Valid entries are "1" through "999."
- Allow override – Allows protected media to be cleared by UltraBac before backup.
- Expire media after: [####] Uses – Sets the number of times the storage media can be used by UltraBac before the media is considered unusable. Valid entries are "1" through "9999."

NOTE: When backing up to an autoloader, UltraBac uses the protection settings on only the first tape. If the backup uses more than one tape, UltraBac will automatically clear the subsequent tapes.

Holiday Options

The Holiday menu can be configured to alter backup behavior on specified days.
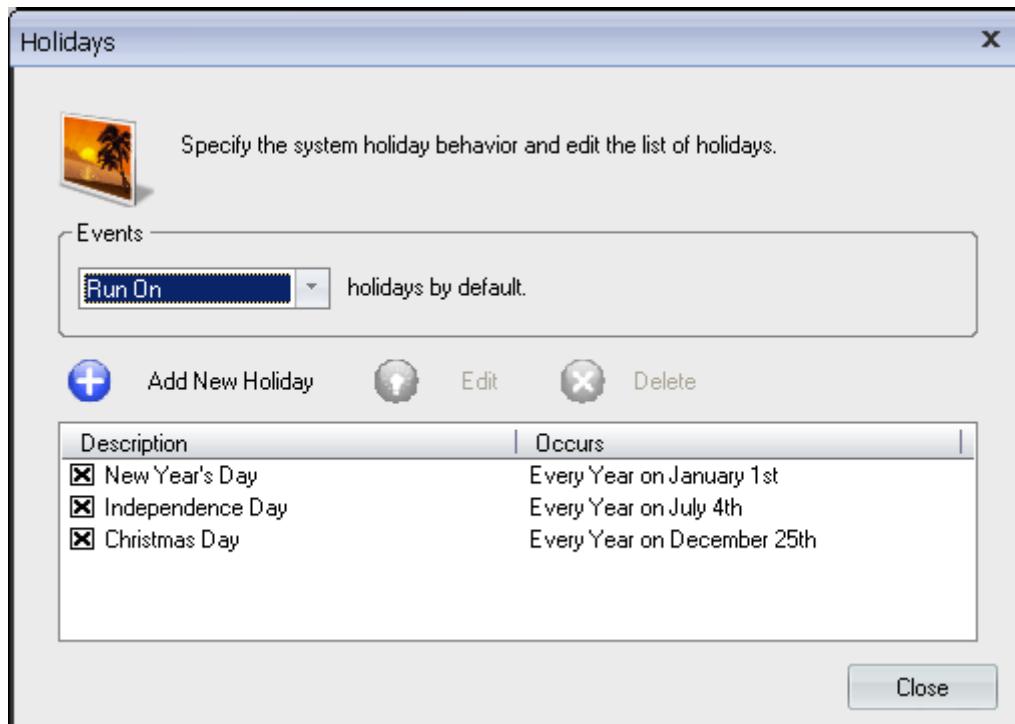
Fig. 13 - Holiday preferences.

Use the "Events [option] holidays by default" field to set holiday behavior:

- Run On – Instructs to run on holidays.
- Do Not Run On – Instructs backups to not run on holidays.

To add a holiday to the Holidays menu:

1. Click the "Add New Holiday" icon.

2. Type a description or name into the "Description" field.
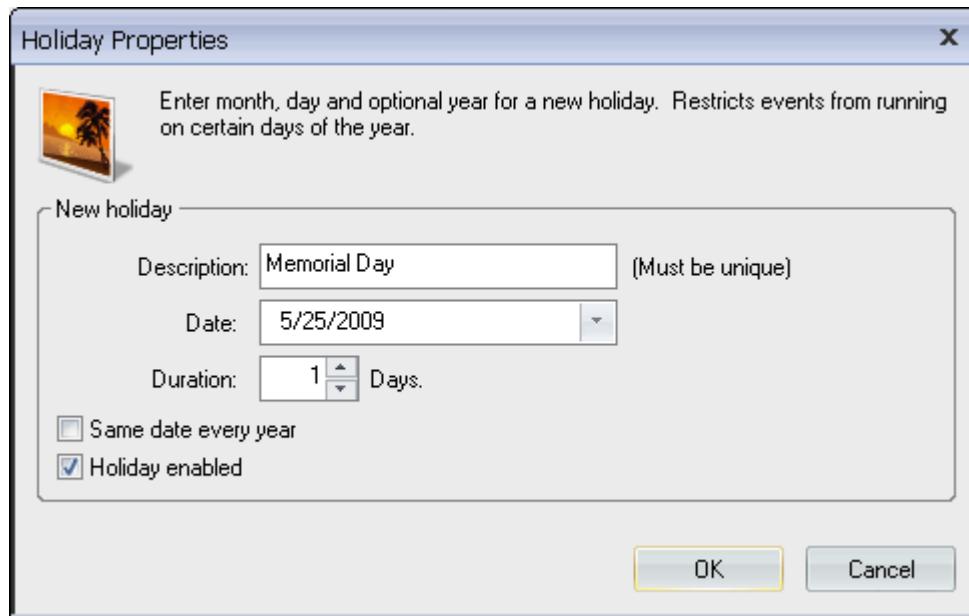
Fig. 14 - Holiday properties.

3. Type or use the drop-down calendar to enter a date for the holiday.
4. Type or use the selection arrows to enter a duration for the holiday.
5. Check "Every Year (same month/day)" to set the holiday for the same date every year.
6. Check "Enable Holiday" to activate the holiday.
7. Click "OK" to add the holiday.

Advanced Options

The Advanced menu contains options for configuring error handling and cluster server behavior. It is not recommended to change these settings from the default values.
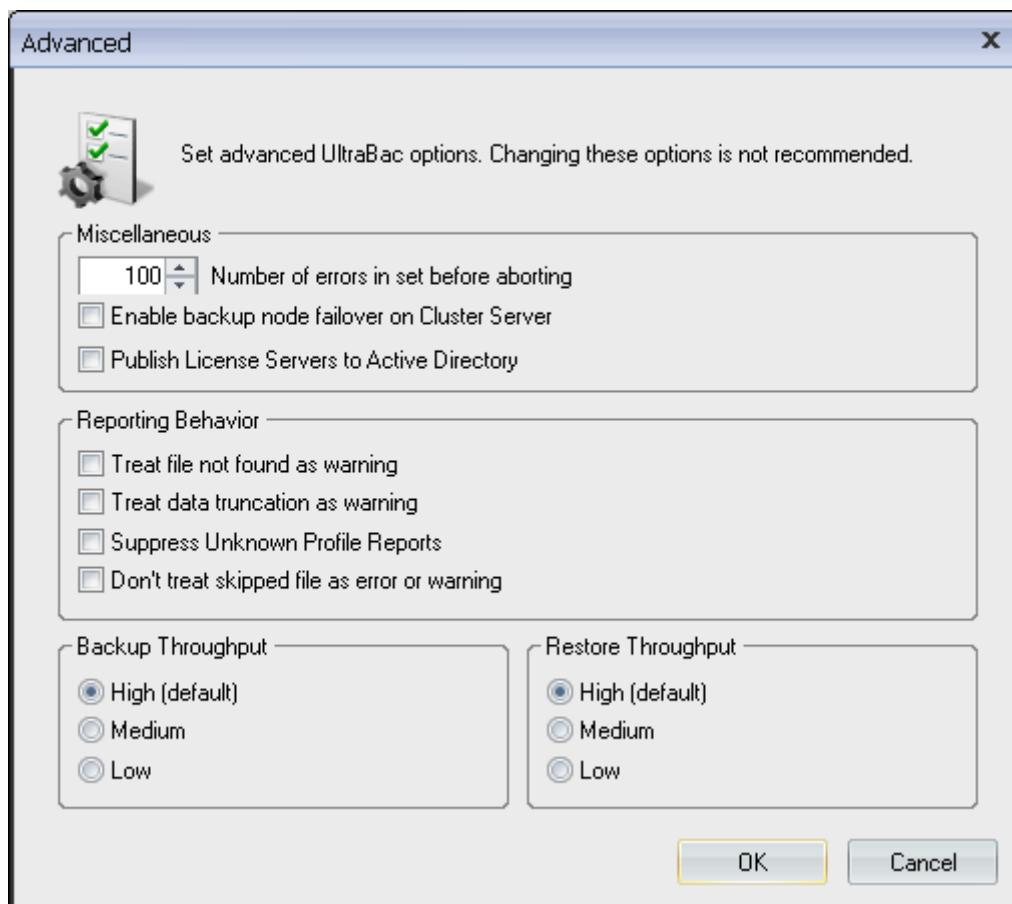
Fig. 15 - Advanced options.

- Number of errors in set before aborting: [###] – Sets the number of errors allowed in each backup set before UltraBac is allowed to abort that set. The default setting is "100."
- Enable backup node failover on Cluster Server – This option should only be enabled if UltraBac is installed on a Microsoft Cluster Server. Should the primary node fail, UltraBac will continue its regular scheduled backup jobs on the secondary node in the cluster.
- Publish License Servers to Active Directory – Records the UltraBac License server in Active Directory for the local domain.

Reporting Behavior

- Treat file not found as warning – Files "not found" during a backup will be reported in the backup logs as a warning only, not an error.
- Treat data truncation as warning – Data truncation during backup will be reported in the backup logs as a warning only, not an error.
- Suppress Unknown Profile Reports – Causes UltraBac to not report 1332 errors when a profile has been partially deleted or corrupted.
- Don't treat skipped file as error or warning – Instructs UltraBac to not record skipped files as either an error or a warning in backup logs.

Backup Throughput

The Backup Throughput options can lower the overall backup and restore speeds by up to 75%.

- High – Runs at full speed
- Medium – Runs at 50% speed
- Low – Runs at 25% speed

Restore Throughput

The Restore Throughput options can lower the overall backup and restore speeds by up to 75%.
- High – Runs at full speed
- Medium – Runs at 50% speed
- Low – Runs at 25% speed

UltraVue Options

UltraVue allows the viewing of active backup jobs on the local system, and all systems in the Maintain Managed Machines list.
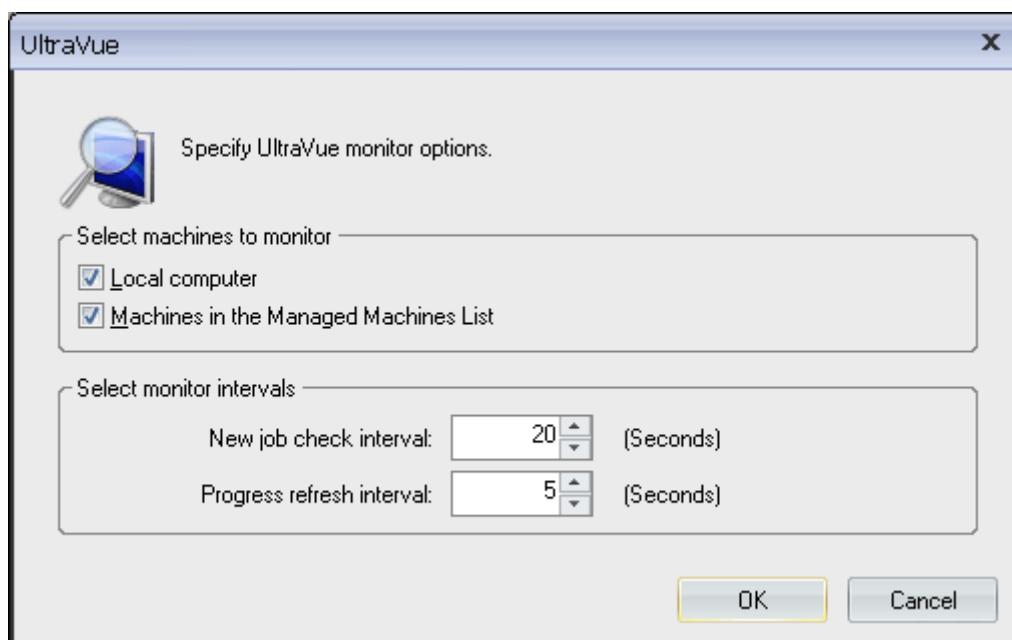
Fig. 16 - UltraVue preferences.

- Local computer – View active backups on the local system.
- Machines in the Managed Machines List – View active backups on all systems in the Managed Machines list.
- New job check interval [###] (Seconds) – The amount of time between backup activity queries, in seconds. Valid entries are "1" through "9999."
- Progress refresh interval [###] (Seconds) – The amount of time between backup activity queries, in seconds. Valid entries are "1" through "9999."

UltraBac Licensing

NOTE: If you do not have a license from UltraBac Software, please request one by visiting our Web site:

http://www.ultrabac.com/licensing/

The initial installation of UltraBac will run as a fully functional trial version for 20 days. After the expiration date is passed, a license must be obtained to run backups.

Each system in the backup scheme must have a valid license, including servers, workstations, and individual agents that UltraBac offers for specialized backups such as SQL, Exchange, Oracle, etc. As a backup progresses, each set is validated by the license server before the backup of that set begins.

Importing a License

After receiving a license file, it will need to be imported into UltraBac. To import the license:

1. Save the file "ublicense.txt" to: "C:\Program Files\UltraBac Software\UltraBac."
2. Launch the UltraBac console from "Start"/"Programs"/"UltraBac"/"UltraBac Management Console."
3. Select the Manage tab, and click "Licensing"/"Import License."
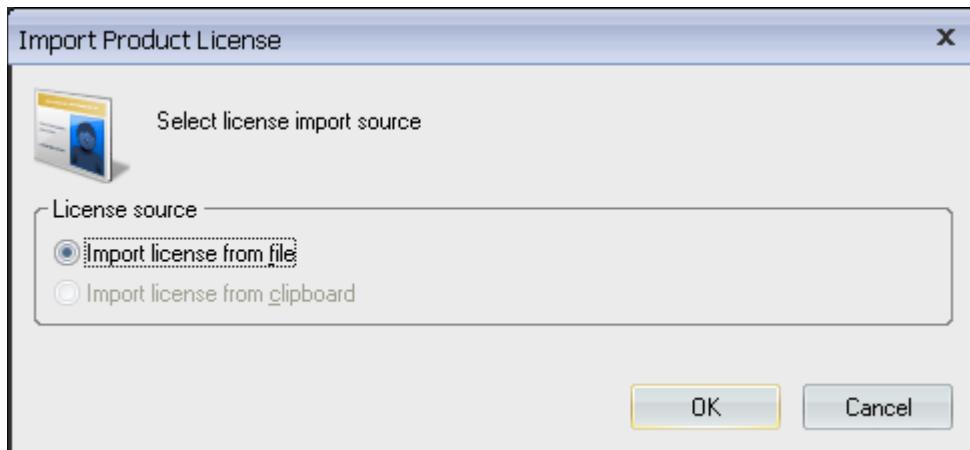
Fig. 1 - Importing a license in UltraBac.

4. Select "Import license from file" and click "OK."
5. Browse to the UltraBac8 directory, select the "ublicense.txt" file, and click "Open."
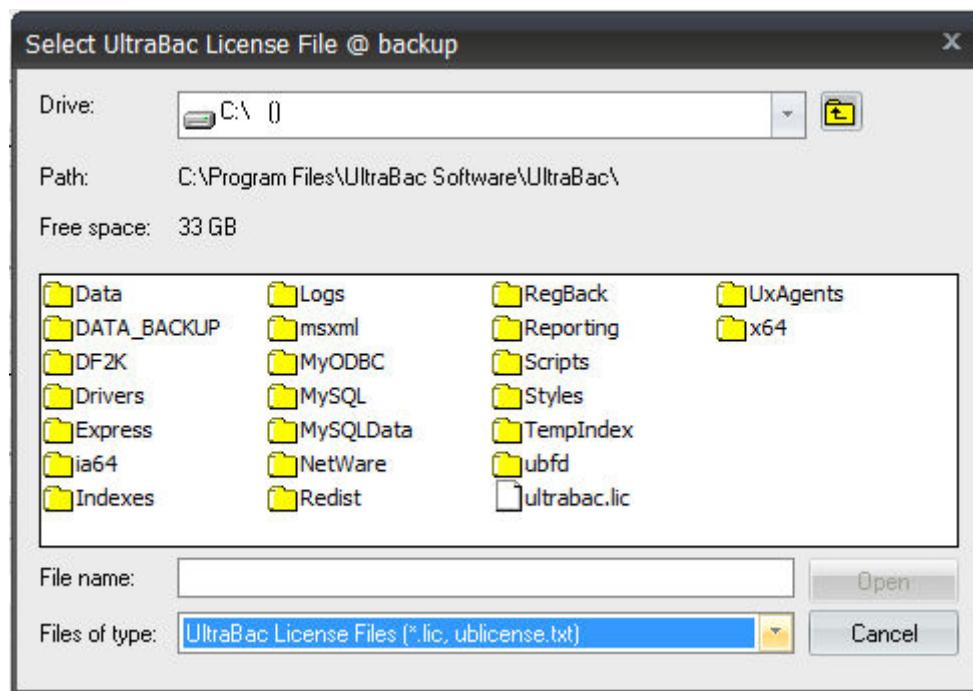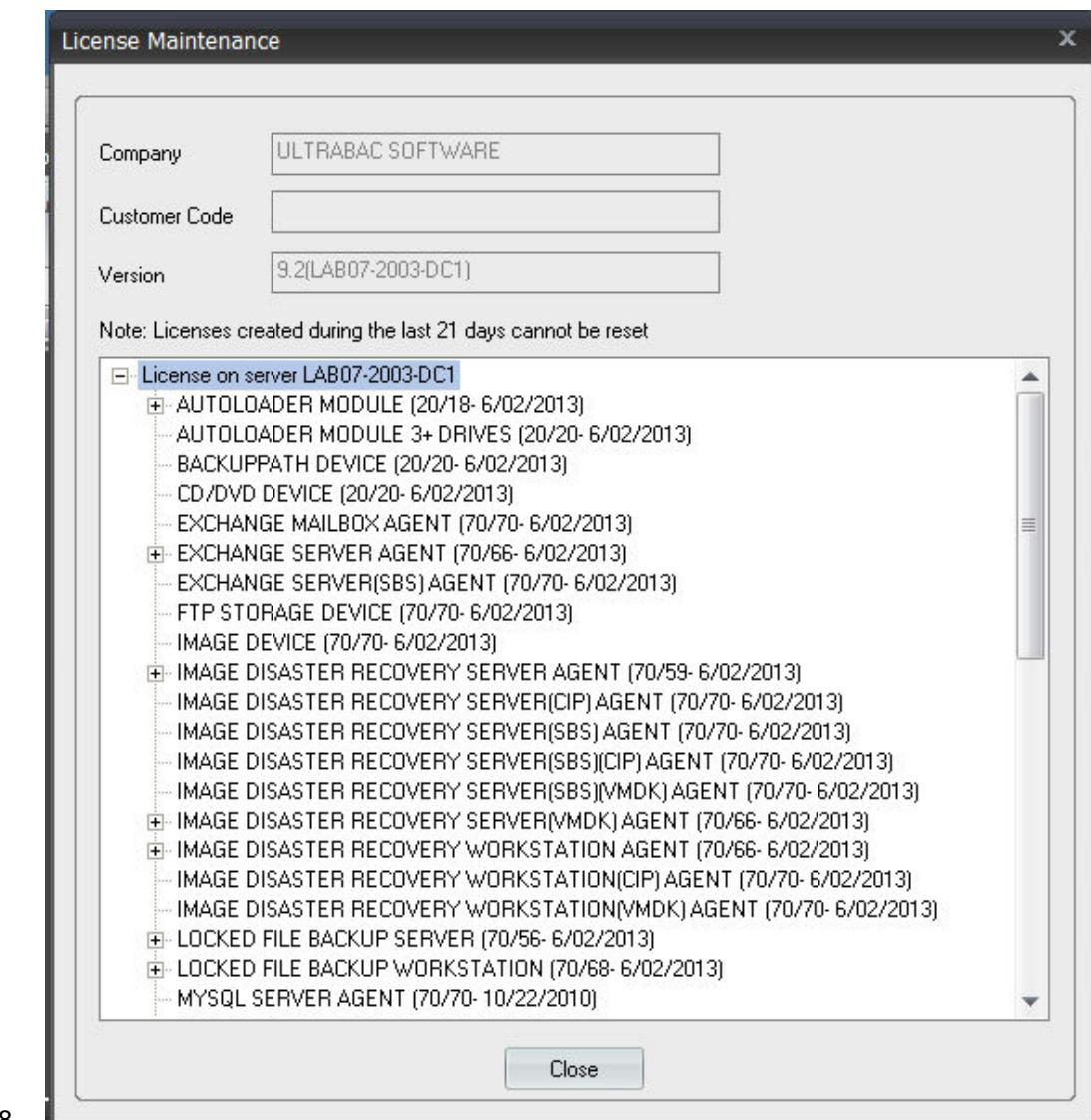
Fig. 2 - Browsing to the license file.

6. If the license was imported successfully, a dialog box will open with the message, "The license has been imported successfully."
7. Confirm the successfully imported license file by accessing "Tools"/"License Management"/"Edit License." A list of licensed components will appear underneath the computer name.

8.

Fig. 3 - License components.

NOTE: The "Edit License" functionality is not supported by Demo licenses.

License Details

The "License Maintenance" screen shows:

- Company
- Customer code
- UltraBac version
- Each component/agent licensed
- Number of licenses issued for each component/agent
- Expiration date for each component/agent licensed

View the list of issued licenses for each agent by clicking on the "plus sign" to the left of the agent. This shows:

- Names of servers that have acquired licenses for each component/agent
- "Modified" date – last date the agent or component was used
- "Created" date – date the license was issued to the system

A license can be reset by expanding the component, right clicking on the server name, and clicking "Reset License."

Updating an Existing License

Adding components of the software will require a new license file, obtained from UltraBac Software. Contact your account manager for pricing.

When the new license is received from licensing@ultrabac.com, import the new license directly over the previous license.

Pushing the License

It is possible to "push" a license to a remote license server when the license is issued to the server by name. Import the license from any UltraBac host and it will automatically export it to the correct system.

When using a centralized license server, it is only necessary to point the remote systems to the license server by selecting the Manage tab, and click "Licensing"/"Set License Server."

Upgrading to Version 9

To upgrade a prior Version 7 or 8 license to Version 9, please visit:

http://www.ultrabac.com/licensing/

Upon completion, submitting this form will send it to the UltraBac Software Licensing department.

UltraBac Management Console

The UltraBac Management Console is used to configure, manage, and maintain all UltraBac operations. The Management Console can show backup, verify, and restore logs along with scheduled backups and backup sets.

UltraBac Management Console Toolbars
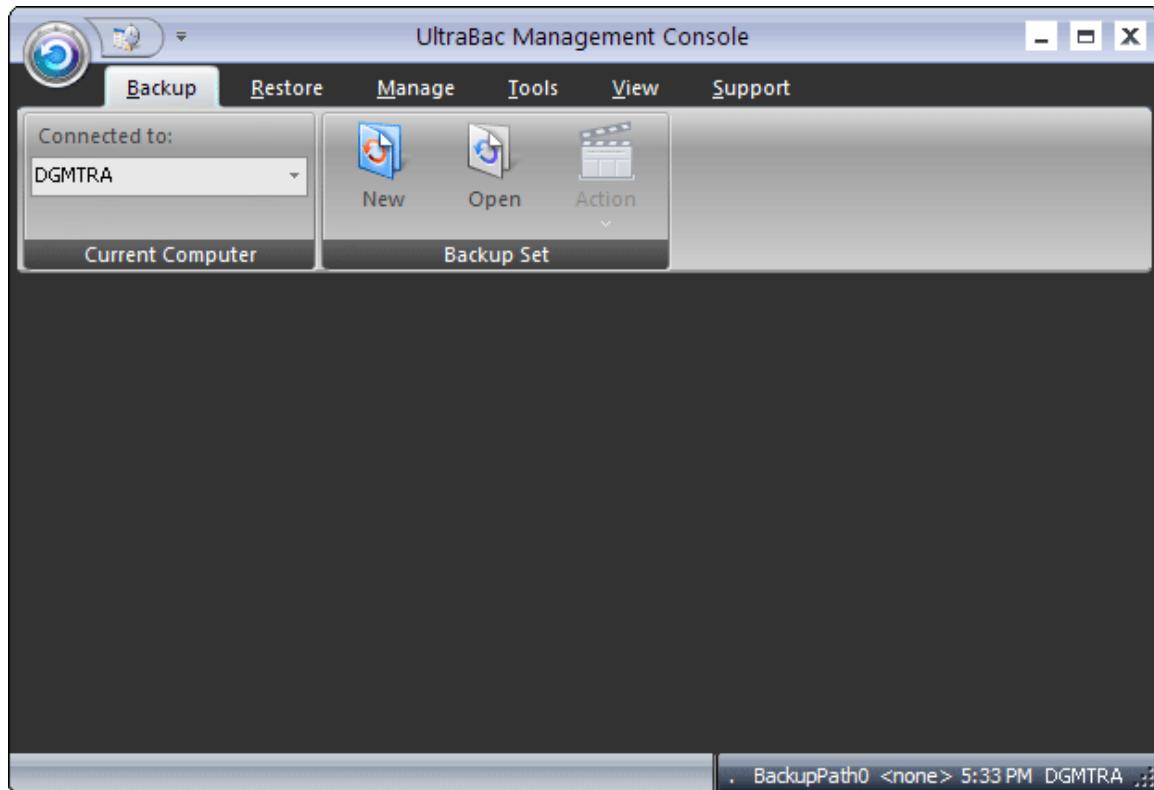
Fig. 1 - The UltraBac Management Console.

The UltraBac Management Console now has multiple tabs that each contain options, settings, and other management functionality. Clicking on each tab will bring up each individual operations menu:

- Backup – Launches the Backup Wizard, opens backup sets/groups, and allows backup operations to be run.
- Restore – Launches the Restore Wizard, and restore operations.
- Manage – Allows the management of UltraBac storage devices, licensing, and other settings.
- Tools – Launches UltraCopy, the UltraBac Scheduler, and the UltraBac Installer.
- View – Used to display log files, reports, and device information.
- Support – Launches the Help file, the UltraBac Web site, and the version information.

Backup Toolbar

The Backup toolbar can be used to create new backup sets, modify existing backup sets, and to modify the properties of sets. This toolbar can also be used to create new scheduled jobs, and to

start a set-level ad hoc job. The "Action" button will remain unavailable until a backup set is opened for enumeration.
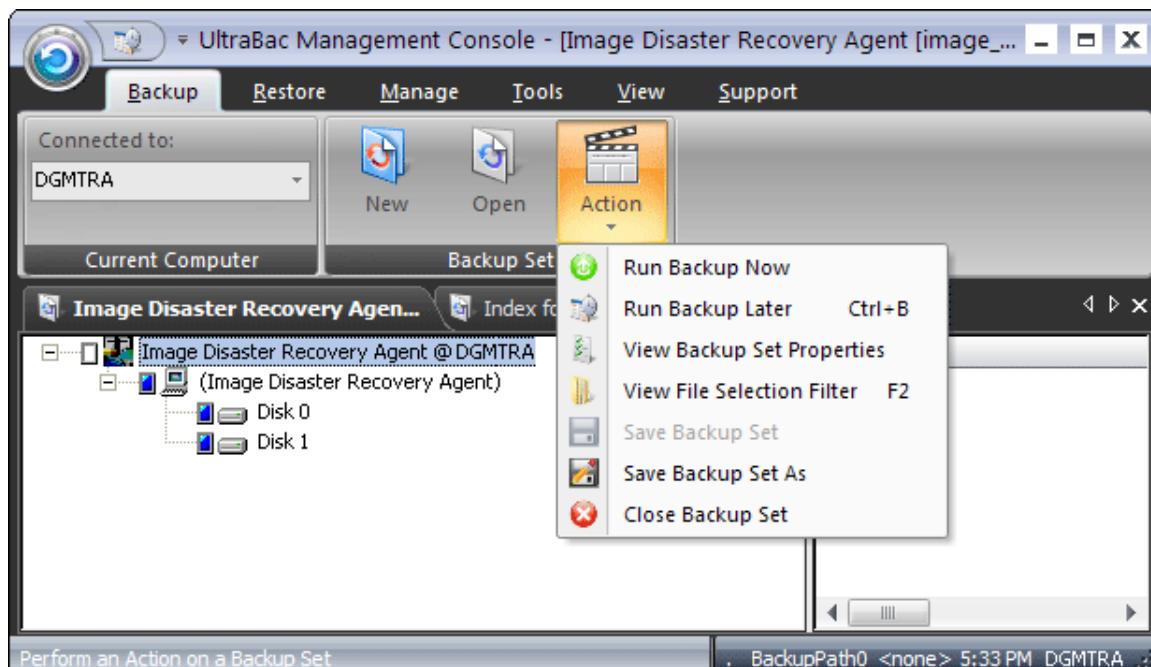
Fig. 2 - The Backup toolbar.

- New – Launches the Backup Wizard used to create backup sets.
- Open – Opens backup sets or groups stored in the "Data" directory ("C:\Program Files\UltraBac Software\UltraBac\Data").
- Action – Displays a sub-menu containing the following options:
    - o Run Backup Now – Runs the open backup set to the selected backup device.
    - o Run Backup Later – Opens the Scheduled Backup Wizard to create a new scheduled backup job.
    - o View Backup Set Properties – Views the properties of the open backup set for editing. Each agent has its own specific options/properties.
    - o View File Selection Filter – Views the file selection logic as used in the open backup set.
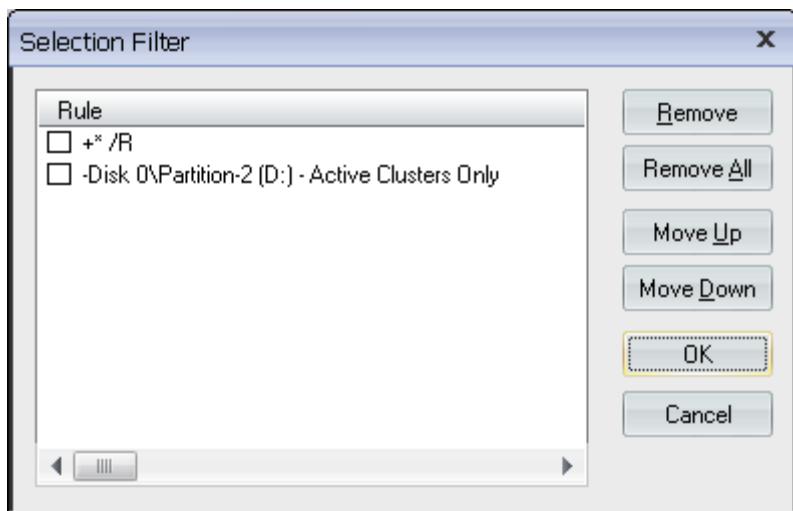
Fig. 3 - UltraBac File Selection Filter.

- o
- o Save Backup Set – Saves the open backup set using the current set name.
- o Save Backup Set As – Saves the open backup set using a user-generated name.
- o Close Backup Set – Closes the open backup set.

Restore Toolbar

The Restore toolbar is used to load backup indexes, view the properties of a completed backup set, and perform backup/verify operations.
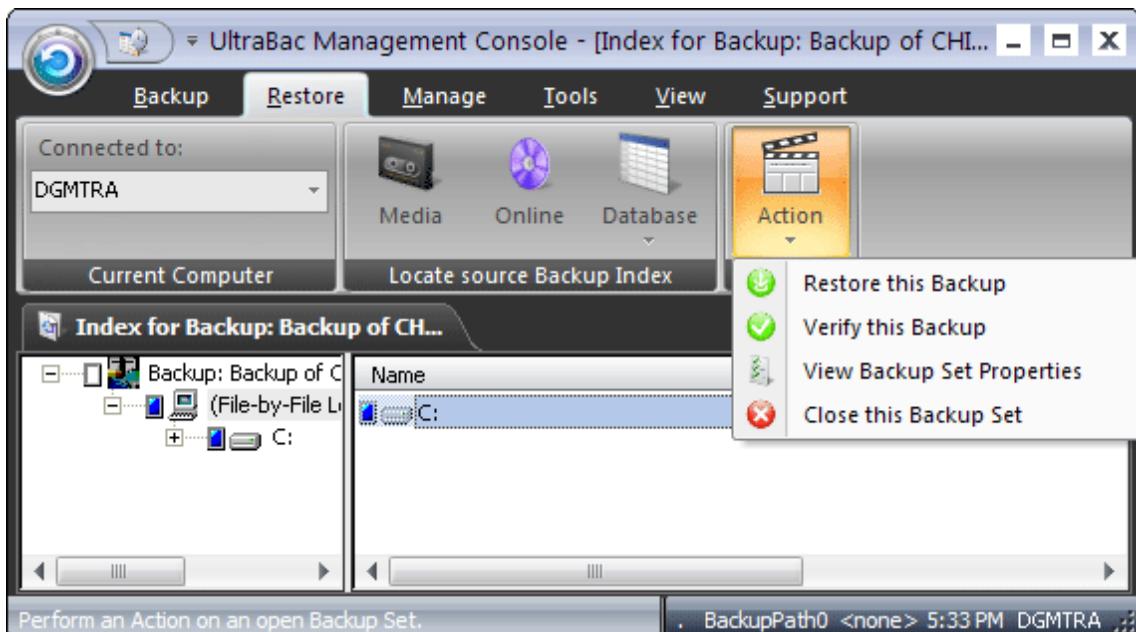
Fig. 4 - The Restore toolbar.

Locate source Backup Index:
- Media – Loads a list of all backup set indexes stored on the selected backup media.
- Online – Loads a list of all backup set indexes stored on the disk of the backup host.
- Database – Loads a list of options for selecting an index stored in the Index Database:

- Retrieve From Current Media in the Drive – Load a list of all indexes on the selected device.
- Retrieve From Storage Media Group – Load a list of all indexes used in the backup on the selected device and any other devices used in that job.
- Retrieve All Sets in the Database for the local machine – Load a list of all indexes in the database for the local system.
- Retrieve All Sets in the Database – Load a list of all sets in the database.
- Action – Loads a list of operations:
  - Restore this Backup – Start the restore process for all selected data.
  - Verify this Backup – Perform a manual verify of all selected data.
  - View Backup Set Properties – View the properties of the currently loaded backup set index.
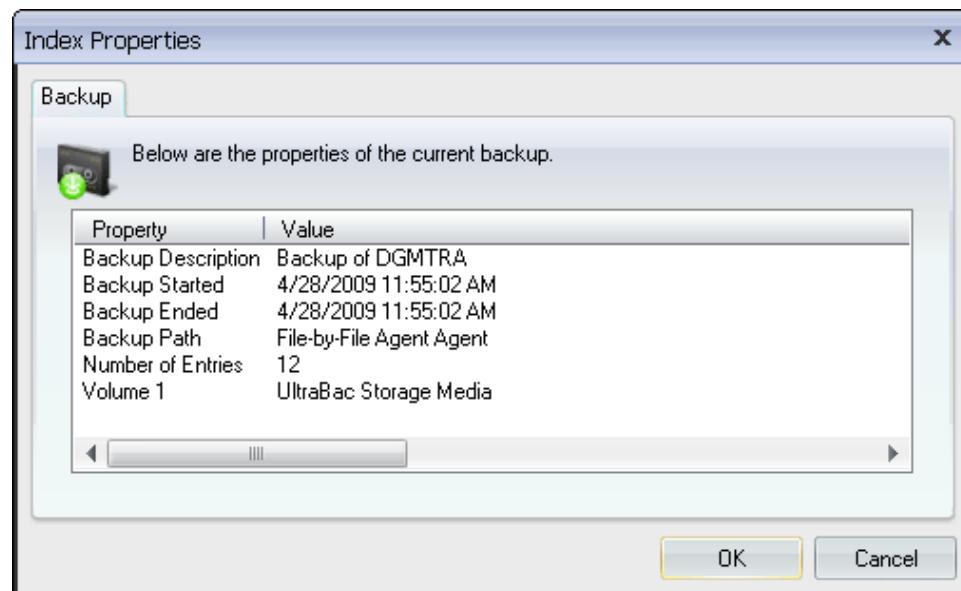
Fig. 5 - Properties of the selected file-by-file backup index.

- Close this Backup Set – Closes the backup set index.

Manage Toolbar

The Manage toolbar is used to set global options for backups, and to maintain backup devices, licensing, and Index Database functionality.
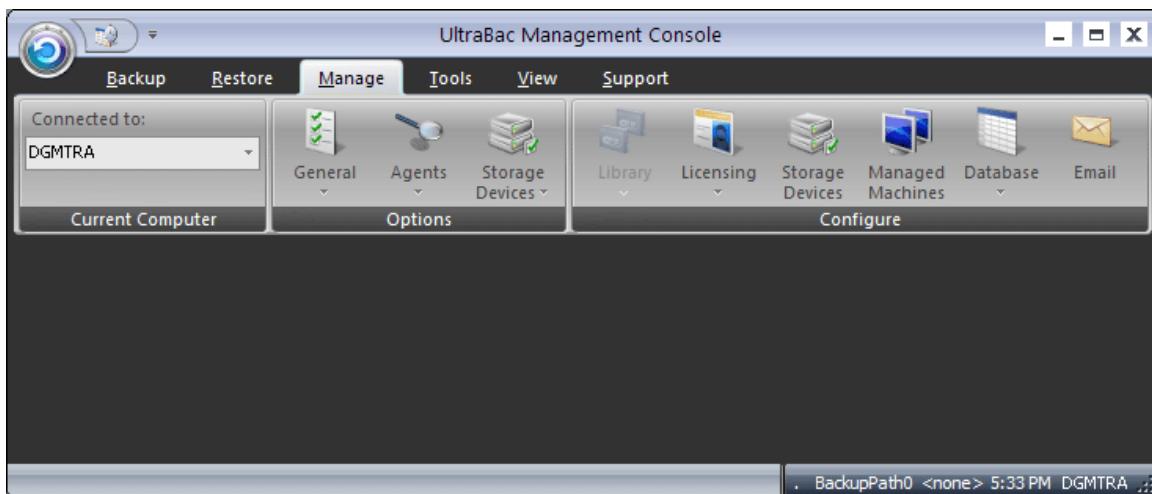
Fig. 6 - The Manage toolbar.

Options:
- General – Lists the available global options for UltraBac.
- Agents – Lists the available global options for all UltraBac agents.
- Storage Devices – Lists the available global options for all UltraBac devices.

Configure:
- Library – Allows users to maintain and manage a media library.
- Licensing – Used to import and maintain UltraBac licenses.
- Storage Devices – Allows the creation of backup path devices, and the selection of the default device.
- Managed Machines – Opens the Managed Machines list, allowing users to add and delete machines from the list.
- Database – Launches the Index Database Configuration Wizard.
- Email – Launches the SMTP Configuration Wizard.

Tools Toolbar

The Tools toolbar has options for Media tools, remote installation, and backup job scheduling.
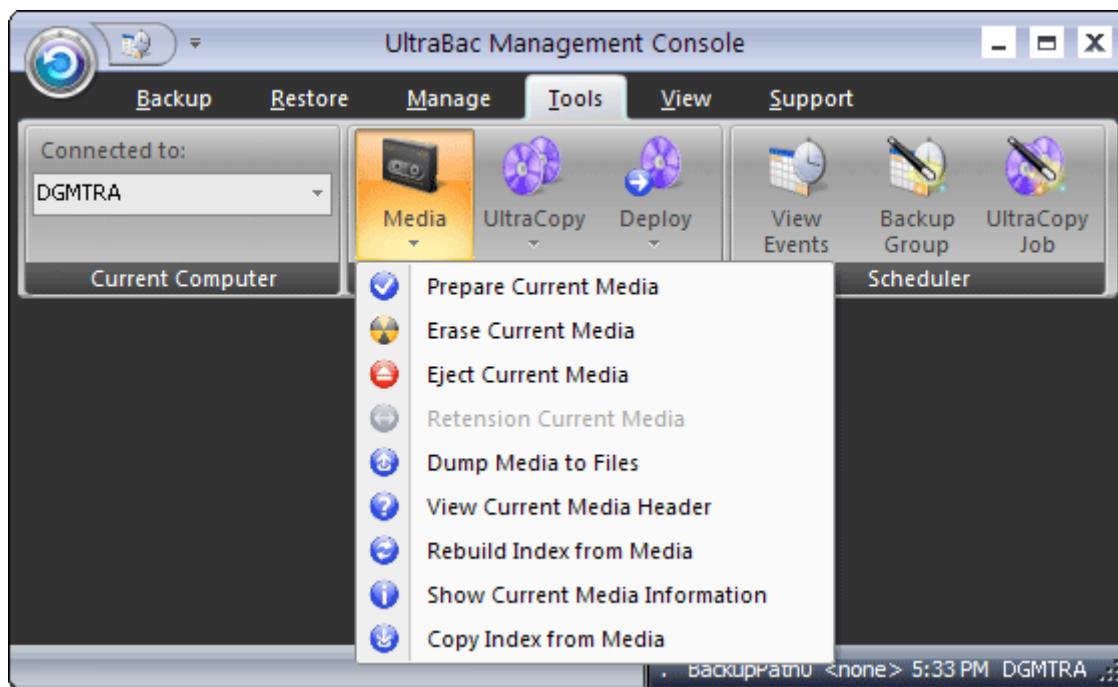
Fig. 7 - The Tools toolbar.

Tools:
- Media – Allows users to perform multiple media operations:
  - Prepare Current Media – Deletes the existing media header and all backup data on any selected disk based media, and creates a new header.
  - Erase Current Media – Deletes the media header, and all backup data on any selected disk based media.
  - Eject Current Media – Ejects removable media.
  - Retension Current Media – Winds the selected tape media to the end of the tape and then rewinds. This option is only used on legacy tape devices.
  - Dump Media to Files – Dumps the contents of tape media to a disk path.
  - View Current Media Header – Views the header of the selected media.
  - Rebuild Index from Media – Scans the selected media for all file-by-file backup data.
  - Show Current Media Information – Shows statistics of the selected media, such as capacity and media remaining.
  - Copy Index from Media – Copies the selected media's indexes to the Online Index.
  - UltraCopy – Launches UltraCopy for ad-hoc copy operations, or the UltraCopy Scheduler Wizard.
- Deploy – Launches the UltraBac Remote Installer.

Scheduler:
- View Events – Opens the UltraBac Scheduled Events pane.
- Backup Group – Launches the UltraBac Scheduler Wizard.
- UltraCopy Job – Launches the UltraCopy Scheduler Wizard.

View Toolbar

The View toolbar gives access to UltraBac/UltraCopy logs, Current/Future operations, and additional device information.
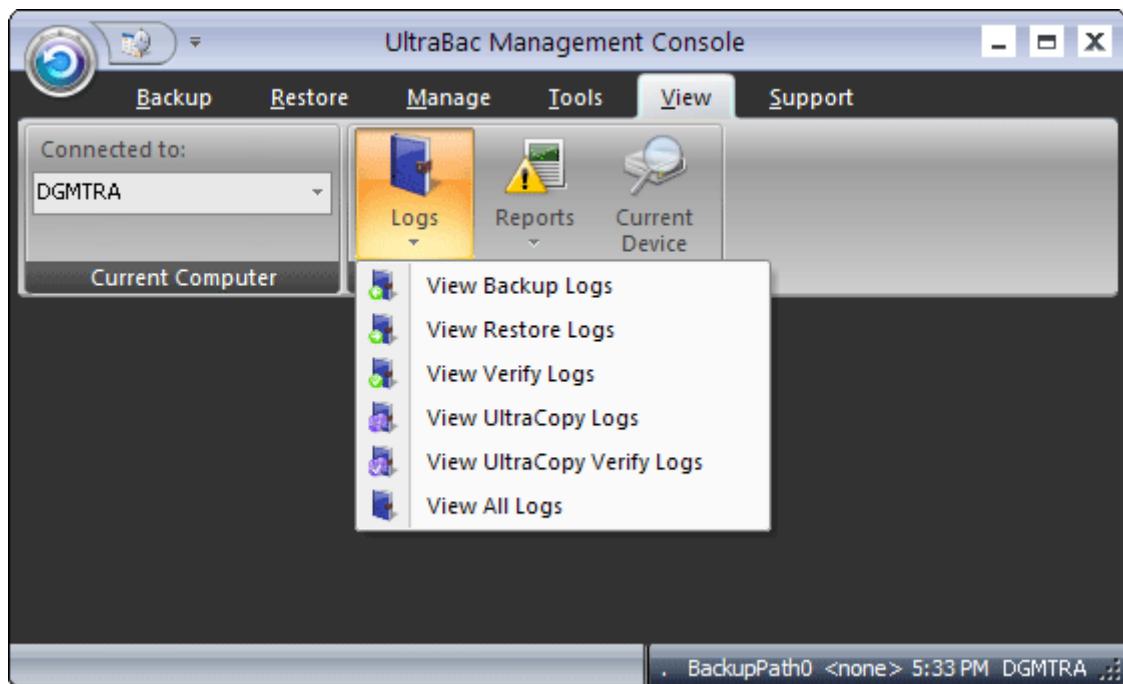
Fig. 8 - The View toolbar.

Logs:

- View Backup Logs – Launches the Log File screen, filtered to view only backup logs.
- View Restore Logs – Launches the Log File screen, filtered to view only restore logs.
- View Verify Logs – Launches the Log File screen, filtered to view only verify logs.
- View UltraCopy Logs – Launches the Log File screen, filtered to view only UltraCopy copy logs.
- View UltraCopy Verify Logs – Launches the Log File screen, filtered to view only UltraCopy verify logs.
- View All Logs – Launches the Log File screen, with no filter.

Reports:

- View Current Operations – Launches the Current Operations workspace.
- View Future Operations – Opens a list of enabled backup jobs.

Current Device:

The Current Device option opens a list of all features and functions supported by the selected device.

Current Operations
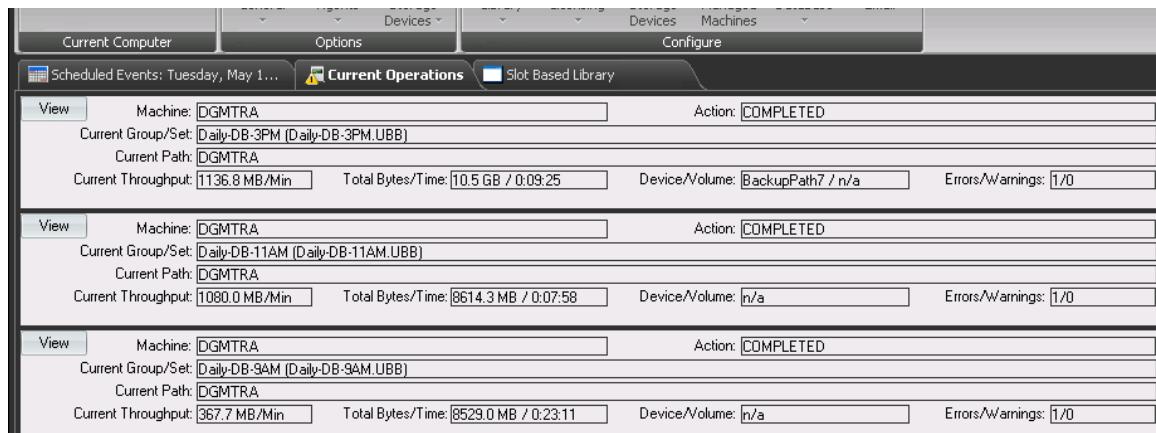
Fig. 9 - The Current Operations workspace.

Process statistics and information shown in the Current Operations workspace:

- Machine – System hosting the active process.
- Action – Type of active process, and current status of the process.
- Current Group/Set – Current set being backed up.
- Current Path – Current file being backed up.
- Current Throughput – Current data transfer rate of the active process.
- Total Bytes/Time – Total amount of data transferred, and elapsed time.
- Device/Volume – Storage device being used, and volume number of the device.
- Errors/Warnings – Total number of errors and total number of warnings reported during the active process.

View button – Launches the UltraBac progress screen.

The Current Operations workspace can display the backup host and/or the systems listed in the Managed Machines list. This preference is set under "Manage"/"General"/"UltraVue Options."

UltraBac keeps a user specified list of machines (UltraBac backup hosts) to be managed. To view the Managed Machines list, click "Managed Machines" from the Manage toolbar.

File Viewer

The UltraBac File Viewer can be used to show the contents of backup sets, indexes, and all log files.
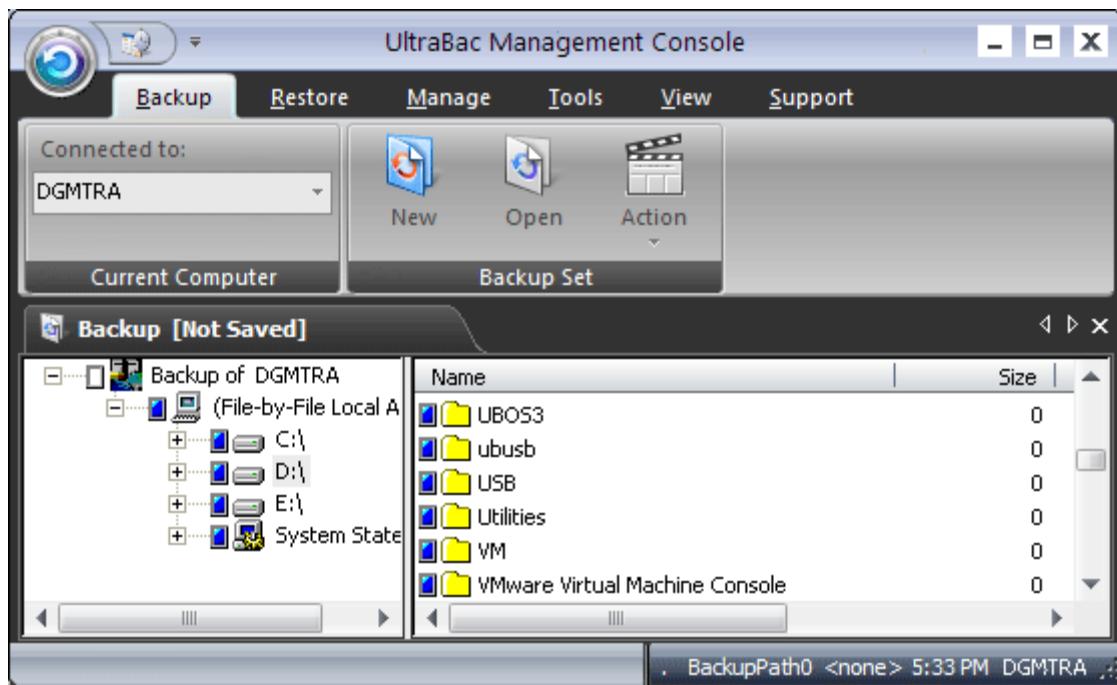
Fig. 10 - Backup set loaded in the File Viewer.

Remote Administration

Using the "Connect" feature, it is possible to administer all UltraBac operations from a remote server or workstation. This includes creating sets, scheduling backups, editing sets, restoring from tape, setting preferences, etc. When connected to the remote system through the "Connect" feature, the UltraBac user interface will act as if logged into the backup host locally, similar to Windows Terminal Services.

Usage

The UltraBac Management Service must be installed and running on the connection target system. UltraBac receives the security information required for user authentication on the remote system from the UltraBac Management Service. When authenticating through a domain, UltraBac will use an account specified for the target system (listed in "Manage"/"General"/"Authentication Options"/"Show Accounts") to gain access to the remote UltraBac host. If no specified account is available, UltraBac will use the default account.
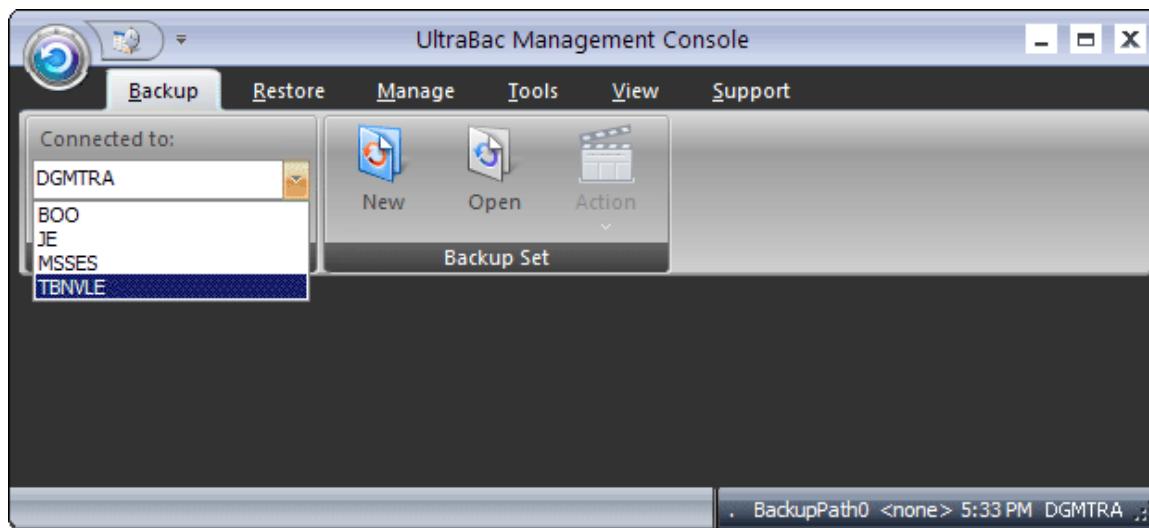
Fig. 11 - The "Connect" feature.

To connect to the remote system's console:
1. Add the target system to the Managed Machines list:
    1. Select the Manage tab.
    2. Click "Managed Machines."
    3. Click "Add Machine."
    4. Type in the Windows name of, or browse to, the target system, and click "OK."
    5. Click "Close."
2. From the "Connected to:" menu, select the target system.

After a system has been added to the Managed Machines list, it will appear in the main toolbar drop-down list box, making it easy to switch from one UltraBac host to another.

Once connected to another system, move through the UltraBac user interface as if you were logged into the managed system locally.

Selecting the local system from the menu will break the connection and return to the local machine's interface.

Storage Device Manager

UltraBac stores information on backup output devices in the UltraBac Storage Device Manager. This utility allows the administrator many different kinds of storage devices. To access the UltraBac Storage Device Manager, click "Select"/"Storage Devices" from the main UltraBac menu.

- Tape – locally attached tape devices, including libraries.
- CD\DVD – locally attached CD\DVD writers.
- BackupPath – disk path devices.
- Tivoli – IBM Tivoli devices.
- FTP – internet FTP\SFTP sites.
- Image – unpartitioned disk used for static mirror imaging.
- Partition – partitioned disk used for static mirror imaging.
- Remote – UltraBac devices configured on remote systems.

Tape Devices

To use a locally attached tape device, ensure that the latest Windows device driver is loaded for each tape device. Locally attached tape devices are automatically enumerated by UltraBac, numbered in sequential order starting with the lowest SCSI ID. UltraBac will automatically assign names to these devices, starting with "Tape0."
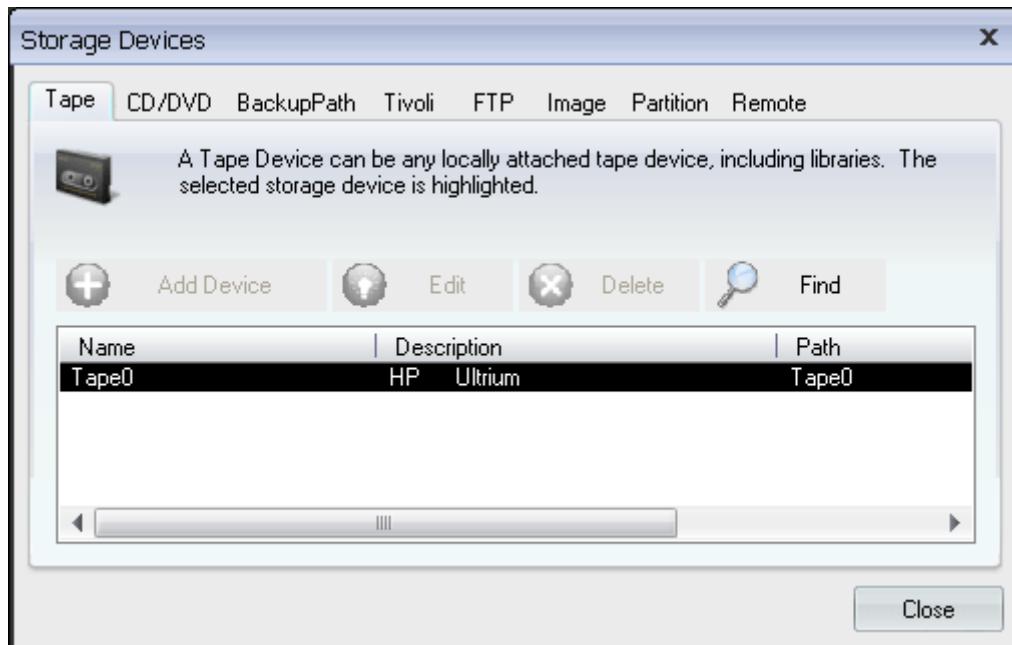
Fig. 1 - Tape devices.

CD/DVD Devices

If a CD/DVD writable drive is installed in the backup host, it will automatically appear in the CD/DVD tab.
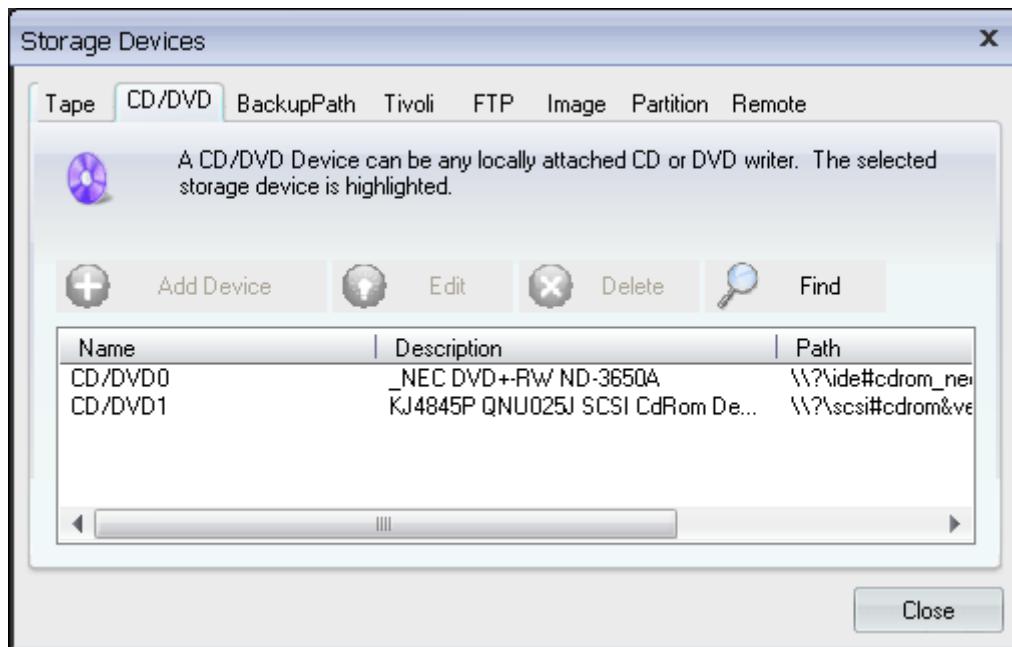
Fig. 2 - CD/DVD devices.

The UltraBac CD/DVD device uses two methods to write backup data to disc in a RAW format. This format makes the disc unreadable to the Windows operating system. To set the write method of CD/DVD devices, highlight the device to select and click the "Properties" button:
- Unformatted – Allows for the full capacity of the disc to be used, but the disc can only be used for one backup job before being erased.
- Formatted – Formats the disc upon first usage to allow for multiple backups.

BackupPath Devices

BackupPath devices are user-created output targets that point to a folder on the backup host, or on a network path. When creating a BackupPath device, there must be enough space to hold all data being backed up to that device. To create a BackupPath device:

1. Open the Storage Device Manager by selecting the Manage tab, and clicking "Storage Devices."
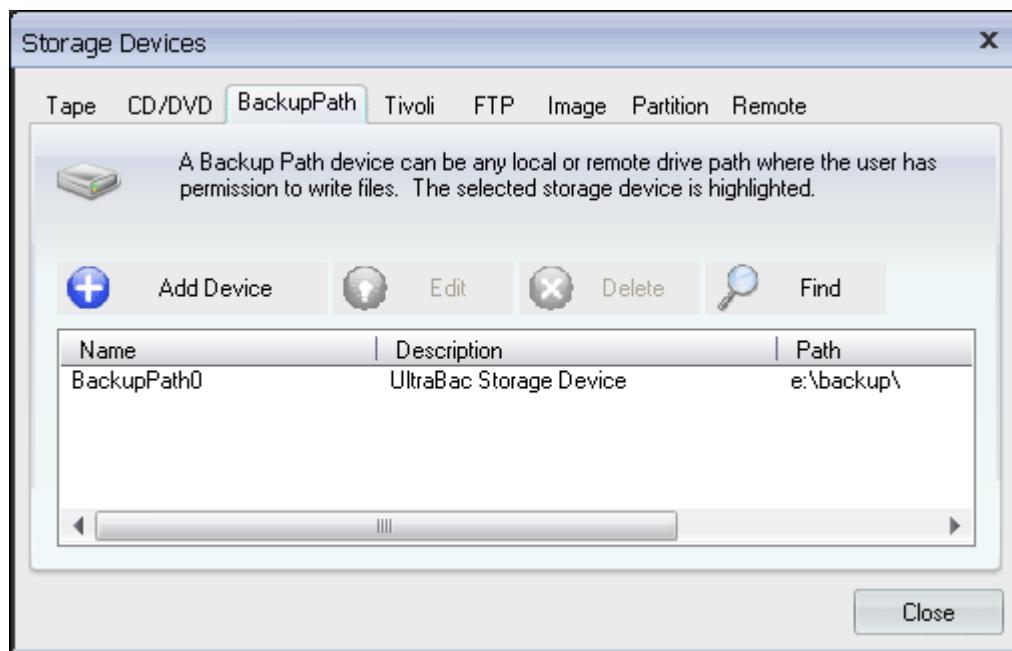
Fig. 3 - Creating a BackupPath device.

2. Select the BackupPath tab.
3. Click "Add Device."
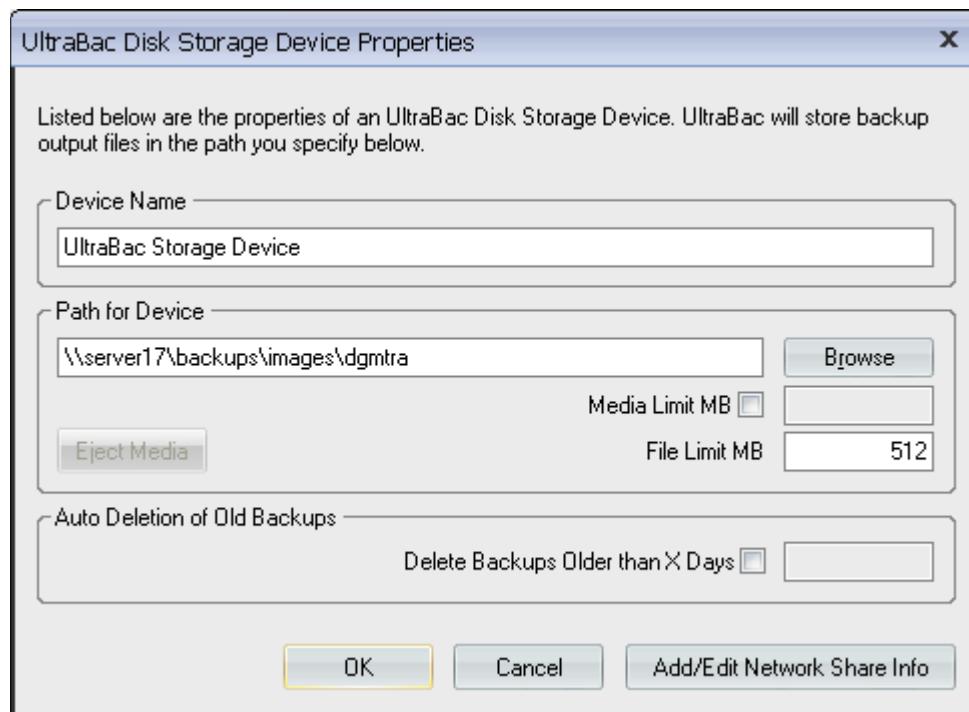
Fig. 4 - Disk Storage Device properties.

4. Enter a unique name in the "Device Name" field.
5. Enter a local or UNC path to be used as an output target in the "Directory for Device" field.

6. Click "OK" to save. If the directory specified does not exist, UltraBac will create it.
7.

To limit the amount of data that can be written to the BackupPath, enter the maximum folder size in the "Limit size per media" field. This will force UltraBac to write to a failover device, or abort the backup, if the amount of data written to the disk path reaches the specified limit.

To change the size of the files written to the BackupPath, enter the desired size in the "Limit size per file" field. It is not recommended to use a file size larger than the 512 MB default.

Auto Deletion of Old Backups

Checking "Delete Backups Older than X Days" will allow UltraBac to write multiple days' worth of backups to the same BackupPath device, and keep only an archive of the specified number of days.
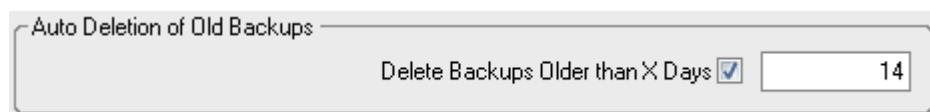
Fig. 5 - Auto deletion of old backups.

To specify the number of days to store backups:
1. Check "Delete Backups Older than X Days."
2. Specify the number of days to store the backups in the field to the right of the checkbox.
3. Click "OK" in the "Disk Storage Device Properties" screen.

NOTE: For information on configuring a Backup Path to a CIFS Share or an HP StorageWorks D2D Backup System, please see the UltraBac Knowledge Base articles:

See UBQ000264: Writing to CIFS Backup Path
See UBQ000260: HP StorageWorks D2D Backup Systems Support

Tivoli Devices

NOTE: To use the Tivoli device, the backup host must be running the Tivoli client software. You can download the client software from the following link:

http://service.boulder.ibm.com/storage/tivoli-storage-management/maintenance/client/

To define a Tivoli device:

1. Open the Storage Device Manager by selecting the Manage tab, and clicking "Storage Devices."
2. Select the Tivoli tab.
3. Click "Add Device."
4. Enter a unique device name in the "Device Name" field.
5. Enter the name or IP address of the Tivoli server in the "Server" field.
6. Enter the password defined on the selected Tivoli server for the Node name in the "Password" field.
7. Enter the Folder (high-level name) to use for backup in the "Folder" field.
8. Enter the output file size in the "Object Size" field.
9. Click "OK" to save.
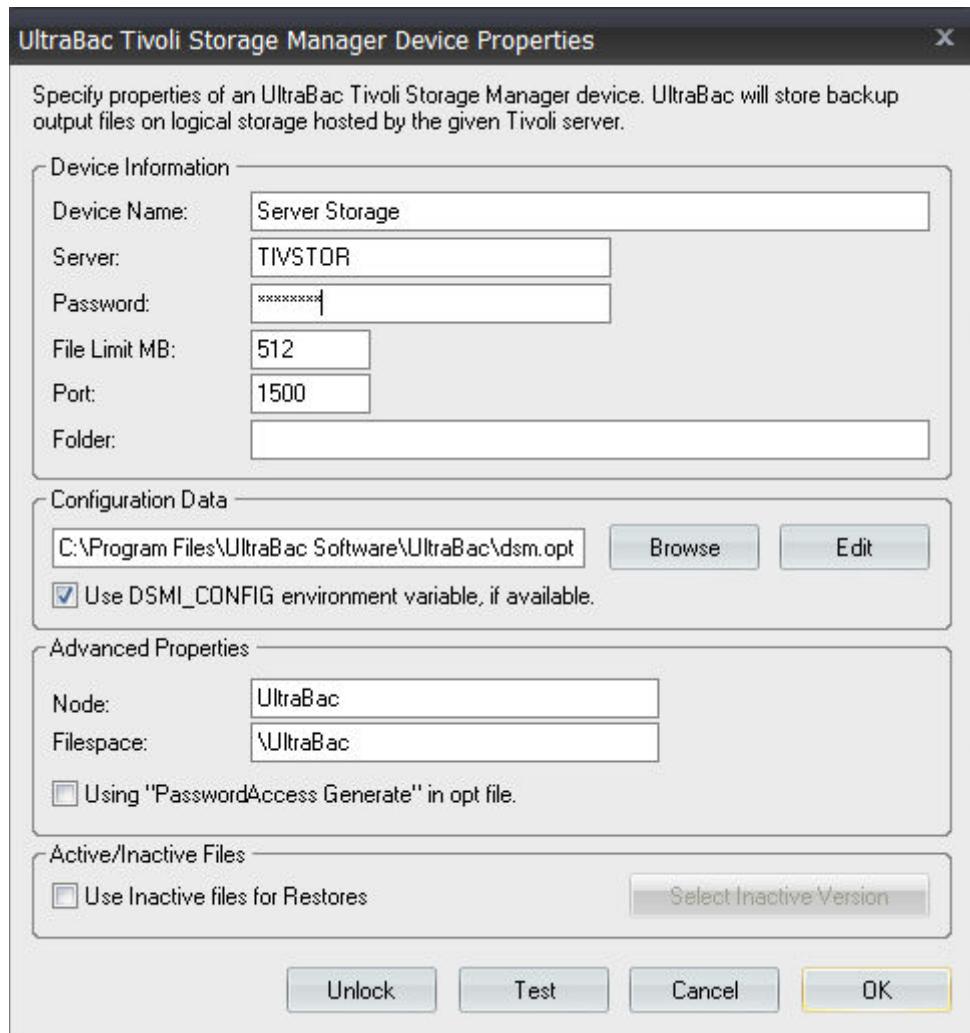
Fig. 6 - Tivoli device properties.

Advanced Properties

- Configuration File – This is the TSM Client config file and defines things like the communication protocol and port number to use when communicating with the server.
- Use DSMI_CONFIG environment variable, if available – Selects whether the DSMI_CONFIG environment variable, if set, overrides the above path.
- Node – The Node name that UltraBac passes to the Tivoli server.
- Filespace – Part of an object's full name and stems from ADSM being designed to back up servers.

Click "Test" to ensure the device is working correctly.

FTP Device

The FTP device provides UltraBac with the ability to direct backups to any FTP server compliant with the RFC 959 specification and sufficient space to store backup output files. This is especially useful for configuring an offsite backup location, or to non-Windows file storage.

To add an FTP device:

1. Open the Storage Device Manager by selecting the Manage tab, and clicking "Storage Devices."
2. Select the FTP tab.
3. Click "Add Device."
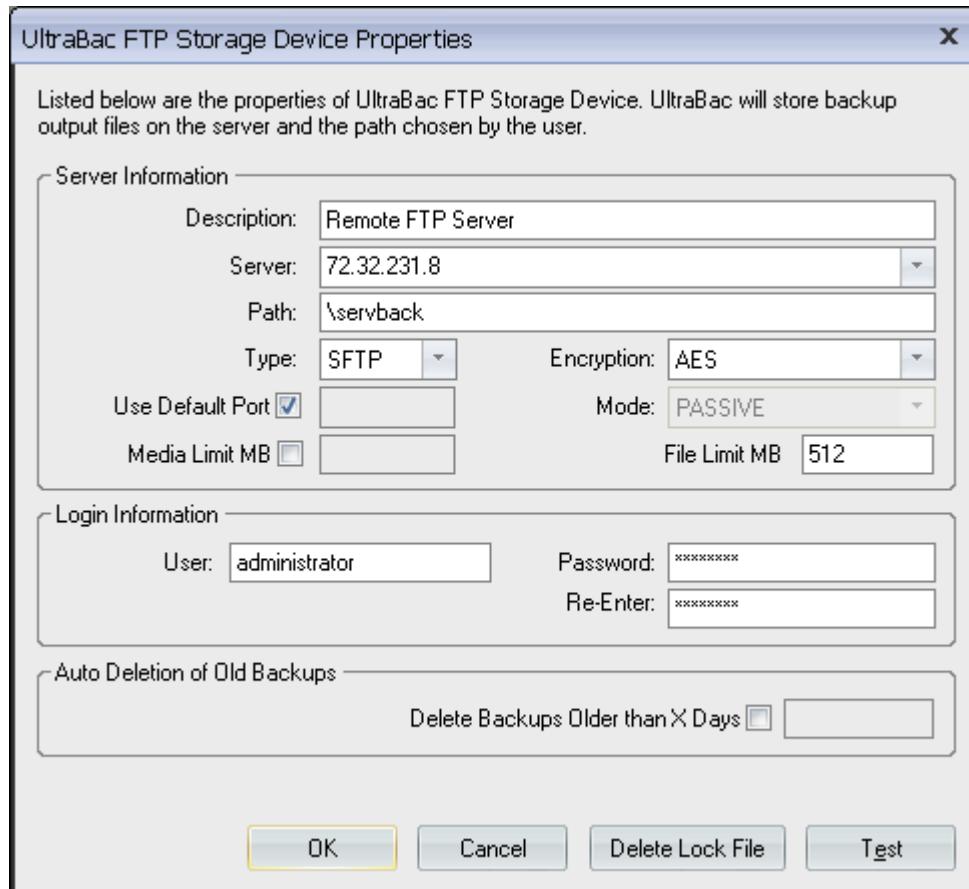
Fig. 7 - Adding an FTP device.

4. Type a unique device description (as it will appear in the backup log) into the "Description" field.
5. Type an FTP server name or IP address in the "Server" field.
6. Type a folder path to be used to store backup data in the "Path" field. This must be the full path, from the FTP root directory to the location where the backup files will be stored.
7. Type the user name for the FTP server in the "User" field.
8. Type the password for the user name in the "Password" field.
9. Re-type the password for the user name in the "Re-Enter" field.
10. Click "OK" to save.

Additional FTP Device Options

- Media Limit MB – Restrict the amount of data the device can accept to the amount (in megabytes) listed in this field.

- Limit size per file – Limit the backup output file size to the amount (in megabytes) listed in this field.
- Test – Establish a test connection to the FTP directory.
- Delete Lock File – Deletes the .ubd file that is created when the device is in use.
- Type: – This allows the FTP device to use standard FTP or SFTP servers.
    - FTP – File Transfer Protocol server.
    - SFTP – Secure FTP server, allowing UltraBac to encrypt the all data transferred to the SFTP server.
- Encryption
    - Blowfish – Uses the Blowfish encryption algorithm when writing to the SFTP server.
    - DES – Uses the Data Encryption Standard algorithm when writing to the SFTP server.
    - None – Do not use encryption during data transfer.
    - ThreeDES – Uses the ThreeDES encryption algorithm when writing to the SFTP server.
- Use Default Port – Uncheck this field to specify a port other than the default FTP port.

Auto Deletion of Old Backups

Checking "Delete Backups Older than X Days" will allow UltraBac to write multiple days' worth of backups to the same BackupPath device, and keep only an archive of the specified number of days.
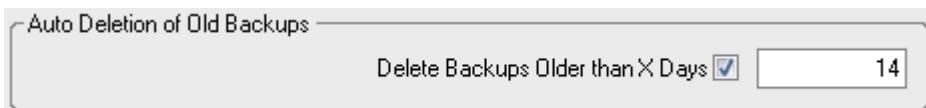
Fig. 8 - Auto deletion of old backups.

To specify the number of days to store backups:
1. Check "Delete Backups Older than X Days."
2. Specify the number of days to store the backups in the field to the right of the checkbox.
3. Click "OK" in the "Disk Storage Device Properties" screen.

Image and Partition Devices

A static mirror image backup requires the creation of either an Image or Partition device. It is necessary to have either Partition or Image devices that are of the same size, or larger, than the original disk/partition. These backups can only be performed to a local disk.

- Image device – If a hard disk is present with all partitions deleted, it will be available for addition as an Image device.
- Partition – If a partition is created on a hard disk, with no assigned drive letter, it will be available for addition as a Partition device.

NOTE: For additional information on Static Mirror Image backups, please visit the "**UltraBac Disaster Recovery**" section of the User Manual:

UltraBac User Manual: UltraBac Disaster Recovery

Remote Device

The Remote device option allows UltraBac to use a tape device attached to a system other than the UltraBac backup host.

NOTE: The "UltraBac Device Drivers" must be installed on the system hosting the tape drive. Tape devices are automatically enumerated when UltraBac is installed on the tape host, and these devices are numbered in sequential order starting with the lowest SCSI ID. UltraBac will automatically assign names to these devices, starting with "Tape0."

1. Open the Storage Device Manager by selecting the Manage tab, and clicking "Storage Devices."
2. Select the Remote tab.
3. Click "Add Device."
4. Enter the Windows name or IP address of the tape host in the "Device Host" field.
5. Enter the UltraBac assigned device name in the "Remote Device" field, or click "Browse" to select.
6. Click "OK" to save.
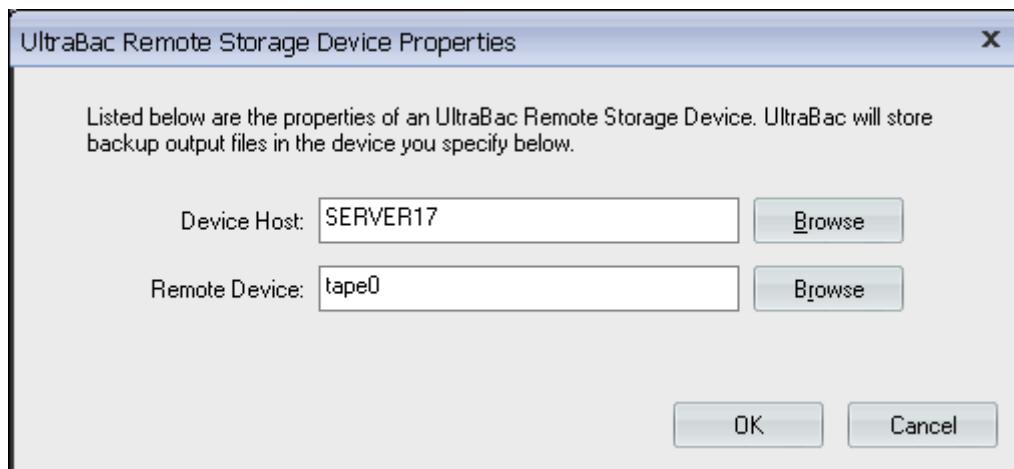
Fig. 9 - Remote device properties.

Device Selection

The currently selected device is shown on the main title bar of UltraBac.

To set a device as the default:

1. Click the device to highlight it.
2. Click "OK."

To select the device for use during an ad-hoc backup:

1. Start an ad hoc backup.

2. Click the "Browse" button in the "Backup Options."
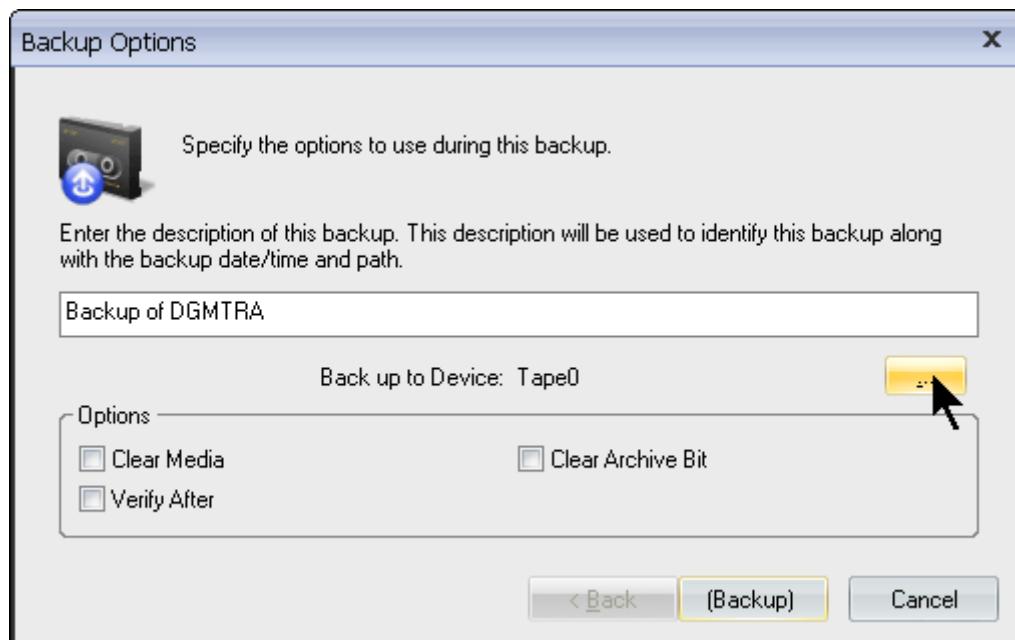
Fig. 10 - The "Browse" button in the "Backup Options."

3. In the "UltraBac Device Browser," click on the device to use for backup.
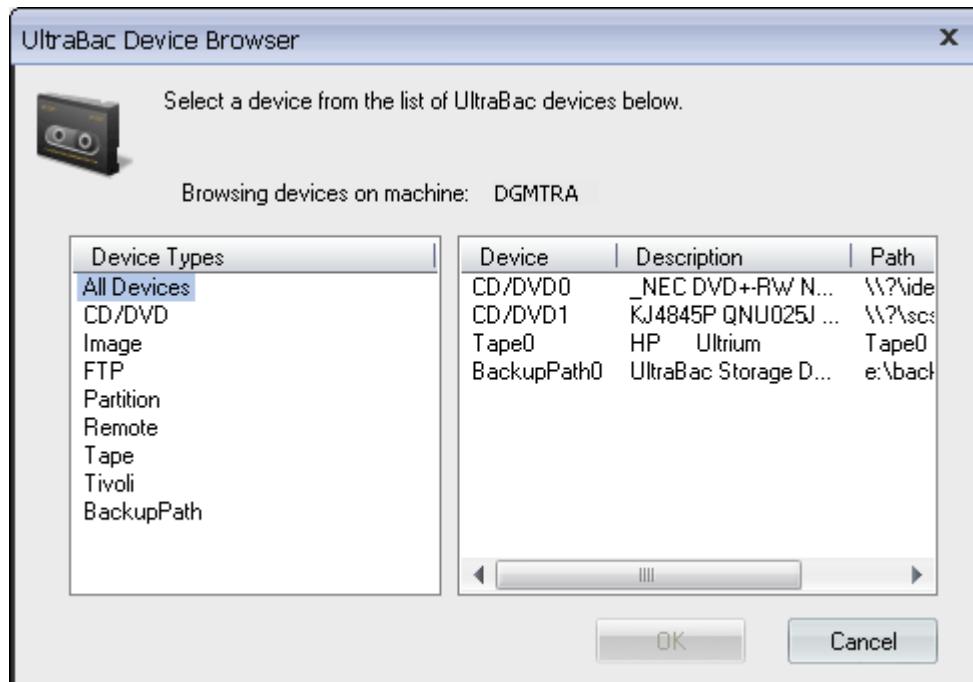
Fig. 11 - UltraBac Device Browser.

4. Click "OK" to select.

UltraCopy

UltraCopy is a utility used to copy the contents of one storage media to another, such as "Backuppath0" to "Tape0." This utility can provide for redundant copies of backups for safekeeping off-site.

To copy storage media:

1. From the Tools tab, click "UltraCopy"/"Run UltraCopy Now."
2. Under "Available Devices," highlight the source device to copy from, and add it to the "Selected Devices" by clicking the "Add>>" button. Click "Next."
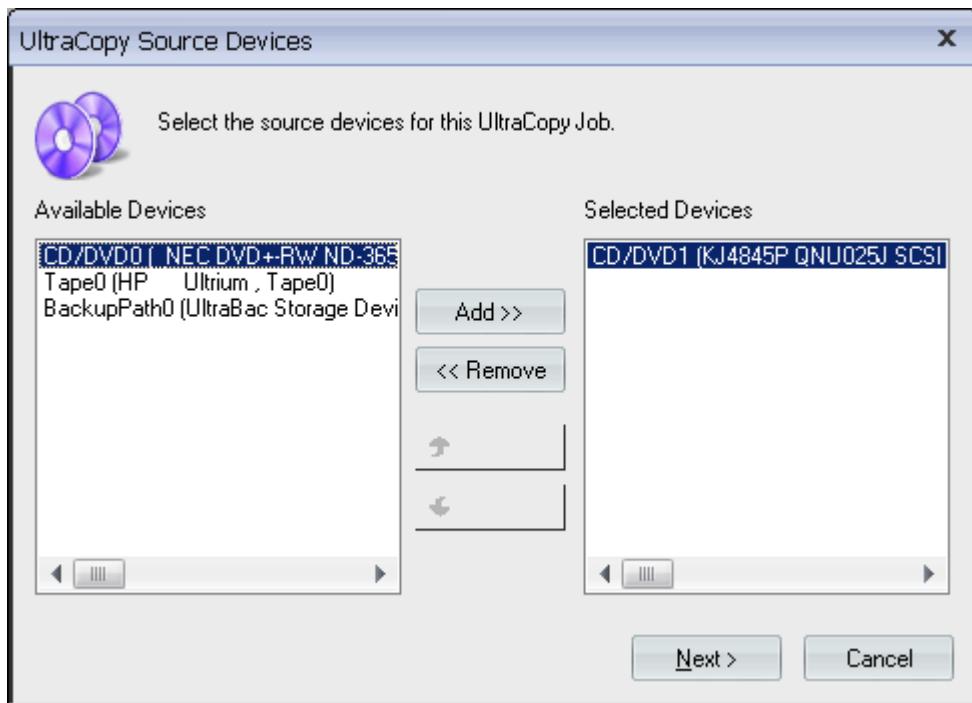
Fig. 1 - Selecting the source device.

3. Under "Available Devices," highlight the target device to copy to, and add it to the "Selected Devices" by clicking the "Add>>" button. Click "Next."
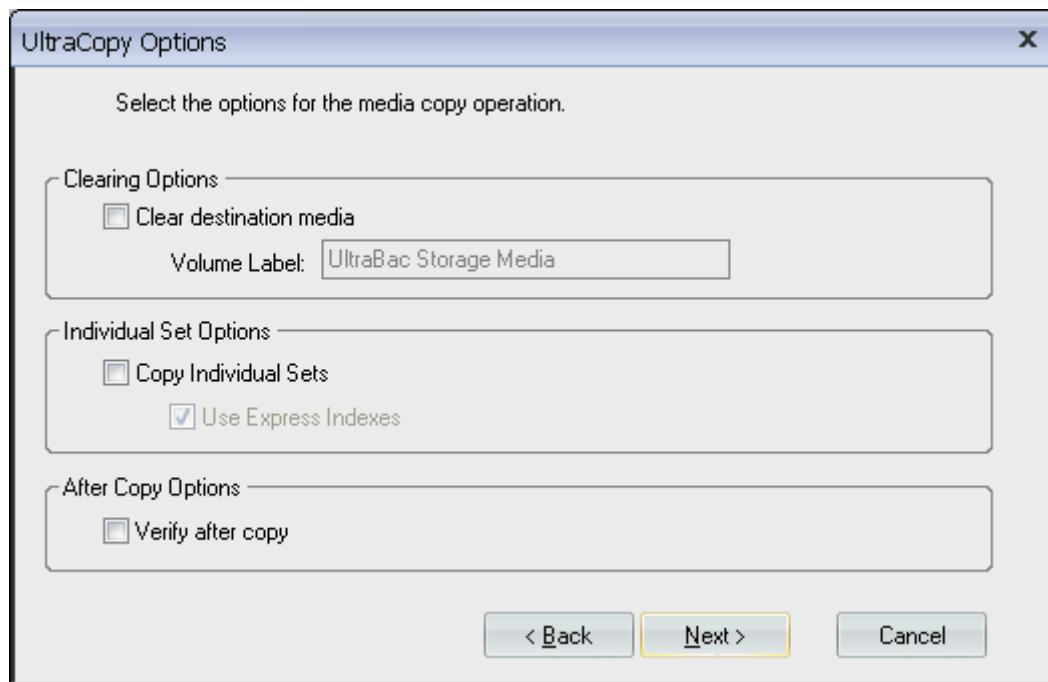
Fig. 2 - UltraCopy options.

4. Set the UltraCopy options to be used during the copy job, and click "Next."
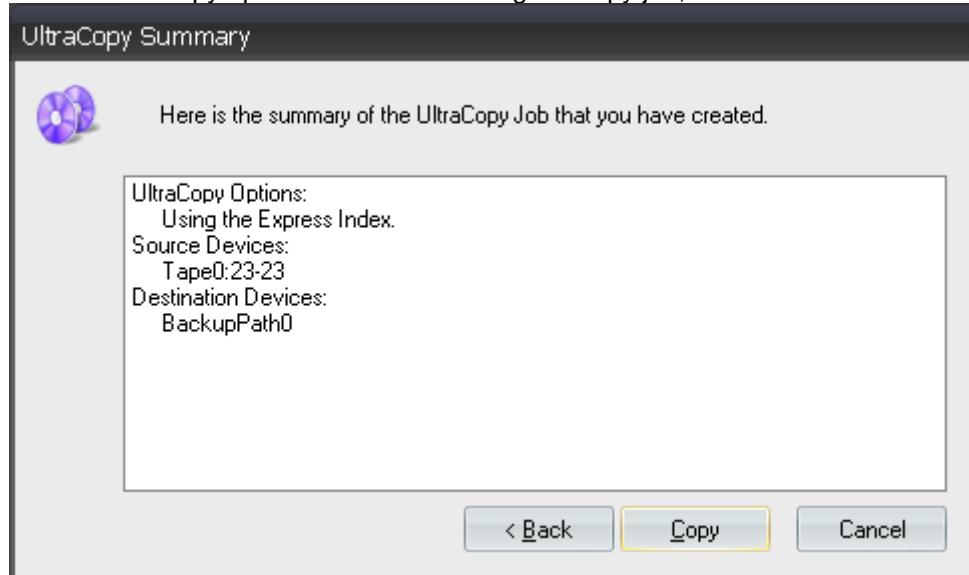
Fig. 3 - UltraCopy job summary.

5. Click "Copy" to begin the copying process.

UltraCopy Options

Clearing Options:
- Clear Destination Media – Clears the contents of the target media before it is used by UltraCopy.
- Volume Label – Specifies a volume label on the cleared media.

Individual Set Options:
- Copy Individual Sets – Allows UltraCopy to select and exclude specific sets from being copied to the destination media. Selecting this option will add a set selection screen to the UltraCopy wizard.
- Use Express Indexes – Uses the Express index for each source device when scanning for sets. When unchecked, the full media is searched for all sets. This process can be time consuming when copying from tape devices, using the Express index is highly recommended.

After Copy Options:
- Verify after copy – Runs a CRC verify operation on the destination media after the copy completes.

Copying Individual Sets

When selected, this option allows the user to only copy specific sets to the destination media.
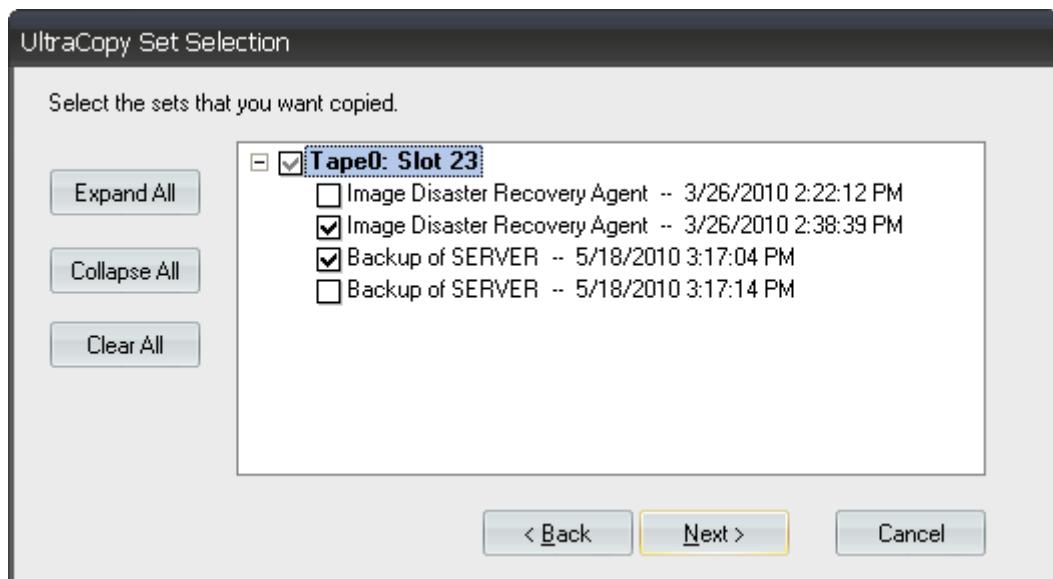
Fig. 4 - Selecting individual sets in UltraCopy.

To select individual sets:
1. Ensure the "Copy Individual Sets" option is selected in the UltraCopy Options screen.
2. Expand the media to be searched for individual sets.
3. Check the box to the left of each set to be copied. Only selected sets will be copied.
4. Click "Next."

Using a Library with UltraCopy

In UltraBac v9.2, media library functionality has been incorporated into UltraCopy. This functionality allows UltraCopy to easily copy data from a spanned volume to a single storage location, or to copy a backup that would require multiple tapes from a path to a range of slots, or to a media pool.

