UltraBac Documentation

ULTRABAC

Backup and Disaster Recovery Software

ULTRABAC SOFTWARE

Administrator Guide v10

UltraBac Administrator Guide v10.0

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.

Copyright Notice

© 2015 UltraBac Software, Inc. All rights reserved.
Any documentation that is made available by UltraBac Software is the copyrighted work of said corporation and is owned by UltraBac Software.
NO WARRANTY. The technical documentation is being delivered to you AS-IS, and UltraBac Software makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. UltraBac Software reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of UltraBac Software, 15015 Main Street, Suite 200, Bellevue, WA 98007.

Trademarks

UltraBac Software, UltraBac, UBDR Gold, UltraCopy, Continuous Image Protection (CIP), Backup and Disaster Recovery Software for Business, and UltraBac Software logos are trademarks of UltraBac Software. Other brand and product names mentioned herein may be trademarked and are property of their respective companies.

Table Of Contents

UltraBac Administrator Guide 1
Introduction 1
Minimum System Requirements 1
Conventions Used In This Manual 3
Setup and Configuration 5
Installing UltraBac 5
UltraBac Preferences 12
UltraBac Licensing 31
UltraBac Management Console 35
Storage Device Manager 47
UltraCopy 61
Backup Migration 67
Media Library Controls 78
UltraBac Database 90
Backup and Restore Basics 95
Backup Set Basics 95
Scheduled Backup Basics 99
Scheduled Backup Options 109
Viewing Scheduled Backups 119
Before and After Jobs 122
Restore Basics 124
Command Line Functionality 131
UltraBac Agents 134
Disaster Recovery 135
Image Disaster Recovery Agent 135
UBDR - UltraBac Disaster Recovery 144
Writing an Image Backup to VHD File 185
Writing an Image Backup to VMDK File 188
Incremental/Differential Backups - Image Agent 194
Static Mirror Image Backup 199
File-by-File 201
File-by-File Agent 201
Incremental/Differential Backups - File-by-File Agent 213
Locked File Backup Agent 217
UltraBac System State/Active Directory Restore Windows 2003 Server 219
UltraBac System State/Active Directory Restore Windows 2008/2008 R2 Server 224
UltraBac System State/Active Directory Restore Windows 2012/2012 R2 Server 233
vSphere Agent 241
Hyper-V Agent 252
SQL Agent 260
Exchange Agent 269
Ux Agent 277
Ux Agent (File-by-File) 277
Ux Image Agent 305
Centralized Management 348
UltraBac Media Builder 356
Knowledge Base 365
UBQ000001: Command Line Backup/Restore 365
Summary: 365
Details: 365
UBQ000024: What is an Image Backup? 370
Summary: 370
Details: 370

UBQ000041: Selecting a Storage Device 371
Summary: 371
Details: 371
UBQ000049: Defining a Disk (Backup Path) Storage Device 373
Summary: 373
Details: 373
UBQ000060: Static Mirror Image Recovery 377
Summary: 377
Details: 377
UBQ000069: Troubleshooting SMTP 378
Summary: 378
Details: 378
UBQ000080: Incremental/Differential Backups and the Archive Bit 380
Summary: 380
Details: 380
UBQ000091: Solving SCSI/CRC Errors 386
Summary: 386
Details: 386
UBQ000092: Solving Typical SCSI Problems 389
Summary: 389
Details: 390
UBQ000112: Troubleshooting Permissions Issues 392
Summary: 392
Details: 392
UBQ000150: Installing the Media Library Driver (Autoloader) in Windows 2008 / 2008 R2 394
Summary: 394
Details: 394
UBQ000157: Configuring the UltraBac Centralized Reporting Console 399
Summary: 399
Details: 399
UBQ000158: Copying Restore Logs in UBDR 404
Summary: 404
Details: 404
UBQ000162: Non-UltraBac Specific Registry Keys 406
Summary: 406
Details: 406
UBQ000194: Configuring the (Legacy) UX Agent on a Solaris Client 407
Summary: 407
Details: 407
UBQ000195: Medium Changer Driver Unloading 409
Summary: 409
Details: 409
UBQ000198: Backup Account Permissions 412
Summary: 412
Details: 412
UBQ000202: UltraBac in a Workgroup 414
Summary: 414
Details: 414
UBQ000205: Microsoft SQL "WITH MOVE" Option 416
Summary: 416
Details: 416
UBQ000210: UltraBac Backup Output Files 419
Summary: 419
Details: 419
UBQ000214: Description of License Components 420
Summary: 420

Details: 420
UBQ000229: Unattended Installation of UltraBac 421
Summary: 421
Details: 421
UBQ000230: UBDR Gold Advanced Tools and Utilities 423
Summary: 423
Details: 423
UBQ000234: Common Backup Errors Explained 425
Summary: 425
Details: 425
UBQ000236: UBDR Scripted Restore 427
Summary: 427
Details: 427
UBQ000242: Removing Media Pools 432
Summary: 432
Details: 432
UBQ000250: Exchange 2007 Support 434
Summary: 434
Details: 434
UBQ000251: Encrypting Backup Data with AES in UltraBac 9.x 436
Summary: 436
Details: 436
UBQ000253: Configuring Microsoft SQL or MySQL for use with the UltraBac Database 440
Summary: 440
Details: 440
UBQ000254: Enabling Streaming Backup Support in Microsoft Exchange Server 2007 SP1 448
Summary: 448
Details: 448
UBQ000255: CRITICAL ISSUE - "Error positioning media for backup" error occurs with HP LTO Ultrium tape devices 449
Summary: 449
Details: 449
UBQ0000257: Exchange 2007 SCR / CCR Restores 451
Summary: 451
Details: 451
UBQ000258: Adding additional packages to UBDR 452
Summary: 452
Details: 452
UBQ000259: Single Mailbox Restore with Exchange 2010 Recovery DB 462
Summary: 462
Details: 462
UBQ000260: HP StorageWorks D2D Backup Systems Support 464
Summary: 464
Details: 464
UBQ000261: Additional File and Driver details 465
Summary: 465
Details: 465
UBQ000263: Exchange Flat-File Restore if Original Exchange Server Offline 468
Summary: 468
Details: 468
UBQ000264: Writing to CIFS Backup Path 469
Summary: 469
Details: 469
UBQ000265: Using the Exchange 2007 Recovery Storage Group 470
Summary: 470
Details: 470

UBQ000266: 1450 Errors During Backup 476
Summary: 476
Details: 476
UBQ000267: 2008 / 2008R2 Core Installation and Backups 477
Summary: 477
Detail: 477
UBQ000268: Additional steps for UBDR restore of Windows 7, 2008 R2, and newer Operating Systems. 479
Summary: 479
Details: 479
UBQ000269: Error 0076: UltraBac Exchange Agent does not support Circular Logging 481
Summary: 481
Detail: 481
UBQ000271: Managed Machines List 482
Summary: 482
Details: 482
UBQ000272: Upgrading UltraBac from Older Versions 485
Summary: 485
Detail: 485
UBQ000273: vSphere Agent CBT troubleshooting 487
Summary: 487
Details: 487
UBQ000274: How to Fix Errors Caused by CBT Tracking 491
Summary: 491
Details: 491
UBQ000275: Single Mailbox Restore with Exchange 2013 Recovery DB 495
Summary: 495
Details: 495
Usefull Commands: 496
UBQ000276: How to Boot a Windows Server Domain Controller into Directory Services Restore/Repair Mode 498
Summary: 498
Details: 498
UBQ000277: Accessing the Advanced Boot Options Menu in Windows Server 2012 500
Summary: 500
Details: 500
UBQ000278: Configuring UltraBac Deduplication Server 504
Minimum System Requirements: 504
Configuring deduplication server: 504
Index 509

UltraBac Administrator Guide

Introduction

Minimum System Requirements

OS (running the latest service pack and hotfixes):

- Windows Vista (Business and Ultimate)
- Windows 7 (Professional, Enterprise, and Ultimate)
- Windows 8 /8.1 (Core, Pro, and Enterprise)
- Windows 10 (Home, Pro, Enterprise, and Education)
- Windows Server 2003 / 2003 R2
- Windows Server 2008 / 2008 R2
- Windows Server 2012 / 2012 R2

> NOTE: Windows 2000 (Professional and Server) and Windows XP Professional are no longer supported beginning with UltraBac version 9.3.5.

Updates (depending upon OS):

- .NET 2.0
- .NET 3.5.1
- .NET 4.5

> NOTE: The UltraBac installer will automatically launch the ".Net 4.5" installer if ".Net 4.5" does not already reside on the system and an agent being installed requires it.
>
> On older hardware or within virtual machines, the ".Net 4.5" installer is very CPU intensive. For these systems it is recommended that ".Net 4.5" be manually installed PRIOR to the installation of UltraBac.
>
> The ".NET 4.5" installer can be found within the downloaded .zip file in the "ubinstall\dotnet" folder. Launch the "dotnetfx45_full_setup.exe" to manually install ".Net 4.5."

Screen:

- A minimum screen display of 1024x768 is required as lower resolutions will be unable to display some agent dialog boxes in their entirety.
- A 256 color display is required and 65,536 colors are recommended

Memory:

- Windows Server 2003 / 2003 R2 / 2008 / 2008 R2 / 2012 /2012 R2 / Vista / Windows 7 / 8 / 8.1 / 10 – 2 GB or greater recommended.
- UBDR Gold – 2 GB or greater recommended.

Hard Disk:

- Full install of OS architecture - 1 GB required. Doubled if copying additional binaries for alternate OS architecture (x86 or amd64)
- UltraBac database requires 20GB of free hard disk space, 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 Section Name	**"Bold Type"**
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	"Underlined"
Convention:	"Underlined File Path"
Example:	"C:\UltraBac\"
Sample:	By default, UltraBac installs into the "C:\UltraBac\" directory
Keyboard Shortcut	"First Alpha Character Underlined"
Convention:	"New"
Example:	A keyboard shortcut for creating a new backup is executed by pressing and holding the Ctrl key while pressing the "n"
Sample:	key. "Ctrl" + "n"
Keyboard Shortcut	"First Alpha Character Underlined"
Convention:	"New"
Example:	A keyboard shortcut for creating a new backup is executed by pressing and holding the Ctrl key while pressing the "n"
Sample:	key. "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, copying additional binaries, should be performed on the backup host. Then any necessary agents (or a recommended 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 media libraries.

NOTE: During both the installation and uninstallation of UltraBac the program 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

NOTE: The UltraBac installer will automatically launch the ".Net 4.5" installer, for operating systems other than Server 2003, if ".Net 4.5" does not already reside on the system and an agent being installed requires it. For Server 2003, UltraBac will install ".Net 4.0."

On older hardware or within virtual machines, the ".Net 4.5" installer is very CPU intensive. For these systems it is recommended that ".Net 4.5" be manually installed PRIOR to the installation of UltraBac.

The ".NET 4.5" installer can be found within the downloaded .zip file in the "ubinstall\dotnet" folder. Launch the "dotnetfx45_full_setup.exe" to manually install ".Net 4.5."

The ".NET 4.0" installer can be found within the downloaded .zip file in the "ubinstall\dotnet" folder. Launch the "dotNetFx40_Full_x86_x64.exe" to manually install ".Net 4.0."

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.

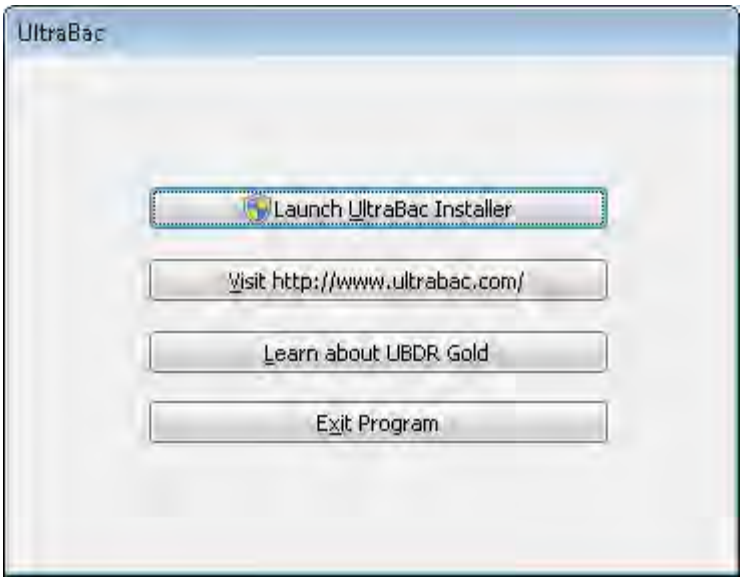


Fig. 1 - Launch screen for the UltraBac Installer.

3. Click "Launch UltraBac Installer."
4. Check box to copy binary files for optional CPU architecture. Necessary to deploy UltraBac in a mixed architecture environment and to build UBDR for additional architecture.

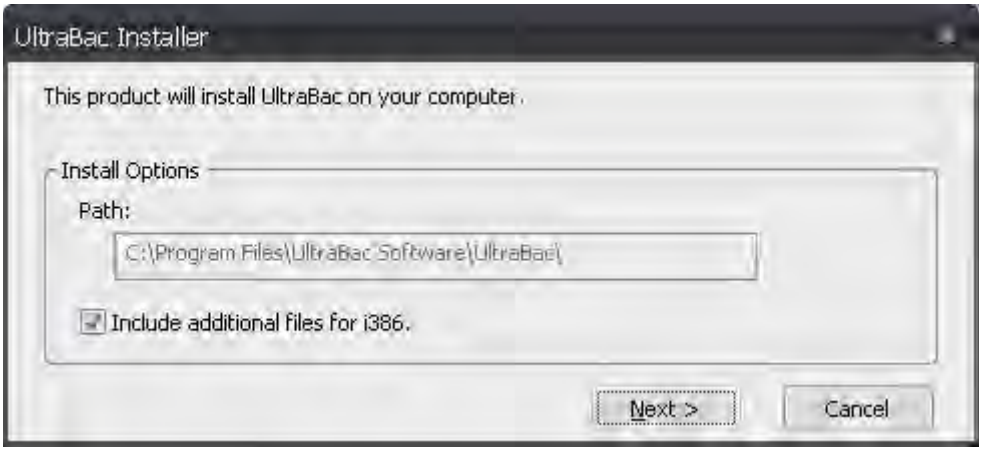


Fig. 2 - Copying additional binaries.

3. Click "Next" in the "UltraBac Installer" screen.
4. Read the UltraBac Licensing Agreement text, and check "I accept the terms of the licensing agreement."
5. Click "Next" to continue.

Installing UltraBac on the Backup Host

1. 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 service 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:

UBQ000198: Backup Account Permissions

More information:

UBQ000112: Troubleshooting Permissions Issues
UBQ000202: UltraBac in a Workgroup

2. Type the account name to be used for backup in the "Account Information" \ "User:" field.



Fig. 3 - Entering account information into UltraBac.

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

Checking "Set as default for all connections" will instruct UltraBac to use the specified account to run all scheduled backups as this user. Ad hoc backup jobs and restores are run as the currently logged on user.

Installing UltraBac on a Remote Client

After the initial installation completes, the UltraBac installer will give the option to launch the UltraBac Management Console or the Remote Installer. The Remote Installer can also be launched from the Windows Start menu or from the Management Console via "Tools"/"Deploy"/"Install UltraBac."

To install UltraBac on a client using the Remote Installer:

1. Click "Start"/"Programs"/"UltraBac"/"UltraBac Installer."
2. Click "Next," ignoring "Install Options."
3. Accept the EULA by checking "I accept the terms of the licensing agreement."
4. Select "Install to machine(s)" and click "Next."

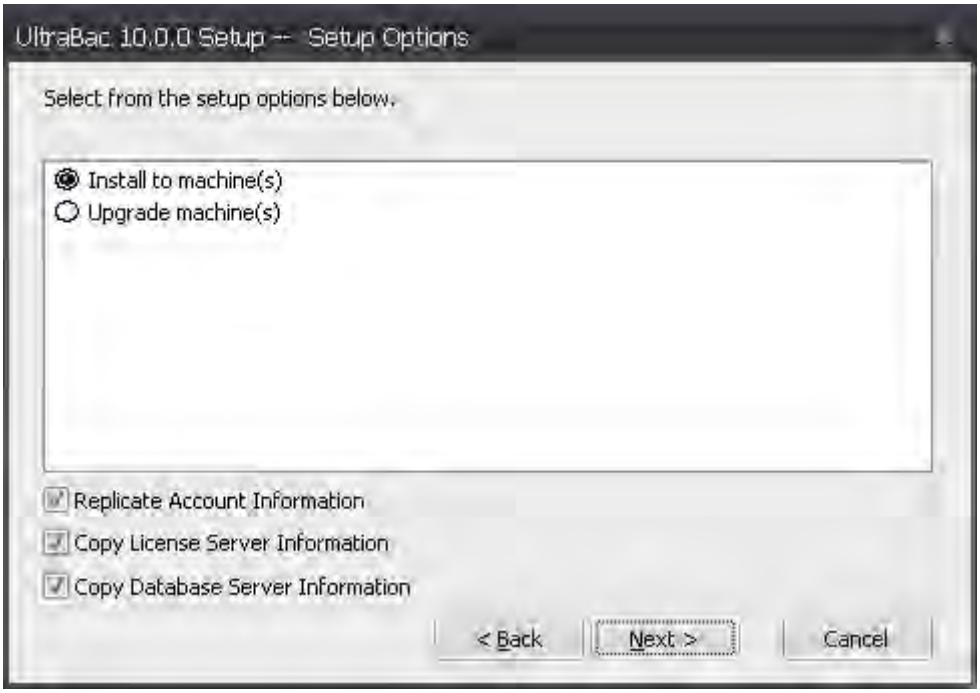


Fig. 4 - Setup options.

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."

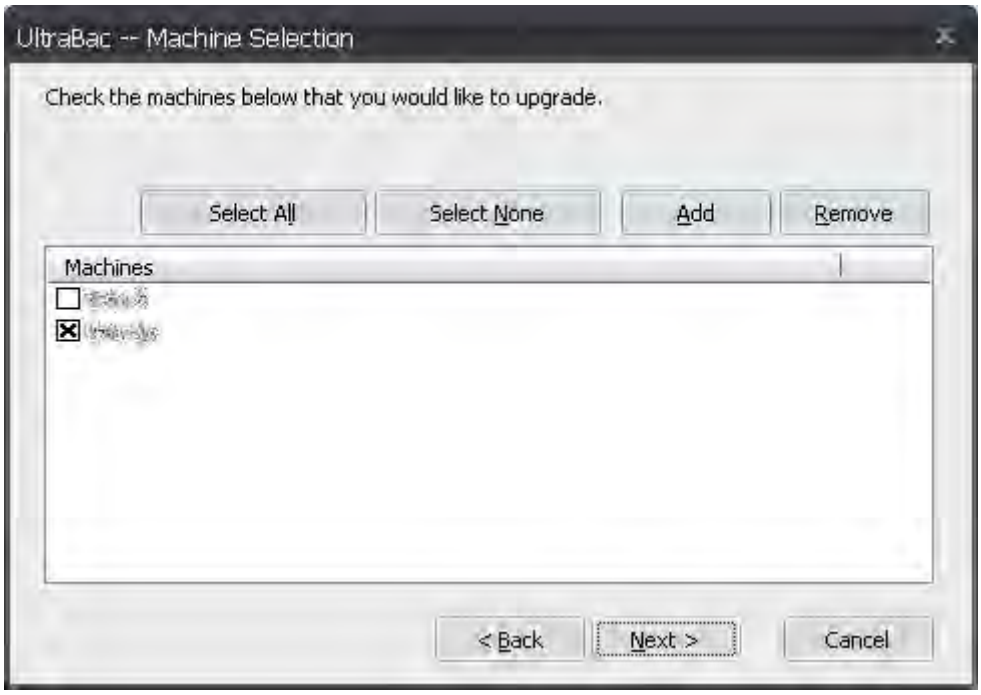


Fig. 5 - Selecting systems for installation.

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:

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.

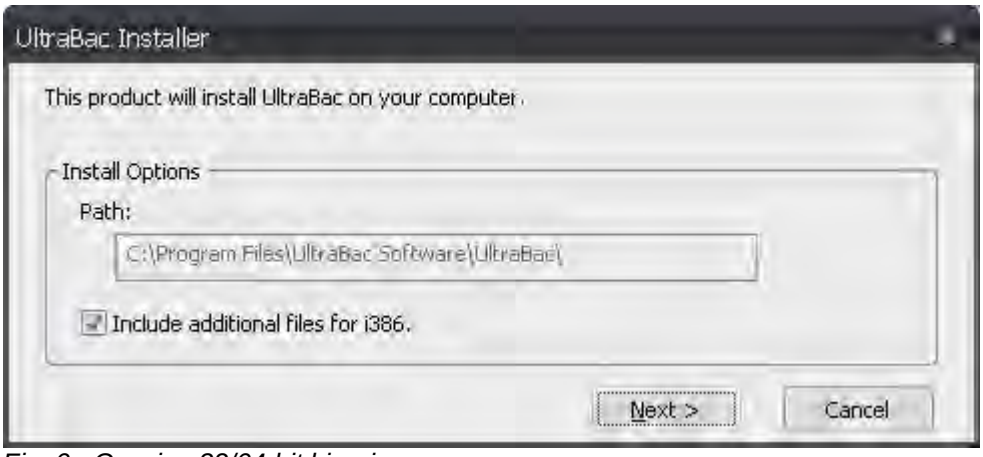


Fig. 6 - Copying 32/64-bit binaries.

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."

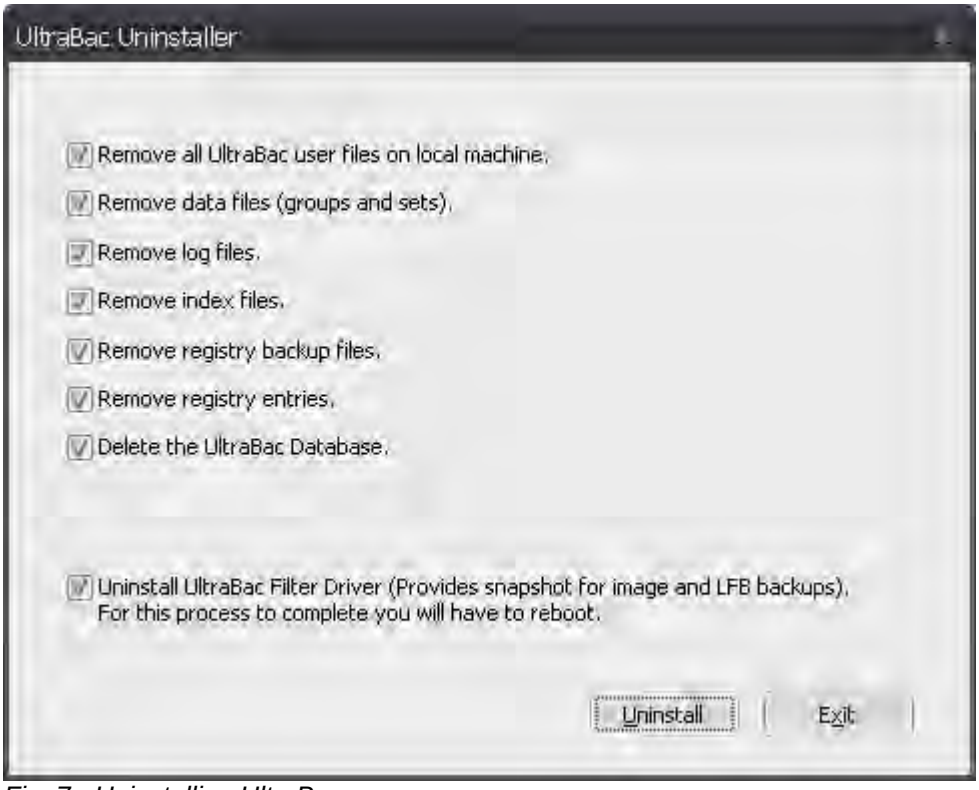


Fig. 7 - Uninstalling UltraBac.

2. Check "Remove all UltraBac user 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 files on local machine" 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 not been installed, the option "Delete the UltraBac Database" will not appear in the list.
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."

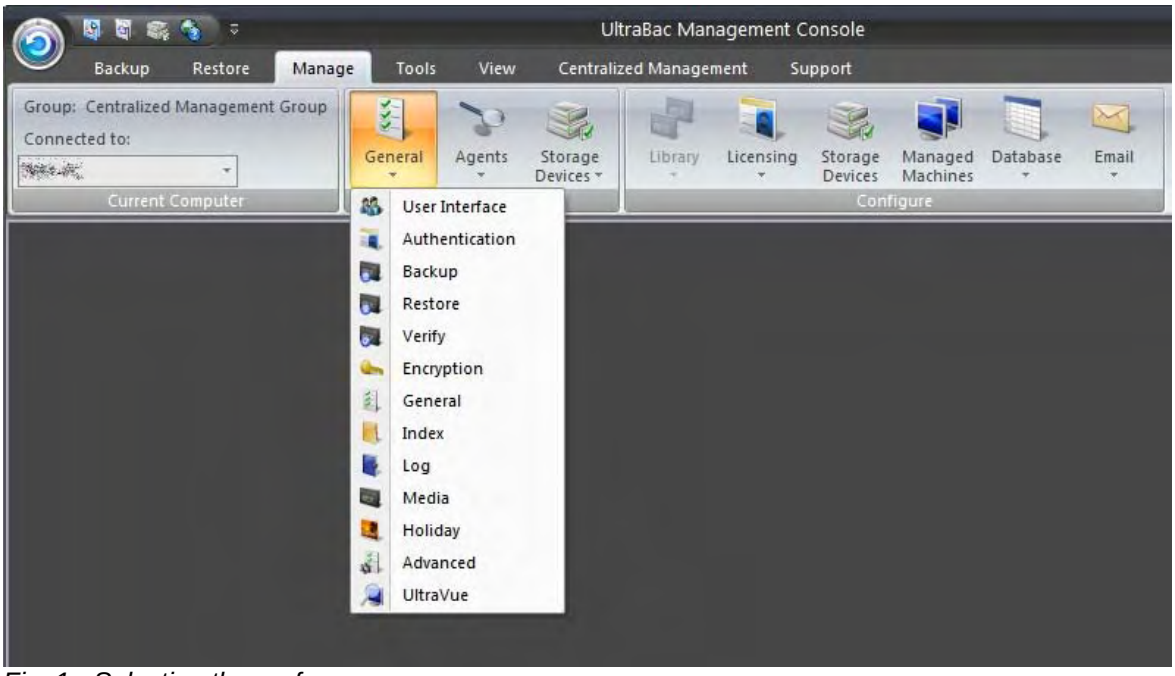


Fig. 1 - Selecting the preferences.

User Options

The User menu modifies the default behavior of the UltraBac user interface.

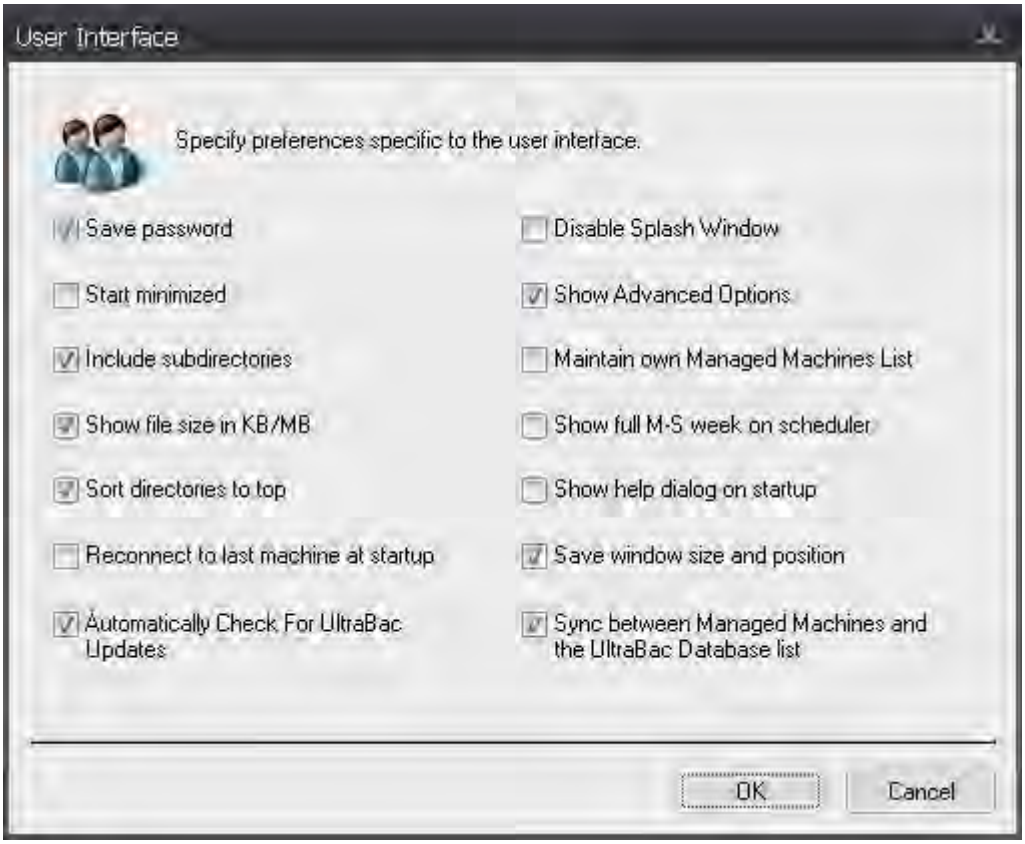


Fig. 2 - User preferences.

User Preferences:

- Save password – If a user name 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.
- Show 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.
- Automatically Check For UltraBac Update – Will check to see of there is a newer version of UltraBac available.
- 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. It also enables "Enterprise Control File."
- 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.

- Save window size and position – UltraBac will remember its previous window size when opened.
- Sync between Managed Machines and the UltraBac Database list – Only visible if connected to an UltraBac database. Adding machines to a Managed Machine list will add them to the database for Centralized Management monitoring.

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.

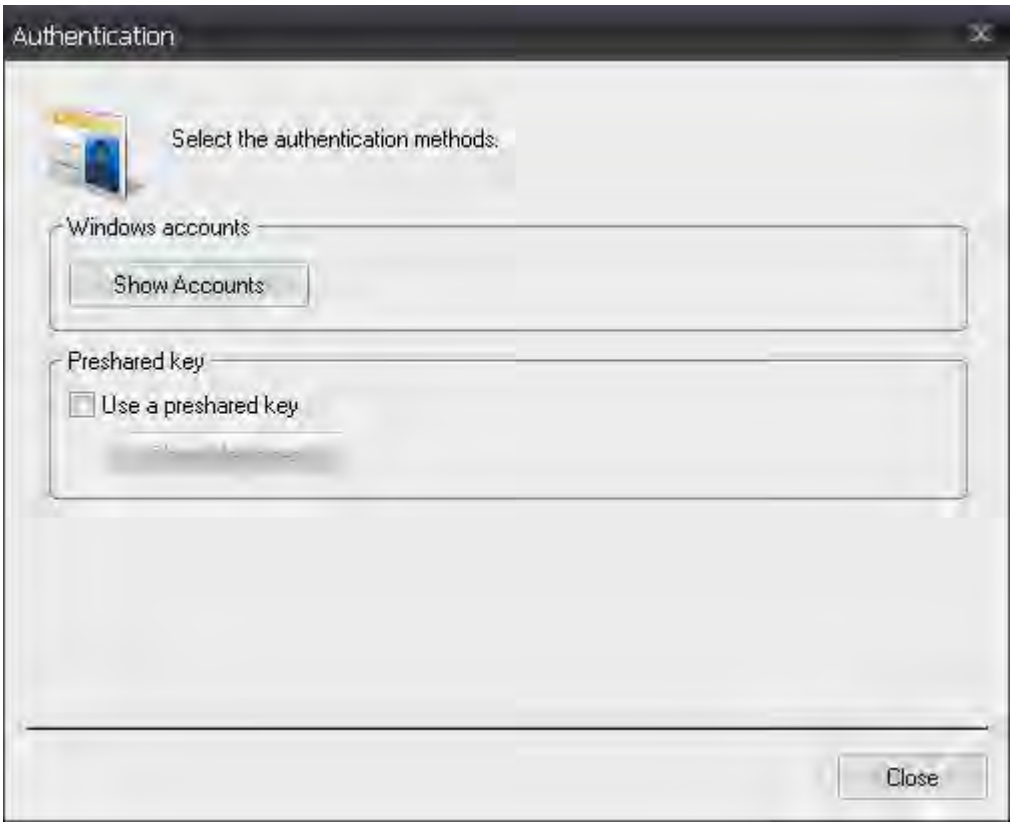


Fig. 3 - Authentication methods.



Fig. 4 - Show accounts.

To add a domain user account in UltraBac:

1. Click the "Show Accounts" button in the Authentication tab.
2. Click the "Add Account" 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.

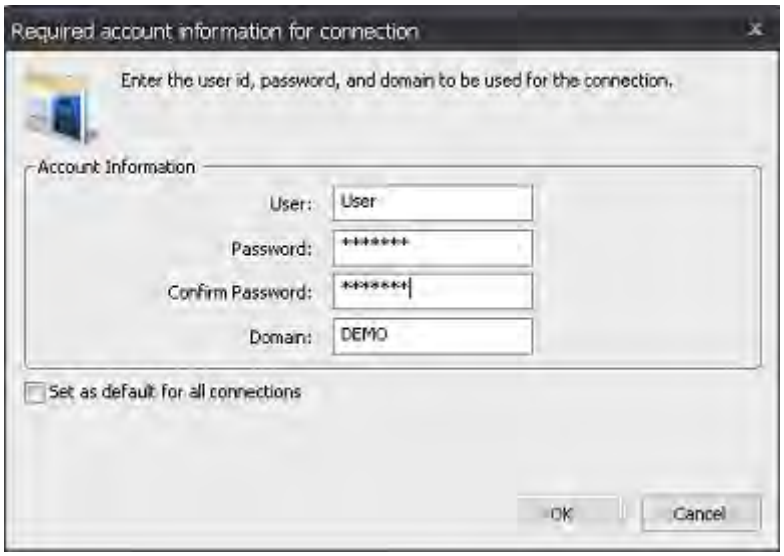


Fig. 5 - Account Information.

Checking "Set as default for all connections" will instruct UltraBac to use the specified account to run all scheduled backups as this user. Ad hoc backup jobs and restores are run as the currently logged on user.

To add a workgroup user account in UltraBac:

1. Click the "Show Accounts" button in the Authentication tab.
2. Click the "Add Account" 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 Account" 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.

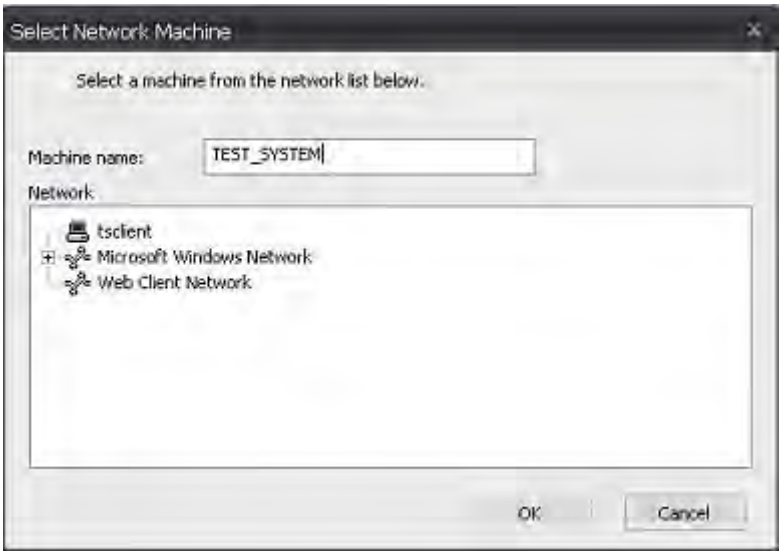


Fig. 6 - Specifying a system in the "Select Network Machine" screen.

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 "Edit" icon.
4. Click "OK" when finished.

Pushing Authentication to Managed Machines

To push out account Authentication to managed machines:

1. Click the "Show Accounts" button in the Authentication tab
2. Highlight the account you wish to push out.



Fig. 7 - Highlight account.

3. Click on the "Export" button.
4. Select the Managed Machine Group(s) to push authentication to and click "OK."

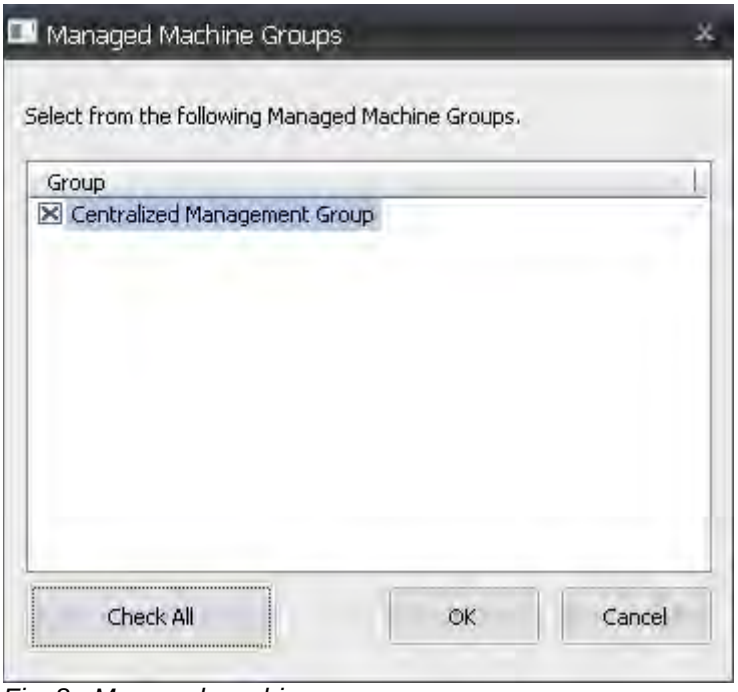


Fig. 8 - Managed machine groups.

5. A window will appear if the account authentication export was successful.

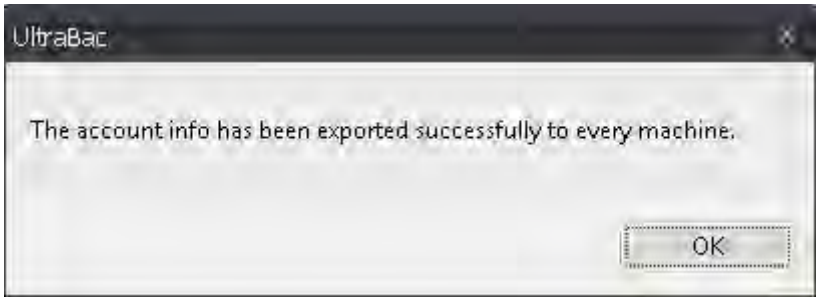


Fig. 9 - Export successful window.

Backup Options

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

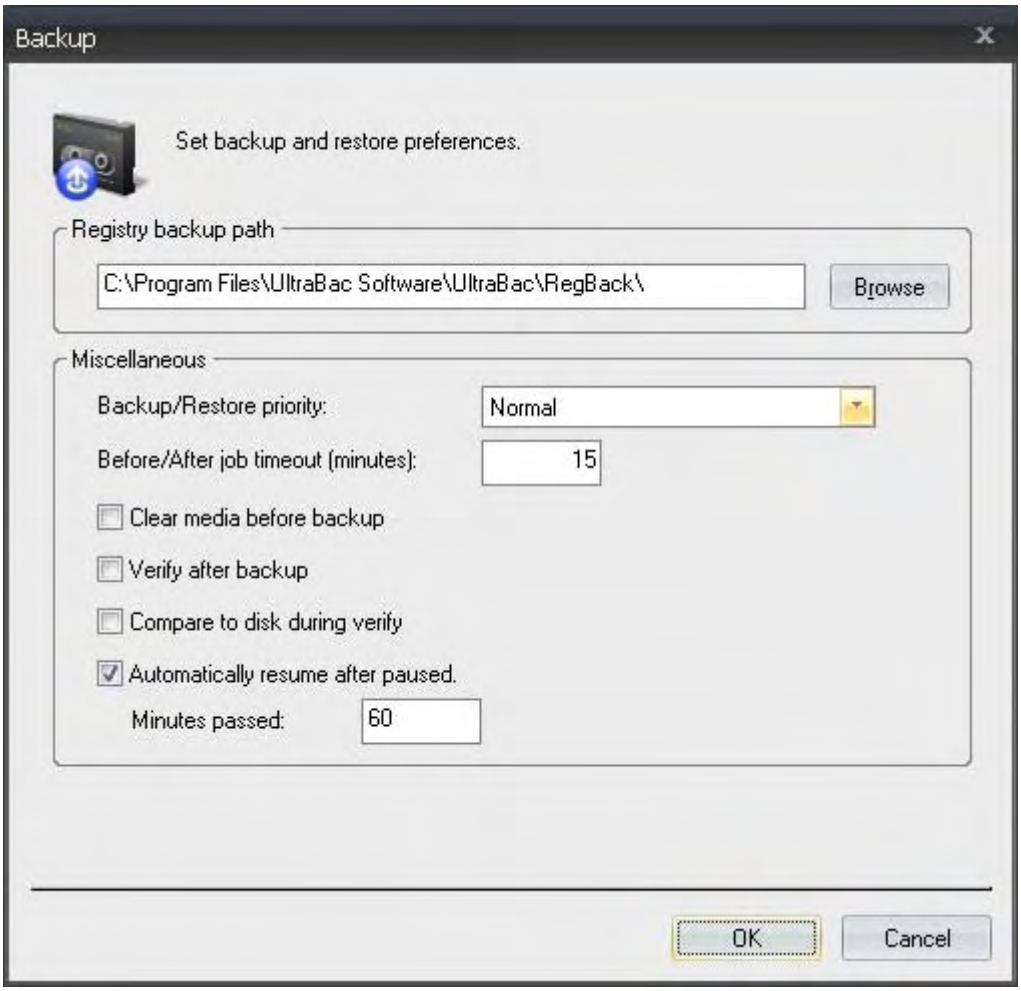


Fig. 10 - Backup preferences.

- Backup/Restore priority – This setting designates the priority of the system's resources when UltraBac is running:
    - Normal – Default priority.

  - High – If a thread runs at the highest priority level for extended periods, other threads in the system will not get processor time.
  - Realtime – This interrupts system threads that manage mouse input, keyboard input, and background disk flushing. System may appear unresponsive. NOT RECOMMENDED.
  - Idle – This prevents the threads of this process, which do not have high priority, from interfering with higher priority threads.

- 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.
- Automatically resume after paused – Automatically resume the backup if the backup is paused.
- Minutes passed: XX – Minutes until the backup is resumed if the backup is paused.

Restore Options

The Restore Options menu is used to set two restore options.

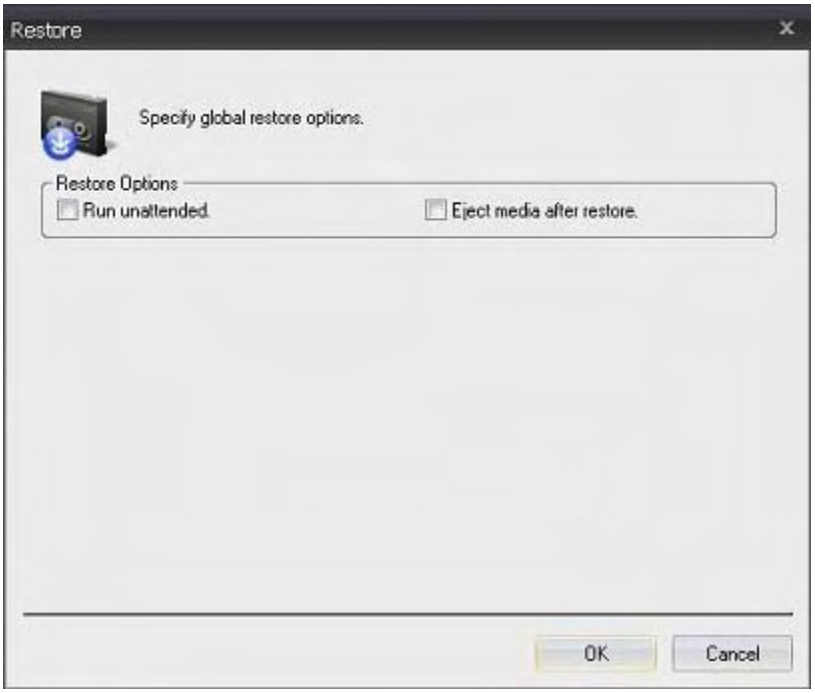


Fig. 11 - Restore preferences.

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 verify options.

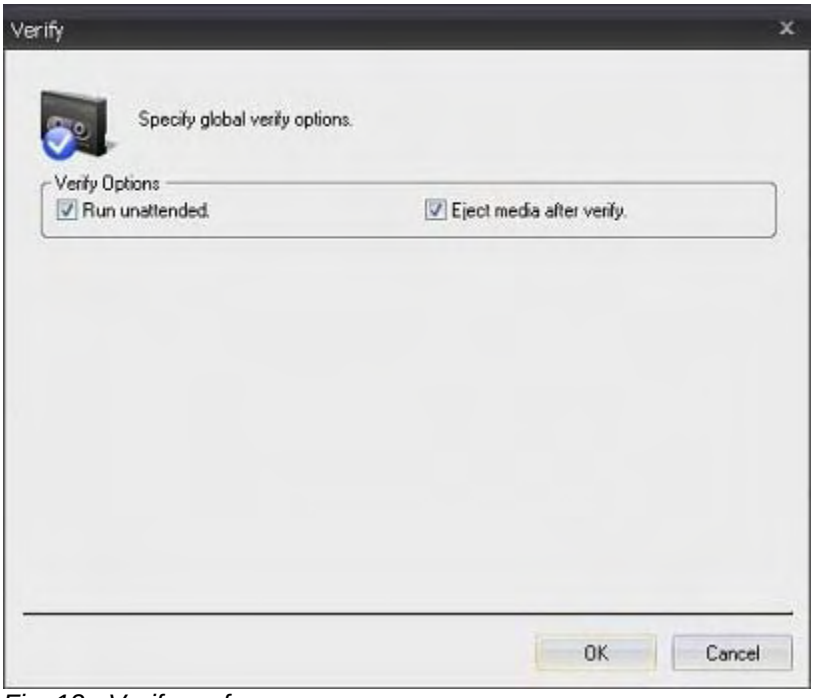


Fig. 12 - Verify preferences.

Verify Options:

- Run unattended – Do not prompt the user during ad hoc backups.
- Eject media after verify – 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.

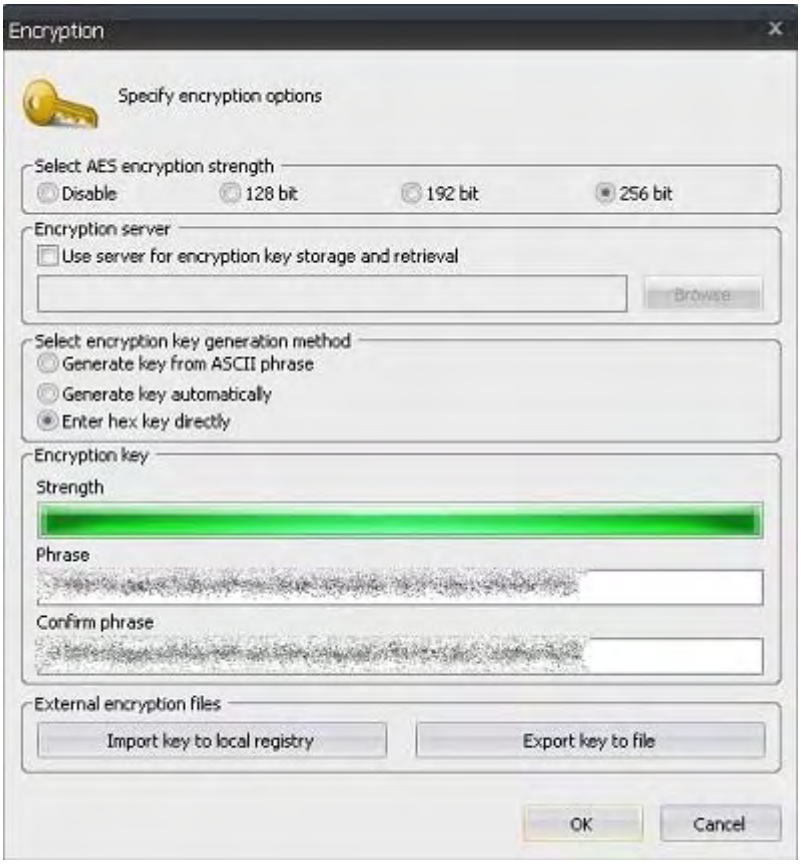


Fig. 13 - AES encryption options.

To enable encryption:

1. From the main UltraBac toolbar, click "Manage"/"General"/"Encryption."
2. Set the AES encryption strength: Disable – Turns off all AES usage.

    - 128-bit – Sets AES to use a 128-bit key.
    - 192-bit – Sets AES to use a 192-bit key.
    - 256-bit – Sets AES to use a 256-bit key.

3. Select the method for generating the encryption key:

    - Generate key from ASCII phrase – Creates an encryption key using any ASCII characters, of the specified encryption strength.
    - Generate key automatically – Creates a random encryption key using HEX characters, of the specified encryption strength.
    - 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.

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

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."

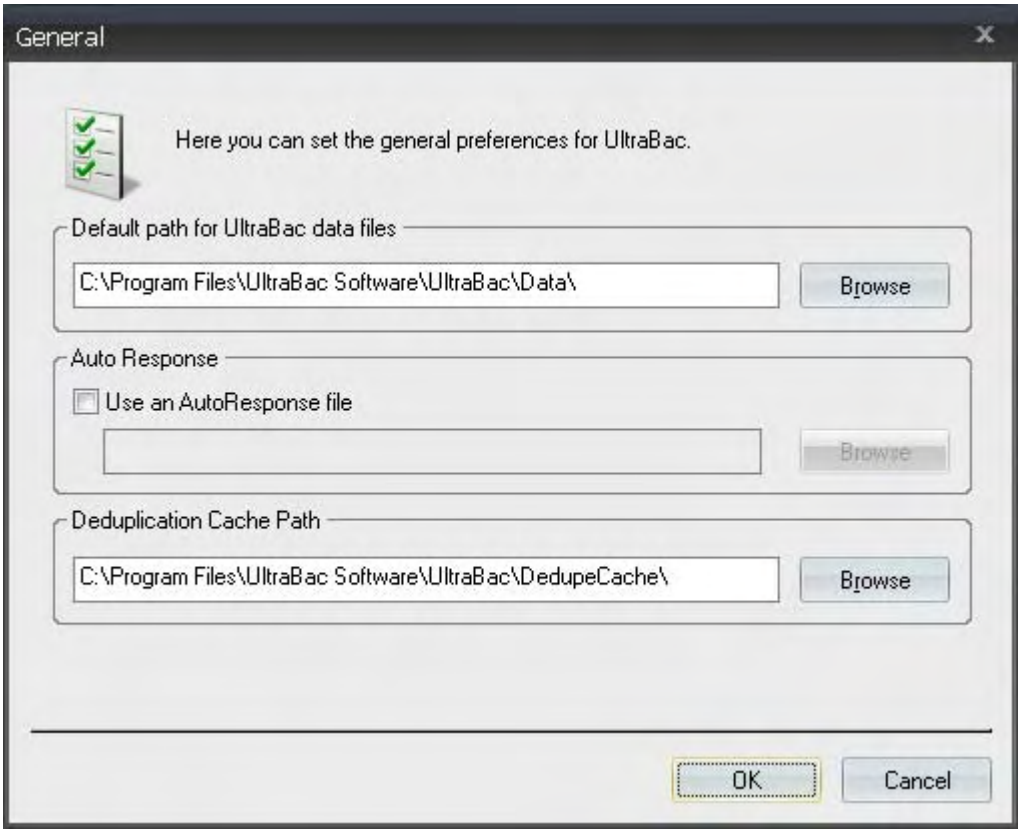


Fig. 14 - General preferences.

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.

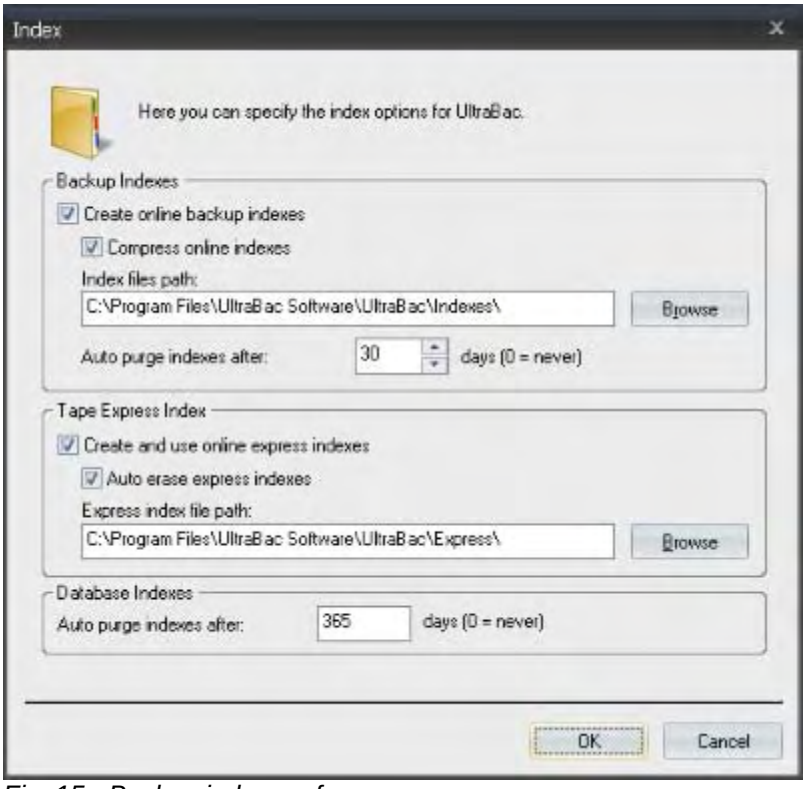


Fig. 15 - Backup index preferences.

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.

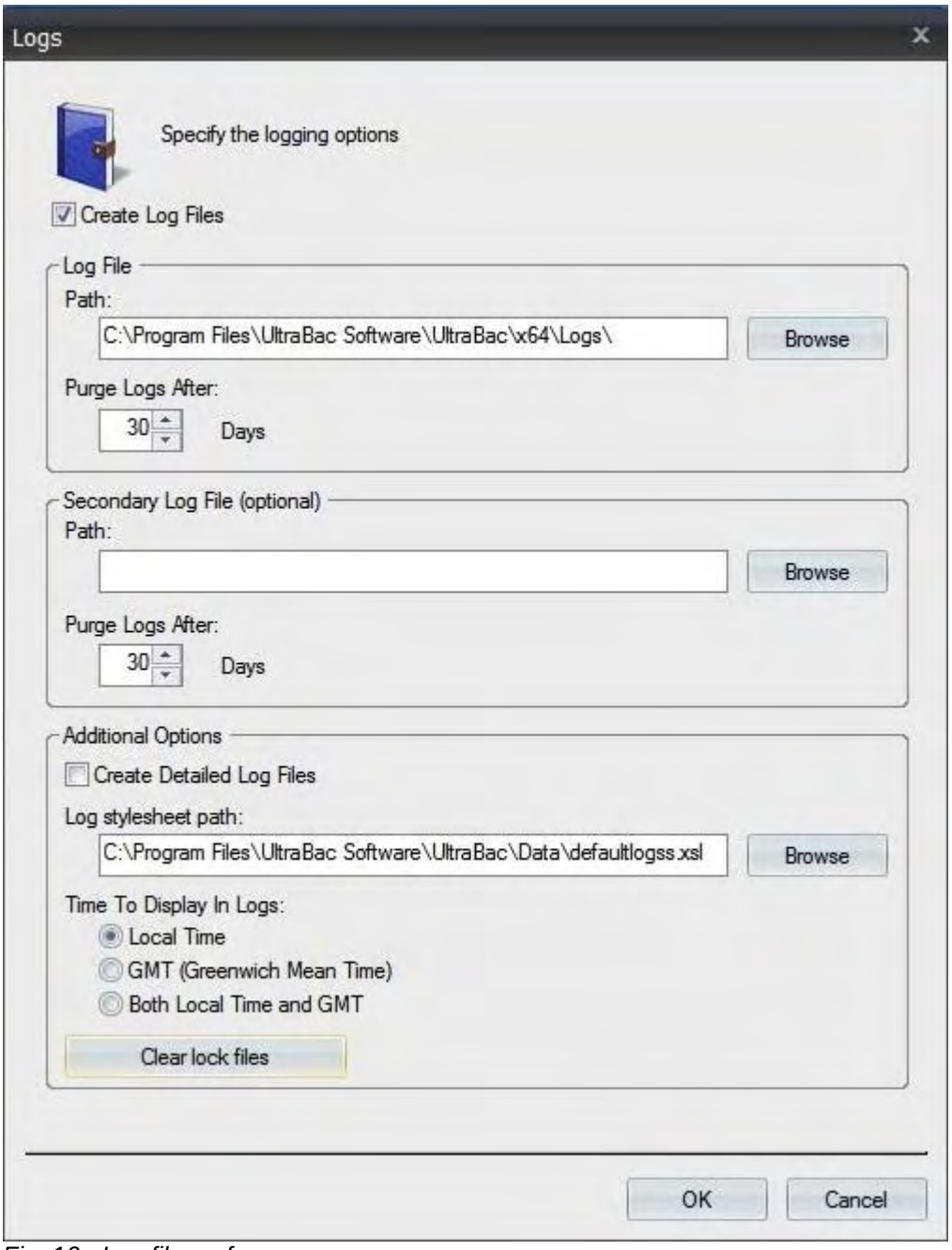


Fig. 16 - Log file preferences.

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.

- Create Log Files – Enables the creation of backup, verify, and restore logs.

Log File / Secondary Log File (optional)

- Path – 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."

Additional Options

- 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.
- Time To Display In Logs – Time displayed in logs for start, end, errors, warnings.
- Clear lock files – Deletes all .lck files from the logs directory.

Media Options

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

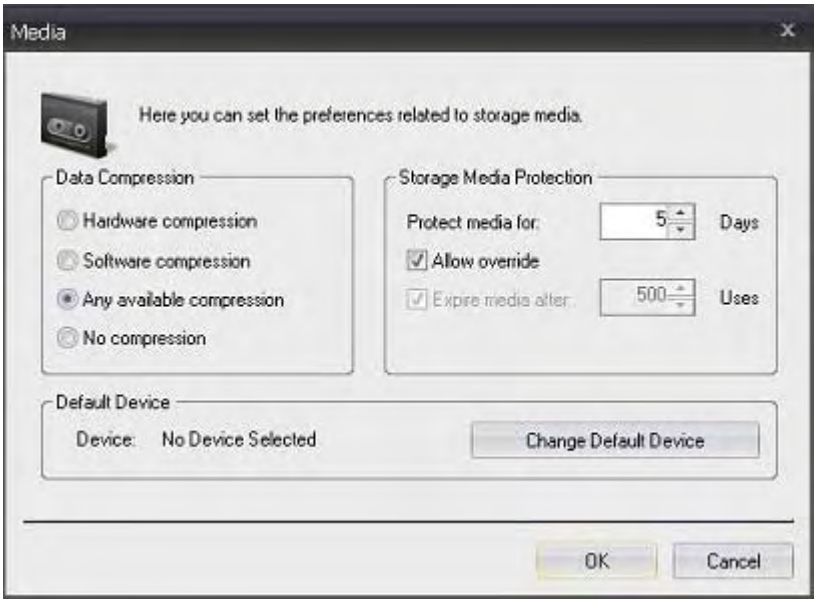


Fig 17 - Media options.

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. 18 - 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.

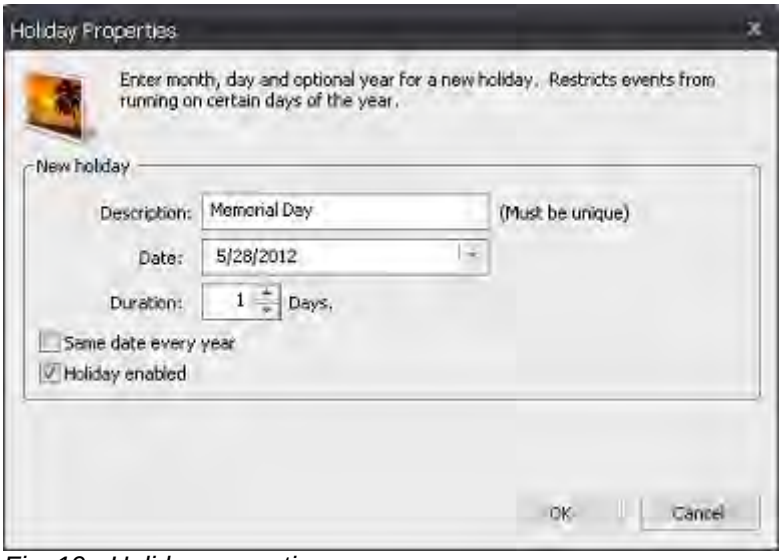


Fig. 19 - Holiday properties.

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.

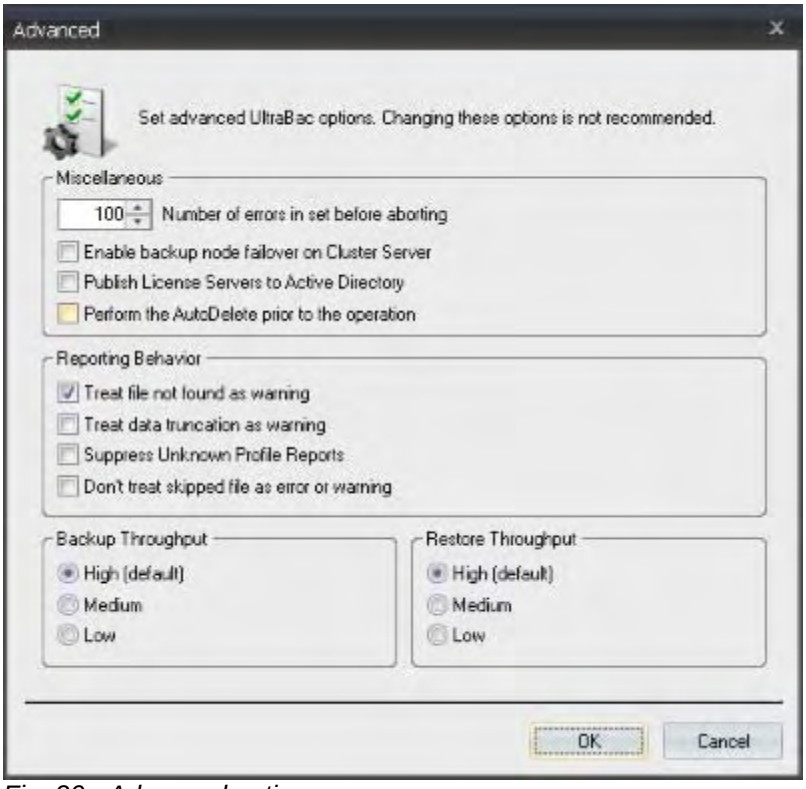


Fig. 20 - Advanced options.

Miscellaneous

- 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. Requires UltraBac services to be configured on the cluster.
- Publish License Servers to Active Directory – Records the UltraBac License server in Active Directory for the local domain.
- Perform the AutoDelete prior to the operation – Perform AutoDelete on a BackupPath before the backup runs rather than after a successful completion.

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.

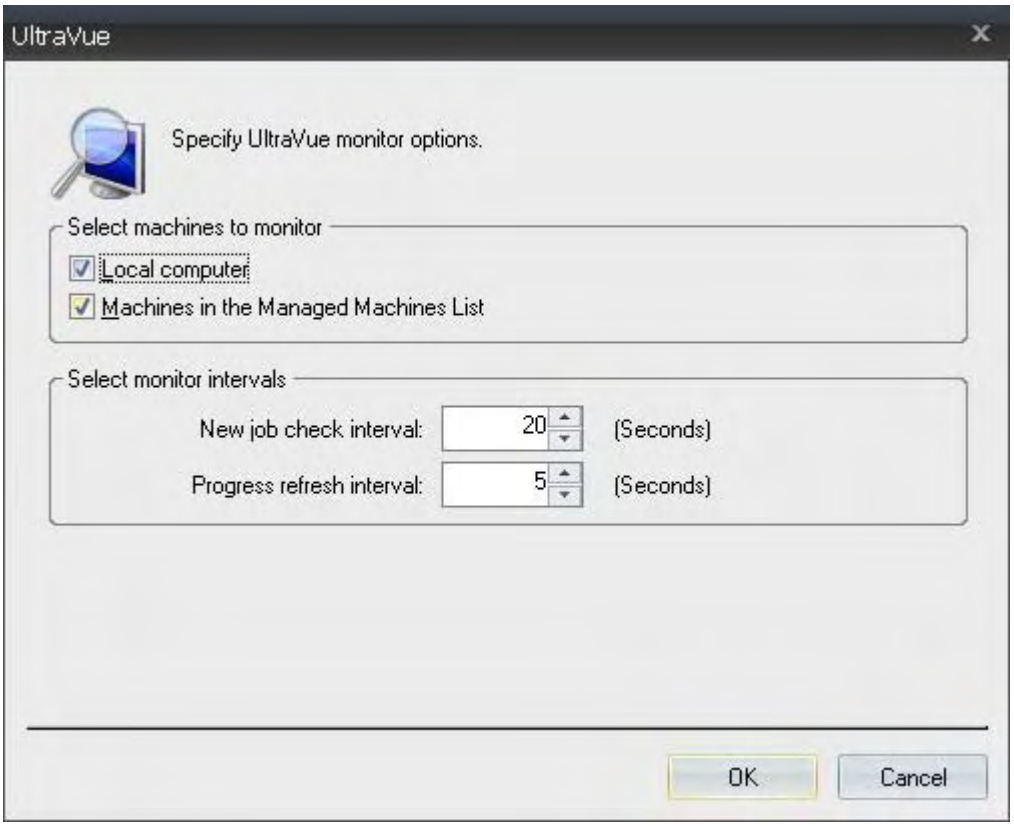


Fig. 21 - UltraVue preferences.

- 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:

https://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.

NOTE: For additional information on a description of license components, please see the UltraBac Knowledge Base:

UBQ000214: Description of License Components

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.

3. Select "Import license from file" and click "OK."
4. Browse to the UltraBac directory, select the "ublicense.txt" file, and click "Open."

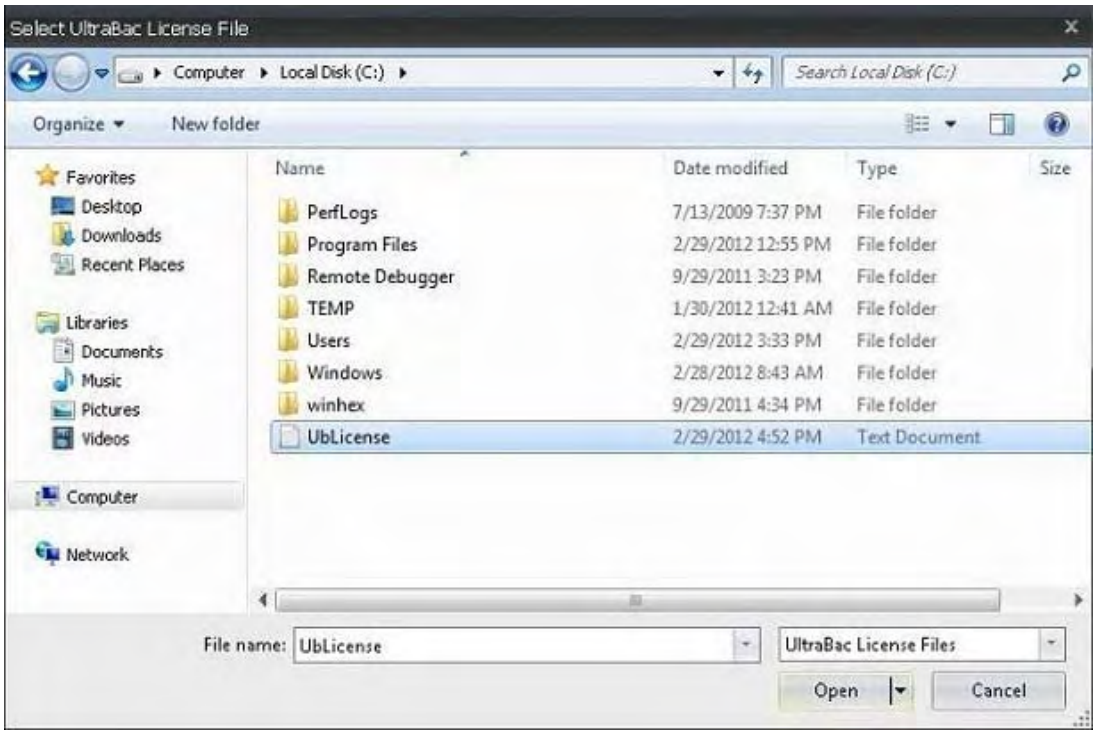


Fig. 2 - Browsing to the license file.

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

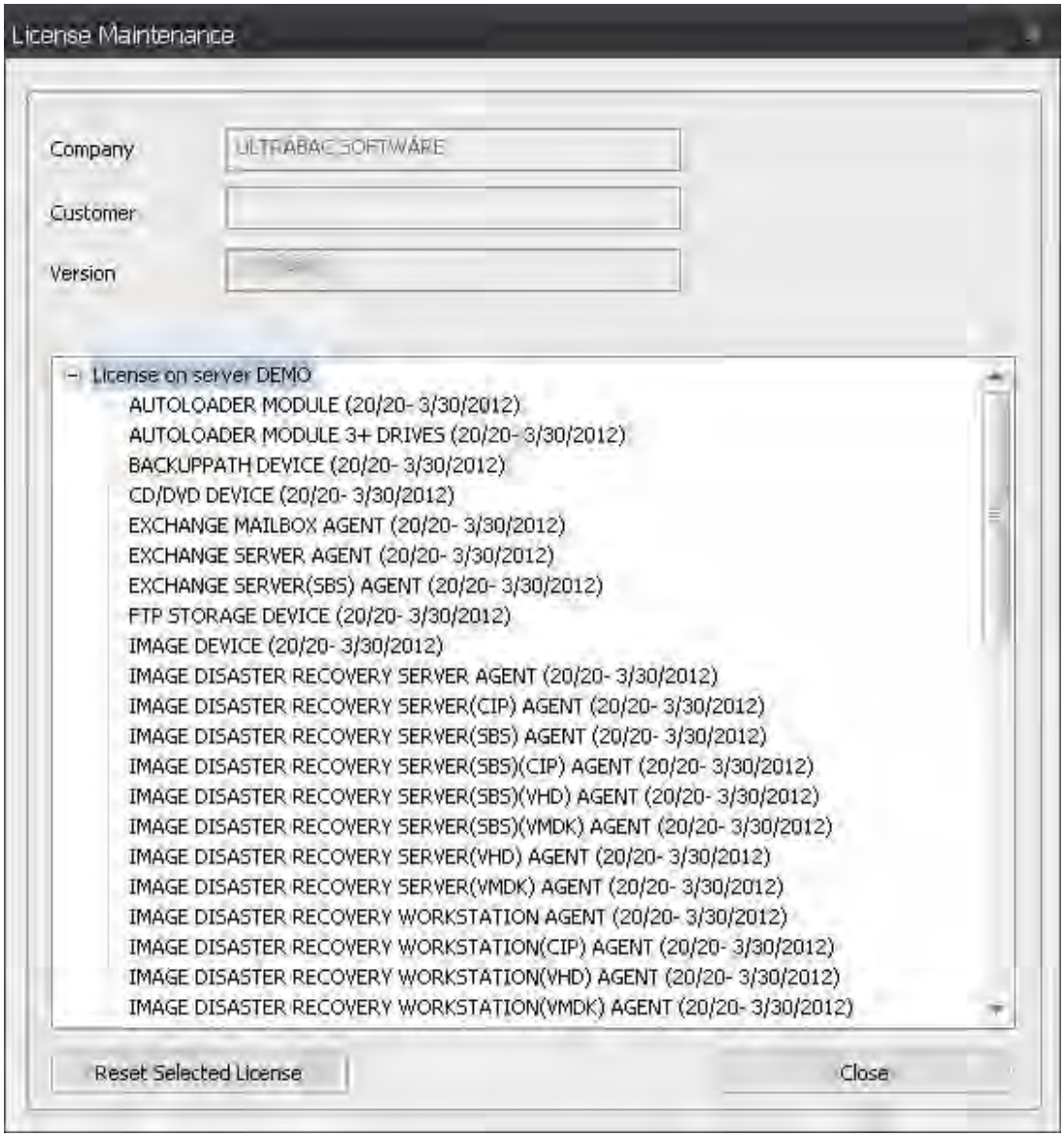


Fig. 3 - License components.

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 10

To upgrade a prior Version 7,8, or 9 license to Version 10, please visit:

https://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

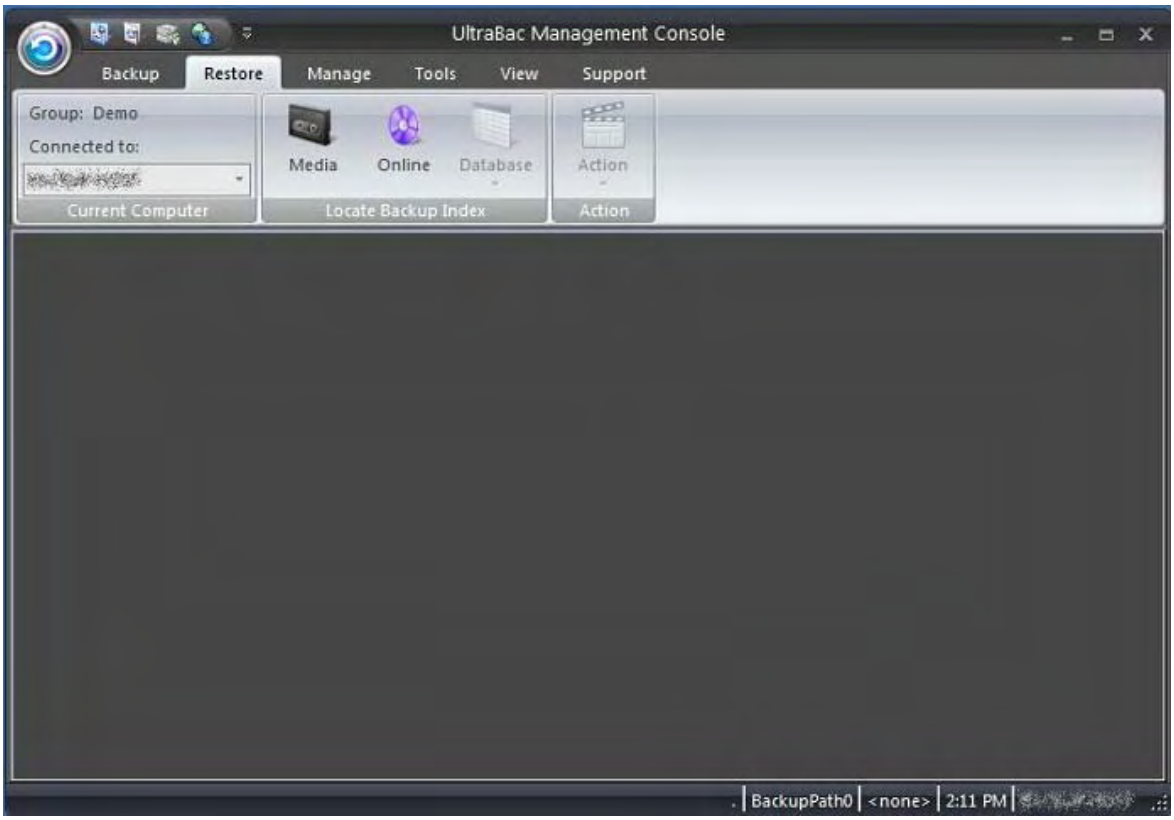


Fig. 1 - The UltraBac Management Console.

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, the UltraBac Installer, and the Backup Migration Tool.
- 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.

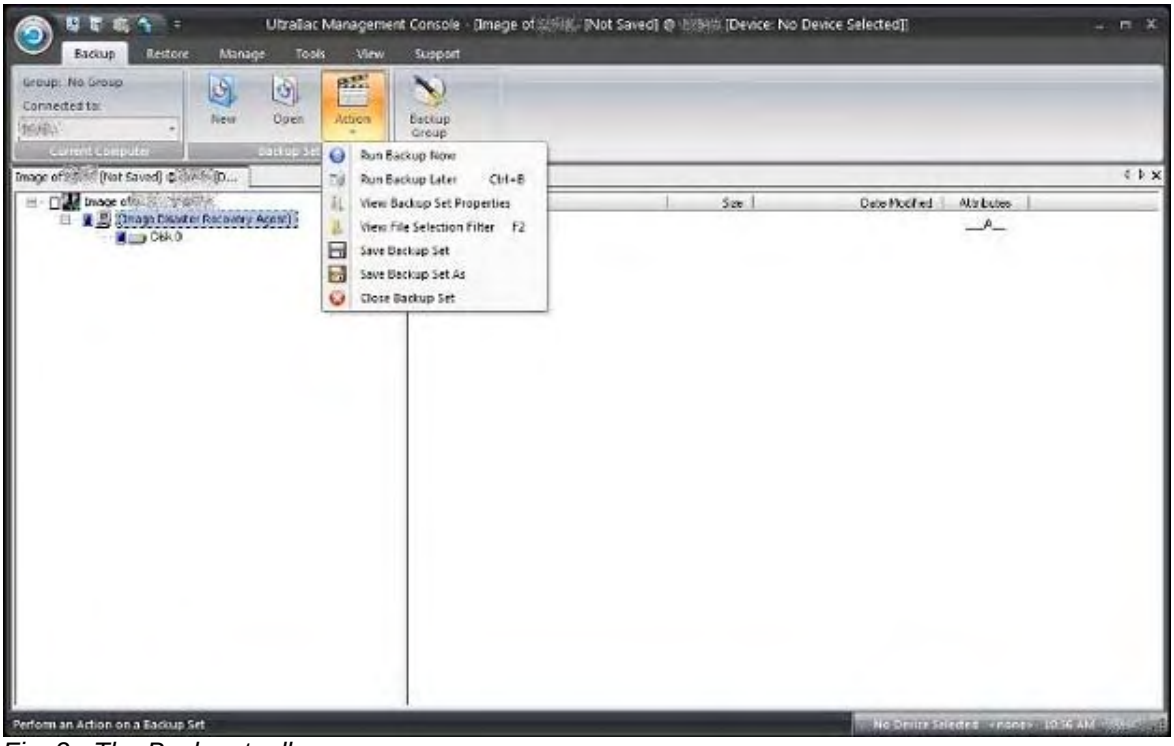


Fig. 2 - The Backup toolbar.

- 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:
    - Run Backup Now – Runs the open backup set to the selected backup device.
    - Run Backup Later – Opens the Scheduled Backup Wizard to create a new scheduled backup job.
    - View Backup Set Properties – Views the properties of the open backup set for editing. Each agent has its own specific options/properties.
    - View File Selection Filter – Views the file selection logic as used in the open backup set.



Fig. 3 - UltraBac File Selection Filter.

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

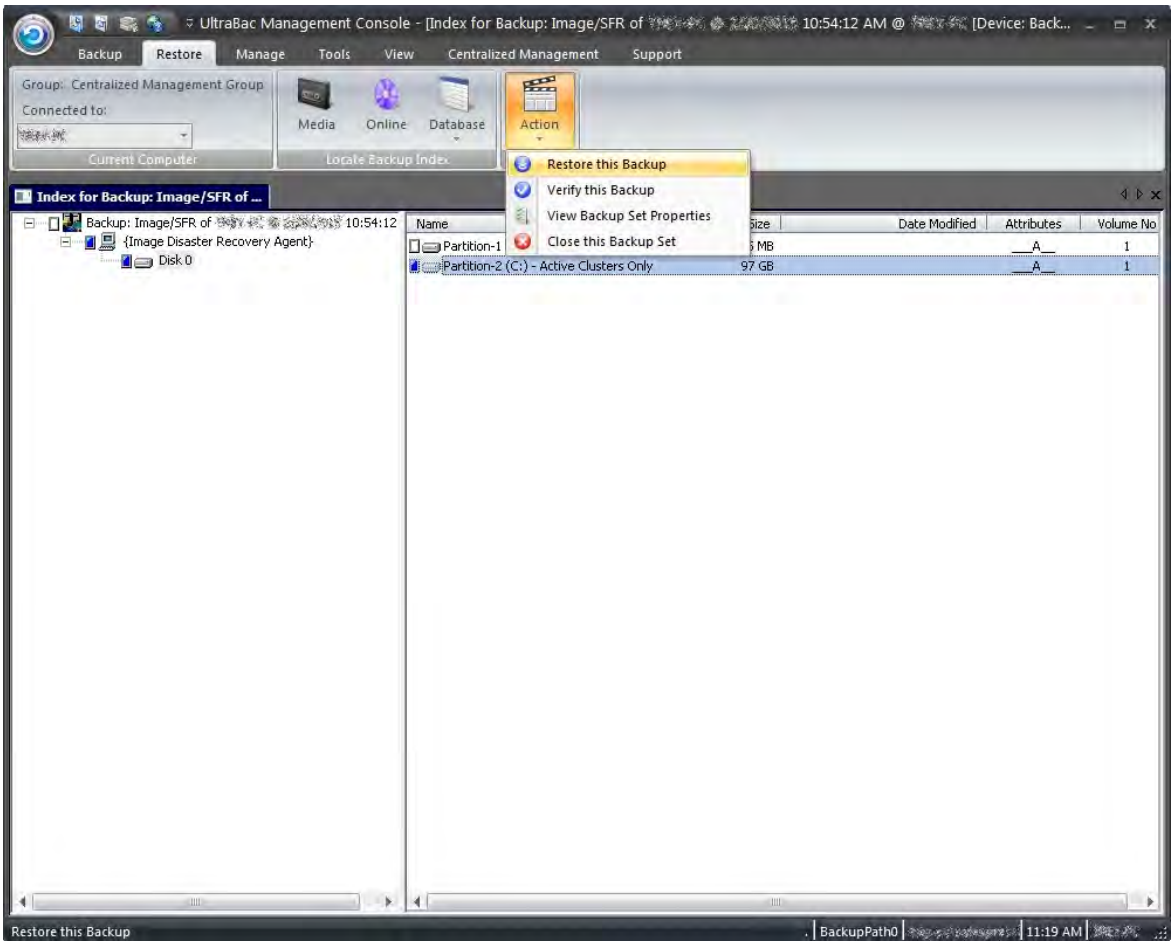


Fig. 4 - The Restore toolbar.

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.

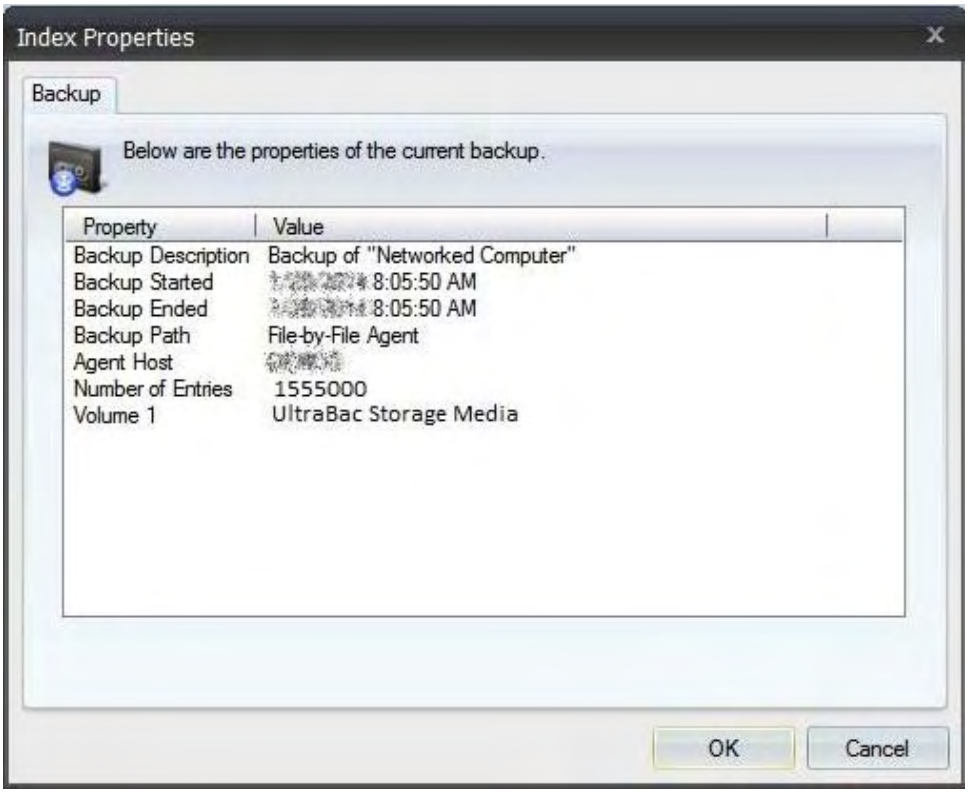


Fig. 5 - Properties of the selected file-by-file backup index.

- 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.

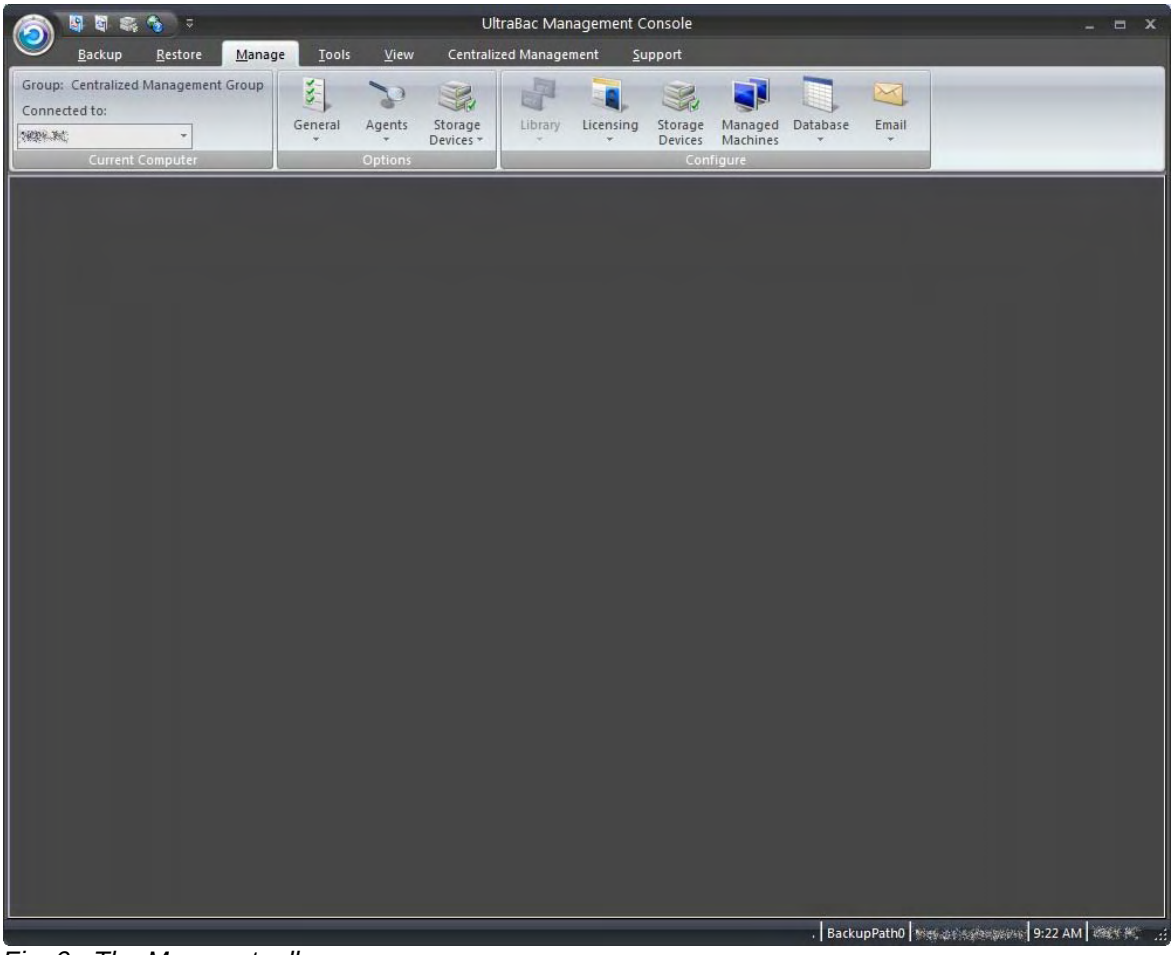


Fig. 6 - The Manage toolbar.

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.

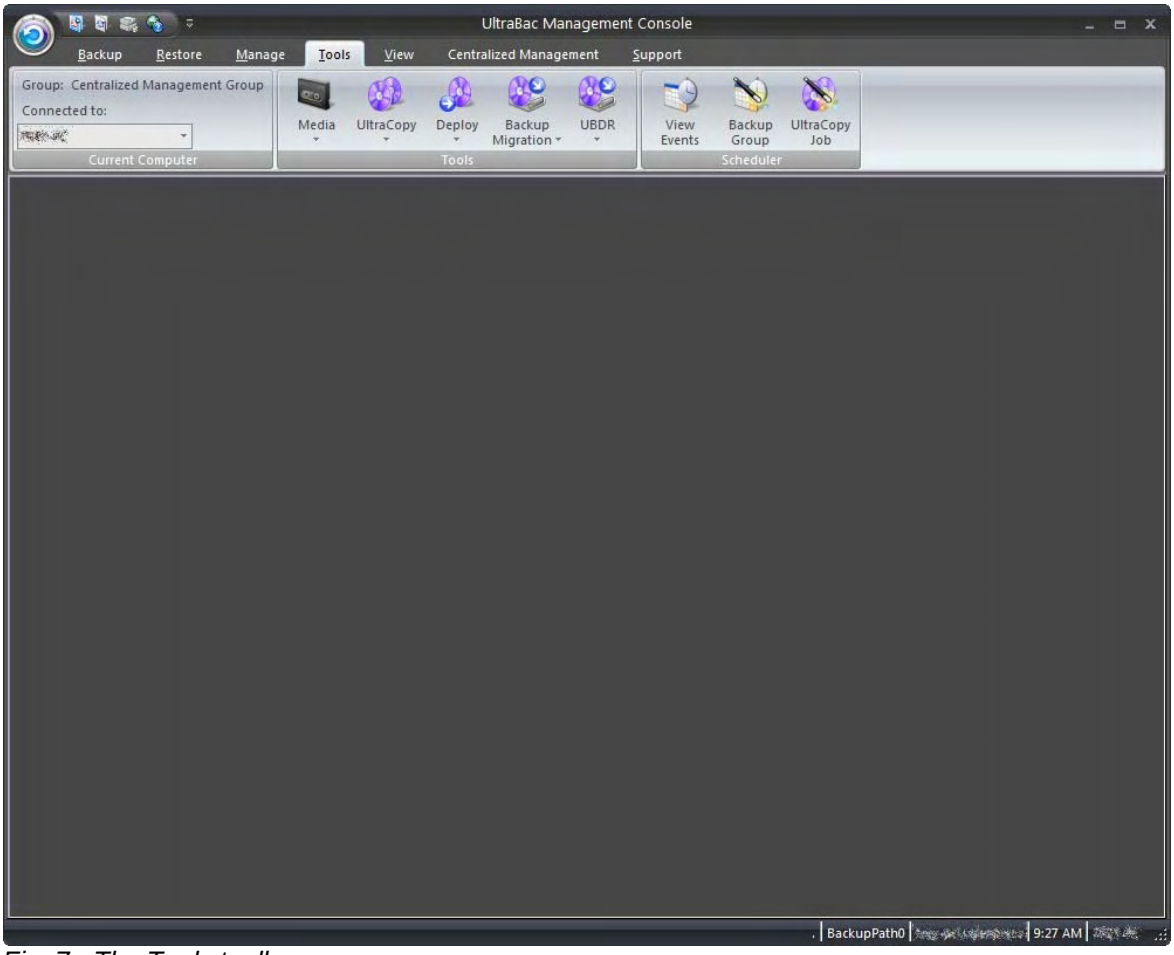


Fig. 7 - The Tools toolbar.

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 – Copy existing Backups between Storage Devices
  - Run UltraCopy Now – Run an ad-hoc UltraCopy job
  - Schedule UltraCopy for Later – Create an UltraCopy job using the scheduler

- Deploy – Launches the UltraBac Remote Installer.
  - Install UltraBac – Install UltraBac on computers in the Managed Machines List
  - Uninstall UltraBac – Uninstall UltraBac on computers in the Managed Machines List
  - Upgrade UltraBac Version – Upgrade UltraBac on computers in the Managed Machines List

- Backup Migration – Automatically Copy Backups to Other Storage Devices
  - Add a Single-Use Backup Migration Job – Run an ad-hoc migration (UltraCopy).
  - Add/Edit the Migration Pools – Create new pools or edit exist pool contents (devices).
  - Backup Migration Options – Turn off Backup Migration, set stale options, concurrent Jobs.
  - View Groups containing Migration Pools – Lists all scheduled jobs and any that are using Migration Pools

- UBDR – Launches the UltraBac Remote Installer.
  - Unmount All Volumes – Unmount all Image SFR mounted backups.

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.

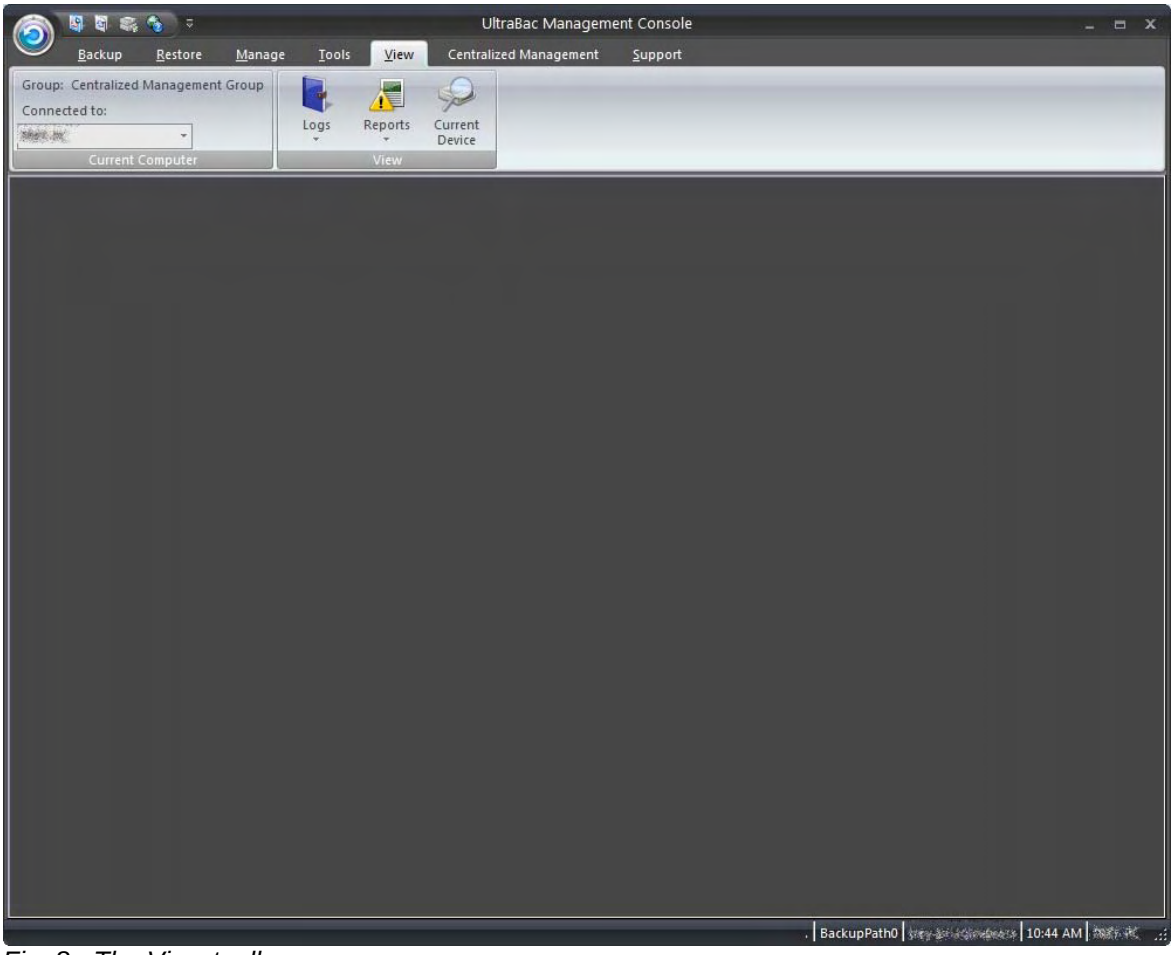


Fig. 8 - The View toolbar.

Logs:

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

Reports:

- Current Operations – Launches the Current Operations workspace.
- Future Operations – Opens a list of enabled backup jobs.
- Database Reports
- Migration Queue

Current Device:

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

Current Operations

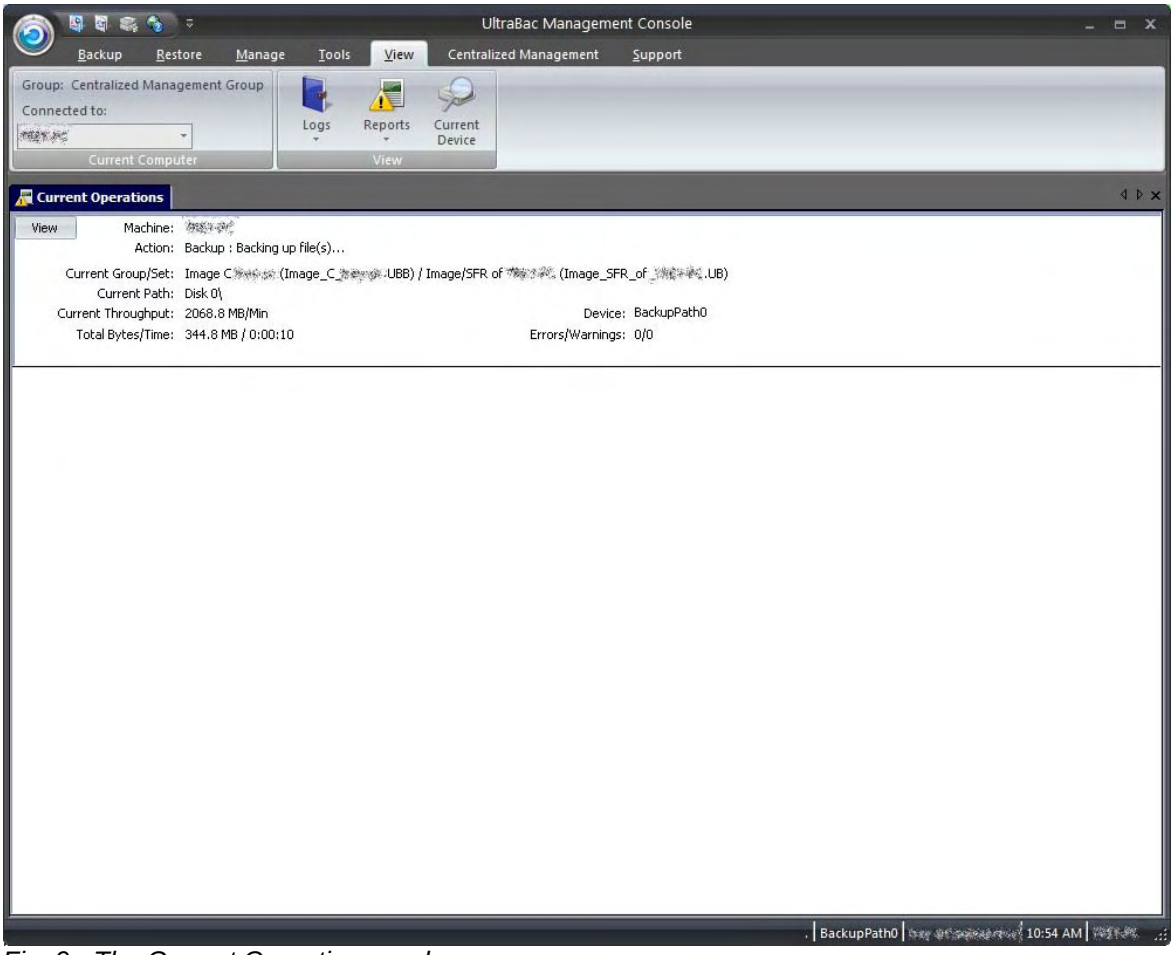


Fig. 9 - The Current Operations workspace.

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.

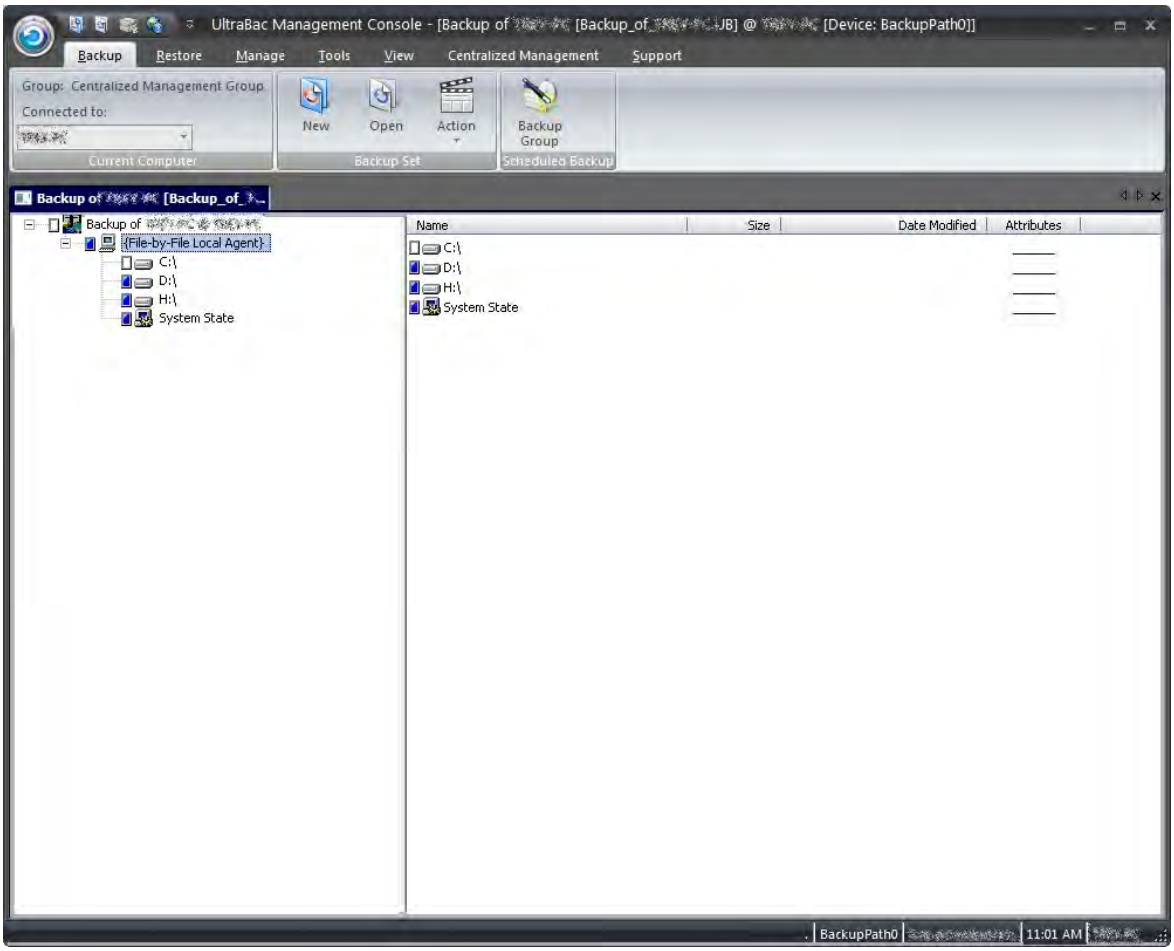


Fig. 10 - Backup set loaded in the File Viewer.

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.

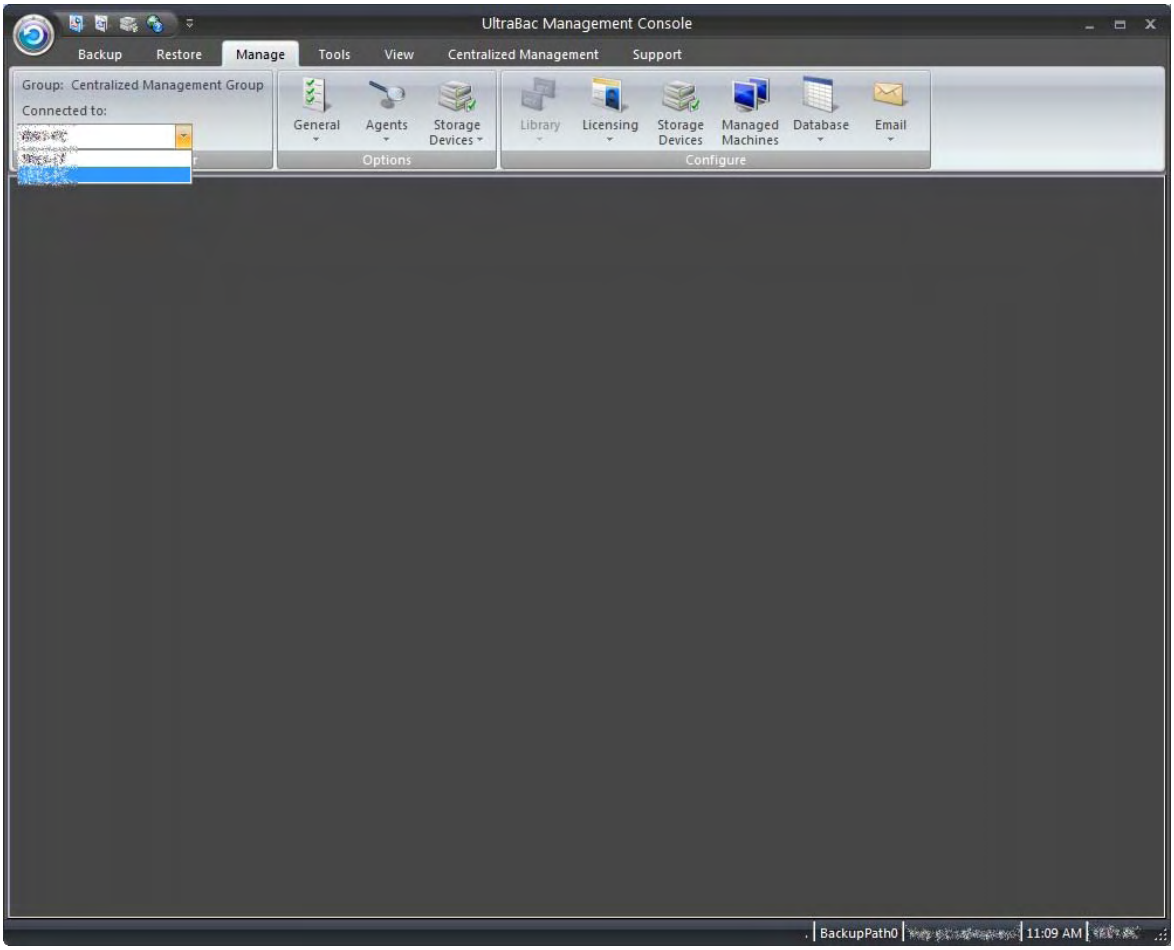


Fig. 11 - The "Connect" feature.

To connect to the remote system's console:

1. Add the target system to the Managed Machines list if not already present:
   i. Select the Manage tab.
   ii. Click "Managed Machines."
   iii. Click "Add Group" and type the Group Name. Click "OK" (skip this step if using an existing group).
   iv. Highlight "Group Name" and click the "Edit" icon.
   v. Click "Add Machine" icon.
   vi. Type in the Windows name of, or browse to, the target system, and click "OK."
   vii. Click "Close."

2. From the "Connected to:" drop down list, 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 "Storage Devices" from the Manage tab in the "Configure" dialog box.

- Tape – locally attached tape devices, including libraries.
- CD/DVD – locally attached CD/DVD writers.
- BackupPath – local disk or UNC path devices.
- Cloud – write to cloud providers
- Tivoli – IBM Tivoli devices.
- DiskMirror – locally attached unpartitioned disk used for static mirror imaging.
- FTP – internet FTP\SFTP sites.
- PartitionMirror – locally attached partitioned disk used for static mirror imaging.
- Remote – UltraBac devices configured on remote systems.

NOTE: For additional information on Selecting a Storage Device, please see the UltraBac Knowledge Base:

UBQ000041: Selecting a Storage Device

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."

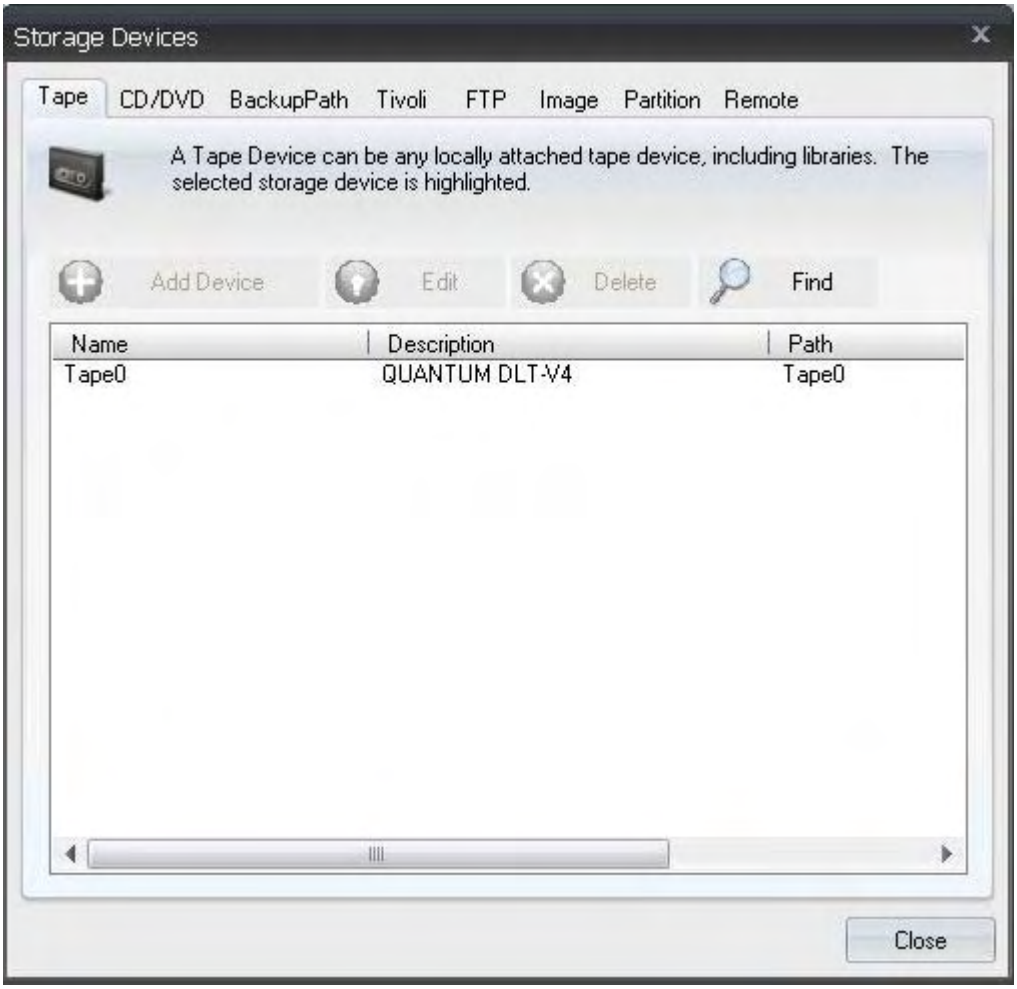


Fig. 1 - Tape devices.

CD/DVD Devices

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

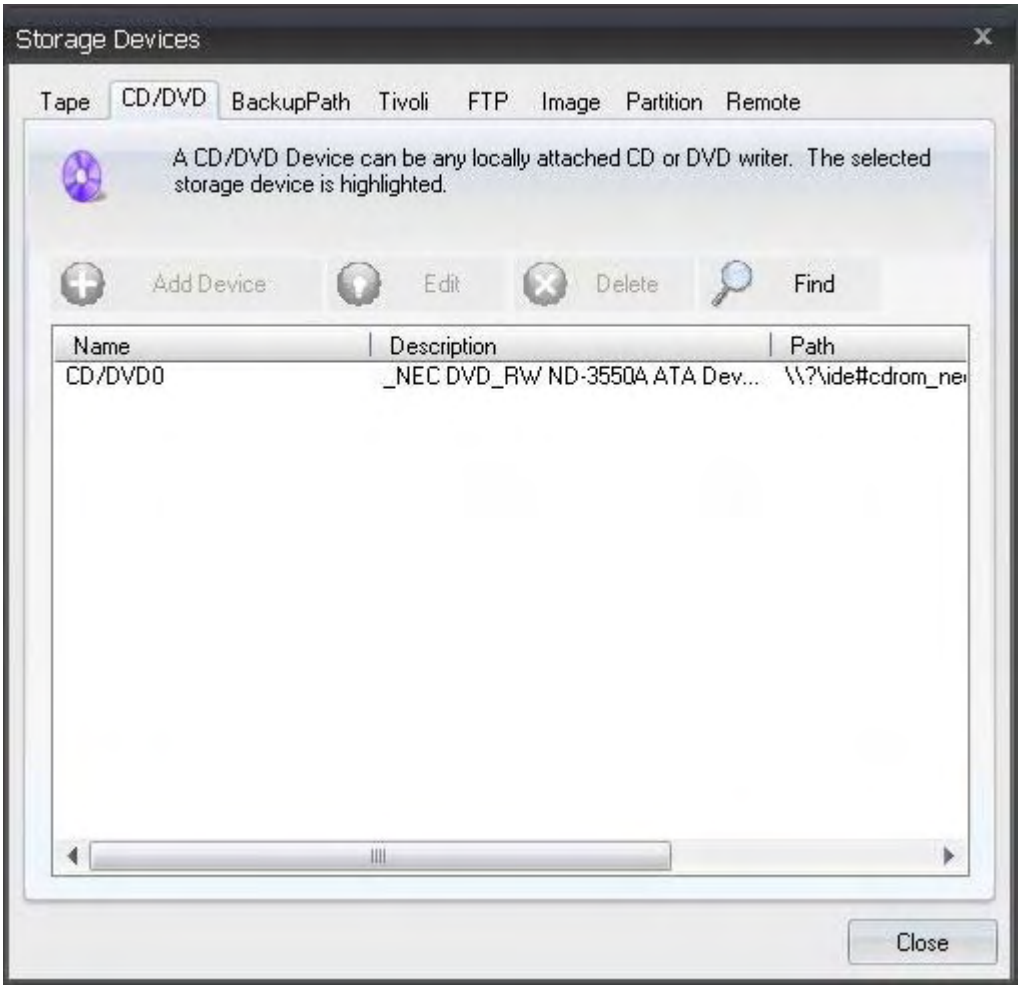


Fig. 2 - CD/DVD devices.

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 "Edit" 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."

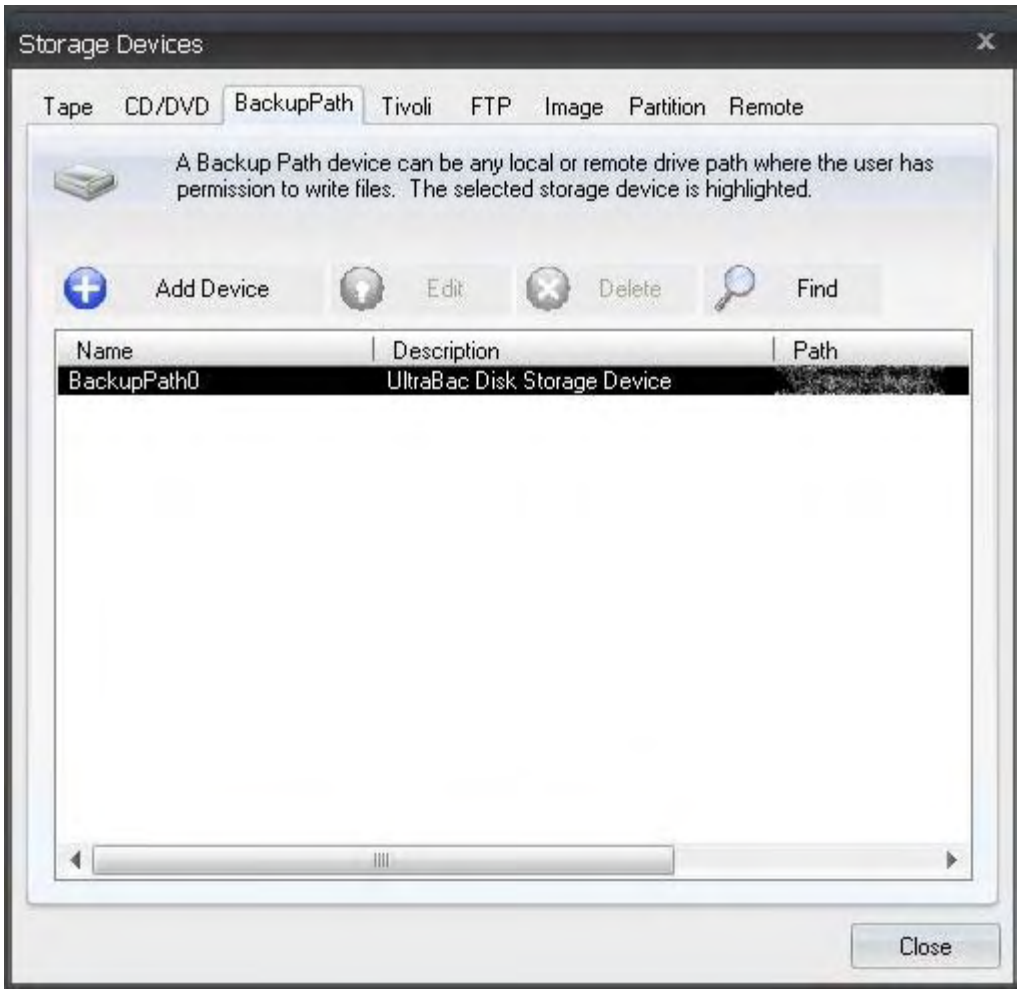


Fig. 3 - Creating a BackupPath device.

2. Select the BackupPath tab.
3. Click "Add Device."

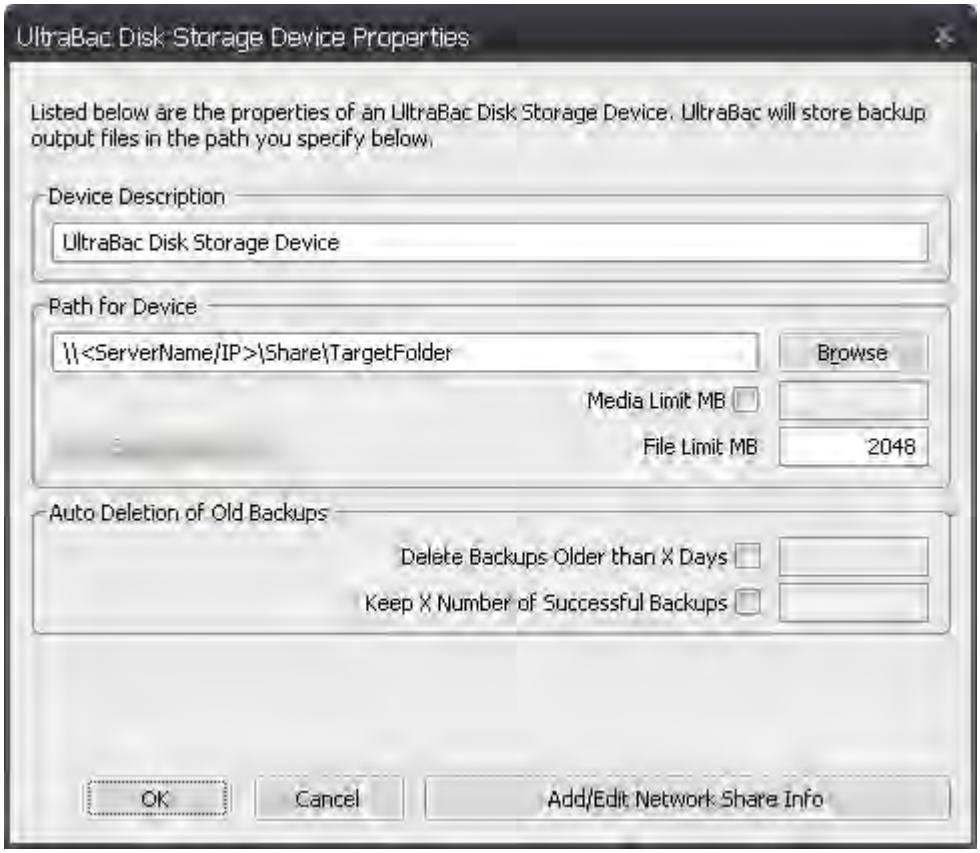


Fig. 4 - Disk Storage Device properties.

4. Enter a name in the "Device Description" field or leave the default value.
5. Enter a local or UNC path to be used as an output target in the "Path for Device" field.
6. Click "OK" to save. If the directory specified does not exist, UltraBac will create it.

To limit the amount of data that can be written to the BackupPath, check the box next to and enter the maximum folder size in the "Media Limit MB" 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 "File Limit MB" field. It is not recommended to use a file size larger than 4096 MB.

NOTE: For additional information on Defining a Disk (BackupPath) Storage Device, please see the UltraBac Knowledge Base:

UBQ000049: Defining a Disk (BackupPath) Storage Device

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.

Checking "Keep X Number of Successful Backups" will keep X number of successfully completed backups.

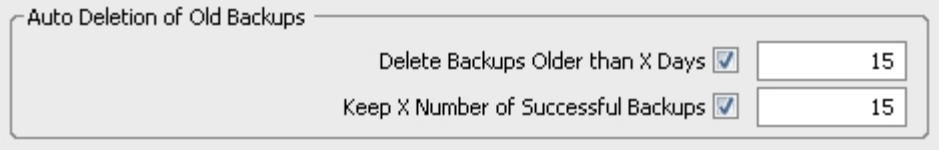


Fig. 5 - Auto deletion of old backups.

A successful backup is defined as a backup with no errors.

Example: If the device is only to keep 15 successful backups, after the 16th backup the oldest one will be deleted.

This option can be combined with the "Delete Backups Older than X Days" option.

Example: The "Keep X Number of Successful Backups" takes precedence over "Delete Backups Older than X Days" if there is a conflict. Once the required number of successful backups have been kept, older backups for the specific device are deleted based upon their age.

Both features can be overridden to perform the deletion prior to the backup taking place via "Manage" / "General" / "Advanced" and checking the box "Perform the AutoDelete prior to the operation." Only recommended if storage device is running low on space.

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:

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

Cloud Devices

NOTE: To use a cloud device you will need to already have an account with one of the public cloud providers: Amazon S3, Rackspace, Microsoft Azure, Google Cloud Storage, HP Helion, Internap, or a private OpenStack setup.

To define a cloud device you will need to know the provider you are using along with:

- Region – Named set of resources in a geographical area.
- ID – Used in conjunction with the Secret key to cryptographically sign programmatic requests to identify the sender and prevent the requests from being altered.
- Secret – Key used in conjunction with the ID to cryptographically sign programmatic requests to identify the sender and prevent the requests from being altered.
- Bucket Name – A container for objects. If the provider is Amazon, bucket names must be UNIQUE across ALL AWS users, so use a naming scheme that will not conflict with any other users' bucket names.
- Path for Device – The subfolder(s) to store files.
- Endpoint – A URL that identifies a host and port as the entry point for a Web service.

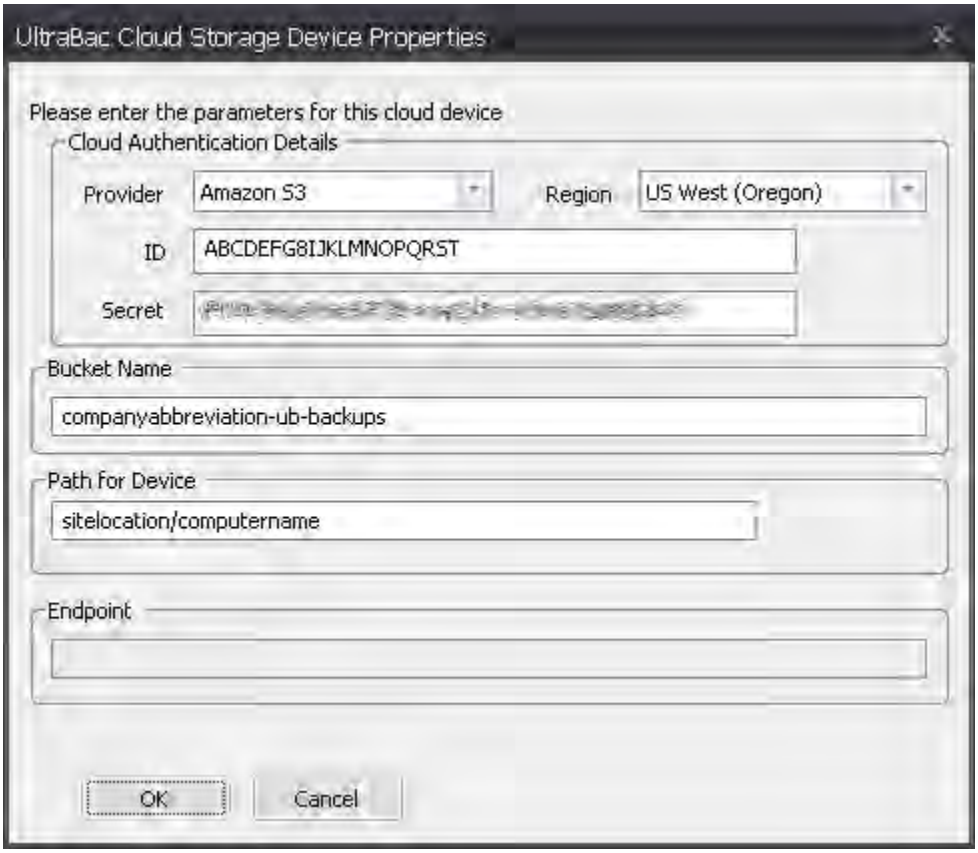


Fig. 6 - Creating cloud device.

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 device name in the "Device Information" "Description" 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 output file size in the "File Limit MB" field.
8. Change the Port field if TSM server has been changed from the default 1500 port number.
9. Enter the Folder (high-level name) to use for backup in the "Folder" field. Recommended to leave blank on new devices.
10. Enter a "Node" name and "Filespace" under Advanced Properties.
11. Click on "OK."

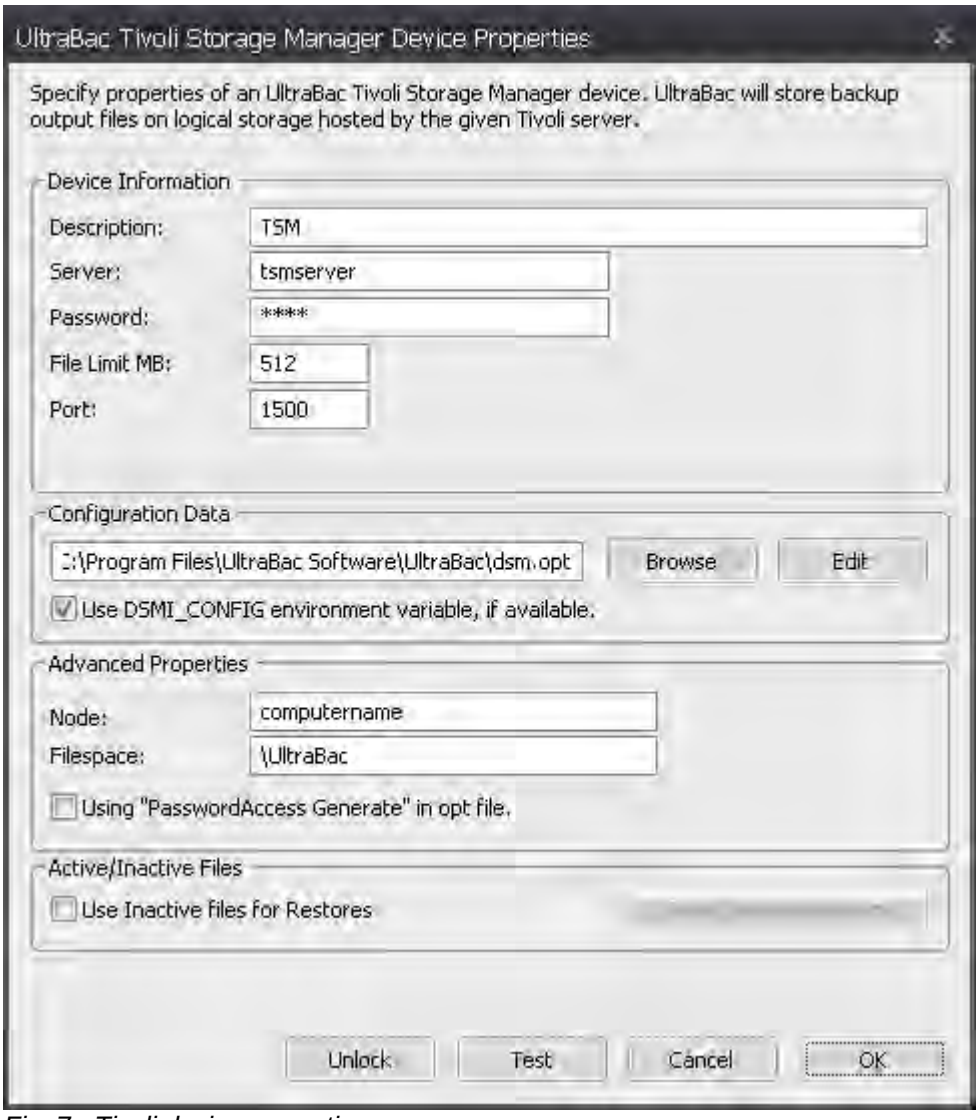


Fig. 7 - Tivoli device properties.

Configuration Data

- 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 checked, overrides the above path.

Advanced Properties

- 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.
- Using "PasswordAccess Generate" in opt file.

Active/Inactive Files

- Use Inactive files for Restore – To make use of TSM's file versioning, it is recommended to "Clear Storage Media" which for TSM devices marks all active files as inactive rather than actually clearing the storage device. Check this box to enable "Select Inactive Versions" to chose an inactive backup index to restore from.

Advanced Options

The Tivoli devices have global available advanced options that are found via "Manage" / Options "Storage Devices" / "Tivoli"

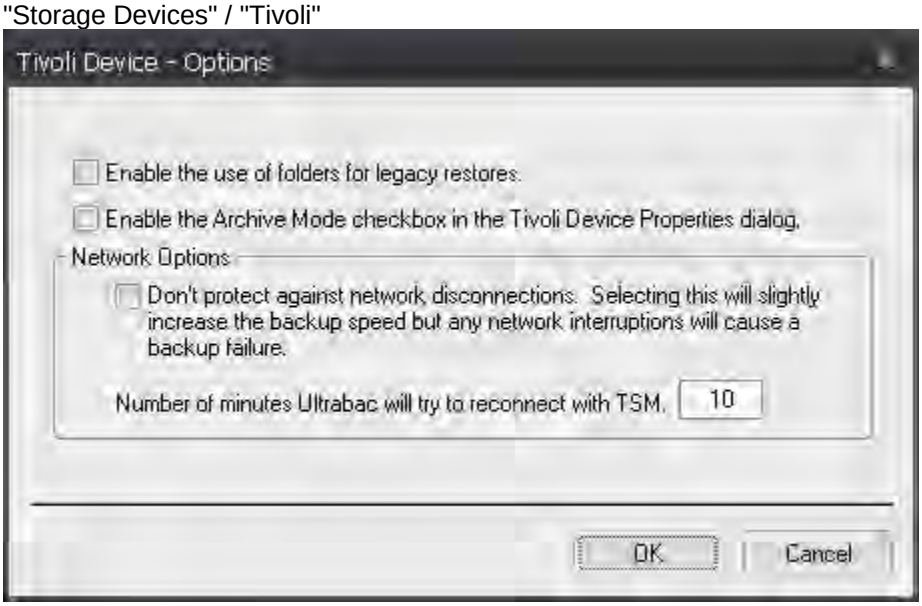


Fig. 8 - Advanced Tivoli device options.

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 off-site backup location, or to a non-Windows file storage configured to use FTP.

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."

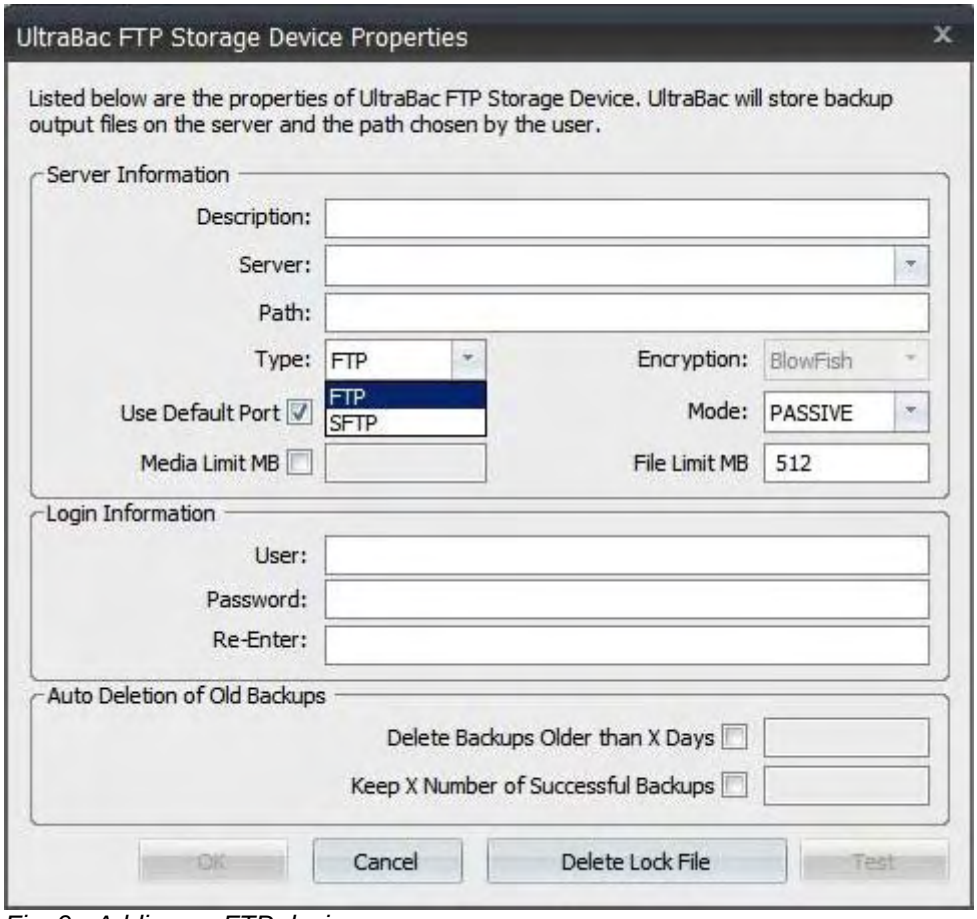


Fig. 9 - Adding an FTP device.

4. Type a 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

- 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 all data transferred to the SFTP server.

- Encryption
  - AES – Use AES encryption algorithm when writing to the SFTP serve
  - 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.
- Media Limit MB – Restrict the amount of data the device can accept to the amount (in megabytes) listed in this field.
- File Limit MB – Limit the backup output file size to the amount (in megabytes) listed in this field.
- Delete Lock File – Deletes the .ubd file that is created when the device is in use.
- Test – Establish a test connection to the FTP directory.

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.

Checking "Keep X Number of Successful Backups" will keep X number of backups with no errors reported within the "Delete Backups Older than X Days" criteria.

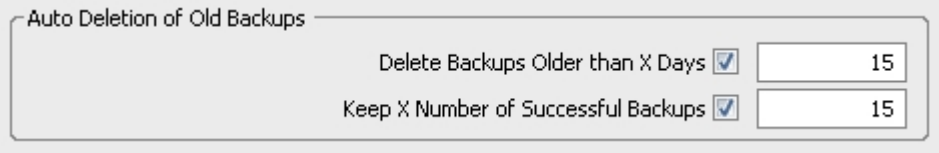


Fig. 10 - Auto deletion of old backups.

A successful backup is defined as a backup with no errors.

Example: If the device is only to keep 15 successful backups, after the 16th backup the oldest one will be deleted.

This option can be combined with the "Delete Backups Older than X Days" option.

Example: The "Keep X Number of Successful Backups" takes precedence over "Delete Backups Older than X Days" if there is a conflict. Once the required number of successful backups have been kept, older backups for the specific device are deleted based upon their age.

Both features can be overridden to perform the deletion prior to the backup taking place via "Manage" / "General" / "Advanced" and checking the box "Perform the AutoDelete prior to the operation." Only recommended if storage device is running low on space.

Remote Device

The Remote device option allows UltraBac to use any UltraBac Storage Device, including Tape drives, 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" in the "Configure" dialog box.
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. 11 - Remote device properties.

Disk and Partition Mirrors

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

- Disk Mirror – If a unpartitioned hard disk is present, it will be available for addition as an Image device.
- Partition Mirror – 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 concerning Disk Mirror and Partition Mirror devices, please visit the "**UltraBac Disaster Recovery**" section of the User Manual:

UltraBac User Manual: UltraBac Disaster Recovery

NOTE: For additional information on how to perform Static Mirror Image backups, please visit the "**Static Mirror Image Backup**" section of the User Manual:

UltraBac User Manual: Static Mirror Image Backup

Device Selection

The currently selected device is shown on the lower status 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 "Change Device" button in the "Current Device" group of the "Backup Options"



Fig. 12 - The "Change Device" button in Backup Options.

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



Fig. 13 - UltraBac Device Browser.

4. Click "OK" to select.

UltraCopy

UltraCopy is a utility used to copy the contents of one storage media device 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."