If one of the specified devices is a media library, the library controls will automatically be enabled and allow the selection of any library element that contains media. If the library uses media pools than that can be selected and the pool set in the next screen.
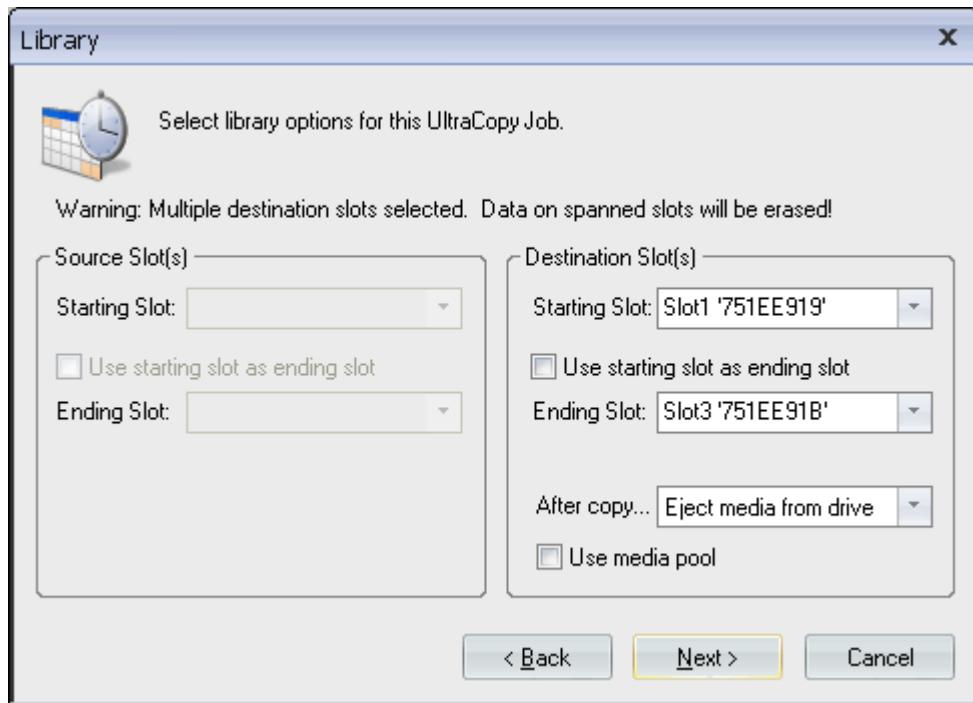
Fig. 5 - Library/Media Pool settings in UltraCopy.

Command Line Options

UltraCopy can be run from the Windows command line, or a .bat file using the following syntax:

UBCopy <source> <destination> [options]

When specifying multiple source devices, separate each device with a comma:

UBCopy tape0,tape1 backuppath0

```
 C:\WINDOWS\system32\cmd.exe                                    _ □ ×

C:\Program Files\UltraBac Software\UltraBac>ubcopy /?

ULTRACOPY Version 9
UltraCopy enables customers to copy backups (or non UltraBac
              media via MirrorCopy) from one device/medium to another.

 USAGE:UBCopy.exe [Source] [Destination] [Commands]

 COMMON COMMANDS:
 Source        The source device(s).  (i.e. BackupPath1)
 Destination   The destination device(s).  (i.e. Tape0)
               NOTE: Type "UBCopy.exe /DeviceFormatHelp" for
               help on how to use multiple devices, autoloaders, and
               the copying of individual sets.

 /AutoResponse:<AutoResponse file> auto respond to messages.
 /DecryptKey:<key>
               The Decryption key for encrypted sets.
               NOTE: All encrypted sets must use the same key.  If any other
               sets that are to be copied use a different key, those sets
               will be skipped over.

 /ListSets:<device>
               Lists the sets on a device via Index or Express Index.

 /DontUseExpressIndex
               Tells UltraCopy to scan the device for indexes instead of using
               the Express Index.  Only valid when copying via individual sets.

 /PrepareMedia  Prepare the destination media first before copying.  Assigns
               the attached label to the device.
               Example: /PrepareMedia:New Label
 /pm           Same as /PrepareMedia.  Example: /pm:New Label

 /MediaPoolDest Use a media pool(s) for the copy.  To use multiple media pools,
               separate them with a comma.
               Example: /MediaPoolDest:Wed_Pool or
                        /MediaPoolDest:Wed_Pool, Fri_Pool
               NOTE: Media pools can only be used as destination devices.

 /Verify       Verify after the copy.
 /V            Same as /Verify.

 /Quiet        Only the start and end time of UltraCopy will be printed
               to the console.  Issues where UltraCopy needs user
               intervention will also be printed.

 /Unattended   Do not prompt the user for additional information or
               assistance through the course of the copy.  Basically set
               it and forget it.

 AUTOLOADER COMMANDS:
 /EjectToMailSlot
               When we are done with a tape, it will be ejected to
               the first empty mailbox slot.
 /EjectFromDrive
               After we use a tape, it will be ejected from the
               drive and placed back into its previous slot.
 /RewindMedia
               After we use a tape, we will simply rewind it.
               This is the default

 MEDIA POOL COMMANDS:
 /Append       Start off by appending to the last used media.
 /New          Start off with a new or expired tape.
 /UseCurrent   Use the media that is currently in the drive.

 ENCRYPTION COMMANDS:
 /AESKey:<key>          AES Key.
 /AESPhrase:<phrase>    AES Phrase.  Must Specify AESEncryptStr to use.
 /AESEncryptStr:<0\128\192\256> The Strength of the AES Phrase.
```

Fig. 6 - UltraCopy command line switches.

Media Library Controls

Both locally attached and remote media libraries can be controlled through the UltraBac user interface with the use of the UltraBac Media Library Controls. UltraBac can use a media library in three different ways:

- Sequential mode – Media is moved by the library as the backup spans from one to the next. The library must be set to "sequential mode," and the UltraBac Media Library Controls will not be usable.
- Slot based backups – A slot range is specified for use in each scheduled group. The media library must be set to "random mode," and the UltraBac Medium Changer device driver must be loaded.
- Media pools – A pool of media is created in UltraBac and specified for use in each scheduled group. The media library must have barcode support, and the UltraBac Medium Changer device driver must be loaded.

Setup and Configuration

To use the UltraBac Media Library Module, the UltraBac Medium Changer device driver must be installed on the system hosting the autoloader.

To install the UltraBac Medium Changer device driver on a
Windows 2000/XP/2003/Vista/Windows 7/2008/2008 R2 system:

1. Open the Windows Device Manager.
2. Expand the "Medium Changers" component appearing on the right side of the screen.
3. Right click the existing device and select "Properties."
4. Select the Drivers tab.
5. Click "Update Driver."
6. Click "Next."
7. Select "Display a list of the known drivers for this device so that I can choose a specific driver" and click "Next."
8. Click "Have Disk."
9. Browse to the location of the "mchgr.inf" file (by default in "C:\Program Files\UltraBac Software\UltraBac\Drivers\Win2k"), and click "Open."
10. At the "Select a Device Driver" screen, highlight the "UltraBac Medium Changer Device" and click "Next."
11. Click "Yes," then click "Next" again.
12. Click "Finish."

NOTE: For more information on installing the UltraBac Medium Changer driver, please see the UltraBac Knowledge Base:

See UBQ000150: Installing the Optional Medium Changer Driver (Autoloader) in Windows 2008

Library Configuration

The Library Configuration tool can be used to map the drive layout of the libraries attached to a backup host.
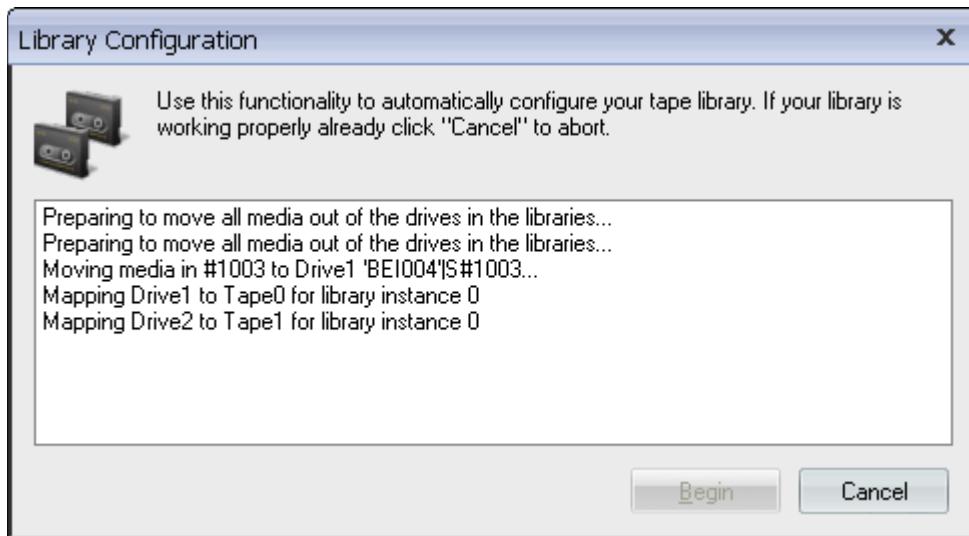
Fig. 1 - Library Configuration tool.

To use the Library Configuration tool:
1. Select the Manage tab, and click "Library"/"Configure Library."
2. Click "Begin" to run the configuration process.
3. Click "OK" when the configuration is complete.

Moving Media

To access the media library, select the Manage tab and click "Library"/"Control Library." The Library Control selection is only available if the tape device is selected as the current storage device. To select the tape drive as the current storage device:

1. Select the Manage tab, and click "Storage Devices"/"Tape."
2. Click on the autoloader's tape device to select the device.
3. Click "Close."

Fig. 2 - Media library controls.

From the above screen, drag and drop tapes into the drive, or right click on an object and move the tape to its destination by choosing a slot or tape drive number.

Right click menus:
- Move to Slot – Move the media from the selected element to the specified available slot.
- Move to Drive – Move the media from the selected element to the specified available drive.
- Move to Mailbox – Move the media from the selected element to the specified available mailbox. This option is only available on libraries that have mailbox slots.
- Move to... – Opens a control screen allowing the selection of the source and destination elements/locations.
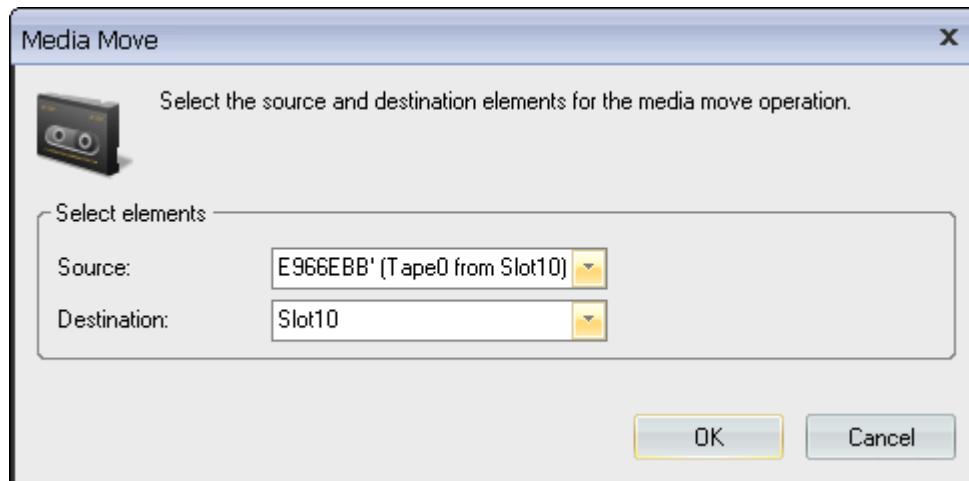
Fig. 3 - Media Move options.

- Media Pool – This option allows media to be added to any available media pools, create new pools, or to manage existing pools.

UltraBac also supports the administration of remote media libraries:

- To control a remote library, the "UltraBac Tape Library Control" and the UltraBac Medium Changer device driver must be installed on the system hosting the library.
- To manually manipulate media in the remote library, use the "Connect" feature to control the library host system, and use the control methods above.
- To use a remote media library for a scheduled backup, create a "Remote" device, select the device as the default, and set the "Remote" device as the first backup storage device under "Use devices in this order."

Configuring Media Pools

Media pooling has been implemented to allow better organization and automation of library backups, as compared to "slot based" backups, or using a media library in "sequential mode." Some benefits of using media pools include space savings on tape, automatic inventory of bar codes, lower-level administration, and more in-depth logging information. To use media pools, the tape library must have barcode support, and only media that has a readable barcode can be used.

Media pools are created through the media library controls:

1. Right click on a tape with a barcode listed.
2. Click "Media Pool"/"Other."
3. In the Media pool name field, type a <name> for the Media Pool.

4. Click "Assign."
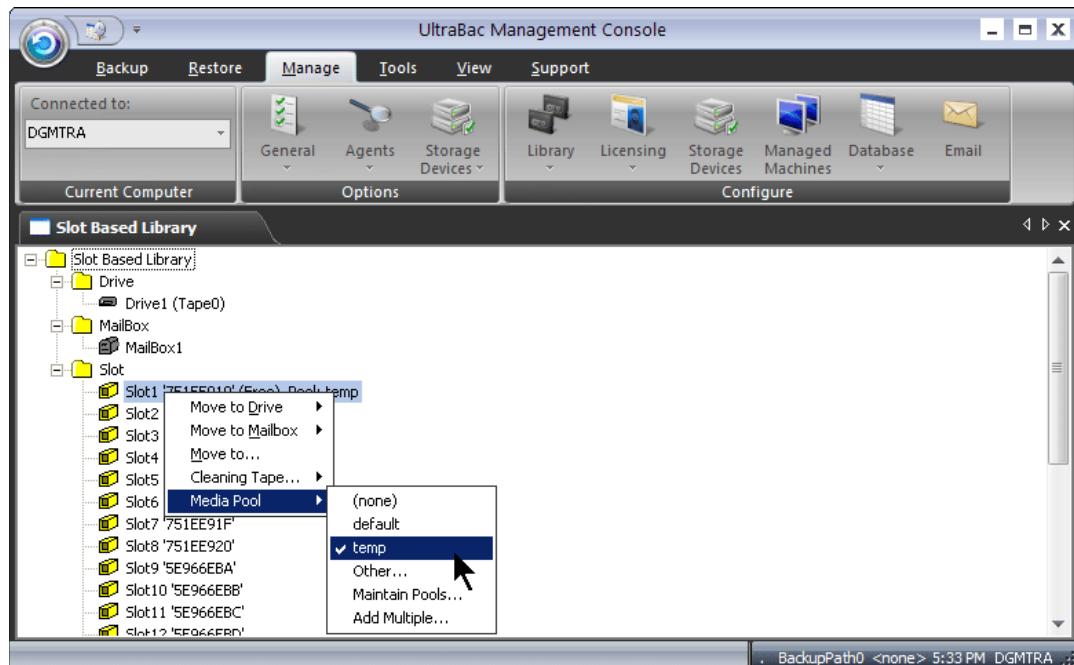
Fig. 4 - Media Pools in the Autoloader Library controls.

Next to the barcode number, the assigned media pool name will appear:
   "Pool: <Media Pool Name>"

Any available barcode can be added to the media pool by right clicking on the barcode number and assigning the desired pool. To add multiple barcode tapes to the media pool:

1. Right click on a tape with a barcode listed.
2. Click "Media Pool"/"Add Multiple."

Other Media Pool Right Click options:
*   (none) – Remove the specified barcode from the media pool.
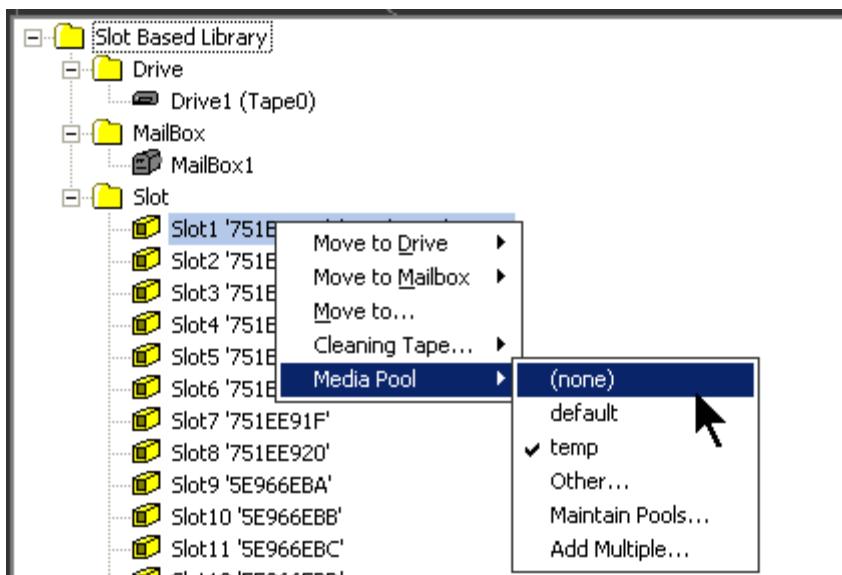
Fig. 5 - Media pool options.

- default – Adds the selected media to the default media pool.
- Other... – Opens a dialog that allows a new media pool name to be specified.
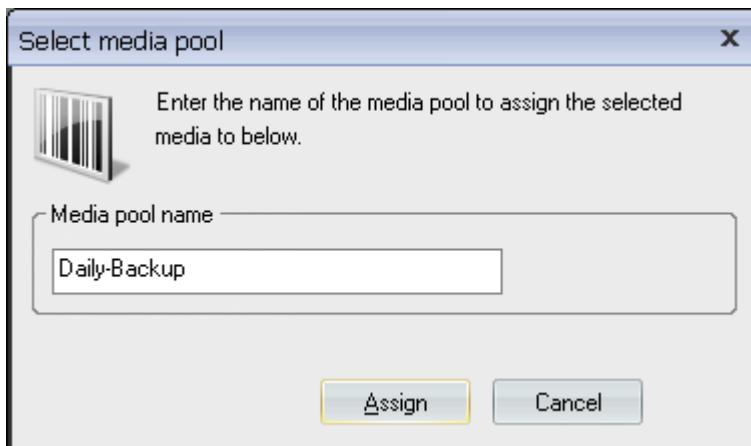
Fig. 6 - Specifying the media pool name.

- Maintain Pools... – Opens the "Media Pools" maintenance screen.
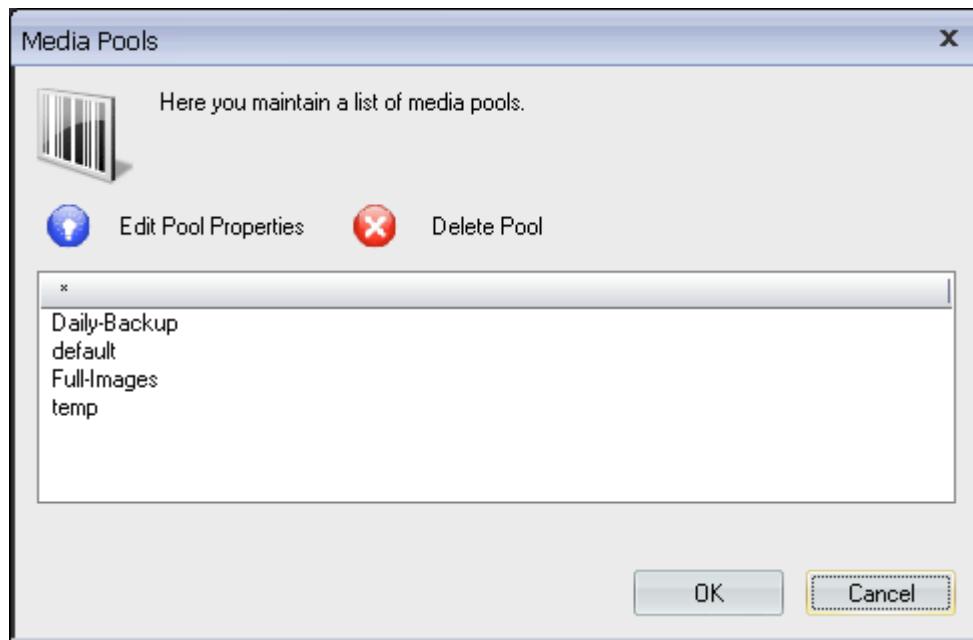
Fig. 7 - Media pool management.

- Add Multiple... – Opens a screen that allows multiple tapes to be added to a media pool.
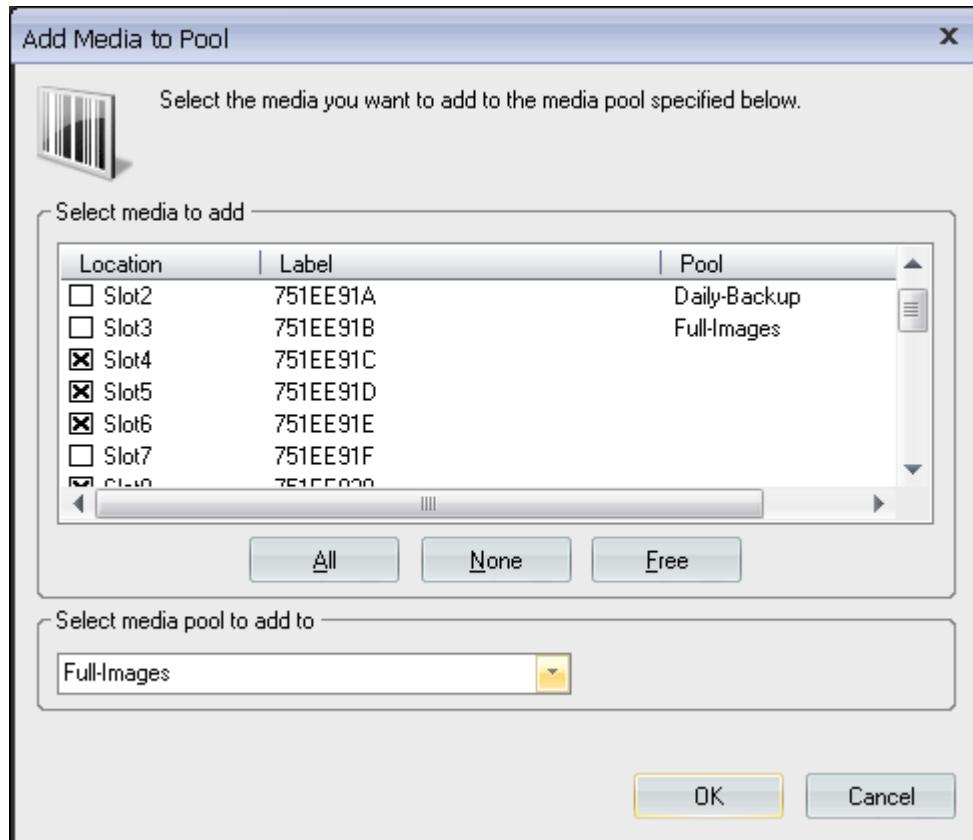
Fig. 8 - Adding multiple barcodes to a media pool.

Using the Library in a Scheduled Backup

NOTE: For instructions on creating a Scheduled Backup group, please visit the "**Scheduled Backup Creation**" section of the User Manual:

UltraBac User Manual: Scheduled Backup Creation

Sequential Mode

When using an autoloader in "sequential mode," the autoloader will appear to UltraBac as a stand-alone tape device. Before backing up, a tape must be put into the drive. If the autoloader is set to run in "sequential mode," all autoloader control functionality in UltraBac is disabled.

NOTE: "Sequential mode" is a setting usually available through a configuration/control screen on the autoloader. Please refer to the manufacturer's documentation for more information on this setting.

Slot Based Backup

This option allows a range of autoloader slots to be specified for use in a scheduled backup group. If the amount of data backed up is larger than the capacity of the slot range, the backup will abort when it reaches the end of the tape.

The slot range is specified during the creation of a scheduled group in the Scheduled Backup Wizard.

NOTE: This setting will only be available if an autoloader tape device is specified as the first device to use, under "Use devices in this order," during a scheduled backup.

To view the media library settings of a group:
1. Select the Tools tab, and click "View Events."
2. Double click the backup job to be viewed.
3. Select the Library tab.
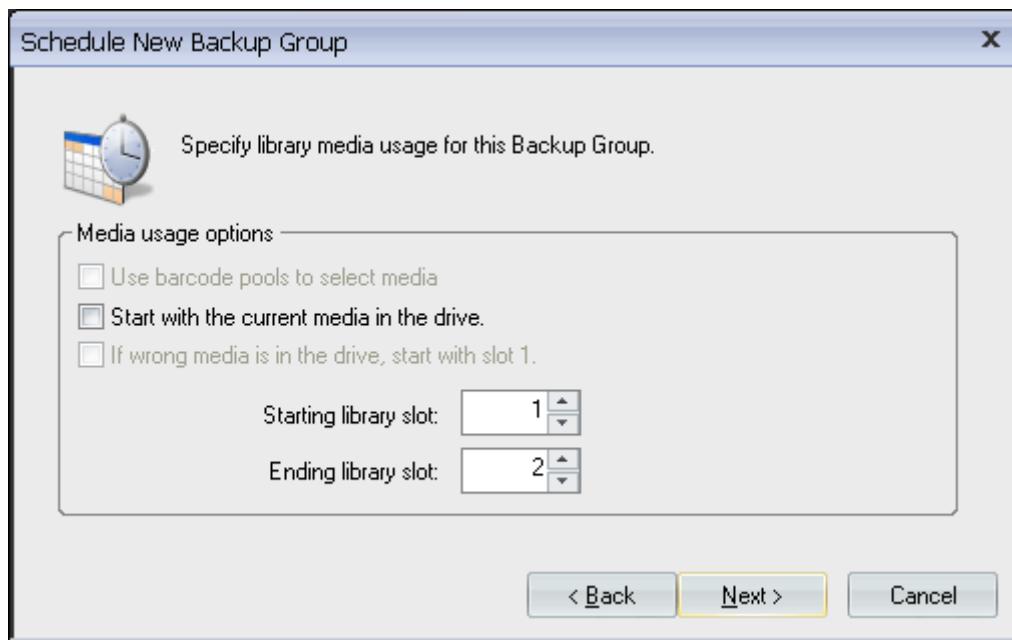
Fig. 9 - Library tab in the properties of a scheduled backup group.

Media Pools

Media pools are assigned to each backup through the Scheduled Backup Wizard, or through the scheduled backup's properties. If the amount of data backed up exceeds the tape space provided in the media pool, a secondary, or spillover, media pool can be defined.

NOTE: This setting will only be available if a media library tape device is specified as the device to use during backup. Failover support to a non-media pool device (BackupPath, stand-alone tape drive) is NOT supported.

To view the media pool settings of a scheduled backup:

1. Select the Tools tab, and click "View Events."
2. Double click the backup job to be viewed.
3. Select the Media Pools tab.
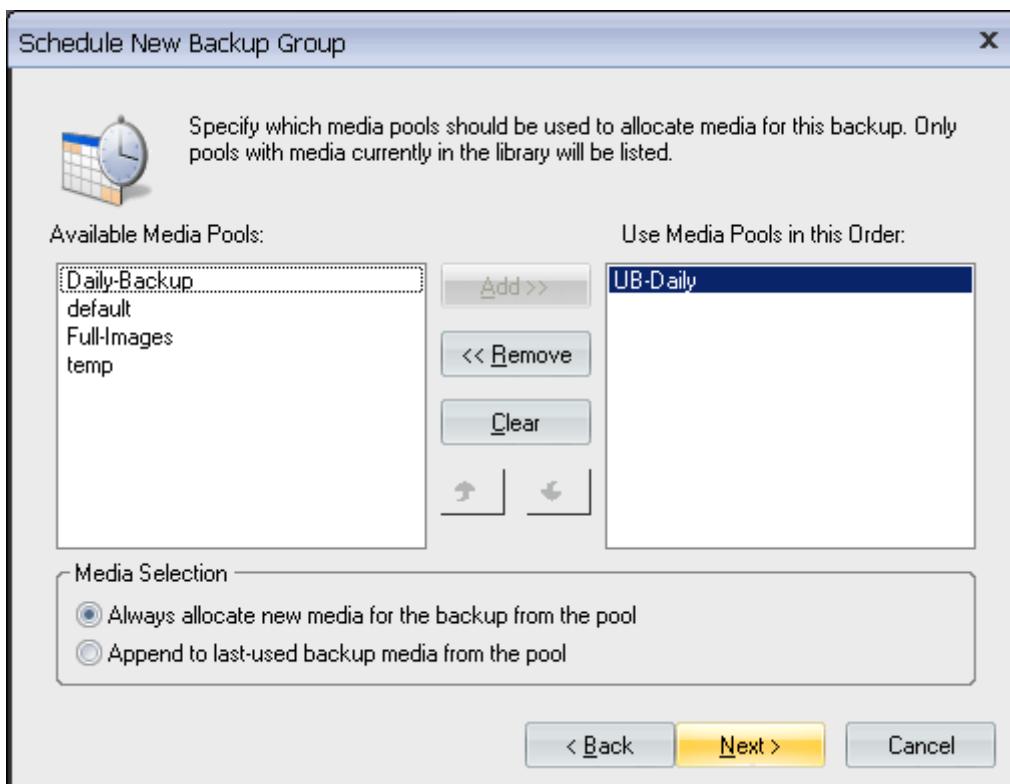
Fig. 10 - Media Pool tab in the properties of a scheduled backup group.

UltraBac will use the blank media in the pool first, then the expired media, protecting the media for five days (the default setting defined in the Manage tab, under "General"/"Media Options"). During the protection period, UltraBac will not be able to overwrite the tapes.

When the protection period has ended, the media will appear as "expired" in the library controls, making the media available for backup rotation. If the protection period has been disabled, UltraBac protects the barcode media automatically for one day.

Media Pool Options

These options define the way UltraBac selects the first tape from the media pool for use during backup:

- Always allocate new media for the backup from the pool – Use the first expired tape in the pool when starting the backup.
- Append to last-used backup media from the pool – Append the backup to the most recently used tape in the media pool.

NOTE: Ad hoc backups cannot use protected media pool tapes, and "Clear storage media" is disabled to eliminate the possibility of overwriting data.

NOTE: For information on removing Media Pools from UltraBac, please see the UltraBac Knowledge Base:

See UBQ000242: Removing Media Pools

Enabling Automatic Cleaning

UltraBac has the ability to automatically schedule a cleaning operation on a cleaning tape in a barcode enabled library.

To specify a tape in the library as a cleaning tape:

1. Select the Manage tab, and click "Library"/"Autoclean Library."
2. Right click on the slot containing the cleaning tape.

Fig. 11 - Specifying a cleaning tape.

3. Select "Cleaning Tape" from the menu options.

To enable library AutoClean options:

1. Select the Manage tab, and click "Library"/"Autoclean Library."
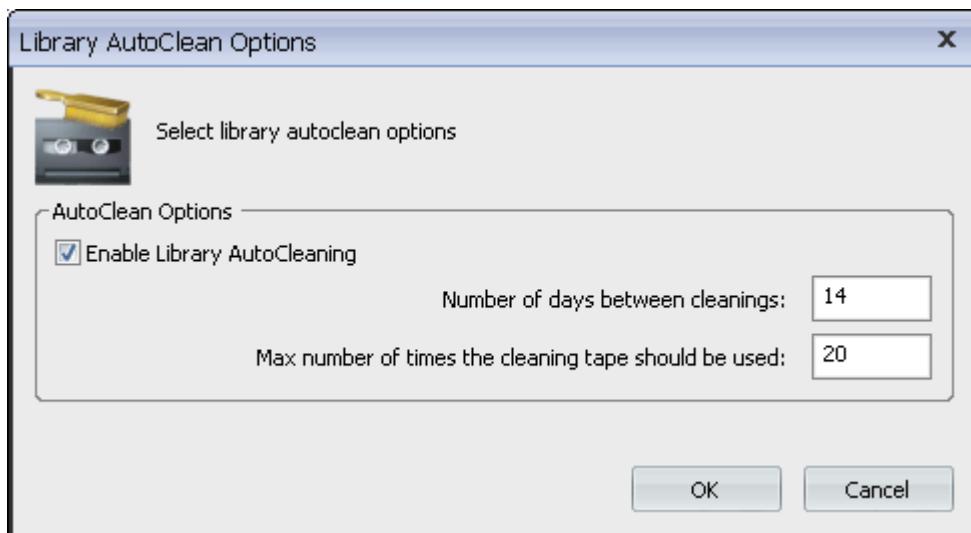
Fig. 12 - Setting the AutoClean options.

2. Check "Enable Library AutoCleaning."
3. Specify the number of days between cleanings as recommended by the manufacturer of the library.
4. Specify the maximum number of times the cleaning tape should be used as recommended by the manufacturer of the cleaning media.
5. Click "OK" to save the settings.

UltraBac Database

UltraBac has the ability to add backup indexes, sets, groups, and logs to several types of database:

Microsoft SQL Server (2008, 2005, and 2000)
Microsoft SQL Server 2008 Express
Microsoft SQL Server 2005 Express
MySQL 5.1

NOTE: For information on configuring the SQL server prior to setting up the UltraBac Database, please see the UltraBac Knowledge Base:

See UBQ000253: Configuring SQL for use with the UltraBac Database

---

Setting up the UltraBac Database

To set up the UltraBac Database:

1. From the Start Menu, click "All Programs"/"UltraBac Software"/"UltraBac Database Setup."
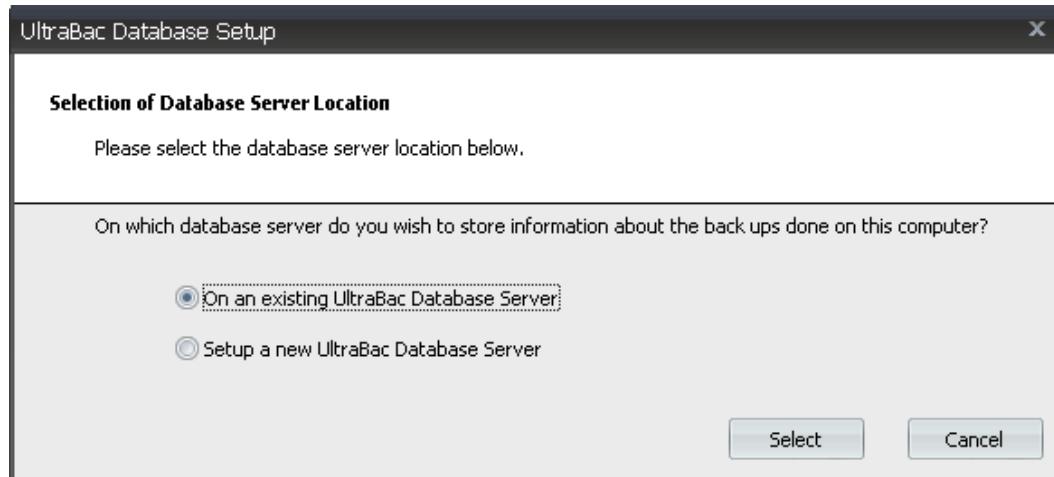
Fig. 1 - UltraBac Database Setup.

2. Select "Setup a new UltraBac Database Server," and click "Select."
3. Select the SQL platform to host the UltraBac Database.
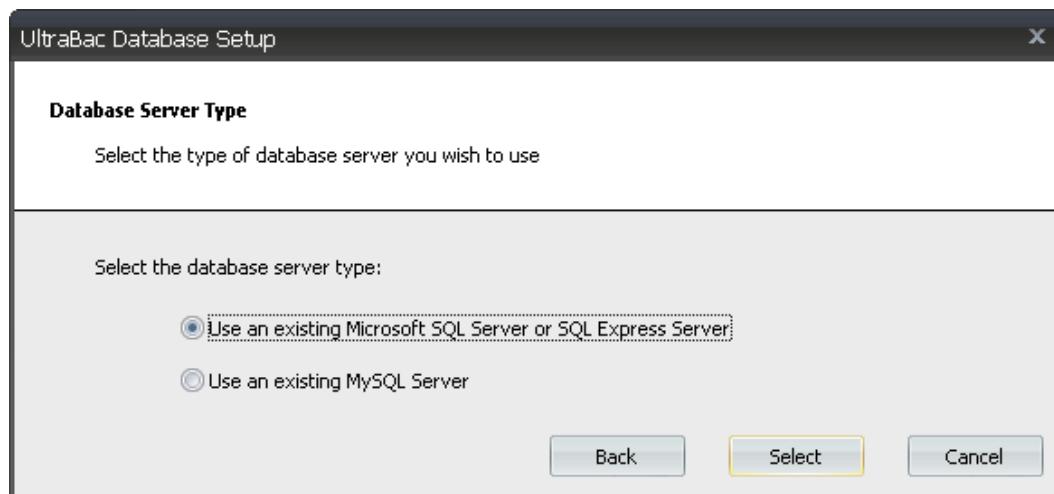
Fig. 2 - Selecting the database platform.

4. Type or browse to the name of the SQL host.
5. Enter the Instance name, if one exists. If not, leave the "Instance Name" empty.
6. Enter the name of a native SQL account (i.e. the "SA" account) that UltraBac will use to create the database.
7. Enter the corresponding password.
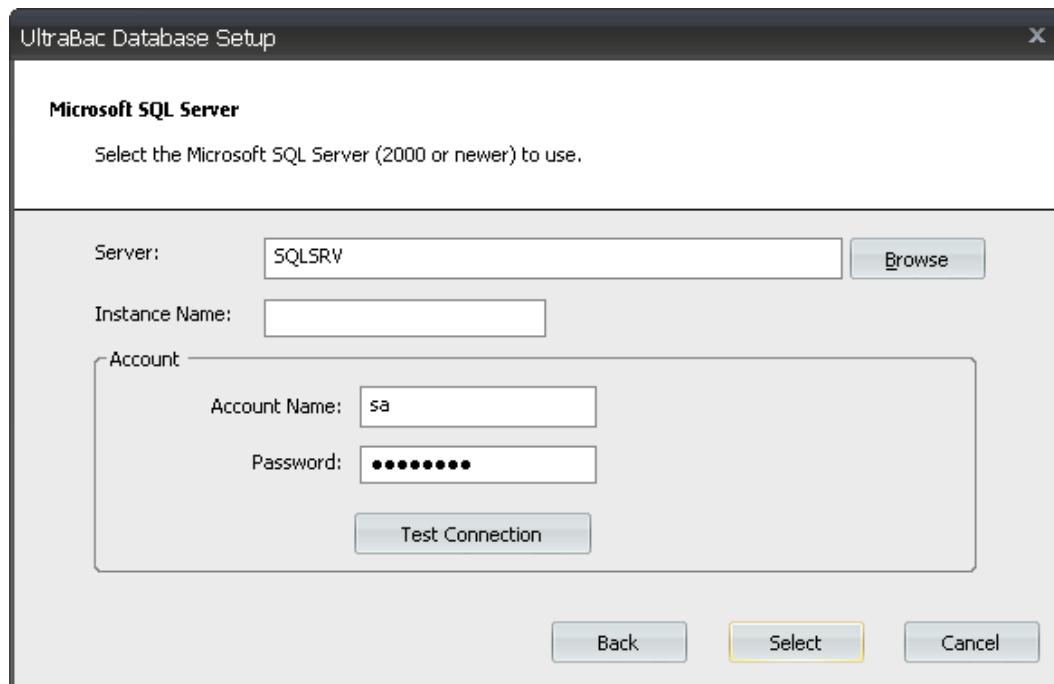
Fig. 3 - Specifying the Microsoft SQL server.

8. Click "Test Connection" to ensure that the specified account has permission to create the UltraBac database.
9. Click Select
10. Enter the account UltraBac will use for connection to the database and click "OK." If the specified account does not exist, UltraBac will create it.
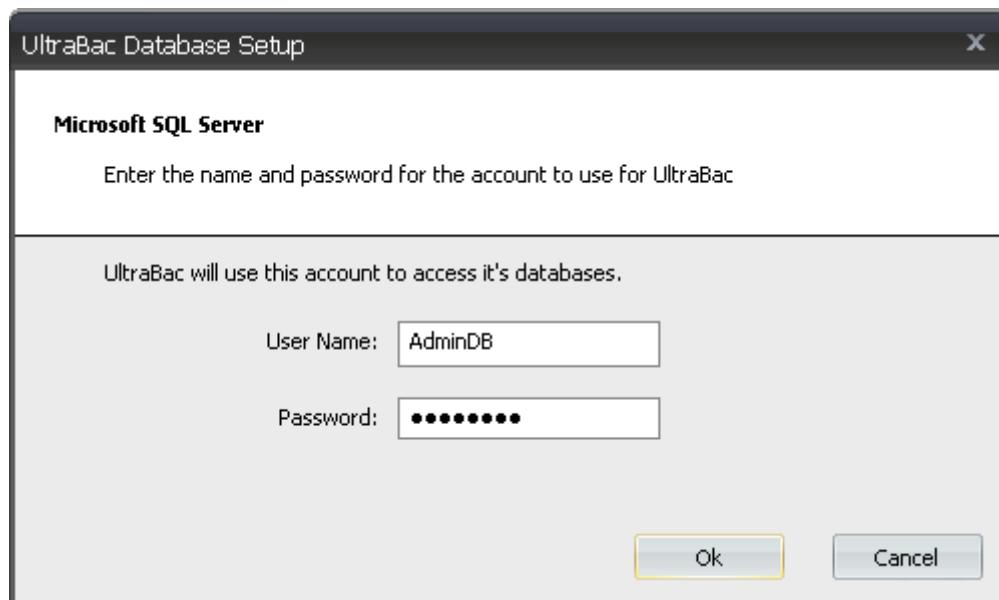
Fig. 4 - Entering the database administration account.

11. Enter the path where the UltraBac databases will be stored. 15 GB free space is required for installation.
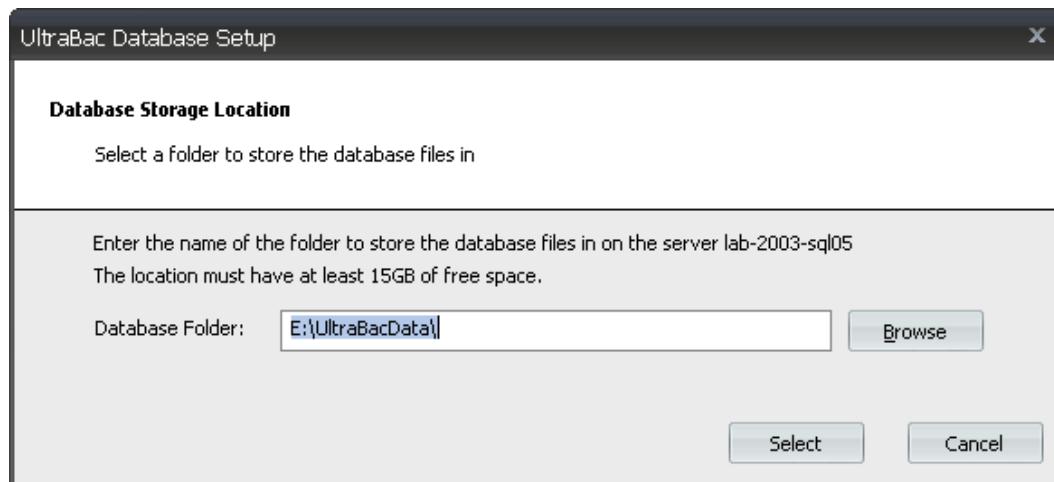
Fig. 5 - Setting the database location.

12. Click "Select" to create the UltraBac databases.

Backup and Restore Basics

Backup Set Basics

A scheduled backup consists of two UltraBac file types:

- Backup Sets – Backup sets define the files, folders, or data to be backed up, and have a ".ub" file extension.
- Backup Groups – Backup groups are used to run one or more backup sets as a part of a backup job. They define time, date, storage devices, and other options. Backup groups have a ".ubb" file extension.

By default, these files are saved in the in the "C:\Program Files\UltraBac Software\UltraBac\Data" directory. Before any backup groups can be created, one or more backup sets must be created.

Creating Backup Sets

UltraBac uses the Backup Wizard to create all backup sets. To access the Wizard, select the Backup tab and click "New."

Backup sets for all agents, including Image Disaster Recovery, Exchange, and File-By-File are created using the Backup Wizard.
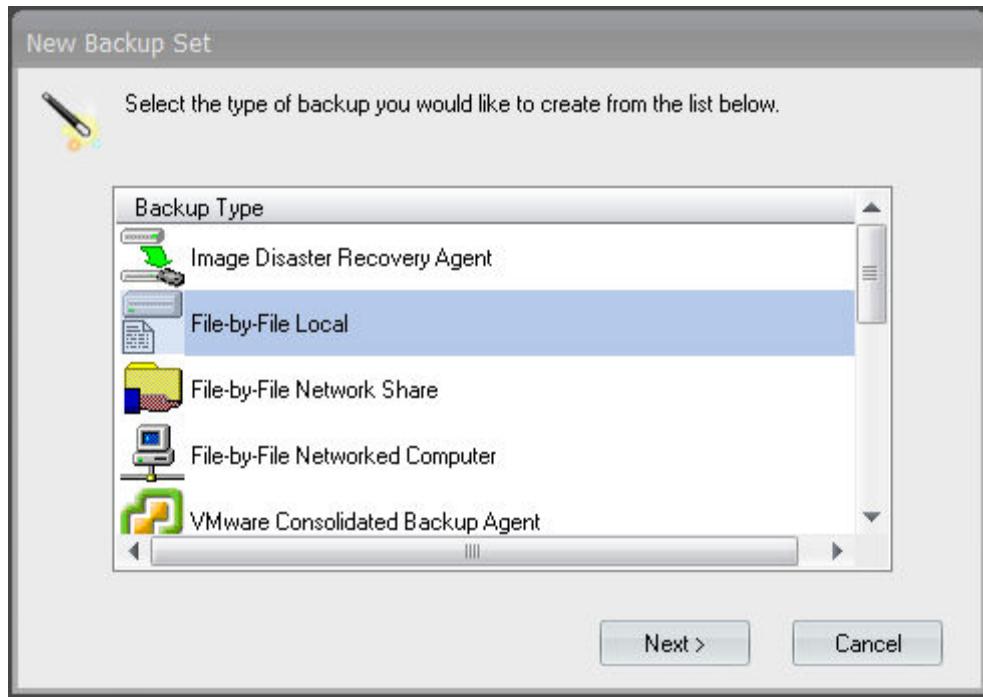
Fig. 1 - Backup Wizard.

After selecting the agent to use in the backup set (in this case the File-by-File Local), and configuring that agent's preferences, UltraBac gives the option of modifying the file selection logic

in the "Selection Criteria" screen before enumerating the set. This is also where the set is given a description that will appear in the backup, verify, and restore logs.
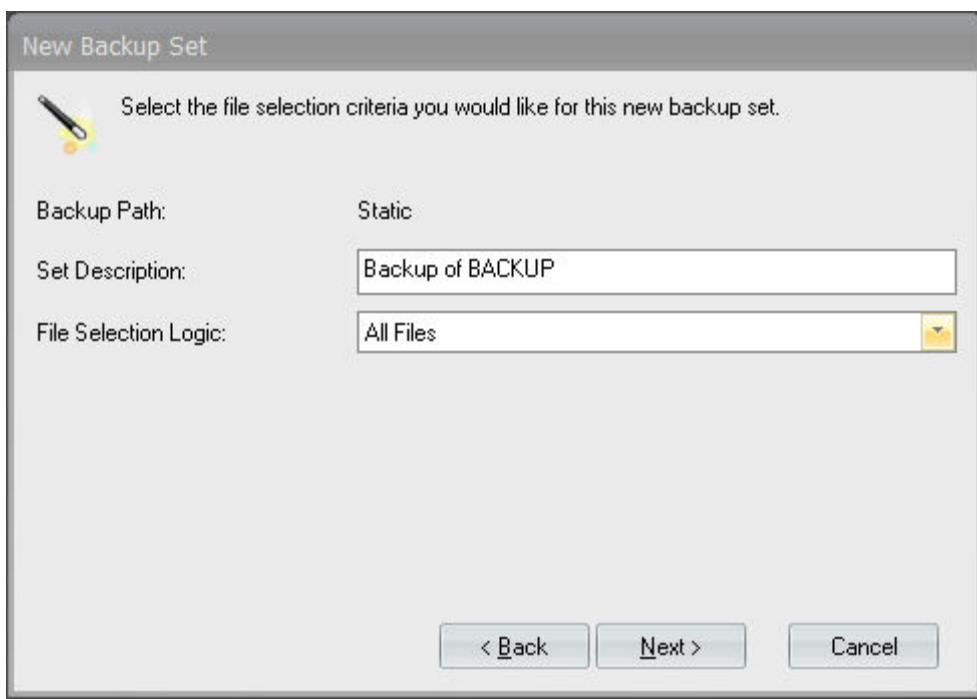
Fig. 2 - Selection criteria.

- Set Description – This is a user-defined field that will appear in the backup log as a description for the set. This field does not affect the file selection logic.
- File Selection Logic – This drop-down list box contains pre-defined options for creating backup sets containing only modified files, or for deselecting all files. The default "All Files" option leaves all files selected.

NOTE: The "File Selection Logic" option DOES NOT affect all agents. The Exchange, Exchange Mailbox, and Image/Disaster Recovery Agents do not support the "Modified Files" selection logic.

After specifying the file selection logic, and entering a description, UltraBac will return a summary of all options selected in the Backup Wizard.
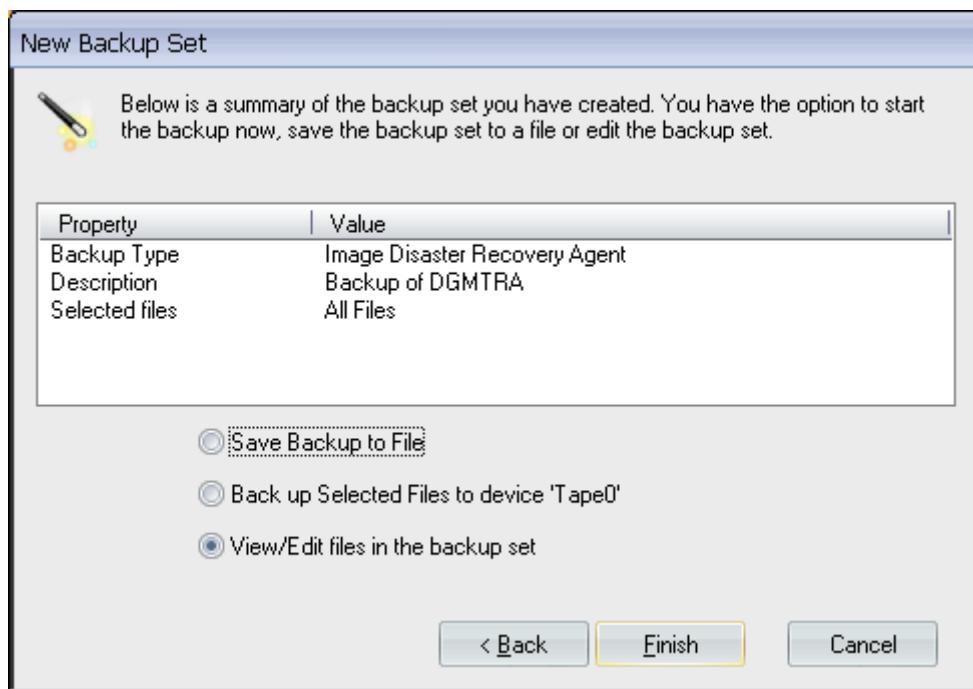
Fig. 3 - Backup Wizard summary.

- Save Backup to File – This option saves the backup set as a ".ub" file in the "C:\Program Files\UltraBac Software\UltraBac\Data" directory.
- Back up Selected Files to device '<backup device>' – This option immediately starts the backup process, using the default backup device.
- View/Edit files in the backup set – This opens the set in the File Viewer, showing all files, directories, and the selected files/data defined in the backup set. This screen is used to select and/or deselect files and data from the backup set.
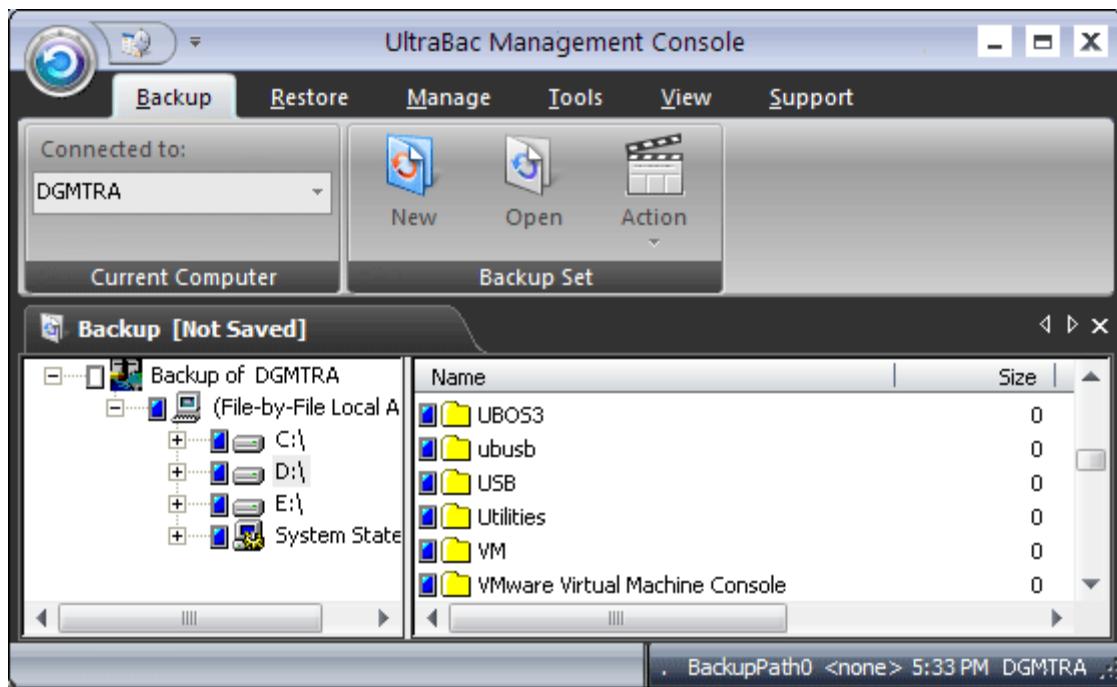
Fig. 4 - Viewing a file-by-file local agent backup set in the File Viewer.

When viewing a backup set, select the files to be backed up by marking the box directly to the left of the desired file/folder/data in blue.

Save the backup set by clicking "Action"/"Save."

Backup Set Properties

When loaded into the File Viewer, each backup set can be modified through the "Set Properties." The Set Properties can include the "Set Description," encryption key settings, or other options. These options can vary, depending on the agent used in the set.

To view the properties of a backup set:

1. Load a backup set into the File Viewer.
2. Click "Action"/"Set Properties."
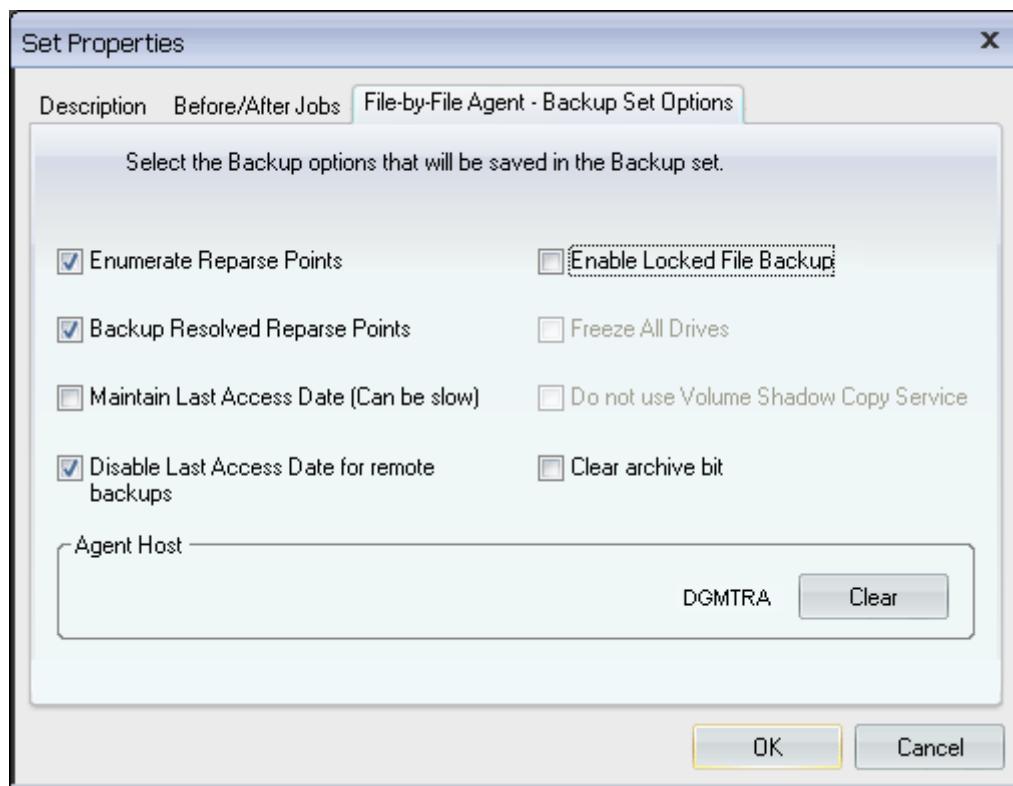
Fig. 5 - File-by-file set properties.

Scheduled Backup Basics

The UltraBac Backup Scheduler is used to create backup jobs consisting of one or more backup sets, to configure those jobs to use a specific device, and run them at a specific time, date, or interval. The scheduled backups can also be configured to send administrative emails, execute batch commands before and after the scheduled jobs, and can be run manually if needed.

Creating the Scheduled Backup

To launch the Scheduled Backup Wizard, select the Tools tab, and click "Backup Group."

1. Type in a description that will appear in the "Scheduler" screen and in the backup log. Click "Next."
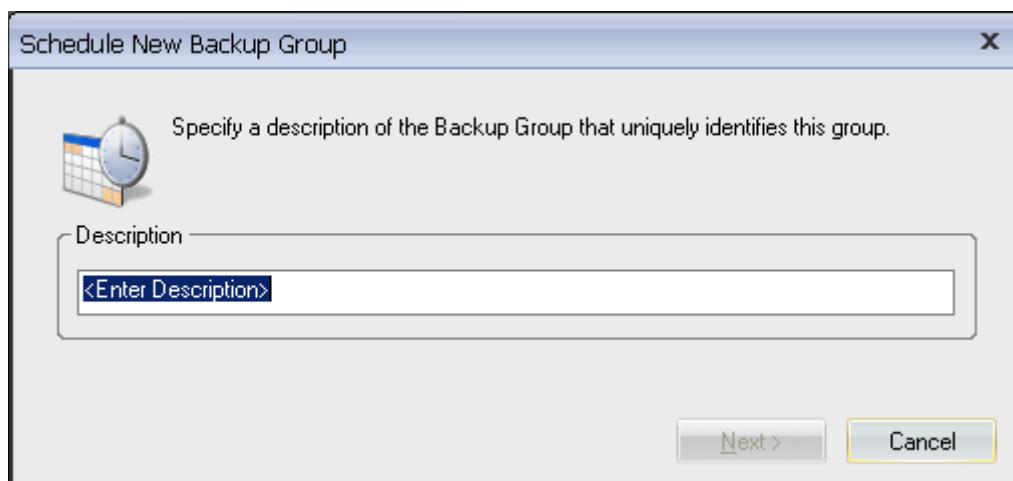
Fig. 1 - Scheduled backup description.

2. Highlight a set in the left column and click "Add" to move it to the right column, adding it to the backup. Sets should be added in the order they are to be run during the job. Click "Next."
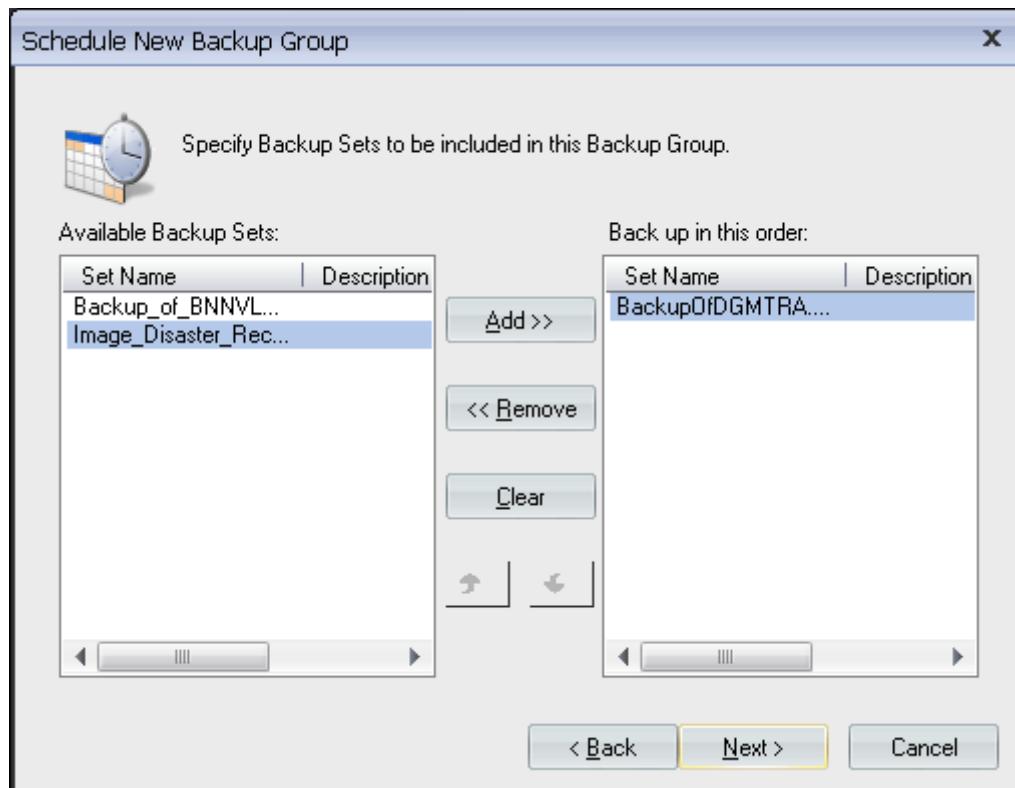
Fig. 2 - Selecting backup sets.

3. Set the Before/During/After backup options, and click "Next."
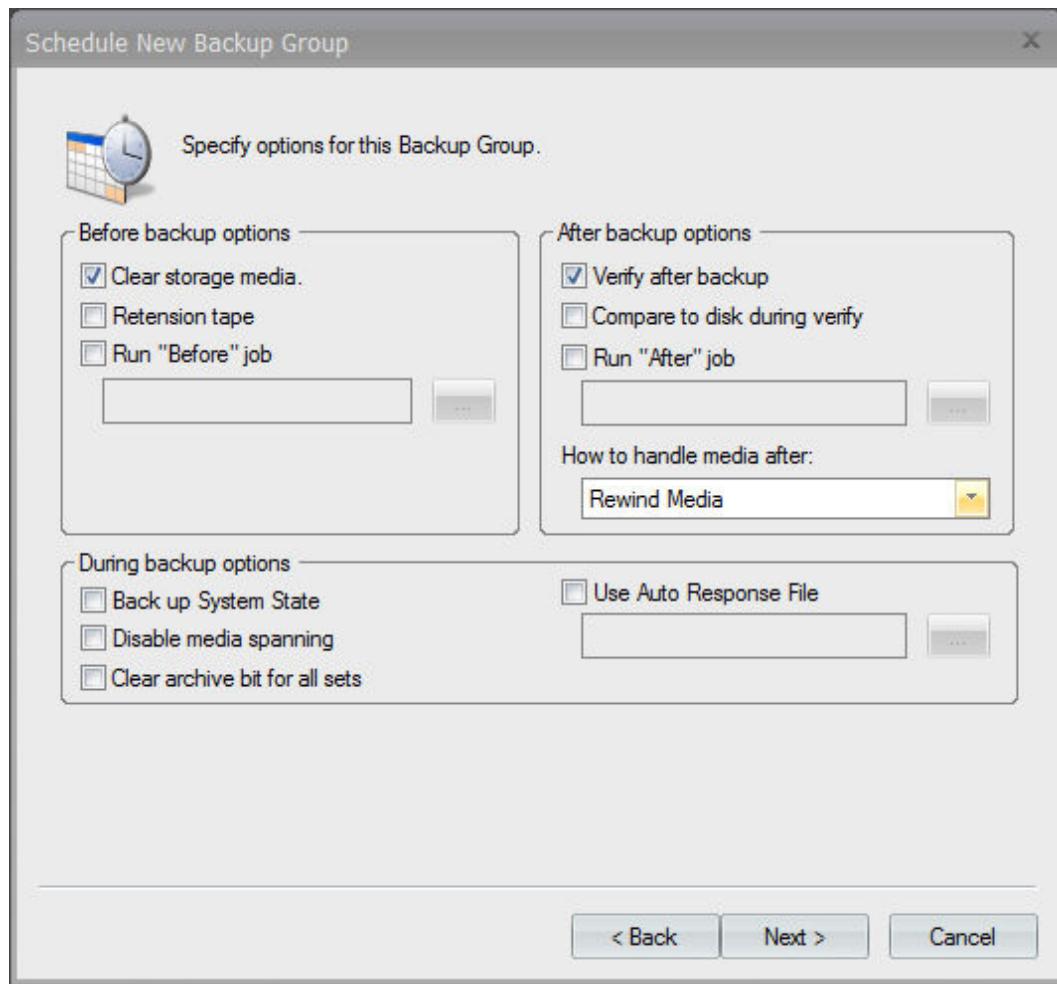
Fig. 3 - Scheduled backup options.

4. Set the notification options, and click "Next."
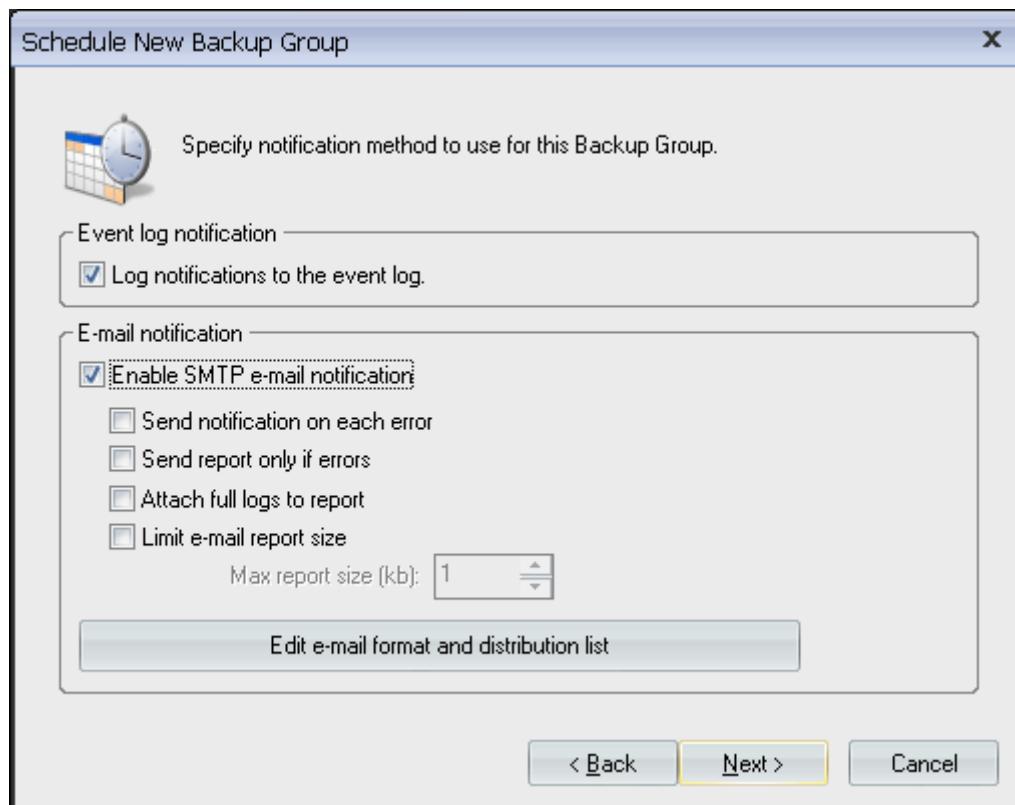
Fig. 4 - Email and event log notification preferences.

5. Highlight a storage device in the left column and click "Add" to move it to the right column, adding it to the backup. Storage devices should be added in the order they are to be used during the job.
6. Set the storage device options, and click "Next."
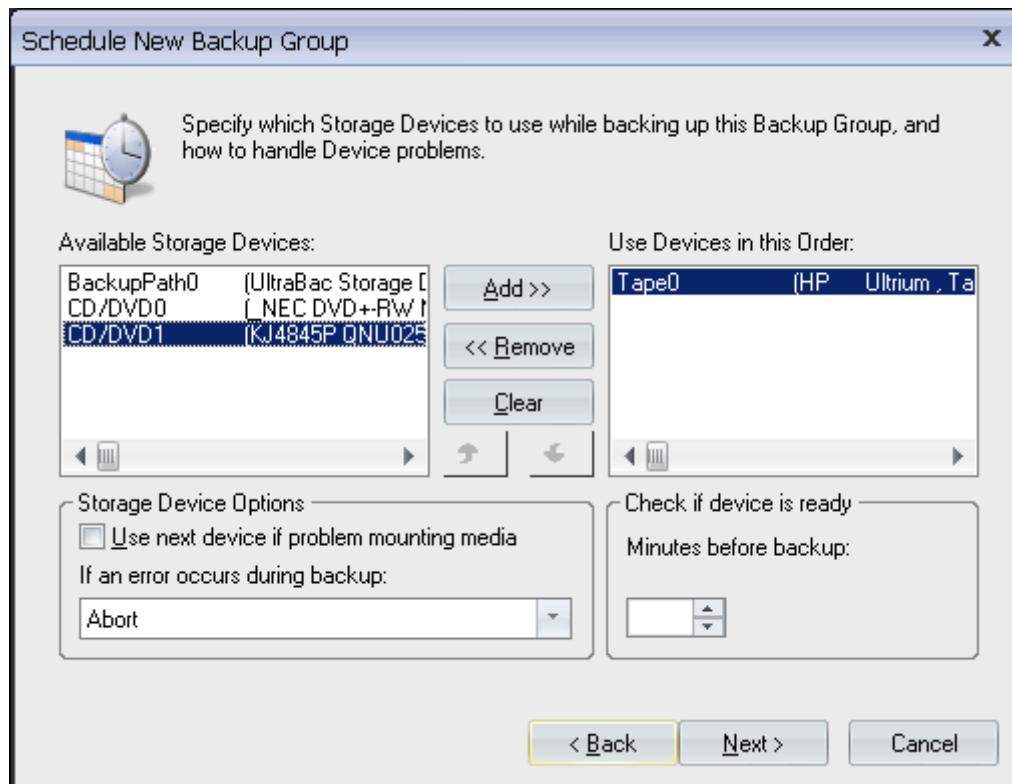
Fig. 5 - Setting the storage device options.

7. Set the options for the Media Library Controls (if applicable), and click "Next."
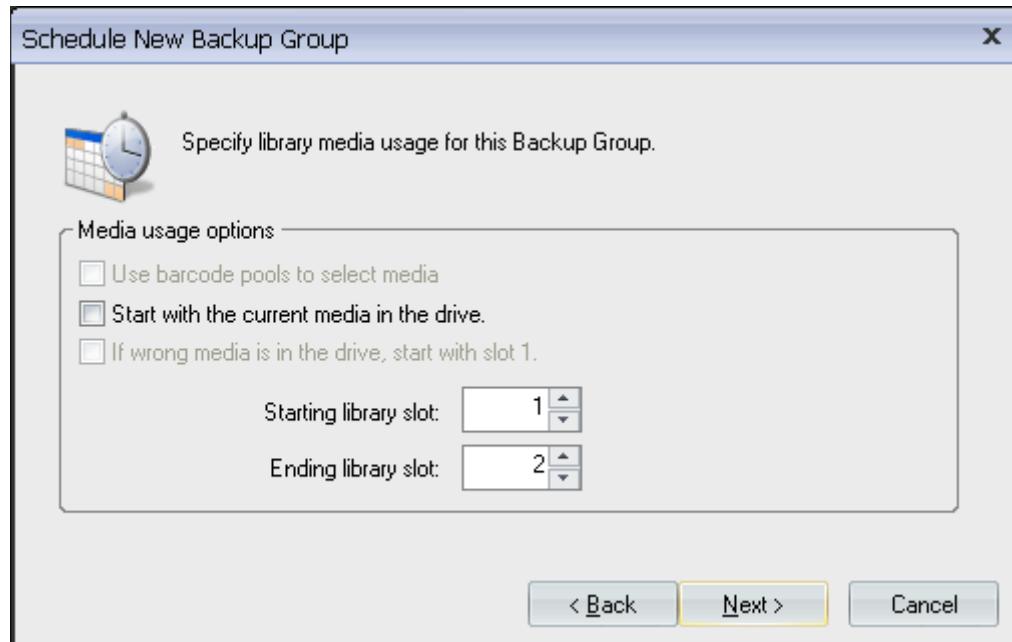
Fig. 6 - Media Library configuration.

8. Set the event time and date options, and click "Next."
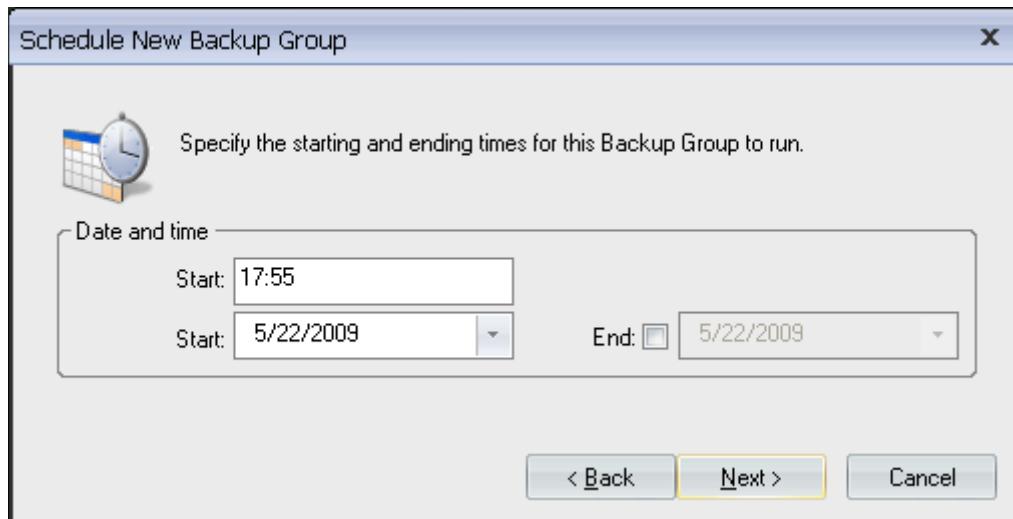
Fig. 7 - Setting the date and time of a scheduled job.

9. Set the frequency/restrictions options, and click "Next."
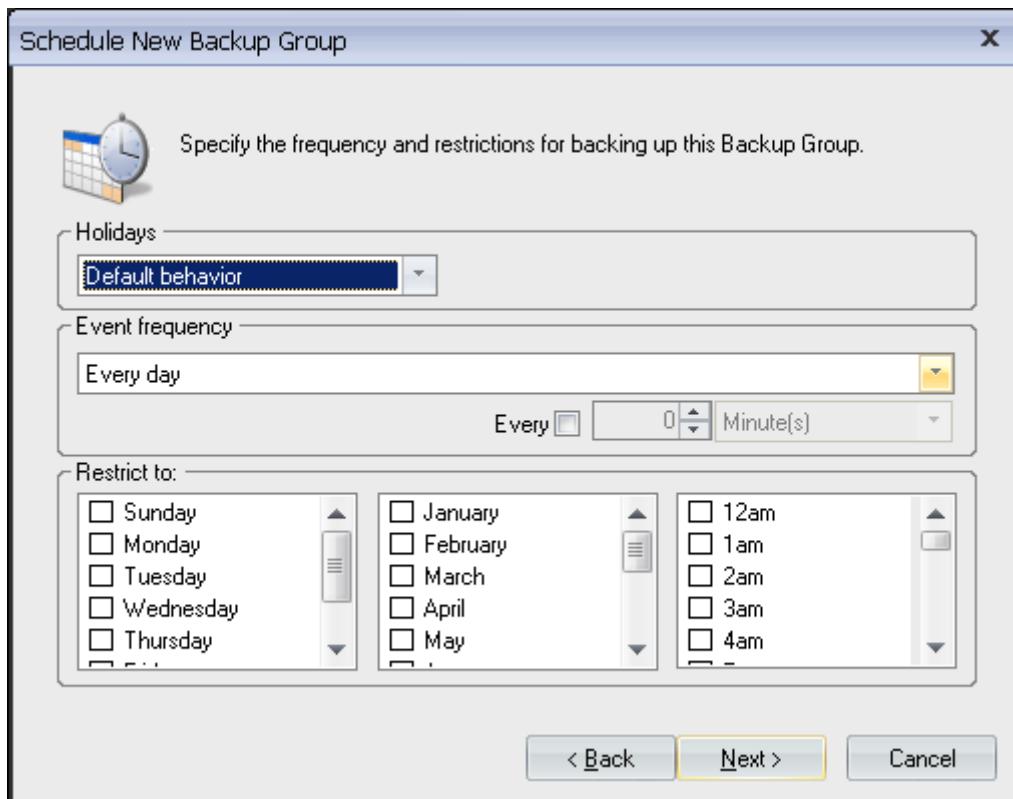
Fig. 8 - Scheduler repeat options.

10. Type in a file name for the scheduled backup, and click "Next."
11. Click "Finish" at the "Summary" screen to enable the scheduled backup.

Deleting a Scheduled Backup

To delete a scheduled backup, it is possible to delete the selected .ubb file from the "Data" directory in the UltraBac install path. It is also possible to delete the scheduled backup in the Scheduler's "Day-at-a-Glance" window:

1. Select the Tools tab and click "View Events," or press "F8."
2. Scroll to the date and time of the job to delete.
3. Right click on the job, and select "Delete."
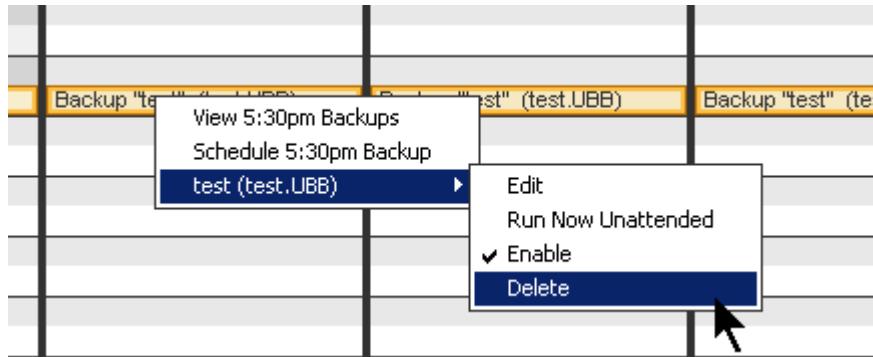
Fig. 9 - Deleting a scheduled backup job.

Scheduled Backup Options

UltraBac can run scripts before and after backup, manage file attributes, and manage the contents and handling of storage media during a scheduled backup.

Backup Options
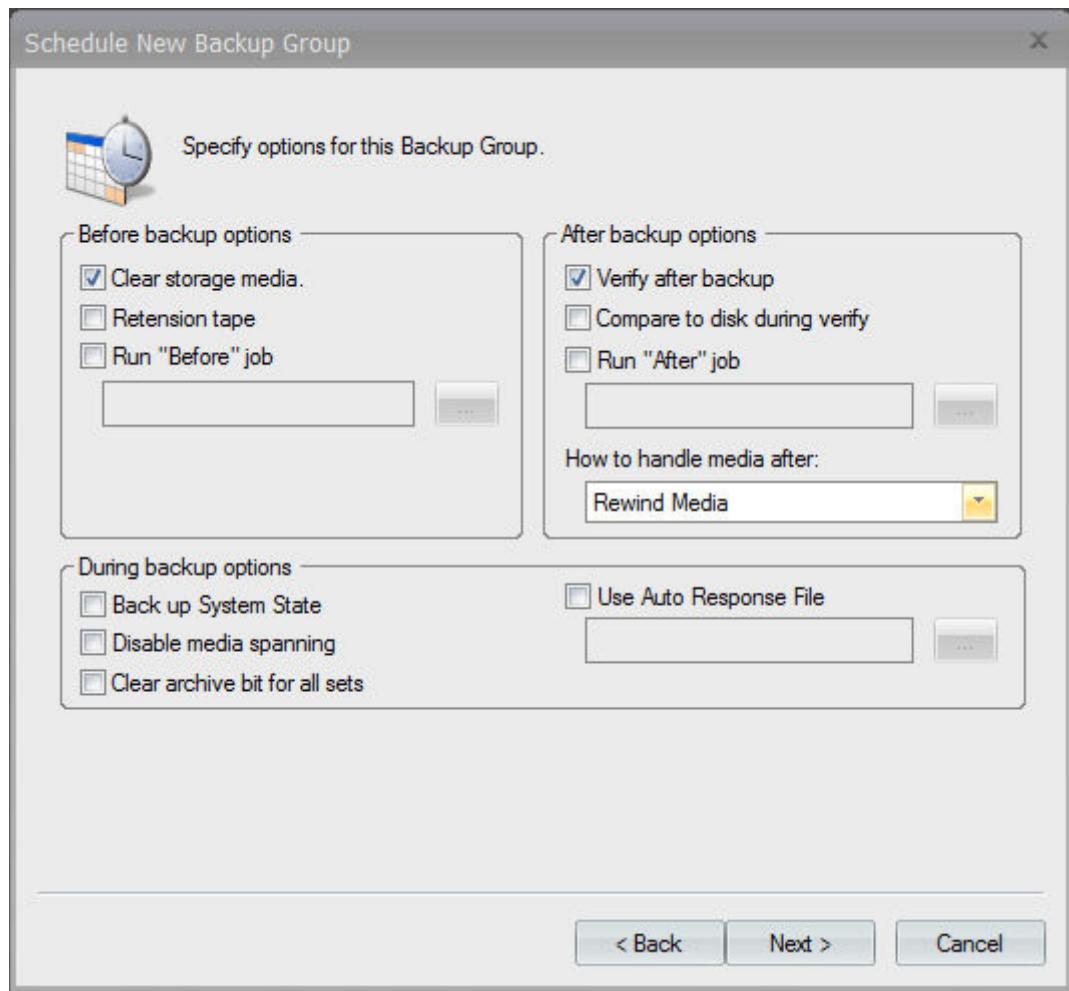
Fig. 1 - Scheduled backup options.

Before backup options:

- Clear storage media – Clear the contents of the currently selected storage media.
- Retention tape – Fast forwards to the end of the tape, then rewinds to remove any slack from the tape.
- Run "Before" job – To execute a script before the backup begins:
    1. Check 'Run "Before" job.'
    2. Type in or browse to a script file (.bat, .exe, .vbs, etc.).

During backup options:

- Back up System State – Global selector instructing all file-by-file backup sets to back up the System State/registry for each Windows NT/2000/XP/2003 system in the job.
- Disable media spanning – Abort the backup when the storage media is full.
- Clear the archive bit for all sets – Clear the "archive bit" file attribute after the file is backed up.

After backup options:

- Verify after backup – Perform a cyclic redundancy check on each file for inconsistencies.
- Compare to disk during verify – Compare the file on the storage media to the file backed up during the CRC check of the data. This option takes longer than the standard verify.
- Media – Media handling options after the backup (and verify, if selected) completes:
  - o Rewind – UltraBac will automatically rewind the media after the job completes.
  - o Eject Media from Drive – Will eject the tape out of the tape drive, if the device supports the function (not supported by all tape drives).
  - o Eject Media To Mailbox – May only be selected with the use of an autoloader containing a built-in mailbox.
- Run "After" job – To execute a script after the backup (and verify, if selected) is complete:

  1. Check 'Run "After" job.'
  2. Type in or browse to a script file (.bat, .exe, .vbs, etc.).

NOTE: It is strongly recommended to perform a Verify operation after backup to check the consistency of the files backed up, and ensure those files can be restored.

Email Notification

UltraBac can relay an email containing backup logs, and can send notifications of backup and verify errors, using a local (to the backup host) SMTP server. Email notification is set up through the "Notification" tab in the properties of a scheduled backup. This can be done during the process of creating a scheduled backup, and the settings can be changed after the job is created. This functionality is not supported on ad-hoc backups.

NOTE: UltraBac's SMTP Email notification only supports local SMTP servers. Servers that are either off-site or separated by a firewall are not supported.

To edit the Notification settings:

1. Open the Properties of a scheduled backup.
2. Select the Notification tab.
3. Click "OK" to save.
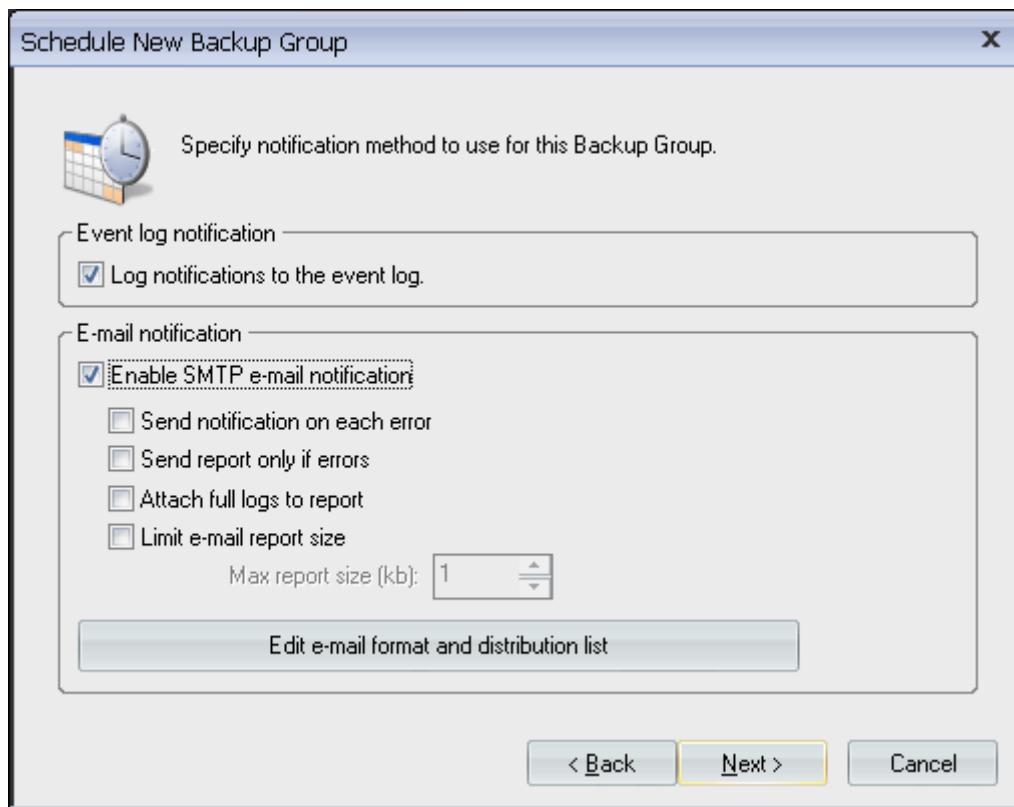
Fig. 2 - Notification tab of the Backup Group properties.

Options

- Log notifications to the Event Log – Write UltraBac events to the Windows Application event log.
- Send notification on each error – UltraBac will send an email for each error encountered in the backup.
- Send report only if errors – If no errors are encountered during the backup, UltraBac will not send email notification.
- Attach full logs to report – UltraBac will attach both the backup and verify logs to the email rather than sending the logs in the body of the message.
- Limit e-mail report size – Restricts the size of the email to prevent it from exceeding the specified number of KB.

Configuration

To enter the email notification settings, click "Edit distribution."
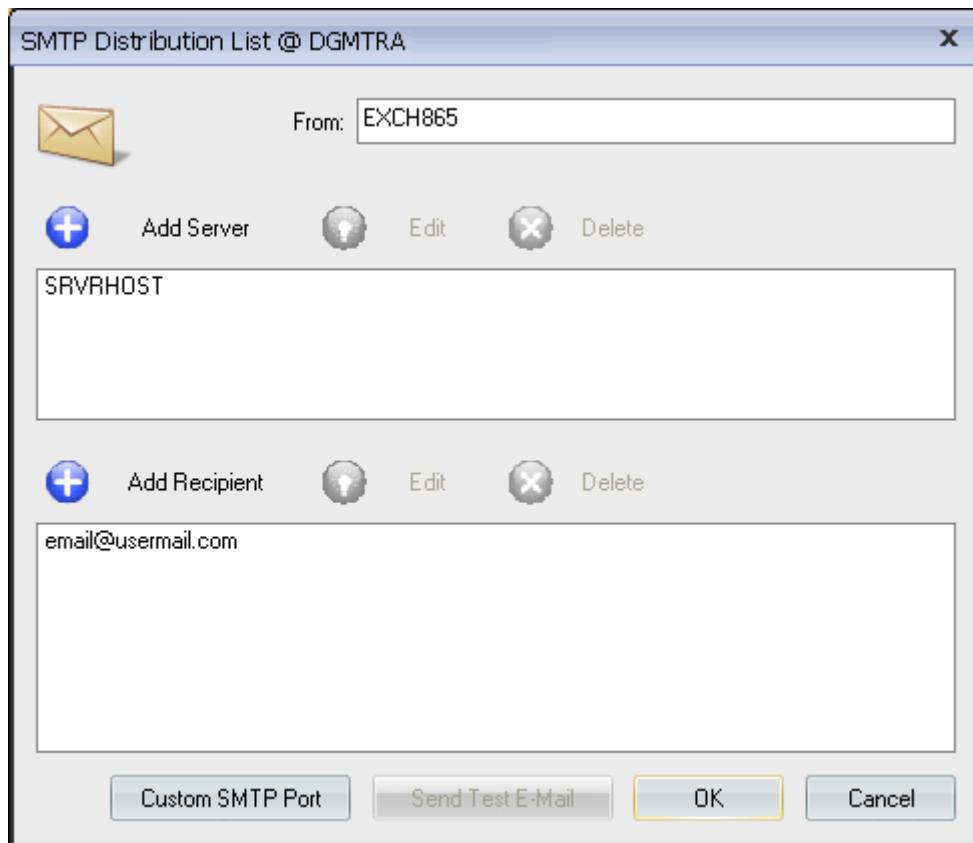
Fig. 3 - SMTP distribution settings.

- From [Address] – Type in a properly formatted email address. This address does not have to be an existing email address; any properly formatted address can be used.
- SMTP Servers – Click the "Add Server" button and type in or browse to the Windows name or IP address of an SMTP server on the network. Multiple servers can be added for redundancy.
- Recipients – Click the "Add Recipient" button and enter a valid and existing email address that should receive the UltraBac notification email(s). Multiple addresses can be added to allow the notification of multiple users.

Device Options
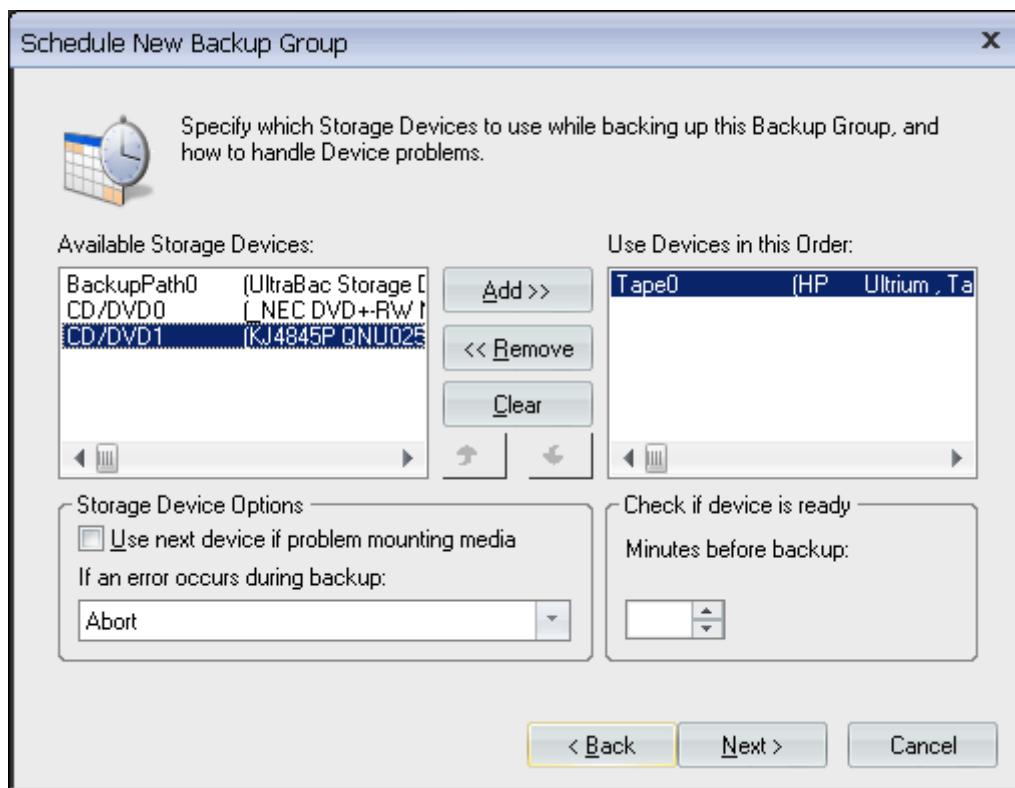
Fig. 4 - Device options.

Available storage devices are added by highlighting and clicking the "Add" button.

Storage Device Options

- Use next device if problem mounting media – If a media error occurs, UltraBac will continue the backup job on the next device. If unchecked, the backup will abort after a media error.
- If an error occurs during backup:
  - Use next device to restart set – Restart the current backup set using the next storage device in line.
  - Use next device to restart group – Restart the scheduled backup using the next storage device.
  - Abort – Abort the backup.

Check If Device Is Ready

- [####] Minutes before backup – Initiates a check of the storage device before the backup is run.

Event Time Options

A scheduled backup can be configured to start at a specified time, date, day of the week, or many other options. Backups can be set to run only in specific months, every few minutes, or only run once.

Start/End Dates and Backup Frequency

- Start Time – Type the appropriate time in the "Start Time" field, using "24 hour" (military) time.
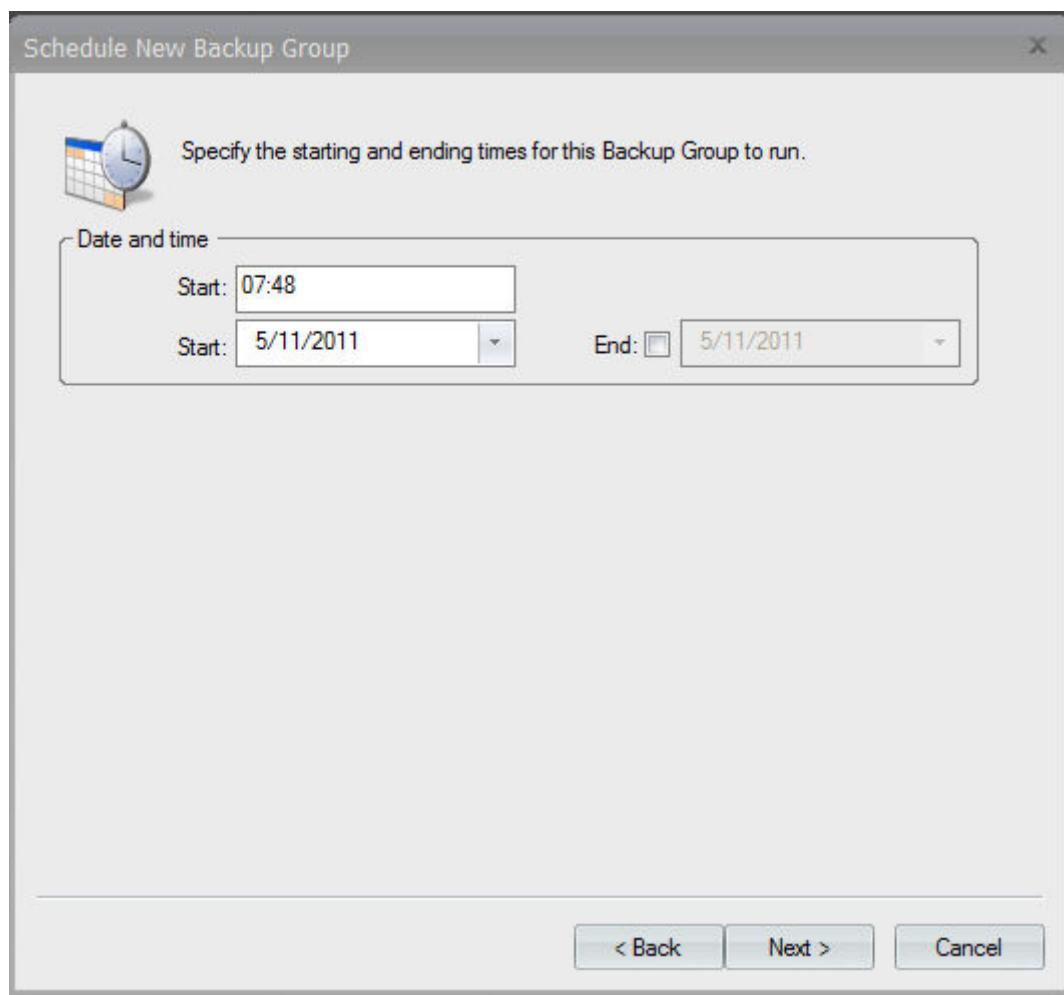
Fig. 5 - Setting the Start/End date and time of a scheduled job.

- Holidays – Set the behavior to use on holidays:
    - Default behavior – Backup runs as specified in the holiday.
    - Event runs on – Backup runs on all holidays.
    - Event skips – Backup does not run on any holidays.
- Event Frequency – Sets how often a backup job repeats after the start date:
    - Never (Run Once)
    - The <Day> of each month – This field is controlled by the start date. If the start date is set to the 15th of November, this field will reflect "The 15th of each month."
    - Every <Day(s) of Week> – This field is controlled by the "Restrict to: Days" check box, and will list all days checked or "Every week" if nothing is checked.
    - Every <Date> – Controlled by the "Start Date" field, this sets the backup to run each year on the specified date.
    - The first day of each month – Run the backup of the first calendar day of each month.

- o First <Day(s) of Week> of each month – This field is controlled by the "Restrict to: Days" check box, and will list all days checked or "First week of each month" if nothing is checked.
- o Second <Day(s) of Week> of each month – This field is controlled by the "Restrict to: Days" check box, and will list all days checked or "Second week of each month" if nothing is checked.
- o Third <Day(s) of Week> of each month – This field is controlled by the "Restrict to: Days" check box, and will list all days checked or "Third week of each month" if nothing is checked.
- o Fourth <Day(s) of Week> of each month – This field is controlled by the "Restrict to: Days" check box, and will list all days checked or "Fourth week of each month" if nothing is checked.
- o The last <Day(s) of Week> of each month – This field is controlled by the "Restrict to: Days" check box, and will list all days checked or "Last week of each month" if nothing is checked.
- o First weekday of each month – Runs the backup on the first Monday of each month.
- o Last weekday of each month – Runs the backup on the last Friday of each month.
- o Last day of each month – Runs the backup on the last calendar day of each month.
- o Every [###] Minute(s) – Launch the scheduled backup again after the specified number of minutes.

- Restrict to:
    - o Days – The backup will only run on the selected days. If no selections are made, the backup will run every day.
    - o Months – The backup will only run in the selected months. If no selections are made, the backup will run every month.
    - o Hours – The backup will only run during the selected hours. If no selections are made, the backup will run only at the scheduled time.

UltraBac Administrative Guide v9.2
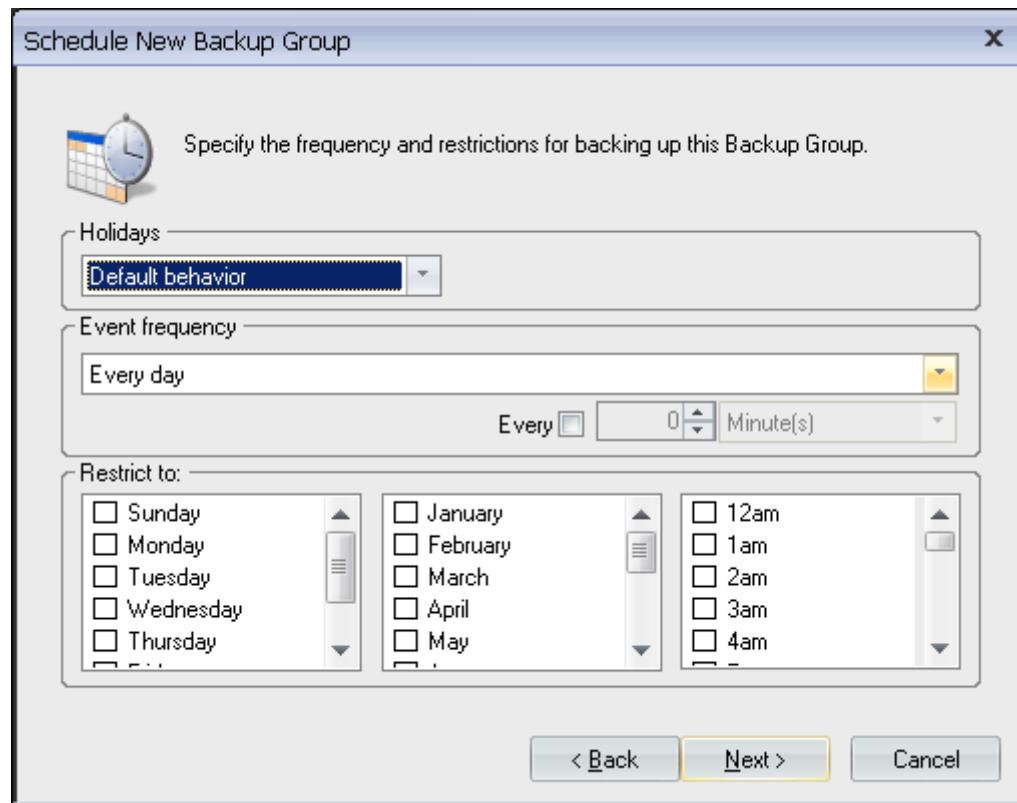
Fig. 6 - Setting the frequency and repeats of a scheduled job.

More Information

See UBQ000069: Troubleshooting SMTP

88

Viewing Scheduled Backups

UltraBac has both a Day-at-a-Glance and Month-at-a-Glance calendars that can be used to view scheduled backups. The Month-at-a-Glance calendar lists the number of events on each day of the month, while the Day-at-a-Glance calendar shows all events for the specified day by time and description.

To open the Scheduled Events calendar, select the Tools tab, and click "View Events.":

Fig. 1 - Day-at-a-Glance calendar.

Scheduled backups can be added, opened, viewed, disabled, and deleted through the Day-at-a-Glance calendar.

To view the properties of a scheduled backup:

1. Right click on the backup to be viewed.
2. Mouse over the scheduled job to view.
3. Click "Edit" from the expanded menu.

Scheduled Backup Properties

All preferences set during the creation of a scheduled backup can be modified by opening the properties of the job. The scheduled backup can also be run manually through this screen.

To open the properties of a scheduled backup through the Scheduler:

1. Select the Tools tab, and click "View Events."
2. Browse to the day of the backup to edit.
3. Double click on the description of the backup to edit.

To open the properties of a scheduled backup through the UltraBac console:

1. Select the Backup tab and click "Open."
2. Set the "Files of type" to "UltraBac Backup Set (*.UBB)."
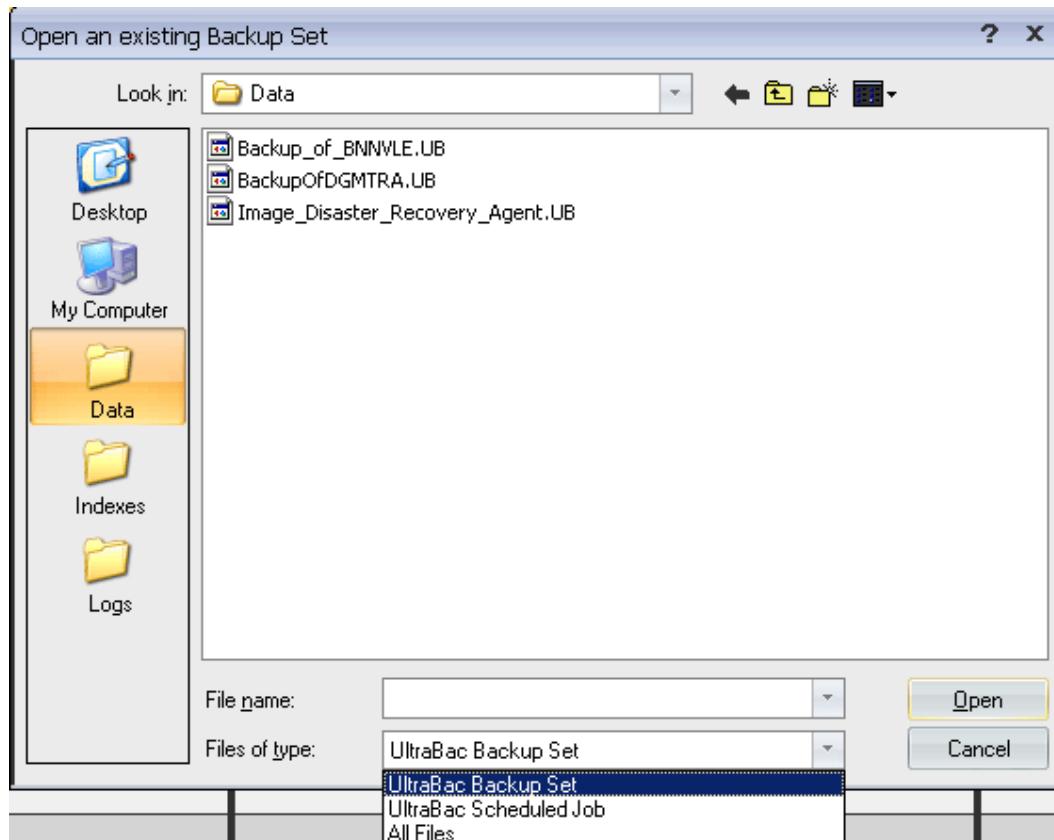
Fig. 2 - Opening the properties of a scheduled job

3. Select the backup to edit.
4. Click "Open."

Dates

The Dates tab shows the "Start Date," "End Date," and "Next Event" dates of the selected backup. It also allows scheduled backups to be run manually, backup times to be modified, and events to be added to a scheduled backup.

Events toolbar:

*   Add New Event – Adds a new event for the scheduled backup, allowing the scheduled backup to be run on more than one date or time.
*   Edit– Opens the date and time properties of the selected event.
*   Delete – Deletes the selected event.
*   Run Now Attended – Immediately starts the scheduled backup in "interactive" mode. Backup errors are reported in the backup log and with a pop-up message, causing the backup to pause until "OK" or "Cancel" is clicked.

- Run Now Unattended – Immediately starts the scheduled backup in "unattended" mode. Backup errors are reported only in the backup log.
- Email Group File – Emails the group and all sets in the group to UltraBac's Technical Support staff. Use only when instructed by an UltraBac Technical Support representative.
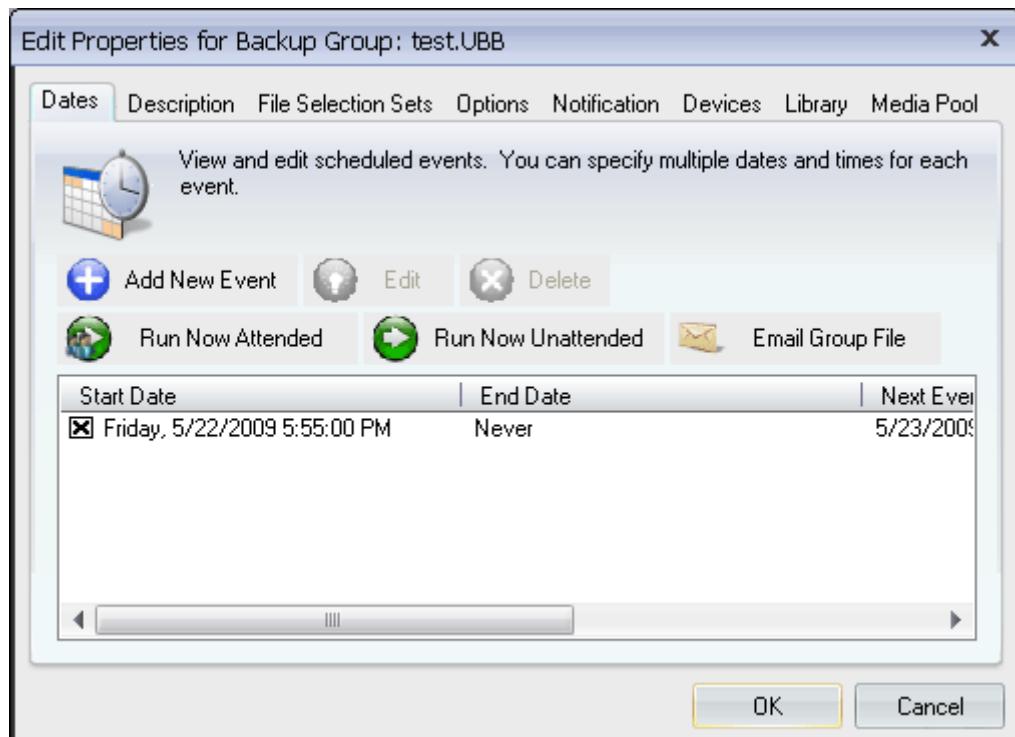
Fig. 3 - Viewing the properties of a scheduled backup with two scheduled events.

The scheduled backup can be disabled (stopped from running) by un-checking the box next to the event information.

NOTE: For more information on the scheduled backup options, please visit the "**Scheduled Backup Options**" section of the User Manual:

UltraBac User Manual: Scheduled Backup Options

Before and After Jobs

UltraBac has the ability to launch scripts or batch files before a backup set runs and after the backup set completes. This can be used to create and run customized scripts to stop the services of a relational database before the backup begins, or run any other commands that can be issued in a scripted format.

Set Level

Before/After commands are inserted in the set after the set has been "enumerated" by the Backup Wizard, in the "Set Properties":

1. Create or open a backup set.
2. Click "Action"/"View Backup Set Properties."
3. Select the Before/After Jobs tab.
4. Browse to or enter in the path to the script(s) to be run during, before, or after the set is backed up.
5. Click "OK" to save.
6.
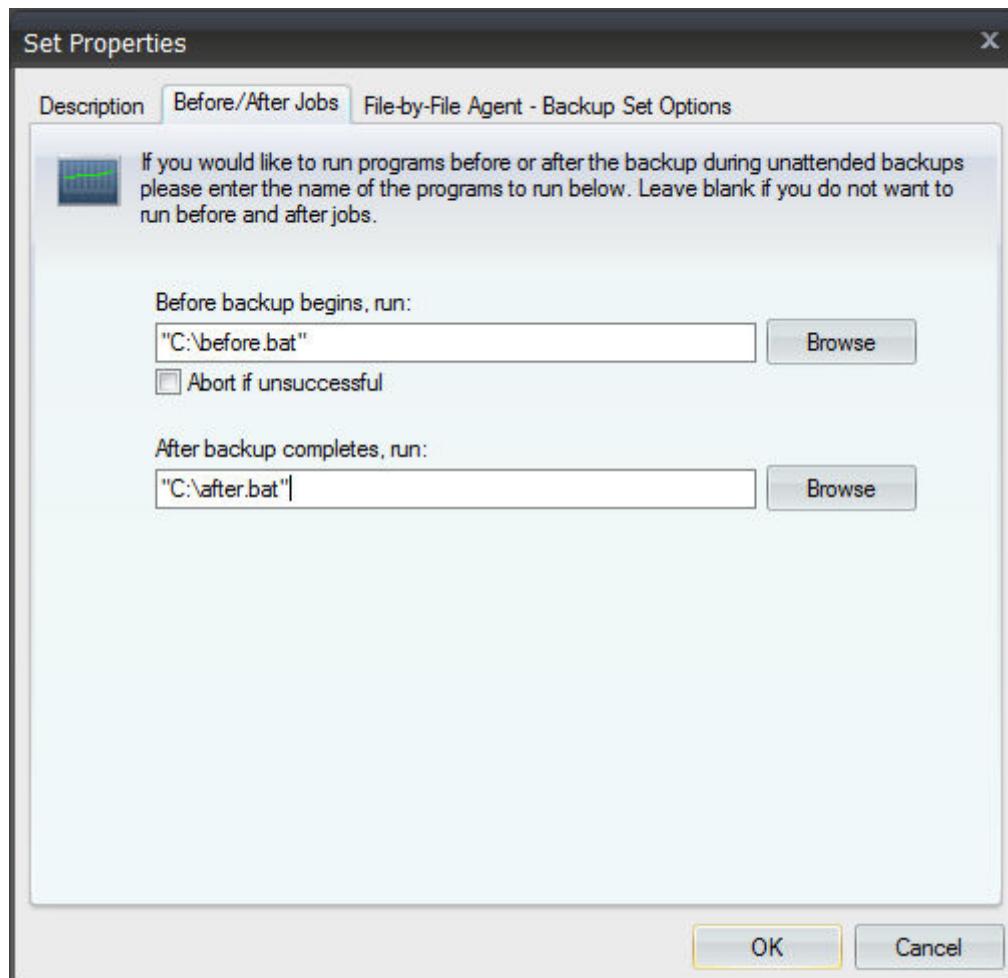
Fig. 1 - Before/After Jobs tab in the Set Properties.

NOTE: Before/After Jobs are only executed when the set is run as a part of a scheduled backup.

Group Level

1. Open the properties of a scheduled backup.
2. Select the Options tab.
3. Check the box before the "Run Before job" or "Run After job" fields to enable the appropriate type of job.
4. Browse to or enter in the path to the script(s) to be run during, before, or after the scheduled job in the appropriate field.
5. Click "OK" to save.
6.
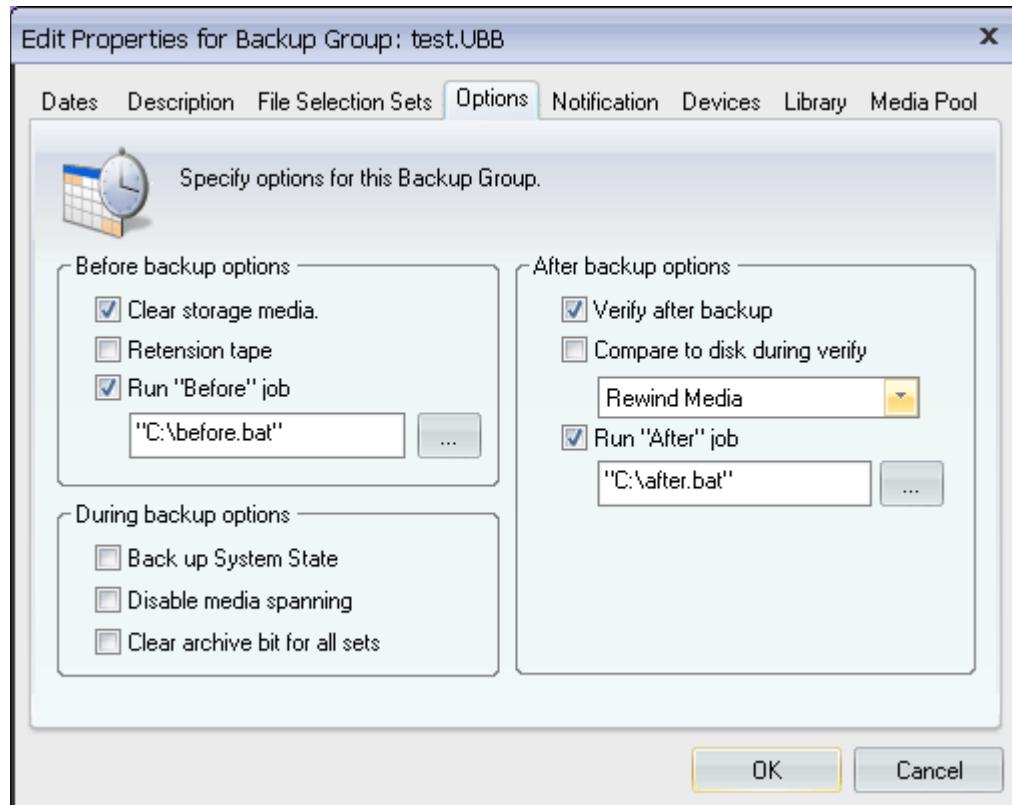
Fig. 2 - Options tab in the properties of a scheduled backup.

NOTE: For more information on creating or editing a scheduled backup, please visit the "**Scheduled Backup Creation**" section of the User Manual:

UltraBac User Manual: Scheduled Backup Creation

Restore Basics

To restore data, the files to restore must be selected from a backup index loaded into the File Viewer, the media used for the backup must be selected, and the target location for the restored data must be specified.

UltraBac is optimized to quickly and efficiently restore files back to the original path, or a remote location, using a variety of indexing options. An index of all files backed up is automatically written to the storage media, and can also be written to an online disk index and/or an index database.

An Express Index, listing all backup sets written to the storage media, is also written to disk and is used to minimize the amount of time used searching the storage media.

Selecting the Storage Device

The first step when performing a restore is selecting the device used during backup. This will ensure that UltraBac looks at the correct media when looking for the data being restored. To find the media used during backup, check the backup log under "Device."

To select the storage device to use during the restore:

1. From the Manage tab, click "Storage Devices."
2. Click the appropriate tab to select the type of media used during the backup.
3. Click and highlight the storage device used during backup.
4. Click "Close."

Loading a Backup Index

To begin the restore process, launch the Restore Wizard by selecting the index source:

1. Select the Restore tab.
2. Click the index source to be used for restore:
    o Retrieve from online disk index – Retrieve backup index list from the "Indexes" folder on the backup host.
    o Retrieve from Storage Media – Retrieve backup index list from the currently selected storage device.
    o Database Index options:
        ▪ Retrieve From Current Media in the Drive – Query the index database for all sets written to the currently selected storage media.
        ▪ Retrieve From Storage Media Group – Query the index database for all sets written to the currently selected storage media, including any media spanned to during the backup.
        ▪ Retrieve All Sets in the Database for <backup host> – Query the index database for all sets that backed up the backup host system.
        ▪ Retrieve All Sets in the Database – Query the index database for all sets in the database.
3. Click "Next."
4.
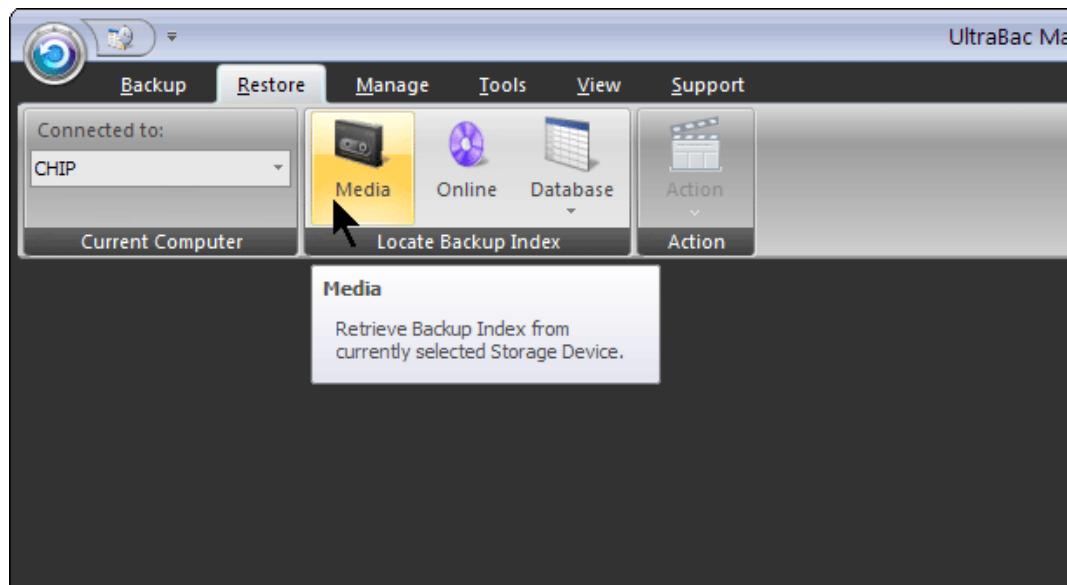
Fig. 1 - Selecting the index source.

NOTE: For more information on the setup and configuration of an index database, please visit the "**UltraBac Database**" section of the User Manual:

UltraBac User Manual: UltraBac Database

Each index source has advantages and disadvantages, depending on the restore situation:

- Retrieve from index database – The fastest and most flexible method, but may not be usable if the database is not available. Also, if the correct storage media is not selected, the restore may not be successful.
- Retrieve from online disk index – Almost as fast as the index database, but does not list the media used by each index, and may not be usable if the online indexes are not available. Also, if the correct storage media is not selected, the restore may not be successful.
- Retrieve from Storage Media – Only slightly slower than the online index when using the Express Index, the indexes kept on the storage media index will always be available and are the easiest to use for restore.

Selecting the Index

Once the index source is selected, the backup index must be selected and loaded into the File Viewer.
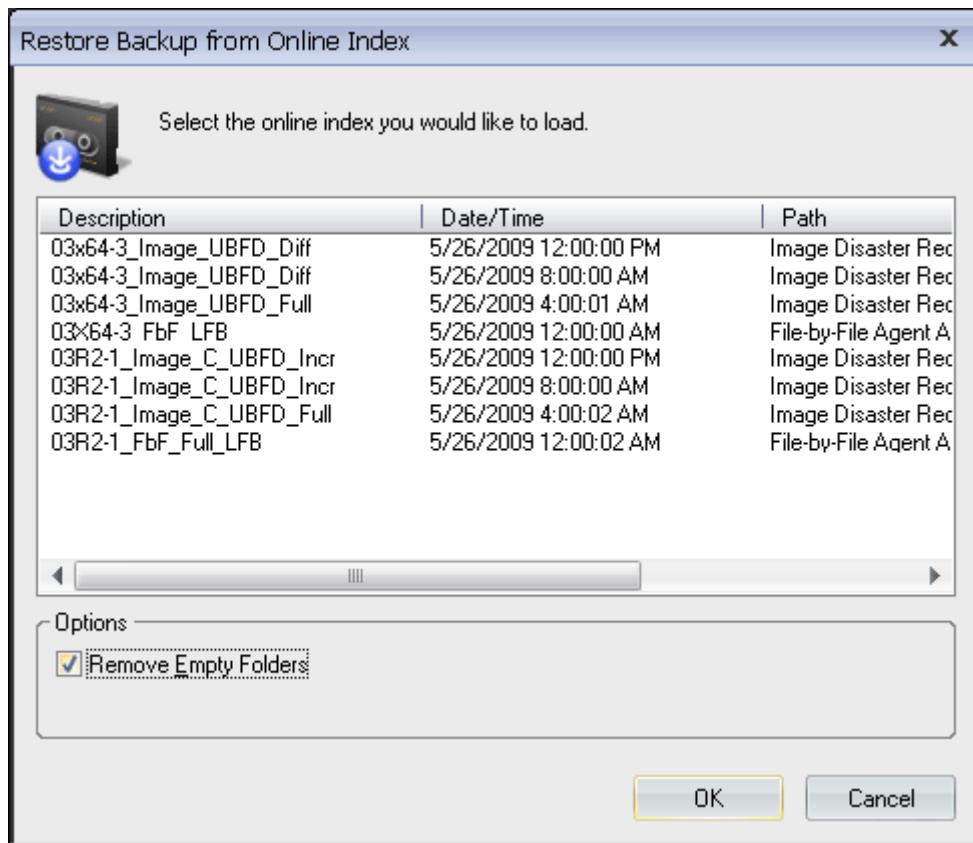
Fig. 2 - Selecting the backup index to load from the online disk index.

To load a backup index into the File Viewer:

1. Click on and highlight the index to load.
2. Click "OK."

NOTE: It is only possible to select and load one index at a time.

Index Options
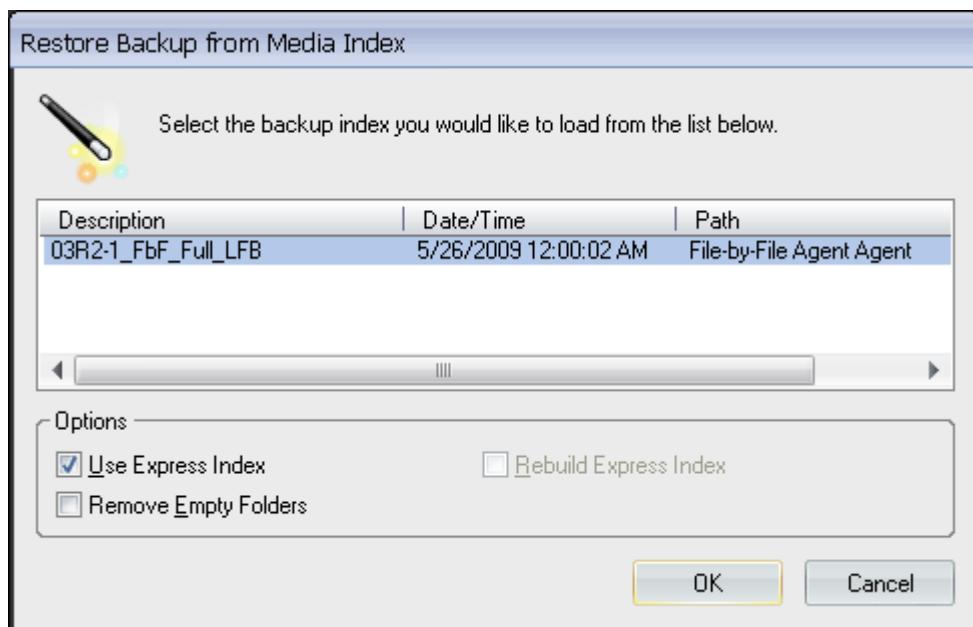
Fig. 3 - Selecting the backup index to load from the storage media.

Several options are available that modify the way UltraBac handles backup indexes:

- Use express index – Uses an index on disk to quickly find all indexes on the storage media. This option is only available when loading the index from storage media.
- Remove Empty Folders – Instructs UltraBac to not enumerate empty folders when loading an index for restore. This option is only available when loading the index from online disk index or storage media.
- Rebuild Express Index – Rebuilds the express index by searching the media for all indexes. This option is only available when loading the index from storage media.

Selecting Files for Restore

When an index is loaded, the index opens in the UltraBac File Viewer. The File Viewer displays all data backed up in the selected set.

Select the files to be restored by marking the box directly to the left of the desired file/folder/data in blue.
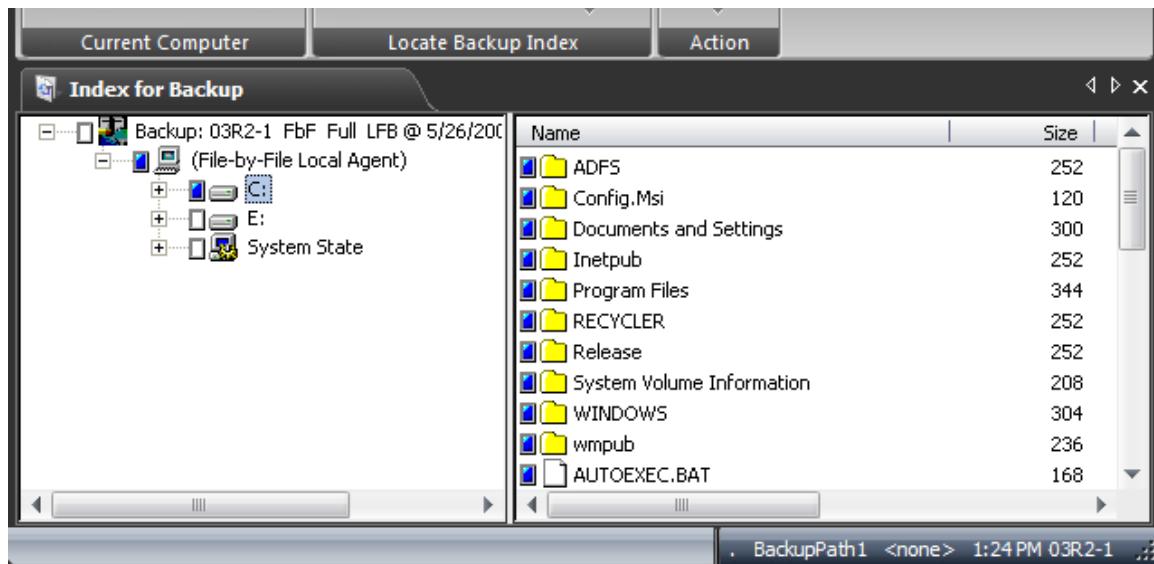
Fig. 4 - File-by-file backup set loaded in the File Viewer.

Restoring Data from a Backup

To restore the selected data:

1. From the Restore tab, click "Action"/"Restore This Backup."
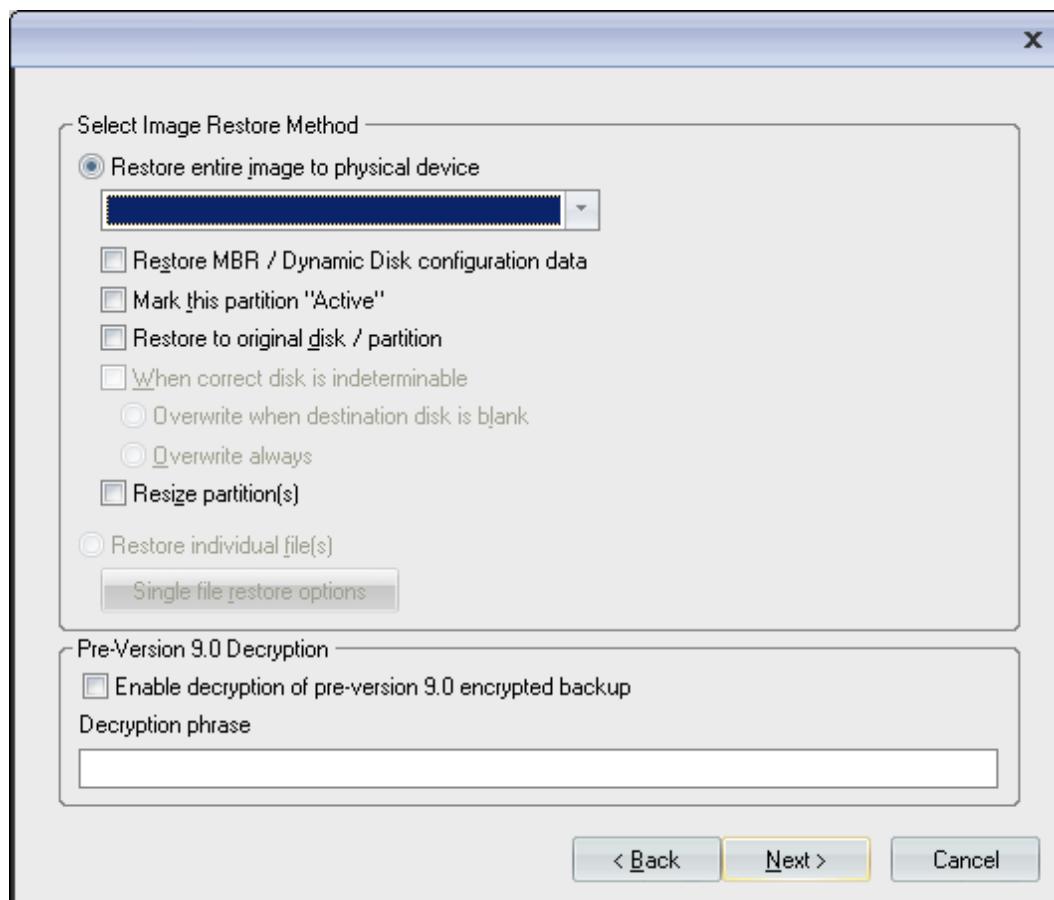
Fig. 5 - Restore options of an image backup set.

2. Set the options for restore in the agent's "Restore Options" screen.
3. Enter the decryption phrase, if an encryption phrase was entered in the backup set. The decryption phrase is the exact same phrase as was entered for the encryption phrase. If the decryption phrase is not entered correctly, the restore will not be successful.
4. Click "Next."
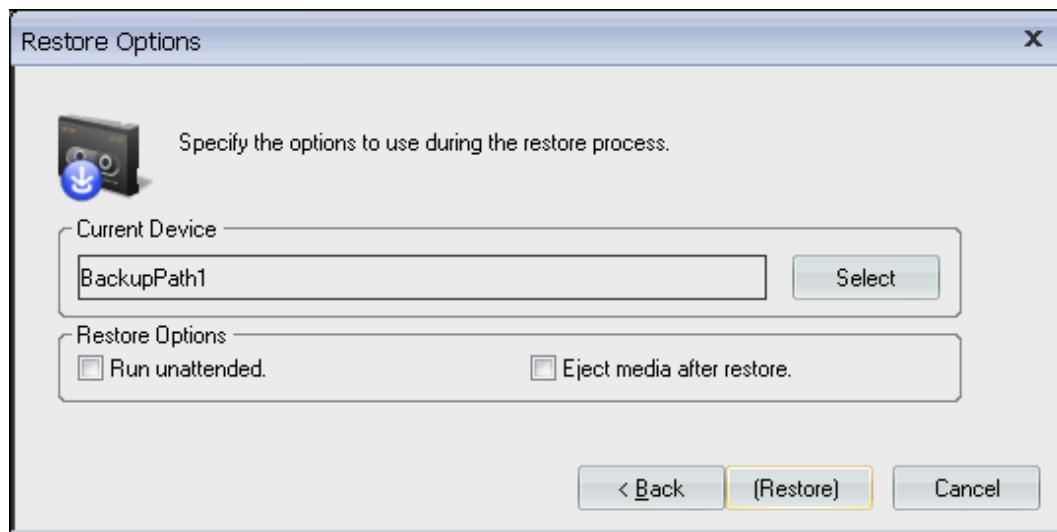
Fig. 6 - Restore options.

5. Check "Run unattended" to disable user prompts during the restore.
6. Click "Restore" to begin restoring the data.

Command Line Functionality

UltraBac has the capability of running almost all backup and restore functions through the DOS shell in Windows. These commands can be scripted or run manually through the command prompt, allowing manual interaction or the automation of backups using other applications or task schedulers. The command line interface cannot be used to create a set or to schedule a backup.

NOTE: For additional information on running UltraBac with DOS commands, please see the UltraBac Knowledge Base:

See UBQ000001: Command Line Backup/Restore

Fig. 1 - Command prompt displaying the UltraBac command line options.

NOTE: To view a list of all command line options in UltraBac, enter "ub /?" into the command prompt and press "ENTER."

Backup Commands

When specifying a group to run from the command line, no options need be set. This is a sample backup command using a Backup Group:

ub.exe /backup tuesday.ubb

When specifying a set to run from the command line, several options can be set. This is a sample backup command using a Backup Set:

ub.exe /backup server_full.ub /device:backuppath0 /preparemedia:tuesday /verify:crc

Options listed:

- /backup <set/group name> – Back up the specified set or group.
- /Device:<device number or name> – Select device for use during a "set-level" backup (overrides default).
- /PrepareMedia:<volume label> – Prepare media with the specified volume label.
- /Verify:<CRC/Compare/No> – Verify after backup.

To run an unattended backup through the UltraBac scheduler, use the following command:

scheduler.exe /E /NOW:<filename.ubb>

Restore Commands

It is also possible to run a restore using the command line. Sample command line for restore:

ub.exe /findfiles:* /restore:c:\temp /device:backuppath0

Options listed:

- /FindFiles:<file pattern> – File files specified by the file pattern.
- /Restore:[path] – Restore with optional restore to path.
- /Device:<device number or name> – Select device (overrides default).

UltraBac Agents

UltraBac Disaster Recovery

Image Disaster Recovery Agent

The Image Disaster Recovery Agent in UltraBac is the same Image Disaster Recovery Agent that is used in UBDR Gold. The functions and screens are the same as the Image Disaster Recovery Agent in UBDR Gold as well as the instructions.

The UltraBac Image Disaster Recovery Agent uses "snapshot" technology to take a sector level backup of a physical disk or partition. The UltraBac Locked File Backup Agent is integrated with the Image Disaster Recovery Agent, ensuring the backup is a complete and consistent snapshot of the selected disk(s). An Image Disaster Recovery Agent backup is used to quickly restore a failed disk or operating system without the need for re-installing the operating system.

> NOTE: For information on performing a Static Mirror Image backup using the Image Disaster Recovery Agent, please visit the "**Static Mirror Image**" section of the User Manual:
>
> **UltraBac User Manual: Static Mirror Image**

> NOTE: The UltraBac Image Disaster Recovery Agent supports Windows software RAID only when configured as RAID-0 or RAID-1.

Setup and Configuration

> NOTE: To create an image backup of a remote system, the UltraBac Image Disaster Recovery Agent must be installed on the system being imaged. For more information on installing the Image Disaster Recovery Agent, please visit the "**Installing UltraBac**" section of the User Manual:
>
> **UltraBac User Manual: Installing UltraBac**

Creating an Image Set

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Click "Image Disaster Recovery Agent" to highlight the option, and click "Next."
3. Set the Image Agent options, and click "Next."
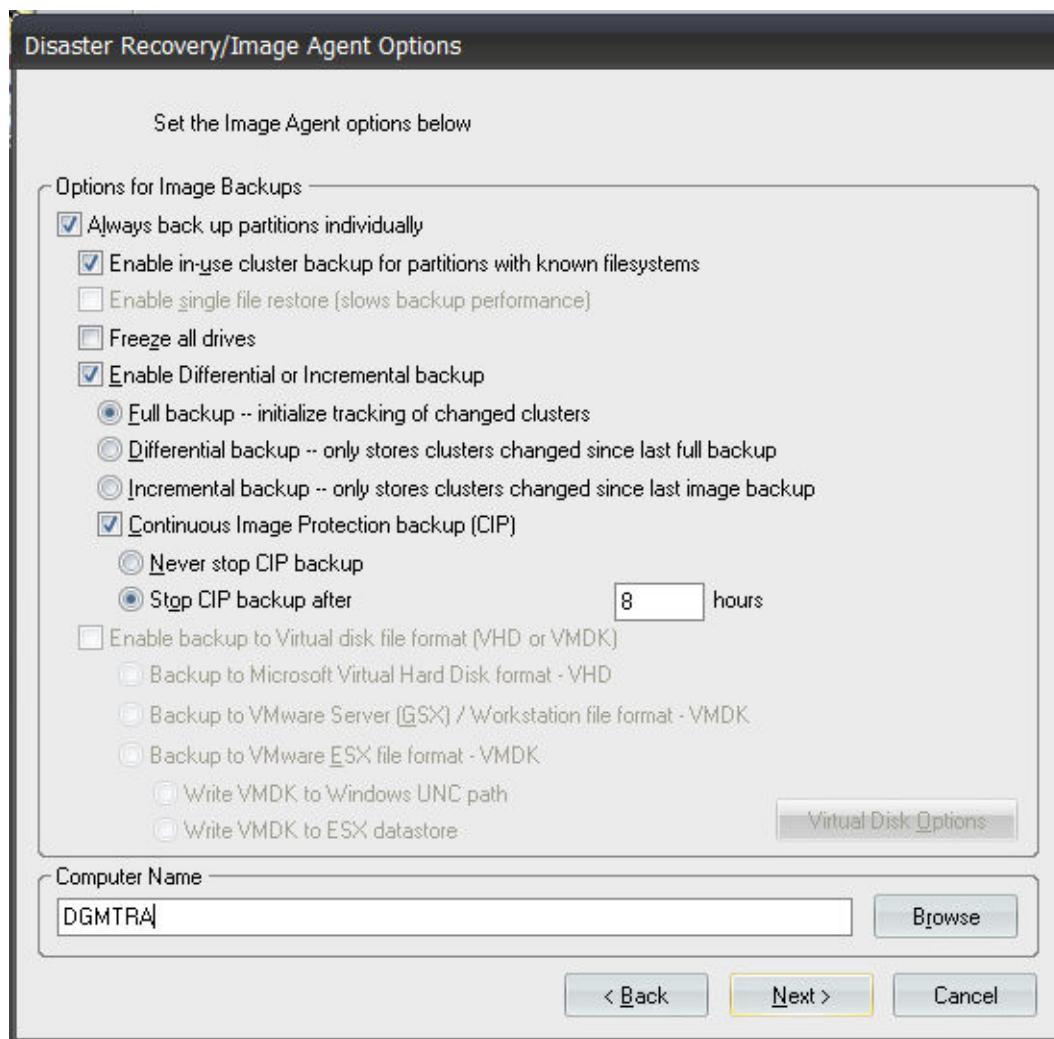
Fig. 1 - Disaster Recovery/Image Agent Options.

4. Type a set description, as it will appear in the backup log, into the "Set Description" field but do not modify the "File Selection Logic." Click "Next."
5. Check "View/Edit files in the backup set" and click "Finish."
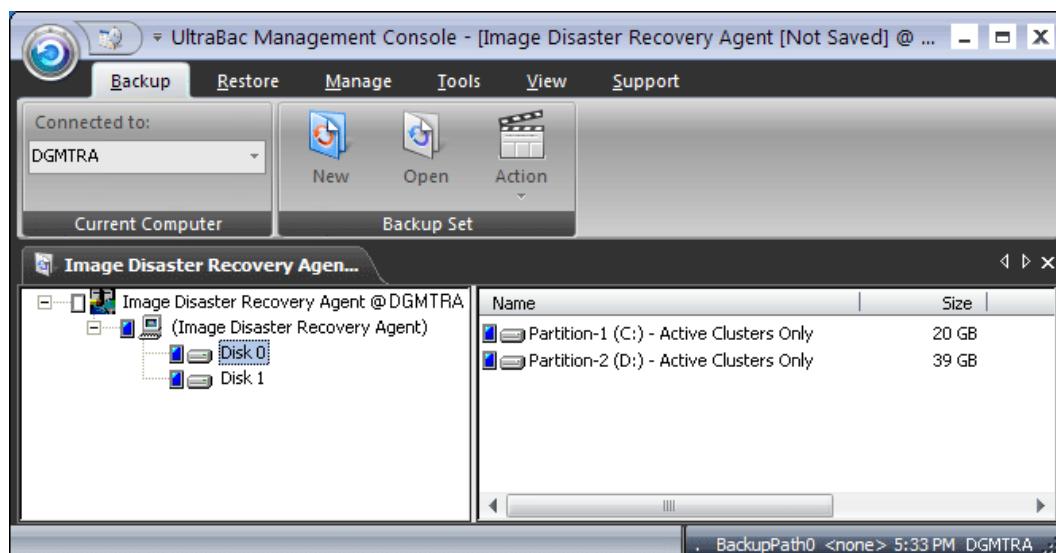
Fig. 2 - Image set loaded in the File Viewer.

6. Save the set by clicking "Action"/"Save" from the main "Backup Set" menu.

Image Agent Options
Options for image backups:

- Always back up partitions individually – Allows partitions to be individually selected. If unchecked, only a full disk can be selected.
- Enable in-use cluster backup for partitions with known file systems – The image set will only back up the in-use clusters on the selected disk or partition, excluding all empty disk space.
- Enable single file restore (slows backup performance) – Indexes the image backup to allow the restore of one or more files from the set.
- Freeze all drives – Freezes all physical disk drives during an image backup of the system. This will allow databases and other applications that are installed across multiple partitions to remain consistent when restored from an image backup.
- Enable Differential or Incremental backup – Enables the tracking of changed clusters and set creation necessary to perform a differential image backup.
  - o Full backup – Backs up the full partition or disk, and clears the ".idx" file used to track disk changes.
  - o Differential backup – Backs up all clusters modified after the last full backup.
  - o Incremental backup – Backs up all clusters modified after the last full or incremental backup.
  - o Continuous Image Protection backup (CIP) – Monitors all changes made to the disk.
    - ▪ Never Stop CIP backup – Continue CIP backup indefinitely.
    - ▪ Stop CIP backup after <##> hours.
- Enable backup to Microsoft Virtual Server / Hyper-V file format (VHD) or VMware file format (VMDK) – Writes the backup output to a VHD or VMDK file in a secondary data stream.
- Computer Name – Type in or browse to the computer name of the remote system to be backed up.

NOTE: For more information on creating a VHD or VMDK file during an image backup, please visit the "**Writing to VHD**" or "**Writing to VMDK**" section of the User Manual:

UltraBac User Manual: Writing to VHD
UltraBac User Manual: Writing to VMDK

NOTE: With "Enable Differential or Incremental backup" checked, a full backup must be performed before a differential/incremental backup can be run.

Restoring an Image Backup

An image backup can be restored several ways:

- Partition or disk restore using the UltraBac Management Console
- Single file restore using the UltraBac Management Console
- Partition or disk restore using UBDR Gold
- Static Mirror Image restore

NOTE: An active operating system partition cannot be overwritten by an image restore.

Partition/Disk Restore
A full image restore through the UltraBac Management Console requires the target disk be prepared before restore:

- Partition level restore – Restore target partition must be of equal or greater size than the original source partition, and unassigned of a drive letter.
- Disk level restore – Restore target disk must be of equal or greater size than the original source disk, and the disk must be unpartitioned.

NOTE: Only one disk or partition can be restored per restore job.

To begin the restore process:

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the index for restore.
3. Select the disk or partition for restore.
4. Click "Action"/"Restore this Backup."
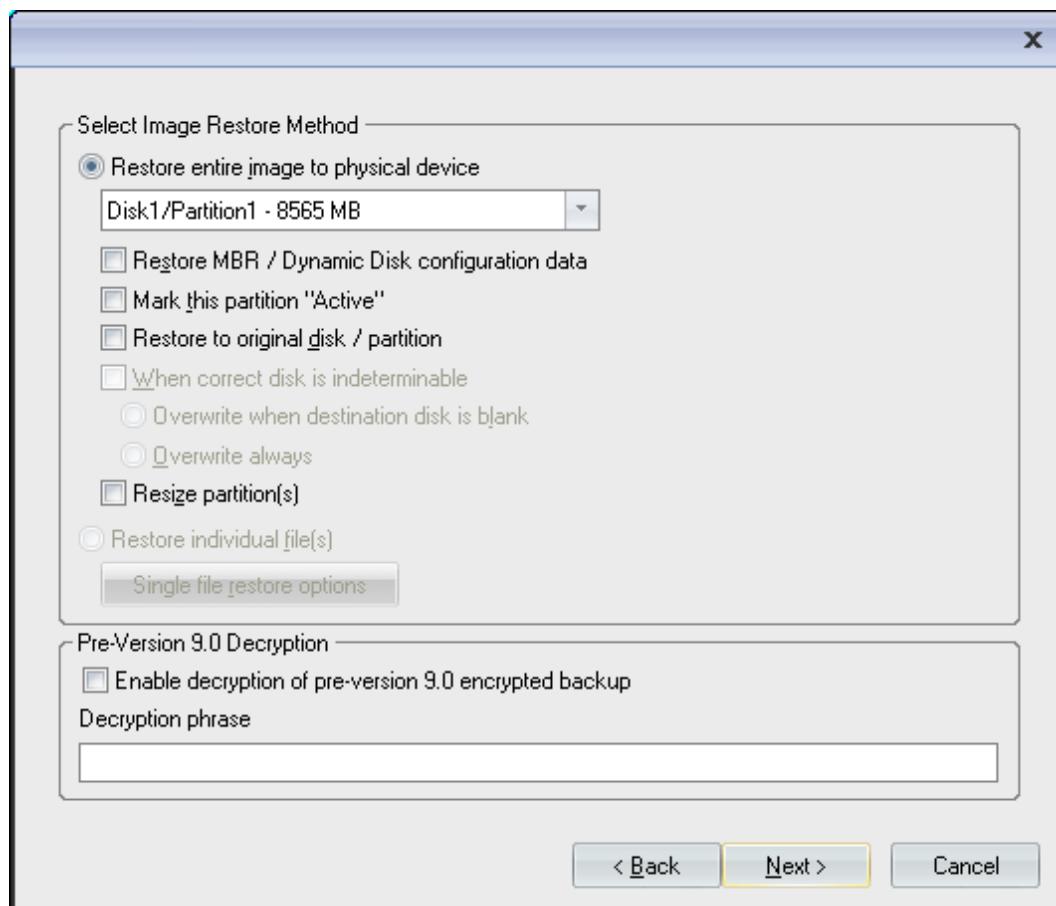
Fig. 3 - Disaster Recovery/Image Restore Options .

5. Click the "Restore entire image to physical device" radio button, select the restore target partition from the drop-down menu, and click "Next."
6. Check "Run Unattended," and click "Restore."
7. After the restore completes, reboot the system to activate the restored disk or partition.

NOTE: For resizing the partition during an image restore, please visit the "**UBQ000233: Resize Partitions During Image Restore**"

See UBQ000233: Resize Partitions During Image Restore

Single File Restore
This option is available only if "Enable Single File Restore" is checked during the creation of the image set. If the preference was selected, each partition backed up will have an available directory tree to use for restore selection logic.

NOTE: Single file restore is not supported on the NT4 operating system.

NOTE: Single file restore can only restore from one partition per restore session.

To begin the restore process:

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the index for restore.
3. Select the files or folders for restore.
4. Click "Action"/"Restore this Backup."
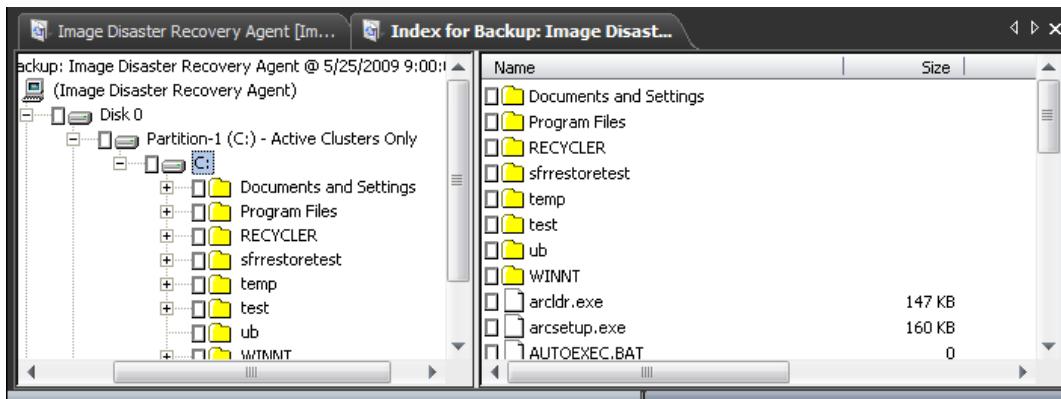
Fig. 4 - Single File Restore index loaded in the File Viewer.

5. Click "Single File Restore Options."
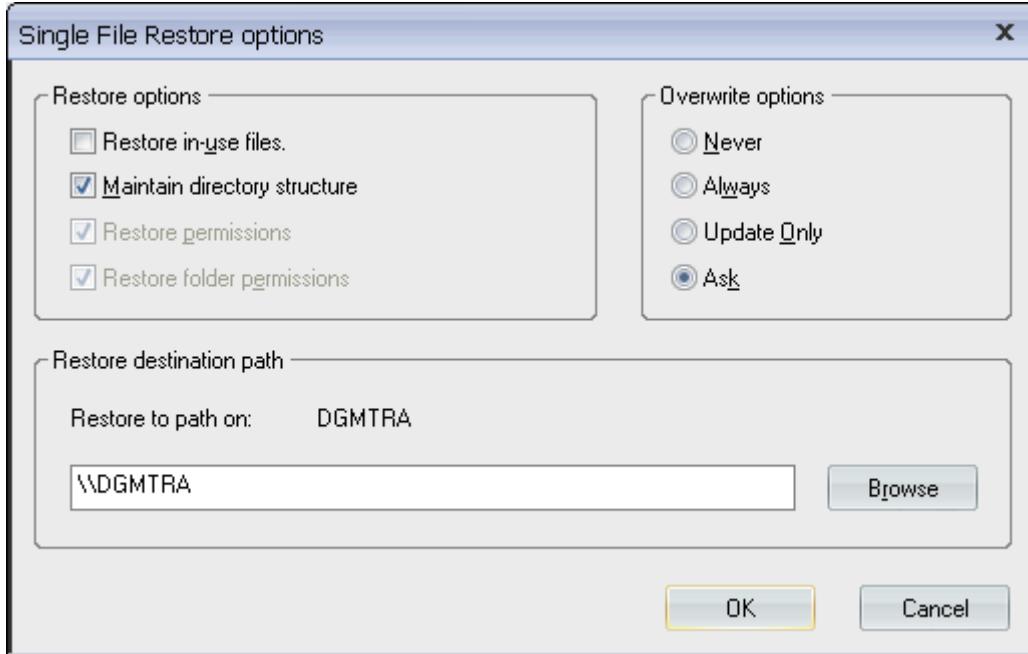
Fig. 5 - Single File Restore options.

6. Set the restore options, overwrite options, and the "Restore Destination Path." Click "OK."
7. Click "Next."

8. Check "Run Unattended" and click "Restore."

Single File Restore Options
Restore Options:

- Restore in-use files – Forces the restoration of in-use files. The overwritten in-use files will not become active until the system is rebooted.
- Maintain directory structure – Restore files and folders with the original parent folder structure. This preference can only be disabled when restoring to an alternate path.
- Restore permissions – Restores previously existing permissions on files. This preference cannot be disabled.
- Restore folder permissions – Restores previously existing permissions on folders. This preference cannot be disabled.

Overwrite Options:

- Never – Do not overwrite any existing files.
- Always – Overwrite existing files with the files being restored.
- Update Only – Only overwrite if the file being restored is newer than the existing file.
- Ask – Prompt the user before overwriting any existing files.

Restore Destination Path:

- Type or browse to the restore target directory.

RAID Array Strategies and Considerations
There is no distinguishing difference in the process of backing up and restoring to a RAID array or restoring to an ordinary IDE drive. There are some limitations to be aware of when imaging and restoring RAID arrays:

- The RAID array must be configured prior to the restore through the manufacturer's RAID configuration utility.
- The level of RAID (RAID 0, striping, RAID1, mirroring , etc.) during backup should be consistent with the level of RAID during restore.
- To restore all partitions back to the original location on a rebuilt RAID array, the MBR should first be restored to the destination disk to create the partition table.

More information
See UBQ000233: Resize Partitions During Image Restore

UBDR - UltraBac Disaster Recovery

UBDR Gold v5.0 and v6.0 are on bootable CDs. UBDR Gold v5.0 uses Windows PE 2.0 technology, and UBDR Gold v6.0 uses Windows PE 3.0 technology as the platforms to perform UltraBac Image/Disaster Recovery Agent restores. UBDR Gold is designed to retrieve and restore UltraBac image backups of a partition or an entire disk from a locally attached tape device, a remote disk path, an FTP site, Tivoli device, or a remote tape device.

UBDR Gold can also be used to perform both image and file-by-file backups.

When the system boots, the UBDR CD automatically detects and loads drivers for most NIC cards, SCSI cards, and RAID controllers.

Setup and Configuration

NOTE: To use the UBDR Gold CD, the restore target system must be able to boot from CD. Consult the motherboard manufacturer's documentation for more information.

1. Power up the restore target system and insert the UBDR Gold Restore CD into the CD-ROM drive.
2. Check "I accept the above license agreement," and click "Next."
3. Select the network card for use during the restore from the drop-down menu.
4. Set the network configuration, either manually or by enabling DHCP.

If restoring from a locally attached device, it is possible to click "OK" without entering any network configuration information. To prevent UBDR from attempting to retrieve an IP address, click the "x" in the upper right corner of the "Configuration" window.
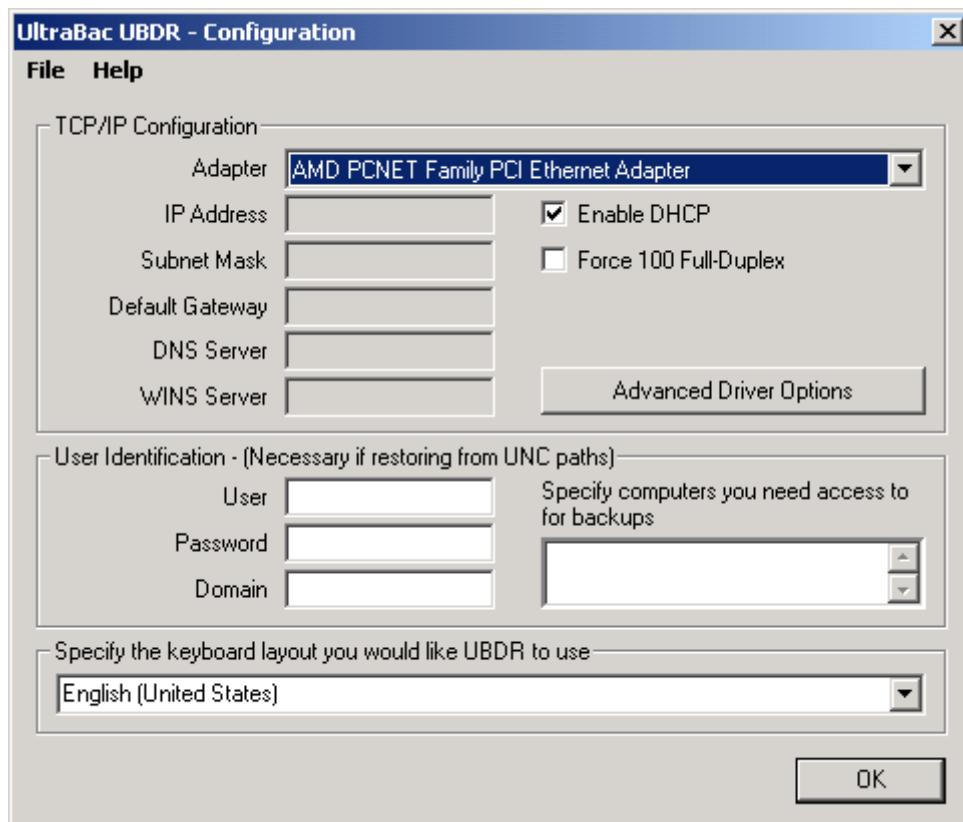
Fig. 1 - Network Configuration.

Adapter – Allows the selection of the NIC to be used by UBDR from a drop-down menu, if multiple NIC cards are installed in the UBDR Gold host system.

- Enable DHCP –Allows UBDR to use a DHCP server to specify the network settings. When disabled, the network fields (i.e. IP Address, Subnet Mask, etc.) are used to configure the network settings.
- Force 100 Full-Duplex – Instructs UBDR to force the NIC to use 100 Full-Duplex.

Network options used when DHCP is unselected:

- IP Address – Specify the subnet mask of the IP address used.
- Default Gateway – Specify the IP address for the default gateway to be used by UBDR. This field can be left blank if UBDR does not need to connect to the internet.
- DNS Server – Specify the IP address of the DNS server used by the system or device hosting the image backup. This field can be left blank if IP addresses are to be used for device configuration.
- WINS Server – Specify the IP address of the WINS server used by the system or device hosting the image backup. This field can be left blank if IP addresses are to be used for device configuration.

International Keyboard Support

- UBDR has keyboard support for 162 languages. To select support for a specific language, choose that language from the drop-down menu. That keyboard layout will begin functioning as soon as the language is selected.

User Identification

- Account – Specify an account that has full read/write access on the system (or share) hosting the image backup.
- Password – Specify the password for the account above.
- Domain – Specify the domain of the account above. If in a workgroup, specify the name or IP address of the system hosting the image backup.
- Specify machine(s) – This field is used to specify all machines with which UBDR will need to establish a connection. It is usually only necessary to specify the machine name or IP address of the system hosting the image backup.

Advanced Driver Options
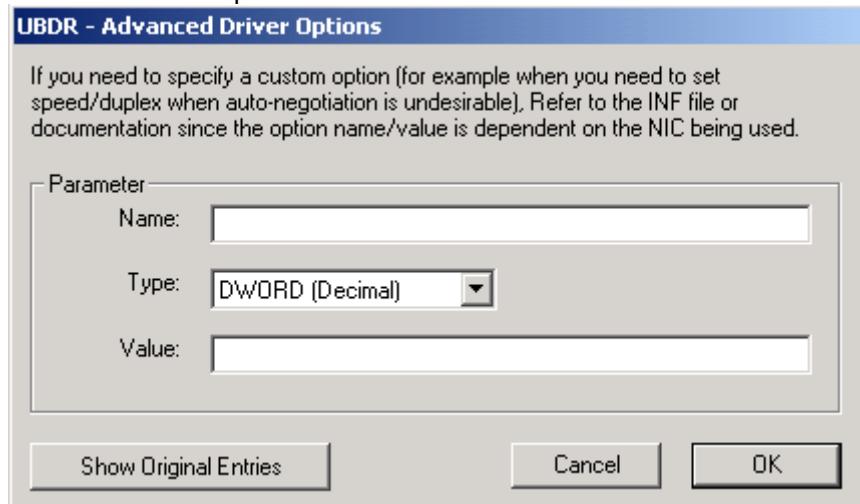
Fig. 2 - Advanced Driver Options.

This allows users to specify custom parameters for the selected NIC by creating registry entries that control the behavior of the NIC. For more information on the values that can be entered into the "Advanced Driver Options," please consult the NIC manufacturer's documentation.
Show Original Entries
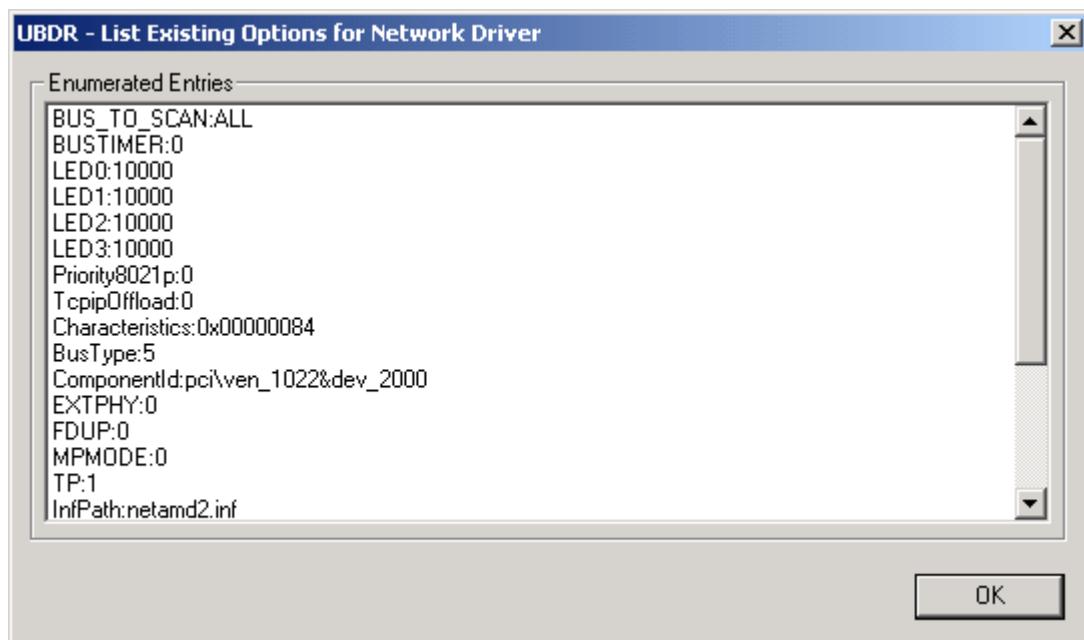
Fig. 3 - Existing Options for Network Drivers.

This shows the registry entries as they currently exist for the selected NIC.

Device Selection

Once the network settings are entered, the storage device can be created/selected. UBDR Gold has the ability to use any type of backup device used by UltraBac. This includes FTP, Tivoli, media libraries, and remote devices. If the backup was written to CD or DVD by any third-party software (i.e. Nero, etc.), specify the CD/DVD drive letter as a BackupPath device.

After clicking "OK" in the "Network Configuration" screen, the device selection/creation process will automatically begin.
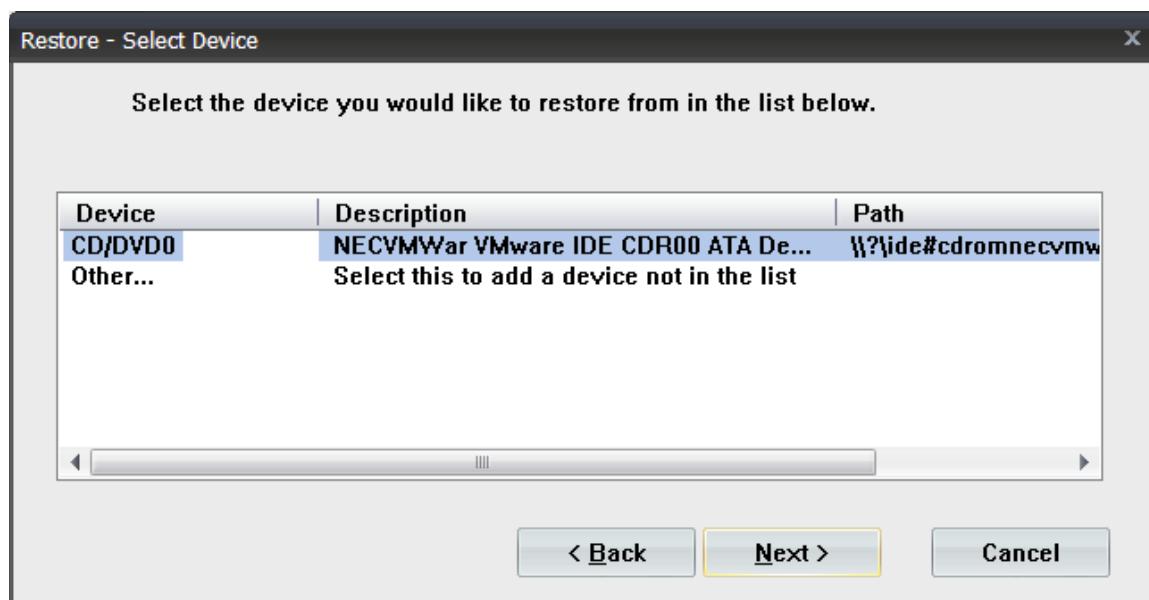
Fig. 4 - UBDR device prompt.

To select a device other than any automatically enumerated tape or CD/DVD devices, select "Other" and click "Next."
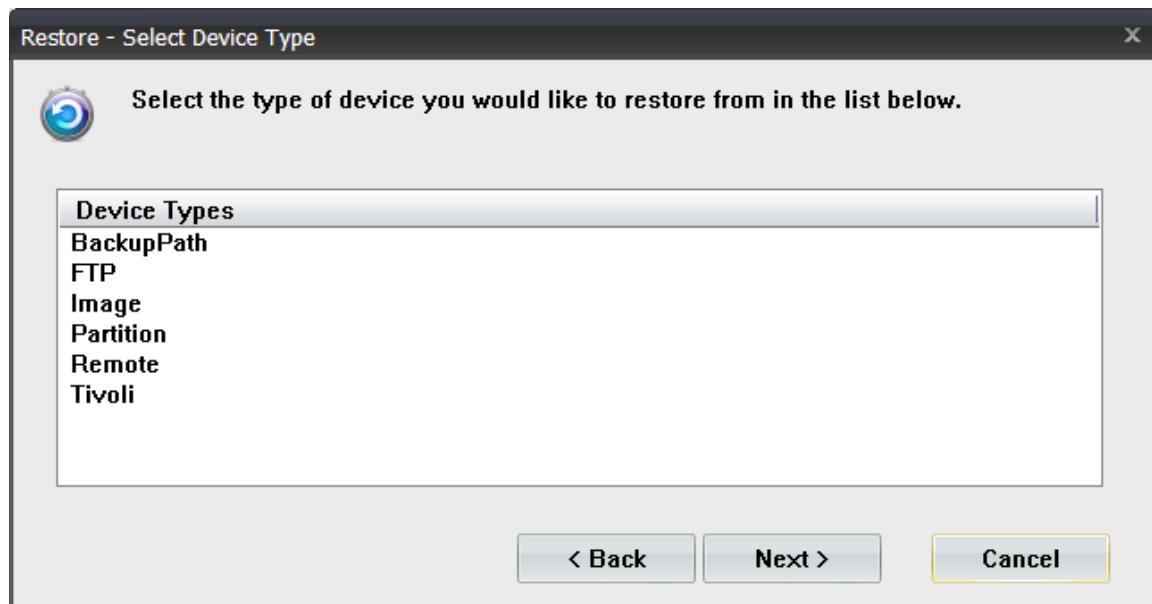
Fig. 5 - Device selection options.
Tape Devices
In the UltraBac Storage Device Manager, tape devices will automatically be listed. UltraBac will automatically assign names to these devices, starting with Tape0.
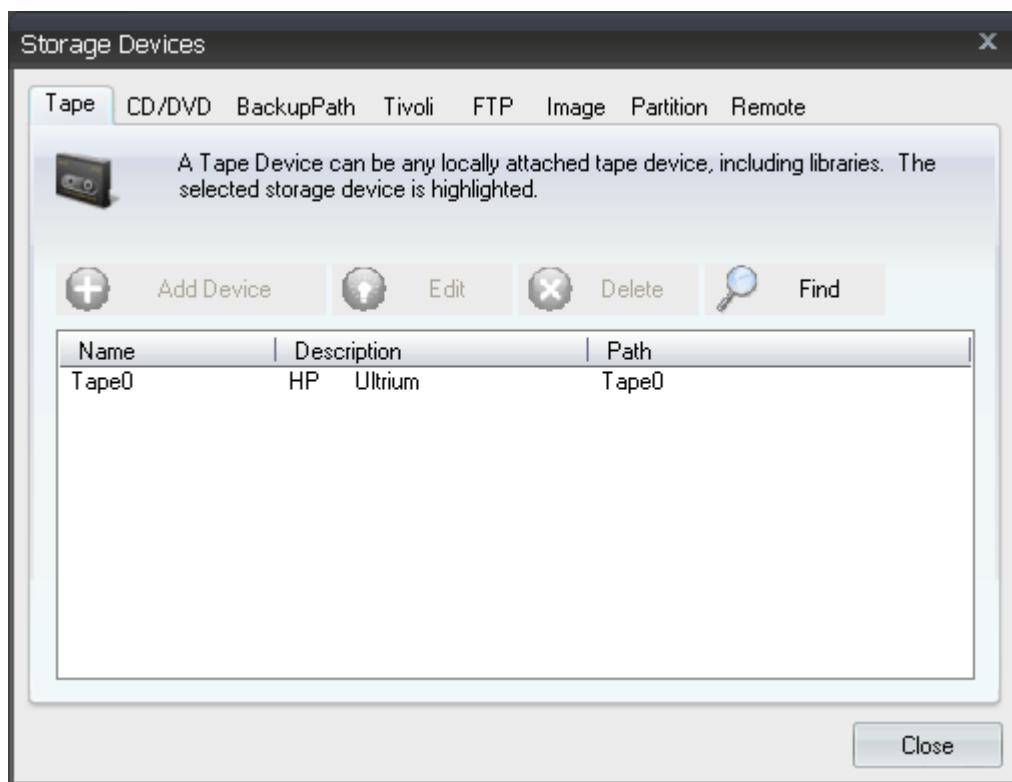
Fig. 6 - Tape devices in UBDR.
CD/DVD Device

If a CD/DVD writable drive is installed in the backup host, it will automatically appear in the CD/DVD tab.
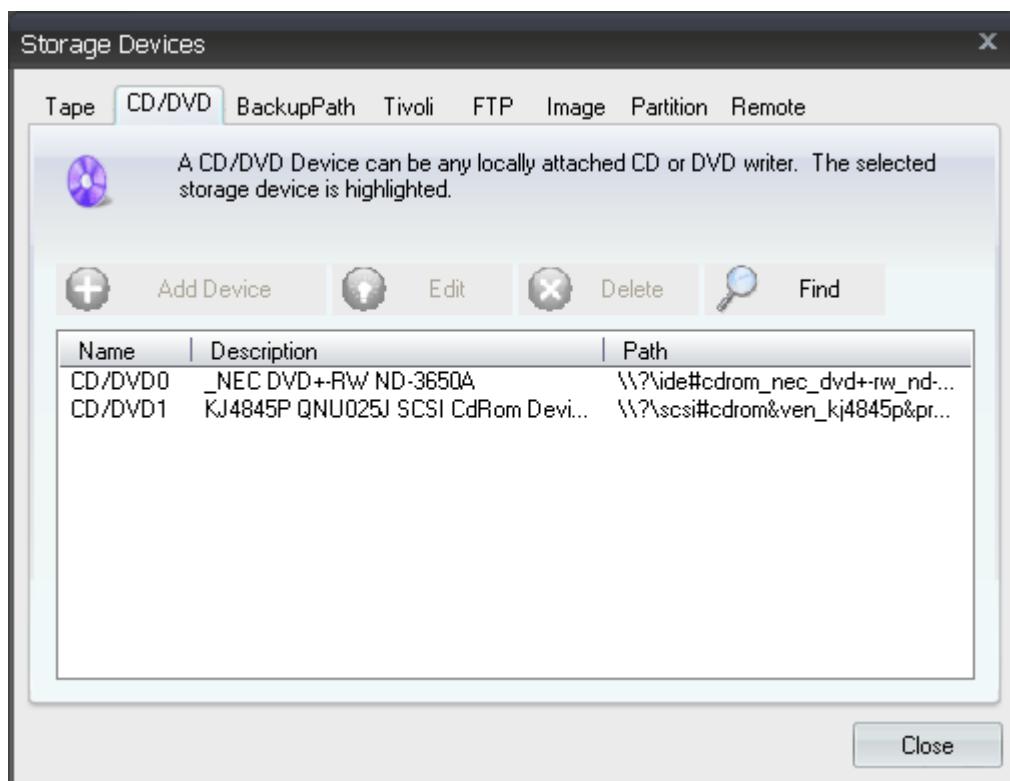
Fig. 7 - CD/DVD devices in UBDR.
BackupPath Device
BackupPath devices are user-created output targets that point to a folder on the backup host, or on a network path. To specify a BackupPath device:

1. Select the BackupPath tab.
2. Click the "Add Device" button.
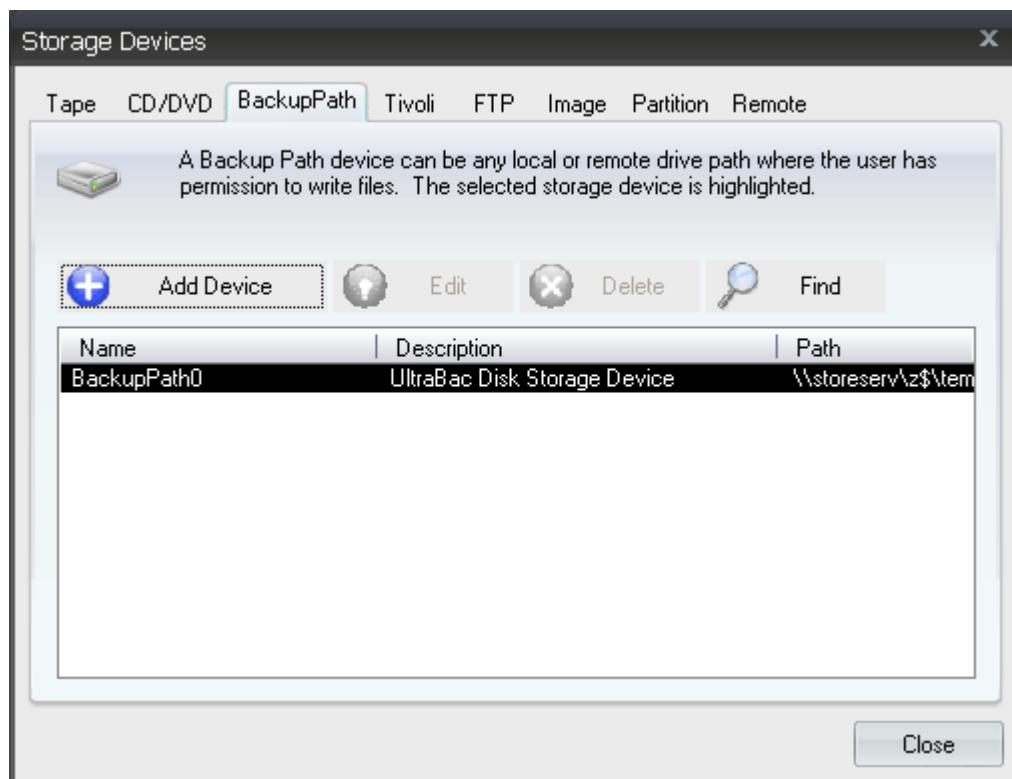
Fig. 8 - Tape devices in UBDR.

3. Enter a unique name in the "Device Name" field.
4. Enter a local or UNC path, to be used as an output target, in the "Directory for Device" field.
5. Click "OK" to save.

It is not necessary to enter the maximum folder size in the "Limit size per media" field, or to enter a size in the "Limit size per file" field. It is recommended to leave both these items at the default value.

FTP Device

To add an FTP device:
1. Select the FTP tab.
2. Click the "Add Device" button.
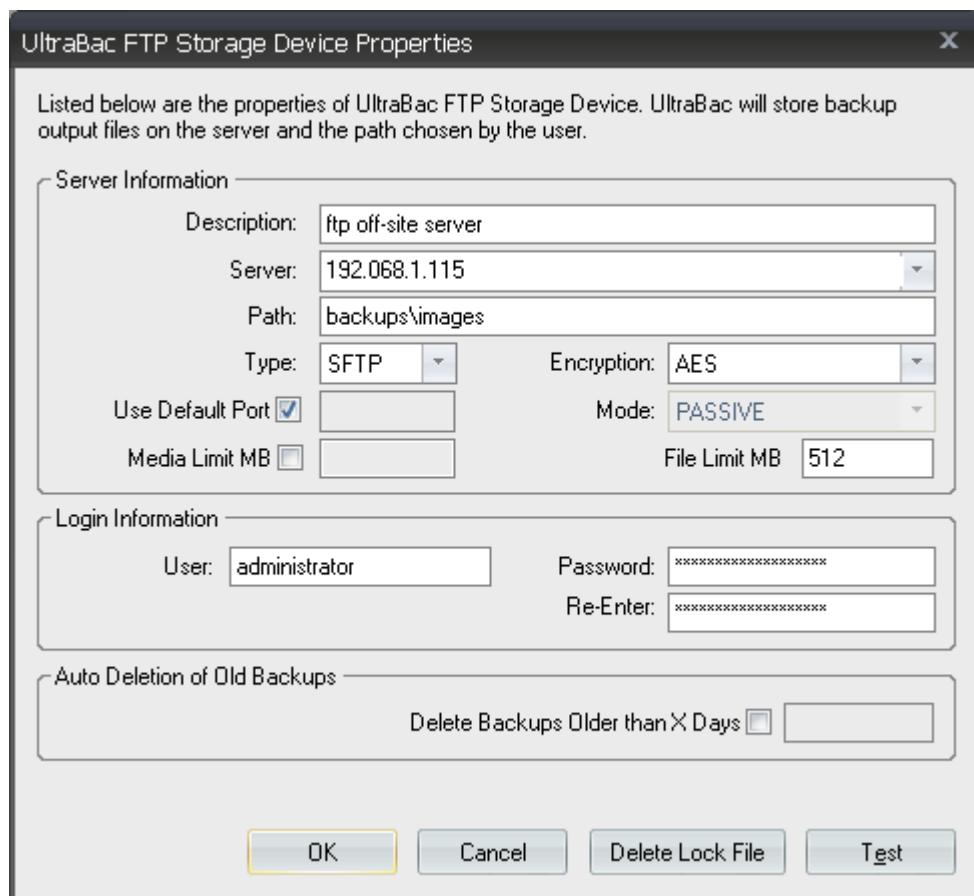
Fig. 9 - FTP device options.

3. Type a device description into the "Description" field.
4. Type an FTP server name or IP address in the "Server" field.
5. Type a folder path to be used to store backup data in the "Path" field. This must be the full path to where the backup files will be stored.
6. Type the user name for the FTP server in the "User" field.
7. Type the password for the user name in the "Password" field.
8. Re-type the password for the user name in the "Re-Enter" field.
9. Click "OK" to save.

It is not necessary to enter the maximum folder size in the "Limit size per media" field, or to enter a size in the "Limit size per file" field. It is recommended to leave both these items at the default value.

Tivoli Storage Manager Device

NOTE: To use the Tivoli device, the backup host must be running the Tivoli client software, which can be downloaded here:

http://www.tivoli.com/support/storage_mgr/clients.html#xp

To define a Tivoli device:

1. Select the Tivoli tab.
2. Click the "Add Device" button.
3. Enter a unique device name in the "Device Name" field.
4. Enter the name or IP address of the Tivoli server in the "Server" field.
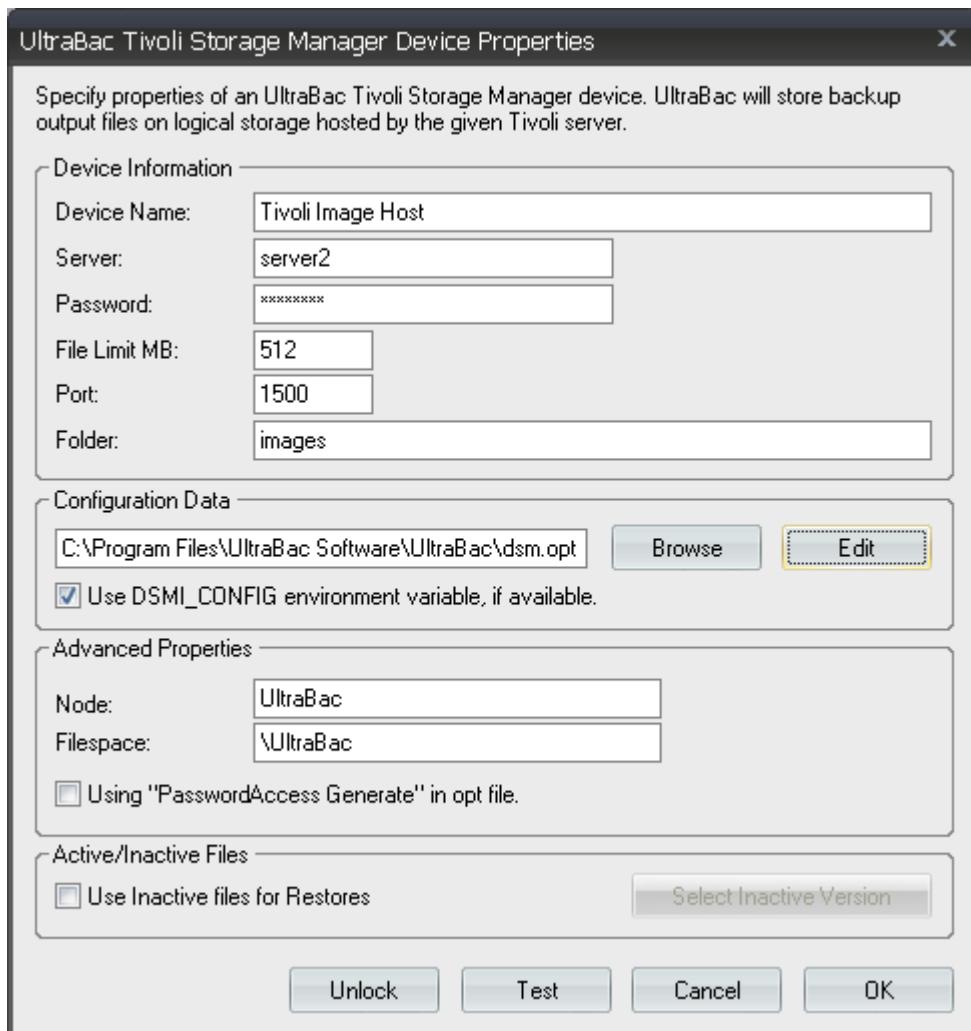
Fig. 10 - Tivoli device options.

5. Enter the password defined on the selected Tivoli server for the Node name in the "Password" field.
6. Enter the folder (high-level name) to use for backup in the "Folder" field.
7. Enter the output file size in the "File Limit MB" field.
8. Click "OK" to save.

Advanced Properties
- Configuration Data – This is the TSM Client config file, and defines things like the communication protocol and port number to use when communicating with the server.
- Use DSMI_CONFIG environment variable, if available – Selects whether the DSMI_CONFIG environment variable, if set, overrides the above path.
- Node – The node name that UltraBac passes to the Tivoli server.
- Filespace – Part of an object's full name and stems from ADSM being designed to back up servers.
- Use Inactive files for Restores – Enables the use of inactive backup files for restore.
- Select Inactive Version – Selects the inactive version to use for restore.

Click "Test" to ensure the device is working properly.
Image and Partition Devices
If UBDR Gold is being used to perform a static mirror image backup, the creation of either an
Image or Partition device is required. It is necessary to have devices that are of the same size (or
larger) than the original disk/partition. These backups can only be performed to a local disk.

- Image device – If a hard disk is present with all partitions deleted, it will be available for
  addition as an Image device.
- Partition device – If a partition is created on a hard disk, with no assigned drive letter, it
  will be available for addition as a Partition device.

Remote Device
The Remote device option allows UltraBac to use a storage device attached to or created on a
system other than the UltraBac backup host.

NOTE: The UltraBac Device Drivers must be installed on the system hosting the tape drive.
Tape devices are automatically enumerated when UltraBac is installed on the tape host, and
these devices are numbered in sequential order starting with the lowest SCSI ID. UltraBac will
automatically assign names to these devices, starting with Tape0.

1. Select the Remote tab.
2. Click the "Add Device" button.
3. Enter the Windows name or IP address of the tape host in the "Device Host" field.
4. Enter the UltraBac assigned device name in the "Remote Device" field.
5. Click "OK" to save.

Fig. 11 - Remote devices in UBDR.

After entering in the name of the device host, it is possible to click "Browse" to select the device from a list of devices available on that host.
Autoloader Support
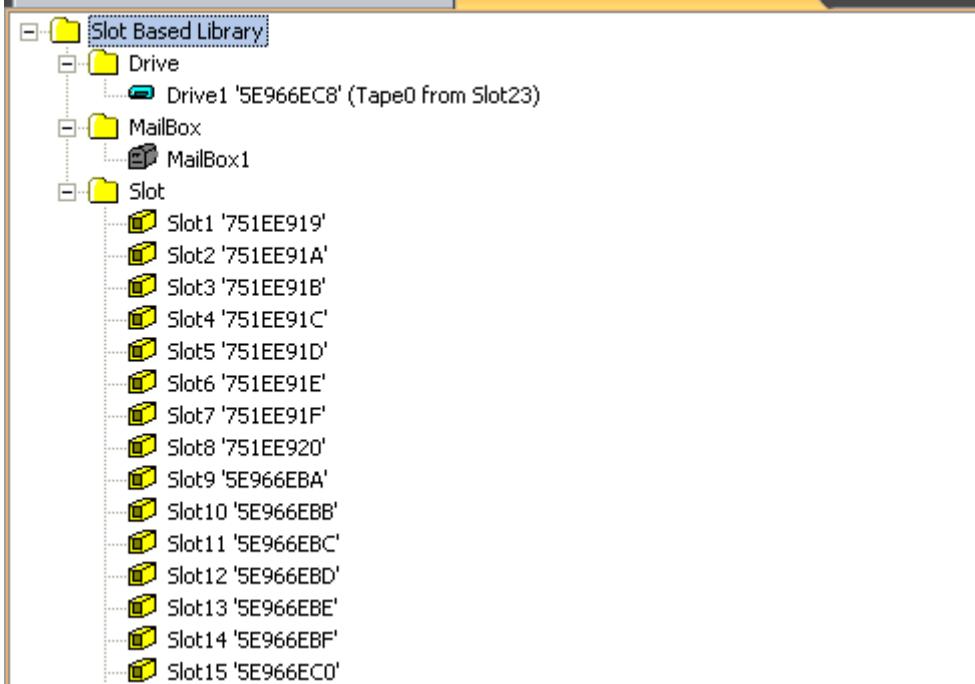
Fig. 12 - Media library controls.

Using UBDR Gold, both local and remote media libraries can be accessed during a restore.