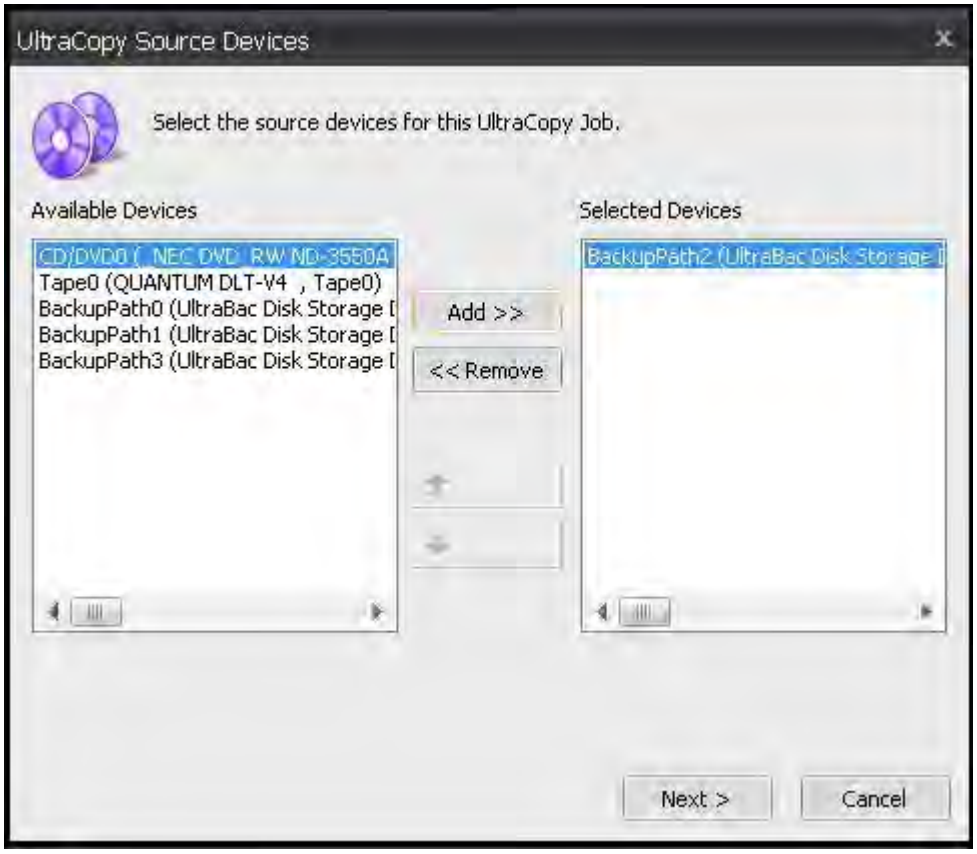


Fig. 1 - Selecting the source device.

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

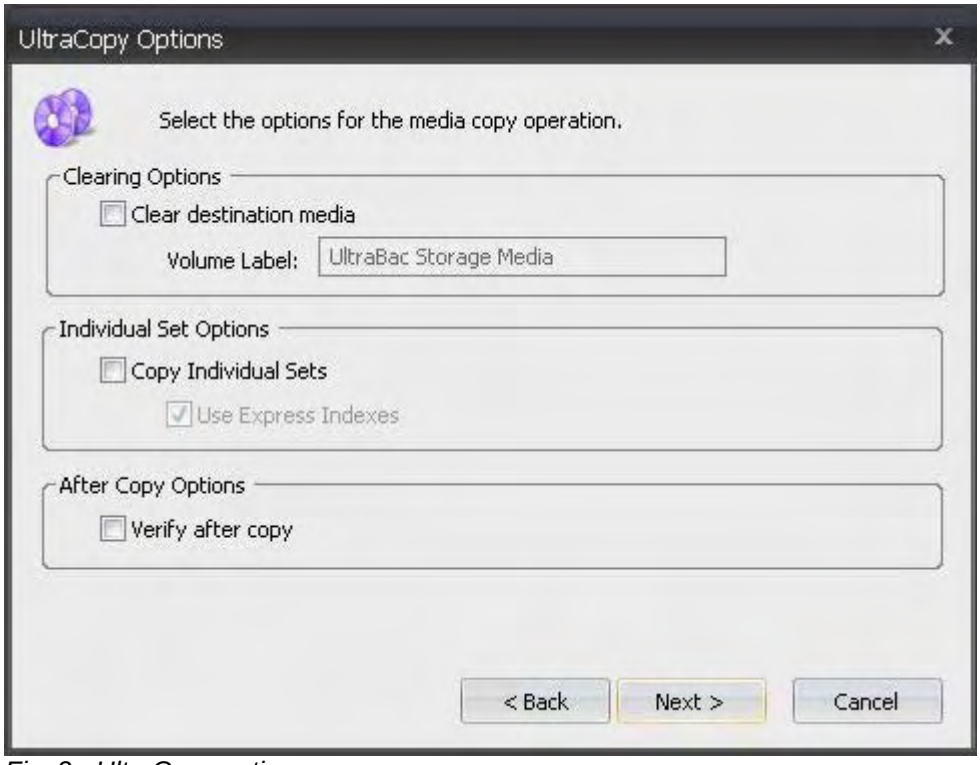


Fig. 2 - UltraCopy options.

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.

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

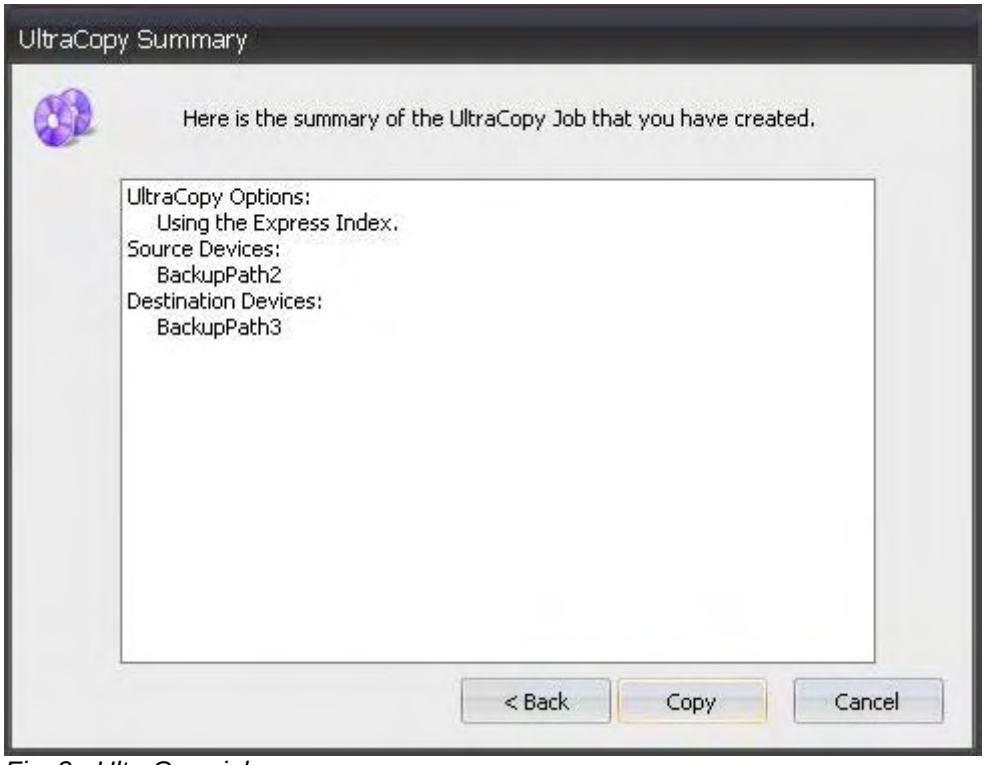


Fig. 3 - UltraCopy job summary.

Copying Individual Sets

When selected, this option allows the user to only copy specific sets to the destination media.

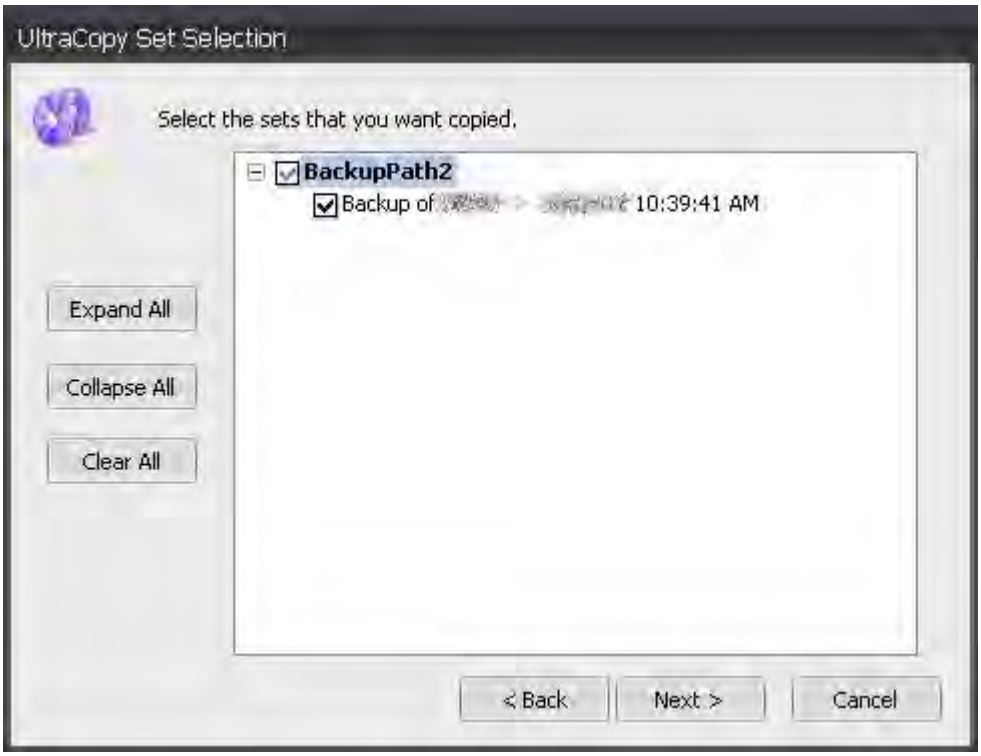


Fig. 4 - Selecting individual sets in UltraCopy.

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

Since 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.

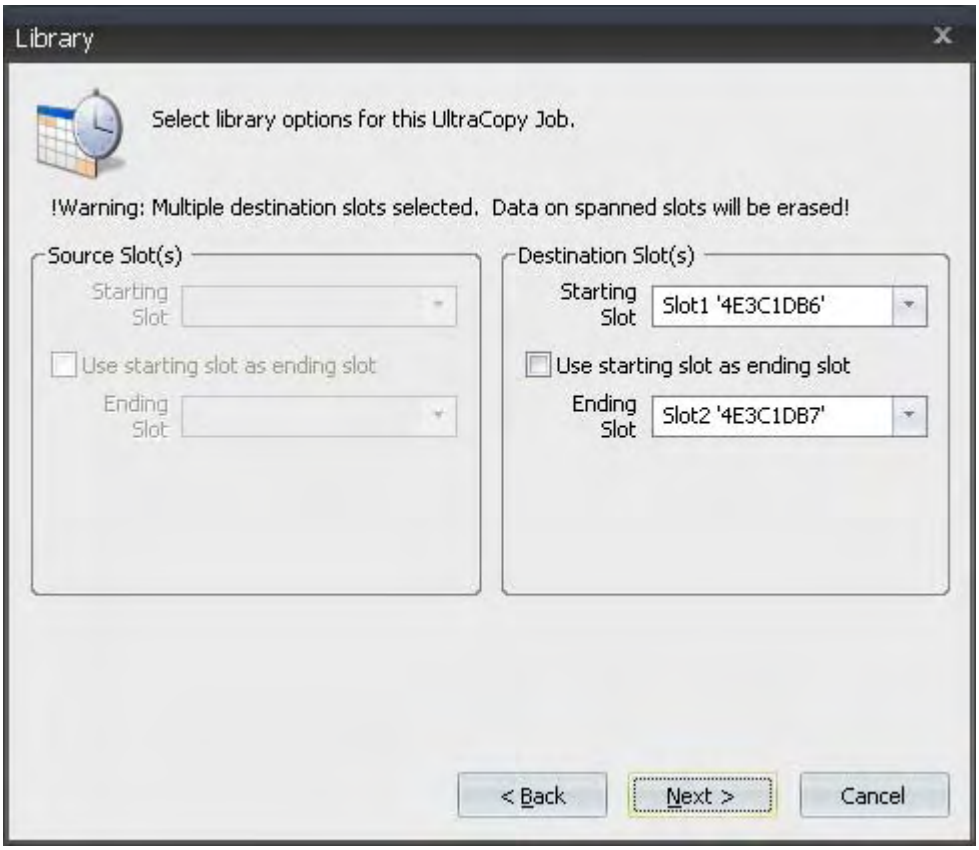


Fig. 5 - Library/Media Pool settings in UltraCopy.

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

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

COMMON COMMANDS:

- Source
  - The source device(s). (i.e. BackupPath1)
- Destination
  - The destination device(s). (i.e. Tape0)
    - Type "UBCopy.exe /DeviceFormatHelp" for help on how to use multiple devices, autoloaders, and the copying of individual sets.
- /Copy:<CopyGroup>
  - Copy using the specified set.
- /AutoResponse:<AutoResponse file>
  - Automatically respond to messages based on answers specified in the text file..
- /DecryptKey:<key>
  - The Decryption key for encrypted sets.
    - 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 individual sets
- /PrepareMedia or /pm
  - Prepare the destination media first before copying. Assigns the attached label to the device.
    - Example: /PrepareMedia:Week1
- /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
    - Media pools can only be used as destination devices.
- /Verify or /v
  - Verify the data using CRC after the copy job is completed.
- /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. Similar to /AutoResponse

AUTOLOADER COMMANDS:

- /EjectToMailSlot
  - When the job is completed, the tape will be ejected to the first empty mailbox slot.
- /EjectFromDrive
  - When the job is completed, the tape will be ejected from the drive and placed back into its previous slot.

- /RewindMedia
    - When the job is completed, the tape will be rewound. This is the default value

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:<128\192\256>
    - The Strength of the AES Phrase.

Backup Migration

UltraCopy is a utility used to copy the contents of one storage media device to another, run either manually or as a scheduled a job. Backup Migration is another utility used to automate the UltraCopy process without having to schedule an UltraCopy job and to add more options to the backup migration process.

Backup Migration has the ability to:

- Manage and monitor multiple device backup migrations.
- Skip backup migrations if a destination target device is busy, until the device is available.
- Configure alternate destination target devices if the first device is busy.
- Set how long of a delay the backup job can take before the backup migration is removed from the queue.
- Set how many backup migration jobs run at once.
- Set how many times a backup migration job can fail before it is removed from the queue.

Backup Migration jobs go into a Backup Migration queue. The queue manages the sorting and running of jobs based upon the Backup Migration options chosen. You will be able to queue jobs in a few ways:

- Automatically after a Scheduled Backup Job finishes. The settings for configuring are found on the Options tab in the "Backup Group Properties" of the Scheduled Backup Job.
- Automatically after an ad hoc (single) Backup Job. The Backup Migration option will be appear in a dialog box after you select the files to backup.
- Manually add a job to the queue via the Backup Migration Queue User Interface.

Many factors will determine which jobs should run:

- Backup Migration Jobs will be given a "Stale" number. This number will indicate how long a Migration Job will sit in the queue before it is removed.
  - Scheduled Backup Jobs will have a stale number based on how often the Backup Job is scheduled.
  - The stale number for manually created jobs can be entered by the user. The closer the stale date is, the higher priority that job will receive.

- Priority of Backup Migration Jobs is also determined by what devices are currently in use. If a device is in use, Migration will skip it, until the device is available, unless a fail-over device is defined.

- You will have the option to specify how many jobs to run at once since running multiple UltraBac jobs can impact a computers bandwidth,

Backup Migration Options



Fig. 1 - Backup Migration options.

- Turn off Backup Migration – Allows you to disable migration
- Remove Jobs After Stale date – Allows the migration queue to clear expired jobs
- The default number of days before a job becomes stale – allows you to change default setting
- The maximum number of concurrent jobs – Sets how many copy processes can run at once
- The maximum number of times a Job can fail before being canceled – Allows the migration queue to cancel any job that has failed X amount of times preventing migration getting stuck in a loop.

Creating Migration Pools

To create a migration pool:

1. Select "Tools"/"Backup Migration"/"Add / Edit Migration pools."



Fig. 2 - Backup Migration menu.

2. Click the "New" button.

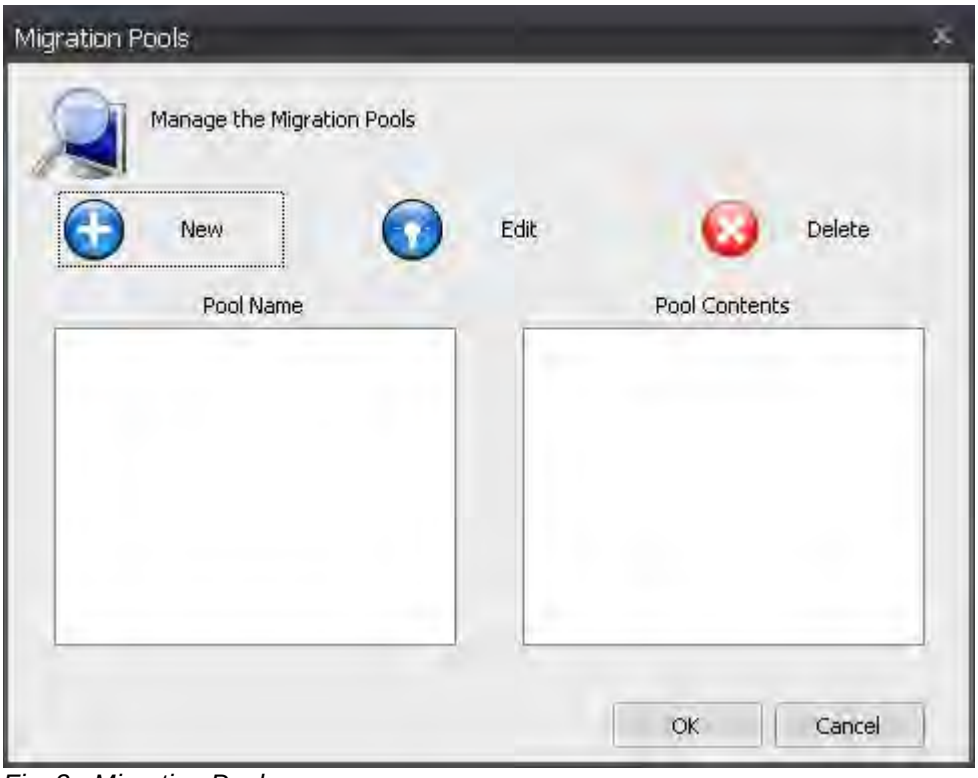


Fig. 3 - Migration Pools.

3. Type in the name you want to call the migration pool, select the devices you want added to the migration pool automatically, and click the “OK” button.

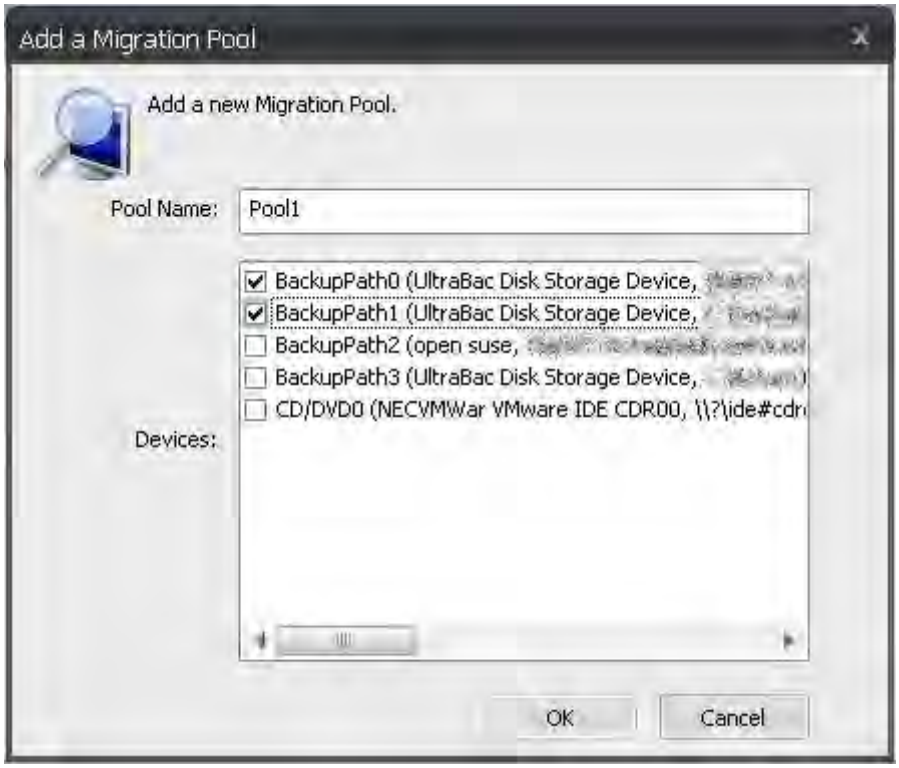


Fig. 4 - Add a migration pool.

Adding Backup Migration Jobs Manually

To add a Backup Migration Job to the Migration queue manually:

1. Select "Tools"/"Backup Migration"/"Add Backup Migration Job."



Fig. 5 - Backup Migration menu.

2. Choose an available source device and click "Add >>" to add the device as a selected source device. Click "Next."

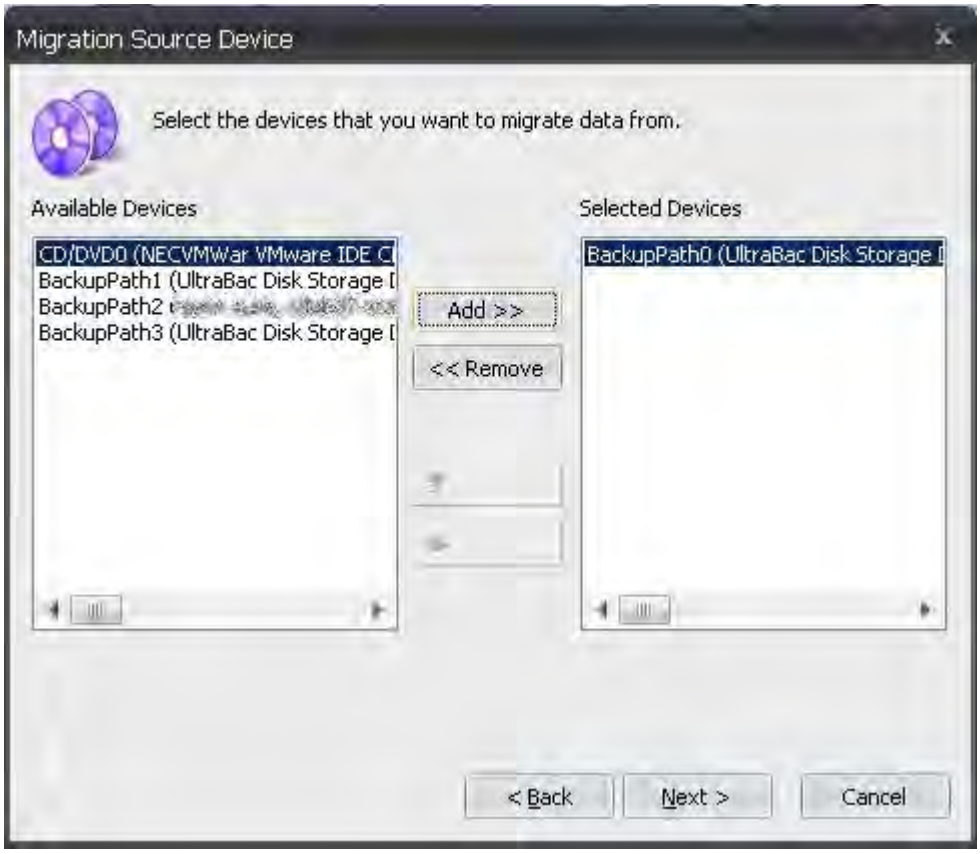


Fig. 6 - Migration source device.

3. Select the Migration pool you want to use, or create a new migration pool (see section on Creating Migration Pools), and click "Next."

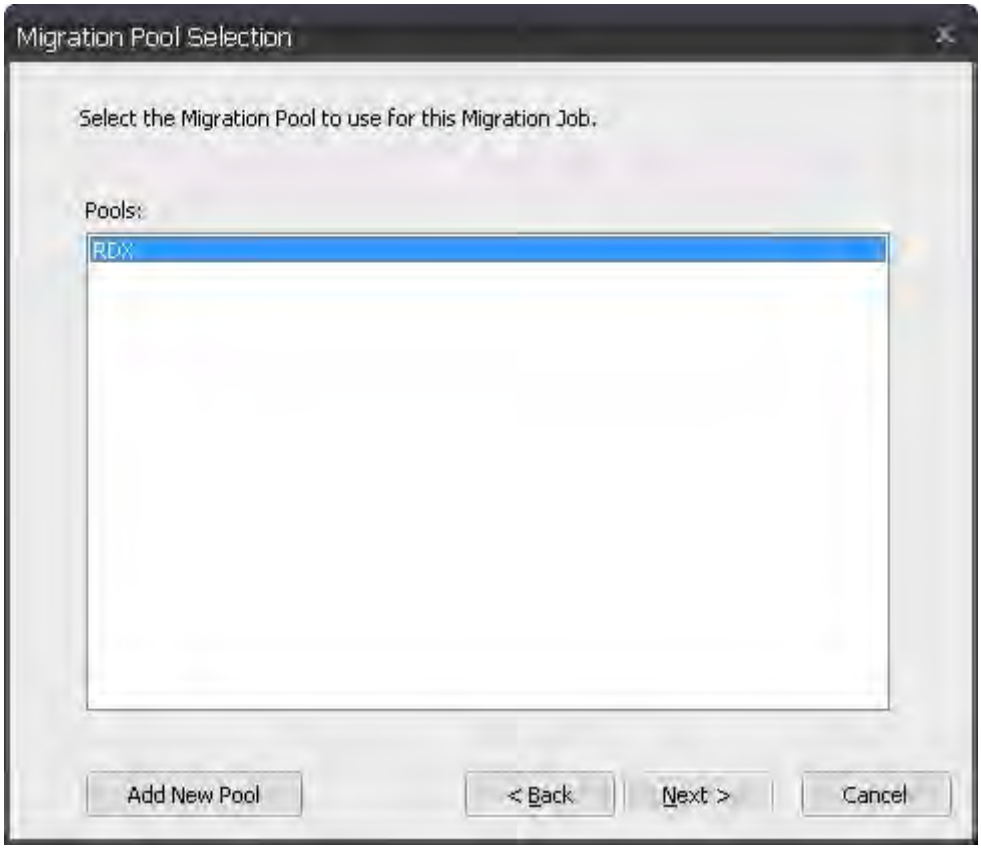


Fig. 7 - Migration pool selection.

4. Select the Backup Migration Options for the job and click "Next."

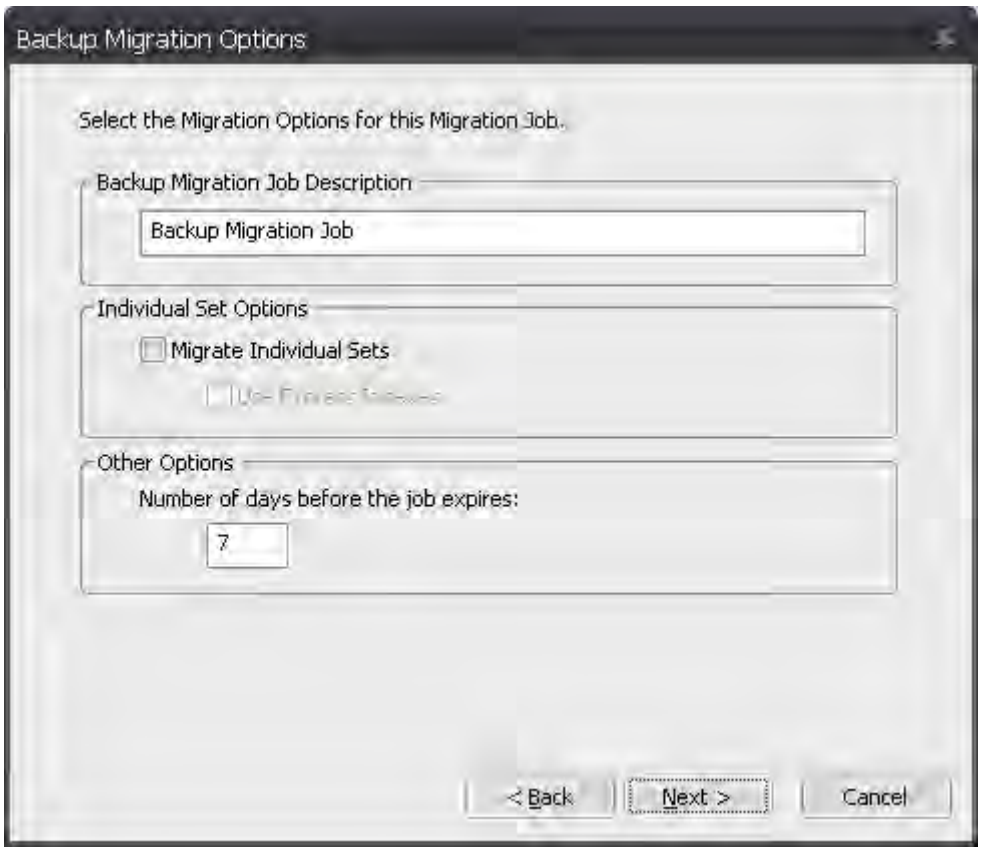


Fig. 8 - Backup migration options.

- Backup Migration Job Description – give the job a description name.
- Migrate Individual Sets – allows you to select specific backups to migrate.
  - Use Express Index – saves time when loading sets from tape media.
- Other Options – define the number of days a job can sit idle before the job expires and is deleted from the queue.

5. A summary screen of your Backup Migration Job configuration will appear. Click "Migrate" to schedule the backup migration job in the backup migration queue.

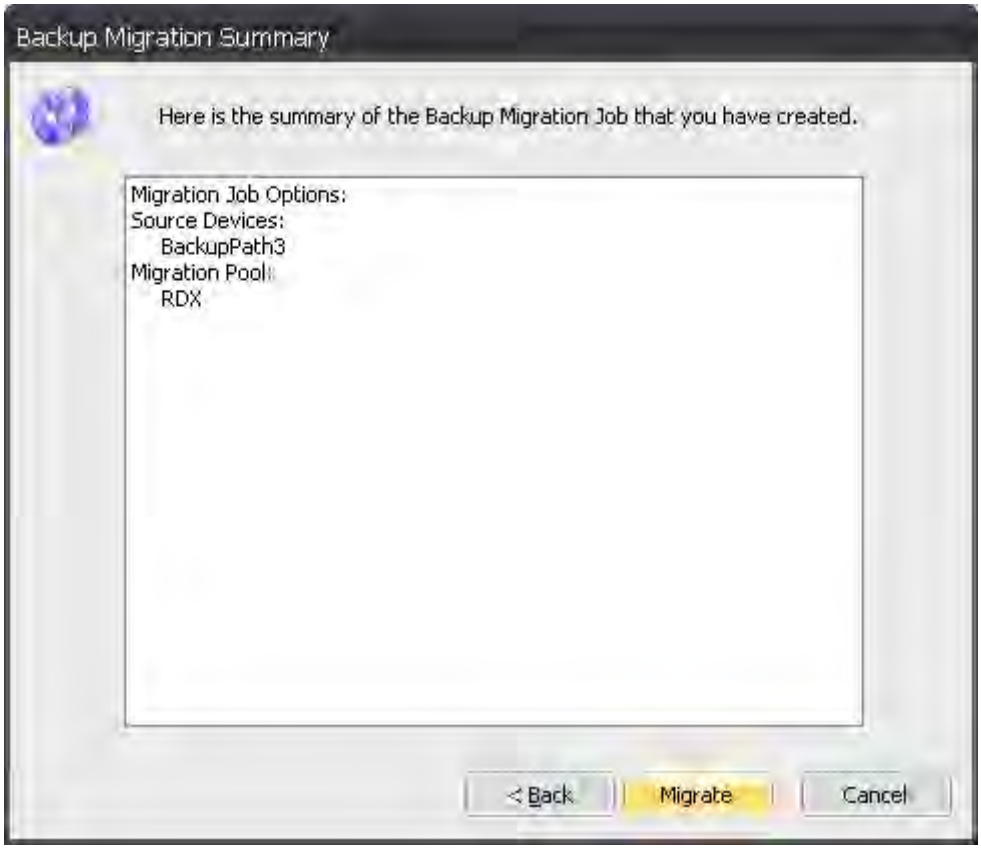


Fig. 9 - Backup migration summary.

Adding a Migration Job to an ad hoc Backup

1. Create a backup set of any agent.
2. In the Backup window, from the menu bar select "Action"/"Run backup now" and you will see the Backup Options including the options for "Migration Job."

    - Choose the migration pool that will be used for this migration job and the days before the migration job becomes stale.

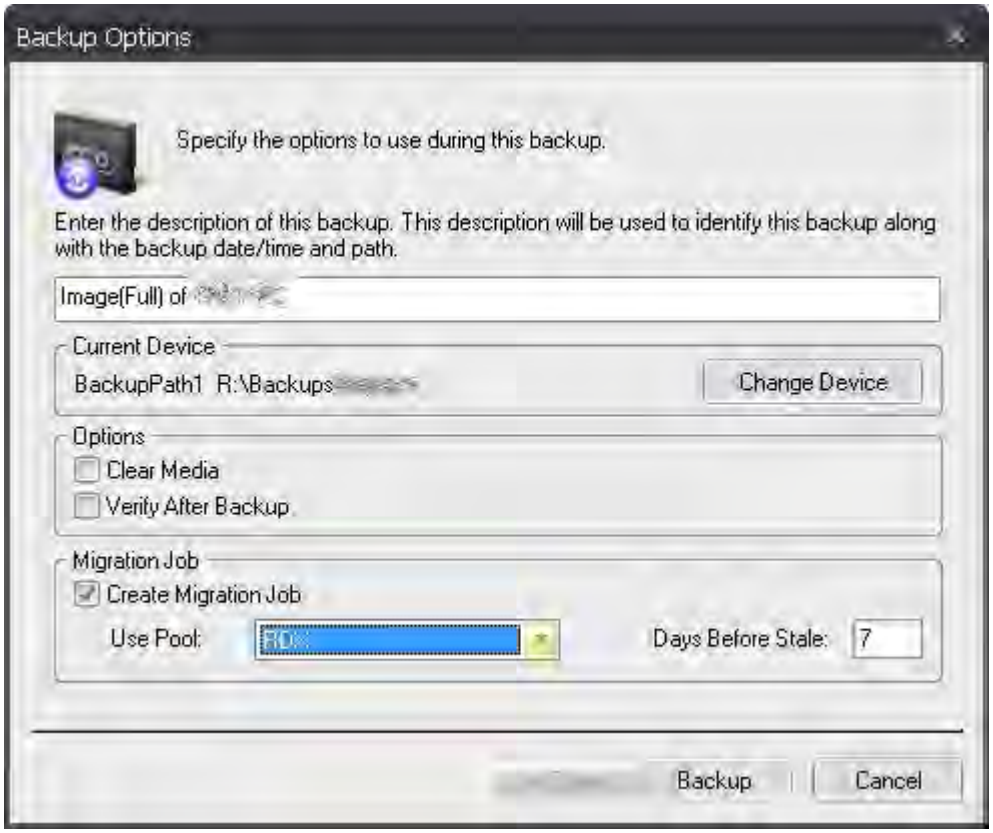


Fig. 10 - Ad hoc backup job migration options.

Adding a Migration Job to a scheduled Backup

1. Create a new scheduled job, or modify an existing scheduled job.
2. From the Properties window of the scheduled job, select the Options tab. On the Options tab, you will see the Backup Options including the options for "Migration Job."

    - Choose the migration pool that will be used for this migration job and the days before the migration job becomes stale.

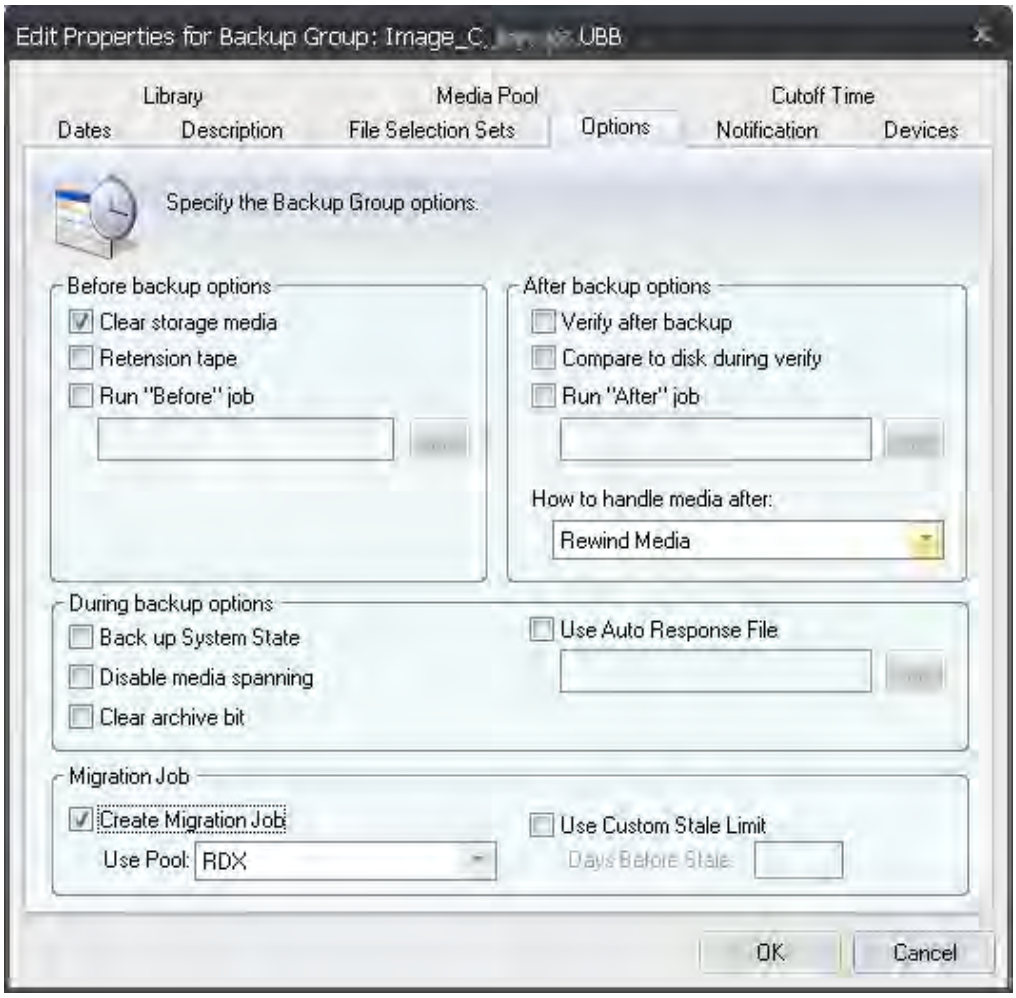


Fig. 11 - Schedule backup job migration options.

Viewing Active Migration Jobs

To view the Migration Jobs in the Migration Queue, select "View" from the menu bar, and then select "Reports"/"View Migration Queue." All of the backup migration jobs will appear in the Migration Queue.

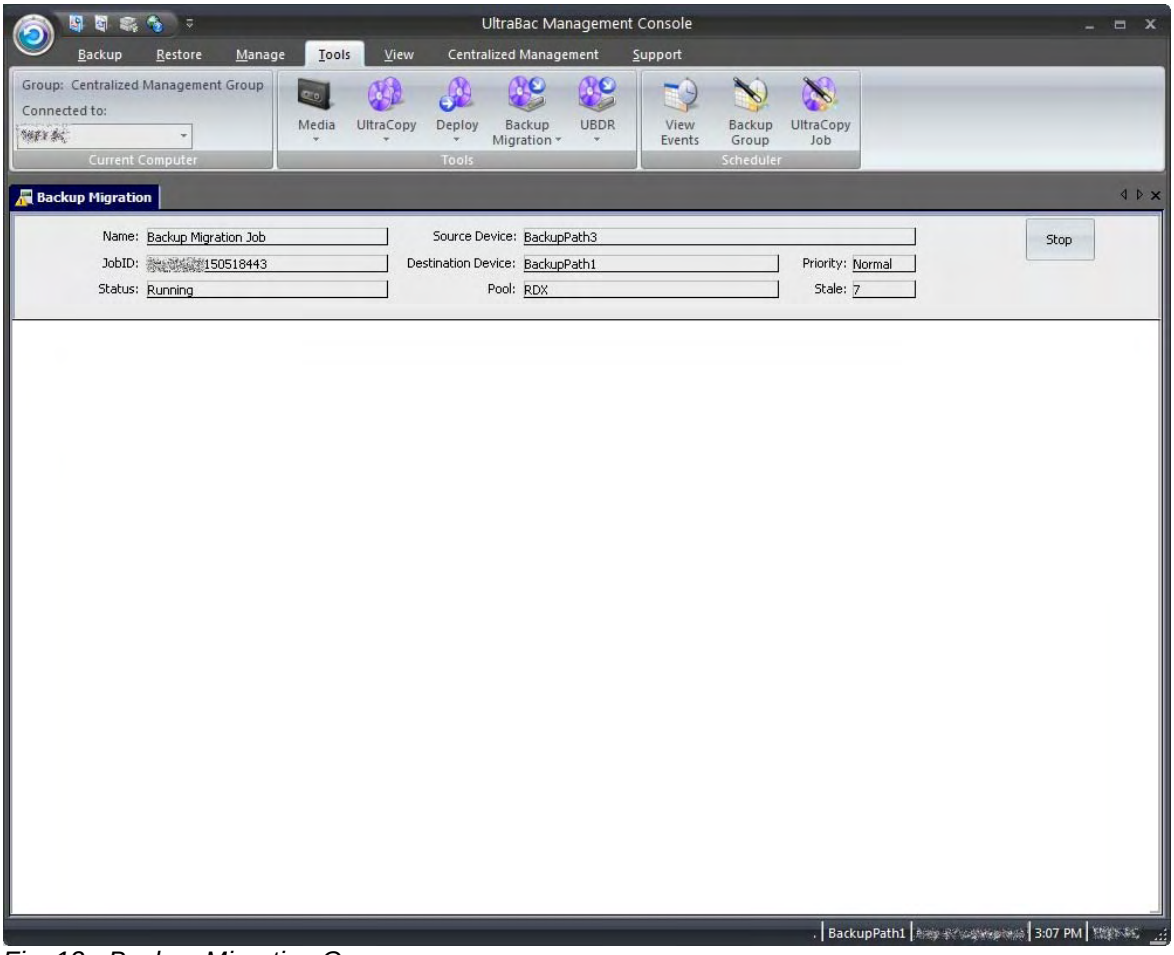


Fig. 12 - Backup Migration Queue.

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 2003/Vista/Windows 7/2008/2008R2/2012 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: The UltraBac Medium Changer device driver must be updated to the newest driver even on systems already running UltraBac and just upgrading to version 9.3. The old driver will no longer work for remote backups nor work on Windows Server 2012 servers.

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

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

2008

NOTE: For more information on unloading the UltraBac Medium Changer driver, please see the UltraBac Knowledge Base: **UBQ000195: Medium Changer Driver Unloading**

Library Configuration

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

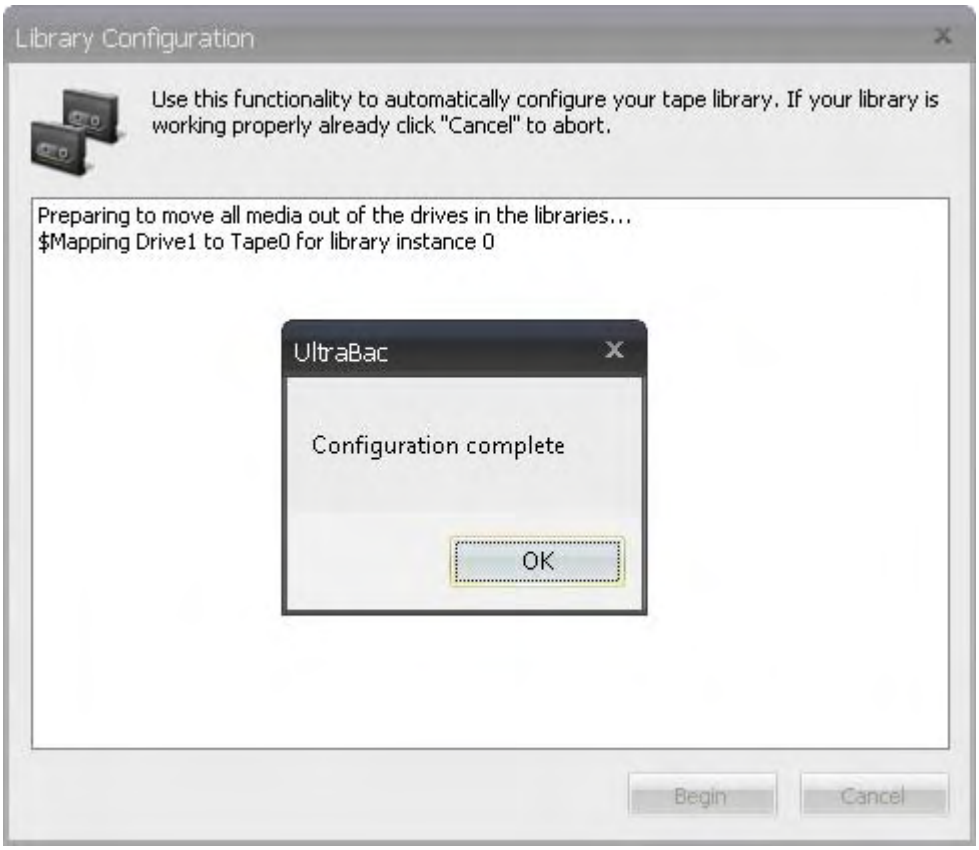


Fig. 1 - Library Configuration tool.

To use the Library Configuration tool:

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

Moving Media

First, select a tape drive as a default. To select the tape drive as the current storage device:

1. Select the Manage tab. In the Configure box on the menu bar click "Storage Devices"/"Tape."
2. Click on the autoloader's tape device to select the device.
3. Click "Close."

Then, access the media library.

1. Select the Manage tab and click "Library"/"Control Library" or press the keyboard shortcut F9. The Library Control selection is only available if the tape device is selected as the current storage device.

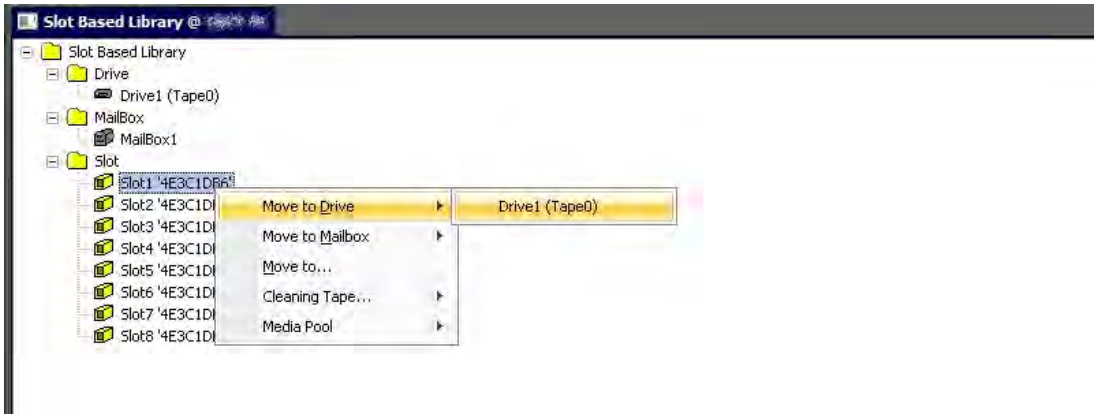


Fig. 2 - Media library controls.

From the above screen, drag and drop tapes into the Drive, Mailbox, or Slot, or right click on an object and move the tape to its destination by choosing a Slot, Mailbox, or 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, UltraBac must be installed on the remote server 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"/"Create New Pool"

3. In the Media pool name field, type a <name> for the Media Pool.
4. Click "Create"

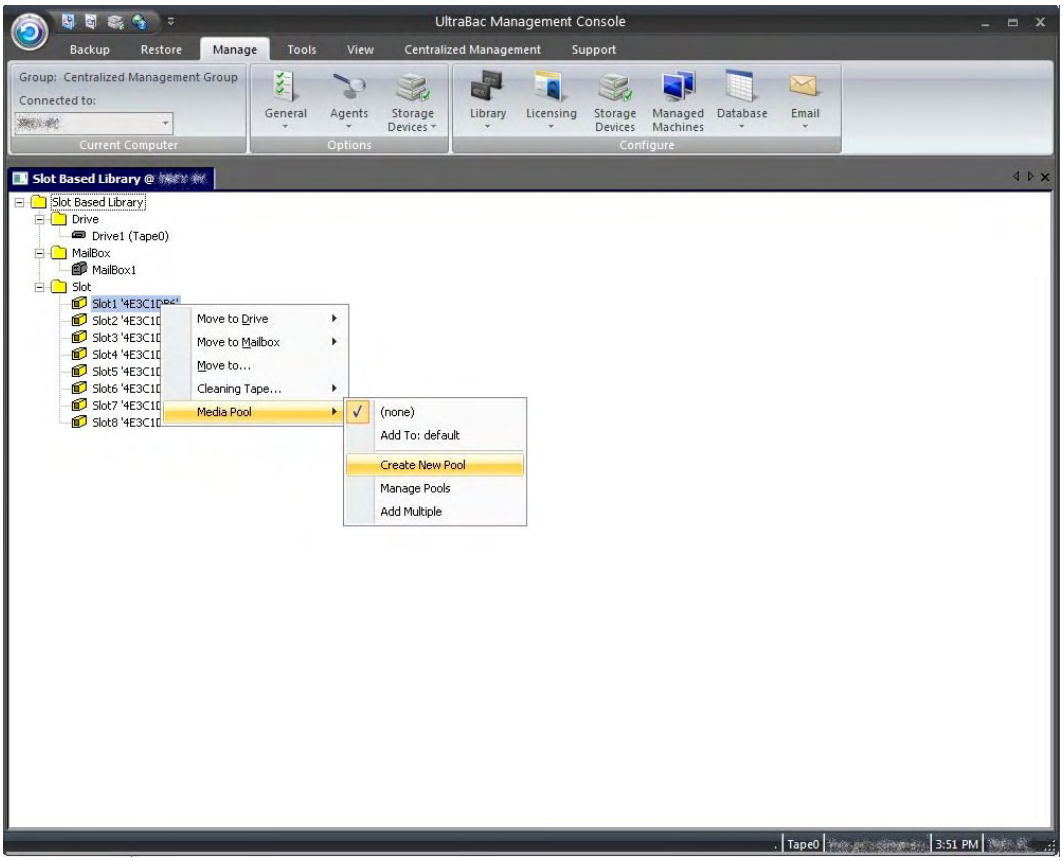


Fig. 4 - Media Pools in the Autoloader Library controls.

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.

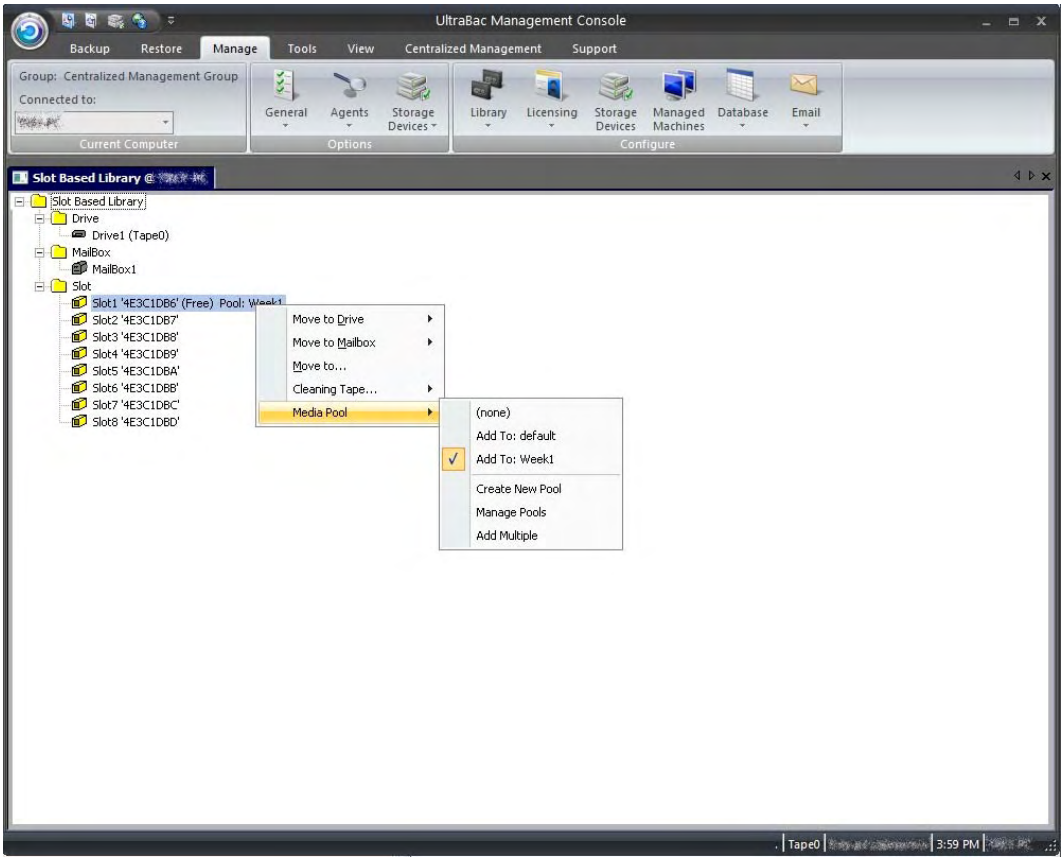


Fig. 5 - Media pool options.

- Add to: default – Adds the selected media to the default media pool.
- Create New Pool – Opens a dialog that allows a new media pool name to be specified.



Fig. 6 - Specifying the media pool name and management.

- Manage Pools – Opens the "Media Pools" maintenance screen.
- Add Multiple – Opens a screen that allows multiple tapes to be added to a media pool.

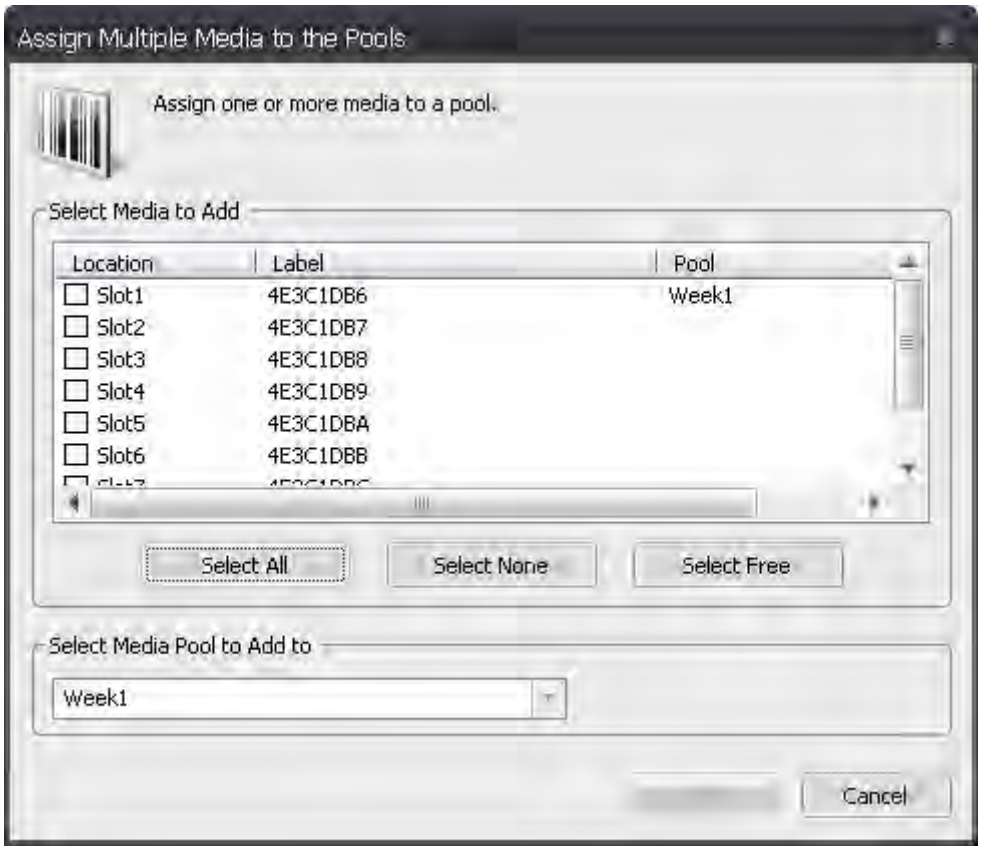


Fig. 7 - Adding multiple barcodes to a media pool.

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.

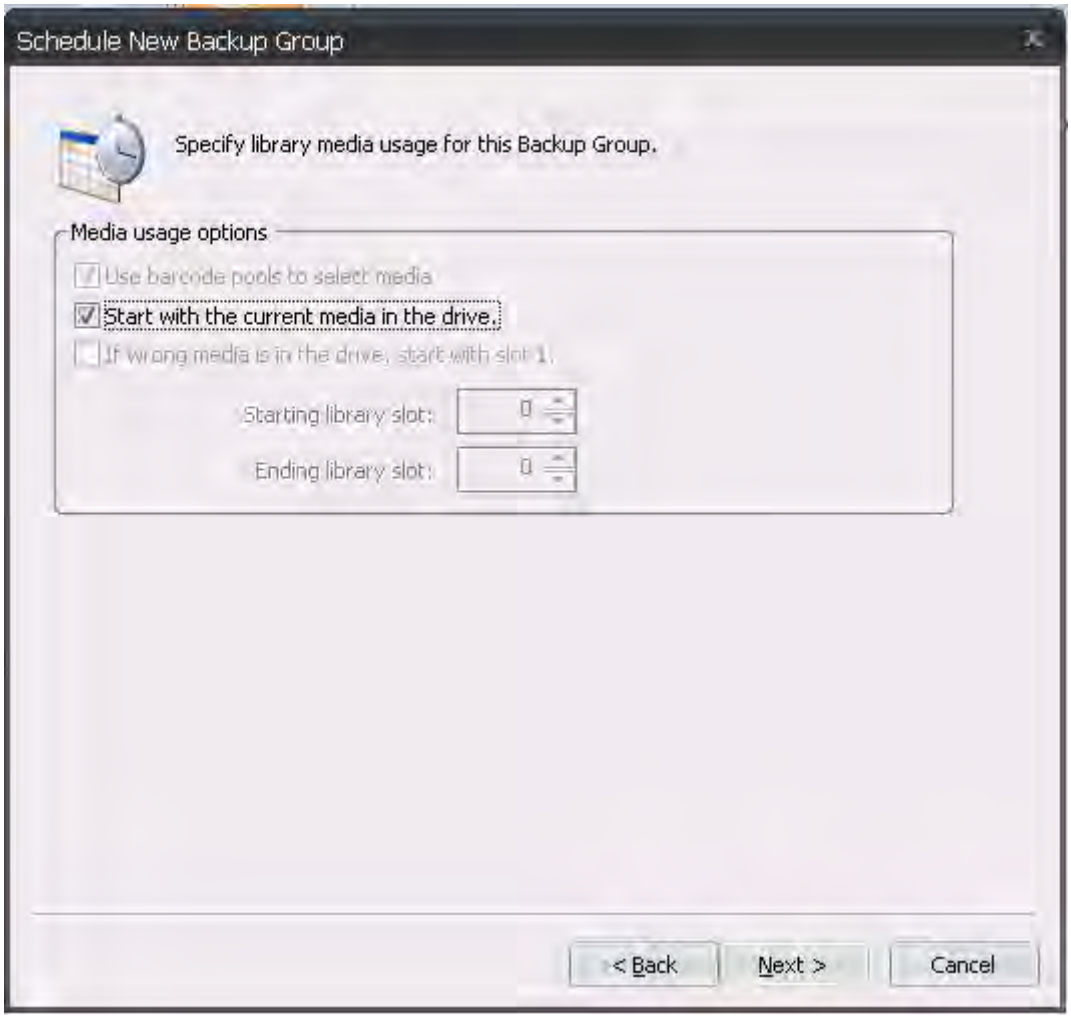


Fig. 8 - Library tab in the properties of a scheduled backup group.

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.

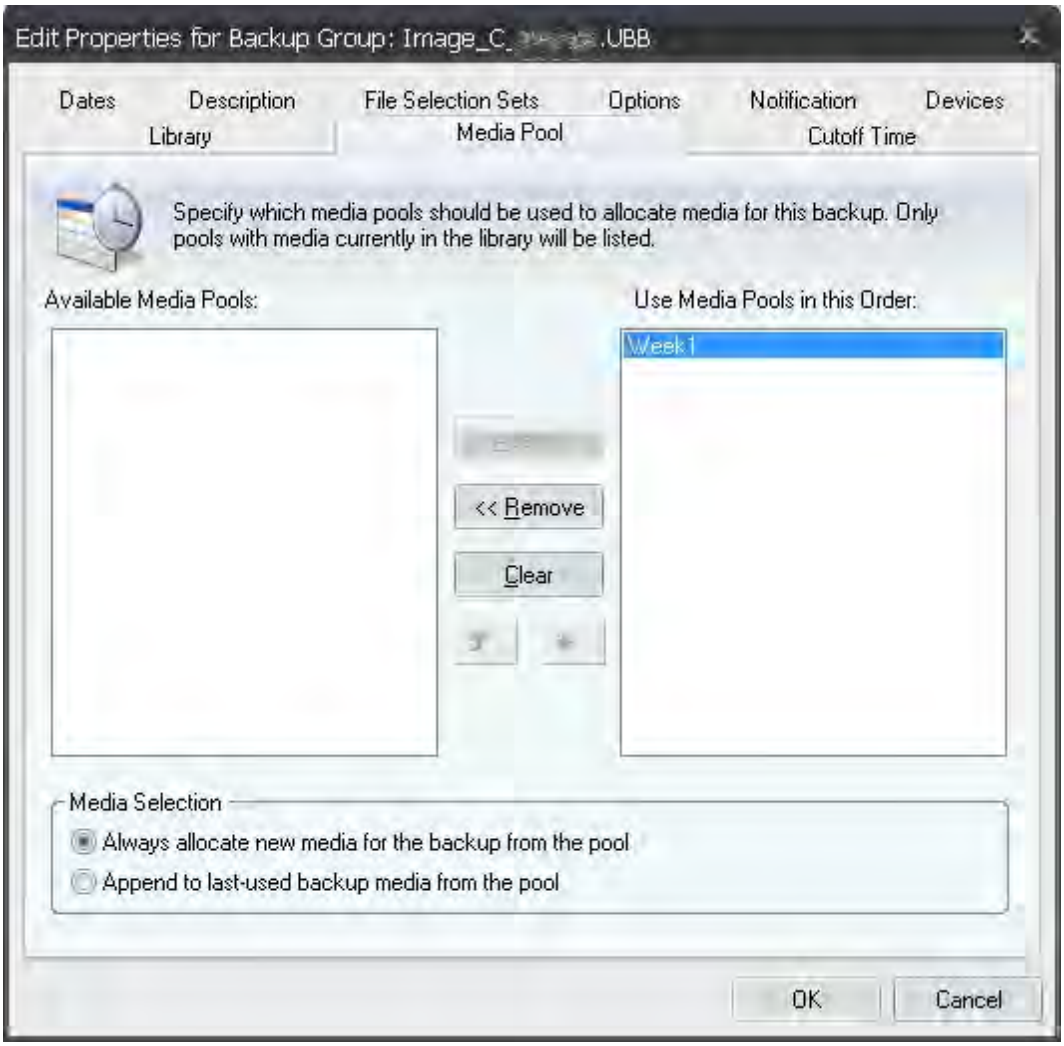


Fig. 9 - Media Pool tab in the properties of a scheduled backup group.

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"). 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 Selection 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:

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.

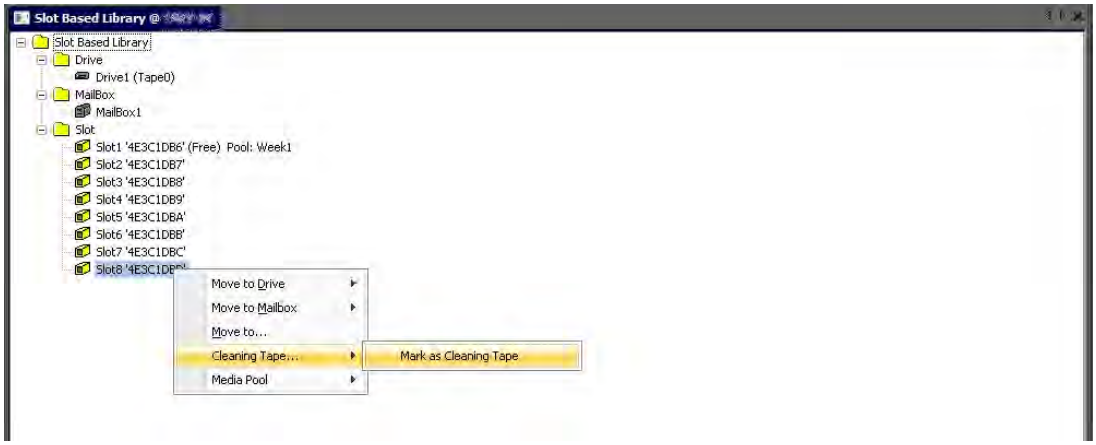


Fig. 10 - Specifying a cleaning tape.

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

To enable library AutoClean options:

1. Select the Manage tab, and click "Library"/"Autoclean Library."

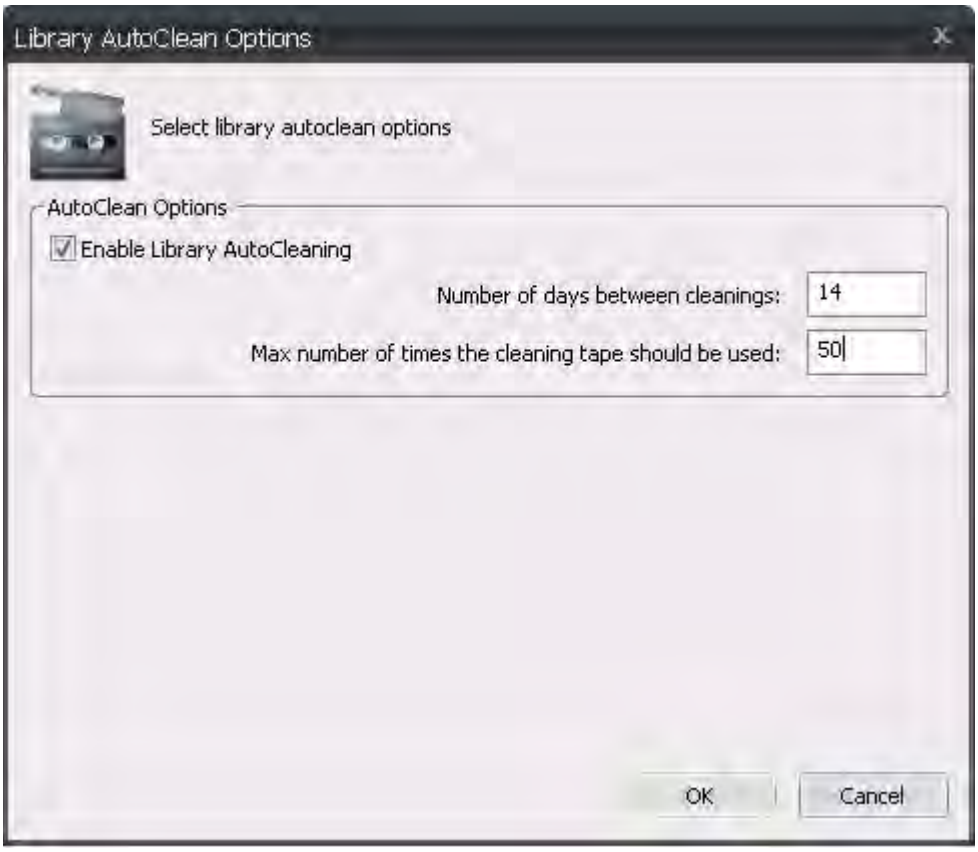


Fig. 11 - Setting the AutoClean options.

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

Requirements:

- SQL Server (MS SQL 2000+, MS SQL Express 2005+, MySQL 5.0+).
- 20GB of free hard disk space required; 50 GB recommended.
- For MS SQL either the default UltraBac account needs permissions to create users and databases, or you will need a local SQL account with those permissions.
- For MySQL you will need a local SQL account that has permissions to create users and databases.

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

UBQ000253: Configuring SQL for use with the UltraBac Database

Setting up the UltraBac Database

1. Select the Manage tab, and click "Database" / "Database Wizard."



Fig. 1 - Launching Database Wizard.

2. Then select the appropriate action. Selecting "Use an existing UltraBac Database Server" the database will be upgraded to support the new version.



Fig. 2 - Select database location.

3. UltraBac's database can be installed on MS SQL or MySQL database.

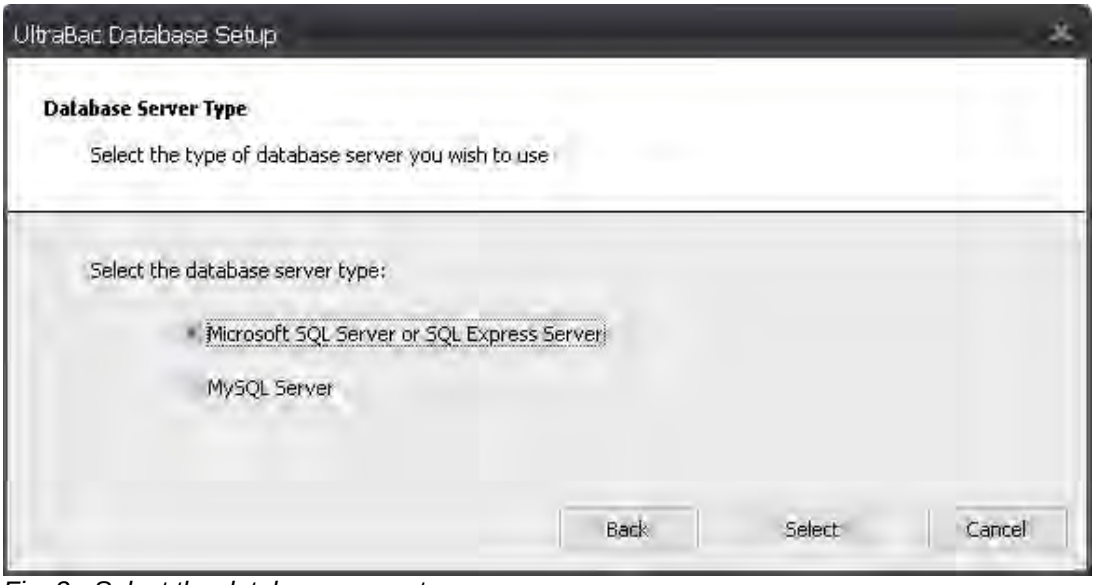


Fig. 3 - Select the database server type.

4. Enter in credentials to create UltraBac database.
    i. For MS SQL you will need the server name as well as the Instance Name. Leave the Instance Name empty if SQL was installed as the "default" instance. If the Account Type is Windows Authentication, click 'Select" and proceed to step 6; UltraBac will use the default UltraBac account for all connections to the database.
        - Once the fields are filled in, you can click "Test Connection" to connect to the database server using the supplied credentials.

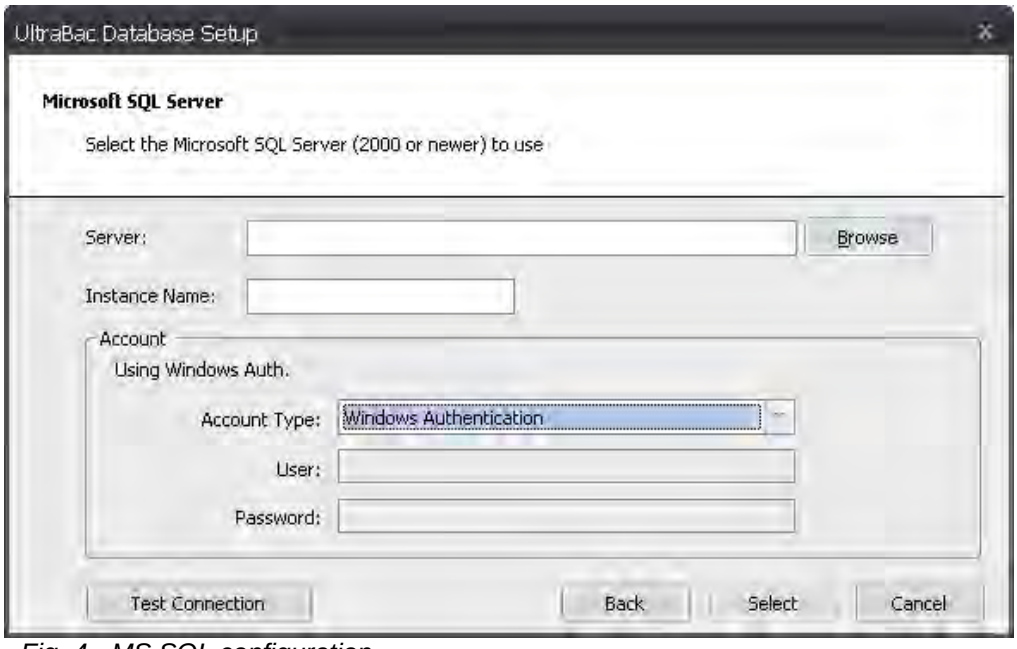


Fig. 4 - MS SQL configuration.

ii. If you are using MySQL, you will need the server name and the port number MySQL is listening on. You will also need a MySQL account credential to create the database along with the MySQL account UltraBac will use to connect to the database to update tables and run queries.

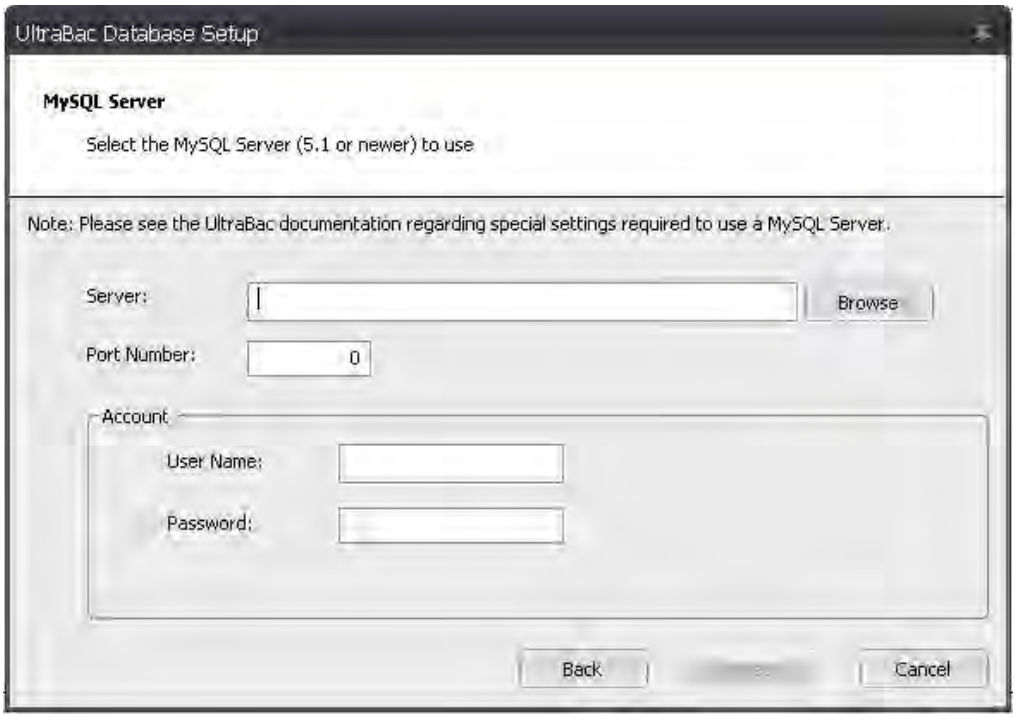


Fig. 5 - MySQL configuration.

5. Enter the account credentials UltraBac will use to connect to the database in order to upload data and run queries. Setup will create this account if it does not already exist.



Fig. 6 - Account to connect to the UltraBac database.

6. Click "OK" to complete the UltraBac database setup.

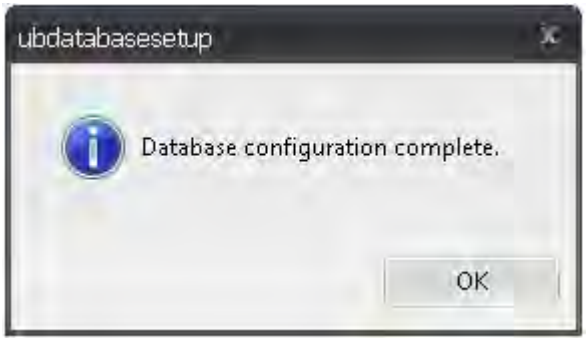


Fig. 7 - Database configuration complete.

7. Once the configuration is complete you will be prompted to add all the servers in your Managed Machine list(s) to the database.

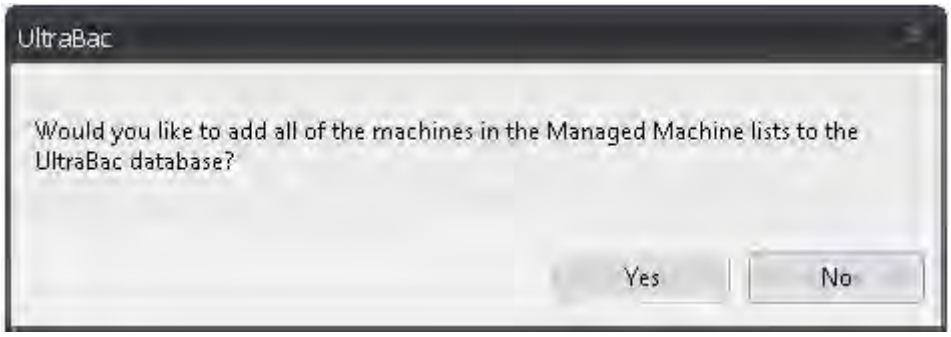


Fig. 8 - Sync Managed Machine list to the database.

8. You must add machines to the Managed Machines list and sync them up to the database before you can see any data in the "Overview" or "Machine View" options on the Centralized Management tab.

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 "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.

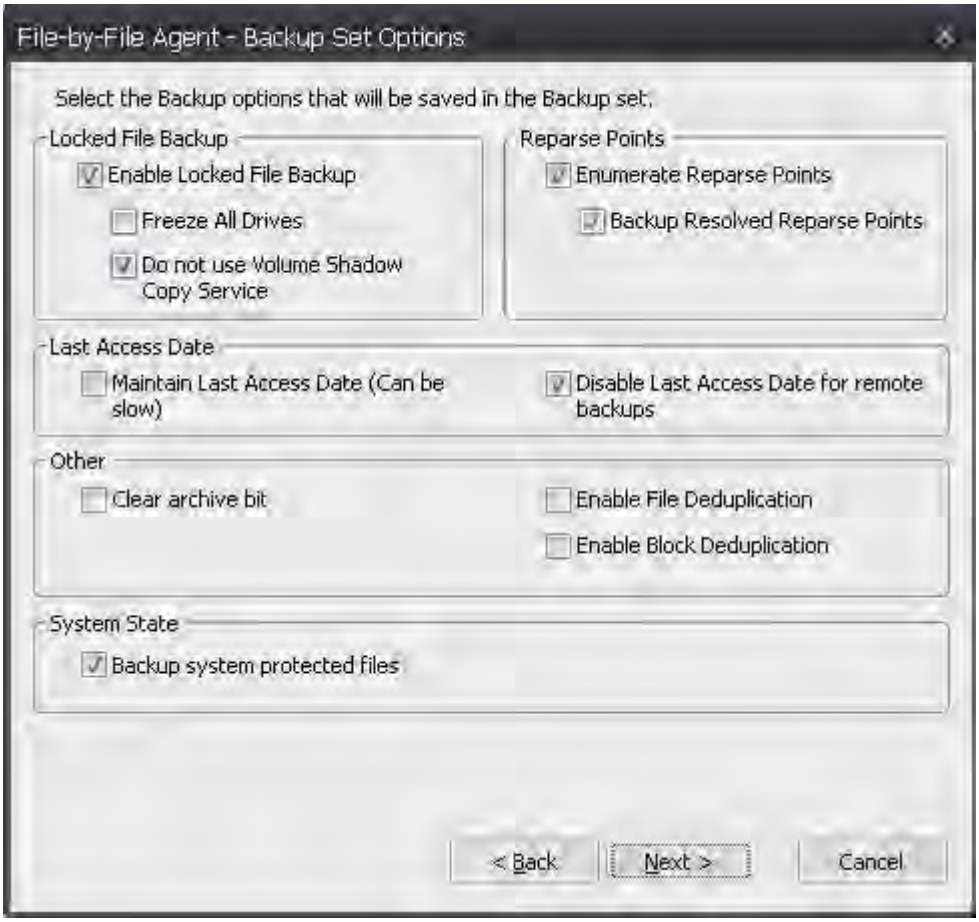


Fig. 2 - File-by-File Agent - Backup Set Options.

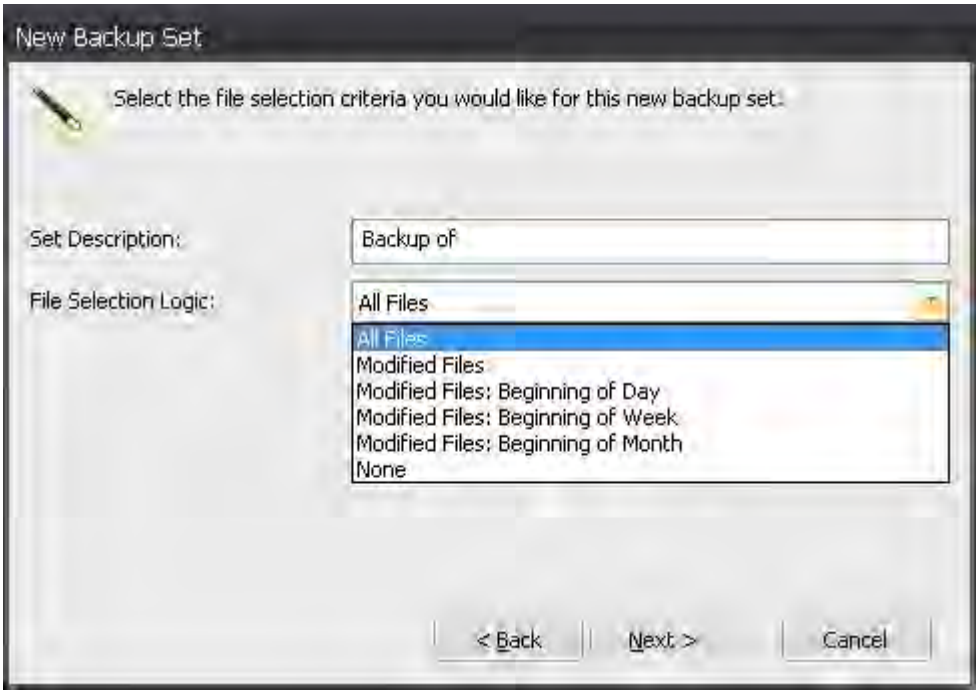


Fig. 3 - Selection criteria.

- 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, Image/Disaster Recovery Agents and Ux File-by-File/Image 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.

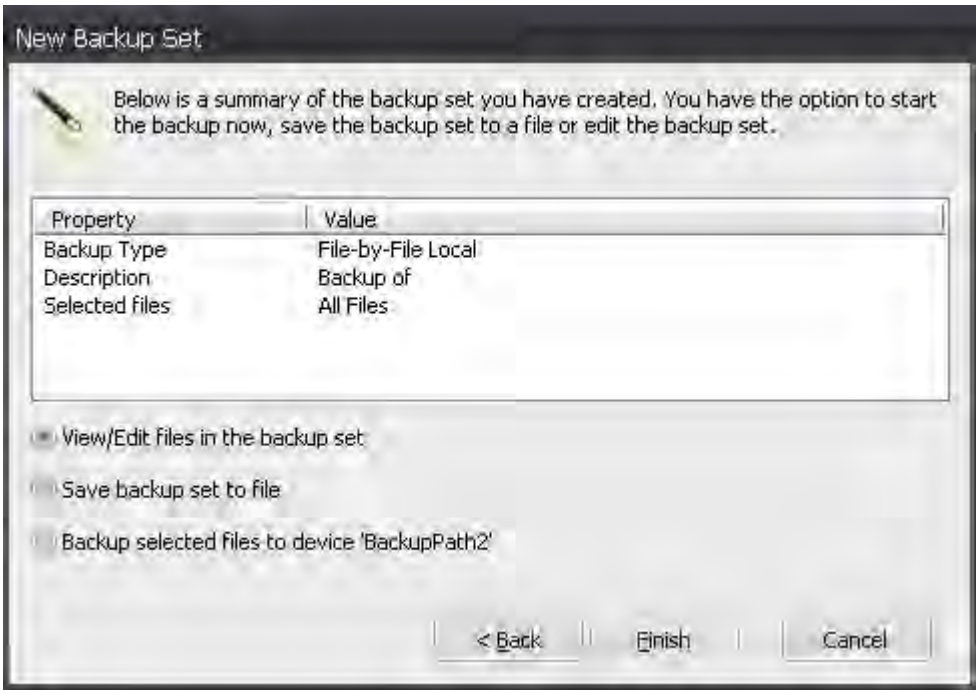


Fig. 4 - Backup Wizard summary.

- 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.

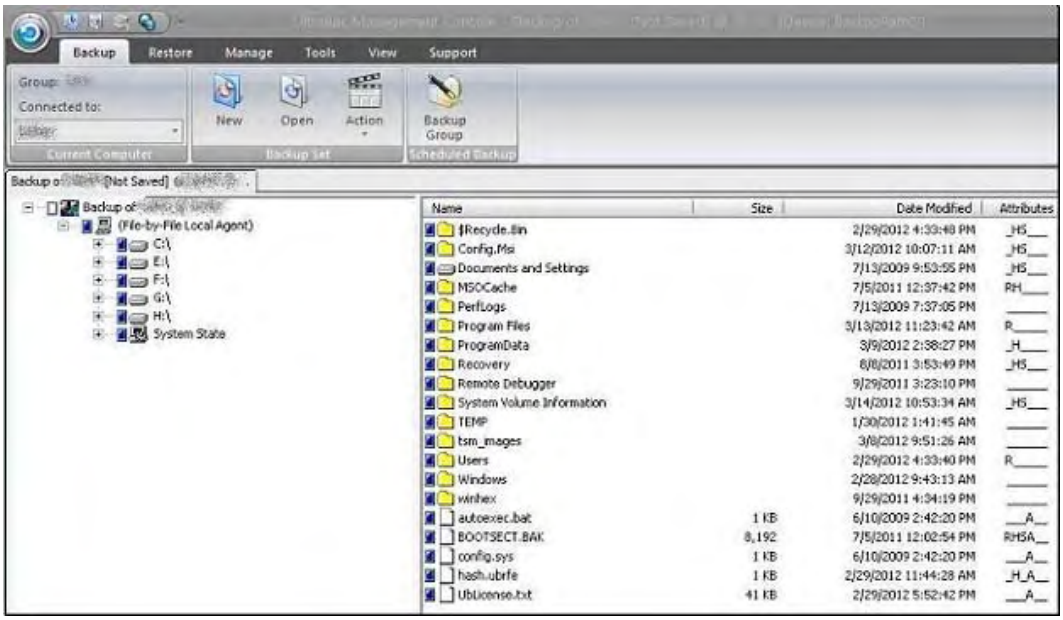


Fig. 5 - Viewing a file-by-file local agent backup set in the File Viewer.

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."

NOTE: For additional information on UltraBac backup output files, please see the UltraBac Knowledge Base:

See UBQ000210: UltraBac Backup Output Files

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."

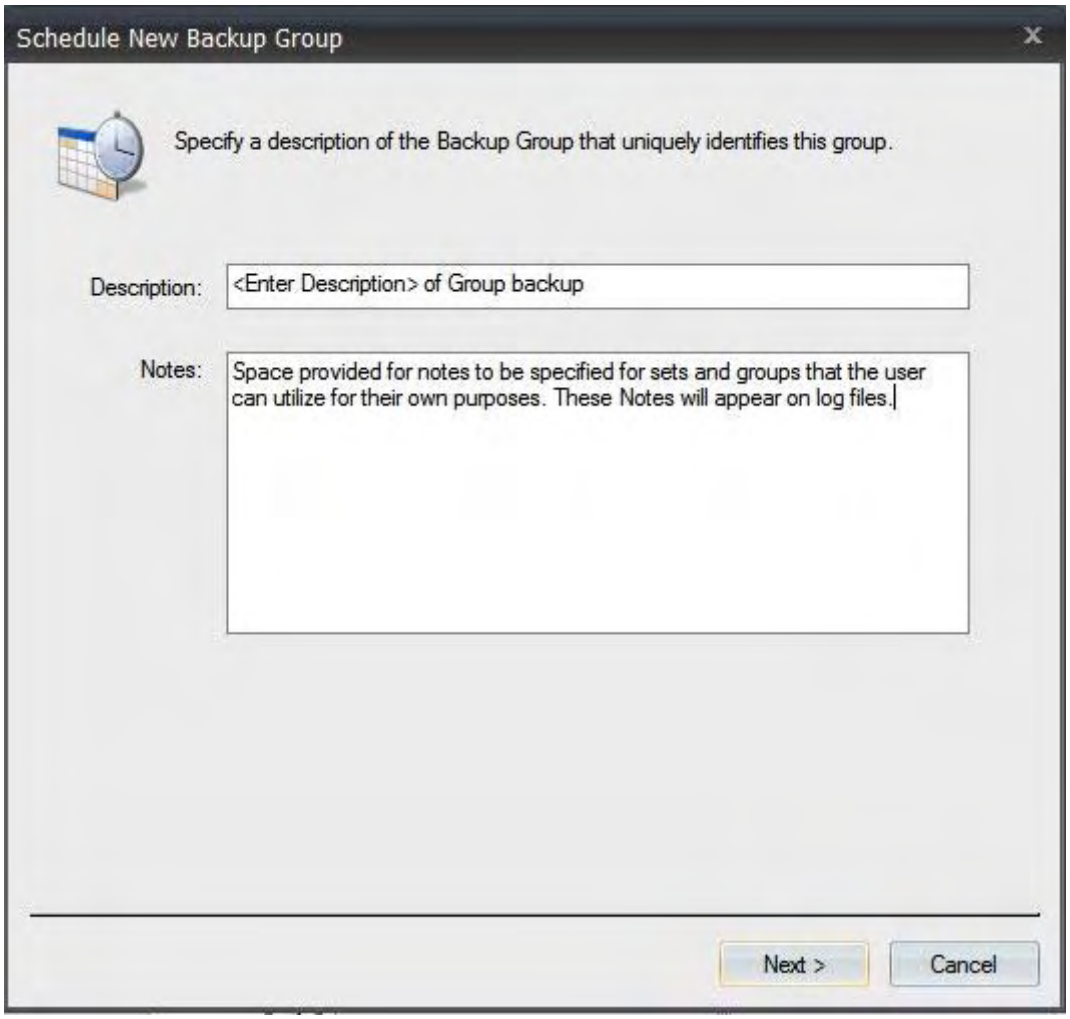


Fig. 1 - Scheduled backup description.

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."

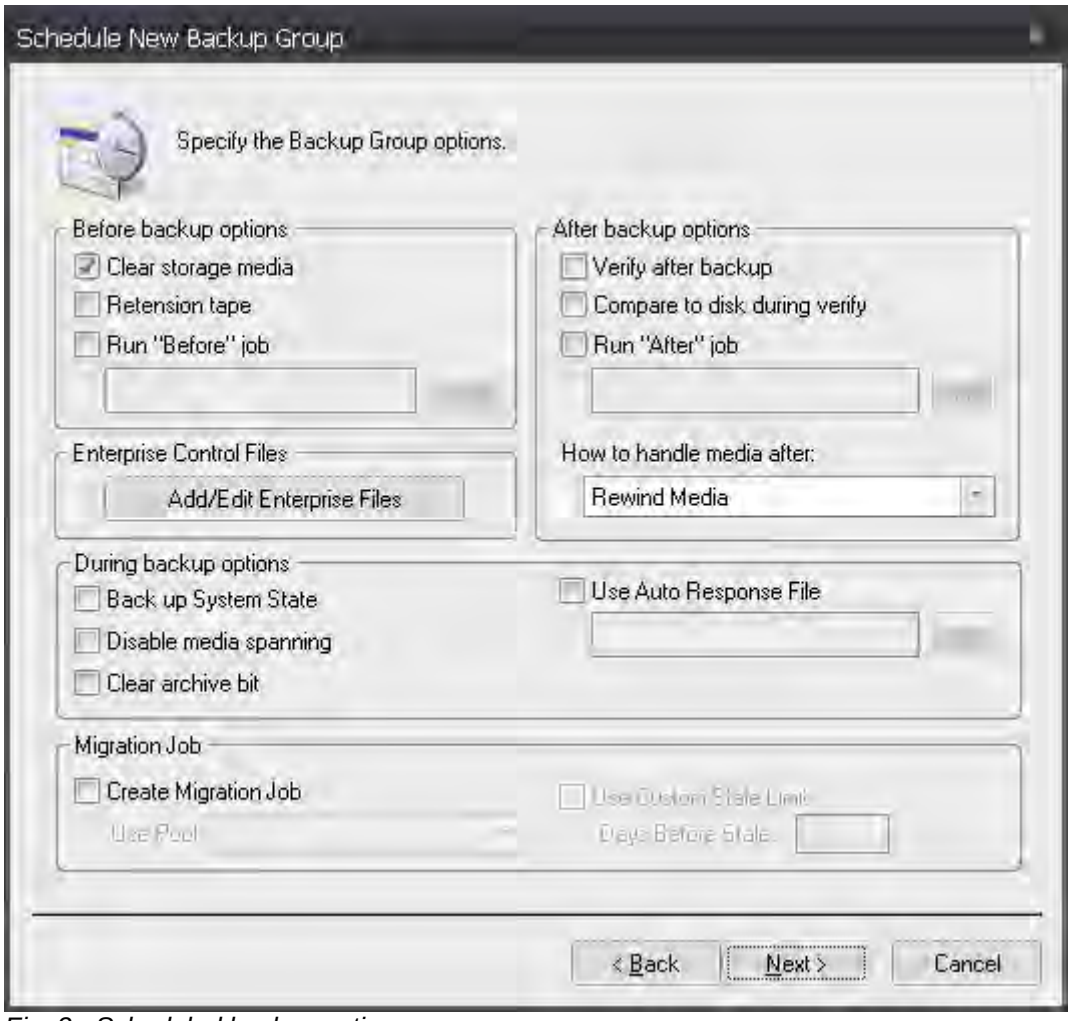


Fig. 3 - Scheduled backup options.

4. Set the notification options, and click "Next."

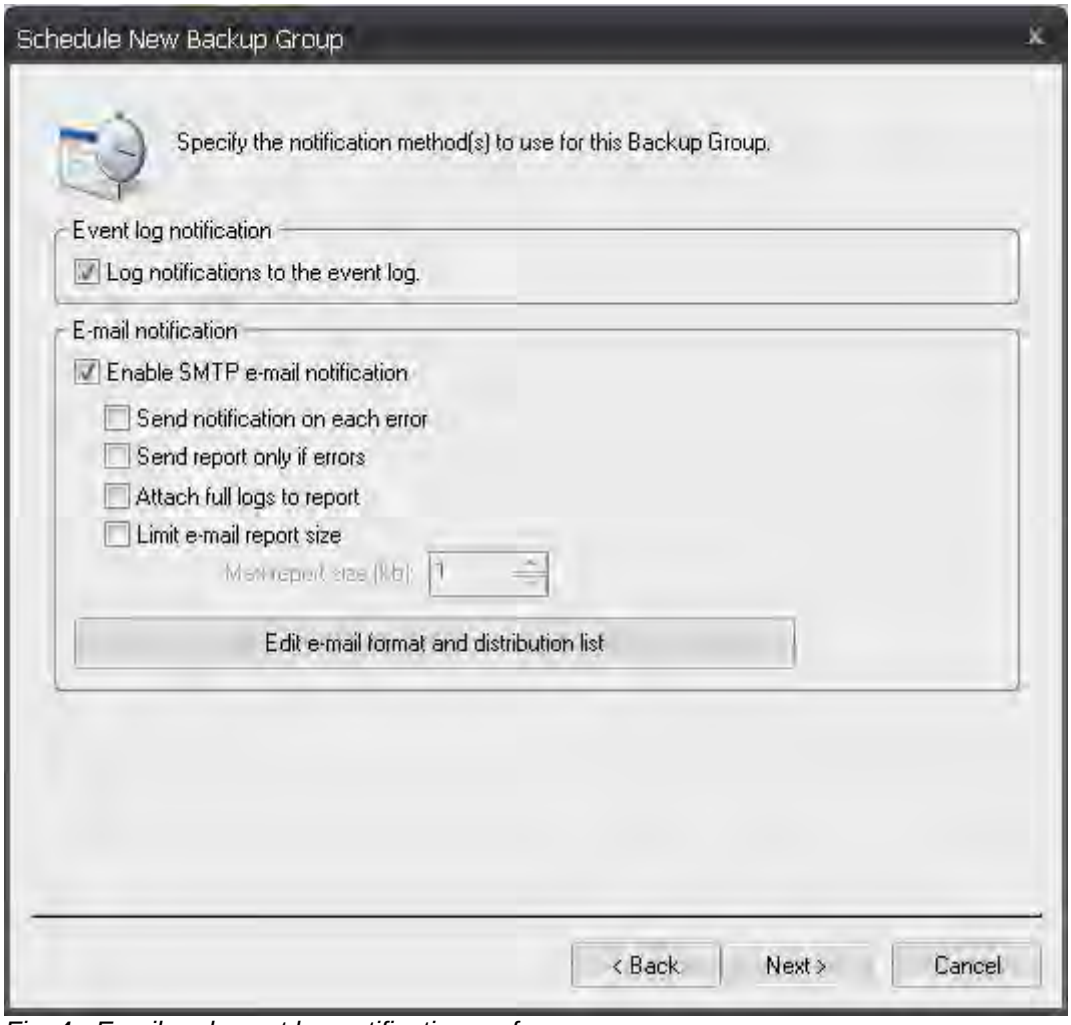


Fig. 4 - Email and event log notification preferences.

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."

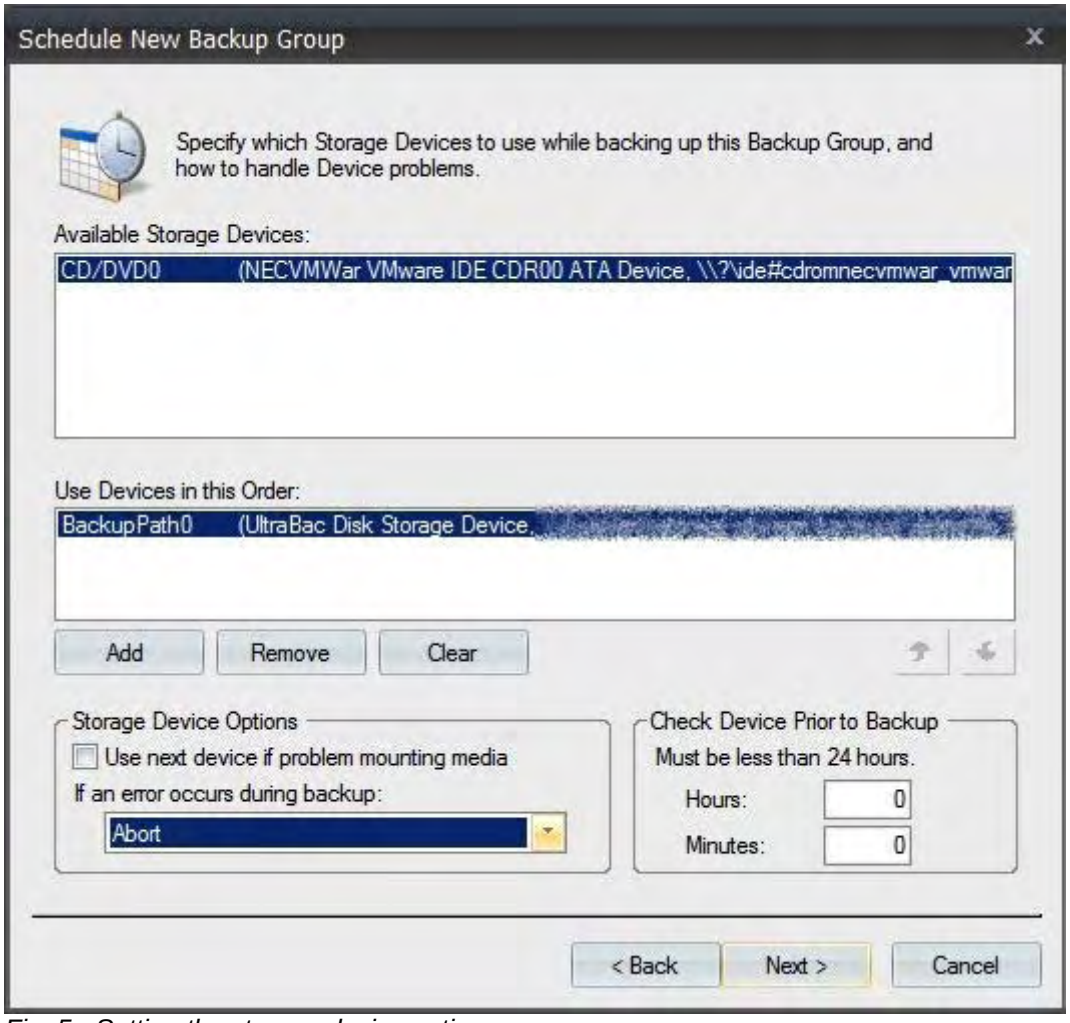


Fig. 5 - Setting the storage device options.

7. Set the Backup Time Limit options (if applicable), and click “Next."

   A scheduled backup can be configured to stop if it runs past either a specified amount of run-time or a specified clock time. How the backup stops can also be specified.

   - Limit backup run time – toggle whether a specified time will stop a scheduled job.
   - Cancel backup if it runs longer that a specified number of minutes – set a maximum number of minutes the backup will be allowed to run.
   - Cancel backup at a specific time – set a specific time to stop the backup
   - Cancellation action:
     - After current file (Default) – finish backing up the file in process, then stop.
     - After current set – finish backing up the full set in process, then stop.
   - Immediately – abort instantly.

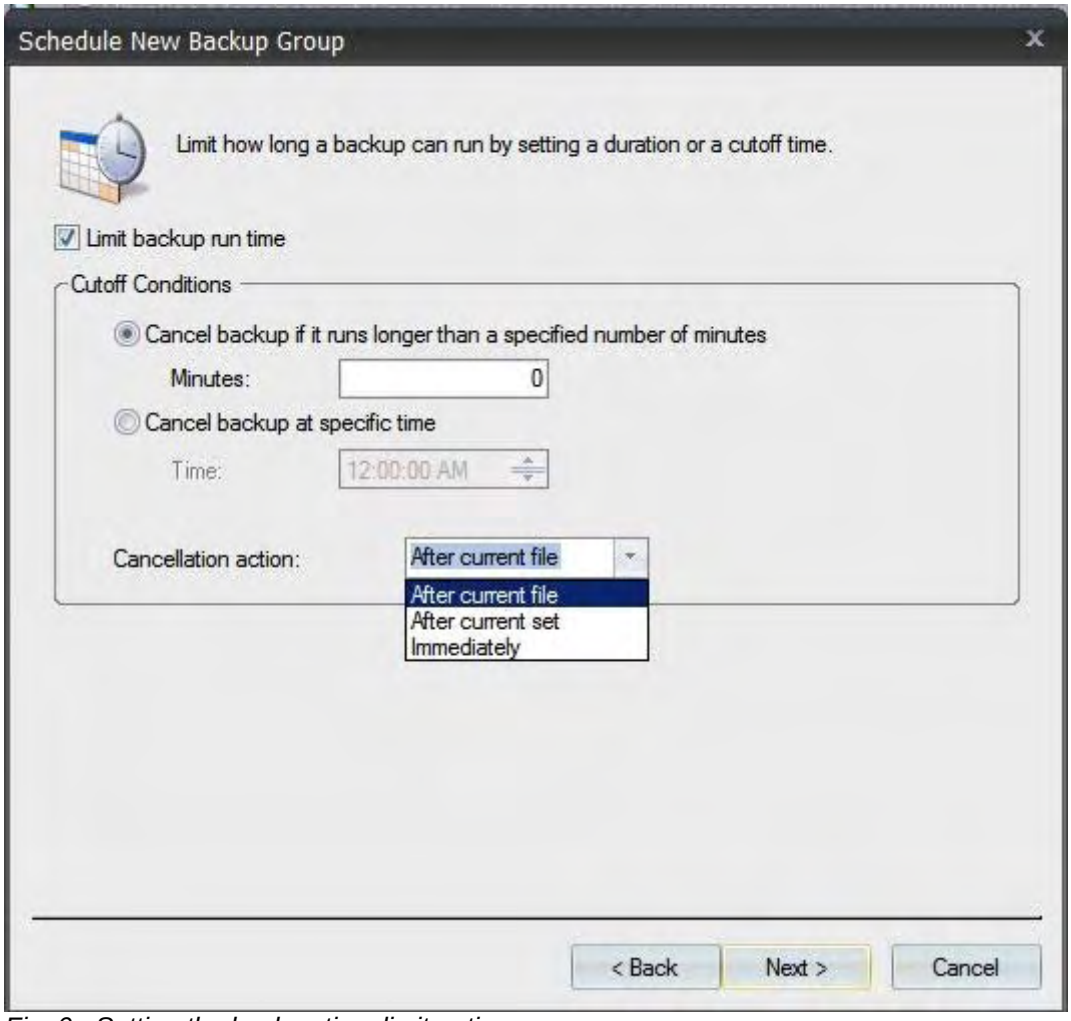


Fig. 6 - Setting the backup time limit options.

8. Set the options for the Media Library Controls (if applicable), and click "Next."

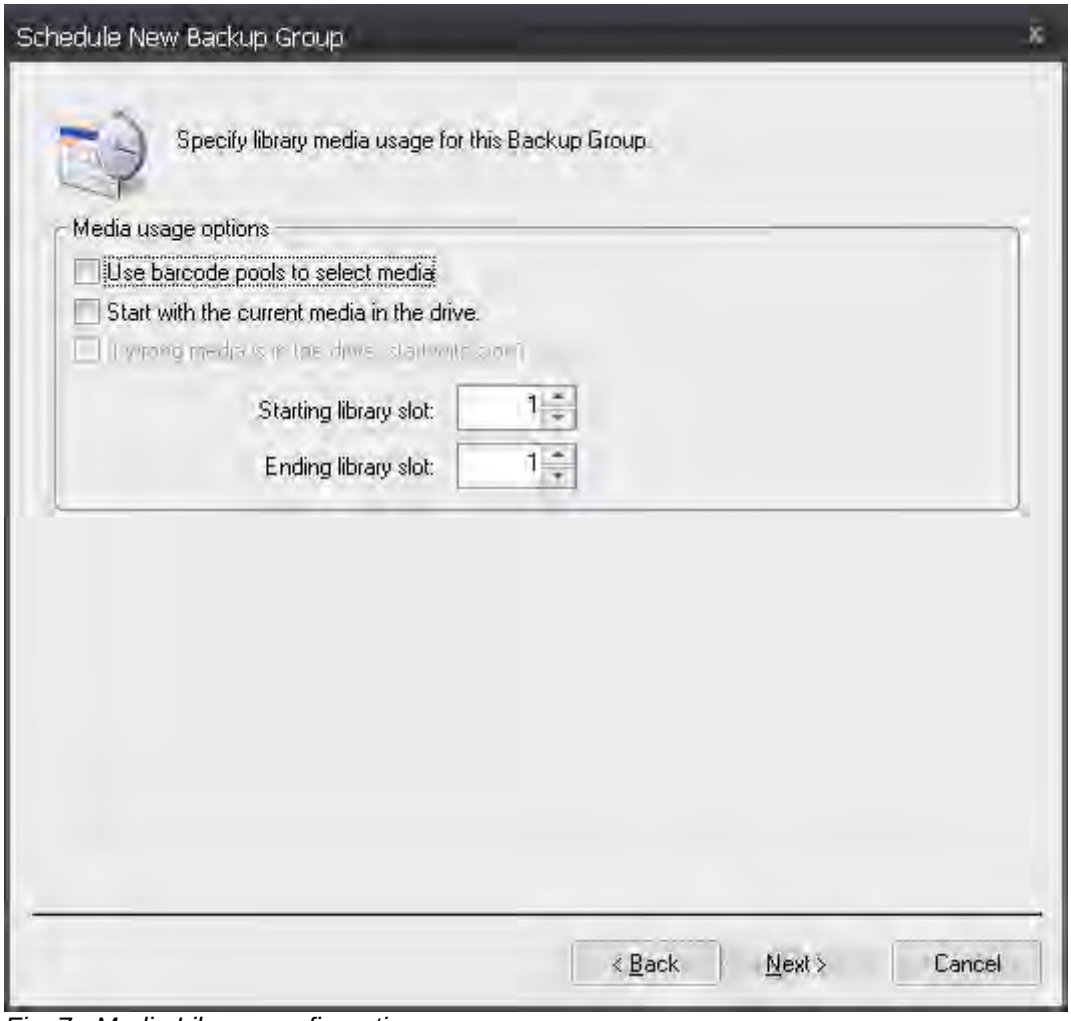


Fig. 7 - Media Library configuration.

9. Set the event time and date options, and click "Next."

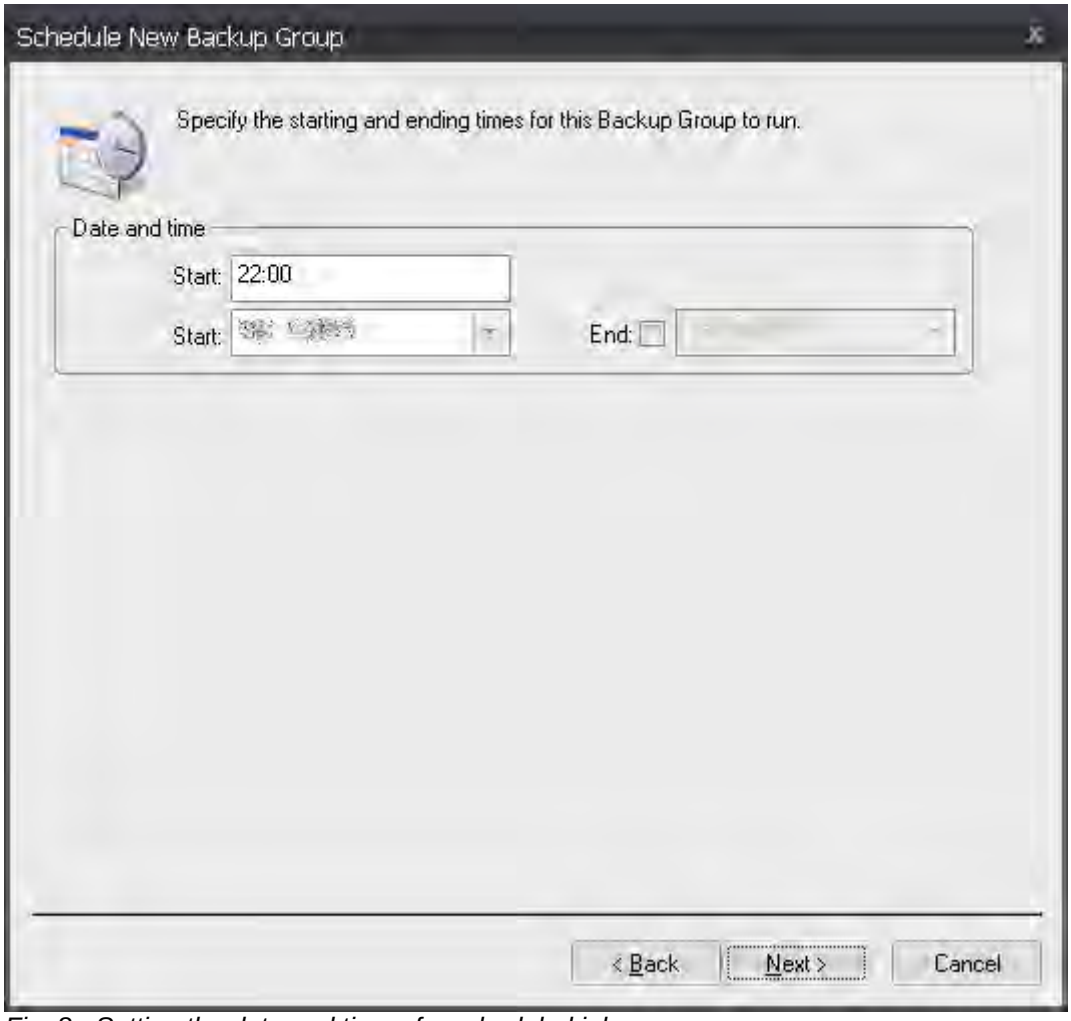


Fig. 8 - Setting the date and time of a scheduled job.

10. Set the frequency/restrictions options, and click "Next."

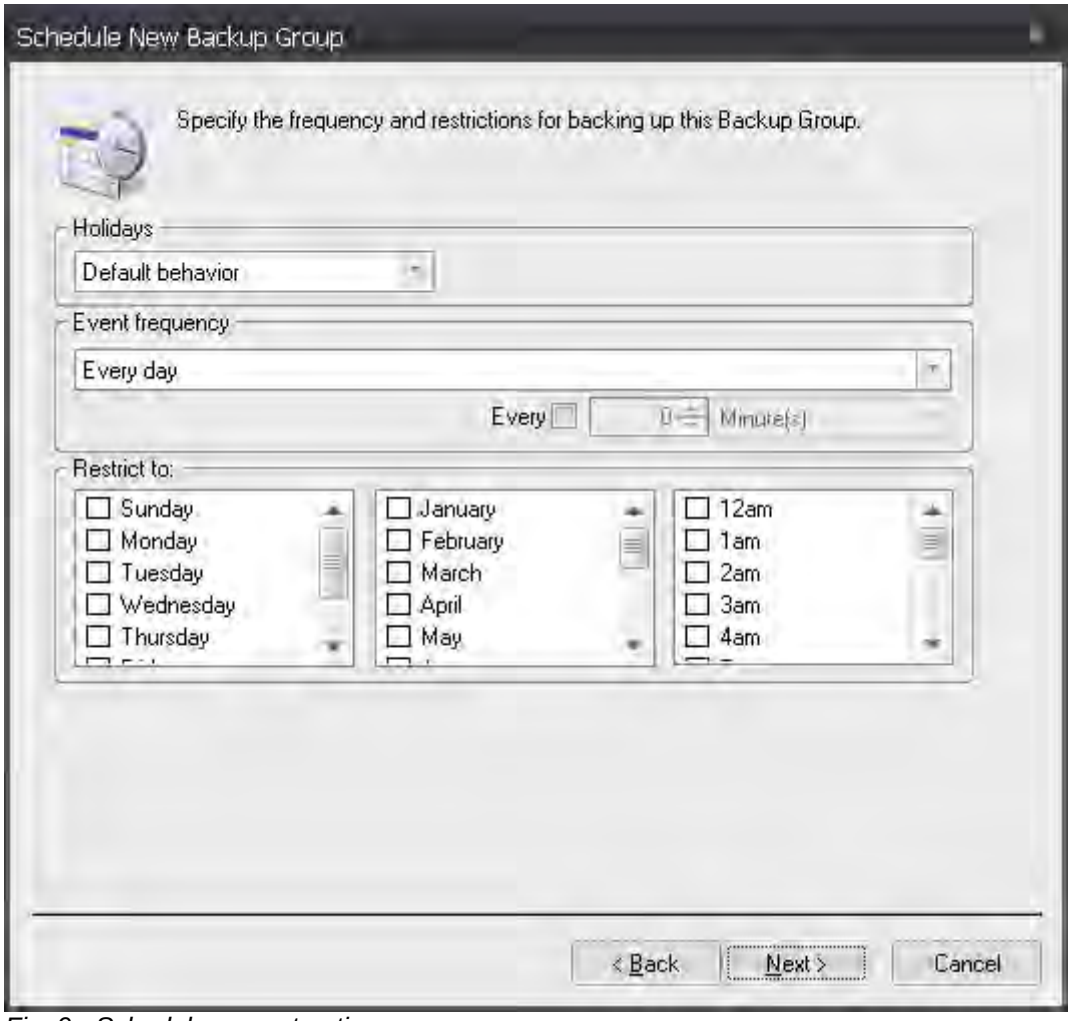


Fig. 9 - Scheduler repeat options.

11. Type in a file name for the scheduled backup, and click "Next."
12. 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. 10 - 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.).

Enterprise Control Files:

- Add/Edit Enterprise Level File/Scripts for Enterprise Scheduler. Enable Control File Option from "Manage" / "General" / "User." Enable - "Show Advance Option."
- Enable Redundant File Elimination - (Future Feature)

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 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.
- Use Auto Response File – The user may create a file for response to the backup group. This option will take precedence over the global and the command line entered options.

Migration Job:

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.
- How to handle media after – Media handling options after the backup (and verify, if selected) completes:
  - Rewind – UltraBac will automatically rewind the media after the job completes.
  - 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).
  - 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

Using Email Notifications, users can configure how backup results are relayed to them. With multiple notification options, such as error notifications and backup summaries, UltraBac gives the users the information they need as soon as it happens. This can be configured during the process of creating a scheduled backup and can be changed after the job is created. This functionality is not supported on ad hoc backups.

Email notification is set up through the “Notification” tab in the properties of a scheduled backup.

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.

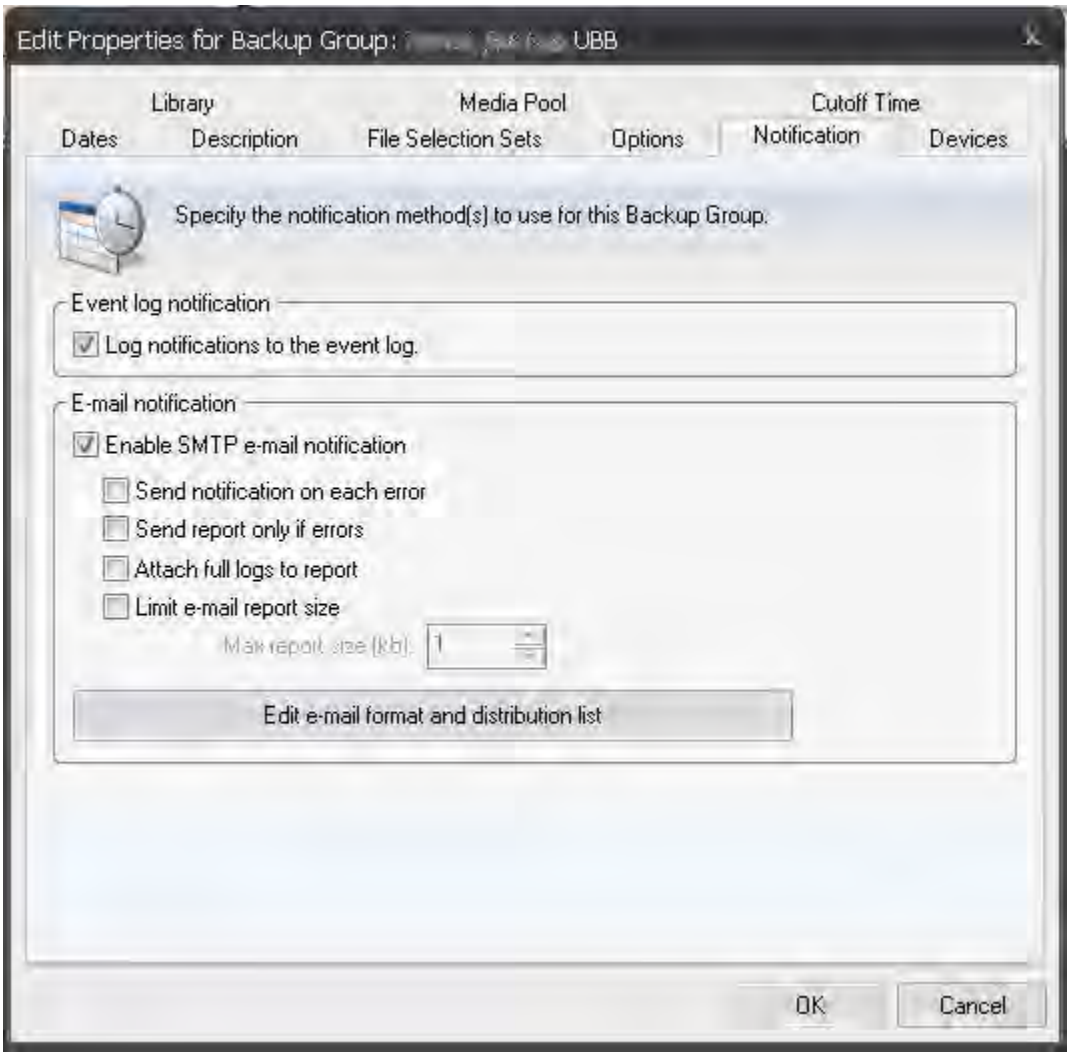


Fig. 2 - Notification tab of the Backup Group properties.

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 e-mail for each error encountered in the backup.
- Send report only if errors – If no errors are encountered during the backup, UltraBac will not send e-mail notification.
- Attach full logs to report – UltraBac will attach both the backup and verify logs to the e-mail.
- Limit e-mail report size – Restricts the size of the e-mail to prevent it from exceeding the specified number of KB.

Configuration

To enter the e-mail notification settings, click "Edit e-mail format and distribution list."

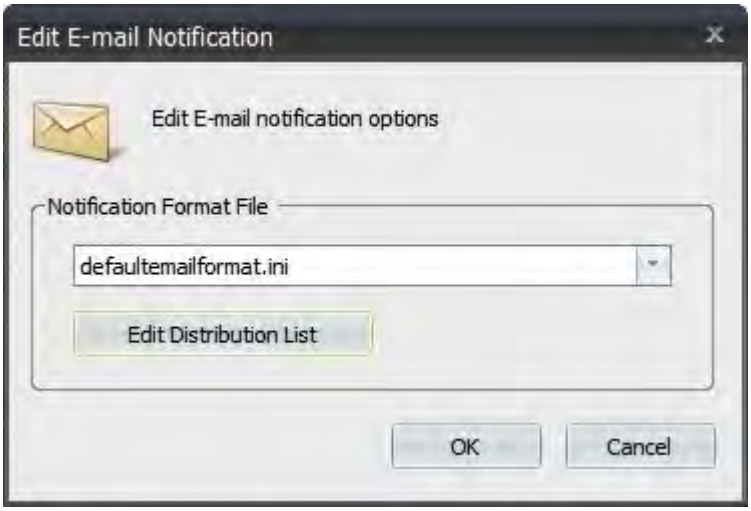


Fig. 3 - Edit Email Notification settings.

Settings

Edit distribution list – Opens the SMTP Distribution List settings dialog.

SMTP Settings

To edit the SMTP settings, select the "Edit distribution list" button on the "Edit Email Notification" dialog.

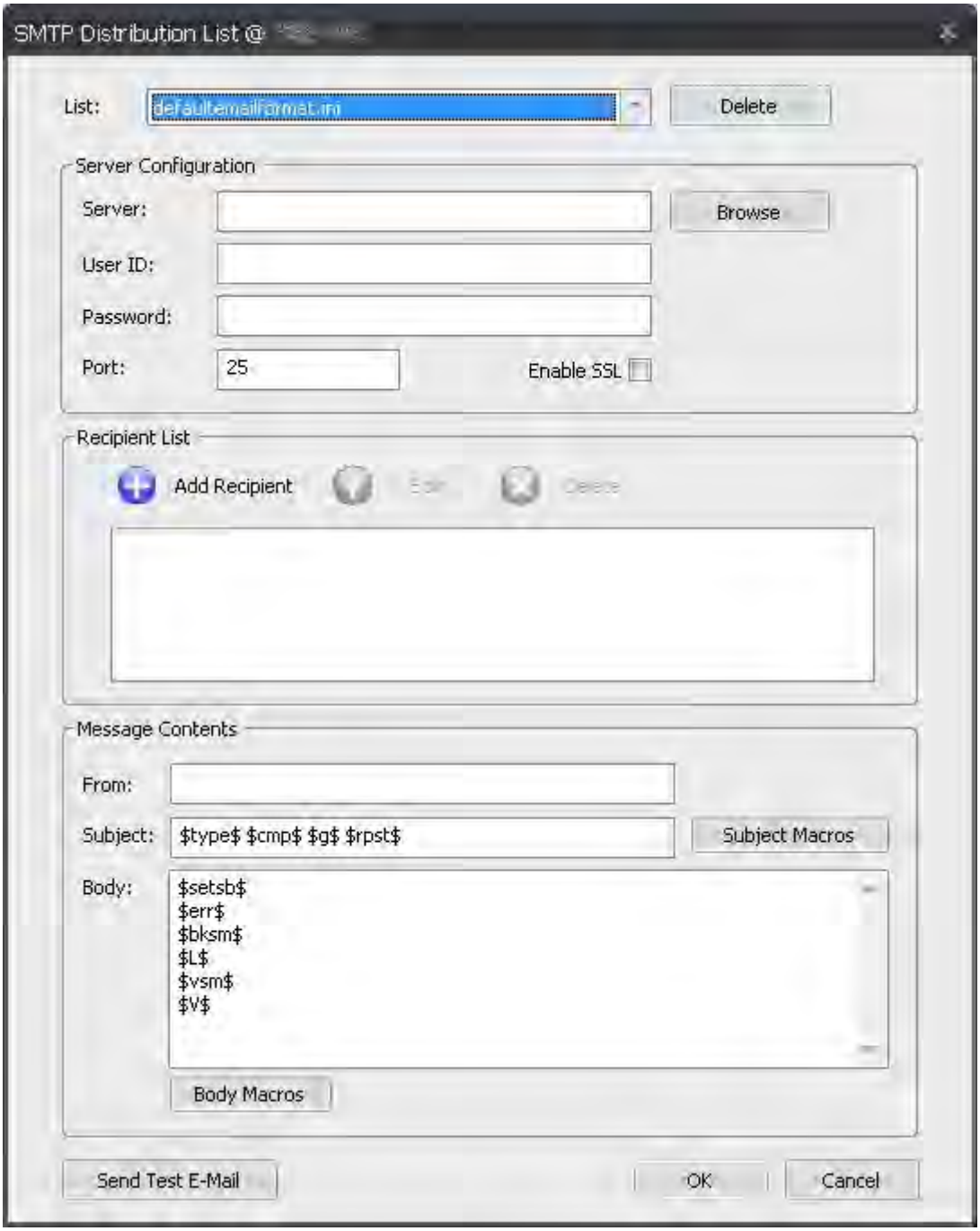


Fig. 4 - SMTP Distribution List settings window.

Settings

- Server Configuration – The SMTP server settings and authentication information.
  - Server – Enter or Browse to set the name or IP address of a valid local SMTP server.
  - User ID – Enter a user with permission to the SMTP server.
  - Password – Enter the password for the User ID to the SMTP server.
  - Port – Enter the port information for the SMTP server.
  - Enable SSL – For ESMTP Authentication on Exchange server.

- Recipient List – Holds the list of e-mail addresses that will receive e-mail notification.
  - Add Recipient – Select this button to open a dialog to add a valid e-mail address of a recipient.
  - Recipient List Box – Holds the list of added e-mail addresses. Select an address to either edit or delete.

- Message Contents – Define the content of the notification e-mail. Several macros can be used to set system of backup specific information.
  - From – Define what will appear in the "From" line of the e-mail.
  - Subject – Define what will appear in the "Subject" line of the e-mail. Macros will be defined below.
  - Subject Macros – Displays a pop-up list of the macros that can be used in the Subject line.
  - Body – Define what will appear in the "Body" section of the e-mail. Macros will be defined below.
  - Body Macros – Displays a pop-up list of the macros that can be used in the Body of the e-mail.

Macros

Email Macros – These can be used in either the Subject or the Body. Please note that set specific macros will only show the current or last set backed up.

- g - Group Filename
- s - Set Filename
- t - Tape Label Name
- n - Current Volume Number
- l - Backup Log Filename
- v - Verify Log Filename
- d - Device Number
- ev - Total Verification Errors
- sf - Total Skipped Files
- if - Total Inuse Files
- st - Status
- se - Sets With Errors
- mb - Total MB Written
- tm - Total Backup Time in Seconds
- fc - Total File/Folder Count
- err - Total Errors
- $setsb$ - Sets Begin
- $bksm$ - Backup Summary
- vsm - Verify Summary
- cmp - Computer
- $rpst$ - Report Status
- $type$ - Type

Device Options

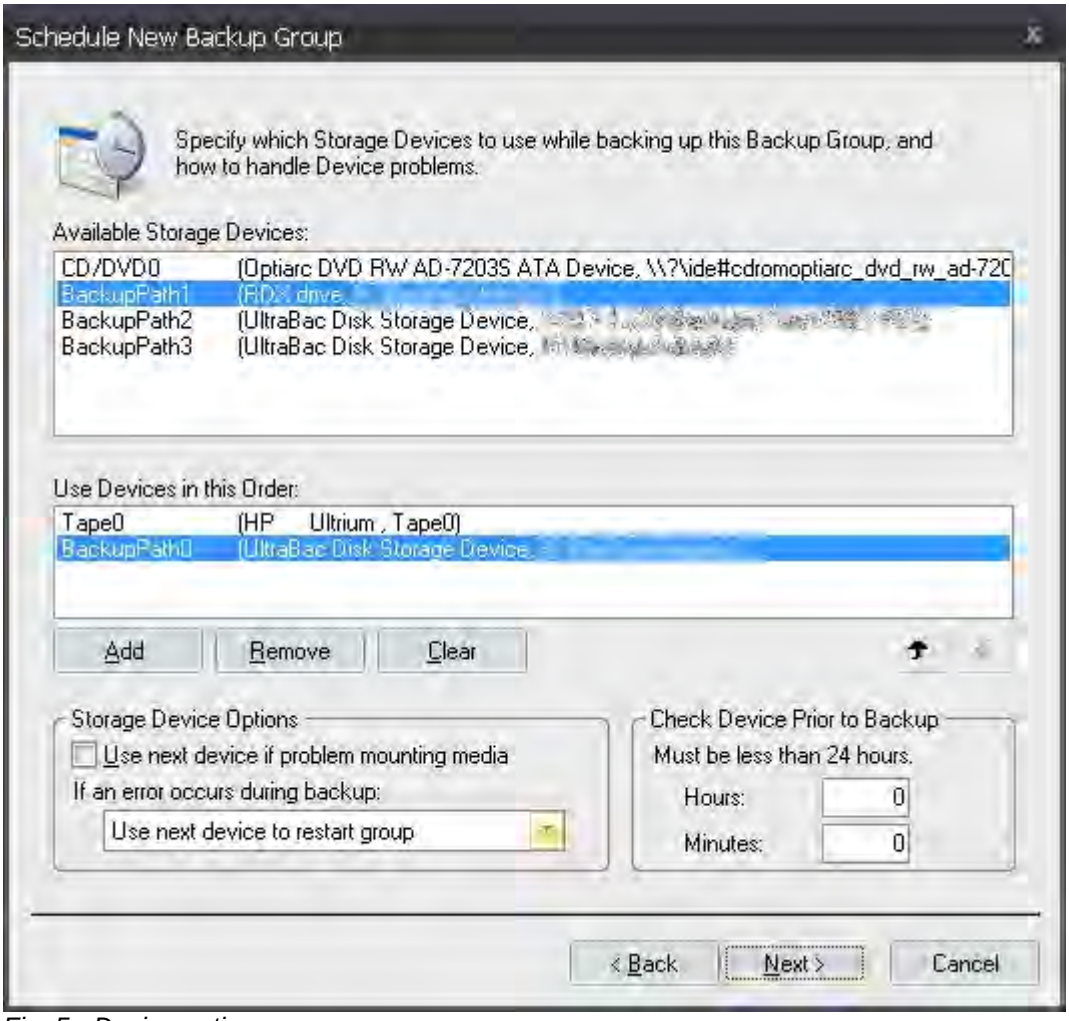


Fig. 5 - Device options.

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 job using the next storage device.
  - Abort – Abort the backup.

Check If Device Is Ready

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

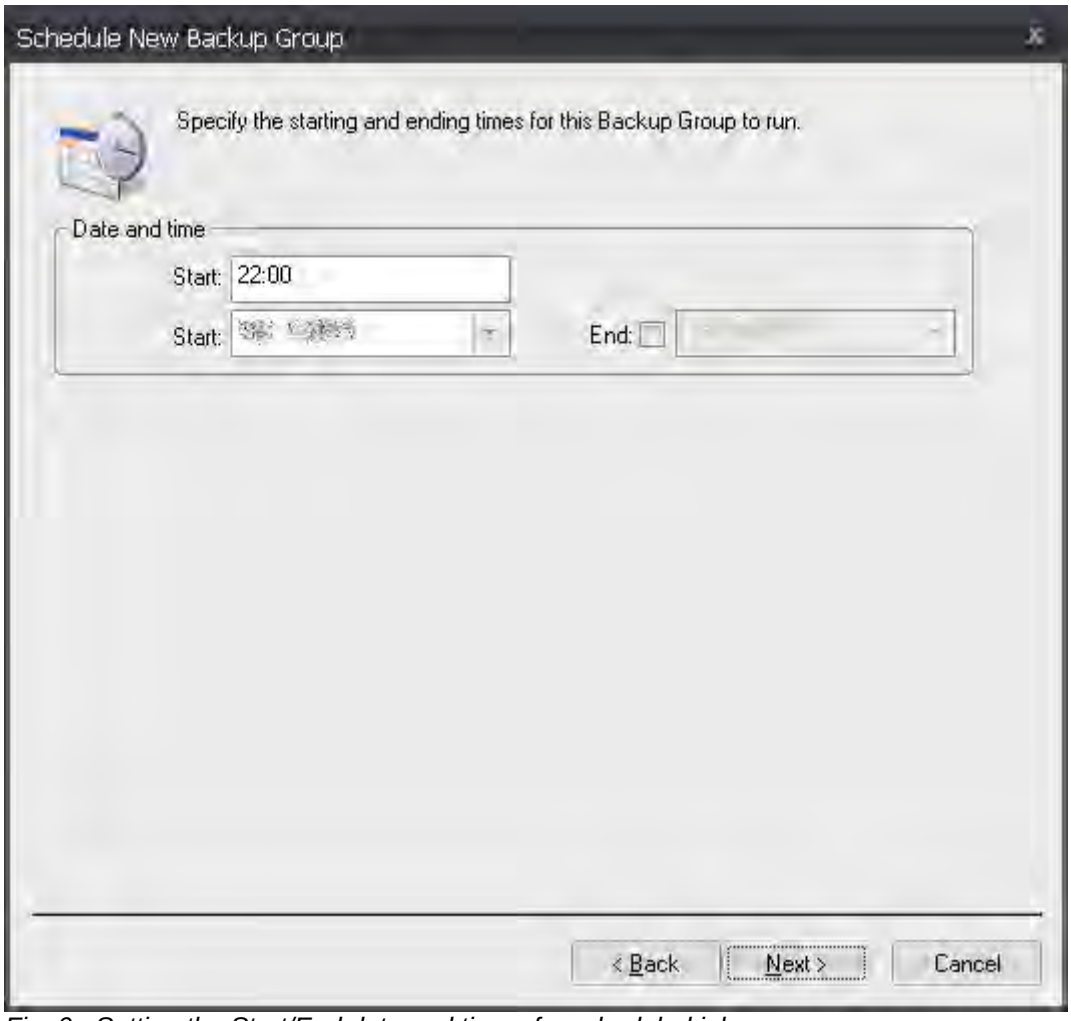


Fig. 6 - Setting the Start/End date and time of a scheduled job.

- Start Time – Type the appropriate time in the "Start Time" field, using "24 hour" (military) time.
- Start Date – Type or select the appropriate start date from the calendar drop date.
- End Date – Type or select the appropriate end date from the calendar drop date. Leave unselected to run indefinitely.

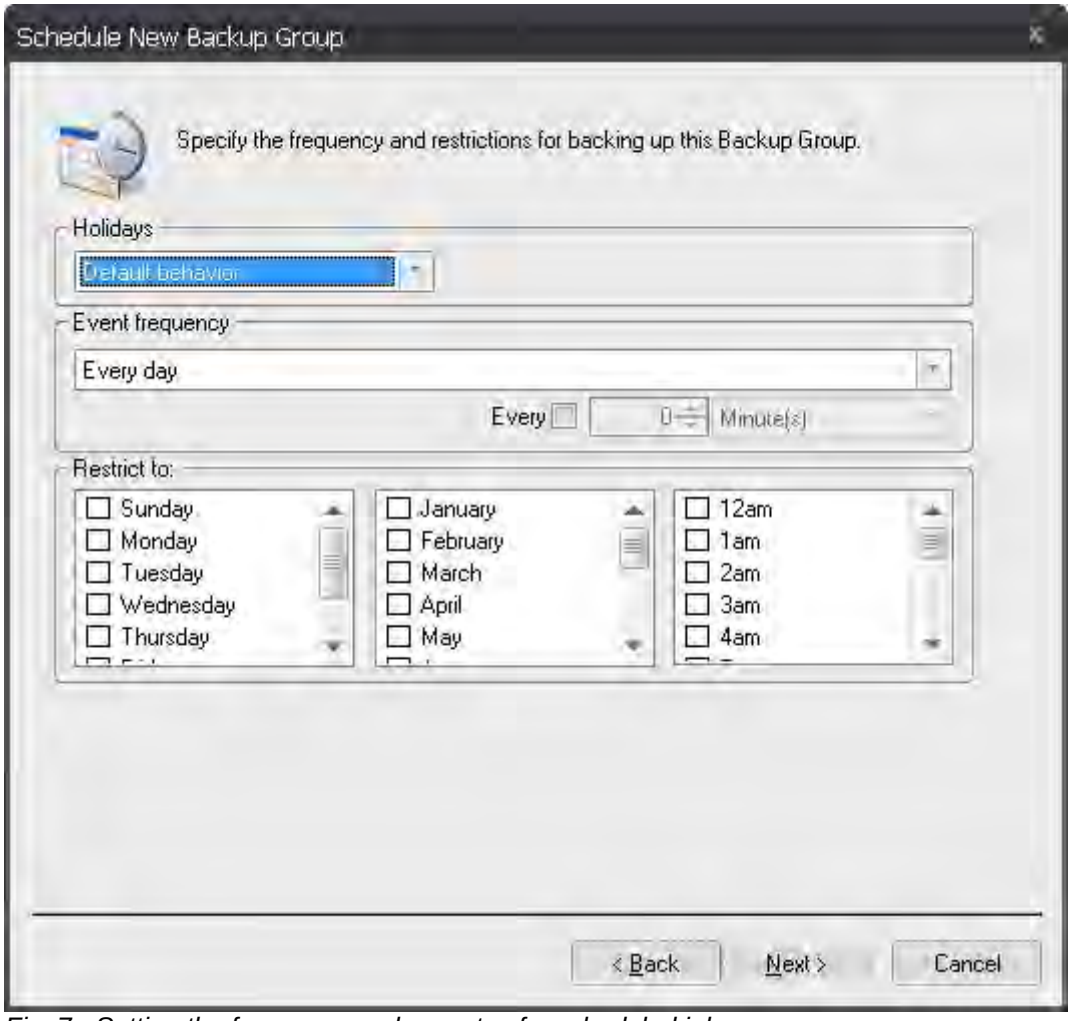


Fig. 7 - Setting the frequency and repeats of a scheduled job.