To access a local autoloader:

- Select a tape device residing in the media library when making the device selection during the UBDR Gold restore process.
- Click "Select"/"Storage Devices" from the main UBDR Gold menu, and highlight a tape device residing in the media library from the Storage Device Manager.
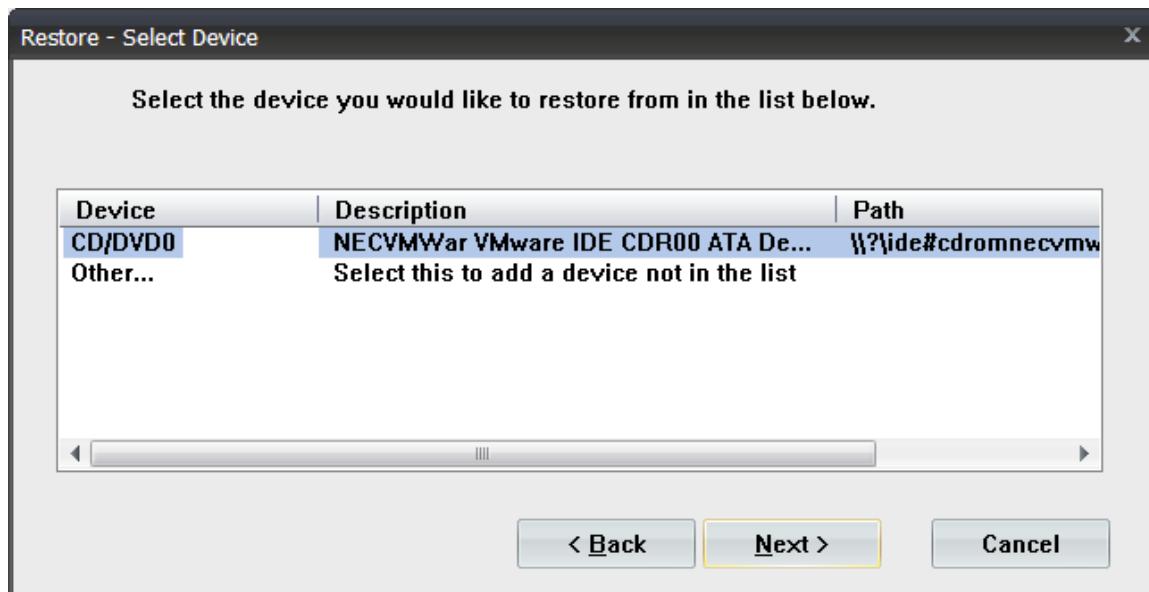
To access a remote autoloader:

1. Select "Other" when making the device selection during the UBDR Gold restore process.
2. Select "Remote" from the Storage Device Manager.
3. Add a remote tape device residing in a media library.

Starting the Restore

Once the storage device is configured, it can be selected and enumerated for restore by UBDR.

Highlight the correct backup storage device, and click "Next".

/
Fig. 13 - Selecting the device for restore.

UBDR Gold will automatically begin searching the media for backup sets.
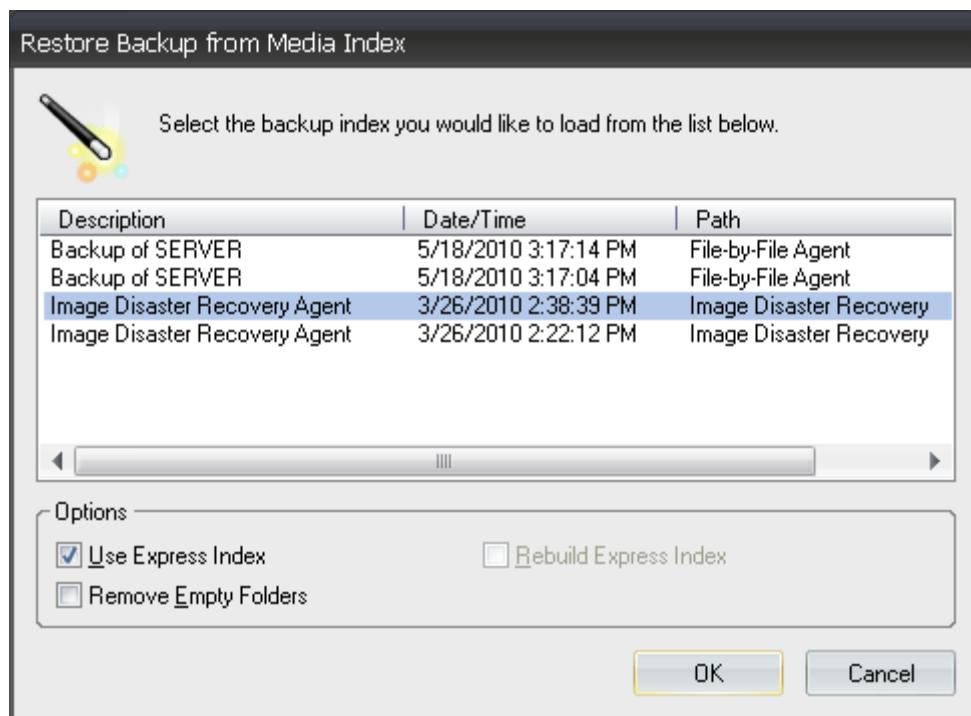
Fig. 14 - Selecting the set for restore.

Select the backup set to restore and click "OK".

Restoring the Image

The Image Restore Method options allow an image backup to be restored to the original server with either a new disk or the original drive. These options also allow the backup to be restored to

a virtual server (both VMware and Microsoft Virtual Server) or even a new system with dissimilar hardware.

By default, all disks and partitions in the backup index are selected for restore.

Click "Cancel" on the Image Restore Method screen to return to the main UltraBac window. This window will allow the selection of individual tools, and allows other advanced operations and utilities to be accessed.
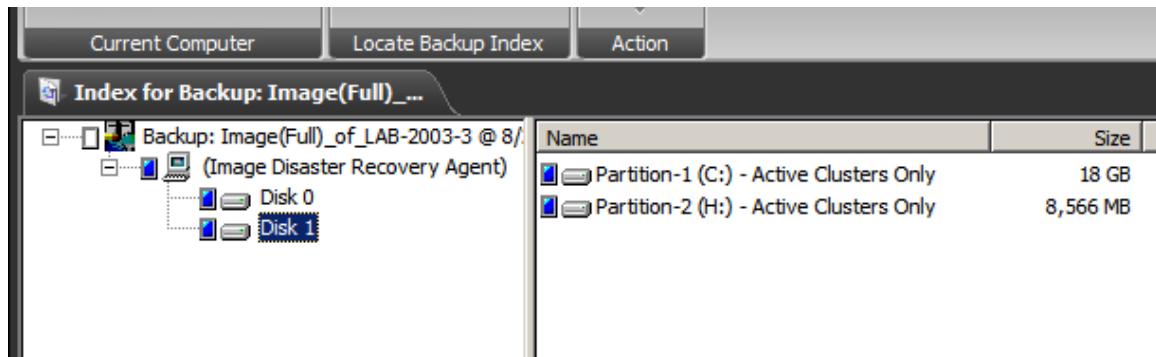
Fig. 15 - Loaded backup index in the file viewer.

Index Properties

The Index Properties option shows additional information about the original disk from the system backed up. To access this information, click the "Set Properties" button from the UltraBac Set toolbar.
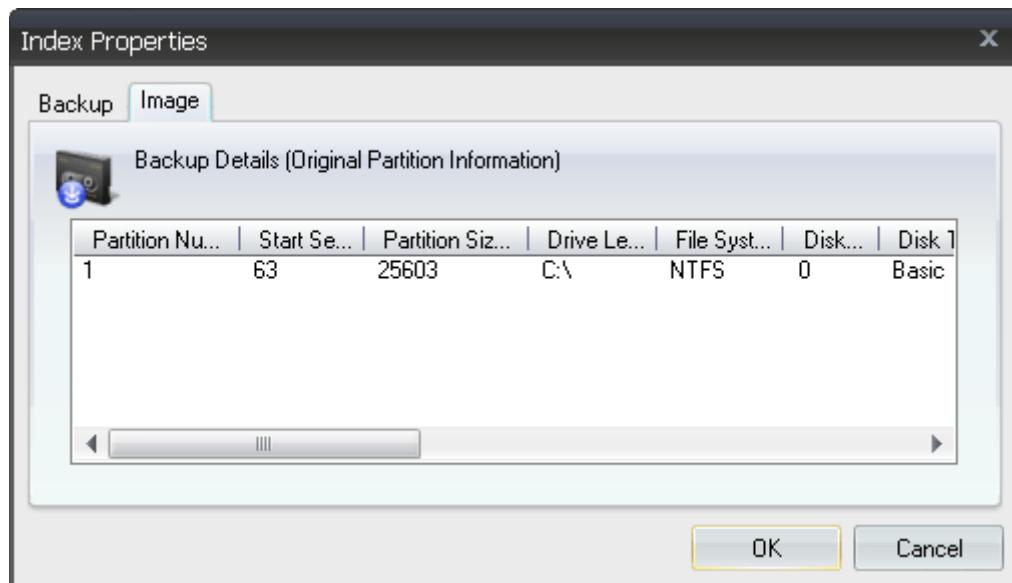
Fig. 16 - Set properties and original disk information.

The following information is contained in the Index Properties for each partition backed up:

- Partition Number
- Start Sector
- Partition Size
- Drive Letter
- File System
- Volume Label

- Disk Number
- Disk Type
- Sectors/Track
- Cylinders
- Heads
- Sectors per Cluster
- Bytes per Sector
- Free Clusters
- Total Clusters

Image Restore Options

The Image Agent restore options allow the selected partition(s) to be restored to specified target partitions, marked as active, resized, and other additional operations. These options can be used in combination to allow a system to be restored to a different hardware platform or even a virtual platform.
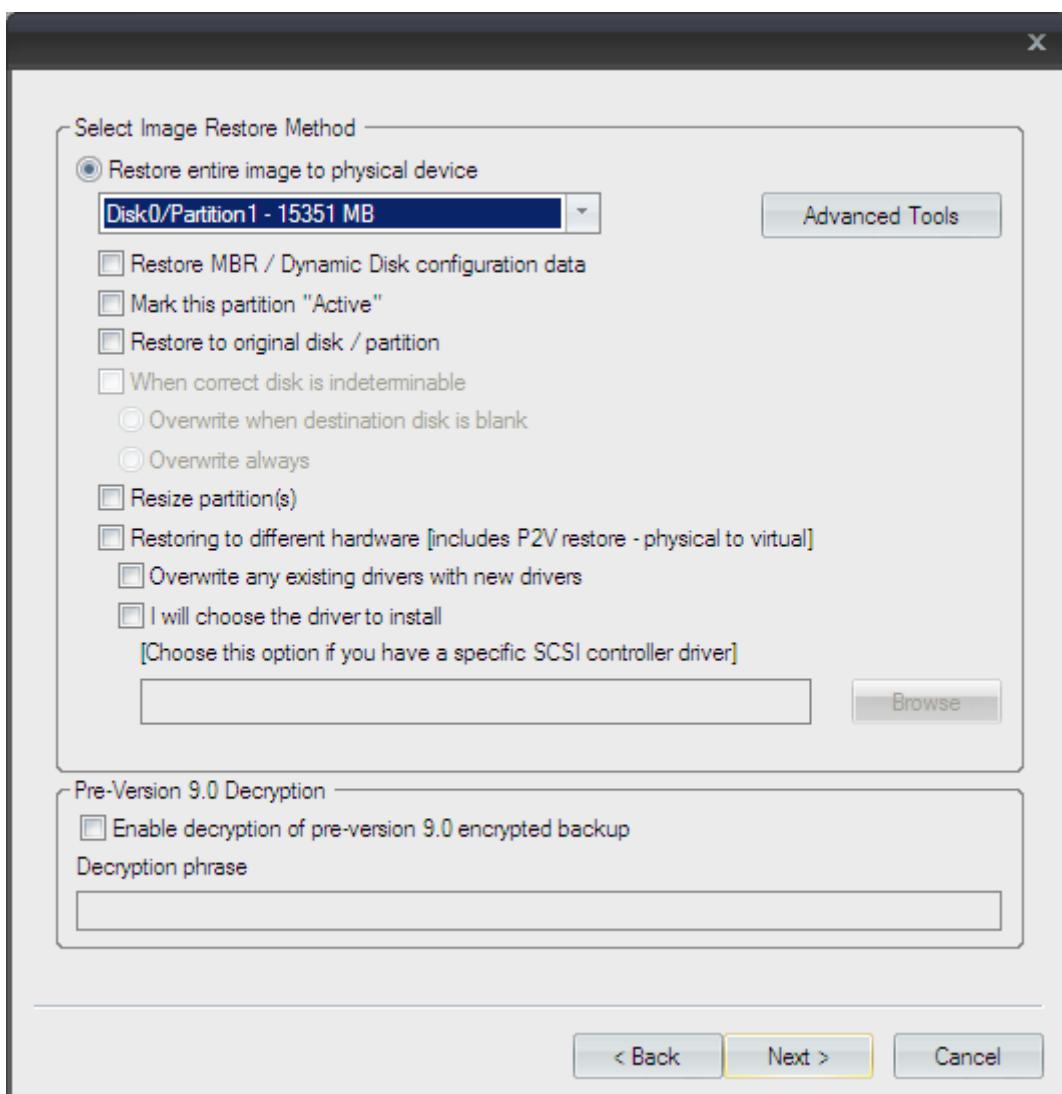
Fig. 17 - Image restore options.

> NOTE: When selecting the restore options, some options may be mandatory and some may be unavailable.

- Restore entire image to physical device – This drop-down menu lists all target partitions available for restore.
- Restore MBR / Dynamic Disk configuration data – Forces the restore of the Master Boot Record or the Dynamic Disk configuration table. If no partitions exist on the restore target disk, this can be used to quickly configure the disk to match the original partition configuration.
- Mark this partition Active – Used when restoring the OS partition to a user-created partition; this will signify that the restored partition is the OS partition.
- Restore to original disk / partition – Instructs the restore to write the selected image to the original disk location (i.e. Disk0/Partition1, Disk0/Partition2). This option must be used when restoring multiple partitions. Enabling this option also enables the following options:
    - Restore MBR / Dynamic Disk configuration data.
    - When correct disk is indeterminable:
        - Overwrite when blank – Overwrite the target disk only if that disk has no disk signature.
        - Overwrite always – Overwrite the target disk, regardless of existing data.
- Resize partition(s) – Used when restoring to a larger partition, this option allows the restored partition to use the full amount of space in the target partition. This option cannot be used when restoring multiple partitions.
- Restoring to different hardware – Instructs UBDR Gold to update the OS partition after restore, to allow the image to be restored to a different physical or virtual system.
    - Overwrite any existing drivers with new drivers – Forces the use of the selected drivers by overwriting any existing drivers of the same name on the target partition.
    - I will choose the driver to install – Allows a driver to be used during the restore process that is not contained on the UBDR Gold CD.
- Pre-Version 9.0 Decryption
    - Enable decryption of pre-version 9.0 encrypted backup – Allows UBDR to restore backup sets that were encrypted using the Blowfish algorithm.
    - Decryption phrase – Use this field to enter the Blowfish decryption phrase.

> NOTE: When restoring from backup data hosted on a locally attached USB hard drive, "Overwrite when destination disk is blank" should ALWAYS be used, or the backup data may be overwritten.

Advanced Tools
The Advanced Tools allow users to create and delete partitions from any basic disk in the system, while booted into UBDR. This can be used to create larger partitions on a new disk, to remove unwanted partitions, or to make other layout changes to the system before restoring data.
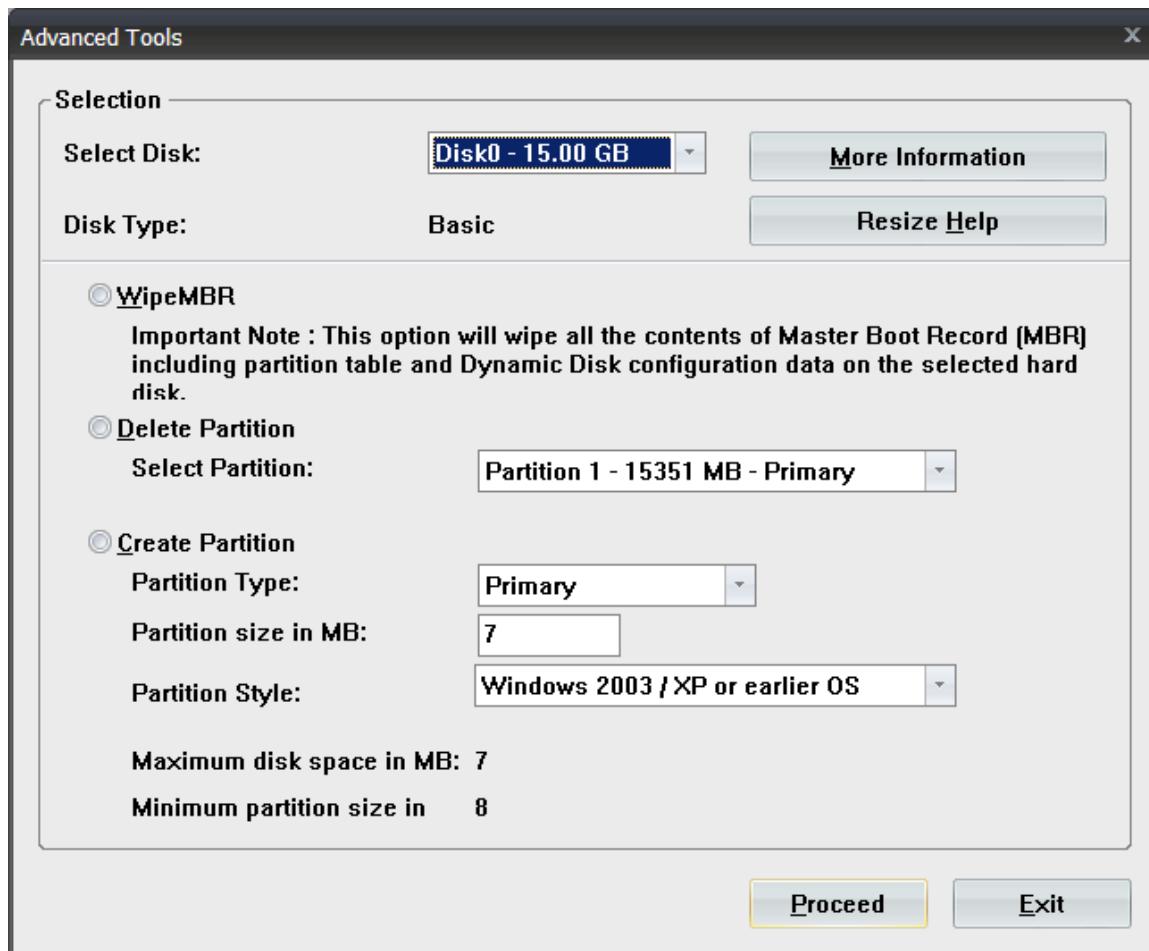
Fig. 18 - Advanced Tools options.

- Select Disk – This drop-down menu allows the selection of all disks in the system for viewing in the "Advanced Tools" screen.
- WipeMBR – This option will delete the Master Boot Record (including all partition information) on the selected disk.
- Delete Partition – This option allows one partition to be deleted via drop-down menu.
- Create Partition – This allows users to create a partition on the selected disk.
  - Partition type - This option allows the creation of one partition, either Primary, Extended, or Logical.
  - Partition size in MB – Specifies the size of the partition to be created.
  - Partition Style:
    - Windows 2003 / XP or earlier OS – Sets the partition's starting sector at 63.
    - Windows 2008 / Vista or later OS – Sets the partition's starting sector at 2048.
  - Maximum disk space in MB – Specifies the available space on disk.
  - Minimum partition size in MB – Specifies the maximum size available for a partition.

After manually creating a partition, ensure the partition has been successfully created by checking the Select Partition drop-down menu on the "Select Image Restore Method" dialog. It may be necessary to create a partition up to 8MB smaller than the available space in order for the partition to actually be created.

More Information
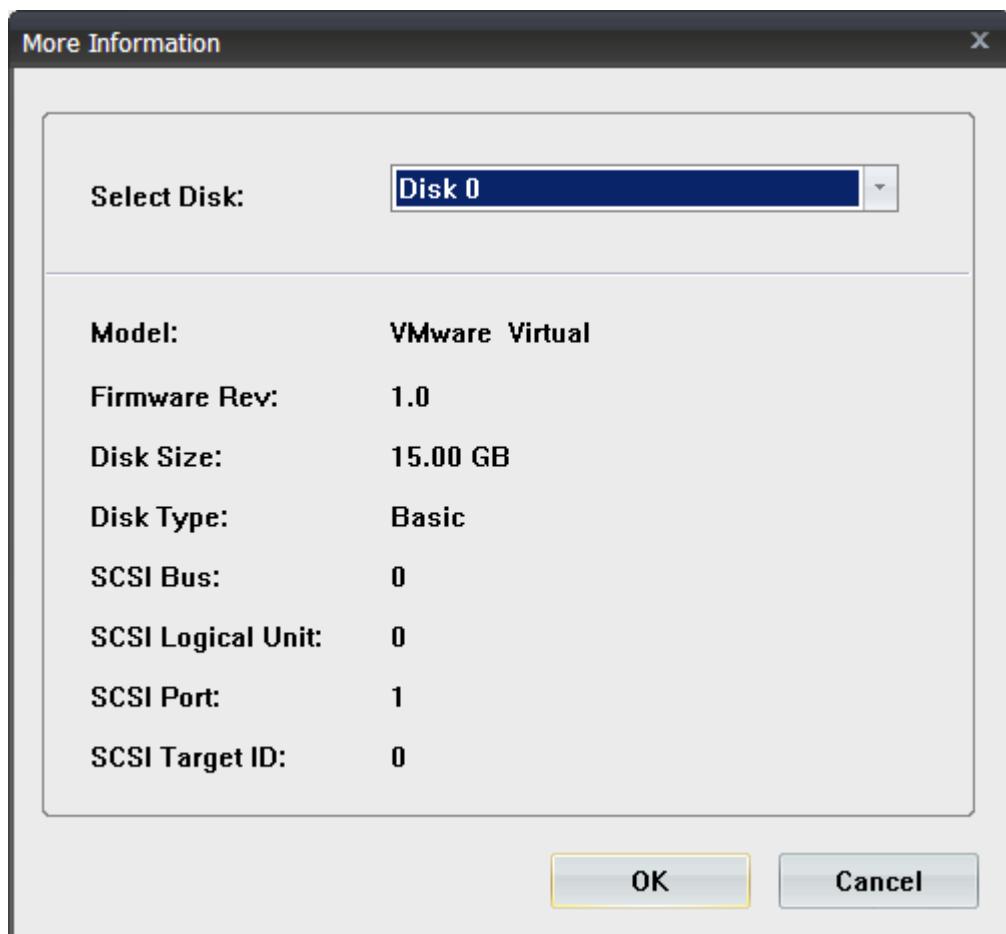
Fig. 19 - Additional information on the disk layout.

The "More Information" option allows the following disk information to be viewed:

- Model
- Firmware Revision
- Disk Size
- Disk Type
- SCSI Bus Number
- SCSI Logical Unit ID
- SCSI Port
- SCSI Target ID

Clicking "OK" or "Cancel" will close the "More Information" screen.

Restoring the OS to the Original Server

There are several common scenarios for doing an Image restore, each requiring different options to be set. These include:
- Restoring to the original disk(s).
- Restoring to a new partition/disk/array of the same size.

- Restoring to a new partition/disk/array of a larger size.

Many of these options will require the de-selection of partitions prior to restore. To enter the file selection screen, click the "Cancel" button in the "Restore Options" screen.

Restoring to the Original Disk(s)

When restoring to the original disk(s), the following options should be selected:
- Restore entire image to physical device.
- Restore to original disk / partition.
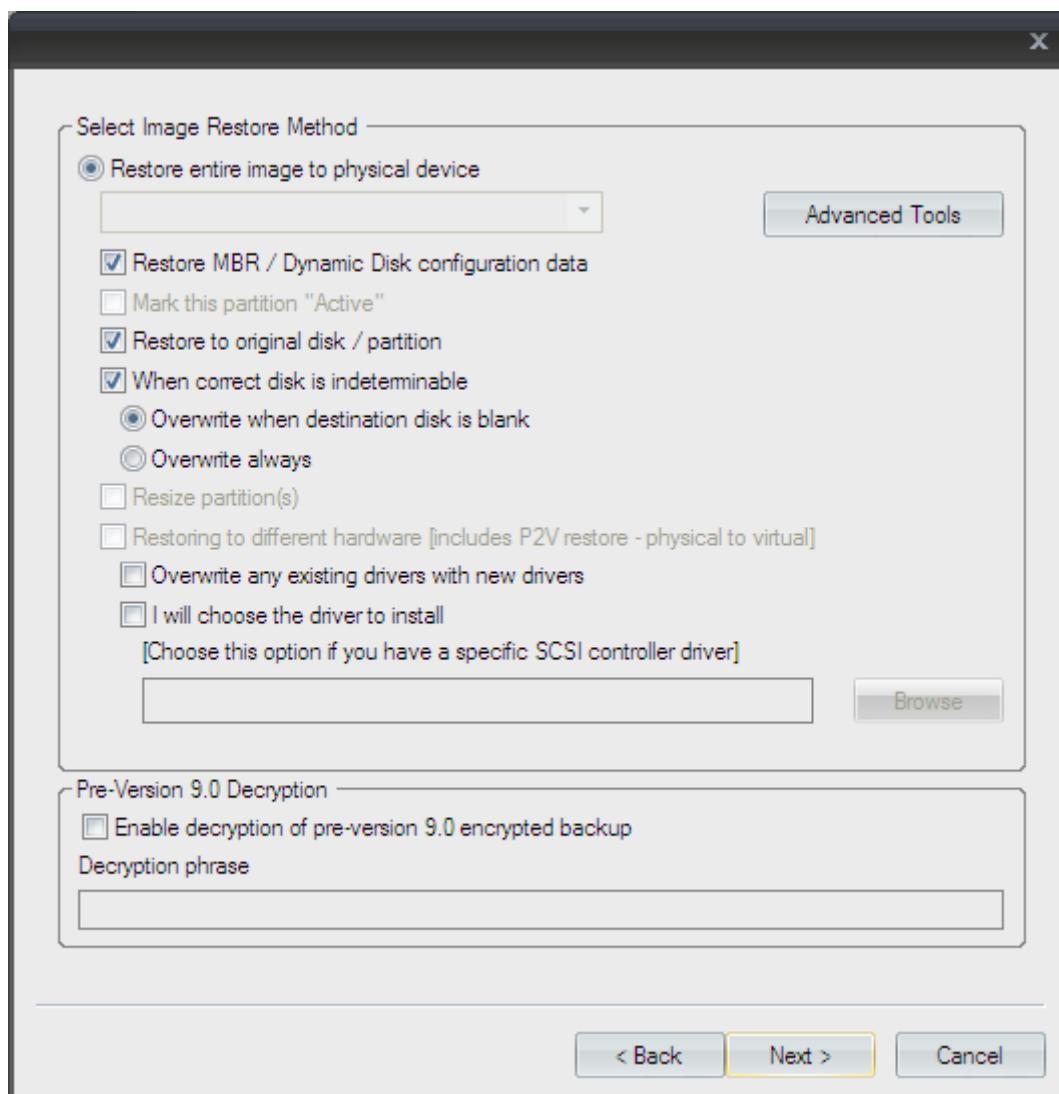
Fig. 20 - Options used when restoring to the original system.

If all partitions are still on the target disk(s), it is not necessary to restore the MBR.

Restoring the OS to a New Partition/Disk/Array of the Same Size as Original

When restoring to a new partition/disk/array of the same size as the original disk, select these options:

- Restore entire image to physical device.
- Restore MBR / Dynamic Disk configuration data.
- Restore to original disk / partition.
- Partition selection drop-down box will be grayed out.

Restoring the OS to a New Partition/Disk/Array Larger than the Original

When restoring to a larger partition/disk/array, only one partition can be restored per restore operation. It is necessary to manually create the larger partition(s) if the partitions do not currently exist on the target disk.

The 'Mark this partition "Active"' option should ONLY be selected when restoring the OS partition:
- Restore entire image to physical device.
- From the drop-down menu select the restore target partition.
- Mark this partition as "Active" (only when restoring the OS partition).
- Resize partitions.

Restoring the Partition

Once the options are set, the image can be restored:
1. Click "Next" to finalize the restore options.
2. Click "Restore" to start the restore process.
3. Reboot the server when the restore is complete.

Restoring the OS to a New Partition/Disk/Array Smaller than the Original

NOTE: This operation supports the NTFS file system only. Also, Windows 2000/NT4 OS partitions cannot be restored to smaller partitions.

When restoring to a smaller partition/disk/array, only one partition can be restored per restore operation. It is necessary to manually create the new partition(s) if the partitions do not currently exist on the target disk.

NOTE: When restoring to a smaller partition, it is recommended that the target partition be at least 60% of the original partition size.

The 'Mark this partition "Active"' option should ONLY be selected when restoring the OS partition:
- Restore entire image to physical device.
- From the drop-down menu select the restore target partition.
- Mark this partition as "Active" (only when restoring the OS partition).
- Resize partitions.

Restoring the Partition

Once the options are set, the image can be restored:
1. Click "Next" to finalize the restore options.
2. Click "Restore" to start the restore process.
3. Reboot the server when the restore is complete.

NOTE: In rare cases, when restoring to a smaller partition the resize operation can take as long as an hour. Canceling the restore operation during this time may make the partition unreadable. Running a defragmentation operation before backup will greatly reduce the amount of time needed for the resize operation to complete.

Restoring the OS to an Alternate Physical Server

Before restoring any partitions, the system disk will need to be partitioned. This can be accomplished by either restoring the Master Boot Record or by creating the partitions manually with the Advanced Tools.

Restoring the Master Boot Record

To restore the MBR:
1. Select the OS partition by marking the box directly to the left in blue.
2. Click "Action"/"Restore this Backup."
3. Select the target disk from the drop-down menu.
4. Check "Restore MBR / Dynamic Disk configuration data."
5. Click "Next."
6. Click "Restore."

Restoring OS Partition

After partitioning the disk, the OS partition should be restored. When restoring the OS partition, the following process should be used:
1. Select the OS partition by marking the box directly to the left in blue.
2. Click Click "Action"/"Restore this Backup."
3. Select the restore target partition from the drop-down menu.
4. Check the following options:
    o Restoring to different hardware.
    o If the target partition was manually created, check 'Mark this partition "Active"'.
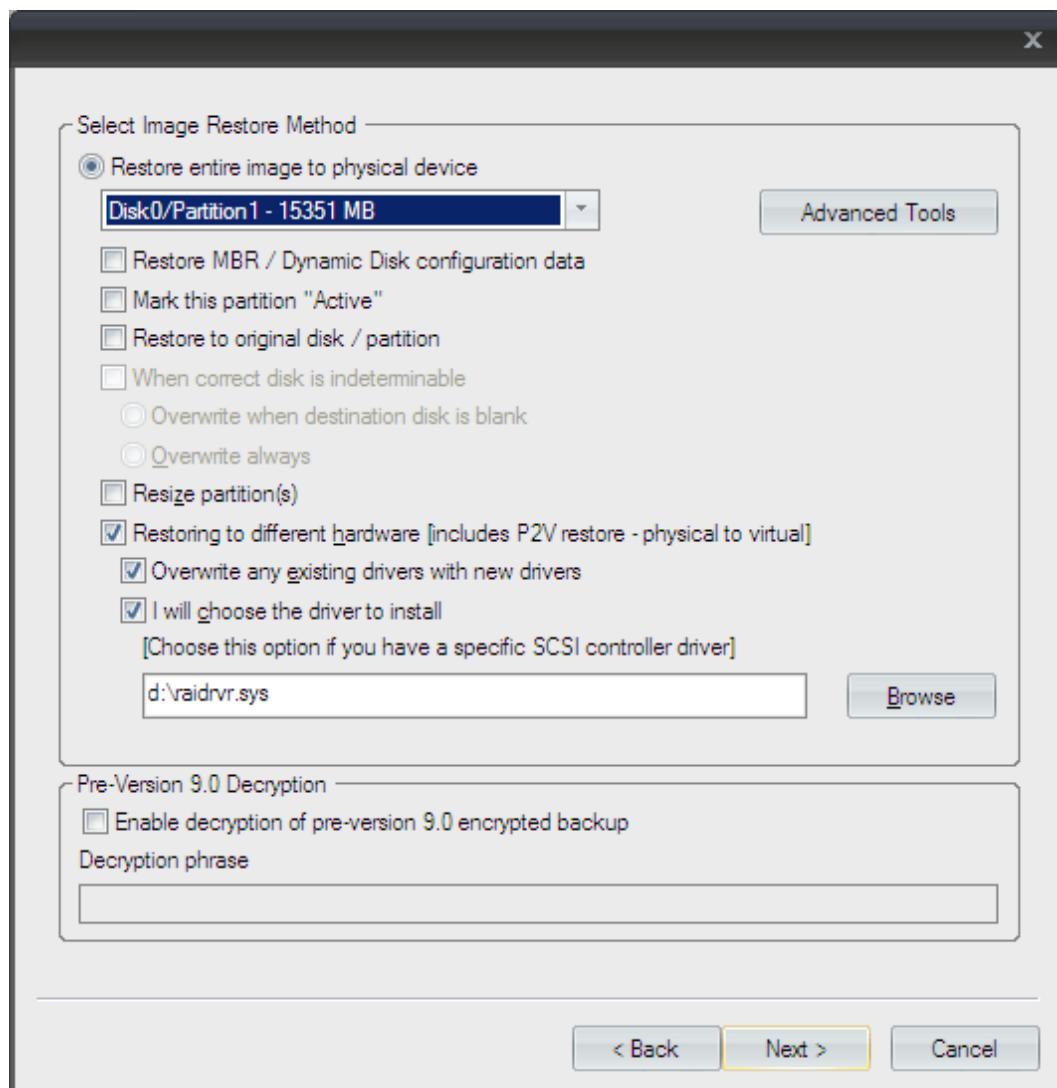
Fig. 21 - Restoring to dissimilar hardware.

    5.   Click "Next."
    6.   Click "Restore."
    7.   If only the OS partition is being restored, reboot the system.

Restoring Data Partition(s)

When restoring data partitions, all data partitions can be restored in one restore operation only if the Master Boot Record has been restored. Do not check "Restoring to different hardware" when restoring a data partition.

    1.   Select the partitions to be restored by marking the boxes directly to the left in blue.
    2.   Click "Action"/"Restore this Backup."
    3.   Check the following options:
         •   Restore entire image to physical device.
         •   If the Master Boot Record was restored, check "Restore to original disk / partition."
         •   Overwrite always.
    4.   Click "Next."
    5.   Click "Restore."

6.   Reboot the system when the restore is complete.

Before restoring any partitions, the virtual disk will need to be partitioned. This can be accomplished by either restoring the Master Boot Record or by creating the partitions manually with the Advanced Tools.
Restoring the Master Boot Record
To restore the MBR:

1.   Select the OS partition by marking the box directly to the left in blue.
2.   Click "Action"/"Restore this Backup."
3.   Check "Restore MBR / Dynamic Disk configuration data."
4.   Click "Next".
5.   Click "Restore."

```
Restore To Path: Disk0 - MBR Restore only - 20473 MB
MBR/Dynamic Disk configuration data restore completed successfully for Disk 0.


RESTORE SUMMARY:
Begin: 4/4/2007 4:50:09 PM
End:   4/4/2007 4:50:16 PM
Duration: (00:00:06)  Rate: (16.67 KB/Sec   0.98 MB/Min  58.59 MB/Hour)
Media Capacity: 558.917 GB
Media Remaining: 17.318 GB
0 Errors and 0 Warnings.
0 Partitions Completed/1 Partition Selected.
1 Disk Completed/1 Disk Selected.
100.14 KB Completed/2138.61 MB Selected.



END OF LOG
```

Fig. 22 - Successful MBR Restore log.
Restoring the OS Partition
After partitioning the disk, the OS partition should be restored. When restoring the OS partition, the following process should be used:
1.   Select the OS partition by marking the box directly to the left in blue.
2.   Click "Action"/"Restore this Backup."
3.   Select the restore target partition from the drop-down menu.
4.   Check the following options:
     o   Restoring to different hardware.
     o   If the target partition was manually created, check "Mark this partition Active."
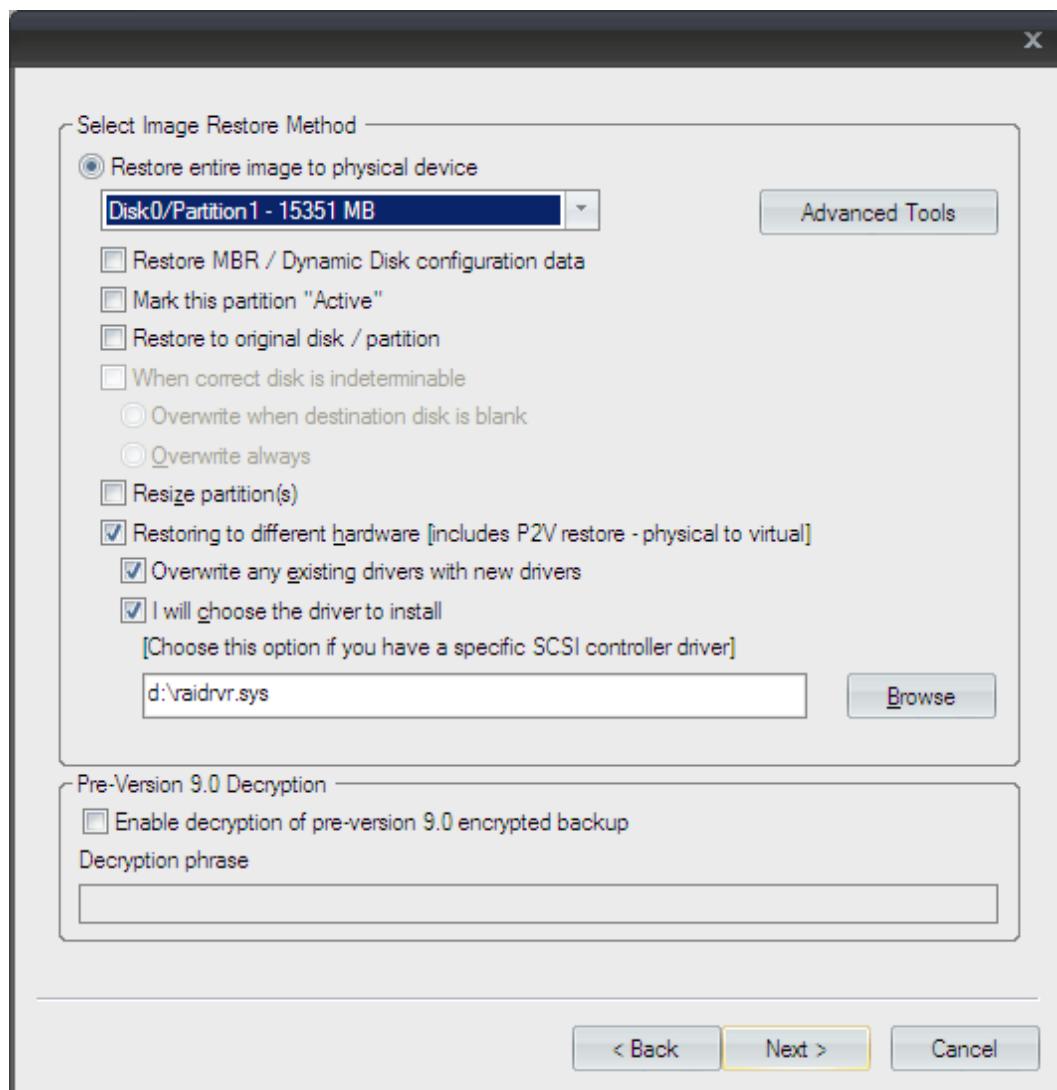
Fig. 23 - Restoring to a virtual server.

5. Click "Next"
6. Click "Restore."

If only the OS partition is being restored, reboot the system.

Restoring Data Partition(s)

When restoring data partitions, all data partitions can be restored in one restore operation only if the Master Boot Record has been restored. Do not check Restoring to different hardware when restoring a data partition.

1. Select the partitions to be restored from the loaded backup index by marking the boxes directly to the left in blue.
2. Click Click "Action"/"Restore this Backup."
3. Select the restore target partition from the drop-down menu.
4. Check "Restore entire image to physical device."
5. If the Master Boot Record was restored, check "Restore to original disk / partition."
6. Check "Overwrite always."
7. Click "Next."
8. Click "Restore."

Reboot the system when the restore is complete.

Restoring a CIP Image Using UBDR Gold

If the CIP monitoring ended before completion, it will be necessary to rebuild the index of the media before restore.

To rebuild the index of the media:

1. Click "Select"/"Storage Devices" and ensure the device used for backup is selected.
2. From the Tools tab, select "Media"/"Rebuild Index from Media."
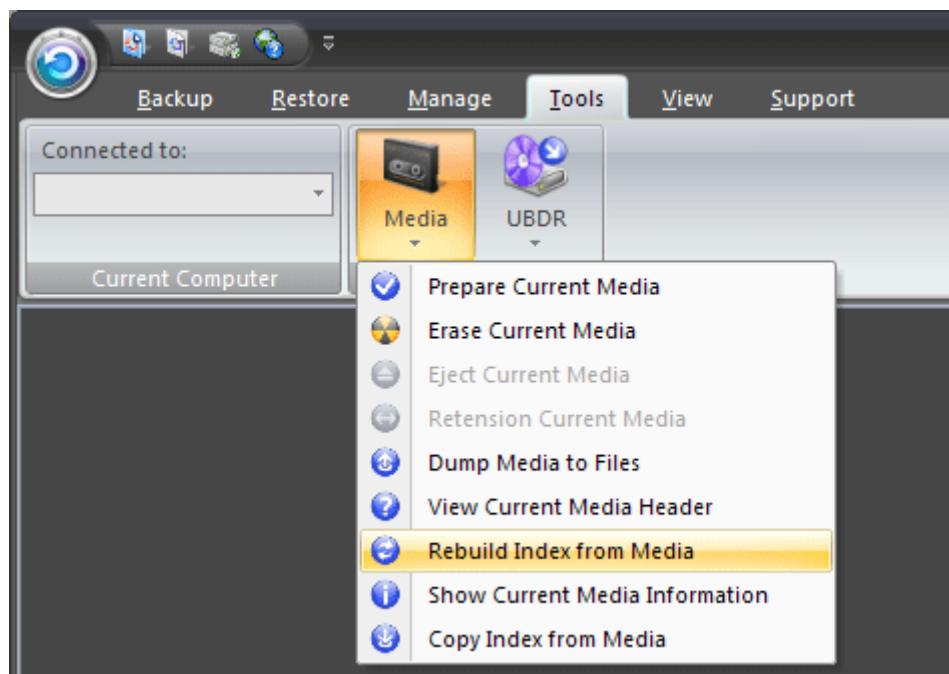
Fig. 24 - Rebuilding the CIP index.

To begin the restore process:

1. From the Restore tab, click "Online."
2. Select and load the recovered index for restore.
3. Select the partition for restore.
4. Click "Operations"/"Restore Selected Files."
5. Click the "Restore entire image to physical device" radio button, select the restore target partition from the drop-down menu, and click "CIP Options."
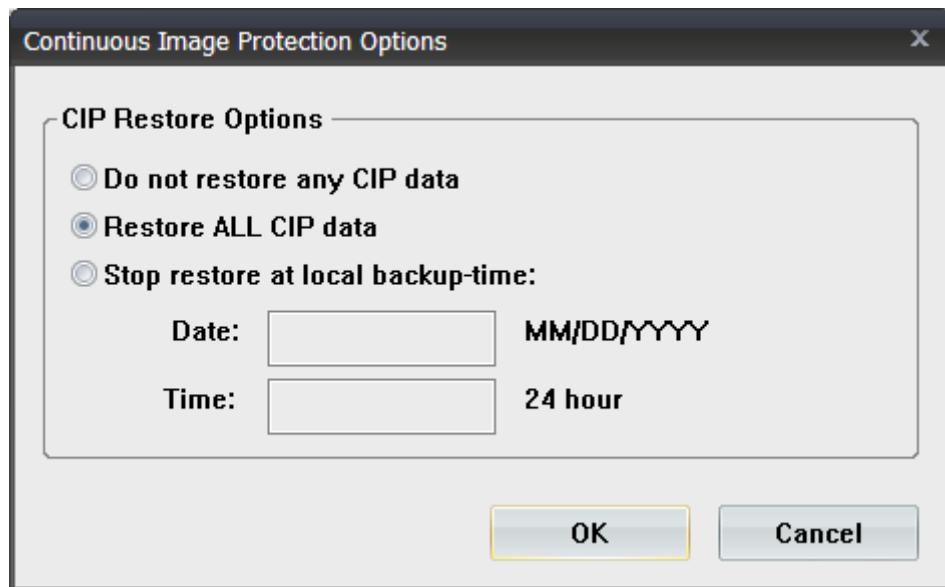
Fig. 25 - Continuous Image Protection restore options.

6. Set the CIP restore options, and click "OK."
7. Click "Next."
8. Check "Run Unattended," and click "Restore."
9. After the restore completes, reboot the system.

Advanced Tools

UBDR has several advanced utilities to assist in troubleshooting, and to simplify the addition of hardware and drivers to the active UBDR booted system.
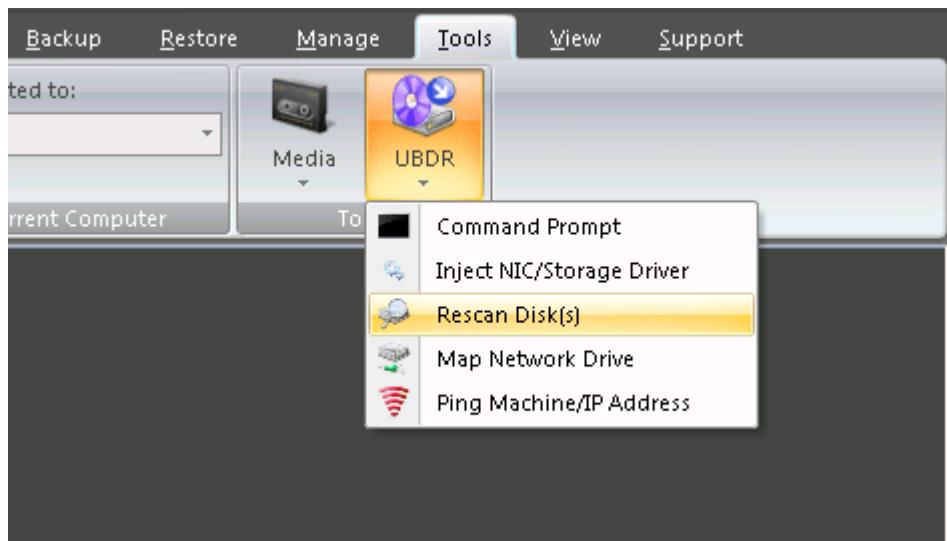
Fig. 26 - Additional UBDR tools.

- Command Prompt – Opens the standard Windows Command Prompt.
- Inject NIC/Storage Driver – Allows a NIC or device driver to be added to the active system without reboot.

- Rescan Disk(s) – Rescans the system disks allowing a newly attached disk to be used as either storage media or a restore target.
- Map Network Drive – Maps a network path as a drive letter.
- Ping Machine/IP Address – Pings a remote system via Network Name or IP Address.

Command Prompt

Fig. 27 - Windows Command Prompt, running DiskPart.exe.

Inject NIC/Storage Driver
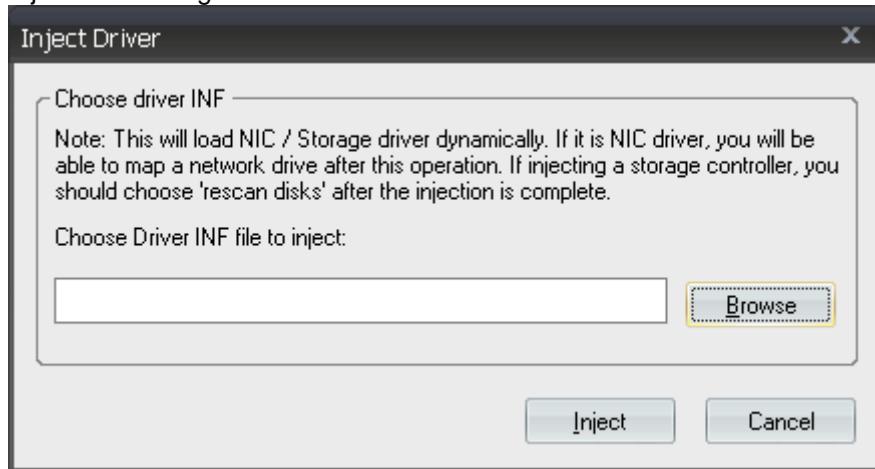
Fig. 28 - Injecting a driver into UBDR.

If the system being used as a restore target does not have the proper NIC or storage driver automatically available, this option allows users to specify a driver for that hardware without needing to reboot the system. To inject a driver:
1. From the Tools menu, select "UBDR"/"Inject NIC/Storage Driver."
2. Type or browse to the location of the driver's INF file.
3. Click "Inject."
4. Close the UltraBac Management Console.
5. When prompted to reboot, click "No."

When the Network screen opens, the newly injected driver will be loaded and ready for use.

Rescan Disks

After attaching a plug-and-play disk to a system (USB, VMDK, VHD), clicking "Rescan Disks" will force UBDR to re-scan the system for the newly added disks without the need to reboot.
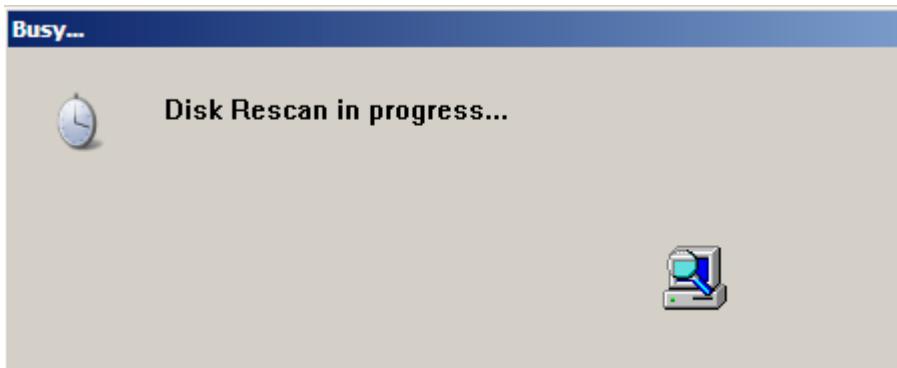
Fig. 29 - Re-scanning the system for newly added disks.

Map Network Drive

UltraBac has the ability to map a network path as a drive letter through the UBDR Management Console. This mapped drive letter can be used as a storage device, log path, index path, or as a driver location.
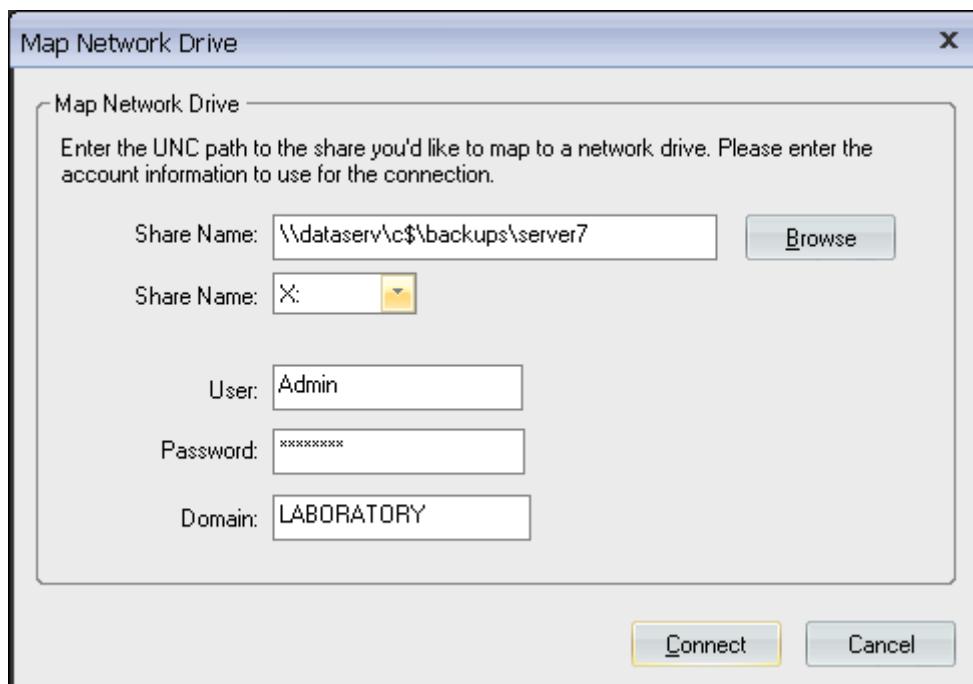
Fig. 30 - Mapping a network drive.

To map a network drive:
1. From the Tools tab, select "UBDR"/"Map Network Drive."
2. In the "Share Name" field, type or browse to a UNC path.
3. From the "Share Name" menu, select the letter to use for the mapped drive.
4. In the "User" field, type the name of a user that has the necessary permissions to access the UNC path entered above.
5. Enter the password for the user account in the "Password" field.
6. Enter the domain for the user account in the "Domain" field.
7. Click "Connect" to create the mapped drive.

Ping Machine/IP Address

This function can be used to test connectivity via Windows name or IP address.
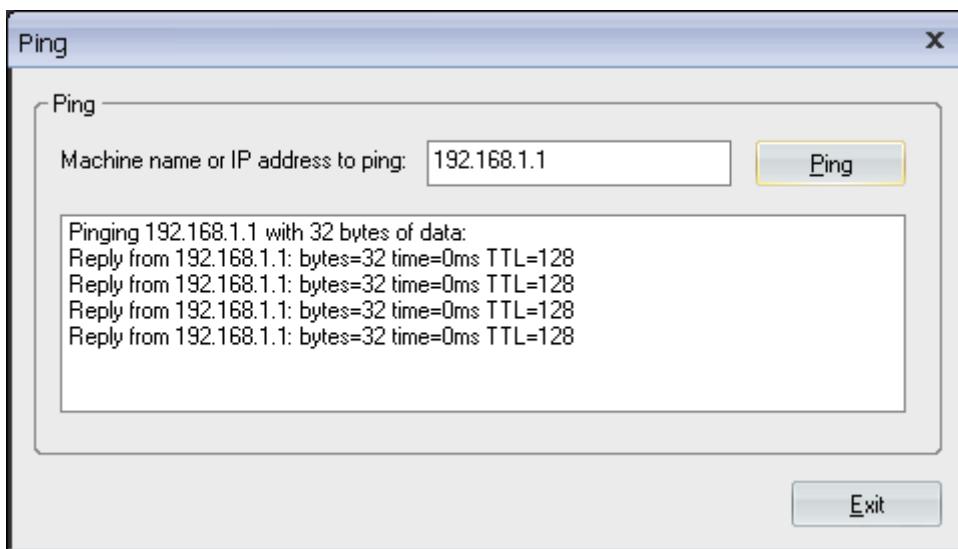
Fig. 31 - Pinging a remote system via IP address.

To ping a remote system:
1. From the Tools tab, select "UBDR"/"Ping Machine/IP Address."
2. Enter the machine name or IP address to ping into the box.
3. Click "Ping."

TROUBLESHOOTING TIPS

Issue: Failed attempting to restore to dissimilar hardware.

Error! 1/13/2006 5:47:56 PM
Failed attempting to restore to dissimilar hardware - unable to find existing registry file at
C:\WINDOWS\system32\config\system, error: 3. See
http://www.ultrabac.com/kb/error.asp?error=2237 for additional information.
Resolution - UBDR is unable to mount the restored volume to updated critical drivers and registry
keys:
1. Wipe the Master Boot Record or delete all existing partitions.
2. Restore the Master Boot Record, or create a target partition manually (using the
    Advanced Tools).
3. Restore the OS partition only with "Restoring to different hardware" checked.

Issue: When browsing to a BackupPath device, UBDR does not show the backup files.

UBDR does not show the backup files in the Browse screen.
Resolution - UBDR file browser does not display UBD files:
1. Browse to the target folder and click "OK."
2. Select "File"/"Load Index For Restore/Verify" to scan the folder for a backup set index.
3. If no sets are found, ensure the correct path is listed in the BackupPath tab, under
    "Select"/"Storage Device."

Issue: System fails to boot after restore.

A system boot failure can show itself in several ways:
*   Flashing/blinking cursor
*   Ntldr failed to load message
*   Blue Screen

Resolution - Run chkdsk to find problems with the target disk:
1. Select the Tools tab, and click "UBDR"/"Command Prompt."
2. Change to the drive letter assigned to the OS partition.
3. Type "chkdsk /f c:" and press "Enter."

Fig. 32 - Running chkdisk from the UBDR command window.

Issue: System fails to boot after restore.

A system boot failure can show itself in several ways:
*   Flashing/blinking cursor
*   Ntldr failed to load message
*   Blue Screen

Resolution - The boot partition may not be marked Active.

To mark the partition as Active while booted into UBDR Gold:
1. Select the Tools tab, and click "UBDR"/"Command Prompt."
2. Type "diskpart" and press "Enter".
3. At the DiskPart prompt, type "select disk <n>" and press "Enter."
4. At the next DiskPart prompt, type "select partition <n>" and press "Enter."
5. Type "active" and press "Enter."

Fig. 33 - DiskPart from the command window.

Issue: System fails to boot after restore.

A system boot failure can show itself in several ways:
*   Flashing/blinking cursor

- Ntldr failed to load message
- Blue Screen

Resolution - The original system disk had an EISA partition and target disk does not have the partition.To fix this problem, edit boot.ini and change the boot partition from 2 to 1:

1. Select the Tools tab, and click "UBDR"/"Command Prompt."
2. Type "notepad" and press "Enter."
3. Click "File"/"Open", and type "c:\boot.ini".
4. Modify the target partition to show 1 instead of 2.
5. Click "File"/"Save".
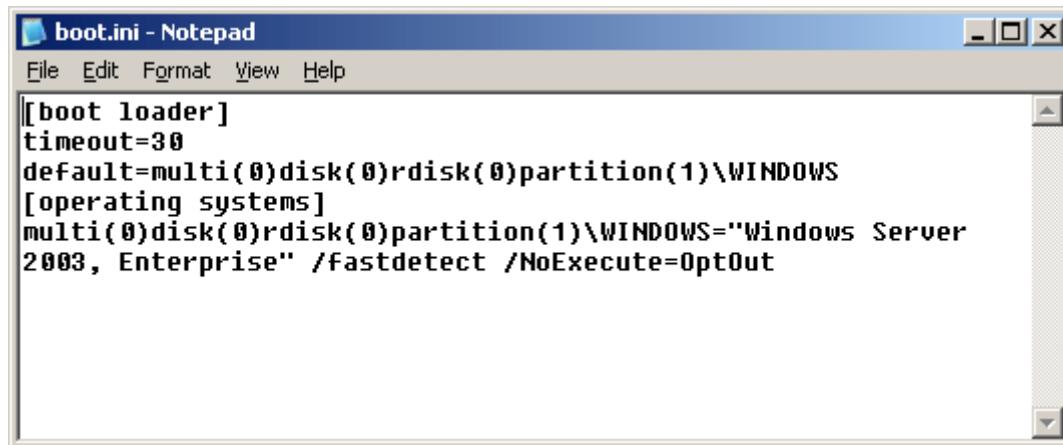
Fig. 3 - Boot.ini in Notepad.

Writing an Image Backup to VHD File

UltraBac has the capability of writing to the native HyperV / Microsoft Virtual Server format. This backup is written to a UNC path, and can be written in parallel with the backup data. When creating a VHD file, UltraBac automatically performs all necessary changes to allow the OS within the file to be directly bootable by a HyperV / Windows Virtual Server. The Virtual Disk Agent is an extra-cost option that can be added on to the standard Image Disaster Recovery Agent.

The VHD file will be written with a filename that corresponds with the system name and number of the disk selected. This filename will not denote the partitions backed up:

<server>_disk<n>.vhd

```
NOTE:  VHD files cannot be created when Continuous Image Protection (CIP) or any
VMDK option is selected.
```

Creating VHD Files

To enable the VHD option in an Image Disaster Recovery Agent backup set:
1. Select the Backup tab from the main UltraBac toolbar.
2. Click "New."
3. Select "Image/Disaster Recovery Agent" and click "Next."
4. Check "Enable backup to Virtual disk file format (VHD or VMDK)"
5. Select "Backup to Microsoft Virtual Hard Disk format - VHD"
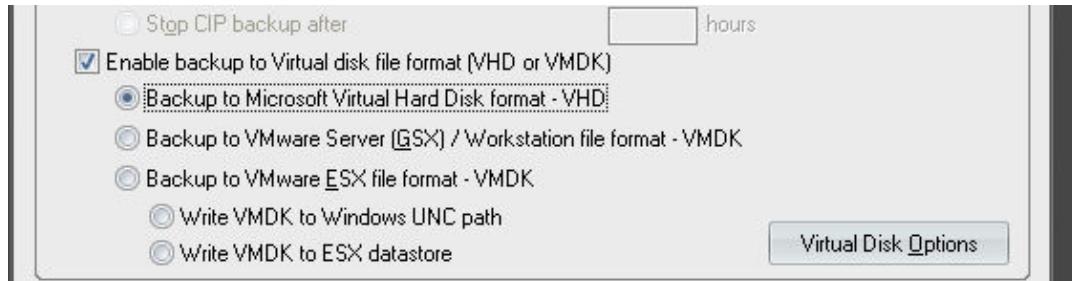
Fig. 1 - Enabling the creation of VHD files.

6. Click "Virtual Disk Options."
7. Enter the UNC path for where the VHD file(s) should be written.
8. Enter Account information for connection to the UNC path.
9. Click "OK."
10. If you do not want UltraBac to write a parallel image backup in its native format, choose the option "Create virtual disk files only".

```
NOTE:  UltraBac will still write a small file to your backup device even if you select the
option "Create virtual disk files only."
```

11. At the "Disaster Recovery/Image Agent Options" screen, click "Next."
12. Enter a description of the data to be backed up, and click "Next."
13. To modify the file selection logic, click "Finish."

```
NOTE:  VHD files do not use AES encryption.
```

Incremental/Differential VHD Files

Incremental/Differential backups will automatically update the VHD files with any incremental or differential changes if both the Full and Differential/Incremental sets have the same VHD output settings.

For further information on Incremental/Differential Image Disaster Recovery Agent backups, please see the UltraBac User Manual:

UltraBac User Manual: Incremental/Differential Backups - Image Agent

Writing an Image Backup to VMDK File

UltraBac has the capability of writing to the native VMware formats, both ESX and GSX. This backup is written to a UNC path, and can be written in parallel with the backup data. When creating a VMDK file, UltraBac automatically performs all necessary changes to allow the OS within the file to be directly bootable by the selected VMware platform. The Virtual Disk Agent is an extra-cost option that can be added on to the standard Image\Disaster Recovery Agent.

The VMDK file will be written with a filename that corresponds with the system name and number of the disk selected. This filename will not denote the partitions backed up:

<server>_disk<n>_<VMware platform>.vmdk

NOTE: VMDK files cannot be created when Continuous Image Protection (CIP) or VHD option is selected.

Creating VMDK Files

To enable the VMDK option in an Image/Disaster Recovery Agent backup set:

1. Select the Backup tab from the main UltraBac toolbar.
2. Click "New."
3. Select "Image/Disaster Recovery Agent" and click "Next."
4. Check "Enable backup to Virtual disk file format (VHD or VMDK)."
5. Select either "Backup to VMware Server (GSX) / Workstation file format - VMDK" or "Backup to VMware ESX file format - VMDK"
    - If "Backup to VMware ESX file format - VMDK" is selected than choose either "Write VMDK to Windows UNC path" or "Write VMDK to ESX datastore.
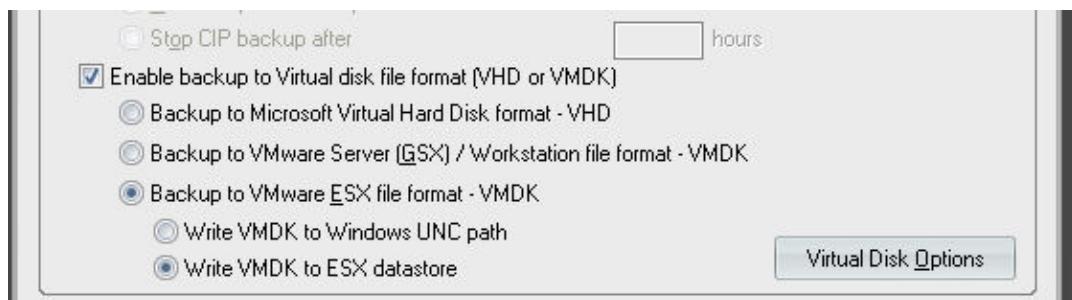
Fig. 1 - Enabling the creation of VMDK files.

6. Click "Virtual Disk Options."
7. Enter the data for where the VMDK file(s) should be written.
8. Click "OK."
9. If you do not want UltraBac to write a parallel image backup in its native format, choose the option "Create virtual disk files only".

NOTE: UltraBac will still write a small file to your backup device even if you select the option "Create virtual disk files only."

---

10. At the "Disaster Recovery/Image Agent Options" screen, click "Next."
11. Enter a description of the data to be backed up, and click "Next."
12. To modify the file selection logic, click "Finish."

NOTE: VMDK files do not use AES encryption.

GSX File Format Options

NOTE: When writing to GSX file format, it is necessary to write to a remote UNC path. A local path cannot be specified.

When creating a backup set that will write a VMDK file in the GSX format, it is necessary to specify a target UNC path in the Virtual Disk Options:

- UNC Path – Enter the UNC path where the VMDK file will be written.
- Create Virtual Disk file(s) only – Allows you to create only the VMDK file and not the UltraBac format backup.
- Optional Account Information – Used when the default UltraBac Account does not have permission to access the target location.
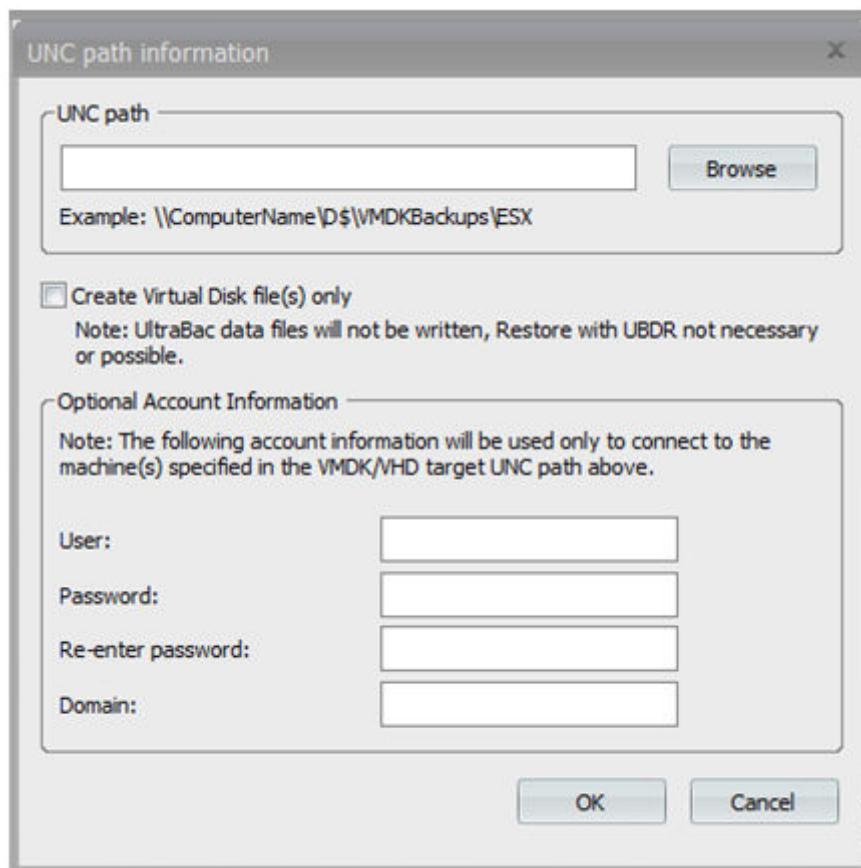
Fig. 2 - Writing to the GSX file format.

ESX File Format Options - Writing to UNC Path

When writing an ESX formatted VMDK file to a UNC path, UltraBac creates a UBMS connection to the target system specified in the UNC path. If UltraBac is not installed on the target system or does not have permission to write to the path specified, the VMDK file will not be created. If the default UltraBac account does not have permission to write to the target system, a secondary account will have to be specified.

NOTE: For more information on creating a secondary UltraBac account, please visit the "**UltraBac Preferences**" section of the User Manual:
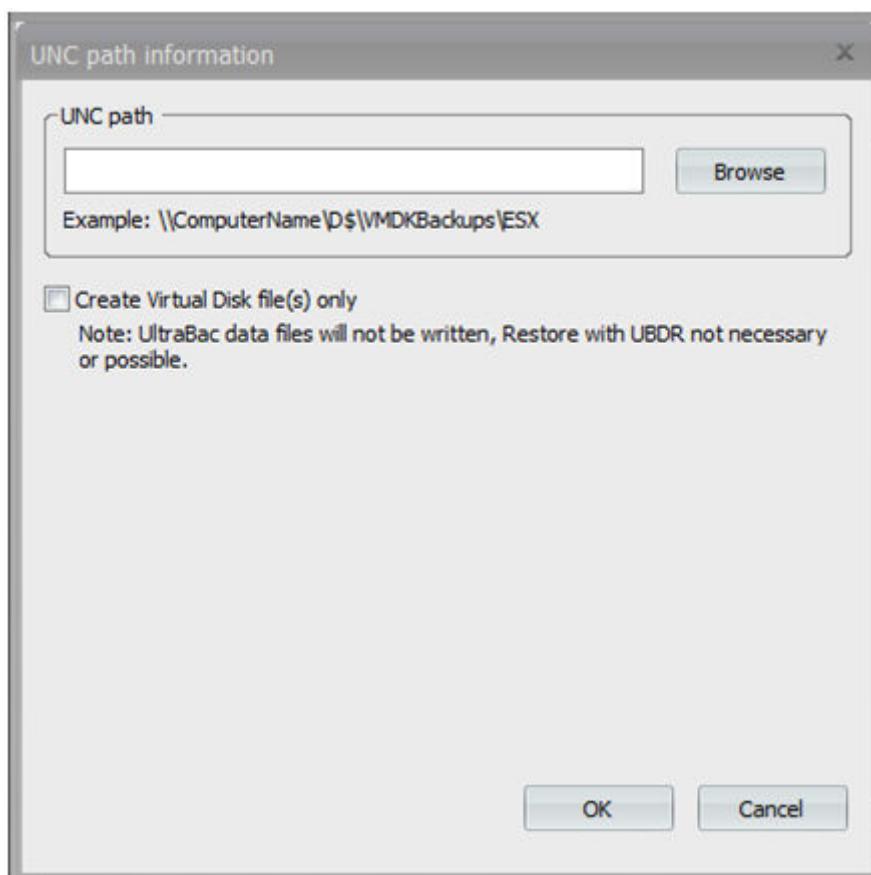
Fig. 3 - Setting the VMDK target path.
ESX File Format Options - Writing to ESX Datastore
When writing to a VMDK file in the ESX format, it in necessary to specify the target location in the Virtual Disk Options:

- ESX Host Name / IP address – Enter the server name or IP address of of the system that hosts the ESX datastore.
- User name – Enter a username that has permission to write to the server's datastore.
- Password – Enter the password for the previously specified account.
- Port – Enter the port number for the server hosting the data store.
- Inventory path of the virtual disk – Specify the server and the data store in brackets as shown in Fig. 4, followed by the directory path.
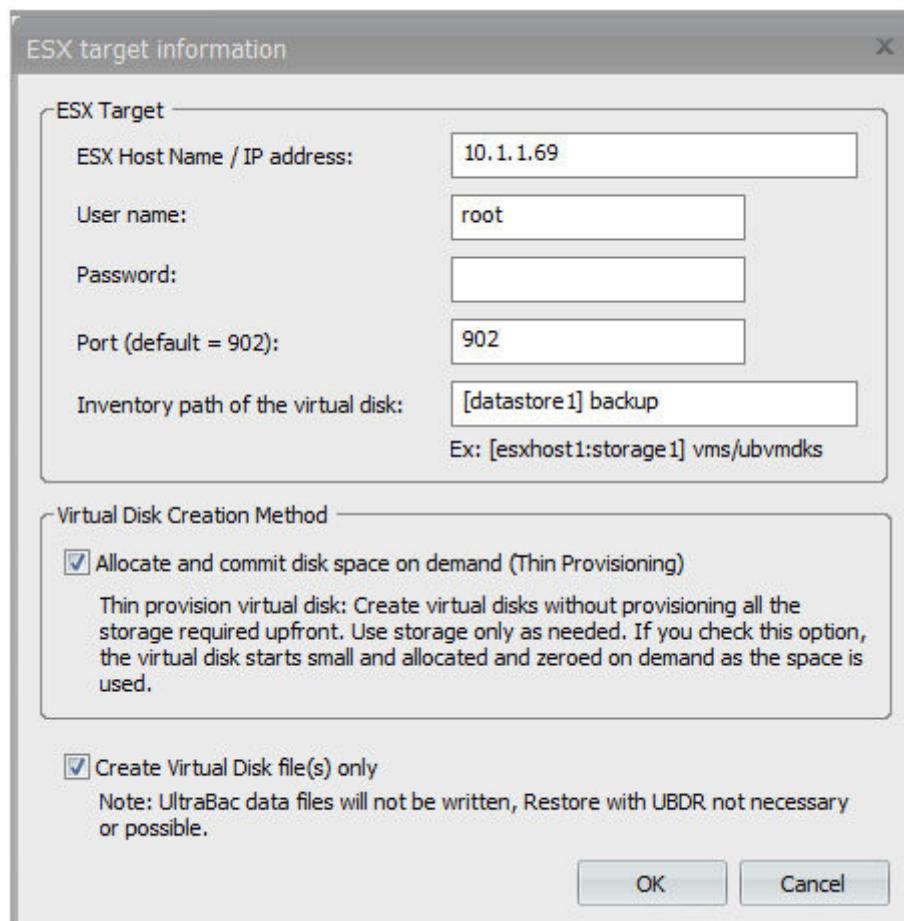
Fig. 4 - ESX output options.

- Virtual Disk Creation Method – This option allows the creation of a virtual disk using thin disk provisioning. Only the used space will be allocated to the VMDK file.
- Create Virtual Disk file(s) – Allows you to create only the VMDK file and not the UltraBac format backup.

NOTE: ESXi versions prior to Version 4.1 require additional licensing from VMware to write directly to the data store.

NOTE: Thin disk provisioning is supported only when writing to ESX 3.5 or greater.

Incremental/Differential VMDK Files

Incremental/Differential backups will automatically update the VMDK files with any incremental or differential changes, if the both the Full and Differential/Incremental sets have the same VMDK output settings.

For further information on Incremental/Differential Image/Disaster Recovery Agent backups, please see the UltraBac User Manual:

UltraBac User Manual: Incremental/Differential Backups - Image Agent

Mounting a VMDK File

After running an image backup with the VMDK option enabled, upload the VMDK file to the datastore for the ESX or GSX server (if necessary). After uploading the VMDK file to the correct location (if necessary) create a new virtual machine on the VMware host, selecting the custom option to use an existing virtual disk and recommended controller for the OS being restored.

For further instructions, please consult VMware's documentation.

Continuous Image Protection

The UltraBac Image Disaster Recovery Agent uses "snapshot" technology to take a sector level backup of a physical disk or partition. The UltraBac Locked File Backup Agent is integrated with the Image Disaster Recovery Agent, ensuring the backup is a complete and consistent snapshot of the selected disk(s). An Image Disaster Recovery Agent backup is used to quickly restore a failed disk or operating system without the need for re-installing the operating system.

After performing an Image Disaster Recovery Agent backup, backing up all active clusters of a partition, UltraBac begins Continuous Image Protection (CIP) monitoring. This process copies all modified sectors to the backup media in near real-time, and allows point-in-time recovery of the partition.

NOTE: After starting a CIP set, subsequent backup sets will not start until the CIP monitoring is complete.

Setup and Configuration

NOTE: To create an image backup of a remote system, the UltraBac Image Disaster Recovery Agent must be installed on the system being imaged. For more information on installing the Image Disaster Recovery Agent, please visit the "**Installing UltraBac**" section of the User Manual:

UltraBac User Manual: Installing UltraBac

Creating a CIP Backup Set

1. Launch the Backup Wizard by selecting the Backup tab and clicking "New."
2. Click "Image Disaster Recovery Agent" to highlight the option, and click "Next."
3. Set the following Image Agent options:
   o Always back up partitions individually.
   o Enable in-use cluster backup for partitions with known filesystems.
   o Enable Differential or Incremental backup.
   o Continuous Image Protection backup (CIP).
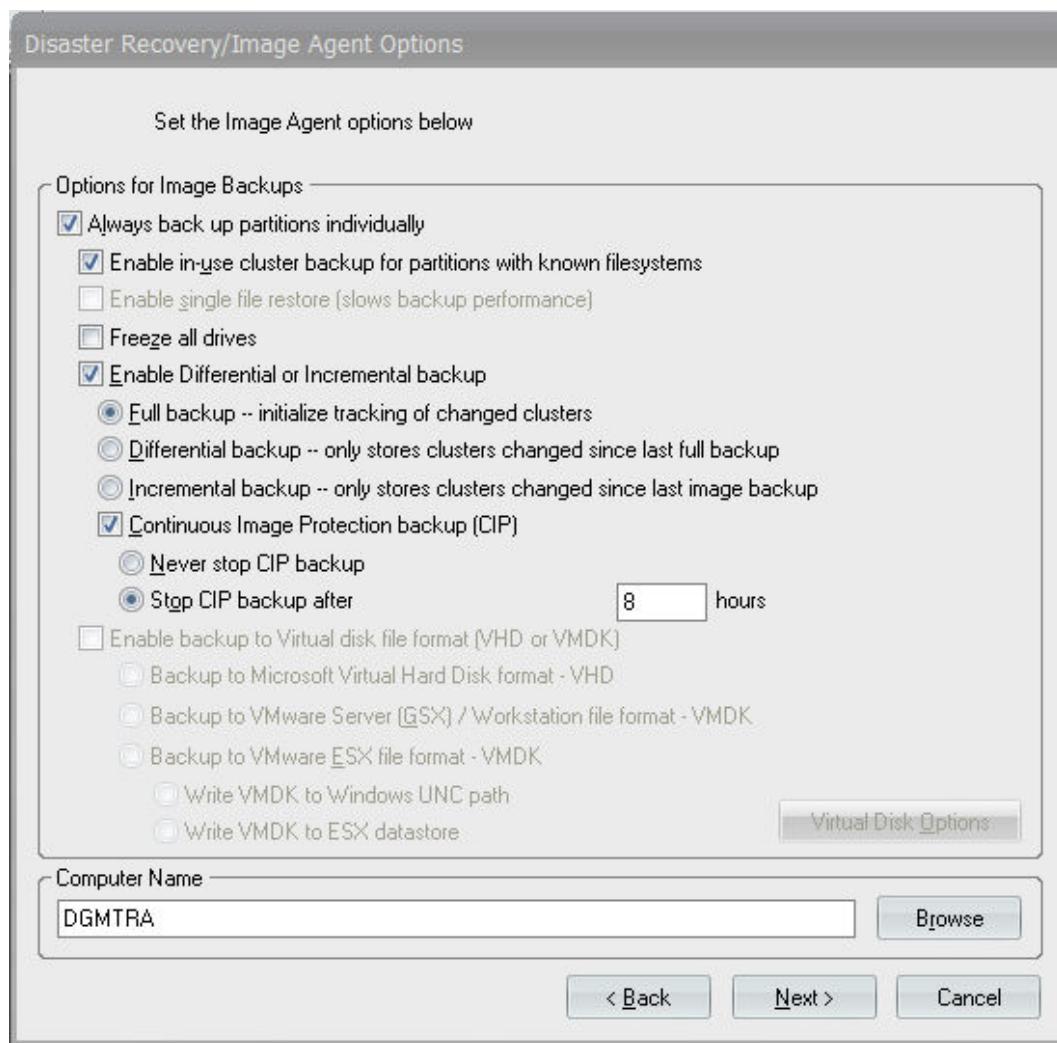
Fig. 1 - Disaster Recovery/Image Agent Options with CIP selected.

4. Set the stop time for the CIP monitoring and click "Next."
5. Type a set description, as it will appear in the backup log, into the "Set Description" field but do not modify the "File Selection Logic" menu. Click "Next."
6. Check "View/Edit files in the backup set" and click "Finish."
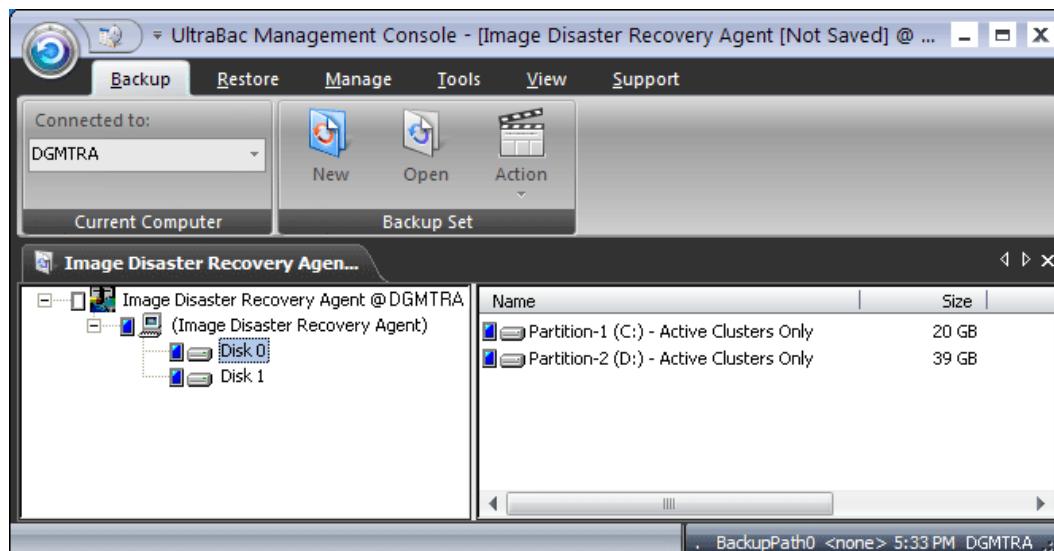
Fig. 2 - Image set loaded in the File Viewer.

7. Select the partition to be backed up.
8. Save the set by clicking "File"/"Save" from the main UltraBac menu.

NOTE: Only one partition can be selected per CIP backup set.
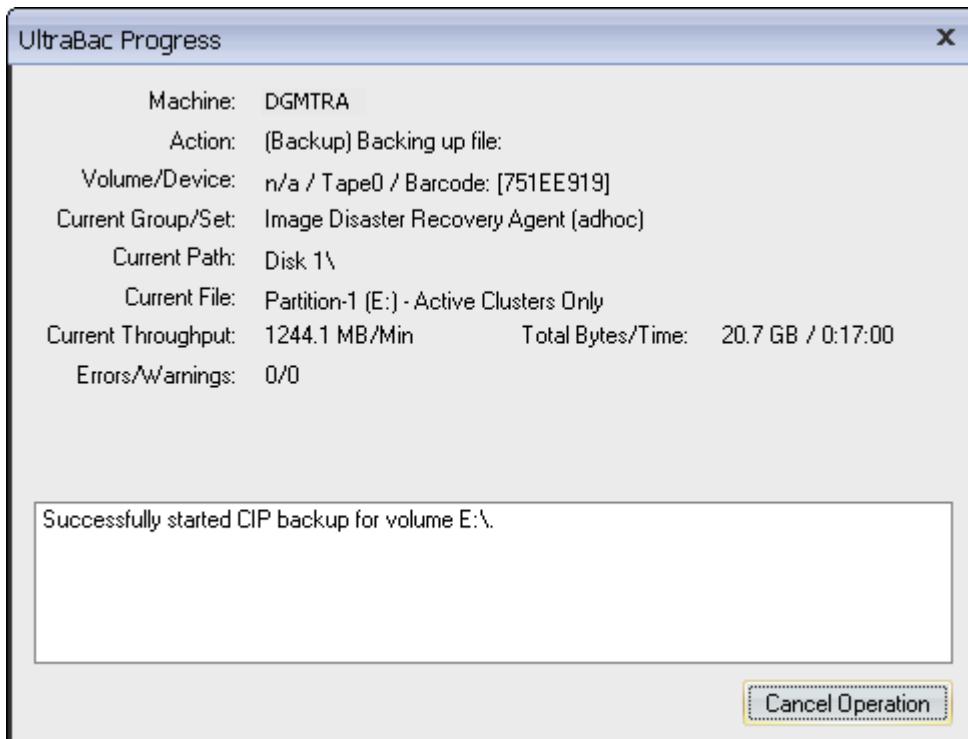
Fig. 3 - CIP monitoring begins after the full image backup is complete.
Image Agent Options Using CIP
Options for CIP backups:

- Always back up partitions individually – Allows partitions to be individually selected. If unchecked, only a full disk can be selected.
- Enable in-use cluster backup for partitions with known file systems – The image set will only back up the in-use clusters on the selected disk or partition, excluding all empty disk space.
- Enable single file restore (slows backup performance) – the Single File Restore option cannot be used during a CIP image backup.
- Freeze all drives – Freeze all drives cannot be used during a CIP image backup.
- Enable Differential or Incremental backup – Enables the tracking of changed clusters and set creation necessary to perform a differential image backup.
  - o Full backup – Backs up the full partition or disk, and clears the ".idx" file used to track disk changes.
  - o Differential backup – Backs up all clusters modified after the last full backup.
  - o Incremental backup – Backs up all clusters modified after the last full or incremental backup.
- Computer Name – Type in or browse to the computer name of the remote system to be backed up.

Restoring a CIP Image Backup

An Image Agent backup using CIP can be restored two ways:

- Partition restore using the UltraBac Management Console.
- Partition or disk restore using UBDR Gold.

NOTE: An active operating system partition cannot be overwritten by an Image restore using the UltraBac Management Console.

Partition Restore using the UltraBac Management Console
A restore of a CIP image through the UltraBac Management Console requires the target partition be prepared before restore by removing the drive letter from the partition. If the CIP monitoring ended before completion, it will be necessary to rebuild the index of the media before restore.

To rebuild the index of the media:

1. Ensure the device used for backup is selected as the current device.
2. Select the Tools tab, and click "Media"/"Rebuild Index from Media"
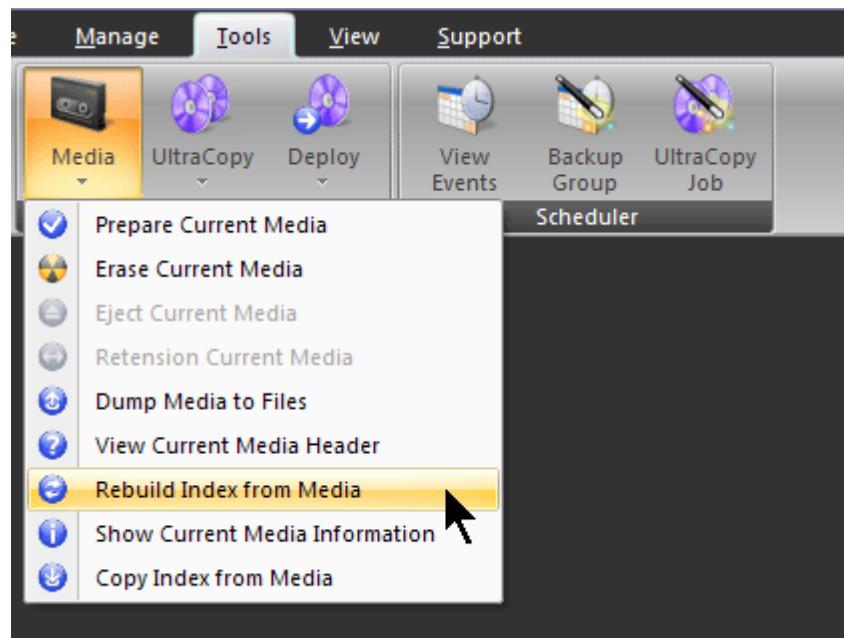
Fig. 4 - Rebuilding the CIP Index.

To begin the restore process:

1. Launch the Restore Wizard by selecting the Restore tab and clicking selecting the source of the backup index.
2. Select and load the index for restore.
3. Select the disk or partition for restore.
4. Click "Action"/"Restore this Backup."
5. Click the "Restore entire image to physical device" radio button, select the restore target partition from the drop-down menu, and click "CIP Options."
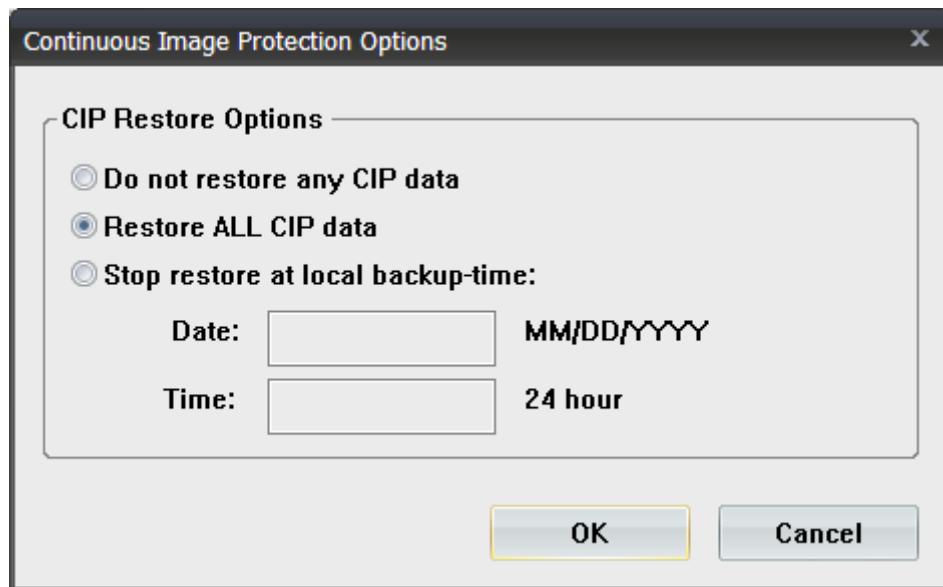
Fig. 5 - Continuous Image Protection options.

6. Set the CIP restore options, and click "OK."
7. Click "Next."
8. Check "Run Unattended," and click "Restore."
9. After the restore completes, reboot the system to activate the restored disk or partition, or manually assign the restored partition a drive letter.

Restoring a CIP Image Using UBDR Gold

NOTE: To restore the CIP data using UBDR Gold, it will be necessary to boot from a UBDR Gold CD/ISO/USB Key. For instructions on preparing a system for restore using UBDR Disaster Recovery media, please visit the "**UBDR Gold v5.0/v60**" section of the User Manual:

UltraBac User Manual: UBDR Gold v5.0/v6.0

If the CIP monitoring ended before completion, it will be necessary to rebuild the index of the media before restore.

To rebuild the index of the media:

1. Click "Select"/"Storage Devices" and ensure the device used for backup is selected.
2. Click "Tools"/"Media"/"Rebuild Indexes."
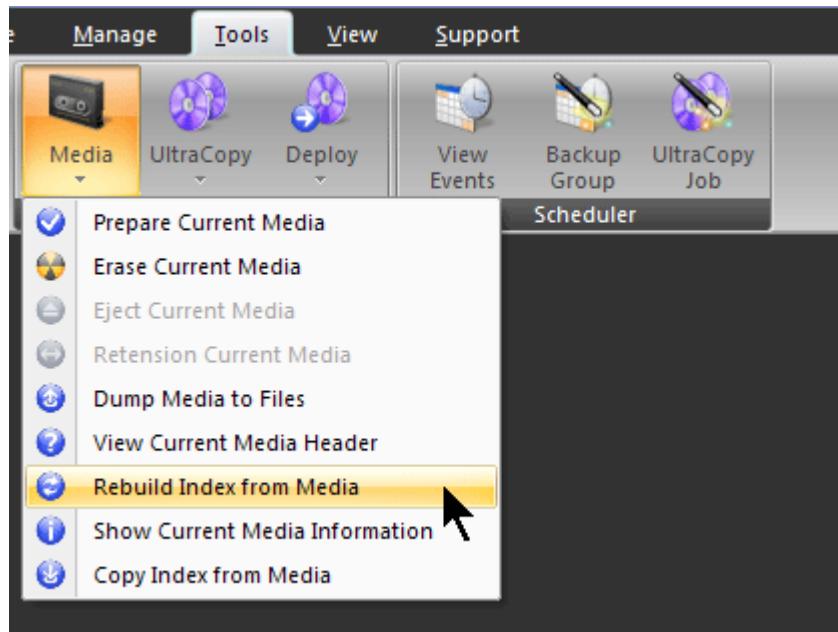
Fig. 6 - Rebuilding the CIP index.

To begin the restore process:

1. Select the Restore tab, and click "Online".
2. Select and load the recovered index for restore.
3. Select the partition for restore.
4. Click "Action"/"Restore this Backup."
5. Click the "Restore entire image to physical device" radio button, select the restore target partition from the drop-down menu, and click "CIP Options."
6. Set the CIP restore options, and click "OK."

153

7. Click "Next."
8. Check "Run Unattended," and click "Restore."
9. After the restore completes, reboot the system.

CIP Strategies and Considerations
There are several important considerations to be aware of while implementing CIP Image backups:

- Only one partition can be backed up per CIP backup set.
- Any backup sets scheduled to run after a CIP backup set (in the same job) will not run until CIP monitoring is complete.
- If a CIP image backup fails to complete or is aborted, it can take several minutes to rebuild the backup index.
- The larger the quantity of data backed up during a CIP set, the longer the index rebuild will take.
- Currently it is not possible to restore a single file out of a CIP set.

Incremental/Differential Backups - Image Agent

UltraBac has the ability to track and back up an image of only the disk sectors that have been modified since the last full image backup. This ability will help minimize the amount of space required to store image backups, and will allow a server to be quickly backed up and restored as necessary.

UltraBac creates a file called "UltraBac_DF2K.idx" (a hidden "system" file) on each partition being backed up differentially or incrementally. This file tracks all modified clusters on the partition, and is cleared during a full or incremental image backup.

NOTE: If you reboot the system, the sector tracking will be reset and UltraBac will perform a full backup automatically on the next Backup.

NOTE: The UltraBac Image Disaster Recovery Agent does not support differential images of dual-boot systems. A full image backup will have to be performed after each boot into the secondary OS.

Setup and Configuration

NOTE: To create an image backup of a remote system, the UltraBac Image Disaster Recovery Agent must be installed on the system being imaged. For more information on installing the Image Disaster Recovery Agent, please visit the "**Installing UltraBac**" section of the UltraBac User Manual:

UltraBac User Manual: Installing UltraBac

Creating a Differential/Incremental Image Set

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Click "Image Disaster Recovery Agent" to highlight the option, and click "Next."
3. Check the Image Agent option "Enable Differential or Incremental backup," and choose the type of differential backup to be performed:
    o Full backup – creates/clears the file (.idx) used to track changed clusters.
    o Differential backup – back up only the clusters changed since the last full backup.
    o Incremental backup – back up only the clusters changed since the last full or incremental backup.
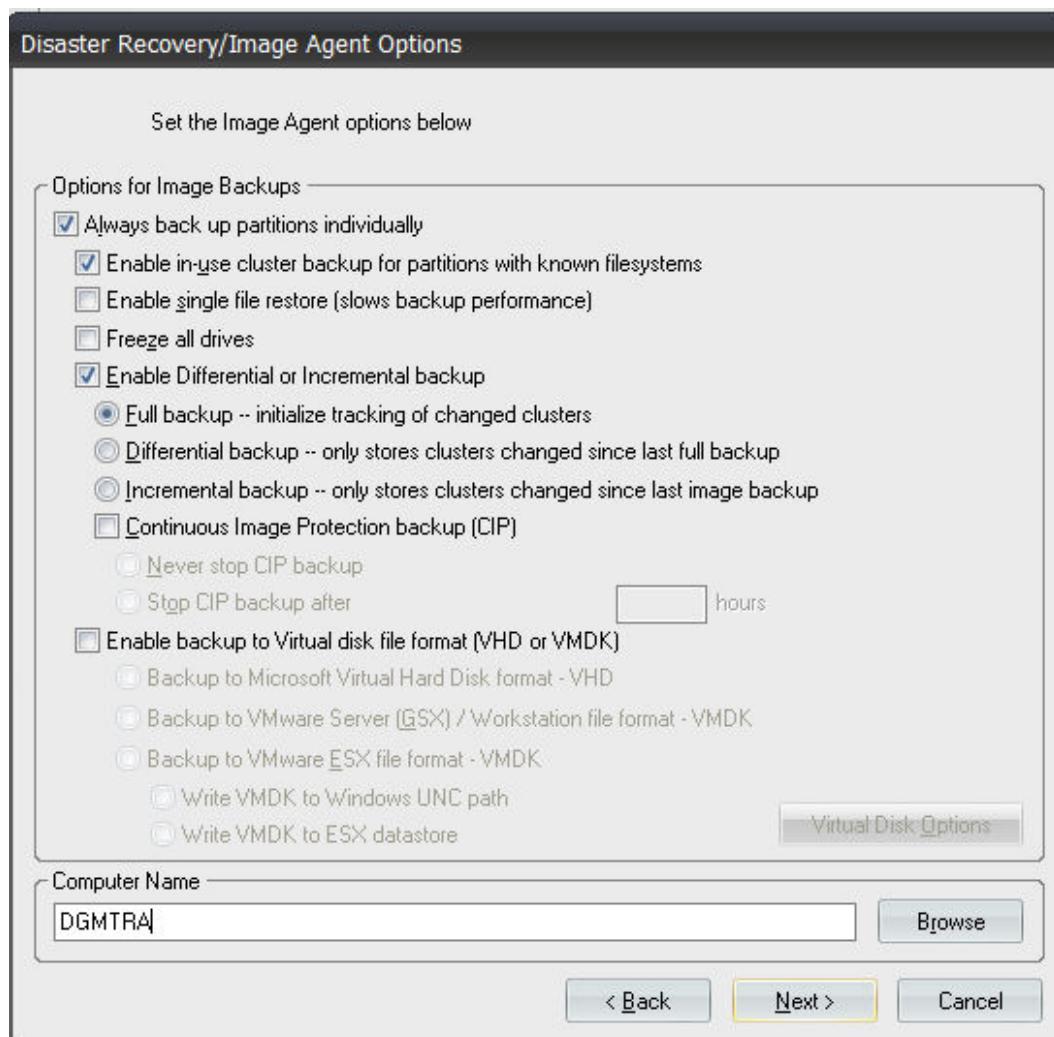
Fig. 1 - Image Agent options.

4. Type a set description as it will appear in the backup log, into the "Set Description" field, but do not modify the File Selection Logic menu. Click "Next."
5. Check "View/Edit files in the backup set" and click "Finish."
6.
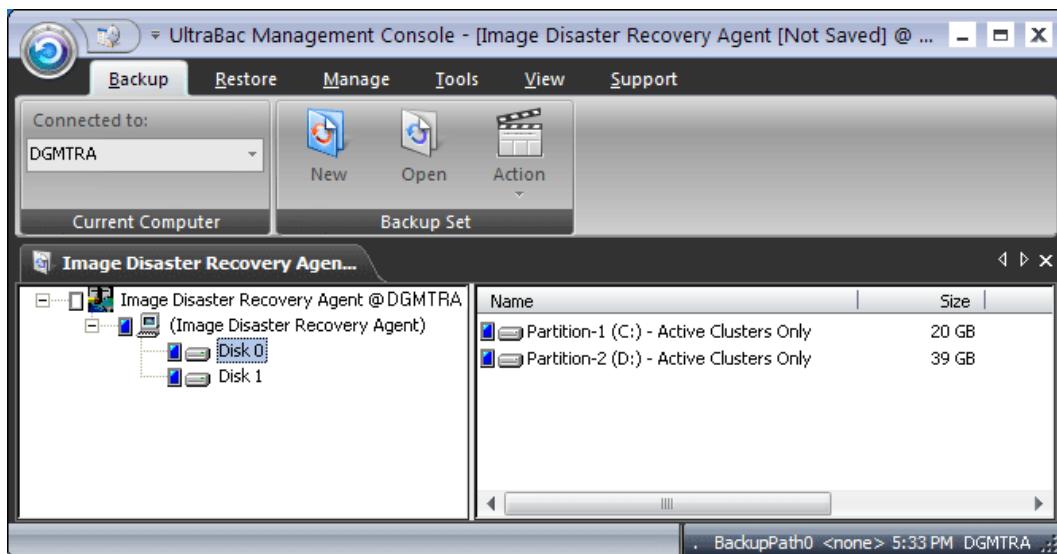
Fig. 2 - Image set loaded in the File Viewer.

6. Save the set by clicking "Action"/"Save" from the main UltraBac menu.

Restoring an Incremental/Differential Image Backup

To restore an Incremental/Differential Image backup, the full backup prior to the incremental/differential backup must first be restored. Once the full backup is restored, the differential backup can be restored. If restoring an incremental image, each backup must be restored in chronological order starting with the full backup.

NOTE: If one incremental image backup is lost or corrupt, all subsequent incremental image backups will become unrestorable.

To begin the restore process:

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the index for restore.
3. Select the disk or partition for restore.
4. Click "Action"/"Restore this Backup."
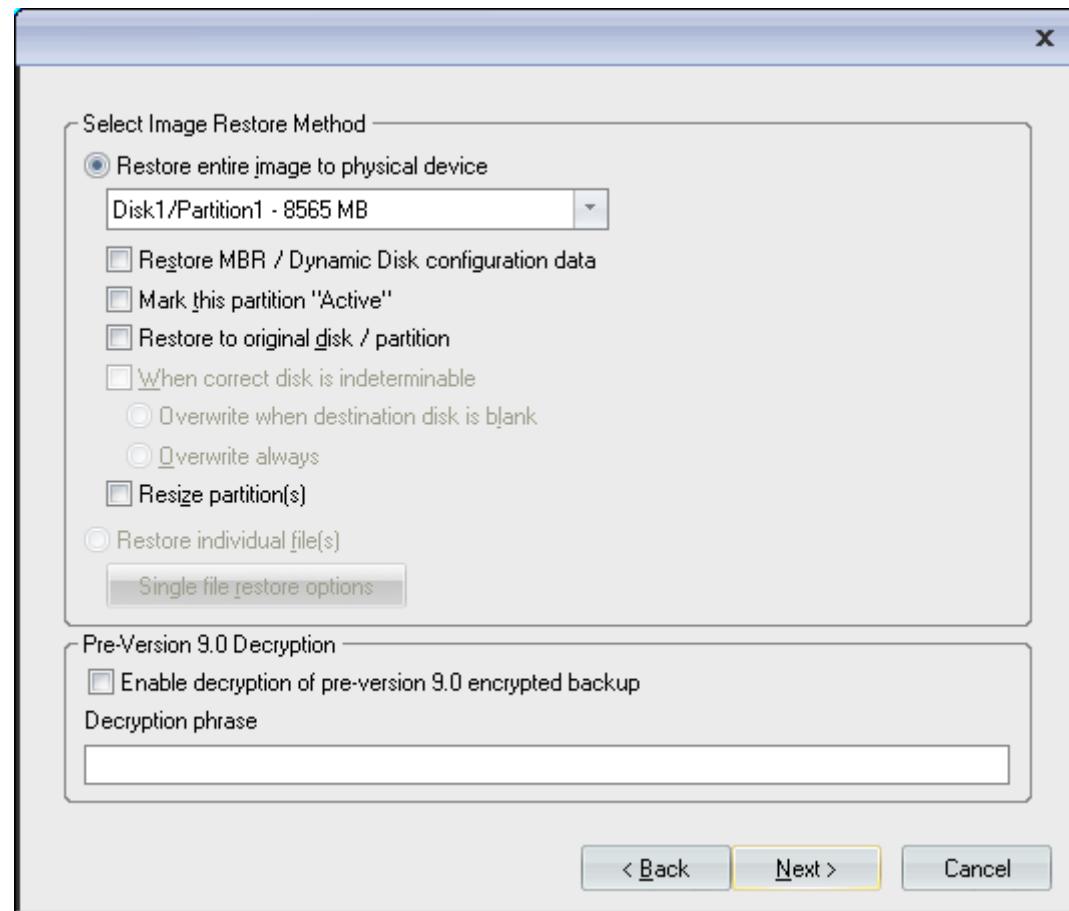
Fig. 3 - Image Restore options.

NOTE: The "Resize Partition(s)" checkbox should only be checked when performing the final restore of an incremental or differential image backup.

5. Click the "Restore entire image to physical device" radio button, select the restore target partition from the drop-down menu, and click "Next."
6. Check "Run Unattended," and click "Restore".
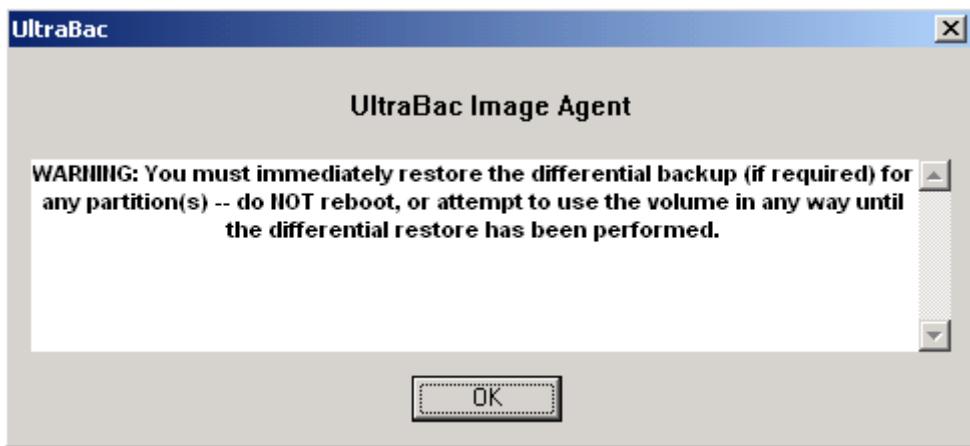
Fig. 4 - Incremental/Differential Restore prompt.

7. After the restore completes, immediately restore the most recent corresponding differential or all corresponding incremental backups beginning with the oldest incremental backup.
8. Reboot the system to activate the restored disk or partition.

One-Step Incremental Restore

Starting in UltraBac version 9.x, it is possible to a one-step restore with incremental restores. To do this style of restore, you must configure UltraBac to save both the full image backups and the incremental backups to the same backup device (i.e. all the backups would go to backuppath0).

To begin the restore process:

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the most recent Incremental image backup index for restore.
3. Select the disk or partition for restore.
4. Click "Action"/"Restore this Backup."
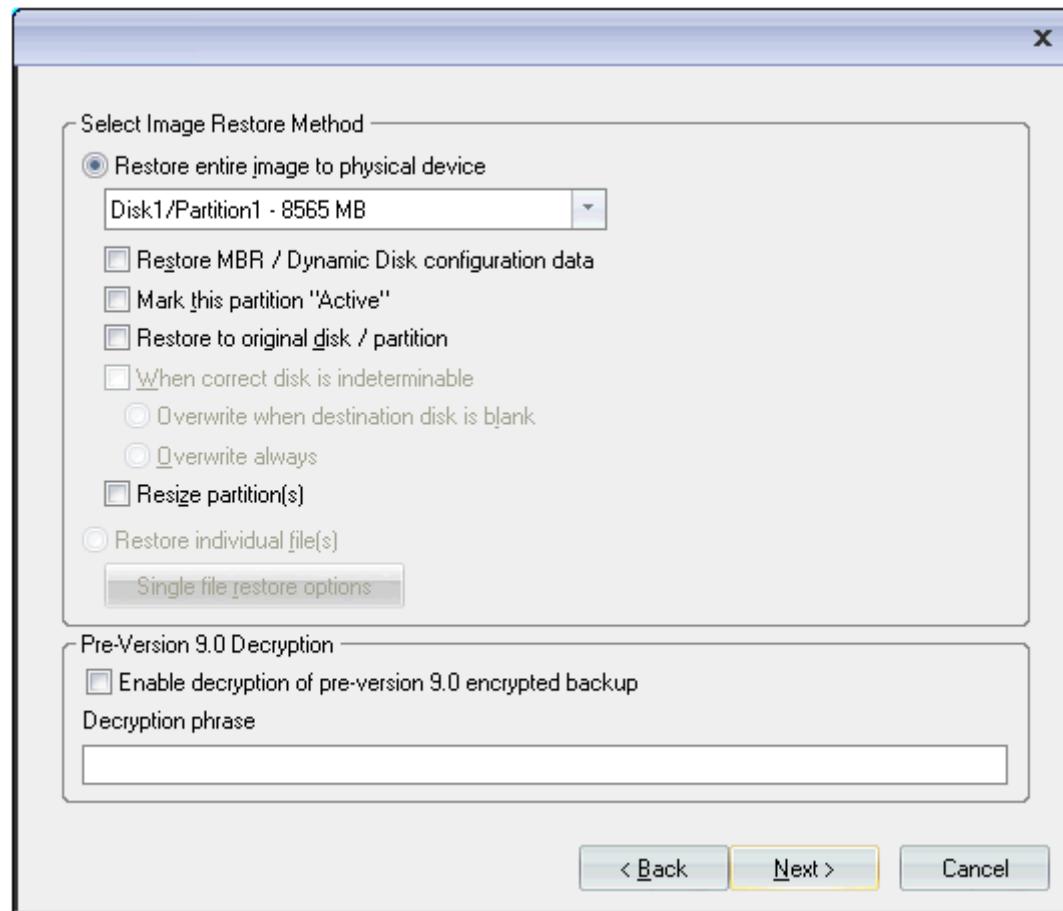
Fig. 5 - Image Restore options.

5. Click the "Restore entire image to physical device" radio button, select the restore target partition from the drop-down menu, and click "Next."
6. Check "Run Unattended," and click "Restore".
7. Reboot the system to activate the restored disk or partition.

Static Mirror Image Backup

A Static Mirror Image is a sector-level copy of a source disk to a target disk in the same system, on either the partition or disk level. This method of imaging provides the fastest backup and restore process available, but can only be run locally on the system being imaged.

NOTE: Only one partition (partition level) or one physical disk (disk level) can be backed up per Static Mirror Image backup job. To back up multiple disks or partitions, multiple jobs must be created.

NOTE: The UltraBac Image Disaster Recovery Agent supports Windows software RAID only when configured as RAID-0 or RAID-1.

Setup and Configuration

There are two types of Static Mirror Image backups:

- Partition level – Mirror image backup of an individual partition on the source disk. Partitions should be created on the target disk of equal or greater size than the partitions being backed up from the source disk, and those partitions should be unassigned of a drive letter.
- Disk level – Mirror image backup of the full source disk. Target disk should be unpartitioned, and of equal or greater size than the source disk.

Creating the Storage Device
After configuring the target disk, the target device (or devices) must be created in the Storage Device Manager.

To create the target device:

1. Select the Manage tab, and click "Storage Media" to launch the Storage Device Manager.
2. Select the device type to create:
    o   Partition level – Select the Partition tab.
    o   Disk level – Select the Image tab.
3. Click the "Add New" button.
4. Select the partition or disk to be used as the target device from the drop-down list.

Creating the Backup Set
An Image/Disaster Recovery backup set must be created for the Static Mirror Image backup that has only one partition or disk selected.

To create the Static Mirror Image backup set:

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Click "Image Disaster Recovery Agent" to highlight the option, and click "Next."
3. Configure the set option and click "Next":
    o   Partition level – "Always back up partitions individually" must be checked and "Enable Differential backup" must be unchecked.
    o   Disk level – "Always back up partitions individually" must be un-checked.
4. Type in a set description and click "Next."
5. Select "View/Edit files in the backup set" and click "Finish."

6. Clear the file selection logic from the backup set by un-checking the "top level" selection.
7. Select only the disk or partition to be backed up.
8. Save the set by clicking "Action"/"Save" from the main UltraBac menu.

Running the Static Mirror Image Backup

When scheduling a Static Mirror Image backup, only one set can be run per scheduled backup due to the limitations of the image and partition devices.

Add only the Static Mirror Image set and the corresponding image or partition device when creating the scheduled backup group.

NOTE: For instructions on creating a scheduled backup group, please visit the "**Scheduled Backup Basics**" section of the User Manual:

UltraBac User Manual: Scheduled Backup Basics

Recovering a Static Mirror Image

Recovering a Static Mirror Image is as simple as booting off the target disk or assigning a drive letter to the mirrored partition.

Using a mirrored SCSI disk, point the SCSI bios to boot off of the SCSI ID assigned to the target disk. If the system has swappable drives, replace the failed disk with the target disk.

File-by-File Agent

File-by-File Agent

The most commonly used agent in a backup strategy is the File-by-File Agent. This agent is used to back up files and directories on the backup host, or any networked system. This agent can also be used to back up the System State/Active Directory of the backup host or any networked system. File-by-file backups can be used to recover anything from a single file on a workstation to a full system recovery of a domain controller.

File-by-File Local Backup Set Creation

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Select the type of file-by-file backup to be run, and "Next:"
   - File-by-File Local – Backs up the locally attached physical disks.
   - File-by-File Network Share – Backs up a UNC path.
   - File-by-File Networked Computer – Backs up all locally attached physical disks on a remote system.
3. Enter a set description and choose the file selection logic to be used for this set. Click "Next."
4. At the Backup Wizard Summary select "View/Edit files in the backup set" to view the file selections and modify the selection logic. Click "Finish."
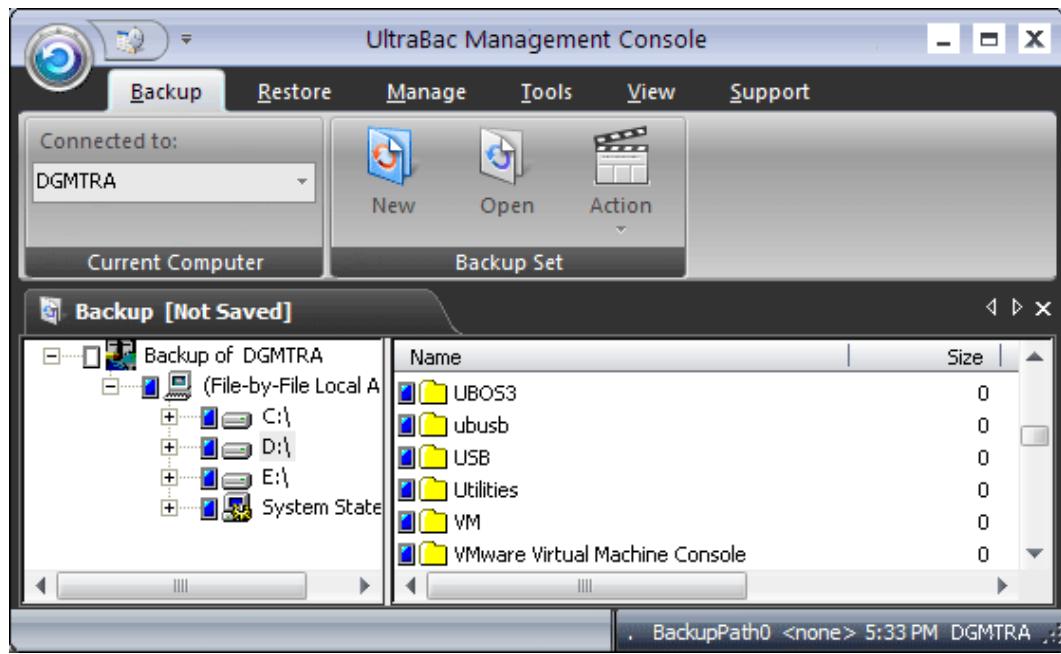
Fig. 1 - Viewing a File-by-File Local Agent backup set in the File Viewer.

5. Save the set by clicking "Action"/"Save."

File-by-File Network Backup Set Creation

NOTE: The backup of a remote System State/Registry requires the installation of the UltraBac System State Agent on the remote system. For more information on installing UltraBac agents, please visit the "**Installing UltraBac**" section of the User Manual:

UltraBac User Manual: Installing UltraBac

Two options exist for backing up remote systems:

- File-by-File Network Share – This agent allows the backup of a UNC path, or remote share.
- File-by-File Networked Computer – Selects all drives and the System State/Active Directory on a remote system.

NOTE: The remote registry, or System State, cannot be backed up using the "File-by-File Network Share" option.

File-by-File Network Share Set

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Click "File-by-File Network Share" to highlight the option. Click "Next."
3. To use an account other than the default account (specified on the Manage tab, under /"General"/"Authentication Options"/"Show Accounts"), check "Enable Advanced Account Usage" and enter an account with administrative access to the share being selected for backup. Click "Next."
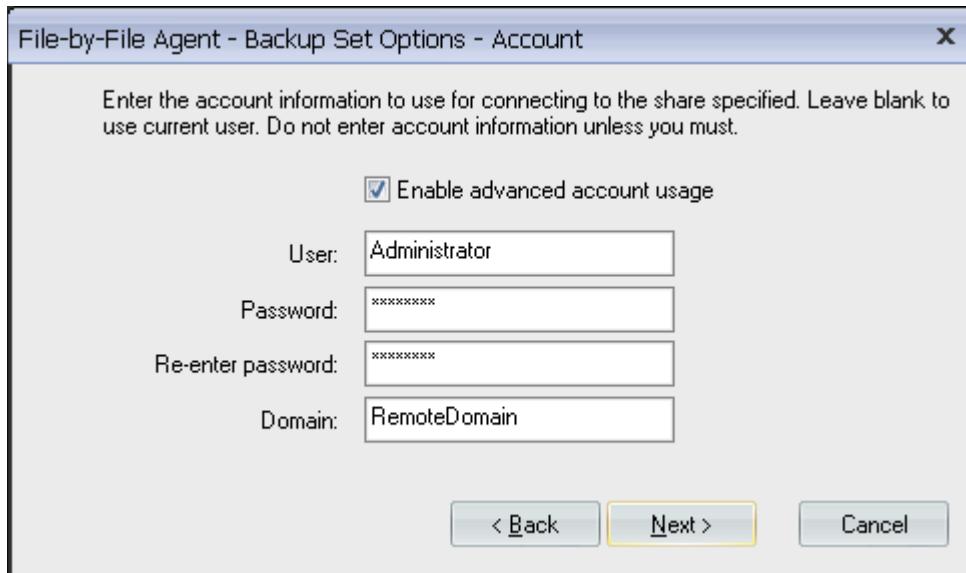
Fig. 2 - Advanced account usage enabled.

4. From the "Select Network Share" screen, browse to or type the network share/UNC path to be backed up. Click "Next."
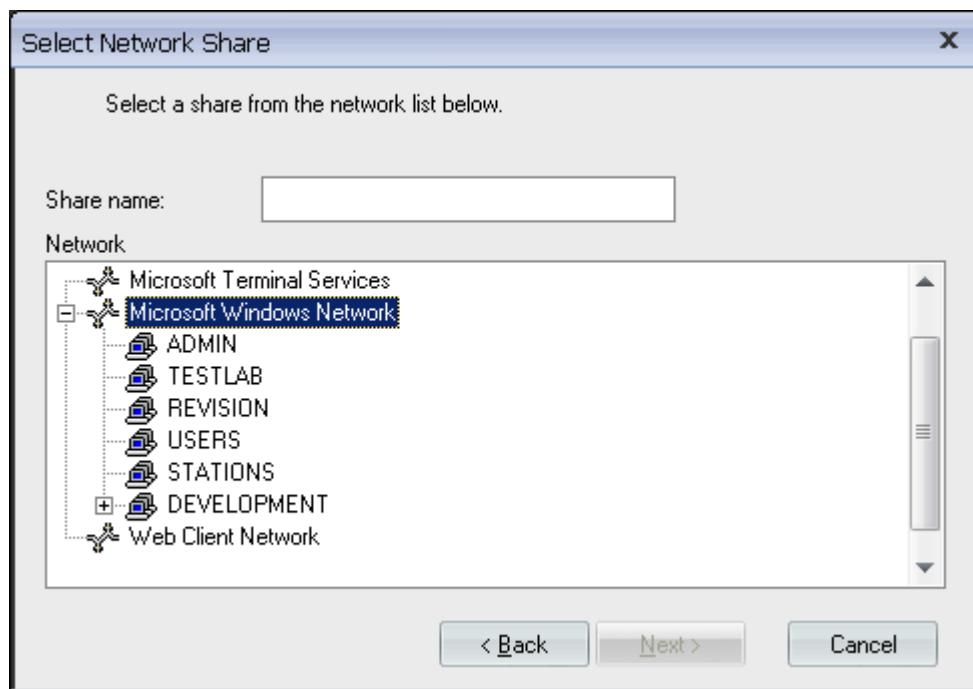
Fig. 3 - Network share browser.

5. Enter a set description and choose the "File Selection Logic" to be used for this set. Click "Next."
6. View or save the backup set.

File-by-File Networked Computer Set

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Click "File-by-File Network Share" to highlight the option. Click "Next."
3. To use an account other than the default account (specified on the Manage tab, under /"General"/"Authentication"/"Show Accounts"), check "Enable Advanced Account Usage" and enter an account with administrative access to the share being selected for backup. Click "Next."
4. From the "Select Network Machine" screen, browse to or type in the network name of the system to be backed up. Click "Next."
5. Enter a set description and choose the "File Selection Logic" to be used for this set. Click "Next."
6. View or save the backup set.

File-by-File Agent Set Properties
To view the properties of a backup set:

1. Load a backup set into the File Viewer.
2. Click "Action"/"Set Properties."
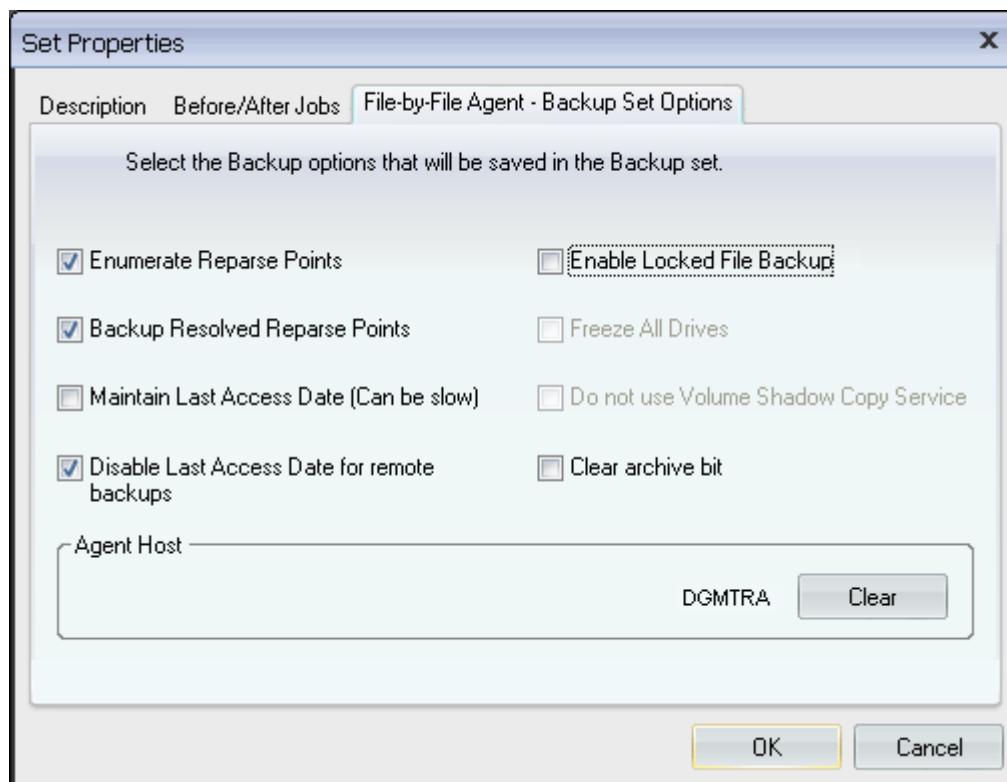
Fig. 4 - File-by-File Agent set properties.

- Description – Set the description as it will appear in the backup, restore, and verify logs.
- Before/After Jobs – Set scripts to run before or after the backup set is run.
- File-by-File Agent - Backup Set Options - Account – Set the account information to be used during the backup set.
- File-by-File Agent - Backup Set Options:
  - Enumerate Reparse Points – Enumerate and back up any selected reparse points.
  - Backup Resolved Reparse Points – Back up the data linked by the reparse points.
  - Maintain Last Access Date (Can be slow) – UltraBac will not show the file as being accessed during backup. Use this preference only if necessary.
  - Disable Last Access Date preservation for remote backups – This preference will disable the "Maintain Last Access Date" preference when backing up a remote systems.
  - Enable Locked File Backup – Freeze the target partition using the "UltraBac Locked File Backup" driver prior to the backup, and thaw the partition after the set is finished.
  - Freeze All Drives – Freeze all partitions on the backup target prior to running the backup. This option should be used if backing up a relational database spanning multiple partitions to ensure that the database and its logs maintain their integrity.
  - Do not use Volume Shadow Copy Service – Forces UltraBac to use the UltraBac Locked File Backup driver when backing up on Windows 2003/XP. VSS is not available on versions of Windows prior to 2003/XP.
  - Clear archive bit – Clears the archive bit attribute after the file is backed up. This option is used when performing incremental or differential backup jobs.
  - Agent Host – The system where the UltraBac File-by-File Agent will be hosted. This defaults to the backup server if blank.

File-by-File Agent Properties
The default behavior of the UltraBac File-by-File Agent can be modified in the "Manage"/"Agents"/File-by-File Local" menu. This allows specific options to be selected by default when creating file-by-file backup sets. Other than the "Files to skip" option, these options can be overridden by the properties of each backup set or when a restore is performed.
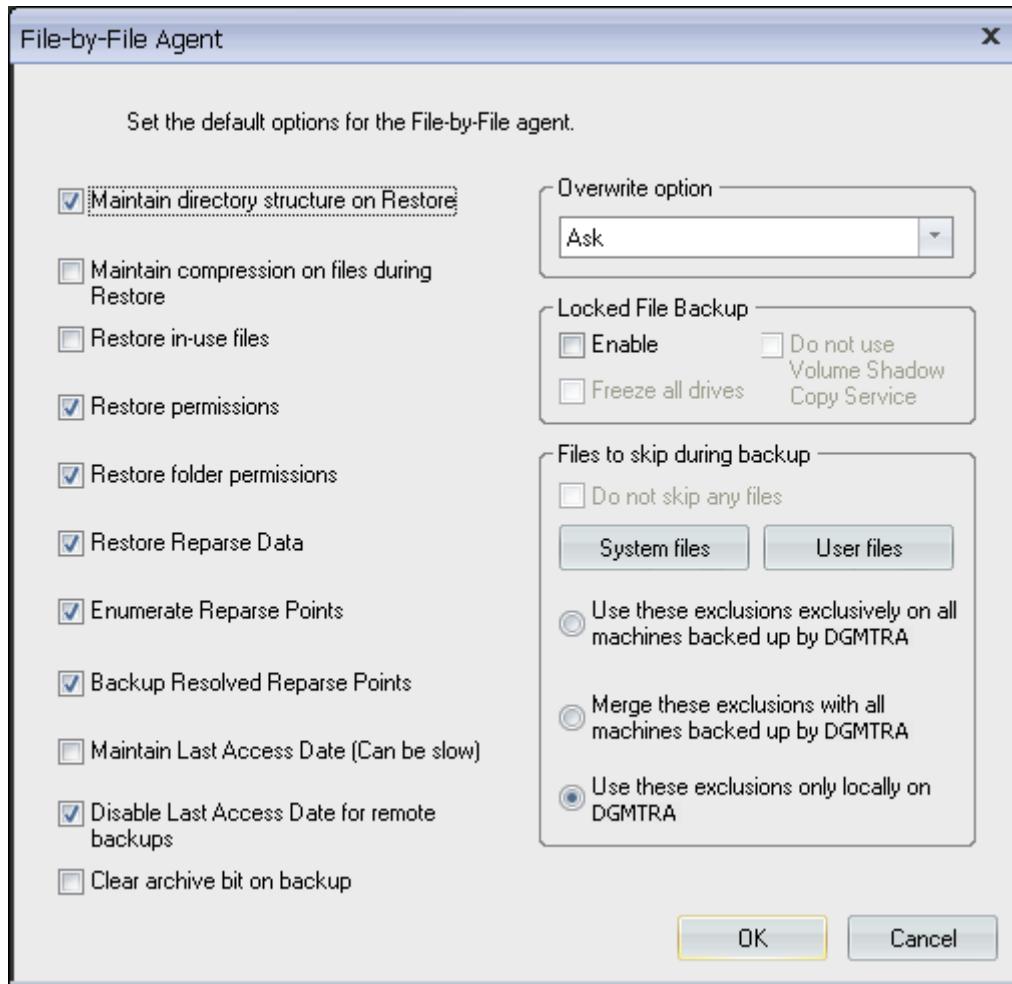
Fig. 5 - File-by-File Agent properties.

The available default options to be set:

- Maintain directory structure on Restore – Restore files and folders with the original parent folder structure.
- Maintain compression on files during Restore – If a file was compressed when backed up, that compression will be maintained after restore.
- Restore in-use files – Forces the restoration of in-use files. The overwritten in-use files will not become active until the system is rebooted.
- Restore permissions – Restores previously existing permissions on files.
- Restore folder permissions – Restores previously existing permissions on folders.
- Restore Reparse Data – Restores the data linked by the reparse point.
- Enumerate Reparse Points – Enumerate and back up any selected reparse points.
- Backup Resolved Reparse Points – Back up the data linked by the reparse points.
- Maintain Last Access Date (Can be slow) – UltraBac will not show the file as being accessed during backup. Use this preference only if necessary.

- Disable Last Access Date for remote backups – This preference will disable the "Maintain Last Access Date" preference when backing up remote systems.
- Clear archive bit on backup – Clears the archive bit attribute after the file is backed up. This option is used when performing incremental or differential backup jobs.

Overwrite Options

These options specify how files should be handled when selecting existing files for restore. This preference can be overruled by the option selected during the restore operation.

- Ask – Prompt before overwriting any existing files.
- Never – Do not overwrite any existing files.
- Always – Overwrite existing files with the files being restored.
- Update Only – Only overwrite if the file being restored is newer than the existing file.

Locked File Backup

These options enable the Locked File Backup Agent in all file-by-file sets created from the local system.

- Enable – Freeze the target partition using the "UltraBac Locked File Backup" driver (or VSS on Windows 2003/XP) prior to the backup, and thaw the partition after the set is finished.
- Freeze All Drives – Freeze all partitions on the backup target prior to running the backup. This option should be used if backing up a relational database spanning multiple partitions to ensure that the database and its logs maintain their integrity.
- Do not use Volume Shadow Copy Service – Forces UltraBac to use the UltraBac Locked File Backup driver when backing up on Windows 2003/XP. VSS is not available on versions of Windows prior to 2003/XP.

Files to Skip During Backup

This option allows files and directories to be globally excluded from all file-by-file backups. This option must be configured on each system running the UltraBac File-by-File Agent.

NOTE: The "Do not skip any files" option is only available when the Locked File Backup Agent is enabled in the backup set.
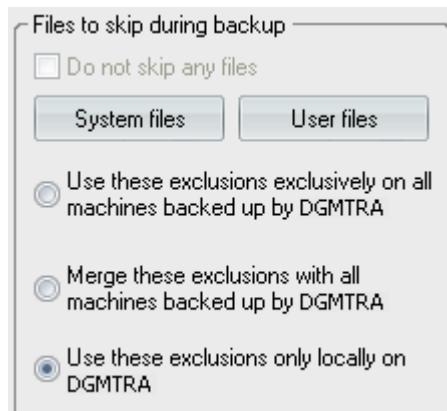
Fig. 6 - Files to skip during backup.

- Do not skip any files – Forces all files (including page files, hyberfil.sys, etc.) to be backed up. This option is only available when the Locked File Backup Agent is enabled.
- System files – This displays a non-modifiable list of system files that are skipped during backup.
- User files – A user created list of files/directories to be skipped during backup.
- Use these exclusions exclusively on all machines backed up by <local machine> – Applies the list of user created exclusions to all file-by-file backup sets run from the local backup host.
- Merge these exclusions with all machines backed up by <local machine> – Copies the list of user created exclusions to all remote systems backed up with the File-by-File Agent, forcing the selected files to be skipped in file-by-file backup sets run from all backup hosts.
- Use these exclusions only locally on <local machine> – Applies the list of user created exclusions only to file-by-file backup sets run from the local backup host that back up the local backup host.

Configuring Exclusions

Clicking the "User Files" button opens a screen that allows specific files, folders, or "wildcard" entries to determine the files/directories to be skipped during all file-by-file backups.
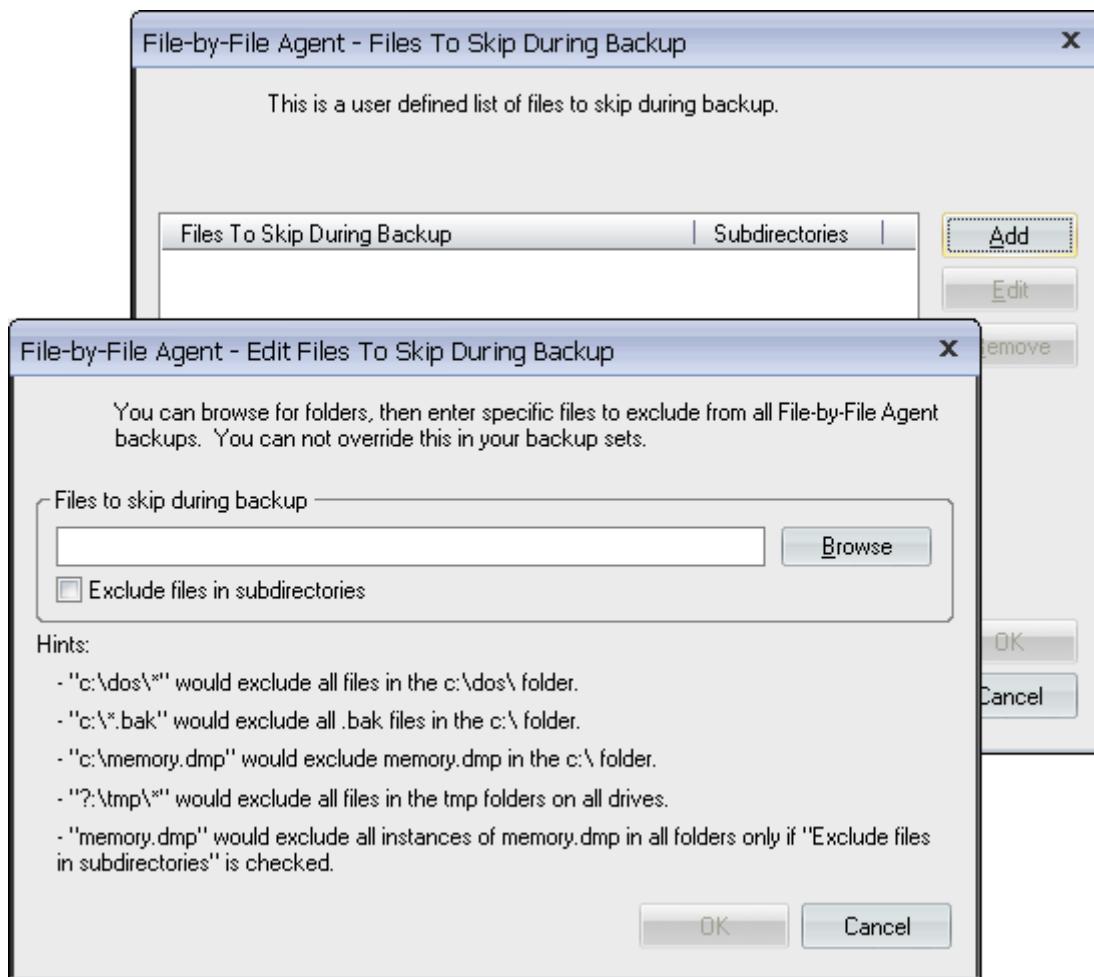
Fig. 7 - Adding files or directories to the list of files not to back up.

Restoring a File-by-File Backup

To begin the restore process:

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the index for restore.
3. Select the objects for restore.
4. Click "Action"/"Restore this Backup."

Restore Options
The "Restore Options" screen allows the user to restore to an alternate location, determine overwrite options, and more.
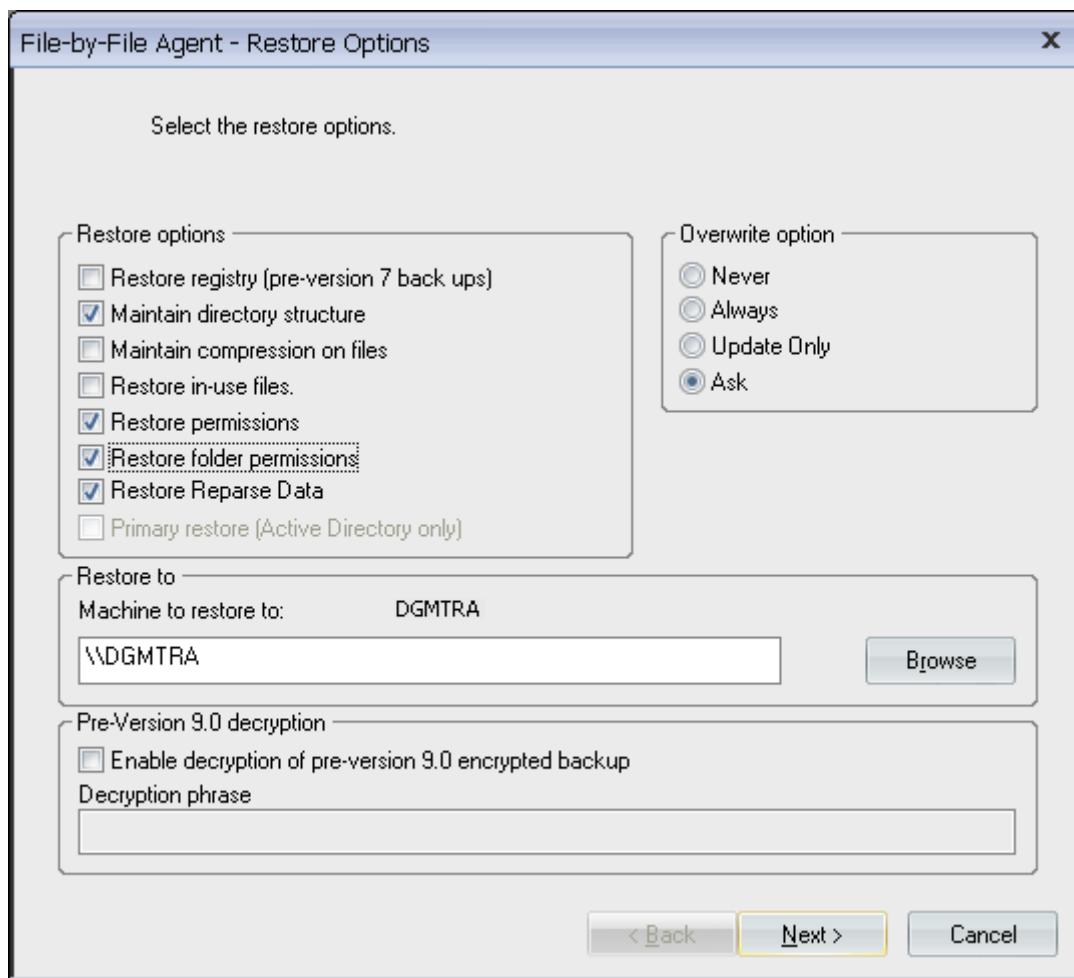
Fig. 8 - Restore options.

- Restore Registry (pre-version 7 back ups) – Used when restoring the registry from a backup made with a previous version of UltraBac.
- Maintain directory structure on Restore – Restore files and folders with the original parent folder structure.
- Maintain compression on files during Restore – If a file was compressed when backed up, that compression will be maintained after restore.
- Restore in-use files – Forces the restoration of in-use files. The overwritten in-use files will not become active until the system is rebooted.
- Restore permissions – Restores previously existing permissions on files.
- Restore folder permissions – Restores previously existing permissions on folders.
- Restore Reparse Data – Restores the data linked by the reparse point.

- Primary restore (Active Directory only) – Only enabled when booted into Directory Services Restore Mode, this option sets the Active Directory restore type as "Primary."
- Restore to path on: <servername> – Type in or browse to a UNC path to be used for the restore. Leave as "<Original Path>" to restore files to their original location.

Overwrite options:

- Never – Do not overwrite any existing files.
- Always – Overwrite existing files with the files being restored.
- Update Only – Only overwrite if the file being restored is newer than the existing file.
- Ask – Prompt before overwriting any existing files.

Fig. 9 - Overwrite options when selecting "Ask" during restore.

The options available for a duplicate file are:

- Skip File – Do not restore the specified file, and continue the restore.
- Update – Only overwrite if the file being restored is newer than the existing file.
- Overwrite – Overwrite the file on disk with the file being restored.
- Overwrite All – Overwrite existing files with the files being restored.
- Rename – Rename the file being restored, or restore it to an alternate directory.

Full OS Restore

To perform a full restore of a failed operating system, it is necessary to have a full backup of the system partition, including the System State (Registry for NT4 machines). When restoring a failed operating system, hardware identical to the original machine should be used. If the system is being restored to different hardware, the restore of the registry could be unsuccessful, or the system may not be stable after reboot. If it is not possible to restore to identical hardware, try to match the new hardware as closely as possible to the old. In addition, it is possible to restore only the "Software" hive of the registry under "HKey_Local_Machine."

Install the operating system back to the original %systemroot% name, which is named "WINNT" or "Windows" by default. The Windows name, or computer name, also must be the same the original system that was backed up. If %systemroot% or the computer name on the new machine is different than the source backup, the restore will not be successful. When the new operating system has been installed, install UltraBac on the system.

Once the operating system and UltraBac are installed, restore the entire system partition and system state back to its original location. In the restore options, ensure that "Restore in-use files" is checked. Also, ensure the "Unattended" box is checked before starting the restore. If "Unattended" is not checked, UltraBac will return a prompt every time a file is skipped or overwritten.

NOTE: For more information on the full restore of a 2000/2003 domain controller, please visit the "**Active Directory Restore 2000/2003**" section of the User Manual and for the full restore of a 2008/2008 R2 domain controller please visit the "**Active Directory Restore 2008/2008 R2**" section of the User Manual:

UltraBac User Manual: Active Directory Restore 2000/2003
UltraBac User Manual: Active Directory Restore 2008/2008 R2

Incremental/Differential Backups - File-by-File Agent

UltraBac has the ability to perform backups of only modified files, using modified file dates or the Archive Bit file attribute.

Incremental vs. Differential Backups

"Incremental" and "differential" backups are very similar in their function and creation, as both are used to minimize the amount of time needed to complete a backup as well as the amount of storage space used. Incremental and differential backup sets will back up only the files that have been modified within a specified time period, or that have the "archive bit" attribute set. The archive bit attribute is set by Windows when a file is modified.

NOTE: For a detailed description of incremental and differential backup sets, including contents and format, please see the UltraBac Knowledge Base:

See UBQ000080: Incremental/Differential and Archive Selections

- Incremental Backup – UltraBac backs up all files modified since the last backup, incremental or full, and the "Clear Archive Bit" option is selected (if using the archive bit file selection logic). To perform a full system restore, all incremental backups performed since the last full backup must be restored, after restoring the full backup.
- Differential Backup – UltraBac backs up all files modified since the last full backup. The "Clear Archive Bit" option is not selected when a "differential" backup is run, only during full backups (if using the archive bit file selection logic). To perform a full system restore, only the most recent differential backup must be restored, after restoring the full backup.

Creating Incremental/Differential Sets

NOTE: It is now possible to set archive bit attributes in the backup sets, as well as in backup operations. Both scheduled and ad-hoc backups can clear the archive bit. For more information on setting the "Clear Archive Bit" option in a backup set, please visit the "**File-by-File Agent**" section of the User Manual:

UltraBac User Manual: File-by-File Agent

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Click the "File-by-File Agent" to highlight the option. Click "Next" to continue.
3. Enter a set description and choose the Modified file selection logic to be used for this set. Click "Next."
4. At the New Backup Set summary, select "View/Edit files in the backup set" to view the file selections and modify the selection logic. Click "Finish."
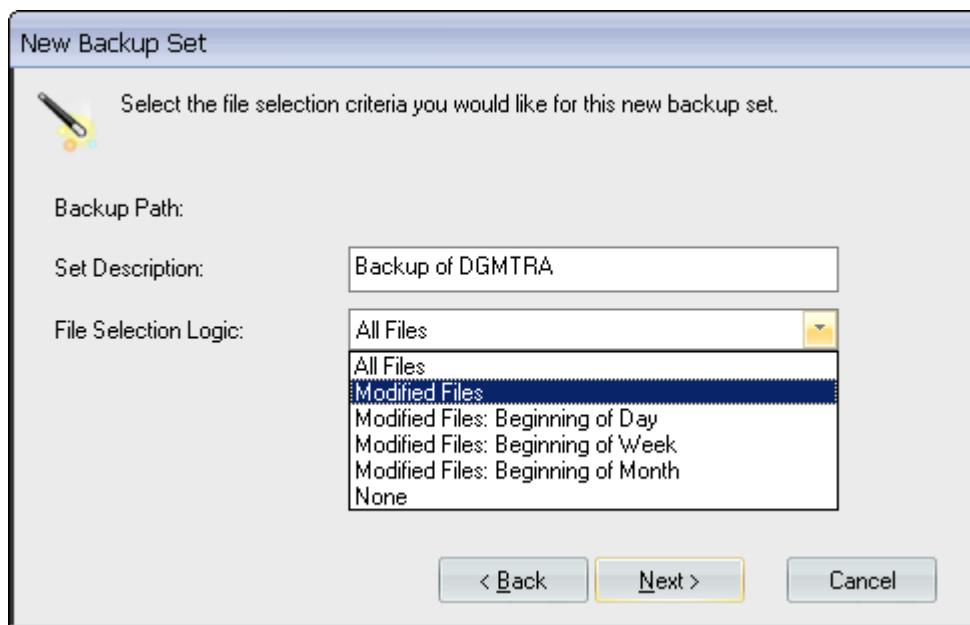
Fig. 1 - Available file selection logic in the Selection Criteria.

Modified file selection logic options:

- All Files – All files selected.
- Modified Files – All files with the archive bit checked.
- Modified Files: Beginning of Day – All files created/modified the day the backup is run (used for incremental backups only).
- Modified Files: Beginning of Week – All files created/modified the week the backup is run (used for differential backups only).
- Modified Files: Beginning of Month – All files created/modified the month the backup is run (used for differential backups only).
- None – No files selected.

> NOTE: Incremental backup sets should have the option "Clear Archive Bit" checked, while differential sets should not. When using a "differential" backup strategy, the archive bit is only cleared during the full backup.

When performing a "Modified File" backup, it is recommended to use the archive bit attribute in the backup set's file selection logic.

It is also possible to include the modified files of any given directory, after a set is loaded:

1. Open a backup set by selecting the Backup tab and clicking "Open" from the main UltraBac menu.
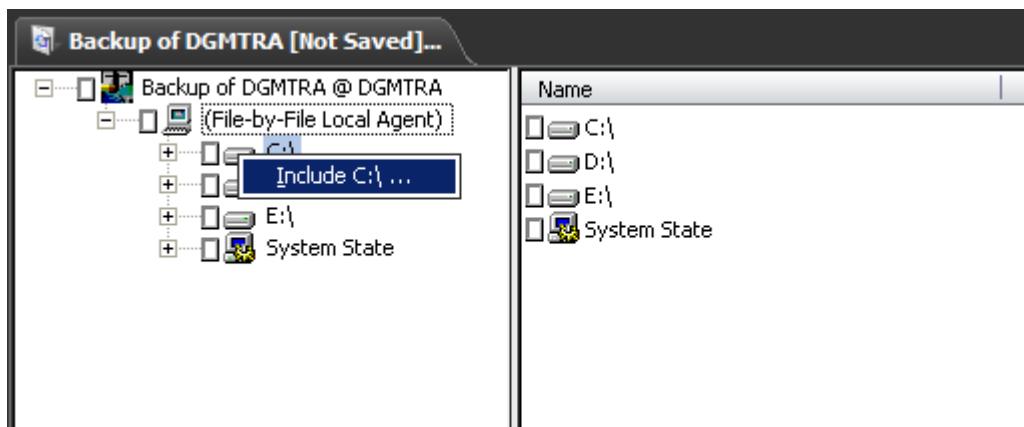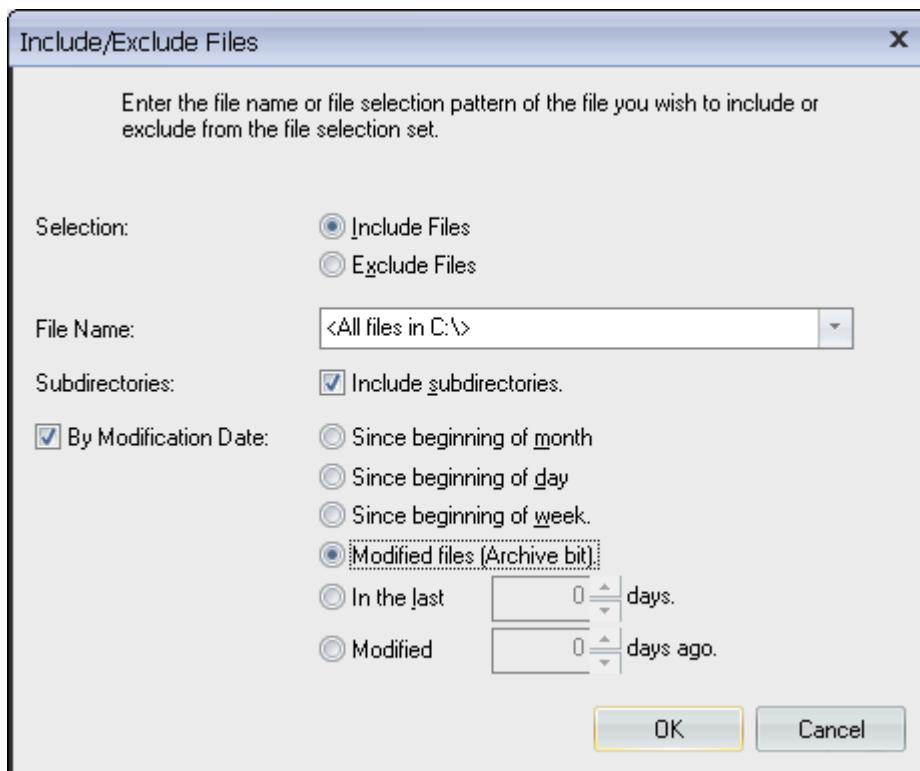
Fig. 2 - Including a drive in the File Viewer.

2. Deselect all files and directories in the backup set.
3. Right click on the directory to be backed up, and click "Include <directory name>" to bring up the "Include/Exclude Files" screen.
4. Select "Include Files."
5. Check "Include subdirectories" if sub-folders are to be included.

6.
Fig. 3 - "Include/Exclude files" screen.

7. Check "By Modification Date."
8. Choose the file selection logic to be used in backing up the directory.
9. Click "OK" to apply the changes to the set.

Selecting Files with Specific Extensions
UltraBac also allows the selection of files with only particular extensions, such as executables (.exe) or text files (.txt) for both backup and restore. This selection screen can also be used to create modified file backups, or exclude files with a particular extension.

To select files of a specific extension:

1. Right click on the parent directory containing the files to be selected, and click "Include 'directory'."
2. Type "*.<file extension>" in the "File Name" field.
3. Click "OK."

Locked File Backup Agent

The Locked File Backup Agent is designed to temporarily "freeze" the target partition before the backup begins, and "thaw" the partition after the backup completes. Freezing the partition allows UltraBac to back up files that are exclusively locked by an application or service and would otherwise be skipped.

Installation

The Locked File Backup Agent is automatically installed when the File-by-File or Disaster Recovery/Image Agents are installed. The system must be rebooted after install for the Locked File Backup Agent to be activated.

NOTE: For more information regarding the installation of the File-by-File Agent and Disaster Recovery/Image Agent, please visit the "**Installing UltraBac**" section of the User Manual:

UltraBac User Manual: Installing UltraBac

Using the Locked File Backup Agent

NOTE: The UltraBac Locked File Backup Agent is automatically used by the DR/Image backups, and cannot be controlled via user preference.

The global preference to enable the Locked File Backup Agent is located on the Manage toolbar, under "Agents"/"File-by-File Agent." This preference will enable the agent in all File-by-File Agent sets created on the backup host.

To enable the Locked File Backup driver in a specific backup set:

1. Create or open a backup set.
2. Click "Action"/"Set Properties" from the main UltraBac menu.
3. Click on the "File-by-File Agent – Backup Set Options" tab.
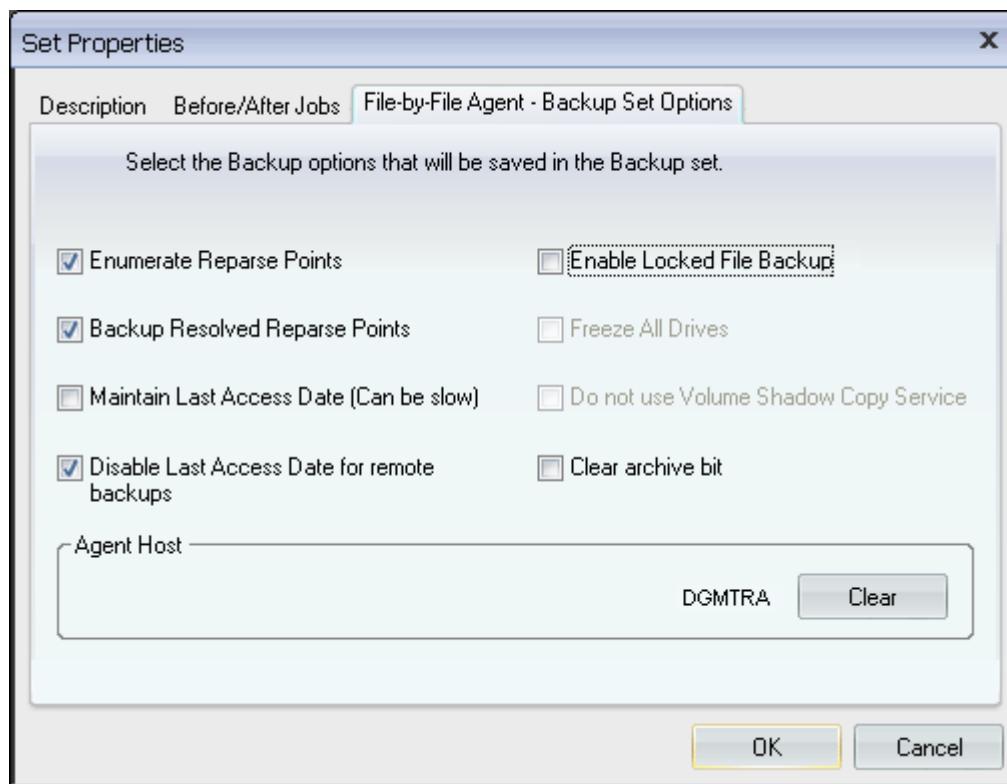
Fig. 1 - File-by-File backup set preferences.

    4.   Check "Enable Locked File Backup."
    5.   Click "OK" to save.

After checking "Enable Locked File Backup," the option to "Freeze All Drives" and "Do not use Volume Shadow Copy Service" will become available. These options should be used to maintain the integrity of files or applications (i.e. relational databases) during the freeze, when the files or applications are spread across multiple partitions or disks.

- Freeze all Drives – Freeze all drives/partitions on the system at the beginning of the backup.
- Do not use Volume Shadow Copy Service – Use the UltraBac Locked File Backup driver to freeze the system.

Uninstalling the Locked File Backup Agent

The Locked File Backup Agent can be uninstalled through the Device Manager in Windows XP/2000/2003. Complete the following steps to remove the Locked File Backup driver.

    1.   Access "Computer Management."
    2.   Highlight "Device Manager," right click, and select "View"/"Show Hidden Devices."
    3.   Right click on "Device Manager" again and select "View"/"Devices by Connection."
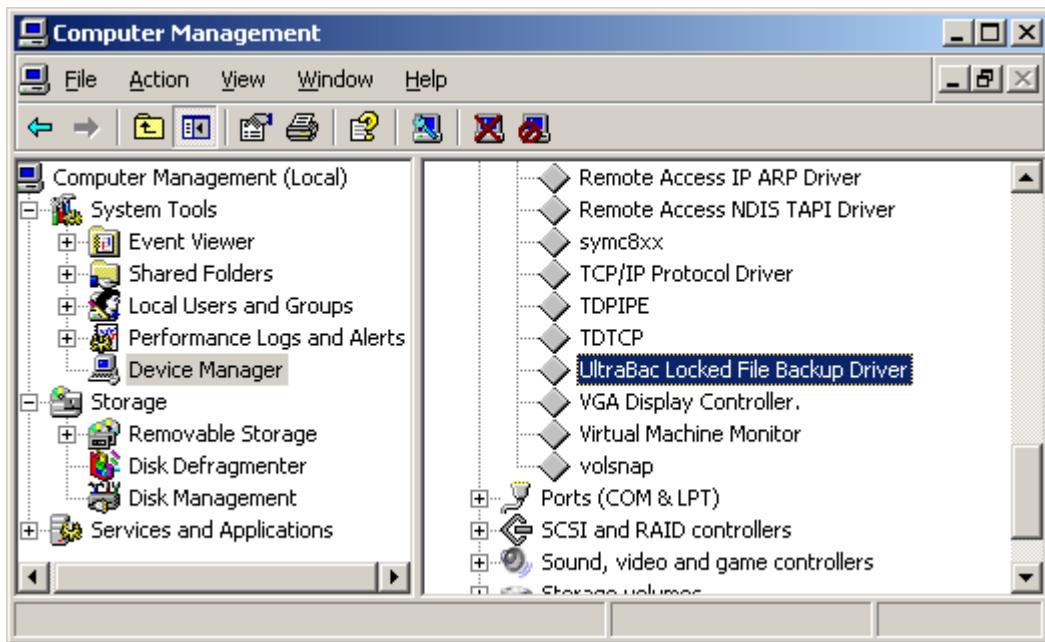
Fig. 2 - UltraBac Locked File Backup Driver in the Windows Device Manager.

4. Scroll down to "UltraBac Locked File Backup Driver," right click on it, and select "Uninstall."
5. Reboot the system to complete the removal of the UltraBac Locked File Backup Agent.

UltraBac System State/Active Directory Restore Windows 2000/2003 Server

Overview

Three types of Active Directory restores exist for Windows 2000/2003 Server: Authoritative, Non-Authoritative, and Primary.

- Authoritative restore – Running NTDSUTIL after the restore updates the USN (Updated Sequence Numbers) to be greater than any other member domain controller to which the machine formerly replicated. This will cause the restored domain controller to replicate its Active Directory information to all other domain controllers.
- Non-Authoritative restore – A restore overwriting the System State to the point at which it was backed up. A Non-Authoritative System State restore is usually done when there are other domain controllers on the network responsible for replicating the Active Directory changes to systems with older Updated Sequence Numbers.
- Primary restore – A Primary restore is performed when no other domain controllers are present on the network. This type of restore can also be used when the machine is the only functioning server in a replicated data set.

A base installation of Windows 2000/2003 will have four sub-objects under "System State" in a File-by-File Agent set. These objects are seen when a local or remote file-by-file set is loaded, assuming the File-by-File Agent has been installed on the system being backed up. The subcomponents of the System State are the following:

- Event Logs
- Registry Hives
- Boot Files
- COM+ Database

The System State of an Active Directory host contains more subcomponents under the "System State" icon seen in the UltraBac interface:

- Event Logs
- Registry Hives
- Active Directory
- Boot Files
- COM+ Database
- Sys Vol

NOTE: The latest Windows Service Pack must be applied to the restore target prior to attempting the restore.

NOTE: When pushing the restore to a remote system booted into Directory Services Mode, be sure that the UltraBac System State Agent is installed on the restore target.

Restoring the System State Using UltraBac

NOTE: When attempting to restore an Active Directory host to a new installation of Windows, a base version of Active Directory, using only the default components, must be installed before attempting the restore.

Start the domain controller in "Directory Services Restore" mode before restoring the System State:

1. Reboot the system.
2. When prompted to select an operating system or when Windows displays the "Starting Windows" progress bar, press "F8."
3. Select "Directory Services Restore Mode" from the boot options, and press "Enter."
4. If prompted, select the appropriate operating system and then press "Enter."
5. Log in using the Administrator account and password stored in the SAM (Security Accounts Manager), created when Active Directory was installed.
6. Select "OK" within the "*Desktop*" dialog box. This dialog box starts with the text, "Windows is running in Safe Mode."

NOTE: Active Directory/domain administrator accounts are not available, as the Active Directory is offline. The SAM account must also be defined in UltraBac before attempting restore.

Authoritative System State Restore

To perform a System State restore, follow these steps:

1. Run UltraBac by selecting from the Windows task bar:
   "Start"/"Programs"/"UltraBac"/"UltraBac Management Console."
2. Access the "Accounts" section from the Menu bar, under
   "Manage"/"General"/"Authentication Options," and click "Show Accounts."
3. Edit the "Default Account" to use the account name and password with which you are currently logged into Directory Services mode, making sure that the "Domain" field is blank. When the system is rebooted after restore, this account will need to be returned to the Backup Administrator account.
4. Load the index containing the System State backup that is to be restored. The Active Directory components will appear as objects under the System State icon in UltraBac.

   NOTE: When restoring the System State/Active Directory, all System State components must be restored. If one component is excluded from the restore, all objects will be excluded.

5.
6. From the Restore tab in UltraBac, select "Action"/"Restore This Backup" to bring up the "Restore Options" screen.
7. At the "Restore Options" screen, click "Next."
8. Check "Run unattended" if you wish to view errors in the restore log, rather than interactively, and click "Restore."
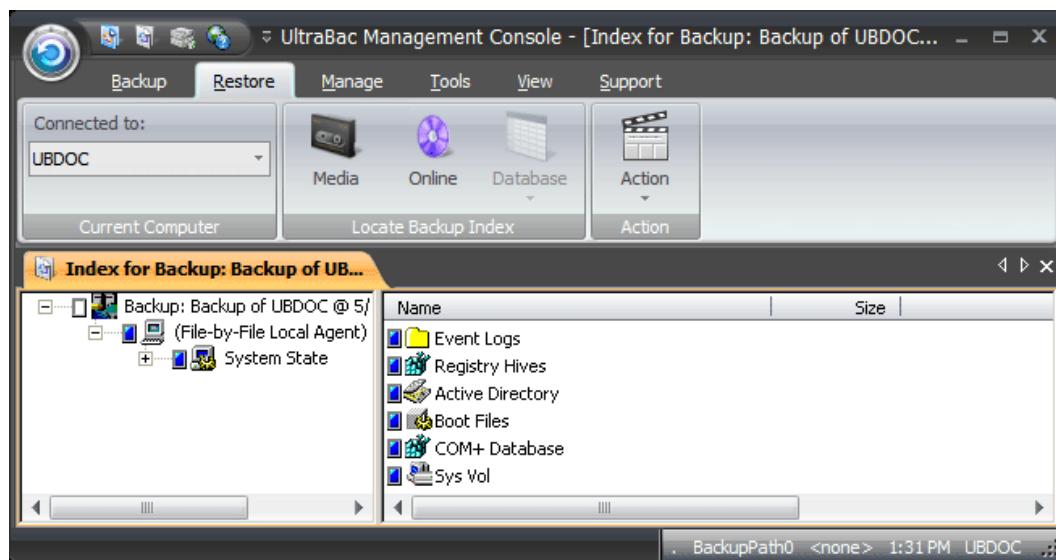
Fig. 1 - Backup index in the File Viewer showing System State components.

NOTE: When restoring the entire operating system, ensure that "Restore in-use files" is checked in the "Restore Options" screen.

9. When the restore completes, a prompt will appear confirming the reboot. If NTDSUTIL is to be run, click "Cancel" to override the reboot request.
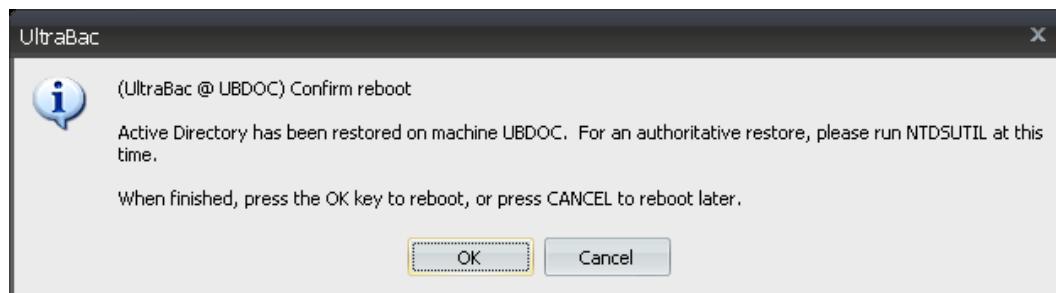
Fig. 2 - Reboot confirmation prompt.

10. Select "Restore Log" when the "UltraBac Progress" screen appears and verify the restore was successful.
11. When finished viewing the restore log, exit UltraBac. This concludes the UltraBac portion of the restore.
12. Run NTDSUTIL to synch the newly restored Active Directory database.

Running NTDSUTIL
Run NTDSUTIL and mark all appropriate objects as "Authoritative." To mark just a subtree as authoritative, type in the text "restore subtree <name>", where <name> is a string (e.g. "restore subtree cn=DomainController,ou=DomainControllers,c=DomainName,dc=TopLevelDomainName"), at the authoritative restore prompt and press "Enter." For more information, see Microsoft's documentation on restoring subtrees. NTDSUTIL can be run from the Command prompt.

NOTE: Type "ntdsutil/?" for help on this utility.

1. From the Command prompt type <NTDSUTIL> and press "Enter."
2. Type <authoritative restore> at the "NTDSUTIL.EXE" prompt and press "Enter."
3. Type in the text <restore database> at the "authoritative restore" prompt and press "Enter" to make the full Active Directory restore Authoritative. This command will be used in most cases.
4. Select "Yes" when prompted with the Authoritative Restore confirmation screen.
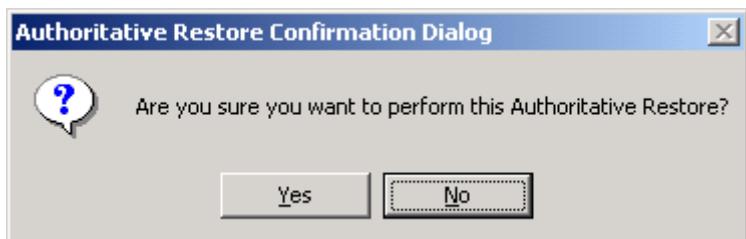
Fig. 3 - Authoritative restore confirmation prompt.

5. NTDSUTIL will return the number of records that need updating, as well as the number of records updated.

Fig. 4 - NTDSUTIL from a DOS prompt.

6. Type in <quit> at the "authoritative restore" prompt and press "Enter."
7. Type in <quit> at the "NTDSUTIL.EXE" prompt and press "Enter."
8. Reboot.

NOTE: The system must be REBOOTED before the restored System State files will be activated.

NOTE: Only restored objects specifically marked as authoritative will update the objects on other domain controllers. All other objects will be non-authoritative. See Microsoft's documentation on authoritative restores for more information:

Microsoft KB article 216243 - Authoritative Restore of Active Directory and Impact on Trusts and Computer Accounts

Non-Authoritative System State Restore

Non-authoritative System State restores are usually done when there are other domain controllers on the network responsible for replicating the proper changes to machines with older Updated Sequence Numbers. When the newly restored domain controller announces itself on the network again, other domain controllers will replicate their information to the restored domain controller. Follow the steps shown below to complete a non-authoritative restore.

To perform a non-authoritative System State restore, start the domain controller in "Directory Services Restore" mode:

1. Reboot the system.
2. When prompted to select an operating system, or when Windows displays the "Starting Windows" progress bar, press "F8."
3. Select "Directory Services Restore Mode" from the boot options, and press "Enter."
4. If prompted, select the appropriate operating system and then press "Enter."
5. Log in using the Administrator account and password stored in the SAM (Security Accounts Manager), created when Active Directory was installed.
6. Select "OK" within the *"Desktop"* dialog box. This dialog box starts with the text, "Windows is running in Safe Mode."

Run the restore exactly as indicated above. The only difference between an "authoritative" and "non-authoritative" restore is that the NTDSUTIL is NOT used in a non-authoritative restore.

Reboot the machine when UltraBac finishes the restore by clicking "OK" at the Confirm Reboot prompt.

Primary Restore System State Restore

A primary restore is performed when restoring the first domain controller in a domain that is being entirely recreated, and when no other domain controllers are present on the network. This type of restore is also used when restoring the only functioning server in a replicated data set.

The primary restore is completed in almost exactly the same manner as a non-authoritative System State restore. The one difference is that the "Primary Restore (Domain Controllers Only)" option must be checked in the *"*Restore Options" screen. Follow the instructions for restoring non-authoritatively, but ensure the primary restore option is checked, and reboot after the restore is complete.

UltraBac System State/Active Directory Restore Windows 2008/2008 R2 Server

Prerequisites for Full Operating System Restore

- **The restore target must be booted into Directory Services Restore mode.**
- The Windows name and OS version of the restore target must match the original system.
- The OS on the restore target must be installed to the path as the original system. WINDOWS is the default name for the %SYSTEMROOT% path.
- All of the latest OS service packs must be applied to the restore target.
- Install the full version of UltraBac on the restore target.
- Any new hardware should be matched to the original hardware as closely as possible.
- If the restore is being performed remotely, ensure the default UltraBac account has enough authority on the restore target to perform an OS restore.
- You must know what schema your domain/forest is in (2003 vs 2008) as the restore steps are different

Restoring the System State Using UltraBac

Start the domain controller in "Directory Services Restore" mode before restoring the System State:

1. Boot the system.
2. When prompted to select an operating system or when Windows displays the "Starting Windows" progress bar, press "F8."
3. Select "Directory Services Restore Mode" from the boot options, and press "Enter."
4. Log in using the Local Administrator account and password stored in the SAM (Security Accounts Manager), created before DC-Promo was initiated. For the domain use the local computer name.
5. Install UltraBac.
6. Enter the local administrator account when prompted by UltraBac.
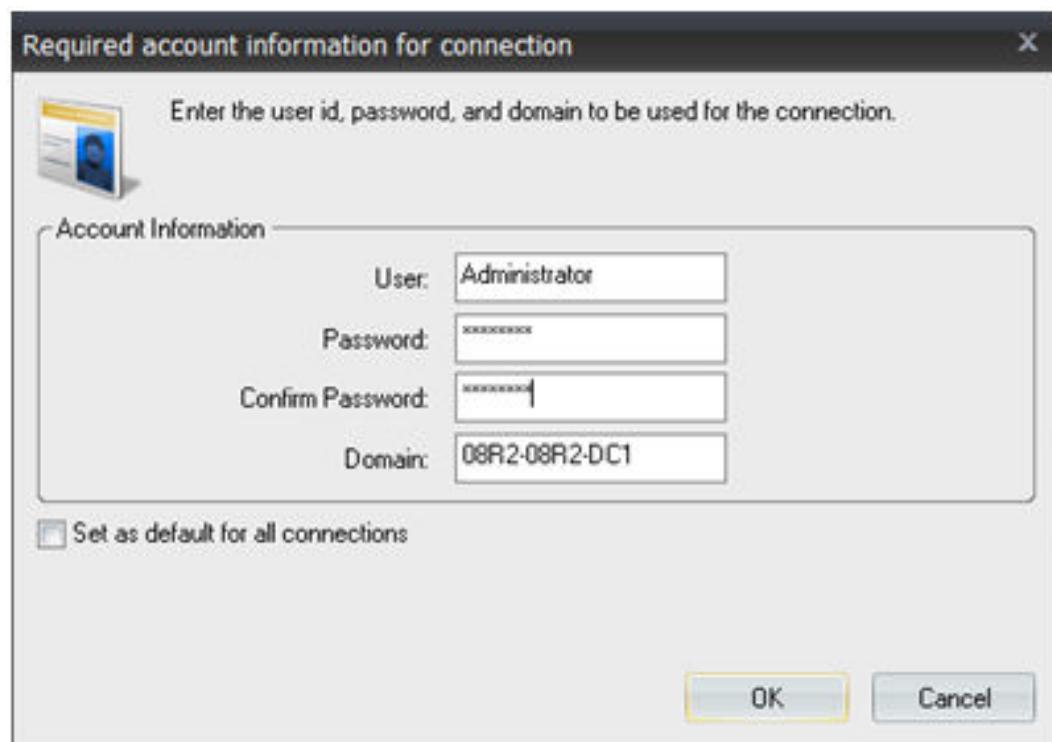
Fig. 1 - Authentication Options

> NOTE: Active Directory/domain administrator accounts are not available, as the Active Directory is offline. The SAM account must also be defined in UltraBac before attempting restore.

7.   Load your backup, and choose both System State and the OS partition for restore

> NOTE: When restoring the System State/Active Directory, all System State components must be restored. If one component is excluded from the restore, all objects will be excluded.

8.   On the Restore Options screen "Restore in-use files" and "Overwrite Always" must be selected.
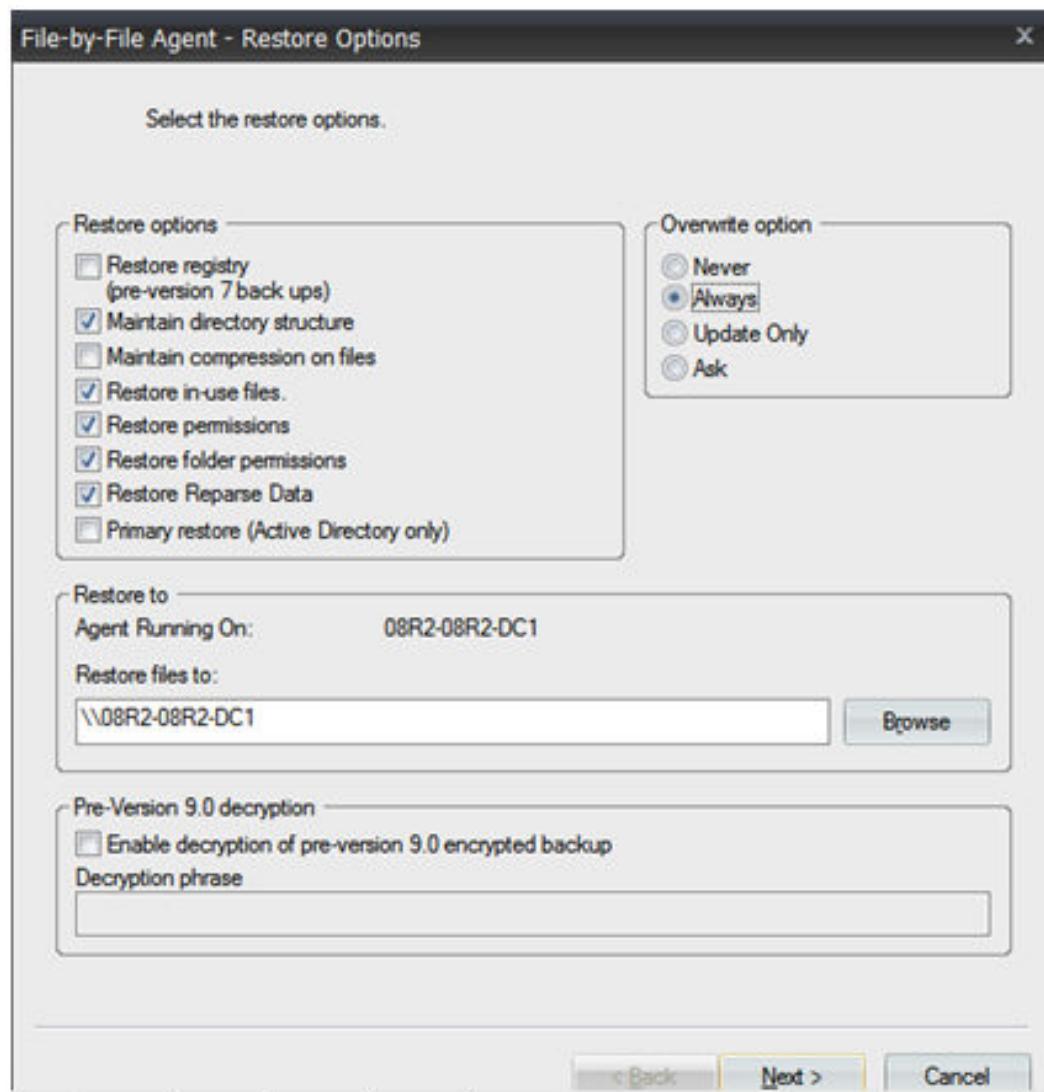
Fig. 2 Restore Options

9. Once the restore is done, reboot into 2008/2008 R2 normally.
10. Now you have to restore the SYSVOL portion of Active Directory, to complete the restore. Since the methodology is different between what Active Directory schema is in place at the time of backup, please scroll down to the appropriate area.

2008/2008 R2 Active Directory Schema with Multiple Domain Controllers.

NOTE: It is highly recommended to do the authoritative restore from an existing domain controller and not the one you are restoring, this way you will not lose any AD objects and changes since the last backup.

1. Stop the DFSR Service on all domain controllers.
2. Start the Registry Editor.
3. Navigate to "HKLM\SYSTEM\CurrentControlSet\Services\DFSR".

4. Create a key called "Restore".
5. Create a string value called "SYSVOL".

On one of the existing domain controllers,

6. For the string value called "SYSVOL" give it the value of "authoritative".
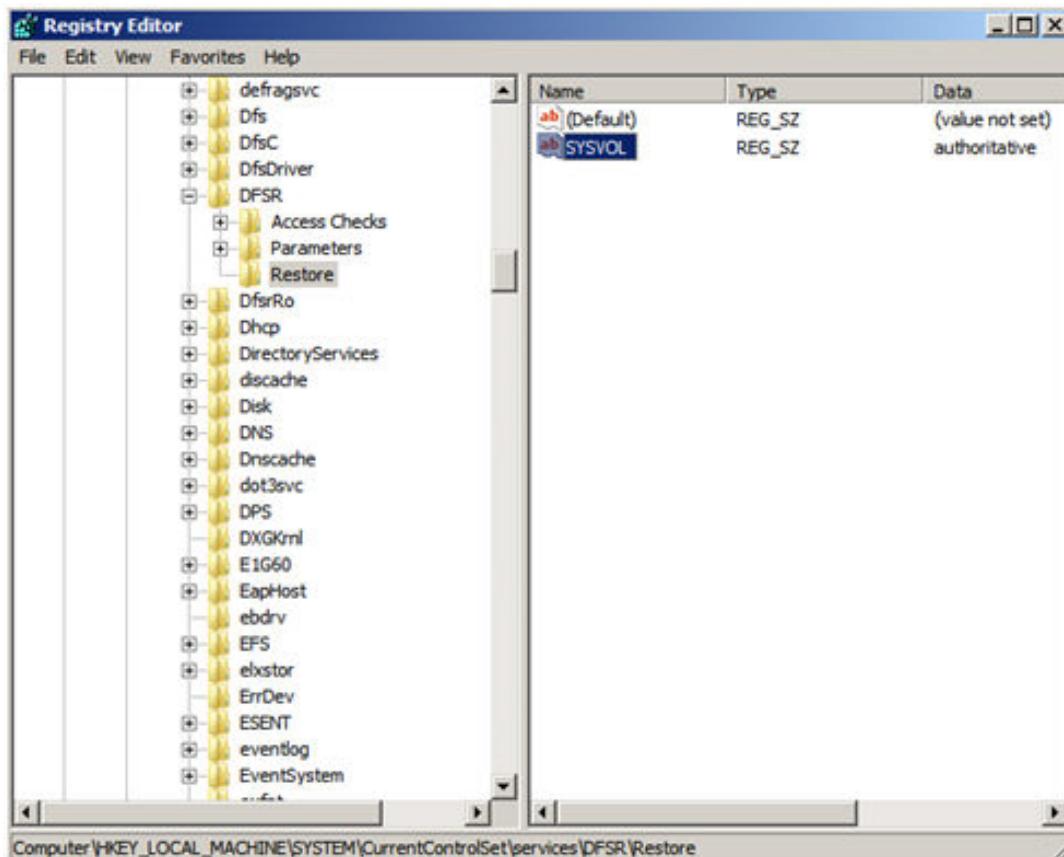
Fig 3. Registry Options

On the remaining domain controllers,

7. For the string value called "SYSVOL" give it the value of "non-authoritative"
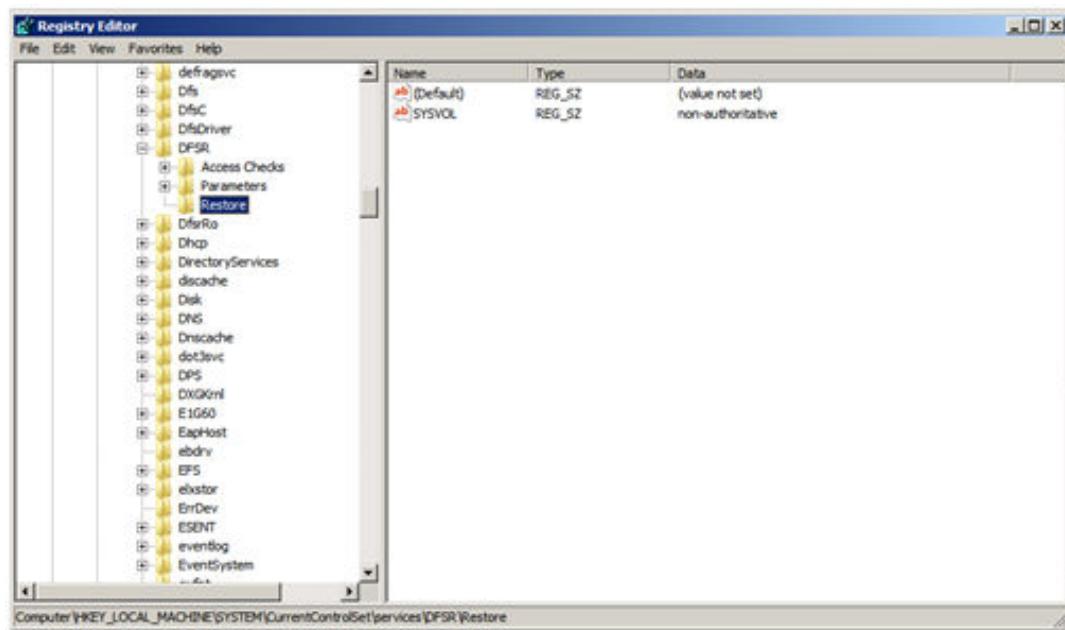
Fig 4. Registry Options

8. Navigate to "HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore".
9. Create a key called "SystemStateRestore".
10. Create a string value called "LastRestoreId".
11. For the string value called "LastRestoreId" give it the value of "10000000-0000-0000-0000-000000000000".
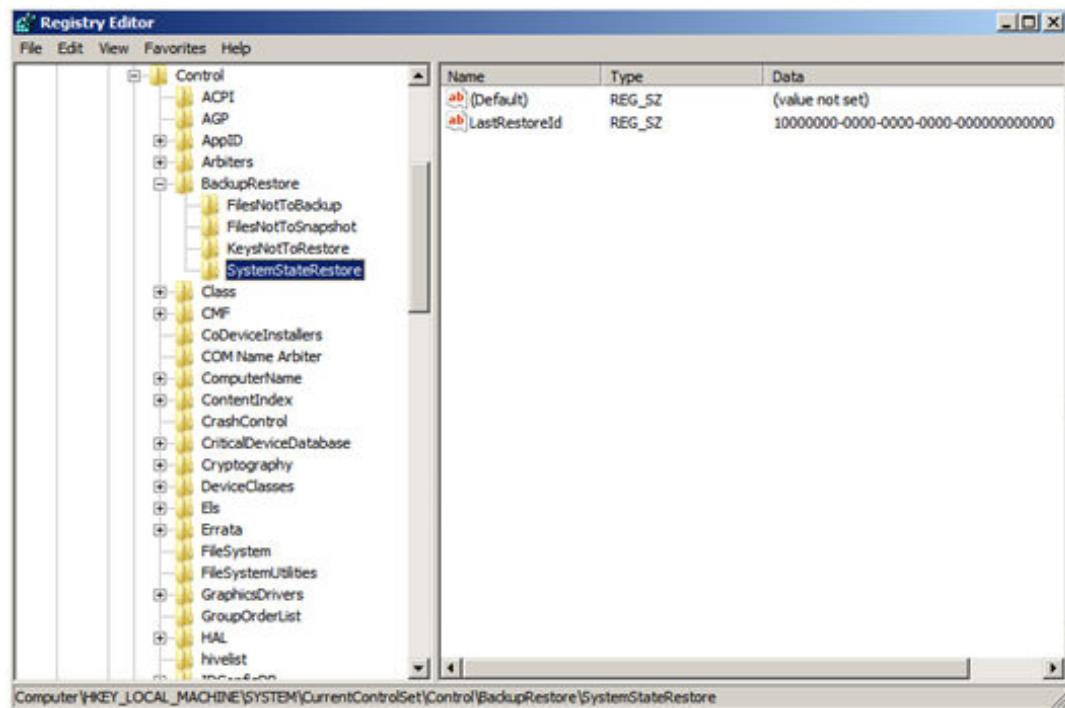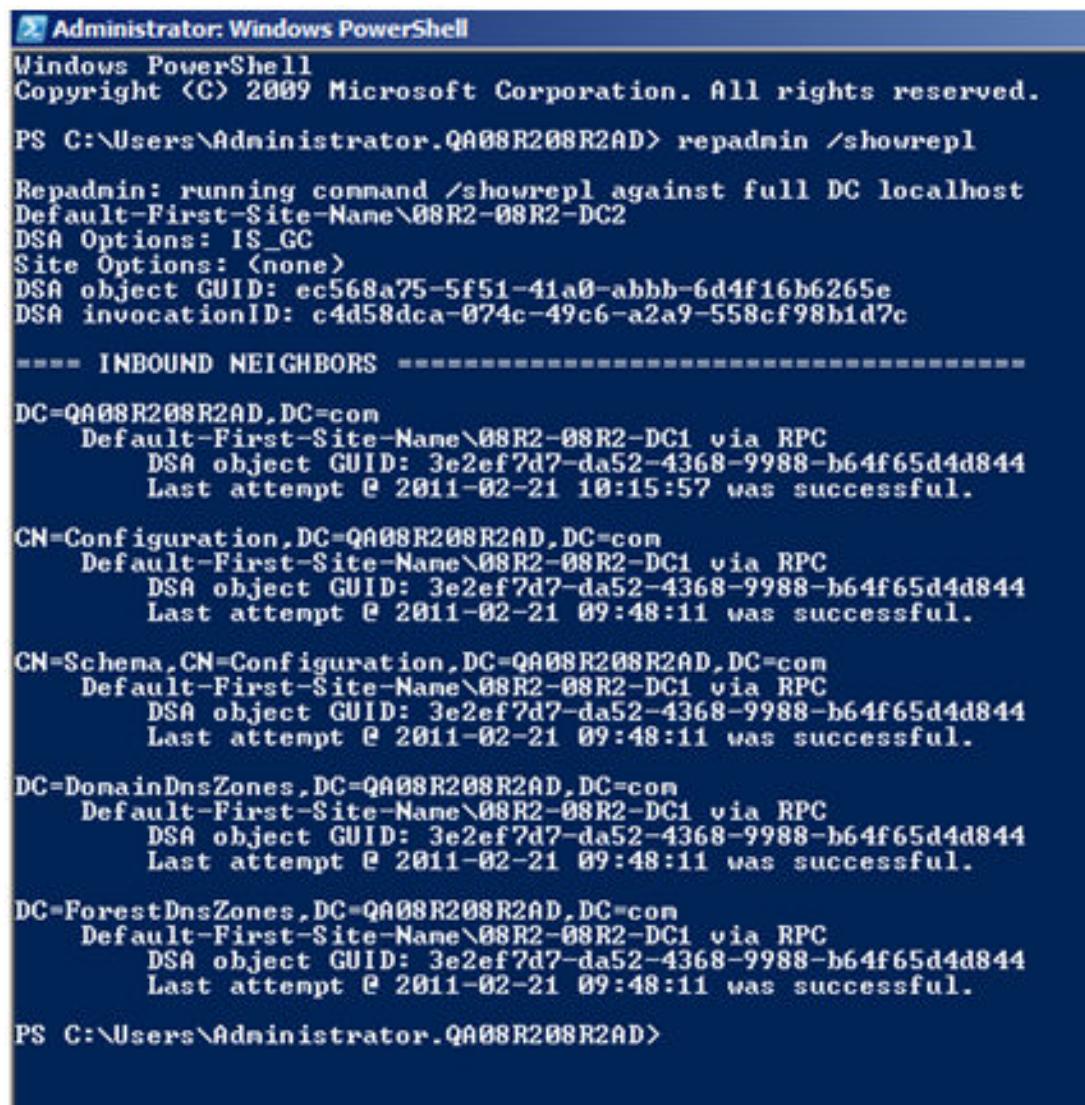
Fig 5. Registry Options

Once the registry settings have been put into place, you must start the DFSR service on the domain controller that was made authoritative, and then on each of the other domain controllers.