- 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.
  - 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.

  - 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.
  - 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.
  - 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.
  - 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.
  - First weekday of each month – Runs the backup on the first Monday of each month.
  - Last weekday of each month – Runs the backup on the last Friday of each month.
  - Last day of each month – Runs the backup on the last calendar day of each month.
  - Every [###]
    - Minute(s) – Launch the scheduled backup again after the specified number of minutes.
    - Hour(s) – Launch the scheduled backup again after the specified number of hours.
    - Day(s) – Launch the scheduled backup again after the specified number of days.
    - Week(s) – Launch the scheduled backup again after the specified number of weeks.

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

NOTE: For information on troubleshooting SMTP, please see the UltraBac Knowledge Base:

UBQ000069: Troubleshooting SMTP

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.":

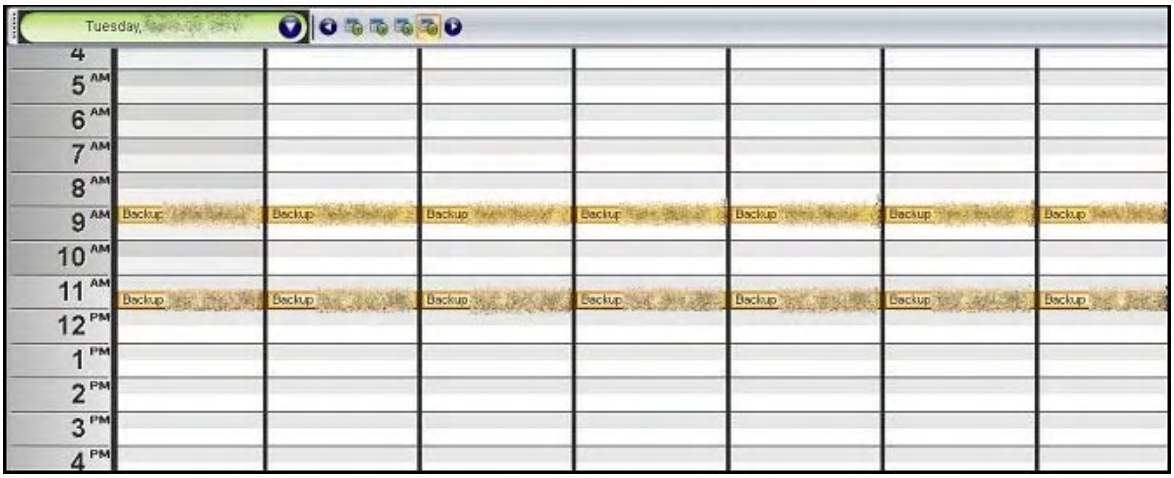


Fig. 1 - Day-at-a-Glance calendar.

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)."

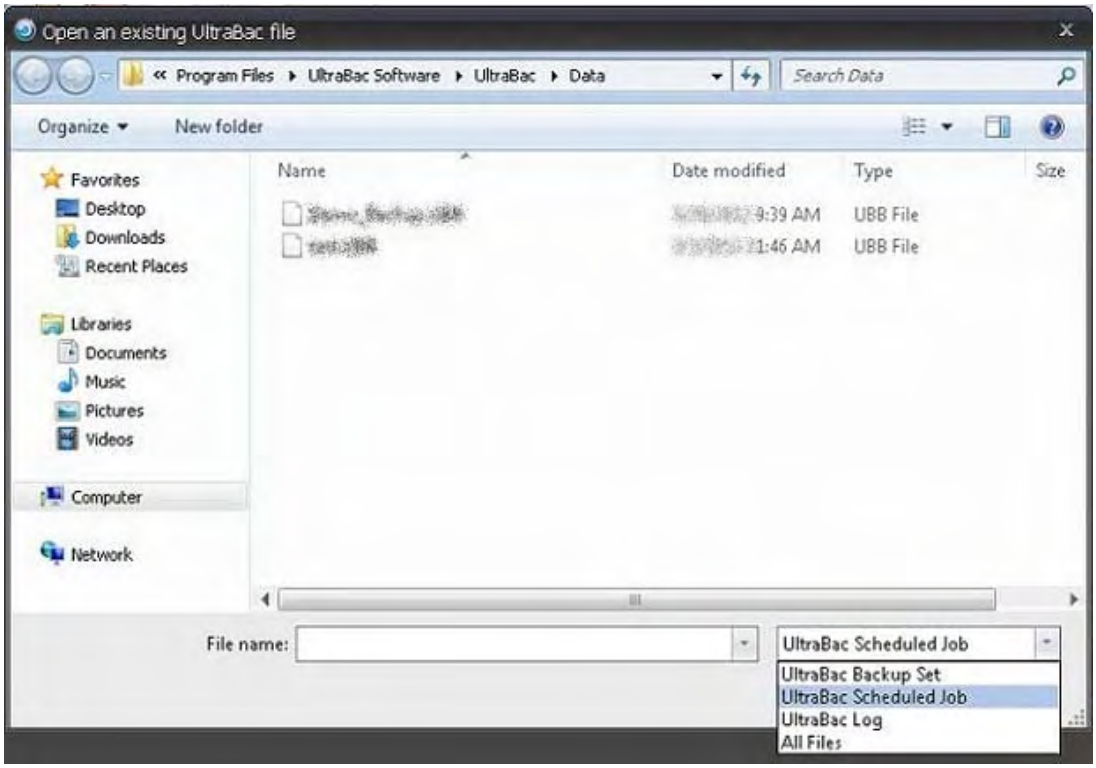


Fig. 2 - Opening the properties of a scheduled job.

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.

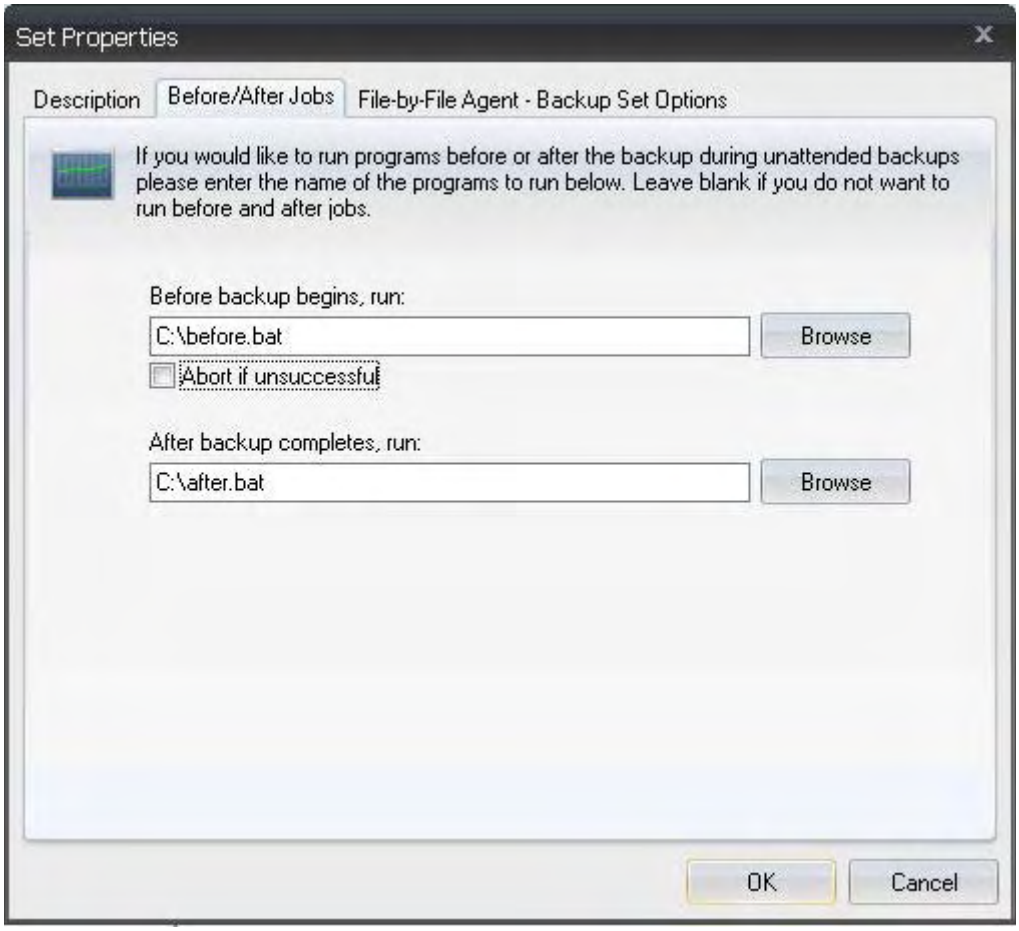


Fig. 1 - Before/After Jobs tab in the Set Properties.

NOTE: Before/After Jobs are only executed when the set is run as 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.

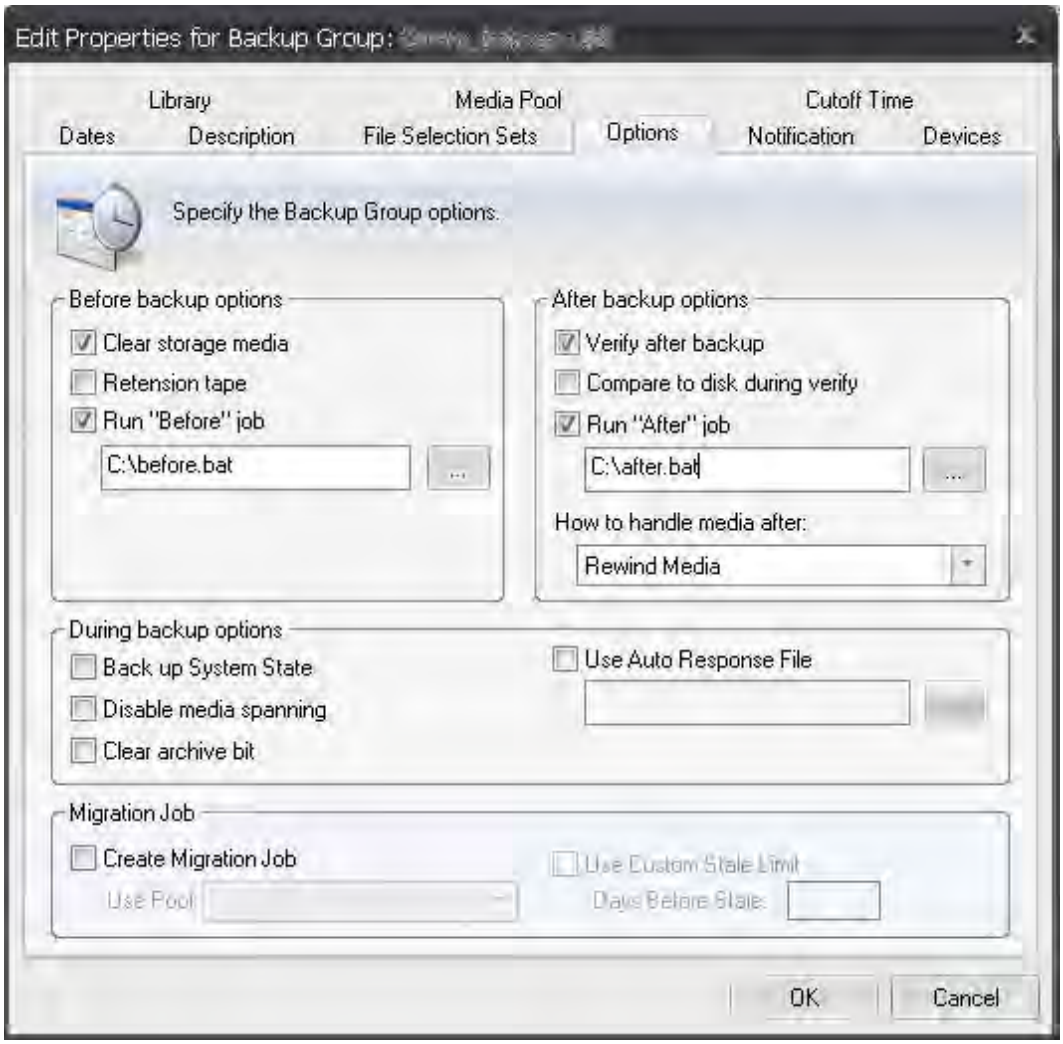


Fig. 2 - Options tab in the properties of a scheduled backup.

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 Basics

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." The selected storage device is listed on the bottom menu bar of the UltraBac user interface.

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:
    - Retrieve from Storage Media – Retrieve Backup Index from currently selected Storage Device.
    - Retrieve from online disk index – Retrieve Backup Index from 'Indexes' folder on Backup Host.
    - 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 the local machine – Query the index database for all sets backed up by the local system.
        - Retrieve All Sets in the Database – Query the index database for all sets in the database.
3. Click "Next."

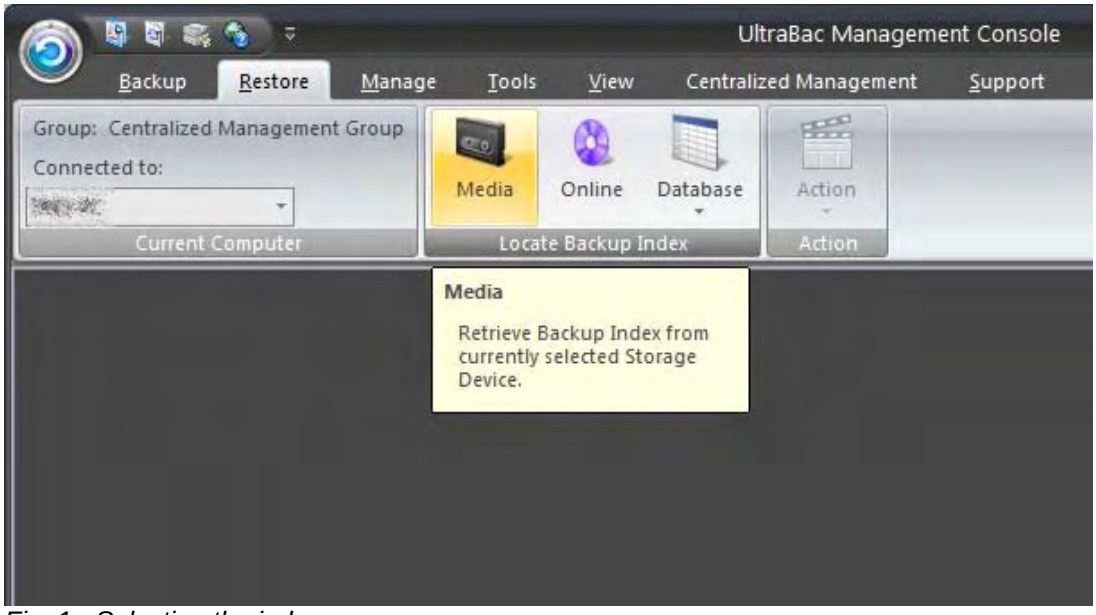


Fig. 1 - Selecting the index source.

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 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.
- 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 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.

Selecting the Index

Once the index source is selected, the backup index must be selected and loaded into the File Viewer.

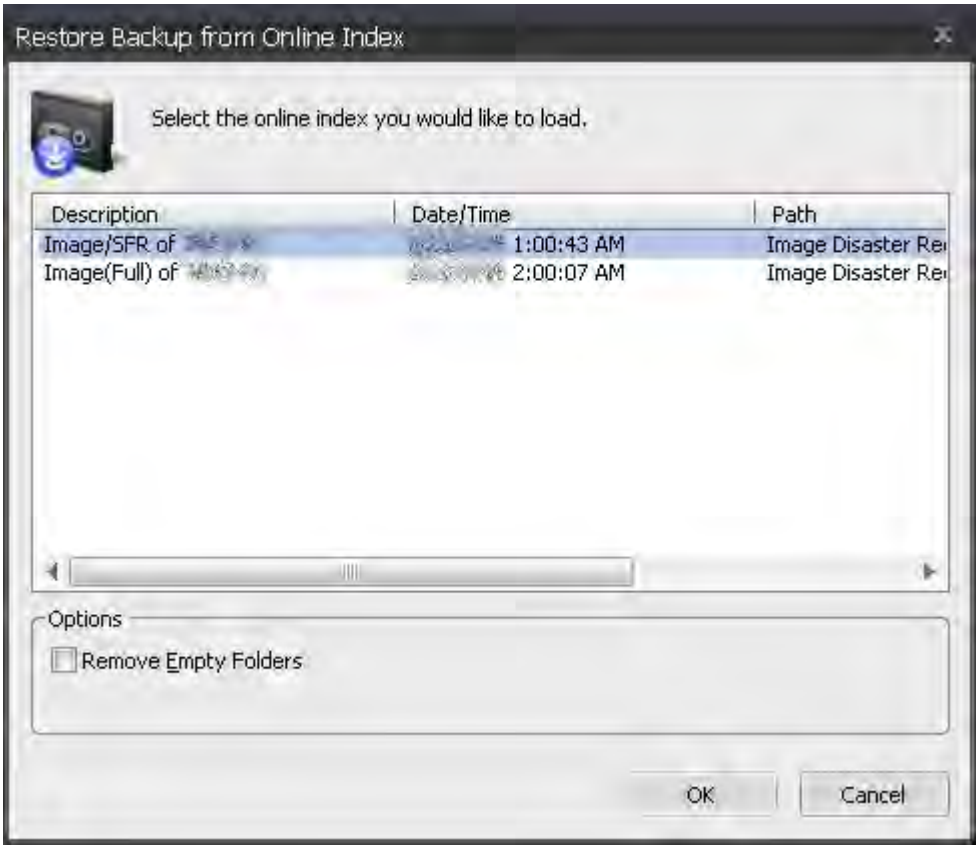


Fig. 2 - Selecting the backup index to load from the online disk index.

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

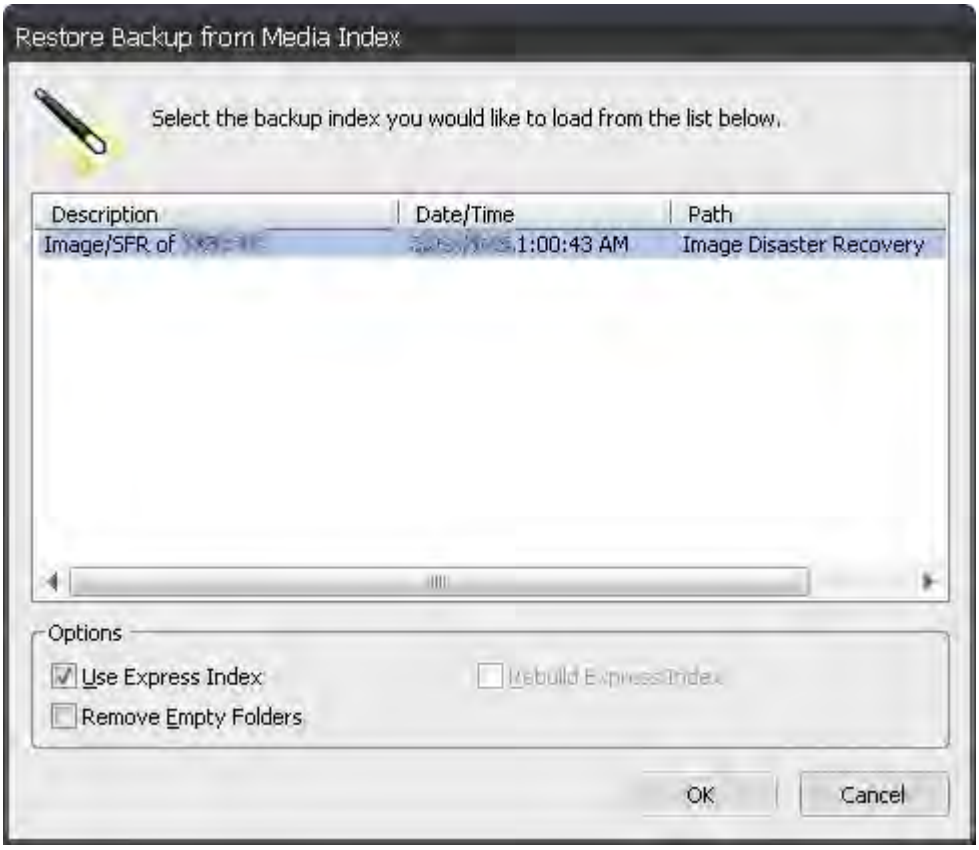


Fig. 3 - Selecting the backup index to load from the storage media.

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.

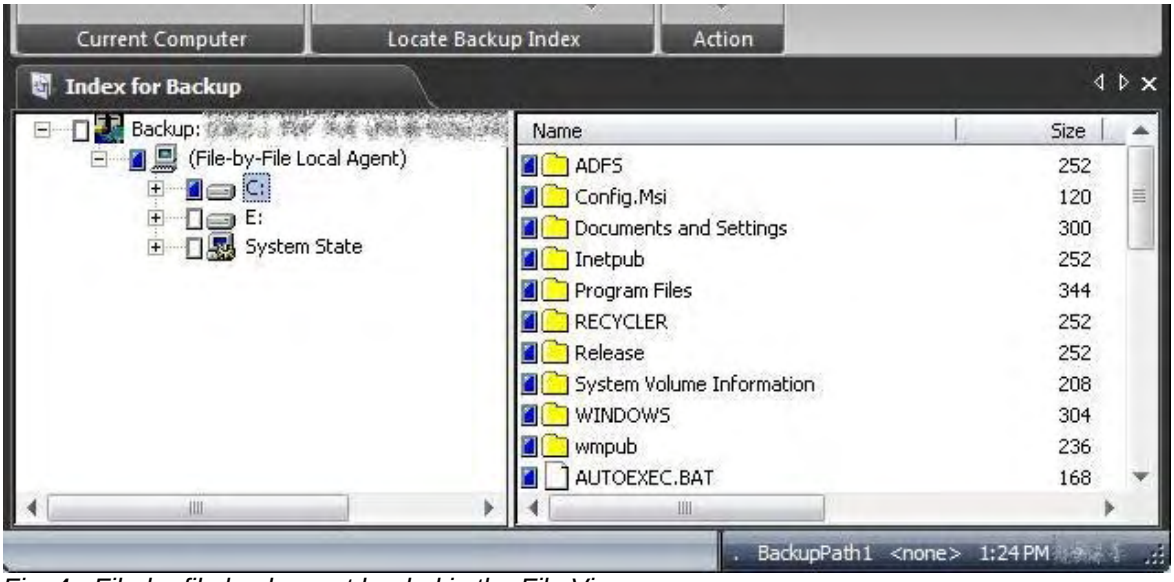


Fig. 4 - File-by-file backup set loaded in the File Viewer.

Restoring Data from a Backup

To restore the selected data:

1. From the Restore tab, click "Action"/"Restore This Backup."

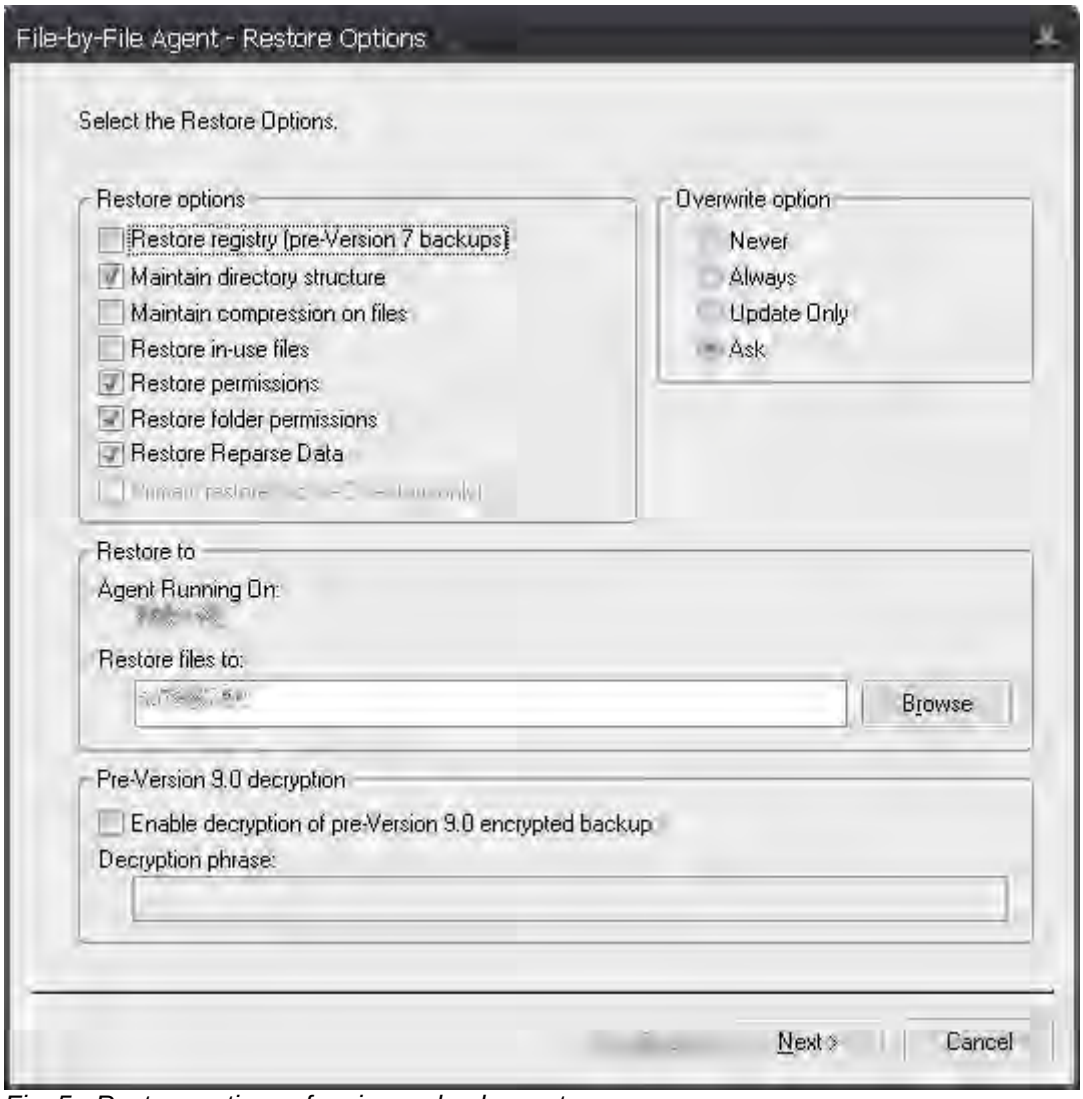


Fig. 5 - Restore options of an image backup set.

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."

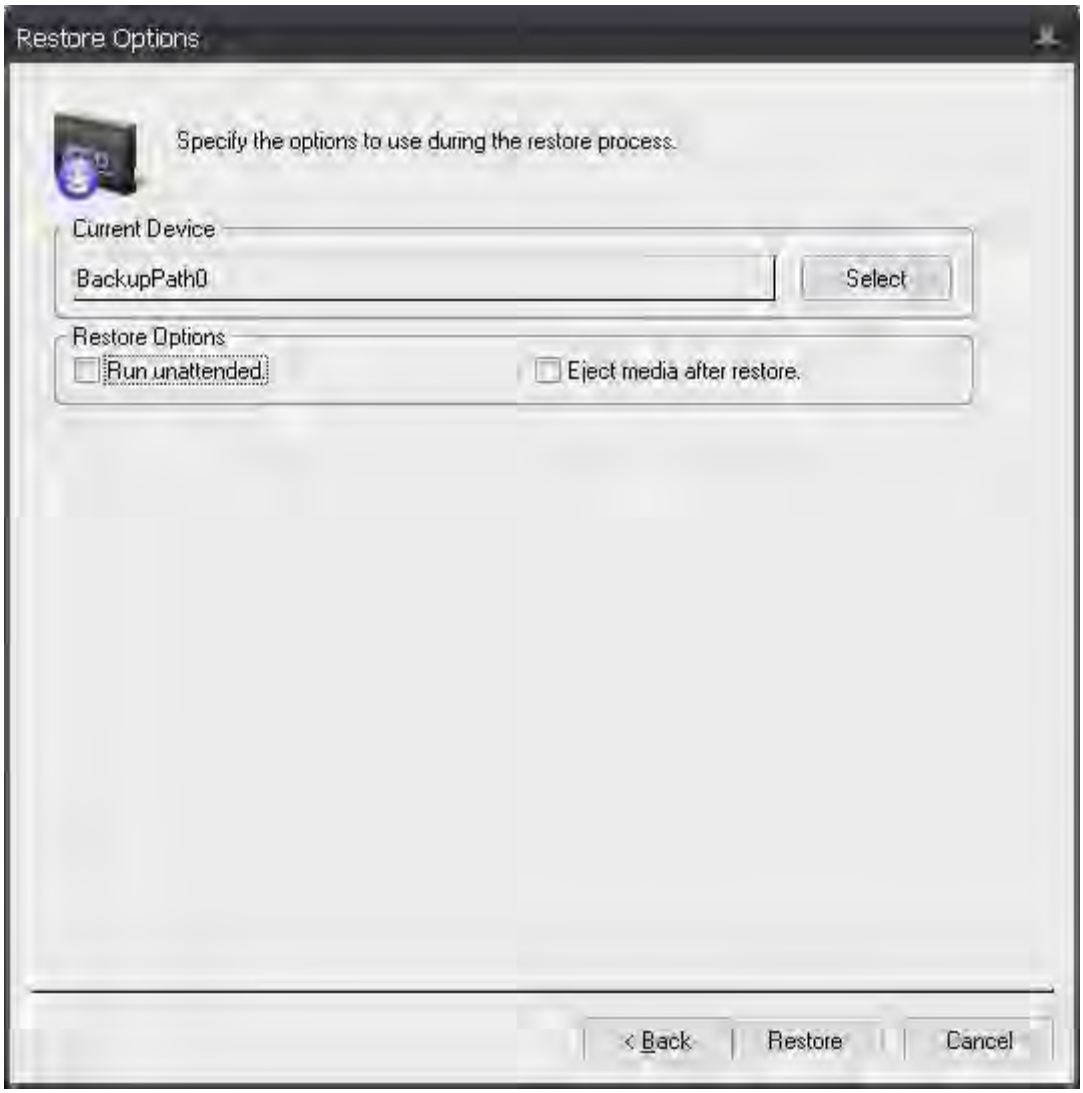


Fig. 6 - Restore options.

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:
>
> **UBQ000001: Command Line Backup/Restore**

Usage: UB [option] [command]
Values in all caps are the default value.
Options and commands are NOT case sensitive

Options

[option] can be one or more of the following:

- /PrepareMedia:<volumelabel>
  - Prepare media with label
- /Device:<device number or name>
  - Select device (overrides default)
- /IncludeRegistry
  - Include the registry in the backup
- /Set:<set specifier>
  - Specify the set to operate on by set number or index file name
- /StartFileTime:<MMDD[YYYY][:HHMM]>
  - Specify start file time for operation.
- /EndFileTime:<MMDD[YYYY][:HHMM]>
  - Specify end file time for operation.
- /TimeType:[MODIFIED|accessed|created]
  - Specify the time type of StartFileTime and EndFileTime
- /Restore:[path]
  - Restore to optional restore to path otherwise restore to original location.
- /Overwrite:[Yes/No/Update]
  - Overwrite storage media or append.
- /R
  - Recurse into subdirectories
- /KeepStructure:[YES/No]
  - Maintain directory structure on restore
- /KeepSecurity:[No/File/Folder/BOTH]
  - Maintain directory/file security on restore
- /RestoreInUseFiles:[NO/Yes]
  - Restore files that are currently open
- /Password:<password>
  - Set password
- /Verify:[CRC/Compare/No]

    - Verify after backup.
- /Quiet
    - Do not prompt for user input.
- /Server:<Server Name>
    - Performs /Backup or /Jobs on remote machine.
- /AutoResponse:<AutoResponse File>
    - Auto respond to messages
- /Y
    - Forces protected media to be erased or prepared.
- /AESKey:<key>
    - AES Key.
- /AESPhrase:<phrase>
    - AES Phrase. Must Specify AESEncryptStr to use.
- /AESEncryptStr:<128\192\256>
    - The Strength of the AES Phrase.
- /CreateMigrationJob:<pool_name>
    - Create a Migration Job and use the specified pool.
- /Stale:<###>
    - Number of days before the Migration becomes Stale.

Commands

[command] can be ONLY one of the following

- /Backup <set/group name>
    - Back up the specified set or group
- /CheckDevice
    - Check to see if device is connected or currently in use.
- /EjectMedia
    - Eject media from tape device
- /ViewHeader
    - View media Header
- /ViewMediaIndex
    - View list of backups on media
- /FindFiles:<file pattern>
    - File files specified by the file pattern
- /Erase
    - Erase the default device or media specified with the /Media option
- /Jobs
    - List jobs currently running on the local system or computer specified by /Server option.

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

NOTE: Only File-by-file backups can be restored via the command line.

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> – 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

Disaster Recovery

Image Disaster Recovery Agent

The Image Disaster Recovery Agent in UltraBac is the same agent that is used in UBDR. The functions and screens are the same, 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.

NOTE: For information on what an image backup is, please see the UltraBac Knowledge Base:

UBQ000024: What is an Image Backup?

NOTE: Starting with UltraBac v.9.5.0 the Single File Restore (SFR) option has been modified to use mountable image backups, and only supports writing to BackupPath devices.

NOTE: UltraBac cannot restore to smaller GPT partitions. If it is a necessity, you will need to plan ahead as this cannot be done in a disaster situation. Using Windows Device Manager, right click the partition in question and select "Shrink Volume." Enter a size that is smaller than the partition size you wish to restore to. Once the volume size has been reduced, run an image backup. You can now restore this new backup to the smaller GPT configuration.

NOTE: For information on configuring deduplication server, please see the UltraBac Knowledge Base:

UBQ000278: Configuring UltraBac Deduplication Server

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."

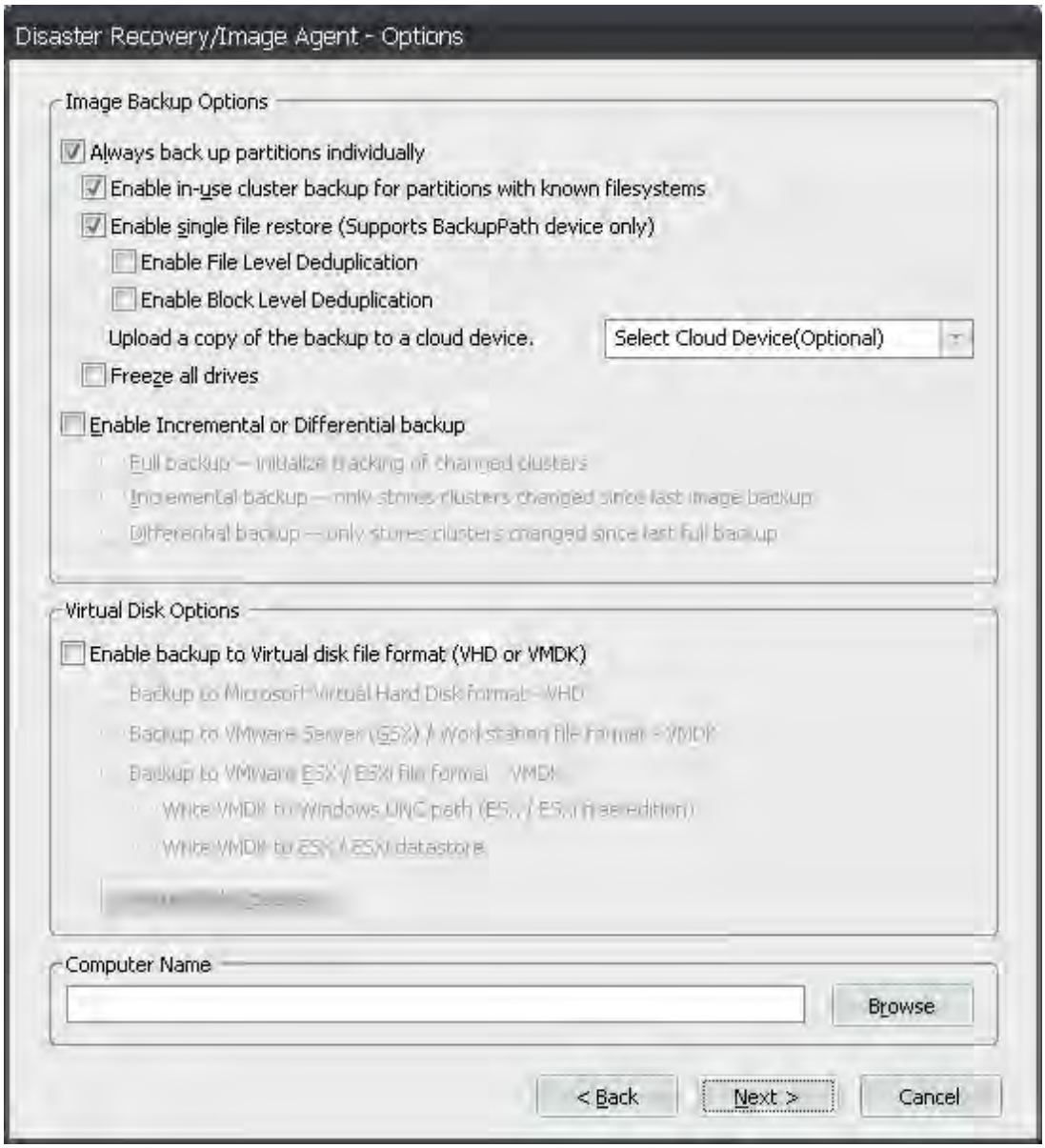


Fig. 1 - Disaster Recovery/Image Agent Options.

4. Type a set description, as it will appear in the backup log, into the "Set Description" field. Click "Next" and "Finish."

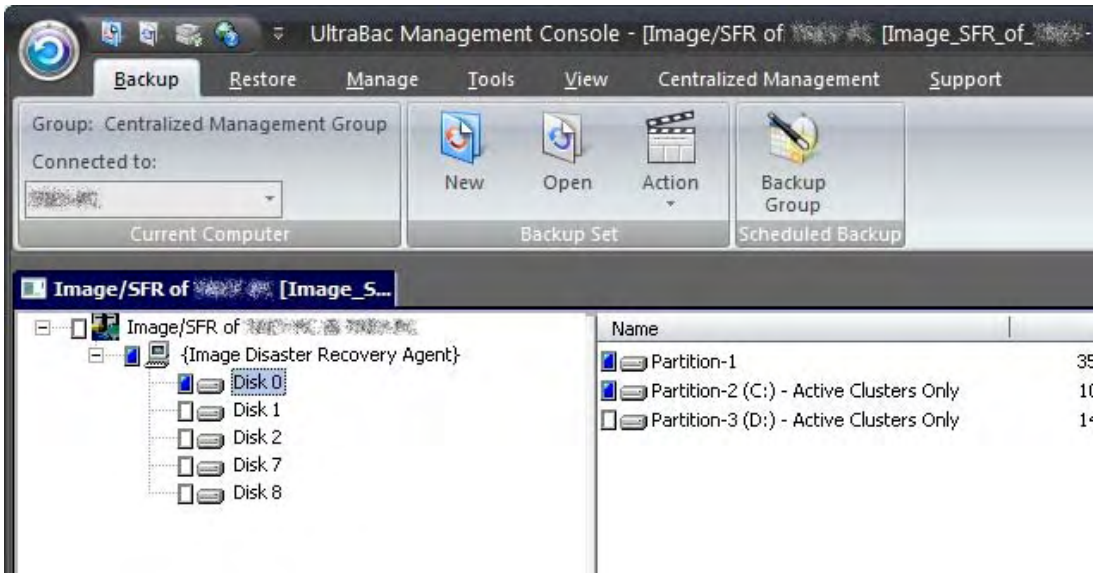


Fig. 2 - Image set loaded in the File Viewer.

5. Save the set by clicking "Action"/"Save Backup Set" 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 filesystems – 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 (Supports BackupPath only) – Writes the backup to a new UltraBac format that allows mounting of the image backup. This provides the ability to mount a virtual volume of the backup to allow individual files and folders to be restored. Enabling this option also allows the image to be deduplicated at the file and/or block level as well as to be uploaded to a cloud device in addition to a backuppath device.
    - Enable File Level Deduplication
    - Enable Block Level Deduplication
    - Upload a copy of the backup to a cloud device. – In addition to writing a SFR backup to a backuppath, the backup will be copied to the specified cloud device.
- 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. UltraBac strongly recommends that you use a database agent to back up databases.

- Enable Incremental or Differential backup – Enables the tracking of changed clusters and set creation necessary to perform an incremental or differential image backup.
    - Full backup – Backs up the full partition or disk, and clears the ".idx" file used to track disk changes.
    - Incremental backup – Backs up all clusters modified after the last full or incremental backup.
    - Differential backup – Backs up all clusters modified after the last full backup.

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

- Enable backup to Virtual disk file format (VHD or VMDK) – Writes the backup output to a VHD (Microsoft Hyper-V) or VMDK (VMware ESX) 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

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."

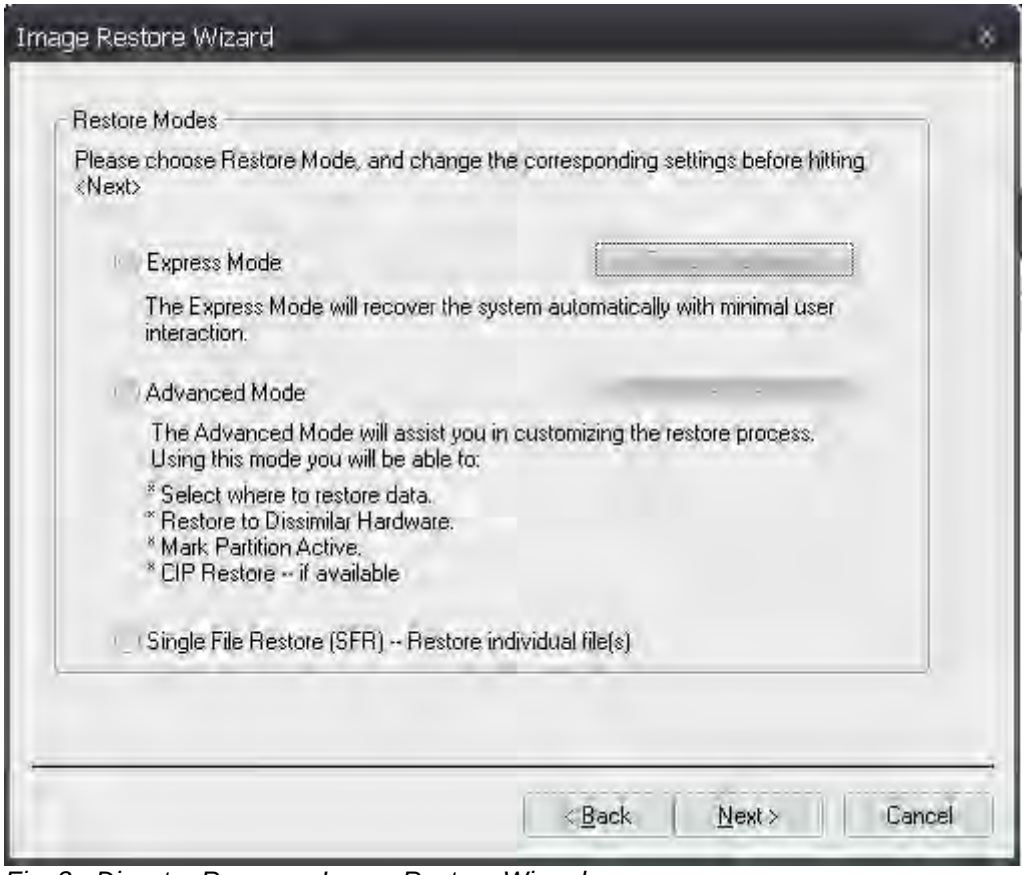


Fig. 3 - Disaster Recovery Image Restore Wizard.

5. Choose either Express Mode or Advanced Mode. Express Mode chooses the "Source Information" by default, while Advanced Mode allows the user to select the "Source Information." Click "OK."

NOTE: Single File Restore (SFR) is only displayed if the image was taken with SFR enabled.

- Express Mode – Can only be used if you are restoring an image back to the same hardware using the same disk configuration (MBR). This mode will attempt to match source and target partitions. If you cannot restore or use the original MBR (meaning you which to change partition size or location), you must use the Advanced Mode.
    - When correct target disk is indeterminable – If the disk signature does not match the source disk
        - Overwrite when destination disk is blank (MBR wiped disk) – The restore will always overwrite data on an existing disk and partition. If a backup of Disk 3 was taken, the restore will only be attempted if Disk 3 does not contain an MBR.
        - Overwrite always (Overwrite the target disk always) – The restore will always overwrite data on an existing disk and partition. If a backup of Disk 3 was taken, the restore will

overwrite Disk 3 regardless of the data currently contained on the disk

- Restore MBR (Master Boot Record) before start data restore -
- Resize Partition(s) -

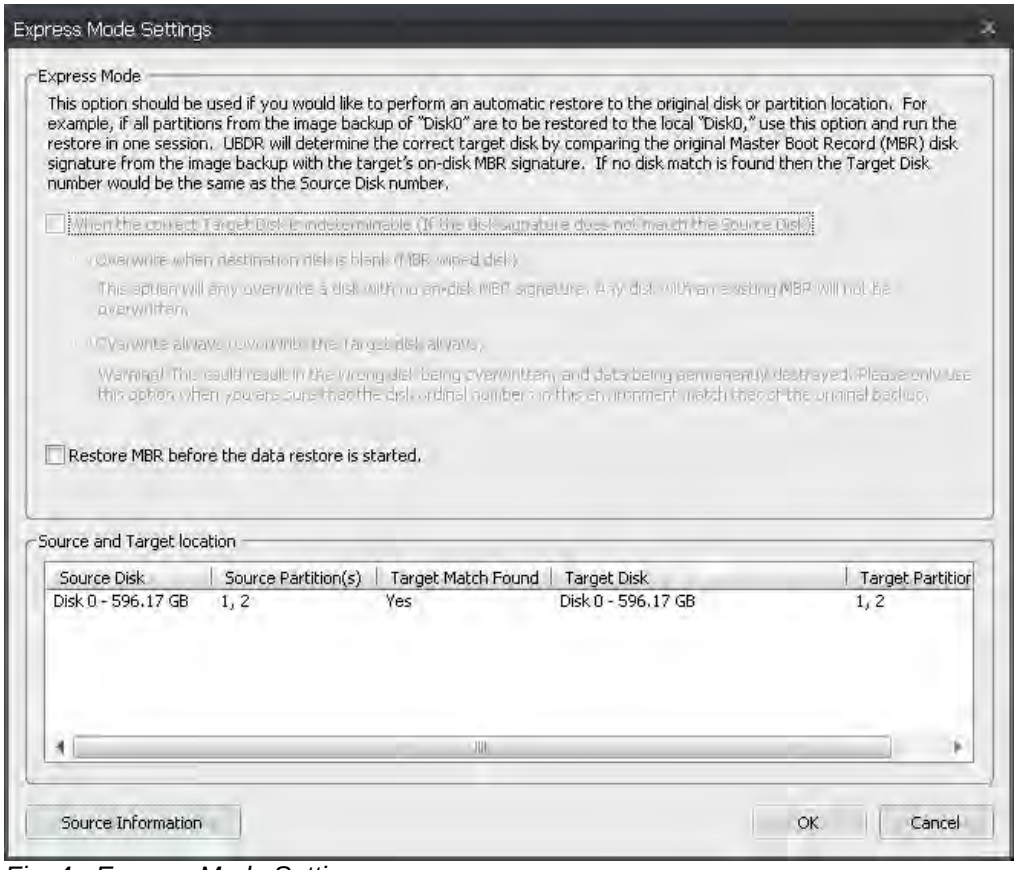


Fig. 4 - Express Mode Settings.

- Advanced Mode - Allows you to change a partition's size, or restore to a partition located on a different disk. This option is also used to perform a dissimilar hardware restore.
    - Source – List of disk(s) / partition(s) contained in the backup. If a disk / partition is selected and added to the queue it will be removed from the list.
    - Target – List of disk(s) / partition(s) available to be restored to. If a disk / partition is selected and added to the queue it will be removed from the list.
    - Mark Partition as Active – The target disk will be marked as active. This disk will then be used to attempt to boot the restored OS. Should only be used on the disk containing the Windows boot loader partition.
    - Restore MBR (Master Boot Record) – Will restore the MBR of the selected source disk to that of the selected target. This will overwrite an existing MBR on the target. This will fail if the target disk is too small. If the source disk contains multiple partitions and the target disk is too small, only partition(s) that will fit on the disk will be created.

- Restoring to Dissimilar Hardware (P2P, P2V, V2P, V2V) – After the restore is completed UltraBac will inject driver(s) necessary to allow the restored OS to boot on the dissimilar hardware. Chipset, display, network, etc. drivers will need to be updated manually after booting into Windows.
- Add to Restore Queue – Adds the selected source and target partition to the restore queue.
- Remove from Queue – Removes the highlighted line from the restore queue.

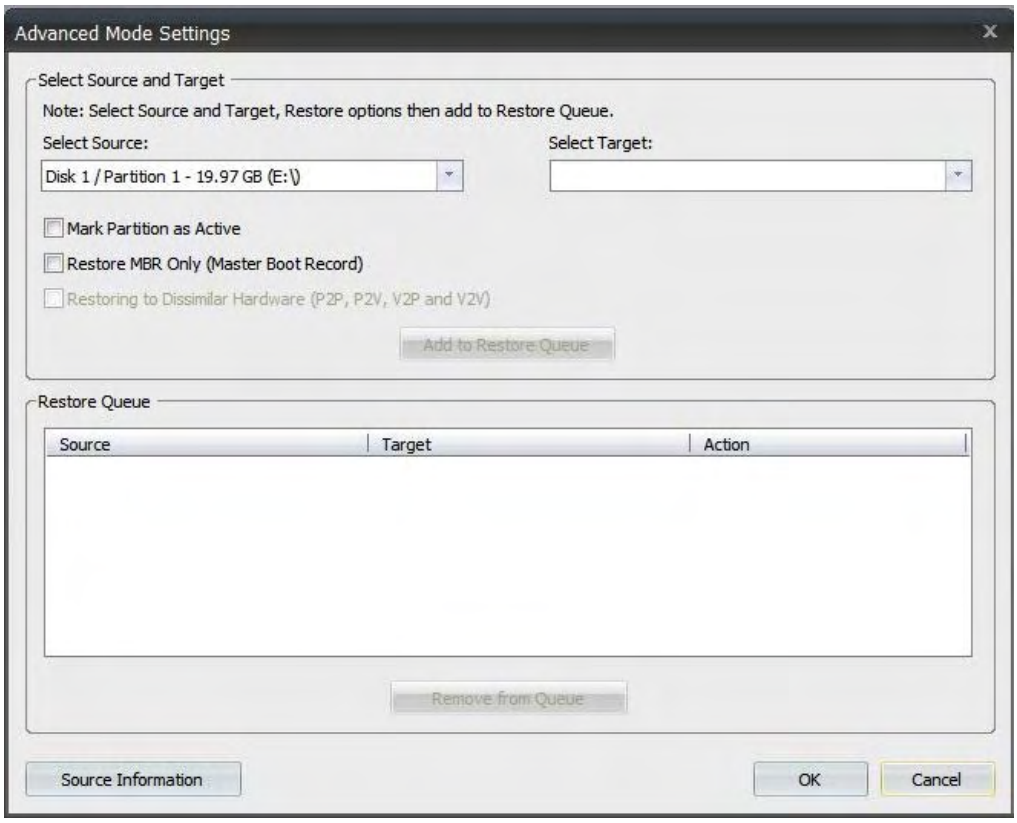


Fig. 5 - Advanced Mode Settings.

- Source Information - Shows the disk and partitions information contained in the backup.

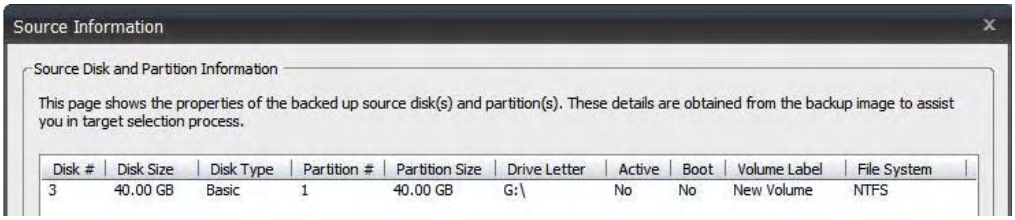


Fig. 6 - Source Information.

6. After the restore completes, reboot the system to activate the restored disk or partition.

NOTE: After performing a dissimilar hardware restore, additional steps may be required on certain Operating Systems. Please see: UBQ000268: Additional steps for UBDR

restore of Windows 7, 2008 R2, and newer Operating Systems.

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, you will be able to mount each partition.

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(s) for restore.
4. Click "Action"/"Restore this Backup."
5. Click "Single File Restore Options."

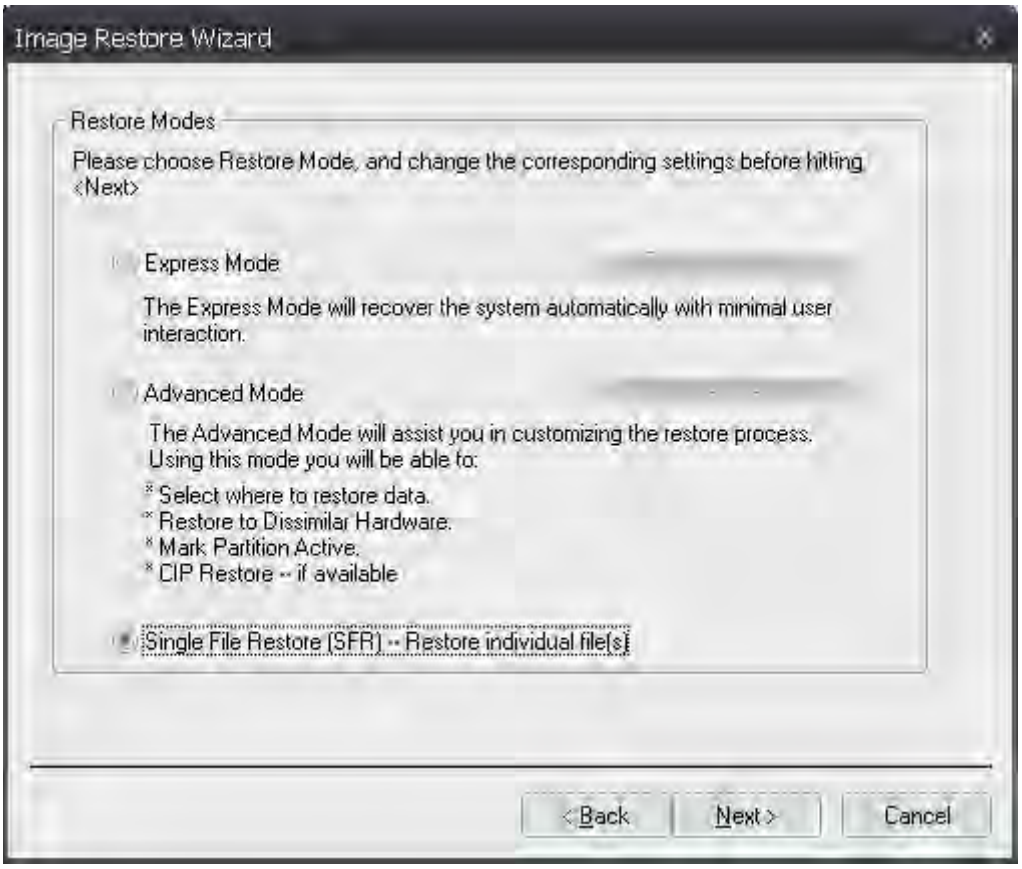


Fig. 7 - Single File Restore Index loaded in the File Viewer.

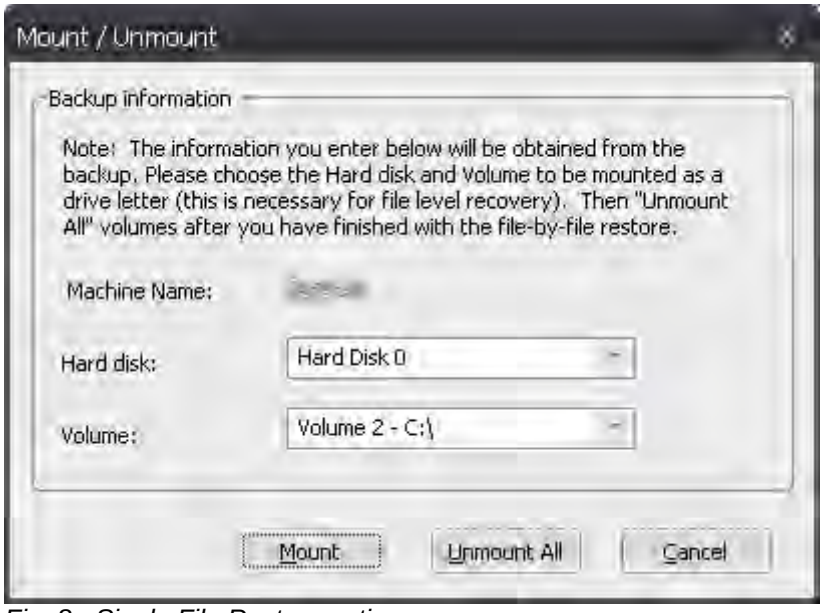


Fig. 8 - Single File Restore options.

6. Select the correct "Hard disk" and "Volume" to be mounted. Click "Mount."
7. Once the volume is mounted, a Windows Explorer window will be opened to the mounted RAM disk drive letter.
8. Copy the files or folders needed.
9. Click "Unmount All" when you are finished.

NOTE: If the set or UltraBac is closed before the backup is unmounted, simply launch UltraBac Management Console and click on “Unmount All Volumes” located at “Tools” / “UBDR.” This will unmount any UltraBac mounted Image SFR, Hyper-V, or vSphere agent backups. Alternatively, follow the same steps required to mount a backup until the "Unmount All" option button is visible.

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.

UBDR - UltraBac Disaster Recovery

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 file-by-file backups.

UBDR Gold is on a bootable CD. UBDR Gold uses multiple versions of WinPE for dissimilar restore capability. WinPE 3.0 (Windows AIK) is used for Vista / Windows 7 / Windows Server 2008 / Windows Server 2008 R2, while WinPE 4.0 (Windows ADK8) is used for Windows 8 / Windows Server 2012. WinPE 5.0 (Windows ADK8.1) is used for Windows 8.1 / Windows Server 2012 R2.

When the system boots, the UBDR Gold Restore CD automatically detects and loads drivers for most NIC cards, SCSI cards, and RAID controllers. The drivers may be added to the Media Build CD or injected when the UBDR CD boots.

NOTE: For more information, see "Inject NIC/Storage Driver" under the "Additional Tools" section further below.

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 correct UBDR Gold Restore CD for your operating system 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, and click "OK."

    - 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 to close it.

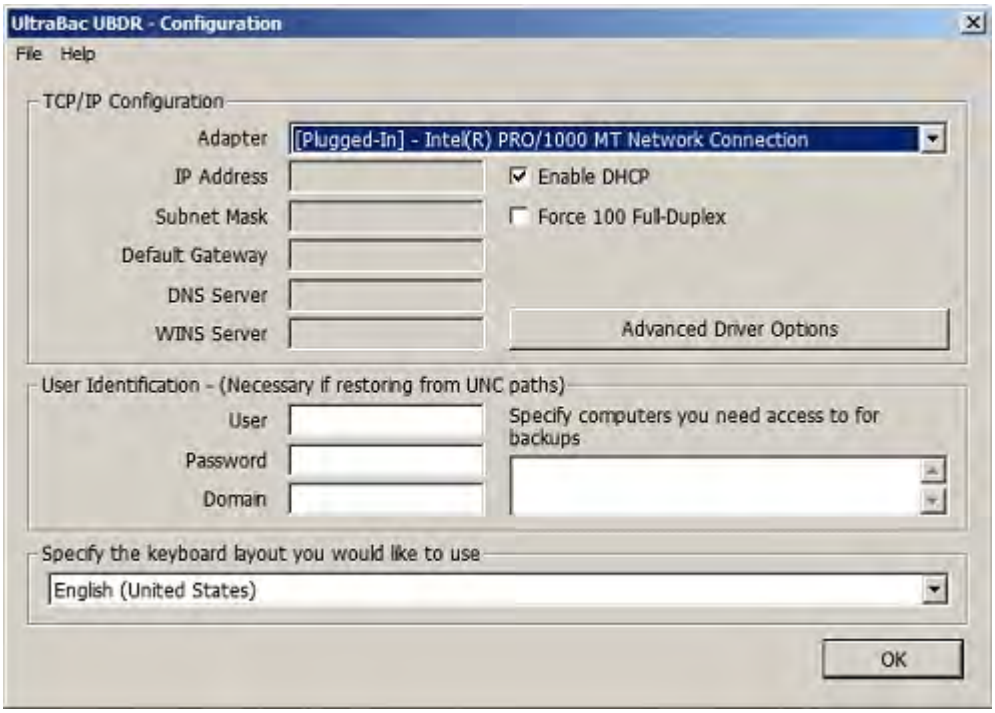


Fig. 1 - Network Configuration.

- 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 – 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.

Advanced Driver Options

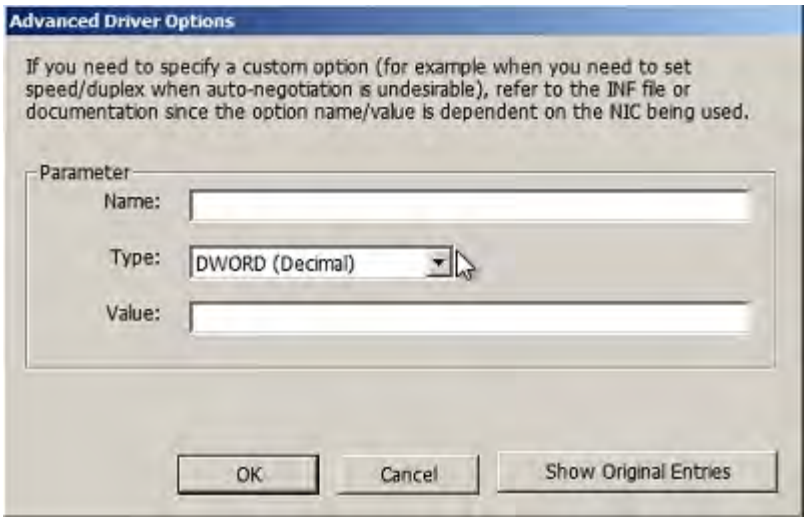


Fig. 2 - Advanced Driver Options.

- 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

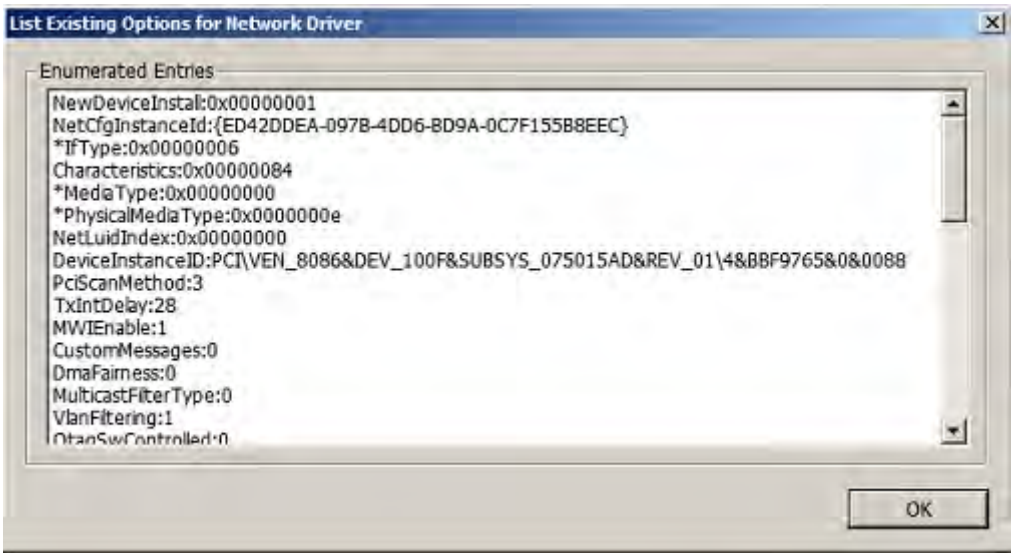


Fig. 3 - Existing Options for Network Drivers.

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

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.

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.

Device Selection

Once the network settings are entered, the storage device can be created/selected. UBDR Gold has the ability to utilize 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 “Restore – Select Device” wizard will automatically begin. The wizard launches when you first launch and configure UBDR Gold. After the initial wizard, any other changes are done through the manual process.

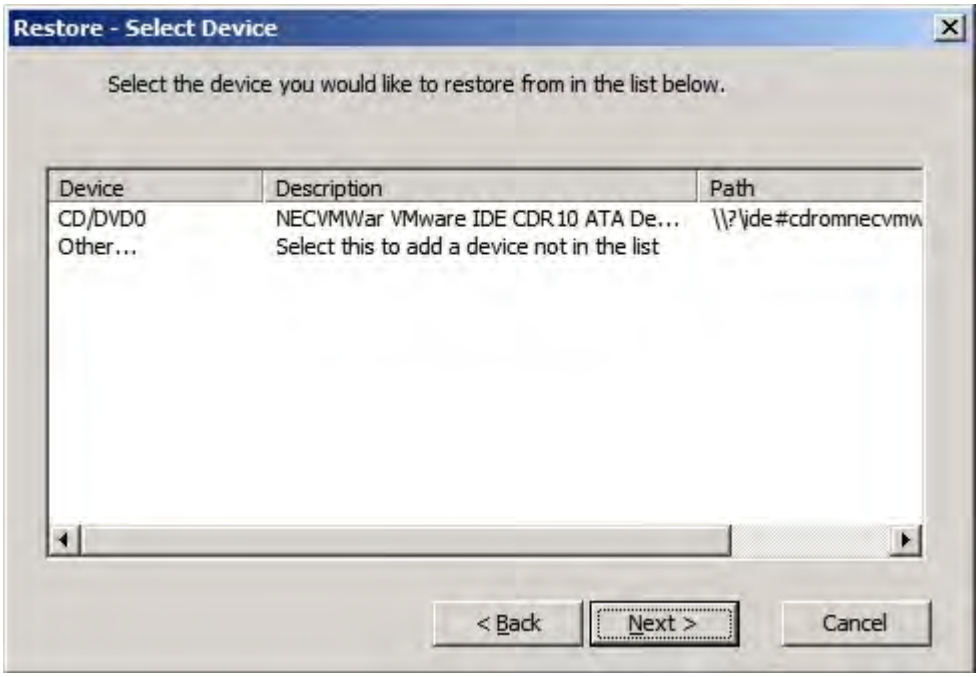


Fig. 4 - UBDR device prompt.

To select a device other than any automatically enumerated tape or CD/DVD devices, select "Other" and click "Next."

NOTE: A local tape device will only enumerate if the tape device driver is recognized by UBDR Gold. The tape device driver can be manually added using the “Advanced Driver Options” under NIC configuration above.

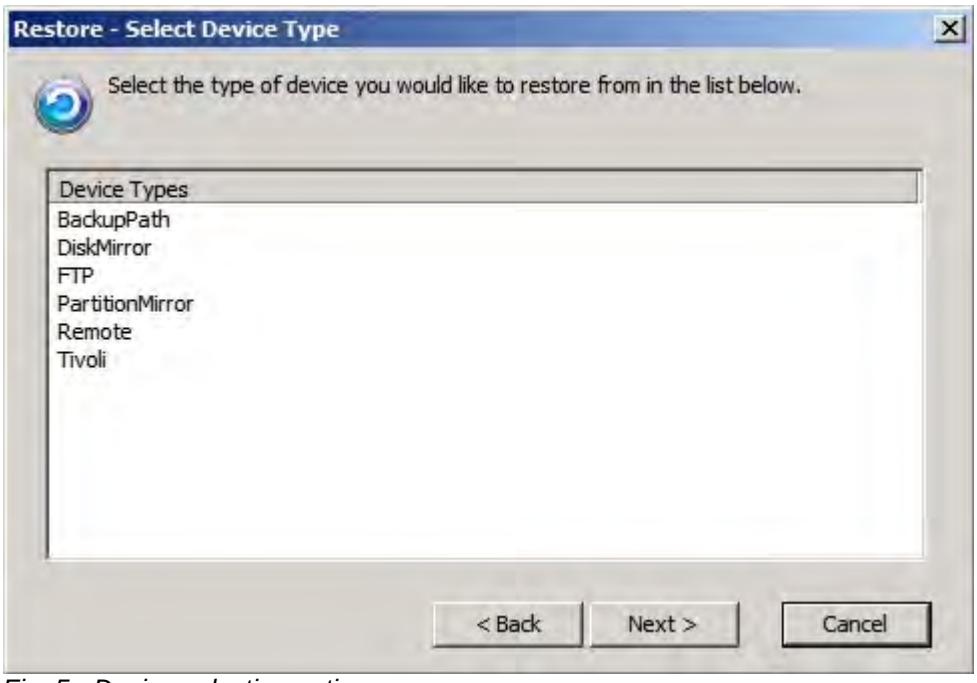


Fig. 5 - Device selection options.

Each device type selection will bring up a different configuration window. Each device type configuration will be covered below through the manual Storage Device configuration.

1. To exit the initial wizard and manually configure the storage device type, click “Cancel,” which brings you to the main UltraBac Management Console.
    - If you stay in the wizard, once the device configuration is complete it will automatically take you to the “Restore Backup from Media Index” and begin the steps under “Starting the Restore.”

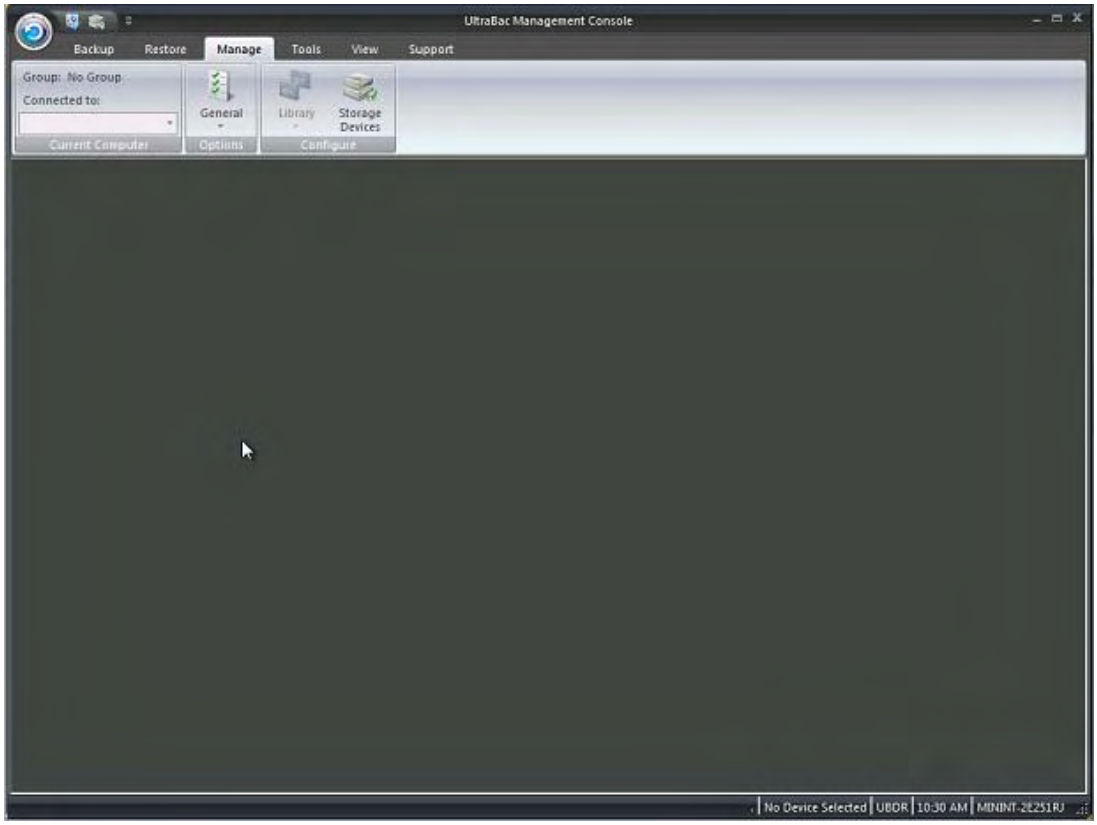


Fig. 6 - UltraBac Management Console.

2. Click the "Manage" tab and select "Storage Devices."



Fig. 7 - Storage Devices.

Tape Devices

In the UltraBac Storage Device Manager, tape devices will automatically be listed if the driver is recognized. UltraBac will automatically assign names to these devices, starting with Tape0.

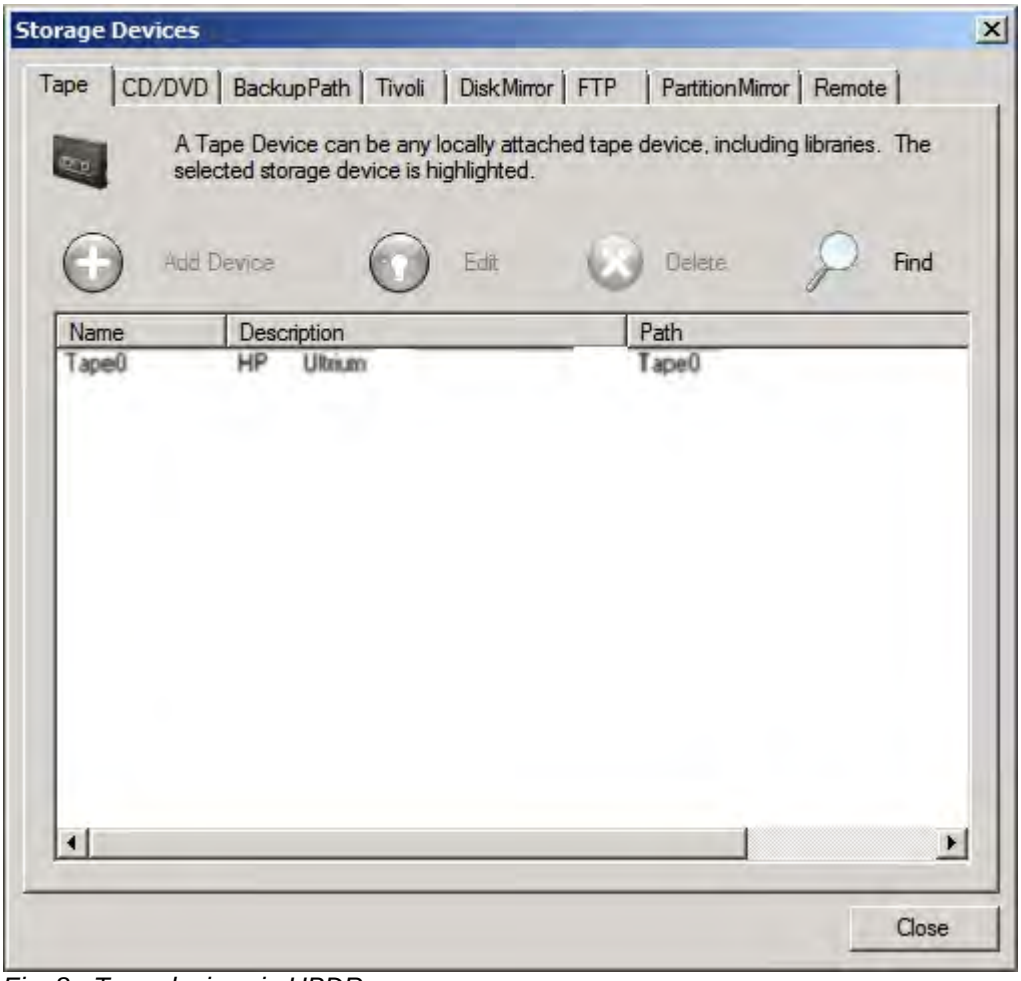


Fig. 8 - Tape devices in UBDR.

CD/DVD Device

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

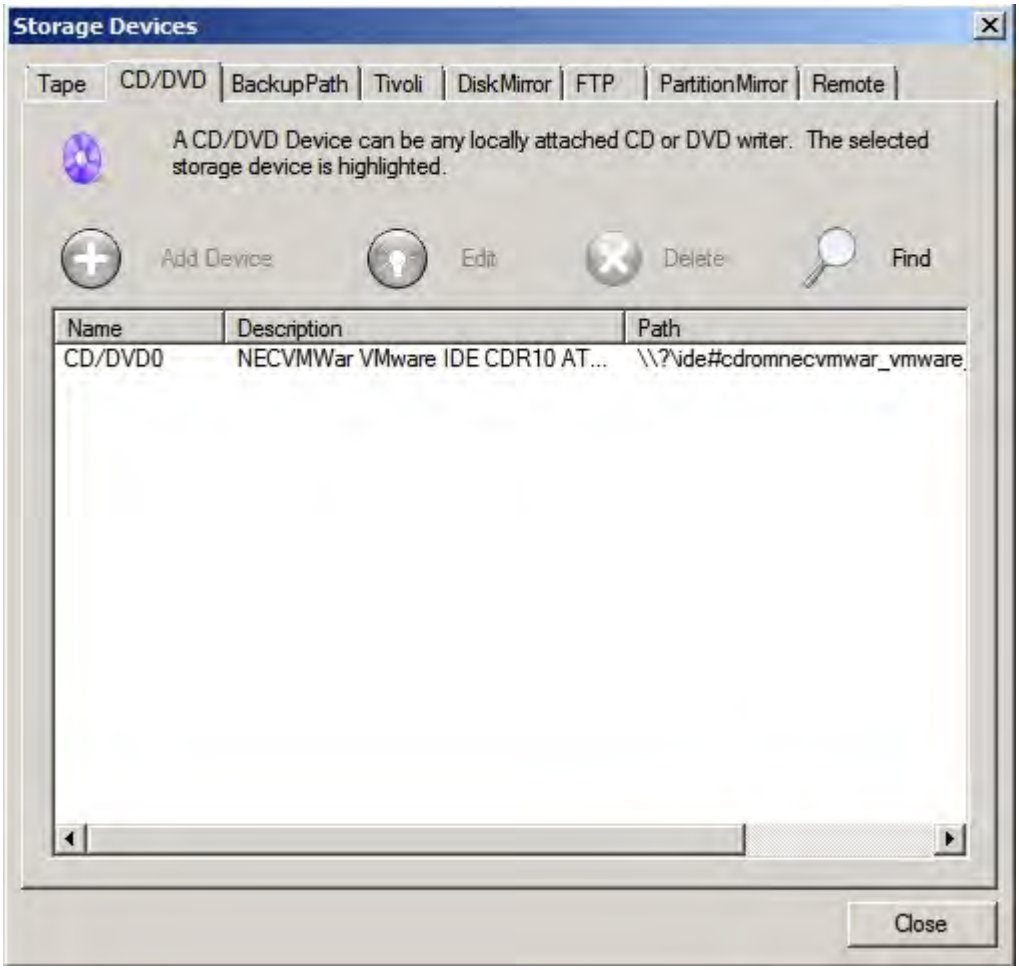


Fig. 9 - CD/DVD devices in UBDR.

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.

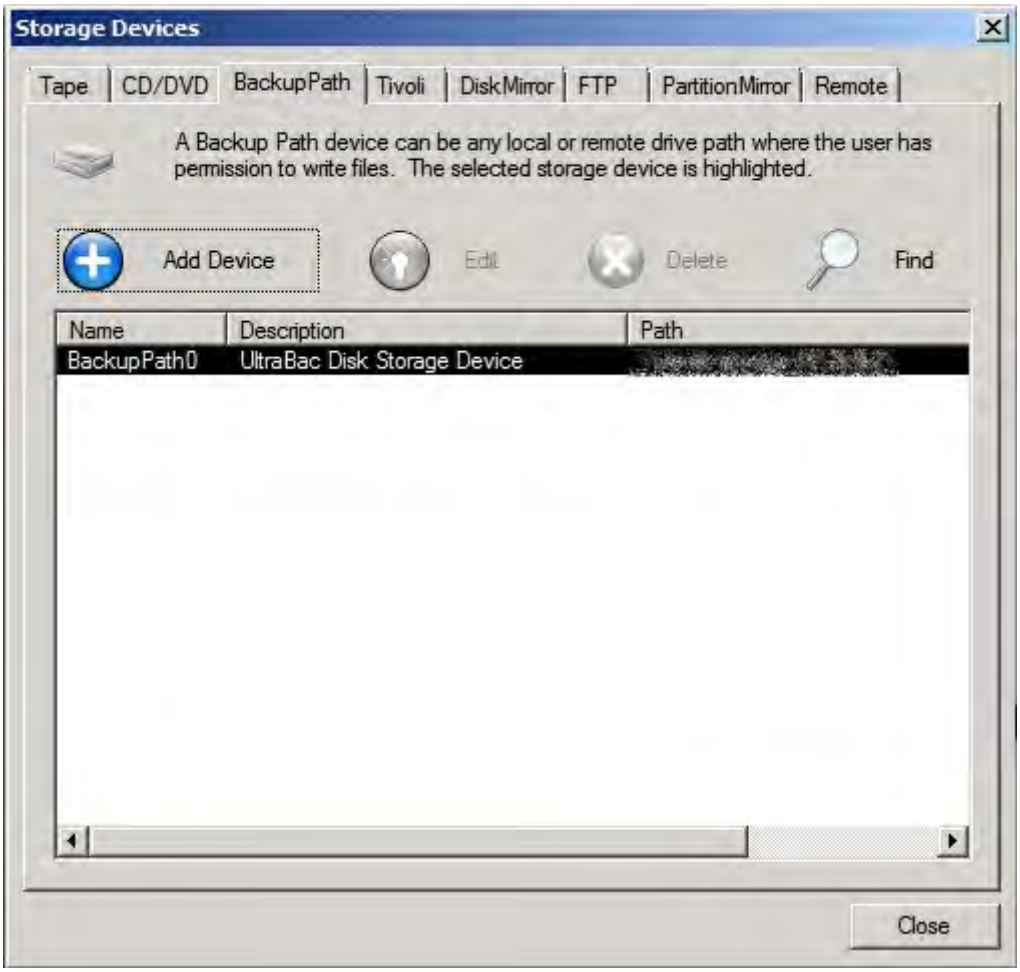


Fig. 10 - BackupPath in UBDR.

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.
    - It is not necessary to enter the "Media Limit MB" field, or the "File Limit MB" field.
5. Click "OK" to save.

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.

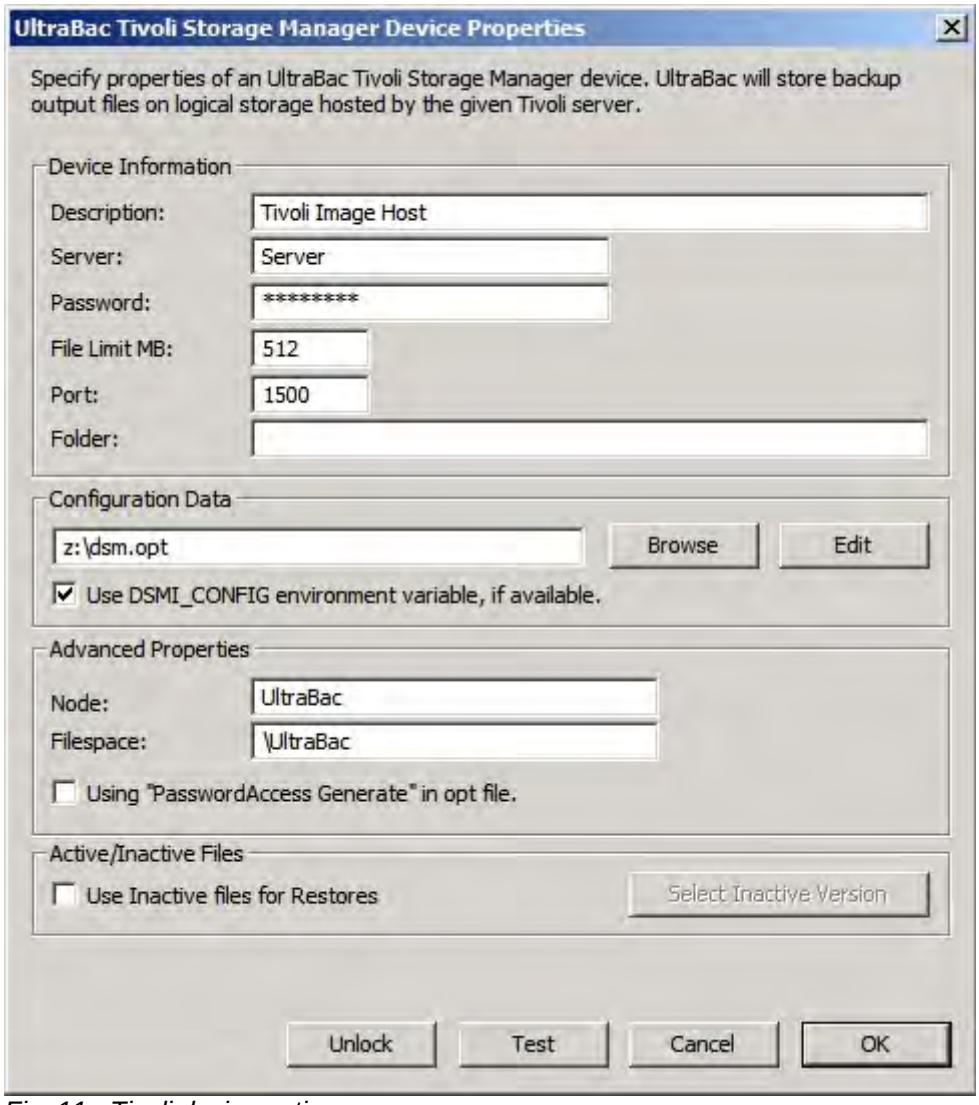


Fig. 11 - Tivoli device options.

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.

Configuration Data

- Configuration Data – This is the TSM Client config file, and defines things such as 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.

Advanced Properties

- 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.

Active/Inactive Files

- 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.

9. Click "Test" to ensure the device is working properly.
10. Click "OK" to save.

DiskMirror and Partition Mirror Devices

If UBDR Gold is being used to perform a static mirror image backup, the creation of either a DiskMirror or PartitionMirror 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.

- DiskMirror device – If a hard disk is present with all partitions deleted, it will be available for addition as an Image device.
- PartitionMirror 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.

FTP Device

To add an FTP device:

1. Select the FTP tab.
2. Click the "Add Device" button.

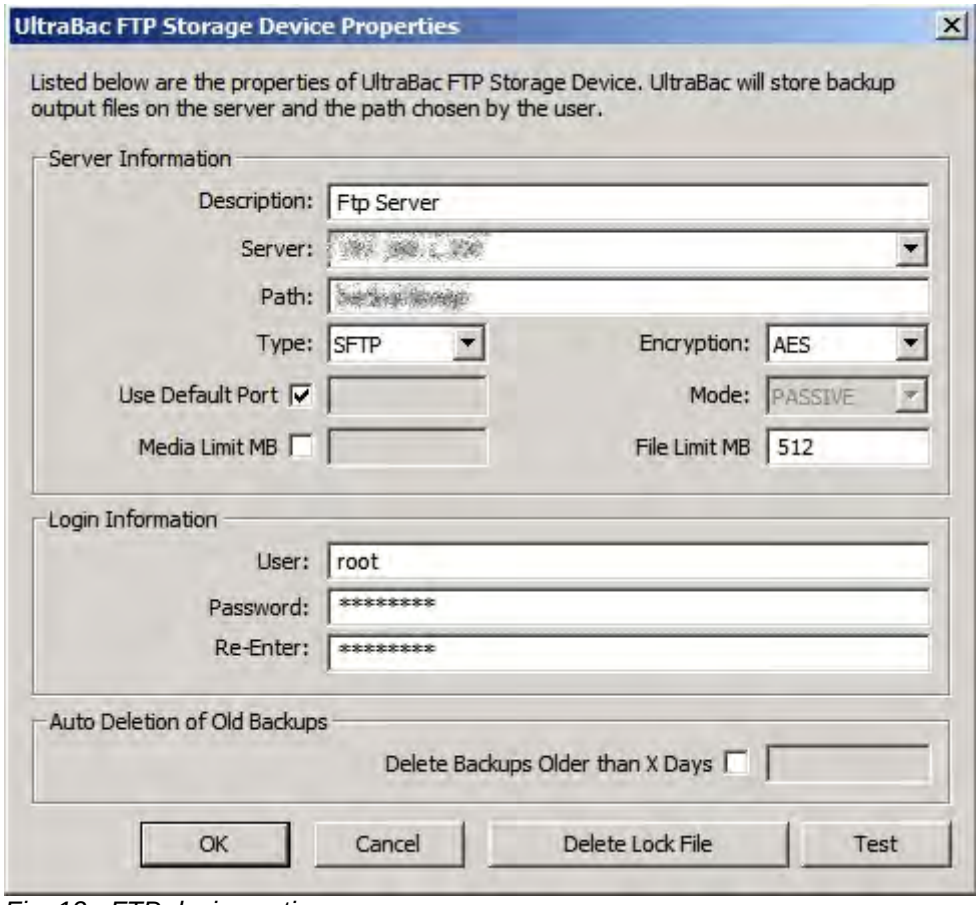


Fig. 12 - FTP device options.

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.

NOTE: It is not necessary to enter the maximum size in the "Media Limit MB" field or "File Limit MB" field. It is recommended to leave both these items at the default value.

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.

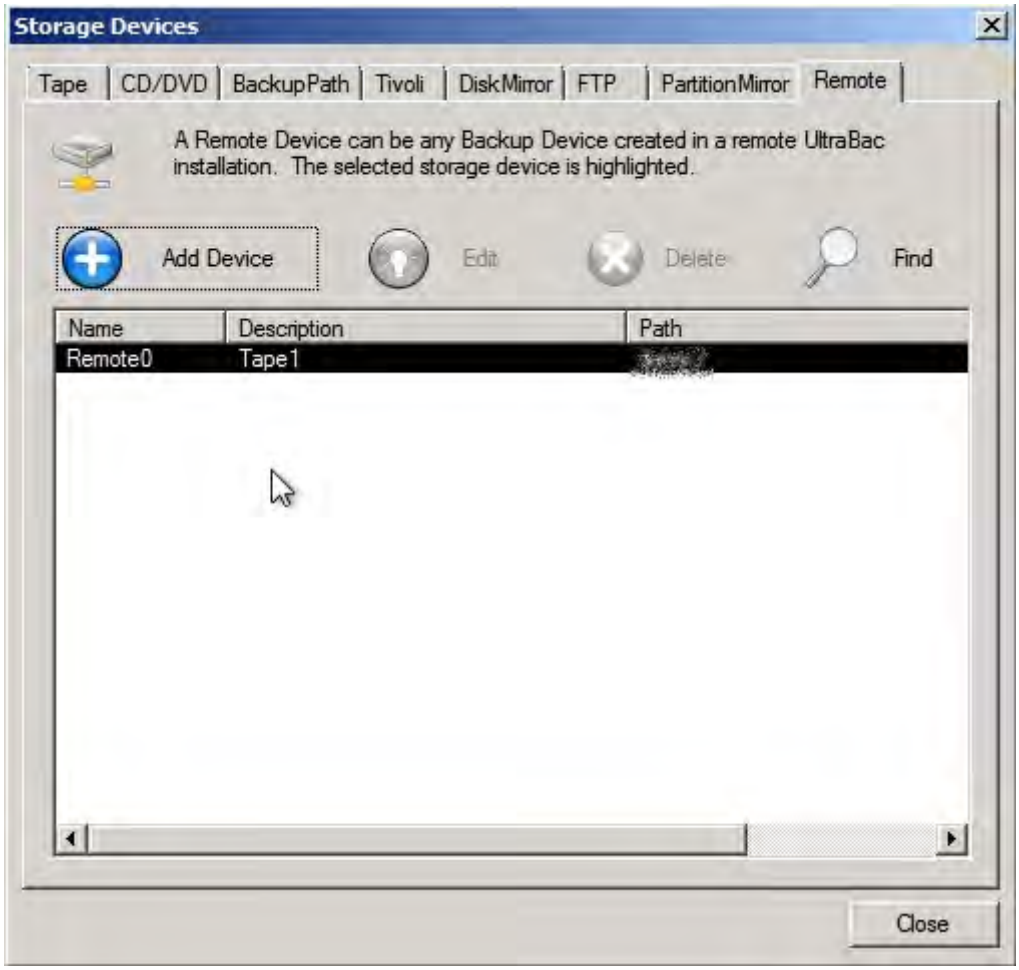


Fig. 13 - Remote devices in UBDR.

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

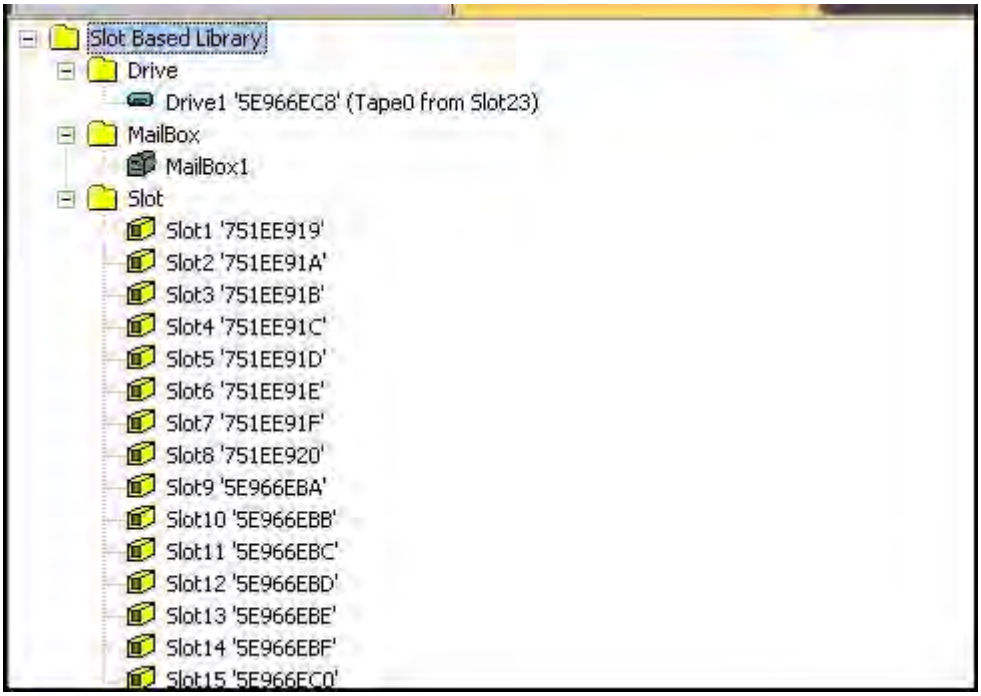


Fig. 14 - Media library controls.

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.

1. From the UltraBac Management Console screen, click the “Restore” tab and select “Media.” UBDR Gold will automatically begin searching the media for backup sets.
    - If you configured the storage device selection using the initial wizard, than you will already be at the “Restore Backup from Media Index” screen.

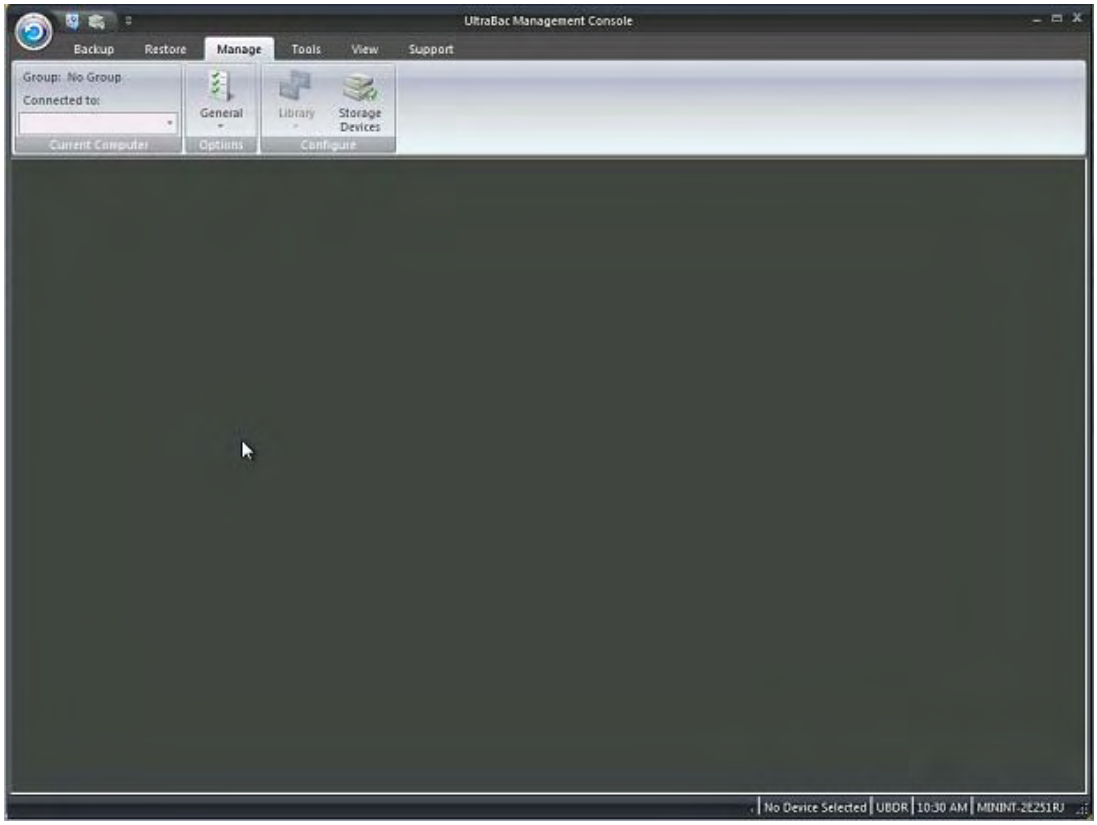


Fig. 15 - Restore tab.

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

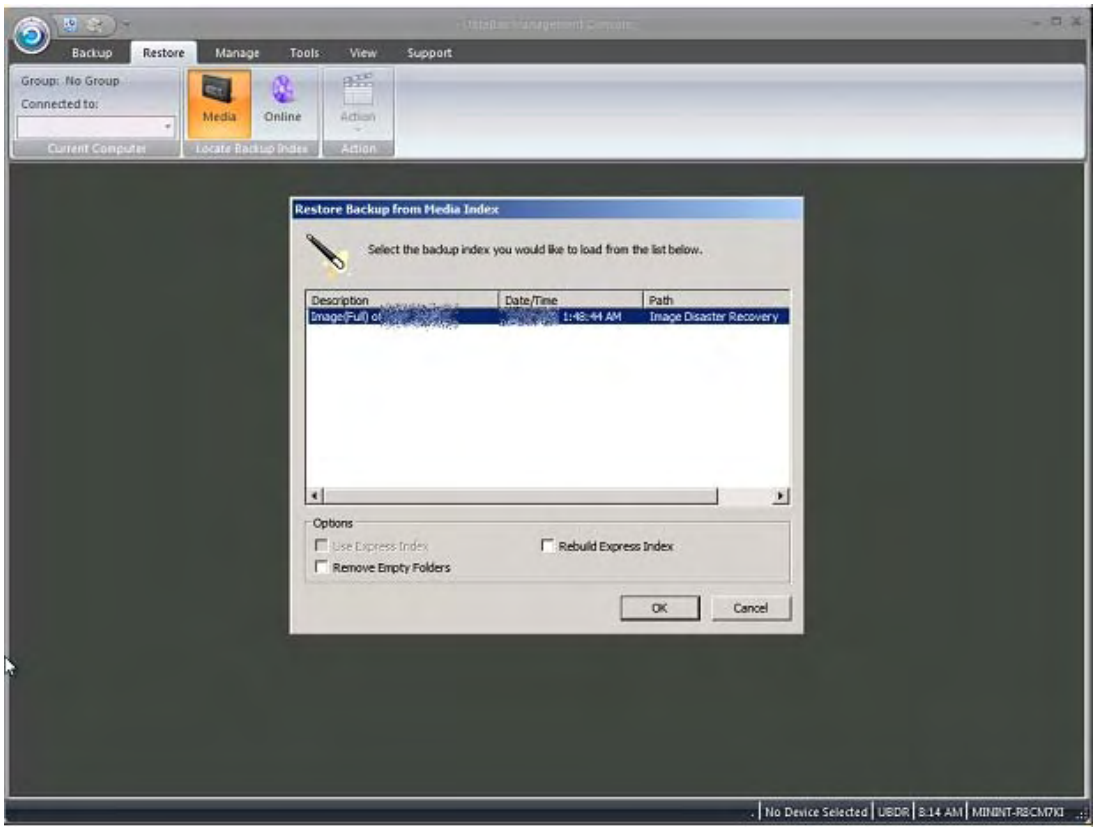


Fig. 16 - "Restore Backup from Media Index" set selection.

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 Hyper-V Server) or even a new system with dissimilar hardware.

By default, when using the initial wizard, all disks and partitions in the backup index are selected for restore and you are taken to the "Image Restore" wizard.

- If during the Device Selection or Starting the Restore process, you left the wizard to perform manual configurations, you will need to manually select the drive(s)/partition(s) to restore and click "Action"/"Restore this Backup" to bring up the Image Restore wizard.

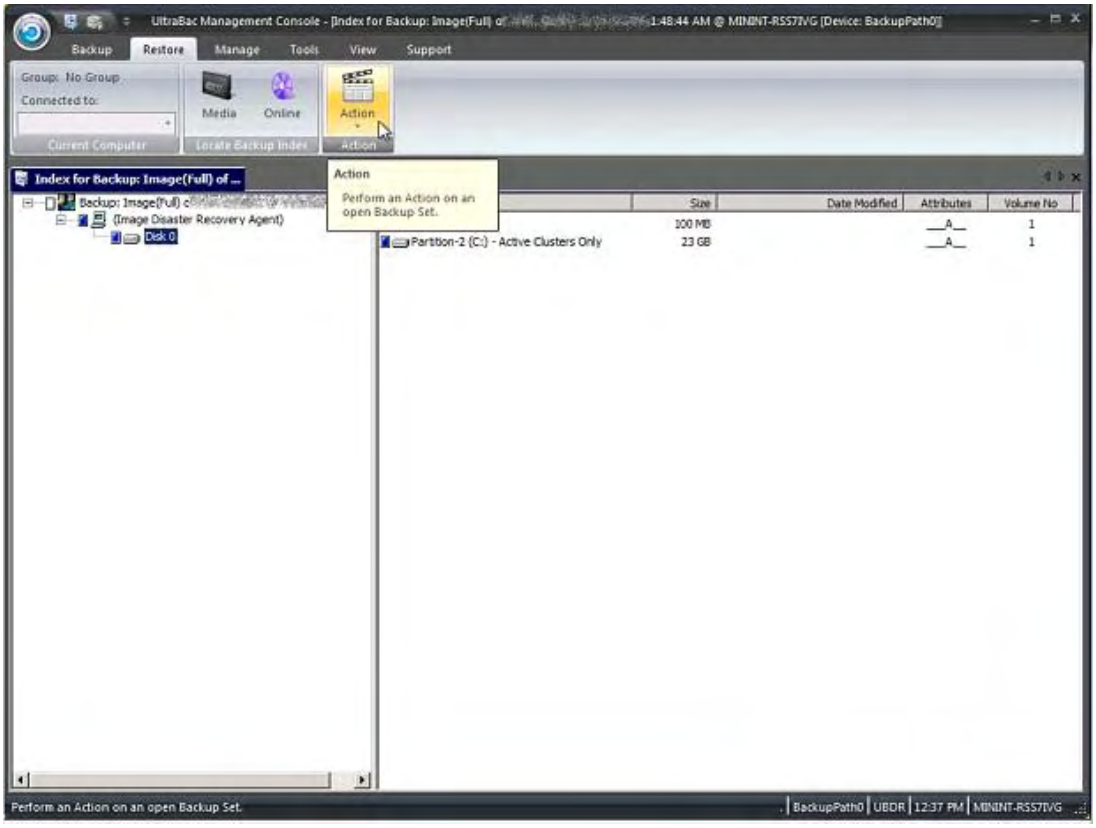


Fig. 17 - "Action" icon for "Restore this Backup."

The Image Restore wizard allows the selection of individual tools, as well as other advanced operations and utilities to be accessed. There are two image restore modes – Express Mode and Advanced Mode.

- If you would like to go to the UltraBac Management Console window to make disk(s) / partition(s) changes, click "Cancel" on the Image Restore Method screen to return to the main UltraBac window.

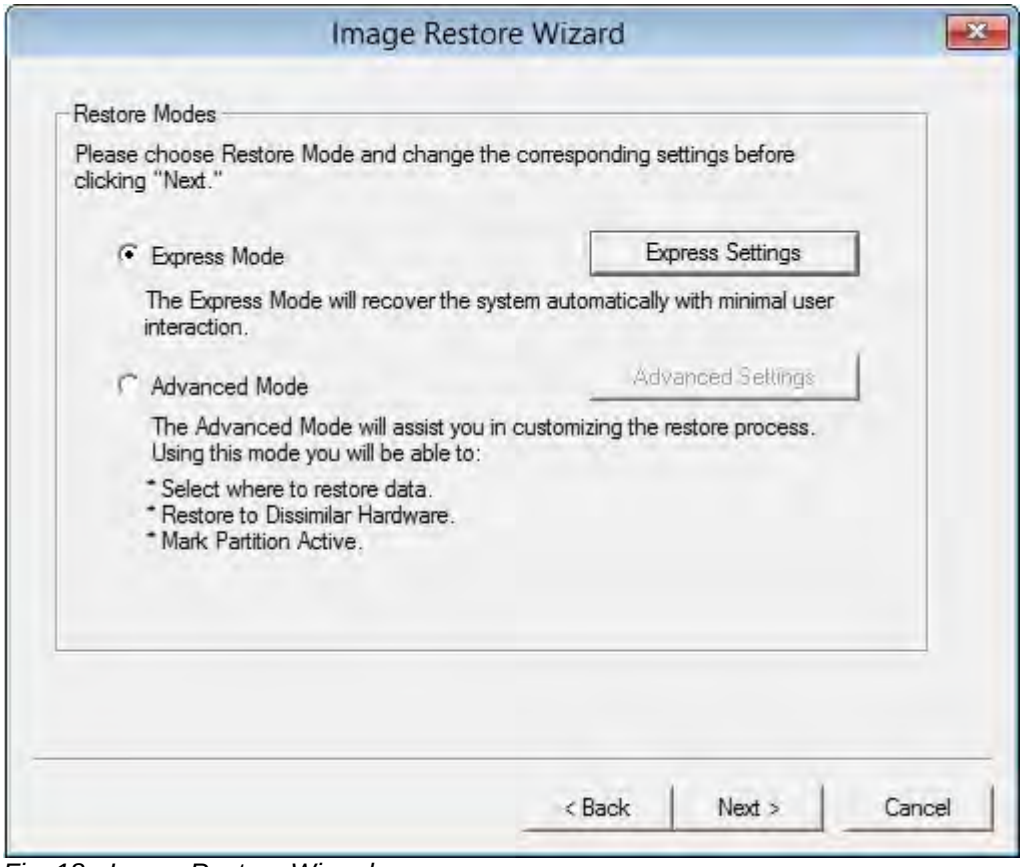


Fig. 18 - Image Restore Wizard.

Express Mode

This option will allow you to restore back to the original system with minimal user action required.

When this setting is selected, UBDR will scan to see if it can detect the original backup source disk. The options available will be based on what is detected.

> NOTE: Express Mode only works on backups created with UltraBac Version 9.3.5 or later. To restore backups created by earlier versions of UltraBac please use "Advanced Mode."

Restore Process when Original Source Disk is Found

1. When the source disk is found, it will give you the ability to restore the Master Boot Record (if desired).

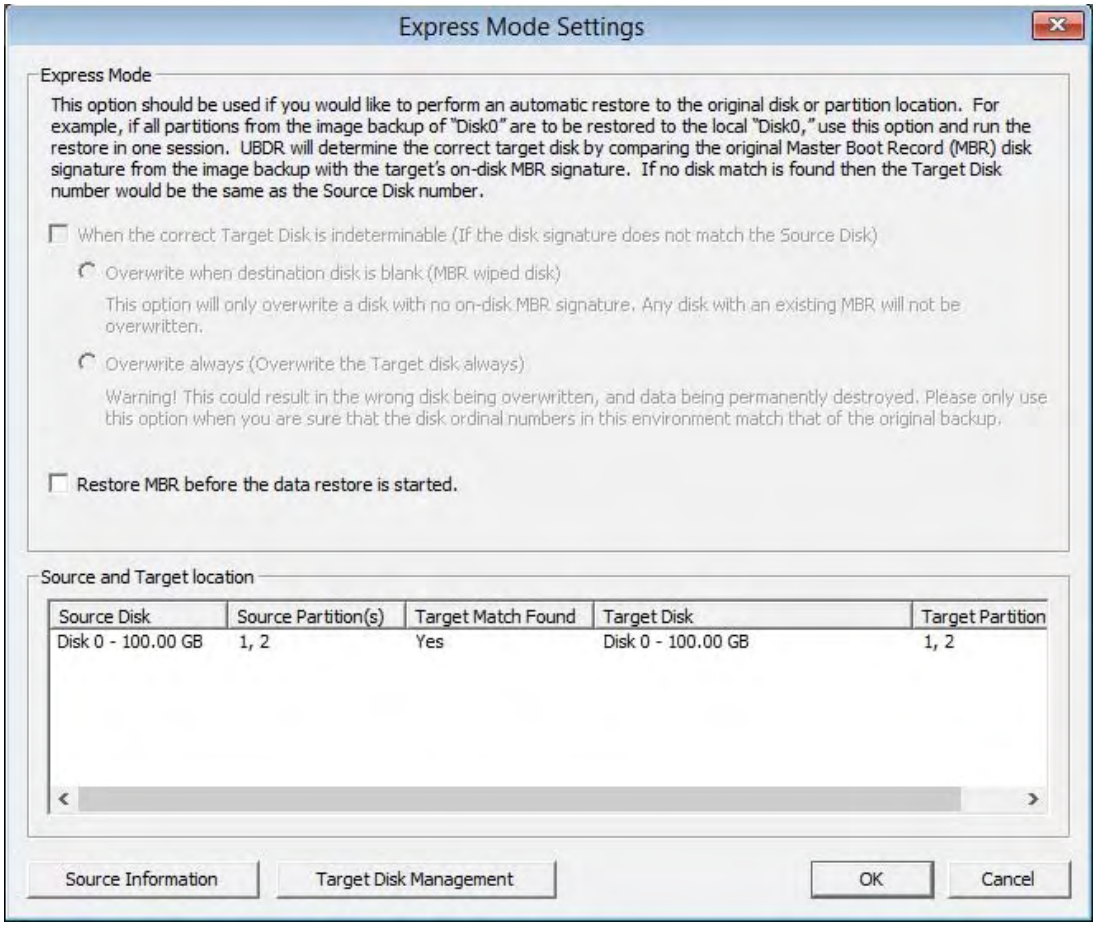


Fig. 19 - Express Mode settings.

2. To continue the restore click ”OK.”
3. A warning prompt that this process will overwrite any data that is currently on the disk will appear. Click "Yes" to continue.

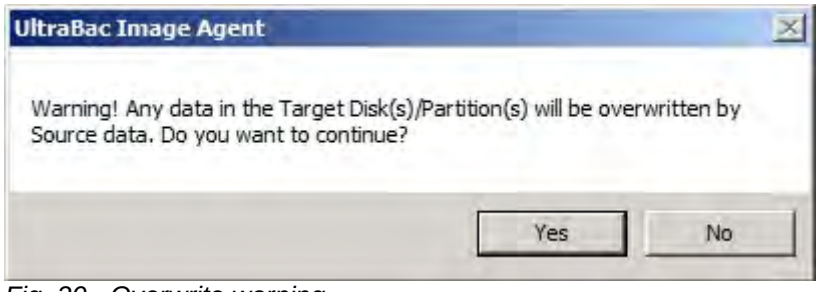


Fig. 20 - Overwrite warning.

4. At the Image Restore wizard screen. Click "Next" to continue.

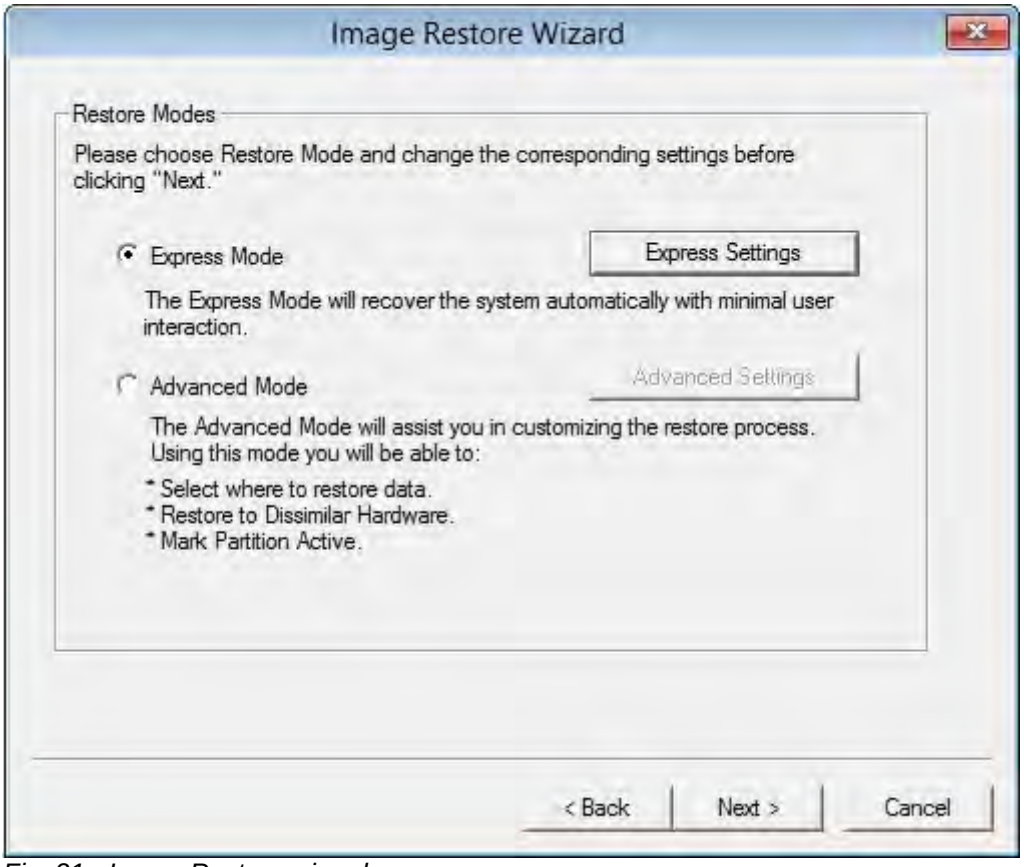


Fig. 21 - Image Restore wizard.

5. On the Restore Options screen there are two additional options:
    - Run Unattended – This option will allow the restore to continue even if any errors or warnings come up during the restore process. If this option is not selected, the restore process will wait until the user responds to the error.
    - Eject media after restore – This option is used when restoring from tape drives and will eject the media once the restore process is complete.

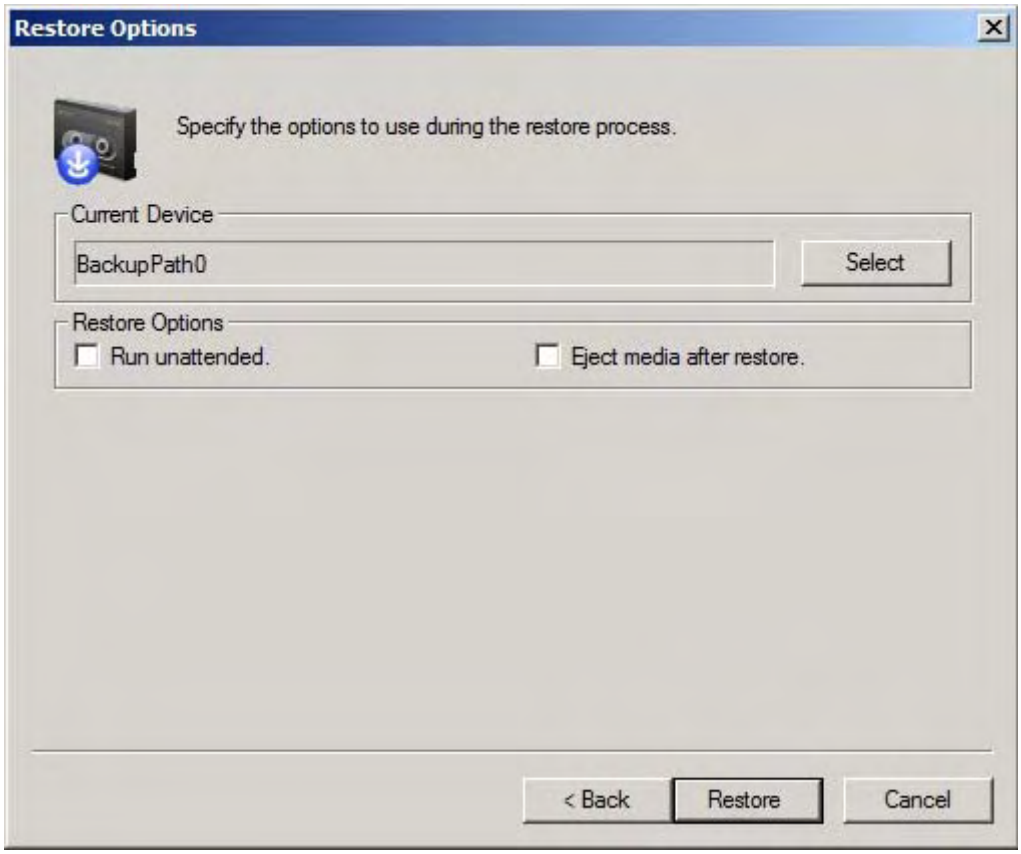


Fig. 22 - Restore Options.

6. Click the "Restore" button to start the restore.
7. Once the restore is complete, reboot the computer.

Restore Process when Original Source Disk in Not Found

1. When the Original Source disk is not detected it provides two additional options:
   - Overwrite when the disk is blank – Used when there is a disk that does not have a Master Boot Record (MBR) written to it.
   - Overwrite Always – This gives the user the option to overwrite the disk when UBDR is not detecting the disk as the original.

NOTE: When choosing the above options, it is highly recommended to choose the option to restore the MBR.

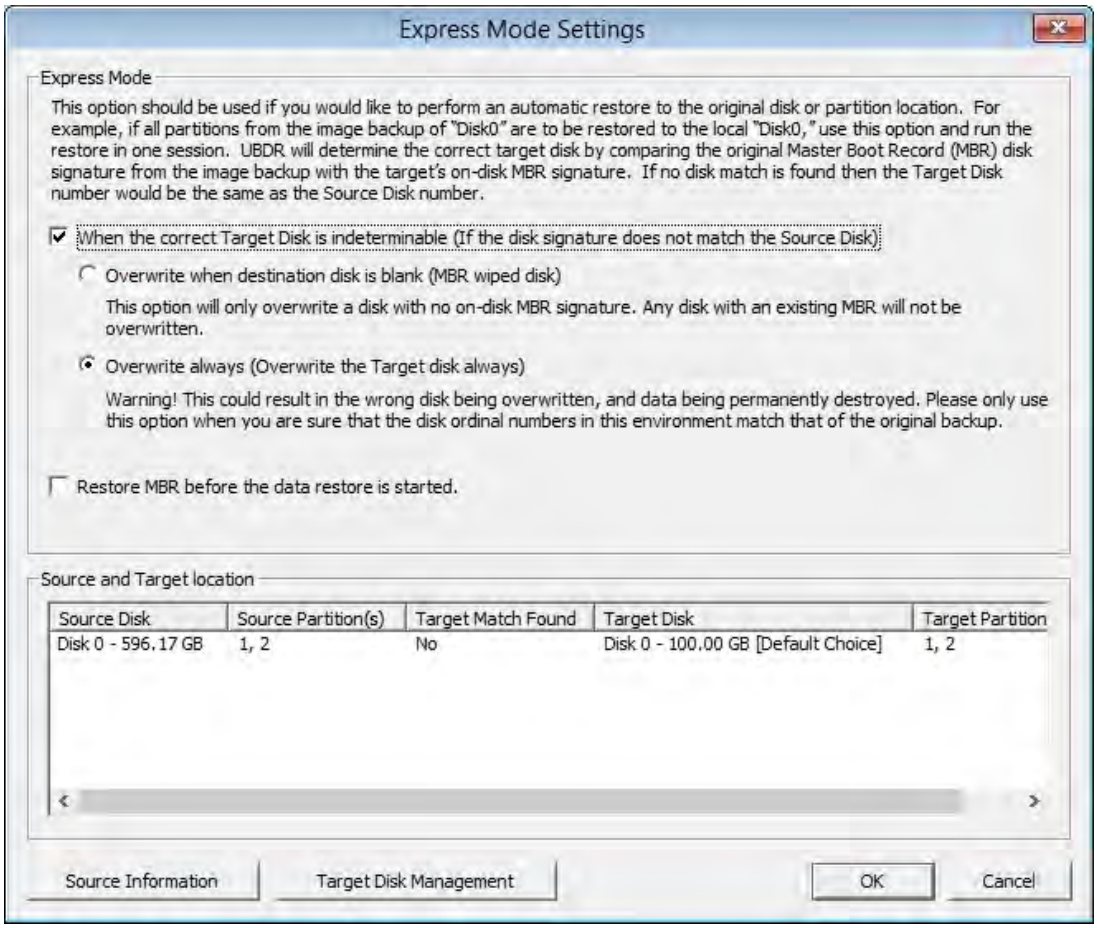


Fig. 23 - Express Mode settings.

2. After selecting an option, click "OK."
3. A warning prompt that this process will overwrite any data that is currently on the disk will appear. Click "Yes" to continue.

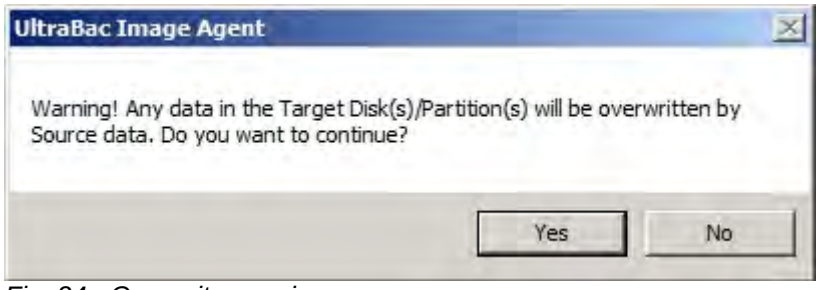


Fig. 24 - Overwrite warning.

4. At the Image Restore wizard screen. Click "Next" to continue.

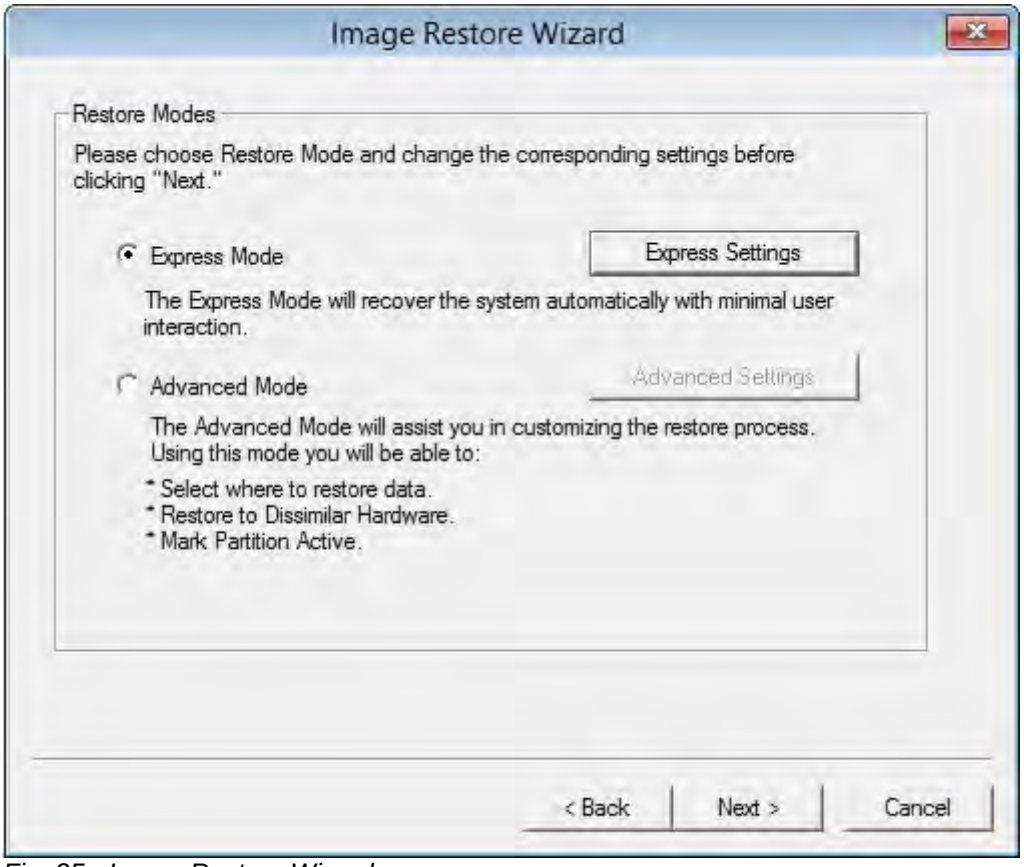


Fig. 25 - Image Restore Wizard.

5. On the Restore Options screen there are two additional options:
    - Run Unattended – This option will allow the restore to continue even if any errors or warnings come up during the restore process. If this option is not selected, the restore process will wait until the user responds to the error.
    - Eject media after restore – This option is used when restoring from tape drives and will eject the media once the restore process is complete.

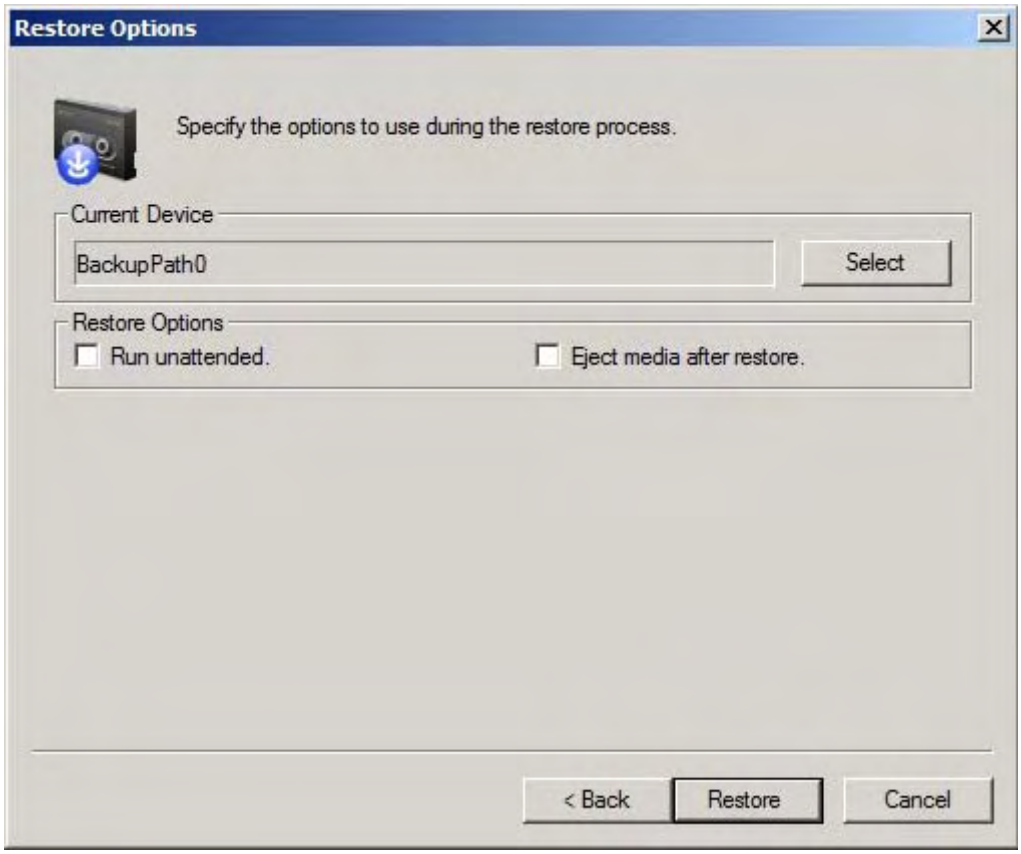


Fig. 26 - Restore Options.

6. Click the "Restore" button to start the restore.
7. Once the restore is complete, reboot the computer.

Additional Options

Source Information:

> NOTE: Source information only appears with backups made using UltraBac Version 9.3.5.

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

- Disk Number
- Disk Size
- Disk Type
- Partition Number
- Partition Size
- Drive Letter
- Active Partition y/n
- Boot Partition y/n
- Volume Label
- File System

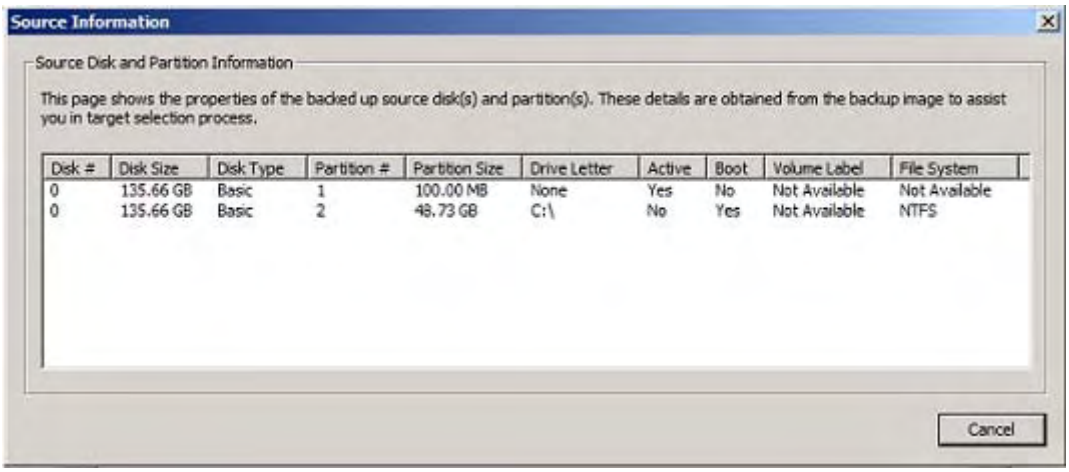


Fig. 27 - Source Information.

Target Disk Management:

> NOTE: The options found in the Target Disk Management are typically used when performing an advanced restore. However, the options are available for Express Restores as they give the user the ability to wipe the MBR and they provide more information on the target disk.

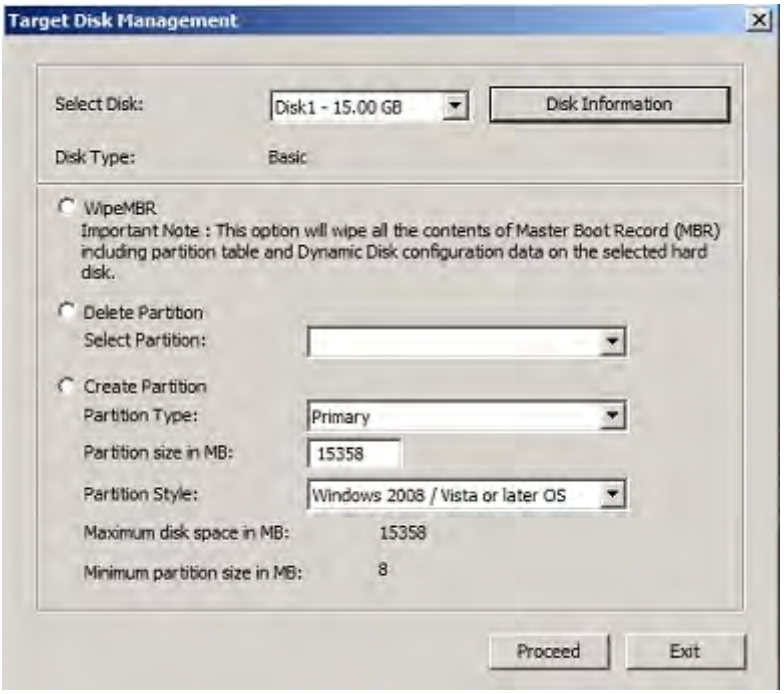


Fig. 28 - Target Disk Management.

Select Disk – This drop-down menu allows the selection of all disks in the system for viewing in the "Advanced Tools" screen. It also allows users to select which disk they want to set options on.

Disk Information – Gives more information on the disk you are restoring to:

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

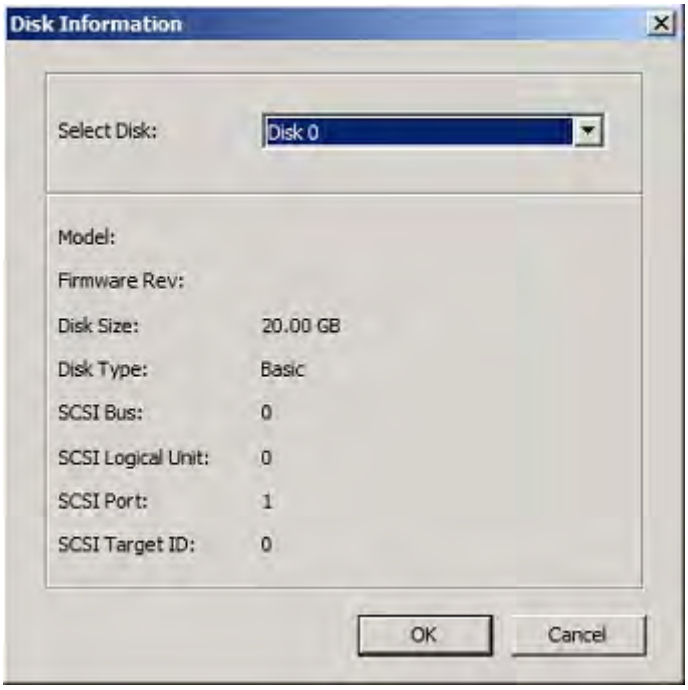


Fig. 29 - Disk Information.

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 the 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.

NOTE: Once the "Proceed" button is clicked, users will not be able to choose any additional options. When the process is done, UBDR will bring up a pop-up box saying

the option is complete.

Advanced Mode

Advanced Mode provides the user with more options during restore, including the ability to restore to different hardware, and the ability to restore to different partitions.

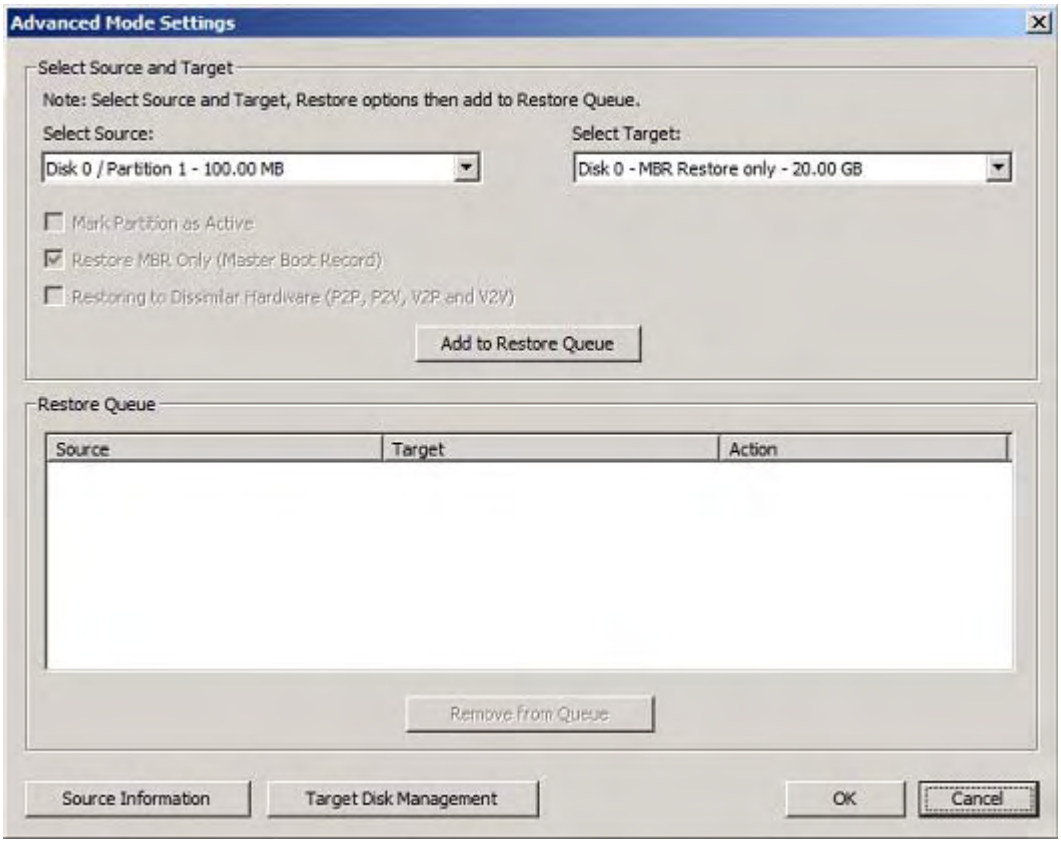


Fig. 30 - Advanced Mode settings.

1. Select the source:

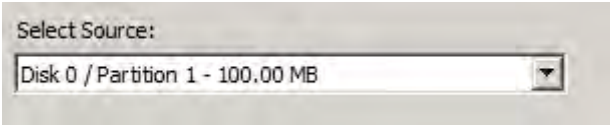


Fig. 31 - Select Source.