To verify the restore was successful open Windows PowerShell and type:

repadmin /showrepl

Fig 6. Repadmin example

You should see a screen similar to the one above showing all connections as successful.

Once everything has been restored, it is highly recommended to remove the registry settings you entered above.

2008/2008 R2 Active Directory Schema with a Single Domain Controller.

1. Stop the DFSR service.
2. Start the Registry Editor.

3. Navigate to "HKLM\SYSTEM\CurrentControlSet\Services\DFSR".
4. Create a key called "Restore".
5. Create a string value called "SYSVOL".
6. For the string value called "SYSVOL" give it the value of "non-authoritative".
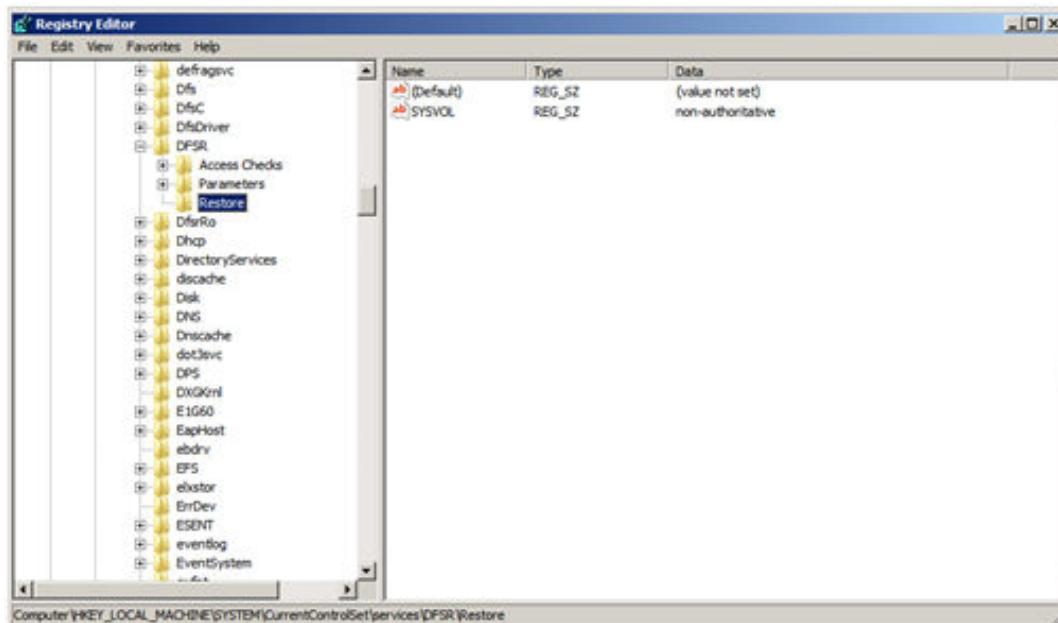
Fig 7. Registry Options

7. Navigate to "HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore".
8. Create a key called "SystemStateRestore".
9. Create a string value called "LastRestoreId".
10. For the string value called "LastRestoreId" give it the value of "10000000-0000-0000-0000-000000000000".
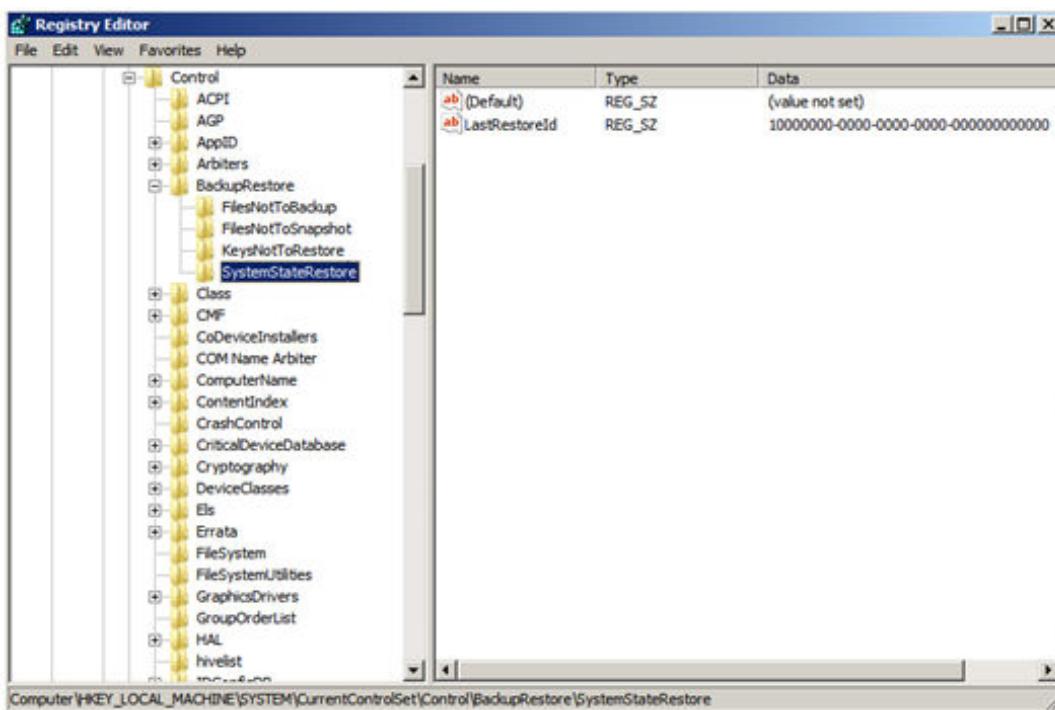
Fig 8. Registry Options

Once the registry settings have been put into place, you must then start the DFSR service. Once everything has been restored, it is highly recommended to remove the registry settings you entered above.

2003 Active Directory schema with multiple domain controllers

NOTE: It is highly recommended to do the authoritative restore from an existing domain controller and not the one you are restoring, this way you will not lose any AD objects and changes since the last backup.

1. Stop the NTFRS Service on all domain controllers.
2. Start the Registry Editor.
3. Navigate to "HKLM\System\CurrentControlSet\Services\NtFrs\Parameters\Backup/Restore\Process at Startup".

4. Double-click on "BurFlags".

On one of the existing domain controllers that will be the "authoritative" Domain Controller,

5. Assign it a value of D4 (hex) or 212 (dec).
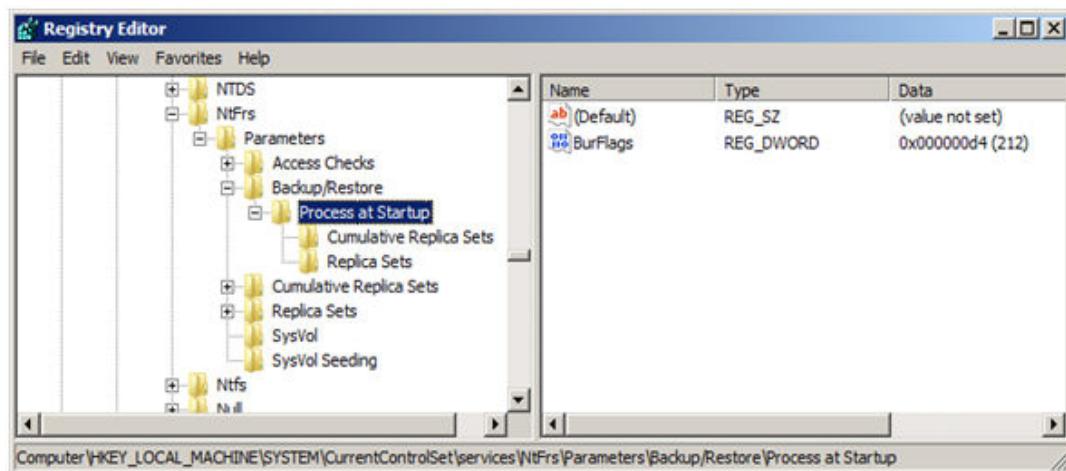
Fig 9. Registry Options

On the remaining domain controllers that are "non-authoritative",

6.   Assign it a value of D2 (hex) or 210 (dec).

Once the registry settings have been put into place, you must start the NTRFS service on the domain controller that was made authoritative, and then on each of the other domain controllers.

To verify the restore was successful open up windows power shell and type:

repadmin /showrepl

In the power shell window you should see all connections as successful

Once everything has been restored, it is highly recommended to remove the registry value from the "BurFlags" registry key you entered above.

2003 Active Directory Schema with a Single Domain Controller.

1.   Stop the NTFRS Service.
2.   Start the Registry Editor.
3.   Navigate to "HKLM\System\CurrentControlSet\Services\NtFrs\Parameters\Backup/Restore\Process at Startup".
4.   Double-click on "BurFlags".
5.   Assign it a value of D2 (hex) or 210 (dec).

Once the registry settings have been put into place, you must start the NTRFS service. Once everything has been restored, it is highly recommended to remove the registry value from the "BurFlags" registry key you entered above.

VMware Consolidated Backup Agent

The UltraBac VMware Consolidated Backup Agent gives users the ability to back up their virtual machines without installing any agent on those machines, and from one central location. Using VMware's snapshot technology, both the FileVM and FullVM selections will back up in-use files and folders.

NOTE: This agent requires that VCB be licensed from VMware, and that a VCB Proxy be configured and available. For more information on VMware Consolidated backup, please see the VMware Web site:

http://www.vmware.com/products/vi/consolidated_backup.html

NOTE: UltraBac's VCB Agent requires that the VMware VCB Framework be installed on the backup host. To download the VCB Framework, please see the VMware Web site:

http://www.vmware.com/download/vi/

VCB Agent Set Creation

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Select the "VMware Consolidated Backup Agent" and click "Next."
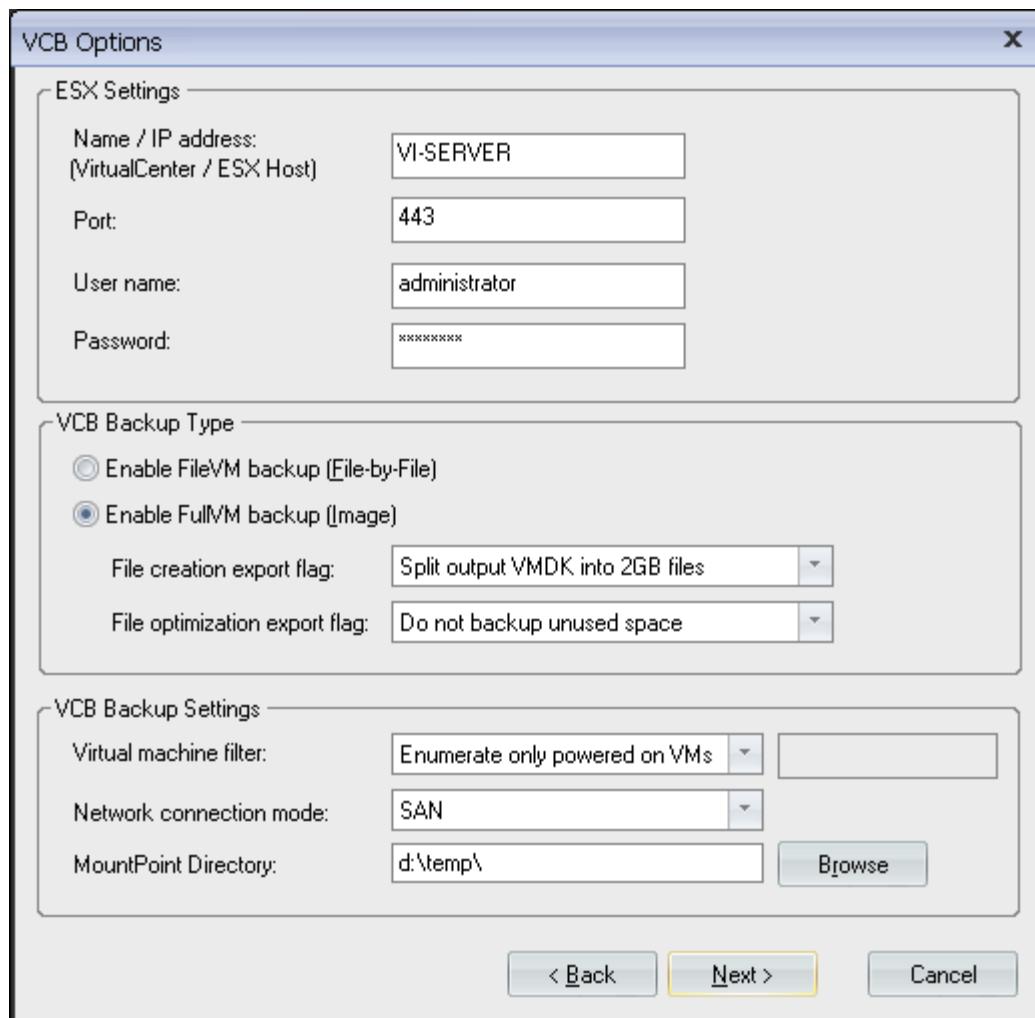
Fig. 1 - VCB Agent options.

3. Type the Windows name or IP address of the VMware proxy in the "Name / IP address" field.
4. Type the port used for connection into the "Port" field. The default is port 443.
5. Type the user name used to log into the VMware proxy in the "User name" field.
6. Type the password for the above user name into the "Password" field.
7. Select the backup type:
   - FileVM – Backs up all files and folders on the selected virtual machine(s).
   - FullVM – Backs up the entire selected virtual machine(s) in one operation.
8. File creation export flag:
   - Split output VMDK into 2GB files
   - Create single monolithic VMDK file
9. File optimization export flag:
   - Do not backup unused space – Only backs up the active clusters on the selected guests.
   - Create flat VMDK with no optimizations – Backs up the entire guest, including unused space.
10. Virtual Machine filter:
   - Enumerate All VMs – Enumerates all VMs available to the VCB proxy.
   - Enumerate only powered on VMs – Enumerates all powered on VMs.
   - Enumerate only powered off VMs – Enumerates all powered off VMs.

- Enumerate by VM name – Enumerates all VMs by VM name.
- Enumerate by IP Address – Enumerates all VMs by IP address
- Enumerate by MoRef – Enumerates all VMs by MoRef ID (Managed Object Reference ID).
- Enumerate by UUID – Enumerates all VMs by UUID (Universally Unique Identifier).

11. Network connection mode:
   - SAN – Reads directly from the SAN used to store the virtual disk. This setting requires VMFS storage and that the SAN/iSCSI location be accessible from both the ESX host and the VCB proxy.
   - NBD – Reads across the network when accessing the virtual disk.
   - NBDSS – Reads across the network when accessing the virtual disk, and all data is transferred across the data in an encrypted stream. Does not support ESX 3.0.x or VC 2.0.x.

12. MountPoint Directory – Used to store the VMDK files during backup.
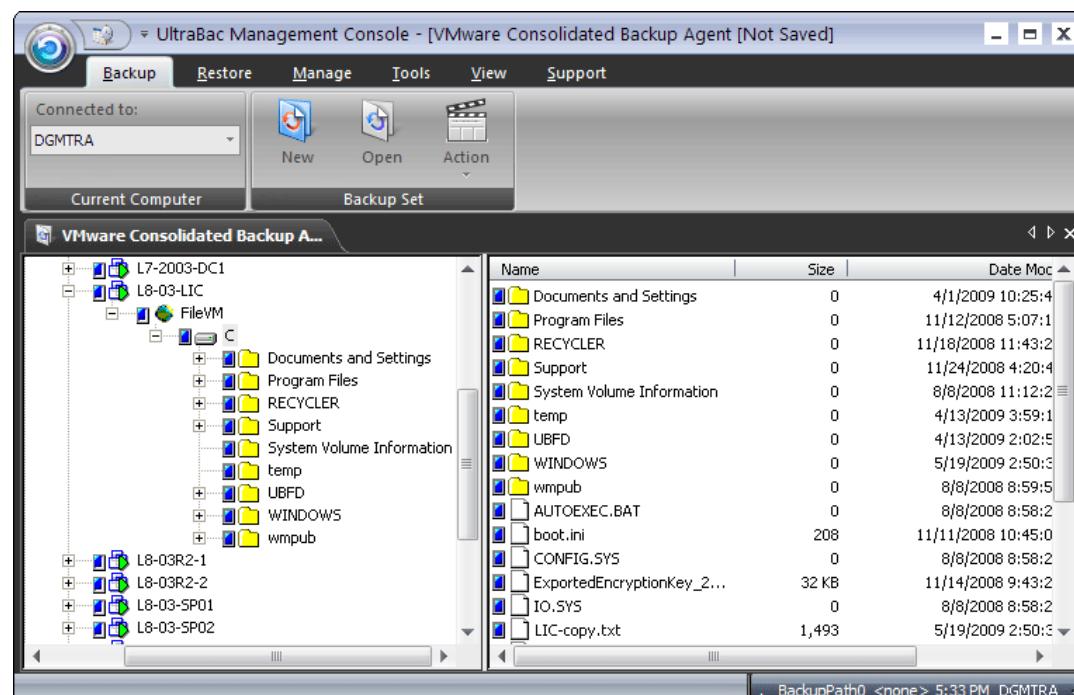
Fig. 2 - Enumerated VCB Agent "FileVM" backup set.

Restoring a VCB Agent Backup

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the index for restore.
3. Select the objects for restore.
4. Click "Operations"/"Restore Selected Files."
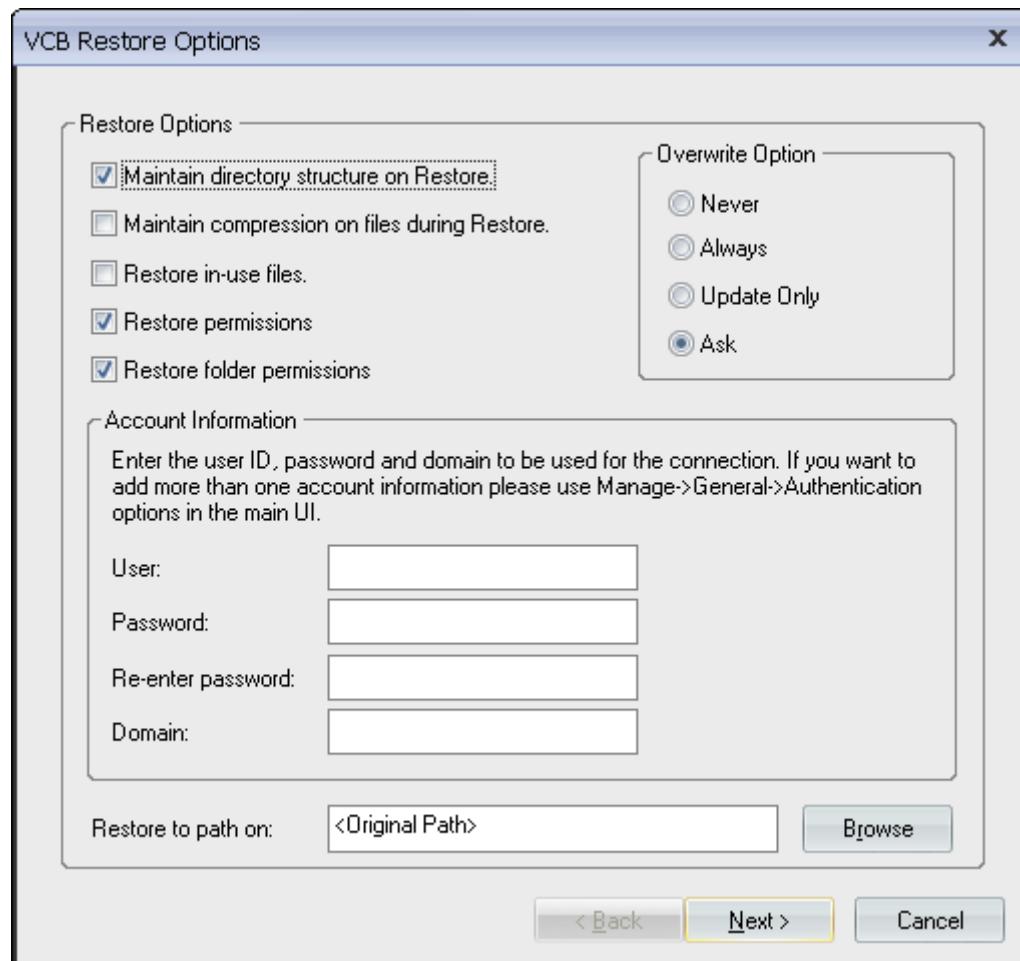
Fig. 3 - VCB Agent Restore Options.

VCB Restore Options:
- Maintain directory structure on Restore – Restore files and folders with the original parent folder structure.
- Maintain compression on files during Restore – If a file was compressed when backed up, that compression will be maintained after restore.
- Restore in-use files – Forces the restoration of in-use files. The overwritten in-use files will not become active until the system is rebooted.
- Restore permissions – Restores previously existing permissions on files.
- Restore folder permissions – Restores previously existing permissions on folders.

Overwrite Options:

- Never – Do not overwrite files.
- Always – Overwrite all files.
- Update Only – Overwrite files when the data being restored is newer than the existing data.
- Ask – When "Ask" is selected, the following options will be available when prompted:
    - Skip File – Do not restore the specified file, and continue the restore.
    - Update – Only overwrite if the file being restored is newer than the existing file.
    - Overwrite – Overwrite the file on disk with the file being restored.
    - Overwrite All – Overwrite existing files with the files being restored.
    - Rename – Rename the file being restored, or restore it to an alternate directory.

Account Information:

When restoring data to a guest in an alternate domain, or where the default UltraBac account does not have access, it is necessary to supply a set of credentials for access to the guest OS.

Restore to path on:

When restoring a VCB Agent backup, the agent will append a path to the restored files:

<vm host>\<guest>\FileVM\<drive letter>

If the specified path is "<u>D:\restore\</u>" and the machine called NEWVM's (hosted on an ESX server named ESXSERVR) C drive is being restored, the path would look like this:

<u>D:\restore\ESXSERVR\NEWVM\C\</u>

SQL Agent

Using the UltraBac SQL Agent, Microsoft SQL can be backed up online, without stopping the services prior to backup. If the SQL services are not running, the backup will not be successful. The SQL agent must be installed on each of the SQL servers you are planning to backup.

Setup and Configuration

Before backup, the SQL server should be registered in the SQL server list:

1. From the Manage tab, click "Agents"/"SQL Agent."
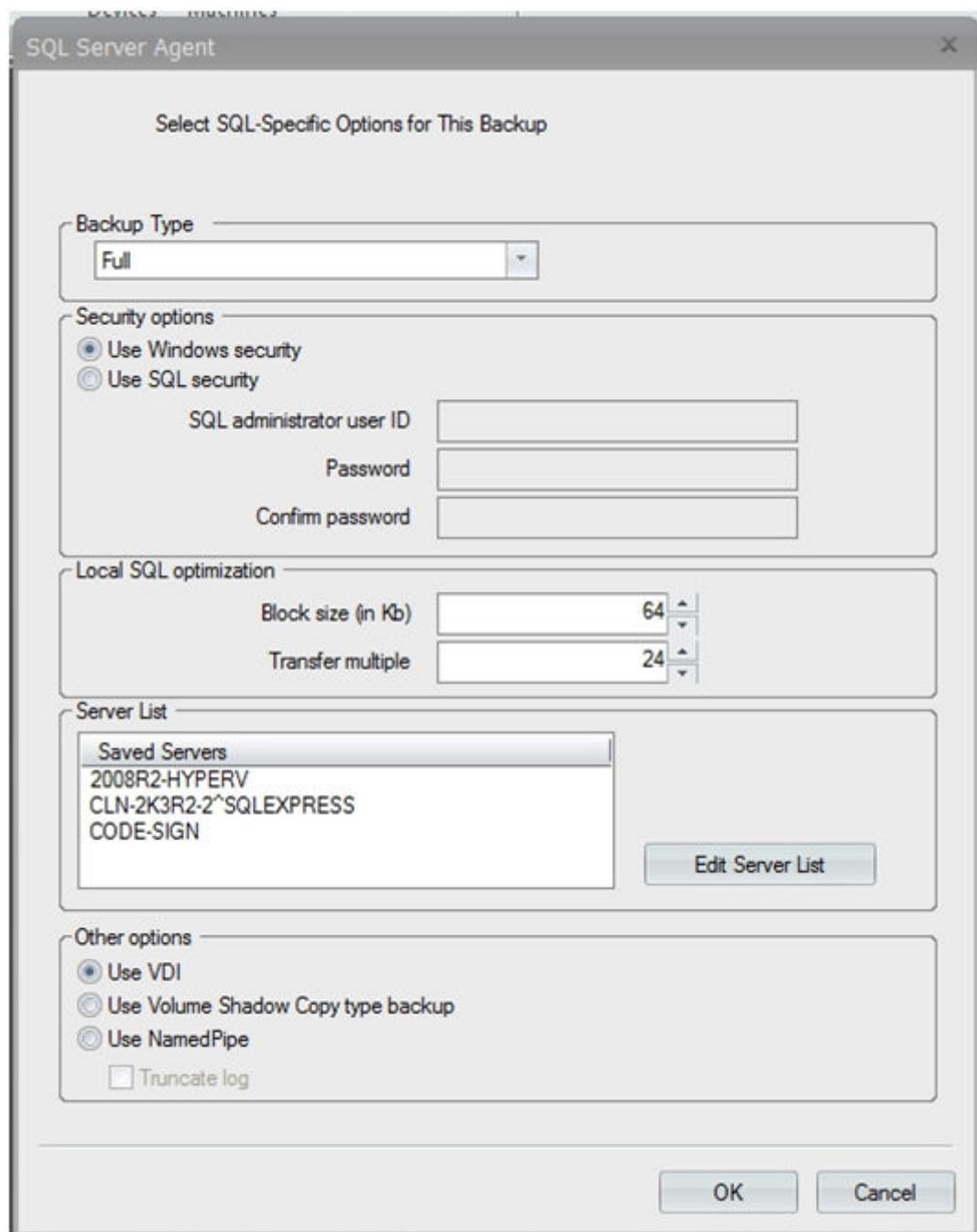
Fig. 1 - SQL Agent options.

2. Click "Edit Server List."
3. Type the SQL server name into the "Server instance" field, or wait for UltraBac to detect the SQL servers in the network and then highlight the desired server by clicking on it.
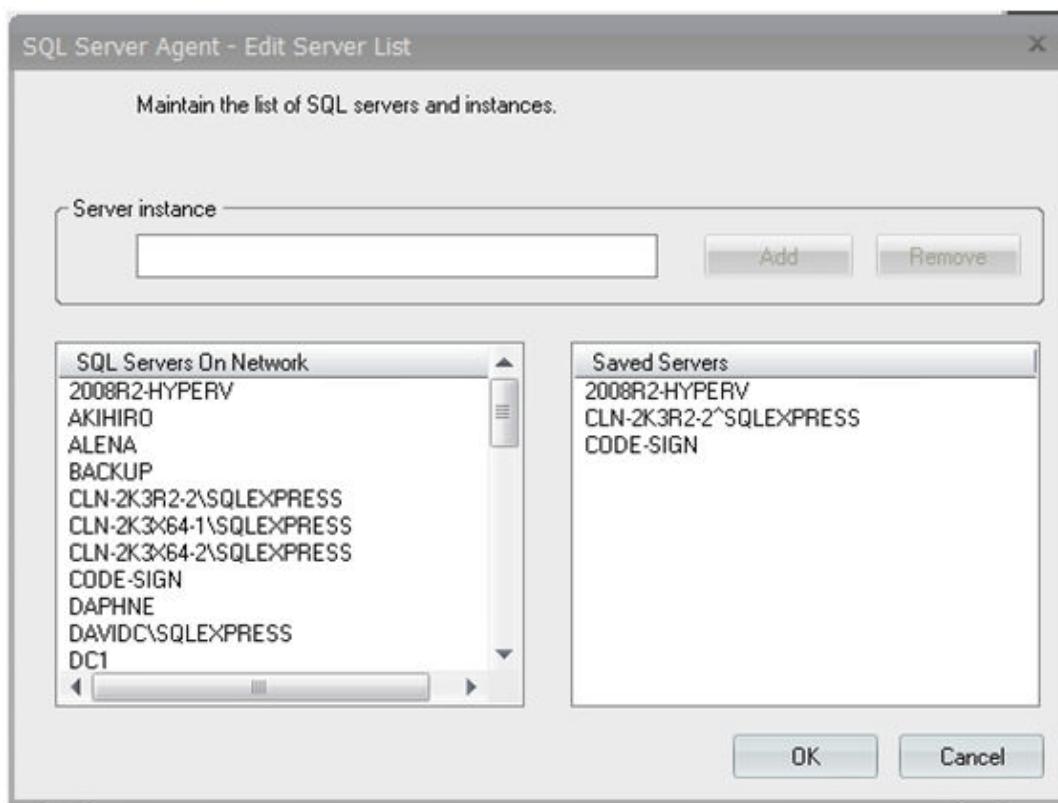
Fig. 2 - Editing the SQL server list.

4. Click "Add."
5. Repeat steps 3 and 4, as needed, for each server to be backed up.
6. When all servers have been added, click "OK."

Creating an SQL Agent Set

After registering all SQL servers to be backed up, create a backup set:

1. Launch the Backup Wizard by selecting the Backup tab and clicking "New"
2. Click "SQL Agent" to highlight the option and click "Next"
3. If the SQL server required isn't displayed (it references the SQL server list), either type in the name of the SQL server \ instance or click the "Discover" button to automatically detect the SQL servers in your network.
4. Check the box next to the servers to be backed up and click "Next".
5. Set the Backup Type from the drop-down box.
6. Check the Security Options and click "Next".
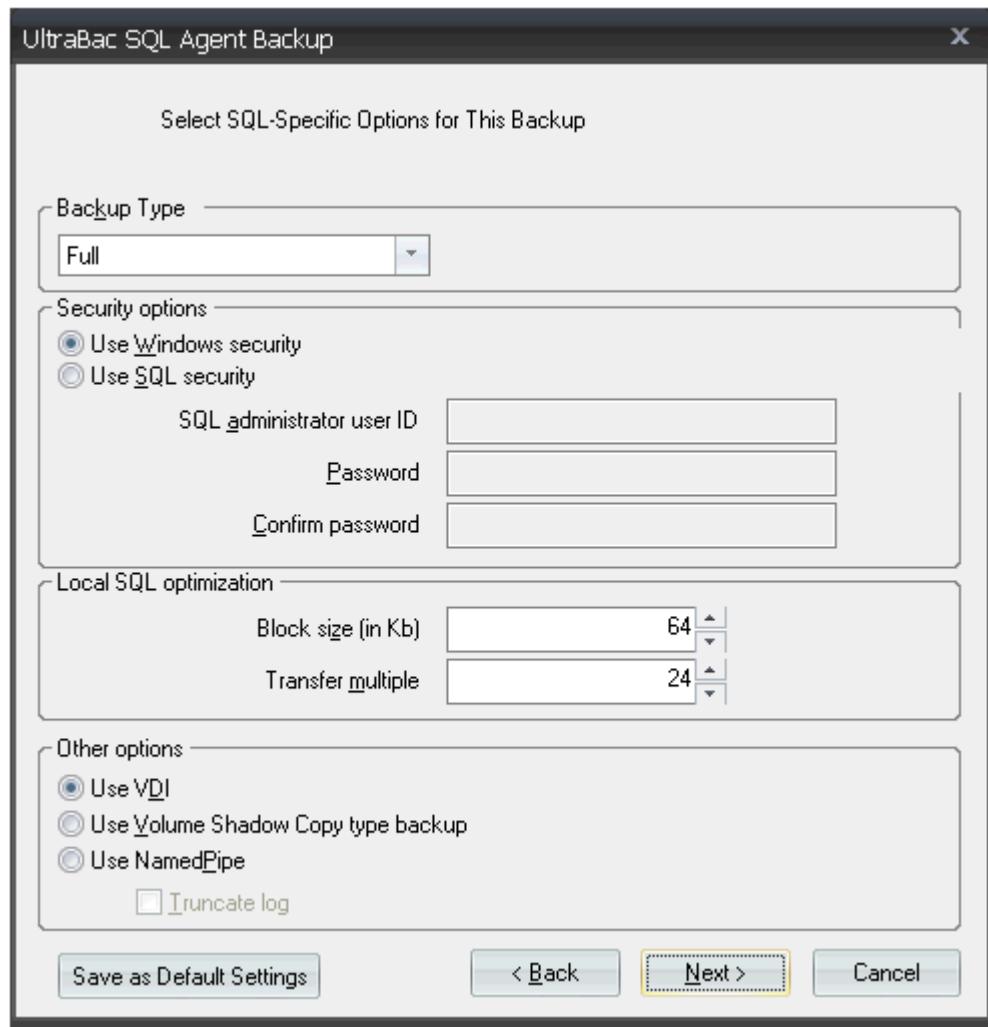
Fig. 3 - SQL Agent Backup options.

7. The Local SQL optimization settings appear as "Block size 64" and "Transfer multiple 24" by default. These are the recommended settings.
8. Select a radio button under Other options. "Use VDI" is automatically selected by default.
9. Click "Next".
10. Type a description for the set as it will appear in the backup log and click "Next".
11. Click "Finish" to load the SQL set into the file viewer.
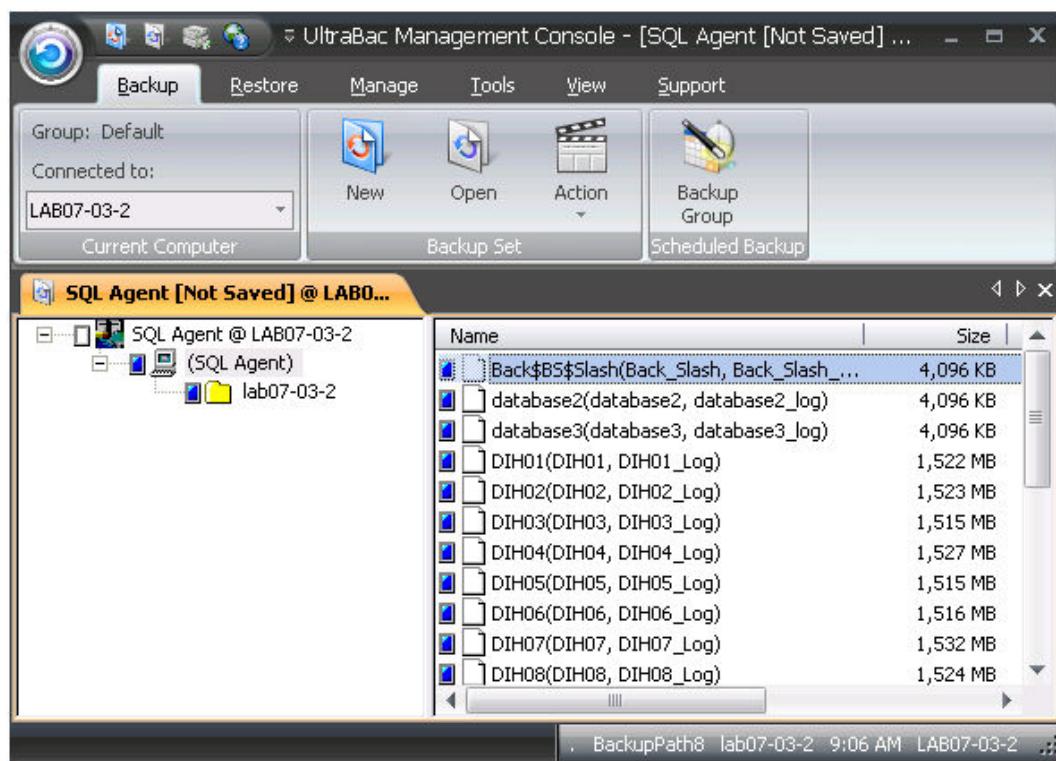
Fig. 4 - SQL backup set loaded in the File Viewer.

Backup Set Options

These options modify the way UltraBac handles SQL data during backup.

Enumeration Mode Options

Specifies the method used to search for and enumerate SQL servers:

- Local Search Only – Displays only the servers listed in the local "Client Network Utility."
- Network Search Only – Queries and displays all SQL servers on the LAN.
- Local and Network Search – Displays all servers listed in the local "Client Network Utility" and all servers queried on the LAN.

UltraBac SQL Agent Backup Options

Backup Type – Specifies the type of backup to be performed:

- Full – Backs up all selected databases and transaction logs.
- Incremental – Backs up and truncates the transaction logs.
- Differential – Backs up the transaction logs, but does not truncate.

Local SQL Optimization – Defines the block size to be used during backup. The default is 64Kb. The transfer multiple is 24. In most cases, these preference should not be changed.

Security Options – Specifies the account information to be used during the SQL backup:

- Windows security – Uses the default UltraBac account during the SQL backup.
- SQL security – Uses the specified SQL security account during the SQL backup.

Other Options:

- Use VDI – Forces UltraBac to use the "VDI" protocol during backup.
- Use Volume Shadow Copy – Forces UltraBac to use the "Volume Shadow copy" protocol during backup.
- Use Named Pipe – Forces UltraBac to use the "Named Pipes" protocol during backup. Truncate Log – Truncates the transaction logs after the selected backup operation is complete. If this preference is not checked, the transaction logs will NOT be truncated.

Restoring an SQL Backup

To restore an SQL database:

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select the objects for restore.
3. Click "Action"/"Restore this Backup."
4. To restore the SQL database to the original location/server, click "Next" at the "UltraBac SQL Agent Restore Options" screen.
5. At the "Restore Options" screen, click "Restore."

> NOTE: When restoring incremental or differential SQL backups, the full backup must be restored first, then all incremental or differential backups must be restored in the order they were backed up.

UltraBac also has the ability to restore a database to an alternate server, or the original server, with alternate database and file names.

SQL Agent Restore Options
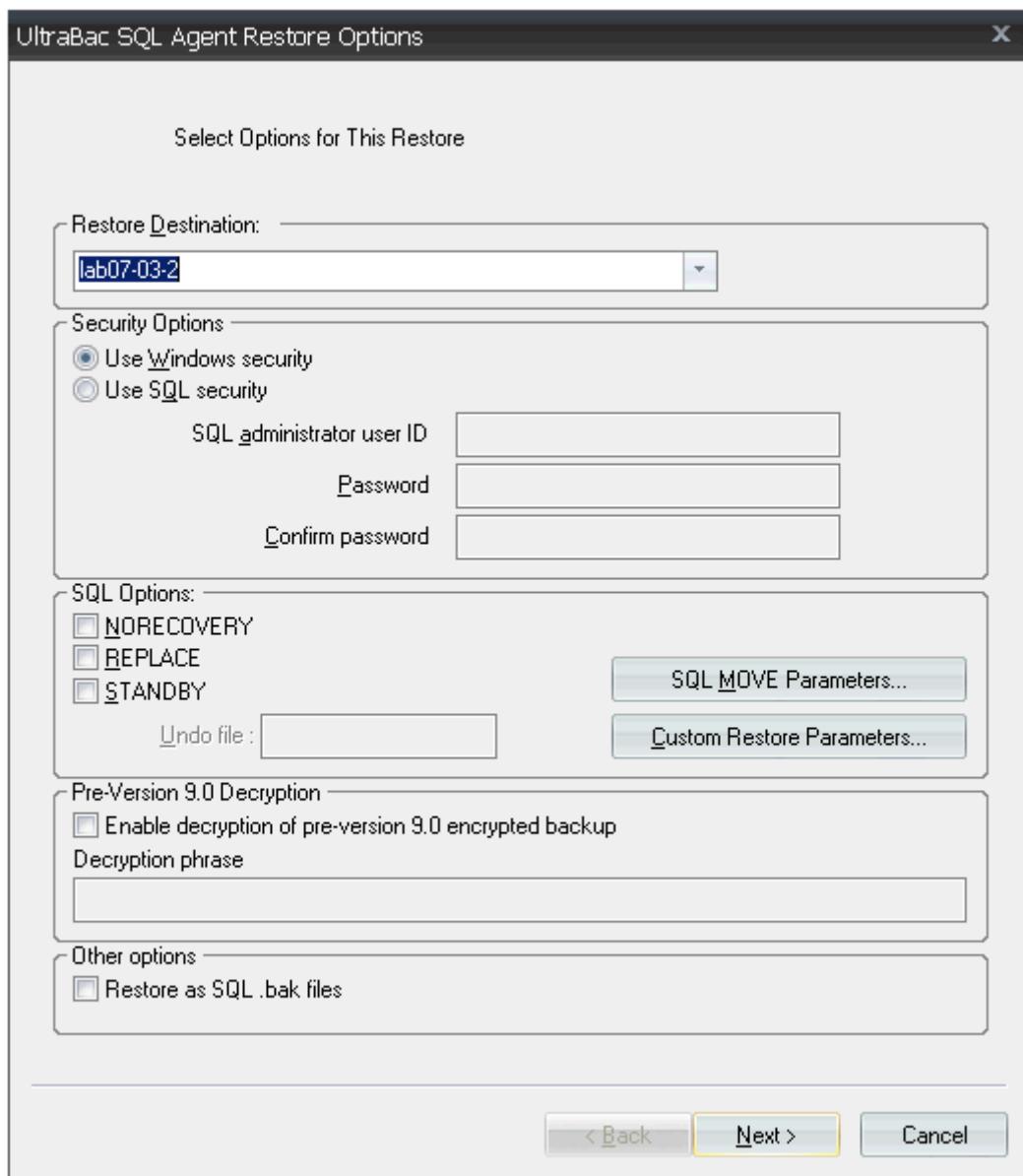
Fig. 5 - SQL Agent Restore Options.

- Restore Destination – Drop-down menu lists all servers registered in the local Client Network Utility.
- Security Options:
    o Use Windows security – Uses the current login account for restore.
    o Use SQL security – Uses the specified credentials for restore.
- SQL Options:
    o NORECOVERY – Equivalent to the NORECOVERY option in Microsoft's SQL. See the Microsoft SQL documentation for information: http://msdn.microsoft.com/en-us/library/aa238405.aspx
    o REPLACE – Used when restoring a database to a remote SQL server, when the same database name exists on the target machine.

- o STANDBY – Equivalent to the STANDBY option in Microsoft's SQL. Refer to Microsoft SQL documentation for information: http://msdn.microsoft.com/en-us/library/aa238405.aspx
- SQL Move Parameters – Use the "SQL MOVE Parameters" to move or rename files when restoring an SQL database.
- Custom Restore Parameters – Custom restore parameters can be specified to perform a "point-in-time" restore, or any custom restore available to SQL.
- Pre-Version 9.0 Decryption – Prior to UltraBac Version 9.0, the software used Blowfish encryption. Selecting this option will allow you to restore any SQL backups that were made with versions of UltraBac prior to 9.0 that used this type of encryption.
- Restore as SQL .bak files – This option will restore the UltraBac SQL backup to a native Windows SQL Backup format. Once in this format, you can restore the database using the standard Microsoft SQL restore methods: http://msdn.microsoft.com/en-us/library/ms177429.aspx

---

NOTE: For a detailed description of the "SQL Move Parameters," please see the UltraBac Knowledge Base:

See UBQ000205: SQL Move Parameters

MySQL Agent

Starting in v9.1, UltraBac now has an agent to back up and restore local MySQL databases.

NOTE: Currently, the UltraBac MySQL Agent only supports the backup and restore of databases that are local to the backup host.

Configuring the MySQL Agent

Before creating a set for using the MySQL Agent, the locations of the MySQL executables and the temporary scripts directory must be set. These options are set under the MySQL Agent options:

1. From the "Options" section of the Manage tab, select "Agents"/"MySQL Agent."
2. In the "MySQLDump.exe Path:" field, type in or browse to the location of MySQLDump.exe.
3. In the "MySQL.exe Path:" field, type in or browse to the location of MySQL.exe.
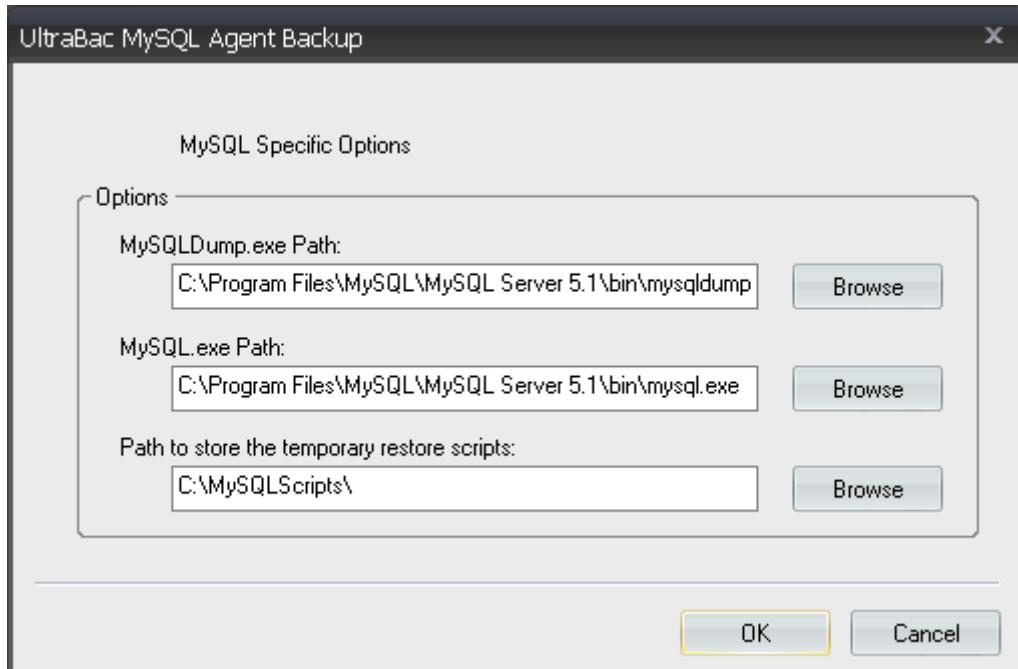
Fig. 1 - MySQL Agent options.

4. In the "Path to store the temporary restore scripts:" field, type in or browse to a directory that will store the specified restore scripts.
5. Click "OK" to save.

Backing up with the MySQL Agent

After setting the agent preferences, a backup set can be created.

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Select "MySQL Agent" from the list, and click "Next."
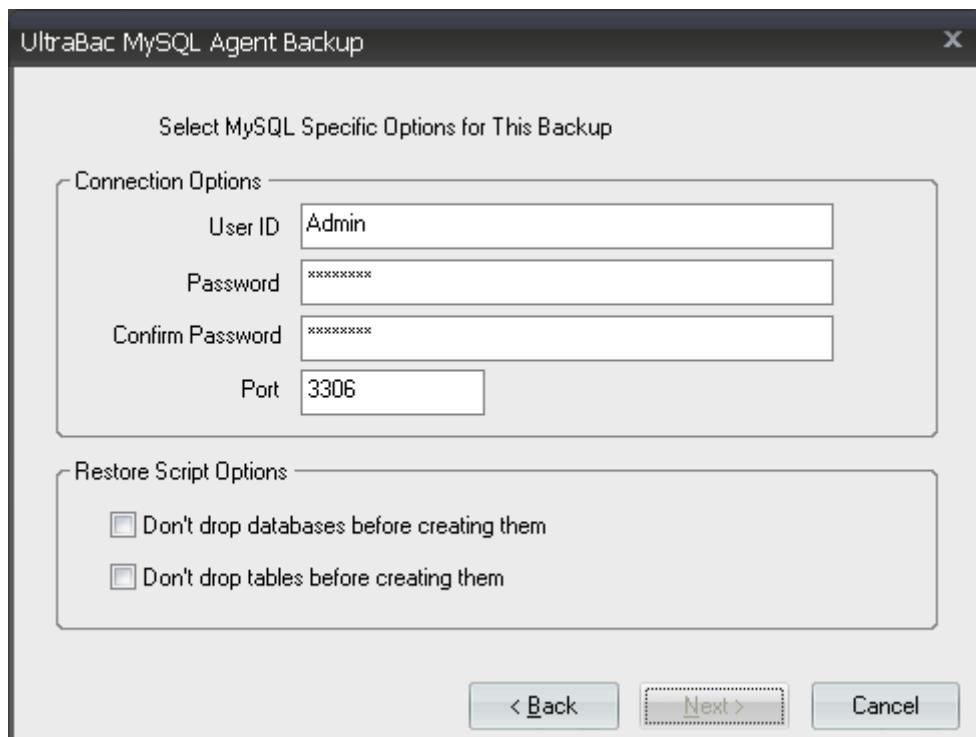
Fig. 2 - Creating the MySQL Agent set.

3. In the User ID field, enter the account used to log in to and administer MySQL.
4. In the Password field, enter the password for the MySQL account.
5. In the Confirm Password field, re-enter the password for the MySQL account.
6. In the Port field, enter the port used by the MySQL instance.
7. Set any other options.
8. Click "Next."
9. Set the backup set description, and click "Next."
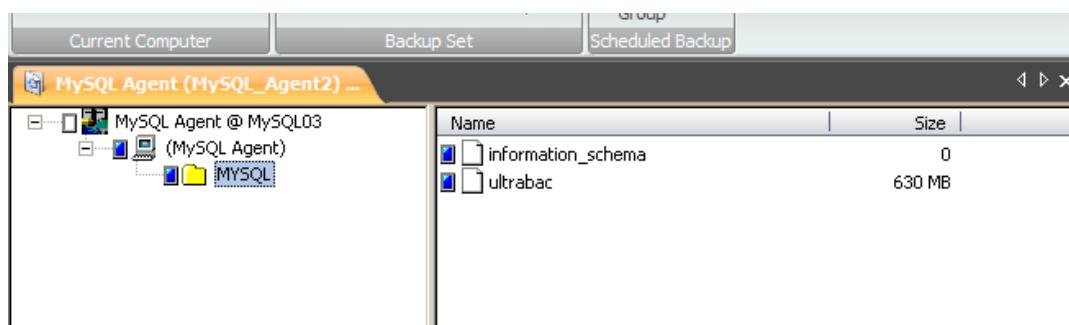
Fig. 3 - Enumerated MySQL Agent set.

10. Select "View/Edit files in the backup set" and click "Finish."

- Don't drop databases before creating them - Sets the restore script to perform the restore without dropping the database.
- Don't drop tables before creating them - Sets the restore script to perform the restore without dropping the tables.

Restoring a MySQL Agent Backup

To begin the restore process:

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the index for restore.
3. Select the objects for restore.
4. Click "Action"/"Restore this Backup."
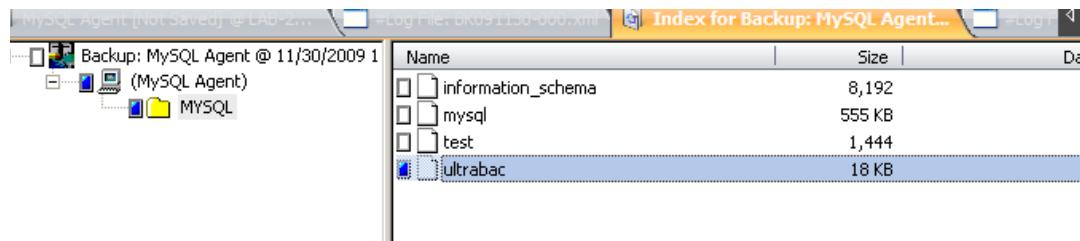
Fig. 4 - MySQL Agent backup index loaded into the file viewer.

Restoring a MySQL Database to a flat File

To begin the restore process:

1. Choose the database you want to restore
2. Go to Action >> Restore
3. Choose the Option "Restore To Flat File"
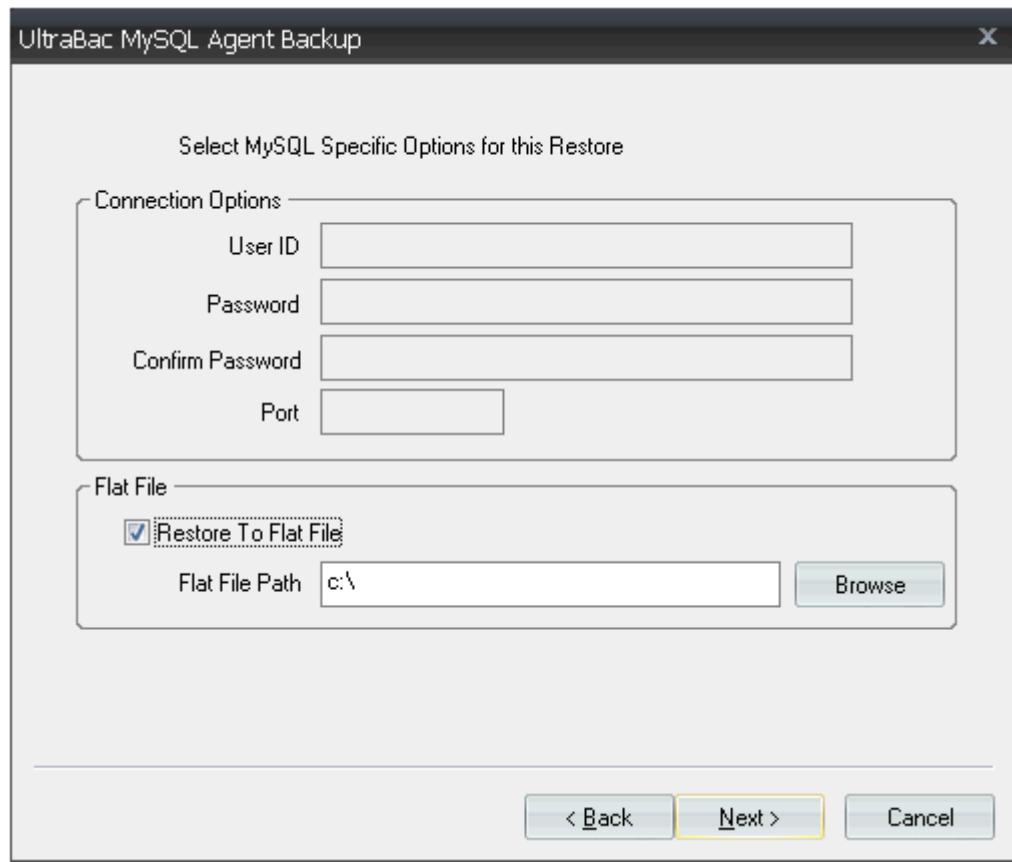
Fig. 5 - Flat File restore options

4. Enter the path you want the restore to backup to.
5. Click "Next".
6. Click "Restore".

Exchange Agent

Exchange Agent

Using the UltraBac Exchange Agent, Exchange versions 2010, 2007, 2003, 2000 and 5.5 can be backed up online without stopping the services prior to backup. If the Exchange services are not running, the backup will not be successful.

Setup and Configuration

> NOTE: The UltraBac Exchange Agent must be installed on the server hosting Exchange.

The default UltraBac account ("Tools"/"Options"/"General"/"Accounts") must have sufficient privileges to run an Exchange backup and restore. These permissions are defined through the Exchange System Manager (or the Exchange 5.5 Administrator), which must be installed on the UltraBac host system in order to perform backups. To confirm the default UltraBac account has sufficient privileges in Exchange 2000/2003:

1. Open the Exchange System Manager.
2. Right click on the "Organization name," and select "Delegate Control."
3. When the Exchange Administrator Delegation Wizard opens, click "Next."
4. If the default account used for backup does not appear, click "Add."
5. In the "Group or User" field, enter the default UltraBac account.
6. Select "Exchange Permissions Admin" from the drop-down "Role" menu.
7. Click "OK" to save changes.

To check permissions in Exchange 2007:

1. Open the Exchange Management Console.
2. Highlight the Exchange Organization Configuration node.
3. If the UltraBac account is not listed, right click on "Organization Configuration" and select "Add Exchange Administrator."
4. When the Add Exchange Administrator wizard appears, click "Browse" and select the UltraBac user account.
5. Ensure that "Exchange Organization Administrator" role is selected and click "Add."

To check permissions in Exchange 2010:

1. Open the Exchange Management Console.
2. Go to the toolbox and open the Role Based Access Control User Editor.
3. Click on Organization Management. If the UltraBac account is not listed, click on "Details" and Scroll down to "Members" and click the UltraBac users and click the "OK" Button
4. Then on the Role Group page, click "Save".

> NOTE: For information on restoring an Exchange 5.5 server, please visit the "**Exchange 5.5 Agent"** section of the User Manual:
>
> **UltraBac User Manual: Exchange 5.5 Agent**

Creating an Exchange Agent Set
After confirming all Exchange permissions are set, create a backup set:

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Click "Exchange Agent" to highlight the option, and click "Next."
3. Enter the name of the exchange server or click "Discover" to have UltraBac search for it.
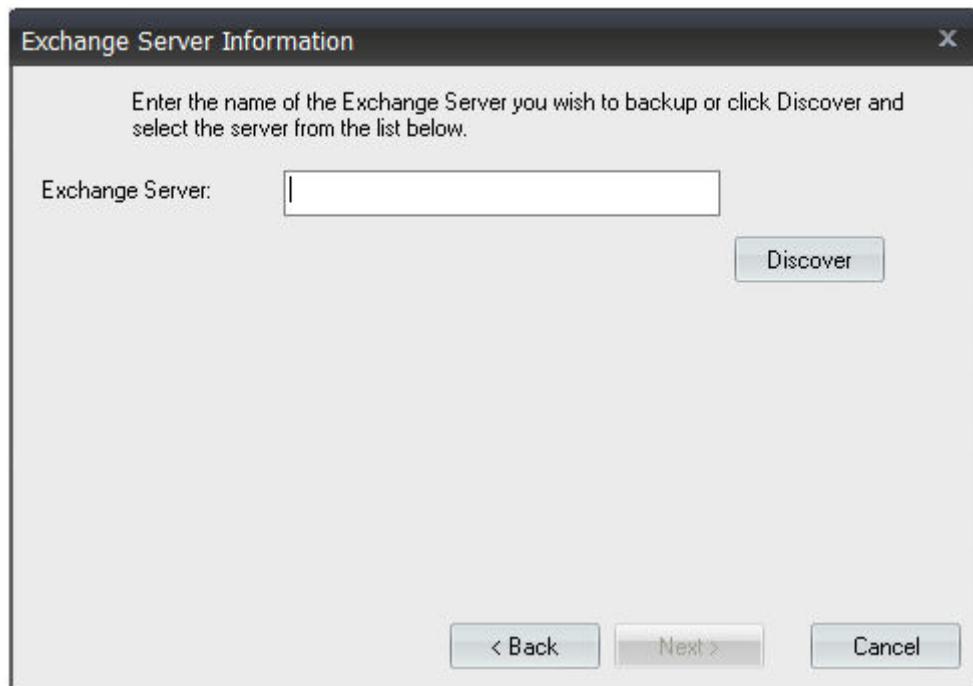
Fig. 1 - Exchange Server Information

4. Select the Exchange server to be backed up.
5. Select the type of Exchange backup to be performed:

   o Full – Back up the database and transaction logs, and truncate the transaction logs.
   o Incremental – Back up only the transaction logs, and truncate the transaction logs.
   o Differential – Back up only the transaction logs, but do not truncate the transaction logs.
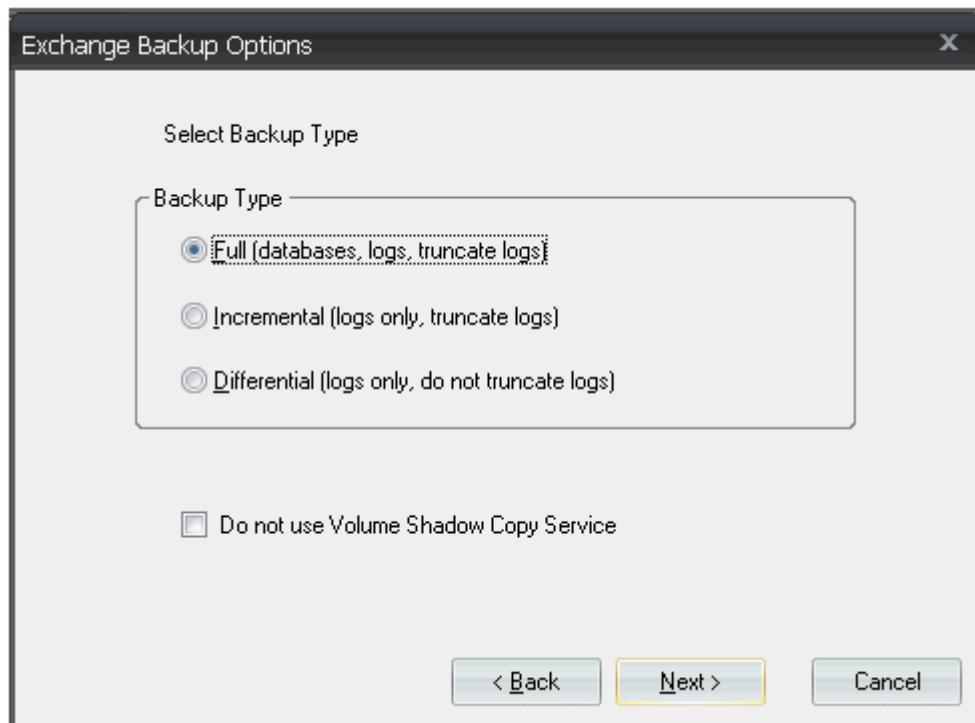
Fig. 2 - Exchange backup options.

NOTE: The Volume Shadow Copy Service must be used in Exchange 2010

6. Enter the description for the backup set as it will appear in the backup log.
7. At the Backup Wizard summary select "View/Edit files in the backup set" to view the file selections and modify the selection logic.
8. Click "Finish."
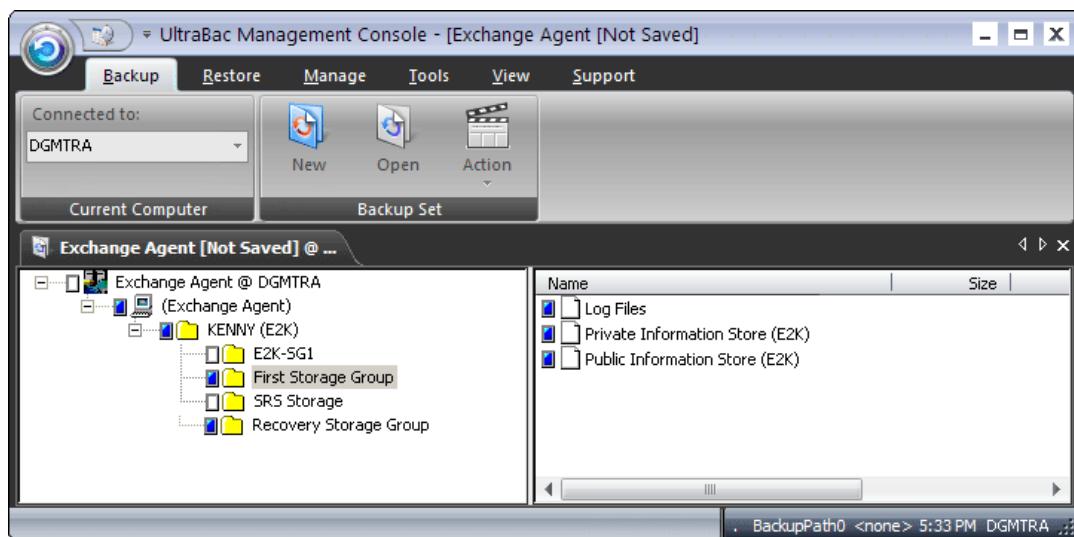
Fig. 3 - Viewing Exchange servers in the File Viewer.

Restoring an Exchange Server - Exchange 2000/2003/2007/2010

> NOTE: To restore an Exchange database, the restore target system must have the same version, service pack, and hotfix level of Exchange installed. If restoring to an alternate Exchange server, the "site" and "organization" must be the same as the original Exchange host.

> NOTE: To restore an Exchange database to the same location as the original, the Recovery Storage Group must first be removed after the database has been unmounted or the restore will attempt to overwrite the Recovery Storage Group.

Preparing the Exchange 2000/2003 Server for Restore

All Microsoft Exchange services must be running, and the Mailbox and Public Folder Stores must be dismounted. Also, the preference, "This Database can be overwritten by a restore," must be checked for a restore to be allowed:

1. Open System Manager.
2. Expand the hierarchical tree until you can see the "Mailbox Store" and "Public Folder Store".
3. Right click on the "Mailbox Store" and select "Dismount Store".
4. Right click on the "Public Folder Store" and select "Dismount Store".

> NOTE: It is highly recommended to move the log files to a separate location so that the log files can be replayed if needed.

5. Clear the contents of the "mdbdata" folder.
6. Right click on the "Mailbox Store," click "Properties," and access the Database tab.
7. Click "This Database can be overwritten by a restore," and click "OK."
8. Right click on the "Public Folder Store," click "Properties," and access the Database tab.
9. Click "This Database can be overwritten by a restore," and click "OK."

Preparing the Exchange 2007 Server for Restore

1. Open the Exchange Management Console.
2. Expand the Server Configuration node and select a mailbox.
3. In the main window, select a database to restore.
4. Right click the database and select "Dismount."

> NOTE: It is highly recommended to move the log files to a separate location so that the log files can be replayed if needed.

5. Clear the contents of the mailbox store folder
6. Right click the database again and select "Properties."

7. In the "Properties" dialog, check "This database can be overwritten by a restore" and click "OK."
8. Repeat for all databases to be restored.

NOTE: If the Exchange 2007 server environment is utilizing the Exchange 2007 High-Availability options (LCR, SCR, or CCR), the restore process is different than a standard Exchange 2007 restore.

See UBQ000257: Exchange 2007 SCR / CCR Restores

NOTE: UltraBac can restore the Mailbox Store to a recovery storage group in order to recover individual mailboxes.

See UBQ000250: Exchange 2007 Support
See UBQ000265: Using the Exchange 2007 Recovery Storage Group

---

Preparing the Exchange 2010 Server for Restore

1. Open the Exchange Management Console.
2. Expand the Organization Configuration node and select a mailbox.
3. In the main window, select a database to restore.
4. Right click the database and select "Dismount."

NOTE: It is highly recommended to move the log files to a separate location so that the log files can be replayed if needed.

---

5. Clear the contents of the mailbox database folder
6. Right click the database again and select "Properties."
7. In the "*Properties*" dialog, check "This database can be overwritten by a restore" and click "OK."
8. Repeat for all databases to be restored.

NOTE: There may be times in which you will need to restore a single mailbox.

See UBQ000259: Single Mailbox Restore with Exchange 2010 Recovery DB

Restoring the Exchange Database

After preparing the server for restore, begin the restore process:

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select the objects for restore. During ALL restore operations, the Exchange logs MUST be selected.
3. Click "Action"/"Restore this Backup."

4. To restore the Exchange database to the original location/server, click "Next" at the "General Restore Options" screen.
5. At the "Restore Options" screen, click "Restore."

NOTE: For information on restoring an Exchange 5.5 server, please visit the "**Exchange 5.5 Agent"** section of the User Manual:

UltraBac User Manual: Exchange 5.5 Agent

Restoring Exchange to a "Flat File"

To restore an Exchange database as a flat file:

1. Check "Restore Files to Non-Exchange Folder."
2. Type in or browse to the target location.
3. Click "Next."
4. Click "Restore."
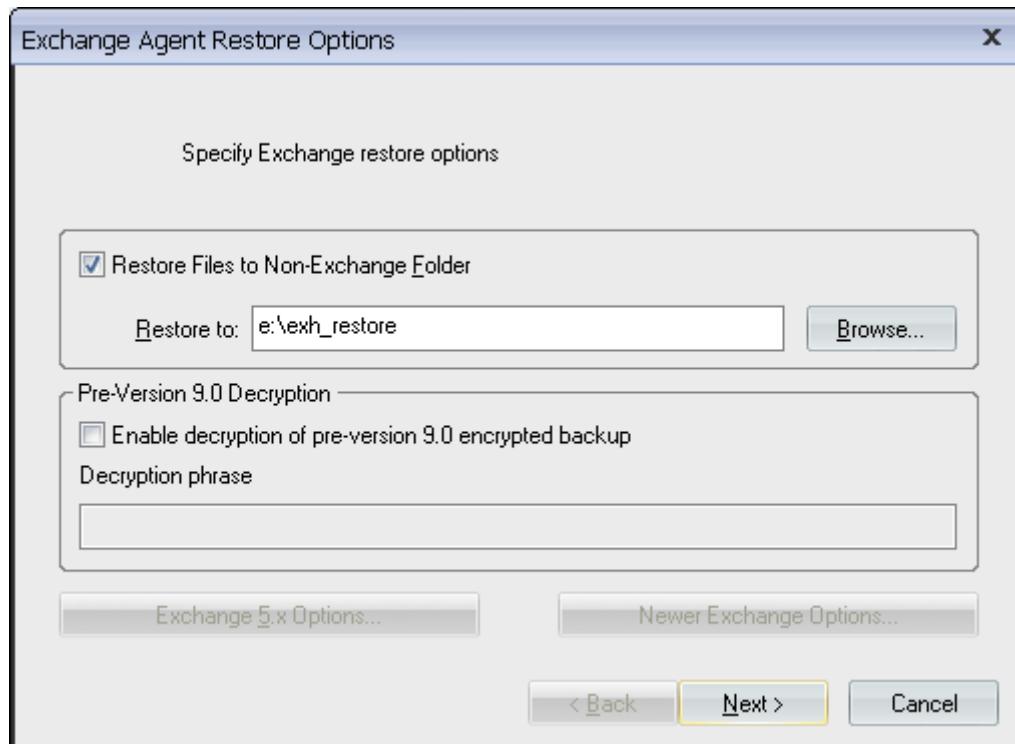
Fig. 4 - Restoring an Exchange backup to a flat file.

NOTE: If the original exchange server is not online, then the flat file restore will fail with an Error 10061. Please visit the following knowledge base article on how to work around this issue.

See UBQ000263: Exchange Flat-File Restore if Original Exchange Server Offline

Exchange 2000/2003 Specific Options

By default, UltraBac is set to restore the Exchange database to its original location and server. To restore to an alternate server, perform a multipart restore, or use other advanced options, click "Newer Exchange Options" from the "Exchange Agent Restore Options" screen.
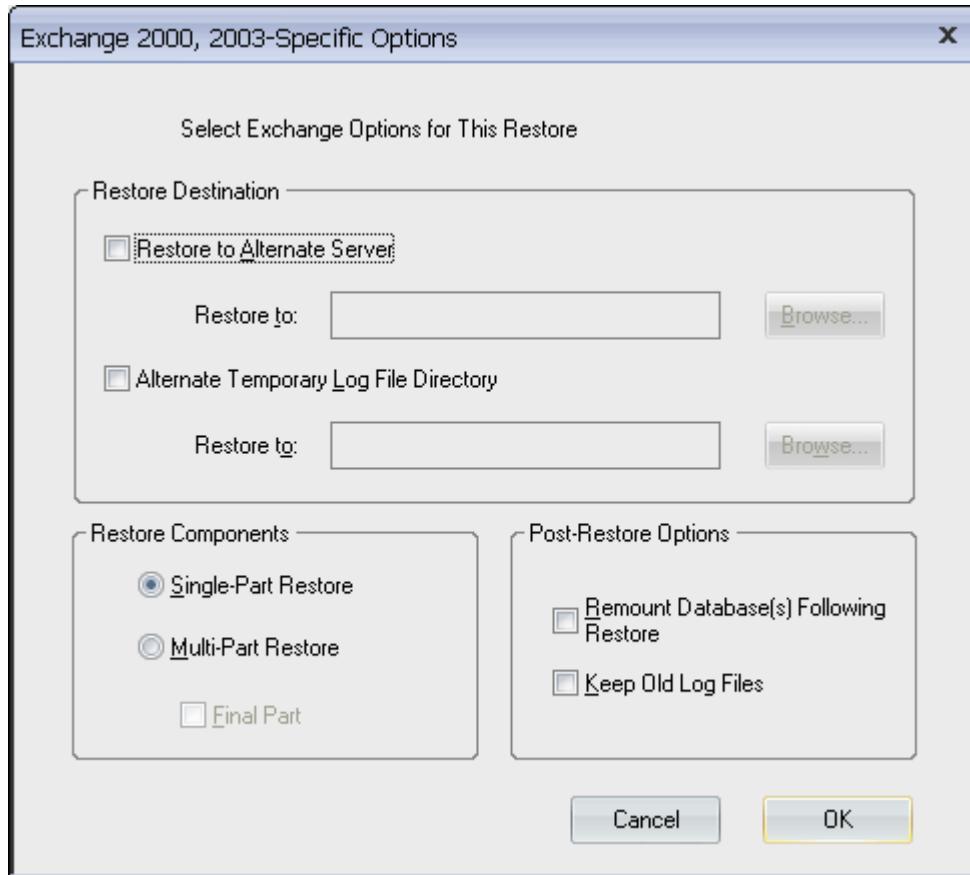
Fig. 5 – Exchange 2000, 2003 options.

To restore to an alternate Exchange server:

1. Check "Restore to Alternate Server."
2. Type or browse to the Windows name or IP address of the restore target.
3. Click "OK."

To restore the Exchange transaction logs to an alternate path:

1. Check "Alternate Temporary Log File Directory."
2. Browse to or type in the target path for the log files. This path should be entered in as it would appear locally on the Exchange restore target (i.e. "C:\Program Files\Exchsrvr\temp_log").
3. Click "OK."

Post-Restore Options

- Remount Database(s) Following Restore – Check this option to remount the Exchange database after restore.
- Keep Old Log Files – This option will instruct UltraBac to not overwrite existing Exchange transaction logs.

NOTE: For a detailed description of restoring an Exchange 2003 database to an Exchange Recovery Store, please see the UltraBac Knowledge Base:

See UBQ00227: - Recovering to an Exchange 2003 Recovery Store

---

Overview of "Multipart Restore"
A "multipart restore" is performed when restoring a full backup, including differentials or incrementals, in one restore "session." A multipart restore is performed using the same basic restore process as the standard Exchange restore. The order of the multipart restore should be:

1. Full backup, with "Multipart Restore" selected.
2. Incremental or differential backups, from oldest to most recent, with "Multipart Restore" selected.
3. Most recent incremental or differential backup, with "Multipart Restore" selected and "Final Part" checked.

When the last restore is complete, the Mailbox and Public Folders store may be mounted again.

NOTE: When restoring incremental backups, the backups must be restored in chronological order from oldest to most recent.

Restoring an Exchange 5.5 Server

NOTE: In Exchange 5.5, the directory store can only be restored when restoring to the original Exchange host, or a server of the same name as the original Exchange host.

NOTE: To restore an Exchange database, the restore target system must have the same version, service pack, and hotfix level of Exchange installed. If restoring to an alternate Exchange server, the "site" and "organization" must be the same as the original Exchange host.

Performing a Restore of Exchange 5.5

1. Start only the "Microsoft Exchange System Attendant" service on the Exchange restore target.
2. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
3. Select the objects for restore.
4. Click "Action"/"Restore this Backup."
5. To restore the Exchange database to the original location/server, click "Next" at the "Exchange Agent Restore Options" screen.
6. At the "Restore Options" screen, click "Restore."

Exchange 5.5 Specific Options
By default, UltraBac is set to restore the Exchange database to its original location and server. To restore to an alternate server, perform a multipart restore, or use other advanced options, click "Exchange 5.x Options" from the "Exchange Agent Restore Options" screen.
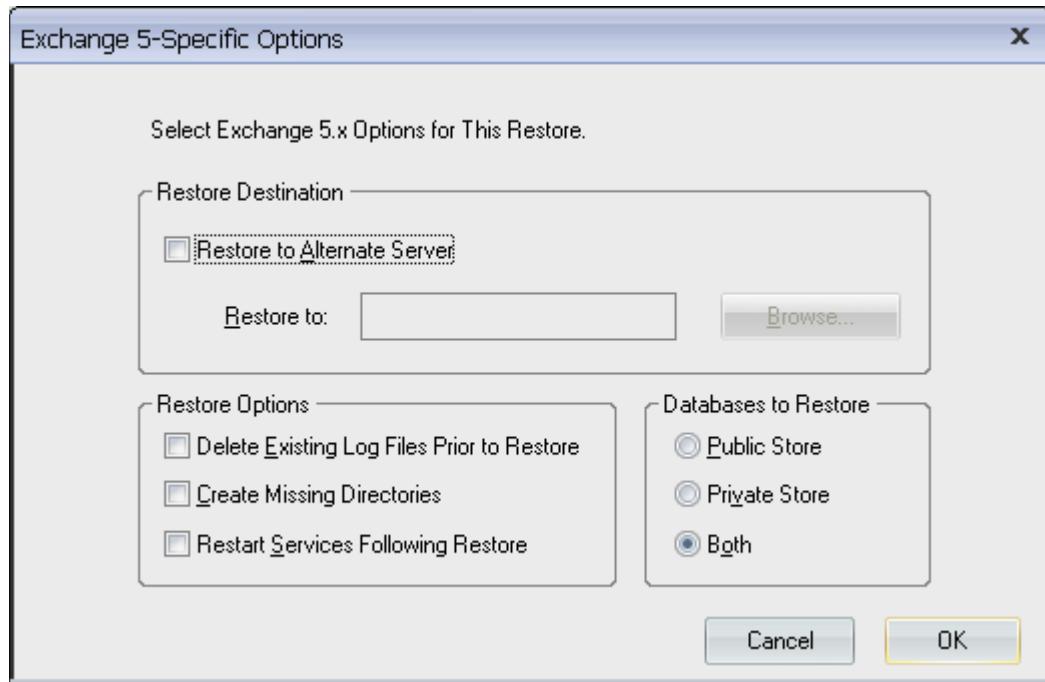
Fig. 1 - Exchange 5.5 restore options.

To restore to an alternate Exchange server:

1. Check "Restore to an Alternate Server."
2. Type or browse to the Windows name or IP address of the restore target.
3. Click "OK."

Restore Options:

- Delete Existing Log Files Prior to Restore – This option deletes all transaction logs on the Exchange server before performing the Exchange restore.
- Create Missing Directories – This option will force UltraBac to create any directories used by Exchange, that existed on the original Exchange host but do not exist on the restore target.
- Restart Services Following Restore – This option will cause the Exchange services to restart after the restore completes.

Databases to Restore – Use this option to select either the public or private stores, or both.
Post Restore
After the restore is complete, UltraBac recommends running the "isinteg -patch" utility. This utility is run through the Command prompt, and the "Directory Store" must be running for successful results.

1. Open a Command prompt, and browse to the "Exchsrvr\bin" directory.
2. Type "isinteg -patch" and press "Enter."

Running the "Isinteg" utility will clean up the newly restored "priv.edb" and "pub.edb," allowing the Information Store service to start.

NOTE: See the Microsoft Exchange 5.5 documentation for more information regarding the "isinteg" utility.

SharePoint Agent

Using the UltraBac SharePoint Agent, Microsoft SharePoint Portal Server 2003 and Microsoft Office SharePoint Server (MOSS) 2007 servers can be backed up online, without stopping the services prior to backup. If the necessary SharePoint services are not running, the backup will not be successful.

Setup and Configuration

Before creating a backup set, the SharePoint Agent should be installed on the SharePoint server.

NOTE: For additional information on installing the SharePoint Agent, please visit the "**Installing UltraBac**" section of the User Manual:

UltraBac User Manual: Installing UltraBac

Microsoft SharePoint Portal Server 2003

Creating a SharePoint Agent Set

NOTE: The UltraBac SharePoint Agent only supports the full backup and full restore of SharePoint Portal 2003 databases. Individual Document restore is not supported.

1. Launch the Backup Wizard by clicking "Backup"/"New."
2. Click "SharePoint Agent" to highlight the option then click "Next."
3. Enter Advanced Account credentials, if necessary, then click "Next."
4. Type in or browse to the name of the SharePoint server and click "Next."
5. Select the Backup Type,
6. Type a description for the set as it will appear in the backup log and click "Next."
7. Click "Finish" to load the SharePoint Agent set into the file viewer.
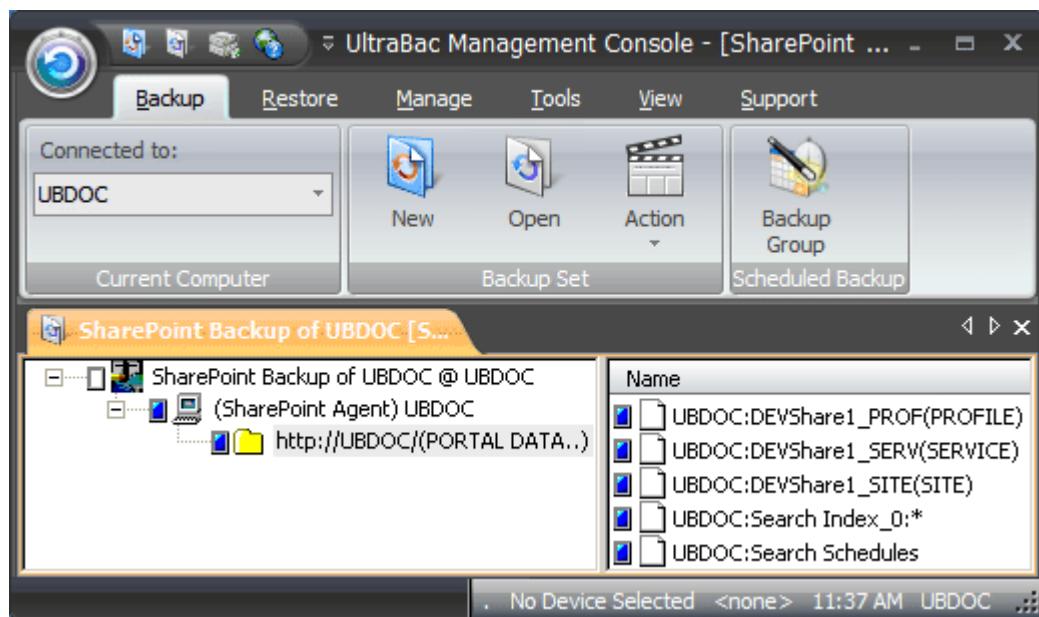
Fig. 1 - SharePoint Portal 2003 backup set loaded in the File Viewer.

Microsoft Office SharePoint Server (MOSS) 2007

Creating a SharePoint Agent Set

NOTE: The UltraBac SharePoint Agent supports individual document restore from SharePoint Portal 2007 sites only when "Enable individual document restores" is selected.

1. Launch the Backup Wizard by clicking "Backup"/"New."
2. Click "SharePoint Agent" to highlight the option then click "Next."
3. Enter Advanced Account credentials, if necessary, then click "Next."
4. Type in or browse to the name of the SharePoint server and click "Next."
5. Select the Backup Type, and choose whether to "Enable individual document restores"
6. Type a description for the set as it will appear in the backup log and click "Next."
7. Click "Finish" to load the SharePoint Agent set into the file viewer.
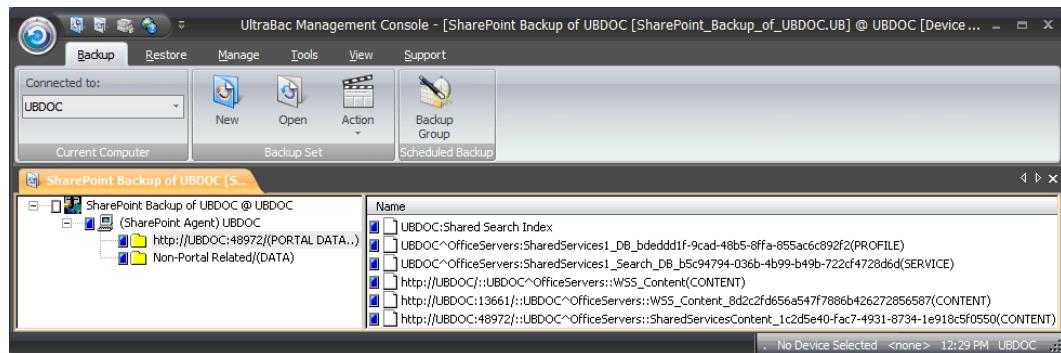
Fig. 2 - Microsoft Office SharePoint Server (MOSS) 2007 backup set loaded in the File Viewer.

Limitations

- The SharePoint configuration and Central Administration content databases cannot be restored using the UltraBac SharePoint Agent. The UltraBac SQL Agent can be used to back up and restore the SharePoint configuration and Central Administration content databases, however, the SharePoint Farm must be in a stopped state for this procedure to work properly. It is strongly recommend that all configuration settings and customizations be fully documented, to facilitate the recreation of the configuration and Central Administration content databases. For detailed information on which settings to document, see: Microsoft TechNet - Choose what to protect: Protecting configuration settings.

- The UltraBac SharePoint Agent does not back up home directories, web.config file, custom assemblies, customizations, site definitions, or list definitions. Use the UltraBac File-by-File Agent to backup these files. For detailed information on which settings to document, see: Microsoft TechNet - Choose what to protect: Protecting customizations.

Backup Set Options
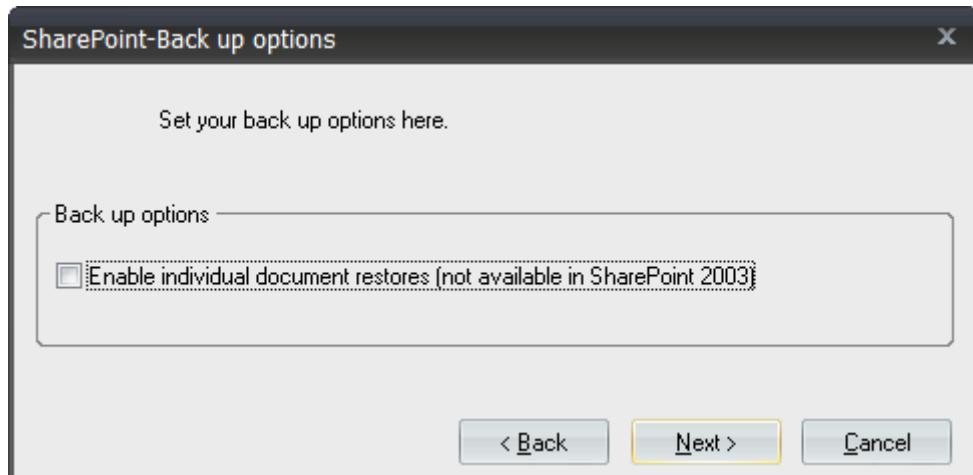
Fig. 3 - SharePoint Agent Backup Options

- Enable individual document restores – Allows restore of Individual Documents in MOSS 2007. SharePoint Portal 2003 is not supported.

Restoring a SharePoint Backup

NOTE: For more information on restore procedures, please visit the "**Restore Basics**" section of the User Manual:

UltraBac User Manual: Restore Basics

Microsoft SharePoint Portal Server 2003

To restore a SharePoint Portal 2003 server:

NOTE: The SharePoint "PROFILE," "SERVICE," and "SITE" databases all must be restored together, and only to the original server.

1. Load the index for restore by clicking the "Restore" tab, then select index retrieval method.
2. Select the objects for restore.
3. Click "Action"/"Restore this Backup"
4. To restore the SharePoint server to the original location/system, click "Next."
5. At the "Restore Options" screen, click "Restore."

Microsoft Office SharePoint Server 2007

NOTE: At this time, all databases must be restored to the original database name and path.

Restoring a Content Database to a New Site Collection

NOTE: For more information on creating a new Site Collection, see: Microsoft TechNet: Office SharePoint Server - Create a site collection.

1. Create a new Site Collection using SharePoint Central Administration.
2. Remove the empty Content Database associated with the new Site Collection.
3. Open the UltraBac Management Console.
4. Load the index for restore by clicking the "Restore" tab, then select index retrieval method.
5. Select the Content Database object for restore.

NOTE: The Content Database being restored cannot exist on the target server. Restore to a new server, or follow the instructions under "Restoring an Existing Content Database" to detach/rename the .MDF and .LDF files.

6. Click "Action"/"Restore this Backup."
7. In the "Content database parameters" section, select the Content Database, then click "Edit."
8. In the "*UltraBac SharePoint Content Parameters*" dialog, click "OK."
9. Click "Next"/"Restore" to restore the Content Database.
10. Verify that the restored Content Database is now mounted/associated with the new Site Collection.

Restoring an Existing Content Database

1. In the Windows Services snap-in, stop the "Windows SharePoint Services Timer" service.
2. Open the Microsoft SQL Server Management Studio (or Microsoft SQL Server Management Studio Express).

3. Right click the Content Database to be restored and select "Properties."
4. Select the "Files" page and note the "Path" to each file, then click "OK".
5. Right click the Content Database to be restored and click "Tasks"/"Detach..."
6. In the "*Detach Database*" dialog, select "Drop Connections" then click "OK."
7. Browse in Windows Explorer to the path of the Content Database files.
8. Rename both the .MDF and .LDF files associated with the Content Database.
9. Open the UltraBac Management Console.
10. Load the index for restore by clicking the "Restore" tab, then select index retrieval method.
11. Select the Content Database object for restore.
12. Click "Action"/"Restore this Backup."
13. In the "Content database parameters" section, click to select the Content Database, then click "Edit."
14. In the "*UltraBac SharePoint Content Parameters*" dialog, click "OK."
15. Click "Next"/"Restore" to restore the Content Database.
16. Repeat this procedure for any additional content databases to be restored.
17. Start the "Windows SharePoint Services Timer" when all databases have been restored.

Oracle Agent

The UltraBac Oracle Agent allows the backup of Oracle databases without shutting down the Oracle services before backup. The agent can perform either "hot" or "cold" backups depending on the mode of the Oracle databases:

- Hot backup – Oracle database must be set in "ARCHIVELOG" mode, and the Oracle database will not be dismounted during backup.
- Cold backup – Oracle database must be set in "NOARCHIVELOG" mode. The Oracle database will be automatically dismounted before, and re-mounted after backup.

Setup and Configuration

The UltraBac Oracle Agent has several requirements for use:

- Oracle Version 8i or greater.
- Oracle client software must be installed on the UltraBac host (the Net8/Net9 Assistant and the Microsoft ODBC Administrator).
- The Oracle database must be in "ARCHIVELOG" mode to perform hot backups, or "NOARCHIVELOG" mode to run cold backups.
- The username and password for the Oracle backup set must be entered in UltraBac, under "Tools"/"Options"/"Agents"/"Oracle Backup Agent."

Configuring the Net8/Net9 Assistant

Before creating a backup set, the Net Assistant must be configured to allow access to the Oracle database.

1. Open the Net8 Assistant (default location is "Start"/"Programs"/"Oracle"/"Network Administration"/"Net8 Assistant").
2. Highlight "Service Naming" and click the "+."
3.
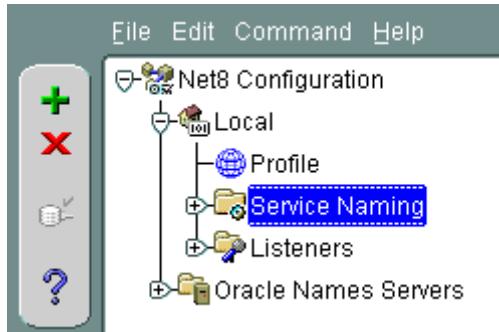
Fig. 1 - Oracle Net8 Assistant.

4. In the Net Service Name Wizard, type in a service name and click "Next."
5.

Fig. 2 - Creating a Net Service name.

6. Leave the default "TCP/IP" (internet protocol) selected and click "Next."
7. Type the computer name of the system running Oracle in the "Host Name" field. Leave the default port number and click "Next."
8. Type the Oracle Service Name in the "Service Name" field and click "Next."

NOTE: To find the Oracle Service Name, check for the "OracleService<service name>" under "Start"/"Programs"/"Administrative Tools"/"Services" on the Oracle host.

---

9. Click "Test" and make sure the connection is completed successfully. Click "Close," then "Finish."
10. Click "File"/"Save Network Configuration" before closing the Net8 Assistant.
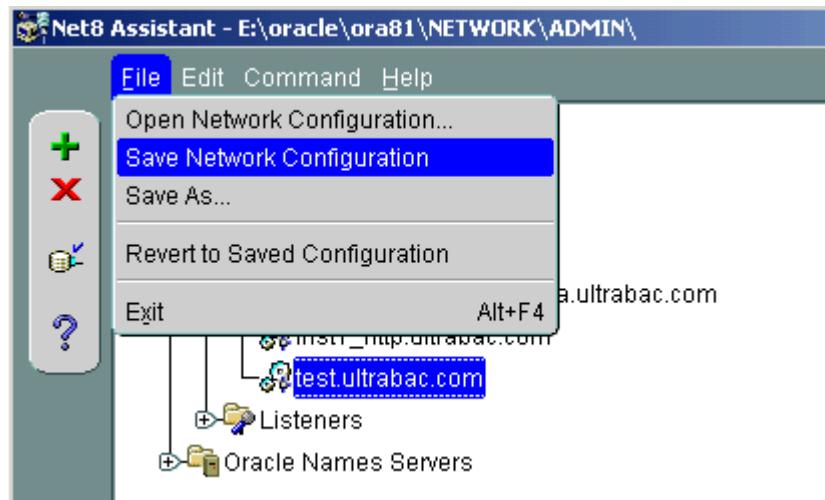
Fig. 3 - Saving the network configuration settings.

Configuring the Microsoft ODBC Driver

Before creating a backup set, the ODBC Driver must be configured to allow access to the Oracle database.

1. Open "Start"/"Programs"/"Oracle"/"Network Administration"/"Microsoft ODBC Administrator."
2. Click the System DSN tab, and click "Add."
3. Scroll to the bottom, highlight "Oracle ODBC Driver," and click "Finish."
4. Type a name and a description in the "Data Source Name" and "Description" fields.
5. In the "Service Name" field, type in the Net Service Name as specified in the configuration of the Net8 Assistant.
6.
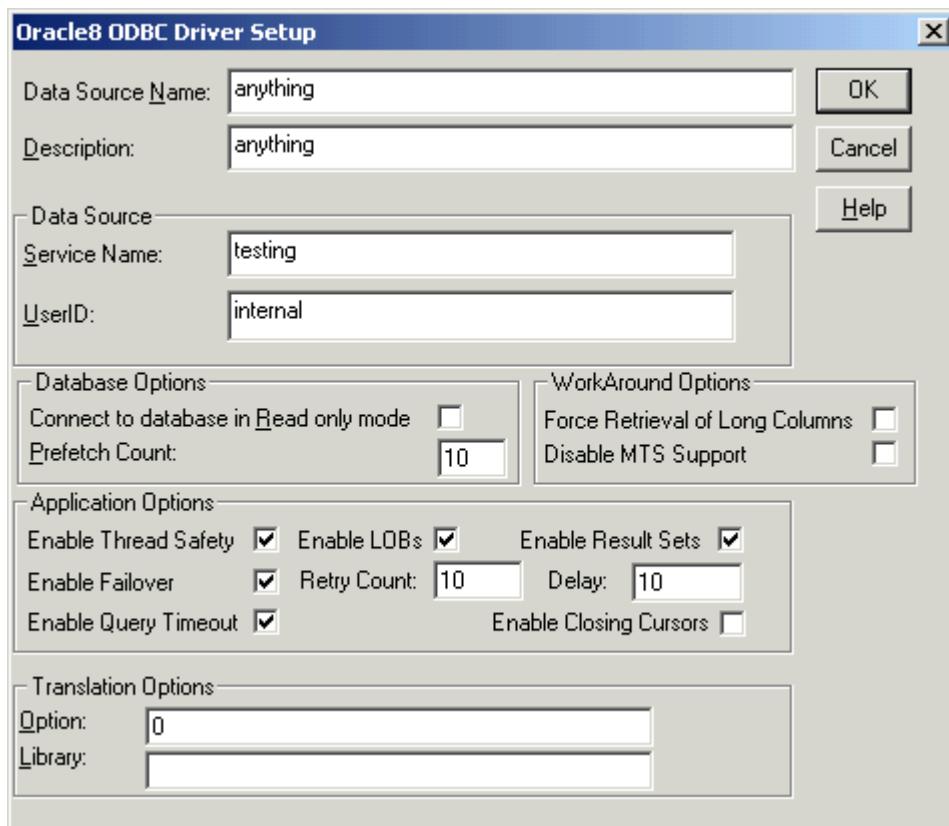
Fig. 4 - Oracle ODBC driver configuration screen.

7. Type the user ID in the "UserID" field and click "OK."

To test the Oracle configuration:

1. Run the "Oracle ODBC Test" located in "Start"/"Programs"/"Oracle"/"Network Administration."
2. Click "Connect," go to the Machine Data Source tab, and double click the "Data Source Name" specified in the ODBC driver setup.
3. When prompted by the Oracle ODBC driver connect screen, type the password and click "OK."

4. Click "All Tables" and data will appear in the query box, indicating the agent has been set up correctly.

Creating an Oracle Backup Set

To create an Oracle Agent backup set:

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Click "Oracle Agent" to highlight the option. Click "Next" to continue.
3. Select the object to be backed up, or "All Objects." Click "Next."
4.
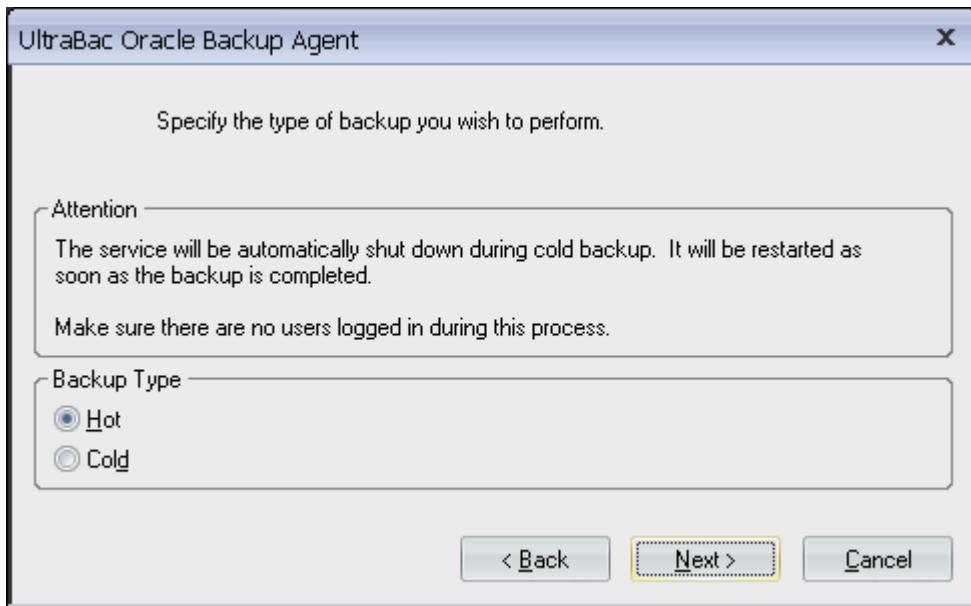
Fig. 5 - Backup type selection.

5. Select the type of backup to be performed. This setting must match the mode of the Oracle database. Click "Next."
6. Enter a Set Description, and click "Next."
7. Select "View/Edit files in the backup set," and click "Finish."
8.
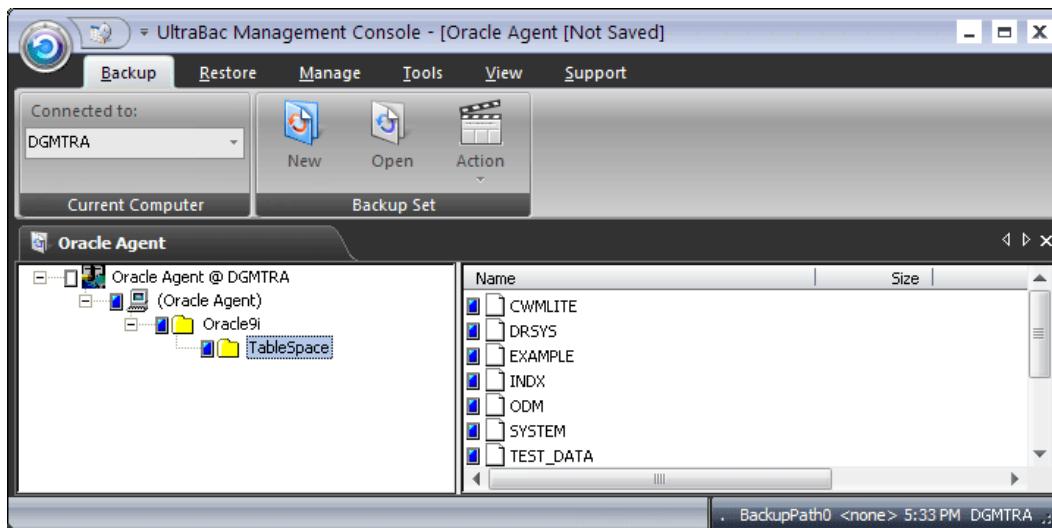
Fig. 6 - Oracle set loaded in the File Viewer.

Dividing the Backup to Improve Speed Performance

If the Oracle machine exceeds storage capacity, or if the entire "TableSpace" doesn't fit on one tape, the Oracle Agent backup can be divided into separate sets. Dividing the backup in this manner will allow the Oracle database to be backed up to more than one storage device simultaneously, increasing backup speed. Instead of backing up the entire Oracle database with one session directing the backup to one storage device, three sets can be used:

- First set – Used to back up the first half of the "TableSpace."
- Second set – Used to back up the second half of the "TableSpace."
- Third set – Used to back up the "ControlFiles" and "ArchiveLogs."

The "ArchiveLogs" are deleted immediately after the backup completes. Due to the fact that many logs are generated when a "TableSpace" is taken offline, it is strongly recommended to back up the "ArchiveLogs" after the "TableSpace," when the "TableSpace" is divided into two sets. The Init.ora file is not enumerated in the backup sets, but is always backed up, in both hot and cold backups.

During enumeration of an Oracle cold backup set, "OnlineRedoLogs" will replace the "ArchiveLogs." During a cold backup, the "OnlineRedoLogs" are never deleted.

NOTE: During a cold backup of an Oracle database it may appear as if the backup is hanging. Depending on the size of the Oracle database, it may take several minutes for the database to dismount, and for backup to begin.

Restore

Restoring an Oracle database requires the data to be restored using UltraBac, then the database must be mounted by the Oracle administrator.

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select the objects for restore.
3. Click "Operations"/"Restore Selected Files."
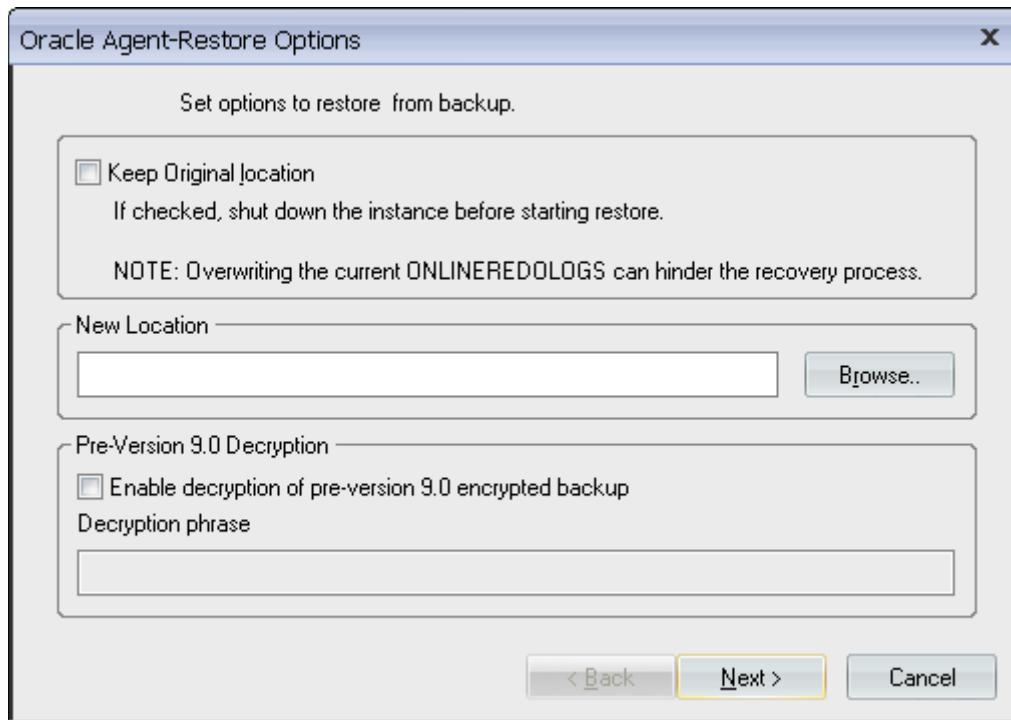
Fig. 7 - Oracle Agent Restore Options.

4. Check "Keep Original Location" to restore the Oracle database to its original location.
5. To restore to an alternate location, type in or browse to an alternate restore path in the "New Location" field and click "Next."
6. Check "Unattended," and click "Restore."

Ux Agent

The UltraBac Ux Agent provides UltraBac with the ability to back up files from the following platforms:

- HPUX
- Linux RPM
- Linux
- OSX
- AIX
- BSD
- Sparc / Solaris
- Intel / Solaris
-

It is possible to back up a Unix client via Samba (or similar applications), using a standard network backup set. Such a backup is limited, as the read/write/execute file attributes cannot be backed up.

Setup and Configuration

The Ux Agent packages are saved in the "UxAgents" folder by default:

"C:\Program Files\UltraBac Software\UltraBac\Agents\UxAgents"

To begin the setup process, copy the appropriate platform specific installation files to the desired Unix client.

HP-UX

Uses the file "ubux-2.31-hpux.tar.gz"

1. Transfer the ubux-2.31-hpux.tar.gz file to your HPUX machine.
2. Logon as the "Root" user to obtain administrative authority.
3. Navigate to the "opt" folder

   cd /opt

4. Make an "ultrabac" folder in and "opt" folder:

   mkdir ultrabac

5. Navigate to where you saved the UltraBac installer and move the file to /opt/ultrabac

   mv ubux-2.31-hpux.tar.gz /opt/ultrabac

6. Navigate to /opt/ultrabac

7. Uncompress and run the UltraBac installer

       tar -zxvf ubux-2.31-hpux.tar.gz
       ./install.sh

8.   Set up the password.

       ./ubuxpwd -i

9.   It will prompt you to enter a password. **Important** You must use the same password used for Root User. If Root has no password, you must set one.

       sudo su – [enter]
       passwd root

10. Once the password for UltraBac is set, restart the inetd service

       inetd -c

Uninstall: Run the "deinstall.sh" script.

LINUX RPM

Uses the file "ubuxagentd-2.3-1.i386.rpm".

1.   Transfer the ubuxagentd-2.3-1-i-386.rpm file to your Linux machine.
2.   Logon as the "Root" user to obtain administrative authority.

3.   Navigate to where you saved the UltraBac installer and run the installer

       rpm -ivh ubuxagentd-2.3-1-i-386.rpm

4.   Navigate to /opt/ultrabac
5.   Set up the password.

       ./ubuxpwd -i

6.   It will prompt you to enter a password. **Important** You must use the same password used for Root User. If Root has no password, you must set one.

       sudo su – [enter]
       passwd root

7.   Once the password for UltraBac is set, restart the XINETD services

       service xinetd restart

Uninstall: Run the "deinstall.sh" script.

LINUX

Uses the file "ubux-2.31-linux.tar.gz."

1.   Transfer the ubux-2.31-linux.tar.gz file to your Linux machine.

2. Logon as the "Root" user to obtain administrative authority.
3. Navigate to the "opt" folder

   cd /opt

4. Make an "ultrabac" folder in and "opt" folder:

   mkdir ultrabac

5. Navigate to where you saved the UltraBac installer and move the file to /opt/ultrabac

   mv ubux-2.31-linux.tar.gz /opt/ultrabac

6. Navigate to /opt/ultrabac

7. Uncompress and run the UltraBac installer

   tar -zxvf ubux-2.31-linux.tar.gz
   ./install.sh

8. Set up the password.

   ./ubuxpwd -i

9. It will prompt you to enter a password. **Important** You must use the same password used for Root User. If Root has no password, you must set one.

   sudo su – [enter]
   passwd root

10. Once the password for UltraBac is set, restart the XINETD services

    service xinetd restart

Uninstall: Run the "deinstall.sh" script.

osx

Uses the file "ubux-2.31-osx.dmg.gz"

1. Transfer the ubux-2.31-osx.dmg.gz file to your OSX machine.
2. Logon as the "Root" user to obtain administrative authority.
3. Navigate to the /Applications folder.
4. Make an "ubinstall" folder:

   mkdir ubinstall

5. Navigate to where you saved the UltraBac installer and move the file to /Applications/ubinstall

   mv ubux-2.31-osx.dmg.gz /Applications/ubinstall

6. Navigate to /Applications/ubinstall

    gunzip ubux-2.31-osx.dmg.gz

7. Mount the ubux-2.31-osx..dmg file

    hdiutil mount /Applications/ubinstall/ubux-2.31-osx.dmg

8. Go to the desktop. Double-Click the ubux-2.31-osx icon
9. Double click the ubux-2.31-osx.pkg icon.
10. Run through the UltraBac OSX Agent Installer.
11. Using a Terminal window, navigate to where you installed UltraBac.
12. Set up the password.

    ./ubuxpwd -i

13. It will prompt you to enter a password. **Important** You must use the same password
    used for Root User. If Root has no password, you must set one.

    sudo su – [enter]
    passwd root

14. Once the password for UltraBac is set, run the ubuxagentd service.

    ./ubuxagentd

Uninstall: Run the "deinstall.sh" script.

FreeBSD:

Uses the file "ubux-2.31-bsd.tar.gz"

1. Transfer the ubux-2.31-bsd.tar.gz file to your FreeBSD machine.
2. Logon as the "Root" user to obtain administrative authority.
3. Navigate to the root "/"

    type cd /

4. Make an "ultrabac" folder in and "opt" folder:

    mkdir opt
    cd /opt
    mkdir ultrabac

5. Navigate to where you saved the UltraBac installer and move the file to /opt/ultrabac

    mv ubux-2.31-bsd.tar.gz /opt/ultrabac

6. Navigate to /opt/ultrabac

7. Uncompress and run the UltraBac installer

   tar -zxvf ubux-2.31-bsd.tar.gz
   ./install.sh

8. Set up the password.

   ./ubuxpwd -i

9. It will prompt you to enter a password. **Important** You must use the same password
  used for Root User. If Root has no password, you must set one.

   sudo su – [enter]
   passwd root

10. Once the password for UltraBac is set, it is not necessary to restart the INETD service;
  start the ubux service

   ./ubuxsrv &

Uninstall: Run the "deinstall.sh" script.

Solaris:

Uses the file "ubux-2.31-sparc.gz" or "ubux-2.31-intel.gz"

Install command – "pkgadd -d ubxu-2.31-intel" or "pkgadd -d ubxu-2.31-sparc."

Uninstall command – "pkgrm BEIubux."

NOTE: For additional information on installing the Ux Agent for Solaris, please see the
UltraBac Knowledge Base:

See UBQ000194: Configuring the Ux Agent on a Solaris Client

Backing up a Unix Client

1. Launch the Backup Wizard by clicking "File"/"New Backup Wizard" from the main
  UltraBac menu.
2. Click "Ux Agent" to highlight the option. Click "Next" to continue.
3. Type the client name or IP address into the "Server" field.
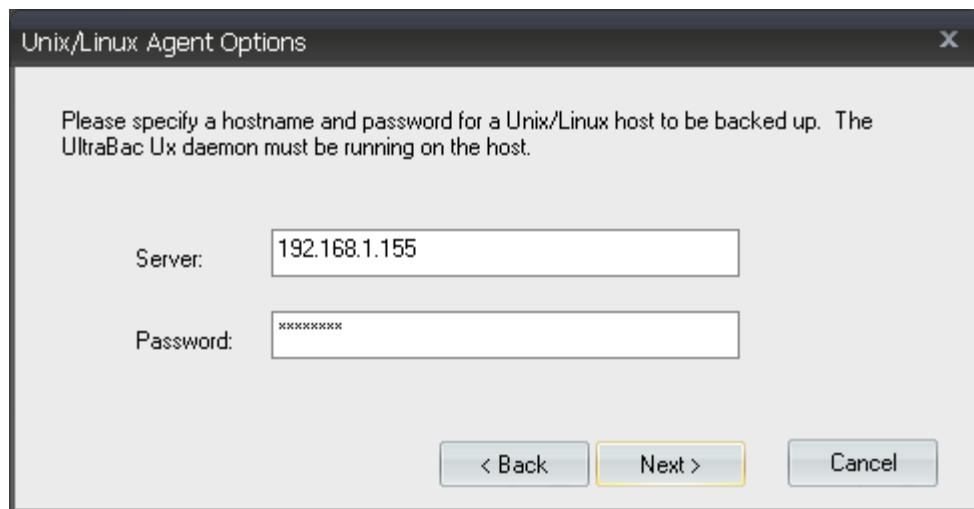
Fig. 1 - Unix/Linux Agent Options.

4. Type the password into the "Password" field, and click "Next."
5. Type a set description and click "Next."
6. At the "Backup Wizard Summary," select "View/Edit files in the backup set" and click "Finish."
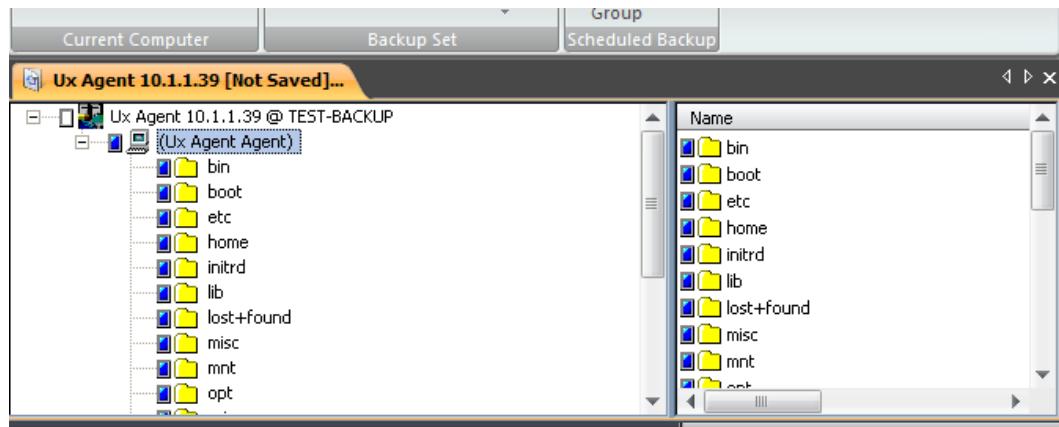
Fig. 2 - Ux Agent set loaded in the File Viewer.

7. Save the set by either clicking the "Save" icon on the toolbar, or by clicking "File"/"Save As" from the main UltraBac menu.

Restoring a Unix Client

1. Launch the Restore Wizard, by clicking "File"/"Load Index for Restore/Verify" from the main UltraBac menu.
2. Select and load the index for restore.
3. Select the objects for restore.
4. Click "Operations"/"Restore Selected Files."
5.
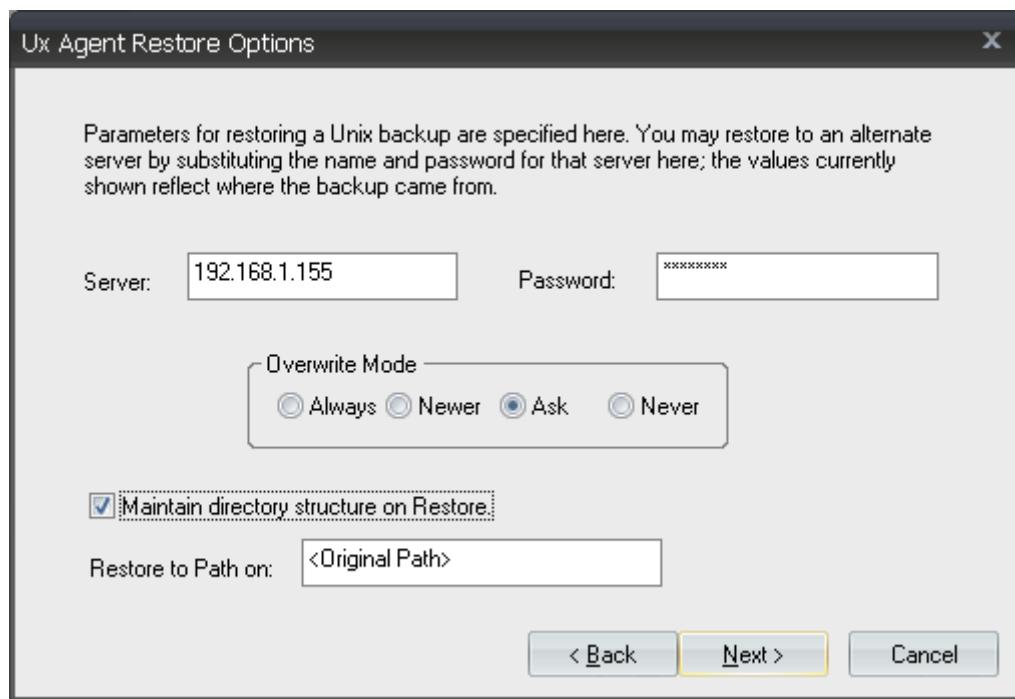
Fig. 3 - Ux Agent restore options.

5. Set the restore options, and click "Next."
6. Check "Restore Unattended" and click "Restore."

Ux Agent Restore Options

Server – Restore destination system
Password – Password for the restore destination system.
Overwrite Mode:

- Always – Overwrite existing files with the files being restored.
- Newer – Only overwrite if the file being restored is newer than the existing file.
- Ask – Prompt before overwriting any existing files.
- Never – Do not overwrite any existing files.

Maintain directory structure on Restore

- This option restores the selected files to their full original path. When unchecked, this option restores all selected files to the top level of the selected directory structure.

Restore to path on

- Allows the restoration of selected files to either the default "<original path>" or a user defined path on the target server.

vSphere Agent

The vSphere Agent provides users with the ability to back up their virtual machines without installing any agents on those machines. It also allows users to backup from one central location.

NOTE: Only vSphere Essentials 4.x (and above) is supported. ESXi free edition is not supported due to licensing limitations set by VMware.

NOTE: Virtual Machines must have Virtual Hardware Version 7. Virtual Machines configured with Raw Disk Mappings (RDM) or Independent Disks cannot be backed up.

vSphere Agent Set Creation

1. Launch the Backup Wizard by selecting the Backup tab, and clicking "New."
2. Select the "VMware vSphere Agent" and click "Next."
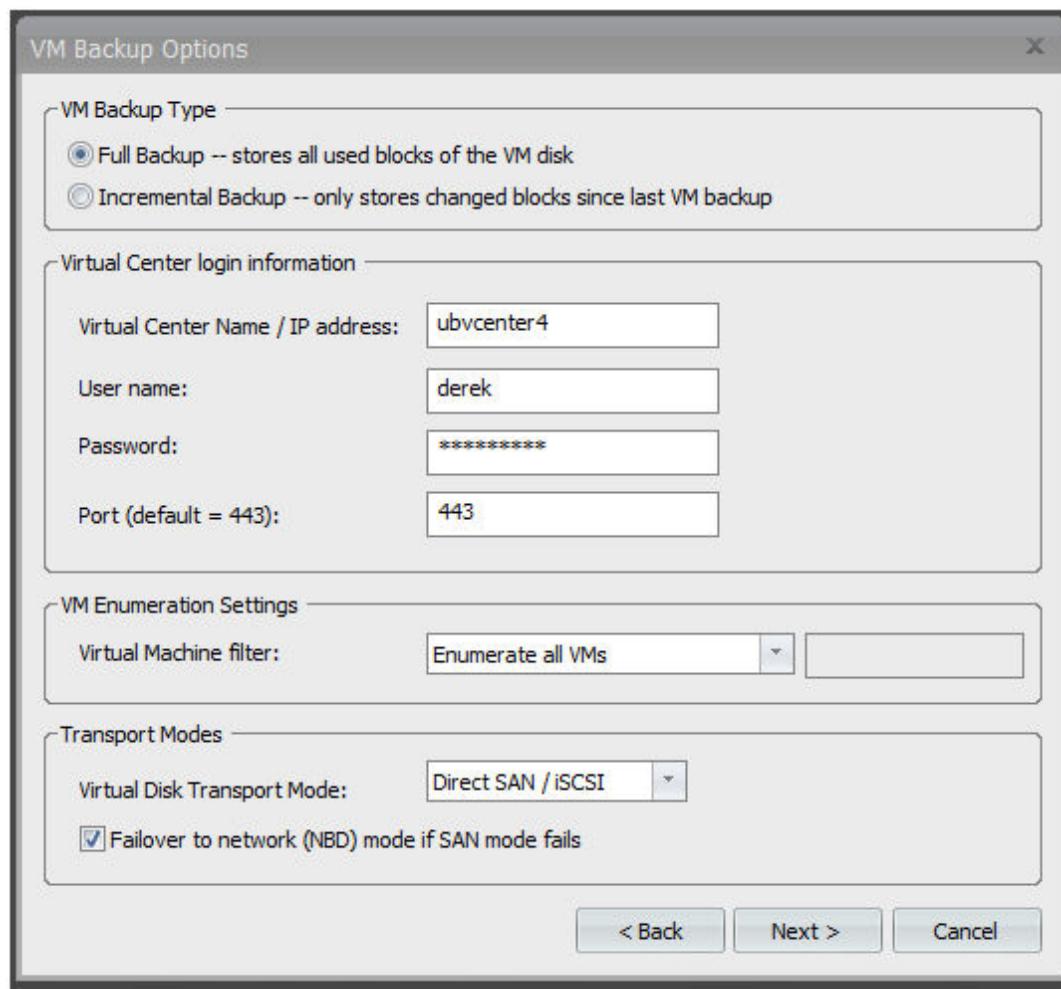
Fig. 1 - vSphere Agent options

3. Select either Full or Incremental backup

> NOTE: Full and incremental backups must be written to the same backup path.

4. Type the Windows name or IP address of the Virtual Center in the "Virtual Center Login Information" field.
5. Type in the User name of the account you use to connect to vSphere. The user must have vCenter administrative privileges.
6. Select how you would like UltraBac to enumerate the Virtual Machines:

- Enumerate all VM's
- Enumerate only powered on VM's
- Enumerate only powered off VM's
- Enumerate by VM name
- Enumerate by VM IP address
- Enumerate by MoRef
- Enumerate by UUID

7. Select the transport mode selecting how we transfer the backup data:
    - Direct SAN / iSCSI

    > NOTE: Full and incremental backups must be written to the same backup path.

    - LAN (NBD)

8. Select Failover to NBD mode, if you want UltraBac to attempt to use the NBD if the SAN / iSCSI connection Fails
9. Enter the name you wish to assign to the UltraBac set.
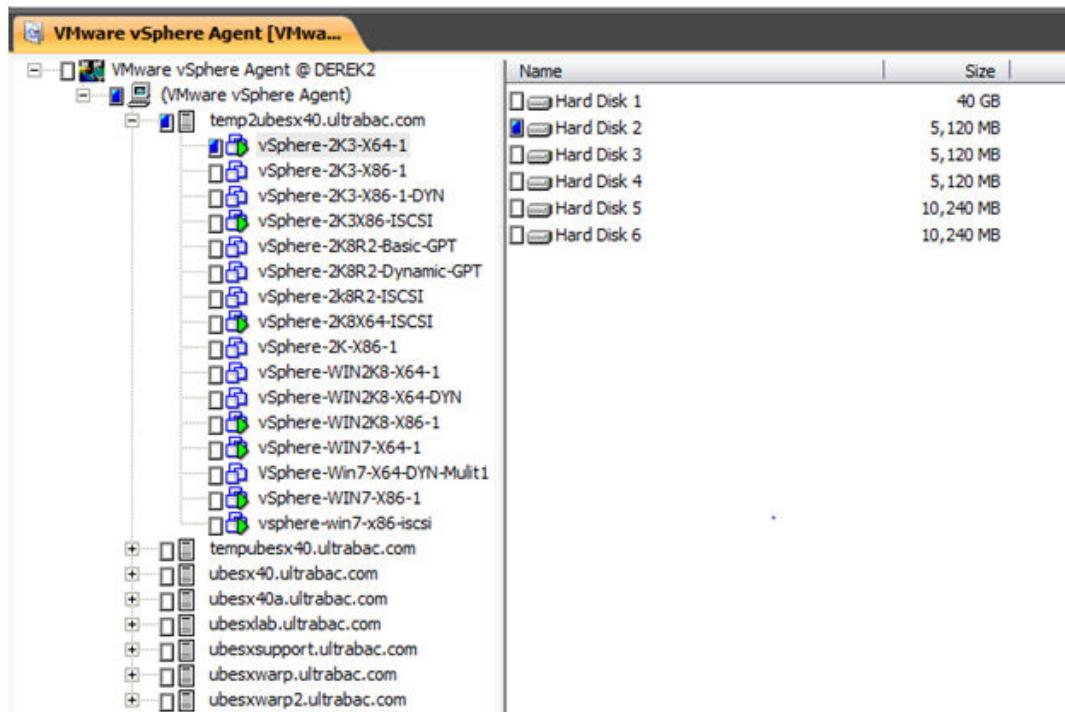
Fig. 2 - Enumerated vSphere Agent backup set.

Current Limitations to Scheduling a vSphere Agent Backup

The following are limitations of the vSphere Agent:

1. Backups can only be saved to a backup path. If scheduled to a different device the set will be skipped.
2. The option to "Delete backups after x amount of days" is not supported, this feature will effect incremental backups making it so you can not restore them!
3. Verifications of vSphere backups are not supported and will be skipped during the verification process.
4. UltraCopy cannot currently be used in conjunction with this agent.
5. Encryption is not supported.

Restoring a Full vSphere Backup to an ESX Store

NOTE: All restores are done via a LAN (NBD) connection.

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the index for restore.
3. Select the VM Disks for restore.
4. Click "Action"/"Restore Selected Files".
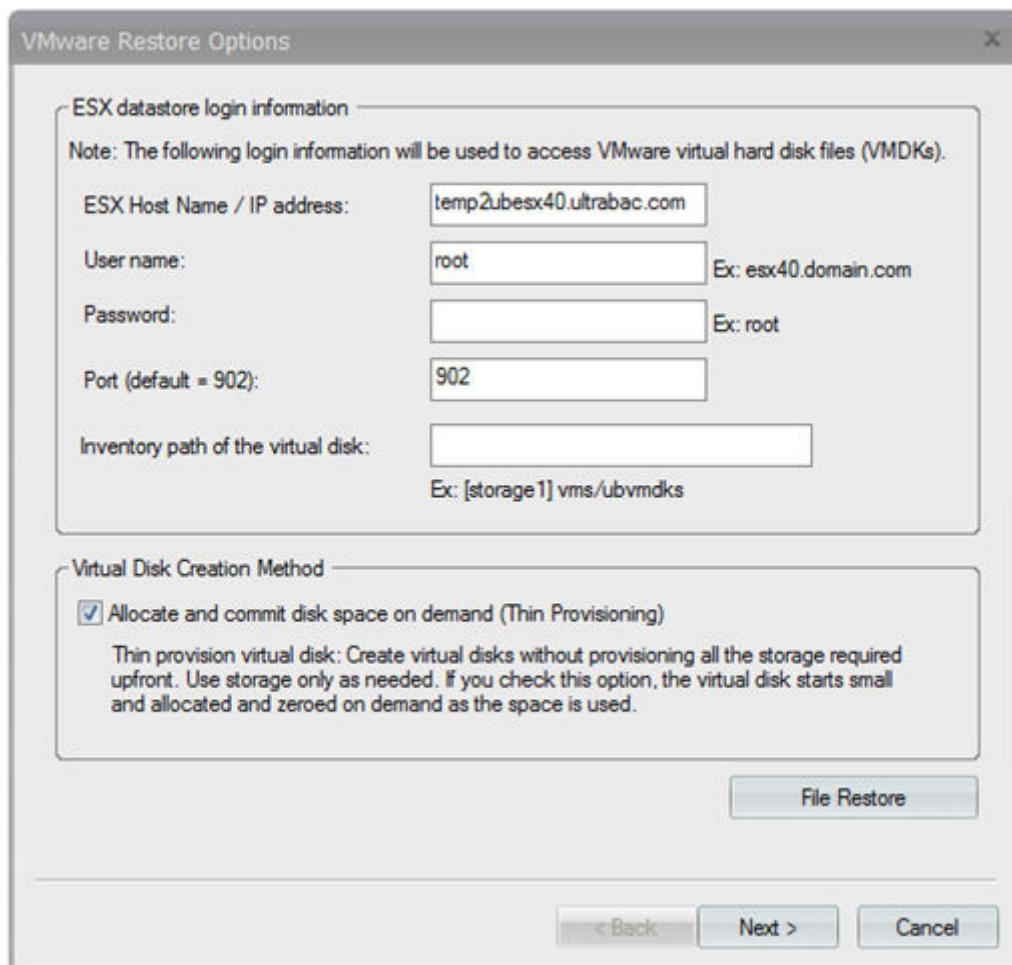
Fig. 3 - vSphere Agent Restore Options.

5. Type the ESX host name or IP address of the ESX Host in the "ESX Host Name / IP address" field.
6. Enter the vSphere account that has full read and write permissions to the datastore you are recovering to in the "User name" field.
7. Enter the port used for connection into the "Port" field. The default is port 902.
8. Type in the Inventory path where you want to restore the virtual disk (case sensitive).

NOTE: If you choose to restore the VM back to its original location (and the original

disk exists), the restored disk will be named vmwarediskname-UBRestore.vmdk.

9. "Allocate and commit disk space on demand" will be checked by default. We recommend this option to save disk space.
10. Click "Next".
11. Then select "Restore".

Restoring an Incremental vSphere Backup to an ESX Store

NOTE: All restores are done via a LAN (NBD) connection.

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the Incremental Index for a "point in time" restore (UltraBac will automatically restore the previous incremental and full backups.
3. Select the VM Disk for restore.
4. Click "Action"/"Restore Selected Files."
5. Type the ESX host name or IP address of the ESX Host in the "ESX Host Name / IP address" field.
6. Enter the vSphere account that has full read and write permissions to the datastore you are recovering to in the "User name" field.
7. Enter the port used for connection into the "Port" field. The default is port 902.
8. Type in the Inventory path where you want to restore the virtual disk (case sensitive).

NOTE: If you choose to restore the VM back to its original location (and the original disk exists), the restored disk will be named vmwarediskname-UBRestore.vmdk.

9. "Allocate and commit disk space on demand" will be checked by default. We recommend this option to save disk space.
10. Click "Next".
11. Then select "Restore".

Mounting a vSphere Backup for File-By-File Restores

UltraBac has the ability to mount the vSphere backup as a local drive letter on the backup machine. This allows users to simply drag and drop files that are needed from the backup.

To perform this operation:

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the index for restore.
3. Select the VM Disk for restore.
4. Click "Action"/"Restore" selected files.
5. Click the "File Restore" button.
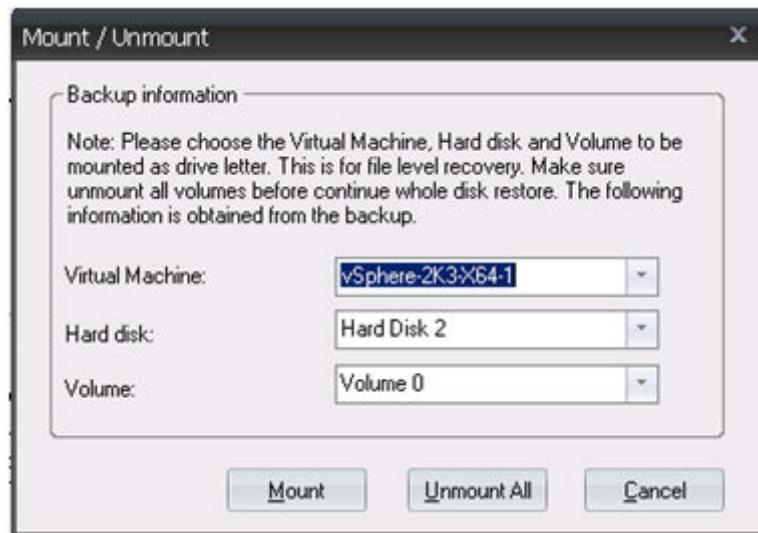
Fig. 4 – vSphere Mounting Options.

6. Select the Virtual Machine from the dropdown box.
7. Select the Hard disk from the dropdown box.
8. Select the preferred Volume from the dropdown box.
9. Click "Mount".

Once the drive is mounted, the necessary files can be dragged and dropped as needed.

To un-mount a drive(s), click "Unmount All".

NOTE: If you forget to un-mount the drive and close UltraBac, you will need to reload the restore. Follow the same steps required to mount a backup until the "Unmount All" option button is visible.

Knowledge Base

UBQ000001: Command Line Backup/Restore

UBQ ID Number: UBQ000001
Last Modified 2009-10-26
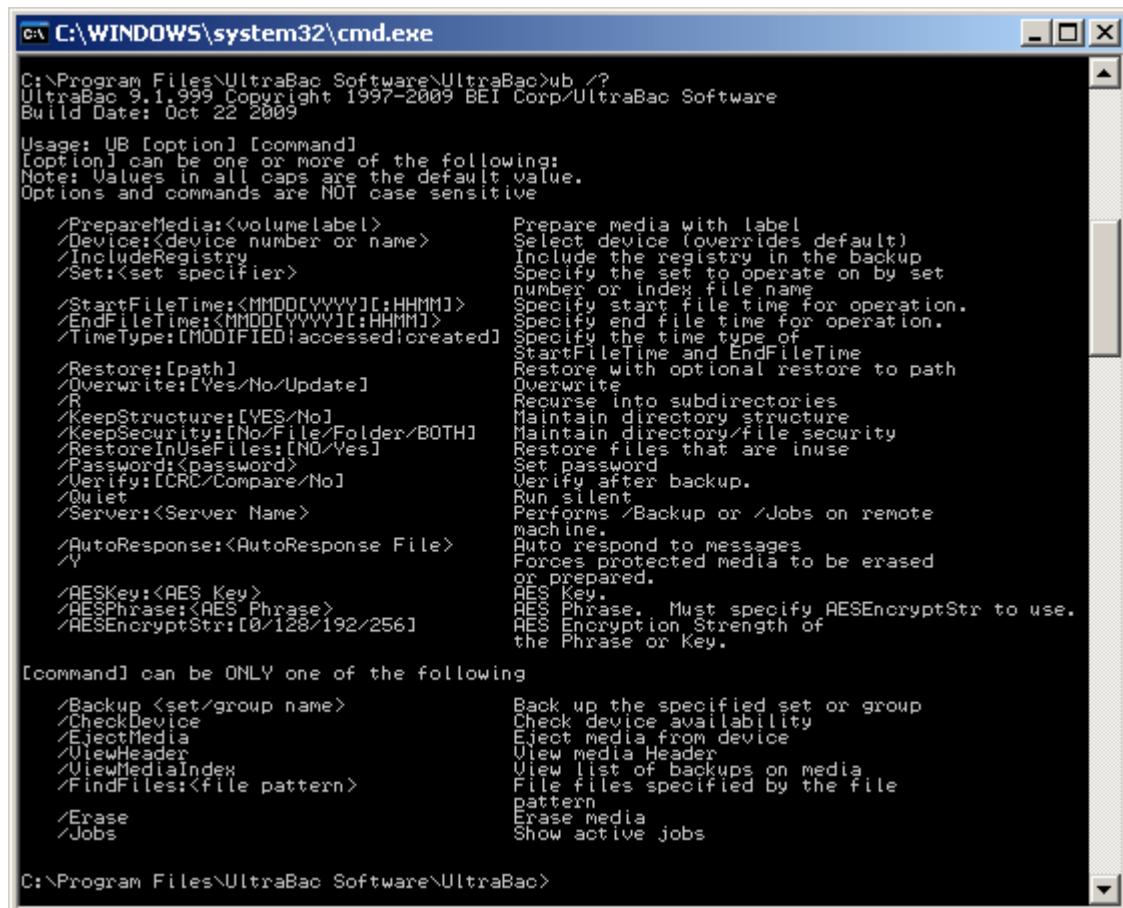
Summary:

This document details the functionality of UltraBac Software v9 command line interface.

Details:

Many of UltraBac's features, such as backup and restore, can be used through a command line interface. This is helpful for those that would like to use scripts to automate backups, or to chain backup jobs, or to have another application kick off your backup. This can also be an effective method of troubleshooting.

Fig.1 - Command line options.

Backup

The options for backup are set in the UBB (backup group) file. If you chose to perform a command line backup of a .UB (backup set) file, you will need to specify the following options:

- /PrepareMedia:<volumelabel> - This option will clear the storage media and give the media a new Volume Label. If this option is excluded, the backup will append to the media.
- /Device:<device number or name> - This option will allow you to select a storage device other than the default device. For a tape drive, use the device number as specified in UltraBac. To backup to a disk path, use the format "BackupPath0" to back up to device BackupPath0 as defined in UltraBac. UltraBac will not recognize a UNC path as a storage device.

Example:

C:\Programs\UltraBac Software\UltraBac>ub.exe /Backup TestSet.ub /Device:BackupPath0 /PrepareMedia:TestMedia

This command line will back up the set 'TestSet.ub' using any preferences contained within the set. It will use the device designated 'BackupPath0' which also can be specified as "/Device:1000" . Before using that device for backup, it will prepare the media using "TestMedia" as the media label.
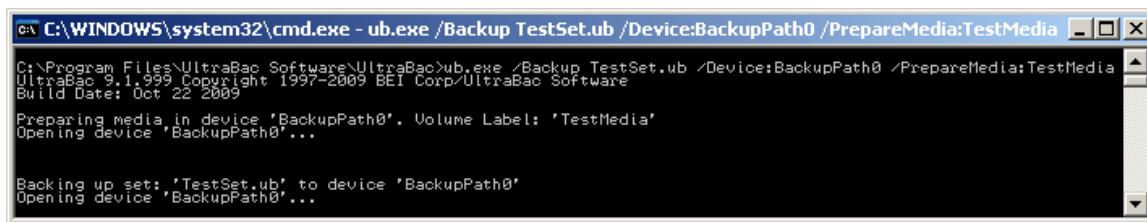
Fig. 2 - Command line backup results (backup).

Restore

The default options for restore are:

- /Overwrite:Ask - UltraBac will prompt you before overwriting any files
- /KeepStructure:Yes - UltraBac will restore the files to the original directory structure
- /RestoreInUseFiles:No - UltraBac will not overwrite files that are in-use

UltraBac will also restore to the original path as the default option, unless another path is specified after the "/restore" option. To change any of those options from the default, you would need to specify the option and the selected preference in the command line.

NOTE: The "/Restore" switch is a modifier for "/FindFiles", telling UltraBac to restore the files found to the path specified.

Example:

C:\Programs\UltraBac Software\UltraBac>ub /FindFiles:* /Restore:C:\TestRestorePath /Device:Tape0 /Set:1

This command line will restore all files contained in "Set 1" of backup device "Tape0" (which also can be specified as "/Device:0), and restore them to the path "C:\TestRestorePath." The "/FindFiles:" command tells UltraBac to find files of a specific type in the specified media. In the example above, the type of files specified is "*", which means "find all files." If you only wanted files with the extension ".bmp," you would enter "/FindFiles:*.bmp" in the command.

Fig. 3 - Command line results (restore).

View Media Index

This command will allow you to check the media to see which sets it holds in the index.

Example Command line:

C:\Programs\UltraBac Software\UltraBac>ub.exe /ViewMediaIndex /Device:BackupPath0

The command line above instructs UltraBac to show the media index held in BackupPath0.

Fig. 4 - Checking Media.

Eject Media

This command will allow you to eject the media thru the command line.

Example Command line:

C:\Programs\UltraBac Software\UltraBac>ub.exe /EjectMedia /Device:0

The command line above tells UltraBac to eject the media in Device 0, which is also Tape0.

Fig. 5 - Ejecting media

View Header

This command will allow you to view the media header.

Example command line:

C:\Programs\UltraBac Software\UltraBac>ub.exe /ViewHeader /Device:BackupPath0

The command above tells UltraBac to view the media header of BackupPath0.

Fig. 6 - Viewing Media Header

Shortcuts

The following shortcut commands are equal to typing the entire command. For example, "ub /bu" would be the same as "ub /backup."

248

/bu: = /backup:
/PM: = /preparemedia:
/D: = /device:

More Information:

[See User Manual: Command Line Functionality](#)

UBQ000024: What is an Image Backup?

UBQ ID Number: UBQ000024
Last Modified: 2000-06-01 at 10:43:09

Summary:

Explanation of an Image (Disaster Recovery) backup as opposed to a standard file-by-file backup

Details:

What is an image backup?

An Image backup bypasses the OS file system and reads the physical sectors of a disk sequentially until all of its active sectors have been backed up. An Image backup can inadvertently perform a "dirty" backup of an open file or related set of files that are in a state of modification – there is no OS file integrity guarantee. This means that applications such as SQL, Exchange and other programs that could be modifying data on the disk should be closed prior to backup. The Image set can perform any required "before" and/or "after" batch command to shut down and start up an application or service, with minimal down time.

An Image set automatically defines the entire disk drive, but individual partitions can be included or excluded. The benefit of an Image backup is that every partition on a disk is 100% backed up, including the Master Boot Record and the file systems contained on the physical disk. The major drawback of an Image backup is, you cannot restore one file from an Image. UltraBac's Disaster Recovery has been designed to work alongside file-by-file backup – not replace it.

An Image backup set can be included as an additional set in a scheduled backup group, it does not need to be run separately. It is recommended to make the Image set(s) the first sets within the group, and clear the storage media whenever possible. This will ensure that the Image backup will start at the beginning of the media, should the backup span to a second tape or disk. The Image set being the first set greatly improves access time when locating an Image set stored on tape during disaster recovery.

Performing an Image backup or restore is essentially a matter of copying the Image from the source device to the
target device.

UltraBac's Disaster Recovery provides the user with the ability to back up only the "Active Clusters" on the source disk. UltraBac will also exclude the system page file and the hyberfil.sys. from image backups, greatly reducing the amount of storage space, and time necessary for backup.

More Information:

See User Manual: Image Disaster Recovery Agent
See User Manual: UBDR Gold v5.0/6.0
See User Manual: Static Mirror Image Backup
See UBQ: UBQ000060 - Static Mirror Image Recovery

UBQ000041: Selecting a Storage Device

UBQ ID Number: UBQ000041
Last Modified: 2011-02-25 at 10:43:26

Summary:

Selecting the UltraBac storage media to use during an interactive backup or as the default device.

Details:

UltraBac supports several types of storage devices. These are displayed by selecting "Select"/"Storage Device."
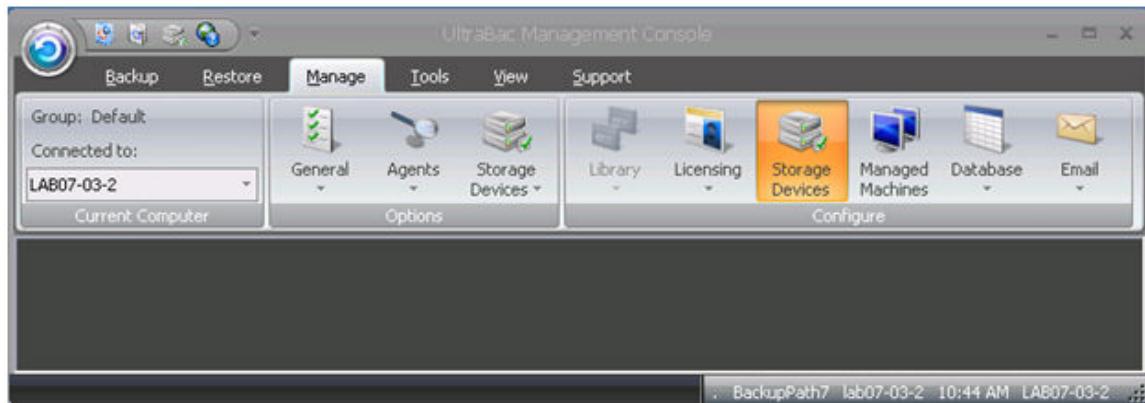
Fig. 1 - Opening Device selection screen.

Select which type of storage device to list by clicking on the appropriate tab. The types of storage devices include Tape, BackupPath, Remote, FTP, Tivoli, Image and Partition.
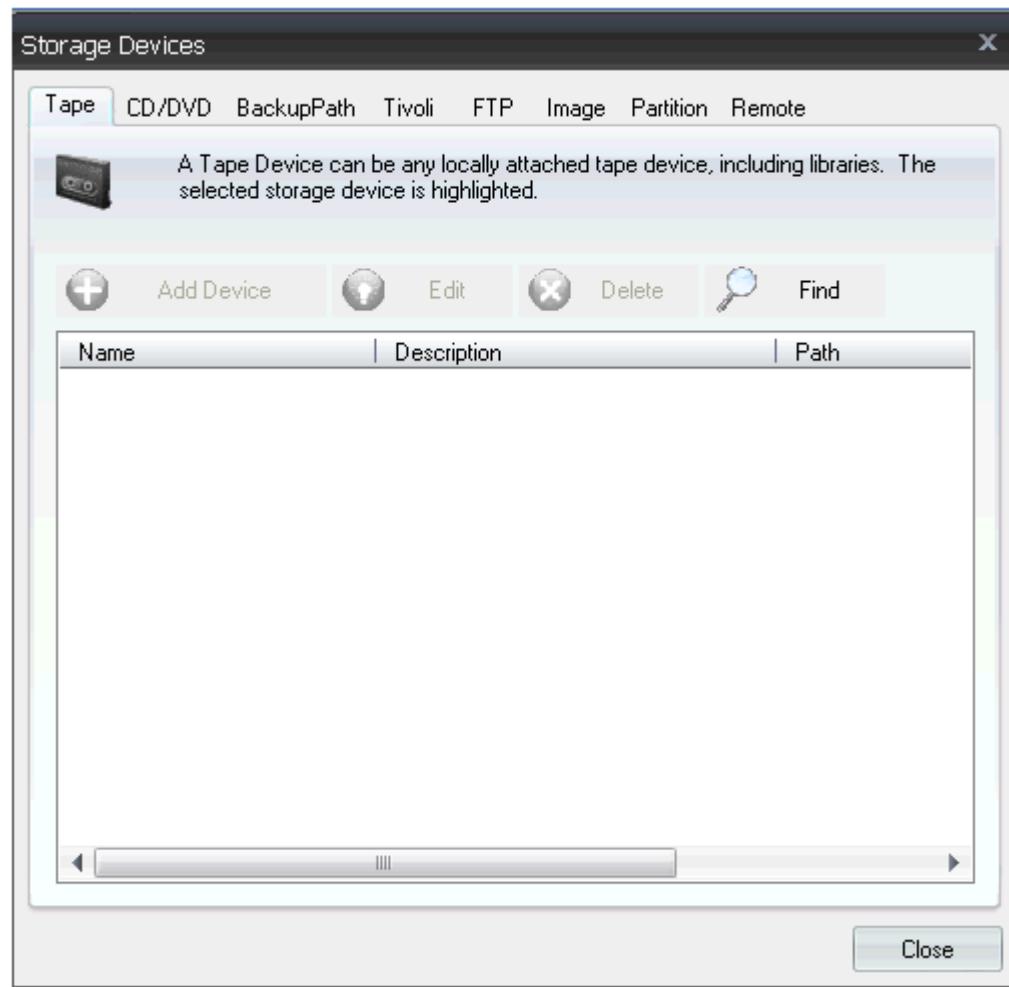
Fig. 2 - Storage device selection screen.

The active storage device is displayed on the Title line of the UltraBac Main Window when a set is loaded. This is the storage device used when performing an Ad-hoc (Perform Backup) backup. The default storage device becomes the active device when UltraBac is invoked and is the storage device used when creating a scheduled backup group unless otherwise specified.

To change the active storage device without making it the default storage device, highlight the storage device and select "OK." This change will be reflected on the Title line of the UltraBac Main Window. To change both the active and default storage devices, highlight the storage device, select "Save as Default Device" option and then select "OK."

Use the slider to view columns not displayed. The "Select Storage Device:" list box displays the "Device", "Identifier", and "Path" columns. The "Device" column lists the members of the device category displayed in the "Show" list box. Windows NT/2000 assigns the "Identifiers" for tape devices, while the user assigns the identifier for disks and images during their creation. The "Path" applies to disk paths defined as storage devices.

More Information:

See User Manual: Storage Device Manager
See UBQ: UBQ000049 – Defining a Disk (disk-path) Storage Device
See UBQ: UBQ000210: UltraBac Backup Output Files

UBQ000049: Defining a Disk (BackupPath) Storage Device

UBQ ID Number: UBQ000049
Last Modified: 2011-02-25

Summary:

This article details the necessary steps to create a "BackupPath" device.

Details:

Upon initial installation of UltraBac, there will be no defined disk paths. The maximum number of BackupPath devices allowed is (by default) 1000. Supported target disks include any disk path that can be written to by NT/2000. This includes a Linux/Unix disk path via Samba or any SAN device.

Creating a BackupPath Device

From the main UltraBac toolbar, click "Select"/"Storage Device" to open the Device selection window
Select 'BackupPath' tab.
Press the "Add New" button to create a new path.
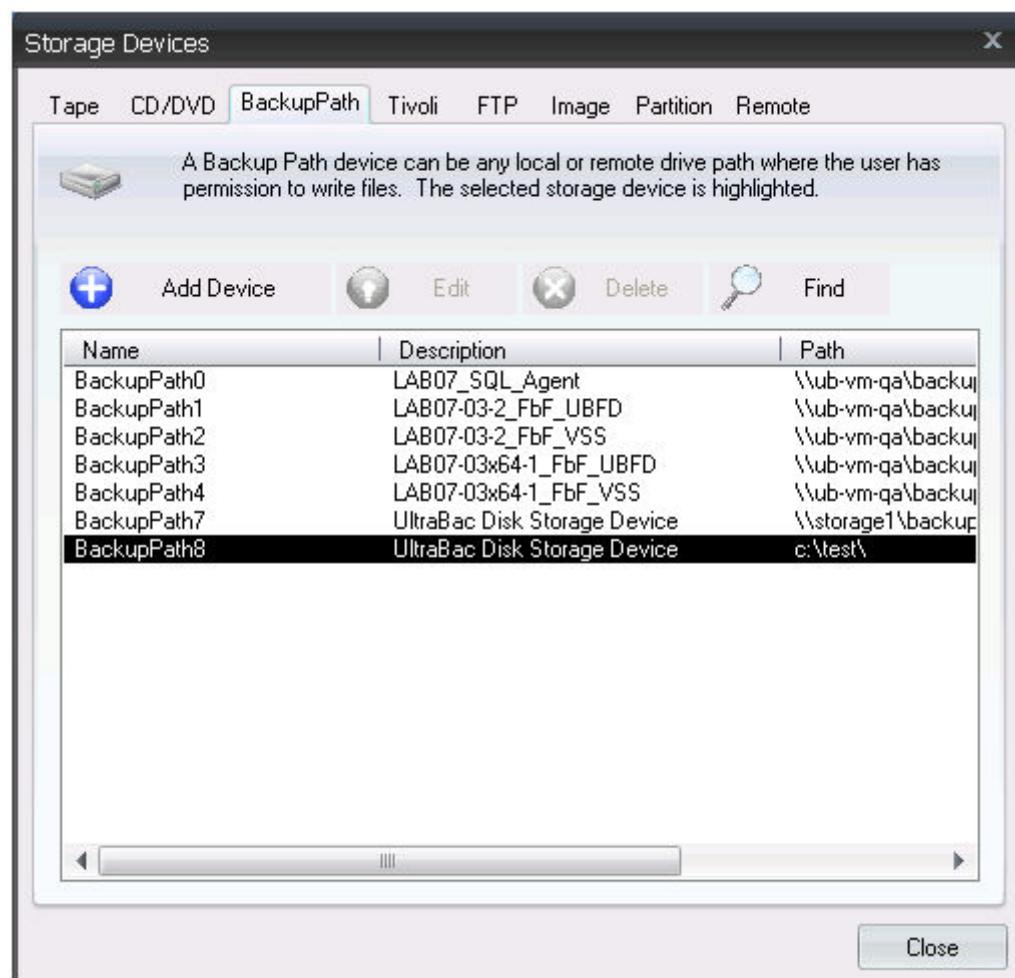
Fig. 1 - Storage device selection window.

Type a user defined name into the "Device Name" field as it should appear in UltraBac's log files.
Type the UNC path to be used for storing UltraBac's output files.
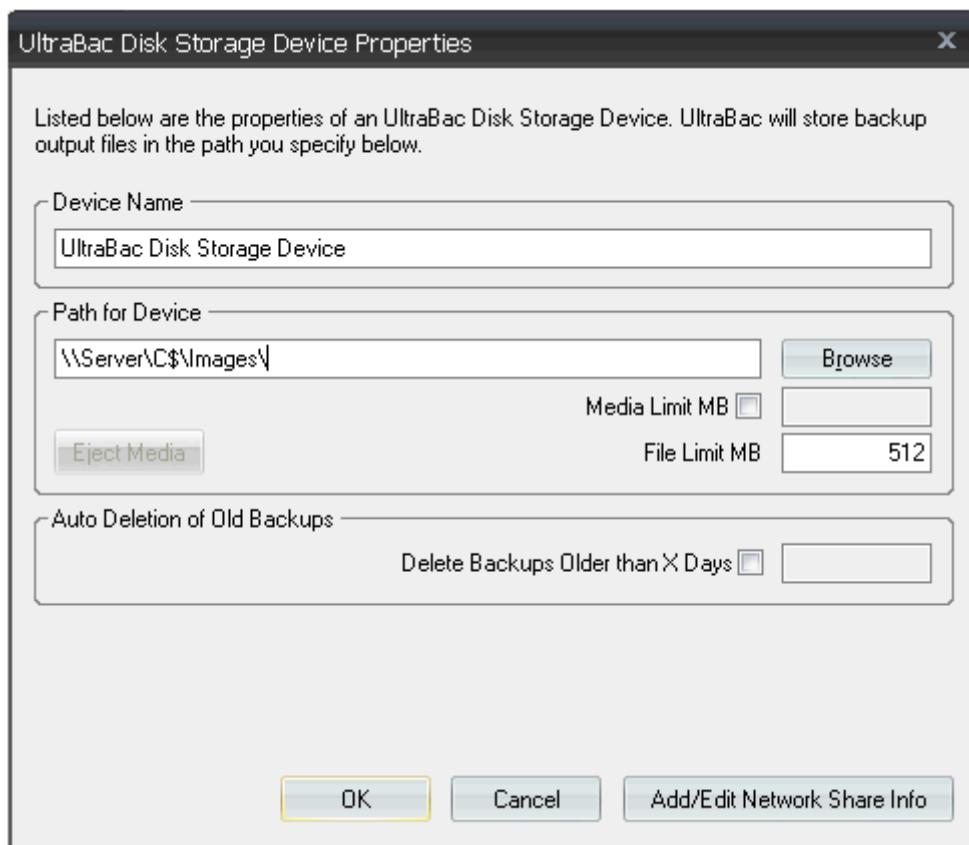
Fig. 2 - Specifying the backup target path.

When selecting the "Limit Size per media" option, enter the maximum disk space, in MBs, that UltraBac is allowed to use.

When no longer necessary, defined disk paths can be deleted using the "Delete" button or edited by using the "Properties" button. Refer to the Chapter "Disk-to-Disk Backups" in the manual for more information.

NOTE: If a fixed disk device reaches capacity during backup the user will be prompted to supply another volume to continue. If the user selects OK at the prompt, the previous backup files are in danger of being overwritten. If there is the possibility the fixed disk device will reach capacity during a scheduled backup, supply an alternate target device to which an overflow may cascade.

Auto Deletion of Old Backups

Checking "Delete Backups Older than X Days" will allow UltraBac to write multiple days' worth of backups to the same BackupPath device, and keep only an archive of the specified number of days.
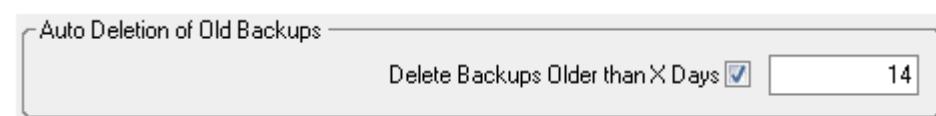
Fig. 5 - Auto deletion of old backups.

To specify the number of days to store backups:

1. Check "Delete Backups Older than X Days."
2. Specify the number of days to store the backups in the field to the right of the checkbox.
3. Click "OK" in the "Disk Storage Device Properties" screen.
NOTE: UltraBac will clear the old backups at the end of a successful backup.

More Information:

See UBQ: UBQ000041 – Selecting a Storage Device

UBQ000060: Static Mirror Image Recovery

UBQ ID Number: UBQ000060
Last Modified: 2005-05-19

Summary:

Recovering a system disk from a Static Mirror Image backup

Details:

There are several ways to recover a failed system using a static mirrored image hard drive:

1. Change SCSI BIOS – Used to minimize down time when the failed drive is the system drive.

    1. Modify the SCSI BIOS to boot from the mirrored hard drive.
    2. Reboot (This must be an image of the system drive.)
    3. Perform any other applicable restores.
    4. Replace failed hard disk as soon as possible.

2. Replace failed hard drive with image hard drive (Used for any failed drive.)
    1.
    2. Power down, remove the failed hard drive, and substitute it with the image hard drive.
    3. Reboot.
    4. Perform any other applicable restores.
    5. Replace failed hard disk as soon as possible.

> NOTE: With each Integrated Static Mirror Image backup, UltraBac compares disk size and checks for an assigned drive letter before using a target drive. This helps prevent the production disk (which was a backup target disk) from being used as a target disk during future backups.

More Information:

See User Manual: Static Mirror Image Backup
See UBQ: UBQ000024 – What is an Image Backup?

UBQ000069: Troubleshooting SMTP

UBQ ID: UBQ000069
Last Modified: 2005-09-13

Summary:

UltraBac has the ability to use SMTP notification using any local SMTP server. UltraBac's SMTP notification does not support off-site SMTP servers or have the ability to pass through a firewall.

Details:

The "From" and "To" email addresses must be of a proper form. (example: something@something.something). test@asdf is not of valid form because it doesn't contain a period or top level domain. Additionally, if relaying is prohibited on the target SMTP server, and/or only certain users are allowed to use the SMTP server, then it may be necessary to provide a legitimate email address in the "From" and "To" fields.

SMTP TROUBLESHOOTING SCRIPT

Use the following script to test SMTP. Type only the **bold** text:

1. C:\>**telnet mail.mailserver.com** 25
    Trying 207.149.155.154...
    Connected to mail.mailserver.com.
    Escape character is '^]'.
    220 SERVER.MAILSERVER.COM ESMTP Server (Microsoft Exchange Internet Mail Service 5.5.1960.3) ready
    helo mailserver.com
    250 OK
    mail from:<sender@mailserver.com>
    250 OK - mail from <sender@ultrabac.com>
    rcpt to:<recipient@mailserver.com>
    250 OK - Recipient <recipient@mailserver.com>
    data
    354 Send data. End with CRLF.CRLF
    Date: 3 Jan 00 1429 EDT
    From: Sender <sender@mailserver.com>
    Subject: Testing
    To: Recipient <recipient@mailserver.com>
    To: Recipient1 <recipient1@mailserver.com>
    cc: Recipient2 <recipient2@mailserver.com>
    Testing Line 1
    Testing Line 2
    .
    quit

If this script fails, UltraBac will not be able to connect to the SMTP server.

ERROR WSA 10060

258

Q. Why do I get an error like: "SMTP error connecting to SMTP server WSA 10060"?

A. The connection may be timing out due to a slow link. Increase the retransmission timeout value of the following registry key to 10 or even 20.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxData Retransmissions

See UBQ: UBQ000162 Non-UltraBac Specific Registry Keys

More about this registry key is found in Microsoft's Q191143 article. For information: http://support.microsoft.com/support/kb/articles/Q191/1/43.ASP

More Information:

See User Manual: Scheduled Backup Options
See UBQ000162: Non-UltraBac Specific Registry Keys

UBQ000080: Incremental/Differential Backups and the Archive Bit

UBQ ID Number: UBQ000080
Last Modified: 2010-01-15

Summary:

How to set up incremental and differential backup sets, and how to use the "clear archive bit" function.

Details:

Once the drives from a computer have been loaded into the Backup Set Editor screen, unselect all files by deselecting the blue box at the top of the file tree.

Modified files can then be selected by right-clicking the desired drive\folder and clicking "Include <drive\folder>..." This will open the "Include/Exclude Files" dialog (see Fig. 2).
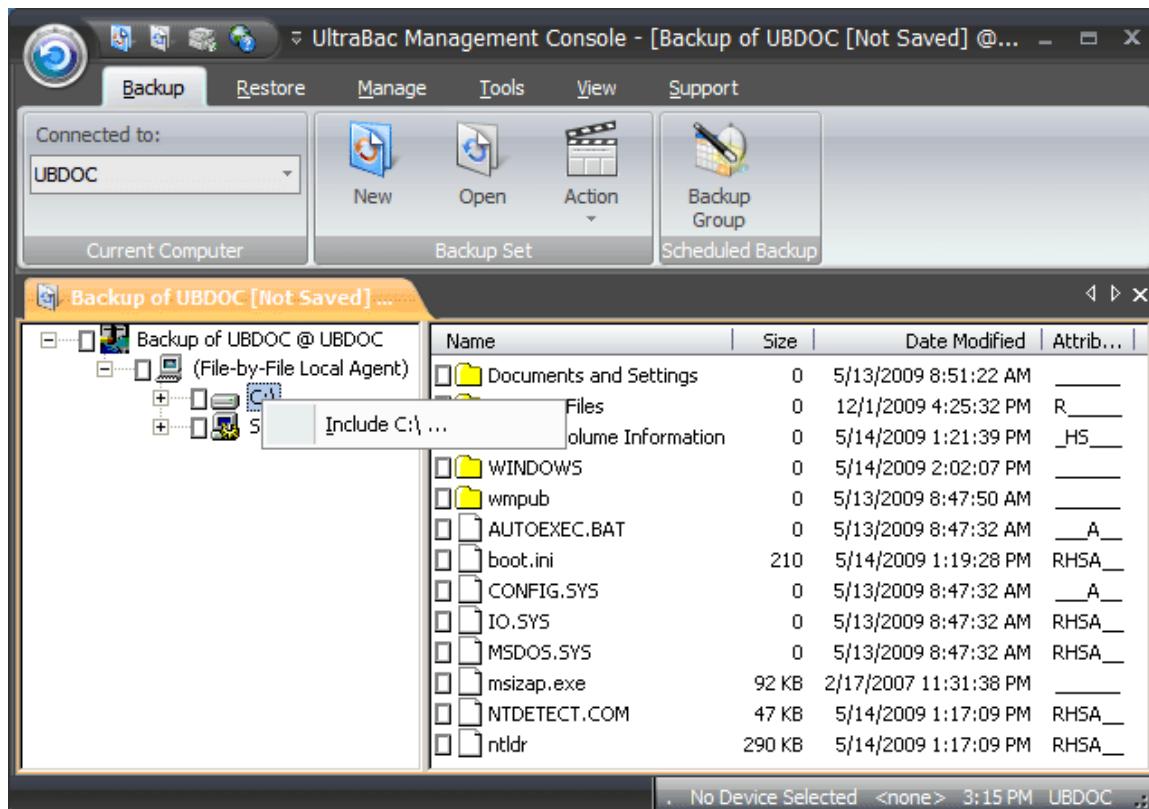
Fig. 1 - Backup Set Editor "Include" option.

The "Include/Exclude Files" dialog allows the user to either include or exclude files based on creation/modification date, name, and file extension.
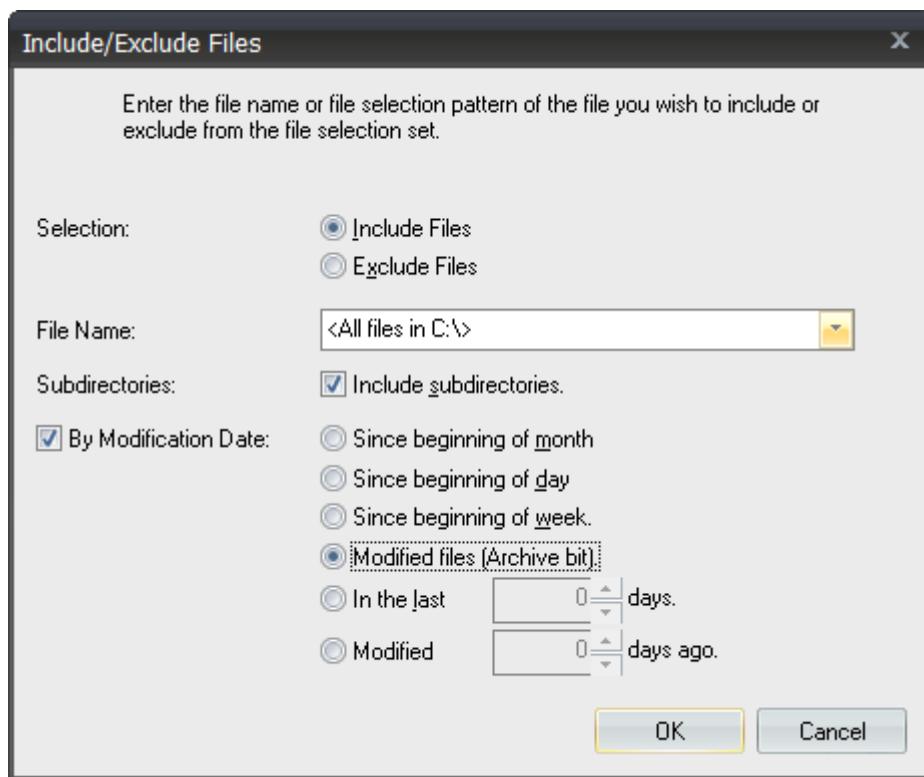
Fig. 2 - "Include/Exclude Files" Dialog.

The "By Modification Date" option lists:
- Since beginning of month
- Since beginning of day
- Since beginning of week
- Modified files (Archive bit)
- In the last <x> days
- Modified <x> days ago

The "Since beginning of month" option automatically selects all files modified since the first of the month for backup. This selection is a "pseudo" differential backup based on having performed a full backup at the end of the previous month.

The "Since beginning of week" option automatically selects all files modified beginning on Monday. This selection is a "pseudo" differential backup based on having performed a full backup at the end of the previous week.

The "Since beginning of day" option automatically selects all files modified beginning at "00:01" or "12:01am." This selection is a "pseudo" differential backup based on having performed a full backup at the end of the previous day.

The "Modified files (Archive bit)" option automatically selects any file with its archive bit set.

The "In the last <x> days" option automatically selects all files modified beginning "<x>" days ago, the user-specified number determining the selection logic. This selection is a "pseudo" differential backup based on having performed a full backup at the end of the day prior to <x>. For example, a value of 0 means "files modified since today." A value of 10 means "files modified since 10 days ago."

The "Modified <x> days ago" option automatically selects all files modified "<x>" days ago. This selection only backs up files modified on the user-specified day.

NOTE: The selection logic is relative to when the set starts not when the backup group is launched. Starting a multiple set backup that spans across midnight will result in all post-midnight sets using the next day as the selection logic base. In other words, when the group/job spans midnight it results in different selection logics being applied to pre-midnight and post-midnight sets.

Clearing the Archive Bit - Scheduled Backups

The option to clear archive bits during scheduled backups can be set in either the Backup Group Options (Fig. 3) to clear the archive bits following all File-by-File backup sets included in the Group, or the Backup Set Options (Fig. 4) to clear the archive bits for the individual set. When the archive bits are cleared during a backup, this sets up the possibility of using the "Modified files (Archive bit)" option to perform an incremental or differential backup.
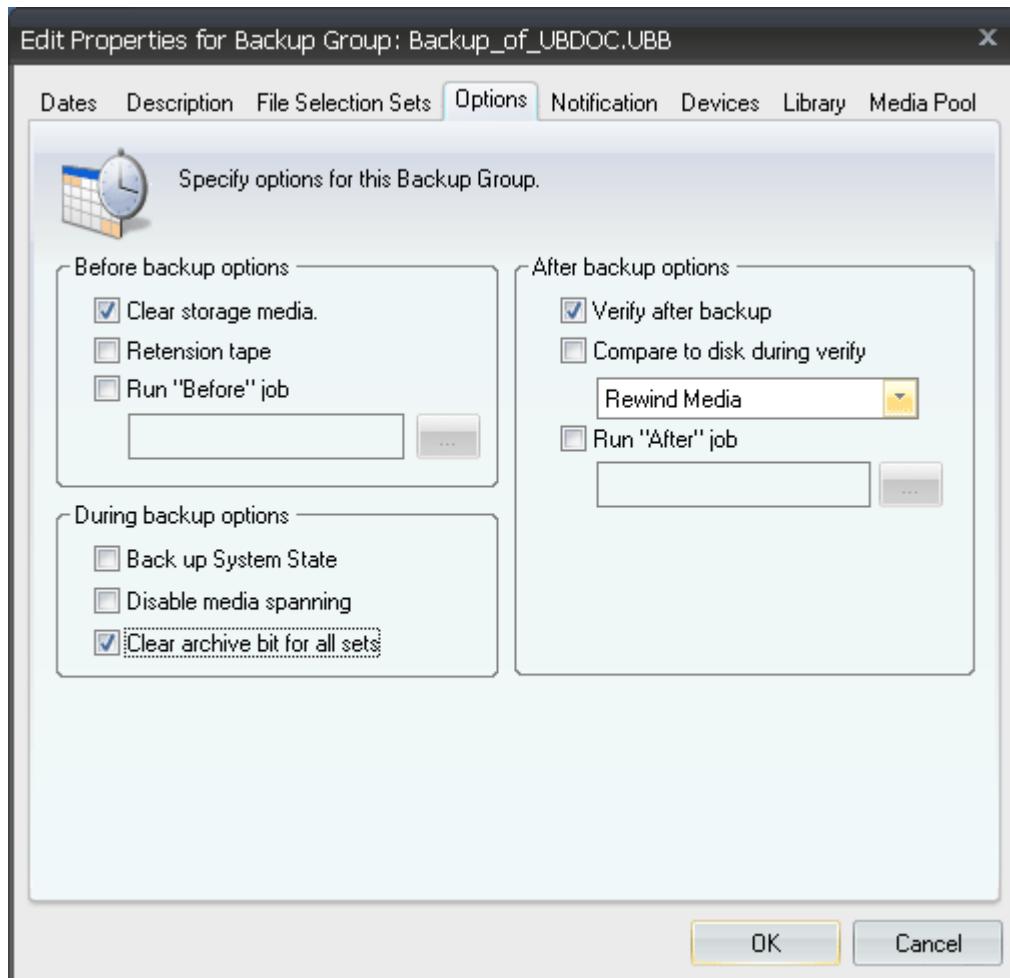
Fig. 3 - Backup Group Options, "Clear archive bit for all sets."
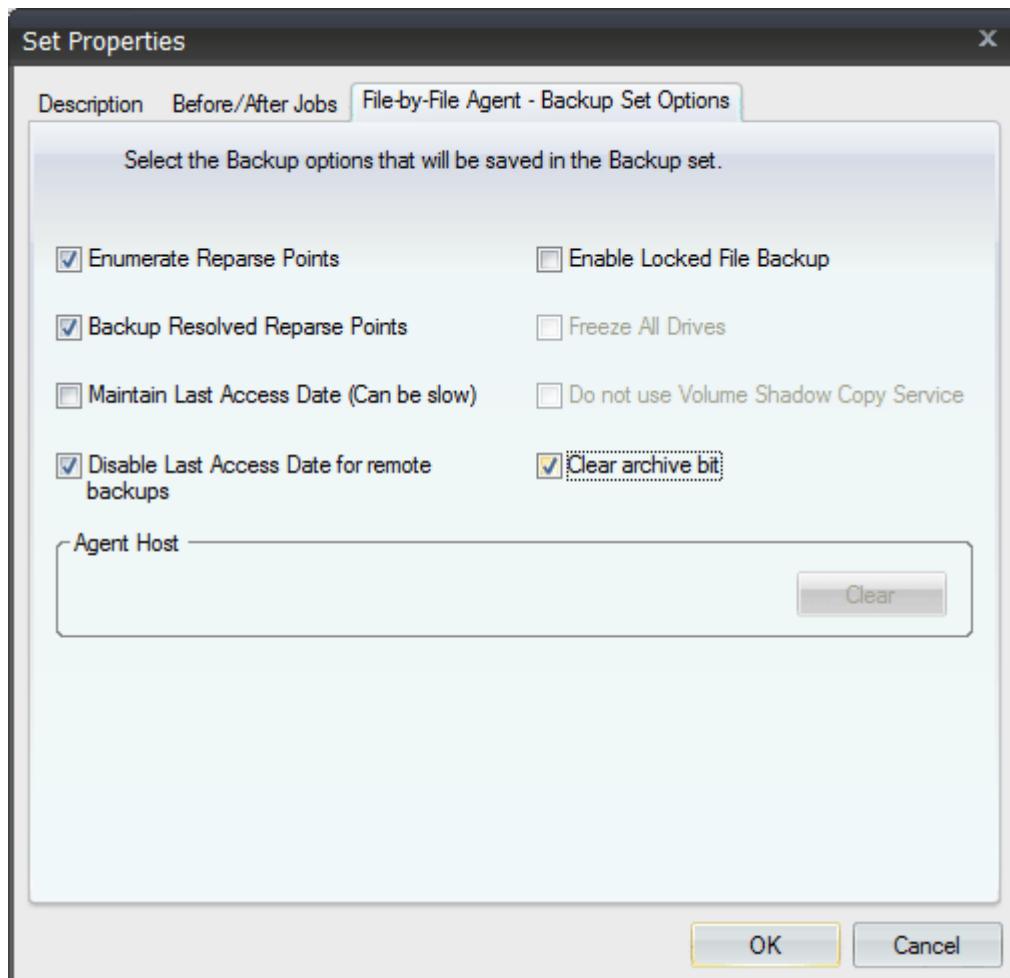
Fig. 4 - Backup Set Options, "Clear archive bit."

Clearing the Archive Bit - "Run Backup Now" (Ad-hoc) Backups

The setting to clear archive bits during "Run Backup Now" (ad-hoc) backups can be set in either the Backup Set Options (Fig. 4), or in the "Backup Options" dialog (Fig. 5) prior to starting the backup. When the archive bits are cleared during a backup, this sets up the possibility of using the "Modified files (Archive bit)" option to perform an incremental or differential backup.
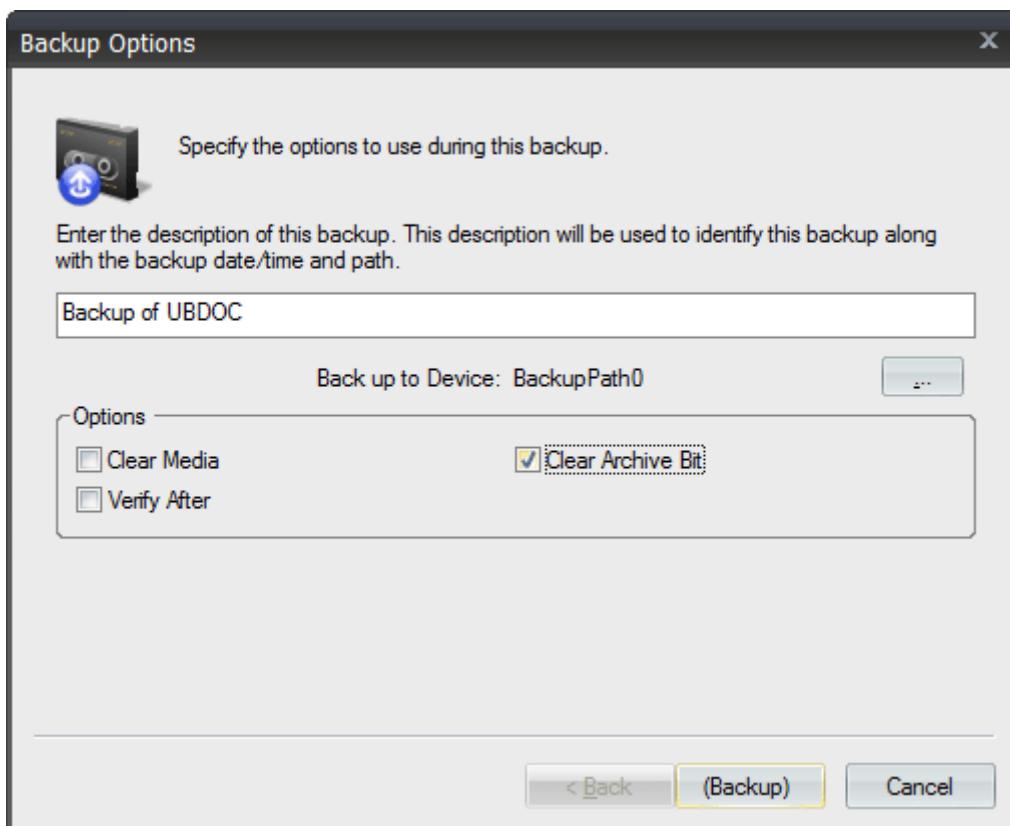
Fig. 4 - "Run Backup Now" Backup Options, "Clear archive bit."

Incremental vs. Differential Backups

The difference between incremental and differential backups is simply when and how often the archive bits are cleared. If you choose to clear the archive bits during the full backups, and then run a series of backups where the "Modified files (Archive bit)" option is selected but the archive bit is not cleared, then this is a "differential" backup. However, if you continue to clear the archive bits during the backups where the "Modified files (Archive bit)" option is selected, this is called an "incremental" backup. There are pros and cons to each type of backup.

Incremental backups where the archive bits are cleared during the "modified files" backup means that each backup will be relatively small and take less time. However, it also means that if a restore of the entire disk is needed, the last full backup then *each* subsequent incremental backup will need to be restored, in the correct order, to get all files to their most recent backup state.

With a differential backup, the archive bits are only cleared during the full backup, but not during each "modified files" backup. This means that each backup will gradually increase in both time and size, but also means that if a restore of the entire disk is needed, only two restores are needed – the full backup, and the last differential backup.

Both backup methods reduce backup time and size, an incremental reducing backup time and storage requirements, and a differential reducing restore time but requiring more space. The particular method employed will depend on the client's needs, as both incremental and differential backups have reasons for being used, or not used, as the case might be.

More Information:

See User Manual: Incremental/Differential Backups - Image Agent
See User Manual: Incremental/Differential Backups - File-by-File Agent

UBQ000091: Solving SCSI/CRC Errors

UBQ ID Number: UBQ000091
Last Modified: 2005-09-13

Summary:

Common causes of errors such as "Cyclic Redundancy Check" (CRC), "Write Worker Thread", and errors 23, 1111, and 1117.

Details:

Question:

I am getting CRC errors/SCSI errors. What is causing this?

Answer:

When you start seeing cyclic redundancy check (CRC) errors, that generally indicates one of a few things:

Dirty Tape Head

To fix this, run a tape head cleaner through your tape device a few times.

Bad Tape

The tape may have bad sectors or is getting old and the coating material is coming off or has stretched due to high heat and/or use. Do you retire your 4/8mm tapes after 30-50 passes? Based on our experience, after approximately 50 passes, 4/8mm tapes can become unreliable. If a tape has defective segments, the drive will attempt to write a data block "NNN" number of times (127 times for 4mm) before it skips a bad tape segment and moves on to the next. In such a case, a backup that normally takes 1 gigabyte can fill a tape. Another tip off is a backup that starts taking a lot more time than normal. There is a life cycle variation with some brands and types of tapes becoming unreliable earlier than others; e.g. DLT tapes can be used 100's of times. It's not worth jeopardizing your backups by using a tape until it fails! Also note that some brands of tapes seem to be more prone to bad sectors than others when used on different manufacturers tape drives. If a new tape fails, try using another brand of tape, or use a tape that is absolutely known to be good and see if it behaves differently.

Bad Tape Drive

A bad tape drive can be manifested any number of ways, including I/O errors, CRC errors and filling up tape. In one documented case, a technician removed the top of a 4mm tape drive and watched a backup go through an error free cycle without the tape moving an inch! This is a good example why it's important to always verify after a backup -- it would show an immediate error in such a case as the previous example. UltraBac has been programmed to accumulate tape drive errors and terminate a backup if more than "NNN" number of errors occur during a backup. The default registry setting is 100 errors.

Termination or Other Cabling Problems

Check to make sure your system is using active termination. Only very old SCSI devices use passive termination! Note that every SCSI controller has both internal & external device capability. If your system does not have any external devices, you must either have an active terminator plugged into the controller's external socket or you must deactivate the external SCSI devices option by using the manufacturer's software utility. Also note that almost every disk offers active termination through a jumper setting option on the drive itself. If you are experiencing SCSI errors, first remove all non-disk and tape SCSI devices from the bus experiencing the problem, e.g. scanners, CD drives, etc. Some of these devices can cause undue noise on the bus resulting in SCSI CRC errors. If problems continue, check each disk device and verify that it has not been jumped to provide active termination unless it is the last internal device on the cable! If you have an external disk cabinet, verify the same but the cabinet should be terminated with an external active terminator (so that another device can be easily added). If problems persist, remove all non-essential devices except one disk & tape. Swap cables to eliminate this as a problem. Sometimes an external cable will work between the controller and the first device but won't work between the first and second device (due to low quality).

Bus Termination Power

Normally the SCSI controller provides power to the bus for termination (this is the power source that makes the light shine on the active terminator at the end of the SCSI chain). When a new computer system is delivered from a major vendor, bus power is almost always properly applied. However, a serious problem can exist or be created because brand new disk drives are usually jumpered to also apply bus termination power when pulled new out of the box. If the SCSI controller and a disk drive both apply bus termination power, intermittent SCSI problems will occur during backup. Based on our experience, double bus termination power is a leading cause of backup problems when upgrading to a high performance backup program even though normal disk activity does not seem to suffer or the standard NT/2000 backup applet works OK. Unfortunately, the only way to eliminate this as a problem is by examining each internal & external disk for its jumper settings.

A problem with the SCSI card on the computer itself.

Question:

I am receiving 1111 or 1117 errors. What is most likely the problem?

Answer:

Check your SCSI configuration:

- What type SCSI controller do you have?
- What is the physical configuration, internal and external?
- Check for proper termination power, termination (Active, NOT Passive).
- Check your Cabling. Swap cabling if possible and retest.
- Check the card itself. Run diagnostics and/or switch cards if possible.

Termination is quite often the problem with 1111 and 1117 errors especially if these errors don't occur on backup and DO occur on verify. You should always verify all backups for this reason.

More Information:

See UBQ: UBQ000092 – Solving Typical SCSI Problems

UBQ000092: Solving Typical SCSI Problems

UBQ ID Number: UBQ000092
Last Modified: Last Modified: 2010-01-21

Summary:

Installing a SCSI based storage device drive with removable media often creates a problem which can be extremely frustrating and time consuming to track down! Understanding SCSI is a fundamental requirement to solving problems introduced by changing or adding devices on a SCSI bus.

SCSI stands for Small Computer System Interface. SCSI has allowed diverse peripheral manufacturers to develop new devices for a broad range of platforms.

SCSI devices are connected and cabled together in a daisy chain to the SCSI adapter card or controller. Each device must have a unique address which is normally 0-6. A SCSI controller supports one chain usually which allows both internal and external devices to be connected. The controller is normally assigned device number 7. The internal cable is a flat ribbon cable with 1-7 IDC connectors. One end of the ribbon cable is plugged into a connector block on the controller card and then is plugged into each internal device and is terminated at the last device. The external cable is round and connects to the outside plug on the controller card and can come with 3 different combinations of external connector plugs. The connector plug will either be a 50 pin Centronics (SCSI 1), a 50 pin mini-D shell or MDS50 (SCSI 2), or a 68 pin mini-micro (SCSI 3) connector. Note that the controller card may have a jumper setting which must be enabled to allow external devices. When the controller is set to allow external devices, an external termination plug is then required.

SCSI devices can be connected together using either a Single Ended or Differential SCSI Bus. Basically, Single Ended Buses are less expensive and more restrictive in length (from to 3 to 6 meters). Differential Buses are more expensive and allow a much longer cable length (up to 12 meters). The vast majority of devices installed today are Single Ended, therefore, for the purpose of the following discussion, it is assumed that you will have a Single Ended bus and devices.

The primary problem with connecting external SCSI devices to a working system is corruption (electrical noise on the bus and/or termination voltage that is either too high or too low) which is interjected by either cabling or termination. ***There is no substitute for quality cabling and termination!***

Excessive electrical interference is invisible to see, however, the result is always (1) the device is not recognized by the adapter card, (2) it completely fails to work, (3) seems to work but has excessive errors or, (4) works for awhile but then has a fatal error. The errors can be either on the backup or restore/verify operation side. The device may seem to backup OK but then will fail when attempting to read the media. These are all classic SCSI problems.

In some instances, the cause for electrical interference on a SCSI bus already exists but is only manifested when either a new device is added or when an application is installed which drives the bus to higher performance levels. Either condition can cause a marginal system with a problem to fail where previously the level of corruption did not cause any noticeable failures. A SCSI peripheral will retry sending a block of data a number of times before failing, with a hardware error, therefore, note that a system with a marginal problem can also cause the system to run slowly but without any hard errors until something changes on the system like adding a new device.

Details:

Cabling

Cabling can be too long, too short, be of poor quality or simply defective. A 100% SCSI 1 system can have a maximum cable length of 6 meters (about 19 feet). This includes both the internal & external cable length from the controller card to the ends of the SCSI chain (including the ribbon cabling inside external cabinets). SCSI 2/3 systems can only be about 3 meters. As a general rule, keep cables as short as possible but not under 6 inches. Be wary of inexpensive cables, which are often delivered with a new device. A quality cable is always thick because it has every data wire wrapped with a separate ground wire. The best cables have gold-coated connectors for maximum conductivity and have a ferrite ring around the cable end closest to the device to reduce or eliminate interference and cost around $85 dollars.

Termination

There are two types of termination, passive and active. An external terminator is a cap that fits on the last device in the chain. The internal chain is also terminated on the last device, however, termination may be provided by either a jumper setting on the last device (typically a disk drive), a set of removable resistors (either tape or disk), or by an external terminator block which is specially designed to terminate the last device on an internal SCSI bus.

Only SCSI 1 systems can use passive terminators! Passive terminators do not regulate voltage, which can end up being either too high or too low. Either condition will cause corruption that gets progressively worse as the length of the chain gets longer. Even if you have a SCSI 1 system, use an active terminator. All current model disk drives provide active termination when this option is used. *Never mix passive and active terminators on the same bus!*

While each end of the SCSI bus must be terminated properly (internal & external), accidental double termination will also cause excessive electrical interference. Double termination is most often caused when one or more SCSI devices on either the internal or external chain are set to provide termination. An "internal" example of this would be to add a new tape drive as the last device on the internal cable and setting it to provide termination without removing the termination setting of the disk drive which was the previous last device. An "external" example would be to add another external device and add a terminator plug when the previous last device is also set to provide termination.

Active terminators use one or more voltage regulators to ensure that the correct voltage is provided with lower signal distortion. *A high quality active terminator provides better voltage regulation*! Granite Digital's active terminator automatically adjusts voltage and provides information regarding both the status of bus termination and power but also activity. Granite Digital products can be purchased through BEI or can be ordered directly from Granite Digital at (510) 471-6442 or "http://www.scsipro.com ".

Bus Termination Power

Power to the terminator is either supplied by the adapter card or is provided by a SCSI peripheral device, e.g. disk drive. *Termination of the last device and termination power are not the same thing!* Another common cause for corruption is when both the adapter card and a SCSI peripheral device are set to provide termination power to the bus. As a general rule, only the adapter card should be set to provide termination power to the SCSI chain. Newer SCSI devices usually have a setting which can also provide termination power. All external and internal devices should have termination power disabled! Note, however, the bus must have termination power.

This is normally visible with active termination. An external active termination cap has an LED diode which is lighted (typically green) when power is applied to the bus.