2. Select Target disk to restore to:

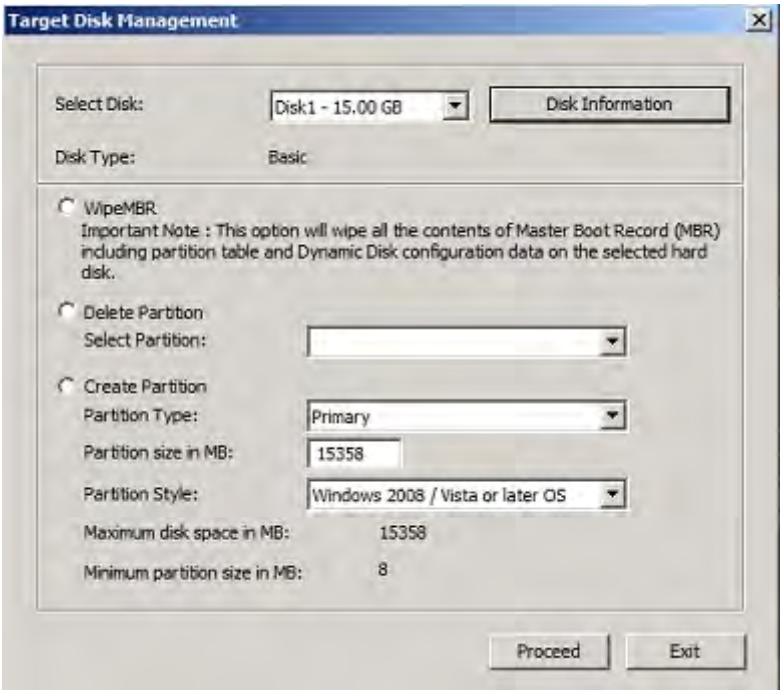


Fig. 32 - Select Target.

3. Choose Restore Options.
    - Mark Partition as Active – Only needed if MBR was not restored.
    - Restore MBR Only – Restores the MBR.
    - Restoring to Dissimilar Hardware – Brings up an additional screen allowing the user to set options to restore to different hardware.

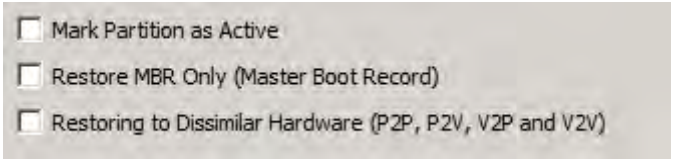


Fig. 33 - Restore Options.

4. Select "Add to Restore Queue." User selection(s) will be listed in the "Restore Queue" box.

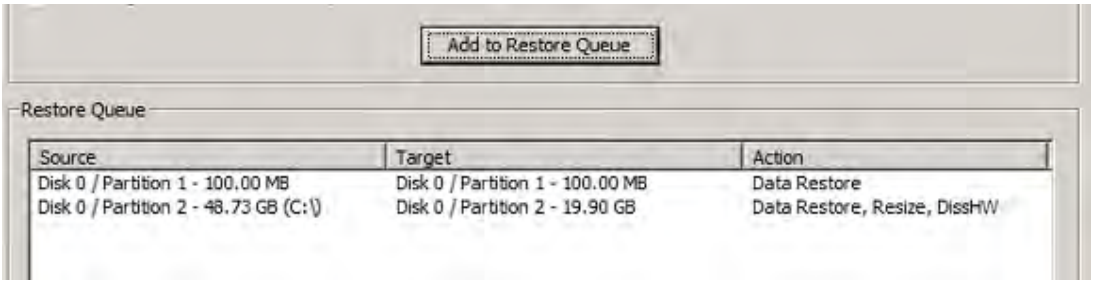


Fig. 34 - Restore Queue.

5. Click "OK."
6. At the Image Restore wizard screen click "Next" to continue.

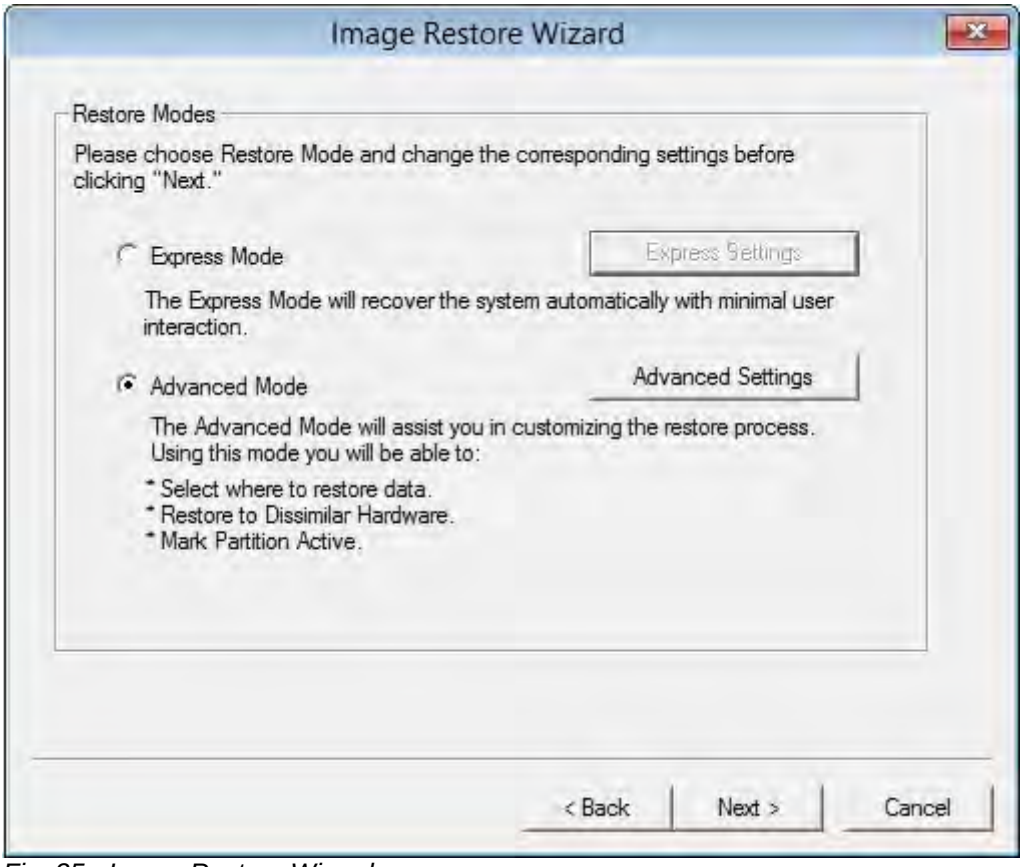


Fig. 35 - Image Restore Wizard.

7. On the Restore Options screen there are two additional options:
    - Run Unattended – This option will allow the restore to continue even if any errors or warnings come up during the restore process. If this option is not selected, the restore process will wait until the user responds to the error.
    - Eject media after restore – This option is used when restoring from tape drives and will eject the media once the restore process is complete.

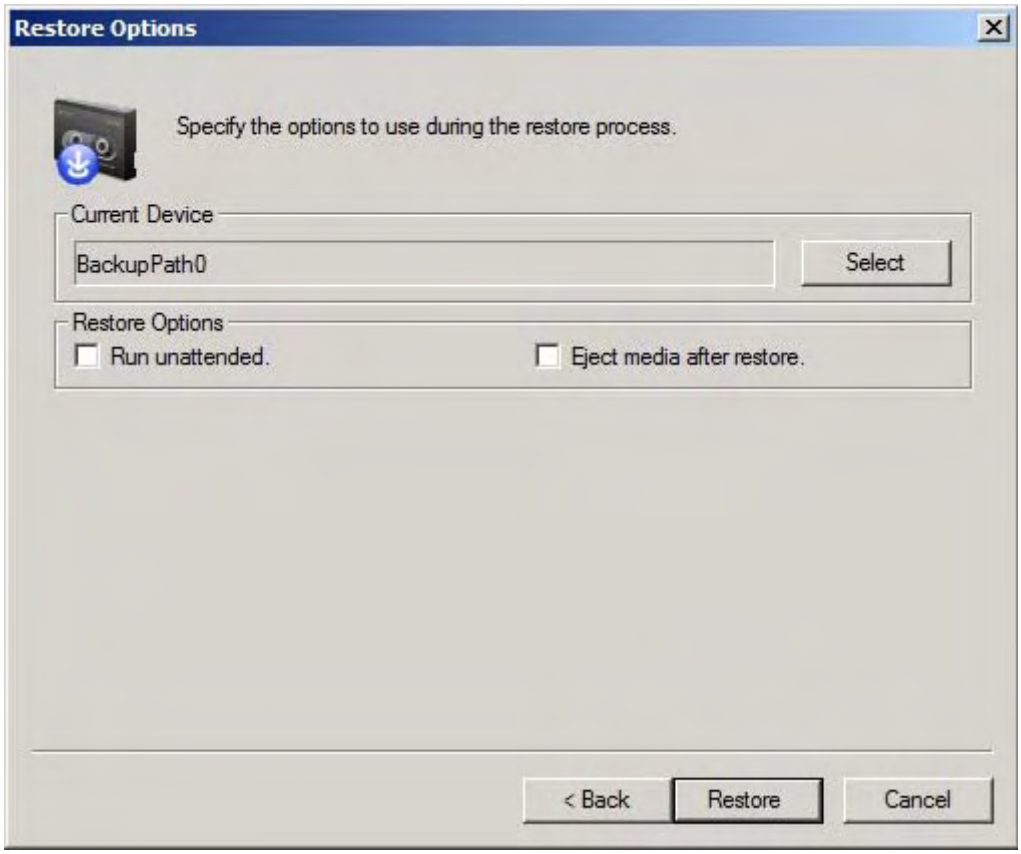


Fig. 36 - Restore Options.

8. Click the "Restore" button to start the restore.

Restoring Only the Master Boot Record (MBR)

1. Select a partition on the Source disk (it doesn't matter which partition is selected).

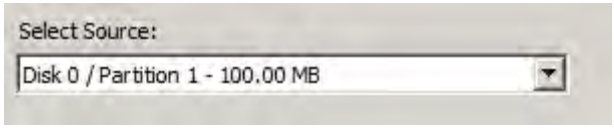


Fig. 37 - Select Source.

2. Select a partition on the Target disk (it doesn't matter which partition is selected).

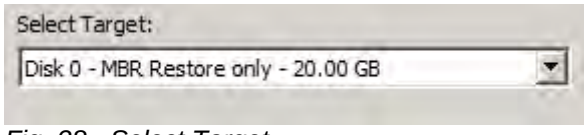


Fig. 38 - Select Target.

3. Check the option "Restore MBR Only."



Fig. 39 - Restore MBR Only.

4. Click the "Add To Restore Queue" button.



Fig. 40 - Add to Restore Queue.

5. The job is added to the queue.

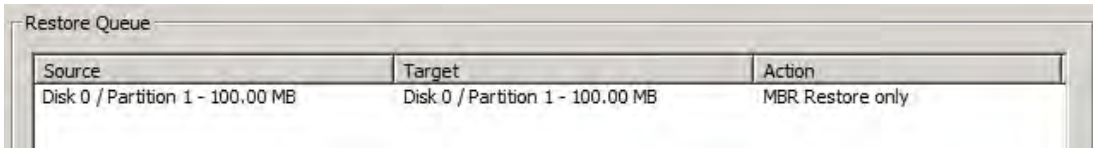


Fig. 41 - Restore Queue.

6. Click "OK."
7. On the Image Restore wizard screen, click "Next" and perform the restore.

Restoring to Different Hardware

> NOTE: The option to restore to different hardware is only available when restoring to the OS partition.

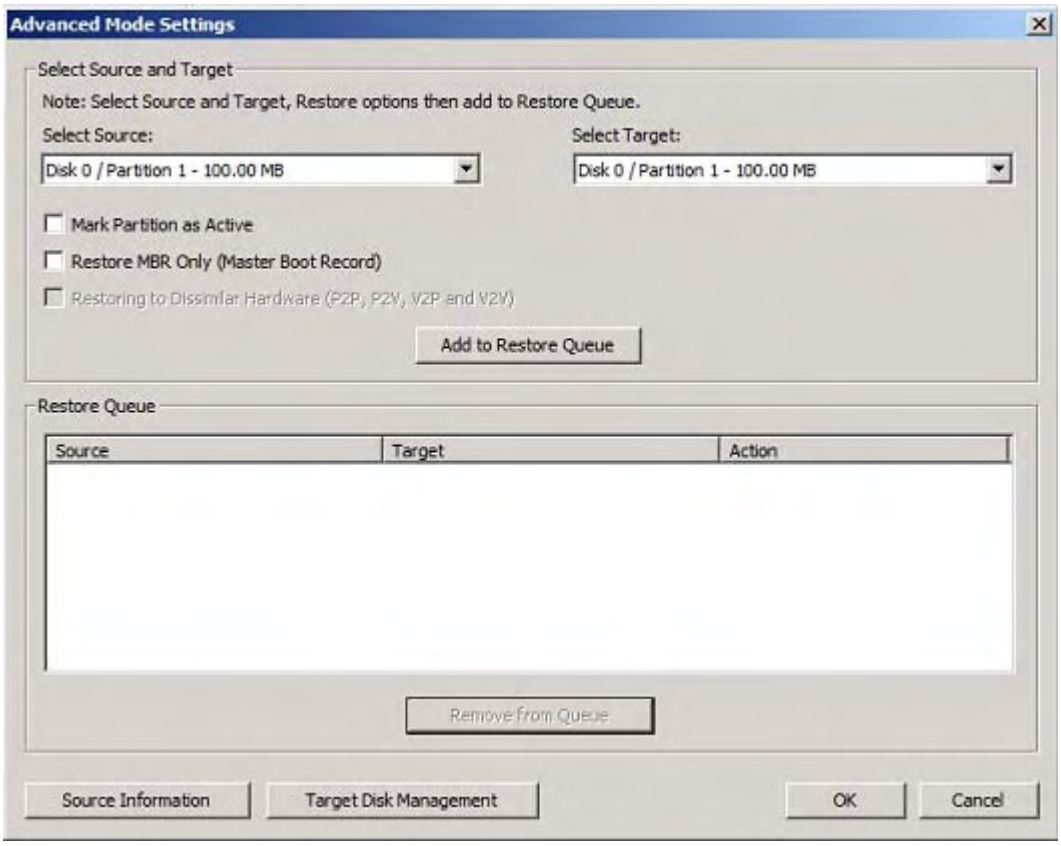


Fig. 42 - Advanced Mode Options.

1. Select the OS partition on the Source disk.



Fig. 43 - Select Source.

2. Select the Target partition.

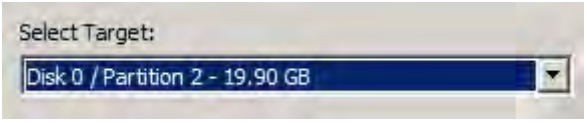


Fig. 44 - Select Target.

3. Choose the option to Restore to dissimilar hardware. This will automatically bring up a new option screen. In most cases, the recommended option is all that is needed. If a specific driver is required that is not in the UBDR Gold library, it can be installed at this point in the operation.

NOTE: In most cases, if the Target disk is listed for restore, UBDR already has the driver for the dissimilar hardware in its library.



Fig. 45 - Dissimilar Hardware Restore Options.

4. Click the "Add To Restore Queue" button.
5. The job is added to the queue, which will show under "Action" as "DissHW."

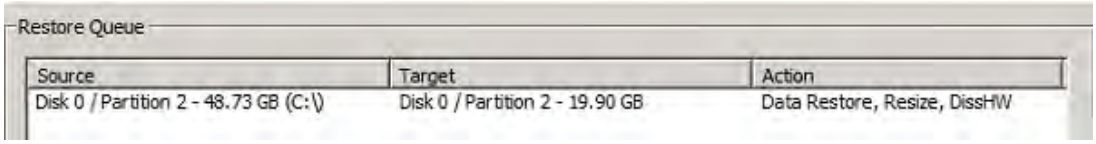


Fig. 46 - Restore Queue.

6. Click "OK."
7. On the Image Restore wizard screen, click "Next" and perform the restore.

Restoring to a Different Size Disk

NOTE: It is recommended to first restore the MBR, and then delete the partitions you want to resize.

Resizing the 100MB / 350MB Windows boot partition can cause the system to not boot properly.

UBDR can restore to a partition size that is 40% smaller than the Source Partition.

1. In Advanced Mode Settings, click on "Target Disk Management."

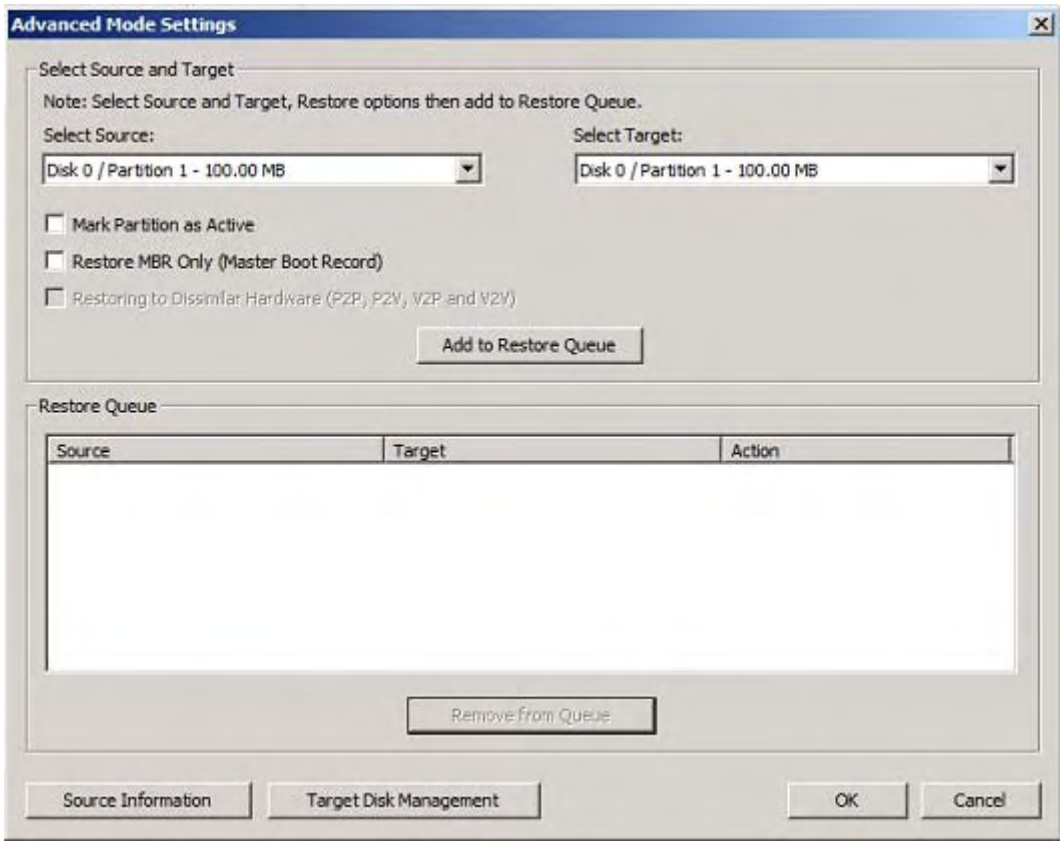


Fig. 47 - Advanced Mode Settings.

2. Select the disk that you want to resize the partition on.

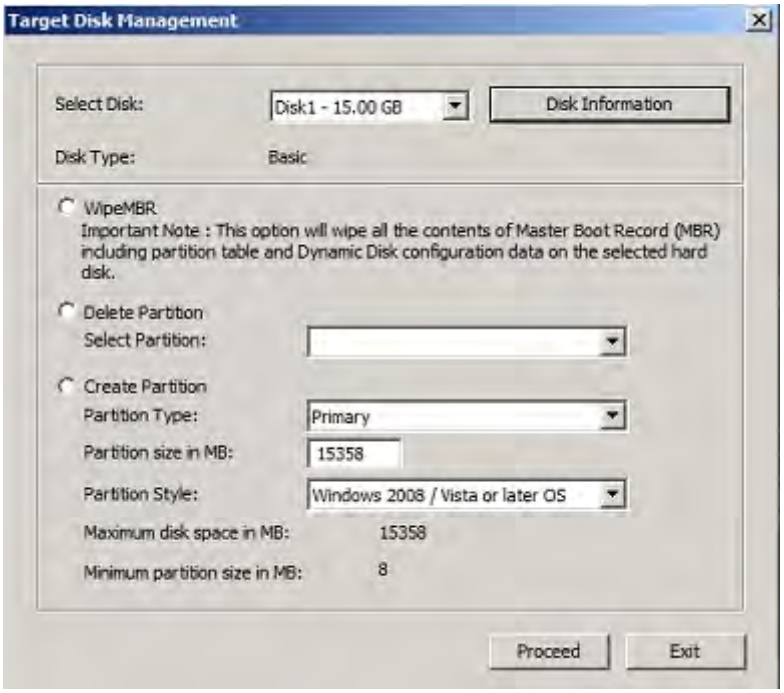


Fig. 48 - Target Disk Management.

3. Select the option to "Delete the Partition," select the partition you want to delete, and then click "Proceed."

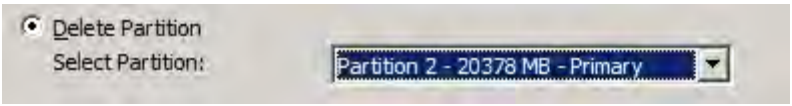


Fig. 49 - Delete Partition.

4. Click "Yes" to proceed when asked to continue.

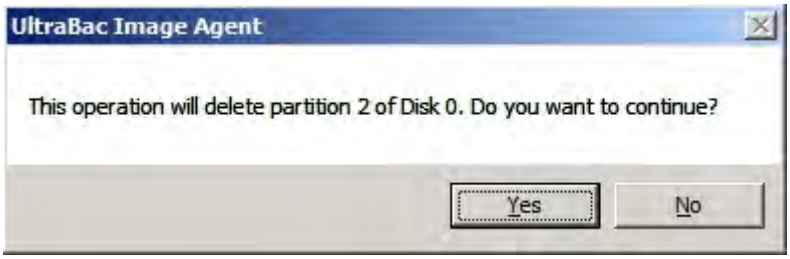


Fig. 50 - Confirmation dialog.

5. Next, select the option to “Create Partition.” Type the size in MB to create, select the Partition Type, and Partition Style and then click “Proceed.”

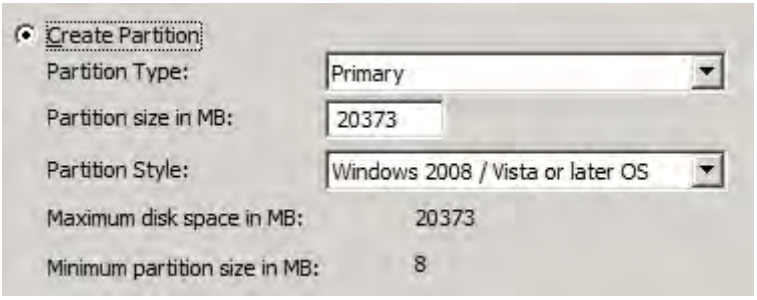


Fig. 51 - Create Partition.

6. The job is added to the queue, which will show under "Action" as "Resize."

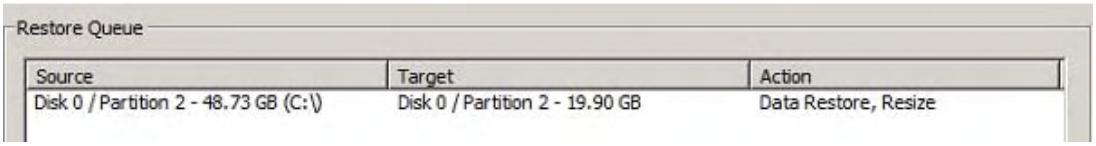


Fig. 52 - Restore Queue.

Restoring Encrypted Backups

When a restore of an encrypted backup is performed, UBDR will automatically bring up the decryption screen.

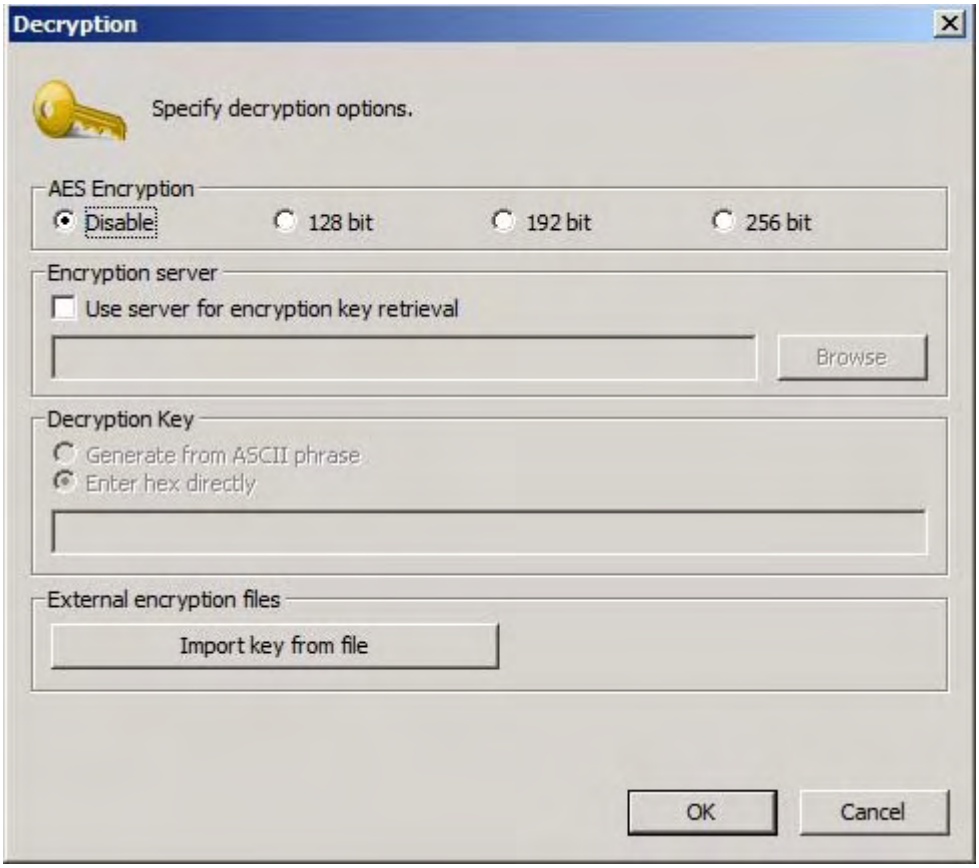


Fig. 53 - Decryption screen.

NOTE: For more information on Encrypted backups please see the UltraBac Knowledge Base: **UBQ000251: Encrypting Backup Data with AES in UltraBac 9.x.**

Pre-Version 9.0 Decryption is not supported. Please use UBDR Gold Version 7.0 to restore.

Restoring a CIP Image Using UBDR Gold

Restoring a CIP Image is not currently supported in this version. Please use UBDR Gold Version 7.0 to perform the restore.

Additional Tools

UBDR has additional tools to assist in troubleshooting, and to simplify the addition of hardware and drivers to the active UBDR booted system.

To access the additional tools, click on the Tools tab in the main UltraBac Management Console window and click the "UBDR" icon.

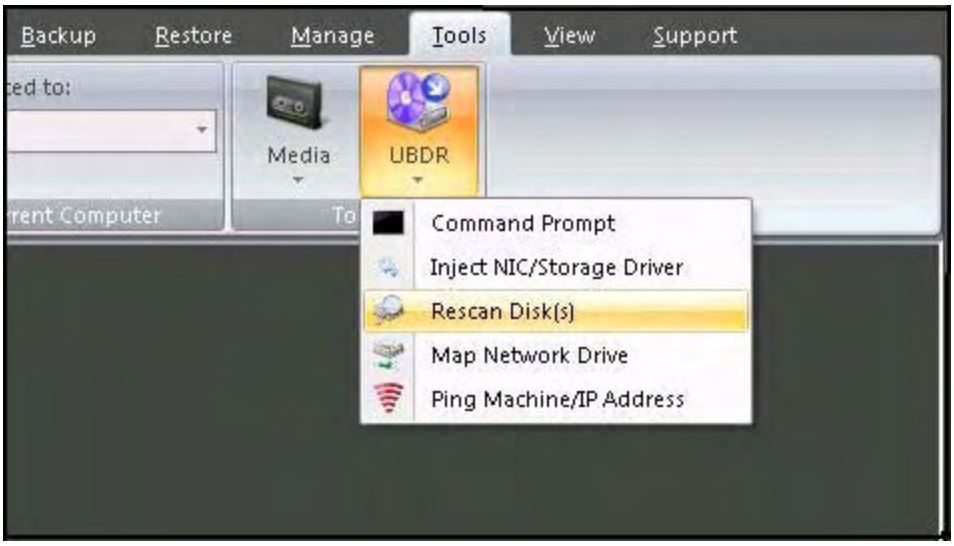


Fig. 54 - Additional UBDR tools.

- 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.

NOTE: For more information on UBDR Gold Advanced Tools and Utilities, please see the UltraBac Knowledge Base:

UBQ000230: UBDR Gold Advanced Tools and Utilities

NOTE: For copying restore logs in UBDR, please see the UltraBac Knowledge Base:

UBQ000158: Copying Restore Logs in UBDR

Command Prompt

"Command Prompt" opens a Windows command line interface (cmd.exe) to perform any additional commands.



Fig. 55 - Windows Command Prompt, running DiskPart.exe.

Inject NIC/Storage Driver

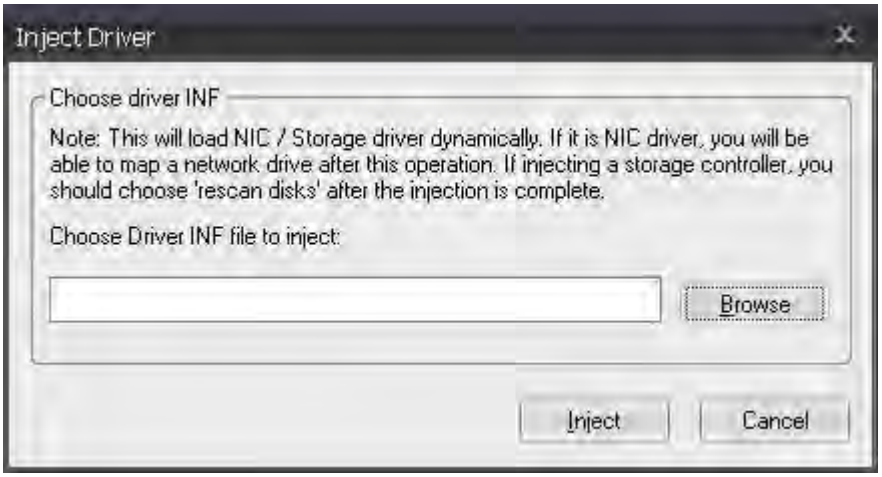


Fig. 56 - Injecting a driver into UBDR.

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.

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, etc), clicking "Rescan Disks" will force UBDR to re-scan the system for the newly added disks without the need to reboot.

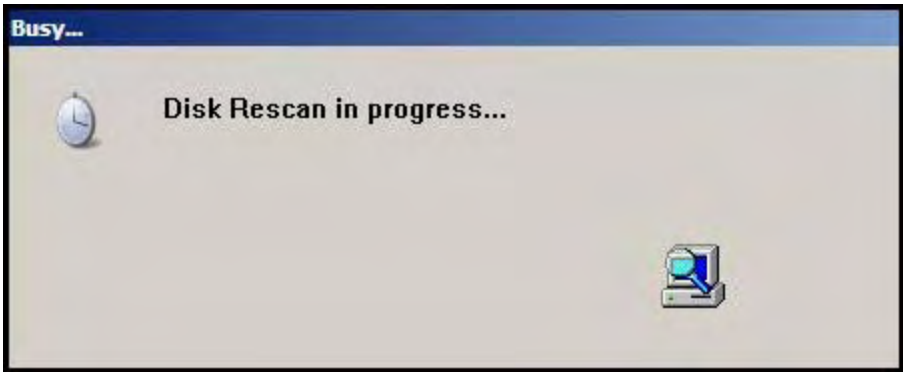


Fig. 57 - Re-scanning the system for newly added disks.

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.

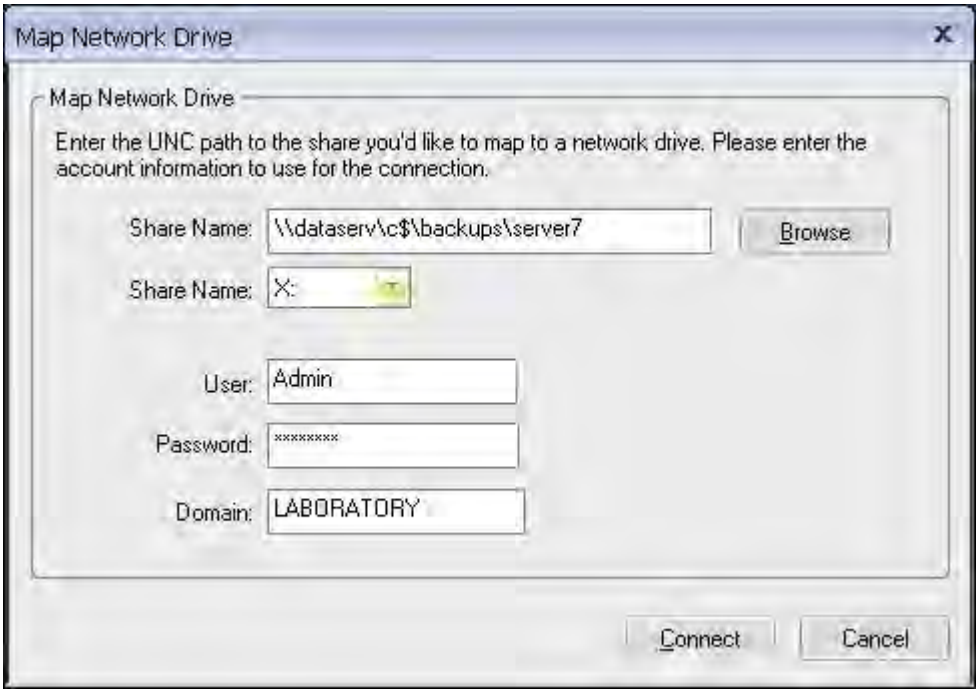


Fig. 58 - Mapping a network drive.

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.

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."

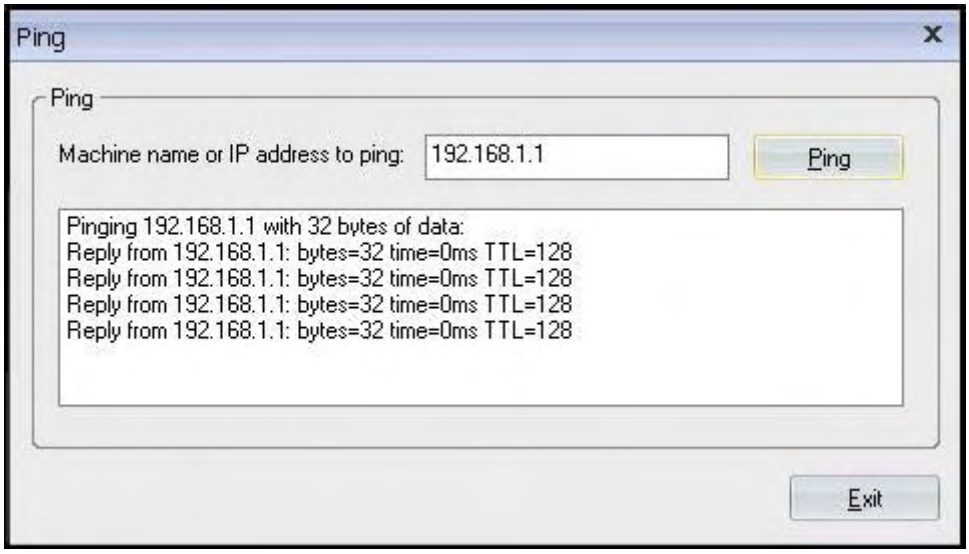


Fig. 59 - Pinging a remote system via IP address.

Writing an Image Backup to VHD File

UltraBac has the capability of writing to the native Hyper-V / 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 Hyper-V / 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[#].vhd

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.

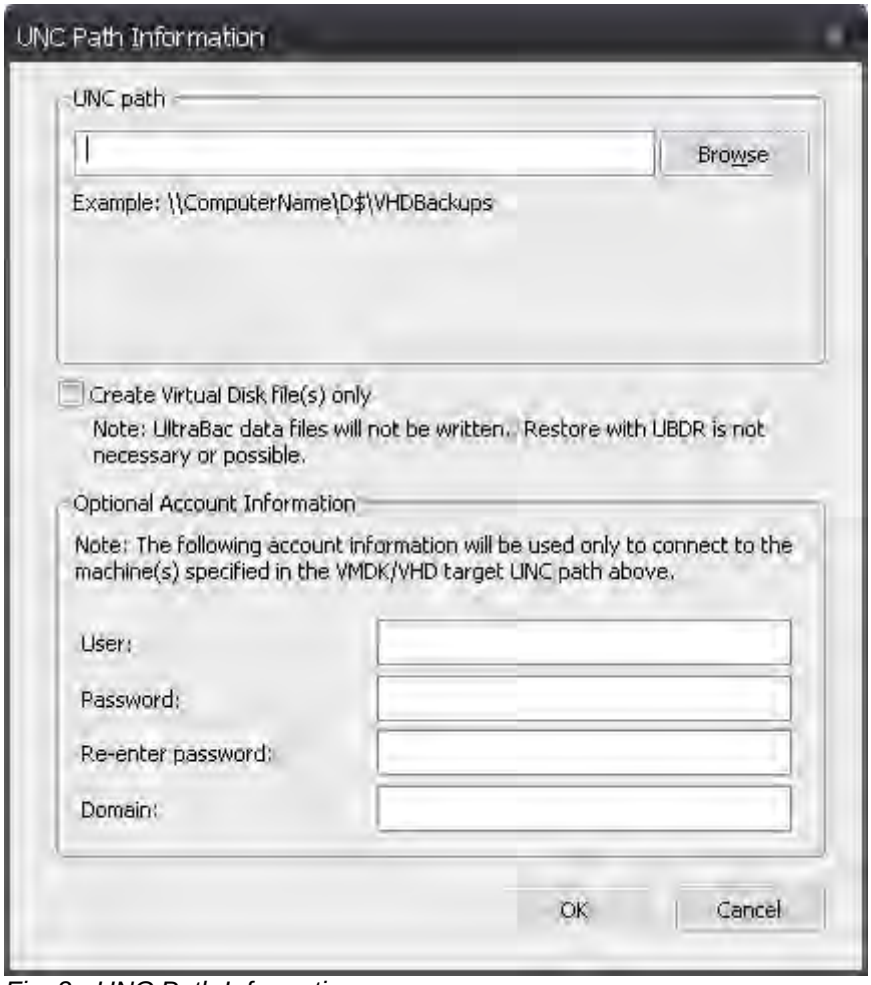


Fig. 2 - UNC Path Information.

8. Enter Optional 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." Restoring to original or dissimilar hardware will not be available if selected.

NOTE: You will still need to define and use a valid UltraBac device destination as UltraBac will create some small files on that destination device.

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 cannot use AES encryption.

Incremental/Differential VHD Files

Incremental/Differential backups will automatically update the VHD files with any incremental or differential changes. Only the most recent backup is available with VHD file. There is no point in time recovery available with virtual hard disk file(s).

NOTE: 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[#]_<VMware platform>.vmdk

NOTE: VMDK files cannot be created when either the 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 "Back up to VMware ESX file format - VMDK" is selected then choose either "Write VMDK to Windows UNC path" or "Write VMDK to ESX / ESXi datastore."

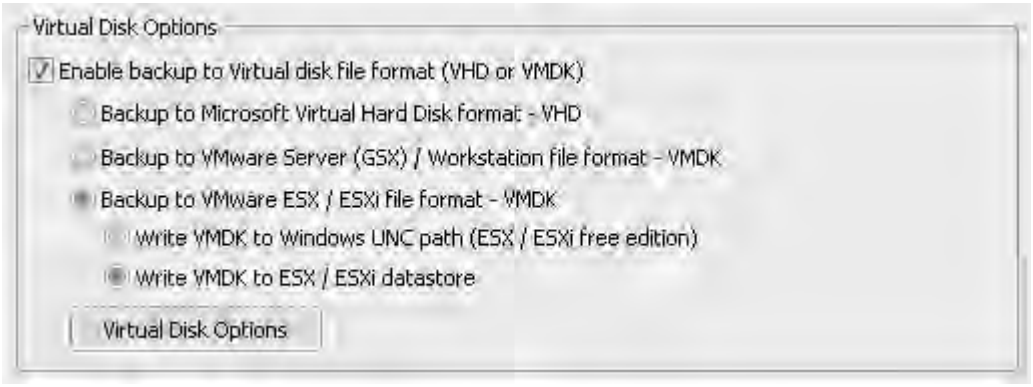


Fig. 1 - Enabling the creation of VMDK files.

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 four small files 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.

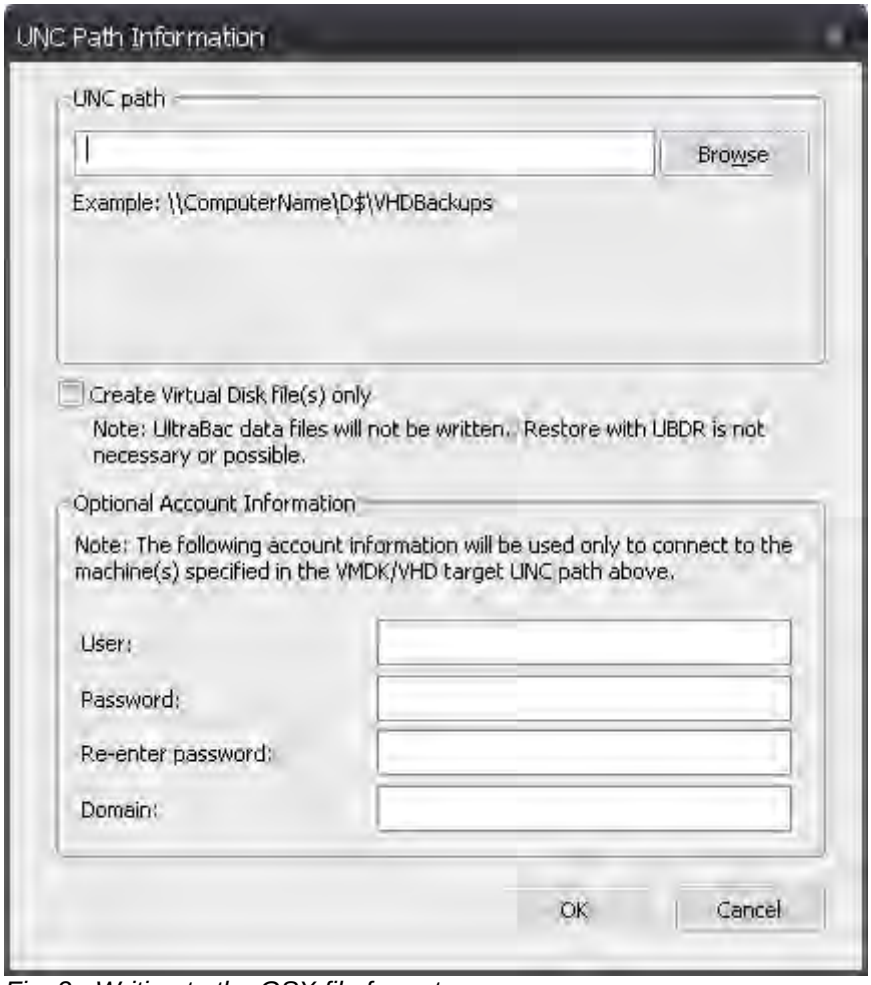


Fig. 2 - Writing to the GSX file format.

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:

UltraBac User Manual: UltraBac Preferences



Fig. 3 - Setting the VMDK target path.

ESX File Format Options - Writing to ESX Datastore

Starting with UltraBac version 10.0, it is now possible to create a stand-by virtual machine (VM). All VMs created will have 2 CPUs, 4GB of memory, and 1 NIC assigned to the default network. If static IP address is used on the source computer it will need to be manually entered after booting the VM into the OS.

When writing to a VMDK file in the ESX format, it is necessary to specify the target location in the Virtual Disk Options:

- Login Credential
  - vCenter / ESX Name – Depending on the VMDK Create Options above, enter the vCenter name or ESX host name to connect and create the stand-by VM or VMDK only virtual disk.
  - User name – Enter a user name that has permission to write to the datastore.
  - Password – Enter the password for the previously specified account.
  - Port – Enter the port number for the vCenter or ESX server.
  - Connect – Will use the credentials entered to connect to the vCenter or ESX server to fill in "ESX Host" and "Datastore" dropdown lists in "Target Location" section.
- Target Location
  - ESX Host – ESX host that the stand-by VM will be placed on.
  - Datastore – Storage location to write the VM configuration file and VMDK file(s).

        - Folder Name – Inventory path of the virtual disk. If stand-by is selected this is a read-only field that defaults to "%computername%_StandByVM."
- Target VMDK Type
    - Target VMDK Type
        - Thin – Only the used space will be allocated to the VMDK file.
        - Thick Lazy Zeroed – Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
    - Create Virtual Disk file(s) only – Allows the creation of only the VMDK file. The normal UltraBac format backup files (*.ubd) will not be created, so an image restore will not be possible.

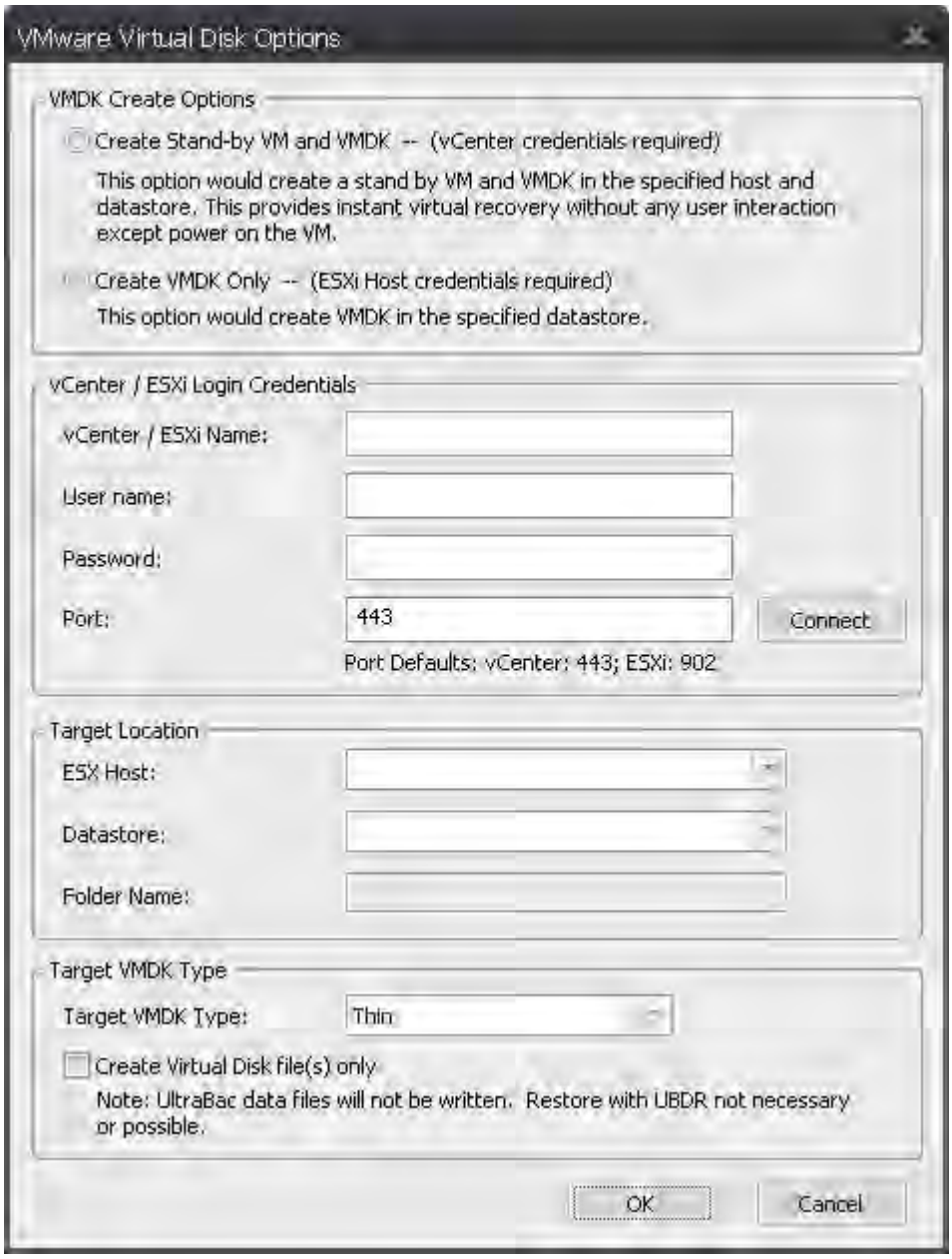


Fig. 4 - ESX output options.

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. Only the most recent backup is available with VMDK file. There is no point in time recovery available with virtual hard disk file(s).

NOTE: 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. Select the custom option to use an existing virtual disk as well as recommended controller for the OS being restored.

For further instructions, please consult VMware's documentation.

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 the system is improperly shut down, 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.

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

UBQ000080: Incremental/Differential Backups and the Archive Bit

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:

    - Full backup – creates/clears the file (.idx) used to track changed clusters.
    - Differential backup – back up only the clusters changed since the last full backup.
    - Incremental backup – back up only the clusters changed since the last full or incremental backup.

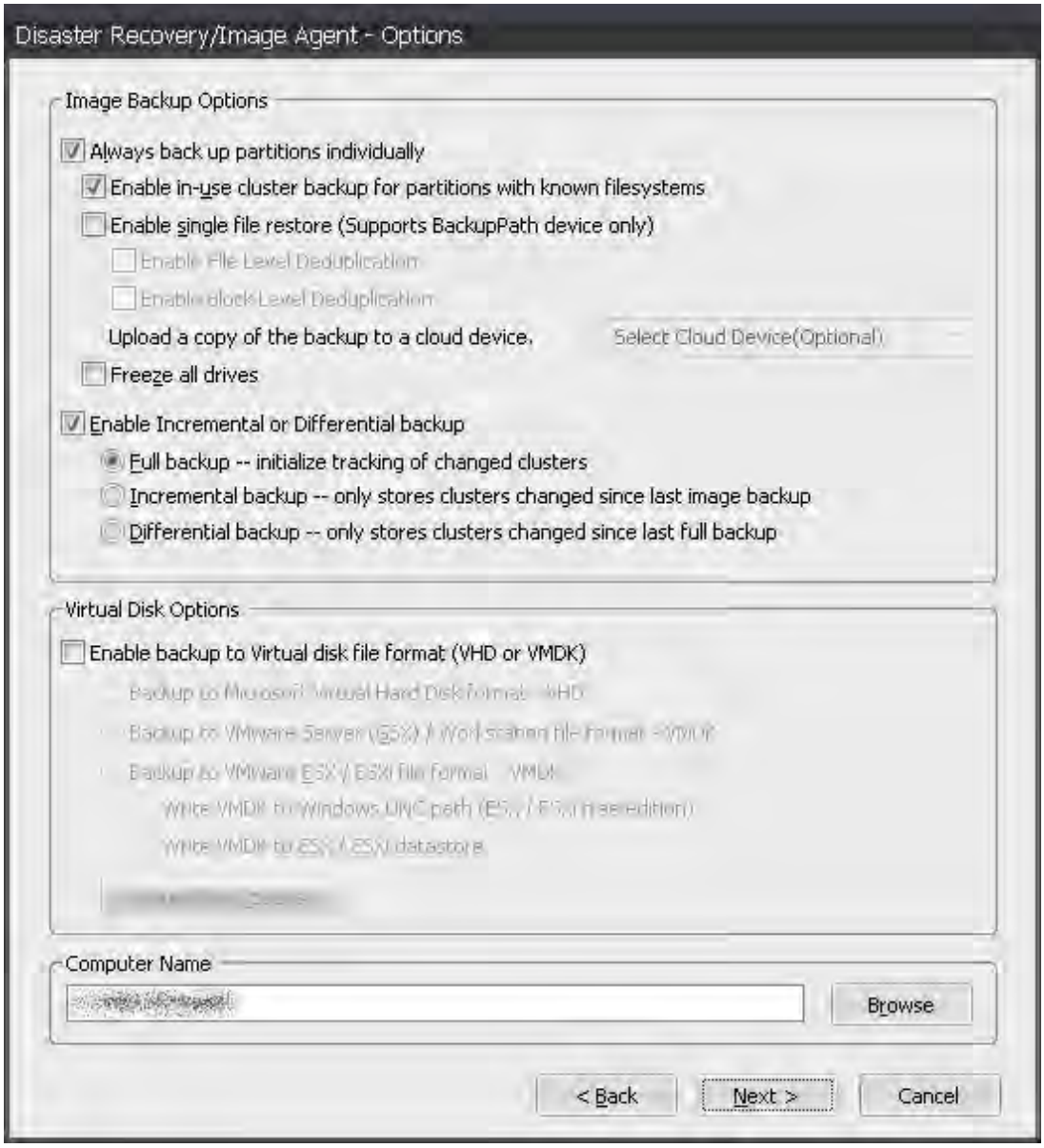


Fig. 1 - Image Agent options.

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."

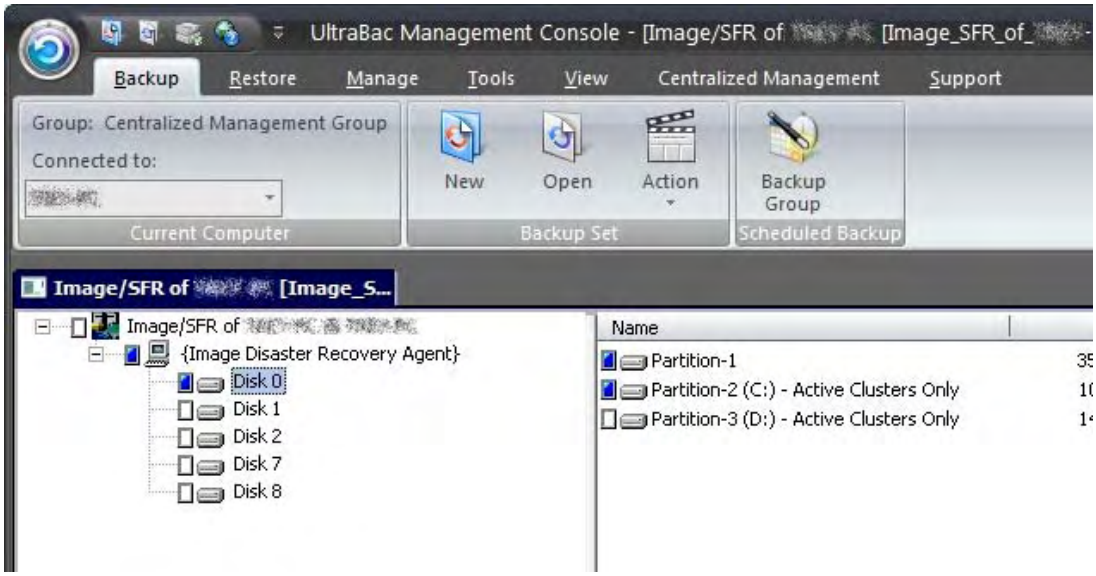


Fig. 2 - Image set loaded in the File Viewer.

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."
5. Choose either Express Mode or Advanced Mode.

NOTE: For more information, please see "Restoring an Image Backup" under the "**Image Disaster Recovery Agent**" section of the UltraBac User Manual.

UltraBac User Manual: Image Disaster Recovery Agent

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

6. Check "Run Unattended," and click "Restore."

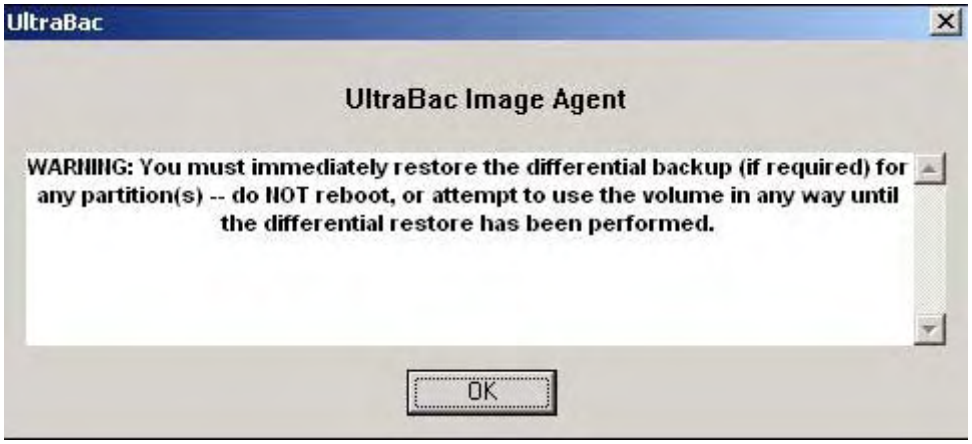


Fig. 3 - Incremental/Differential Restore prompt.

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 Differential or Incremental Restore

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

To begin the point-in-time restore process:

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the index of the differential or incremental backup that is the "point in time" you wish to restore. Click "OK."
3. Select "Yes" or "No" to choose whether the backup will restore to a different machine.
4. Select the disk or partition for restore.
5. Click "Action"/"Restore this Backup."
6. Choose either the "Express Mode" or the "Advanced Mode" radio button and select the appropriate "Settings" box.
7. Choose the desired Settings options. Click "OK."

> NOTE: For more information, please see "Restoring the Image / Express / Advance Mode Restores" under the "**UBDR Gold**" section of the UltraBac User Manual.
>
> **UltraBac User Manual: UBDR Gold**

8. Click "Next" on the Restore Modes Wizard.
9. Check "Run Unattended" and click "Restore."
10. A message box will pop up asking "Would you like to automatically restore all backups in this point in time restore?" Click "Yes."

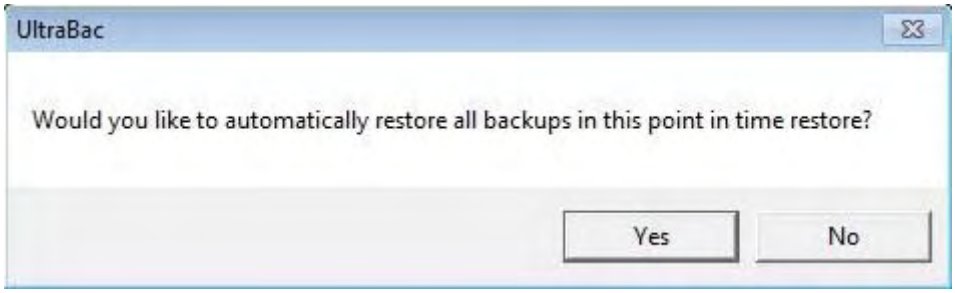


Fig. 4 - Point-in-time automatic restore of multiple backups.

11. Reboot the system to activate the image restore or use Disk Management to assign a drive letter to a non-OS 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:
    - Partition level – Select the Partition tab.
    - 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":
    - Partition level – "Always back up partitions individually" must be checked and "Enable Differential backup" must be unchecked.
    - 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.

NOTE: For additional information Static Mirror Image Recovery, please see the UltraBac Knowledge Base:

UBQ000060: Static Mirror Image Recovery

File-by-File

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.

NOTE: For information on configuring deduplication server, please see the UltraBac Knowledge Base:

UBQ000278: Configuring UltraBac Deduplication Server

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, then click "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."

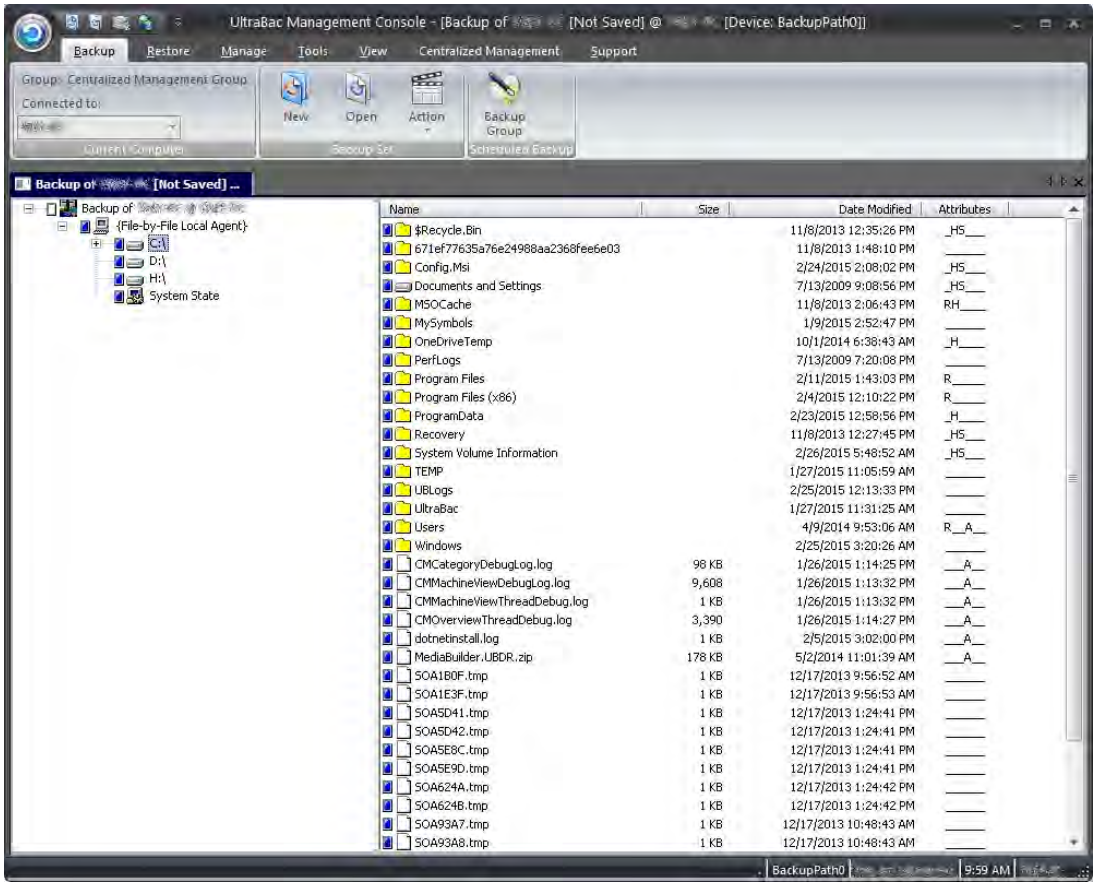


Fig. 1 - Viewing a File-by-File Local Agent backup set in the File Viewer.

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."

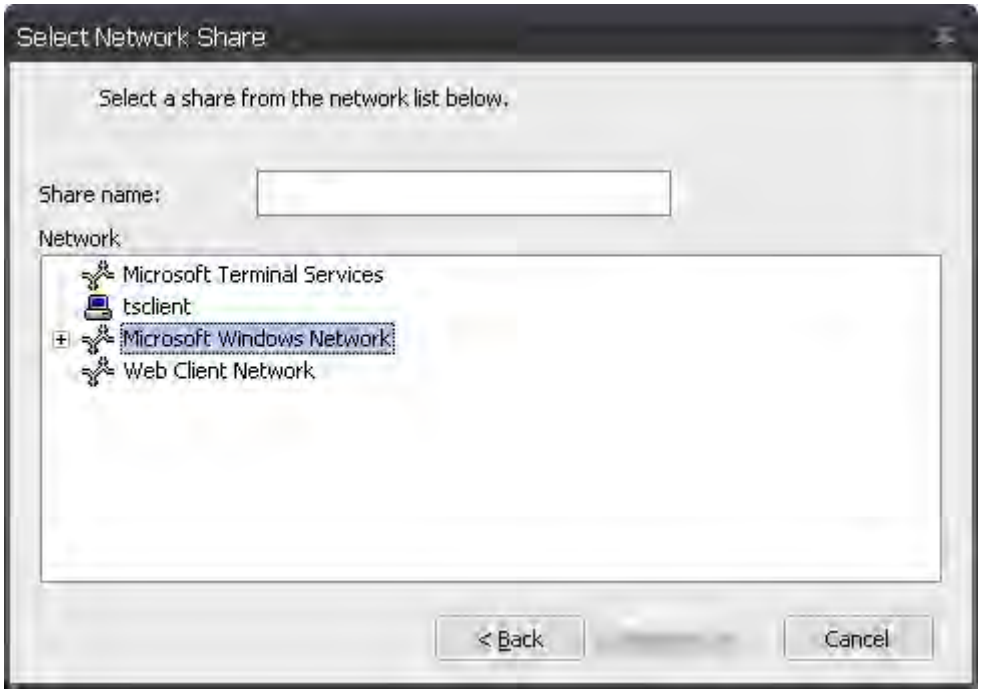


Fig. 3 - Network share browser.

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."

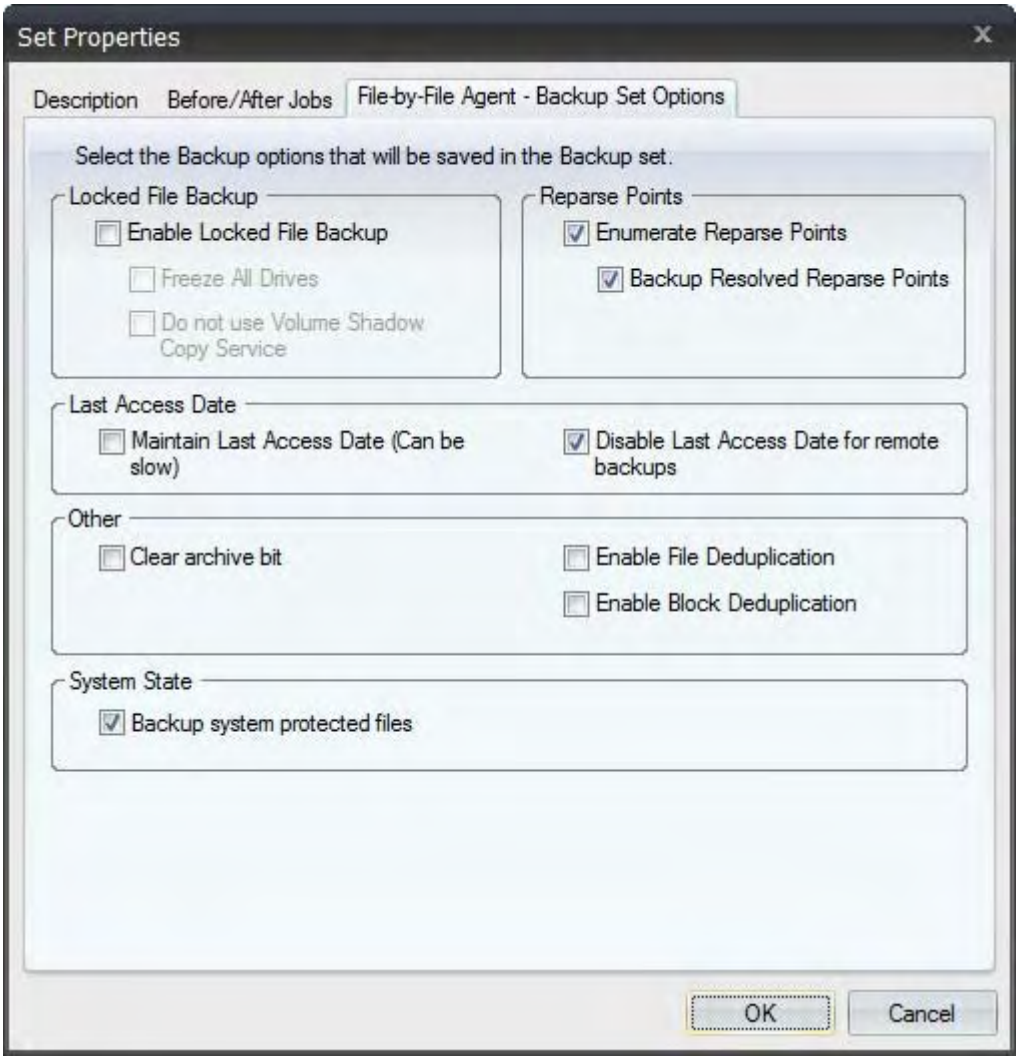


Fig. 4 - File-by-File Agent set properties.

- Description – Set the description as it will appear in the backup, restore, and verify logs; along with Notes for the set.
- Before/After Jobs – Set scripts to run before or after the backup set is run.
- File-by-File Agent – Backup Set Options:
  - 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 UltraBac's locked file driver (ubfd).
  - 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 remote systems.

- 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.
- Enable File Deduplication
- Enable Block Deduplication
- Backup system protected files – The system protected files are the critical files that are installed as a part of the Windows operating system installation. For example, files with a .dll, .exe, .ocx, and .sys extension and some True Type fonts.

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.

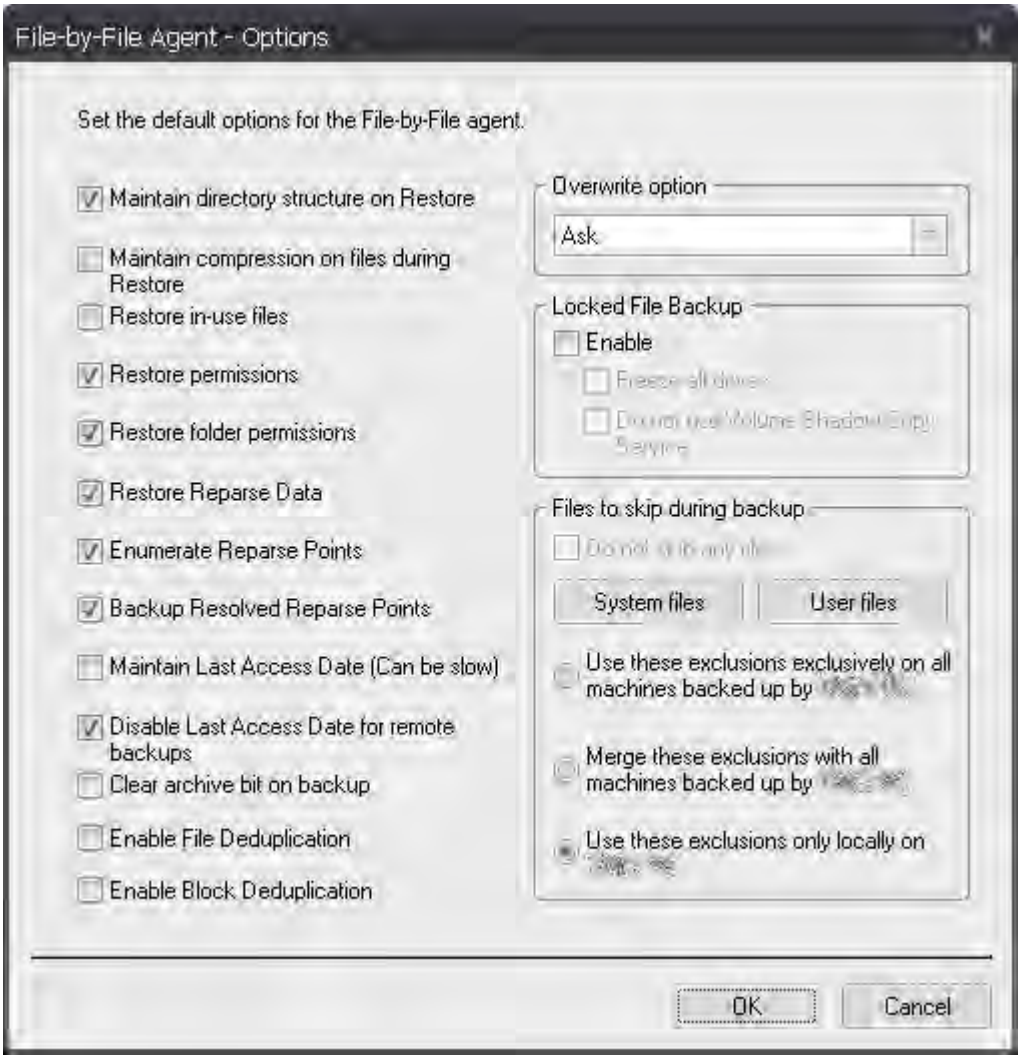


Fig. 5 - File-by-File Agent properties.

The available default options to be set:

- Maintain directory structure on Restore – Restore files and folders with the original parent folder structure. If unchecked all files will be restored into a single directory.

- 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.
- Enable File Deduplication.
- Enable Block Deduplication.

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 either Microsoft's Volume Shadow Copy service (VSS) or "UltraBac Locked File Backup" driver (UBFD) 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 data spanning multiple partitions to maintain integrity.
- Do not use Volume Shadow Copy Service – Forces UltraBac to use UBFD when backing files.

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.

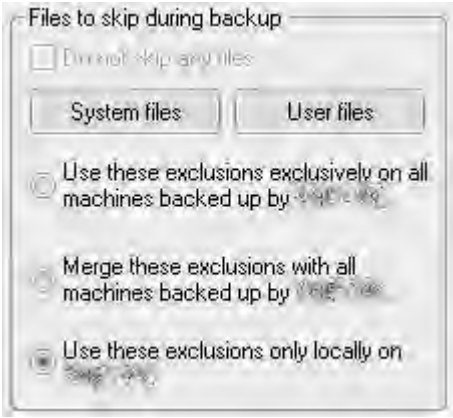


Fig. 6 - Files to skip during backup.

- 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 backups) – 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.

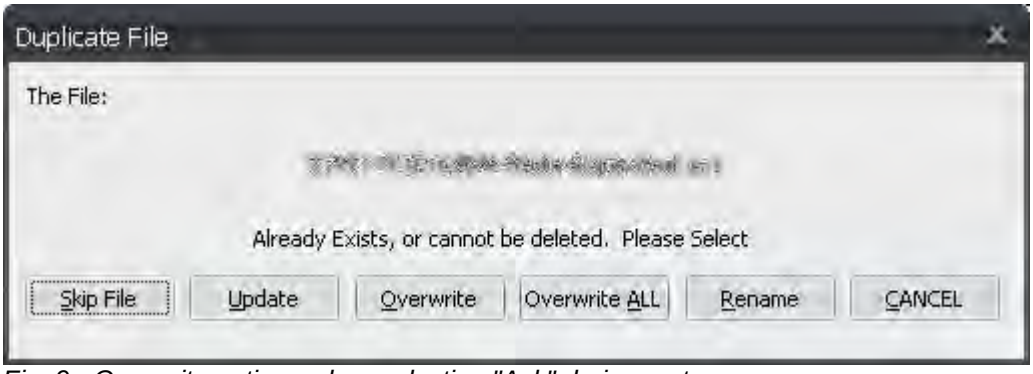


Fig. 9 - Overwrite options when selecting "Ask" during restore.

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 "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. Apply all service packs, updates, and hotfixes up the point of the backup. When the new operating system has been installed and updated, 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 2003 domain controller, please visit the "**Active Directory Restore 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 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:

UBQ000080: Incremental/Differential Backups and the Archive Bit

- 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. Select the appropriate Backup Set Options:
    a. For Incremental file-by-file set, check "Clear archive bit."
    b. For Differential file-by-file set, leave "Clear archive bit" unchecked.
4. Enter a set description and choose the Modified file selection logic to be used for this set. Click "Next."



Fig. 1 - Available file selection logic in the Selection Criteria.

- 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.

5. 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."

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.

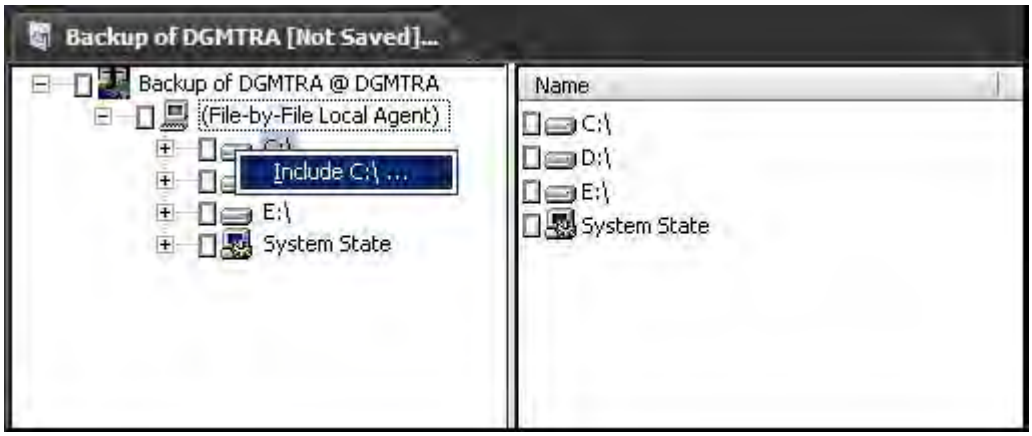


Fig. 2 - Including a drive in the File Viewer.

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.

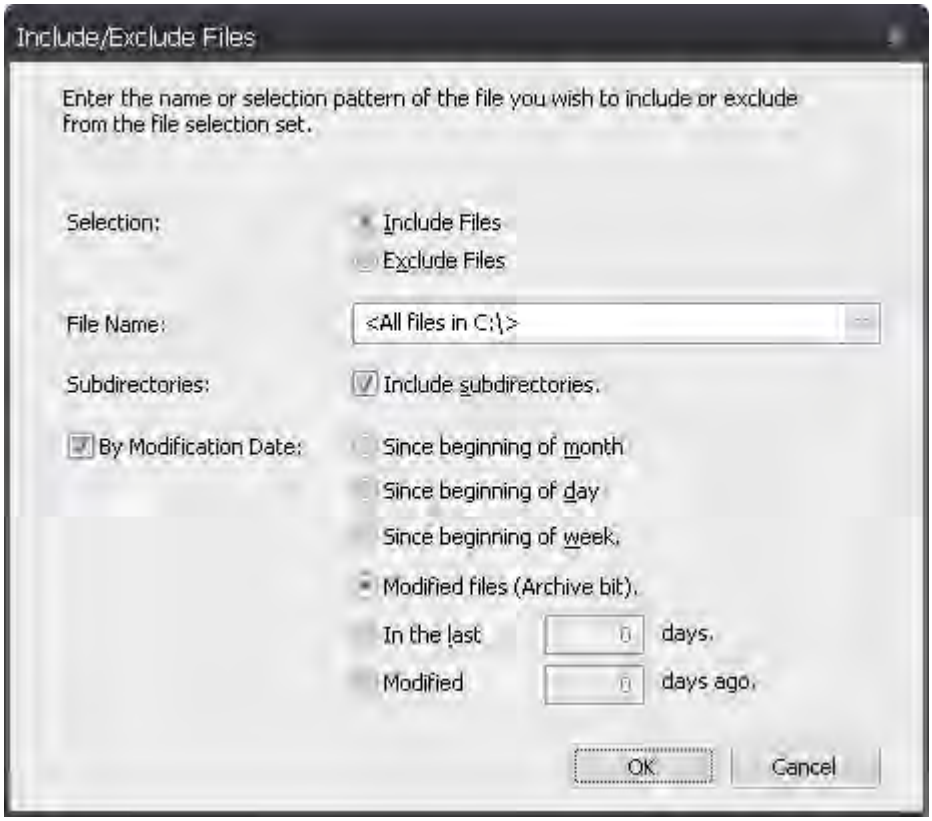


Fig. 3 - "Include/Exclude files" screen.

6. Check "By Modification Date."
7. Choose the file selection logic to be used in backing up the directory.
8. 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 future 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.

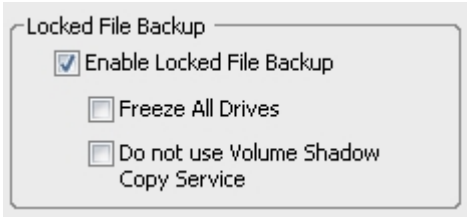


Fig. 1 - "Enable Locked File Backup."

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 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. If left unchecked, partitions will be frozen one at a time and backed up sequentially.
- Do not use Volume Shadow Copy Service – Use the UltraBac Locked File Backup (UBFD) driver to freeze the system.

Uninstalling the Locked File Backup Agent

The Locked File Backup Agent can be uninstalled through "Add/Remove Programs" in Windows Control Panel.

1. Access "Control Panel."
2. Click "Uninstall a program."
3. In the search box, type "UltraBac."

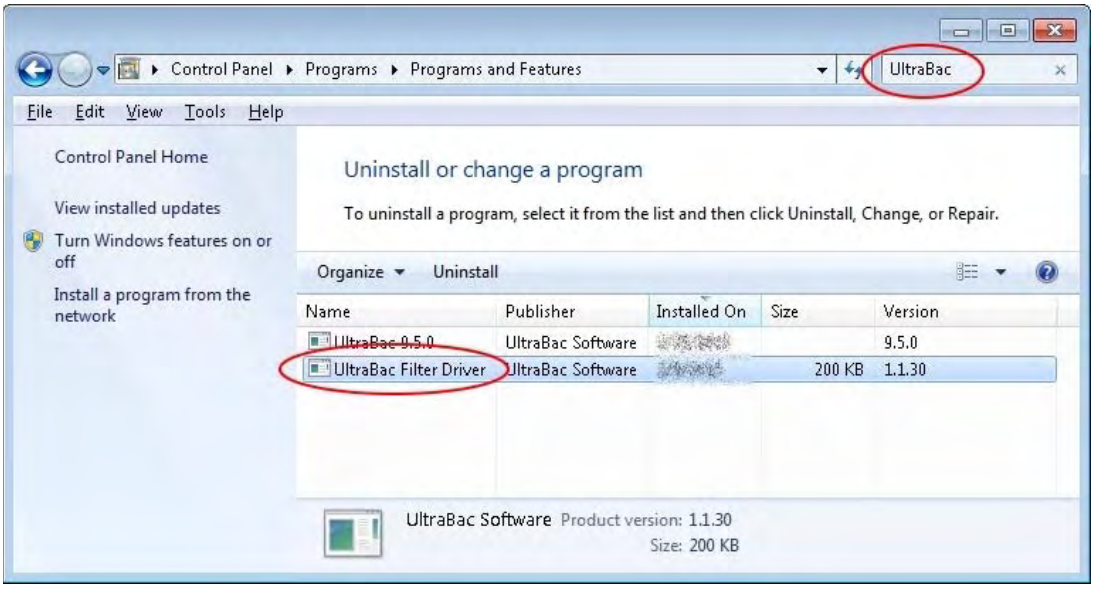


Fig. 2 - UltraBac Locked File Backup Driver in the Windows Device Manager.

4. Highlight "UltraBac Filter Driver."
5. Click "Uninstall" button, or right click and select "Uninstall."
6. Reboot the system to complete the removal of the UltraBac Locked File Backup driver.

UltraBac System State/Active Directory Restore Windows 2003 Server

Overview

Three types of Active Directory restores exist for Windows 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 2003 will have four subobjects 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 Windows Service Pack at the restore target must be the same as that of the machine at the time of backup.

NOTE: When pushing the restore to a remote system booted into Directory Services Mode, be sure that full version of UltraBac 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. From the Restore tab in UltraBac, select "Action"/"Restore This Backup" to bring up the "Restore Options" screen.
6. At the "Restore Options" screen, click "Next."
7. 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.

8. When the restore completes, a prompt will appear confirming the reboot. If NTDSUTIL is to be run, click "Cancel" to override the reboot request.

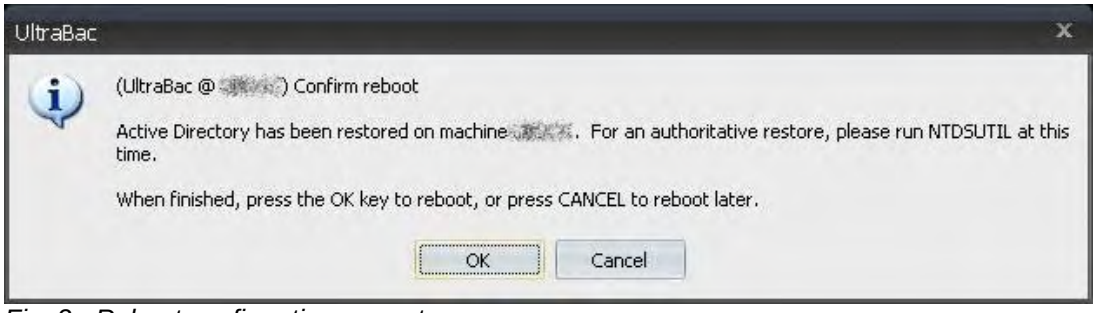


Fig. 2 - Reboot confirmation prompt.

9. Select "Restore Log" when the UltraBac Progress screen appears and verify the restore was successful.
10. When finished viewing the restore log, exit UltraBac. This concludes the UltraBac portion of the restore.
11. 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.

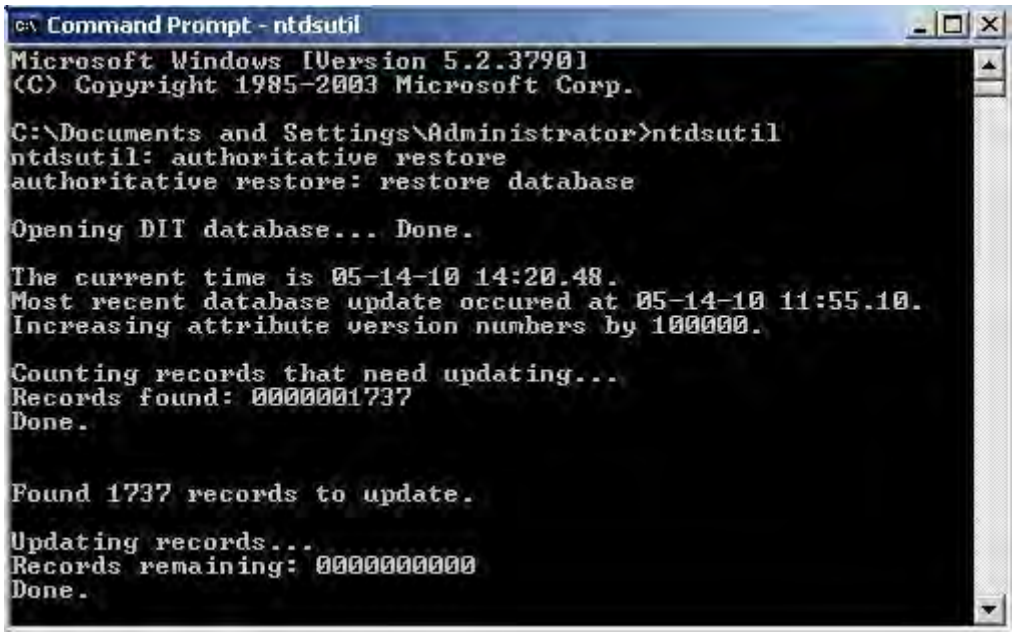


Fig. 4 - NTDSUTIL from a DOS prompt.

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 same 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 functional level your domain/forest is in (2003 / 2008 / 2008 R2) as the restore steps are different.

Restoring the System State Using UltraBac
2008/2008 R2 Active Directory Schema with Multiple Domain Controllers
2008/2008 R2 Active Directory Schema with a Single Domain Controller
2003 Active Directory Schema with Multiple Domain Controllers
2003 Active Directory Schema with a Single Domain Controller

NOTE: The Windows Service Pack at the restore target must be the same as that of the original machine at the time of backup.

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 restore methodologies differ depending on the Active Directory schema you set up at the time of backup, please review the following sections to find the appropriate restore procedure.

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."

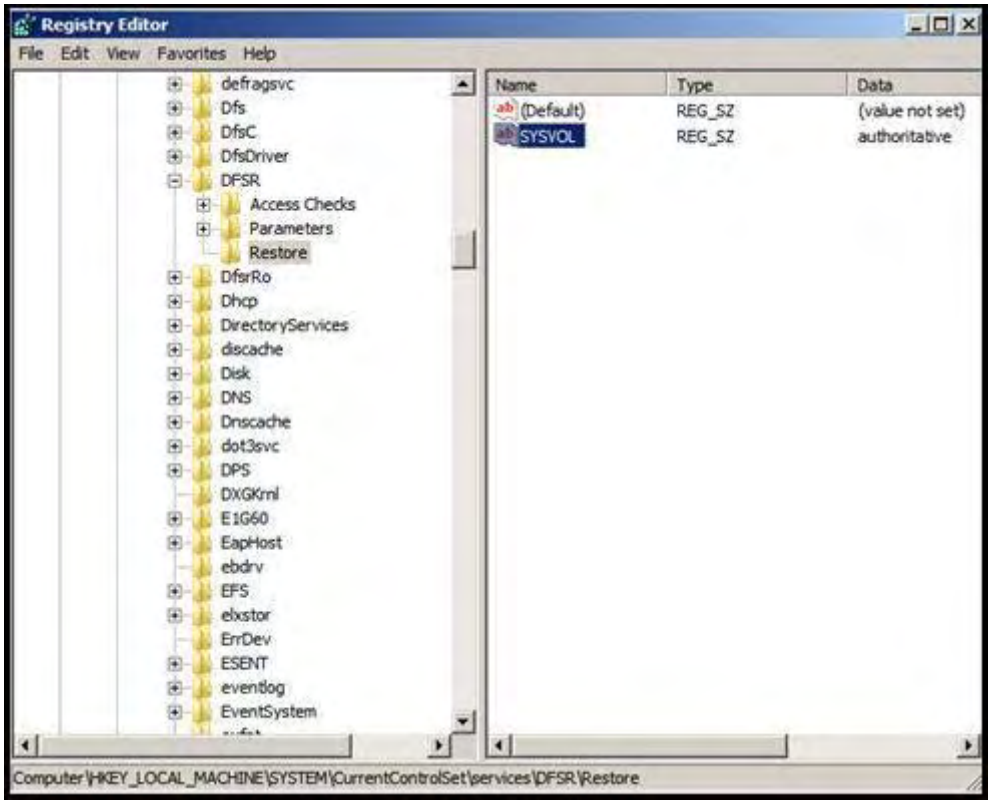


Fig. 3 - Registry Options.

On the remaining domain controllers:

7. For the string value called "SYSVOL," give it the value of "non-authoritative."

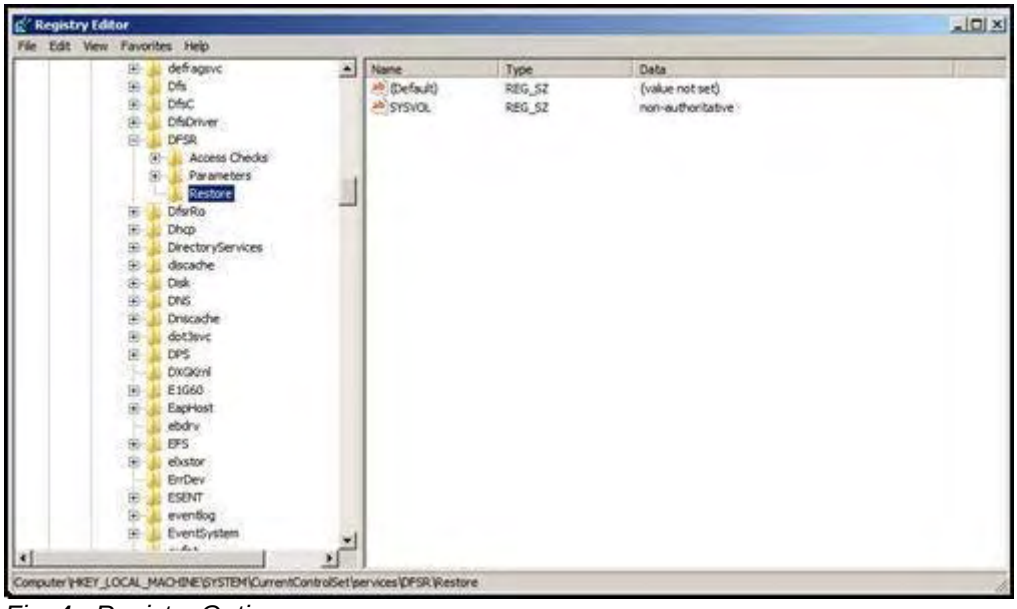


Fig. 4 - Registry Options.

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".

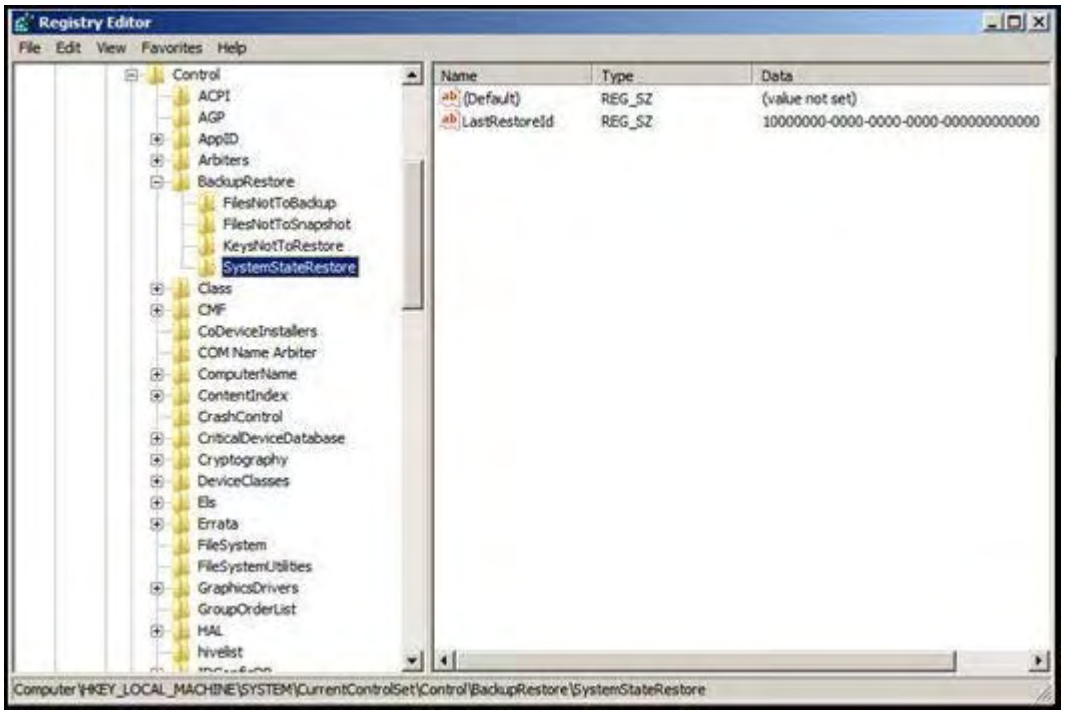


Fig. 5 - Registry Options.

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>.

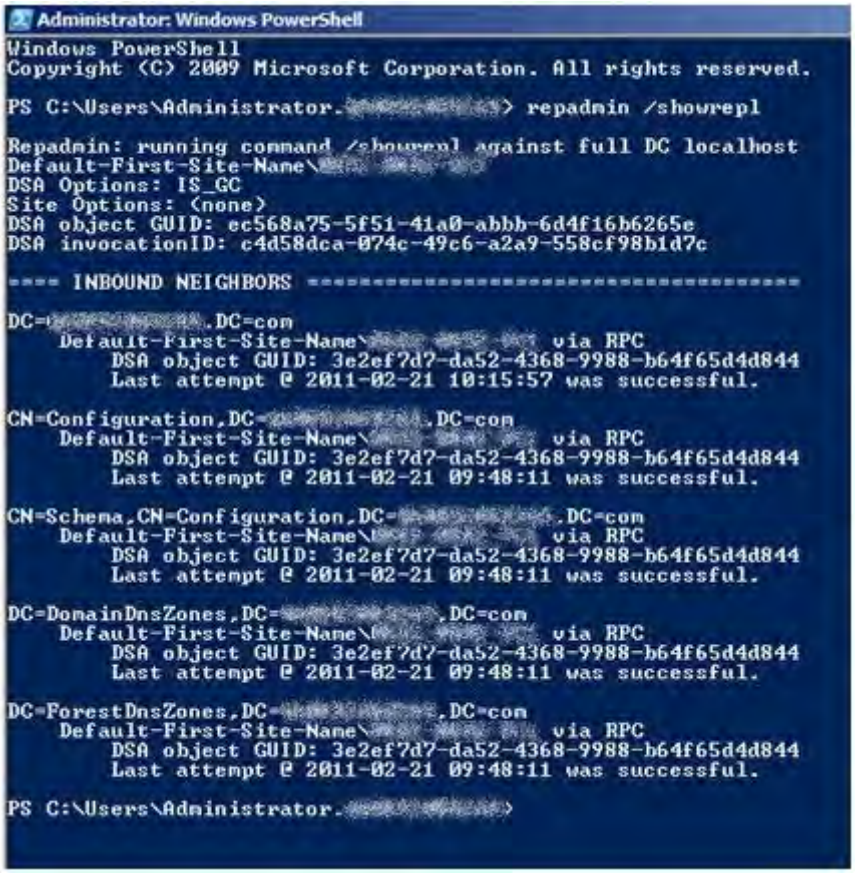


Fig. 6 - Repadmin example.

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."

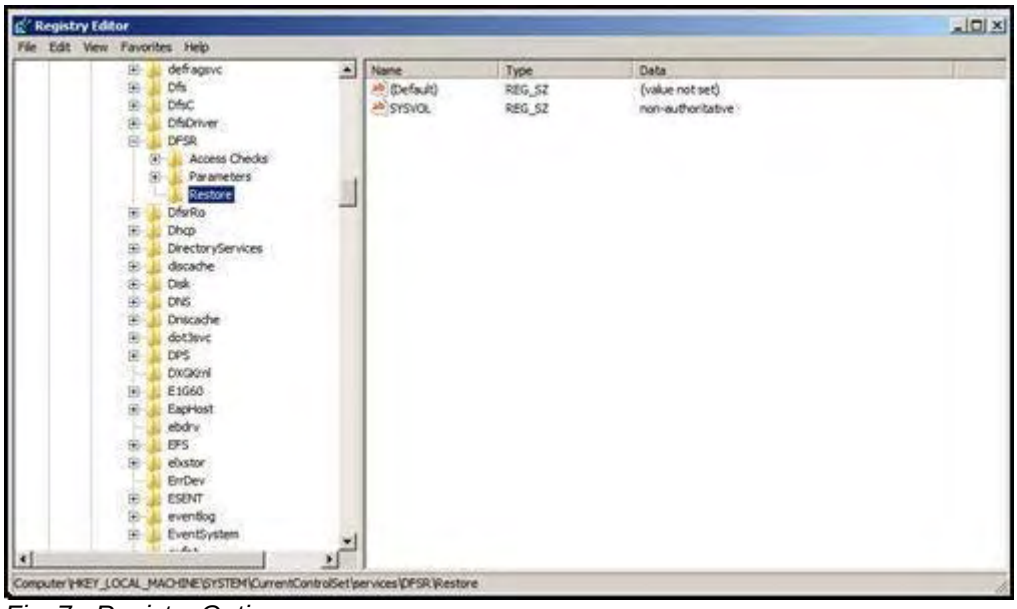


Fig. 7 - Registry Options.

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."

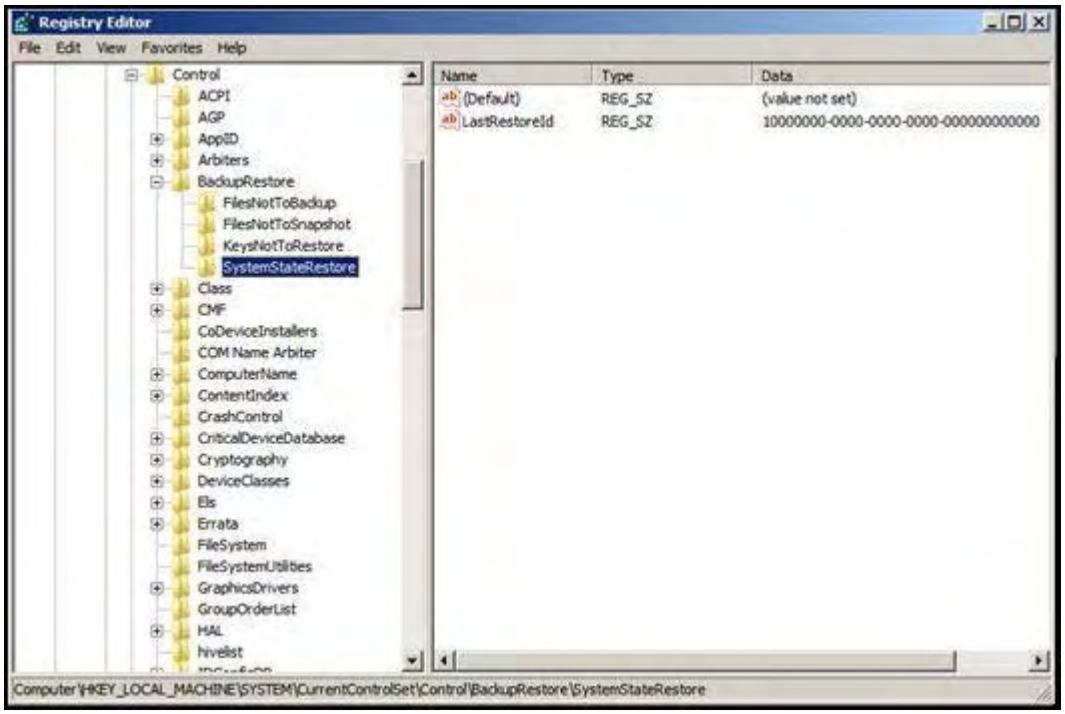


Fig. 8 - Registry Options.

11. Once the registry settings have been put into place, you must then start the DFSR service.

NOTE: It is highly recommended to remove the registry settings you entered above after restore is completed.

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).

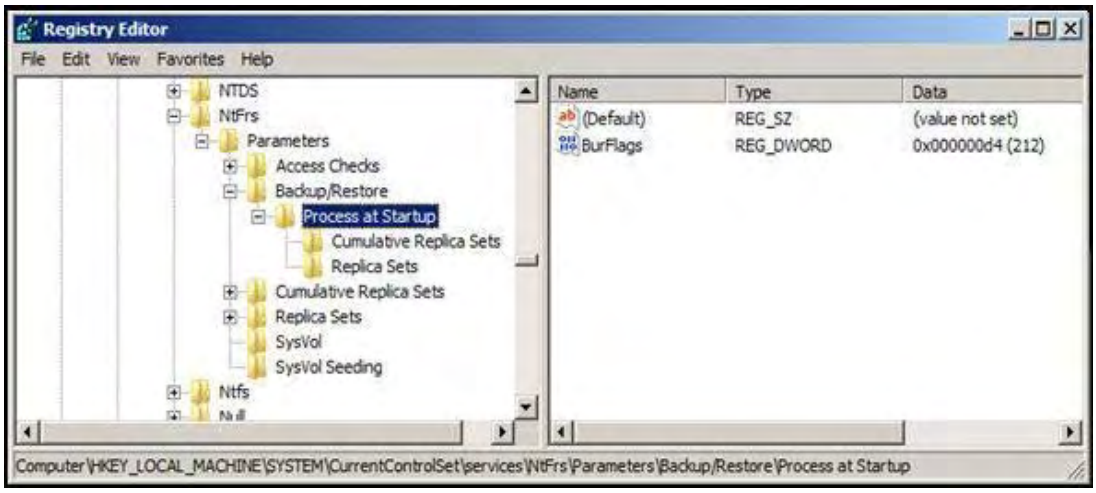


Fig. 9 - Registry Options.

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 PowerShell 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.

UltraBac System State/Active Directory Restore Windows 2012/2012 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 same 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 functional level your domain/forest is in (2003 / 2008 / 2008 R2 / 2012 / 2012 R2) as the restore steps are different.

Restoring the System State Using UltraBac
2012/2012 R2 Active Directory Schema with Multiple Domain Controllers
2012/2012 R2 Active Directory Schema with a Single Domain Controller
2008/2008 R2 Active Directory Schema with Multiple Domain Controllers
2008/2008 R2 Active Directory Schema with a Single Domain Controller
2003 Active Directory Schema with Multiple Domain Controllers
2003 Active Directory Schema with a Single Domain Controller

NOTE: The Windows Service Pack at the restore target must be the same as that of the original machine at the time of backup.

Restoring the System State Using UltraBac

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

1. Reboot the domain controller into DFSR.
    - UBQ000276: How to Boot a Windows Server Domain Controller into Directory Services Restore/Repair Mode
2. 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.
3. Install UltraBac.
4. 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.

5. 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.

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



Fig. 2 - Restore Options.

7. 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, or return to the top and click the appropriate section link.

Return to top

2012/2012 R2 Active Directory Schema with Multiple Domain Controllers

These steps will restore user "John Smith" and an "IT" OU that were accidentally deleted.

1. Restore the system state using the steps provided in Restoring the System State Using UltraBac above.
2. Right click on the Safe Mode Start Menu; click Command Prompt (Admin).
    - For non-authoritative restores, skip to step 9.
3. Type <ntdsutil> and then press "Enter."
4. At the ntdsutil: prompt, type <activate instance ntds>, and then press "Enter."
5. At the ntdsutil: prompt, type <authoritative restore>, and then press "Enter."
6. This will bring up an authoritative restore prompt. At the prompt type the following command:
    - restore object “cn=John Smith,OU=Sales,OU=HeadOffice,DC=mycompanydomain,DC=com”
    - restore subtree “OU=IT,OU=HeadOffice,DC=mycompanydomain,DC=com”

7. Click "Yes" in the message box to confirm the Authoritative Restore. One record will be found and will be successfully updated. You will see the message "Authoritative Restore completed successfully."
    - Notice NTDSUTIL is increasing attribute version numbers by 100,000.
8. At the authoritative restore prompt, type <quit> and press "Enter" to exit authoritative restore and then type <quit> again, then press "Enter" to exit NTDSUTIL.
9. In the same command prompt, type <bcdedit /deletevalue safeboot> and press "Enter."
10. Restart the computer.

Return to top

2012/2012 R2 Active Directory Schema with a Single Domain Controller

1. Restore the System State using the steps provided in Restoring the System State Using UltraBac above.
2. Right click on the Safe Mode Start Menu; click Command Prompt (Admin).
3. In the same command prompt, type <bcdedit /deletevalue safeboot> and press "Enter."
4. Restart the computer.

Return to top

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."

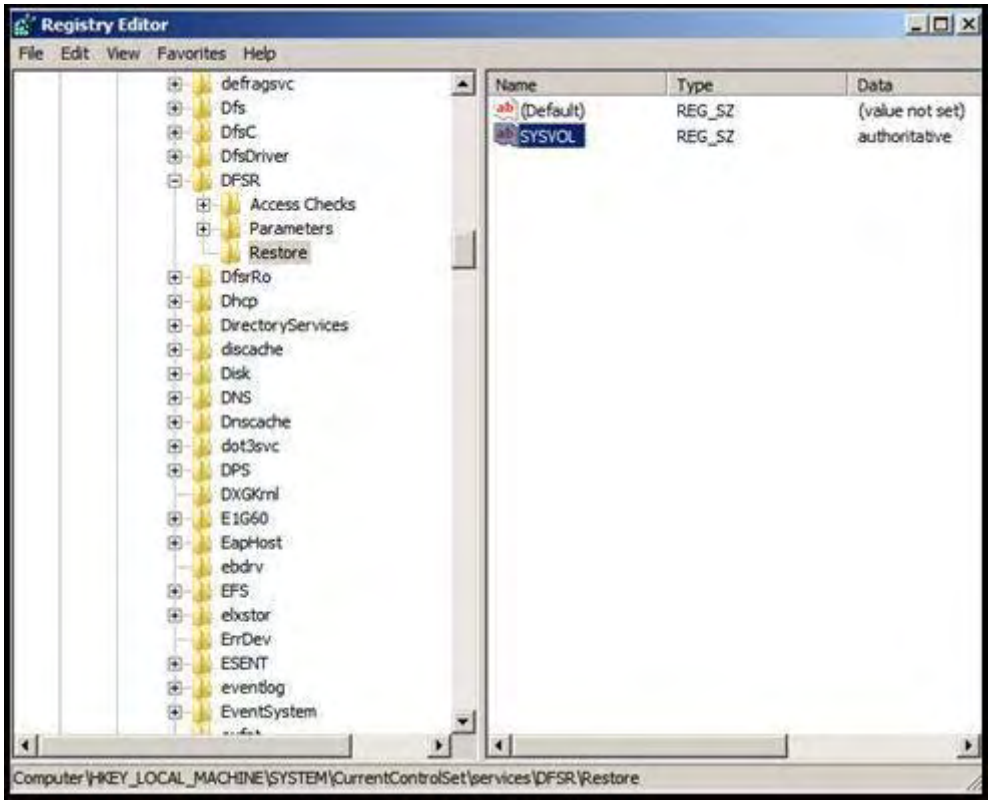


Fig. 3 - Registry Options.

On the remaining domain controllers:

7. For the string value called "SYSVOL" give it the value of "non-authoritative."

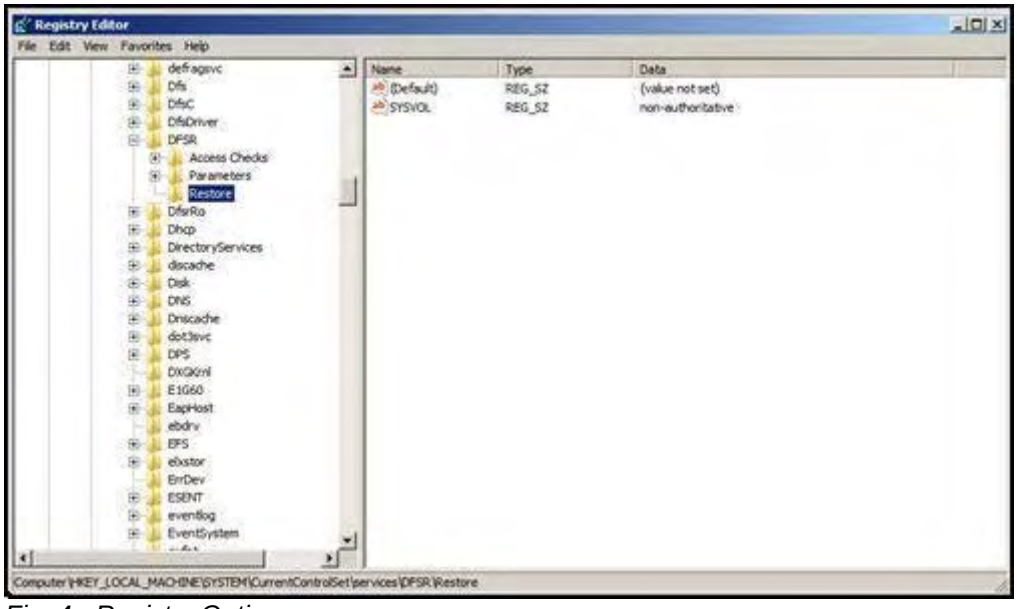


Fig. 4 - Registry Options.

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."

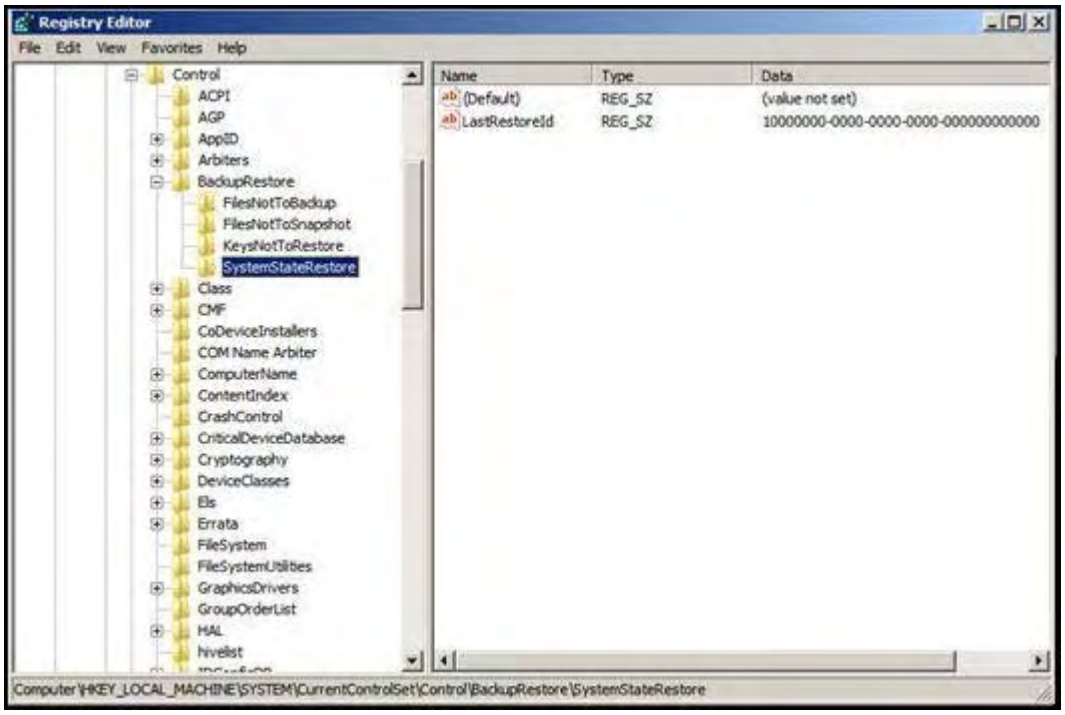


Fig. 5 - Registry Options.

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>.

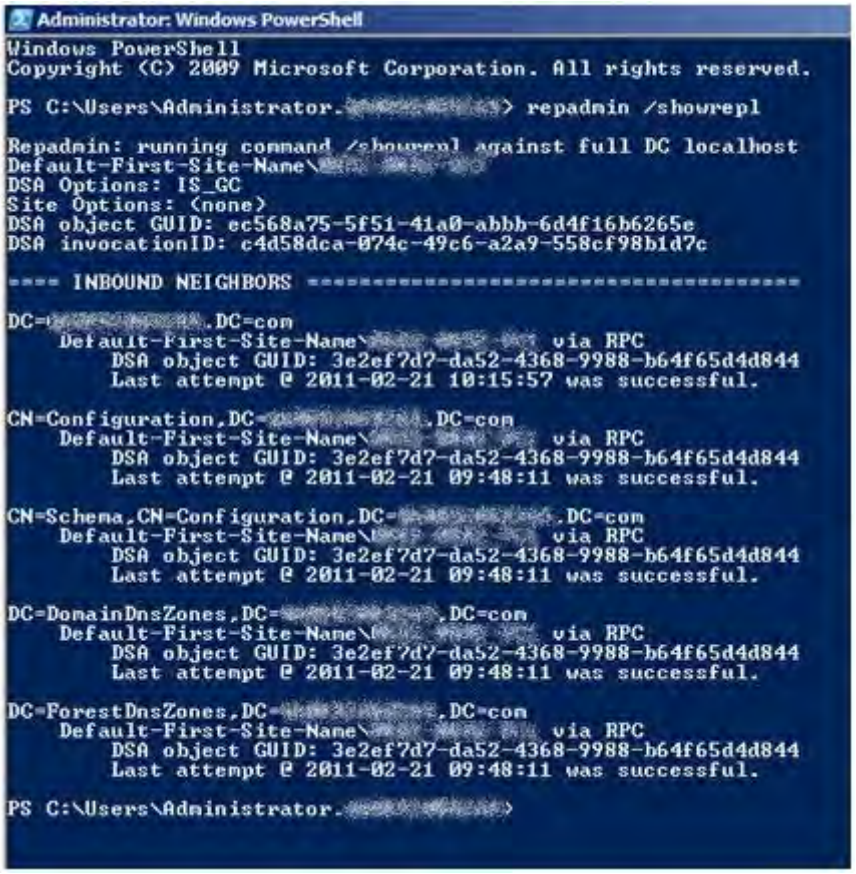


Fig. 6 - Repadmin example.

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.

Return to top

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

1. Restore the System State using the steps provided in Restoring the System State Using UltraBac above.
2. Right click on the Safe Mode Start Menu; click Command Prompt (Admin).
3. In the same command prompt, type <bcdedit /deletevalue safeboot> and press "Enter."
4. Restart the computer.

Return to top

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. Restore the System State using the steps provided in Restoring the System State Using UltraBac above.
2. Right click on the Safe Mode Start Menu; click Command Prompt (Admin).
    - For non-authoritative restores, skip to step 9.
3. Type <ntdsutil> and then press "Enter."
4. At the NTDSUTIL: prompt, type <activate instance ntds> and then press "Enter."
5. At the NTDSUTIL: prompt, type <authoritative restore> and then press "Enter."
6. This will bring up an authoritative restore prompt. At the prompt type the following command:<restore database>.
7. Click "Yes" in the message box to confirm the Authoritative Restore.
8. At the authoritative restore prompt, type <quit> and press "Enter" to exit authoritative restore. Then type <quit> again, then press "Enter" to exit NTDSUTIL.
9. In the same command prompt, type <bcdedit /deletevalue safeboot> and press "Enter."
10. Restart the computer.

Return to top

2003 Active Directory Schema with a Single Domain Controller.

1. Restore the System State using the steps provided in Restoring the System State Using UltraBac above.
2. Right click on the Safe Mode Start Menu; click Command Prompt (Admin).
3. In the same command prompt, type <bcdedit /deletevalue safeboot> and press "Enter."
4. Restart the computer.

Return to top

vSphere Agent

The vSphere Agent provides users with the ability to back up their virtual machines without installing any agents on those virtual machines. It also allows users to back up from one central location.

NOTE: In UltraBac v.9.4.0 support for NDBSSL and NFS backups was added. 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.

NOTE: For information on configuring deduplication server, please see the UltraBac Knowledge Base:

UBQ000278: Configuring UltraBac Deduplication Server

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."

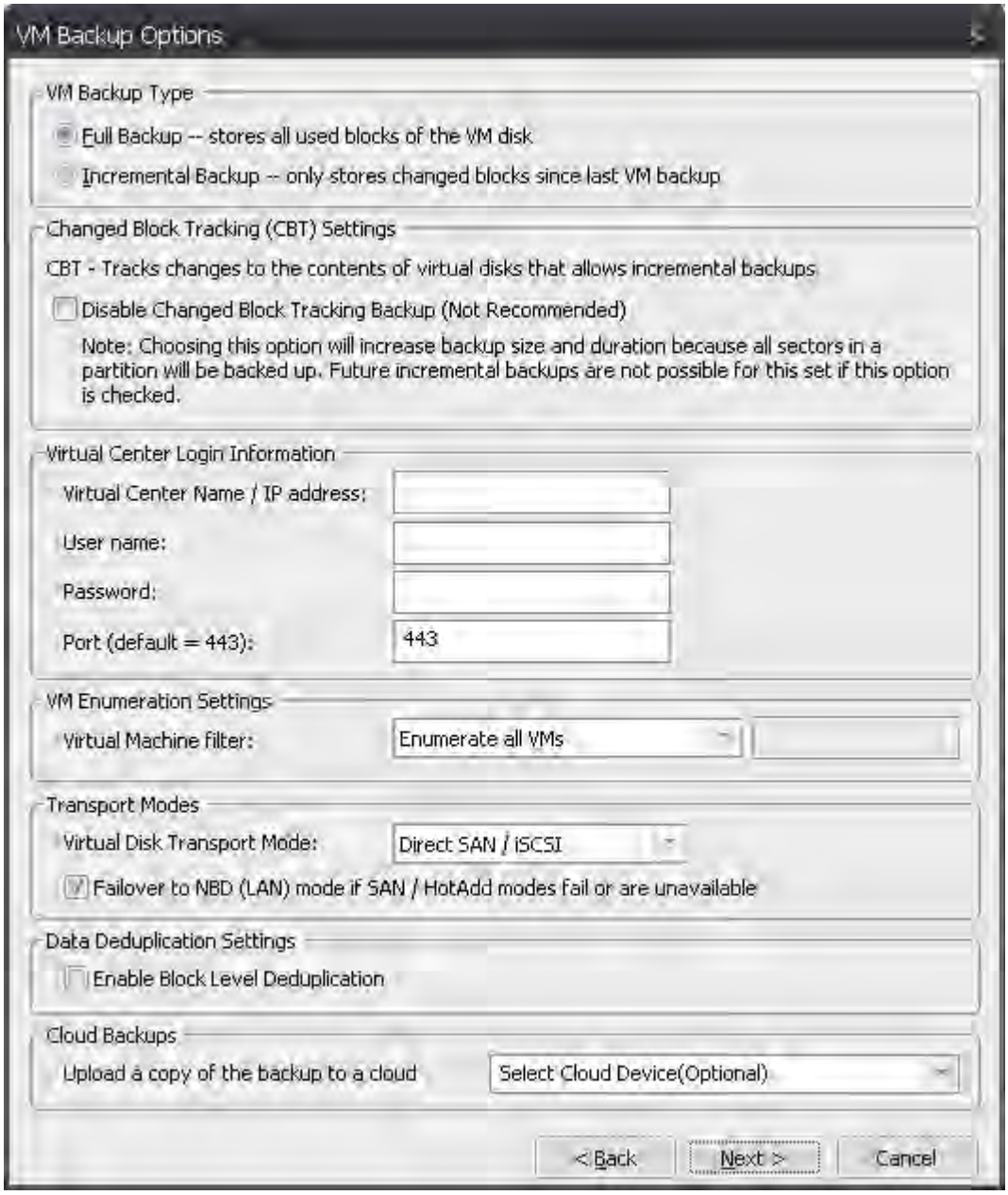


Fig. 1 - vSphere Agent options.

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 Name / IP address" field.
5. Type in the User name and password 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 to determine how the agent transfers the backup data:
   - Direct SAN / iSCSI – Backup server must be connected to the SAN Lun(s) as the ESX datastores. Best performance.
   - LAN (NBD) – Backup will be done over the network. Poor performance.
   - NDBSSL (LAN encrypted) – Backup will be done over the network using an SSL connection. Worst performance.
   - HotAdd (Virtual Appliance) – Backup server needs to be Virtual Machine on shared storage. Good performance.

8. Select "Failover to NBD" mode if you want UltraBac to attempt to use the NBD if the selected transport mode connection fails.
9. Select "Deduplication Options" if necessary.
10. Click "Next."
11. Enter the name you wish to assign to the UltraBac set and click "Next."
12. Click "Finish."

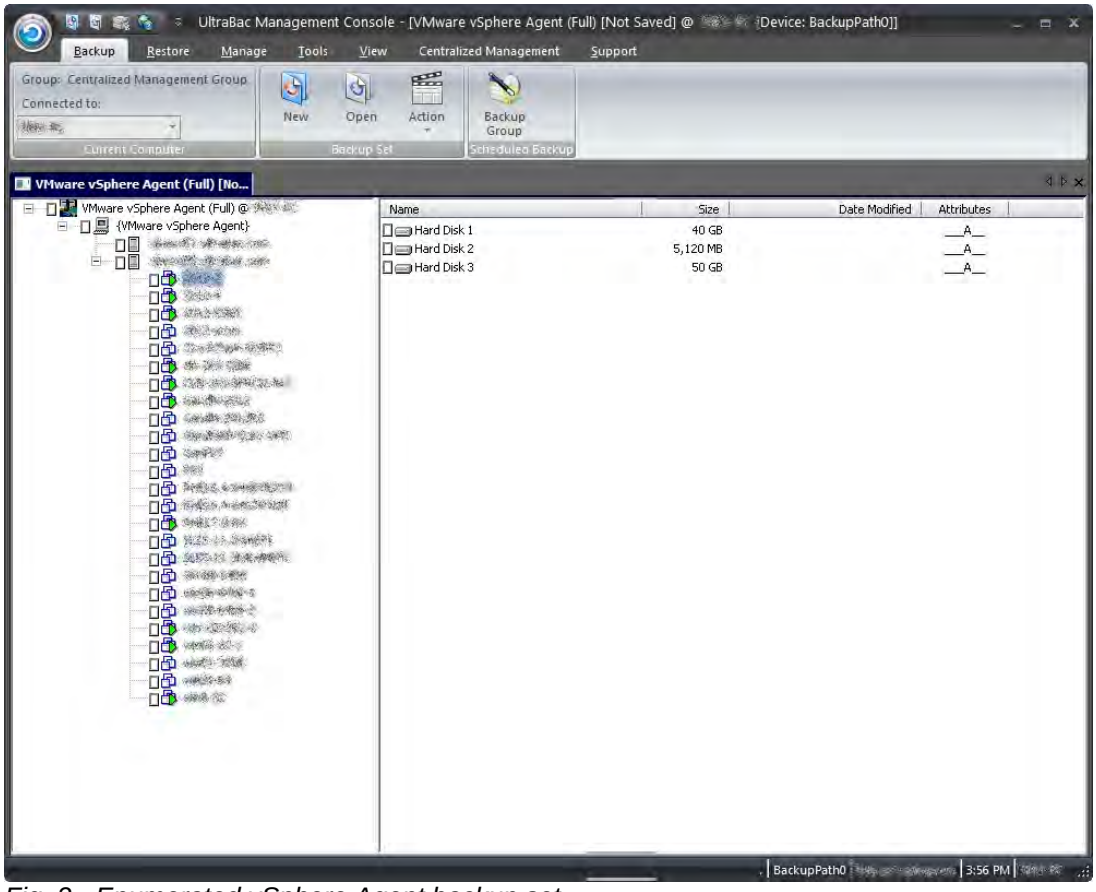


Fig. 2 - Enumerated vSphere Agent backup set.

Current Limitations to Scheduling a vSphere Agent Backup

The following are limitations of the vSphere Agent:

- Backups can only be saved to a backup path. If the backup is scheduled to a different device the set will be skipped.
- Auto Deletion of Old Backups is not supported.
- Verifications of vSphere backups are not supported and will be skipped during the verification process.
- UltraCopy cannot currently be used in conjunction with this agent.

Restoring a vSphere Backup

NOTE: All restores are performed via a LAN (NBD) connection.
NOTE: The default UltraBac device MUST be the one containing the vSphere Agent backup to be restored.

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.
2. Select and load the index for restore.

NOTE: If you choose to restore an incremental index, the necessary full and incrementals will automatically be restored.

3. Select the VM Disks for restore.
4. Click "Action"/"Restore Selected Files."

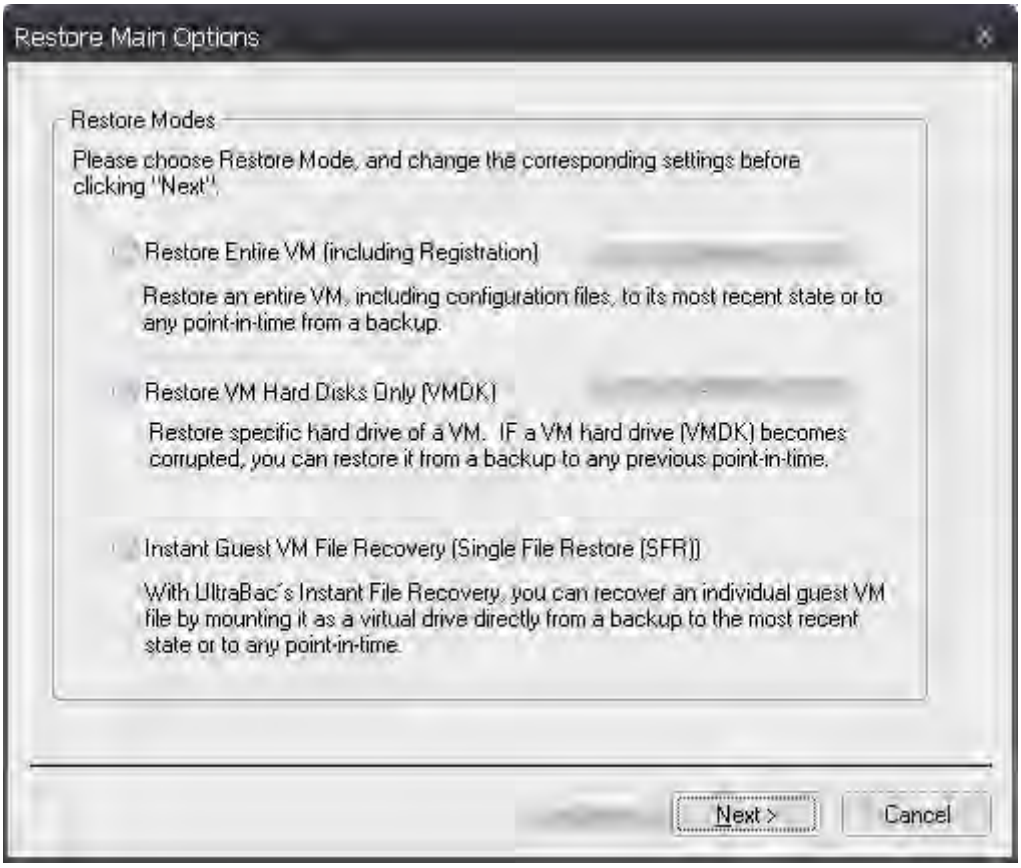


Fig. 3 - vSphere Agent Restore Options.

5. Select the type of restore to perform.
    - o Restore Entire VM (Including Registration)
    - o Restore VM Hard Disks only (VMDK)
    - o Instant Guest VM File Recovery – Single File Restore (SFR)

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.

Restore Entire VM (Including Registration)

1. Select "Restore Entire VM (Including Registration."
2. Click "Settings."

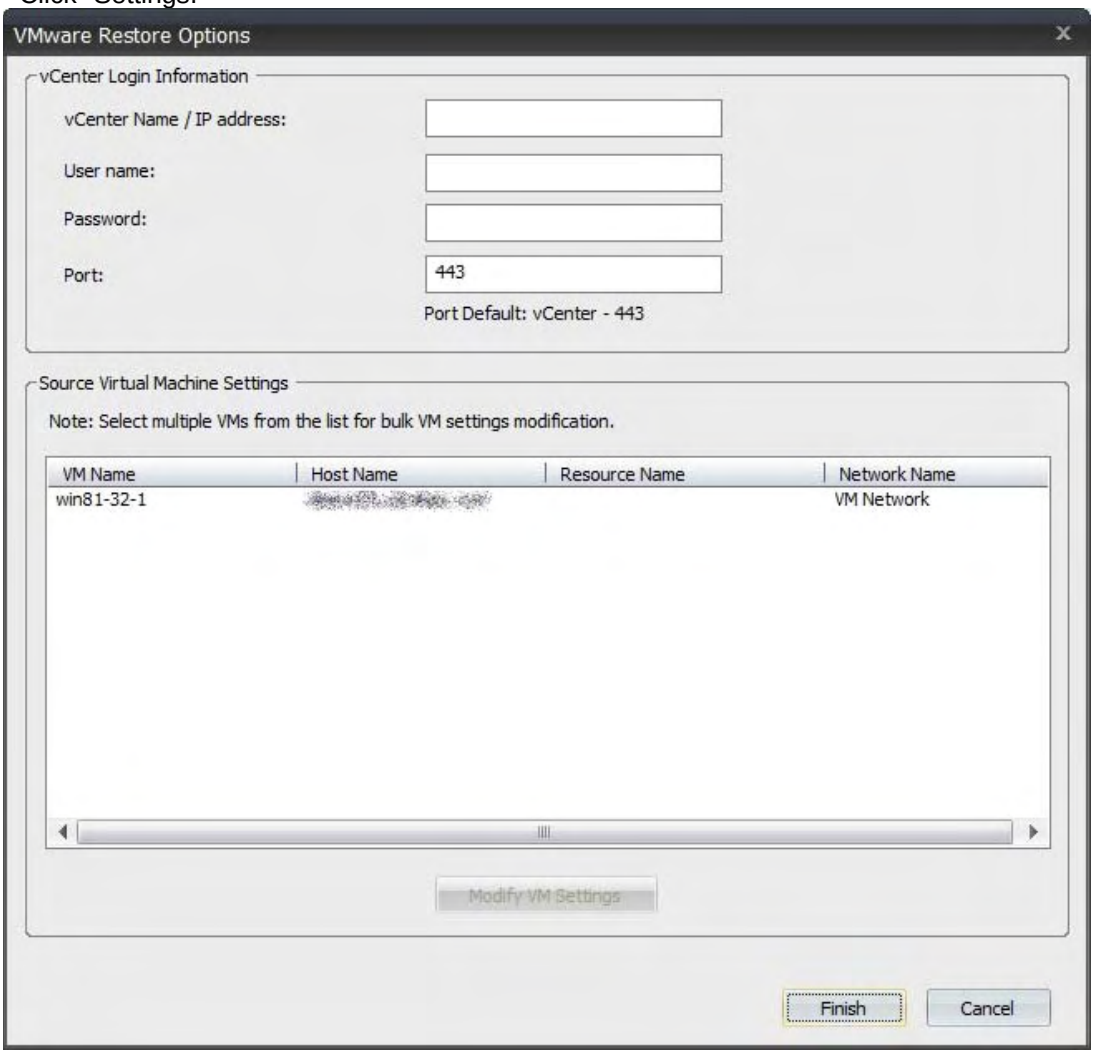


Fig. 4 - Configuring Full VM restore settings.

3. Type the vCenter name or IP address of the in the "vCenter Name / IP address" field. Defaults to the name / IP address used during the backup.
4. Enter a vCenter account that has full read and write permissions to the datastore you are recovering to in the "User name" field. Defaults to the user name used during the backup.
5. Enter the port used for connection into the "Port" field. The default is port 443.
6. Select 1 or more VMs and click "Modify VM Settings."

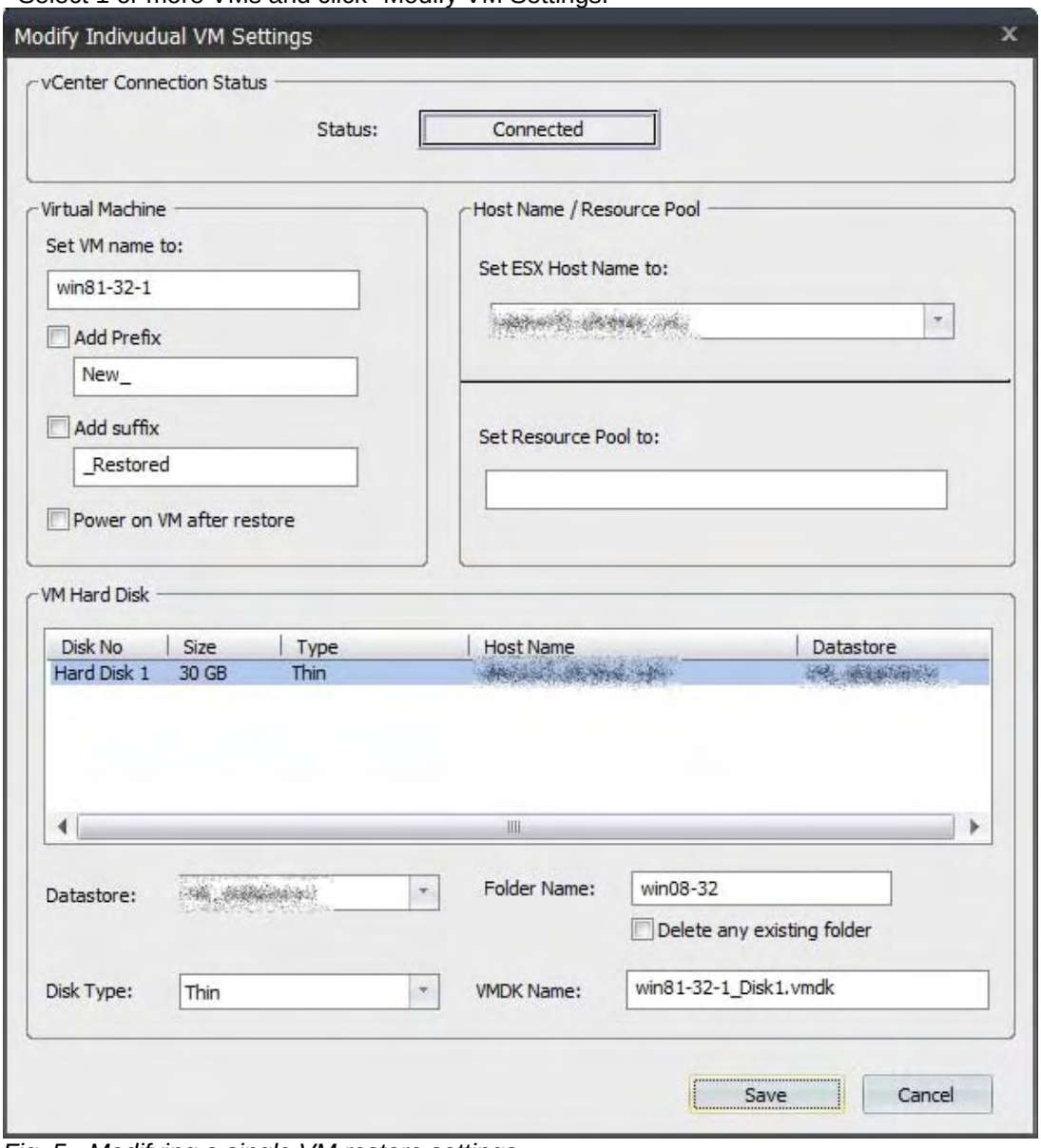


Fig. 5 - Modifying a single VM restore settings.

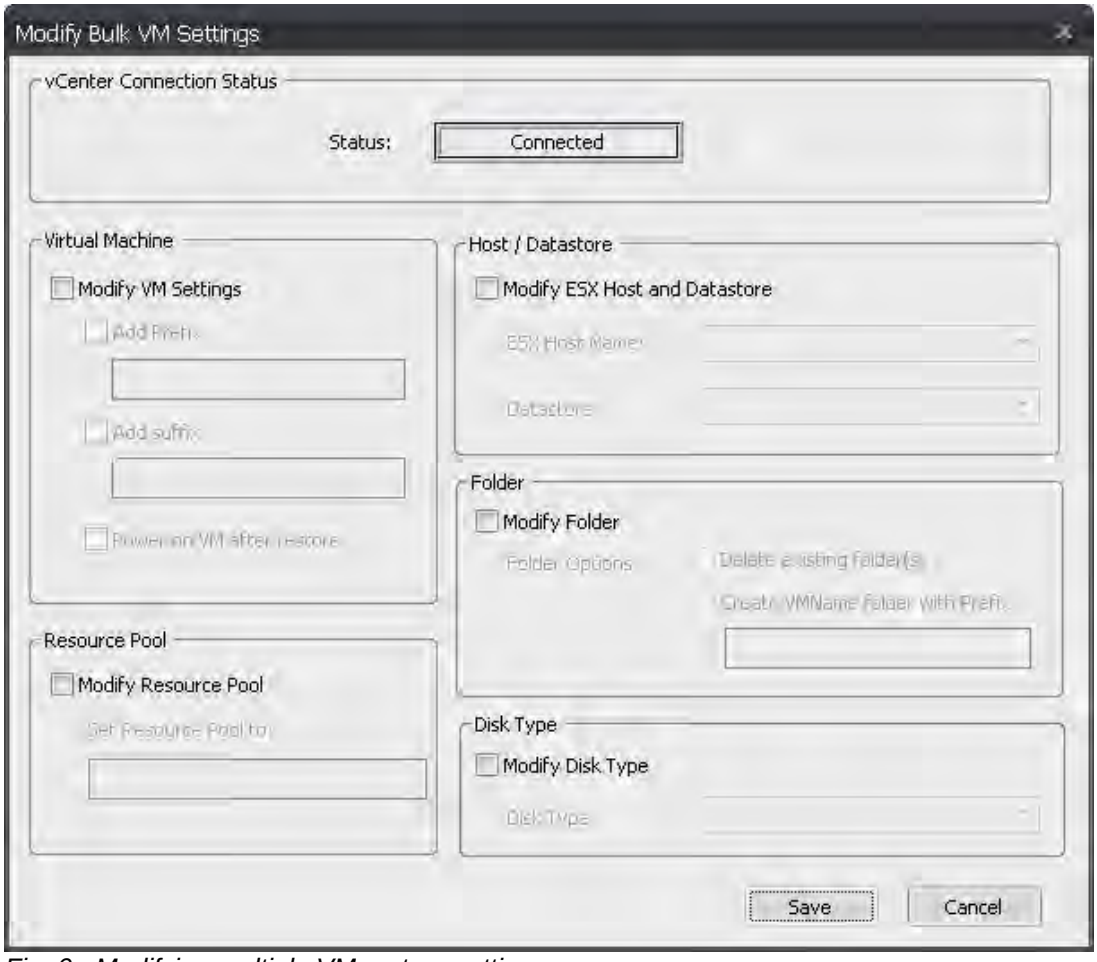


Fig. 6 - Modifying multiple VM restore settings.

7. Click "Save" to keep the changes and return to the previous window.
8. Click "Finish" to return to the main restore dialog.
9. Click "Next" to open the final restore options dialog window.

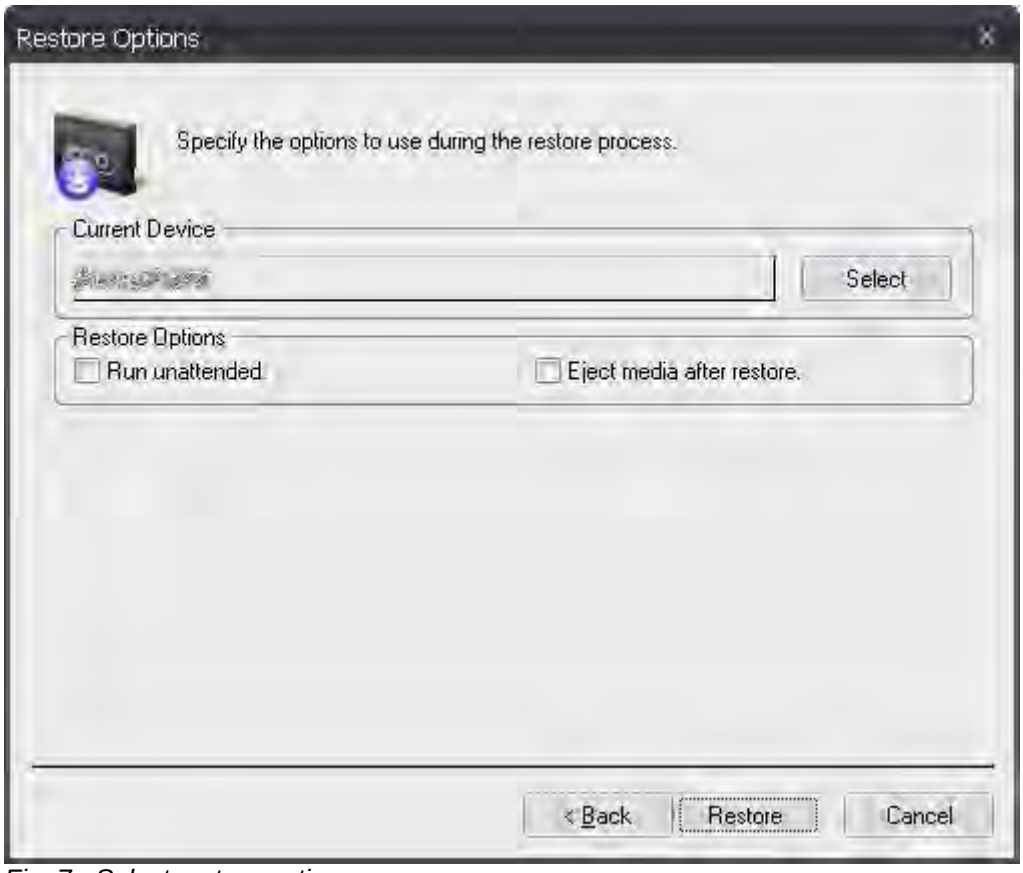


Fig. 7 - Select restore options

10. Click "Restore" to begin the restoration process.

Restore VM Hard Disks only (VMDK)

1. Select "Restore VM Hard Disks only (VMDK)."
2. Click "Settings."

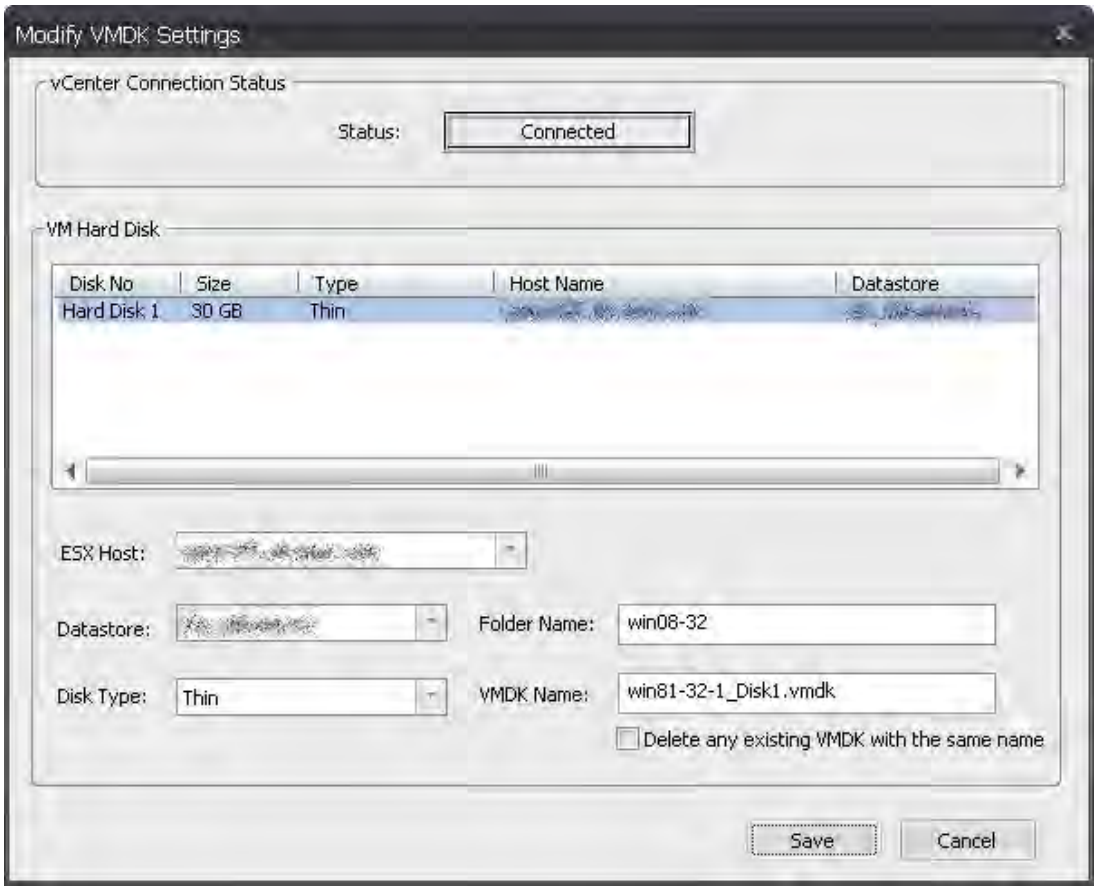


Fig. 8 - VMDK restore settings

3. Click "Save" to keep the changes and return to the previous window.
4. Click "Finish" to return to the main restore dialog.
5. Click "Next" to open the final restore options dialog window.

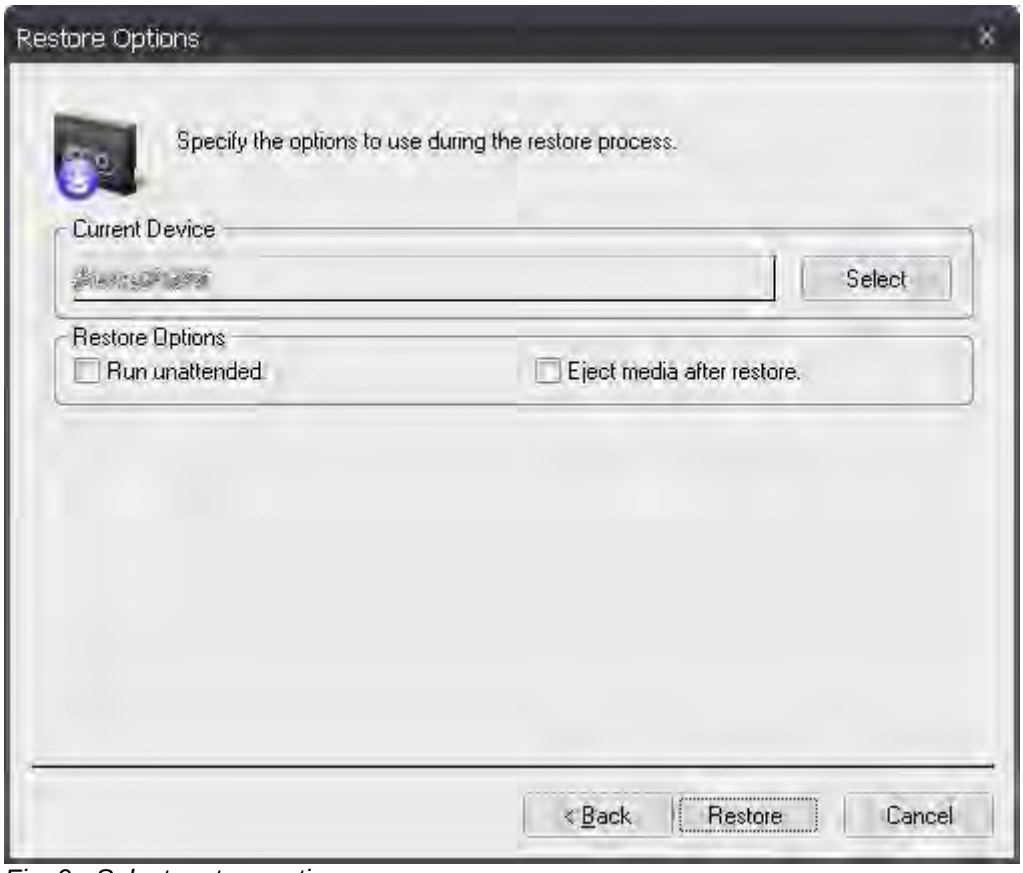


Fig. 9 - Select restore options

6. Click "Restore" to begin the restoration process

Instant Guest VM File Recovery – Single File Restore (SFR)

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.

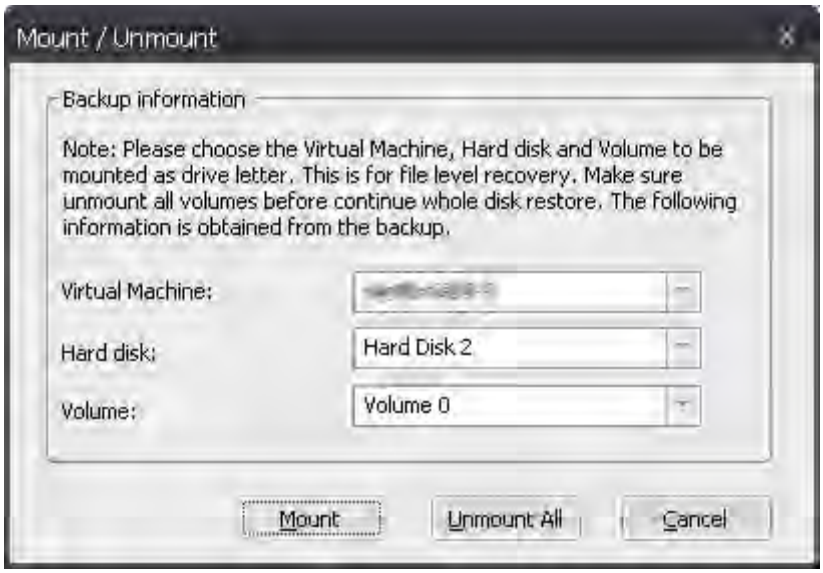


Fig. 10 - vSphere Mounting Options.

6. Select the Virtual Machine from the drop-down box.
7. Select the Hard disk from the drop-down box.
8. Select the preferred Volume from the drop-down box.
9. Click "Mount."

Once the drive is mounted, the necessary files can be dragged and dropped as needed.

To unmount a drive(s), click "Unmount All."

NOTE: If the set or UltraBac is closed before the backup is unmounted, simply launch the UltraBac Management Console and click on “Unmount All Volumes” located at “Tools”/“UBDR.” This will unmount any UltraBac mounted Image SFR, Hyper-V, or vSphere Agent backups. Alternatively, follow the same steps required to mount a backup until the "Unmount All" option button is visible.

Hyper-V Agent

The UltraBac Hyper-V Agent provides users with the ability to back up virtual machines without installing any agents on those virtual machines. It also allows users to back up from one central location.

NOTE: Only Hyper-V versions Windows Server 2008 R2, 2012, and 2012 R2 are supported.

NOTE: For information on configuring deduplication server, please see the UltraBac Knowledge Base:

UBQ000278: Configuring UltraBac Deduplication Server

Hyper-V Agent Set Creation

1. Launch the Backup wizard by selecting the Backup tab, and clicking "New."
2. Select the "Hyper-V Agent" and click "Next."
3. Enter the name of the Hyper-V Host server.

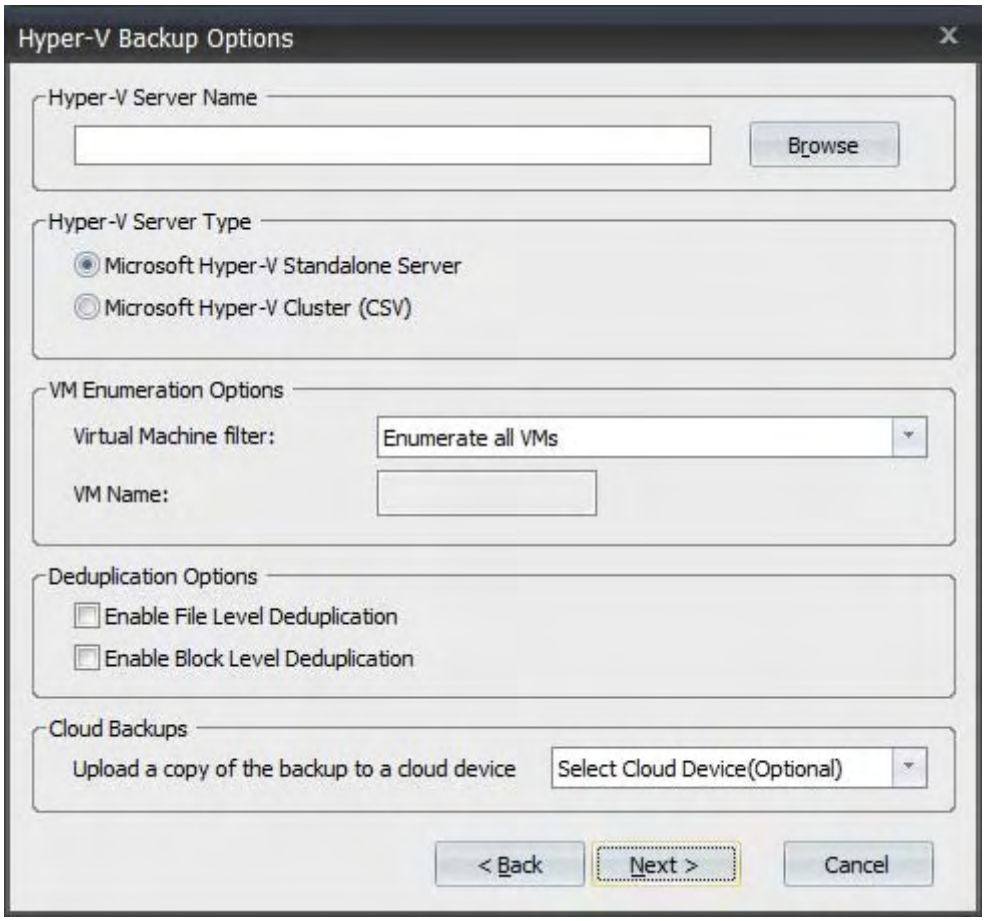


Fig. 1 - Hyper-V Backup Options.

NOTE: Backup user must have administrative privileges on the Hyper-V server.

4. Select how you would like UltraBac to enumerate the Virtual Machines (VM's):

    - Enumerate all VM’s
    - Enumerate only powered on VMs
    - Enumerate only powered off VMs
    - Enumerate by VM name

5. Select "Deduplication Options" if necessary.
6. Enter the name you wish to assign to the UltraBac set.



Fig. 2 - New Hyper-V backup set description.

7. Select the VM(s) you want to back up.

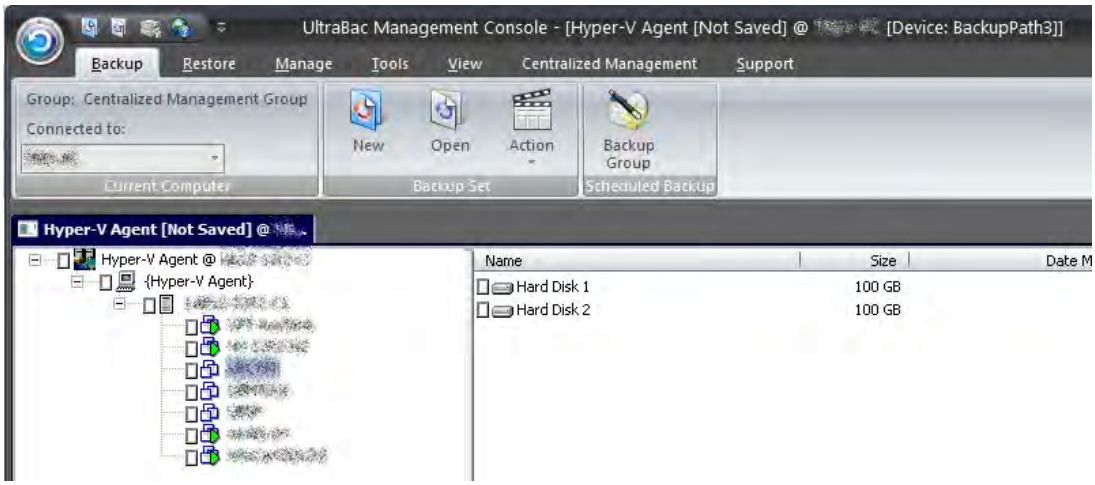


Fig. 3 - Enumerated Hyper-V Agent backup set.

8. Click "Action"/"Save Backup Set."

NOTE: All backups must be saved to a local drive or a UNC share and the Hyper-V server must be able to access the share.

NOTE: The Hyper-V Agent currently only supports MBR basic disks, not GPT basic disks, within the guest VM.

Microsoft has other conditions that must be met for the VSS backup of the guest VM to work:

- Backup (volume snapshot) Integration Service is installed and running in the child VM. The service name is "Hyper-V Volume Shadow Copy Requestor".

  Windows 2000: Backup Integration Service is not supported.

- The child VM must be in the running state.
- The Snapshot File Location for the VM is set to be the same volume in the host operating system as the VHD files for the VM.
- All volumes in the child VM are basic disks and there are no dynamic disks.
- All disks in the child VM must use a file system that supports snapshots (for example, NTFS).

Please see http://msdn.microsoft.com/en-us/library/dd405549(v=vs.85).aspx for more information.

Restoring a Hyper-V Backup

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.

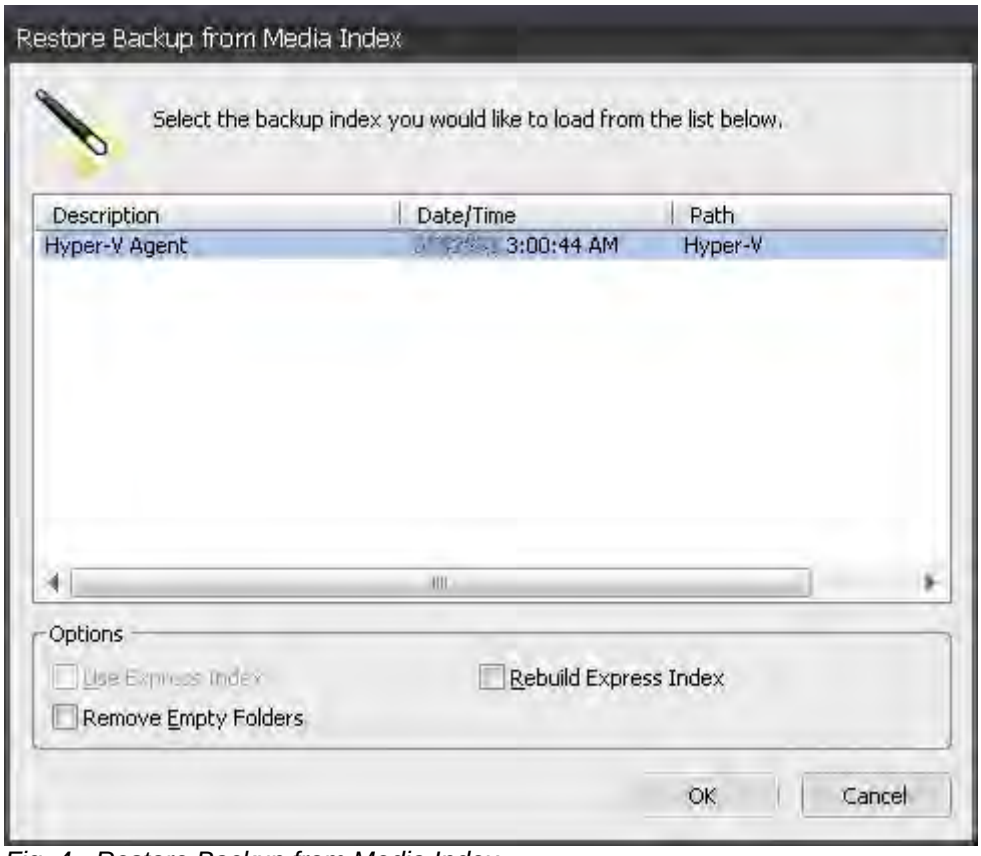


Fig. 4 - Restore Backup from Media Index.

2. Select and load the index for restore.
3. A window will prompt whether to restore to a different machine. Choose “No” to restore back to the original machine, or “Yes” to restore to a different machine.



Fig. 5 - Restore destination prompt.

4. Select the VM disks for restore.
5. Click "Action"/"Restore This Backup."



Fig. 6 - Hyper-V Restore Options.

6. Select the location you want to restore to. When restoring multiple VMs it is recommended you select the option to create sub-folders.

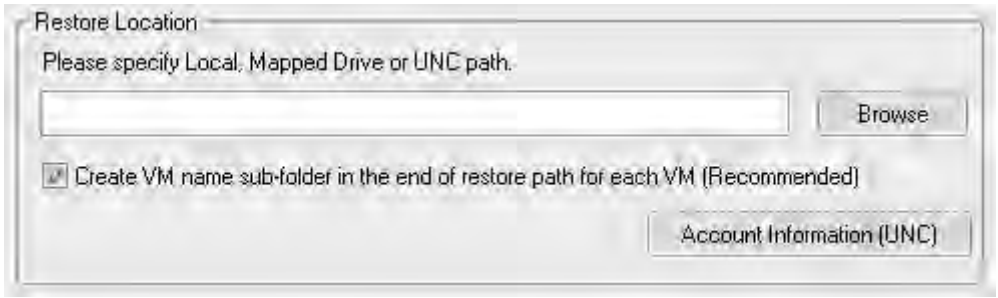


Fig. 7 - Restore Location.

NOTE: The restore must be back to a local share or UNC share.

7. Choose the format of the disk that you want to restore to:
   - VHD
   - VHDX (Windows Server 2012 and later only)
   - Keep Original Source Disk Format (VHD or VHDX)

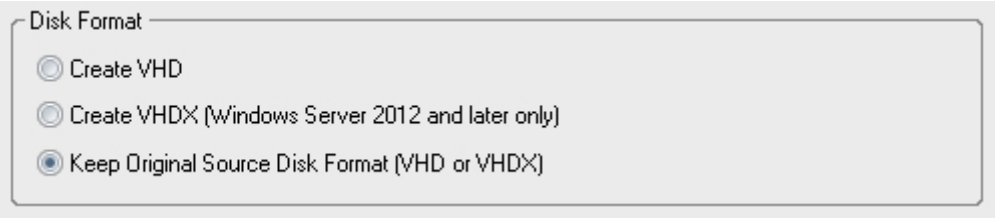


Fig. 8 - Disk Format.

8. Choose the disk type you want to restore to:

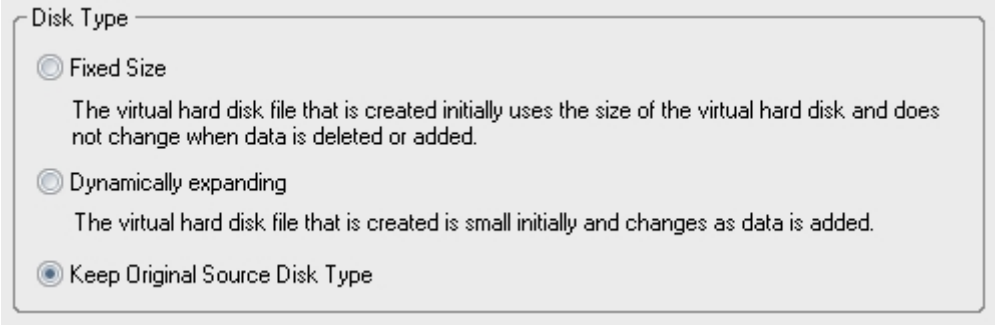


Fig. 9 - Disk Type.

9. Click “Next” and start the restore.

Restoring Individual Files from a Hyper-V Backup

1. Launch the Restore Wizard by selecting the Restore tab, and selecting the index source.

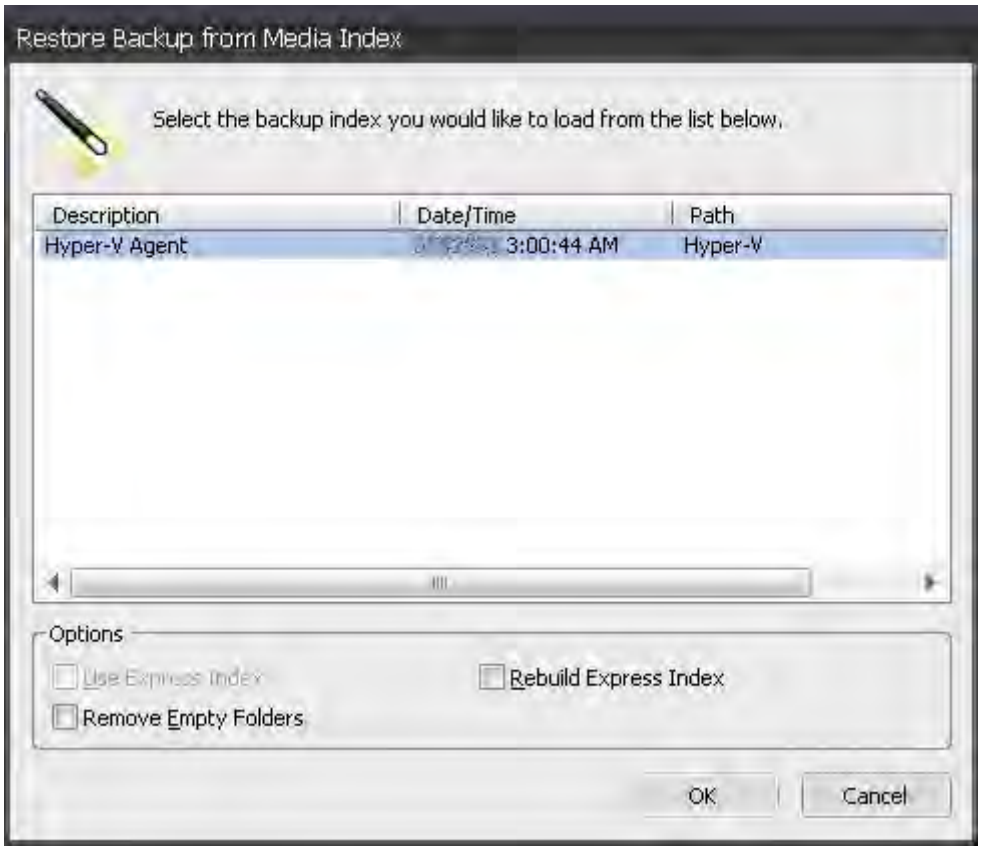


Fig. 10 - Restore Backup from Media Index.

2. Select and load the index for restore.
3. A window will prompt whether to restore to a different machine. Choose “No” to restore back to the original machine, or “Yes” to restore to a different machine.



Fig. 11 - Restore destination prompt.

4. Select the VM disks for restore.
5. Click "Action"/"Restore This Backup."
6. Choose the option for “File Restore.”

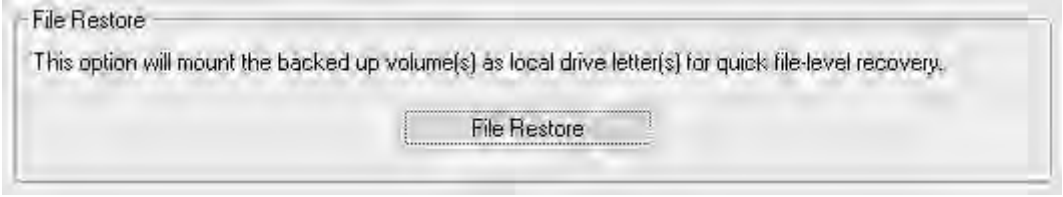


Fig. 12 - File Restore.

7. Select the following options:

    - Virtual Machine (if there were multiple VMs backed up)
    - Hard disk
    - Volume

8. Click the "Mount" button. This will mount the selected volume (VM disk) as a drive letter to the restore computer. From Windows Explorer on the restore computer, the files you want to restore can be drag and dropped from the mounted volume.

NOTE: The VM disk will be assigned the highest drive letter available (i.e. z:\).

9. Once complete, click the "Unmount All" button to unmount the VM Disk.

NOTE: If the set or UltraBac is closed before the backup is unmounted, simply launch UltraBac Management Console and click on “Unmount All Volumes” located at “Tools”/“UBDR.” This will unmount any UltraBac mounted Image SFR, Hyper-V, or vSphere Agent backups. Alternatively, follow the same steps required to mount a backup until the "Unmount All" option button is visible.

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 back up.

UltraBac supports SQL 2005, SQL 2008, SQL 2008 R2, SQL 2012, and SQL 2014. UltraBac no longer supports SQL 2000.

NOTE: The backup account must have either DB ownership or Administrative rights on each of the databases to be backed up.

The databases must have the recovery model set to "Full" or "Bulk Logged." Information on changing the recovery type can be found at:

http://msdn.microsoft.com/en-us/library/ms189275.aspx

NOTE: For information on configuring deduplication server, please see the UltraBac Knowledge Base:

UBQ000278: Configuring UltraBac Deduplication Server

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."

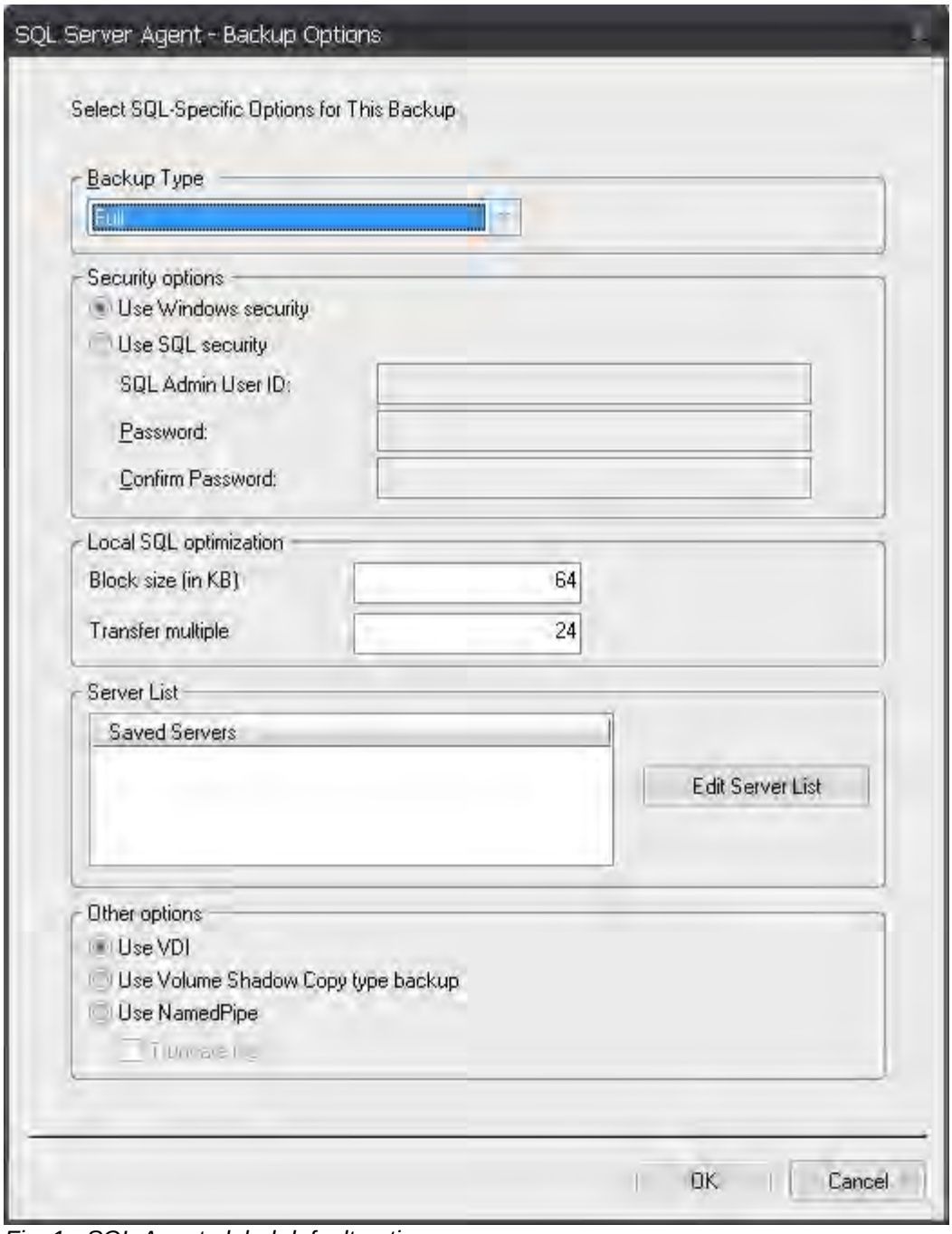


Fig. 1 - SQL Agent global default options.

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.

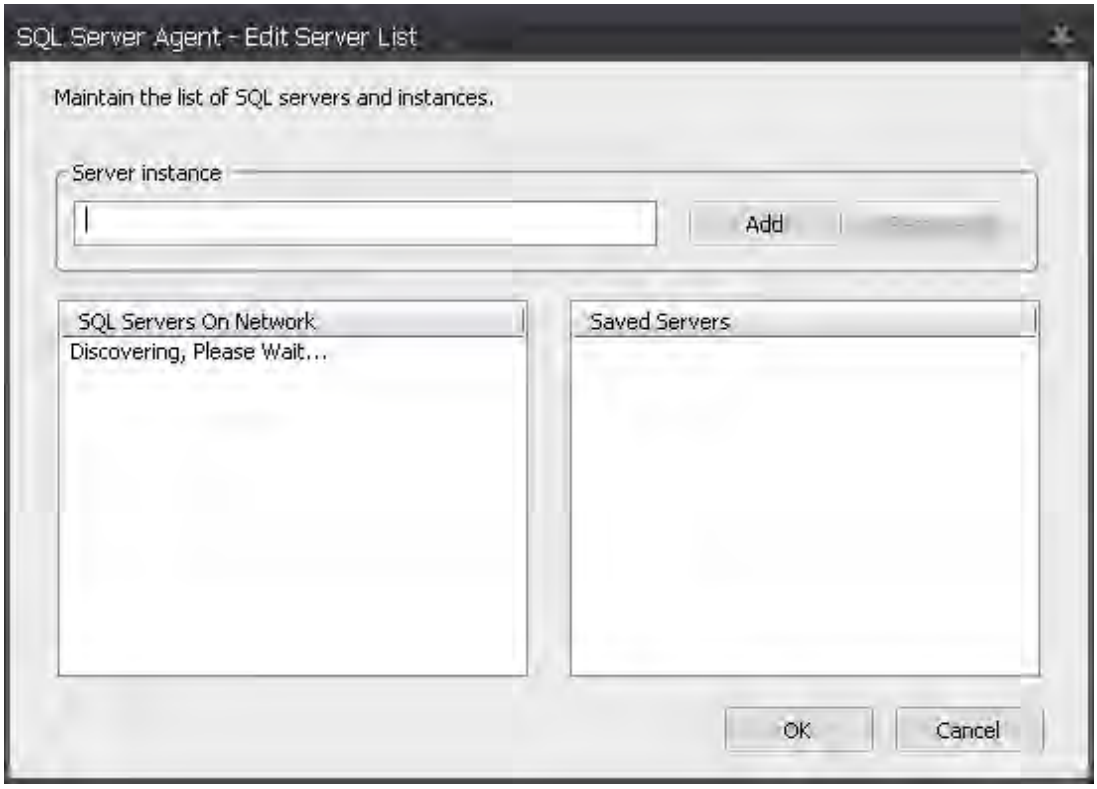


Fig. 2 - Editing the SQL server list.

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."

NOTE: SQL database names cannot contain "(" or ")" characters. If a database has those characters in the name, it will create an enumeration error.

Creating a 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. Highlight the server to be backed up and click "Next."
    - 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.

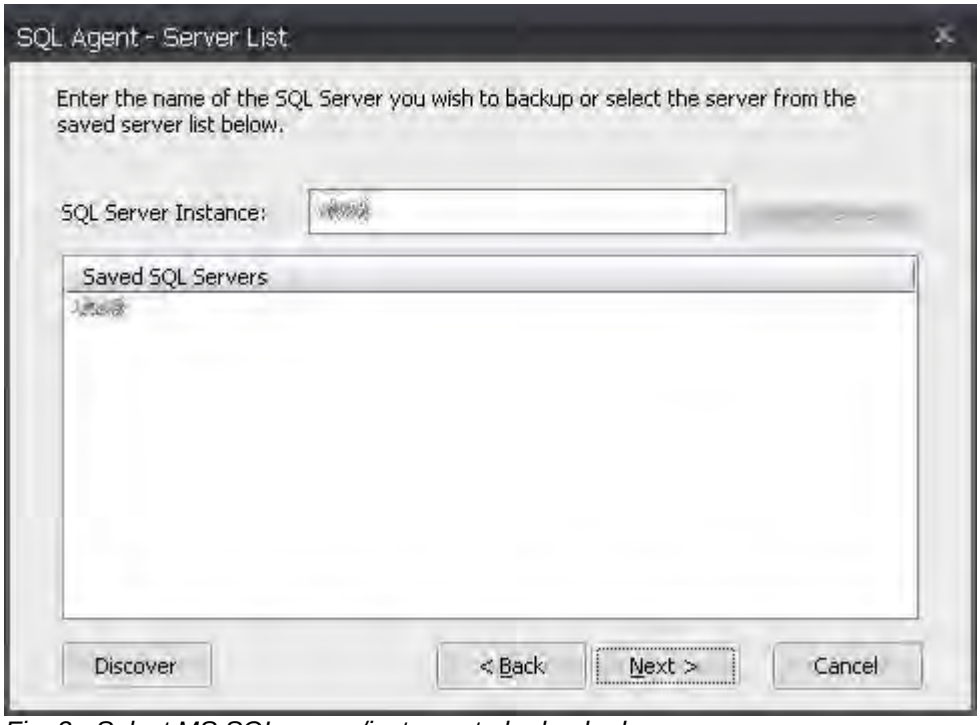


Fig. 3 - Select MS SQL server/instance to be backed up.

5. Set the Backup Type from the drop-down box.
6. Check the Security Options and click "Next."

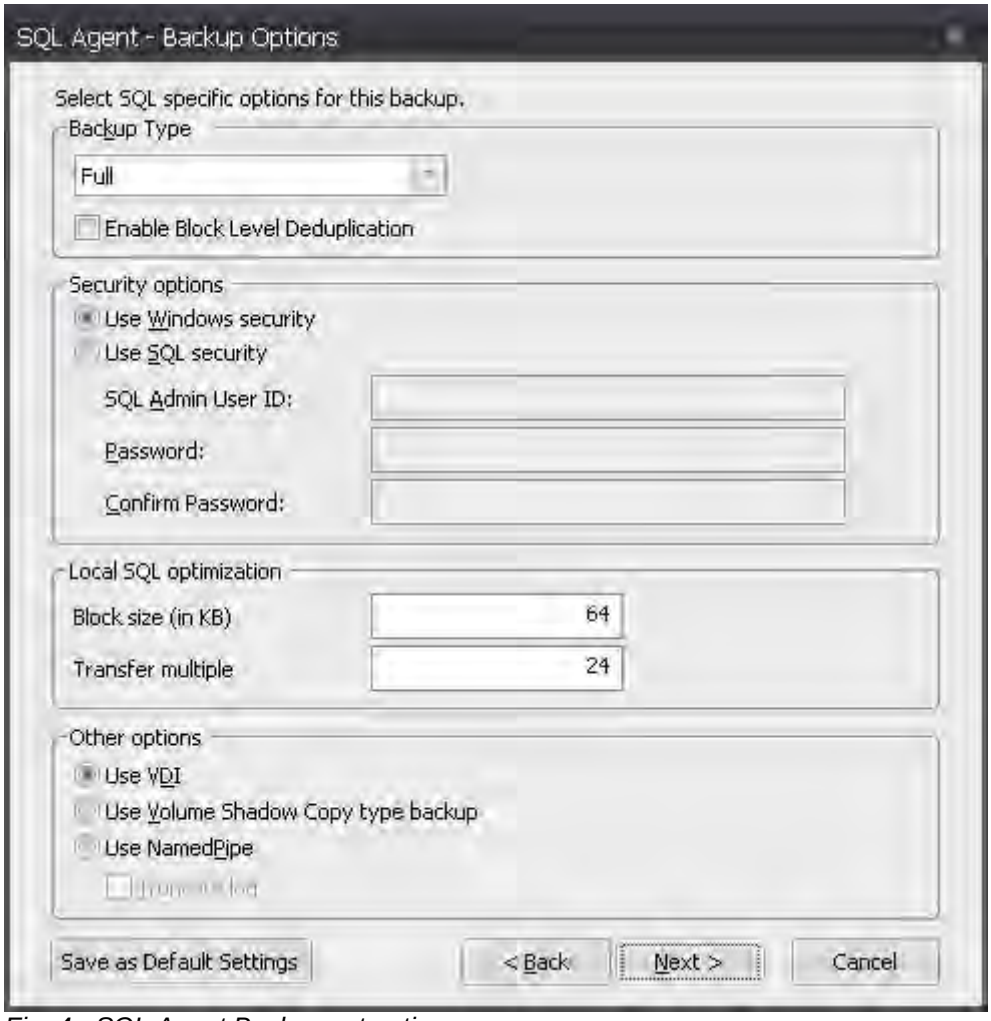


Fig. 4 - SQL Agent Backup set options.

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.
    - Use VDI – MS SQL 2000 and newer.
    - Use Volume Shadow Copy – MS SQL 2008 and newer.
    - Use NamedPipe – MS SQL 2000 only.

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.

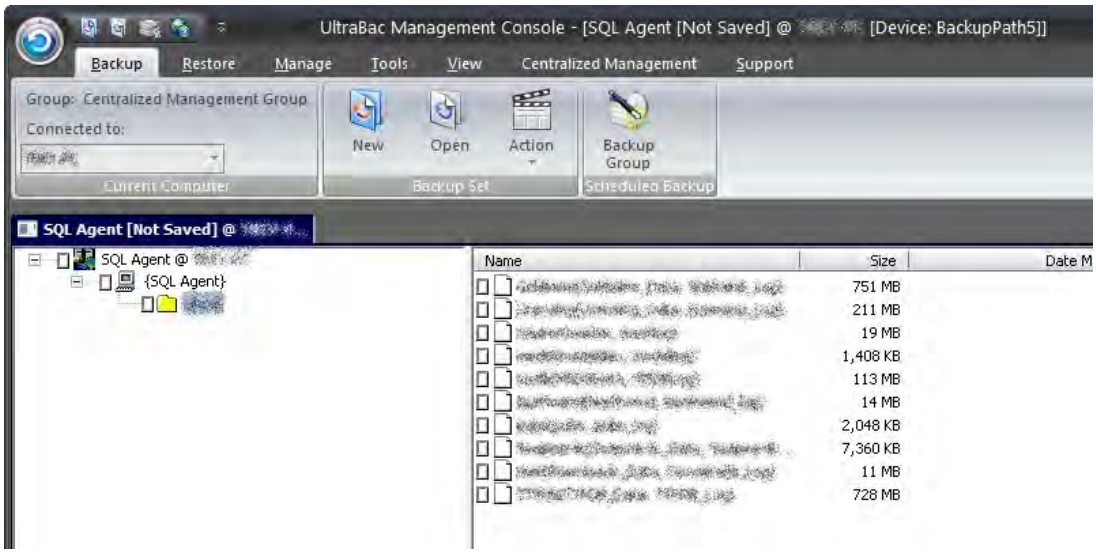


Fig. 5 - SQL backup set loaded in the File Viewer.

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 accounts specified in the UltraBac accounts under "Manage"/"General"/"Authentication"/"Accounts" 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 a 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 "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

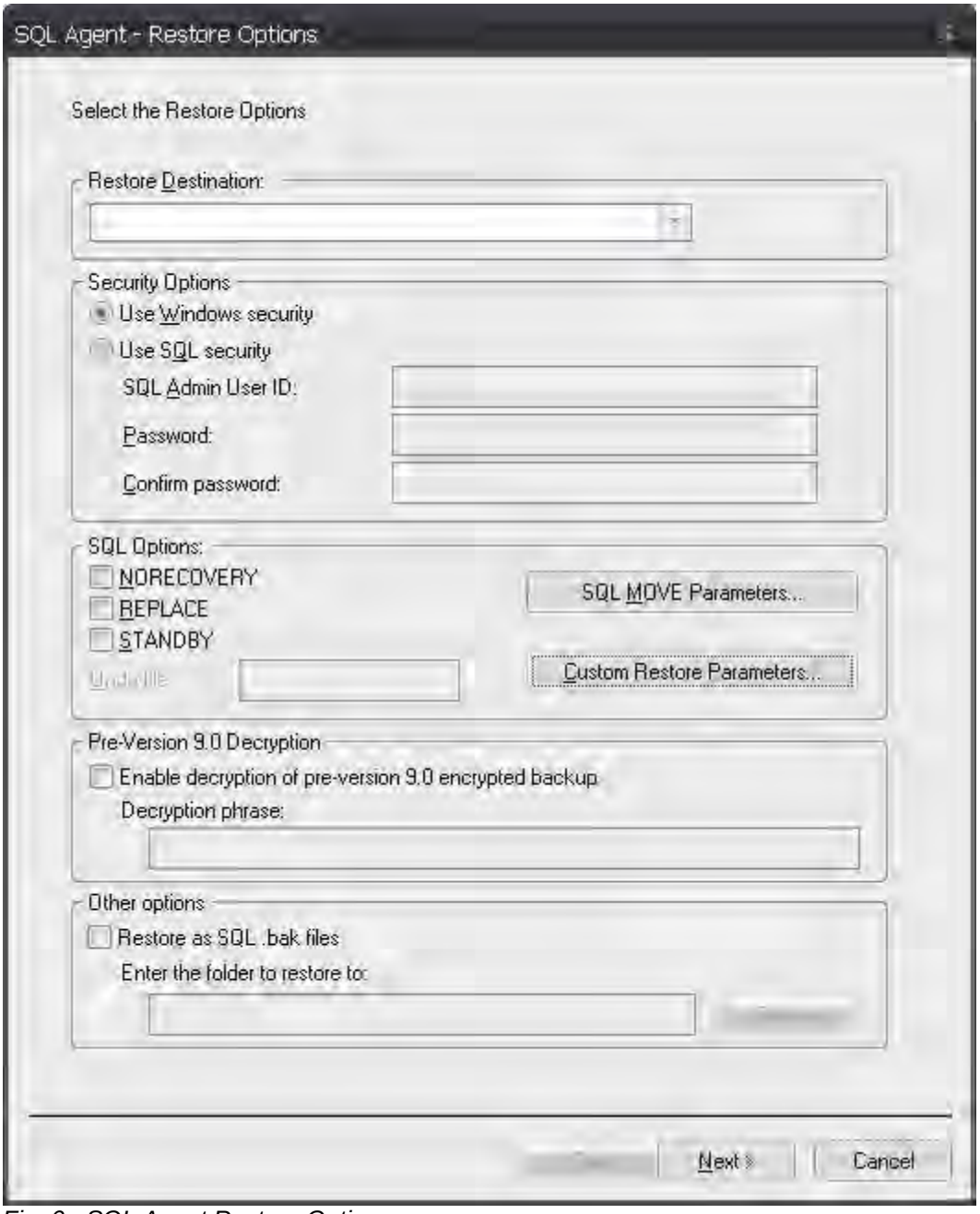


Fig. 6 - SQL Agent Restore Options.

- Restore Destination – Drop-down menu lists all servers registered in the local Client Network Utility.
- Security Options:
  - Use Windows security – Uses the current login account for restore.
  - Use SQL security – Uses the specified credentials for restore.

- SQL Options:
  - 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

  - REPLACE – Used when restoring a database to a remote SQL server, when the same database name exists on the target machine.
  - 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 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:

UBQ000205: SQL Move Parameters

Exchange Agent

Using the UltraBac Exchange Agent, Exchange versions 2007, 2010, 2013, and 2016 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. Support for Exchange 5.5, 2000, and 2003 has been discontinued beginning with UltraBac version 9.3.5. UltraBac version 9.4 has re-implemented support for Exchange version 2003.

Setup and Configuration

NOTE: The UltraBac Exchange Agent must be installed on the server hosting Exchange.

The Microsoft Exchange Tools must be installed on the Backup Host.

The UltraBac Exchange Agent does NOT support circular logging.

NOTE: For more information on enabling streaming backup support in Microsoft Exchange Server 2007 SP1, please see the UltraBac Knowledge Base:

UBQ000254: Enabling Streaming Backup Support in Microsoft Exchange Server 2007 SP1

NOTE: For information on configuring deduplication server, please see the UltraBac Knowledge Base:

UBQ000278: Configuring UltraBac Deduplication Server

An 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, 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 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 use 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," scroll down to “Members” and click the UltraBac users, then click the “OK” button.
4. On the Role Group page, click “Save.”

To check permissions in Exchange 2013 and 2016:

1. Open the Exchange Admin Center.
2. Go to “Permissions” / “Admin Roles.”
3. Click on Organization Management.
    - If the UltraBac account is not listed, click on "Details," Scroll down to “Members” and click the UltraBac users, then click the “OK” Button.
4. On the Role Group page, click “Save.”

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.

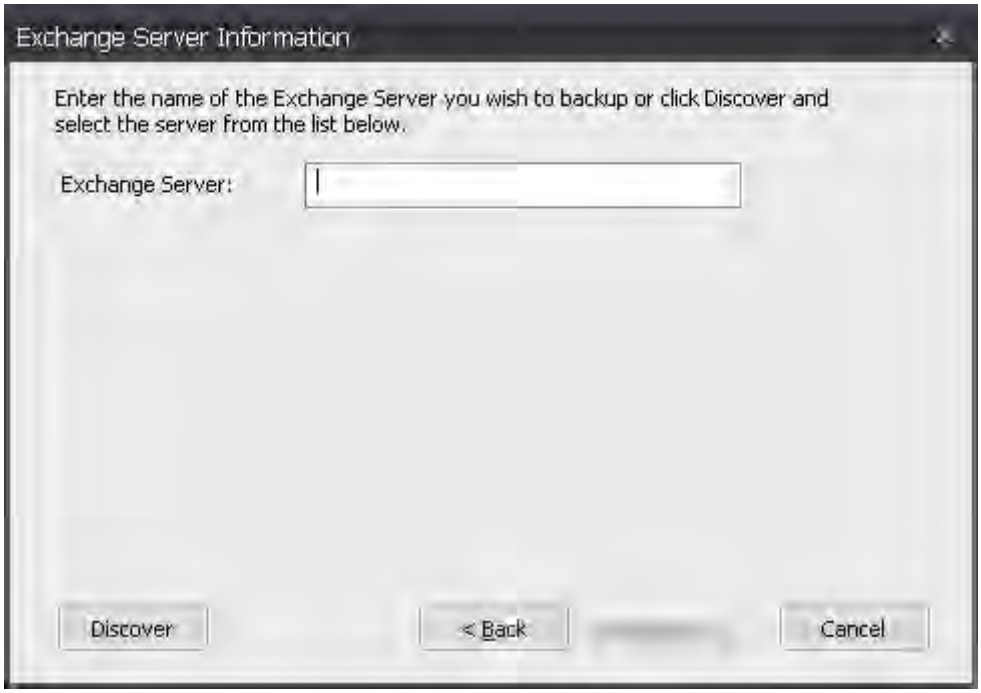


Fig. 1 - Exchange Server Information.

4. Select the Exchange server to be backed up.

5. Select the type of Exchange backup to be performed:
   - Full – Back up the database and transaction logs, and truncate the transaction logs.
   - Incremental – Back up only the transaction logs, and truncate the transaction logs.
   - Differential – Back up only the transaction logs, but do not truncate the transaction logs.

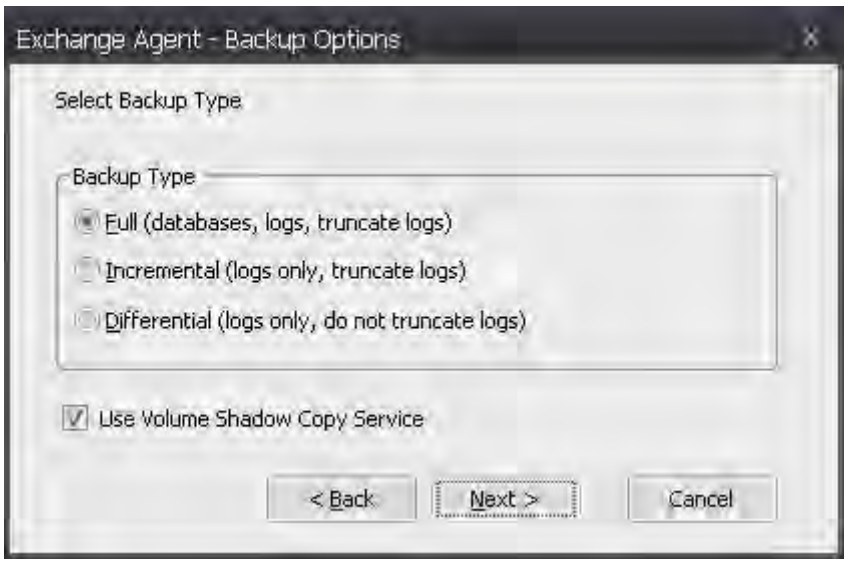


Fig. 2 - Exchange backup options.

NOTE: The "Use Volume Shadow Copy Service" must be used in Exchange 2010 and 2013.

6. Enter the description for the backup set as it will appear in the backup log. Click "Next."
7. At the Backup Wizard summary, click "Finish."

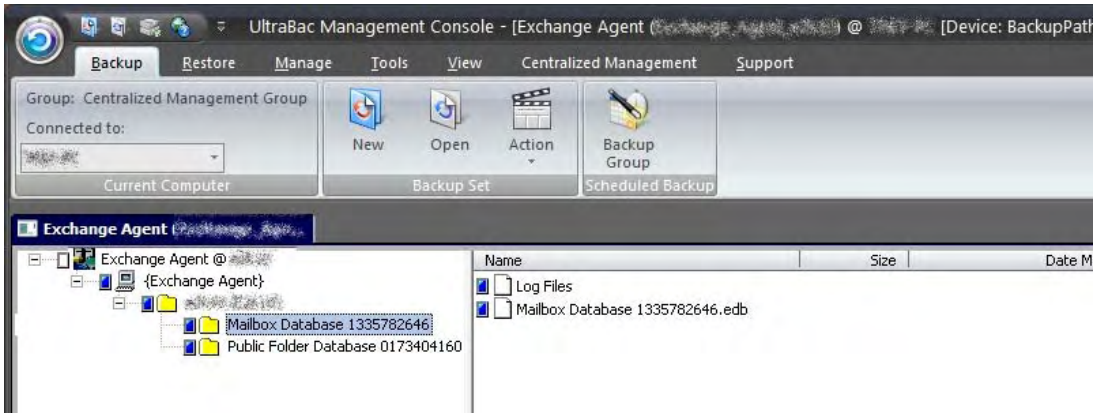


Fig. 3 - Viewing Exchange servers in the File Viewer.

Restoring an Exchange Server - Exchange 2003/2007/2010/2013/2016

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 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. For additional information on Exchange 2007 SCR / CCR Restores, please see the UltraBac Knowledge Base:

UBQ000257: Exchange 2007 SCR / CCR Restores

NOTE: UltraBac can restore the Mailbox Store to a recovery storage group in order to recover individual mailboxes. For additional information on Exchange 2007 Support and Using the Exchange 2007 Recovery Storage Group, please see the UltraBac Knowledge Base:

UBQ000250: Exchange 2007 Support
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. For additional information on Single Mailbox Restore with Exchange 2010 Recovery DB, please see the UltraBac Knowledge Base:

UBQ000259: Single Mailbox Restore with Exchange 2010 Recovery DB

Preparing the Exchange 2013 or 2016 Server for Restore

1. Open the Exchange Admin Center.
2. Go to "Servers"/"Databases.".
3. Select the database to restore.
4. Press the "..." icon and chose “dismount."

NOTE: It is highly recommended to use the option to copy the old log files to a separate location so that the log files can be replayed if needed.

5. Repeat for all databases to be restored.

NOTE: There may be times in which you will need to restore a single mailbox. For additional information on Single Mailbox Restore with Exchange 2013 Recovery DB, please see the UltraBac Knowledge Base:

UBQ000275: Single Mailbox Restore with Exchange 2013 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."

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."

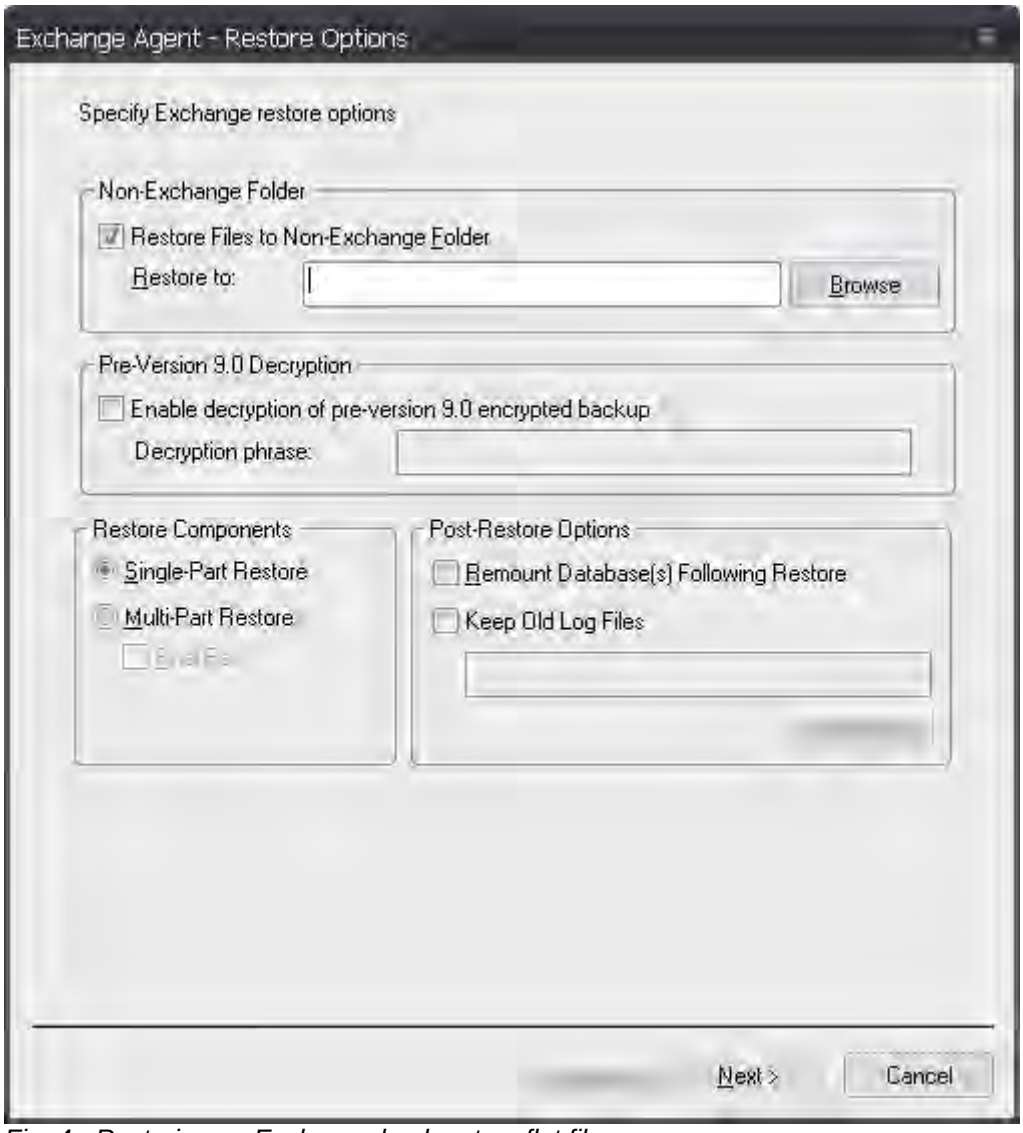


Fig. 4 - Restoring an Exchange backup to a flat file.

NOTE: If the original Exchange server is not online, then the flat file restore will fail with an Error 10061. For additional information on Exchange Flat File Restore if Original Exchange Server offline, please see the UltraBac Knowledge Base:

UBQ000263: Exchange Flat-File Restore if Original Exchange Server Offline

Exchange 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.

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:\ProgramFiles\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 additional information on Recovering to an Exchange 2003 Recovery Store, please see the UltraBac Knowledge Base:

UBQ000227: Recovering to an Exchange 2003 Recovery Store

Ux Agent

Ux Agent (File-by-File)

The UltraBac Ux Agent (File-by-File) provides UltraBac with the ability to back up files from the following platforms:

- Linux – OpenSUSE 11.0 to 11.4
- Linux – SUSE Linux Enterprise Server 11 SP1 to 11 SP3, 12.x
- Linux – Red Hat Enterprise Linux 6.0 to 6.7, 7.x
- Support for both 32 and 64-bit Operating Systems
- Support for ext2, ext3, and ext4 file systems

NOTE: There is a single Ux Agent RPM package for both the Ux Agent (File-by-File) and the Ux Image Agent. The ability to use the Ux Agent (File-by-File) and/or the Ux Image Agent is determined by the UltraBac license on the Windows computer running UltraBac managing the backups.

The installation, configuration, and uninstallation are identical between the File-by-File and Image Agents. The difference between the two are in the backup and restore operations.

Add UltraBac Repository
Install UltraBac RPMs
Upgrading
Uninstalling
Configuration
Backups
Restores

Installation

NOTE: The installation, configuration, and uninstallation is similar for OpenSUSE, SUSE Linux Enterprise Server, and Red Hat Enterprise Server. The examples below are for OpenSUSE.

NOTE: To add a Yum repository, type the following at a shell prompt as **`root`**:

yum-config-manager --add-repo ftp://rpmrepo.ultrabac.com/uxagent/RHEL/6.x/ultrabac.repo

yum-config-manager --enable ultrabac*

Adding UltraBac repository:

1. Open the Software Repositories manager by opening "YaST / Software / Software Repositories."

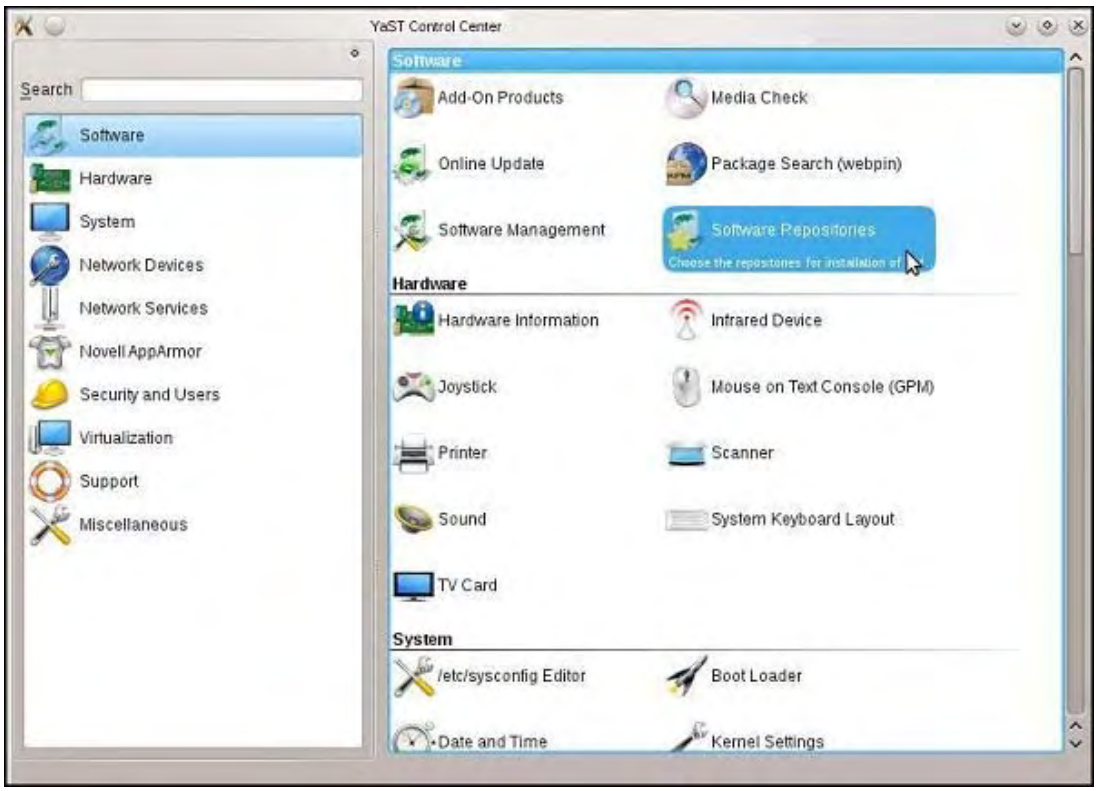


Fig. 1 - Software Repository.

2. Click "Add."

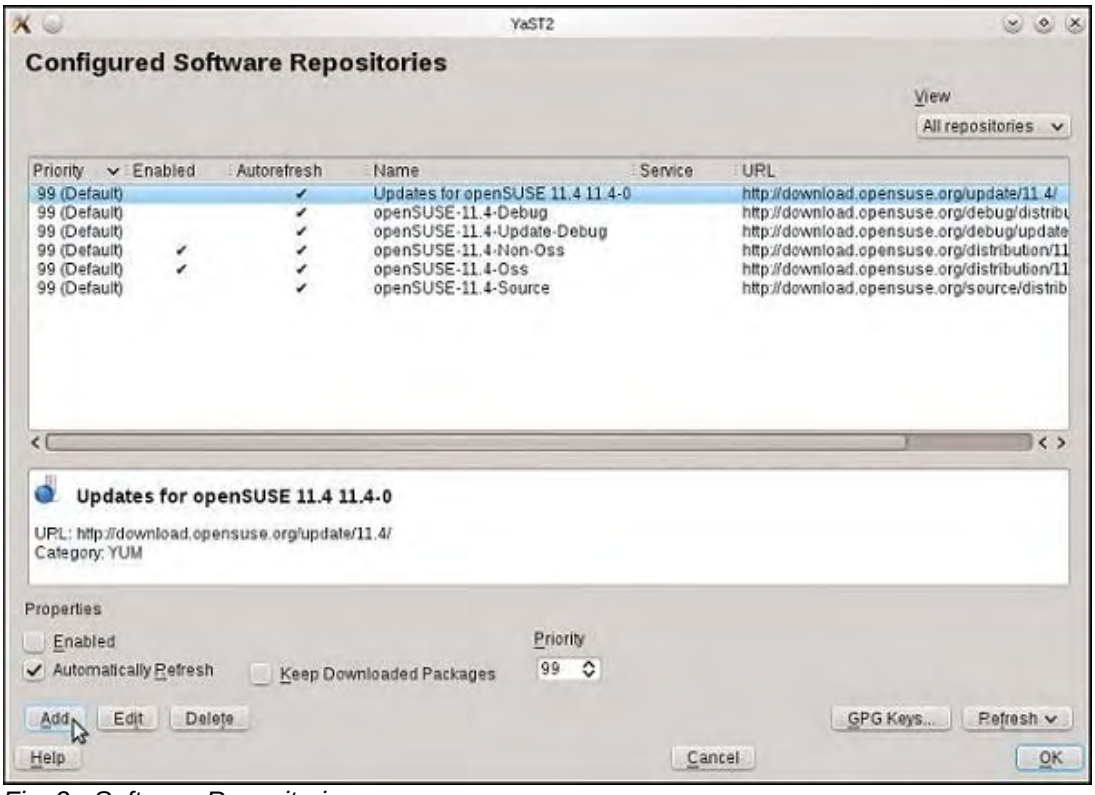


Fig. 2 - Software Repositories.

3. Select the Media Type (FTP) to be used for downloading the repository. Click "Next."

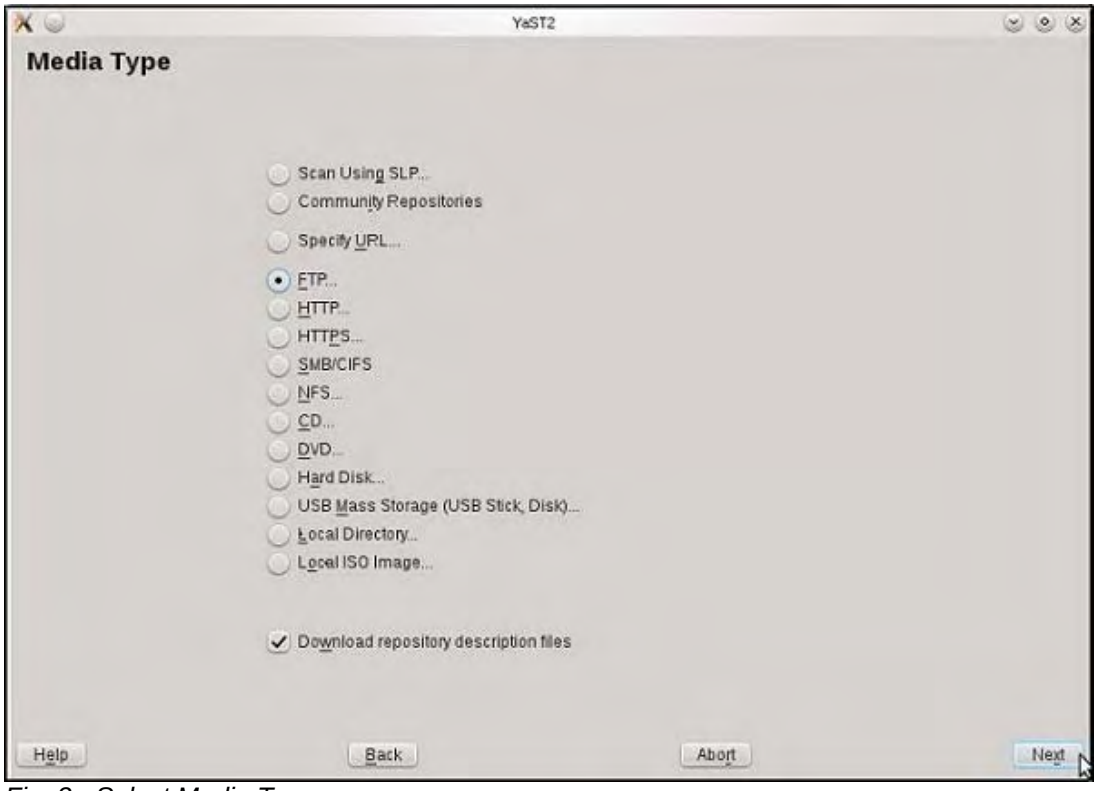


Fig. 3 - Select Media Type.

4. Enter the URL of the repository. Click "Next." The path to the RPM repository for UltraBac containing all the versions of RPMs can be found at "https://www.ultrabac.com/download-linux-free-trial." Select the version and URL path you will be using.

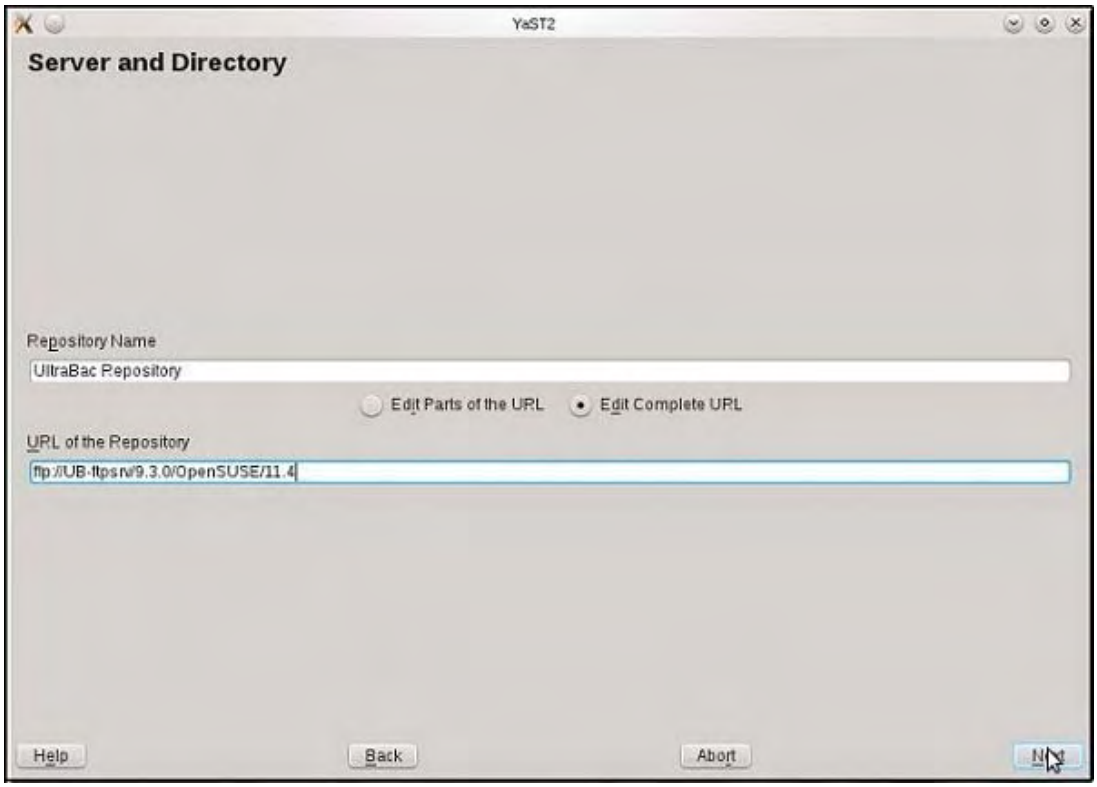


Fig. 4 - Enter repository URL.

5. Progress of the events can be seen in Figure 5.

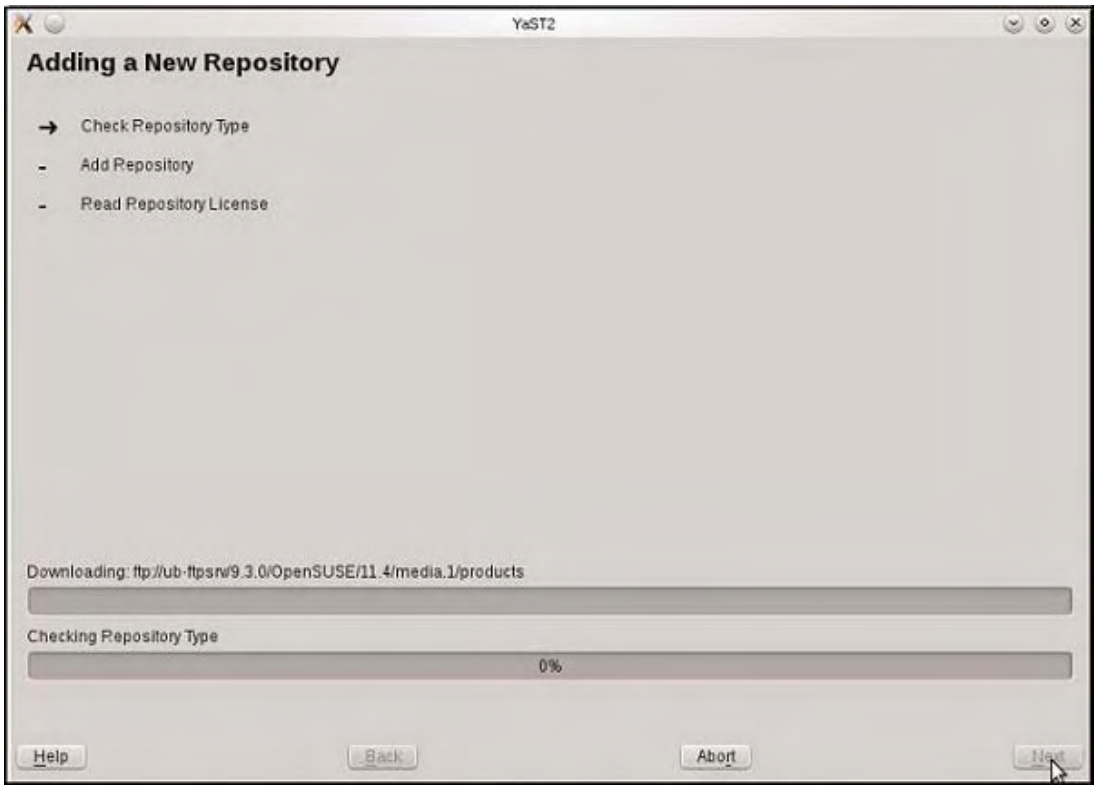


Fig. 5 - Add new repository.

The "UltraBac-UxAgent" RPM has a dependency on the "UltraBac-dm" RPM (driver) which is automatically resolved by the software installer. The Ux Agent can be installed through YaST using the following steps:

1. Start "Software Management" by opening "YaST / Software / Software Management."

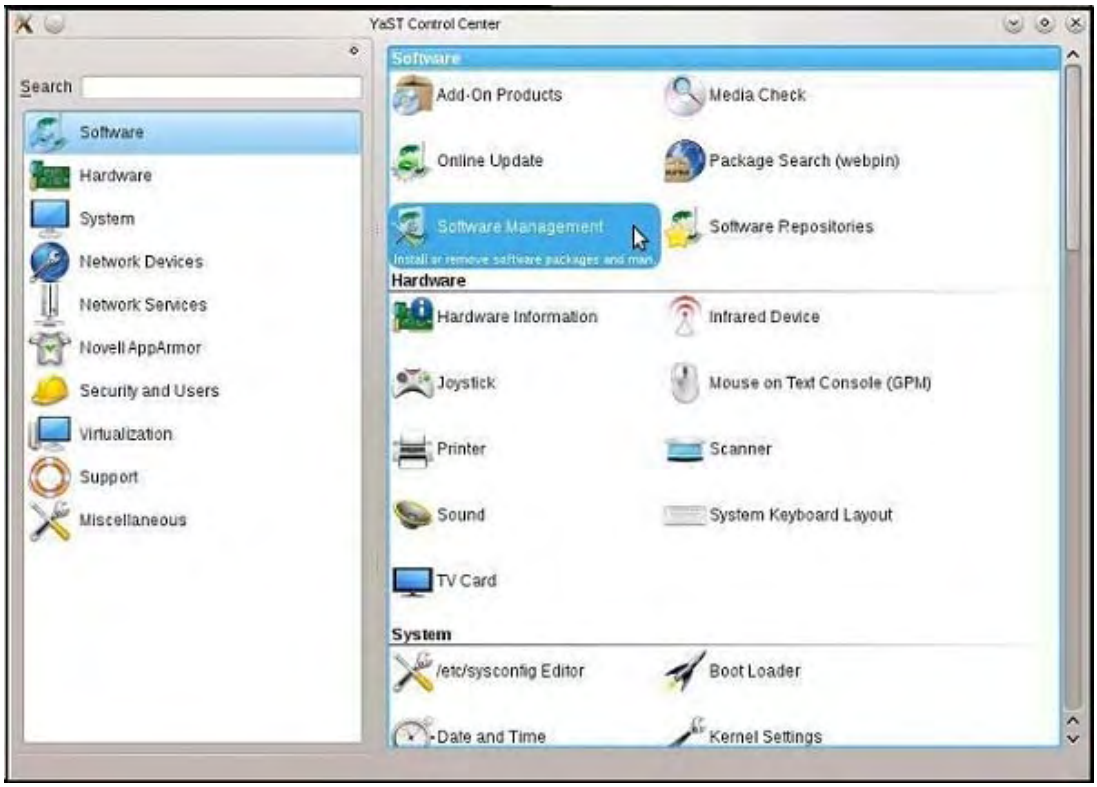


Fig. 6 - Software Management.

2. The progress of the Software Manager can be seen in Figure 7.

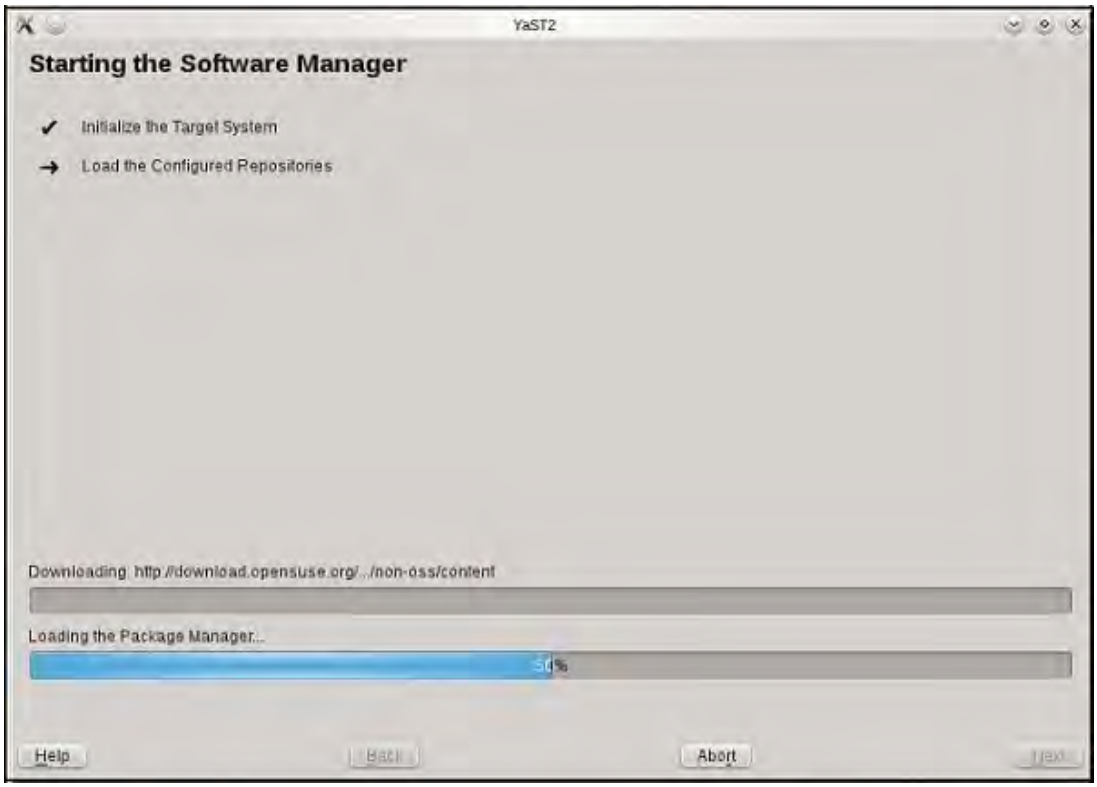


Fig. 7 - Software Manager progress.

3. Search for "ultrabac" and select "UltraBac-UxAgent." Click "Accept."

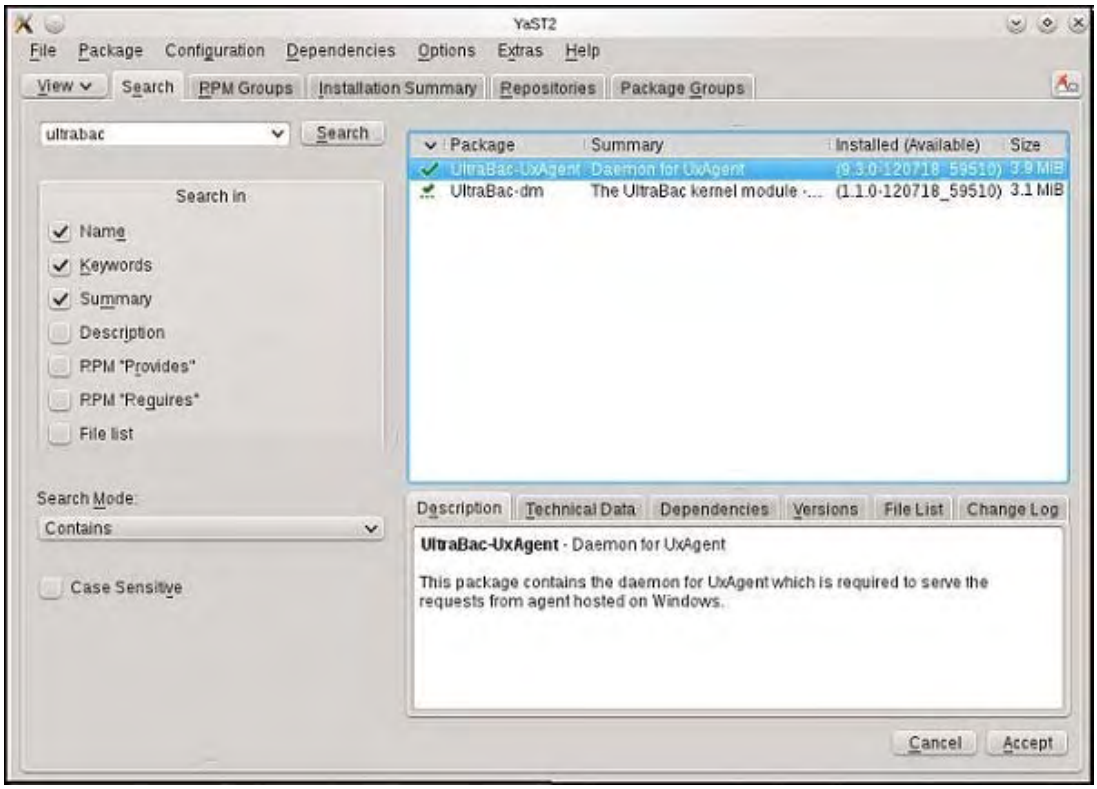


Fig. 8 - Search.

4. Dependencies will be installed automatically. Click "Continue" to perform installation.

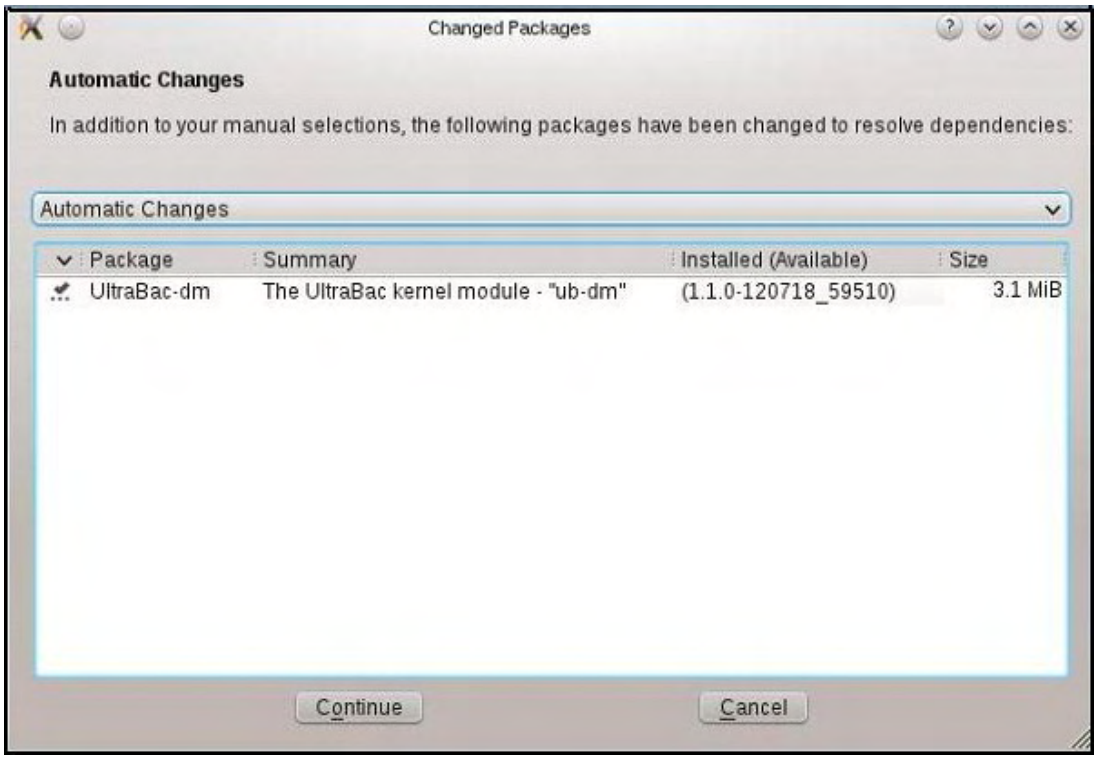


Fig. 9 - Dependencies.

5. The installation progress can be seen in Figure 10.

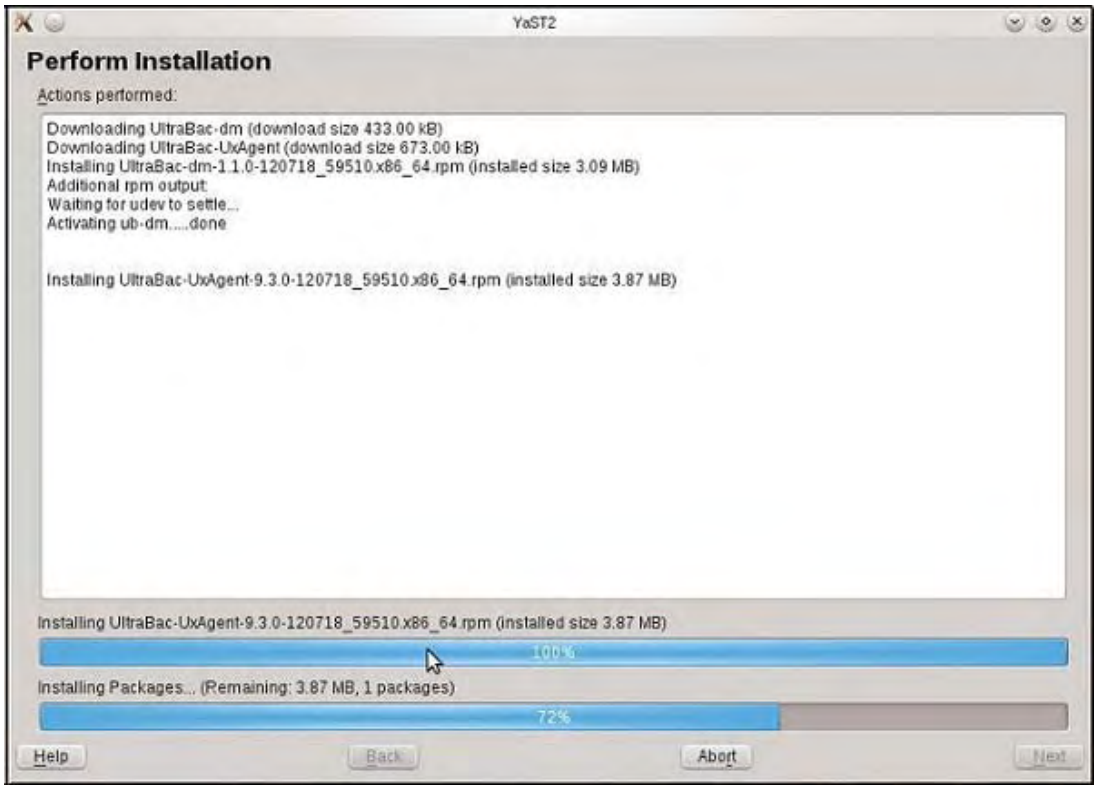


Fig. 10 - Installation progress.

Upgrading

Before upgrading the ultrabac RPM on your Linux computer, remove all devices added under UltraBac Ux Agent protection using the UltraBac UxAgent Device Configuration Menu utility. See the Configuration section on how to remove devices from protection.

Uninstallation

Before removing the UxAgent server RPM from your Linux computer, remove all devices added under UltraBac Ux Agent protection using the UltraBac UxAgent Device Configuration Menu utility. See the Configuration section on how to remove devices from protection.

Manual Uninstallation

1. To uninstall the "UltraBac-UxAgent" from your Linux computer, use the "rpm -e UltraBac-UxAgent" command.
2. To uninstall the "UltraBac-dm" (driver) from your Linux computer, use "rpm -e UltraBac-dm" command.

Uninstallation Using YaST

The "UltraBac-UxAgent" rpm has a dependency on "UltraBac-dm" RPM so "UltraBac-dm" RPM is not removed until "UltraBac-UxAgent" RPM is removed.

1. Start "Software Management" by opening "YaST / Software / Software Management."

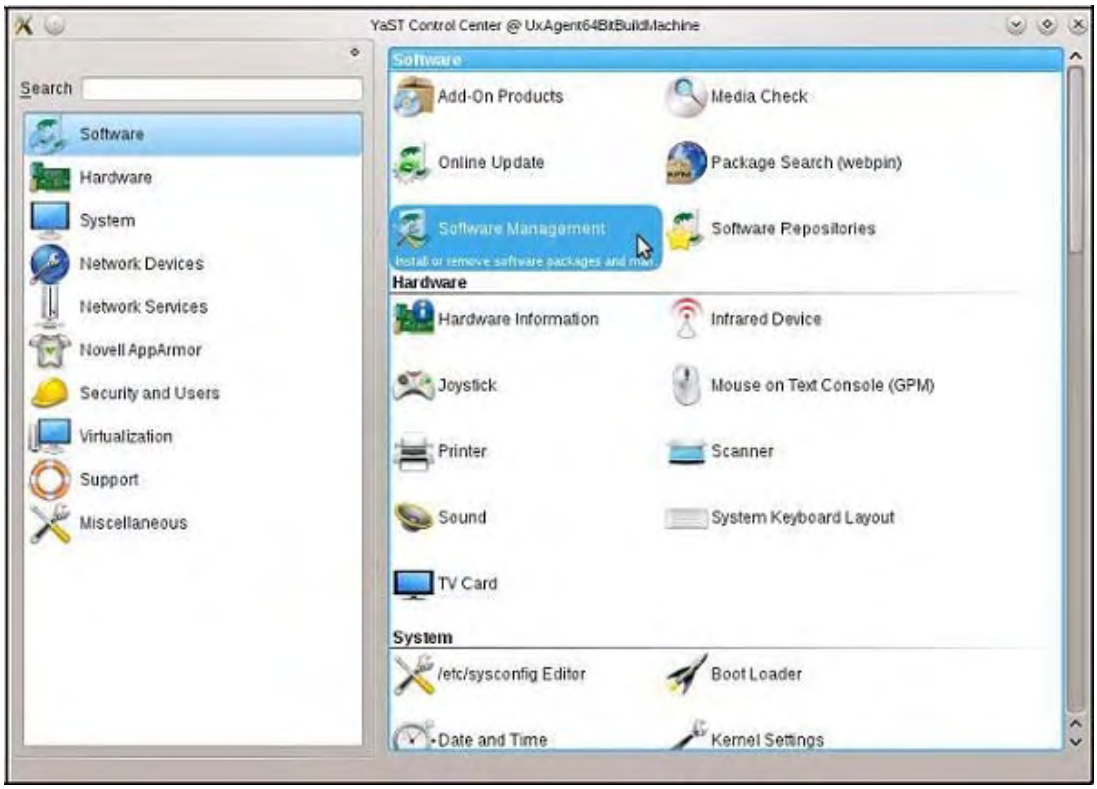


Fig. 11 - Software Management.

2. The progress of the Software Manager can be seen in Figure 27.

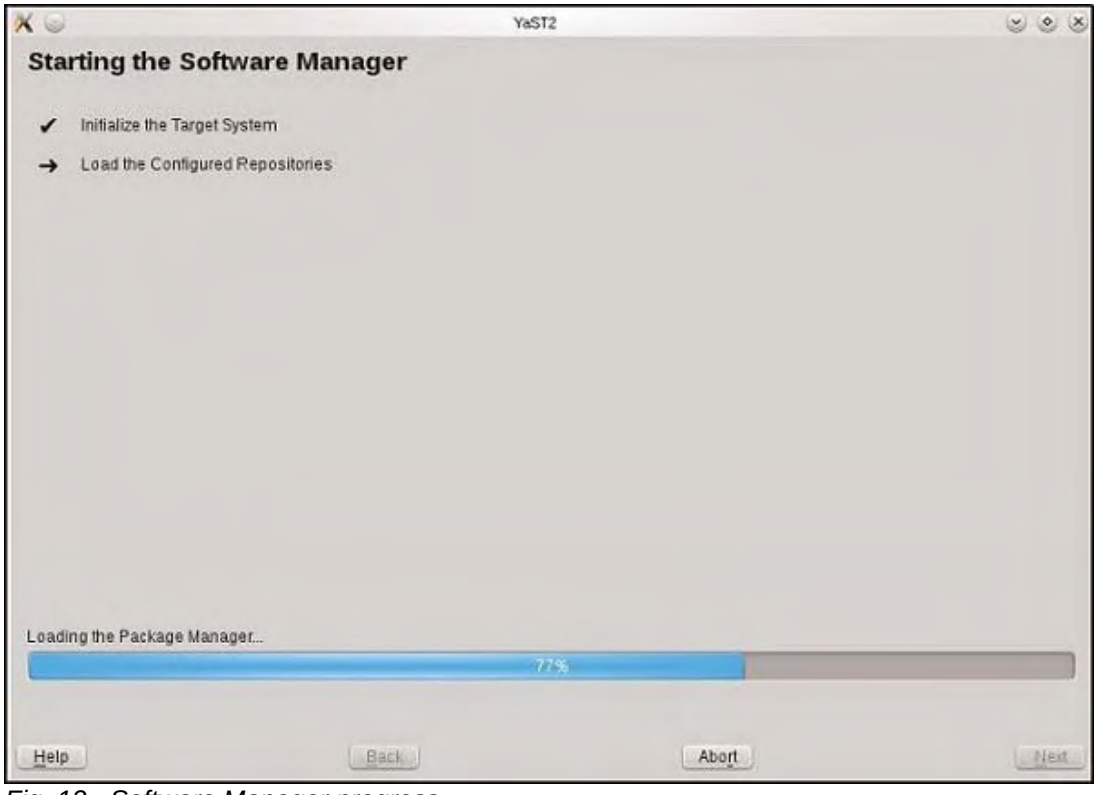


Fig. 12 - Software Manager progress.

3. Search for "ultrabac" and select "UltraBac-UxAgent" and "UltraBac-dm." Click "Accept."

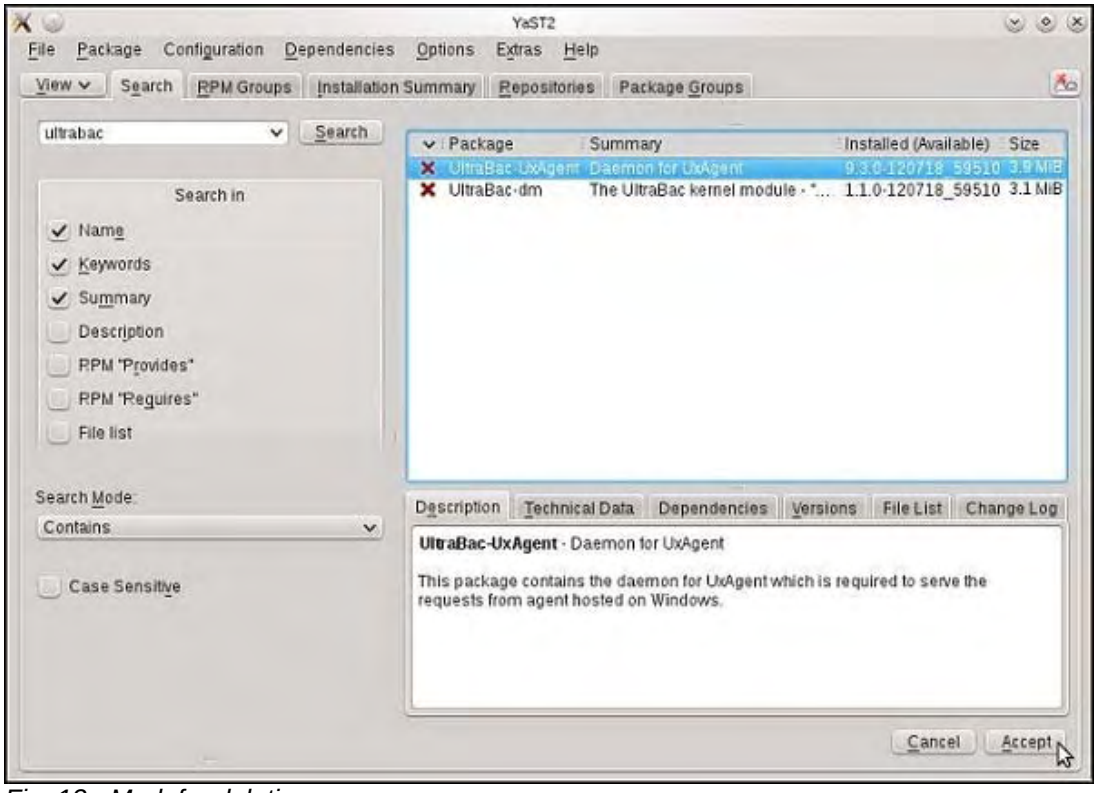


Fig. 13 - Mark for deletion.

4. (Optional) To remove the repository, select "Software Repositories."

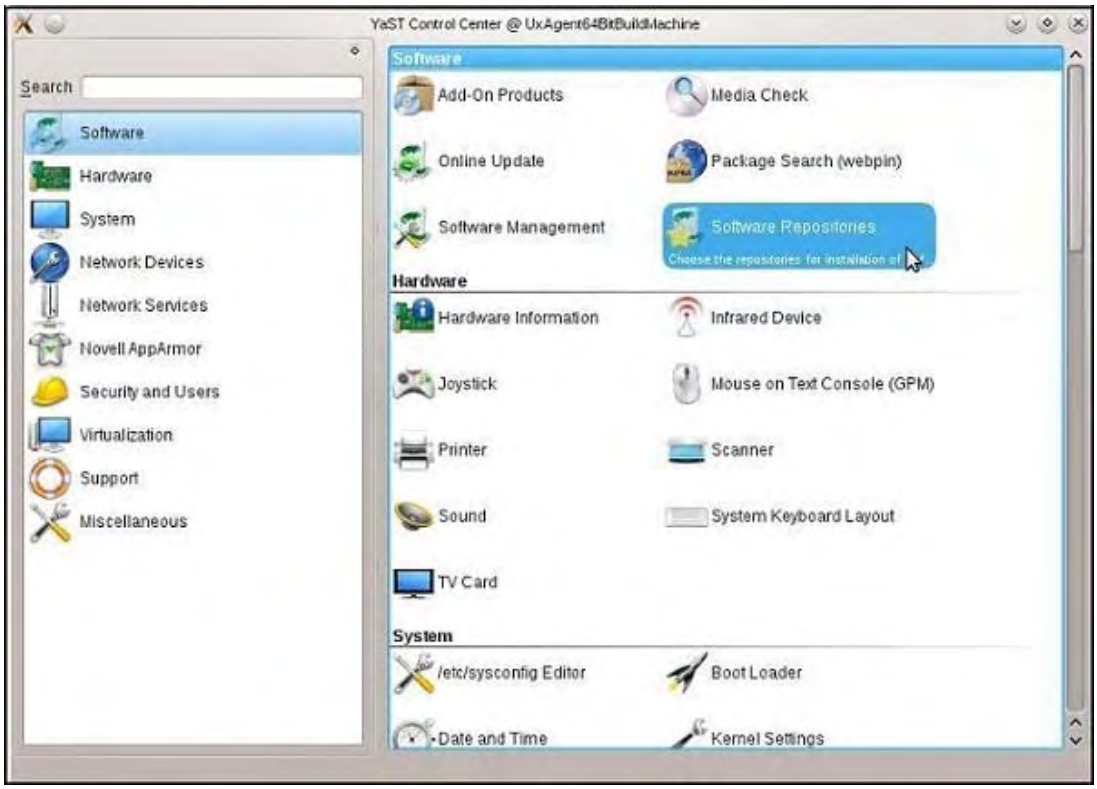


Fig. 14 - Remove repository.

5. (Optional) Select the appropriate UltraBac repository and click on "Delete." Confirm the deletion by clicking "Yes."

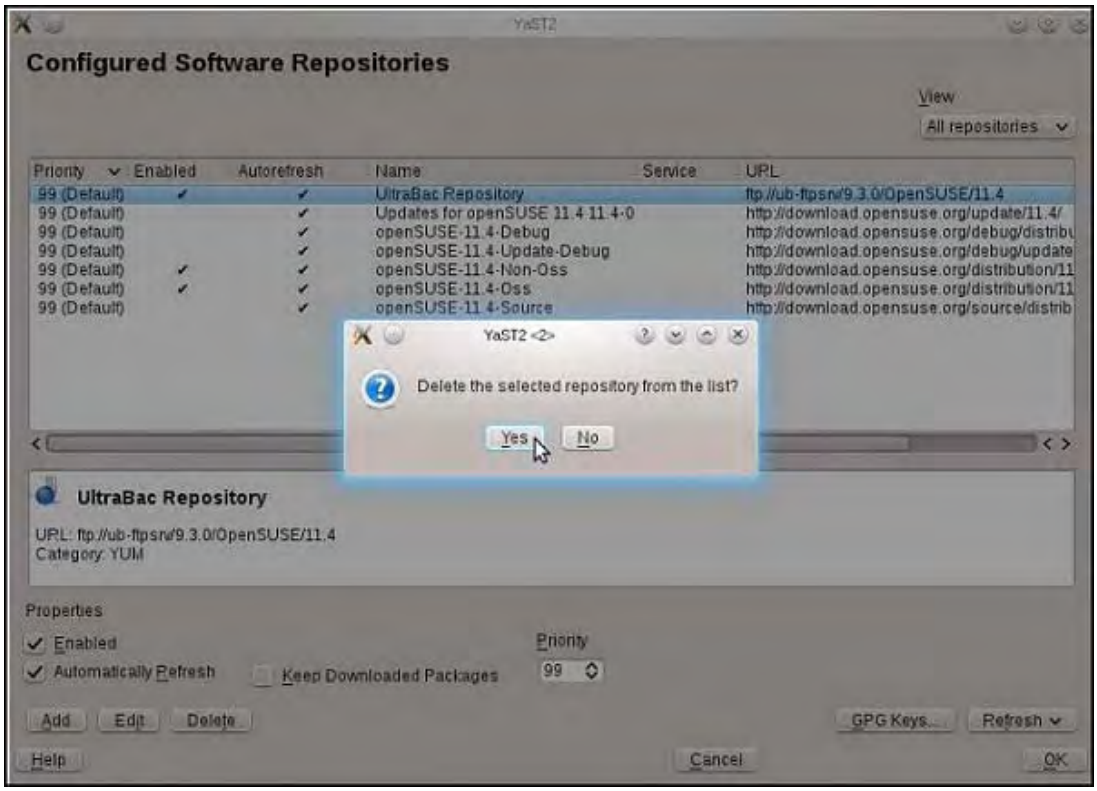


Fig. 15 - Delete repository confirmation.

Configuration

'UxDaemon' is the central process handling all requests from the remote Windows client managing the backups. This daemon starts automatically once the Ux Agent is installed. To check if the daemon process was spawned after installation use the "*rcUxAgent status*" command.



Fig. 16 - rcUxAgent status.

Similar commands like "*rcUxAgent start*" and "*rcUxAgent stop*" can be used to start and stop the daemon. Use the "*UxAgentConfigDevices*" command to invoke the UltraBac UxAgent Device Configuration Menu in order to add or remove device(s) to or from the Ux Agent. Under the Device Configuration Menu you will see the device name(s) to be added with the device's current status and a choice list from which you can select your desired option. Example: "/dev/sda2" in the screenshot below is a root device and is depicted by *.

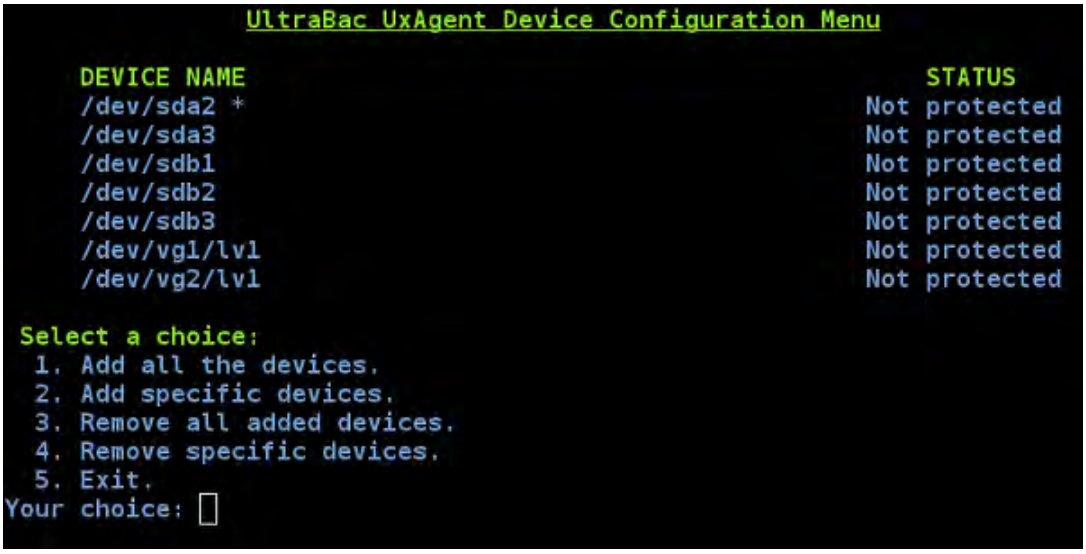


Fig. 17 - UxAgent Device Configuration Menu.

To Add All of the Devices to be Under UltraBac Ux Agent Protection

1. To add all the devices under protection, type "1". You will be asked for a confirmation: "Sure you want to add all devices [y/n]." Type "y" to proceed further as seen in figure 13.

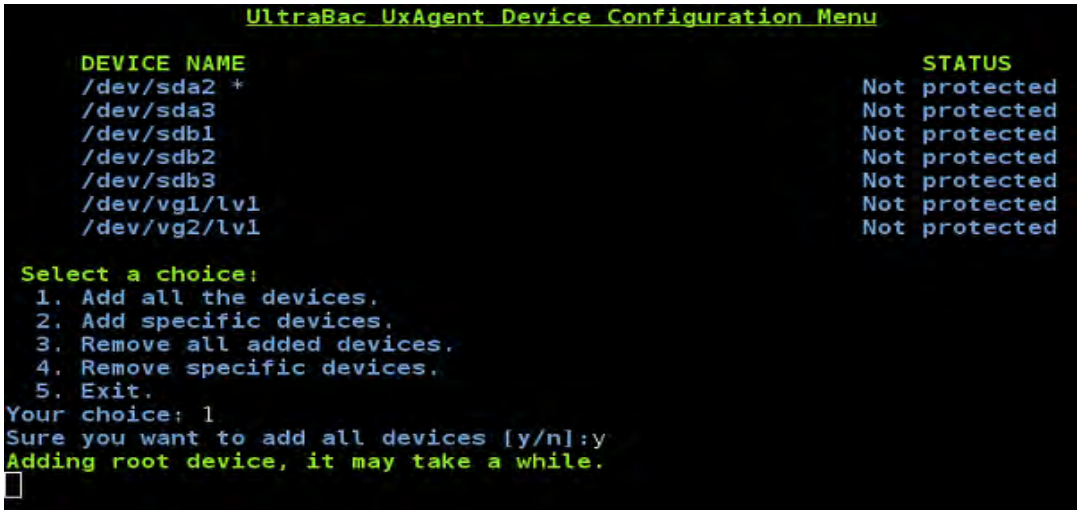


Fig. 18 - Add all the devices.

2. After adding all the devices, you will see the status of each device changed to "Marked for protection." For the configuration to be complete, restart the computer.

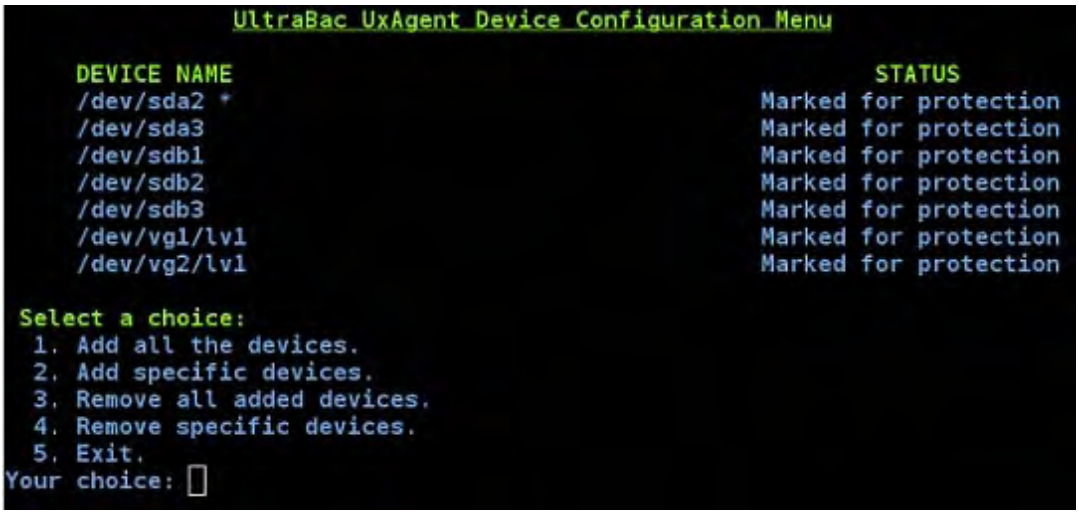


Fig. 19 - After adding devices.

3. After the computer is rebooted, the original (added) devices are replaced by mapped devices which the remote Windows client managing the backups can take a snapshot of. To check whether the device has been added under protection or not, look for the corresponding mapped device under /dev/mapper.



Fig. 20 - After reboot, mapped devices are created.

To Remove All of the Devices from Under UltraBac Ux Agent Protection

1. To remove all the added devices from protection, type <3>. You will be asked for a confirmation: "Sure you want to remove all devices [y/n]." Type <y> to proceed further as seen in Figure 21.

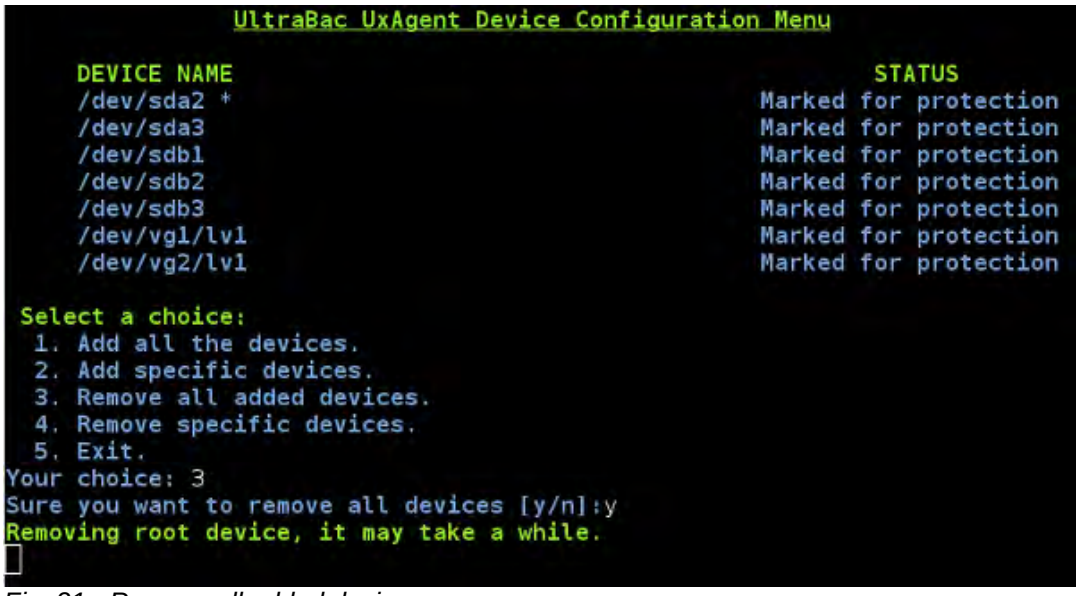


Fig. 21 - Remove all added devices.

2. After removing all the added devices, you will see the status of each device changed to "Not protected." For the configuration to be complete, restart the computer.

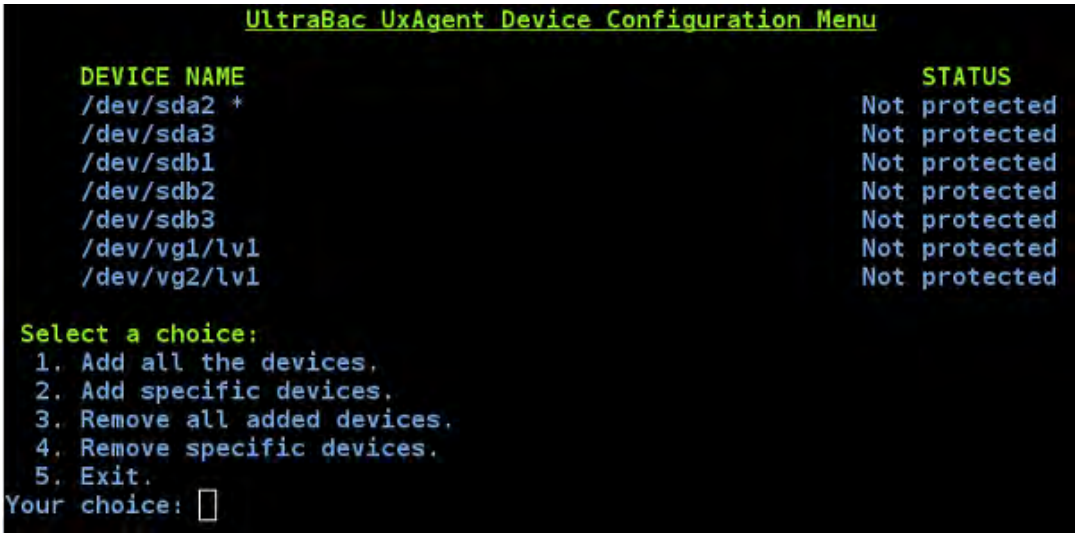


Fig. 22 - Devices removed.

3. After reboot, mapped devices are deleted and can no longer be seen under /dev/mapper.

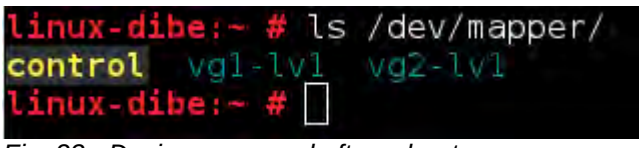


Fig. 23 - Devices removed after reboot.

To Add Specific Devices to be Under UltraBac Ux Agent Protection

1. To add specific devices under protection, type <2>. You will be prompted to enter the desired device names separated by a comma (,) as seen in Figure 24.

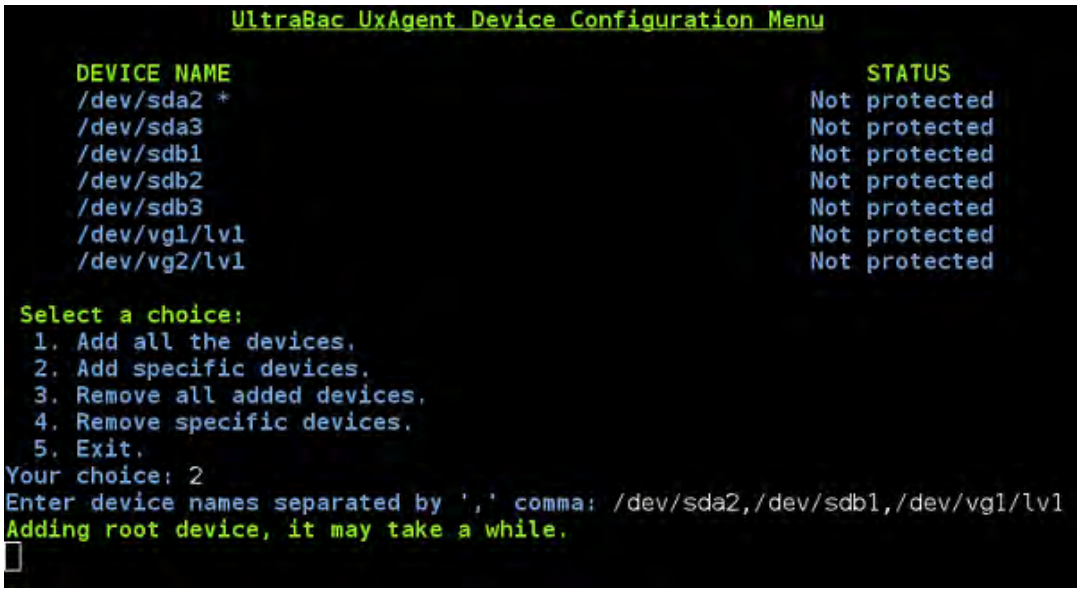


Fig. 24 - Add specific devices.

2. After adding specific devices, you will see the status of those particular devices changed to "Marked for protection." For the configuration to be complete, restart the computer.

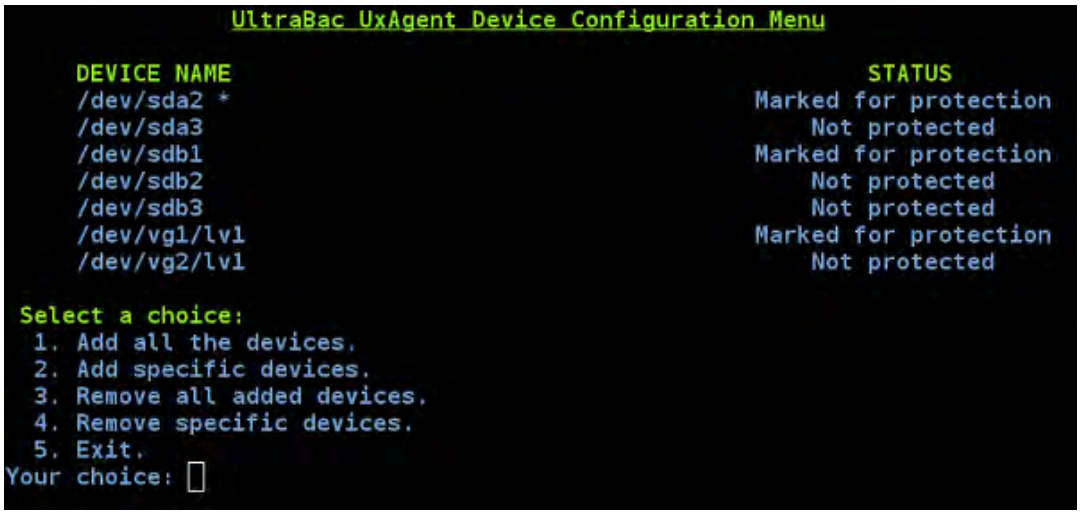


Fig. 25 - After adding specific devices.

3. After reboot, selected mapped devices are created and can be seen under /dev/mapper.

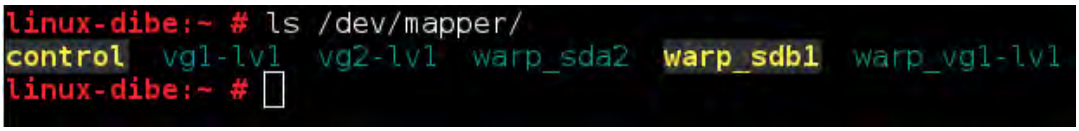


Fig. 26 - Selected mapped devices created after reboot.

To Remove Specific Devices from Under UltraBac Ux Agent Protection:

1. To remove specific devices from protection, type <4>. You will be prompted to enter specific device names that you want to remove from protection as seen in Figure 27.

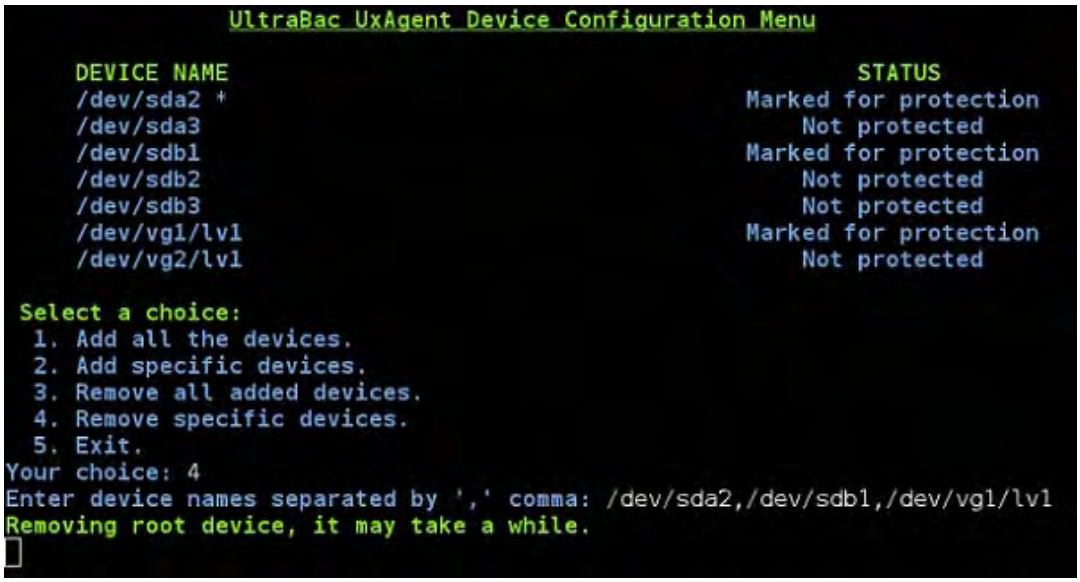


Fig. 27 - Remove specific devices.

2. After removing specific devices, you will see the status of removed devices changed back to "Not protected." For the configuration to be complete, restart the computer.

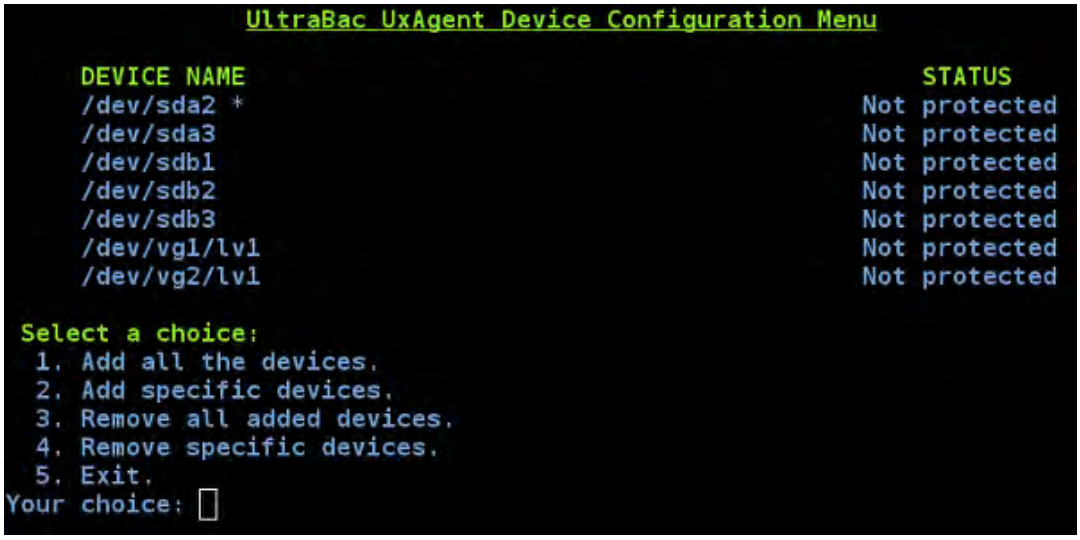


Fig. 28 - After removing specific devices.

3. After reboot, selected mapped devices are deleted and can no longer be seen under /dev/mapper.

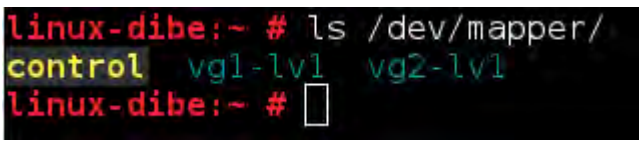


Fig. 29 - Selected devices removed after reboot.

To exit from the UltraBac UxAgent Device Configuration Menu, type <5>.

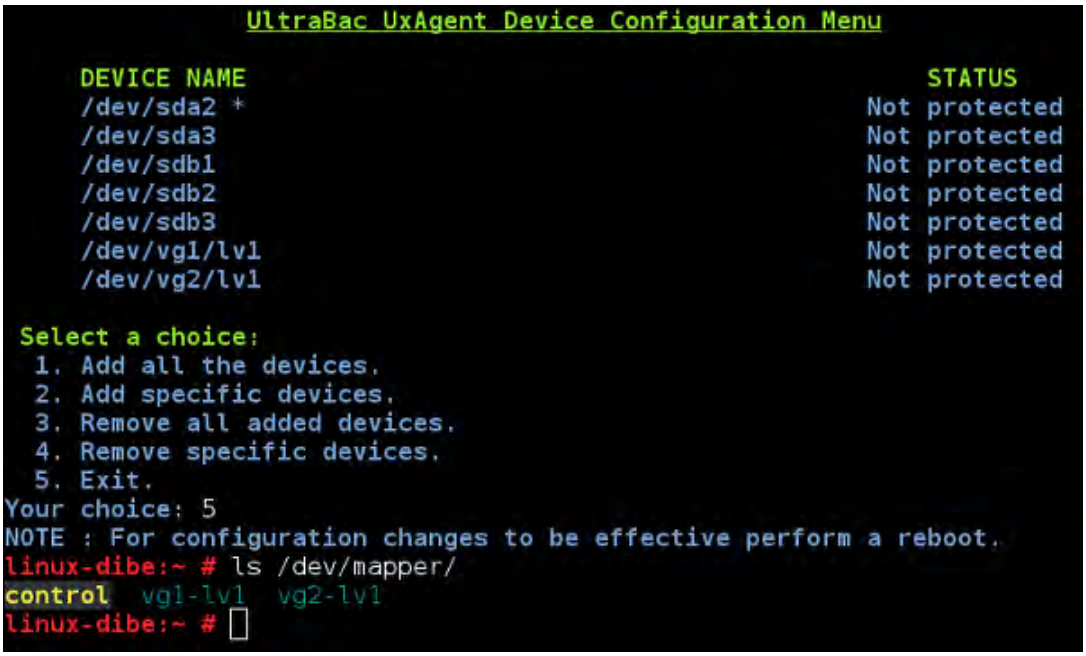


Fig. 30 - Exit.

Backups

Creating a Backup Set

To begin the backup process, follow these steps from the Windows client that will be managing the Ux Agent backups:

1. Open the "UltraBac Management Console."
2. Select the Backup tab and click "New."
3. Select the "Ux File by File." Click "Next" to continue.



Fig. 31 - Select "Ux File by File" Agent.

4. Type the host name or IP address of the UNIX/Linux computer into the "Server" field. Type the username and password into the "Username" and "Password" fields, and click "Next." Please note the username should be valid on a UNIX/Linux computer, should all be lowercase, and the account should have "root" privileges.



Fig. 32 - UNIX/Linux Agent Options.

5. Select the backup options for the Backup Set and click "Next."

- If the "Enable Locked File Backup" option is not selected, a normal backup is taken of the files from their original location.
- If the "Enable Locked File Backup" is selected, a snapshot device of the target partition is temporarily created before backup begins. A Locked File Backup allows UltraBac to back up files that are exclusively locked by an application or service. When the device on which the files are present has a valid UxAgent supported file system and is added under protection, a snapshot device (/dev/mapper/warp_snap_warp_<device_name>) is created. The backup is performed on the files of the snapshot device and the snapshot device is removed once the backup completes.

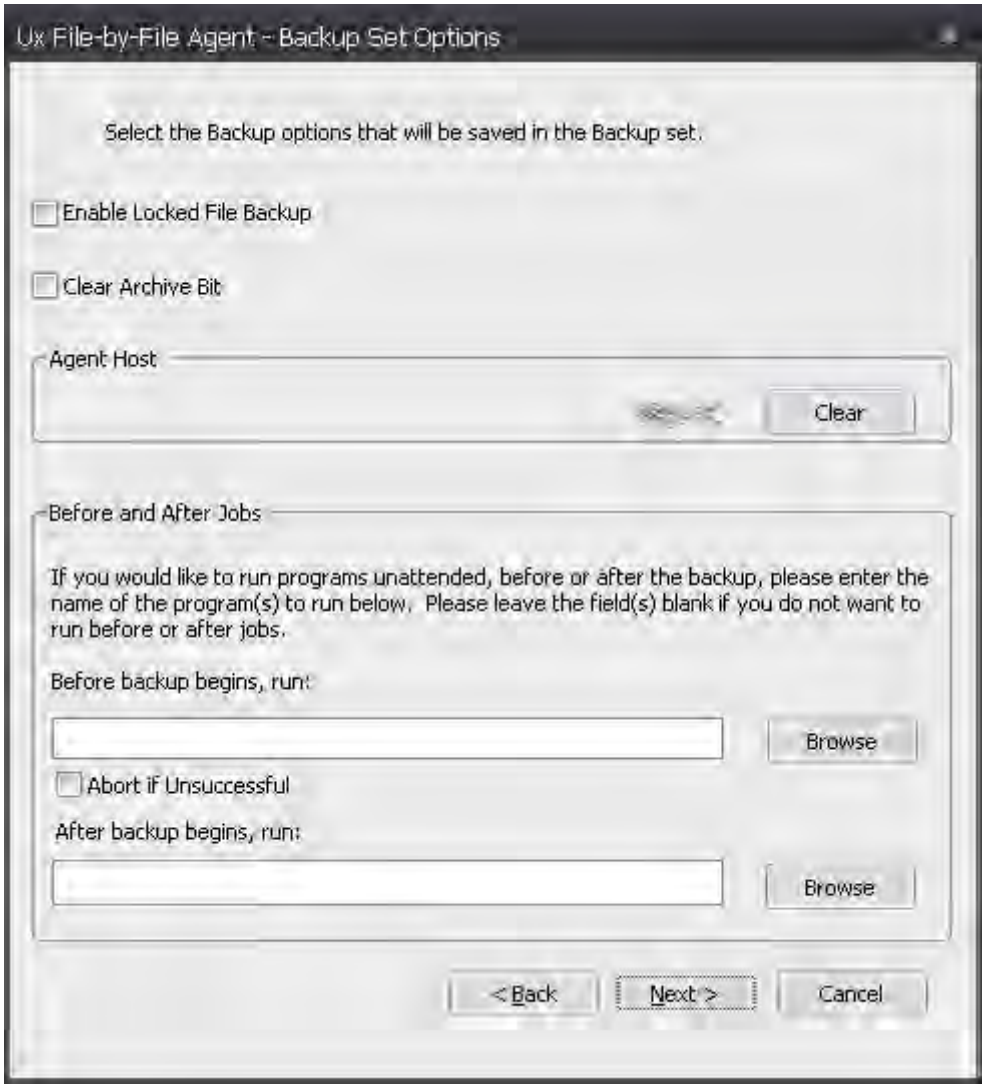


Fig. 33 - Backup Set Options.

6. Enter a set description and choose the file selection logic to be used for this set. Click "Next."



Fig. 34 - New Backup Set.

7. 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. 35 - Backup Set summary.

8. Create a backup set by selecting the files from the enumerated list of files.

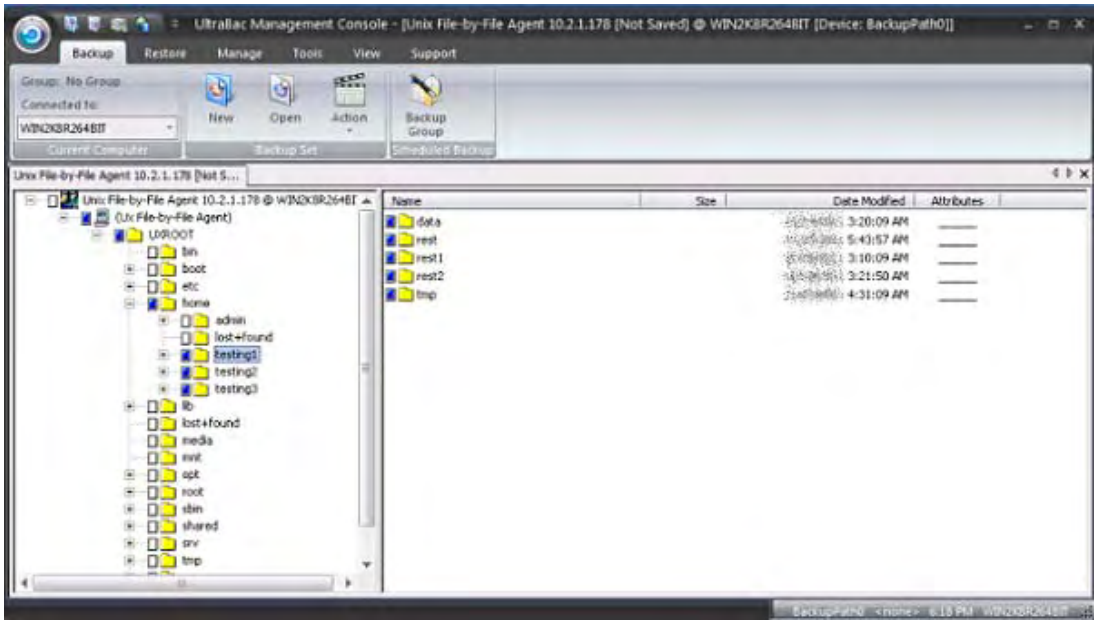


Fig. 36 - Select files for backup.