SCSI Address Conflicts

Each device on an adapter card requires a unique address. A device's unique address is either set by jumper settings or dipswitches on the device itself or by means of an address clicker when housed in an external cabinet. When adding a new device in an external cabinet which is set properly for the address externally but fails to be recognized by the adapter card or the system fails to boot, remove the cabinet cover and verify that the clicker connector is actually connected to the address pins on the device and check the termination status to verify that is set correctly.

Troubleshooting

When trying to solve SCSI induced problems, basically follow these guidelines:
1. Calculate the total SCSI cabling length and verify that it does not exceed the maximum length.
2. Inspect the cables and connectors for problems and fit – disconnect, reconnect and test again.
3. If a storage device drive is added as the last device and does not work, remove all intermediary devices and retest with the storage device drive connected with a known working cable directly to the adapter card.
4. Use the shortest cables possible.
5. Only use quality cables – spend the extra money!
6. Ensure that the adapter card provides termination power and that no other device is also providing power.
7. When attaching external devices, ensure that the adapter card is physically set correctly. Adapter cards must also be modified occasionally to change the default operational characteristics, e.g. set-up mode for Adaptec SCSI controllers is accessed by pressing CTRL-A during the boot process.
8. Only use a quality external terminator – spend the extra money!
9. Ensure that every SCSI device has a unique address.
10. Ensure that only the last device on both the internal and external cable is terminated with active termination.
11. Use a quality external cabinet with the best power supply you can find.
12. Put the PC and all attached SCSI peripherals on a regulated power source, e.g. UPS. BEI has noticed that tape drives are more susceptible to power problems than disk drives.

In closing, when testing a problem SCSI device that is new, it helps to know that the device, the cable and the terminator work correctly. Parallel testing can often be accomplished on another machine or by removing similar equipment from a known working machine and installing and testing on the problem machine. This allows the trouble shooter to focus on the areas, which must actually be causing the problem! In the end, finding a problem is simply a process of elimination. Try the obvious first and then check every possible cause, no matter how remote, one at a time, to discover the source of the problem. It can turn out to be something as simple (but hard to find) as one defective IDC connector on an internal ribbon cable within an external cabinet!

More Information:

See UBQ: UBQ000091 – Solving SCSI/CRC Errors

UBQ000112: Troubleshooting Permissions Issues

UBQ ID Number: UBQ000112

Last Modified: 2011-05-26

Summary:

Troubleshooting steps to be used when receiving "Access Denied" error messages during backups.

Details:

UltraBac Management Service Account Permissions

NOTE: This should only be changed if you are having permission errors.

The following user rights need to be assigned to the account specified for the UltraBac Management service:

- Logon as a Service
- Backup operator.

It is recommended that the UBMS account be given Domain Admin privileges. If UltraBac is going to function in a domain, it really is best to make the UltraBac user a "Domain Admin" as the registry backup functions require access to the admin shares (e.g. C$) of the remote machines. If UltraBac is only going to backup a local machine's resources (not its registry) then membership in "Backup Operators" is sufficient.

Another safety feature that you can do if you are worried about security is to remove the privilege to "Log on locally" from the UltraBac user, and this will prevent anyone from logging on as UltraBac without affecting the operation of scheduled jobs.

File Permissions

There are three situations in which UltraBac will not restore file permissions:

- "Restore security permissions" and "restore security permissions on existing folders" is deselected.
- The restore is being sent to a FAT partition instead of NTFS, so the permissions won't restore
- The files are being restored to a non-NT/2000 machine. (Unix using Samba, etc.)

Backing Up Across Domains

If there is a trust relationship, then make sure that the UltraBac user is a local administrator on the machine you are trying to backup. If there is not a trust relationship, you would treat the remote machines as if they were in a workgroup. To do this you will need to add accounts to the backup machine and the remote machine. So the backup machine will need to have an entry in authentication so it can communicate with the remote machine, and the remote machine will need to have authentication for the backup machine. This way you will have permissions going both ways.

Setting Backup priority

When trying to run remote backup with High priority, you receive the following error:

> Unable to set priority, error 87.

(The account on the remote computer has of course the necessary right to adjust process priority.)

Go to "Manage" / "General" / "Backup Options" and change the priority to Normal and then see if the error disappears. (High should never be selected due to the effect it can have on system performance, and even on the performance of the backup process itself).

More Information:

See UBQ000198: Backup Account Permissions

UBQ000150: Installing the Media Library Driver (Autoloader) in Windows 2008 / 2008 R2

UBQ ID Number: UBQ000150
Last Modified: 2010-01-14

Summary:

Installing the UltraBac Software Medium Changer Driver (Autoloader) in Windows 2008 / 2008 R2

Details:

1. Right-click "My Computer" then click "Manage."
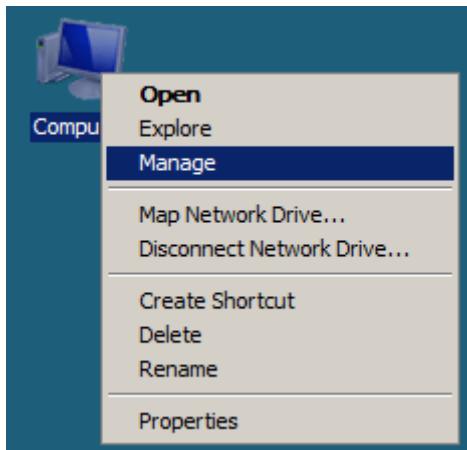
Fig. 1 - Opening the Server Manager Console.

2. Expand "Diagnostics" then click "Device Manager."
3. Expand "Medium Changer devices" in the right pane.

4. Right-click "Unknown Medium Changer" and select "Update Driver Software..."
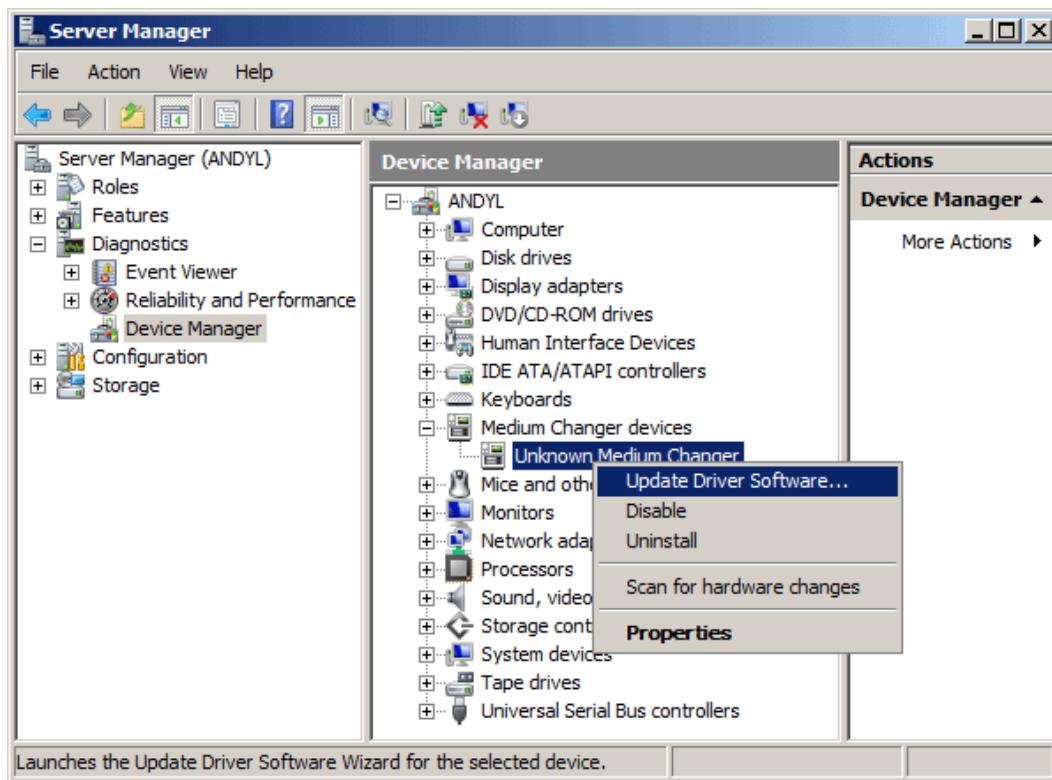
Fig. 2 - "Update Driver Software..." for the Unknown Medium Changer.

5. In the "Update Driver Software - Unknown Medium Changer" dialog, select "Browse my computer for driver software."
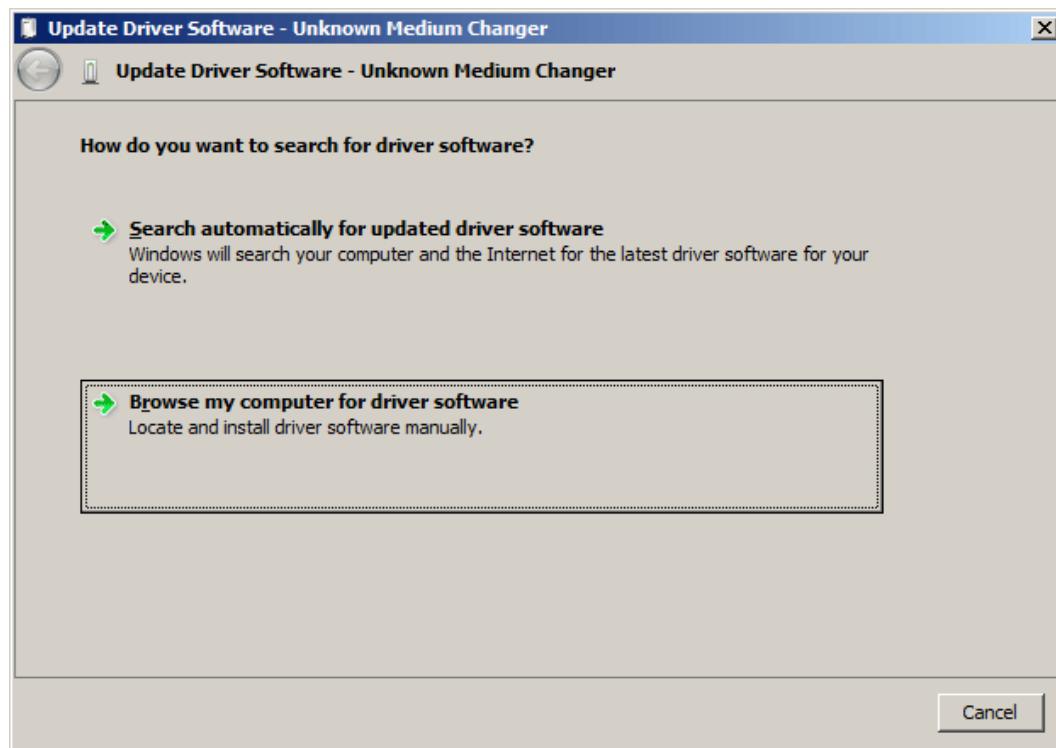
Fig. 3 - "Update Driver Software" Driver Search Method Dialog.

6. Select "Let me pick from a list of device drivers on my computer."

Fig. 4 - "Update Driver Software" Driver Search Location Dialog

7. Click "Have Disk."
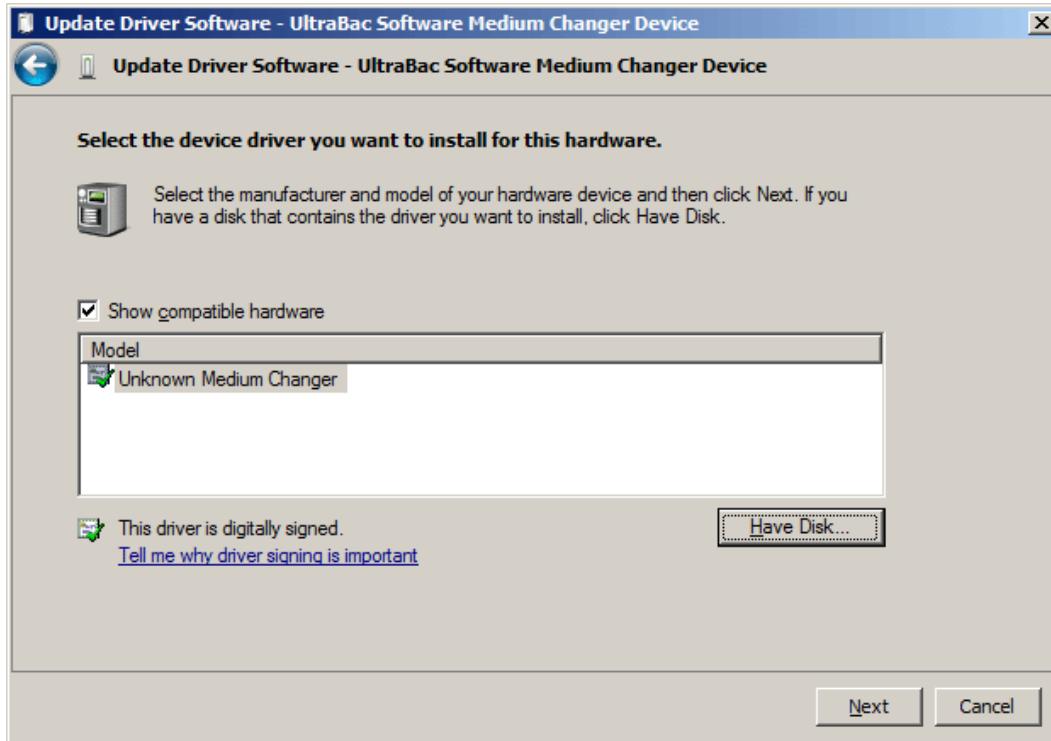
Fig. 5 - "Update Driver Software" Device Driver Selection

8. In the "Install From Disk" dialog, browse to the "\Drivers\Win2k\" ("\Drivers\Win2k\x64" for x64 systems) sub-folder of the UltraBac folder, select "mchgr.inf" then click "Open"/"OK."
9. Select "UltraBac Software Medium Changer Device" then click "Next."
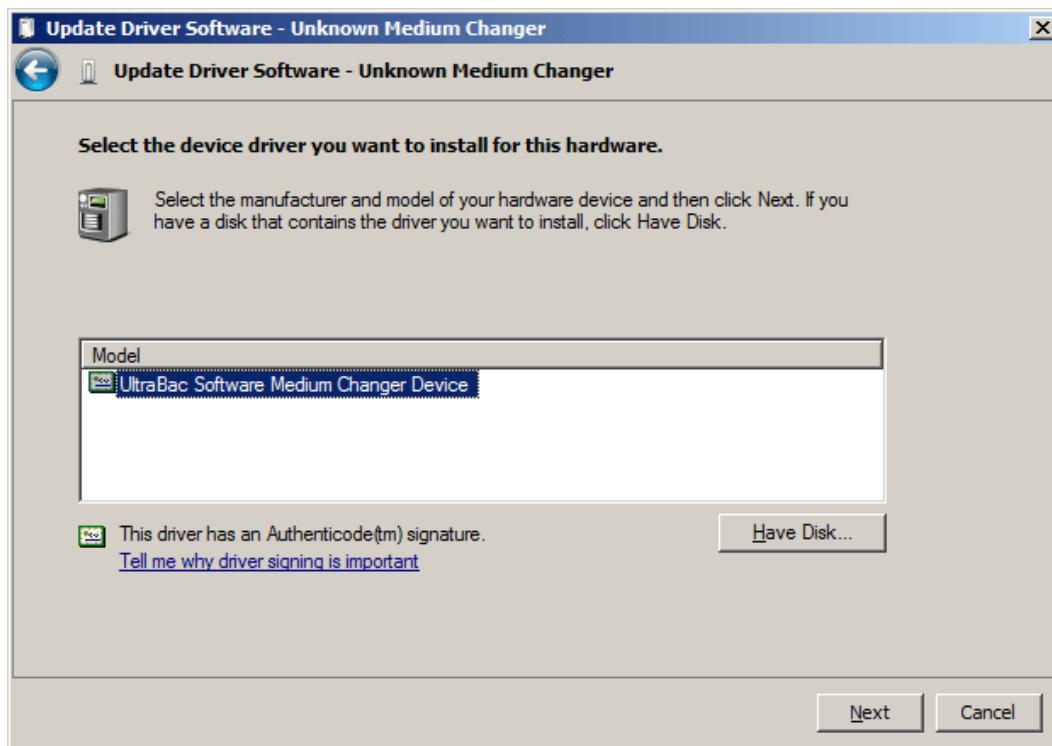
Fig. 6 - "Hardware Update Wizard" Device Driver Selection.

10. An "Update Driver Warning" will appear, click "Yes" to continue.

Fig. 7 - "Update Driver Warning" Driver Installation Warning

11. Click "Close" to close the "Update Driver Software" dialog.
12. Confirm that the "UltraBac Software Medium Changer Device" has been installed successfully.
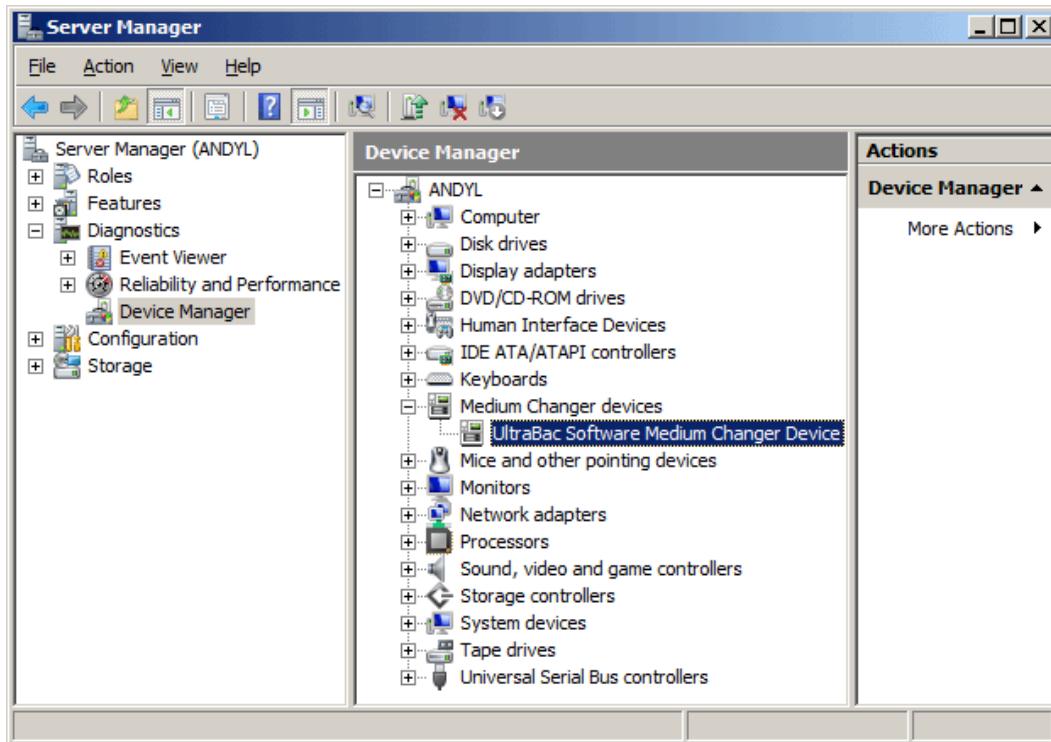
Fig. 8 - "Device Manager" showing the "UltraBac Medium Changer Device" driver.

13. Close the "Server Manager" window.

More Information:

User Manual: Media Library Controls

UBQ000157: Configuring the UltraBac Centralized Reporting Console

UBQ ID Number: UBQ000157
Last Modified: 2009-10-21

Summary:

Using UltraBac's Centralized Reporting Console, users may sync backup, verify, restore and UltraCopy XML logs from multiple backup servers to a central location, then view them in an easy-to-view tree or spreadsheet format. The Reporting Console accepts queries based on the session's date/time range, and results can be restricted based on backup and/or agent host. Results are displayed in either a log file tree or spreadsheet format with color-coded status icons indicating which sessions encountered errors or warnings.

Details:

Prerequisites

- Internet Information Server (IIS) 6.0 (Windows 2003/XP) must be installed on the machine hosting the Centralized Reporting Console. IIS 7.0 (Windows 2008/Vista) is not supported.
- Active Server Pages and ASP.NET support must be installed with IIS.
- Microsoft .NET Framework 2.0 or later must be installed on the machine hosting the Centralized Reporting Console.
- Internet Explorer 6.0 or later must be used to view the logs.
- UltraBac 9.x or later is required. Logs from older versions will not display.

Configuring Centralized Reporting

1. Click "Start"/"Run...," type "notepad" in the text box, then click "OK."
2. Click "File"/"Open," type "C:\Program Files\UltraBac Software\UltraBac\Reporting\synclogs.aspx" in the text box, then click "Open."
3. Replace "*UBCR_SERVERNAME*" with the name of the UltraBac Centralized Reporting Server.
4. Replace "*DOMAIN\username*" with an account to use to connect to the backup server(s).
5. Replace "*PASSWORD*" with the password associated with the account specified.
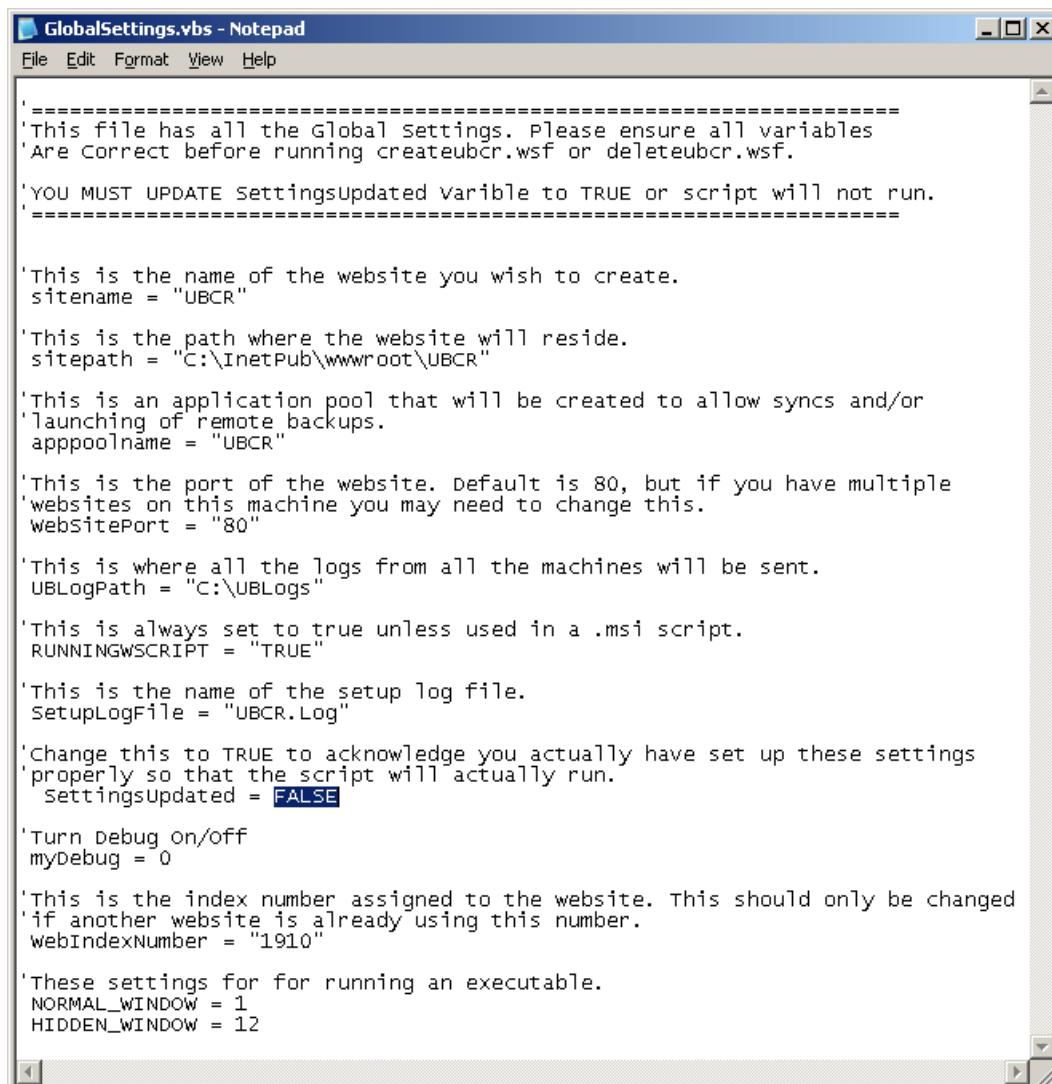
Fig. 1 - Editing the synclogs.aspx file

6. Click "File"/"Save" to save the changes.
7. Next, click "File"/"Open," type "C:\Program Files\UltraBac
   Software\UltraBac\Reporting\synclogs.cmd" in the text box, then click "Open."
8. Replace "*UBCR_SERVERNAME*" with the name of the UltraBac Centralized Reporting
   Server.

Fig. 2 - Editing the synclogs.cmd file

9. Click "File"/"Save" to save the changes.
10. Next, click "File"/"Open," type "C:\Program Files\UltraBac
    Software\UltraBac\Reporting\GlobalSettings.vbs" in the text box, then click "Open."
11. Change the "WebSitePort" if necessary (Default: Port 80), otherwise change
    "SettingsUpdated = FALSE" to "TRUE." The remaining settings are recommended to
    remain unchanged.

Fig. 3 - Editing the GlobalSettings.vbs file

12. Click "File"/"Save" to save the changes then "File"/"Exit" to close Notepad.
13. Click "Start"/"Run...," type "C:\Program Files\UltraBac Software\UltraBac\Reporting\createubcr.wsf" in the text box, then click "OK." This script will perform the following functions:
    - Copy files to the necessary locations.
    - Create the central log folder (C:\UBLogs) and "ublogs" share.
    - Create the UltraBac Centralized Reporting Console Application Pool within IIS.
    - Enable the required ASP/ASP.NET Web Extensions within IIS.
    - Create and start the UltraBac Centralized Reporting Console web site within IIS.
14. Click "OK" to the prompts and note any errors.
15. The UltraBac Centralized Reporting Console has now been created.

Using the UltraBac Centralized Reporting Console

1. Open the Microsoft Internet Explorer web browser.
2. Enter the URL "http://<hostname>" into the "Address Bar."

3. If the list of UltraBac backup servers to be synced from needs to be edited, click "Edit Servers.ini."
4. Add server hostname(s), then click "Save to Servers.ini."
5. Click "Sync Logs from Servers in Servers.ini" to sync logs.

Limitations

- UltraBac must be installed to the default location (e.g. C:\Program Files\UltraBac Software\UltraBac)
- UltraBac Logs must be written to the default location (e.g. ..\UltraBac\Logs or ..\UltraBac\x64\Logs)
- The UltraBac Centralized Reporting Logs Share "ublogs" must be configured to the default location of C:\UBLogs
- UltraBac version 9.0.x or greater must be used for backup.

Troubleshooting:

Windows Script Host Error 807700B7: "Cannot create a file when that file already exists" message when createubcr.wsf is running

Check to make sure another web site is not currently started on the port specified in GlobalSettings.vbs (Default: Port 80).

1. Click "Start"/"Programs"/"Administrative Tools"/"Internet Information Services (IIS) Manager"
2. Expand the tree and click on "Web Sites"
3. Confirm that no web site is currently running using the port specified in GlobalSettings.vbs (Default: Port 80).
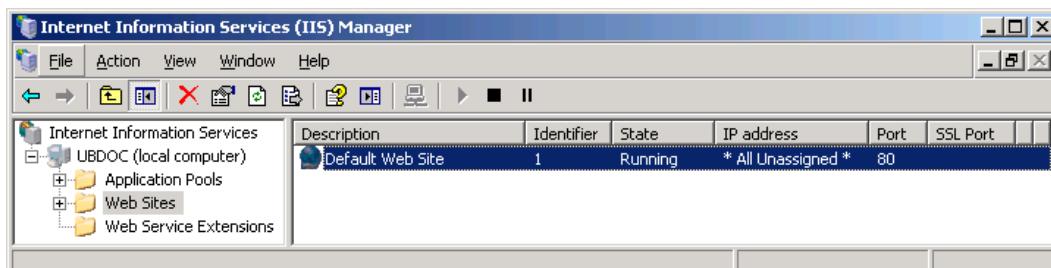
Fig. 4 - The "Web Sites" screen in IIS Manager

If a web site is currently running on the same port, either stop the web site or change the "webSitePort" specified in GlobalSettings.vbs.

Error: "Server Error in '/' Application." message when attempting to sync or display logs

Check to make sure the Web Service Extension "ASP.NET v2.0.xxxxx" is installed and "Allowed" in IIS.

1. Click "Start"/"Programs"/"Administrative Tools"/"Internet Information Services (IIS) Manager"
2. Expand the tree and click on "Web Service Extensions"

3. Confirm that "ASP.NET v2.0.xxxxx" is installed and and the status is "Allowed."
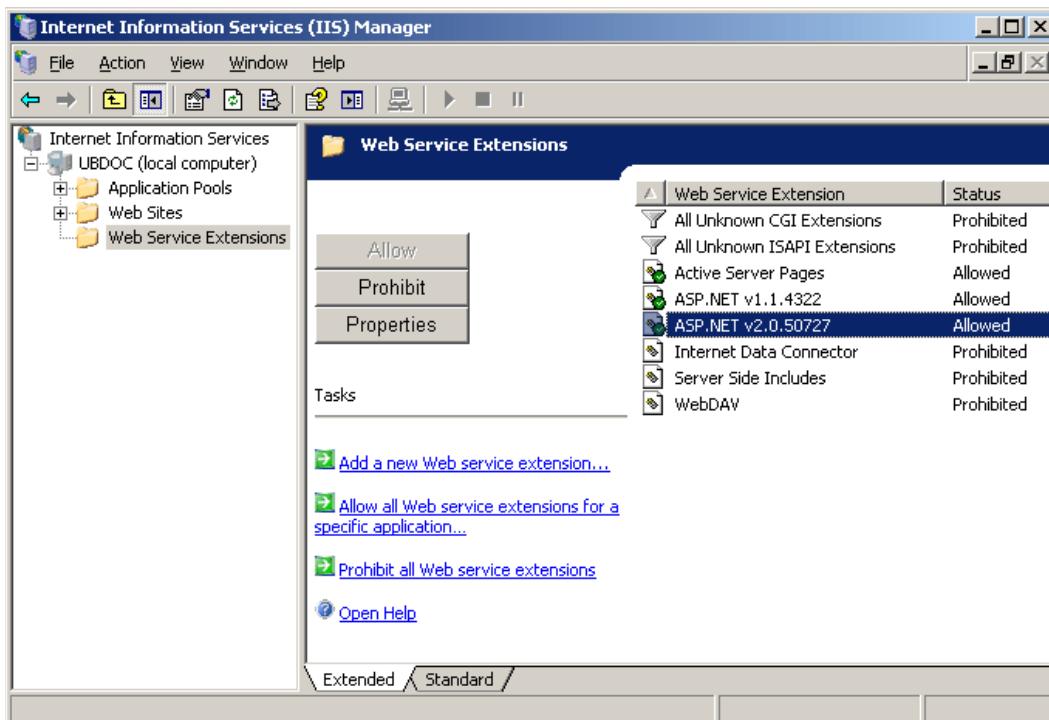
Fig. 5 - The "Web Service Extensions" screen in IIS Manager

If "ASP.NET v2.0.xxxxx" is not listed, install Microsoft .NET Framework 2.0 or later, or perform a repair thru "Add/Remove Programs" in the Control Panel on the latest .NET Framework installed.

UBQ000162: Non-UltraBac Specific Registry Keys

UBQ ID Number: UBQ000162
Last Modified: 2000-06-06

Summary:

Registry keys that affect UltraBac fall into two categories, UltraBac Specific and Non-UltraBac Specific. Non-UltraBac Specific Registry Keys are registry keys that UltraBac does not alter or access directly but may affect the use of UltraBac. This article presents the Non-UltraBac Specific Registry Keys.

When possible, registry keys should be set through their associated applications. Some "hidden" registry keys must be set using Microsoft's regedt32.exe (preferred) or regedit.exe utility.

NOTE: This document supplies information used to edit the registry. Incorrectly editing the registry can corrupt and destabilize your system configuration. Only experienced users should edit the registry. *Ensure spelling and capitalization and avoid typos.* UltraBac suggest performing a complete backup including the registry and familiarizing yourself with the restore process before editing the registry.

Details:

TcpMaxDataRetransmissions:REG_DWORD

This registry entry increases how many times TCP re-transmits. If you configured UltraBac to use SMTP for email notifications and you get an error similar to "SMTP error connecting to SMTP server: WSA 10060" you may need to increase this value. Typically you would set it to 10. If this fails to correct the problem increase this value to 20.
1. HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions:REG_DWORD
   The default value is 5 (which means TCP will re-transmit 5 times).
   A value of 10 (or 20) will increase the re-transmit value accordingly.

More Information:

http://support.microsoft.com/support/kb/articles/Q191/1/43.ASP

UBQ000194: Configuring the UX Agent on a Solaris Client

UBQ ID Number: UBQ000194
Last Modified: 2000-06-06

Summary:

Ultrabac UX Agent - Solaris/Intel Release
Release: 1.1

Details:

Introduction
~~~~~~~~~~~~
The UltraBac UX Agent will allow you to backup files from your
Solaris workstation/server using UltraBac.
The Agent works as a daemon which allows you to connect to the Solaris
system at any time to perform backup or restore operations.
The agent can be used in one of two ways:
- INETD invoked.
- Standalone.

INETD
~~~~~
If you are using INETD or the newer XINETD to launch your network services
then the UBUX agent can automatically install itself. This will involve adding
entries to the /etc/inetd.conf and /etc/services files. After the entries are
added INETD must be restarted.
If you are using INETD run the "./install" script which will complete the
installation.

Standalone
~~~~~~~~~~
Because some administrators prefer to not use INETD UX Agent provides the
"ubuxsrv" module which will once launched watch on TCP/IP port 1910 for
UltraBac connections and launch the Agent when needed. How you start ubuxsrv
is up to you. You may wish to invoke it from the command line as a background
task e.g. "./ubuxsrv &" or you may wish to start it from a start up script.
When run in stand alone mode ubuxsrv assumes the "ubuxagentd" file is located
at "/opt/ultrabac" if this is not the case please read the documentation regarding
"ubux.conf" to change the default location.

Installation Location
~~~~~~~~~~~~~~~~~~~~~~
The Solaris Agent for UltraBac will install to "/opt/ultrabac"
From here you can access the following programs:
ubuxsrv
~~~~~~~
This module allows the UX Agent to work independent of INETD or XINETD
This module still needs the ubuxagentd file.
ubuxpwd

~~~~~~~
This module is used to set the password which will be needed in order
to access the computer to perform a backup or restore.
ubuxagentd
~~~~~~~~~~
This is the actual backup agent file, you cannot invoke this directly.
It is either started by INETD/XINETD or ubuxsrv.

Configuration Files
~~~~~~~~~~~~~~~~~~
/etc/ubuxpwd.conf
~~~~~~~~~~~~~~~~
These are automatically generated when you run ubuxpwd to set the password. You
should not need to manually edit this file.
/etc/ubux.conf
~~~~~~~~~~~~~~
The file contains the configuration data for the agent. See the main documentation
for help on this file.

More Information:

See User Manual: Ux Agent

UBQ000198: Backup Account Permissions

UBQ ID Number: UBQ000198
Last Modified: 2011-05-26

Summary:

This document details the permissions required to run UltraBac software.

Details:

If any of the required permissions aren't allowed you will get an error similar to the following:

1. Unable to acquire backup/restore permissions.
2. Access denied Errors
3. You may not have the required permission to run this program.

To run the UltraBac Management Console, or to run backup jobs with UltraBac, the following permissions are required:

SE_BACKUP_NAME, "Backup Files and Directories"
SE_CHANGE_NOTIFY_NAME, "Bypass Traverse Checking"
SE_INCREASE_QUOTA_NAME, "Increase Quotas"
SE_RESTORE_NAME, "Restore Files and Directories"
SE_SHUTDOWN_NAME, "Shut down the system" (for some reason required for registry backups)

The following permissions are optional, but recommended:

SE_TCB_NAME, "Act as Part of the Operating System"
SE_INC_BASE_PRIORITY_NAME, "Increase Scheduling Priority"
SE_SECURITY_NAME,"Manage auditing and security log"
SE_TAKE_OWNERSHIP_NAME, "Take ownership of files or other objects"

These settings can be viewed on a local computer by going to the run line and typing "secpol.msc". From the domain level you would go to the run line and type" "Dompol.msc"

To refresh the permissions on a windows 2000 machine, you must either reboot, or run the following commands:

SECEDIT /REFRESHPOLICY USER_POLICY /ENFORCE
SECEDIT /REFRESHPOLICY MACHINE_POLICY /ENFORCE

On a 2008r2/2008/2003/XP host, use this command:

gpupdate /force

For more information on the SECEDIT command, please see the following Microsoft KB article: http://technet.microsoft.com/en-us/library/bb490997.aspx

For more information on the GPUPDATE command, please see the following Microsoft KB article: http://technet.microsoft.com/en-us/library/bb490983.aspx

We also have a utility that automates this. To give the necessary privileges to domain\admin on \\SERVER you would use the following utilities: ftp://ftp.ultrabac.com/pub/utils/bupriv/bupriv.zip

This also requires the ntrights.exe from the NT Resource kit.

Once you have ntrights.exe, bupriv.ini and forbupriv.cmd in a temp folder, run the following command:

forbupriv domain\admin \\server

To use this command you must have a file called bupriv.ini in the same directory as this command file. You must also specify at least one command line option.

Example: forbupriv DOMAINNAME\USERNAME

To add the privileges to another machine in the network you must specify 2 options at the command line.

Example: forbuipriv DOMAINNAME\USERNAME \\COMPUTERNAME

Once this has been run you will need to refresh the permissions.

More Information:

See UBQ: UBQ000112 – Trouble Shooting Permissions Issues

UBQ000205: Microsoft SQL "WITH MOVE" Option

UBQ ID Number: UBQ000205
Last Modified: 2010-01-12

Summary:

This document details the process of restoring a Microsoft SQL database to an alternate location (or with an alternate database name) using UltraBac.

Details:

UltraBac has the ability to move Microsoft SQL databases to either an alternate SQL server or to the same server (renaming the Databases) by using the SQL "WITH MOVE" option when restoring.

To use the "WITH MOVE" option, the exact database file names (both the data and log files) will need to be known. This information can be found in the backup index, after the database name. Using the "Northwind" database as an example, the database file names are "Northwind" and "Northwind_log".

Fig. 1 - Names of the database files.

Performing the Restore

In this example, the restore will be moving a database to a different SQL Server. When using the "WITH MOVE" option, only one database can be restored per operation.

The drive and the path where the new files will go does not have to be the same as the original, but the path must exist before the restore is performed. When restoring to the same server the same path where the original files are can be used, but the actual file names MUST be changed

and an alternate database name must be supplied or the original database / database files will be over written.

1. Launch the Restore by clicking the "Restore tab, then selecting an option from "Locate Backup Index."
2. Load the index for restore.
3. Select the database for restore.
4. Click "Action"/"Restore this Backup."
5. In the UltraBac SQL Agent Restore Options dialog, change the "Restore Destination" to the target server name.
6. Click "SQL MOVE Parameters."

Fig. 2 - SQL MOVE Parameters dialog.

7. In the "Alternate database name" box, enter the desired database name.
8. In the "Restore to path" box, type the new path for the database.
9. If the "Database files and logs" section did not auto-populate, click "Add."
10. In the "Original Database File Name" box, type in the original file name (without typing the .mdf).

11. In the "Restore As" box, type the path of the file and the file name (making sure to rename the file if needed) using .mdf/.ldf.
12. Repeat steps 9-11 for the transaction logs.
13. Click "Next"/"Restore"

When the restore is finished there will be a new database with the "Alternate database name" on the SQL server specified.

More Information:

UltraBac User Manual: SQL Agent

UBQ000210: UltraBac Backup Output Files

UBQ ID Number: UBQ000210
Last Modified: 201-02-25

Summary:

This article explains the files structure of how UltraBac writes it's backup files to disk.

Details:

When UltraBac writes to disk, it is VERY important to understand you should NEVER delete files from a backup path. If you delete any of UltraBac's backup files you might not be able to restore from that backup.

UltraBac uses files called .ubd

00010000.ubd --> will always be a Header file. This tells UltraBac that it is an UltraBac Storage device.
00020000.ubd --> will always be Data.
00020001.ubd --> will be data continuing on from the first data file.
00030000.ubd --> will always be an Index.
00040000.ubd --> will either be the End of media marker (0 KB in size) or another Data file

By default UltraBac will break the backups into 512mb chunks.

When "Clear Media" option is checked in the Scheduler, it will clear all UltraBac backup files from that BackupPath. If it is need to have an archive of backups on disk, it is better NOT to delete files from the BackupPath, but to use the option to delete backups after "x" amount of days.

UBQ000227: Recovering to an Exchange 2003 Recovery store

UBQ ID Number: UBQ000227
Last Modified: 2010-01-15

Summary:

Microsoft has added the ability to restore a full Exchange data store to an alternate Recovery store, for the purpose of mail item and mailbox recovery. This can eliminate the need to perform individual mailbox backups.

Details:

The first step in using a Recovery store is creating a Recover Storage Group. In the Exchange System Manager, browse down to the Exchange server (under Servers), right-click and select "New"/"Recovery Storage Group".

Fig. 1 - Creating a Recovery Storage Group.

For detailed directions on setting up a Recovery Storage Group, see:
Microsoft Technet: Setting up a Recovery Storage Group

Once the Recovery Storage Group is created, and the Recovery Store database is dismounted and set to be overwritten, perform an Exchange Database restore as specified in the UltraBac User Manual:
UltraBac User Manual: Exchange Agent

With the Recovery Store in it's default state, the UltraBac Exchange Agent will write the restore to the Recovery Store, and will not effect the active database.

Notes - Please Read:
Do NOT dismount the active Exchange Storage Group.
Do NOT check "This database can be overwritten by a restore" on the active Exchange Storage Group.

At no time during the Recovery Store restore process does the original Storage Group need to be dismounted, or have any settings changed. Any changes made to the original Storage Group could result in that Storage Group being overwritten by the restore.

More Information:

For a full reference guide on using Exchange Recovery Stores, see the Microsoft TechNet:
Using Exchange Server 2003 Recovery Storage Groups

For a full reference guide on merging data from the Recovery Store to the active Exchange store, see the Microsoft TechNet:
Exchange Server 2003 SP1 Recover Mailbox Data Feature

See UBQ000250: Exchange 2007 Support

UBQ000229: Unattended Installation of UltraBac

UBQ ID Number: UBQ000229
Last Modified: 2010-01-21

Summary:

Pushing the UltraBac 9 installation out to several remote machines using the GUI based setup requires some manual work. Each machine name must be specified during the rollout, along with the selection of installation components, depending on the preference of the user. As an alternative, a small batch file may be created and configured to install to several remote machines "unattended," free from error messages if they should occur.

Details:

The UltraBac installation cannot install to a machine that is actively running UltraBac. If a backup job is running or the user interface is launched on the machine to which you're installing, the setup program will fail for that machine, and it will continue going through the list to the next machine in line.

The following options are available by running "setup.exe" through the command line:

/TimeLimit [###] – Limits the amount of time the installation can run on each system to the number of seconds specified.

/InstallTo – A list of machine names separated by spaces is defined.

/Unattended – Suppresses any error messages.

/Logfile X:\path.txt – The path to an output log file, so that errors may be viewed if any occured during the installation.

/Inifile: <filename> -- Allows specification of an "ini" file.

Installing or upgrading to 40+ machines can be very time consuming if one had to do it manually each time new software became available. Writing a batch file automating this process takes a bit of time, but only as much as typing each machine name to which the installation is being pushed. The bulk of the batch file consists of machine names, which are separated by a single space. The following is an example of an unattended installation to five different machines, with a three minute timeout, and an output log file sent to "C:\outputlog.txt."

"C:\Program Files\UltraBac Software\UltraBac\Setup.exe" /TimeLimit [180] /InstallTo <machinename1><machinename2><machinename3> <machinename4><machinename5> /Unattended /Logfile C:\outputlog.txt

Also, if rolling out the software to machines in a different domain, the "Net Use" command may be used to establish connectivity before the installation begins. If access to the \\<machinename>\admin$ share is denied, the setup will fail. A "Net Use" command run prior to the installation with the proper credentials can establish access to the "admin$" share, enabling the installation to complete. An example of the "Net Use" command follows:

Net Use \\machinename /U:domainname\username password

More Information:

See User Manual: Installing UltraBac

UBQ000230: UBDR Gold Advanced Tools and Utilities

UBQ ID Number: UBQ000230
Last Modified: 2011-02-25

Summary:

In UBDR Gold you will sometimes need to restore to a larger or smaller partition. To do this you will need to use the advanced tools to create the new sized partitions.

Details:

Advanced Tools

The "*Disaster Recovery/Image Restore Options*" dialog box has an "Advanced Tools" option through which partitions may be edited, similar to the DOS "FDISK" utility. Editing "dynamic disk" volumes are not supported however, only "basic" disks may be created, deleted, and added. The utility may be used in cases where only one partition is to be restored to a different location, or perhaps when resizing a partition is necessary to expand the target for restore. Clicking "Advanced Tools" will show a dialog box similar to the screenshot below.

The "Select Disk" drop-down box chooses which disk in the computer to edit. The disks are numbered sequentially starting from "Disk0."

WipeMBR -- Clicking this radio button will clear all partition information on the disk, rendering it unbootable. Use this utility with extreme caution. Be certain that the correct disk is chosen through the "Select Disk" drop-down box before executing "WipeMBR."

Delete Partition -- The drop-down box will display all partitions on the selected disk. Choose "Delete Partition" by clicking the radio button beside it, selecting the desired partition through the drop-down box, and clicking the "Proceed" button at the bottom of the window.

Create Partition -- Both primary, extended, and logical partitions may be created through "Create Partition." Choose the type of partition to be created through the drop-down box and define the size of the partition by typing in the number of MB in the "Partition Size in MB" field.

More Information:

[See User Manual: Image Disaster Recovery Agent](#)
[See User Manual: UBDR Gold v5.0/v6.0](#)
[See UBQ000024: What is an Image Backup?](#)
[See UBQ000233: Resize Partitions During Image Restore](#)

UBQ000233: Resize Partitions During Image Restore

UBQ ID: UBQ000233
Last Modified: 2011-02-17

Summary:

UBDR Gold has the ability to restore an image backup to a partition larger than the original.

Details:

NOTE: When resizing partitions, the target partitions must be created before performing the restore operation, and the MBR (Master Boot Record) CANNOT be restored.

Creating the Partitions

If the partitions on the disk have not been created, the target partition(s) can be created through the 'Advanced Tools' in UBDR Gold.

1. Load the index from the backup storage media.
2. Select the partition(s) to restore, and click "Restore."
3. In the "Disaster Recovery/Image Options" screen, click "Advanced Tools."
4. Select WipeMBR and click "Proceed."

Fig. 1 - Advanced Tools in UBDR Gold

5. Click "OK" at the WipeMBR prompt.
6. Select "Create Partition."
7. Select the "Partition Type" from the drop-down menu, and enter the partition size (in MB).
8. Select the "Partition Style" from the drop-down menu, and select the one that pertains to the OS you are restoring
9. Click Proceed to create the partition.. (There will be a delay while the partition is created, you will get a pop-up message stating the process has finished)
10. Click "OK" at the confirmation prompt.
11. Repeat steps 7-9 for each partition to be created.

Performing the Restore

Once the partition(s) are created, cancel out of the "Advanced Tools" screen, returning to the "Disaster Recovery/Image Restore Options" screen.

1. Select the newly created partition from the "Restore entire image..." drop-down menu.

Fig. 2 - Disaster Recovery/Image Restore Options.

2. Check "Resize partition(s)
3. Click "Next."
4. Check "Run Unattended," and click "Restore."

More Information:

See User Manual: UltraBac Disaster Recovery
See User Manual: UBDR Gold v5.0/v6.0
See UBQ000230: UBDR Gold Advanced Tools and Utilities

UBQ000234: Common Backup Errors Explained

UBQ ID: UBQ000234
Last Modified: 2010-01-21

Summary:

The list of errors below are commonly found in UltraBac backup log files. Along with the error, basic trouble shooting steps can help to quickly resolve backup issues.

Details:

Error 5 - Access is denied.

5/31/2005 1:00:39 PM Error!
Failed to open file for backup '\\FIPI\D$\goldmine\GM4W6.DOC', error: (5-Access is denied.)

This error is directly related to permissions. If the user does not have permission to access the specified file, this error will be the result.

Error 23 - Data error (cyclic redundancy check).

5/30/2005 11:52:16 AM Error!
CheckWriteStatus, Error:(23 - Data error (cyclic redundancy check).)

This error usually means the tape device cannot properly read from or write to the current tape. Often times, this error can be cleared by cleaning the tape drive. It is strongly recommended to check the Windows System log for corresponding errors from the tape driver, SCSI driver or other hardware sources.

Error 32 - The process cannot access the file because it is being used by another process.

5/31/2005 3:42:22 AM Warning!
\\FIPI\D:\Program Files\Microsoft SQL Server\MSSQL\Data\master.mdf (32 - File In Use) (SHARING VIOLATION).

This error is returned when the file being backed up is open or exclusively locked by another application or service. To back these files up, either the application or service using the file needs to be closed, or a locked file backup agent can also back up many of these files safely.

In the case of Exchange or SQL database files, it is strongly recommended to use the corresponding backup agent in a separate set to ensure database integrity.

Error 53 - The network path was not found.

5/31/2005 2:02:44 PM Error!
Unable to find files \\LELE\H$*.*, error: (53-The network path was not found.)

This error is returned when the share or folder being backed up cannot be found on the network. This error is often seen when there is a firewall blocking the system being backed up, when there are failures/issues on the network, and when the system to be backed up has been turned off.

Error 64 - The specified network name is no longer available.

5/9/2005 4:11:38 PM Error!
Unable to find files \\LELE\H$*.*, error: (64-The specified network name is no longer available.)

This error is returned when the computer being backed up can no longer be contacted on the network. This error is usually caused by some kind of network issue, or the computer being turned off/rebooted during backup.

Error 170 - The requested resource is in use.

5/15/2005 7:00:20 PM Error!
Could not open device Tape0, error:(170-The requested resource is in use.)

This error is returned when the backup target device is being used by another application or process. Ensure there is not another backup process running when this error occurs. In the Windows Task Manager, check for any orphaned UB.exe processes, or more than one UBMS.exe process. This error can also be caused by UBUI.exe when in the beginning stages of a restore.

Error 1117 - The request could not be performed because of an I/O device error.

This error is often related to error 23. This error is almost always accompanied by entries in the Windows System log from either the SCSI card or the tape device. On occasion, cleaning the device can resolve this error, but usually this error means there is a critical failure in the hardware.

Error 10061 - No connection could be made because the target machine actively refused it.

5/13/2005 3:53:34 AM Warning!
Unable to start agent on FIPI (10061-No connection could be made because the target machine actively refused it.), attempting locally.

This error occurs when UltraBac's management service cannot connect to the management service on a remote system. This error usually means that the UltraBac Management service is either not started or not installed on the connection target (usually specified in the error). Ensure that UltraBac is installed on the remote target, and that there is an instance of UBMS.exe running.

More Information:

See User Manual: Installing UltraBac
See User Manual: Exchange Agent
See User Manual: Locked File Backup Agent
See User Manual: SQL Agent

See UBQ000230: UBDR Gold Advanced Tools and Utilities

Version: UltraBac v9.x
Copyright UltraBac Software 2010

UBQ000242: Removing Media Pools

UBQ ID Number: UBQ000242
Last Modified: 2011-02-25

Summary:

To return the ability of a media library to use slot-based backups, the media pool information must be cleared from the backup host.

Details:

Media pool information is stored in the UltraBac "Data" directory. By default, this is located at:
"C:\Program Files\UltraBac Software\UltraBac\data"

The media pools are stored in ".ini" and ".bak" files that match the name of the media pool. The names are formatted with "ubmp_0_<pool name>."


Fig. 1 - Media pool configuration files.

To remove the media pools:

1. Remove all the ".ini" and ".bak" files from the "Data" directory that correspond with the media pools. "ubholiday.ini" should not be removed.
2. Click "Start"/"Run...," type "services.msc" in the text box, then click "OK."
3. Right-click on "UltraBac Management Service" and select "Restart."

The media pools can be restored by returning the .bak and .ini files to the 'Data' directory and restarting the UltraBac Management Service.

NOTE: Slot based backups will not run if a media pool has been created.

More Information:

See UltraBac User Manual: Media Library Controls
See UBQ000150: Installing the Media Library Driver (Autoloader) in Windows 2008

UBQ000249: SideBySide Errors in System Log

UBQ ID Number: UBQ000249
Last Modified: 2010-04-20

Summary:

Installing UltraBac 9.x has caused event log errors with the source SideBySide.

Details:

Due to a change introduced by Microsoft into Visual Studio 2005, some applications can cause system log errors during initialization. These are the errors that appear when UltraBac is run:

Event Type: Error
Event Source: SideBySide
Event Category: None
Event ID: 59
Date: 7/31/2007
Time: 4:05:37 PM
User: N/A
Computer: SERVER66
Description:
Generate Activation Context failed for C:\Program Files\UltraBac Software\UltraBac9\MFC80U.DLL. Reference error message: The manifest file contains one or more syntax errors.

Event Type: Error
Event Source: SideBySide
Event Category: None
Event ID: 58
Date: 7/31/2007
Time: 4:05:37 PM
User: N/A
Computer: SERVER66
Description:
Syntax error in manifest or policy file "C:\Program Files\UltraBac Software\UltraBac9\Microsoft.VC80.MFCLOC.MANIFEST" on line 5.

Event Type: Error
Event Source: SideBySide
Event Category: None
Event ID: 34
Date: 7/31/2007
Time: 4:05:37 PM
User: N/A
Computer: SERVER66

Description:
Component identity found in manifest does not match the identity of the component requested

Event Type: Error
Event Source: SideBySide
Event Category: None
Event ID: 59
Date: 7/31/2007
Time: 4:05:31 PM
User: N/A
Computer: SERVER66
Description:
Generate Activation Context failed for C:\Program Files\UltraBac
Software\UltraBac9\MFC80U.DLL. Reference error message: The manifest file contains one or
more syntax errors.

Resolution:

Installing the Microsoft Visual C++ 2008 SP1 Redistributable Package (vcredist_<platform>.exe)
will stop the above system log entries from being created.

x86 Platform

x64 Platform

UBQ000250: Exchange 2007 Support

UBQ ID Number: UBQ000250
Last Modified: 2007-10-24

Summary:

This document details the steps to be taken in Exchange before both backup and restore to ensure the success of these operations.

Details:

Adding or Verifying Exchange Permissions

Before backup, it is necessary to confirm in Exchange that the UltraBac backup account has permission to access the Exchange database. To verify permissions:

1. Open the Exchange Management Console.
2. Highlight the Exchange Organization Configuration node.
3. If the UltraBac account isn't listed, Right-click on Organization Configuration and select Add Exchange Administrator.


Fig. 1 - Checking the UltraBac account in the Exchange Management Console.

4. When the Add Exchange Administrator wizard appears, click browse and select the UltraBac user account.
5. Ensure that Exchange Organization Administrator role is selected and click Add.

Preparing the Database for Restore

Before performing a restore operation, the database must be prepared for restore:

1. Open the Exchange Management Console.
2. Expand the Server Configuration node and select mailbox.
3. In the main window, select a database to restore.
4. Right-click the database and select "dismount."

NOTE: It is highly recommended to move the log files to a separate location so that the log files can be replayed if needed.

---

5. Clear the contents of the mailbox store folder
6. Right-click the database again and select "properties."
7. In the properties dialog, check "This database can be overwritten by a restore" and click OK.
8. Repeat for all databases to be restored.

Creating the Recovery Storage Group

The recovery storage group should be created through the Database Recovery Management tool in the Toolbox.

For more information on using a recovery storage group, please check the Microsoft website:

Microsoft Technet: Recovery Storage Groups

Fig. 2 - Disaster Recovery Tools in the Toolbox.

More Information:

See User Manual: Exchange Agent

See UBQ000227: Recovering to an Exchange 2003 Recovery Store
Microsoft Technet: Recovery Storage Groups

UBQ000251: Encrypting Backup Data with AES in UltraBac 9.x

UBQ ID Number: UBQ000251
Last Modified: 2009-12-11

Summary:

How to set up UltraBac to use Advanced Encryption Standard (AES) to protect backup data.

Details:

In prior versions of UtraBac, the Blowfish encryption algorithm was used to encrypt backup data at the set level. In UltraBac 8.3.1, encryption using AES was introduced, though the Blowfish algorithm remained available when AES was not enabled. Beginning with UltraBac 9.0 and later versions, Blowfish encryption support has been removed, though restore support for data encrypted using the Blowfish algorithm will always be available.

AES is enabled globally and operates at the device level; when AES encryption is enabled, backup data written to any UltraBac Storage Device will be encrypted. It is recommended, though not required, to re-create any sets that are configured to use the Blowfish algorithm to remove the existing Blowfish settings. Existing unencrypted UltraBac storage media will need to be re-prepared prior to use. UltraBac jobs that have the "Clear media" option selected will automatically prepare the media prior to backup.

Configuring AES

To enable AES:

1. From the main UltraBac toolbar, click "Manage"/"General"/"Encryption Options"

Fig. 1 - AES Encryption Configuration Options.

2. Set the AES encryption strength:
   - o Disable - Turns off all AES encryption usage.
   - o 128 bit - Sets AES to use a 128 bit key.
   - o 192 bit - Sets AES to use a 192 bit key.
   - o 256 bit - Sets AES to use a 256 bit key.

3. Select the method for generating the encryption key:
   - o Generate key from ASCII phrase - Creates an encryption key using any ASCII characters, of the specified encryption strength.
   - o Generate key automatically - Creates a random encryption key using HEX characters, of the specified encryption strength.
   - o Enter hex key directly - Allows a user to create a specific encryption key using HEX characters, of 32, 48, or 64 characters.

4. Click "OK" to set the encryption options as specified.

Additional AES Options

- Encryption key - The "Phrase" and "Confirm phrase" fields allow users to enter, view, or modify their encryption key.
- Import key to local registry - Allows users to import currently existing encryption key files to the local registry.
- Export key to file - Allows users to export the current encryption key to an encrypted text file.

Using an Encryption Server

Once a system is configured to use AES, it can be used as an Encryption server. For ease of use it is recommended to use only one Encryption Server per network, but multiple servers can be used if such a configuration is necessary.

AES in the UltraBac Log Files

To ensure that AES is being used during backup, check for the following information in the UltraBac log files: **This set is encrypted on the media.**

NOTE: The text in the log file will not be highlighted.

```
------------------------------------------------------------------------------


SET - Backup of UBDOC.

File: Backup_of_UBDOC.UB.

Agent: :WIN32\
Device: BackupPath0 (UltraBac Disk Storage Device (C:\TestBackupPath\))
This set is encrypted on the media


Software compression ratio: 2.51 to 1.

157 File (12 Folders) Totaling 909,362 Bytes Selected.
157 File (12 Folders) Totaling 909,362 Bytes Written.


Begin: 2009-12-11 13:27:12
End: 2009-12-11 13:27:12
Duration: 00:00:01 Rate: (888.00 KB/Sec   52.03 MB/Min   3.05 GB/Hour)
0 Errors and 0 Warnings


Media Volumes:  |No.|  Label  [Barcode/Media Pool]

                |1|  UltraBac Storage Media


------------------------------------------------------------------------------
```

Fig. 2 - AES in the UltraBac log files.

Restoring an AES Encrypted Backup

UltraBac will attempt to use the encryption key stored in the system registry. If the stored AES encryption key is the same as the key used to encrypt the backup, no additional steps will need to be necessary to restore the data. However, if the key does not match, it will be necessary to enter/import the key/phrase when prompted.

Fig. 3 - AES Decryption options during restore.

More Information:

See User Manual: Backup Set Basics
See User Manual: Restore Basics

UBQ000253: Configuring Microsoft SQL or MySQL for use with the UltraBac Database

UBQ ID Number: UBQ000253
Last Modified: 2009-12-08

Summary:

UltraBac can utilize either Microsoft SQL (Full or Express) or MySQL for the UltraBac Database functions. Each platform requires some changes from a "default" install options to ensure proper installation and operation of the UltraBac Database.

Details:

Microsoft SQL Server / SQL Server Express

NOTE: Installation of an UltraBac Database using Microsoft SQL Server / SQL Server Express will require a disk/partition with a minimum of 15GB of free space on the host.

The SQL Server "Authentication Mode" must be set to "Mixed Mode (Windows Authentication and SQL Server Authentication)" in order to set up and utilize the UltraBac Database.

Setting "Authentication Mode" During Installation:

1. Perform a default install of Microsoft SQL Server / SQL Server Express until the "Authentication Mode" screen.
2. Click "Mixed Mode (Windows Authentication and SQL Server Authentication)" radio button.
3. Enter/confirm the password for the "sa" account.

Fig. 1 - SQL Server Setup "Authentication Mode" dialog

4. Complete the installation with the default settings.

Changing "Authentication Mode" of an existing installation:

NOTE: The Microsoft SQL Server Management Studio / SQL Server Management Studio Express is required to alter the "Authentication Mode" of an existing installation.

1. Open the SQL Server Management Studio / SQL Server Management Studio Express.
2. Connect to the SQL Server\Instance to be configured.
3. Right-click on the SQL Server\Instance, then click "Properties."
4. Select the "Security" page.
5. Under "Server authentication" select the "SQL Server and Windows Authentication mode" radio button.

Fig. 2 - SQL Server Management Studio "Authentication Mode" dialog

6. Expand the "Security" folder, then expand "Logins."
7. Right-click on "sa" and click "Properties."
8. In the "General" page, set/confirm a password for the "sa" account.
9. Click on the "Status" page.
10. Under "Login:" select "Enabled" then click "OK."

Configuring SQL Server / SQL Server Express for remote UltraBac Database clients:

NOTE: UltraBac must be installed locally on the SQL Server / SQL Server Express host for remote UltraBac Database clients to work properly.

1. Open the SQL Server Configuration Manager.
2. Expand "SQL Server 2005 Network Configuration."
3. Click on "Protocols for [INSTANCENAME]."
4. Right-click "TCP/IP" and click "Enable."

Fig. 3 - SQL Server Configuration Manager "Protocols" dialog

5. Next, click on the "SQL Server 2005 Services."
6. Right-click on "SQL Server (INSTANCENAME)" then click "Restart."
7. Right-click on "SQL Server Browser" then click "Properties."
8. Click on the "Service" tab.
9. Change the "Start Mode" to "Automatic" then click "OK."

Fig. 4 - SQL Server Browser "Properties" dialog

10. Finally, right-click on "SQL Server Browser" then click "Start."

MySQL Server 5.1

NOTE: The "MySQL Connector/ODBC 5.1" software (a separate download from MySQL) must be installed on each system that will connect to the UltraBac Database.

Performing a new installation of MySQL Server:

1. Perform a "Typical" install of MySQL Server, check "Configure the MySQL Server now" then "Finish."
2. In the MySQL Server Instance Configuration Wizard, click "Next," select "Standard Configuration" then click "Next" again.
3. Click "Next" to accept the default Windows options.
4. Enter/confirm the password for the "root" account, and check the "Enable root access from remote machines" checkbox.
5. Press "Execute" then "Finish" to complete the MySQL Server Instance Configuration Wizard.

More Information:

See User Manual: UltraBac Database

UBQ000254: Enabling Streaming Backup Support in Microsoft Exchange Server 2007 SP1

UBQ ID Number: UBQ000254
Last Modified: 2010-07-26

Summary:

Installing Microsoft Exchange Server 2007 Service Pack 1 (SP1) disables remote streaming backup support, which prevents UltraBac from performing remote backups of Exchange data.

Details:

NOTE: Remote backup of Exchange 2007 SP1 data is not supported from a Windows 2008 backup host, or of a Windows 2008 server hosting Exchange 2007 SP1.

Due to a change introduced in Microsoft Exchange Server 2007 Service Pack 1 (and later), remote streaming backup functionality has been disabled by default. This prevents UltraBac from performing remote backups. To re-enable this remote streaming backup functionality, the following registry value must be entered:

HKEY_LOCAL_MACHINES\System\CurrentControlSet\Services\MSExchangeIS\Parameters System
  Name: **Enable Remote Streaming Backup**
  Type: **DWORD**
  Value: **0 = default behavior (remote backup disabled); 1 = remote backup enabled**

After entering the above registry key, the Microsoft Exchange Information Store service must be restarted to apply the change.

1. Go to "Start"/"Run," type in "cmd" then click "OK" to open a Command Prompt window.
2. At the Command Prompt, type "net stop msexchangeis" to stop the Microsoft Exchange Information Store.
3. Next, type "net start msexchangeis" to start the Microsoft Exchange Information Store.
4. Type "exit" to close the Command Prompt window.

UltraBac should now be able to perform remote streaming backups of Microsoft Exchange Server 2007 SP1 (and later) data.

Version: UltraBac v9.x
Copyright UltraBac Software 2010

UBQ000255: CRITICAL ISSUE - "Error positioning media for backup" error occurs with HP LTO Ultrium tape devices

UBQ ID Number: UBQ000255
Last Modified: 2010-10-04

Summary:

Hewlett-Packard LTO Ultrium devices using driver hplto.sys v1.0.6.2 (07/14/2010) experience "Error positioning media for backup" errors when attempting to write to tape. Until this issue is resolved in an updated HP driver release, there is a high risk for data loss. Downgrading the driver to hplto.sys v1.0.6.1 (05/14/2009) or earlier will fix this issue.

Details:

> NOTE: The HP StorageWorks Tape Drivers for Windows v3.2.0.0 package includes the working HP LTO v1.0.6.1 (5/14/2009) driver.

Hewlett-Packard LTO Ultrium tape device users utilizing hplto.sys v1.0.6.2 (07/14/2010) experience "Error positioning media for backup" errors when attempting to write to tape. Any backup using this driver version will automatically clear the media regardless of any append settings, and fail to write the backup. This affects all backup types: scheduled and ad-hoc. We strongly recommend the driver be replaced until a new driver without this issue becomes available, as there is a high risk for data loss when using this driver. Downgrading to an older version of hplto.sys, such as v1.0.6.1 (05/14/2009), resolves this issue with no impact to device functionality, usability or backup integrity. To downgrade the driver:

Windows 2008/Vista

1. Go to "Start"/"Run," type in "compmgmt.msc" then click "OK" to open the Computer Management console.
2. In the left pane, click "Device Manager" then in the right pane, expand the "Tape Devices" tree.
3. Right-click on the HP LTO Ultrium device to be downgraded, then click "Properties."
4. Select the "Driver" tab and confirm the current driver loaded is HP LTO v1.0.6.2 (07/14/2009), then click "Update Driver..."
5. Click "Browse my computer for driver software."
6. Click "Let me pick from a list of device drivers on my computer."
7. Click "Have Disk..." then click "Browse..."
8. Browse to the location of the older driver (such as v1.0.6.1), then click "Open."
9. Click "OK" to search the location for driver(s).
10. Select the driver, then click "Next" to begin installation of the selected driver.
11. Click "Close" to exit the "Update Driver Software" wizard.
12. Right-click on the updated HP LTO Ultrium device, then click "Properties."
13. Select the "Driver" tab and confirm the driver was properly updated to the older version.
14. If you have any other HP LTO Ultrium devices, repeat steps 3-13 to update the driver for those devices.

Windows 2003/XP

1. Go to "Start"/"Run," type in "compmgmt.msc" then click "OK" to open the Computer Management console.
2. In the left pane, click "Device Manager" then in the right pane, expand the "Tape Devices" tree.
3. Right-click on the HP LTO Ultrium device to be downgraded, then click "Properties."
4. Select the "Driver" tab and confirm the current driver loaded is HP LTO v1.0.6.2 (07/14/2009), then click "Update Driver..."
5. If a Windows Update prompt appears, click "No, not this time" then "Next."
6. Select the option "Install from a list or specific location (Advanced)" then click "Next."
7. Select the option "Don't search, I will choose the driver to install" then click "Next."
8. Click "Have Disk..." then click "Browse..."
9. Browse to the location of the older driver (such as v1.0.6.1), then click "Open."
10. Click "OK" to search the location for driver(s).
11. Select the driver, then click "Next" to begin installation of the selected driver.
12. Click "Finish" to exit the Hardware Update Wizard.
13. Right-click on the updated HP LTO Ultrium device, then click "Properties."
14. Select the "Driver" tab and confirm the driver was properly updated to the older version.
15. If you have any other HP LTO Ultrium devices, repeat steps 3-13 to update the driver for those devices.

UltraBac and the HP LTO Ultrium tape device(s) should now operate properly. Please contact UltraBac Technical Support should any issues arise during or after this driver update..

UBQ0000257: Exchange 2007 SCR / CCR Restores

UBQ ID Number: UBQ000257
Last Modified: 2011-03-03

Summary:

UltraBac has the ability to backup Exchange 2007 SCR and CCR environments. However the restore process is different than a standard Exchange 2007 Restore.

Details:

When dealing with an Exchange disaster that requires a recovery, in most cases you would rely on the High Availability of the SCR / CCR to initiate the recovery. If you are unable to recover from the other node, then you could use UltraBac to restore the active node, and then reseed the other Exchange server.

Restore:

1. Stop the clustered mailbox store.
2. Perform a standard Exchange restore:

> NOTE: Information on doing a standard Exchange Agent Restore
> See User Manual: Exchange Agent

3. Reseed the cluster

> NOTE: Information on how to reseed a CCR environment:
> **http://technet.microsoft.com/en-us/library/bb124706(EXCHG.80).aspx**
>
> Information on how to reseed a SCR environment:
> **http://technet.microsoft.com/en-us/library/bb738131(EXCHG.80).aspx**

UBQ000258: Adding iSCSI Support to UBDR Gold v6.0

UBQ ID Number: UBQ000258
Last Modified: 2011-03-03

Summary:

UltraBac Gold 6 is now based upon the newest Windows PE3, so the Windows Automated Installation Kit (AIK) for Windows 7 can be used to add iSCSI support to your UltraBac Gold v6.0 ISO file.

Details:

Download the Windows 7 AIK and install it on a Windows 7 OS
http://www.microsoft.com/downloads/en/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en

NOTE: If you are going to be adding iSCSI to a 32bit UBDR then you will need to be on a 32bit Windows 7 OS and if 64bit then you will need to be working from a 64bit Windows 7 OS
Or you can install the Windows 7 AIK on any supported OS but you will need to copy the iSCSI files from the correct Windows 7 OS architecture.

Create the registry files that will be needed

NOTE: Create a working directory that will be used throughout the process. For our example we created and use C:\UBDR6

Using a plain text editor (notepad.exe) and create the two registry files that will be needed.
File name: **iSCSIsoft.reg**
Copy and paste to text of document, and save in your working directory:
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\PE_Soft\Microsoft\Windows NT\CurrentVersion\Svchost]
"Godzilla"=hex(7):4d,00,53,00,69,00,53,00,43,00,53,00,49,00,00,00,00,00

[HKEY_LOCAL_MACHINE\PE_Soft\Microsoft\Windows NT\CurrentVersion\iSCSI]

[HKEY_LOCAL_MACHINE\PE_Soft\Microsoft\Windows NT\CurrentVersion\iSCSI\Discovery]
"AllowiSNSFirewallException"=dword:00000001

[HKEY_LOCAL_MACHINE\PE_Soft\Microsoft\Windows NT\CurrentVersion\iSCSI\Discovery\Authentication Cache]

[HKEY_LOCAL_MACHINE\PE_Soft\Microsoft\Windows NT\CurrentVersion\iSCSI\Discovery\Send Targets]

[HKEY_LOCAL_MACHINE\PE_Soft\Microsoft\Windows
NT\CurrentVersion\iSCSI\Discovery\Static Targets]

[HKEY_LOCAL_MACHINE\PE_Soft\Microsoft\Windows
NT\CurrentVersion\iSCSI\Discovery\Tunnel Address]

File name: **iSCSIsys.reg**
Copy and paste to text of document, and save in your working directory:
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Enum\Root\LEGACY_MSISCSI]
"NextInstance"=dword:00000001

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Enum\Root\LEGACY_MSISCSI\0000]
"Service"="MSiSCSI"
"Legacy"=dword:00000001
"ConfigFlags"=dword:00000000
"Class"="LegacyDriver"
"ClassGUID"="{8ECC055D-047F-11D1-A537-0000F8753ED1}"
"DeviceDesc"="@%SystemRoot%\\system32\\iscsidsc.dll,-5000"

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Enum\Root\LEGACY_MSISCSI\0000\Cont
rol]
"ActiveService"="MSiSCSI"

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Enum\Root\ISCSIPRT]

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Enum\Root\ISCSIPRT\0000]
"ClassGUID"="{4d36e97b-e325-11ce-bfc1-08002be10318}"
"Class"="SCSIAdapter"
"HardwareID"=hex(7):52,00,4f,00,4f,00,54,00,5c,00,69,00,53,00,43,00,53,00,49,\
  00,50,00,72,00,74,00,00,00,00,00
"ConfigFlags"=dword:00000000
"Driver"="{4d36e97b-e325-11ce-bfc1-08002be10318}\\0000"
"Mfg"="@iscsi.inf,%msft%;Microsoft"
"Service"="iScsiPrt"
"DeviceDesc"="@iscsi.inf,%iscsiprt%;Microsoft iSCSI Initiator"
"Capabilities"=dword:00000000

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Enum\Root\ISCSIPRT\0000\Device
Parameters]

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Enum\Root\ISCSIPRT\0000\Device
Parameters\StorPort]

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Enum\Root\ISCSIPRT\0000\LogConf]

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Enum\Root\ISCSIPRT\0000\Control]
"ActiveService"="iScsiPrt"

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Services\iScsiPrt]
"DisplayName"="iScsiPort Driver"
"ImagePath"=hex(2):73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,44,00,\
  52,00,49,00,56,00,45,00,52,00,53,00,5c,00,6d,00,73,00,69,00,73,00,63,00,73,\
  00,69,00,2e,00,73,00,79,00,73,00,00,00
"ErrorControl"=dword:00000001

```
"Start"=dword:00000003
"Type"=dword:00000001

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Services\iScsiPrt\Parameters]
"BusType"=dword:00000009

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Services\iScsiPrt\Enum]
"0"="Root\\ISCSIPRT\\0000"
"Count"=dword:00000001
"NextInstance"=dword:00000001

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Services\MSiSCSI]
"DisplayName"="@%SystemRoot%\\system32\\iscsidsc.dll,-5000"
"Group"="iSCSI"
"ImagePath"=hex(2):25,00,73,00,79,00,73,00,74,00,65,00,6d,00,72,00,6f,00,6f,00,\
  74,00,25,00,5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,73,\
  00,76,00,63,00,68,00,6f,00,73,00,74,00,2e,00,65,00,78,00,65,00,20,00,2d,00,\
  6b,00,20,00,47,00,6f,00,64,00,7a,00,69,00,6c,00,6c,00,61,00,00,00
"Description"="@%SystemRoot%\\system32\\iscsidsc.dll,-5001"
"ObjectName"="LocalSystem"
"ErrorControl"=dword:00000001
"Start"=dword:00000003
"Type"=dword:00000020
"ServiceSidType"=dword:00000001
"RequiredPrivileges"=hex(7):53,00,65,00,41,00,75,00,64,00,69,00,74,00,50,00,72,\
  00,69,00,76,00,69,00,6c,00,65,00,67,00,65,00,00,00,53,00,65,00,43,00,68,00,\
  61,00,6e,00,67,00,65,00,4e,00,6f,00,74,00,69,00,66,00,79,00,50,00,72,00,69,\
  00,76,00,69,00,6c,00,65,00,67,00,65,00,00,00,53,00,65,00,43,00,72,00,65,00,\
  61,00,74,00,65,00,47,00,6c,00,6f,00,62,00,61,00,6c,00,50,00,72,00,69,00,76,\
  00,69,00,6c,00,65,00,67,00,65,00,00,00,53,00,65,00,43,00,72,00,65,00,61,00,\
  74,00,65,00,50,00,65,00,72,00,6d,00,61,00,6e,00,65,00,6e,00,74,00,50,00,72,\
  00,69,00,76,00,69,00,6c,00,65,00,67,00,65,00,00,00,53,00,65,00,49,00,6d,00,\
  70,00,65,00,72,00,73,00,6f,00,6e,00,61,00,74,00,65,00,50,00,72,00,69,00,76,\
  00,69,00,6c,00,65,00,67,00,65,00,00,00,53,00,65,00,54,00,63,00,62,00,50,00,\
  72,00,69,00,76,00,69,00,6c,00,65,00,67,00,65,00,00,00,00,00
"FailureActionsOnNonCrashFailures"=dword:00000001
"FailureActions"=hex:50,46,00,00,01,00,00,00,01,00,00,00,03,00,00,00,14,00,00,\
  00,01,00,00,00,c0,d4,01,00,01,00,00,00,e0,93,04,00,00,00,00,00,00,00,00,00
"RebootMessage"="iSCSI Failure"
"FailureCommand"=""

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Services\MSiSCSI\Parameters]
"ServiceDll"=hex(2):25,00,73,00,79,00,73,00,74,00,65,00,6d,00,72,00,6f,00,6f,\
  00,74,00,25,00,5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,\
  69,00,73,00,63,00,73,00,69,00,65,00,78,00,65,00,2e,00,64,00,6c,00,6c,00,00,\
  00
"ServiceDllUnloadOnStop"=dword:00000001

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Services\MSiSCSI\Enum]
"0"="Root\\LEGACY_MSISCSI\\0000"
"Count"=dword:00000001
"NextInstance"=dword:00000001

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}]
"LegacyAdapterDetection"=dword:00000000
```

328

```
"Class"="SCSIAdapter"
"ClassDesc"="@%SystemRoot%\\System32\\SysClass.Dll,-3005"
@="@%SystemRoot%\\System32\\SysClass.Dll,-3005"
"IconPath"=hex(7):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,00,\
  74,00,25,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,73,\
  00,65,00,74,00,75,00,70,00,61,00,70,00,69,00,2e,00,64,00,6c,00,6c,00,2c,00,\
  2d,00,31,00,30,00,00,00,00,00
"Installer32"="SysClass.Dll,ScsiClassInstaller"

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000]
"InfPath"="iscsi.inf"
"InfSection"="iScsiPort_Install_Control"
"ProviderName"="Microsoft"
"DriverDateData"=hex:00,80,8c,a3,c5,94,c6,01
"DriverDate"="6-21-2006"
"DriverVersion"="6.1.7600.16385"
"MatchingDeviceId"="root\\iscsiprt"
"DriverDesc"="Microsoft iSCSI Initiator"
"EnumPropPages32"="iscsipp.dll,iSCSIPropPageProvider"

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters]
"DelayBetweenReconnect"=dword:00000005
"EnableNOPOut"=dword:00000000
"ErrorRecoveryLevel"=dword:00000002
"FirstBurstLength"=dword:00010000
"ImmediateData"=dword:00000001
"InitialR2T"=dword:00000000
"IPSecConfigTimeout"=dword:0000003c
"LinkDownTime"=dword:0000000f
"MaxBurstLength"=dword:00040000
"MaxConnectionRetries"=dword:ffffffff
"MaxPendingRequests"=dword:000000ff
"MaxRecvDataSegmentLength"=dword:00010000
"MaxRequestHoldTime"=dword:0000003c
"MaxTransferLength"=dword:00040000
"NetworkReadyRetryCount"=dword:0000000a
"PortalRetryCount"=dword:00000005
"SrbTimeoutDelta"=dword:0000000f
"TCPConnectTime"=dword:0000000f
"TCPDisconnectTime"=dword:0000000f
"WMIRequestTimeout"=dword:0000001e

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\PersistentTargets]
@=""

[HKEY_LOCAL_MACHINE\PE_Sys\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\Properties]
"DeviceType"=dword:00000004
"DeviceCharacteristics"=dword:00000100
"Security"=hex:01,00,04,90,00,00,00,00,00,00,00,00,00,00,00,00,14,00,00,00,02,\
  00,34,00,02,00,00,00,00,00,14,00,ff,01,1f,10,01,01,00,00,00,00,00,05,12,00,\
  00,00,00,00,18,00,ff,01,1f,10,01,02,00,00,00,00,00,05,20,00,00,00,20,02,00,\
  00
```

Add the iSCSI support to the UBDR Gold v6.0 ISO

1. Create an ISO sub-directory in your working directory to run the operation in
   (C:\UBDR6\ISO)

2. Using an ISO editing application (such as UltraISO) extract the UBDR ISO to your ISO
   directory (C:\UBDR6\ISO)
3. Create another empty directory that will be used for mounting the boot.wim file from the
   UBDR ISO (C:UBDR6\mount):

   mkdir "C:\UBDR6\mount"
4. Mount the boot.wim file to the mount directory:
   "C:\Program Files\Windows AIK\Tools\Servicing\Dism.exe" /Mount-Wim
   /WimFile:"C:\UBDR6\ISO\SOURCES\boot.wim" /index:1 /MountDir:"C:\UBDR6\mount"
5. Copy the files from the OS to the mount directory :
   copy "C:\Windows\System32\iscsicli.exe"
   "C:\UBDR6\mount\Windows\System32\iscsicli.exe"
   copy "C:\Windows\System32\iscsicpl.dll"
   "C:\UBDR6\mount\Windows\System32\iscsicpl.dll"
   copy "C:\Windows\System32\iscsicpl.exe"
   "C:\UBDR6\mount\Windows\System32\iscsicpl.exe"
   copy "C:\Windows\System32\iscsidsc.dll"
   "C:\UBDR6\mount\Windows\System32\iscsidsc.dll"
   copy "C:\Windows\System32\iscsied.dll" "C:\UBDR6\mount\Windows\System32\iscsied.dll"
   copy "C:\Windows\System32\iscsiexe.dll"
   "C:\UBDR6\mount\Windows\System32\iscsiexe.dll"
   copy "C:\Windows\System32\iscsium.dll"
   "C:\UBDR6\mount\Windows\System32\iscsium.dll"
   copy "C:\Windows\System32\iscsiwmi.dll"
   "C:\UBDR6\mount\Windows\System32\iscsiwmi.dll"
   copy "C:\Windows\System32\Drivers\msiscsi.sys"
   "C:\UBDR6\mount\Windows\System32\Drivers\msiscsi.sys"
   copy "C:\Windows\System32\en-US\iscsicli.exe.mui"
   "C:\UBDR6\mount\Windows\System32\en-US\iscsicli.exe.mui"
   copy "C:\Windows\System32\en-US\iscsicpl.dll.mui"
   "C:\UBDR6\mount\Windows\System32\en-US\iscsicpl.dll.mui"
   copy "C:\Windows\System32\en-US\iscsicpl.exe.mui"
   "C:\UBDR6\mount\Windows\System32\en-US\iscsicpl.exe.mui"
   copy "C:\Windows\System32\en-US\iscsiexe.dll.mui"
   "C:\UBDR6\mount\Windows\System32\en-US\iscsiexe.dll.mui"
6. Load the registry hive and add registry entries:
   reg load HKLM\PE_Soft C:\UBDR6\mount\Windows\System32\config\SOFTWARE
   reg import C:\UBDR6\iSCSIsoft.reg
   reg unload HKLM\PE_Soft
   reg load HKLM\PE_Sys C:\UBDR6\mount\Windows\System32\config\SYSTEM
   reg import C:\UBDR6\iSCSIsys.reg
   reg unload HKLM\PE_Sys
7. Commit changes to your boot.wim and unmount:
   "C:\Program Files\Windows AIK\Tools\Servicing\Dism.exe" /Unmount-Wim
   /MountDir:"C:\UBDR6\mount" /Commit
8. Using your ISO editing application, copy the boot.wim file from the ISO\sources in your
   working directory back into your ISO image Sources directory.
9. Save your updated ISO.

UBQ000259: Single Mailbox Restore with Exchange 2010 Recovery DB

UBQ ID Number: UBQ000259
Last Modified: 2011-03-03

Summary:

This document explains how to restore a single mailbox using the Exchange Recovery Database.

NOTE: This method can only be used to recover the mailbox database(s) and not the public database.

Details:

First Restore the Exchange database as a flat file.

1. Load the Exchange Backup
2. Choose the mailbox database and log files and click "Action >Restore"
3. Check "Restore Files to Non-Exchange Folder"
4. Type in or browse to the target location.
5. Click "Next"
6. Click "Restore"

Once the recovery is complete, the database (EDB file) and transaction logs (LOG files) will reside in the path specified.

7. Add the restored database to the Exchange mailbox server as a Recovery Database. This is performed using the Exchange Management Shell (EMS).
8. Run the following command to create a Recovery Database

   New-MailboxDatabase -Recovery -Name RESTORE1 -Server EXA2010 –EdbFilePath C:\restore\Mailbox Database 1882717321.edb" -LogFolderPath "C:\Restore"
A new Recovery Database titled RESTORE1 will be created on server EXA2010 using the restored database and logs in C:\Restore.

Once the command is run, the Recovery Database will appear in the Exchange Management Console (EMC).

NOTE: The Recovery Database must be brought into a clean shutdown state before it can be mounted.

To bring the database into a clean shutdown state, use *ESEUTIL /R* to perform a recovery of the database.

NOTE: If Exchange is unable to perform a successful recovery, a full list of options can be

found at the following link:
http://technet.microsoft.com/en-us/library/bb125218.aspx

Example #1 : Recovering a mailbox, overwriting the existing mailbox

This example restores a mailbox for user UltraBac User1, overwriting the existing mailbox:
In the Exchange Management Shell type:
Restore-Mailbox -ID 'UltraBac User1' -RecoveryDatabase RESTORE1

Example #2 : Restoring a mailbox, to another users mailbox

This example restores 'UltraBac User1' mailbox content into another user's mailbox:
Restore-Mailbox -ID 'UltraBac User1' -RecoveryDatabase RESTORE1

.

UBQ000260: HP StorageWorks D2D Backup Systems Support

UBQ ID Number: UBQ000260
Last Modified: 2011-05-12

Summary:

After firmware update 101.748 on HP StorageWorks D2D Backup Systems line of devices, the new version of firmware does not conform completely for all Microsoft API calls, so file enumeration is affected. HP is working on a solution for this issue; a workaround to enable UltraBac to continue backing up to these backup devices is detailed.

Details:

This issue effects all HP 2nd Generation StorageWorks D2D Backup Systems, and all 1st StorageWorks D2D Backup Systems running firmware newer then 101.748.
When writing to the HP StorageWorks D2D Backup System, you will get an error from UltraBac about positioning device.
To fix this you will need to follow these steps:

1. Upgrade to UltraBac version 9.2.1
2. Create a backup path pointing to the D2D device if there is not one already created
3. Open up your registry editor and go to: HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac\DeviceInfo\Win32 File Device
4. Create a new DWORD value of: BackupPath*X*EnableHPCIFSCompatibility

   X = the backup path # you need to enable it on
   Example: for backup path **2** you would put the value as
   BackupPath**2**EnableHPCIFSCompatibility

5. For the Value enter: 1
6. You will need to create this registry key for each backup path that points to the D2D device.

UBQ000261: Additional File and Driver details

UBQ ID Number: UBQ000261
Last Modified: 2011-05-26

Summary:

Due to the complexity of the files and drivers UltraBac uses to perform its tasks, some files require elevated privileges, some third party / interop files used may not contain file information/properties, and some files perform custom actions. This knowledge base article provides details of these files.

Details:

Files requiring elevated privileges

The following files require elevated privileges in order to perform their functions:
    UBRegDll.exe
    UBUnRegDll.exe
    licensemaint.exe
    setup.exe
    ubms.exe
    ubui.exe

Third Party / Interop files that may not contain file information / properties or valid authenticode signatures

Third party files from CodeJock Xtreme Toolkit:
    ToolkitPro.ResourceFr.dll
    ToolkitPro.ResourceJa.dll

Third party drivers provided by VMware:
    buslogic.sys
    glib-2.0.dll
    gobject-2.0.dll
    gthread-2.0.dll
    gvmomi.dll
    libcurl.dll
    libeay32.dll
    liblber.dll
    libldap.dll
    libldap_r.dll
    libxml2.dll
    mssctlbm.dll
    mssitlbm.dll
    ssleay32.dll
    symmpi.sys
    types.dll
    UBVimServiceStub.XmlSerializers.dll
    zlib1.dll

Third party drivers provided by Microsoft
      psexec.exe
      robocopy.exe

UltraBac generated Interop files:
      UBSharePointLibDMBACKUPLib.dll
      UBSharePointLibWrapper.dll
      UBSharePointLibWrapper2007.dll
      UBVimServiceStub.dll
      UBVMwareUtilityWrapper.dll
      UBxmlinst.dll

Files performing custom actions:

DIFxApp.dll:
- Processes driver packages
- Cleans up on successful installation:

WixUIXixca:

- Validates path
- Prints EULA

DIFxAppA.dll:

- Installs driver packages
- Uninstalls driver packages
- Rolls back installation upon failed installation

Files that self register/unregister in the registry:
      msxml6.dll
      ubxml.dll
      ubxmlinst.dll
      upgrade.dll
      uxagent.dll
      win32fileagent.dll
      ubimage.dll
      ubdisk.dll
      ubcd.dll
      ubnttape.dll
      ubremote.dll
      ubsftp.dll
      ubsharepointagent.dll
      ubslotbasedlibrary.dll
      ubtivoli.dll
      ubvcbagent.dll
      imageagent.dll
      licensemgr.dll
      atlcontrols.dll
      mysqlagent.dll
      sqlagent.dll

exchangent.dll
oracleagent.dll
mailbox.dll
sysstate.dll

UBQ000263: Exchange Flat-File Restore if Original Exchange Server Offline

UBQ ID Number: UBQ000263
Last Modified: 2011-08-23

Summary:

If the original exchange server no longer exists, then flat file exchange restores will fail with a message stating it cannot connect with the exchange server error 10061. This problem affects all versions of Exchange. This knowledge base article provides a work-around for this situation.

Details:

When UltraBac does a flat file exchange restore, it tries to communicate with the original exchange server and then it performs the restore. If the original exchange server is not on-line, then the following steps will allow for the flat-file restore to another server.

On the server where you want to initiate the restore:

1. Open UltraBac and go to "Manage"/"General"/"User Options" and place a checkmark next to the option for Advanced Options.
2. Close UltraBac.
3. Install the Exchange Management tools from the Exchange installation Media.
4. Open Windows Explorer and go to "C:\Windows\System32\drivers\etc"
5. Open the file "hosts" with notepad.
6. Add an entry with the IP address of the computer you are on and the name of the original exchange server.
7. Save the hosts file.
8. UltraBac, load the backup and perform the restore.

UBQ000264: Writing to CIFS Backup Path

UBQ ID Number: UBQ000264
Last Modified: 2011-08-23

Summary:

Some CIFS storage devices do not conform completely for all Microsoft API calls, so file enumeration is affected. To enable a backup path to a CIFS storage device that has this issue, the following workaround will enable UltraBac to back up to these backup devices.

Details:

When writing to a CIFS storage device that does not conform completely for all Microsoft API calls, you will get an error from UltraBac about positioning device.

To fix this you will need to follow these steps:

1. Create a backup path pointing to the CIFS storage device if there is not one already created, "Manage/Storage Devices/Backup path".
2. Open up your registry editor and go to: HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac\DeviceInfo\Win32 File Device
3. Create a new DWORD value of: BackupPath*X*EnableHPCIFSCompatibility

   X = the backup path # you need to enable it on
   Example: for backup path **2** you would put the value as
   BackupPath**2**EnableHPCIFSCompatibility

5. For the Value enter: 1

NOTE: This process will need to be completed for each backup path that requires this functionality.

UBQ000265: Using the Exchange 2007 Recovery Storage Group

UBQ ID Number: UBQ000265
Last Modified: 2012-08-03

Summary:

When performing an Exchange restore, you have the option to restore to a Recovery Storage Group. This is a feature inside of Exchange that allows you to recover individual mailboxes.

Details:

Creating the Recovery Storage Group

The Recovery Storage Group should be created through the Database Recovery Management tool in the Toolbox, which is located in the Exchange Management Console.

1. Open the Exchange Management Console. Click on the "Toolbox," then under Disaster recovery tools click on "Database Recovery Management."

Fig. 1 - Exchange Management Console.

2. Type the name of your Exchange server as well as the Domain Controller name, then click "Next" at the bottom of the screen.

Fig. 2 - Exchange Troubleshooting Assistant.

3. From the Tasks options, choose Manage Recovery Storage Group and then click on "Create a recovery storage group."

Fig. 3 - Options to create Recovery Storage Group.

4. Select the Storage Group that you want to restore from and click "Next."

Fig. 4 - Select database in which to create the Recovery Storage Group.

5. Choose the location to create the Recovery Storage Group. **Please note:** We strongly recommend users keep everything in the same location.

Fig 5. - Enter name of the new Recovery Storage Group.

6. Finish the Recovery Storage Group creation.

Fig. 6 - Successful creation of the Recovery Storage Group.

For more information on using a Recovery Storage Group, please visit the Microsoft Web site: Microsoft Technet: Recovery Storage Groups.

Non-VSS Exchange Backup Restore to a Recovery Storage Group

1. Create the Recovery Storage Group.
2. Verify the database that you are trying to restore is mounted.
3. Perform a standard Exchange Restore. For more information please visit http://www.ultrabac.com/kb/exchange_2k_agent.htm.
4. Mount the Recovery Storage Group.

VSS Exchange Backup Restore to a Recovery Storage Group

Microsoft Exchange backup and restore API's do not support restoring to a Recovery Storage Group. Using UltraBac, you can manually restore the database and perform a soft recovery to a Recovery Storage Group.

1. Create a Recovery Storage Group.
2. Perform a flat file restore of the Exchange database to the location you created the Recovery Storage Group. For more information please visit http://www.ultrabac.com/kb/exchange_2k_agent.htm.
3. Open a command line and go to the location where you restored the files.
4. Type: eseutil /r e01 /d <path to recovery storage group>. See an example in Figure 7.

Fig. 7 - Example of a soft recovery via command line.

5. Mount the recovery storage group.

More Information:
For more information on Exchange Volume Shadow Copy (VSS) support, please visit http://technet.microsoft.com/en-us/library/dd233256%28v=exchg.80%29.aspx.

Index