9. You can save the set by clicking "Action"/"Save."

Starting the Backup

> NOTE: Before beginning the backup, set the backup storage device. For additional information on setting the backup storage device, please visit the "**Storage Device Manager**" section of the User Manual:
>
> **UltraBac User Manual: Storage Device Manager**

1. Click "Actions," select "Run Backup Now."

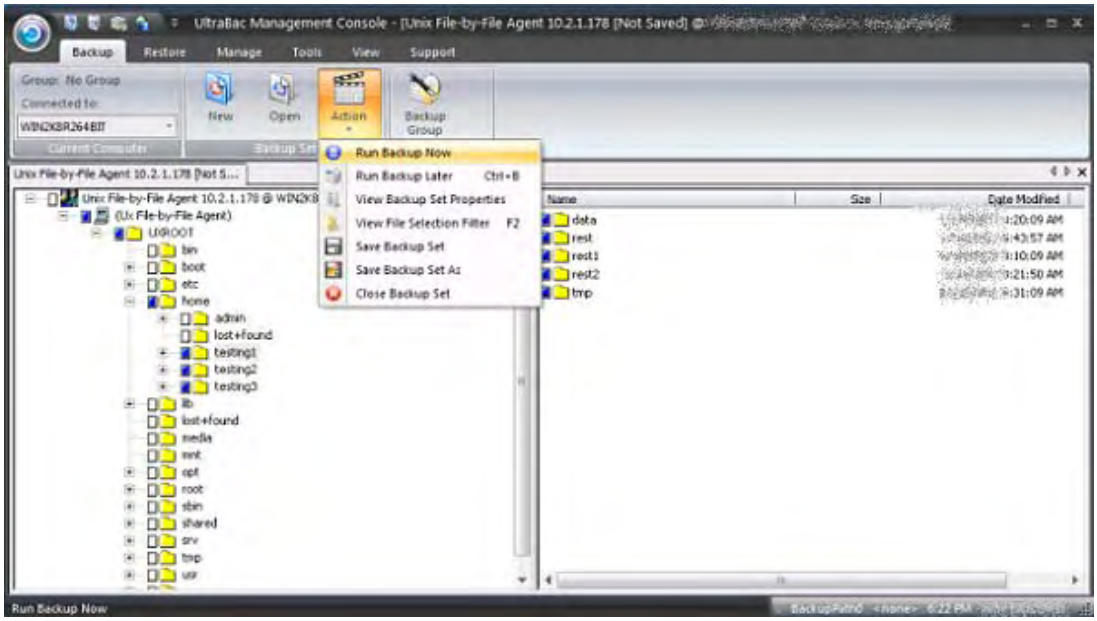


Fig. 37 - Run backup.

2. Select the relevant options to use during this backup. Click "Backup" to start the backup.

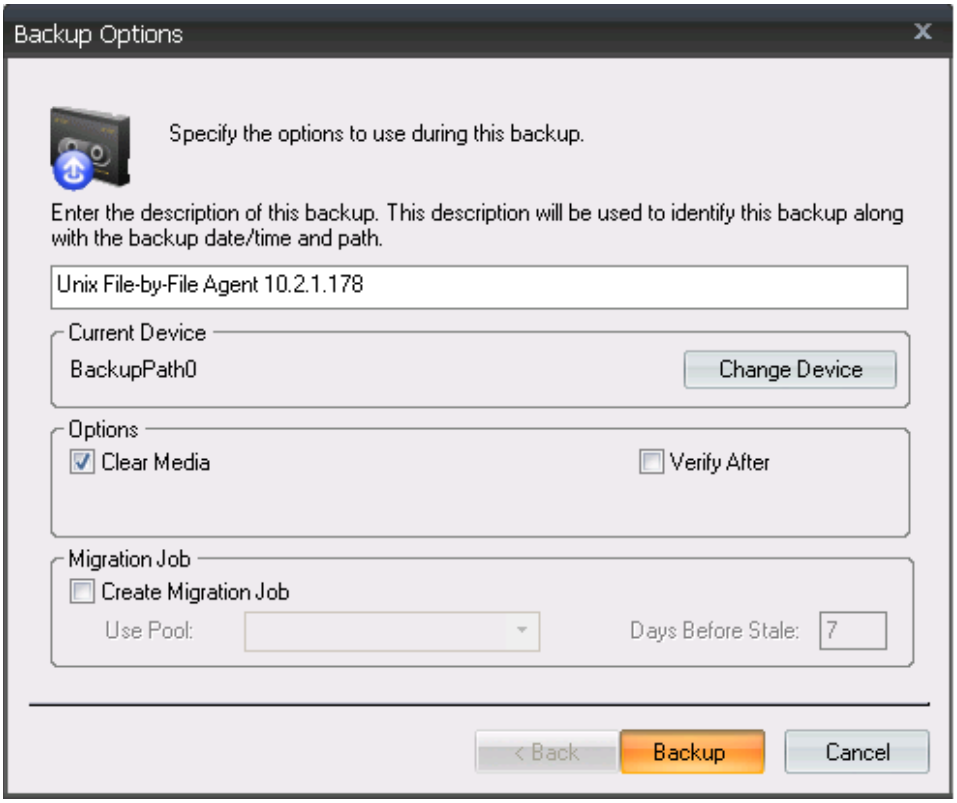


Fig. 38 - Start backup.

3. A progress window shows the status of the backup.

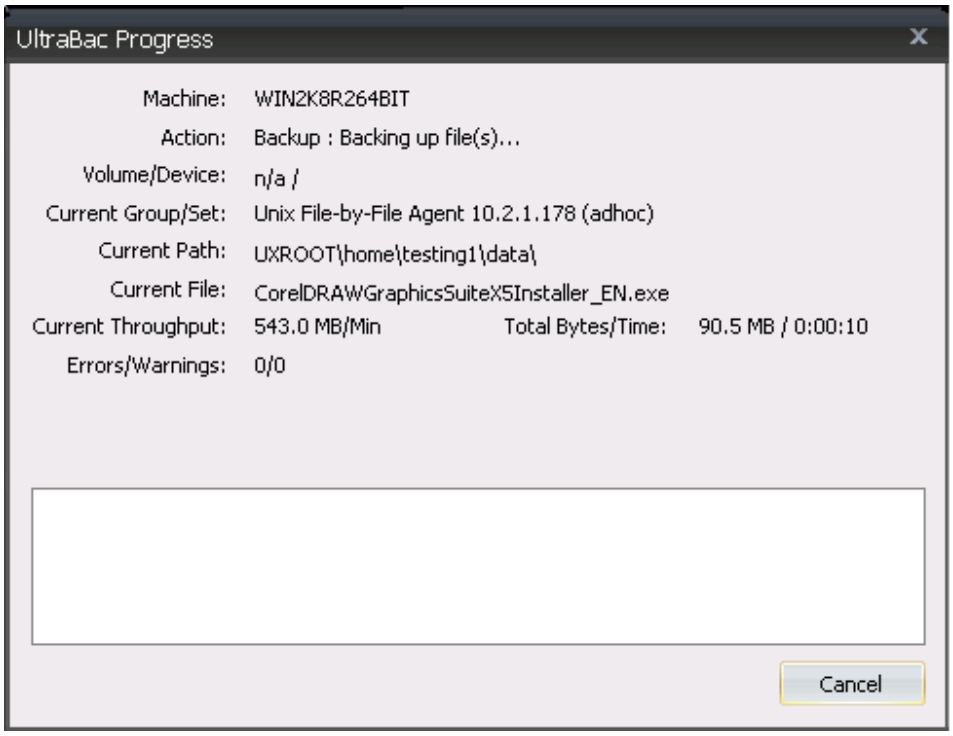


Fig. 39 - Backup progress.

4. After completion of the backup process you will see a message saying "Operation complete."

Restores

NOTE: Before beginning the restore, select the restore storage device where the backup to be restored is saved. For additional information on selecting the restore storage device, please visit the "**Restore Basics**" section of the User Manual:

UltraBac User Manual: Restore Basics

1. Launch the Restore Wizard by selecting the Restore tab, and selecting "Media."

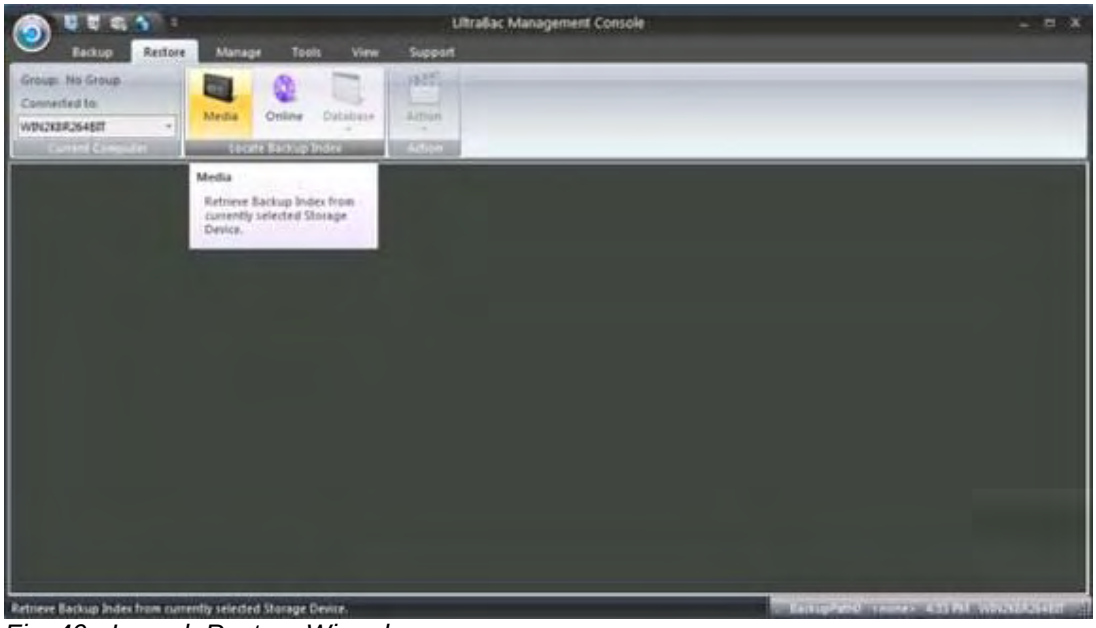


Fig. 40 - Launch Restore Wizard.

2. Select and load the backup index for restore.

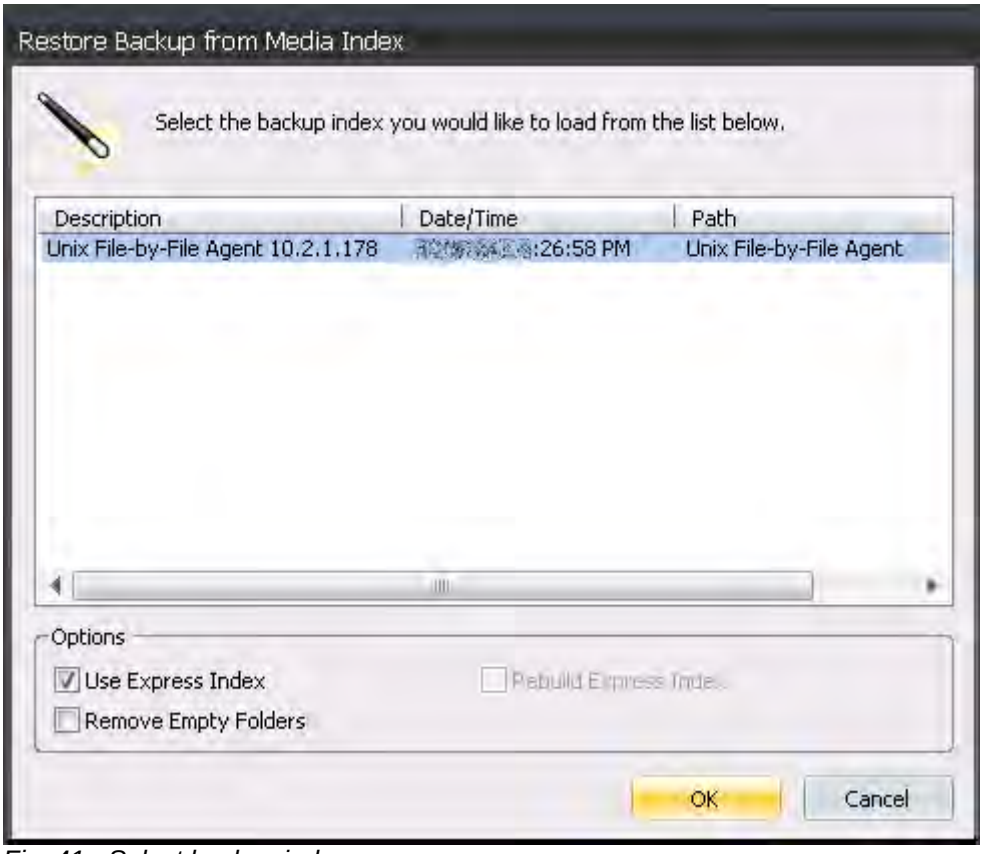


Fig. 41 - Select backup index.

3. Select the files or folders for restore.

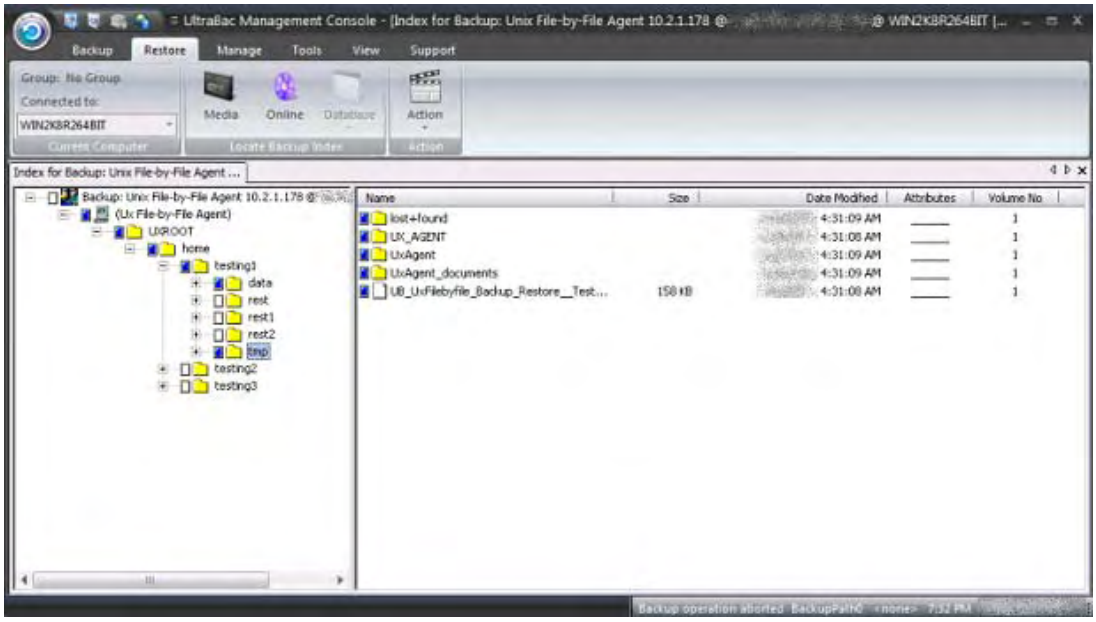


Fig. 42 - Select files or folders for restore.

4. Click "Action," then select "Restore this Backup."

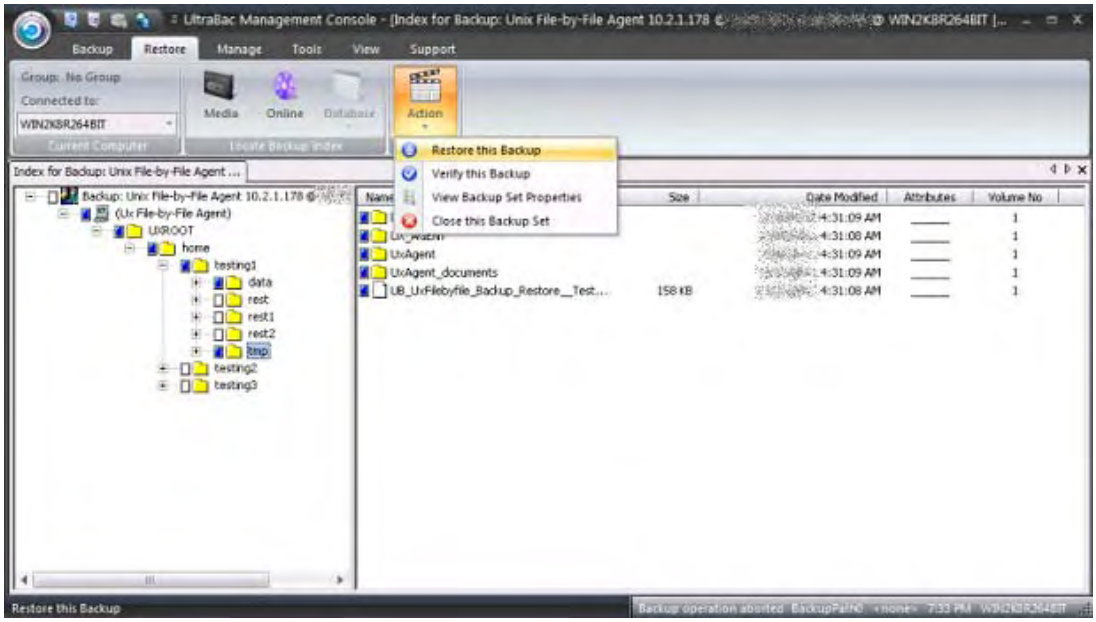


Fig. 43 - Restore action.

5. Set the restore options, and click "Next." You can restore to a different UNIX/Linux computer if you have UxAgent installed on the other computer.
   - Server – Restore destination system.
   - Username – Username for the restore destination system.
     - Root permissions is needed on the computer you are restoring to.
   - Password – Password for the restore destination system.
   - Overwrite Mode:
     - Always – Overwrite existing files with the files being restored.
     - Newer – Overwrite only 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.

- 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.

- 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.

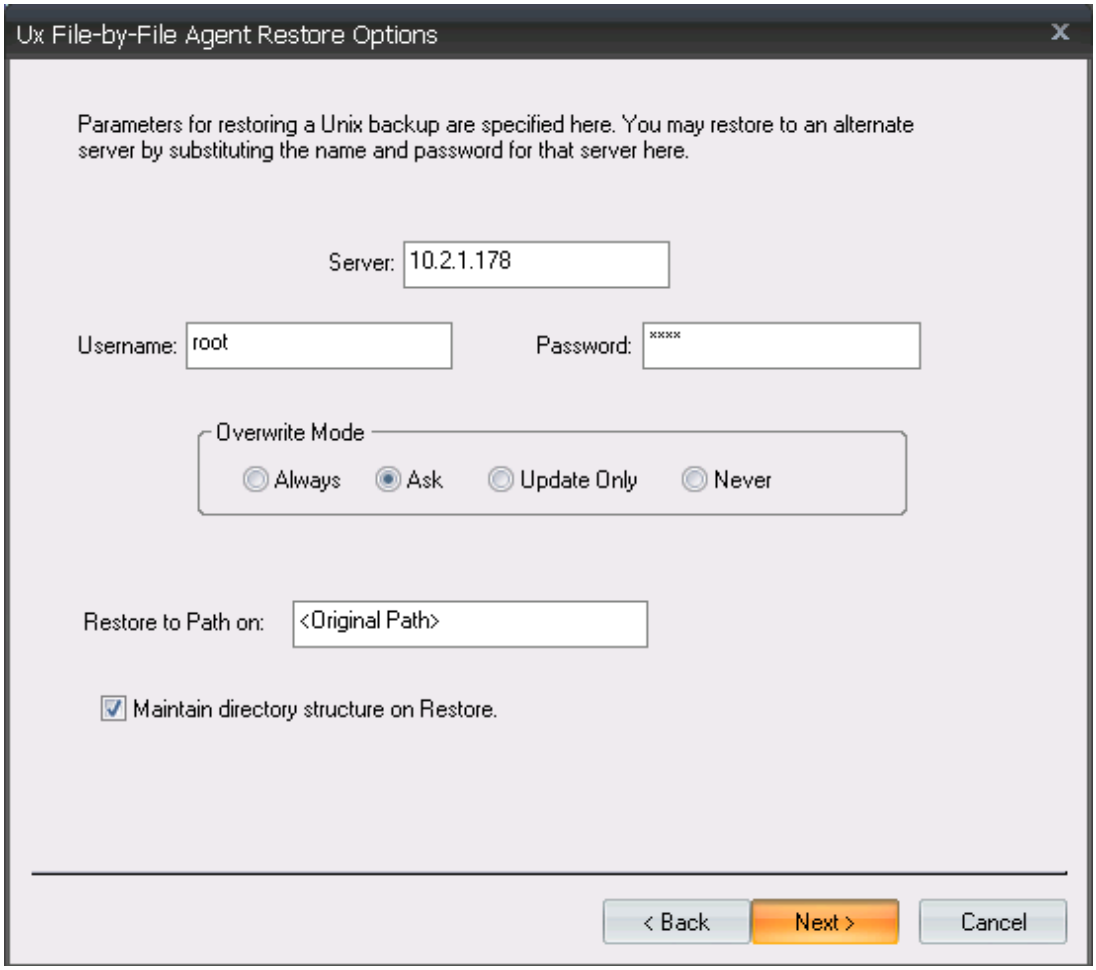


Fig. 44 - Restore options.

6. Click "Restore."

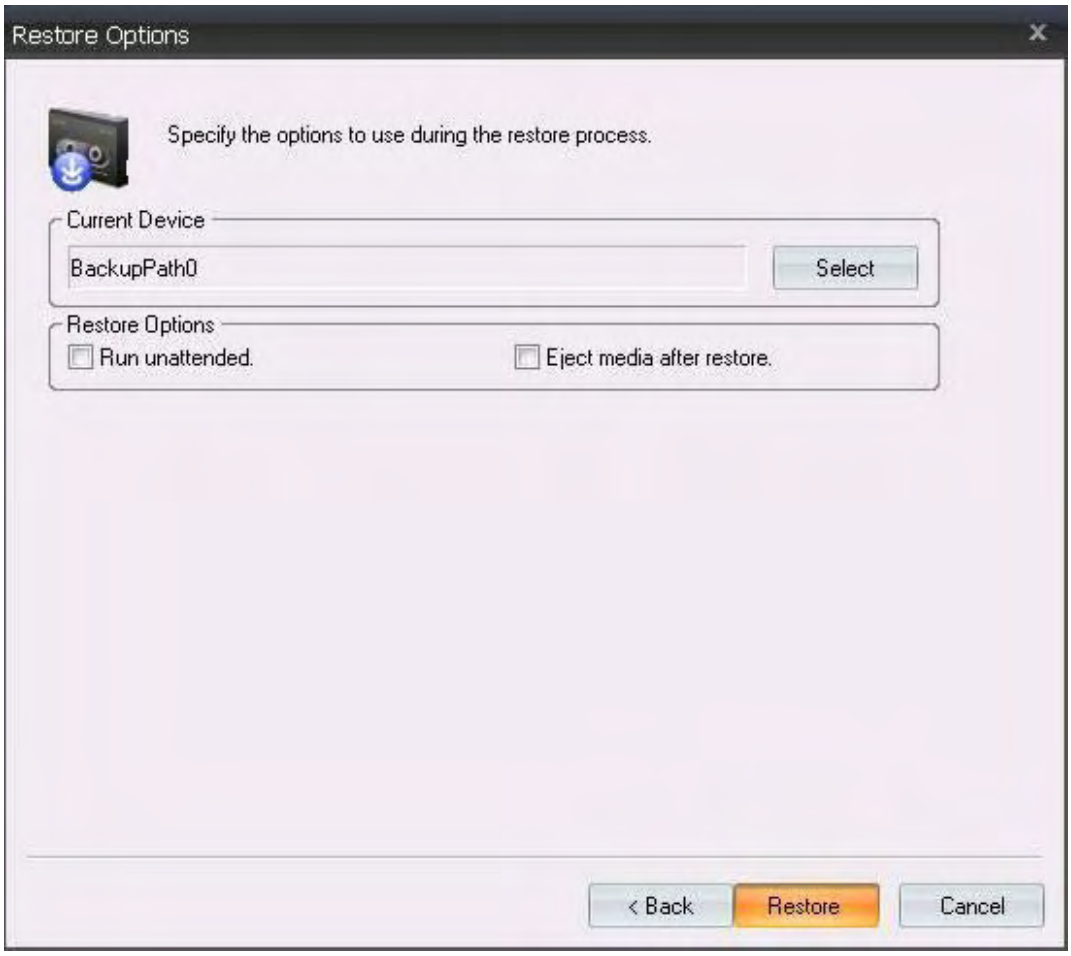


Fig. 45 - Restore.

7. An "UltraBac Progress" window will display showing the status of the restore process.

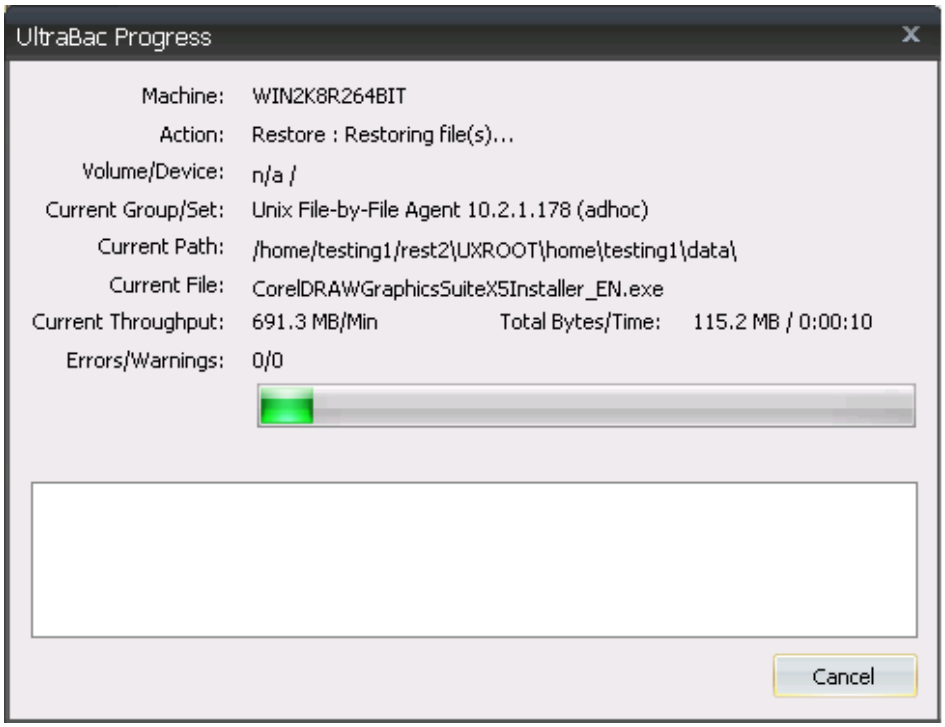


Fig. 46 - Restore progress.

NOTE: Backup/restore is not supported for the Ux Agent (File-by-File) when the computer running the UxAgent is running in Bare Metal Recovery (BMR) mode.

Ux Image Agent

The UltraBac Ux Image Agent provides UltraBac with the ability to back up images from the following platforms:

- Linux – OpenSUSE 11.0 to 11.4
- Linux – SUSE Linux Enterprise Server 11 SP1 to 11 SP3, 12.x
- Linux – Red Hat Enterprise Linux 6.0 to 6.7, 7.x
- Support for both 32 and 64-bit Operating Systems
- Support for ext2, ext3, and ext4 file systems

NOTE: There is a single Ux Agent RPM package for both the Ux Agent (File-by-File) and the Ux Image Agent. The ability to use the Ux Agent (File-by-File) and/or the Ux Image Agent is determined by the UltraBac license on the Windows computer running UltraBac managing the backups.

The installation, configuration, and uninstallation are identical between the File-by-File and Image Agents. The difference between the two are in the backup and restore operations.

Add UltraBac Repository
Install UltraBac RPMs
Upgrading
Uninstalling
Configuration
Backups
Restores

Installation

NOTE: The installation, configuration, and uninstallation is similar for OpenSUSE, SUSE Linux Enterprise Server, and Red Hat Enterprise Server. The examples below are for OpenSUSE.

NOTE: To add a Yum repository, type the following at a shell prompt as **`root`**:

yum-config-manager --add-repo ftp://rpmrepo.ultrabac.com/uxagent/RHEL/6.x/ultrabac.repo

yum-config-manager --enable ultrabac*

Adding UltraBac repository.

1. Open the Software Repositories manager by opening "YaST / Software / Software Repositories."

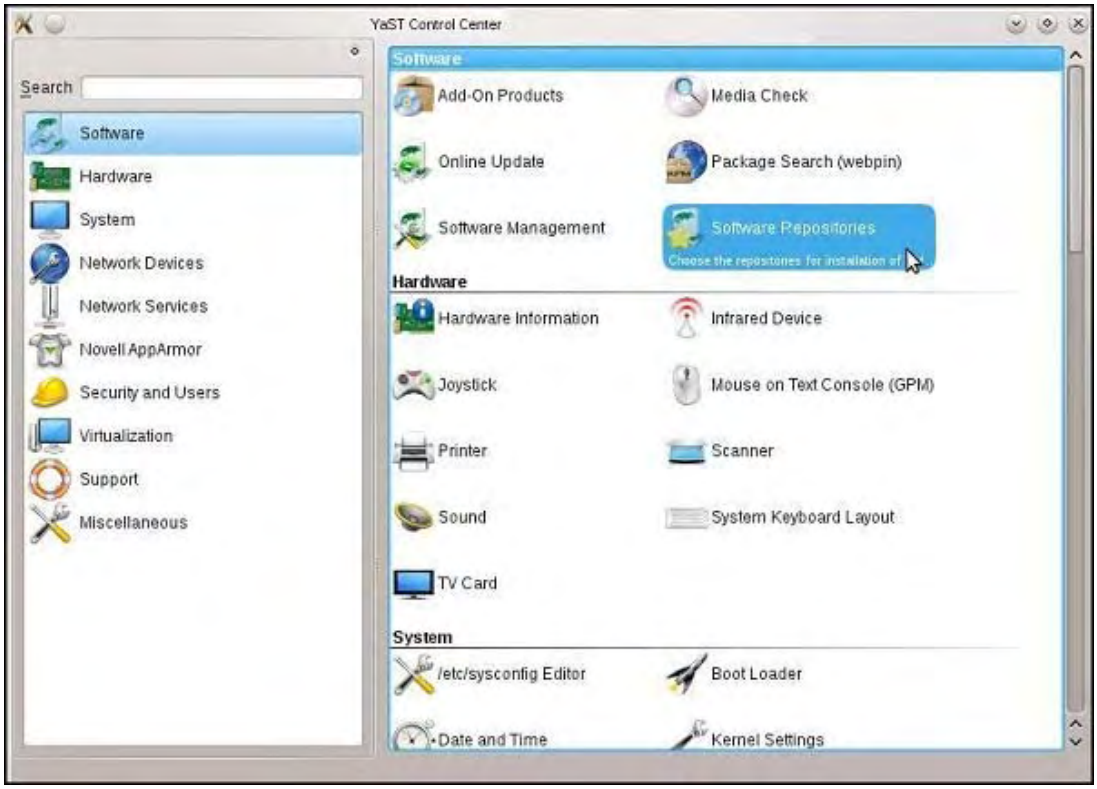


Fig. 1 - Software Repository.

2. Click "Add."

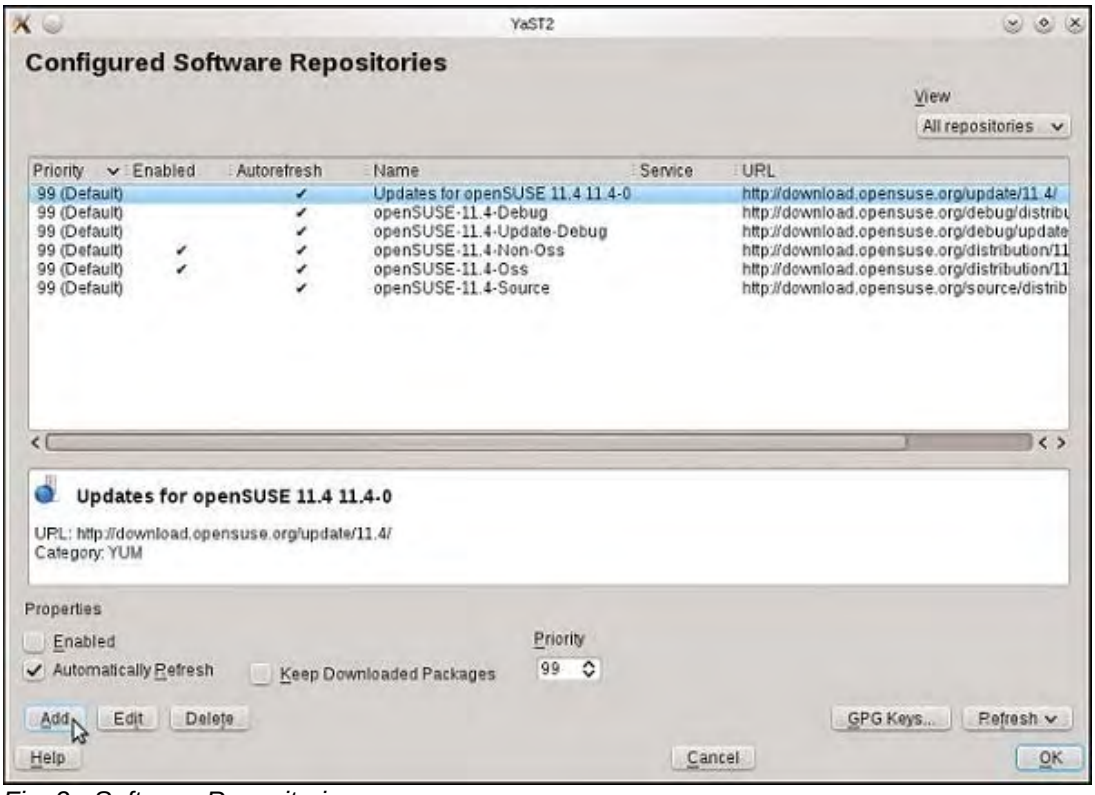


Fig. 2 - Software Repositories.

3. Select the Media Type (FTP) to be used for downloading the repository. Click "Next."

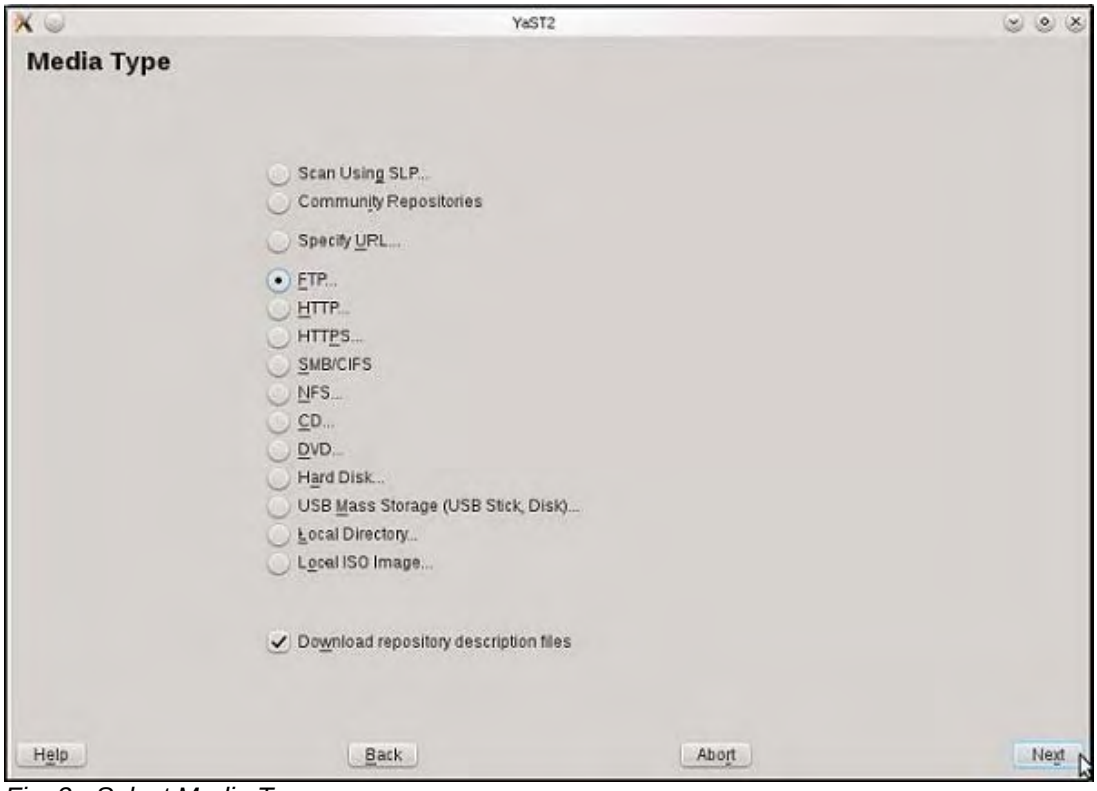


Fig. 3 - Select Media Type.

4. Enter the URL of the repository. Click "Next." The path to the RPM repository for UltraBac containing all the versions of RPMs can be found at "https://www.ultrabac.com/download-linux-free-trial." Select the version and URL path you will be using.

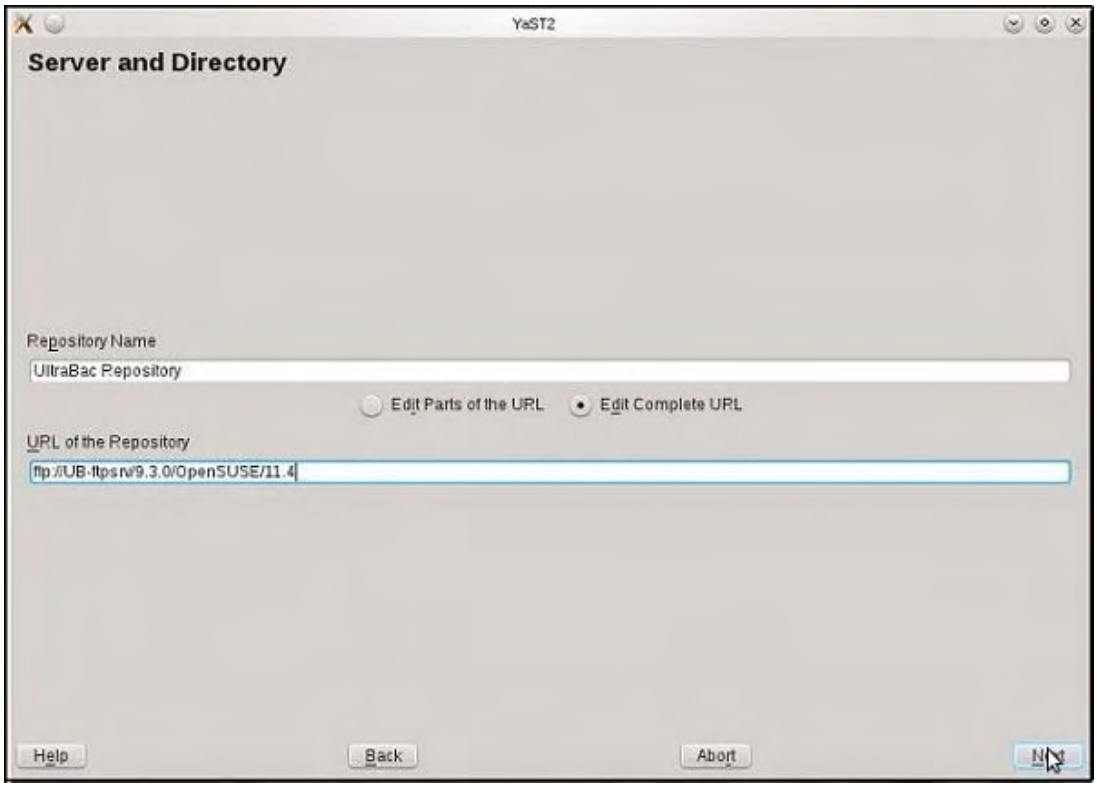


Fig. 4 - Enter repository URL.

5. Progress of the events can be seen in Figure 5.

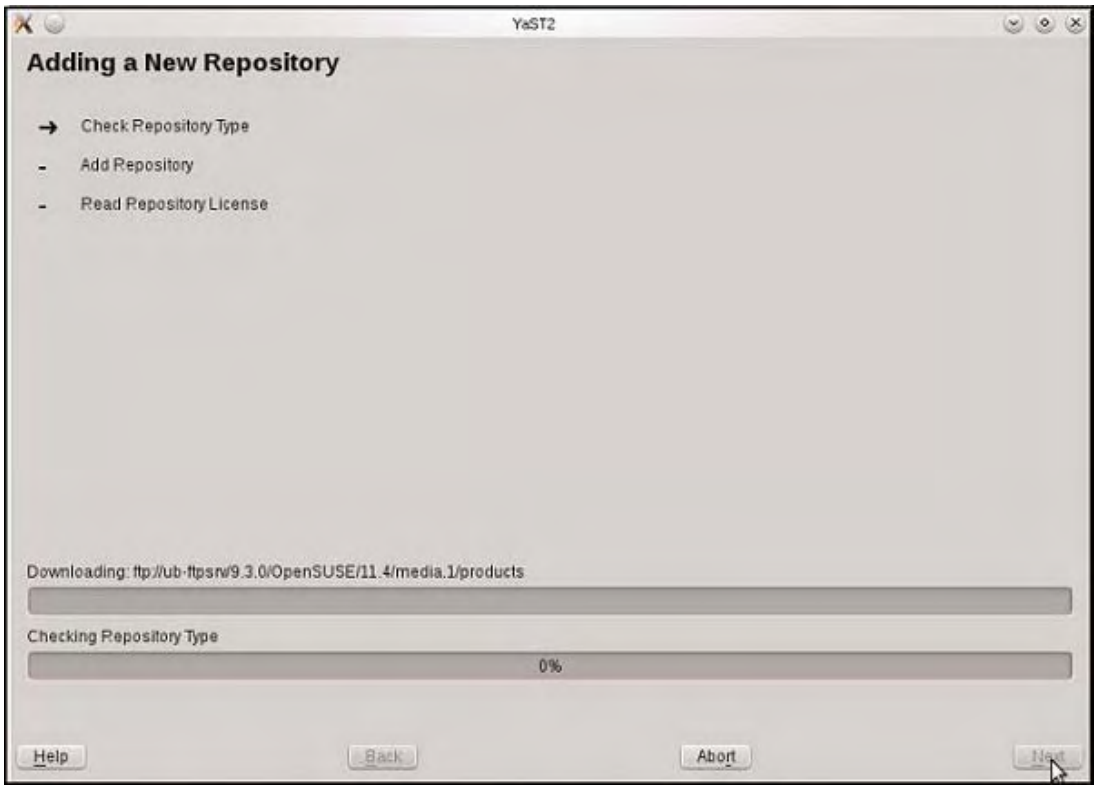


Fig. 5 - Add new repository.

The "UltraBac-UxAgent" RPM has a dependency on the "UltraBac-dm" RPM (driver) which is automatically resolved by the software installer. The Ux Agent can be installed through YaST using the following steps:

1. Start "Software Management" by opening "YaST / Software / Software Management."

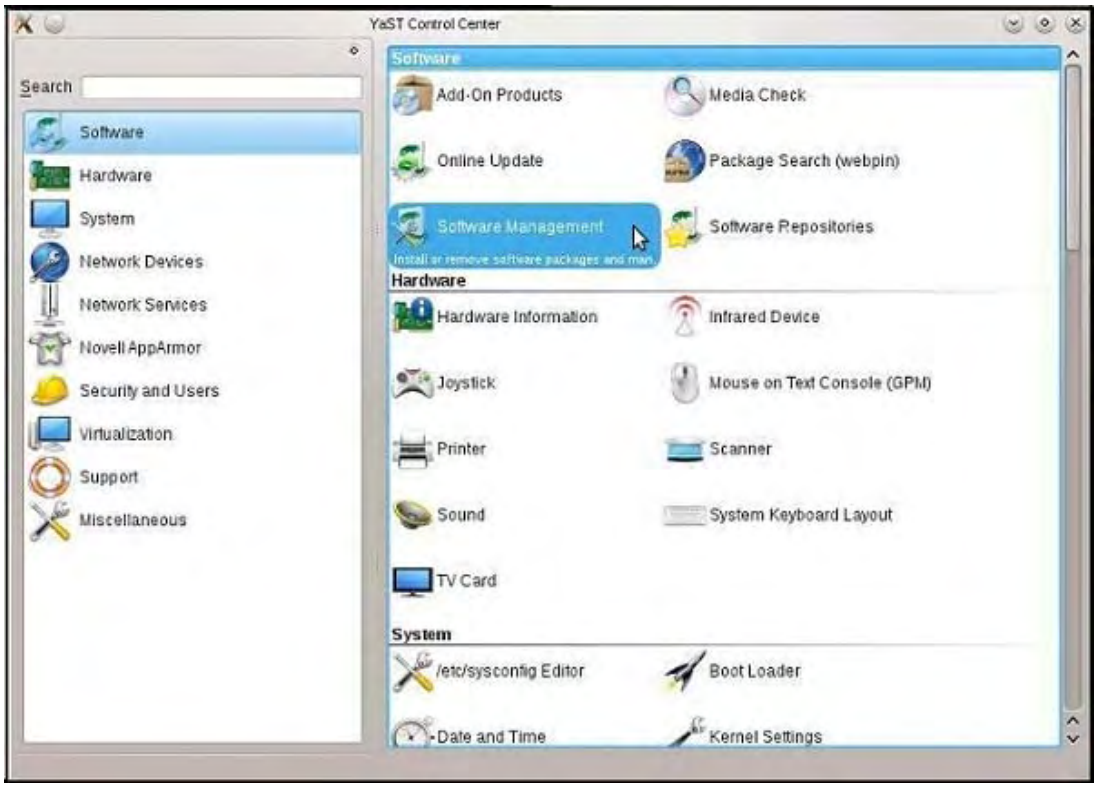


Fig. 6 - Software Management.

2. The progress of the Software Manager can be seen in Figure 7.

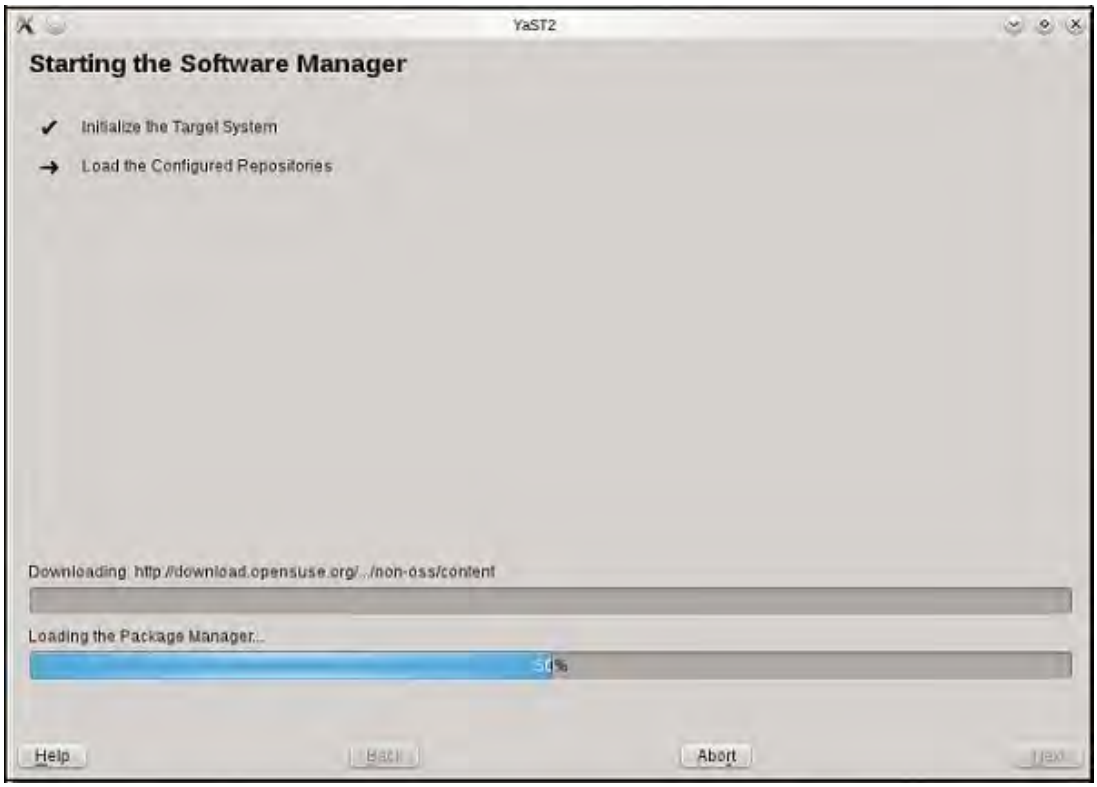


Fig. 7 - Software Manager progress.

3. Search for "ultrabac" and select "UltraBac-UxAgent." Click "Accept."

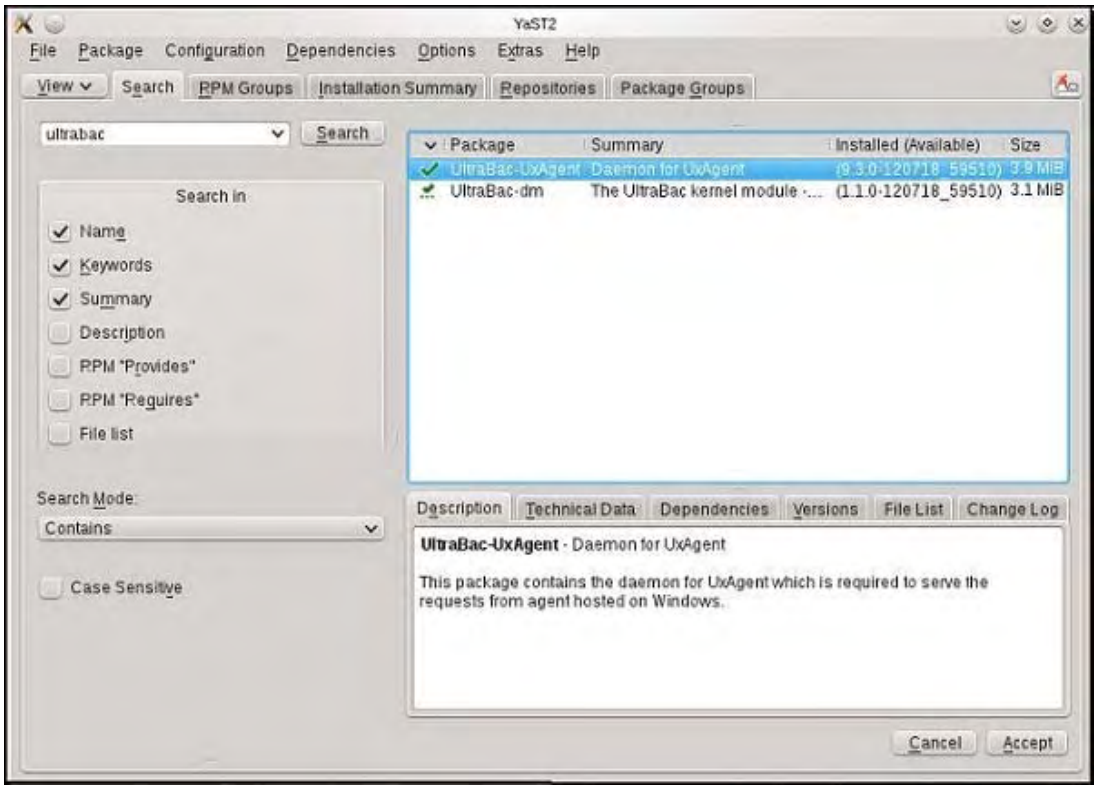


Fig. 8 - Search.

4. Dependencies will be installed automatically. Click "Continue" to perform installation.

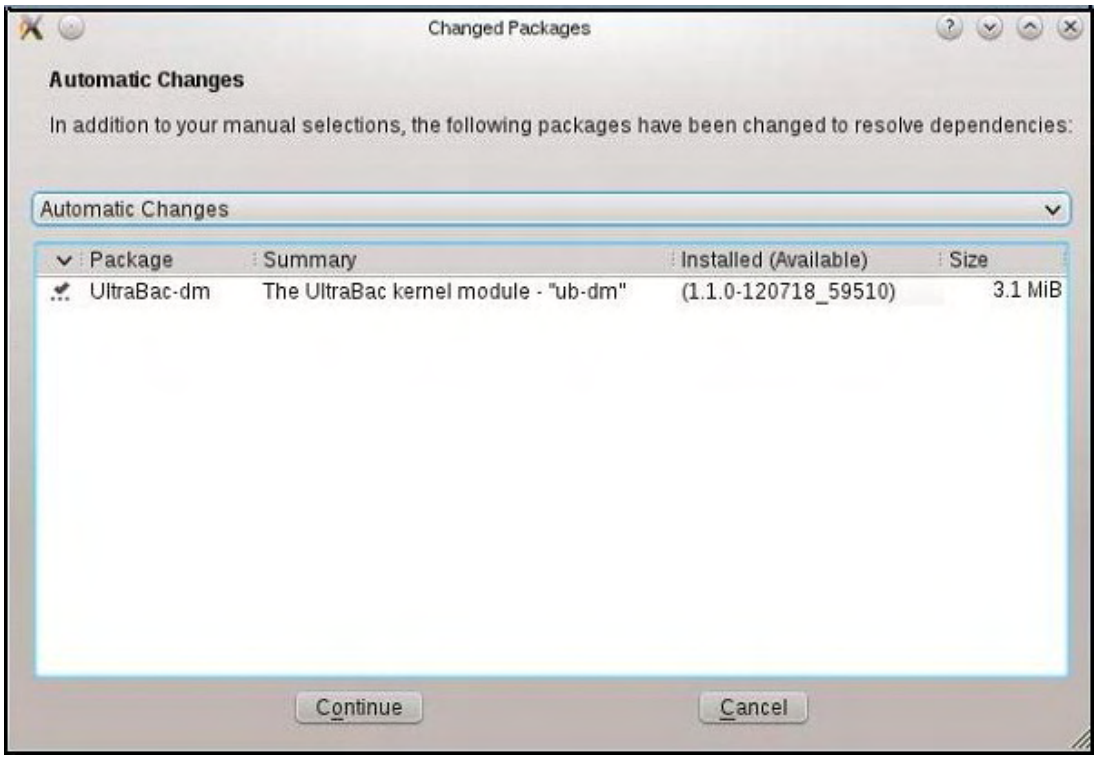


Fig. 9 - Dependencies.

5. The installation progress can be seen in Figure 10.

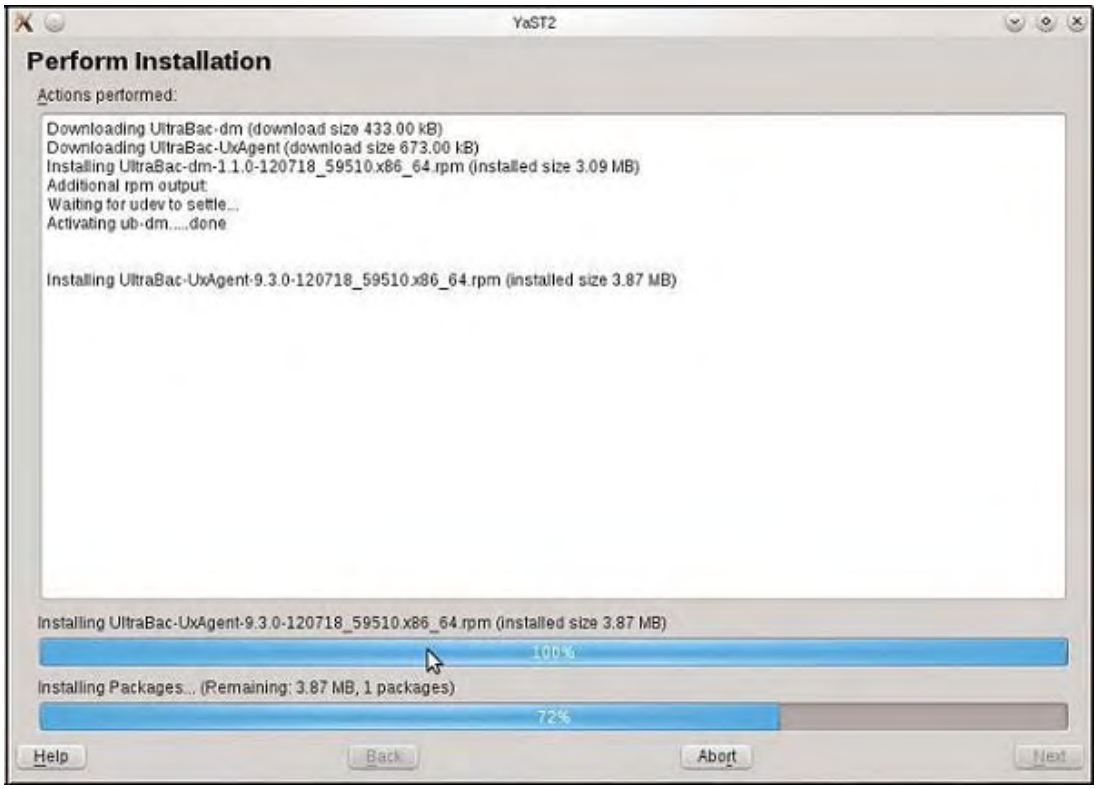


Fig. 10 - Installation progress.

Upgrading

Before upgrading the ultrabac RPM on your Linux computer, remove all devices added under UltraBac Ux Agent protection using the UltraBac UxAgent Device Configuration Menu utility. See the Configuration section on how to remove devices from protection.

Uninstallation

Before removing the UxAgent server RPM from your Linux computer, remove all devices added under UltraBac Ux Agent protection using the UltraBac UxAgent Device Configuration Menu utility. See the Configuration section on how to remove devices from protection.

Manual Uninstallation

1. To uninstall the "UltraBac-UxAgent" from your Linux computer, use the "rpm -e UltraBac-UxAgent" command.
2. To uninstall the "UltraBac-dm" (driver) from your Linux computer, use "rpm -e UltraBac-dm" command.

Uninstallation Using YaST

The "UltraBac-UxAgent" rpm has a dependency on "UltraBac-dm" RPM so "UltraBac-dm" RPM is not removed until "UltraBac-UxAgent" RPM is removed.

1. Start "Software Management" by opening "YaST / Software / Software Management."

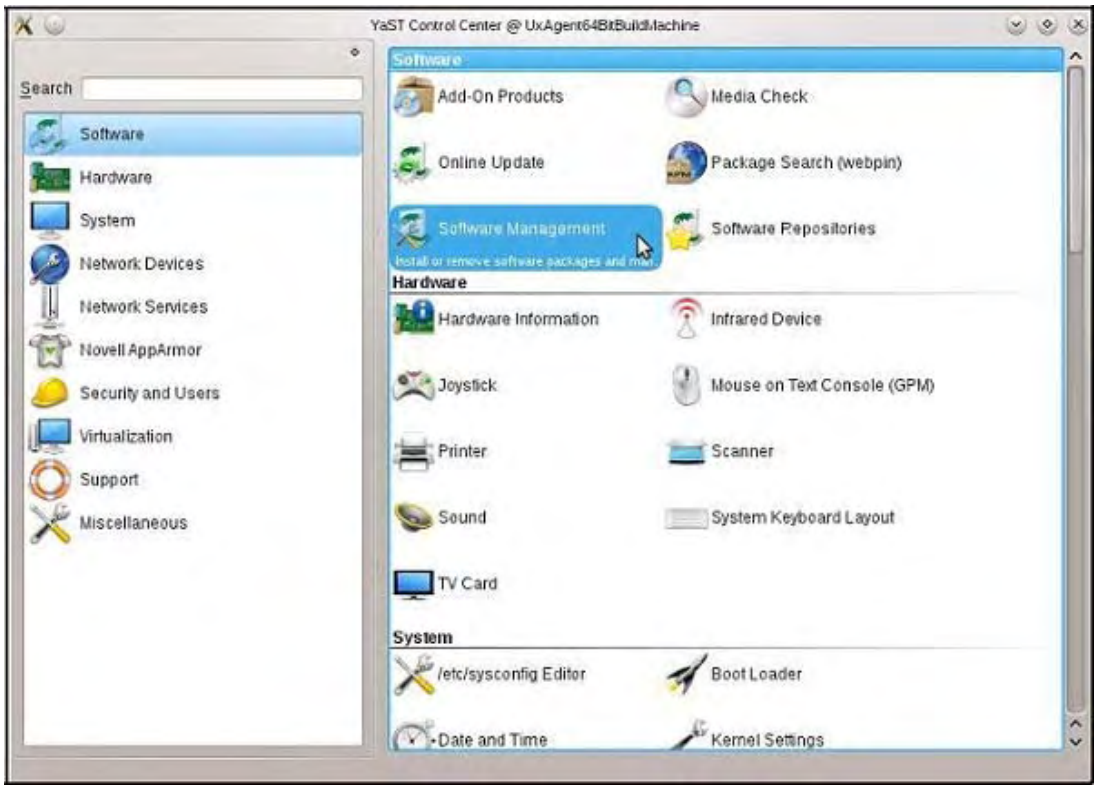


Fig. 11 - Software Management.

2. The progress of the Software Manager can be seen in Figure 27.

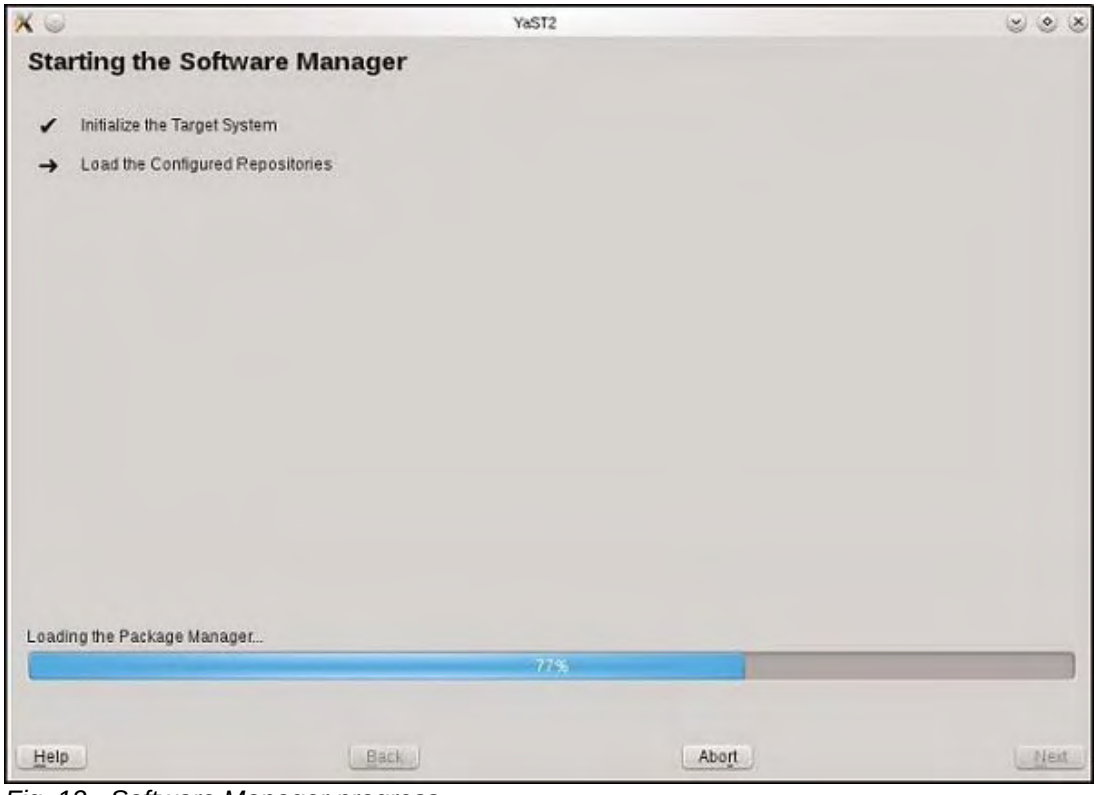


Fig. 12 - Software Manager progress.

3. Search for "ultrabac" and select "UltraBac-UxAgent" and "UltraBac-dm." Click "Accept."

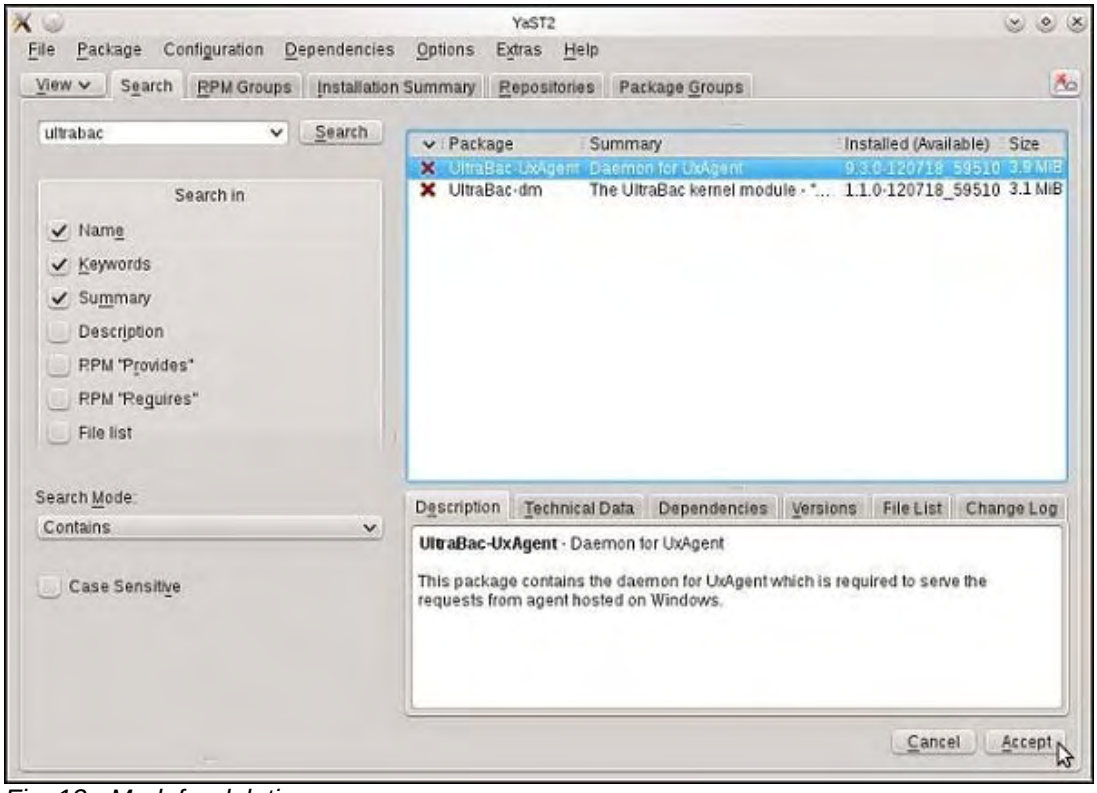


Fig. 13 - Mark for deletion.

4. (Optional) To remove the repository, select "Software Repositories."

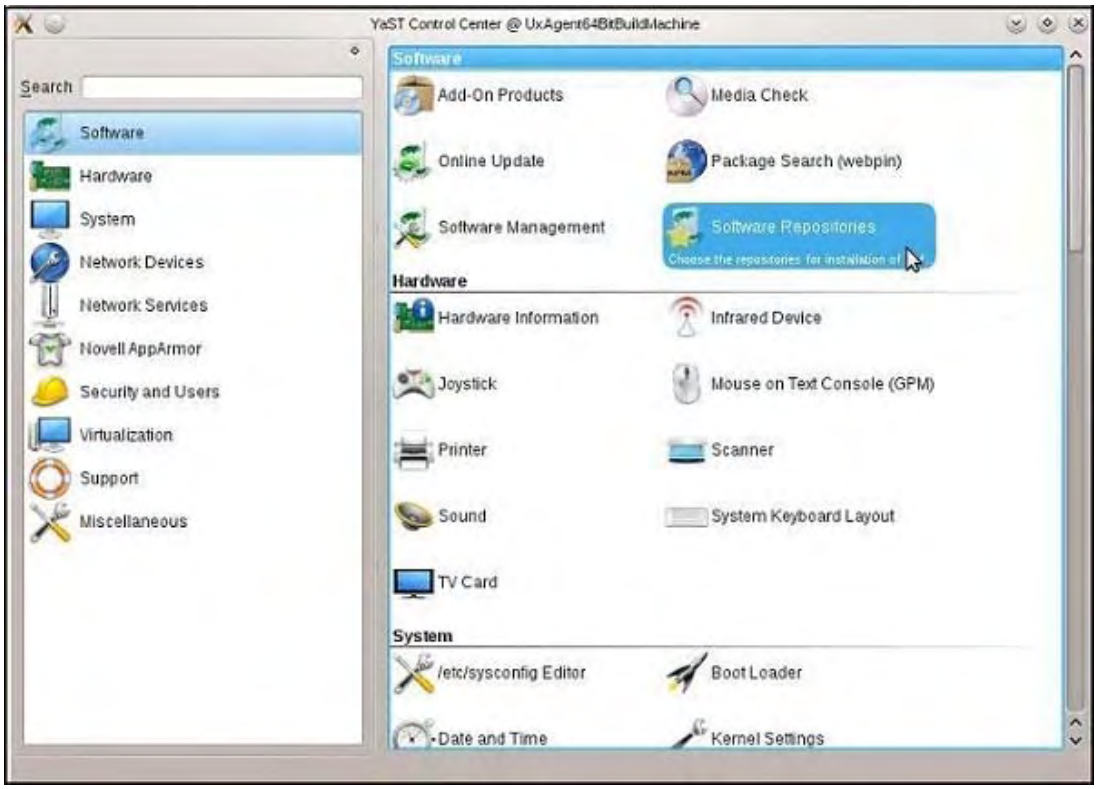


Fig. 14 - Remove repository.

5. (Optional) Select the appropriate UltraBac repository and click on "Delete." Confirm the deletion by clicking "Yes."

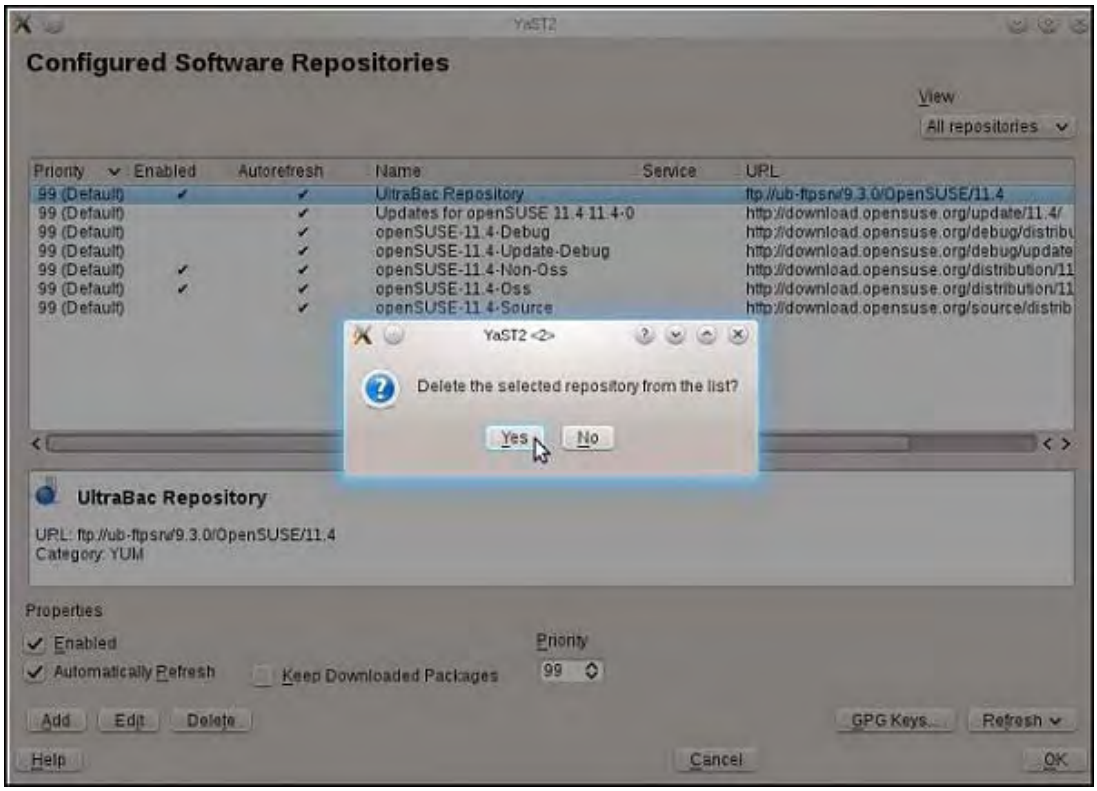


Fig. 15 - Delete repository confirmation.

Configuration

'UxDaemon' is the central process handling all requests from the remote Windows client managing the backups. This daemon starts automatically once the Ux Agent is installed. To check if the daemon process was spawned after installation use the "*rcUxAgent status*" command.



Fig. 16 - rcUxAgent status.

Similar commands like "*rcUxAgent start*" and "*rcUxAgent stop*" can be used to start and stop the daemon. Use the "*UxAgentConfigDevices*" command to invoke the UltraBac UxAgent Device Configuration Menu in order to add or remove device(s) to or from the Ux Agent. Under the Device Configuration Menu you will see the device name(s) to be added with the device's current status and a choice list from which you can select your desired option. Example: "/dev/sda2" in the screenshot below is a root device and is depicted by *.

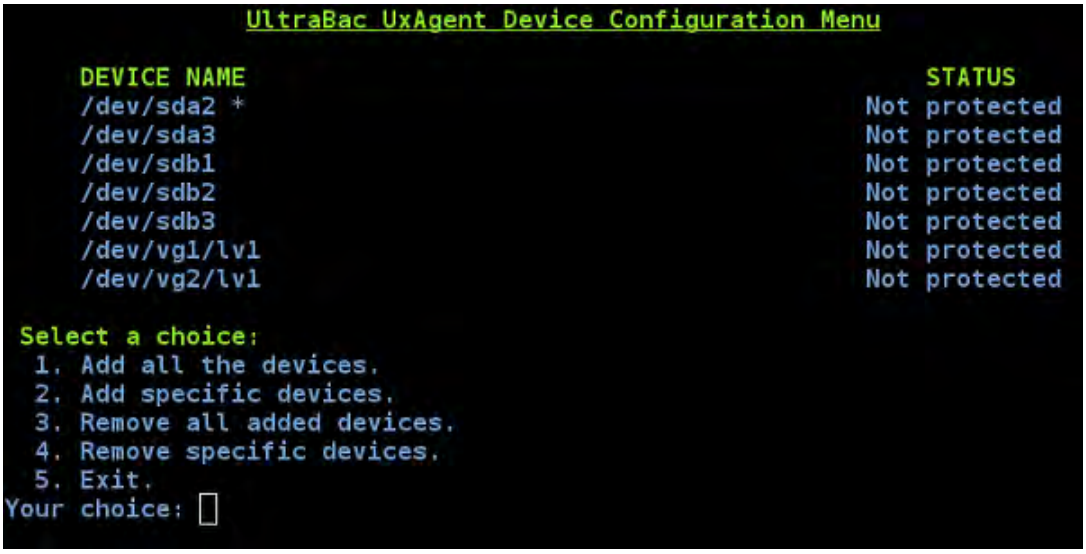


Fig. 17 - UxAgent Device Configuration Menu.

To Add All of the Devices to be Under UltraBac Ux Agent Protection

1. To add all the devices under protection, type <1>. You will be asked for a confirmation: "Sure you want to add all devices [y/n]." Type <y> to proceed further as seen in Figure 18.

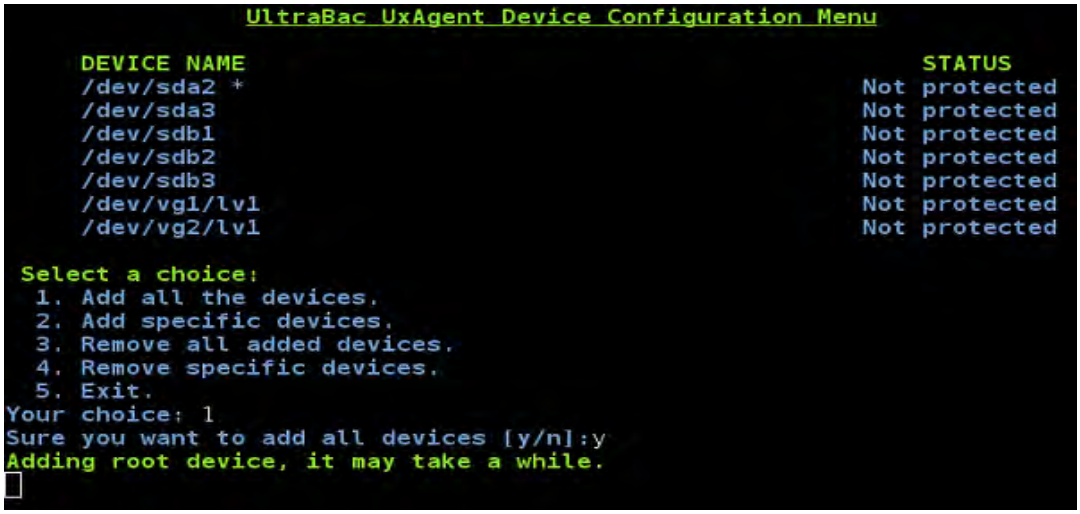


Fig. 18 - Add all the devices.

2. After adding all the devices, you will see the status of each device changed to "Marked for protection." For the configuration to be complete, restart the computer.

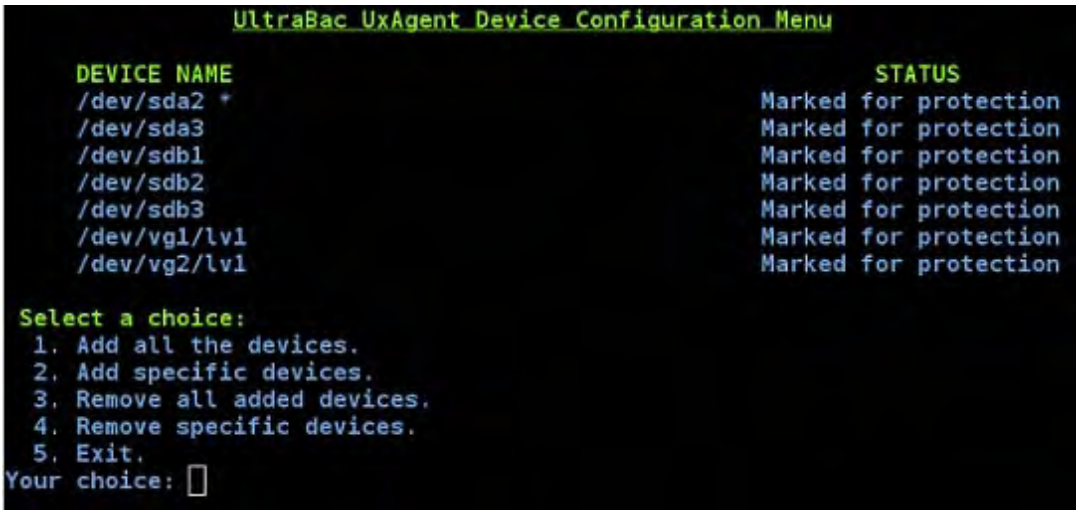


Fig. 19 - After adding devices.

3. After the computer is rebooted, the original (added) devices are replaced by mapped devices which the remote Windows client managing the backups can take a snapshot of. To check whether the device has been added under protection or not, look for the corresponding mapped device under /dev/mapper.



Fig. 20 - After reboot, mapped devices are created.

To Remove All of the Devices from Under UltraBac Ux Agent Protection

1. To remove all the added devices from protection, type <3>. You will be asked for a confirmation: "Sure you want to remove all devices [y/n]." Type <y> to proceed further as seen in Figure 21.

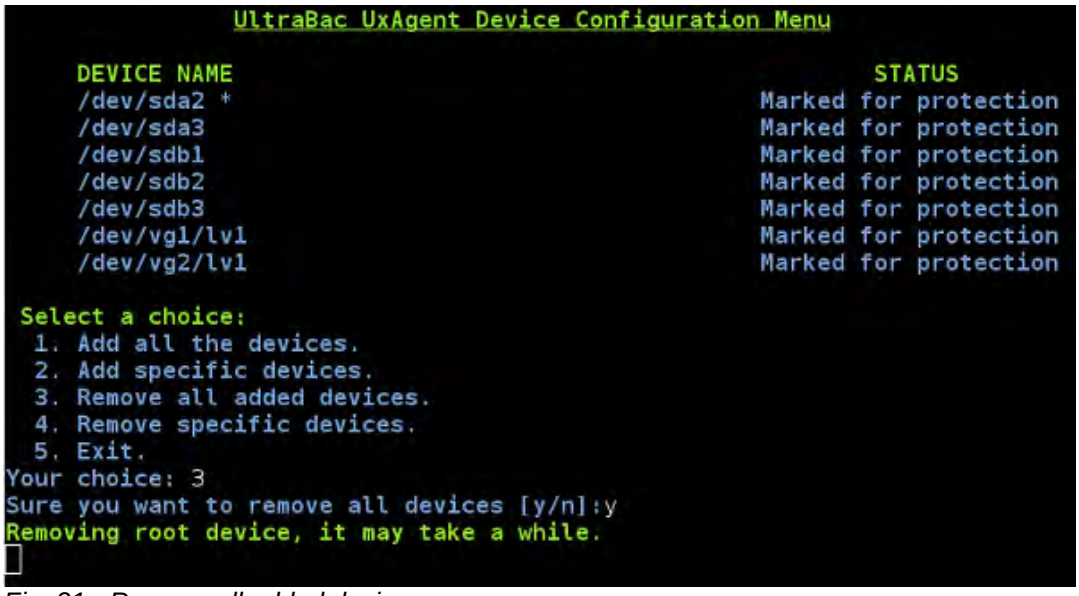


Fig. 21 - Remove all added devices.

2. After removing all the added devices, you will see the status of each device changed to "Not protected." For the configuration to be complete, restart the computer.

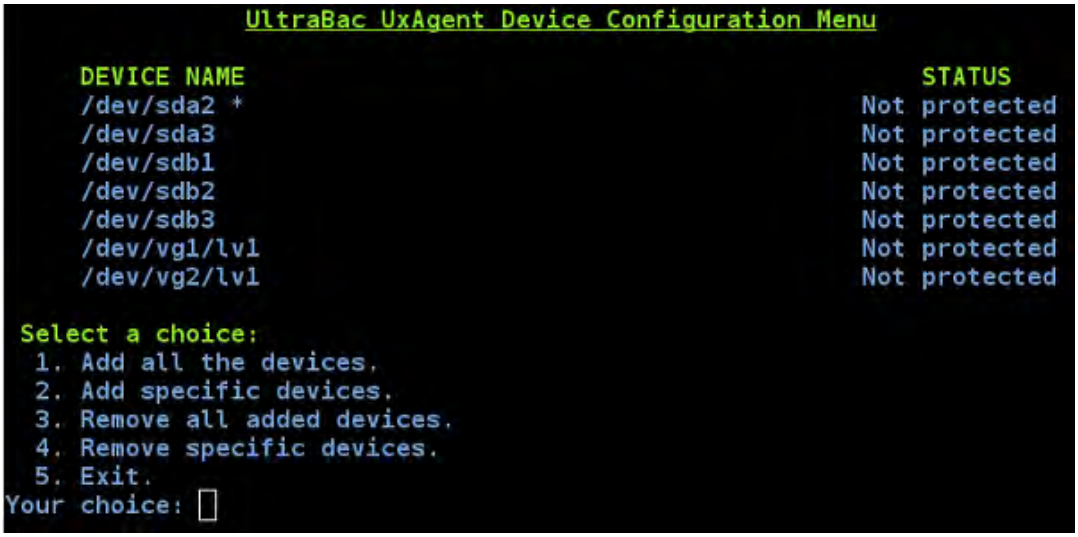


Fig. 22 - Devices removed.

3. After reboot, mapped devices are deleted and can no longer be seen under /dev/mapper.

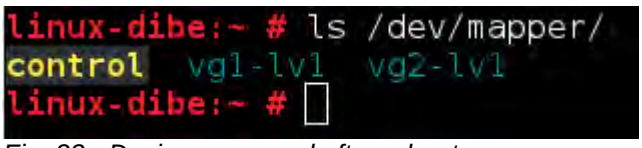


Fig. 23 - Devices removed after reboot.

To Add Specific Devices to be Under UltraBac Ux Agent Protection

1. To add specific devices under protection, type <2>. You will be prompted to enter the desired device names separated by a comma (,) as seen in Figure 24.

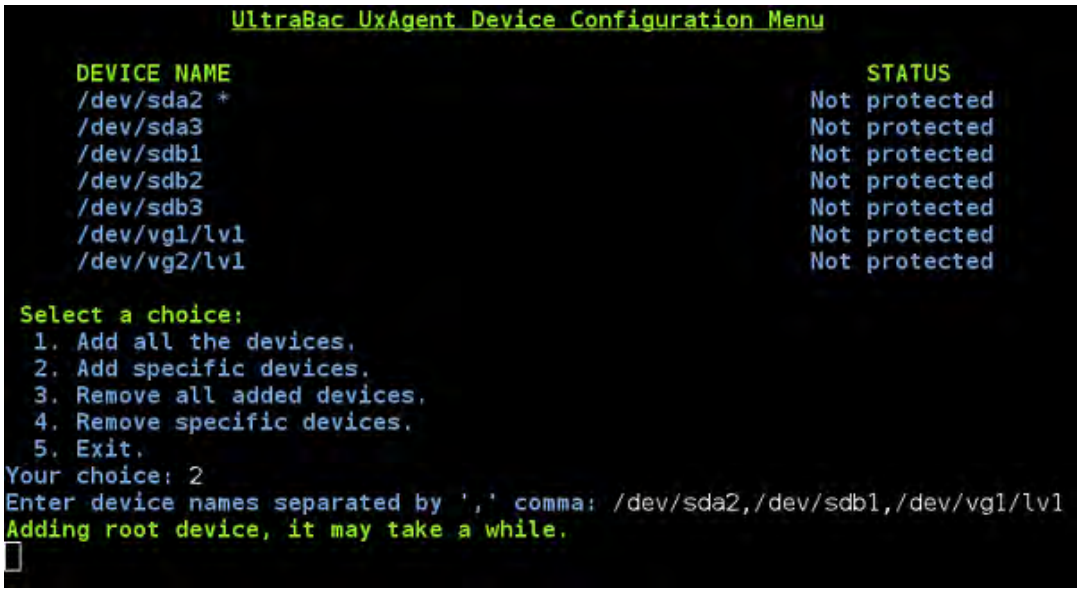


Fig. 24 - Add specific devices.

2. After adding specific devices, you will see the status of those particular devices changed to "Marked for protection." For the configuration to be complete, restart the computer.

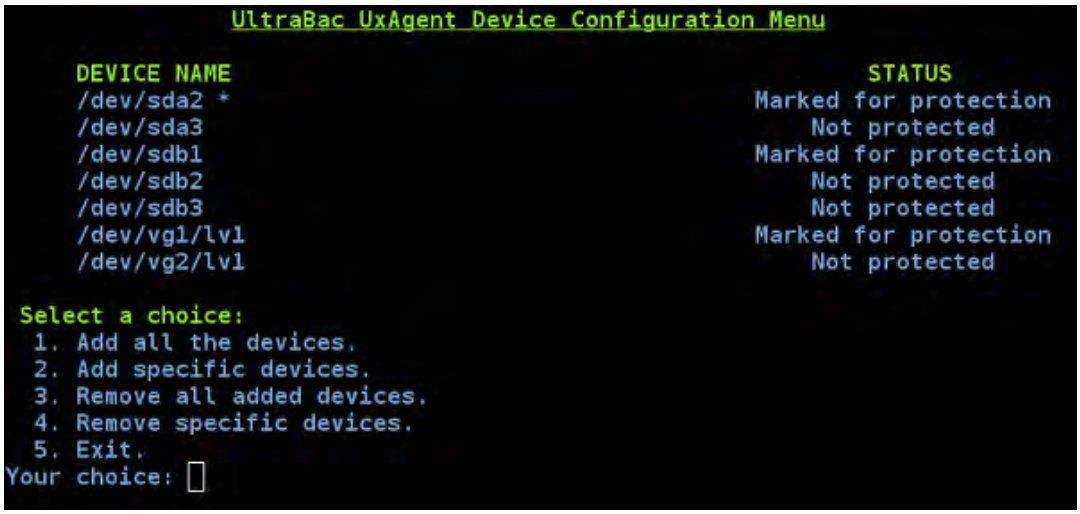


Fig. 25 - After adding specific devices.

3. After reboot, selected mapped devices are created and can be seen under /dev/mapper.

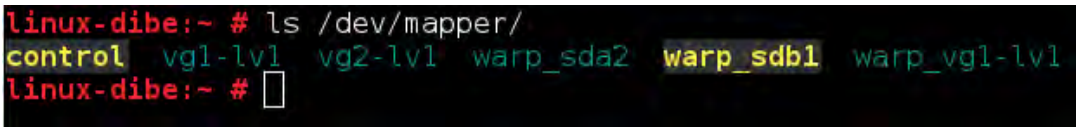


Fig. 26 - Selected mapped devices created after reboot.

To Remove Specific Devices from Under UltraBac Ux Agent Protection

1. To remove specific devices from protection, type <4>. You will be prompted to enter specific device names that you want to remove from protection as seen in Figure 27.

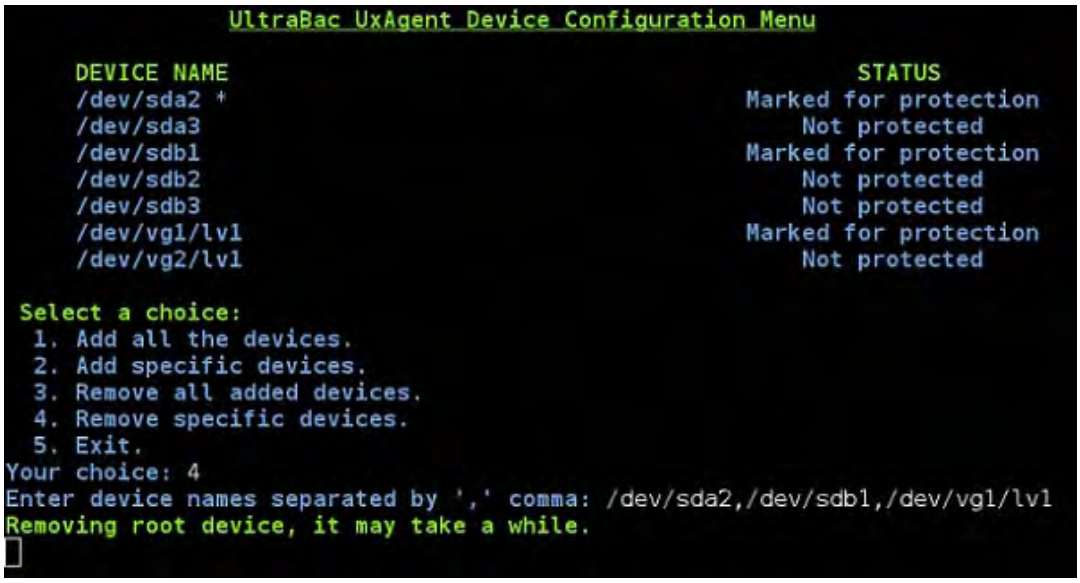


Fig. 27 - Remove specific devices.

2. After removing specific devices, you will see the status of removed devices changed back to "Not protected." For the configuration to be complete, restart the computer.

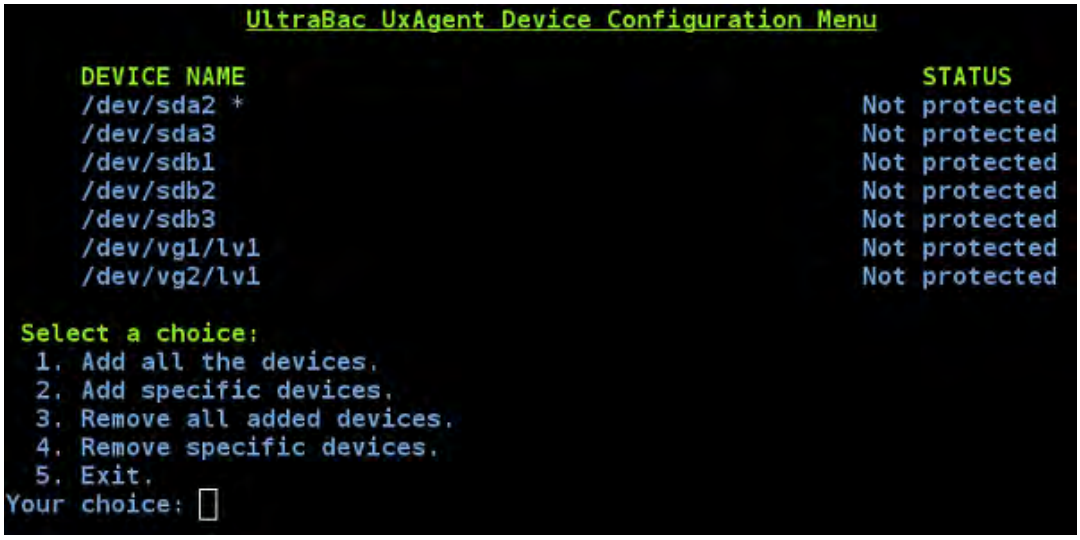


Fig. 28 - After removing specific devices.

3. After reboot, selected mapped devices are deleted and can no longer be seen under /dev/mapper.

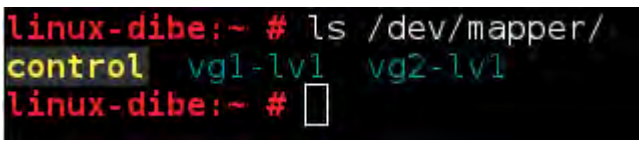


Fig. 29 - Selected devices removed after reboot.

To exit from the UltraBac UxAgent Device Configuration Menu, type <5>.

```
                UltraBac UxAgent Device Configuration Menu

     DEVICE NAME                                              STATUS
     /dev/sda2 *                                          Not protected
     /dev/sda3                                            Not protected
     /dev/sdb1                                            Not protected
     /dev/sdb2                                            Not protected
     /dev/sdb3                                            Not protected
     /dev/vg1/lv1                                         Not protected
     /dev/vg2/lv1                                         Not protected

 Select a choice:
  1. Add all the devices.
  2. Add specific devices.
  3. Remove all added devices.
  4. Remove specific devices.
  5. Exit.
Your choice: 5
NOTE : For configuration changes to be effective perform a reboot.
linux-dibe:~ # ls /dev/mapper/
control  vg1-lv1  vg2-lv1
linux-dibe:~ #
```

Fig. 30 - Exit.

Backups

Creating a Backup Set

To begin the backup process, follow these steps from the Windows client that will be managing the Ux Image Agent backups:

1. Open the "UltraBac Management Console."
2. Select the Backup tab and click "New."
3. Select the "UxImage Agent." Click "Next" to continue.

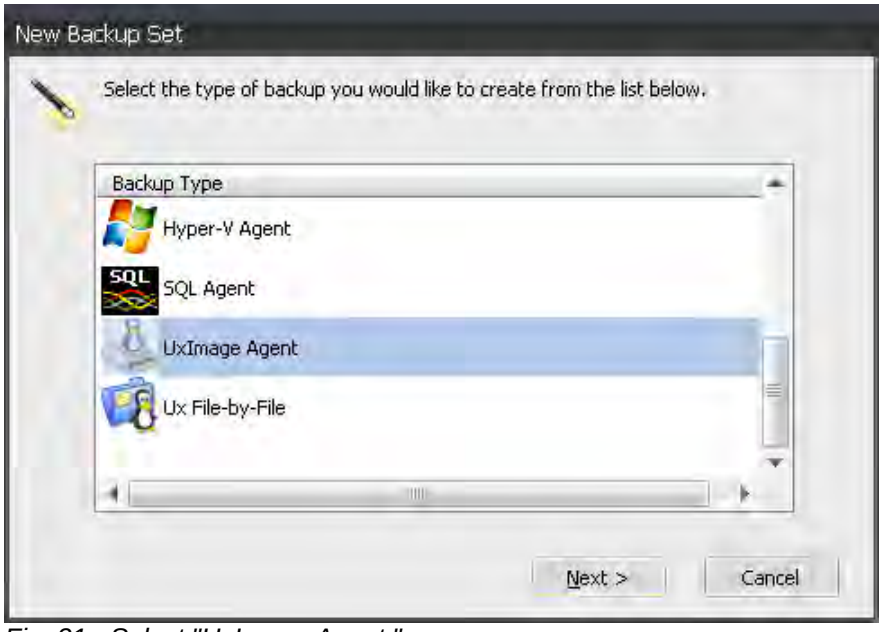


Fig. 31 - Select "UxImage Agent."

4. Type the host name or IP address of the UNIX/Linux computer into the "Server" field. Type the username and password into the "Username" and "Password" fields, and click "Next." Please note the username should be valid on a UNIX/Linux computer, should all be lowercase, and the account should have "root" privileges.

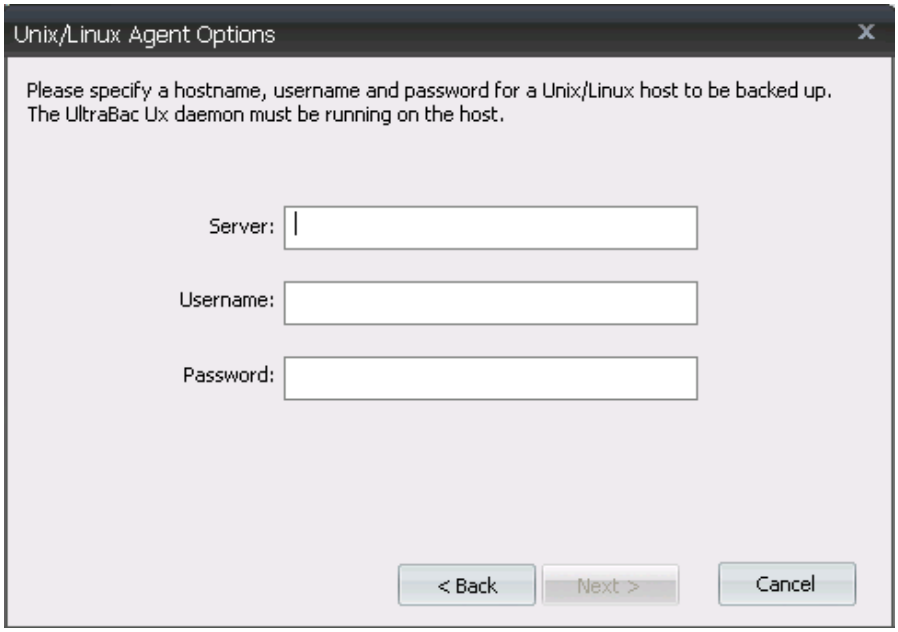


Fig. 32 - UNIX/Linux Agent Options.

5. Select the backup options for the Backup Set and click "Next." Depending on the type of backup you wish to take, click the appropriate check boxes:
   I. To back up the entire disks only (not enumerating partitions), do not check either of the boxes.
   II. To back up the individual partitions on one or more disks, check the upper box "Always back up partitions individually."
   III. To back up only the used blocks of data on the individual partitions, check both boxes: "Always backup partitions individually" and "Enable in-use block backup for partitions with known filesystems."

The details of the three possible option choices are below:

I. To back up the entire disks only (not enumerating partitions), do not check either of the boxes. If neither check box is selected, "Always back up partitions individually" nor "Enable in-use block backup for partitions with known filesystems," as seen in Figure 33, the following occurs:

Enumeration:
1. No partitions are enumerated.
2. Only disks are enumerated whether or not the disks contain a partition.
3. No logical volumes are enumerated. No volume group is enumerated.

Backup:
1. Disks are backed up as raw devices irrespective of the top-level file system.
2. If a partition exists under the disk selected for partition, its metadata is backed up.

Restore:
1. If a partition exists under the disk during a backup, it gets rebuilt once the restore is complete irrespective of the changes done to the disk/partition.

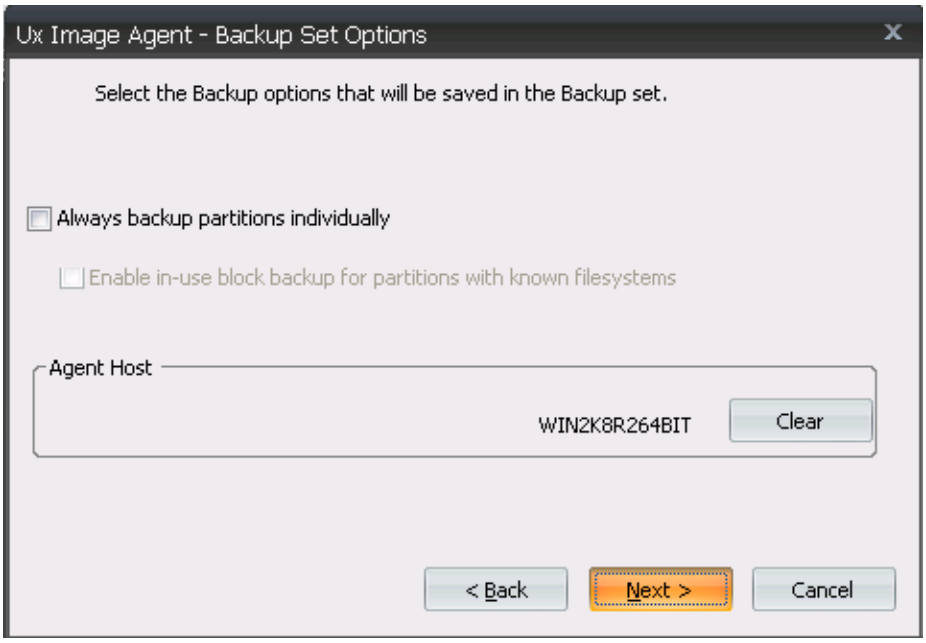


Fig. 33 - Backup Set Options.

II. To back up the individual partitions on one or more disks, check the upper box "Always back up partitions individually." If "Always Backup partitions individually" is selected and "Enable in-use block backup for partitions with known filesystems" is not selected, as seen in Figure 34, the following occurs:

Enumeration:
1. All disks and their partitions are enumerated.
2. Disks with no partitions are NOT enumerated.
3. All logical volumes (created with LVM) are enumerated with volume group (acting as disk) on left pane.
4. If a partition has no file system on it, or has a valid file system but it is not supported by the Ux Agent (such as reiserfs), it will NOT get enumerated.
5. Swap partitions are NOT enumerated.
6. Partitions having the Physical Volume (PV) label are NOT enumerated.

Backup:
1. Whole partitions/logical volumes will be backed up.
2. If the partition has a valid and supported filesystem on it, and it is not protected, the partition should get backed up using the original device with a warning to the user. Snapshot creation is not possible in this case.
3. If the mapped device of the partition is mounted during backup, the backup of the partition will proceed with successful snapshot formation.

Restore:
1. The restore will succeed as long as the original device or mapped device for the device to be restored is present and not mounted. If the original or mapped device is mounted, the restore will fail with an error.
2. If both the mapped device and original device are present, the priority should be given to the mapped device present under /dev/mapper/.

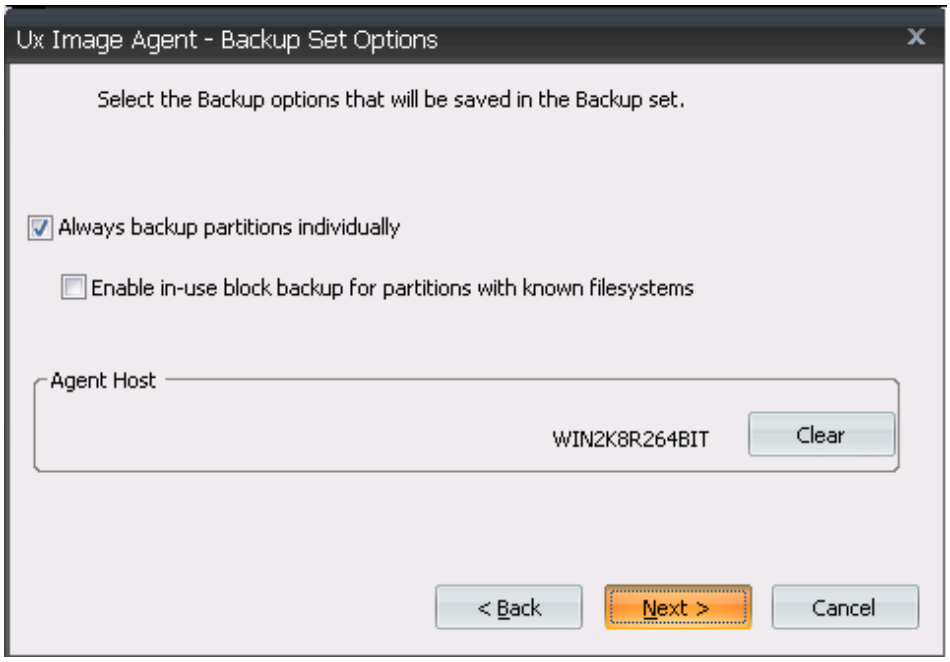


Fig. 34 - Backup Set Options.

III. To back up only the used blocks of data on the individual partitions, check both boxes: "Always backup partitions individually" and "Enable in-use block backup for partitions with known filesystems." If "Always backup partitions individually" AND "Enable in-use block backup for partitions with known filesystems" are selected, as seen in Figure 35, the following occurs:

Enumeration:
1. All disks and their partitions are enumerated.
2. Disks with no partitions are NOT enumerated.
3. All logical volumes (created with LVM) are enumerated with volume group (acting as disk) on left pane.
4. If a partition has no file system, on it or has a valid file system but it is not supported by the Ux Agent (like reiserfs), it will NOT get enumerated.
5. Swap partitions are NOT enumerated.
6. Partitions having the Physical Volume (PV) label are NOT enumerated.

Backup:
1. The used blocks of all the partitions/logical volumes should be backed up as long as the partition has a valid and supported file system on it.
2. If the partition has a valid and supported file system on it, and it is not protected, the partition should get backed up using the original device with a warning to the user. Snapshot creation is not possible in this case.
3. If the mapped device of the partition is mounted during backup, the backup of the partition will proceed with successful snapshot formation.

Restore:
1. The restore will succeed as long as the original device or mapped device for the device to be restored is present and not mounted. If the original or mapped device is mounted, the restore will fail with an error.

2. If both the mapped device and original device are present, the priority should be given to the mapped device present under /dev/mapper.

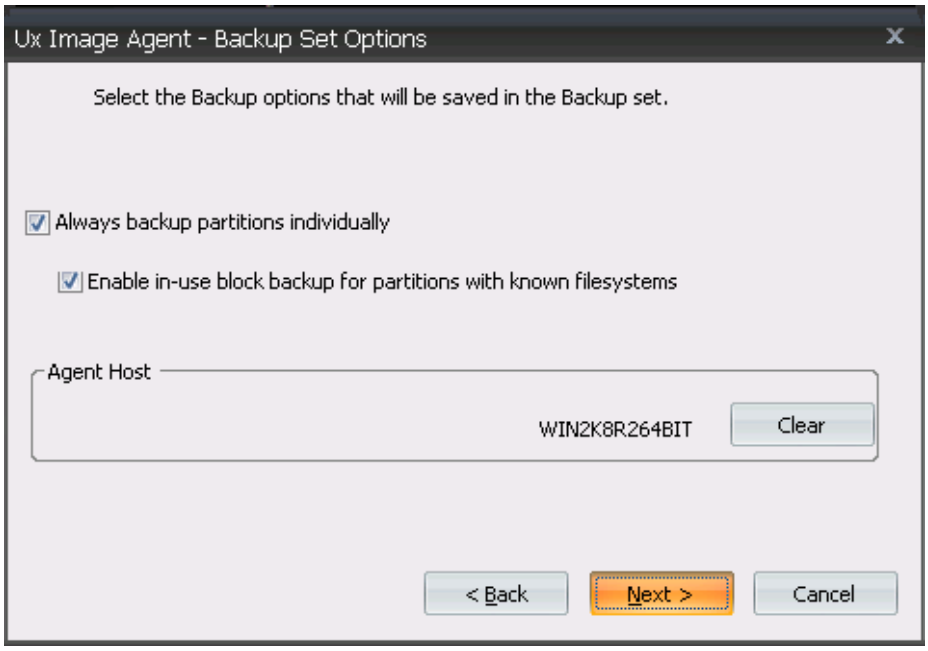


Fig. 35 - Backup Set Options.

6. Enter a set description and choose the file selection logic to be used for this set. Click "Next."

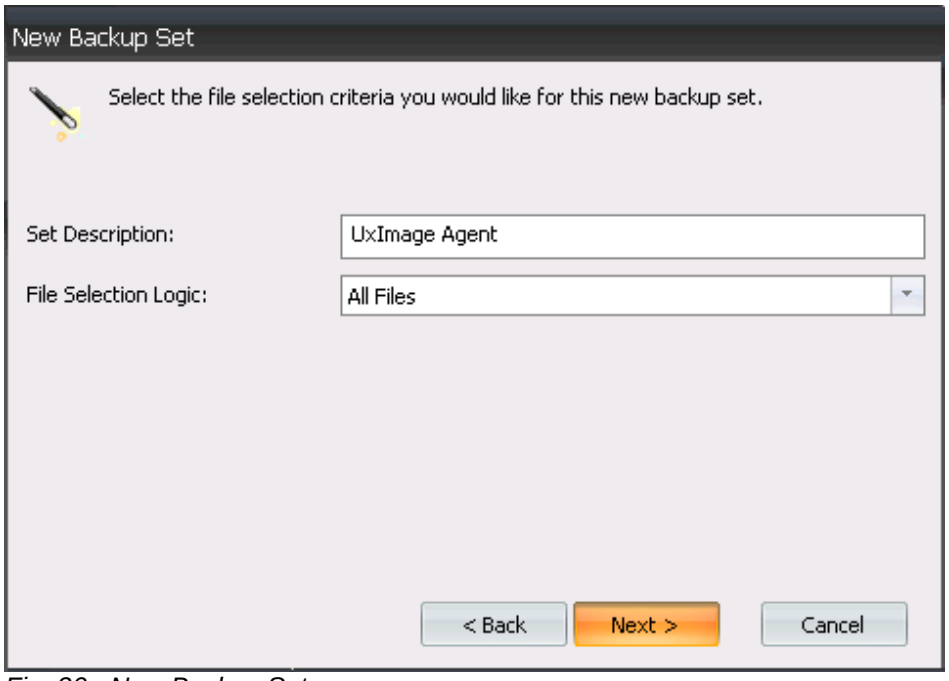


Fig. 36 - New Backup Set.

7. 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." Alternatively you can save the backup to a file or back up selected files to a device.

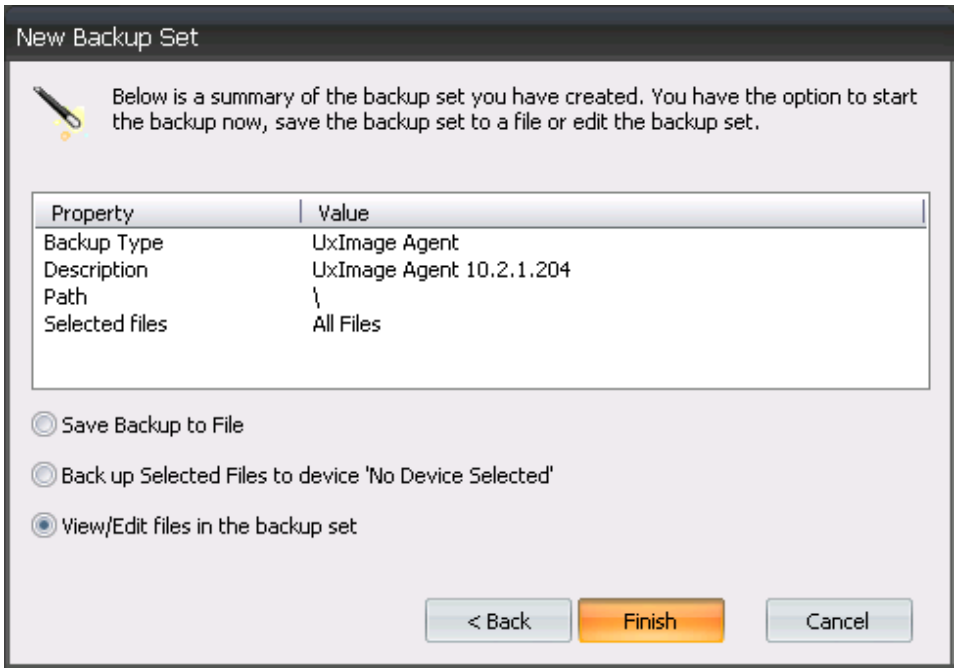


Fig. 37 - Backup Set summary.

8. Depending upon which backup set option you chose in step 5, you will be presented with an enumeration of the disks/partitions to choose for backup in this backup set.
    I. If you chose backup set options "I" (no boxes checked), create a backup set by selecting the desired disks from the enumerated list, as seen in figure 38.

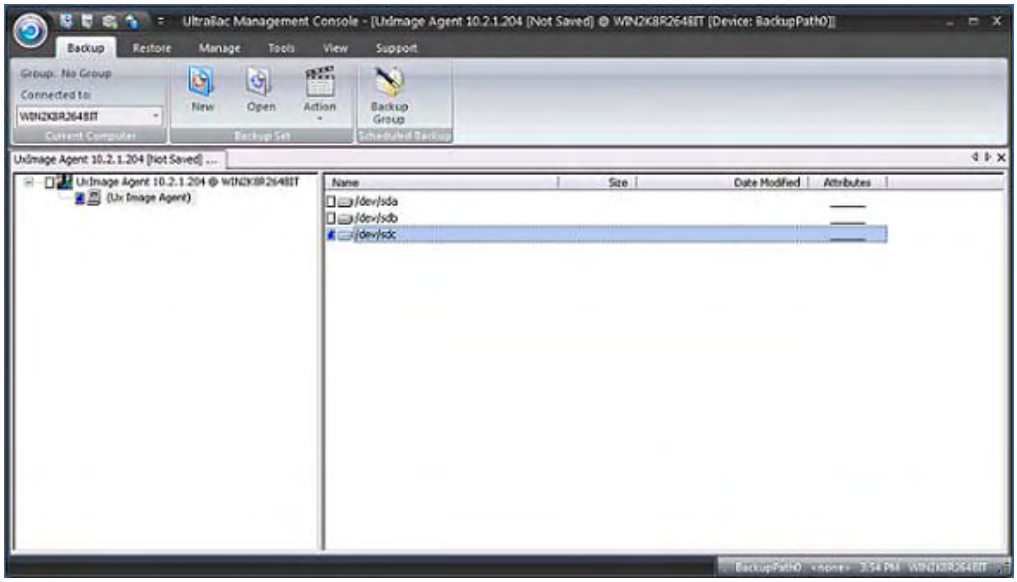


Fig. 38 - Backup Set drives/partitions, option (I).

    II. If you chose backup set option "II" (only "Always backup partitions individually" checked), create a backup set by selecting the desired partitions under any of the disks from the enumerated list. The size of the partitions can be seen alongside the listing, as seen in Figure 39.

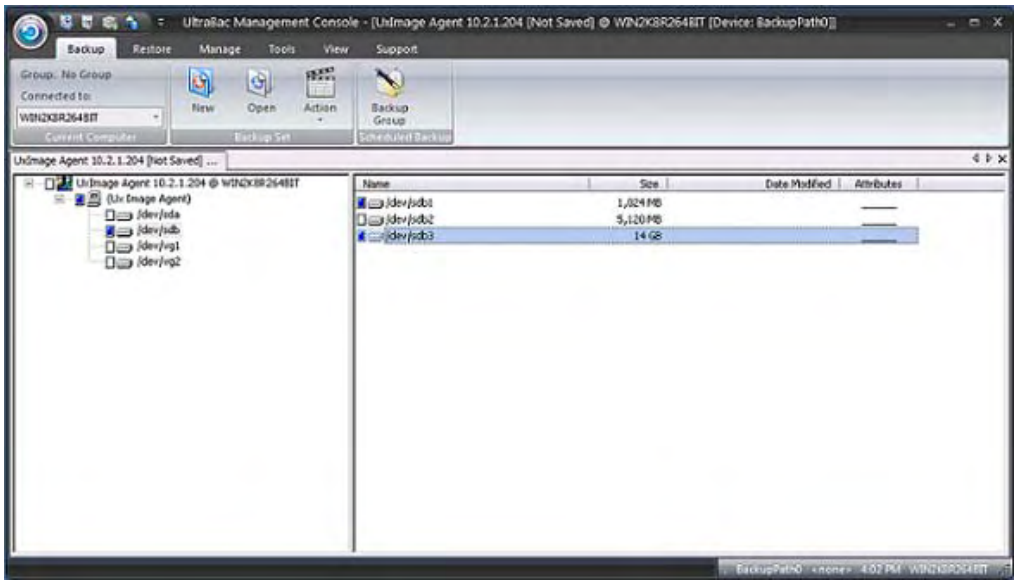


Fig. 39 - Backup Set drives/partitions, option (II).

III. If you chose backup set option "III" (both boxes checked), create a backup set by selecting the desired partitions under any of the disks from the enumerated list. The size of only the used blocks on the respective partitions can be seen alongside the listing, as seen in Figure 40.

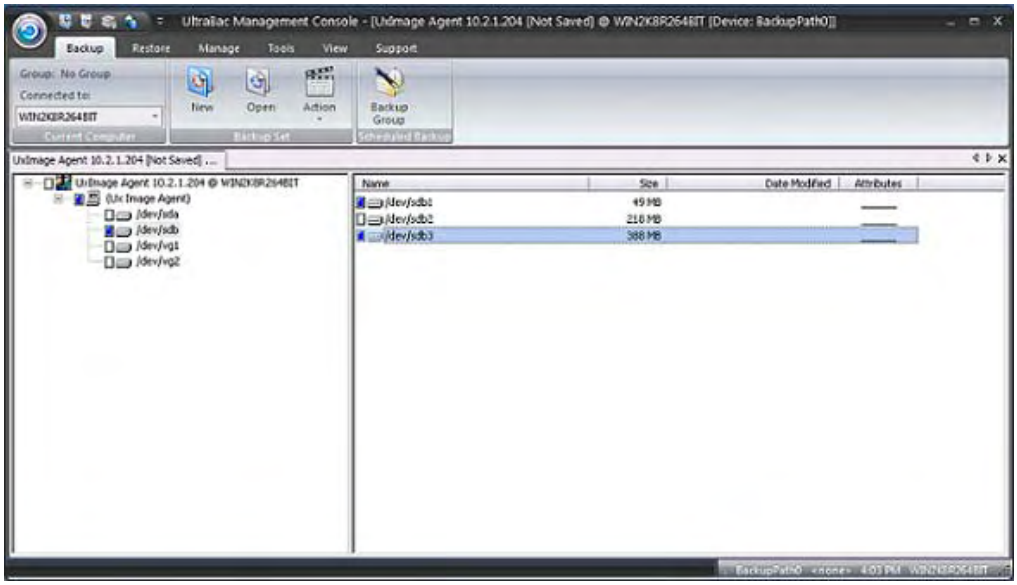


Fig. 40 - Backup Set drives/partitions, option (III).

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

Starting the Backup

NOTE: Before beginning the backup, set the backup storage device. For additional information on setting the backup storage device, please visit the "**Storage Device Manager**" section of the User Manual:

UltraBac User Manual: Storage Device Manager

1. Click "Actions," select "Run Backup Now."

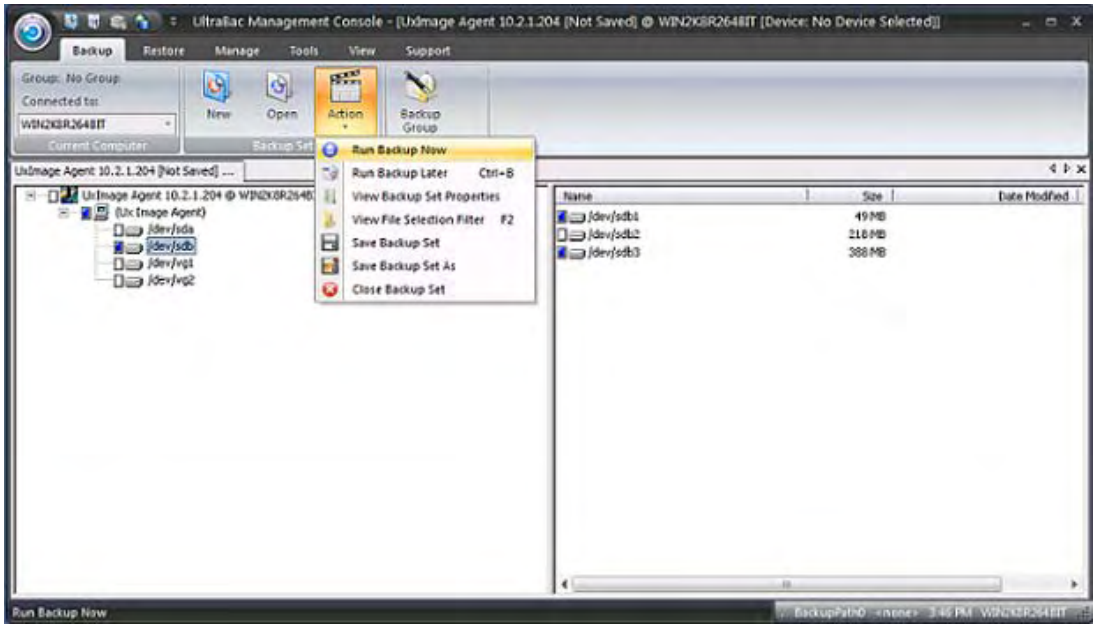


Fig. 41 - Run backup.

2. Select the relevant options to use during this backup. Click "Backup" to start the backup.

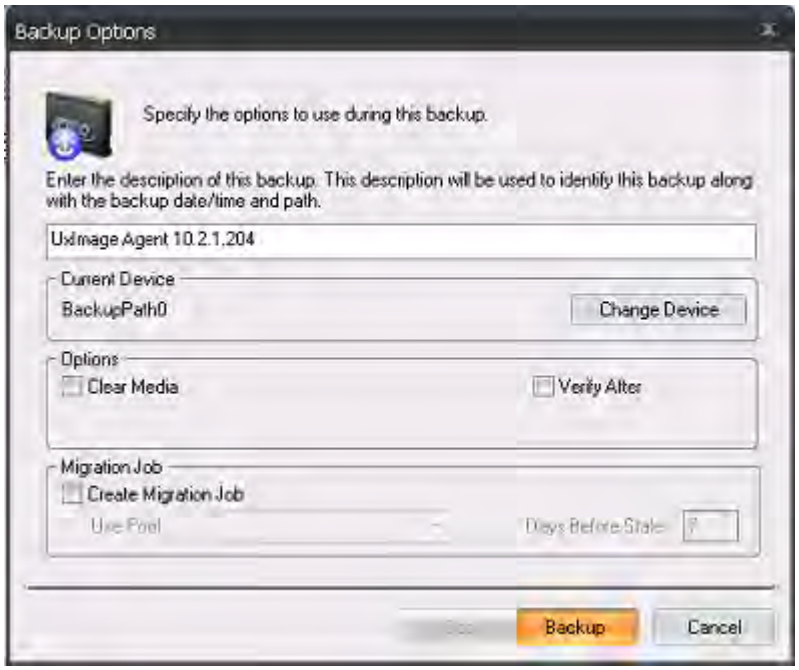


Fig. 42 - Start backup.

3. A progress window shows the status of the backup.

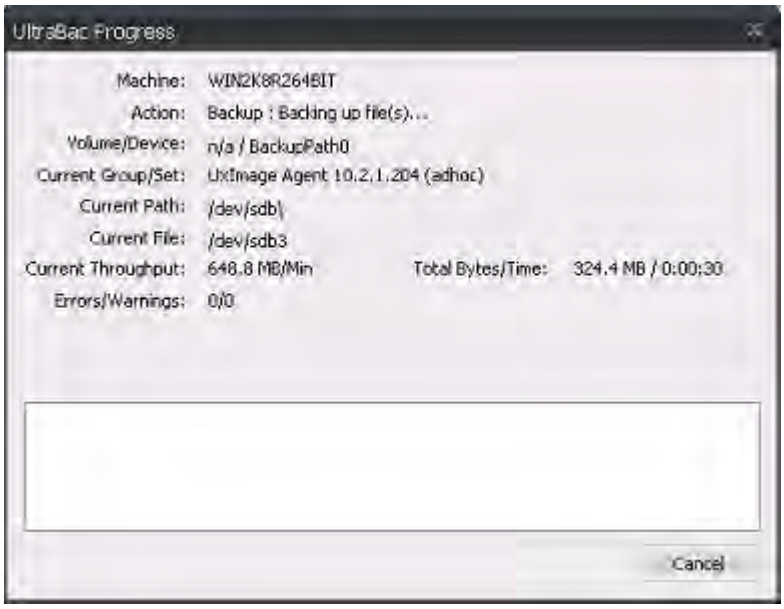


Fig. 43 - Backup progress.

4. After completion of the backup process you will see a message saying "Operation complete."

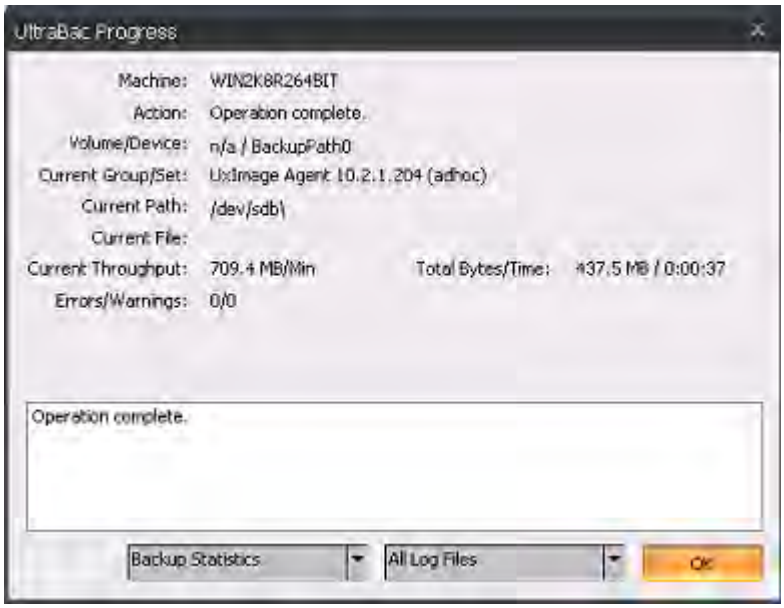


Fig. 44 - Backup process complete.

Restores

NOTE: Before beginning the restore, select the restore storage device where the backup to be restored is saved. For additional information on selecting the restore storage device, please visit the "**Restore Basics**" section of the User Manual:

UltraBac User Manual: Restore Basics

1. Launch the Restore Wizard by selecting the Restore tab, and selecting "Media."

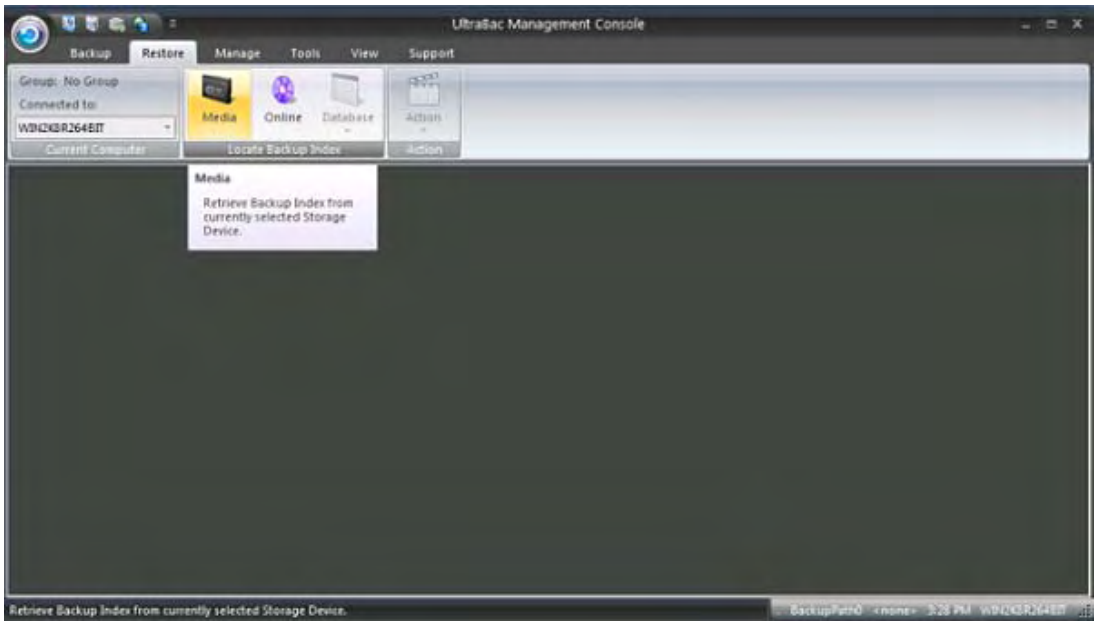


Fig. 45 - Launch Restore Wizard.

2. Select and load the backup index for restore.

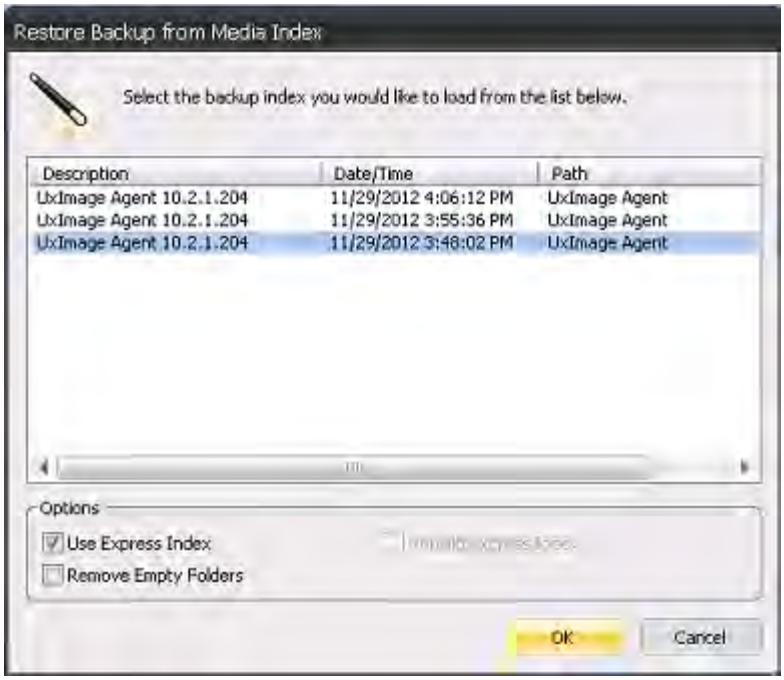


Fig. 46 - Select backup index.

3. The enumerated backup index will display the drives/partitions backed up, depending upon the backup set options chosen for the backup. Select the disks/partitions you wish to restore.
    I. If you backed up using option "I" (no boxes checked), the enumerated list of the backup set will show the disks, as seen in Figure 47.

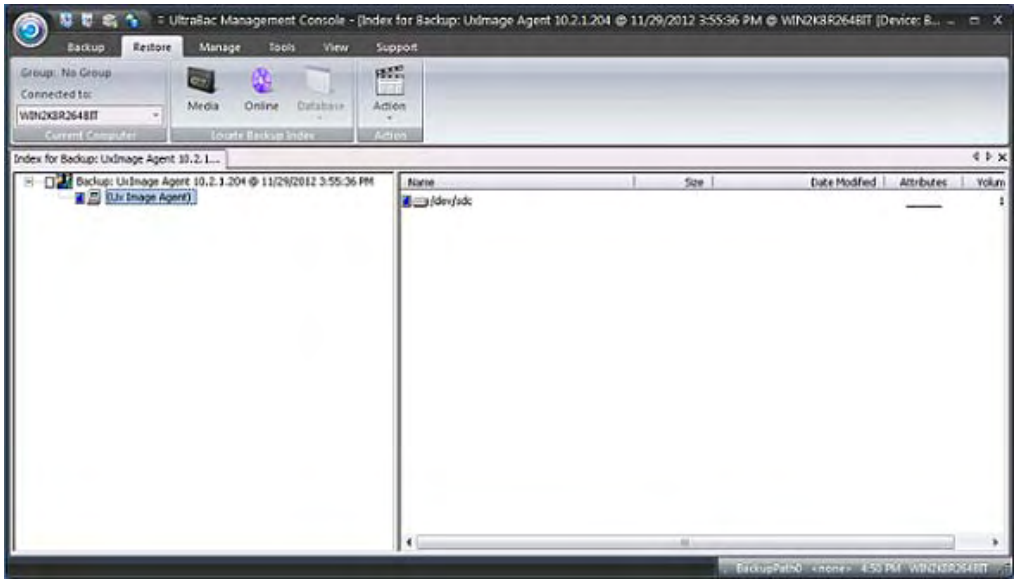


Fig. 47 - Select disks/partitions for restore, backed up option (I).

    II. If you backed up using option "II" (only "Always backup partitions individually" checked), the enumerated list of the backup set will show the partitions. The size of the partitions can be seen alongside the listing, as seen in Figure below.

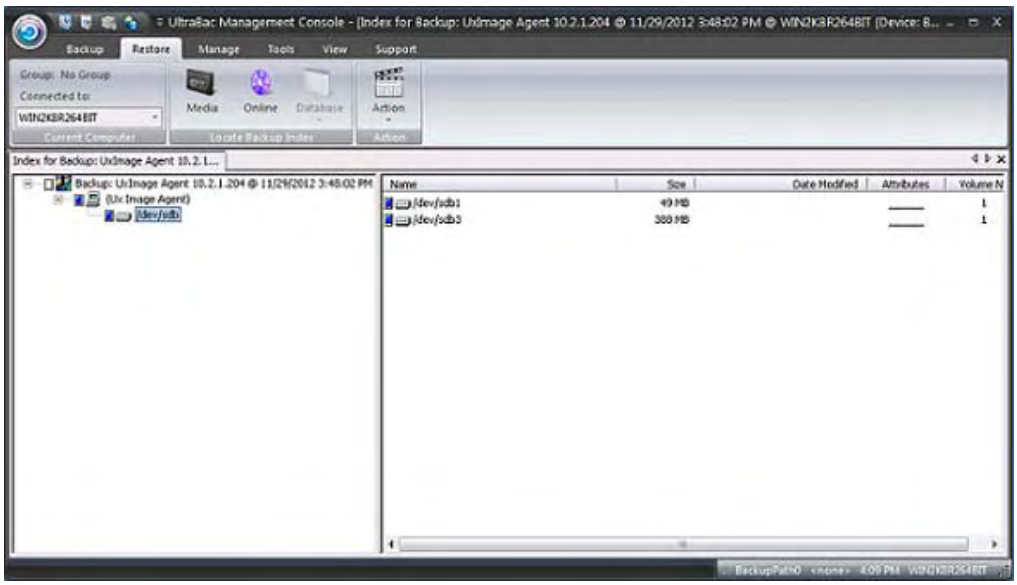


Fig. 48 - Select disks/partitions for restore, backed up option (II).

    III. If you backed up using option "III" (both boxes checked), the enumerated list of the backup set will show the partitions. The size of only the used blocks on the respective partitions can be seen alongside the listing, as seen in Figure below.

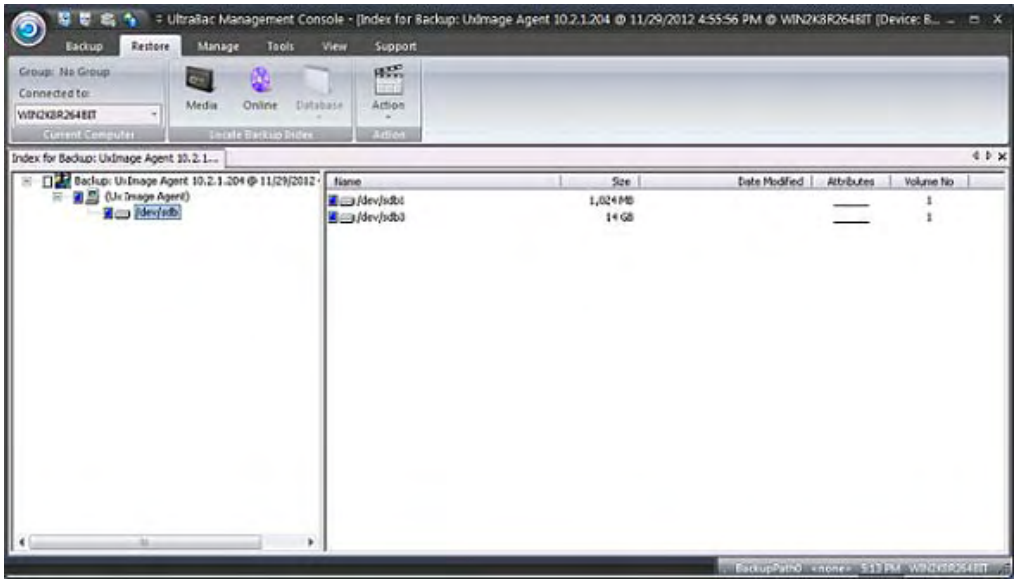


Fig. 49 - Select disks/partitions for restore, backed up option (III).

4. Click "Action," then select "Restore this Backup."

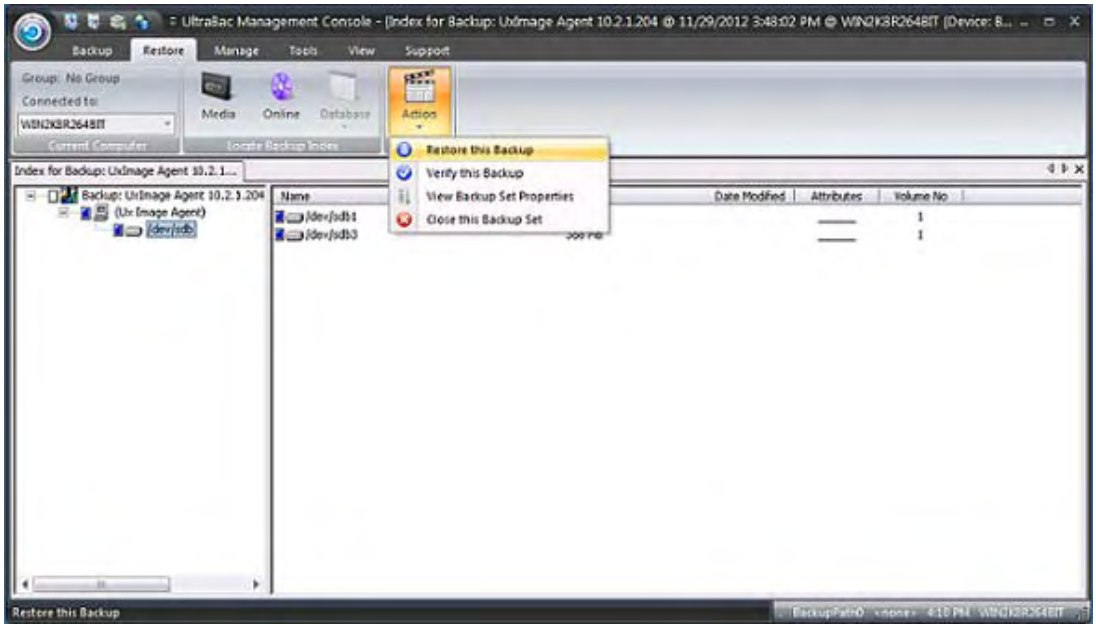


Fig. 50 - Restore action.

5. The "UxImage Agent Restore Options" window is displayed as seen in figure 53. There are three restore scenarios that you may choose:
   I. Restore to the original disk/partition.
   II. Restore to a disk/partition other then the original.
   III. Perform a Bare Metal Recovery (BMR)

> NOTE: To perform a Bare Metal Recovery (BMR), please see the next section of the UltraBac User Manual: "**Bare Metal Recovery (BMR)**."



Fig. 51 - Ux Image Agent Restore Options.

Restore to original disk/partition

I. To restore to the original disk/partition, enter the IP address, username, and password of the original computer that was backed up. Do not select the "Advanced restore mode" or "Restore MBR" options. Click "Next."

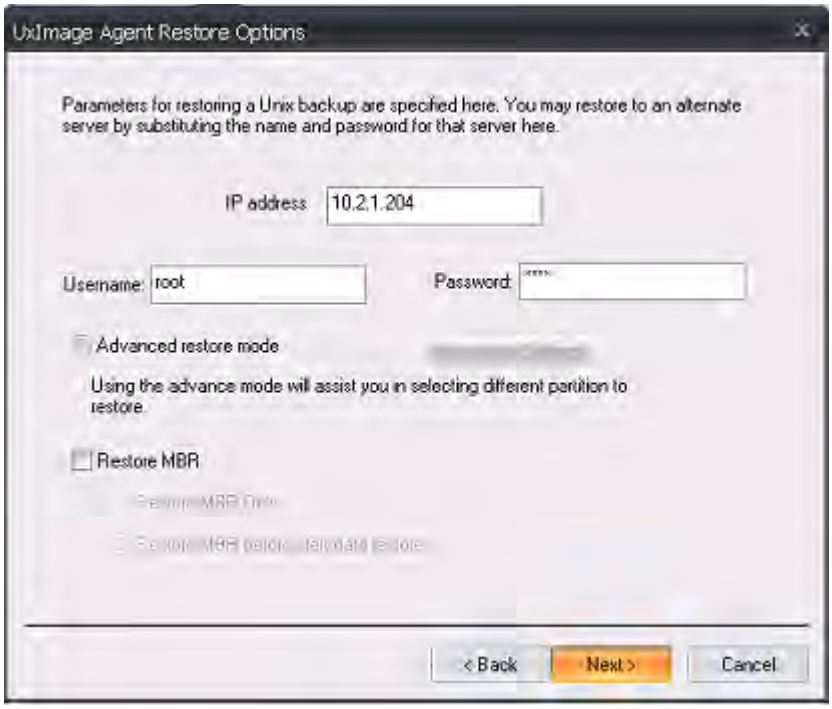


Fig. 52 - Ux Image Agent Restore Options, restore to original disk/partition.

Restore to a disk/partition other than the original (not available in UXBMR, and must be restored to same size partition)

II. To restore to a disk/partition other than the original, follow the steps below:

A. Enter the IP address, username, and password of the computer receiving the restore. Select "Advanced restore mode" and click "Advanced Settings."

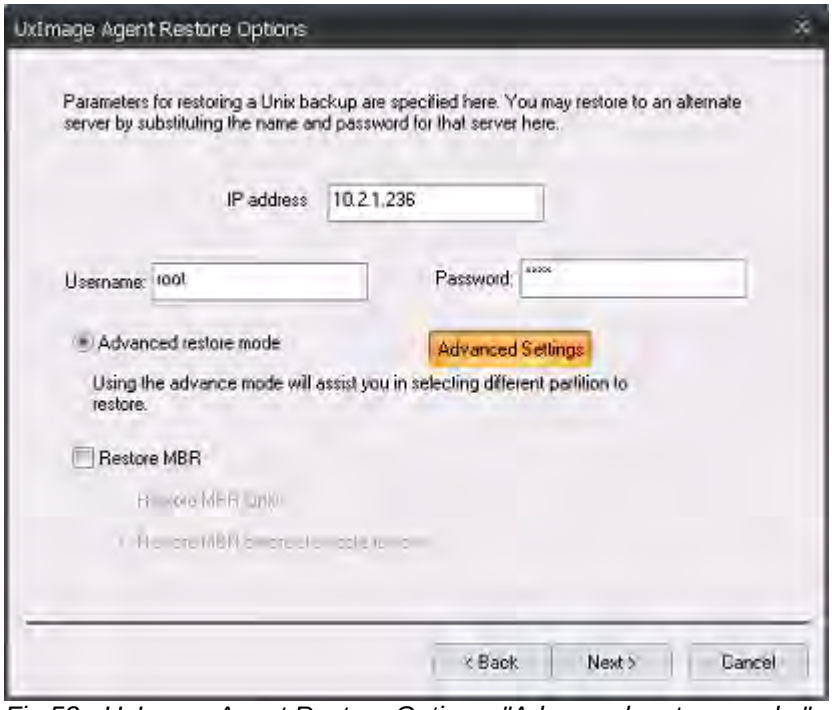


Fig.53 - UxImage Agent Restore Options, "Advanced restore mode."

B. Within the "Advanced Mode Settings" window, under "Select Source," select the backed up disk/partition for restore.

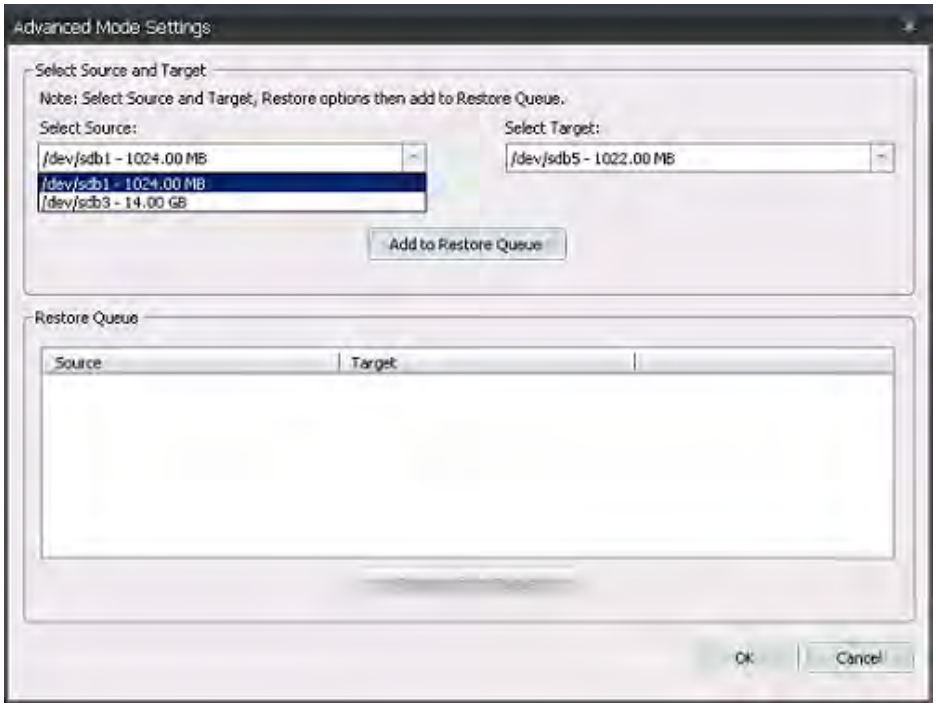


Fig. 54 - Advanced Mode settings, "Select Source."

C. Under "Select Target," depending upon whether the backup was the entire disk only (not enumerating partitions) or individual partitions:
   - In the case of a backup that was entire disk only (not enumerating partitions), on the computer you want to restore:
     - You will see RAW disks with no partitions or RAW disks with all RAW partitions.
     - You will NOT see disks formatted with a filesystem, disks having any one or more formatted partitions, the partitions and Logical Volumes (RAW or formatted), or the Volume Groups (acting as disk).
   - In the case of a backup that was individual partitions (whether or not it was in use block only), on the computer you want to restore:
     - You will see RAW partitions and RAW Logical Volumes.
     - You will NOT see the partitions/Logical Volumes having a filesystem, the disks (RAW or formatted), swap and extended partitions, or partitions having a PV (Physical Volume) label.

D. Select the desired target disk/partition/Logical Volume for restore. It is recommended to choose a target disk/partition/Logical Volume of the same size or larger as the source.

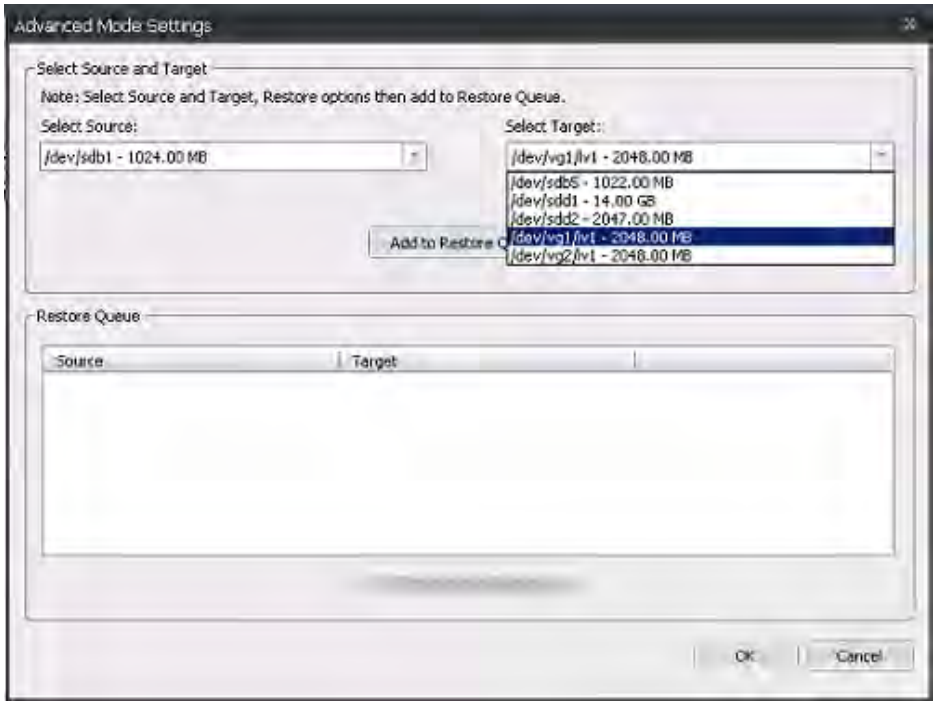


Fig. 55 - Select target disk/partition.

E. Click on "Add to Restore Queue" to add one source-target pair to the queue for restore.
F. You will see the pair added to the "Restore Queue." Repeat steps "B" through "E" to select more or all backed up disks/partitions for restore, if required.

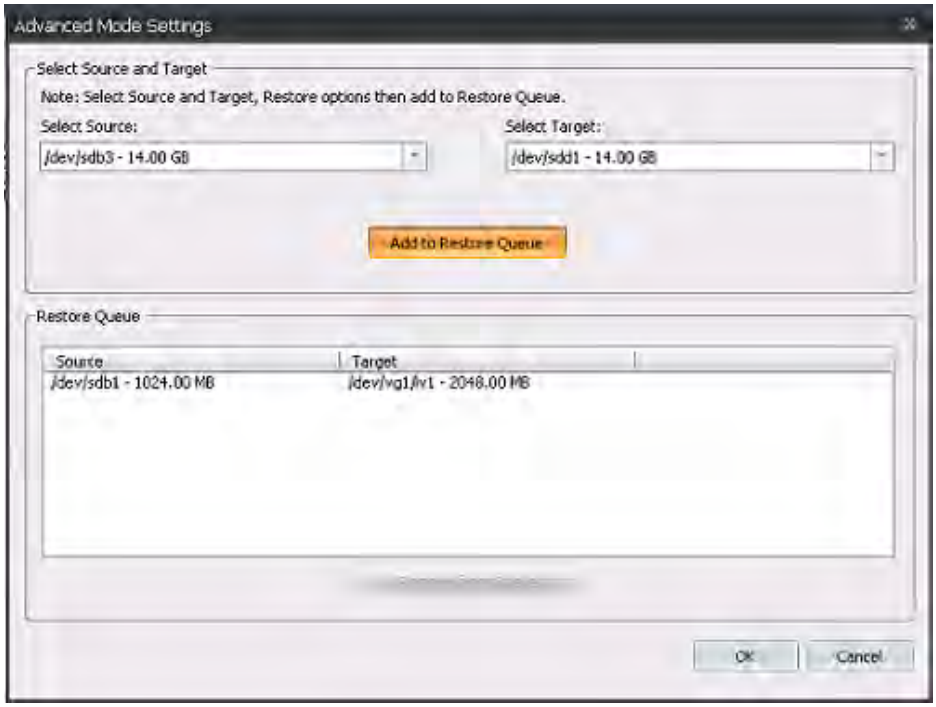


Fig. 56 - Adding to the Restore Queue.

G. (Optional) You can remove items from the "Restore Queue" by selecting the pair from the queue and clicking "Remove from Queue."

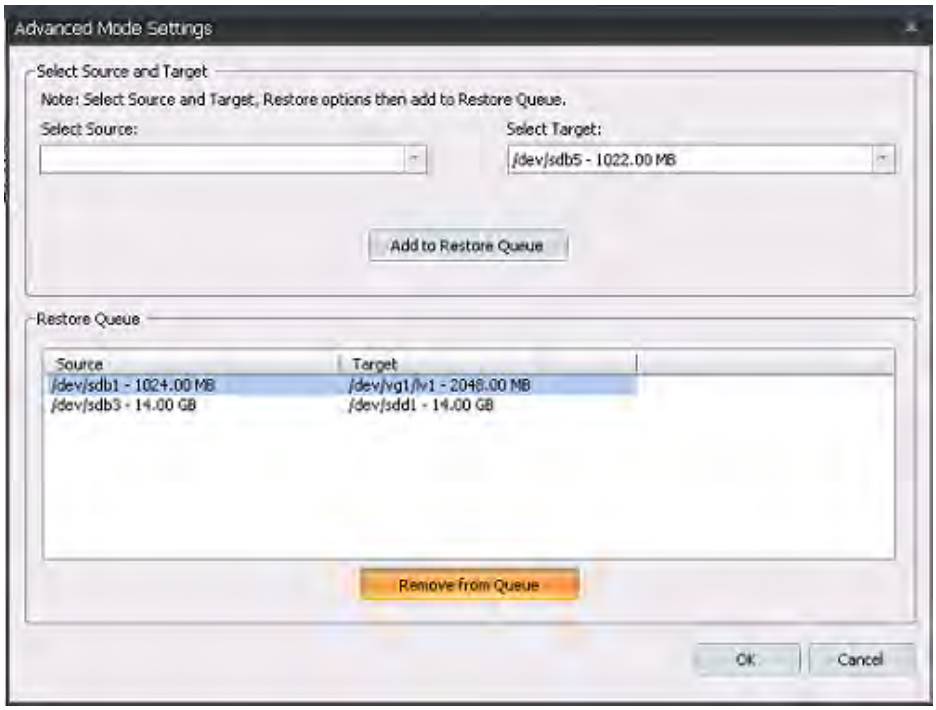


Fig. 57 - Removing from the Restore Queue.

H. Once you have created the "Restore Queue" click "OK."

- If the "Restore Queue" is empty, you will get an error message as seen in figure 58. Click "OK."

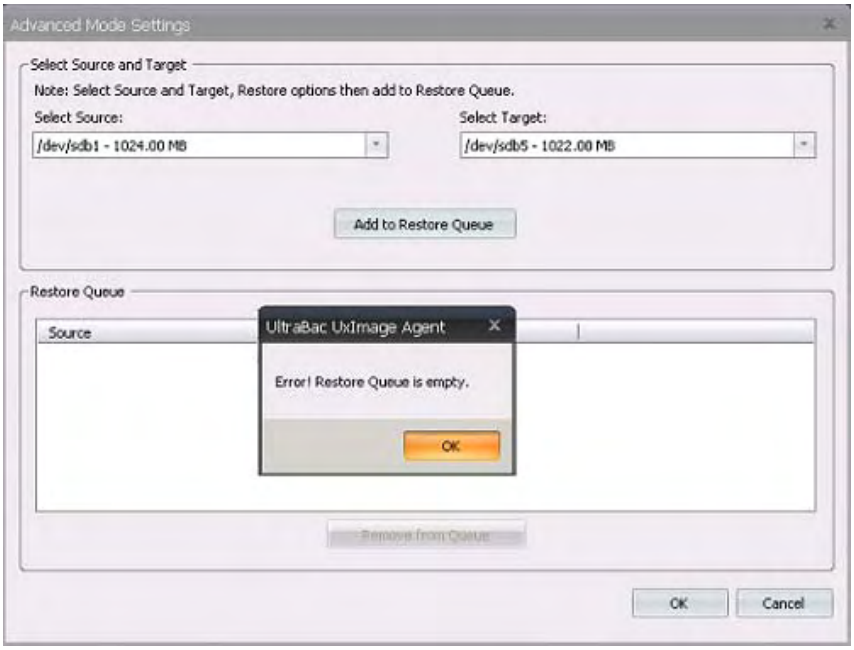


Fig. 58 - Click "OK" on error message.

- If all the backed up disks/partitions are not added to the queue, you will get a warning message as seen in Figure 59. Click "Yes" to continue.

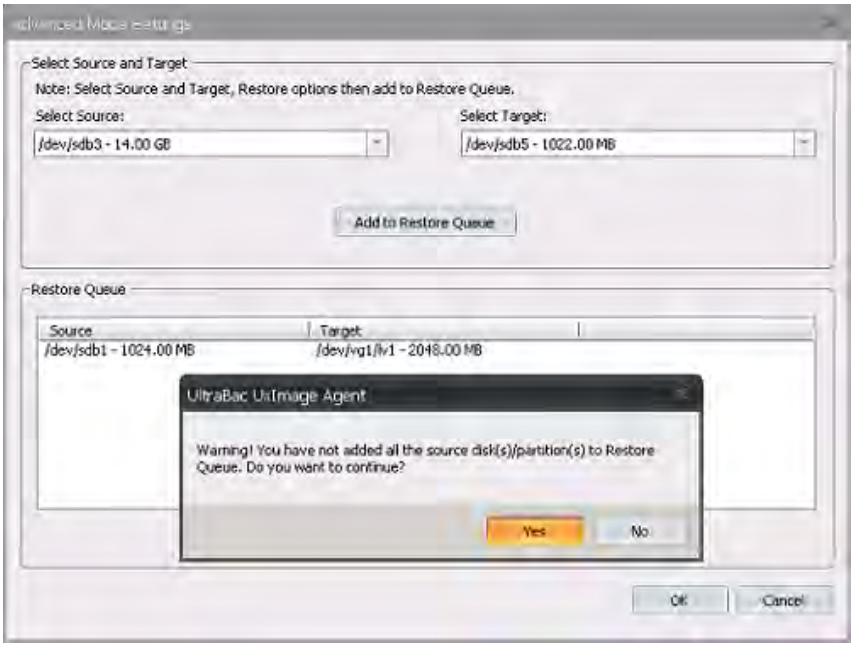


Fig. 59 - Click "Yes" on warning message.

6. After clicking "OK," you will be back to the "UxImage Agent Restore Options" window. At this stage, the Restore MBR option and its sub-options are disabled. Click "Next" to proceed.

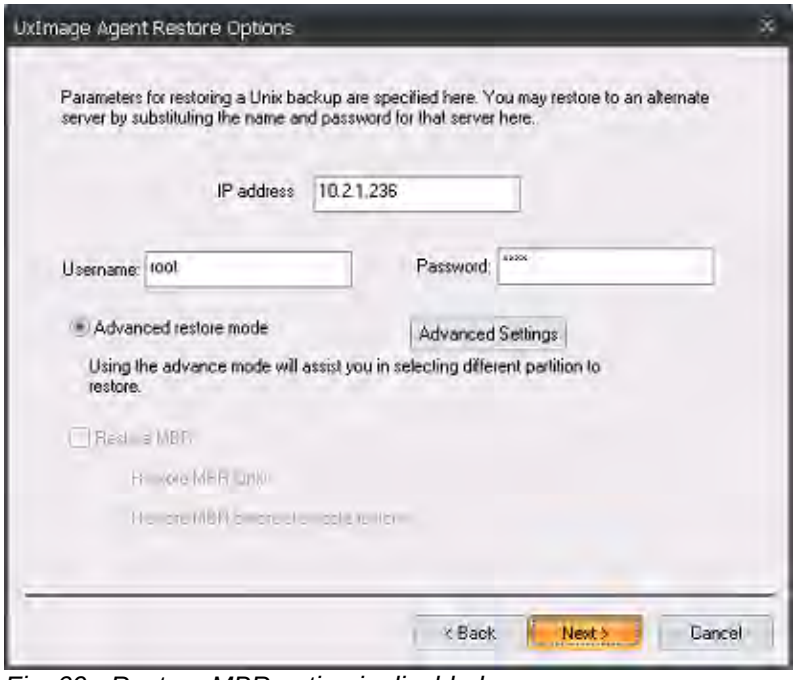


Fig. 60 - Restore MBR option is disabled.

7. Click "Restore."

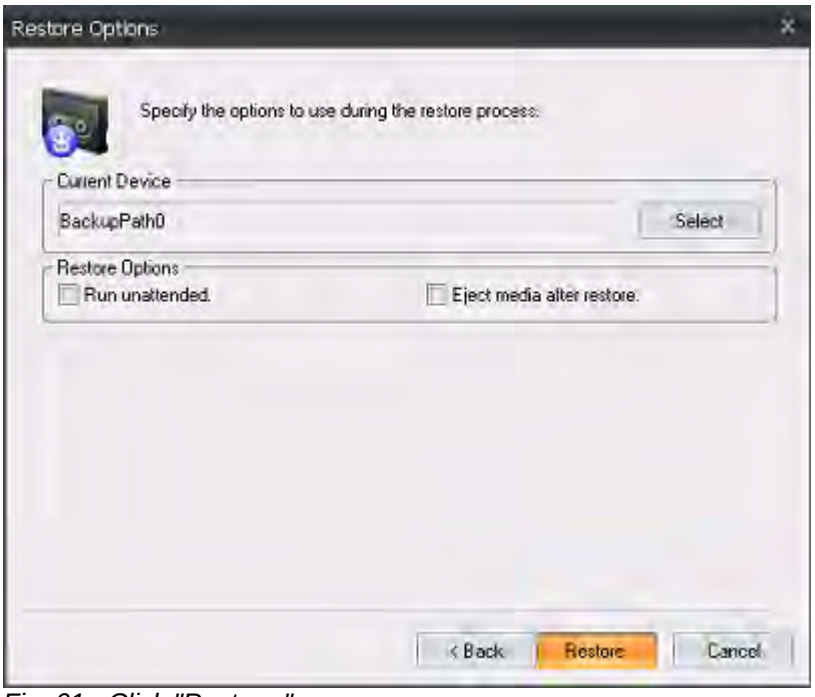


Fig. 61 - Click "Restore."

8. An "UltraBac Progress" window will display showing the status of the restore process.

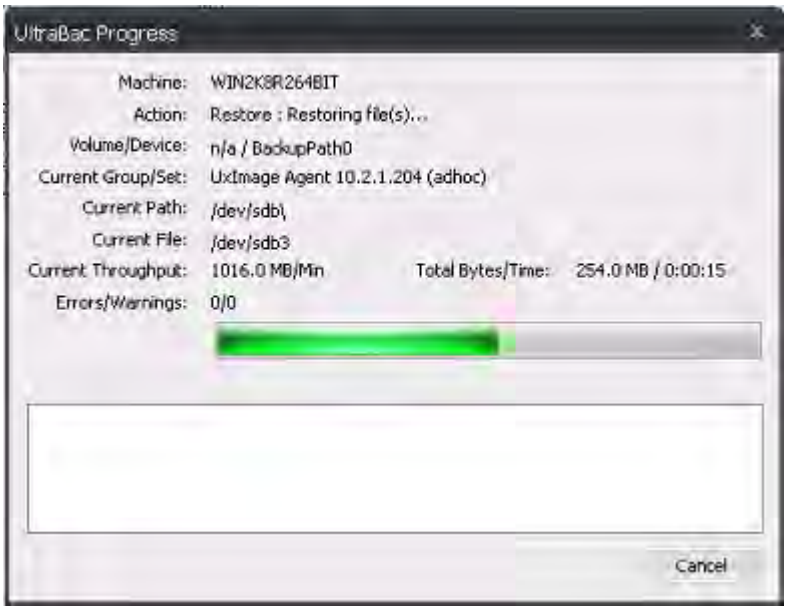


Fig. 62 - Restore progress.

9. After completion of the restore process you will see a message saying "Operation complete."

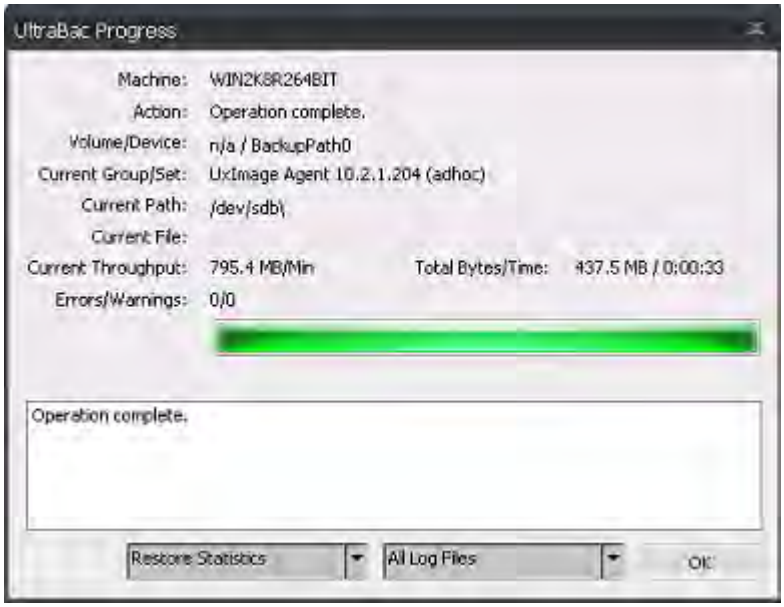


Fig. 63 - Operation complete.

Perform a Bare Metal Recovery (BMR)

The "Ux Image Agent Restore" Bare Metal Recovery (BMR) CD is a separate downloadable ISO image. BMR is the process of rebuilding a computer after a drive failure or system crash. It restores the image of the original disk back onto the new disk and restarts the system. The UNIX/Linux system is booted to the BMR CD to provide it an OS and network configuration, and then the recovery is performed remotely from a Windows computer running UltraBac to the same hardware as the original UNIX/Linux computer. The BMR CD is used to boot and perform a BMR on any UNIX/Linux computer that has already been backed up by an UltraBac Windows client with a valid Ux Image Agent license.

1. Use the ISO image available from UltraBac's ftp site ftp://rpmrepo.ultrabac.com/uxagent/UxAgentBMR/, burned onto a bootable CD, to boot the UNIX/Linux computer. Select "Ux Image Agent Restore."



Fig. 64 - Ux Image Agent Restore CD boot screen.

2. Read the License Agreement and use the “tab” button to move the cursor to the "Yes, I Agree to the License Agreement." Hit the “spacebar” to Choose, then use the “tab” button to move the cursor to continue.

3. The system will then go to a log in screen, wait up to 15 seconds, and the system will automatically log you in.

4. Once the UNIX/Linux computer is booted to the BMR CD, a main screen terminal window helps in verifying the computer configuration. As BMR is mainly used to restore image data, most of the other UltraBac Ux Agent options, like Ux Agent (File-by-File) backup/restore and Ux Image Agent backup, will remain disabled.
    - To check the IP address information, use the "/sbin/ifconfig" command.
    - To check the "UxAgent" daemon status, type <rcUxAgent status>.
    - The default password for the root account of the BMR booted OS is "UxAgentBMR."
5. Check the IP address assigned and whether the Ux Agent service is running on the UNIX/Linux computer by typing <ifconfig>.

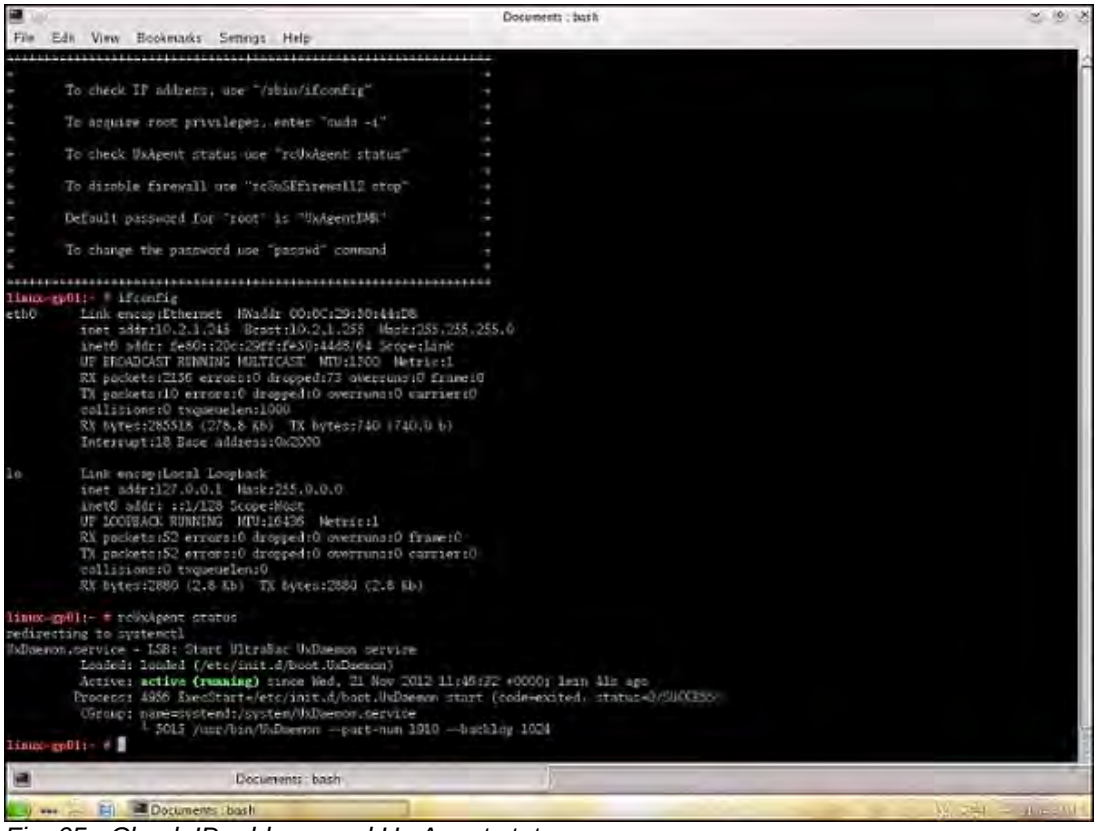


Fig. 65 - Check IP address and Ux Agent status.

6. From the Windows machine where UltraBac is installed, select the restore storage device where the UNIX/Linux computer backup to be restored is saved.

NOTE: Before beginning the restore, select the restore storage device. For additional information on selecting the restore storage device, pease visit the "**Restore Basics**" section of the User Manual:

UltraBac User Manual: Restore Basics

7. Launch the Restore Wizard by selecting the Restore tab, and selecting "Media."

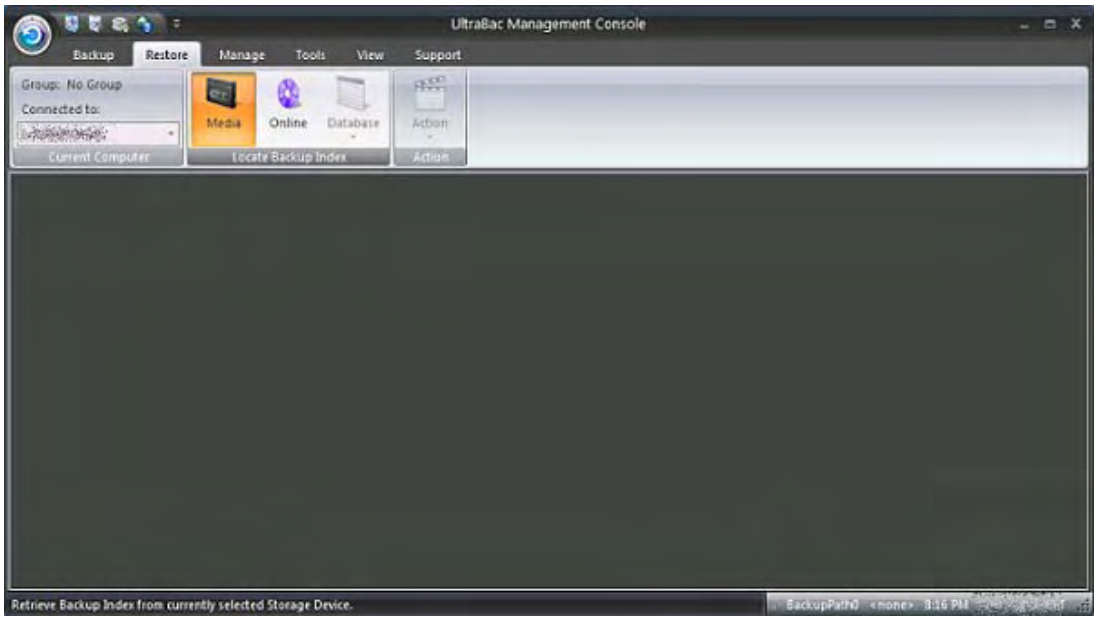


Fig. 66 - Launch Restore Wizard.

8. Select and load the backup index for restore.

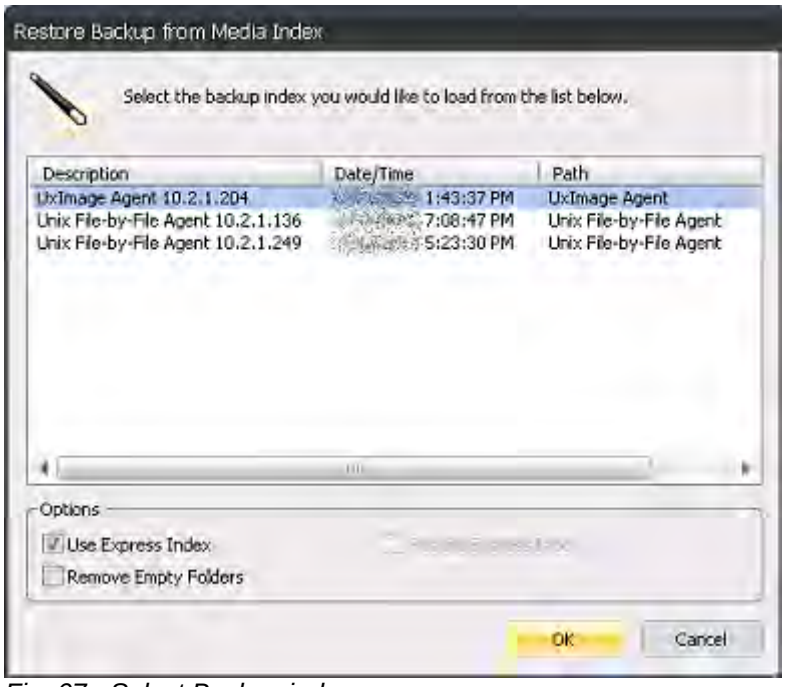


Fig. 67 - Select Backup index.

9. Select the disks/partitions you wish to restore.

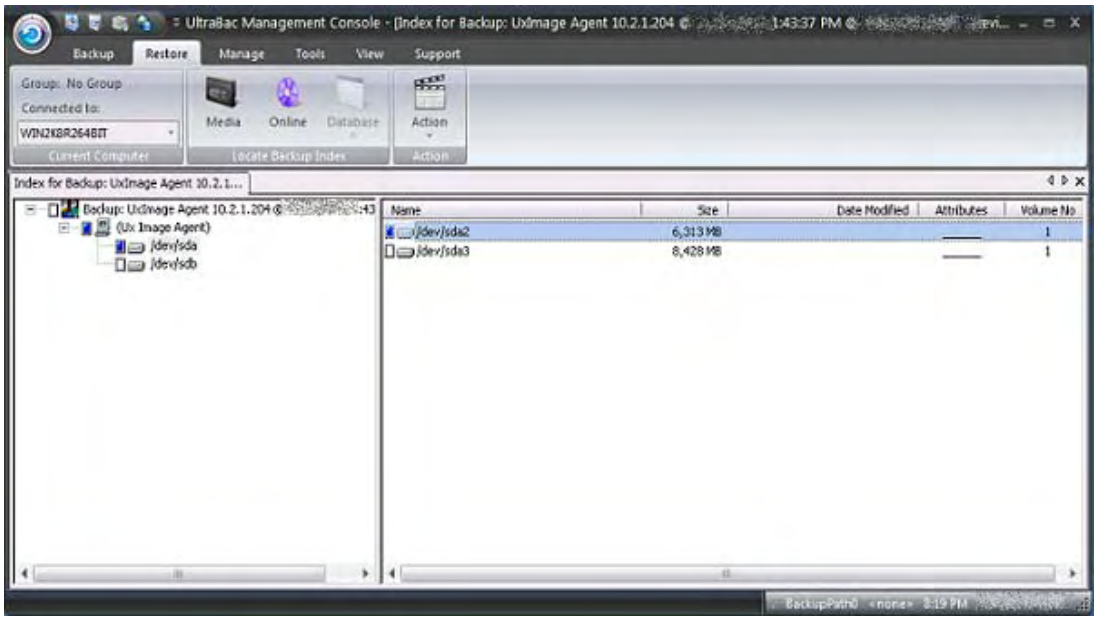


Fig. 68 - Select disks/partitions for restore.

NOTE: If the restore is being performed to a new hard disk, a "Restore MBR"/"Restore MBR Only" must be performed first, and then the logical volumes can be made active for restore.

If the MBR is not restored first on a new hard disk, when a user attempts to show the volume groups, it will return the message "No volume groups found."

10. Click "Action" and select "Restore this Backup."

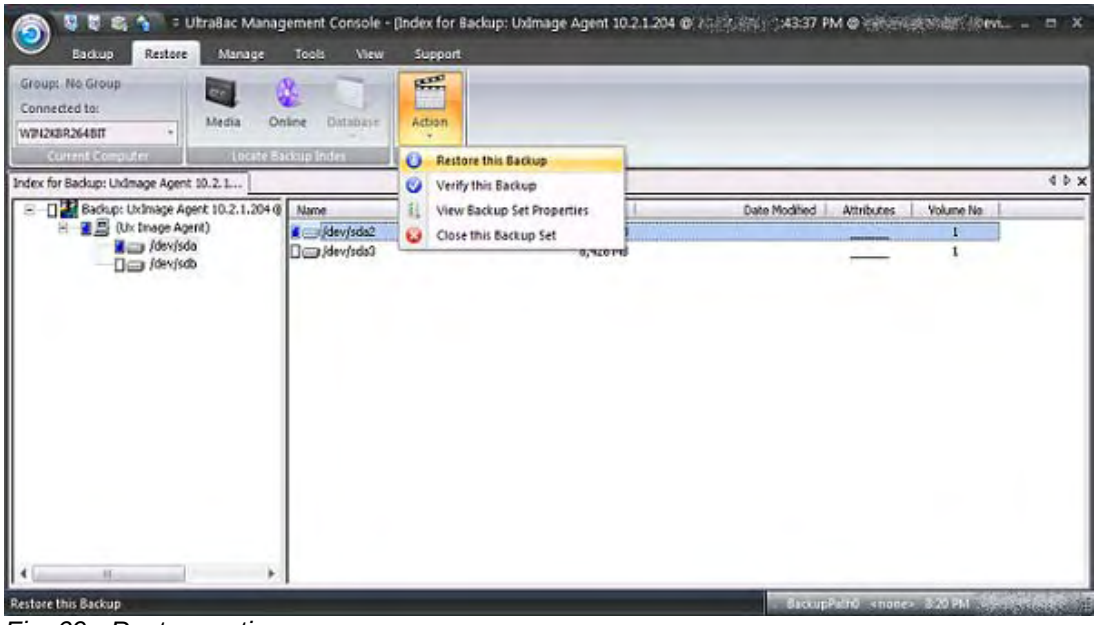


Fig. 69 - Restore action.

11. Fill in the correct IP address, username, and password of the UNIX/Linux computer that is running in BMR mode. Restoring an image requires root privileges. Select the desired option and click "Next."

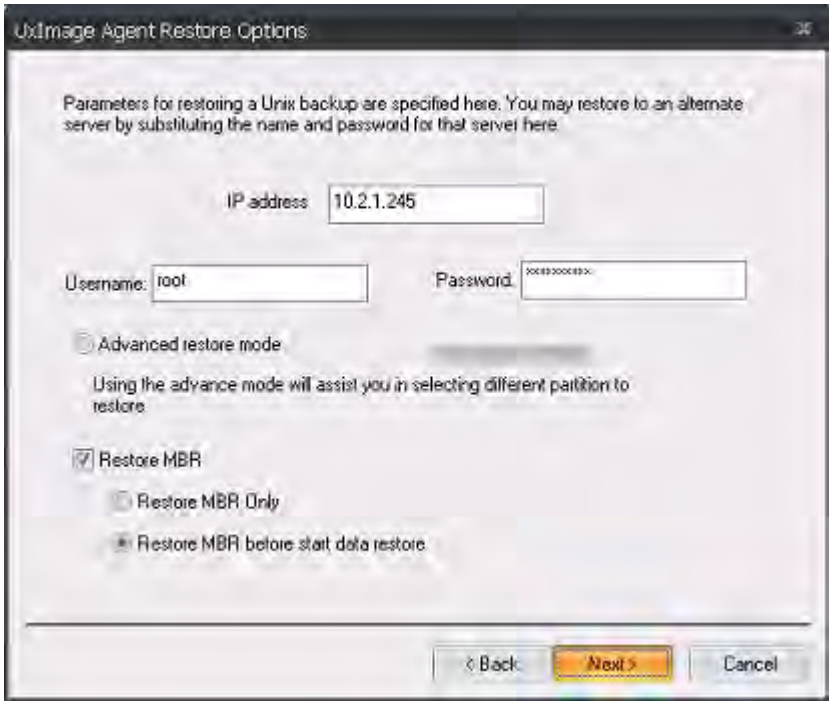


Fig. 70 - UxImage Agent Restore Options "BMR."

12. Click "Restore."

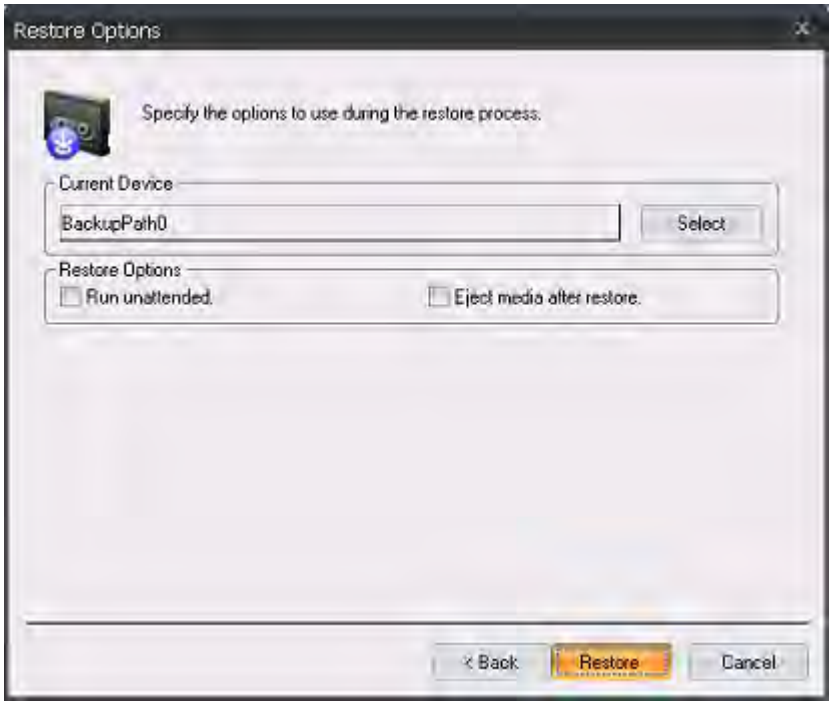


Fig. 71 - Click "Restore."

13. An UltraBac Progress window will be displayed showing the status of the restore process.

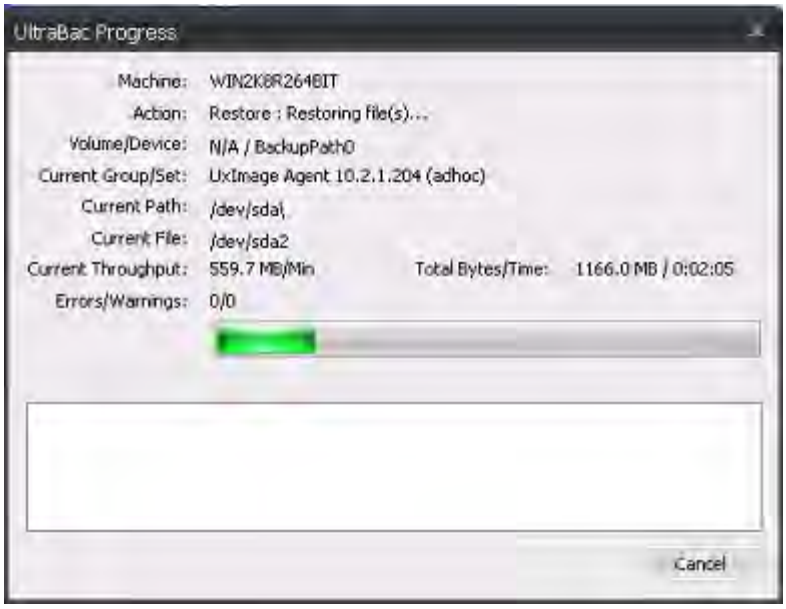


Fig. 72 - Restore progress.

14. After completion of the restore process you will see a message saying "Operation complete."

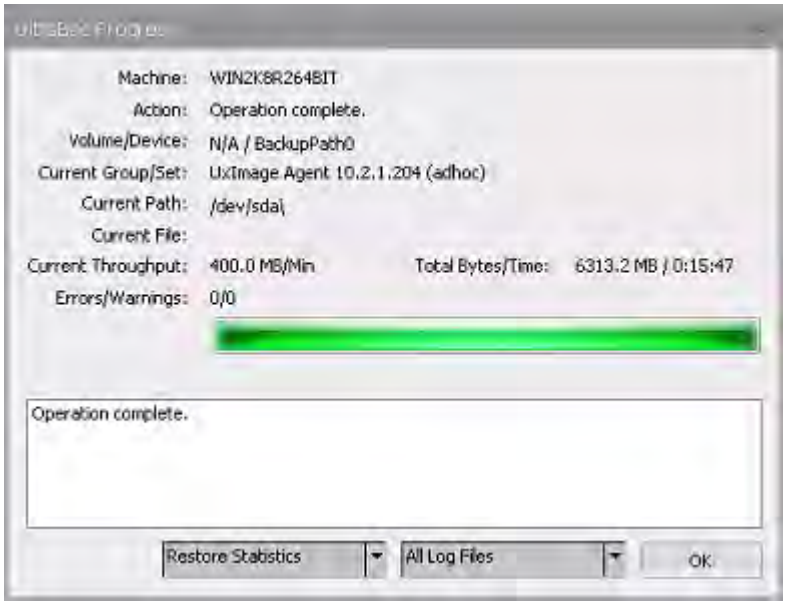


Fig. 73 - Operation complete.

15. Once the restore operation is complete, remove the BMR CD from the UNIX/Linux computer and reboot the computer.

Centralized Management

Centralized Management allows the user to easily manage their entire backup solution from one centralized location. This feature allows backup administrators to easily tell if a backup contained any warning or errors, without having to manually go through each backup log. It also gives an overview of backups that are currently in process and backups scheduled in the future.

NOTE: You must set up UltraBac to use a database, please see:

UltraBac User Manual: Configuring UltraBac Database

Once connected to a database, a new tab will appear in the ribbon.



Fig. 1 - Centralized Management ribbon

Configuration Options

Syncing of Managed Machines

1. Select the Manage tab, and click "General" / "User Interface."

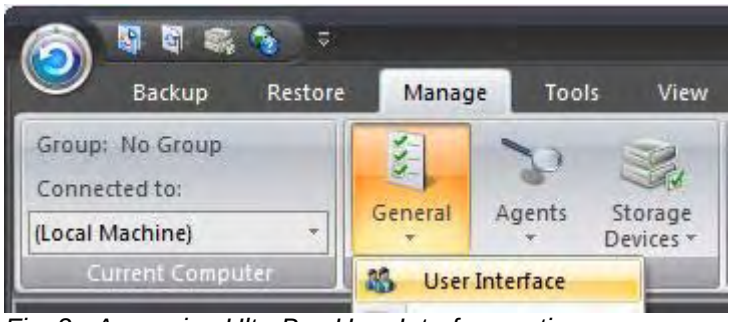


Fig. 2 - Accessing UltraBac User Interface options.

2. Deselect "Sync between Managed Machines and the UltraBac Database list."

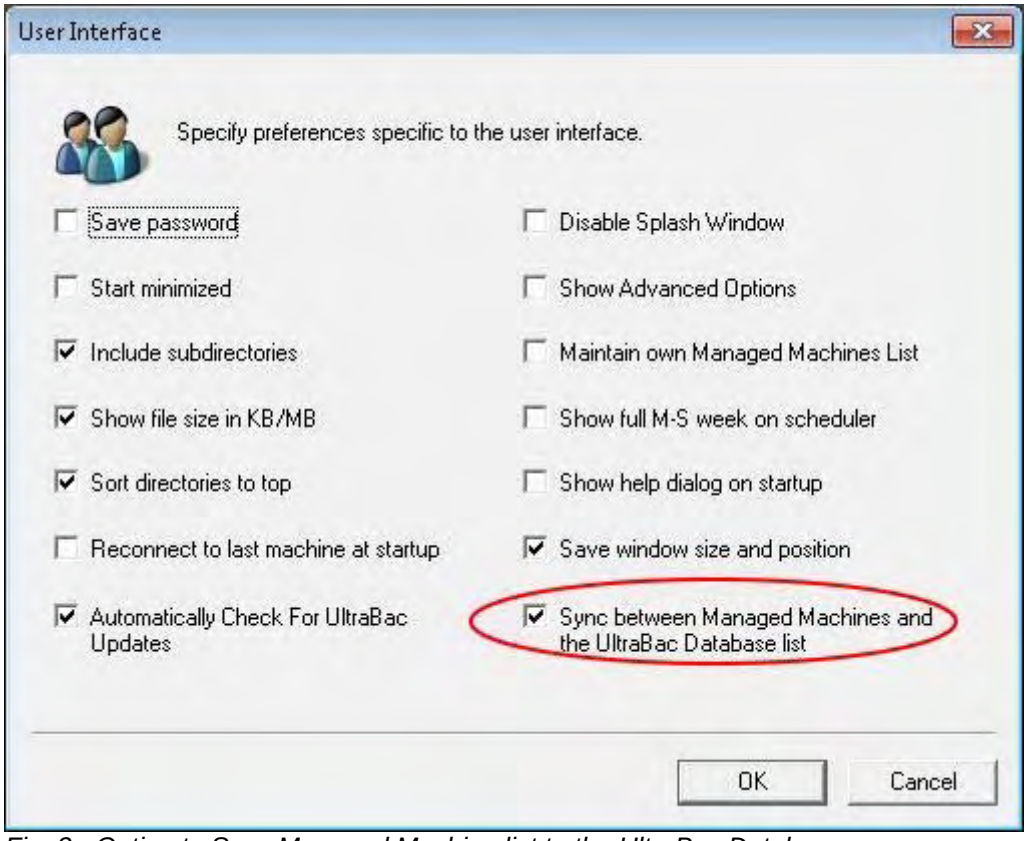


Fig. 3 - Option to Sync Managed Machine list to the UltraBac Database.

Display Settings

Within Centralized Management, you have the ability to specify the refresh rate, cutoff times for past and future jobs, the number of minutes without contact before considering a machine offline, and how many completed and future jobs to display.

1. Select the Centralized Management tab and click "Options."



Fig. 4 - Centralized Management Options.

Using Centralized Management

Overview

From the Overview tab you can see total "Jobs in Progress," "Jobs with Issues," "Pending Jobs," "Completed Jobs," as well as "Offline Machines."

If it is the first time a job is being run, time remaining will show up as "N/A." Subsequent backups will report the time based on previous backup times.

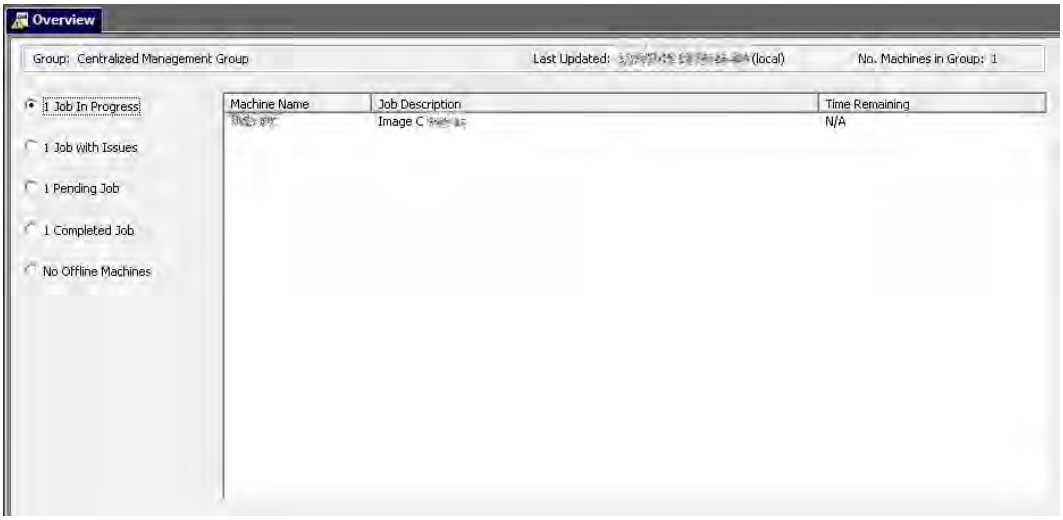


Fig. 5 - Jobs in Progress.

If there are any jobs with issues, you can right click on the job in question and select "View Log." This will open the log in a new tab.



Fig. 6 - Jobs with Issues.

If it is the first time a job is being run, time remaining will show up as "N/A." Subsequent backups will report the time based on previous backup times.



Fig. 7 - Pending Jobs.

Completed Jobs will show all jobs including those with issues and, as with "Jobs with Issues," you can right click on a completed job and select "View Log" for the backup in question.

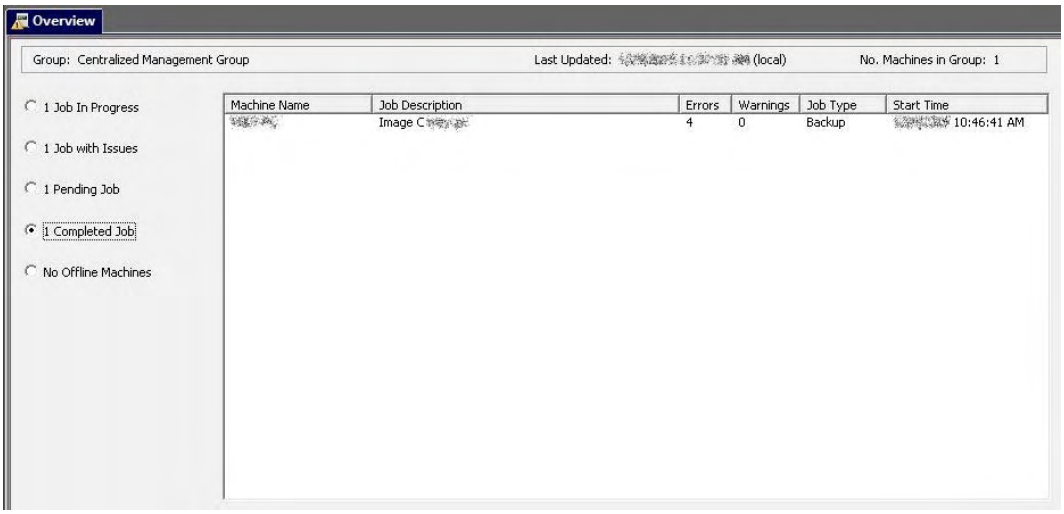


Fig. 8 - Completed Jobs.

Offline Machines will list the server name and the last time it checked in.



Fig. 9 - Offline Machines.

Machine View

The list is sorted based on Managed Group name and then the servers within each group. A server can be part of multiple groups.

<Group 1>
- <Server 1>
- <Server 2>
- <Server 3>
- <Server 4>
- <Server 5>

<Group 2>
- <Server 5>
- <Server 6>
- <Server 7>
- <Server 8>
- <Server 9>

The list is also color coded.

Blue	future job
Green	currently running
Red	completed with errors
Black	completed without errors

Selecting currently running or future job will list details about the job including: server name the backup will be run on; scheduled file name; start time; and, if available, an estimated run time.



Fig. 10 - Machine View of first job run.

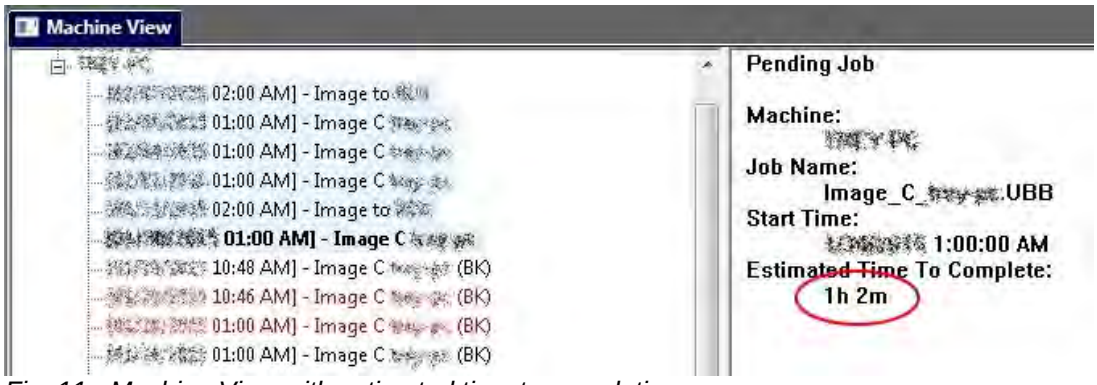


Fig. 11 - Machine View with estimated time to completion.

If the job has finished running you will see the backup log in the right pane.

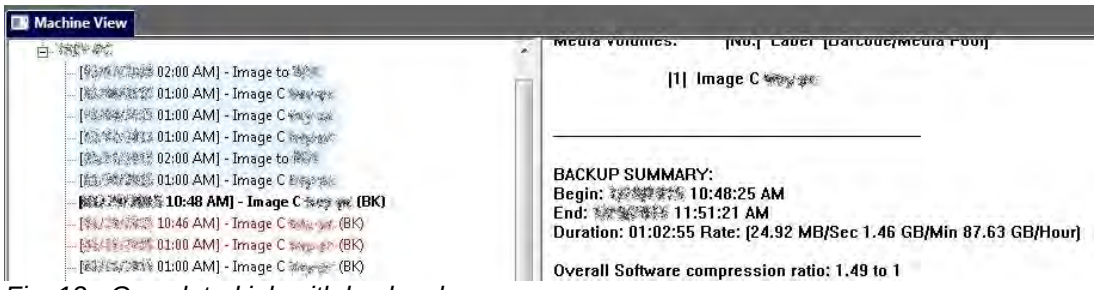


Fig. 12 - Completed job with backup log.

Generating Reports

The reports will contain a summary of the jobs that have been run between the report frequency. If a report is created to run every Monday, the report will contain a summary of all backups since the previous report was run.

1. To create a new report click "Centralized Management" / "Reports" / "Create New."
2. Enter a "Report Name."
3. Select the servers to be contained in the report.
    - All Machines – Report will contain all computers in the database.
    - Machines – Report will only contain the computer(s) that are selected.
    - Groups – Report will contain all computers in the group(s) that are selected.

4. Click "Report Frequency" to open UltraBac Scheduler to set the report start time, date, and event frequency.
5. Check "Email Reports Using SMTP Account." to send the report as an attachment to the user(s) and/or group(s) specified in the distribution list..

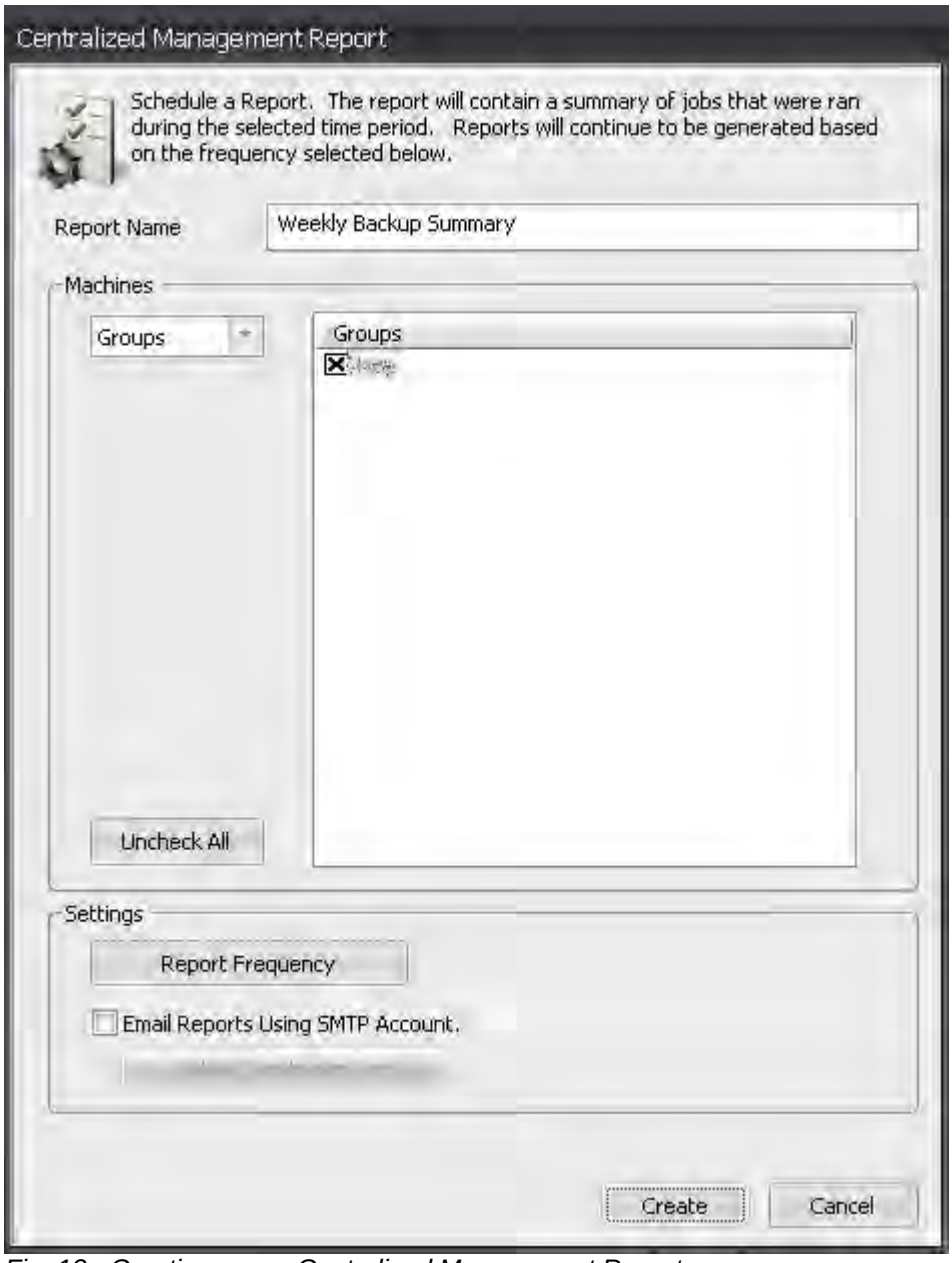


Fig. 13 - Creating a new Centralized Management Report.

UltraBac Media Builder

UltraBac Media Builder is a disk creation utility for generating an UltraBac Disaster Recovery (UBDR) Gold CD or USB key. UltraBac Media Builder is automatically installed when you install UltraBac. There are two different versions of UBDR Gold. Which one you use depends on which operating system you need to restore; both versions support BIOS and UEFI.

UltraBac Media Builder requires that either the Windows Automated Installation Kit (AIK) or the Assessment and Deployment Kit (ADK) be installed. If Windows AIK or ADK is not installed on your computer, UltraBac Media Builder will detect that it is not installed and will prompt the installation by providing a link to its download location. Windows AIK/ADK can be installed on a machine with the Windows 7 or later operating system. Windows AIK/ADK must be installed using an account with Administrator permissions. The machine used for UltraBac Media Builder to generate the UBDR Gold ISO must have a CD/DVD burner in order to burn the ISOs to CD/DVD.

- If you need to restore Windows Vista / 7, or Windows Server 2008 / 2008 R2 then it will require the installation of the Windows Automated Installation Kit (AIK) and use WinPE 3.1. Please see "**UBDR with WinPE 3.1**."
- If you need to restore Windows 8 / 8.1 or Windows Server 2012 / 2012 R2 then it will require the installation of the Assessment and Deployment toolkit (ADK 8.0 / 8.1) and use WinPE 4.0 / 5.0. Please see "**UBDR with WinPE 4.0 / 5.0**."
- If you need to restore Windows 10 then it will require the installation of the Assessment and Deployment toolkit (ADK 10) and use WinPE 10.0. Please see "**UBDR with WinPE 10.0**."

NOTE: You must have a UBDR Gold license in order to use UltraBac Media Builder. An UltraBac license check is performed and, if an evaluation license is detected, the UltraBac Media Builder will not run.

10

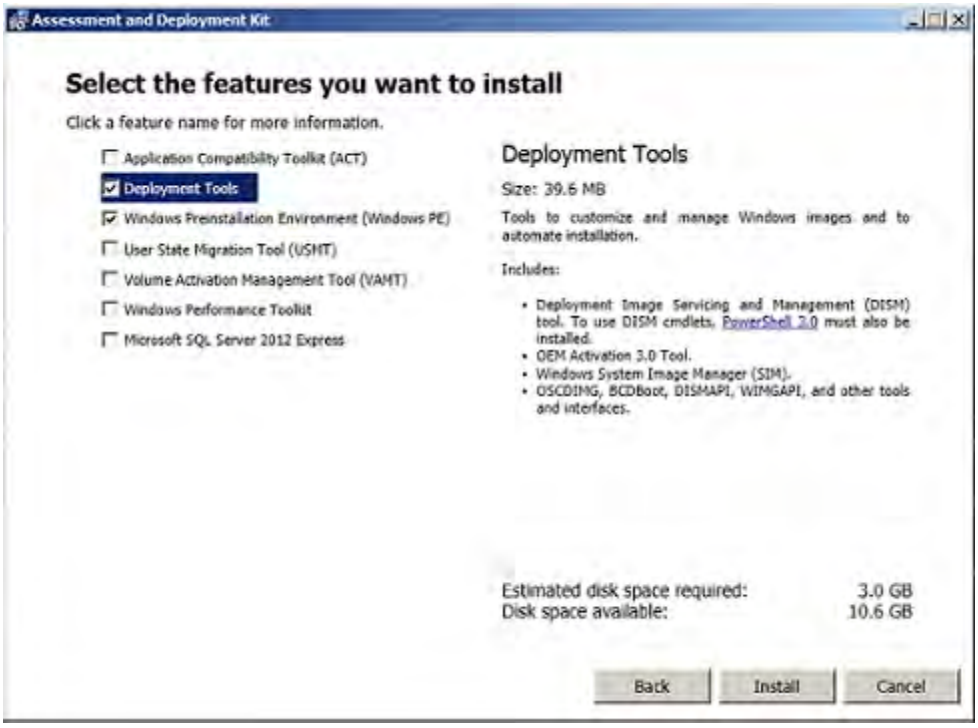
NOTE: If you need to build UBDR for a processor architecture other than the current OS you must select copy additional binaries during the UltraBac installation process.

UBDR with WinPE 3.1

NOTE: Windows AIK must already be installed. You can download it here and the required SP1 supplement here. There is no installer for the supplement, simply mount the ISO and copy the contents (overwriting existing files) in the Windows AIK directory. Default location is "C:\Program Files\Windows AIK\Tools\PETools"

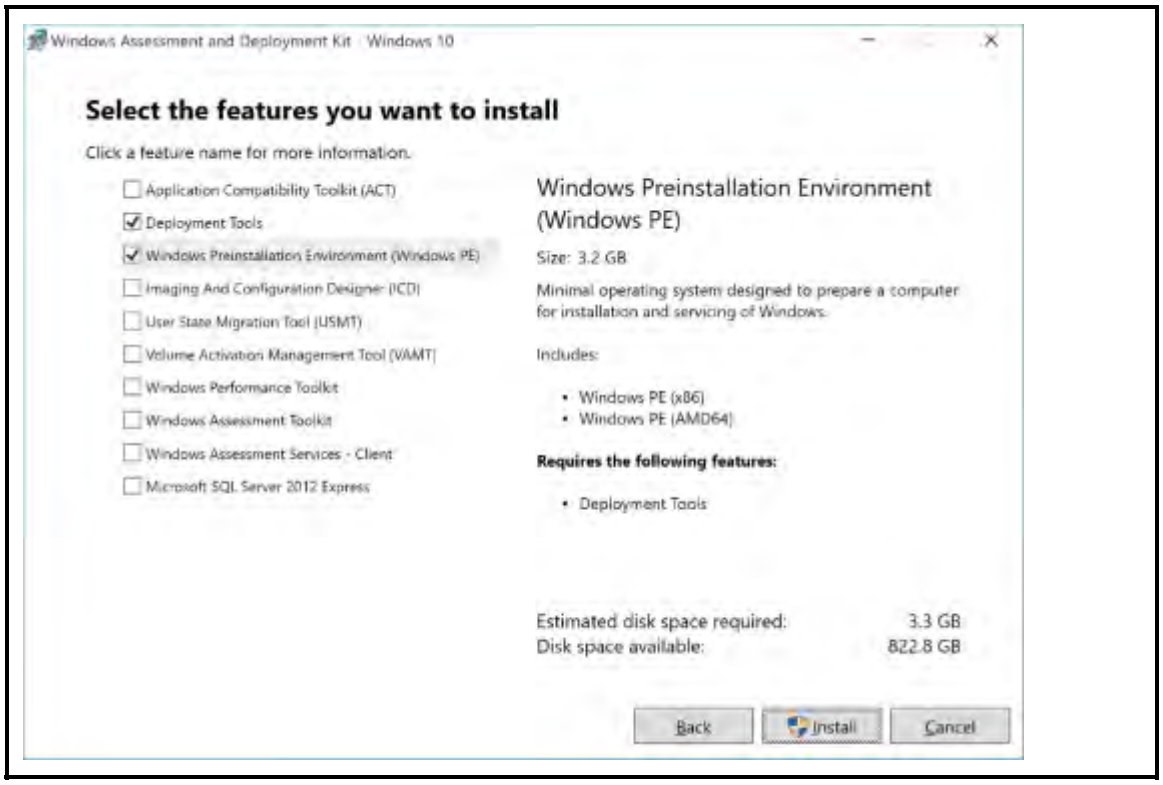
UBDR with WinPE 4.0 / 5.0

NOTE: Either Windows ADK8 or ADK8.1 must already be installed. You can download the latest version of ADK here. You only need to select the "Windows Preinstallation Environment (Windows PE)" feature for installation. This will also select the "Deployment Tools" feature



UBDR with WinPE 10.0

NOTE: Either Windows ADK10 must already be installed. You can download the latest version of ADK here. You only need to select the "Windows Preinstallation Environment (Windows PE)" feature for installation. This will also select the "Deployment Tools" feature



Building UBDR

1. To open UltraBac's Media Builder, click "Start,"/"All Programs,"/"UltraBac,"/"UltraBac Media Builder for UBDR" as seen in Figure 1.

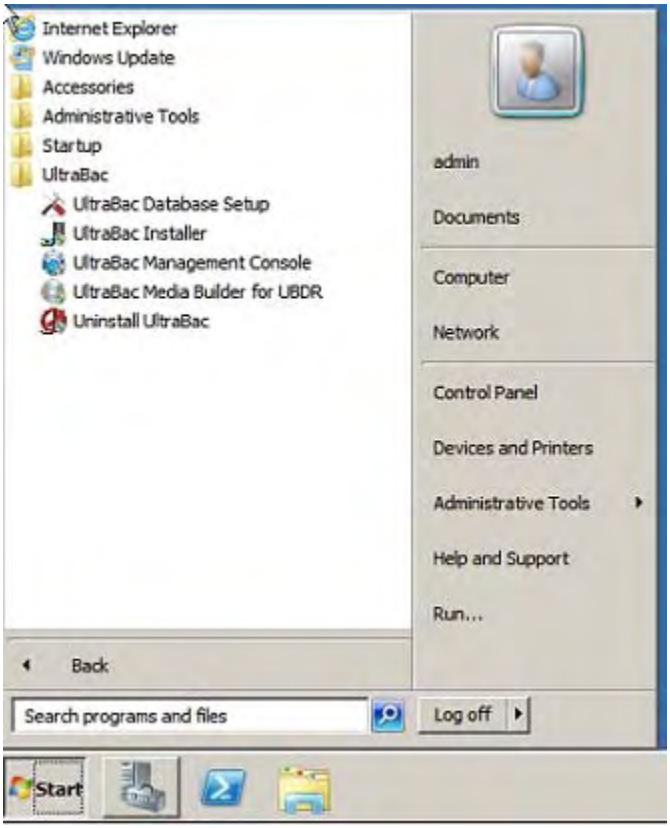


Fig. 1 - Click "UltraBac Media Builder for UBDR."

2. The "UltraBac Media Builder for UBDR" window will open as seen in Figure 2.

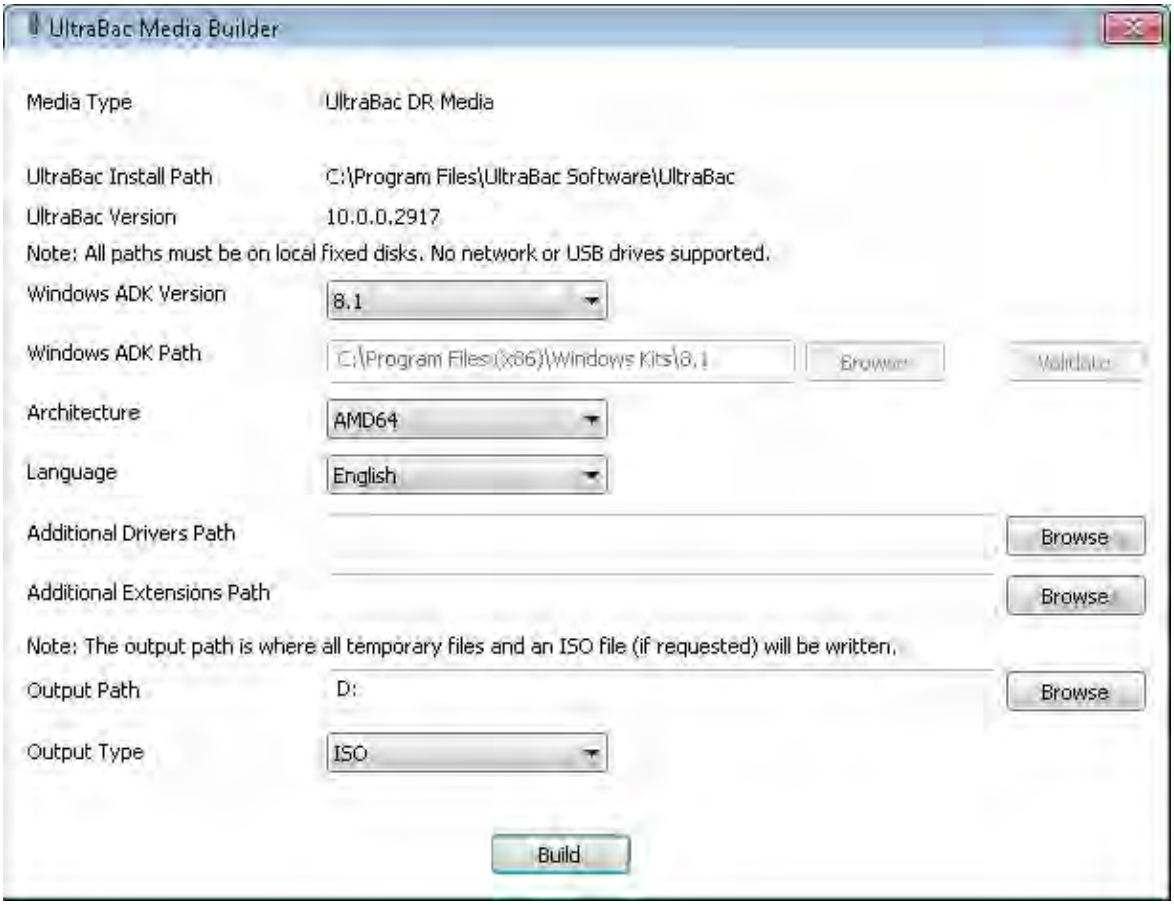
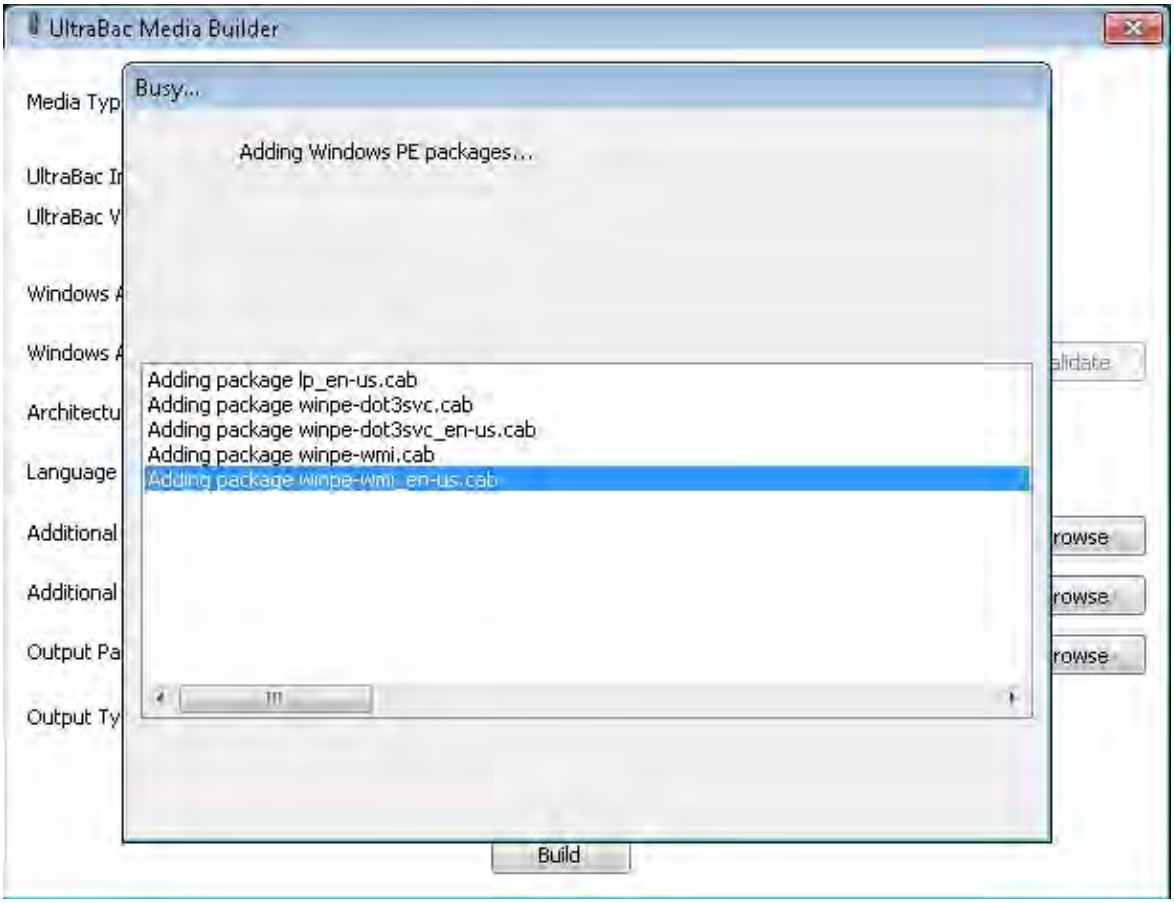


Fig. 2 - UltraBac Media Builder.

3. If you have both AIK and ADK installed, change the "Windows ADK/AIK Version" to "7.0."
    i. If UltraBac Media Builder is not detecting that AIK is installed choose "Custom."
    ii. Change "Windows ADK/AIK Path" to point to the directory where it is installed.
4. Choose the Architecture of the OS you plan to restore.
5. If you have a non-English build of UltraBac installed you may chose a Language other than English.
6. To install additional drivers for network cards, SCSI / SAS / RAID controllers, place them in a single parent directory and browse to the "Additional Drivers Path." Otherwise leave this field blank.
7. To install additional third party applications, place them in a single parent directory and browse to the "Additional Extensions Path." Otherwise leave this field blank. To see how to organize an extension directory see UBQ000???: Creating UltraBac Media Builder Extensions.
8. To change the Output Path from "%HOMEPATH%\Documents\MediaBuiler," click "Browse" and navigate to a new output directory.
9. To create UBDR on a USB drive, change "Output Type" from ISO to USB. It is not necessary to insert a USB drive until prompted to do so.
10. Click "Build" and a progress window will appear displaying the current action.



-

Fig. 3 - Creating UBDR.

11. Once building is complete, a prompt to copy any additional files to the media will appear. Clicking "Yes" will open Windows Explorer to the mounted WIM folder. Once the files are copied close the Explorer window and click "OK" to continue building UBDR.

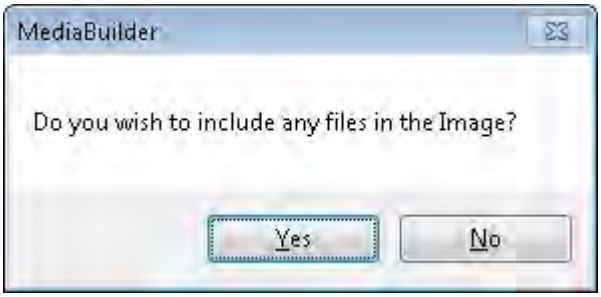


Fig. 4 - Include additional files.

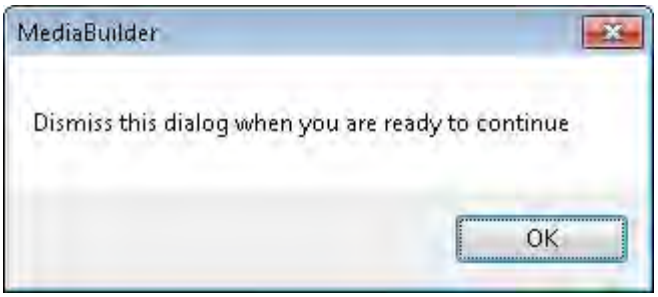


Fig. 5 - After adding additional files.

12. The ISO will now be created, unless USB was selected as the "Output Type."



Fig. 6 - ISO created successfully.

NOTE: When choosing USB, the USB flash disk will be erased and formatted. All contents will be lost.

13. Make sure that the USB drive you wish to use is not plugged into the system. Then click "OK" to scan the drives on the system.

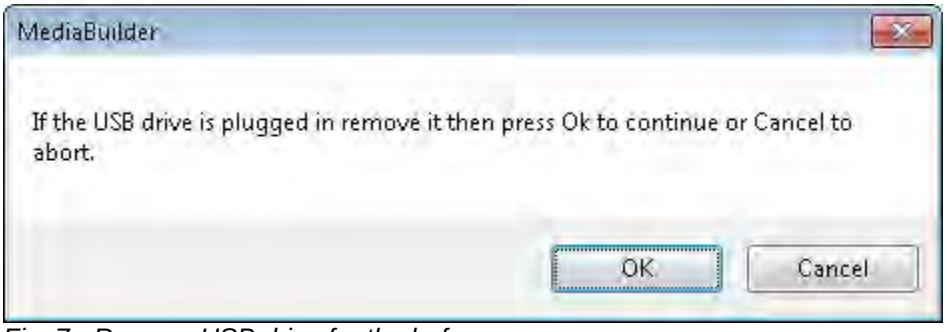


Fig. 7 - Remove USB drive for the before scan.

14. Insert the USB drive and click "OK" to scan the drives on the system. UltraBac will compare the differences between the two scans and use the newly found drive.

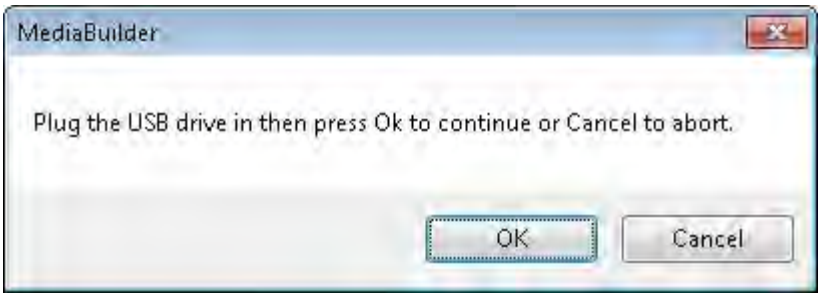


Fig. 8 - Insert USB drive for the after scan.

15. If the drive found is the one you wish to use, click "Yes" to wipe the drive and continue.



Fig. 9 - USB drive detected.

16. After the wipe, partition creation, formatting, and files are copied.

Fig. 10 - UBDR successfully created on USB drive.

Knowledge Base

UBQ000001: Command Line Backup/Restore

UBQ ID Number: UBQ000001
Last Modified: 2009-10-26

Summary:

This document details the functionality of UltraBac v9.x's 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, to chain backup jobs, or to have another application kick off your backup. This can also be an effective method of troubleshooting.

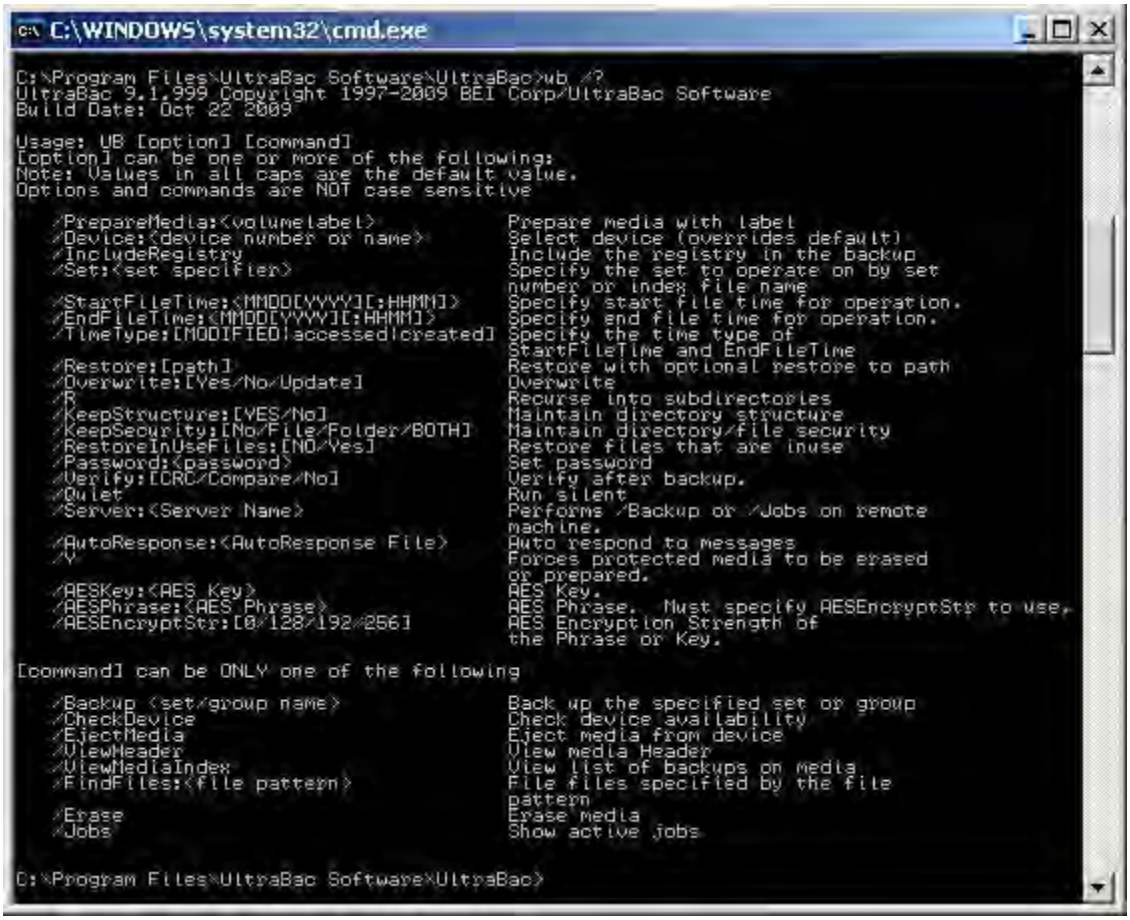


Fig. 1 - Command line options.

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 back up 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.

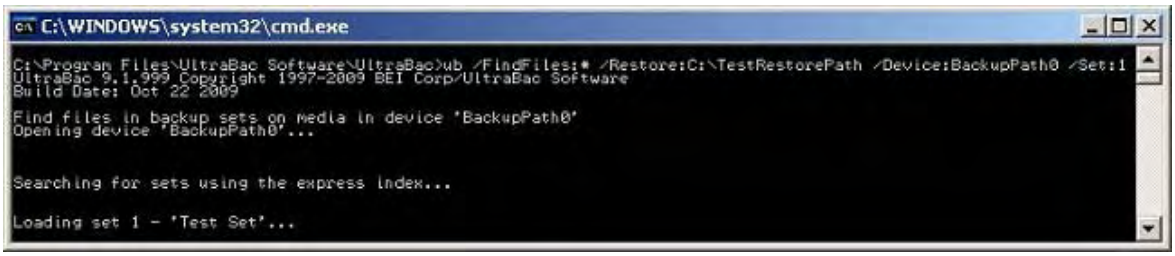


Fig. 3 - Command line results (restore).

View Media Index

This command will allow you to check the media to see which sets it holds in the index.

Example:

C:\Programs\UltraBac Software\UltraBac>ub.exe /ViewMediaIndex /Device:BackupPath0

The command line above instructs UltraBac to show the media index held in BackupPath0.

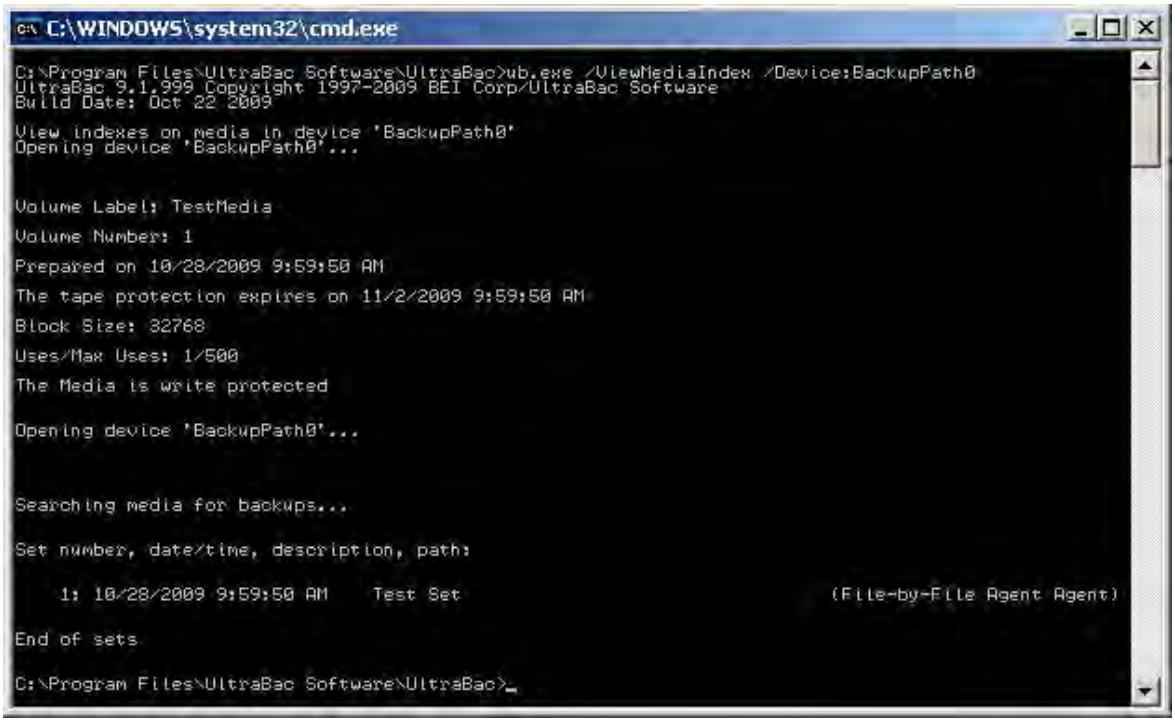


Fig. 4 - Checking Media.

Eject Media

This command will allow you to eject the media thru the command line.

Example:

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.

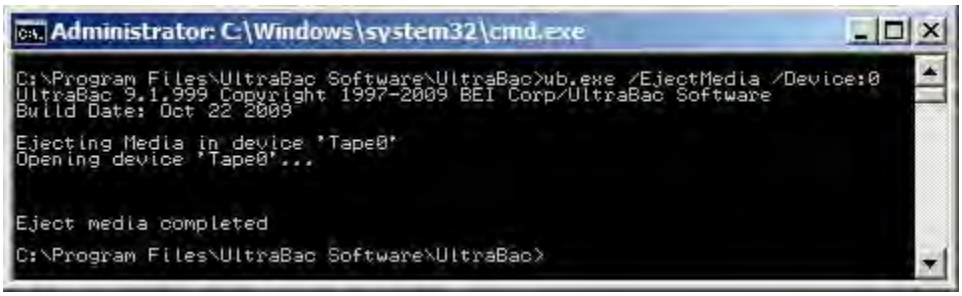


Fig. 5 - Ejecting media

View Header

This command will allow you to view the media header.

Example:

C:\Programs\UltraBac Software\UltraBac>ub.exe /ViewHeader /Device:BackupPath0

The command above tells UltraBac to view the media header of BackupPath0.

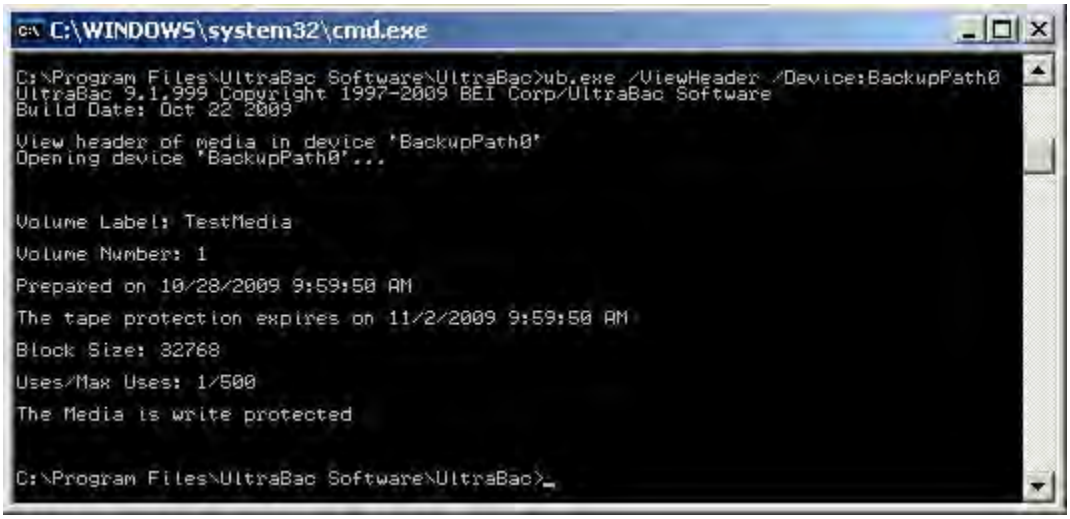


Fig. 6 - Viewing media header.

Shortcuts

The following shortcut commands are equal to typing the entire command. For example, "ub /bu" would be the same as "ub /backup."

/bu: = /backup:
/PM: = /preparemedia:
/D: = /device:

More Information:

See UltraBac User Manual: Command Line Functionality

UBQ000024: What is an Image Backup?

UBQ ID Number: UBQ000024
Last Modified: 2000-06-01

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 that 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 UltraBac User Manual: Image Disaster Recovery Agent
See UltraBac User Manual: UBDR Gold
See UltraBac User Manual: Static Mirror Image Backup
See UBQ000230: UBDR Advanced Tools and Utilities
See UBQ000060: Static Mirror Image Recovery

UBQ000041: Selecting a Storage Device

UBQ ID Number: UBQ000041
Last Modified: 2011-02-25

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."

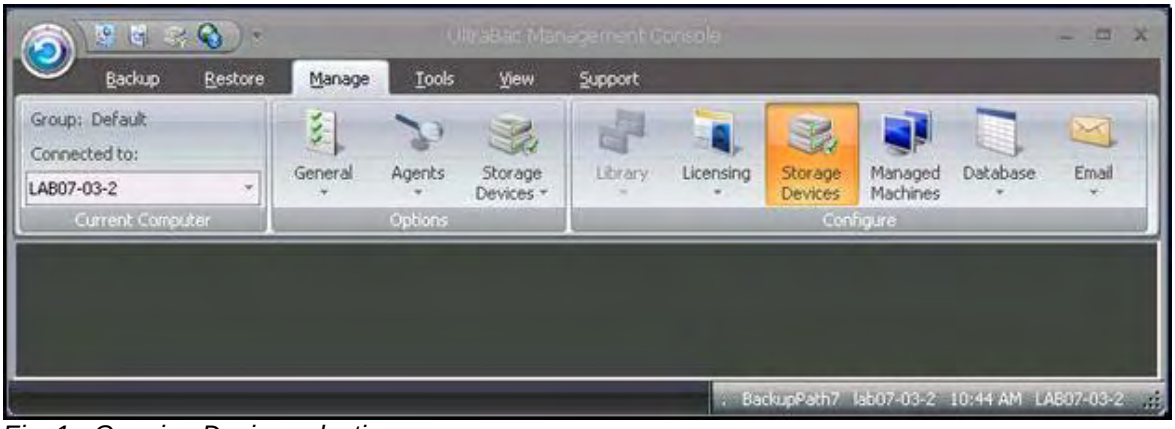


Fig. 1 - Opening Device selection screen.

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.

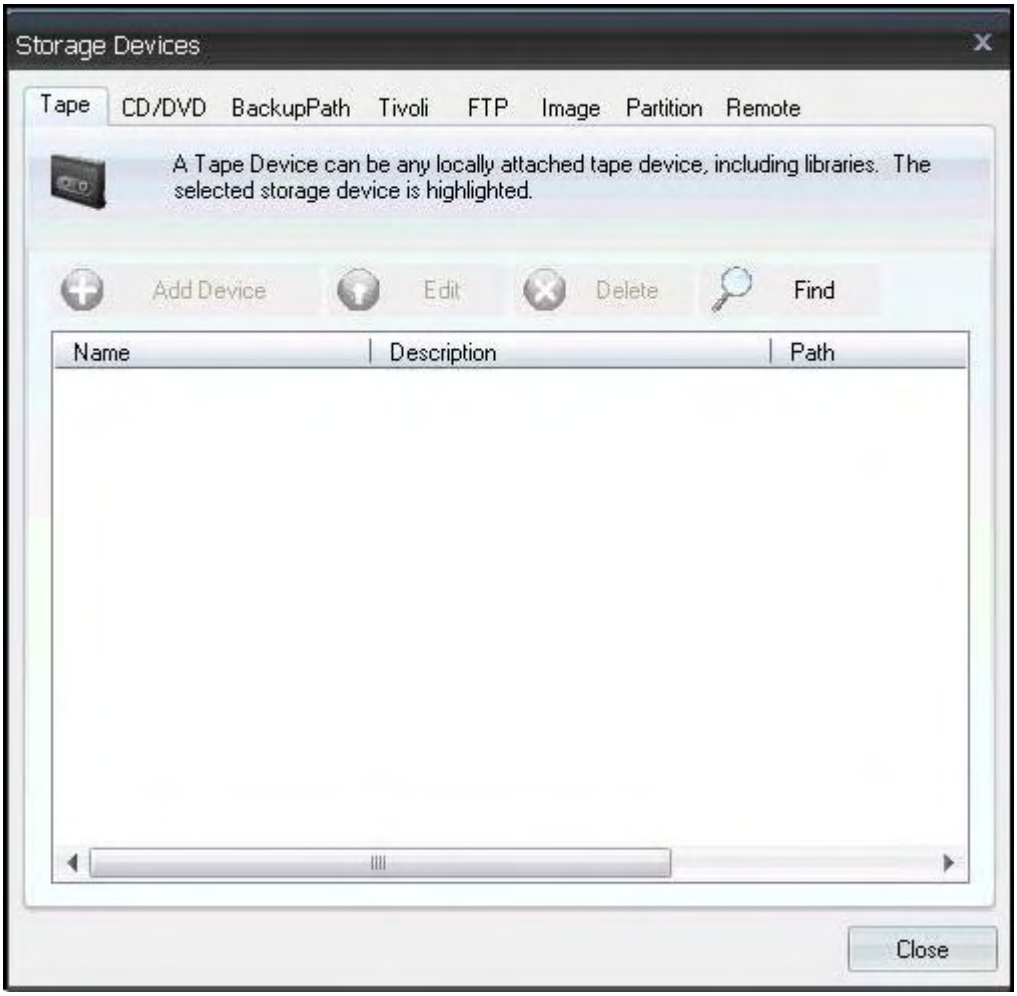


Fig. 2 - Storage device selection screen.

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 UltraBac User Manual: Storage Device Manager
See UBQ000049: Defining a Disk (disk-path) Storage Device
See UBQ000210: UltraBac Backup Output Files

UBQ000049: Defining a Disk (Backup Path) Storage Device

UBQ ID Number: UBQ000049
Last Modified: 2011-02-25

Summary:

This article details the necessary steps to create a "Backup Path" device.

Details:

Upon initial installation of UltraBac, there will be no defined disk paths. The maximum number of Backup Path devices allowed is (by default) 1000. Supported target disks include any disk path that can be written to by a Windows OS. 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.

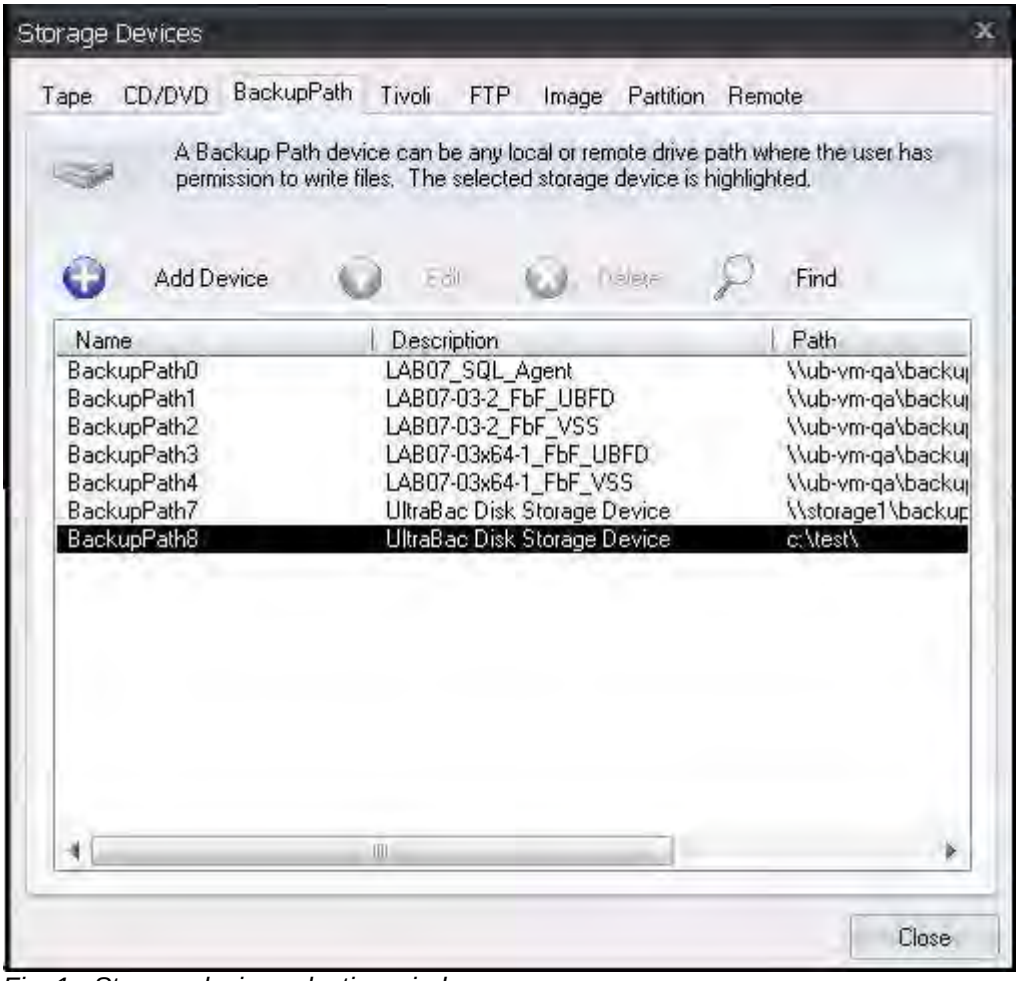


Fig. 1 - Storage device selection window.

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.

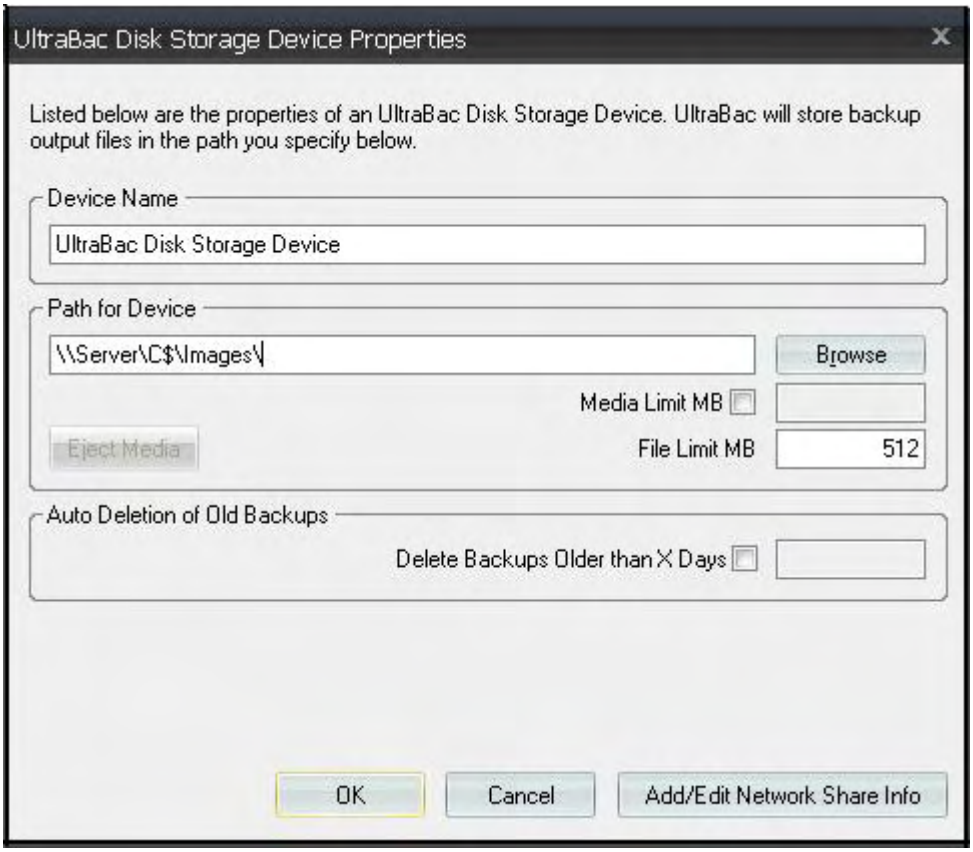


Fig. 2 - Specifying the backup target path.

When selecting the "Media Limit MB" 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 Backup Path device, and keep only an archive of the specified number of days.

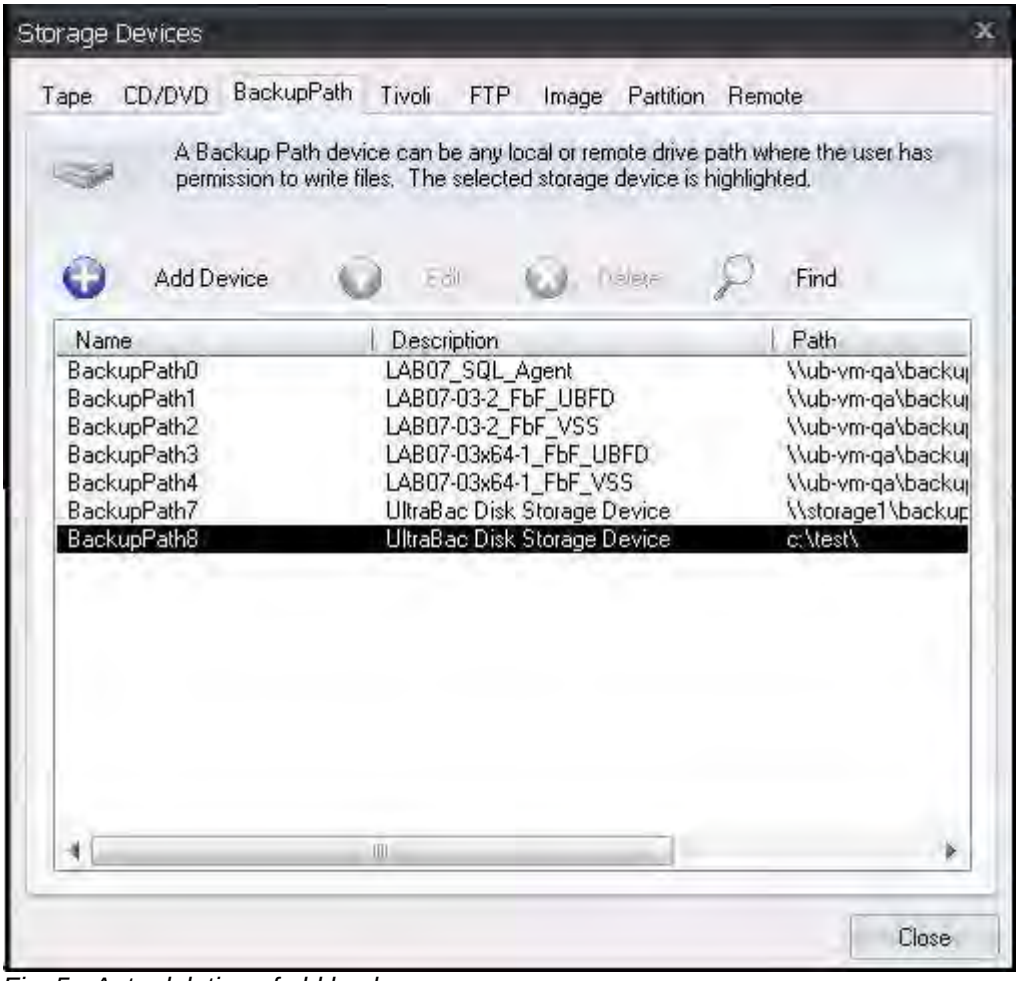


Fig. 5 - Auto deletion of old backups.

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 check box.
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 UltraBac User Manual: Storage Device Manager
See 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.
   I. Modify the SCSI BIOS to boot from the mirrored hard drive.
   II. Reboot (this must be an image of the system drive).
   III. Perform any other applicable restores.
   IV. Replace failed hard disk as soon as possible.

2. Replace failed hard drive with image hard drive (used for any failed drive).
   I. Power down, remove the failed hard drive, and substitute it with the image hard drive.
   II. Reboot.
   III. Perform any other applicable restores.
   IV. 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 UltraBac User Manual: Static Mirror Image Backup
See UBQ000024: What is an Image Backup?

UBQ000069: Troubleshooting SMTP

UBQ ID Number: UBQ000069
Last Modified: 2005-09-13

Summary:

UltraBac has the ability to use SMTP notification using any local / remote SMTP server.

Details:

The "From" and "To" e-mail 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 e-mail address in the "From" and "To" fields.

SMTP TROUBLESHOOTING SCRIPT

Use the following script to test SMTP. Type only the **bold** text:

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

Q. Why do I receive 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\TcpMaxDataRetransmissions

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 UltraBac User Manual: Scheduled Backup Options
See UBQ000162: Non-UltraBac Specific Registry Keys
http://support.microsoft.com/support/kb/articles/Q191/1/43.ASP

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 box (see Fig. 2).

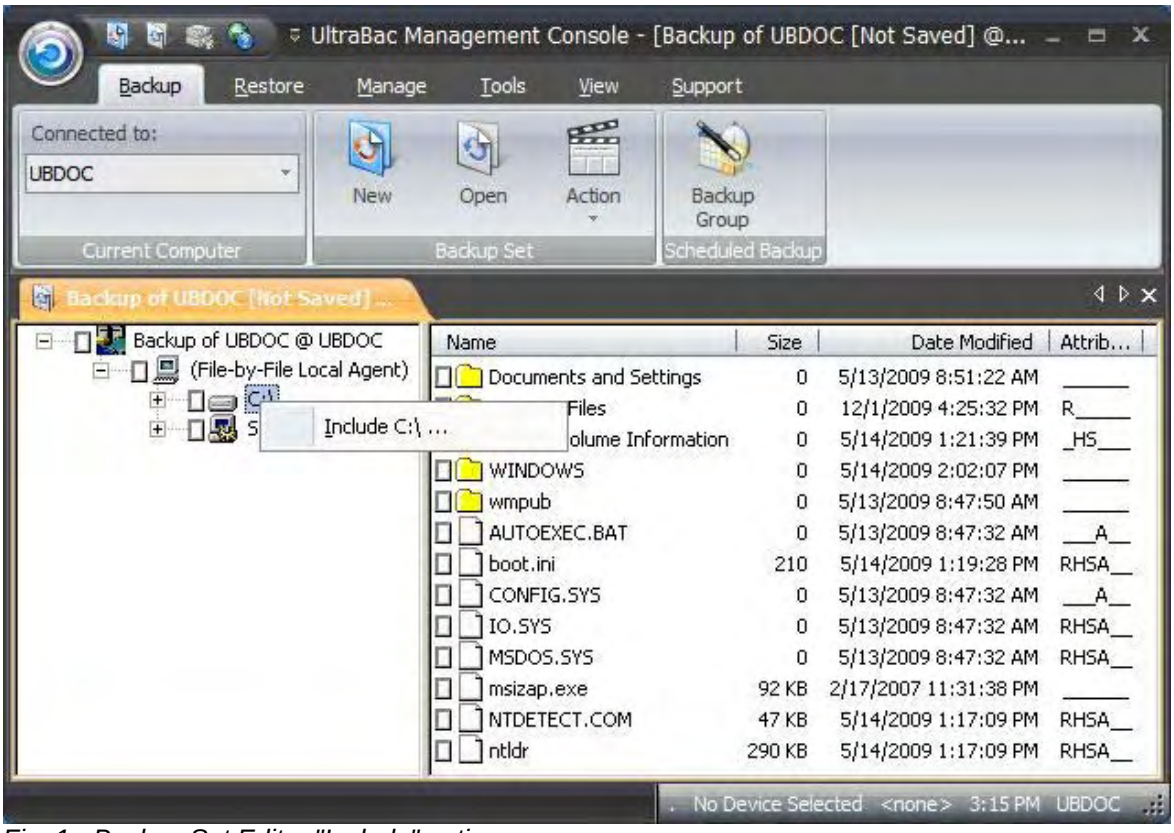


Fig. 1 - Backup Set Editor "Include" option.

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 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 "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 "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.

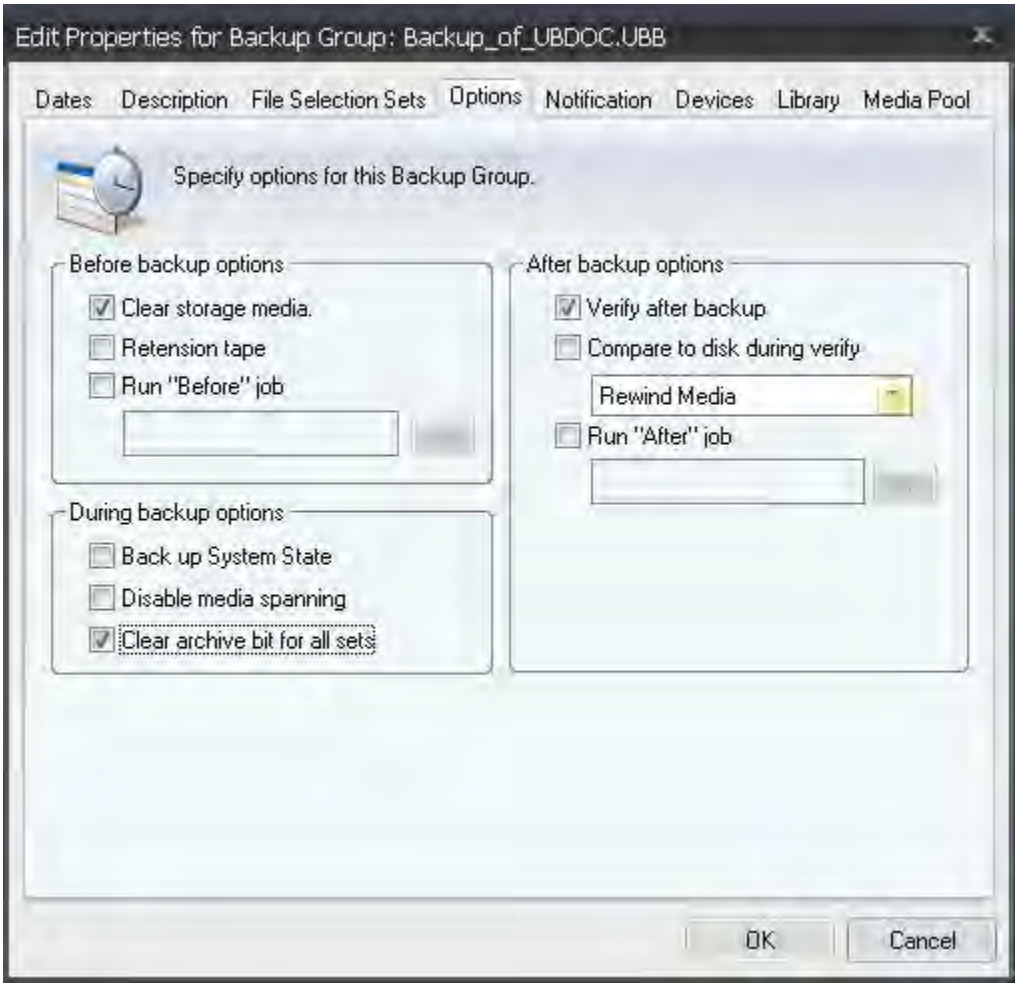


Fig. 3 - Backup Group Options, "Clear archive bit for all sets."

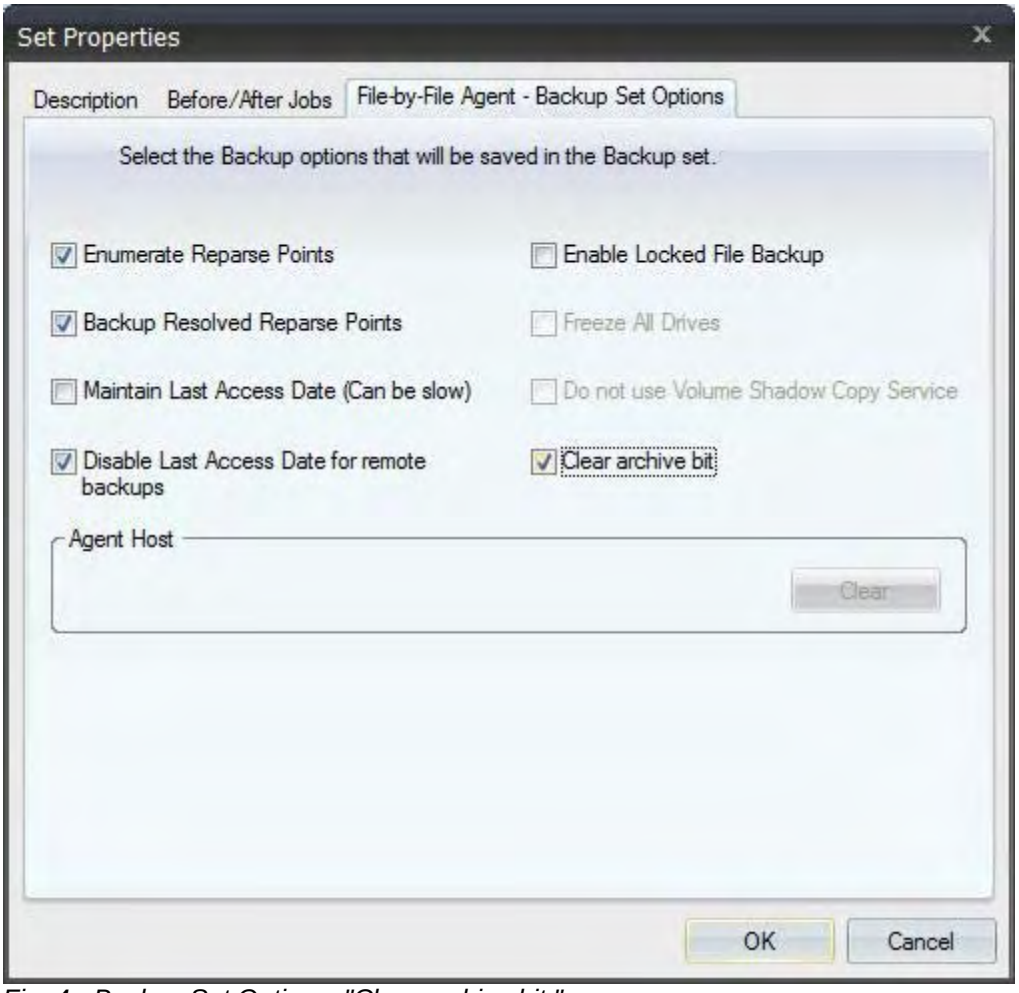


Fig. 4 - Backup Set Options, "Clear archive bit."

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.

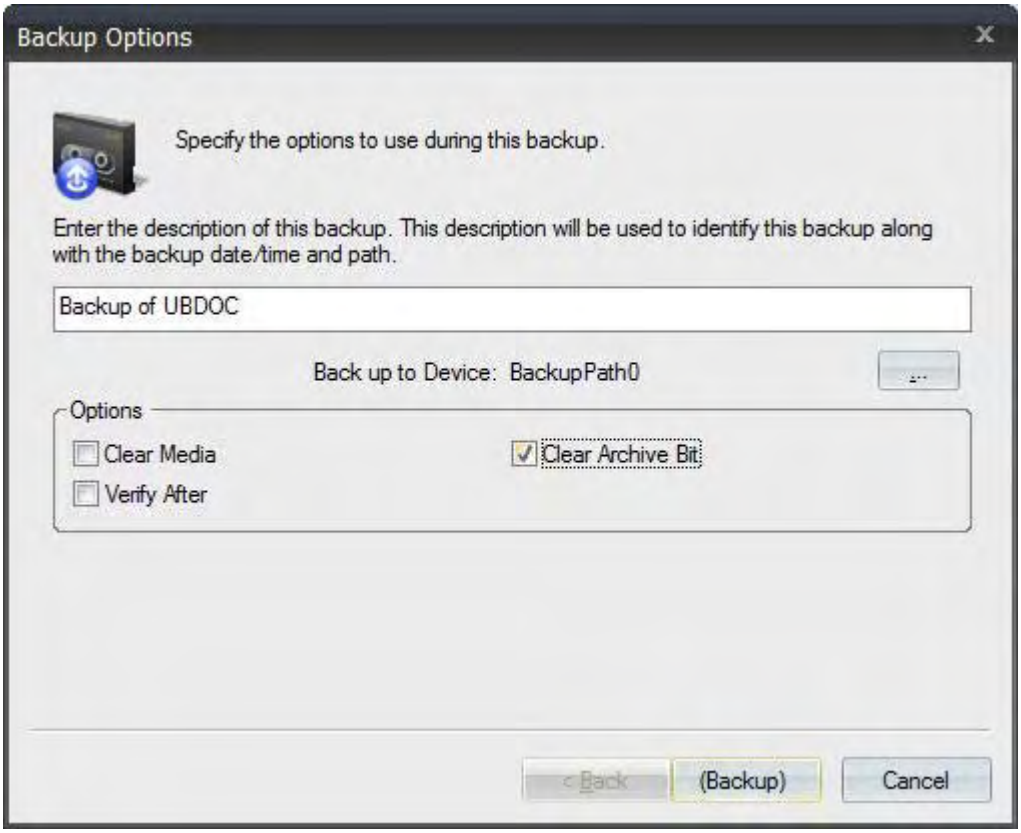


Fig. 5 - "Run Backup Now" Backup Options, "Clear archive bit."

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 and 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 UltraBac User Manual: Incremental/Differential Backups - Image Agent
See UltraBac 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 they generally indicate one of the following:

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 tapes after 30-50 passes? Based on our experience, after approximately 50 passes tapes can become unreliable. If a tape has defective segments, the drive will attempt to write a data block "NNN" a **set** number of times 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. 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 of 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 and 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 and 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 Windows backup applet works normally. Unfortunately, the only way to eliminate this as a problem is by examining each internal and external disk for its jumper settings.

For the reasons stated above, most controller manufacturers recommend that tape hardware not be placed on the same bus as the local hard drives, and that disk drive arrays should not share a controller with tape hardware.

Type of SCSI card

You will need to use a standard SCSI adaptor. SCSI Raid controllers can cause issues varying from intermittent tape hardware errors such as "bad data" and Cyclic Redundancy Check (CRC) errors to complete bus locks or bus resets. A bus reset may require a restart to get the tape device functionality returned to the system.

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 UBQ000092: Solving Typical SCSI Problems

UBQ000092: Solving Typical SCSI Problems

UBQ ID Number: UBQ000092
Last Modified: 2010-01-21

Summary:

Installing a SCSI based storage device drive with removable media often creates a problem that 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 usually supports one chain, 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, then plugged into each internal device, and is terminated at the last device. The external cable is round, connects to the outside plug on the controller card, and can come with three 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 appear to back up normally 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 and 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.

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 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 UltraBac User Manual: Installing UltraBac
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."

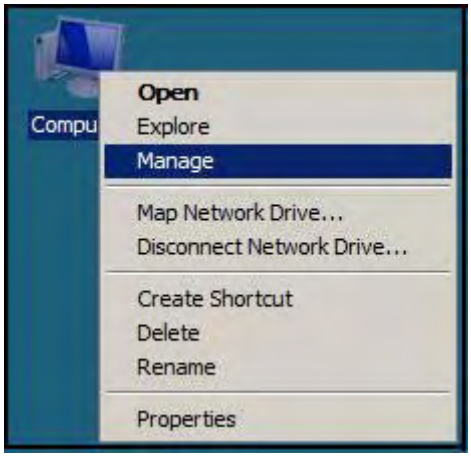


Fig. 1 - Opening the Server Manager Console.

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..."

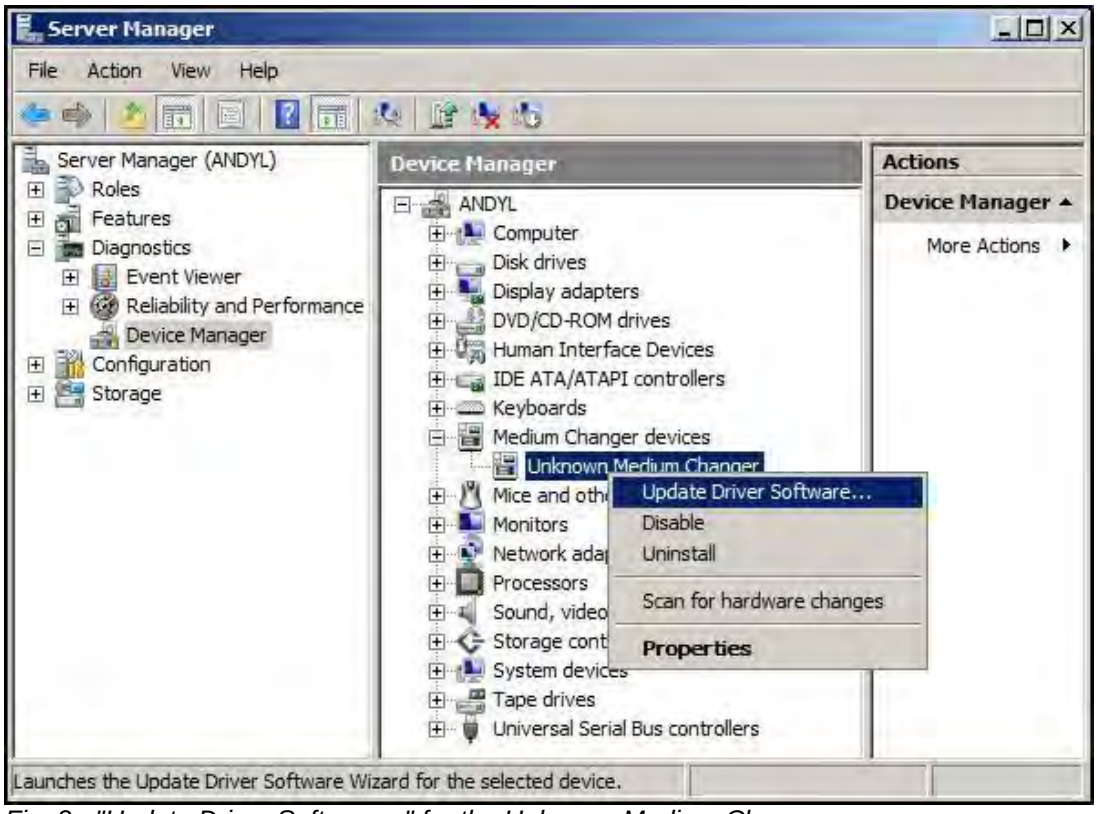


Fig. 2 - "Update Driver Software..." for the Unknown Medium Changer.

5. In the "Update Driver Software - Unknown Medium Changer" dialog, select "Browse my computer for driver software."

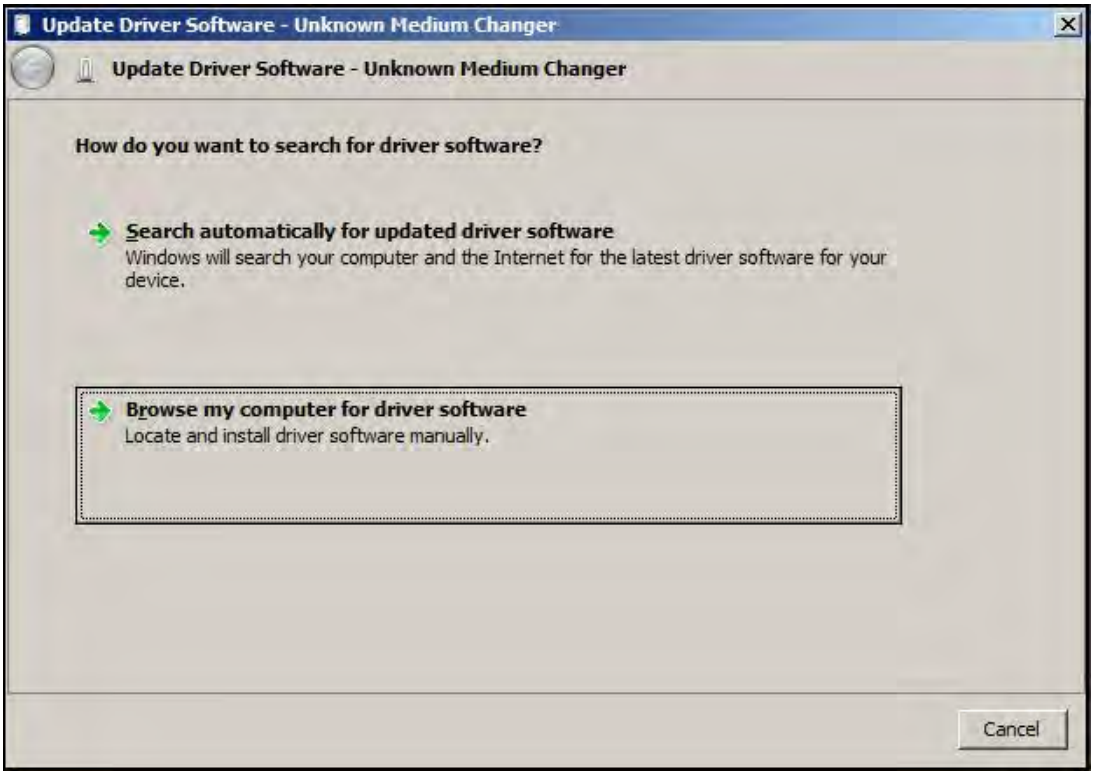


Fig. 3 - "Update Driver Software" Driver Search Method Dialog.

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."

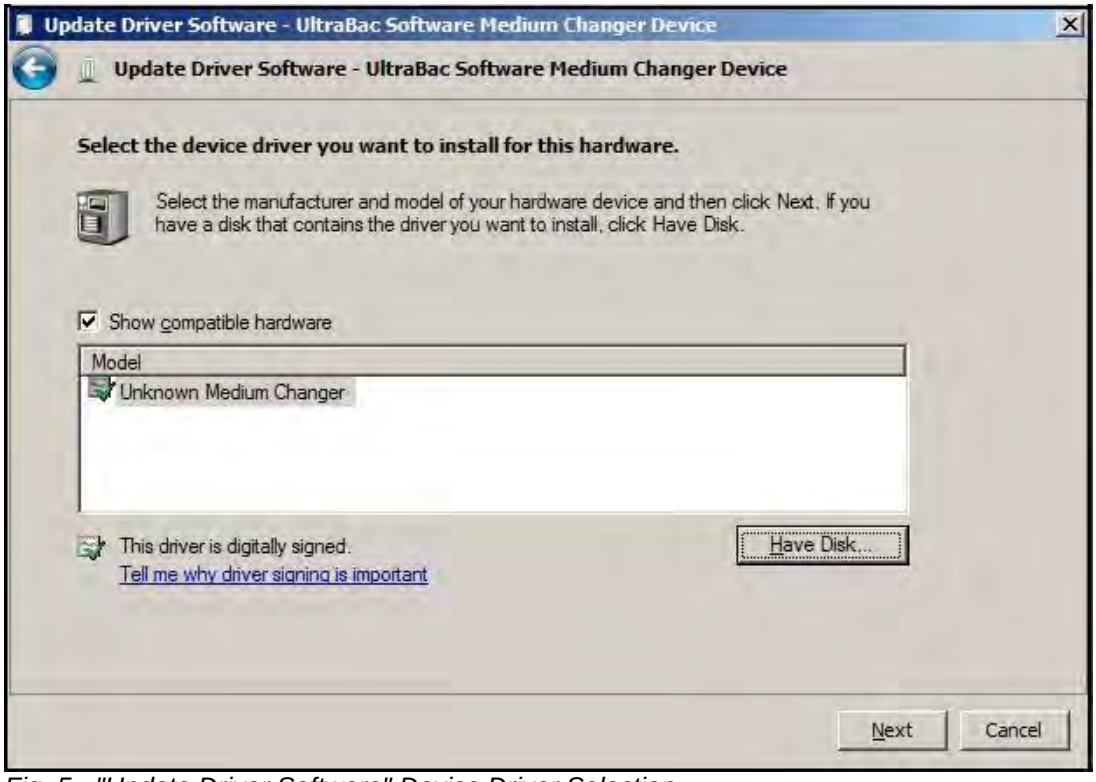


Fig. 5 - "Update Driver Software" Device Driver Selection

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.

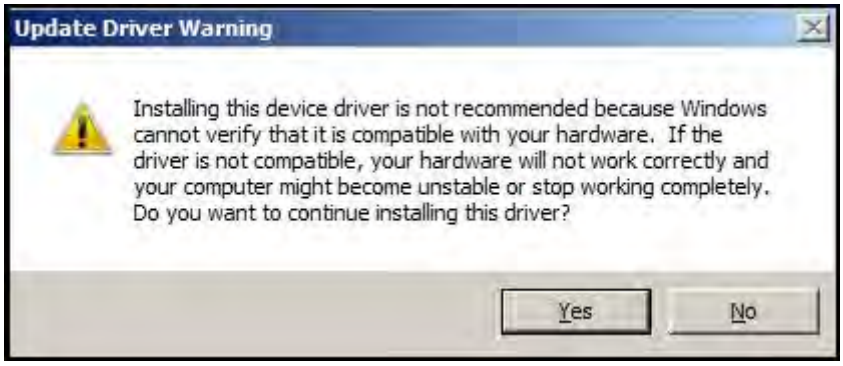


Fig. 7 - "Update Driver Warning" Driver Installation Warning

11. Click "Close" to close the "Update Driver Software" dialog.
12. Confirm that the "UltraBac Software Medium Changer Device" has been installed successfully.

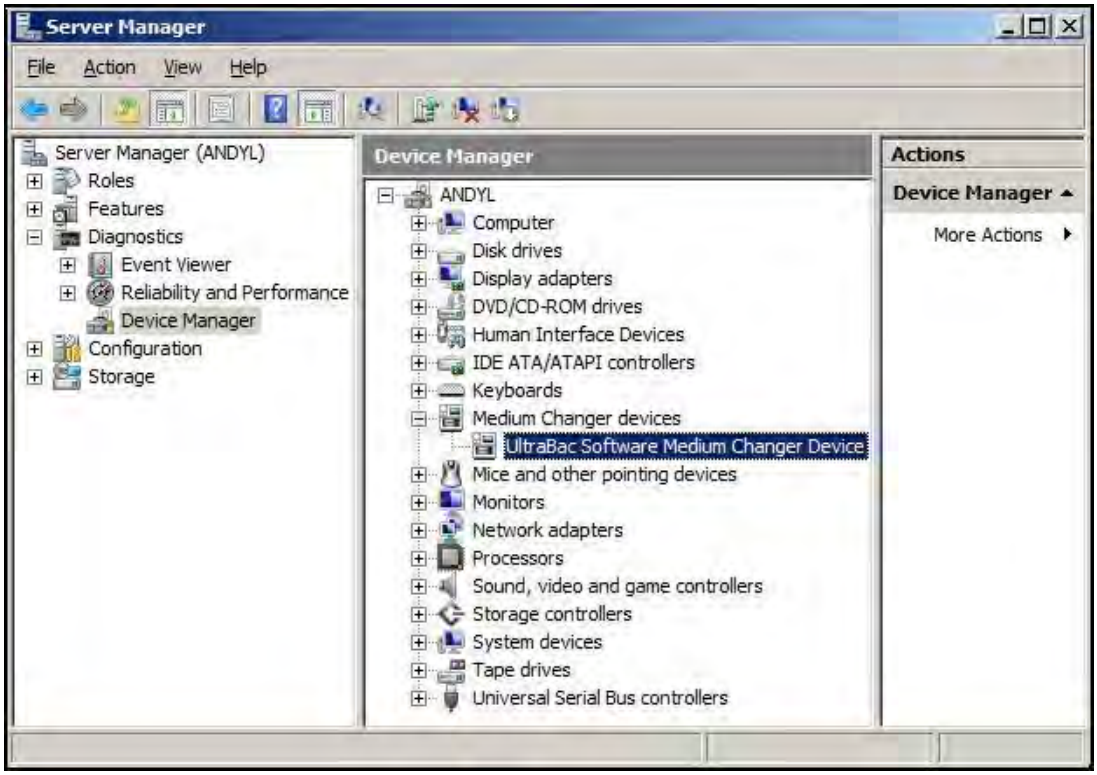


Fig. 8 - "Device Manager" showing the "UltraBac Medium Changer Device" driver.

13. Close the "Server Manager" window.

More Information:

See UltraBac User Manual: Media Library Controls
See UBQ000242: Removing Media Pools

UBQ000157: Configuring the UltraBac Centralized Reporting Console

UBQ ID Number: UBQ000157
Last Modified: 2013-06-10

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) 7.0 (Windows Server 2008/Vista or later) must be installed on the machine hosting the Centralized Reporting Console.
- Active Server Pages and ASP.NET support must be installed with IIS.
- IIS6 Compatibility mode must be enabled.
- IIS6 Management tools must be installed.
- 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.

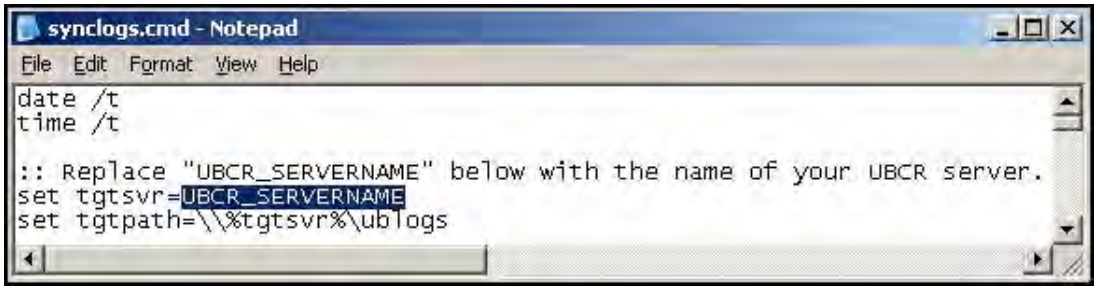


Fig. 2 - Editing the "synclogs.cmd" file.

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.

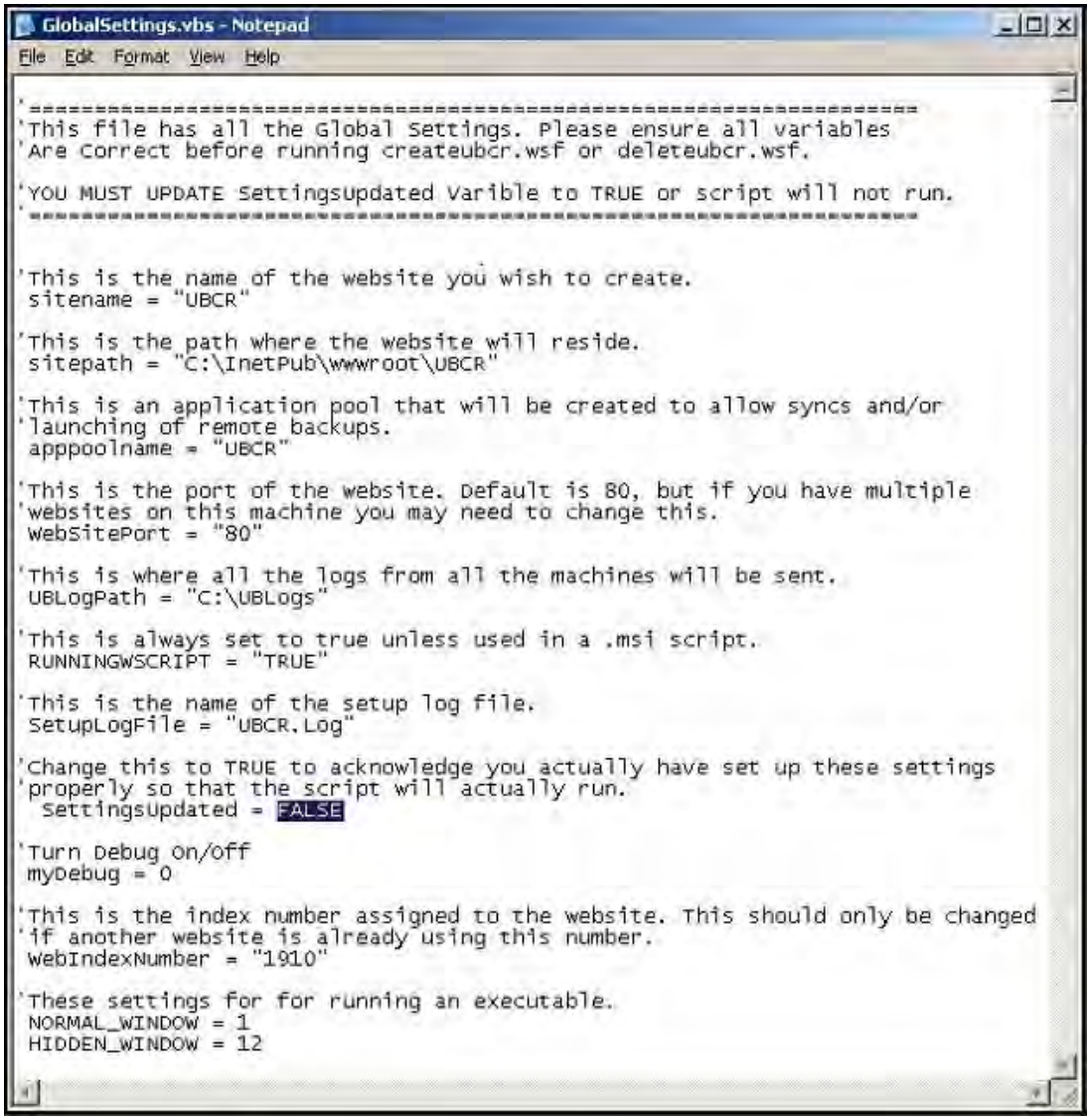


Fig. 3 - Editing the "GlobalSettings.vbs" file.

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 the status is "Allowed."

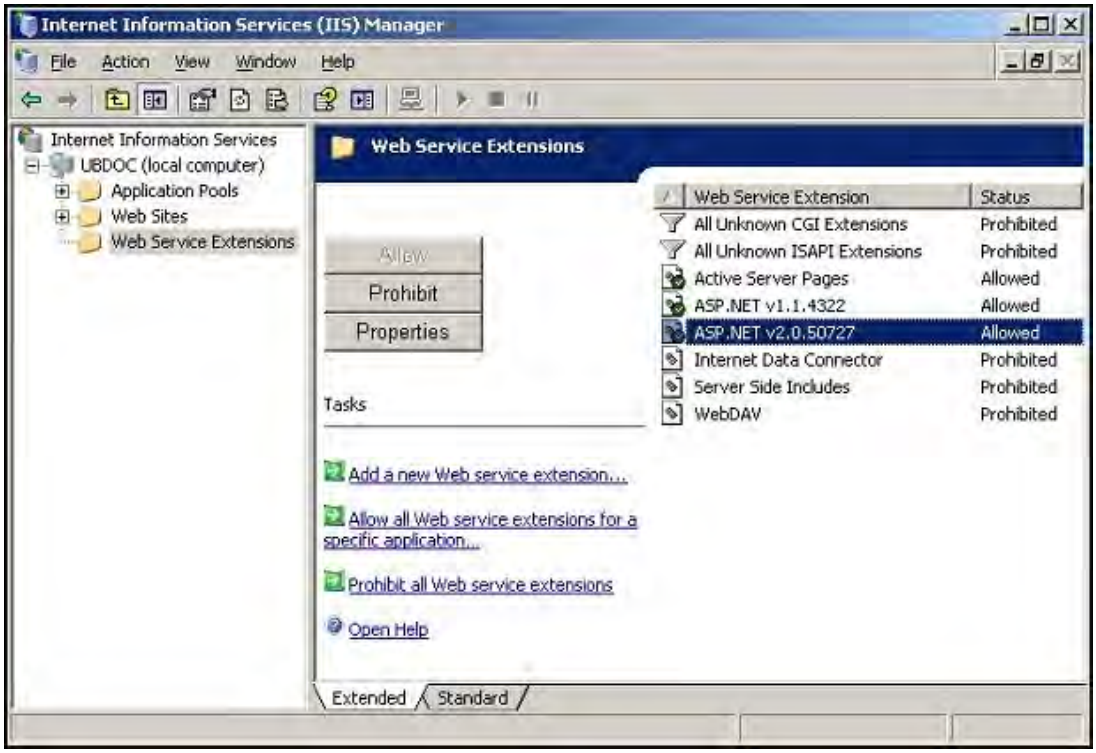


Fig. 5 - The "Web Service Extensions" screen in IIS Manager

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.

More Information:

See UltraBac User Manual: UltraBac Preferences

UBQ000158: Copying Restore Logs in UBDR

UBQ ID Number: UBQ000158
Last Modified: 2012-12-12

Summary:

This article details the process of copying a restore log to a network path in UBDR.

Details:

After completing a restore, the UltraBac restore logs can be copied to a network path for archival, troubleshooting, or other purposes.

1. Click "Tools" / "UBDR" / "Map Network Drive" to create a connection to any Windows 7/8/2003/2008/2008R2/2012 system.

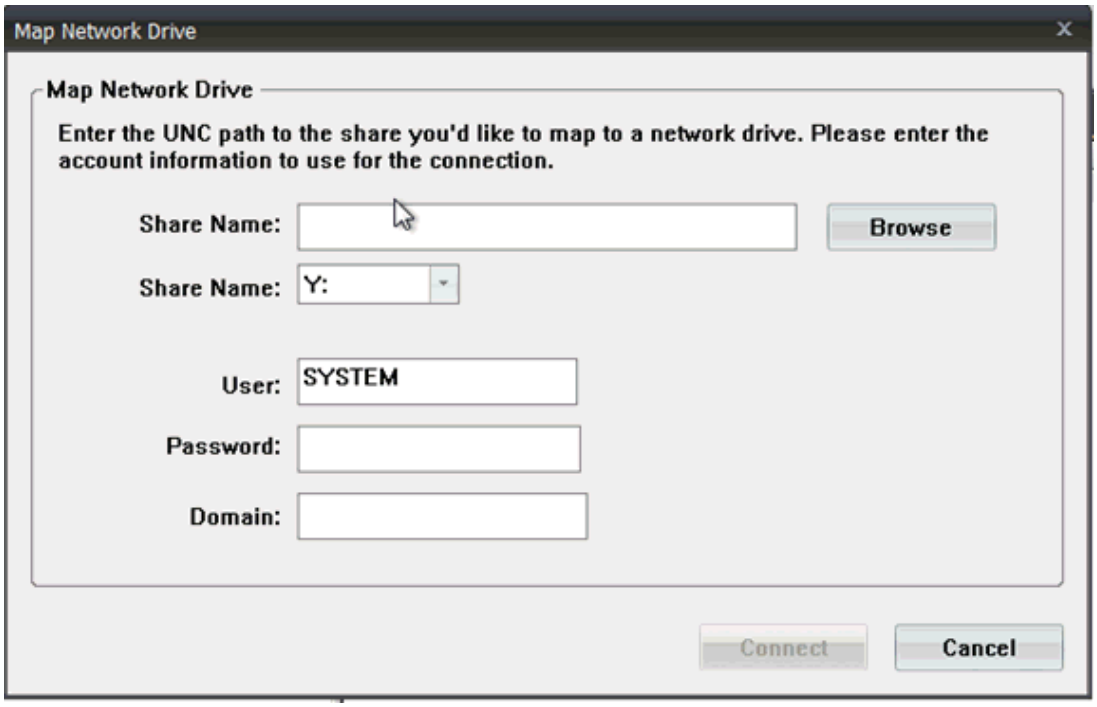


Fig. 1 - Establish Machine Connection window.

2. Enter a UNC path as a Share Name.
3. Enter a User name, password, and domain name (if necessary) into the appropriate fields, and click "Connect."
4. Go to "Tools" / "UBDR" / "Command Prompt".
5. In the command prompt, type "z:" and press Enter.
6. Type "CD logs" and press Enter.

7. Type "copy *.* y:\".

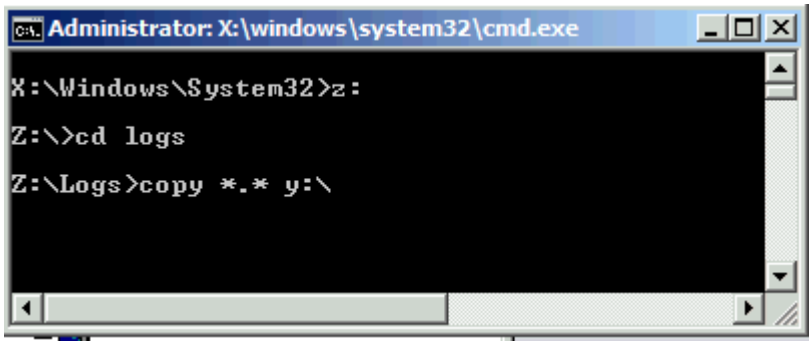


Fig. 2 - Mapping a network location.

More Information:

See UltraBac User Manual: UltraBac Disaster Recovery
See UBQ000230: UBDR Advanced Tools and Utilities

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.

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:

See UBQ000069: Troubleshooting SMTP
http://support.microsoft.com/support/kb/articles/Q191/1/43.ASP

UBQ000194: Configuring the (Legacy) 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 UltraBac User Manual: Legacy Ux File-by-File Agent
~~~~~~~~~~~~~~

UBQ000195: Medium Changer Driver Unloading

UBQ ID Number: UBQ000195
Last Modified: 2012-12-12

Summary:

This document shows the necessary steps to manually configure an autoloader. This manual configuration will allow the autoloader to work in conditions where the device is not usable in its current configuration.

NOTE: As of Version 9.0, The Library Configuration Tool will perform the following steps automatically. In very rare scenarios you will need to manually configure the settings as described below.

For more information on the Library Configuration Tool, please visit the "**Media Library Controls**" section of the User Manual:

UltraBac User Manual: Media Library Controls

Details:

To use the UltraBac Medium Changer Controls, the autoloader must have the UltraBac Medium Changer installed.

UltraBac has added code to the autoloader DLL (ubslotbasedlibrary.dll) that will read the registry to find a manual configuration, overriding the automatic configuration done by the medchg.sys driver. This is useful if the autoloader has not been properly configured, so that SCSI ID's of the drives are lower than the SCSI ID of the media changer device.

Here are the registry values/keys that must be created to perform a manual configuration:

HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac\LibraryInfo\Slot Based Library

Under that new key the user needs to create a key with the ID number of the autoloader he is configuring. If the user only has one then the value is 0. Example:

HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac\LibraryInfo\Slot Based Library\0

Under this key you add string values for each of the drives in the autoloader:

Value Name	Value
Drive1	Tape0
Drive2	Tape1

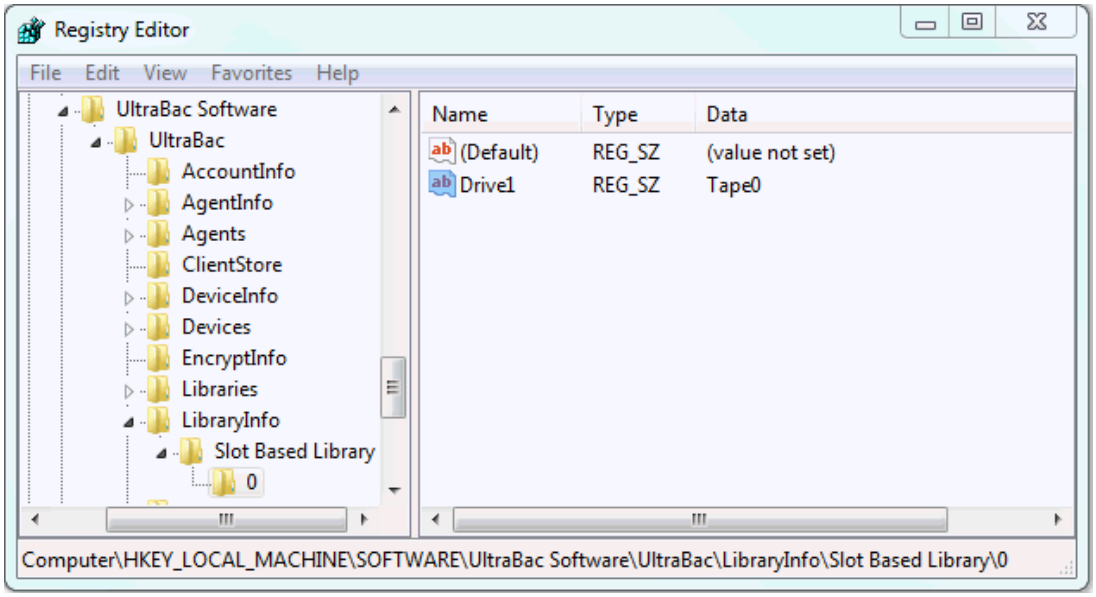


Fig. 1 - Manual entries in the Registry.

The drives in the autoloader are numbered starting at one with the prefix "Drive". Set the "Value Name" as the drive name (i.e. Drive1) and the value as the tape drive name (i.e. tape0). The values should be set according to the information found in the registry.

Use the regdmp.exe (from the NT Resource kit) utility to create a registry dump.

The command line should be (assuming that the regdmp.exe utility is in the root of the c: drive):

```
c:\regdmp HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\SCSI > c:\scsi_reg.txt
```

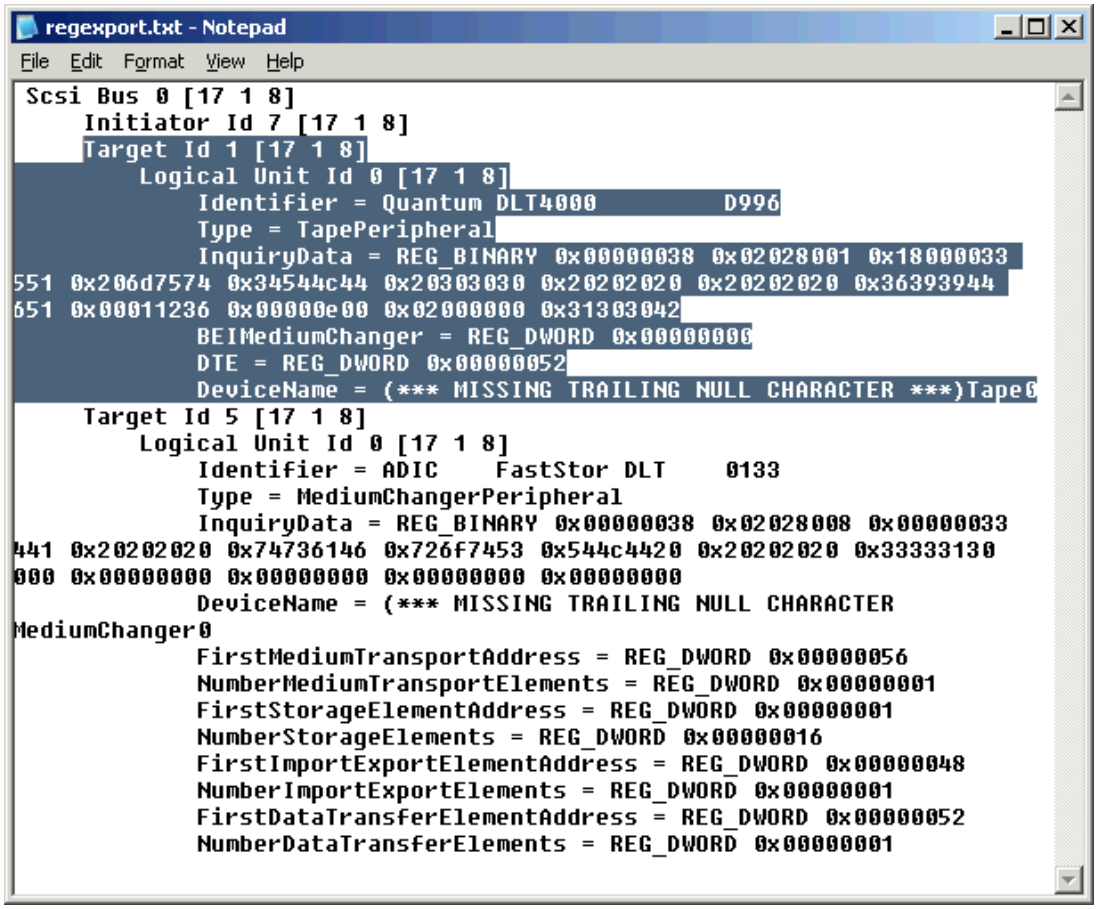


Fig. 2 - Registry Dump.

The tape drive with the lowest SCSI ID needs to be listed in the Registry key created as Drive1. In the image above, the tape drive has a SCSI ID of 1 and a device name of Tape0, so the value for this entry in "HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac\LibraryInfo\Slot Based Library\0\Drive1" should be "Tape0".

More Information:

See UltraBac User Manual: Media Library Controls

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 UltraBac User Manual: Installing UltraBac
See UBQ000112: Trouble Shooting Permissions Issues
See UBQ000202: UltraBac in a Workgroup

UBQ000202: UltraBac in a Workgroup

UBQ ID Number: UBQ000202
Last Modified: 2012-12-12

Summary:

This article describes how to use UltraBac, and particularly authenticating through the UltraBac Management Service, within a workgroup.

Details:

The user must be consistent, using the same password for all machines in the workgroup. The global user ID and password is specified in "Manage"/"General"/"Authentication Options"/"Accounts." When adding an account, the following should be entered for the Default account:

- User ID
- Password
- Confirm password
- Domain (left blank)

When entering the account information for the Default Account, the Domain field should be left blank. This will force UltraBac to log on locally (log on to the backup host) using the account specified.

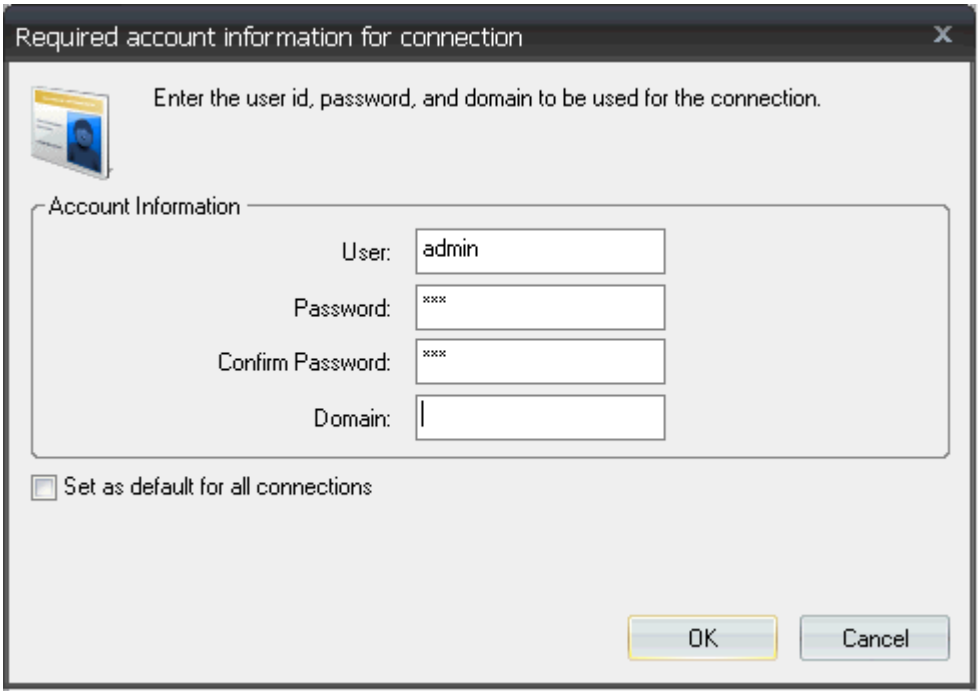


Fig.1 - Account information

It is necessary to create an account entry on the backup host for EACH computer being backed up. Again, the domain field should be left empty. When entering the remote computer account, it is necessary to specify the name of the computer as well.

The following selection box will open when entering the second account into UltraBac. This is where you specify the machine being backed up.

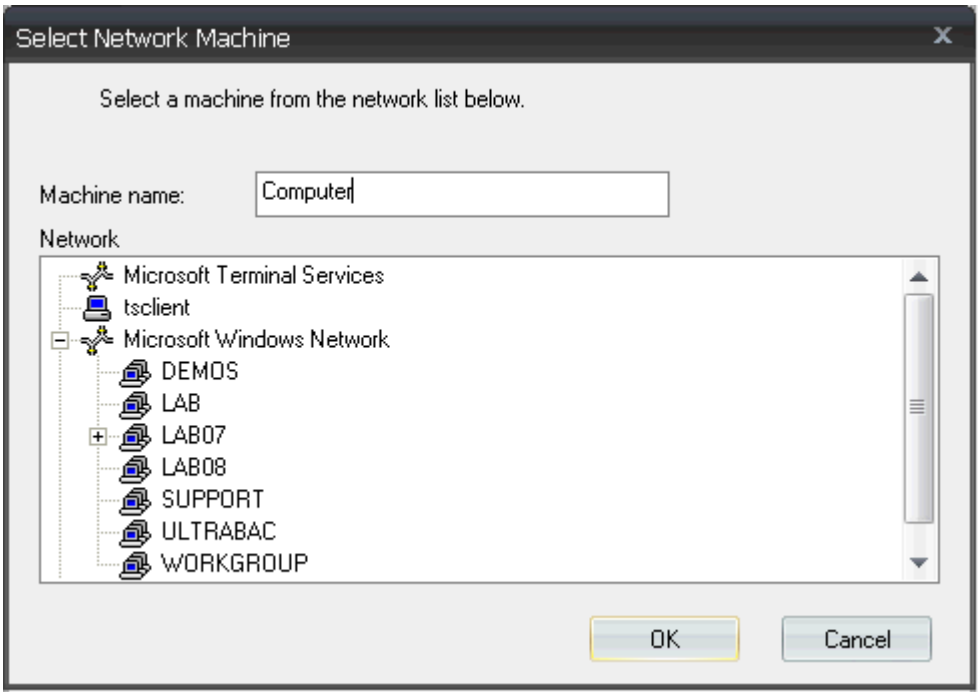


Fig. 2 - Specifying computer name when adding accounts

When configuring UltraBac, do not use an IP address for the license server - ALWAYS use the Windows computer name. You can do this using DNS or WINS. If neither is present use the HOSTS file, located in '%WinDir%\System32\Drivers\etc'.

Use the following format when making entries into the HOSTS file:

IPADDRESS [TAB] COMPUTERNAME.

Example:

```
127.0.0.1    localhost
10.1.1.1     Backupserver
```

You will need to install a full version of UltraBac on each of the machines you are going to backup. On each of the machines, you will need to go into "Manage"/"General"/"Authentication Options"/"Accounts" and add an account for the backup server, so there is authentication for two way communication.

More Information:

See UltraBac User Manual: Installing UltraBac
See UBQ000198: Backup Account Permissions

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".

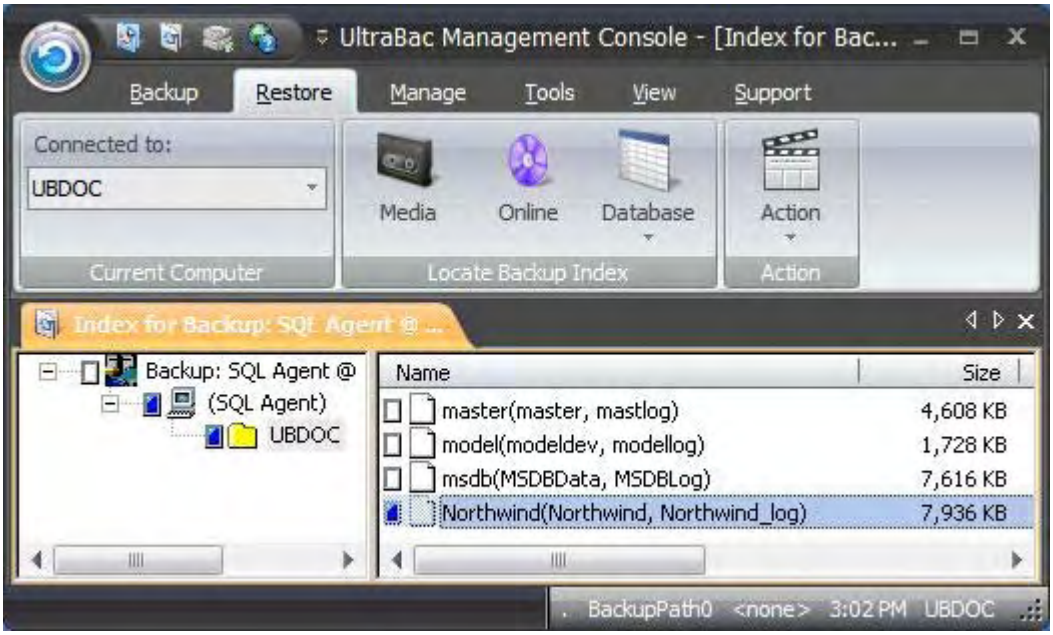


Fig. 1 - Names of the database files.

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:

see 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.

More Information:

See UltraBac User Manual: Backup Set Basics

UBQ000214: Description of License Components

UBQ ID Number: UBQ000214
Last Modified: 2012-12-12

Summary:

What is an Engine Server? What is a Remote Local Server Agent? Why do I need them?

Details:

Any time a backup runs it requires two parts to be licensed - the Engine and "Some" agent.

The Engine is what actually does all the work in a backup. The Agent tells UltraBac what to backup.

Example: File-by-file backups require a Remote Local Server Agent (RLSA) license for each machine that needs to have a file level backup done.

If you purchase a Single Server License, you would have 1 Engine, 1 RLSA, and 100 Remote Local Workstation Agents (RLWA).
This allows you to back up up a server and 100 workstations via file-by-file.

An Enterprise License has 1 Engine, 7 RLSA, and 100 RLWA, allowing you to perform a file backup of a total of 7 servers and 100 workstations from one central server.

More Information:

See UltraBac User Manual: UltraBac Licensing

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 UltraBac 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.

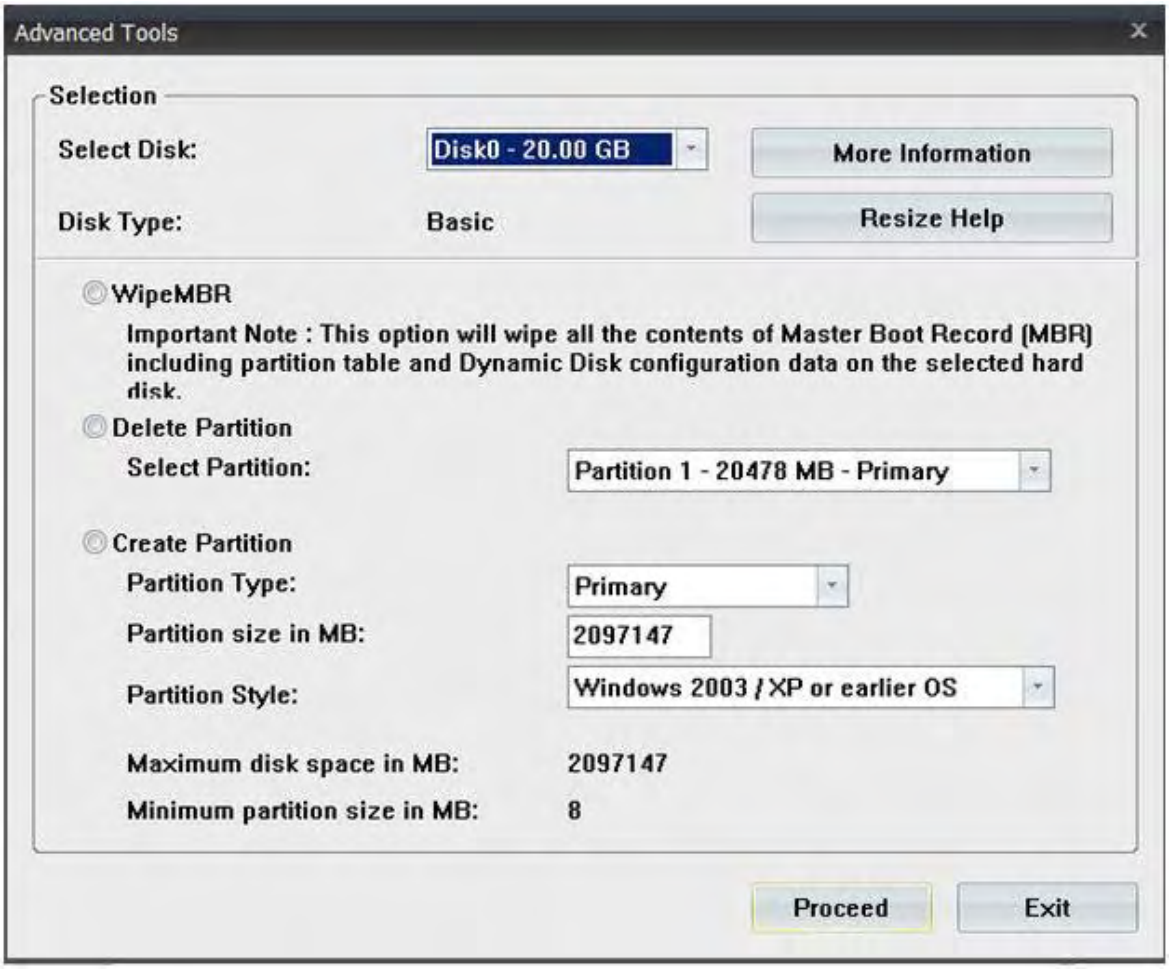


Fig 1. Advanced Tools

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 UltraBac User Manual: Image Disaster Recovery Agent
See UltraBac User Manual: UBDR Gold
See UBQ000024: What is an Image Backup?
See UBQ000158: Copying Restore Logs in UBDR
See UBQ000233: Resize Partitions During Image Restore

UBQ000234: Common Backup Errors Explained

UBQ ID Number: 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 UltraBac User Manual: Installing UltraBac
See UltraBac User Manual: Exchange Agent
See UltraBac User Manual: Locked File Backup Agent
See UltraBac User Manual: SQL Agent
See UBQ000230:UBDR Gold Advanced Tools and Utilities

UBQ000236: UBDR Scripted Restore

UBQ ID Number: UBQ000236
Last Modified: 2007-02-21

Summary:

UBDR Gold has the ability to automate the restore of an image backup, allowing the System to be booted from UBDR media and fully restored with a minimum of user intervention.

Details:

A file named "autorestore.inf" must be created with specific restore instructions and saved to the "UBDR" directory on the CD. The methodology to do this will be at the end of this article

The "autorestore.inf" must have all of the following information. The example below will boot from UBDR and perform a restore of the system to the original location of the OS, even if the target disk is not the original disk:

User:<Username>
domain:<Domain - leave blank when in a workgroup>
password:<Password>
IP:<IP address to be used>
<Subnet Mask>
<Default Gateway>
<DNS>
<WINS>
connectto:<Machine Name>
[HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac\DeviceInfo\Win32 File Device]
"BackupPath0"="\\\\<COMPUTERNAME>\\<sharename>\\<DIR>\\"
"BackupPath0 Name"="Image Path"
"BackupPath0 Size Limit"=dword:00000000
"BackupPath0 File Size Limit"=dword:00000200
[HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac]
"DefaultTape"=dword:000003e8
/findfiles:* /restore: /AO:Type=1,RestToSameDisk=1,OverwriteAlways=1

Network Identification

These entries are used to define the network ID, domain and login information of the system while booted from the UBDR Gold disc:

- User – A user account name that has administrator level access to the stored location of the backup files.
- Domain – Domain where the backup files are stored. Leave blank if used in a workgroup.
- Password – Password for the specified account.

- IP – The IP address to be used by the system once on the network. "DHCP" can be substituted to allow automatic network configuration using a DHCP server.
- Subnet Mask – Subnet mask of the domain where the backup files are stored. This field is not used if DHCP is specified, and should be excluded from the "autorestore.inf".
- Default Gateway – IP address of the default gateway in the domain where the backup files are stored. This field is not used if DHCP is specified, and should be excluded from the "autorestore.inf".
- DNS – IP address of the DNS server in the domain where the backup files are stored. This field is not used if DHCP is specified, and should be excluded from the "autorestore.inf".
- WINS – IP address of the WINS server in the domain where the backup files are stored. This field is not used if DHCP is specified, and should be excluded from the "autorestore.inf".
- connectto – Network name or IP address of the system hosting the backup files.

Device Configuration

These entries in the autorestore.inf file are used to create the device in UltraBac that points to the location of the stored backup files:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac\DeviceInfo\Win32 File Device]
"BackupPath0"="\\\\server2003\\h$\\images\\server5\\"
"BackupPath0 Name"="Image Path"
"BackupPath0 Size Limit"=dword:00000000
"BackupPath0 File Size Limit"=dword:00000200
[HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac]
"DefaultTape"=dword:000003e8
```

This line specifies the location of the registry keys created for the BackupPath device":

```
[HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac\DeviceInfo\Win32 File Device]
```

This entry specifies that the backup files are stored in the UNC path:

```
\\server2003\h$\images\server5
```

When entering the UNC path in the "Backuppath0" key, the path must use double backslashes (including 4 for the beginning of the path) and should be in quotes:

```
"\\\\server2003\\h$\\images\\server5\\"
```

This entry specifies the BackupPath name, and can be any user defined name:

```
"BackupPath0 Name"="Image Path"
```

These two entries specify the total size limit of the backup path, and the size limit of each backup file. These values should be listed exactly as shown:

```
"BackupPath0 Size Limit"=dword:00000000
"BackupPath0 File Size Limit"=dword:00000200
```

The "default device" key instructs UBDR Gold to use the specified device as the default device:

[HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac]
"DefaultTape"=dword:000003e8

When the "autorestore.inf" should perform the restore from Tape0, this key should be:

"DefaultTape"=dword:00000000

Restore Configuration Switches

To perform a restore operation, this line must always be specified exactly as shown below:

/findfiles:* /restore: /AO:

These switches can be added to the Agent Options section to modify the behavior of the restore. They should be added after the "/AO:" switch, and be separated by a comma. None of the switches should be put in quotes:

"Type=1" – Inputs the image restore option.
"RestToSameDisk=1" – Restore to original disk.
"OverwriteWhenDiskIsBlank=1" – Overwrite data when target disk is blank. This option can be used when the "RestToSameDisk=1" switch is set.
"OverwriteAlways=1" – Always overwrite the target disk. This option can be used when the "RestToSameDisk=1" switch is set.
"RestMBR – Restore the Master Boot Record.
"disk=<N>" – Restore to the specified disk, by number. Not used when "RestToSameDisk=1" is set.
"part=<N>" – Restore to the specified partition on the disk set in "disk=<N>". Not used when "RestToSameDisk=1" is set.
"MarkPartnActive=1" – Mark the target partition as active.
"RestDiffHW=1" – Run the dissimilar hardware restore after the data restore is complete.
"EncryptionPhrase=<phrase>" – Allows an encryption phrase to be specified in plain text.

Additional Switches

/Optional – When specified on the first line of the "autorestore.inf", this switch gives a prompt to either start the auto-restore process or to allow the system to boot and use manually specified network/restore parameters.
/Reboot – Instructs the system to restart after the restore is complete.
/Quiet – Instructs the restore to proceed in an "unattended" manner, writing all error/warning messages to the restore logs.

Running a Command Line Option

To run a command line option in the autorestore, use a "RUNCMD" command on a separate line from the restore command:

RUNCMD=<command>

Any executable command can be run from the "RUNCMD" option.

Example: RUNCMD=chkdsk c: /f

Restoring to Dissimilar Hardware Using the Autorestore

When doing a dissimilar hardware restore, it is necessary to break the restore operation into several parts. If the MBR is to be restored, that should be done first, followed by the OS partition (using the dissimilar hardware switch), followed by any data partitions.

Here is an example of an autorestore.inf that will perform a dissimilar hardware restore:

```
User:Admin
domain:TESTING
password:Sample*21
IP:DHCP
connectto:server2
[HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac\DeviceInfo\Win32 File Device]
"BackupPath0"="\\\\server2\\h$\\backups\\images\\server1\\"
"BackupPath0 Name"="my image"
"BackupPath0 Size Limit"=dword:00000000
"BackupPath0 File Size Limit"=dword:00000200
[HKEY_LOCAL_MACHINE\SOFTWARE\UltraBac Software\UltraBac]
"DefaultTape"=dword:000003e8
/Quiet "/findfiles:Partition-1 (C:) - Active Clusters Only" /restore:
/AO:Type=1,RestMBR=1,Disk=0,Part=1
/Quiet "/findfiles:Partition-1 (C:) - Active Clusters Only" /restore:
/AO:Type=1,Disk=0,Part=1,RestDiffHW=1,RestMBR=0
```

Updated Network Entries for Post 2-1-07 Releases

The Default Gateway, DNS, and WINS servers should be specified with placeholder entries of "0.0.0.0" when specifying a static IP address:

```
User:<user>
domain:<domain or ip/network name of backup data host>
password:<password>
IP:192.168.1.50
255.255.255.0
0.0.0.0
0.0.0.0
0.0.0.0
connectto:192.168.1.100
```

To use a NIC card other than the default NIC, specify multiple entries in the autorestore:

```
User:<user>
domain:<domain or ip/network name of backup data host>
password:<password>
IP:0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0
IP:192.168.1.50
255.255.255.0
0.0.0.0
0.0.0.0
0.0.0.0
connectto:192.168.1.100
```

Editing the ISO Image

1. Install Windows AIK. Ex: C:\program files\Windows AIK get it here:

   http://www.microsoft.com/downloads/en/details.aspx?FamilyID=696dd665-9f76-4177-a811-39c26d3b3b34&displaylang=en

2. Open UBDR ISO file and extract boot.wim (from sources directory in the ISO) to some location. Example: C:\WorkDir
3. Create a directory C:\WorkDir\mount
4. Mount the image with RW access:

   "C:\Program Files\Windows AIK\Tools\Servicing\Dism.exe" /Mount-Wim /WimFile:"C:\UBDR Media Builder\TEMP\winpe.wim" /index:1 /MountDir:"C:\UBDR Media Builder\TEMP\mount"

5. Add the autorestore.inf file you want:

   copy c:\workdir\autorestore\autorestore.inf C:\WorkDir\mount\UBDR

6. Commit change(s) and unmount the image:

   "C:\Program Files\Windows AIK\Tools\Servicing\Dism.exe" /Unmount-Wim /MountDir:"C:\UBDR Media Builder\TEMP\mount" /Commit

7. Replace the old boot.wim with the new boot.wim from C:\WorkDir in the ISO.

More Information:

See UltraBac User Manual: UBDR

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>."

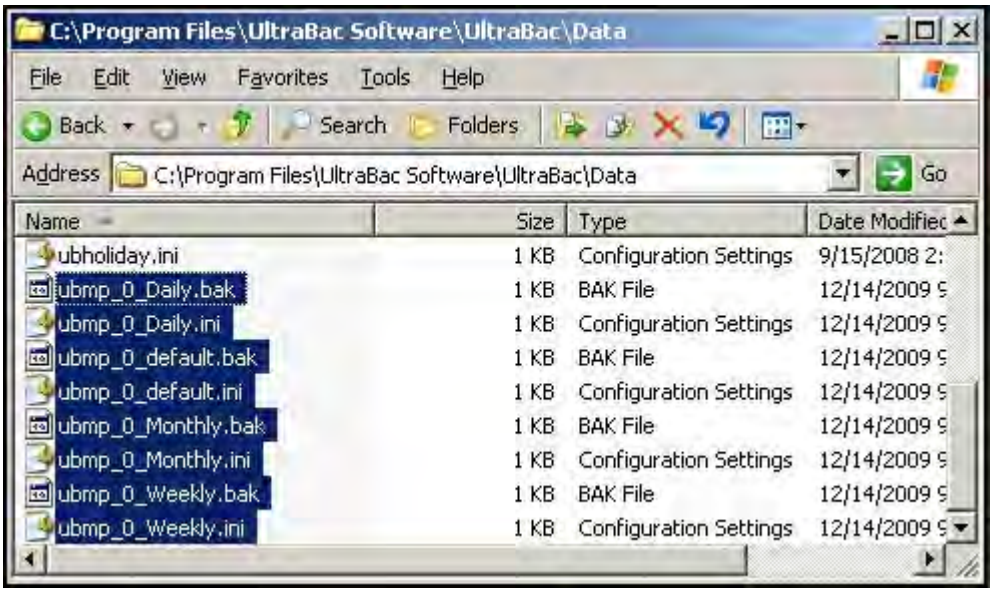


Fig. 1 - Media pool configuration files.

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

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

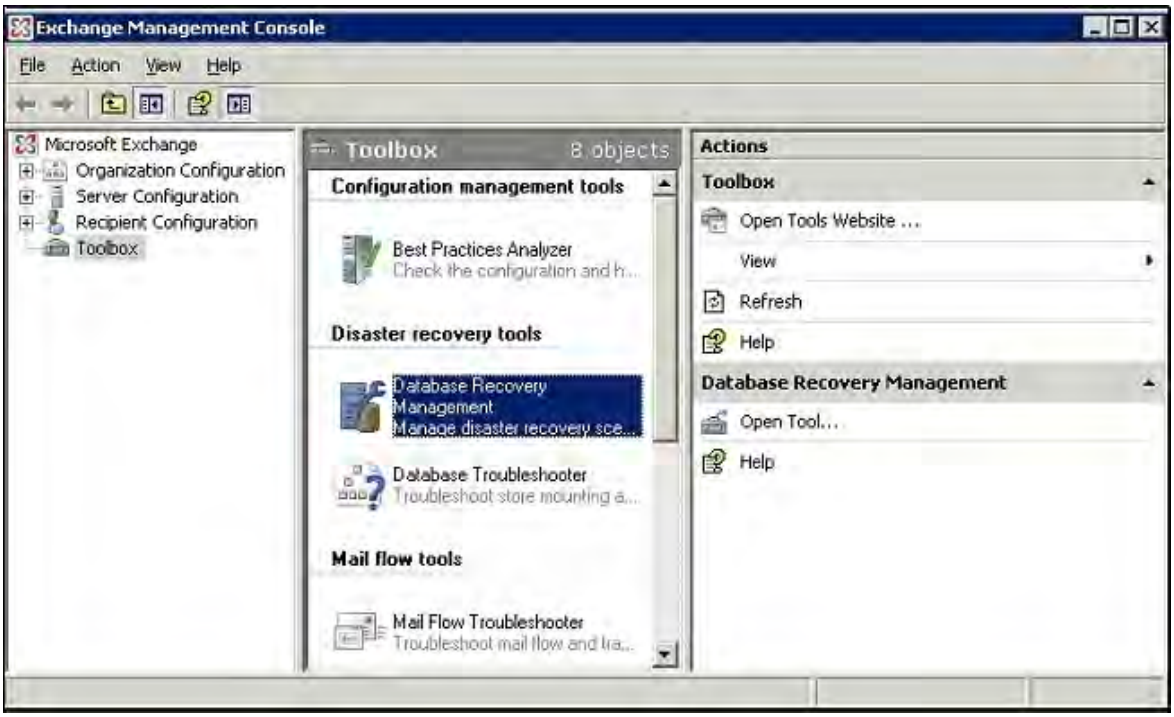


Fig. 2 - Disaster Recovery Tools in the Toolbox.

More Information:

See UltraBac 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."

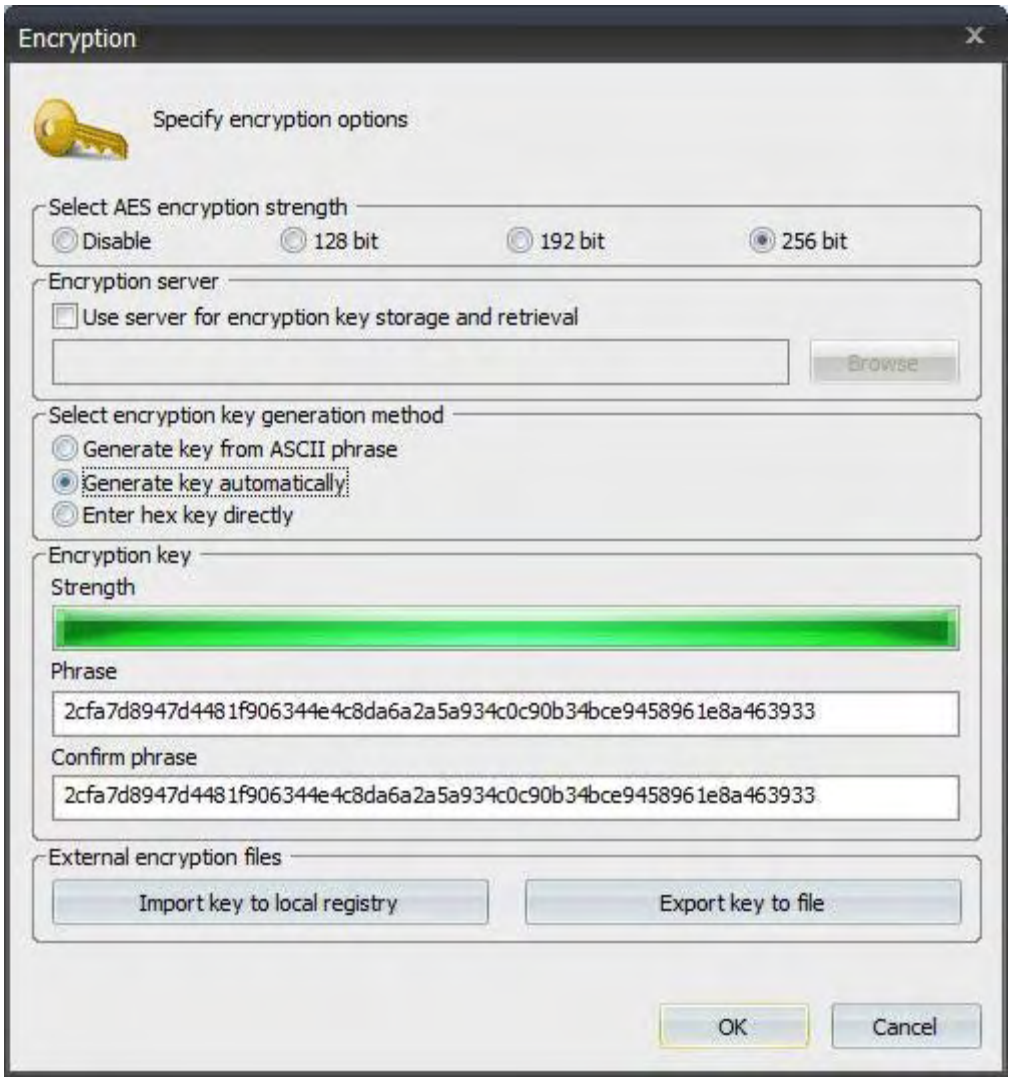


Fig. 1 - AES Encryption Configuration Options.

2. Set the AES encryption strength:
   - Disable - Turns off all AES encryption usage.
   - 128 bit - Sets AES to use a 128 bit key.
   - 192 bit - Sets AES to use a 192 bit key.
   - 256 bit - Sets AES to use a 256 bit key.

3. Select the method for generating the encryption key:
   - Generate key from ASCII phrase - Creates an encryption key using any ASCII characters, of the specified encryption strength.
   - Generate key automatically - Creates a random encryption key using HEX characters, of the specified encryption strength.
   - 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.

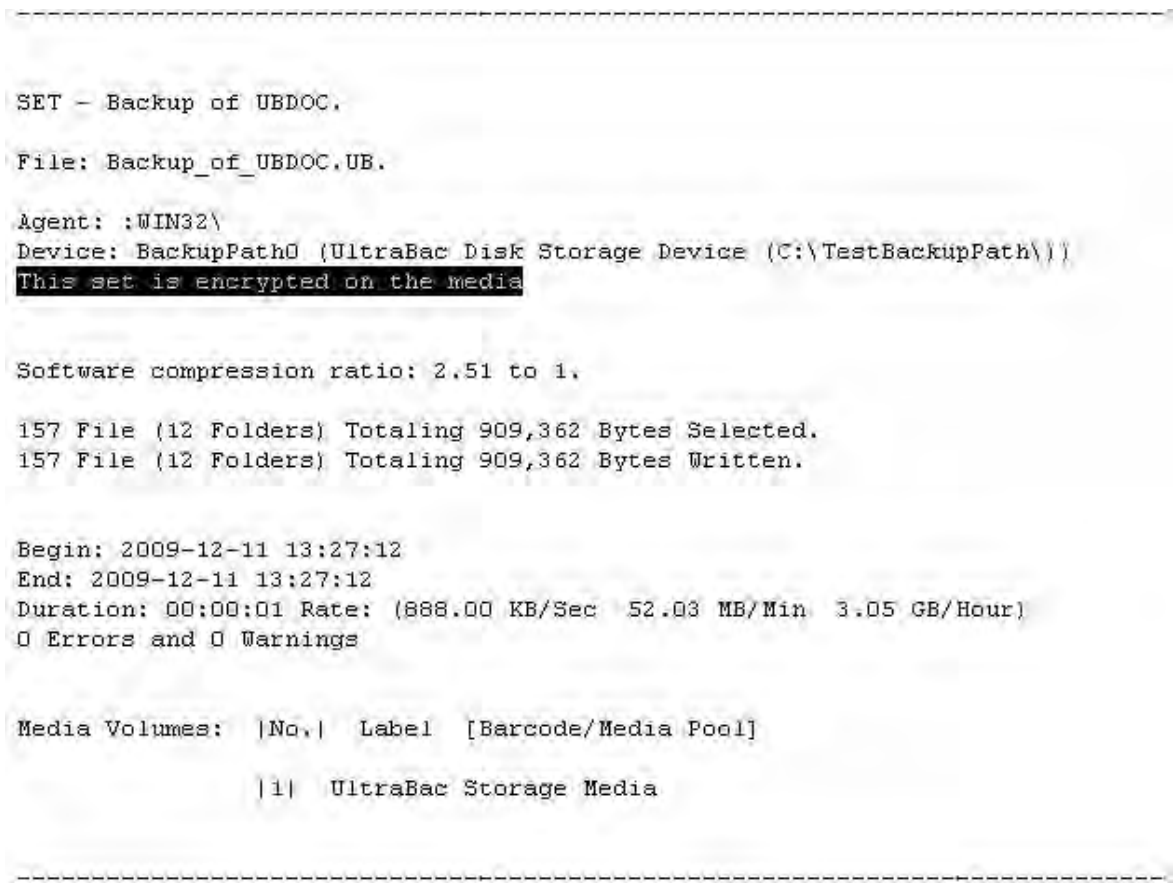


Fig. 2 - AES in the UltraBac log files.

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.

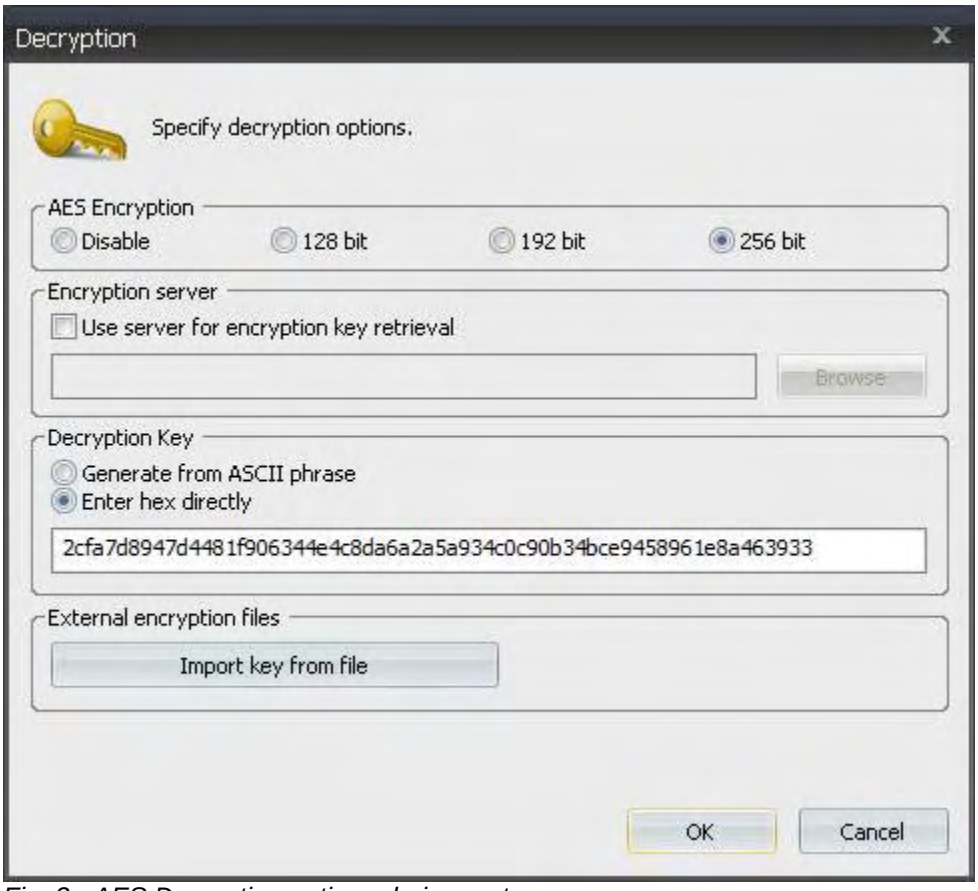


Fig. 3 - AES Decryption options during restore.

More Information:

See UltraBac User Manual: UltraBac Preferences
See UltraBac User Manual: Backup Set Basics
See UltraBac User Manual: Restore Basics

UBQ000253: Configuring Microsoft SQL or MySQL for use with the UltraBac Database

Summary:

UltraBac can utilize either Microsoft SQL (Full or Express) or MySQL for the UltraBac Database functions. Each platform requires some changes from the "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.

NOTE: The SQL Server "Authentication Mode" will need to be set to "Mixed Mode" if your computers are in multiple domains where the domain containing the computer you are trying to add to UltraBac's Centralized Management does not have a trust relationship to the domain containing the SQL server and UltraBac's index manager server; or if you are trying to add computers that are not joined to a domain.

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.

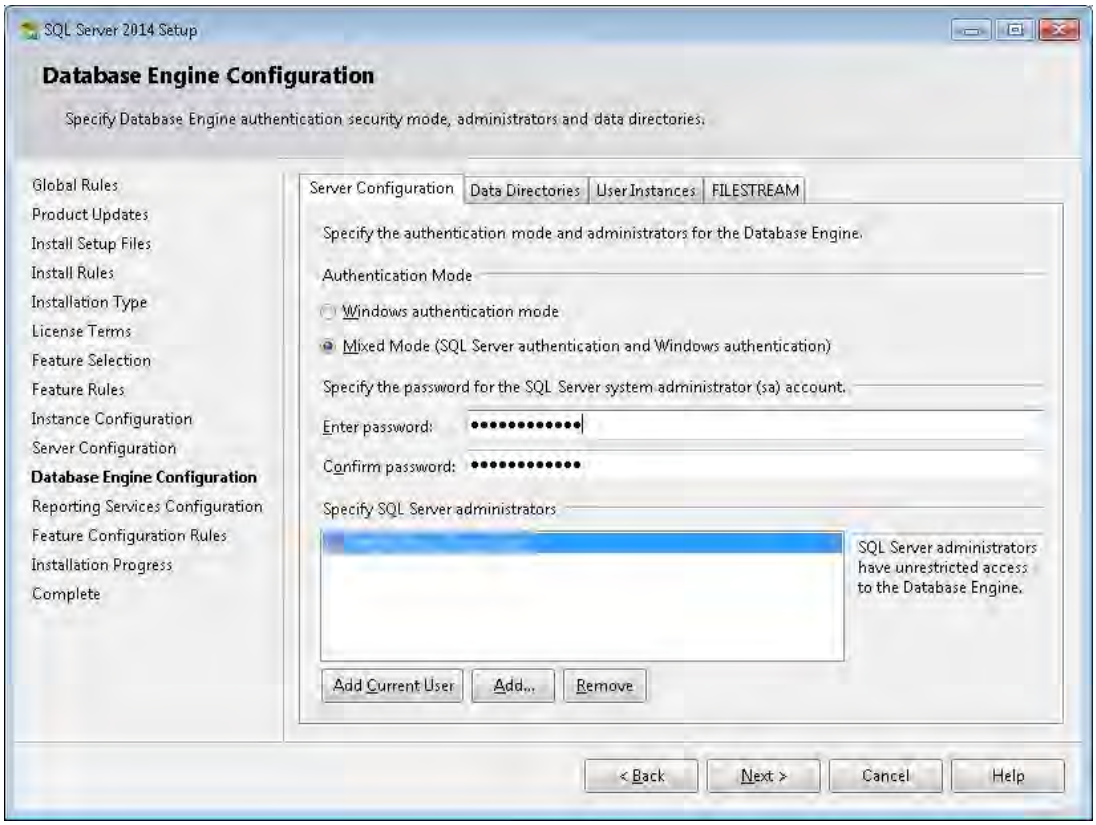


Fig. 1 - SQL Server Setup "Authentication Mode" dialog.

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.

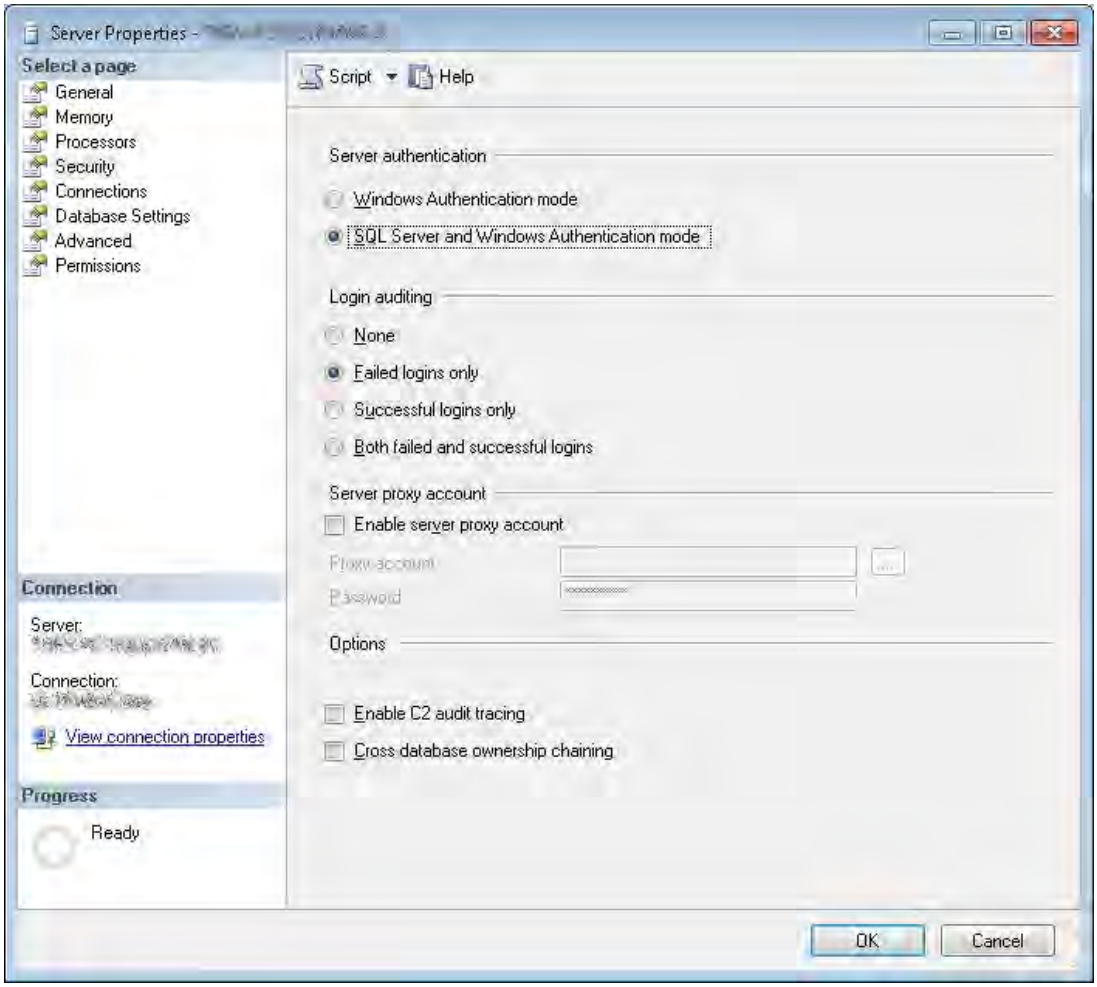


Fig. 2 - SQL Server Management Studio "Authentication Mode" dialog.

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:

1. Open the SQL Server Configuration Manager.
2. Expand "SQL Server Network Configuration."
3. Click on "Protocols for [INSTANCENAME]."
4. Right-click "TCP/IP" and click "Properties."
5. Change "Enabled" to "Yes."
6. Click "OK."

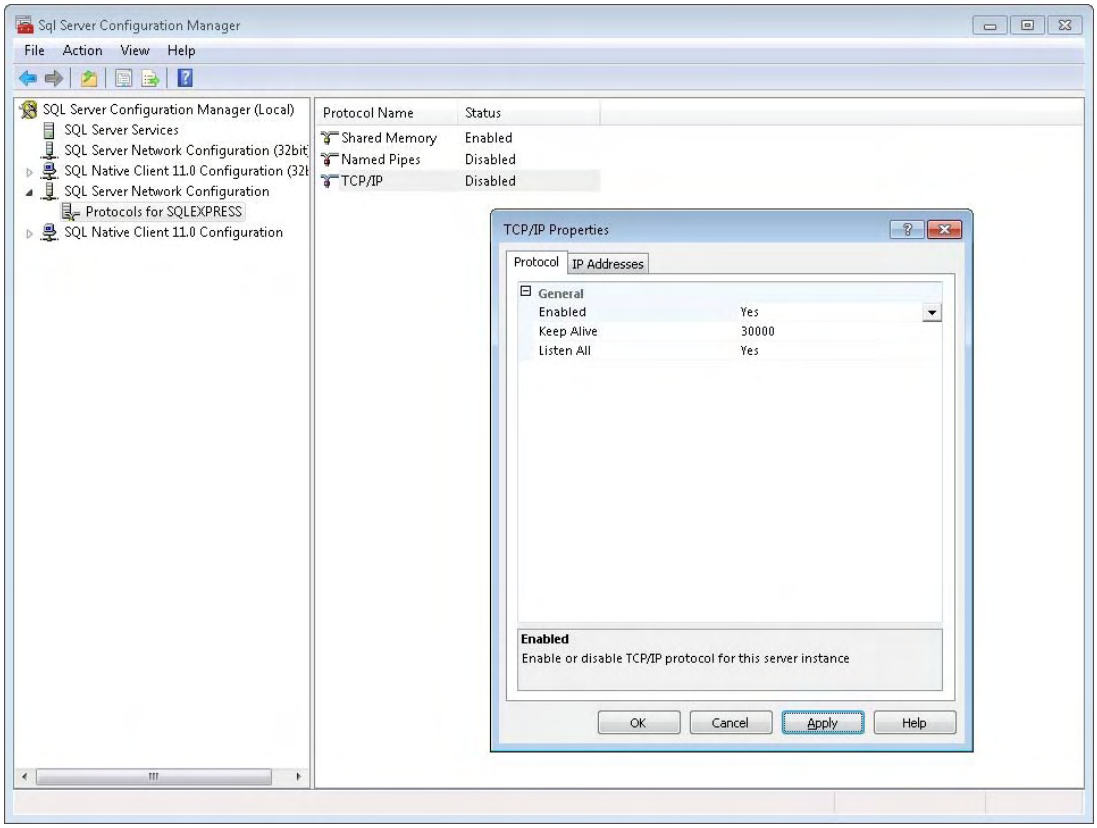


Fig. 3 - SQL Server Configuration Manager "Protocols" dialog.

5. Next, click on the "SQL Server 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 "Apply."

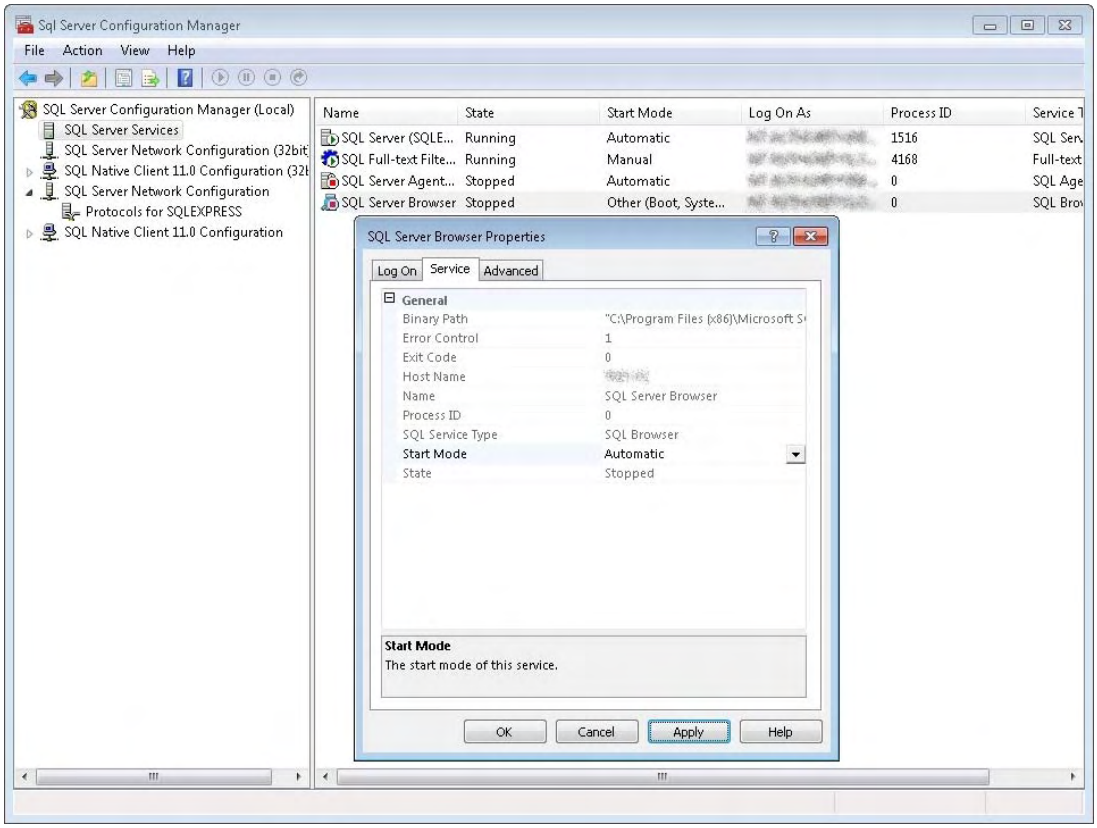


Fig. 4 - SQL Server Browser "Properties/Service" dialog.

10. Click on the "Log On" tab.
11. Click "Start" then click "OK."

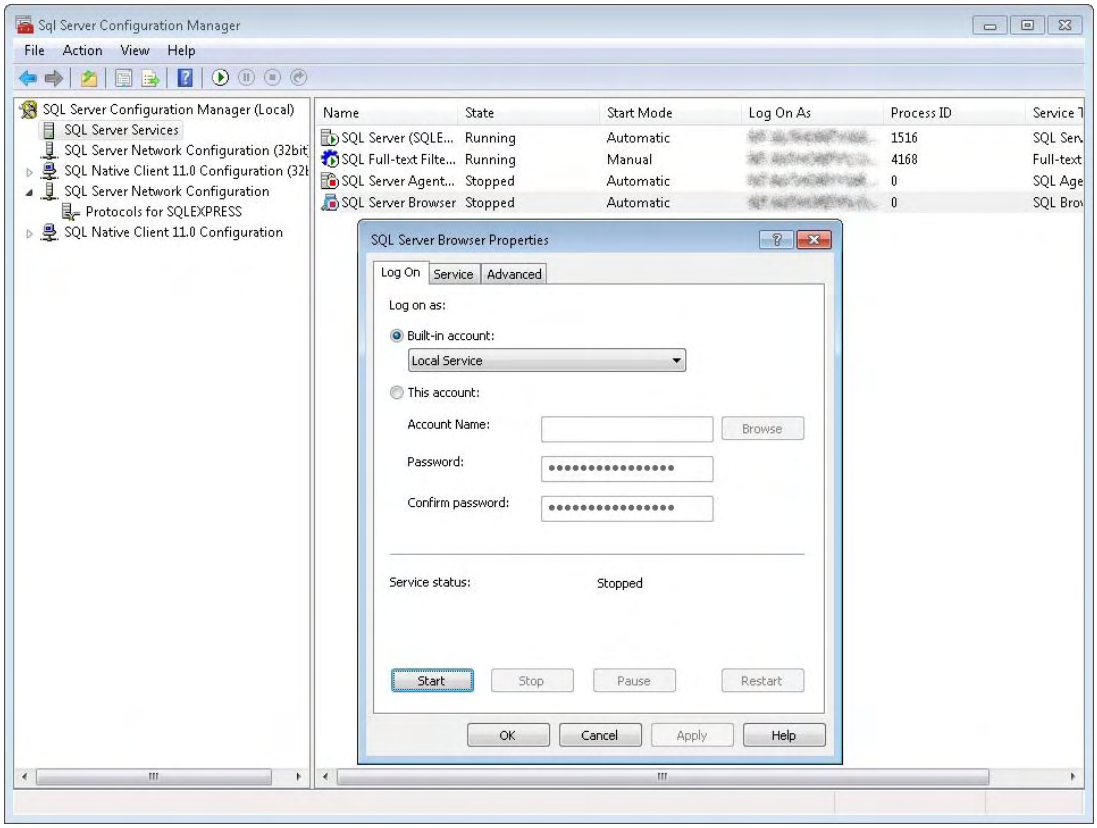


Fig. 5 - SQL Server Browser "Properties/Log On" dialog.

12. Open the SQL Server Management Studio / SQL Server Management Studio Express.
13. Connect to the SQL Server\Instance to be configured.
14. Right-click on the SQL Server\Instance, then click "Properties."
15. Select the "Connections" page.
16. If not already selected, check "Allow remote connections to this server", then click "OK."

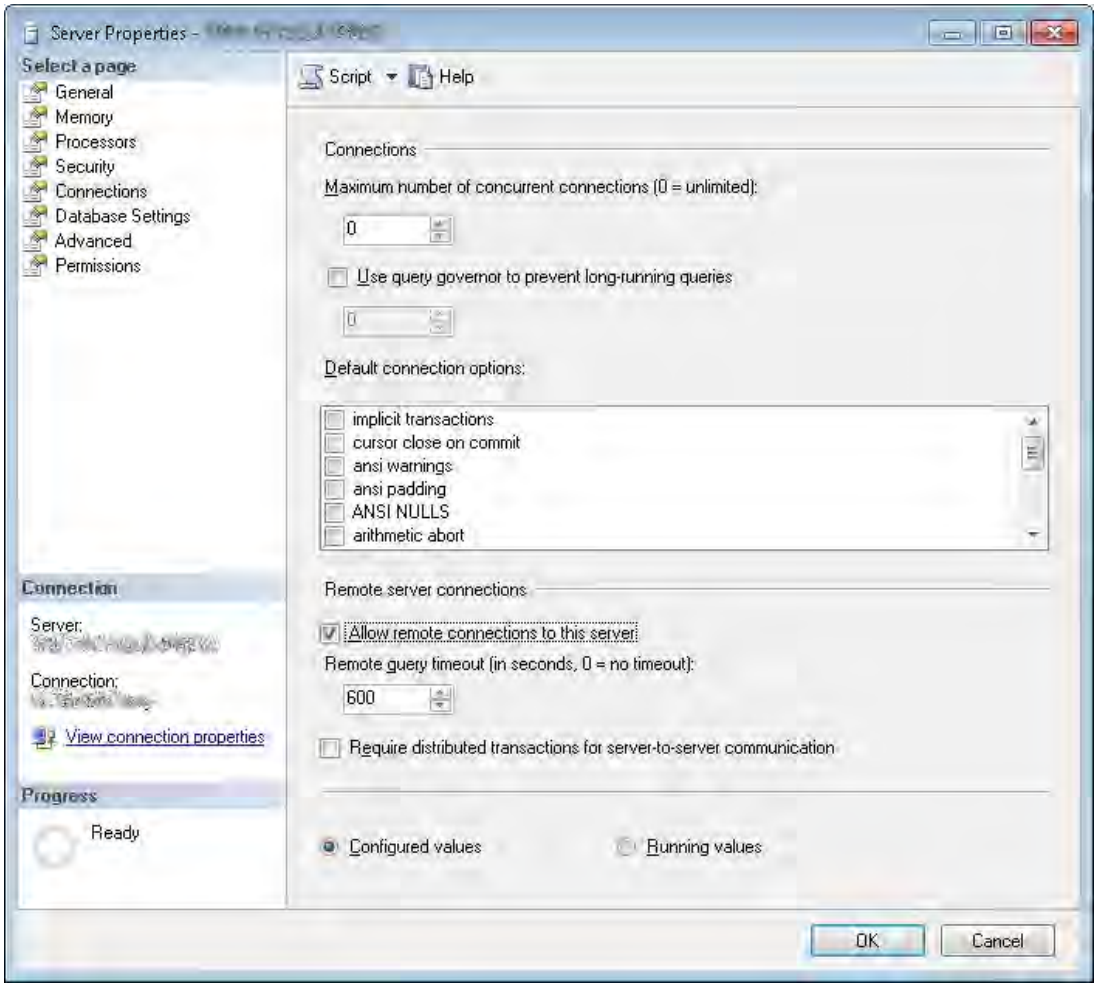


Fig. 6 - SQL Server Browser "Properties/Log On" dialog.

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" check box.
5. Press "Execute" then "Finish" to complete the MySQL Server Instance Configuration Wizard.

More Information:

See UltraBac 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\ParametersSystem
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.

More Information:

See UltraBac User Manual: Exchange Agent

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.

More Information:

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 UltraBac 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**

More Information:

See UltraBac User Manual: Exchange Agent
http://technet.microsoft.com/en-us/library/bb124706(EXCHG.80).aspx
http://technet.microsoft.com/en-us/library/bb738131(EXCHG.80).aspx

UBQ000258: Adding additional packages to UBDR

UBQ ID Number: UBQ000258
Last Modified: 2015-03-25

Summary:

With the release of UltraBac's Media Builder, customers now have the ability to add additional extensions, including file(s), registry key{s) and value(s), to UBDR during the build process.

Details:

The default directory for Media Builder extension packages is: <UltraBac installation directory>\MBResoureces. There are 4 extension folders

Extensions	- Packages will be installed for any version of PE used. Source files should not be OS dependent.
Extensions.PE30	- Packages will only be installed if using Windows AIK (7) to build UBDR. Source files should come from a Windows 7 OS.
Extensions.PE40	- Packages will only be installed if using Windows ADK8 (8) to build UBDR. Source files should come from a Windows 8 OS.
Extensions.PE50	- Packages will only be installed if using Windows ADK8.1 (8.1) to build UBDR. Source files should come from a Windows 8.1 OS.

File and folder layout. As an example any files in the folder ..\<PackageName>\amd64\mount\Windows would show up in the Windows directory of the booted UBDR media (X:\Windows)

<PackageName>

amd64	- Folder containing files only for amd64 based UBDR.
mount	- Files and folders contained in this folder will be copied into the mounted WinPE root folder.
any	- Folder containing files not dependent on %processor_architecture%.
x86	- Folder containing files only for x86 based UBDR.
mount.xml	- Optional file that instructs Media Builder on what to do. Contains extension name, file(s) to copy, registry keys to add/change.

Variables used in mount.xml.

{MOUNTDIR}	- variable for the location to the mount directory used in building UBDR.
{PRODUCTDIR}	- variable pointed to the UltraBac installation folder.
{ARCH}	- specifies the subfolder name based on UBDR version being built.

Tags used in mount.xml.

<Extension>	- Name of the extension. MediaType="UBDR" should always be used.
<Files>	- file(s) to copy using Source, Destination, Name, and Language attributes.
<Reg>	- will allow you to run the reg command against the WinPE image being built.

The WinPE registry hives are loaded at the start of the build process using these names.

HKLM\Temp_System	- '{MOUNTDIR}\Windows\System32\config\SYSTEM'
HKLM\Temp_Software	- '{MOUNTDIR}\Windows\System32\config\SOFTWARE'
HKLM\Temp_User	- '{MOUNTDIR}\Windows\System32\config\USER'
HKLM\Temp_Default	- '{MOUNTDIR}\Windows\System32\config\DEFAULT'

NOTE: If the Source attribute is not used, copy command assumes the file is in the same directory as 'mount.xml'. If the Language attribute is listed, the file will only be copied if building that language version of UBDR.

```
</Files Destination="{MOUNTDIR}\Windows\System32">
	<File Name="WinPE.bmp"/>
</Files>
	<Files Source="{PRODUCTDIR}\Data" Destination="{MOUNTDIR}\UBDR\Data">
	<File Name="defaulthtmllogss.xsl"/>
	<File Name="defaulthtmllogssFRA.xsl" Language="FRA"/>
	<File Name="defaulthtmllogssJPN.xsl" Language="JPN"/>
	<File Name="defaultlogss.xsl"/>
	<File Name="defaultlogssFRA.xsl" Language="FRA"/>
	<File Name="defaultlogssJPN.xsl" Language="JPN"/>
</Files>
```

As an example, this article will create an iSCSI extension package, with source files from a Windows 7 64bit installation.
Open a command prompt and run these commands to create the nessessary directory structure in '..\UltraBac\MBResources\Extensions.PE30'

```
mkdir "C:\Program Files\UltraBac Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Windows\System32"
mkdir "C:\Program Files\UltraBac Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Windows\System32\Drivers"
mkdir "C:\Program Files\UltraBac Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Windows\System32\en-US"
```

Create the file "C:\Program Files\UltraBac Software\UltraBac\MBResources\Extensions.PE30\iSCSI\Mount.xml" for iSCSI extension package. Then copy and paste the following XML code into the file.

```
<?xml version="1.0"?>
<Extension Name="iSCSI" MediaType="UBDR">
```

```
     <Reg>
             <Command Value="add
'HKLM\Temp_Software\Microsoft\Windows NT\CurrentVersion\Svchost' /V
'Godzilla' /T REG_MULTI_SZ /D MSiSCSI /F"/>
             <Command Value="add
'HKLM\Temp_Software\Microsoft\Windows NT\CurrentVersion\iSCSI'
/F"/>
             <Command Value="add
'HKLM\Temp_Software\Microsoft\Windows
NT\CurrentVersion\iSCSI\Discovery' /V 'AllowiSNSFirewallException'
/T REG_DWORD /D 0x00000001 /F"/>
             <Command Value="add
'HKLM\Temp_Software\Microsoft\Windows
NT\CurrentVersion\iSCSI\Discovery\Authentication Cache' /F"/>
             <Command Value="add
'HKLM\Temp_Software\Microsoft\Windows
NT\CurrentVersion\iSCSI\Discovery\Send Targets' /F"/>
             <Command Value="add
'HKLM\Temp_Software\Microsoft\Windows
NT\CurrentVersion\iSCSI\Discovery\Static Targets' /F"/>
             <Command Value="add
'HKLM\Temp_Software\Microsoft\Windows
NT\CurrentVersion\iSCSI\Discovery\Tunnel Address' /F"/>
             <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\LEGACY_MSISCSI' /V
'NextInstance' /T REG_DWORD /D 0x00000001 /F"/>
             <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\LEGACY_MSISCSI\0000' /V
'Service' /T REG_SZ /D 'MSiSCSI' /F"/>
             <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\LEGACY_MSISCSI\0000' /V
'Legacy' /T REG_DWORD /D 0x00000001 /F"/>
             <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\LEGACY_MSISCSI\0000' /V
'ConfigFlags' /T REG_DWORD /D 0x00000000 /F"/>
             <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\LEGACY_MSISCSI\0000' /V
'Class' /T REG_SZ /D 'LegacyDriver' /F"/>
             <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\LEGACY_MSISCSI\0000' /V
'ClassGUID' /T REG_SZ /D '{8ECC055D-047F-11D1-A537-0000F8753ED1}'
/F"/>
             <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\LEGACY_MSISCSI\0000' /V
'DeviceDesc' /T REG_SZ /D '@%SystemRoot%\\system32\\iscsidsc.dll,-
5000' /F"/>
             <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\LEGACY_MSISCSI\0000\Contr
ol' /V 'ActiveService' /T REG_SZ /D 'MSiSCSI' /F"/>
             <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT' /F"/>
             <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000' /V
'ClassGUID' /T REG_SZ /D '{4d36e97b-e325-11ce-bfc1-08002be10318}'
/F"/>
```

```
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000' /V 'Class'
/T REG_SZ /D 'SCSIAdapter' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000' /V
'HardwareID' /T REG_MULTI_SZ /D 'ROOT\iSCSIPrt' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000' /V
'ConfigFlags' /T REG_DWORD /D 0x00000000 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000' /V
'Driver' /T REG_SZ /D '{4d36e97b-e325-11ce-bfc1-
08002be10318}\\0000' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000' /V 'Mfg'
/T REG_SZ /D '@iscsi.inf,%msft%;Microsoft' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000' /V
'Service' /T REG_SZ /D 'iScsiPrt' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000' /V
'DeviceDesc' /T REG_SZ /D '@iscsi.inf,%iscsiprt%;Microsoft iSCSI
Initiator' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000' /V
'Capabilities' /T REG_DWORD /D 0x00000000 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000\Device
Parameters' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000\Device
Parameters\StorPort' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000\LogConf'
/F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Enum\Root\ISCSIPRT\0000\Control' /V
'ActiveService' /T REG_SZ /D 'iScsiPrt' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\iScsiPrt' /V 'DisplayName'
/T REG_SZ /D 'iScsiPort Driver' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\iScsiPrt' /V 'ImagePath'
/T REG_EXPAND_SZ /D 'system32\DRIVERS\msiscsi.sys' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\iScsiPrt' /V
'ErrorControl' /T REG_DWORD /D 0x00000001 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\iScsiPrt' /V 'Start' /T
REG_DWORD /D 0x00000003 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\iScsiPrt' /V 'Type' /T
REG_DWORD /D 0x00000001 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\iScsiPrt\Parameters' /V
'BusType' /T REG_DWORD /D 0x00000009 /F"/>
```

```
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\iScsiPrt\Enum' /V '0' /T
REG_SZ /D 'Root\\ISCSIPRT\\0000' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\iScsiPrt\Enum' /V 'Count'
/T REG_DWORD /D 0x00000001 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\iScsiPrt\Enum' /V
'NextInstance' /T REG_DWORD /D 0x00000001 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V 'DisplayName'
/T REG_SZ /D '@%SystemRoot%\\system32\\iscsidsc.dll,-5000' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V 'Group' /T
REG_SZ /D 'iSCSI' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V 'ImagePath' /T
REG_EXPAND_SZ /D '%systemroot%\system32\svchost.exe -k Godzilla'
/F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V 'Description'
/T REG_SZ /D '@%SystemRoot%\\system32\\iscsidsc.dll,-5001' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V 'ObjectName'
/T REG_SZ /D 'LocalSystem' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V 'ErrorControl'
/T REG_DWORD /D 0x00000001 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V 'Start' /T
REG_DWORD /D 0x00000003 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V 'Type' /T
REG_DWORD /D 0x00000020 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V
'ServiceSidType' /T REG_DWORD /D 0x00000001 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V
'RequiredPrivileges' /T REG_MULTI_SZ /D
'SeAuditPrivilege\0SeChangeNotifyPrivilege\0SeCreateGlobalPrivilege
\0SeCreatePermanentPrivilege\0SeImpersonatePrivilege\0SeTcbPrivileg
e' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V
'FailureActionsOnNonCrashFailures' /T REG_DWORD /D 0x00000001 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V
'FailureActions' /T REG_BINARY /D
504600000100000001000000030000001400000001000000c0d4010001000000e09
3040000000000000000 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V
'RebootMessage' /T REG_SZ /D 'iSCSI Failure' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI' /V
'FailureCommand' /T REG_SZ /D  /F"/>
```

```
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI\Parameters' /V
'ServiceDll' /T REG_EXPAND_SZ /D
'%systemroot%\system32\iscsiexe.dll' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI\Parameters' /V
'ServiceDllUnloadOnStop' /T REG_DWORD /D 0x00000001 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI\Enum' /V '0' /T
REG_SZ /D 'Root\\LEGACY_MSISCSI\\0000' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI\Enum' /V 'Count'
/T REG_DWORD /D 0x00000001 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Services\MSiSCSI\Enum' /V
'NextInstance' /T REG_DWORD /D 0x00000001 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}' /V 'LegacyAdapterDetection' /T REG_DWORD /D
0x00000000 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}' /V 'Class' /T REG_SZ /D 'SCSIAdapter' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}' /V 'ClassDesc' /T REG_SZ /D
'@%SystemRoot%\\System32\\SysClass.Dll,-3005' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}' /VE /T REG_SZ /D 'Storage Controllers' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}' /V 'IconPath' /T REG_MULTI_SZ /D
'%SystemRoot%\System32\setupapi.dll,-10' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}' /V 'Installer32' /T REG_SZ /D
'SysClass.Dll,ScsiClassInstaller' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000' /V 'InfPath' /T REG_SZ /D 'iscsi.inf'
/F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000' /V 'InfSection' /T REG_SZ /D
'iScsiPort_Install_Control' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000' /V 'ProviderName' /T REG_SZ /D 'Microsoft'
/F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000' /V 'DriverDateData' /T REG_BINARY /D
00808ca3c594c601 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
```

```
BFC1-08002BE10318}\0000' /V 'DriverDate' /T REG_SZ /D '6-21-2006'
/F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000' /V 'DriverVersion' /T REG_SZ /D
'6.1.7600.16385' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000' /V 'MatchingDeviceId' /T REG_SZ /D
'root\\iScsiPrt' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000' /V 'DriverDesc' /T REG_SZ /D 'Microsoft
iSCSI Initiator' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000' /V 'EnumPropPages32' /T REG_SZ /D
'iscsipp.dll,iSCSIPropPageProvider' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'DelayBetweenReconnect' /T
REG_DWORD /D 0x00000005 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'EnableNOPOut' /T REG_DWORD
/D 0x00000000 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'ErrorRecoveryLevel' /T
REG_DWORD /D 0x00000002 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'FirstBurstLength' /T
REG_DWORD /D 0x00010000 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'ImmediateData' /T REG_DWORD
/D 0x00000001 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'InitialR2T' /T REG_DWORD /D
0x00000000 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'IPSecConfigTimeout' /T
REG_DWORD /D 0x0000003c /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'LinkDownTime' /T REG_DWORD
/D 0x0000000f /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'MaxBurstLength' /T
REG_DWORD /D 0x00040000 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
```

```
BFC1-08002BE10318}\0000\Parameters' /V 'MaxConnectionRetries' /T
REG_DWORD /D 0xffffffff /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'MaxPendingRequests' /T
REG_DWORD /D 0x000000ff /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'MaxRecvDataSegmentLength'
/T REG_DWORD /D 0x00010000 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'MaxRequestHoldTime' /T
REG_DWORD /D 0x0000003c /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'MaxTransferLength' /T
REG_DWORD /D 0x00040000 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'NetworkReadyRetryCount' /T
REG_DWORD /D 0x0000000a /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'PortalRetryCount' /T
REG_DWORD /D 0x00000005 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'SrbTimeoutDelta' /T
REG_DWORD /D 0x0000000f /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'TCPConnectTime' /T
REG_DWORD /D 0x0000000f /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'TCPDisconnectTime' /T
REG_DWORD /D 0x0000000f /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\Parameters' /V 'WMIRequestTimeout' /T
REG_DWORD /D 0x0000001e /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\0000\PersistentTargets' /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\Properties' /V 'DeviceType' /T REG_DWORD /D
0x00000004 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\Properties' /V 'DeviceCharacteristics' /T
REG_DWORD /D 0x00000100 /F"/>
            <Command Value="add
'HKLM\Temp_System\ControlSet001\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\Properties' /V 'Security' /T REG_BINARY /D
0100049000000000000000000000000014000000020034000200000000001400ff0
```

```
11f1001010000000000051200000000001800ff011f1001020000000000052000000020020000 /F"/>
     </Reg>
</Extension>
```

After the "mount.xml" has been created, you will need to copy the necessary iSCSI files into the previously created package folders. Use the following commands and paste into a Windows command prompt.

```
copy %windir%\System32\iscsicli.exe "C:\Program Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32"
copy %windir%\System32\iscsicpl.dll "C:\Program Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32"
copy %windir%\System32\iscsicpl.exe "C:\Program Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32"
copy %windir%\System32\iscsidsc.dll "C:\Program Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32"
copy %windir%\System32\iscsied.dll "C:\Program Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32"
copy %windir%\System32\iscsiexe.dll "C:\Program Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32"
copy %windir%\System32\iscsium.dll "C:\Program Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32"
copy %windir%\System32\iscsiwmi.dll "C:\Program Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32"
copy %windir%\System32\Drivers\msiscsi.sys "C:\Program
Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32\Drivers"
copy %windir%\System32\en-US\iscsicli.exe.mui "C:\Program
Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32\en-US"
copy %windir%\System32\en-US\iscsicpl.dll.mui "C:\Program
Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32\en-US"
copy %windir%\System32\en-US\iscsicpl.exe.mui "C:\Program
Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32\en-US"
copy %windir%\System32\en-US\iscsiexe.dll.mui "C:\Program
Files\UltraBac
Software\UltraBac\MBResources\Extensions.PE30\iSCSI\AMD64\Mount\Win
dows\System32\en-US"
```

Once the files have been copied, simply launch UltraBac's Media Builder and build UBDR using "7" for the Widows ADK/AIK Version.

More Information:

See UltraBac User Manual: UBDR
See UltraBac User Manual: Media Builder

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:

In the Exchange Management Shell type:

Restore-Mailbox -ID 'UltraBac User1' -RecoveryDatabase RESTORE1

More Information:

See UltraBac User Manual: Exchange Agent
http://technet.microsoft.com/en-us/library/bb125218.aspx

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.

More Information:

See UltraBac User Manual: Storage Device Manager

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

More Information:

See UltraBac User Manual: Installing UltraBac

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.

More Information:

See UltraBac User Manual: Exchange Agent

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
4. For the Value enter: 1

NOTE: This process will need to be completed for each backup path that requires this functionality.

More Information:

See UltraBac User Manual: Storage Device Manager

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.

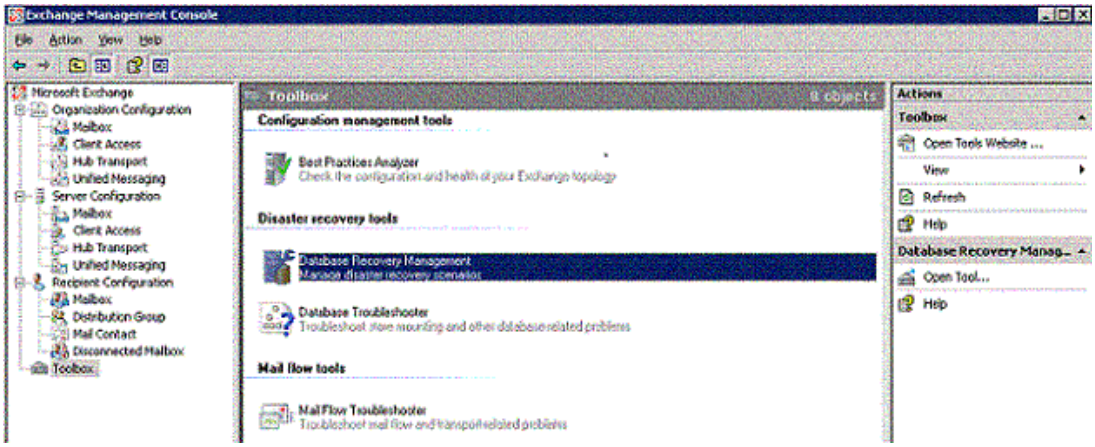


Fig. 1 - Exchange Management Console

2. Type the name of your Exchange server as well as the Domain Controller name, then click "Next" at the bottom of the screen.

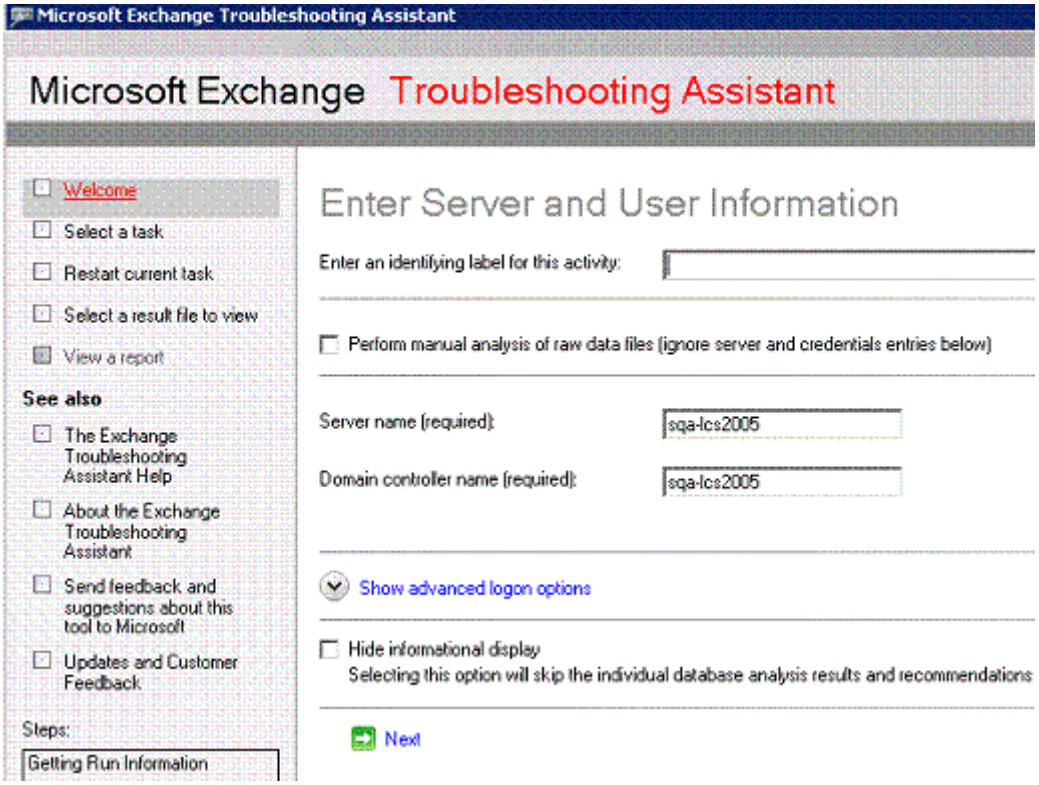


Fig. 2 - Exchange Troubleshooting Assistant

3. From the Tasks options, choose Manage Recovery Storage Group and then click on "Create a recovery storage group."

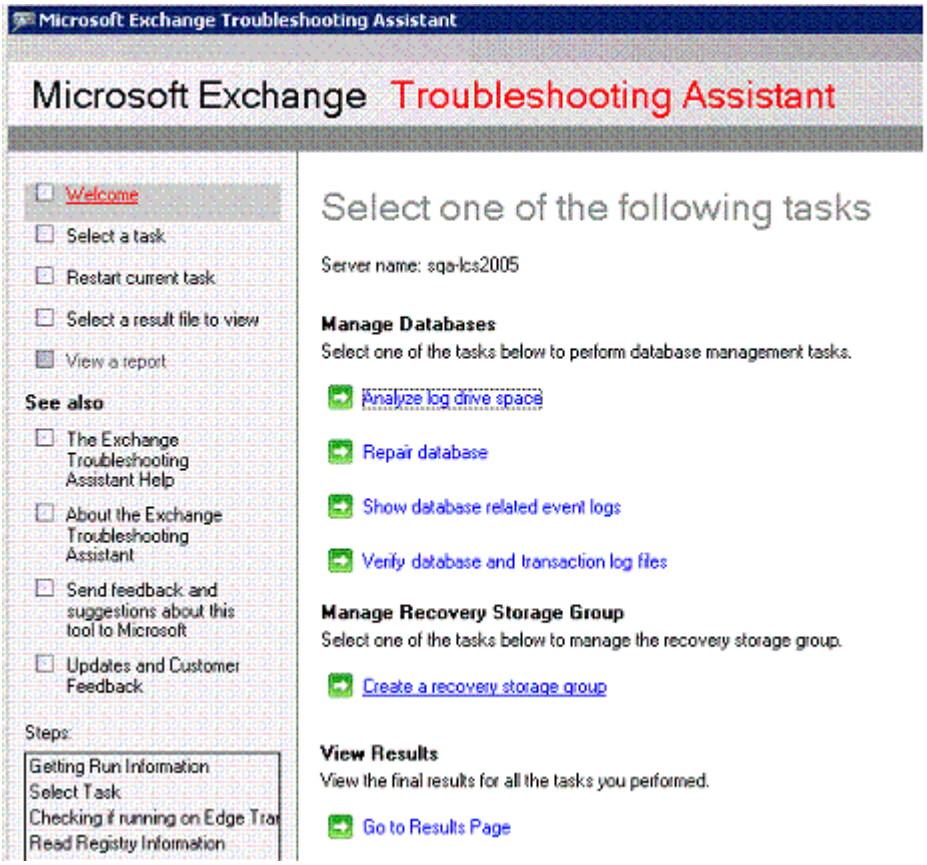


Fig. 3 - Options to create Recovery Storage Group

4. Select the Storage Group that you want to restore from and click "Next."

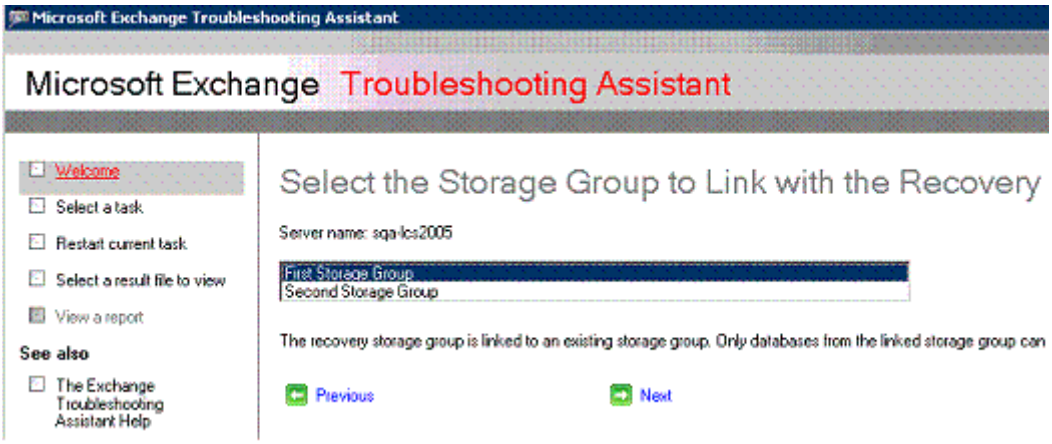


Fig. 4 - Selecting database in which to create the Recovery Storage Group

5. Choose the location to create the Recovery Storage Group.

NOTE:UltraBac strongly recommends users keep everything in the same location.

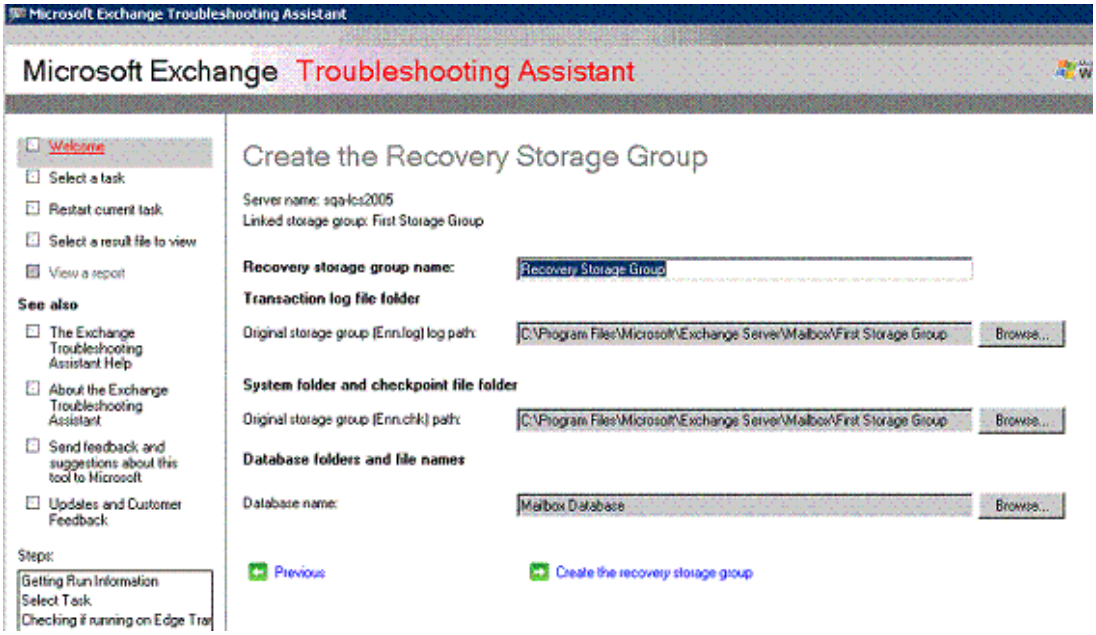


Fig. 5 - Enter name of the new Recovery Storage Group.

6. Finish the Recovery Storage Group creation.

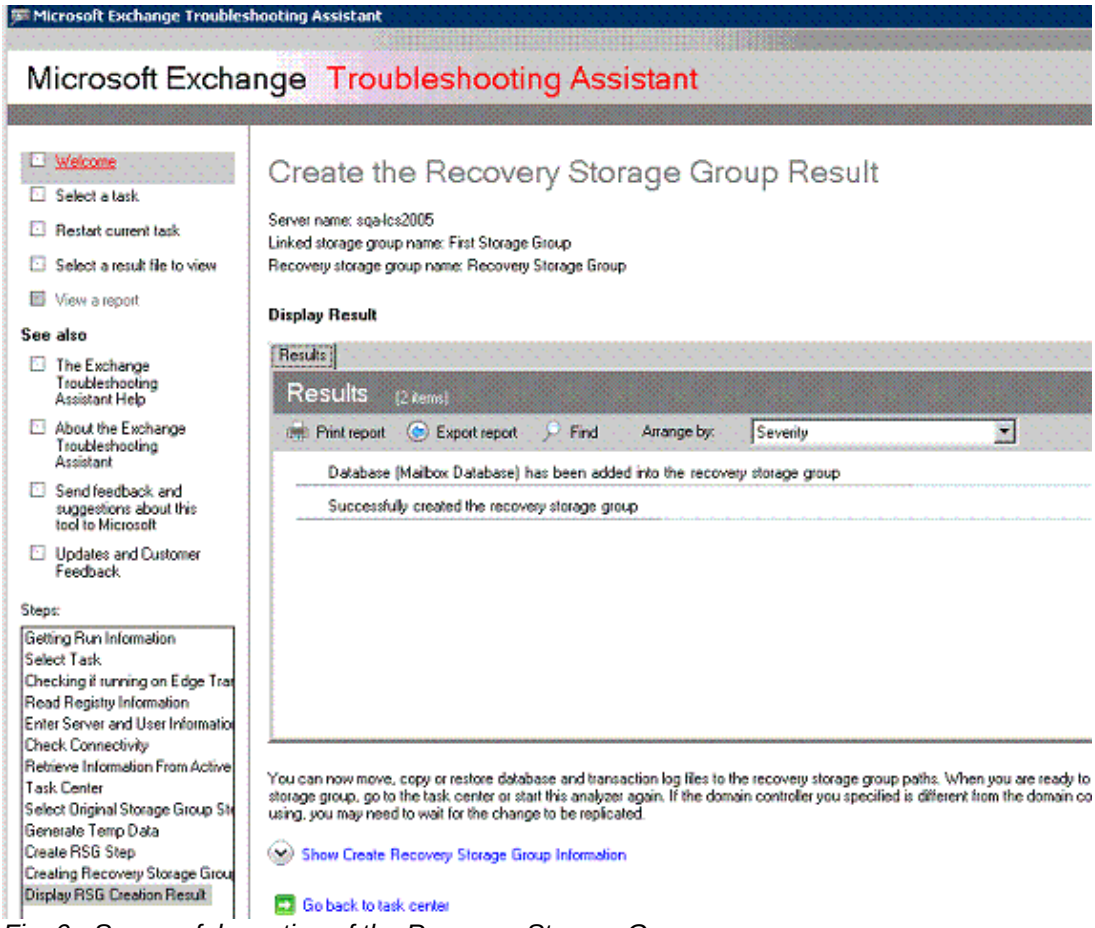


Fig. 6 - Successful creation of the Recovery Storage Group

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 Agent Restore.

> NOTE: Information on doing a standard Exchange Agent Restore:
>
> **See UltraBac User Manual: Exchange Agent**

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.

> NOTE: Information on Restoring Exchange to a "Flat File" :
>
> **See UltraBac User Manual: Exchange Agent**

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.

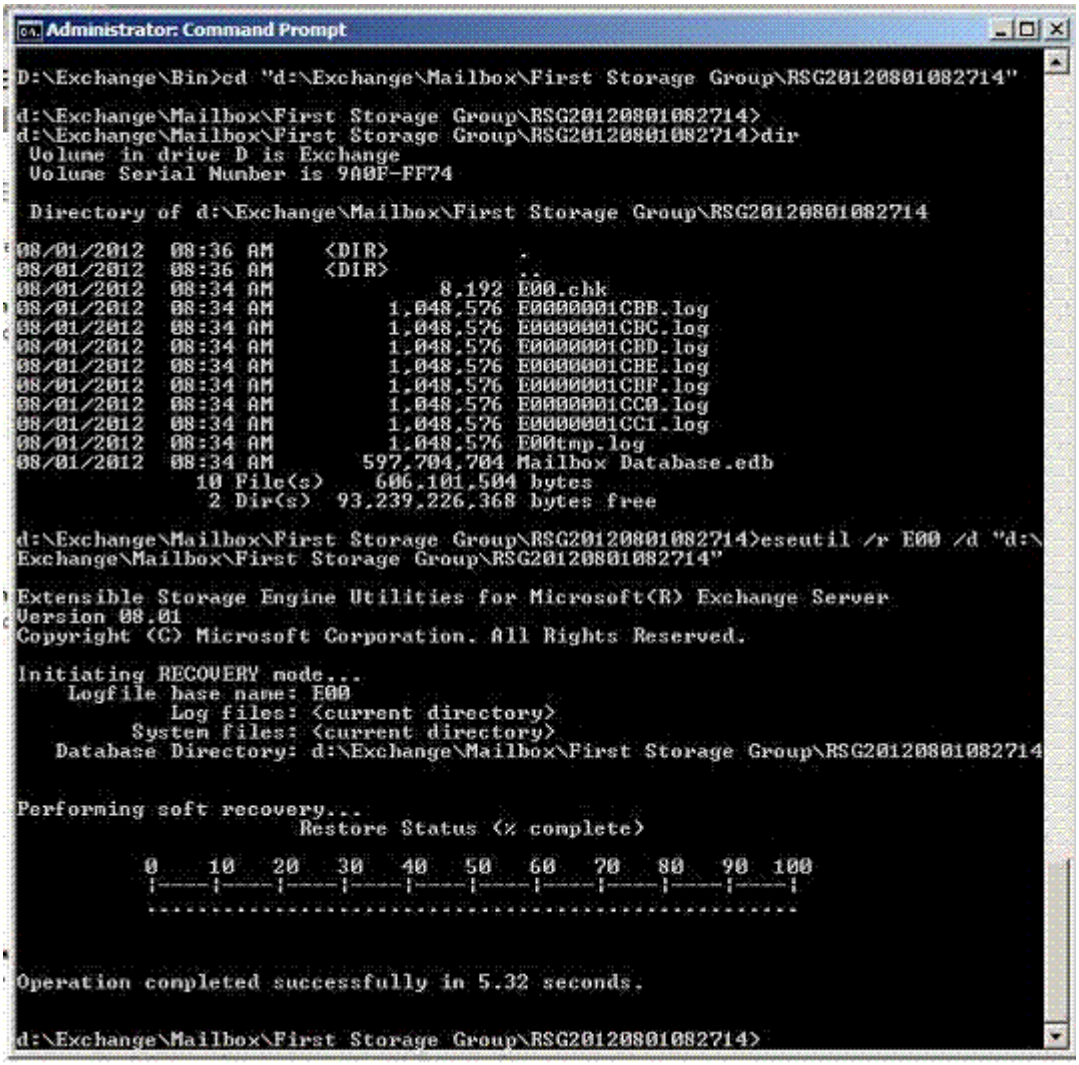


Fig. 7 - Example of a soft recovery via command line

5. Mount the Recovery Storage Group.

More Information:

See UltraBac User Manual: Exchange Agent

For more information on using a Recovery Storage Group, please visit the Microsoft Web site: Microsoft Technet: Recovery Storage Groups

For more information on Exchange Volume Shadow (VSS) Copy support, please visit: http://technet.microsoft.com/en-us/library/dd233256%28v=exchg.80%29.aspx.

UBQ000266: 1450 Errors During Backup

UBQ ID Number: UBQ000266
Last Modified: 2012-12-12

Summary:

During Backup or Verify you may get the following error during backup:

> Skipped Error: (1450 - Insufficient system resources exist to complete the requested service.) See https://www.ultrabac.com/kb/error.asp?error=2907&detail=1450 for additional information.

Details:

This error can be caused by two issues:

- Lack of system resources during backup.
- The system is running a 32-bit OS and has more than 3 GB of system memory.

This error most commonly occurs on 32-bit systems that have more than 3 GB of memory. For information on how to resolve this issue, please review the following KB article:

> http://support.microsoft.com/kb/304101/en-us

If you have less than 3 GB of memory, this error may be occurring due to lack of resources. To identify if this is the issue you are experiencing, the Microsoft Performance Monitor is a good tool. Information on how to use the monitor can be found here:

> http://technet.microsoft.com/en-us/library/cc749115.aspx

More Information:

UBQ000267: 2008 / 2008R2 Core Installation and Backups

UBQ ID Number: UBQ000267
Last Modified: 2012-12-12

Summary:

Due to limitations in 2008 / 2008 R2 Core, UltraBac has some limitations. This article will explain how to make UltraBac function.

Detail:

Installation:

Due to the Windows Shell not being present, our installer will not fully function as it calls on components of the Windows Shell. There are two ways you can install UltraBac:

Install UltraBac locally:

1. Copy the UltraBac installation zip file locally.
2. Extract the files from the zip file.
3. Explore to the location where you extracted the files, and go to the ubinstall folder.
4. Run the setup.exe file.
5. UltraBac will install normally.

Install UltraBac remotely:

1. Go to a machine that has UltraBac already installed.
2. Go to the "Tools" tab.
3. Click on "Deploy."
4. Choose the option to "Install UltraBac."
5. Click "Add Machine" if the computer is not listed.
6. Put a check mark next to the machine you want to install to.
7. Click "Install."
8. Optional: You can choose the options to "copy the license" or "replicate account information."

NOTE: For more information on installing UltraBac, please visit the "**Installing UltraBac**" section of the User Manual:

UltraBac User Manual: Installing UltraBac

9. Click "Next."
10. Choose the location to install to and click "Next."
11. Agree to the License Agreement and click "Next."
12. Choose "Full Install" and click "Next."
13. On the Setup Summary Screen click "Next."
14. UltraBac will now install.

Backups:

You can only back up 2008 / 2008r2 Core machines remotely. Due to the Windows Shell not being present, when you create a back up set locally you cannot save the set. The remote backups can be set up the same way you back up a normal Windows machine.

Restore:

Restores can be preformed both remotely and locally.

More Information:

See UltraBac User Manual: Installing UltraBac

UBQ000268: Additional steps for UBDR restore of Windows 7, 2008 R2, and newer Operating Systems.

UBQ ID Number: UBQ000268
Last Modified: 2012-12-12

Summary:

After completing a dissimilar hardware restore, or a restore to a larger partition of Windows 7, 2008R2 or later, you will receive a message saying the boot manager is missing. Please perform the following steps to resolve the issue using the BootRec command.

Details:

After the restore (using UBDR 5 or later), go to "Tools"/"UBDR"/"Command Prompt" and type the following commands in the following order:

```
diskpart
sel disk 0
sel part 1
list vol
        (to find which drive letters are used)
assign letter D
        (or whichever letter is free)
sel part 2
assign letter C
        (or whichever letter is free)
exit
attrib d:\boot\bcd -s -r -h
        (if D was not assigned, use whichever letter was assigned to the partition with the
        "\boot\bcd" directory)
rename d:\boot\bcd bcd.old
        (if D was not assigned, use whichever letter was assigned to the partition with the
        "\boot\bcd" directory)
bootrec /rebuildbcd
```

It will prompt you to add the installation to the boot list. Type "yes" and hit Enter, and then type the following command:

```
attrib d:\boot\bcd +s +r +h
```

Remove the UBDR CD and reboot back into Windows.

If the restore has already been completed and the system rebooted, boot back into UBDR and skip the following commands:

```
assign letter D
sel part 2
assign letter C
```

NOTE: For more information about the BootRec command please see the Microsoft KB article:

http://support.microsoft.com/kb/927392

More Information:

See UltraBac User Manual: UBDR

UBQ000269: Error 0076: UltraBac Exchange Agent does not support Circular Logging

UBQ ID Number: UBQ000269
Last Modified: 2013-06-10

Summary:

Circular logging must be disabled in order to run a Differential or Incremental backup of the Exchange log files.

Detail:

In order to run a Differential or Incremental backup of the Exchange server, Circular Logging must be disabled. If Circular Logging is enabled, you will receive an Error 0076 when attempting the backup.

How to enable/disable Circular Logging in Exchange 2007/2010:

http://technet.microsoft.com/en-us/library/bb331968.aspx

More Information:

See UltraBac User Manual: UltraBac Exchange Agent
http://msdn.microsoft.com/en-us/library/aa579094(v=exchg.140).aspx

UBQ000271: Managed Machines List

UBQ ID Number: UBQ000271
Last Modified: 2012-12-12

Summary:

UltraBac has the ability to store a list of servers that can be managed from one machine. From this Managed Machine list, you can easily push out an installation or upgrade to a list of machines. In UltraBac version 9.2.0 we added the option to create multiple groups of managed machines. This option is useful if you only want to install one agent, to a specific group of machines, and want to easily manage it, while installing other agents to another group.

Details:

To create a new Managed machine list:

1. Go to "Manage"/"Managed Machines" and click the "Add Group" button.

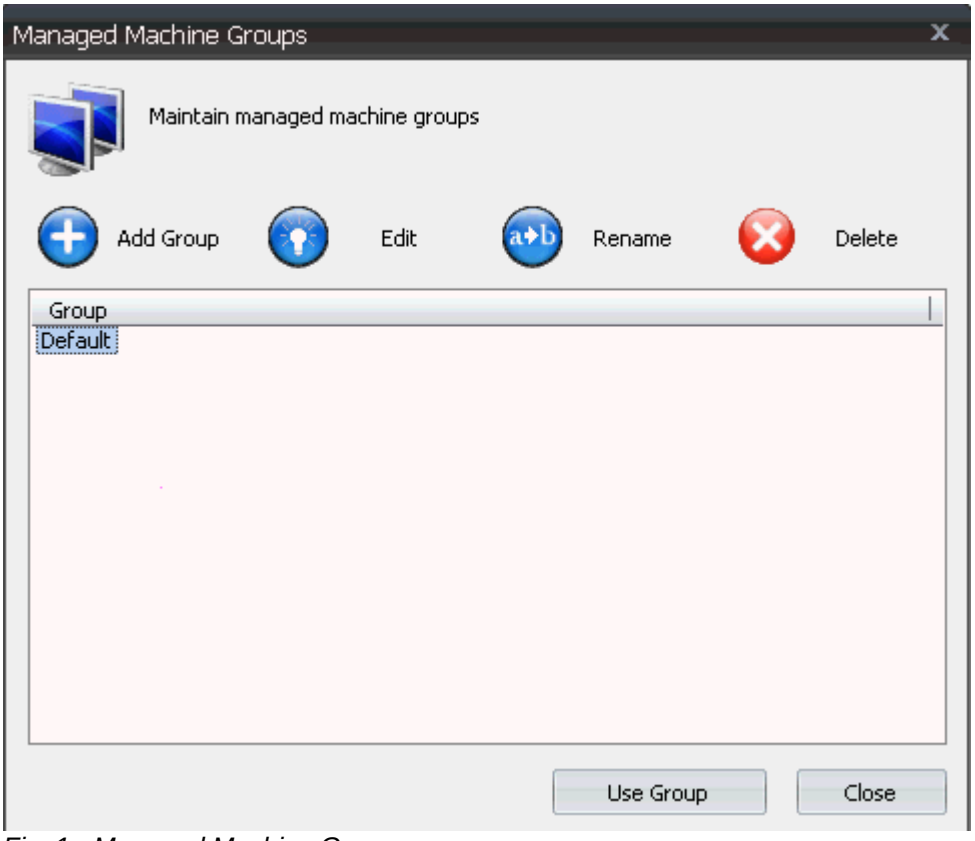


Fig. 1 - Managed Machine Groups screen

2. Enter in the name that you want to call this group.

NOTE: If you are upgrading from an older version of UltraBac, your managed machine list will be part of the group "Default."

3. Highlight the group and click "Edit."
4. Click the "Add Machine" button and add all of the machines you want to manage.

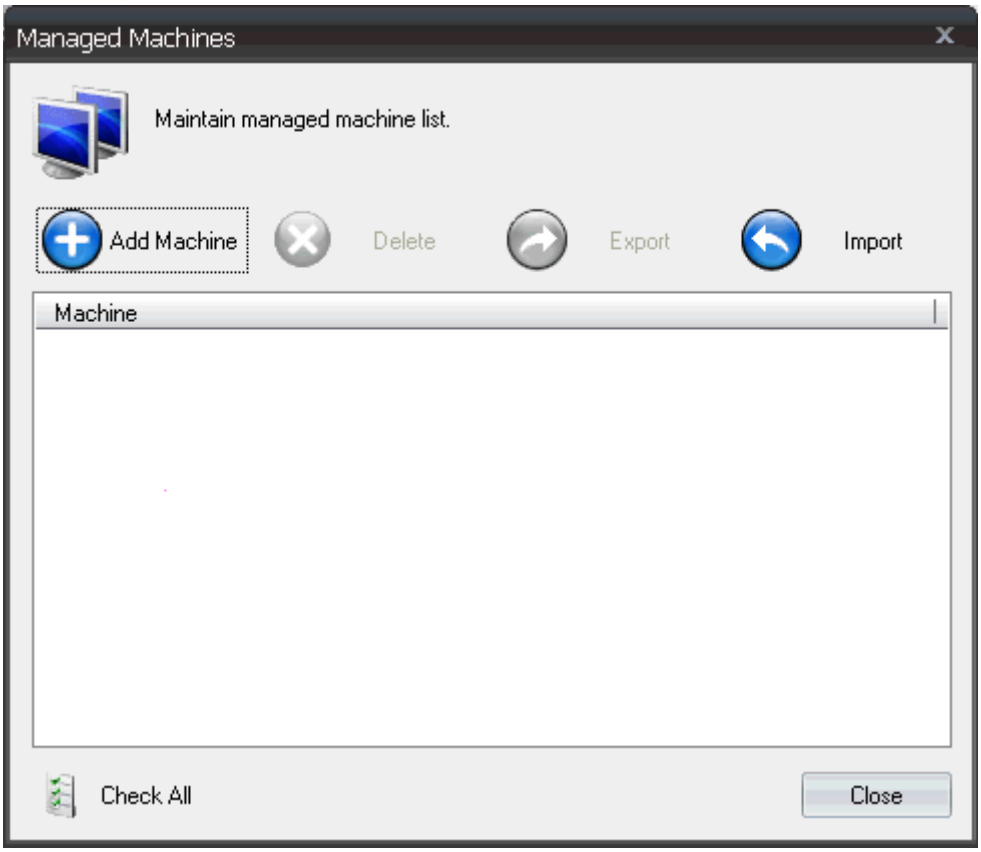


Fig. 2 - Managed Machines "Add machine" dialog.

NOTE: Do not add the name of the machine that is going to be pushing the installs to the group. This will cause the installs to fail.

Exporting / Importing Managed Machines list:

To export the Managed Machines list:

1. Go to "Manage"/"Managed Machines."
2. Highlight the group you want to export and click "Edit."
3. Click the "Export" button.
4. Choose where you want to save the file to.

To import the Manage Machines list:

1. Go to "Manage"/"Managed Machines."
2. Highlight the group you want to import and click "Edit," or create a new group.
3. Click the "Import' button.
4. Browse to where you have the Manage Machines list saved.
5. Click "Open."

More Information:

See UltraBac User Manual: UltraBac Preferences

UBQ000272: Upgrading UltraBac from Older Versions

UBQ ID Number: UBQ000272
Last Modified: 2012-12-12

Summary:

This article will explain the necessary steps of performing an upgrade from an older version of UltraBac to the latest version of UltraBac

Detail:

The current version of UltraBac can be installed over the top of previous versions back to version 8.3.1. If the existing version on your machine is older than this, UltraBac will need to be uninstalled. A reboot will be necessary, to completely remove some files, before installing the most recent version.

> NOTE: When you install UltraBac v9.x, it will convert all of the group files from txt format to xml format. These files will not be compatible with older versions of UltraBac.

Once the installation has been completed you will need to update your license file. If you need an updated license file, please contact our licensing team at Licensing@UltraBac.com or at 425-644-6000.

Recreating Backup sets / groups:

When upgrading from older versions of UltraBac some agents have been rewritten in order to be compatible with newer software versions. We strive not to have to recreate sets / groups, as it is time consuming. However, in some cases it is necessary.

You will need to recreate the following types of sets:

- Exchange Agent
- SQL Agent

Reporting Console:

Beginning with UltraBac version 9, the backup logs have changed from being txt based to xml based. You will need to update the reporting console to view the new log style. You can information on how to set it up here: https://www.ultrabac.com/kb/ubq000157.htm

> NOTE: For more information on configuring the UltraBac Centralized Reporting Console, please visit the UltraBac Knowledge Base:
>
> **See UBQ000157: Configuring the UltraBac Centralized Reporting Console**

Current Issues:

When upgrading, in some cases email notification will stop working. To fix this issue follow these steps:

1. Open the scheduled group.
2. Click on the "Notification" tab.
3. Close the group. UltraBac will update the group file and make the necessary changes.

More Information:

See UBQ000157: Configuring the UltraBac Centralized Reporting Console

UBQ000273: vSphere Agent CBT troubleshooting

UBQ ID Number: UBQ000273
Last Modified: 2013-10-01

Summary:

After a power failure or hard shutdown, you may receive a VMFS error when attempting to back up a virtual machine using the UltraBac vSphere Agent.

Details:

Problem:

After a power failure of an ESX/ESXi host, you may receive a VMFS error:

Error caused by file /vmfs/volumes/<datastore-uuid>/<vm-name>/<filename>

The problem is VMware's CBT (Changed Block Tracking). UltraBac uses CBT to perform full and incremental backups of ESX/ESXi virtual machines. Below is an explanation from VMware's knowledge base:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020128

"In some cases, such as a power failure or hard shutdown while virtual machines are powered on, CBT might reset and lose track of incremental changes. Likewise offline Storage vMotion, but not online Storage vMotion, could reset but not disable CBT."

Solution:

To reset the tracking, follow these steps:

CBT needs to be enabled when no snapshot of the VM exists (Recommended):

1. Power off the VM
2. Remove all snapshots by right clicking on the VM and selecting snapshot.
3. Disable CBT
4. Restart the VM and then shut it down
5. Enable CBT
6. Restart the VM - you must restart the VM otherwise CBT will not be activated.

To Disable/Enable CBT:

1. Right Click the VM.
2. Choose "Edit Settings"/"Options tab"/"Advanced/General"/"Configuration Parameters."

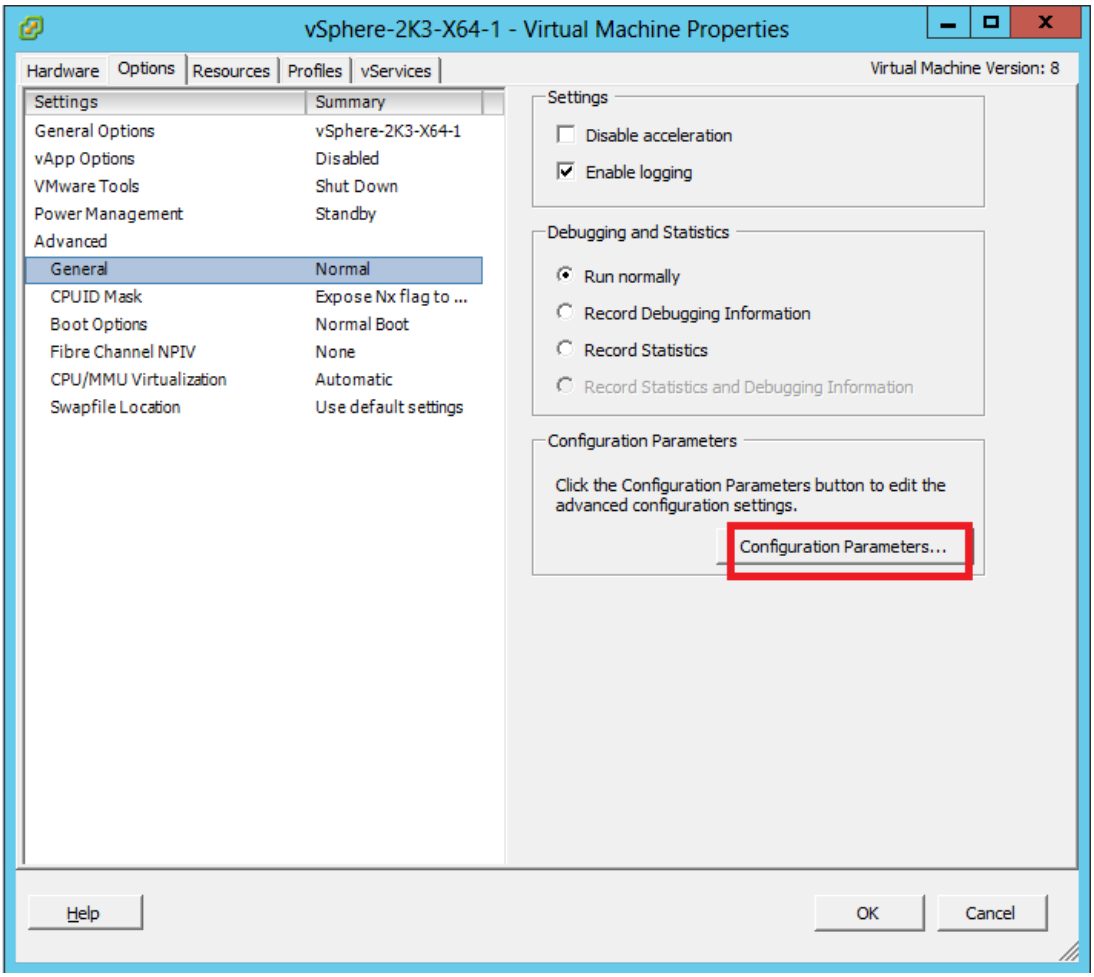


Fig. 1. Virtual Machine Properties.

3. Look for an entry "scsi0:0.ctkEnabled". If it doesn't exist, click "AddRow" and add it.
   - Depending upon the number of hard drives the VM has, there may be additional entries: "scsi0.1.ctkEnabled", "scsi0.2.ctkEnabled".
   - You will need to enable/disable for all the hard drives for this VM.

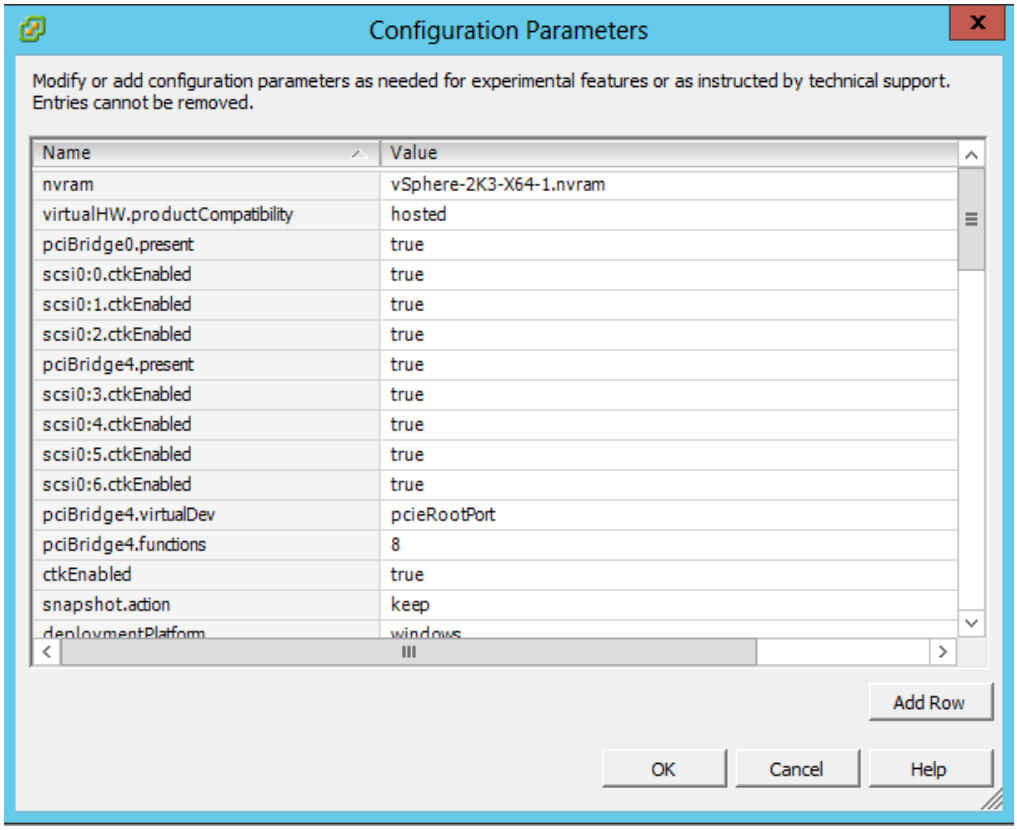


Fig. 2. Configuration Parameters.

4. To enable CBT tracking, the value needs to be "true" and to disable CBT tracking the value needs to be "false". Make sure that all values are changed before clicking "OK". Select "OK" again. The VM will reconfigure.
5. Turn on the VM and log on to the machine. Do not power down before logging in. "Shut Down" after logging in, but do not "Restart".
6. Then right Click “VM”/ “Edit Settings” / “Options” / “Advanced/General” / “Configuration Parameters.” Change all scis0:X.ctkEnabled back to true. Select "OK". Select "OK" again.
7. Turn on the VM.

More Information:

See UltraBac User Manual: vSphere Agent

The above is a temporary fix as it only fixes the corrupted CBT, but does not address the reason why it became corrupted in the first place. There are multiple reasons as to why this happens. A few will be addressed below. This is seen more frequently on vSphere 4.1. vSphere 5.0 and newer versions seem to be more stable.

Reasons for corruption:

1. Power failures and hard shut down while the VM is on.
2. Offline Storage vMotion will cause CBT tracking to be restarted.
3. VMs that have had their hardware version updated from version 4 to 7 or 8 will need to have the CBT reset.

4. Reverting a VM to an earlier snapshot. This has been fixed in vSphere 4.1 with update 3. vSphere 5.0 and later are not affected. More info on the fix can be found here: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1021607

UBQ000274: How to Fix Errors Caused by CBT Tracking

UBQ ID Number: UBQ000274
Last Modified: 2013-09-30

Summary:

Error caused by file /vmfs/volumes/<datastore-uuid>/<vm-name>/<filename>

Example: Error caused by file /vmfs/volumes/4dbb034c-a1d0b36c-1d3f-60eb696eb009/iSCSI-07x86/iSCSI-07x86.vmdk

Details:

UltraBac vSphere Agent uses VMware's CBT (Changed Block Tracking) to do both full and incremental backups. There are scenarios that cause the tracking data to become corrupted or reset.

To reset the tracking, follow these steps:

CBT needs to be enabled when no snapshot of the VM exists (Recommended).

1. Power off VM
2. Remove all snapshots by right clicking on the VM and selecting snapshot.
3. Disable CBT
4. Restart VM and then shut it down
5. Enable CBT
6. Restart VM. This step must be completed or the CBT will not be activated.

How to Disable/Enable CBT:

1. Right Click "VM"/ "Edit Settings" / "Options" / "Advanced/General" / "Configuration Parameters."

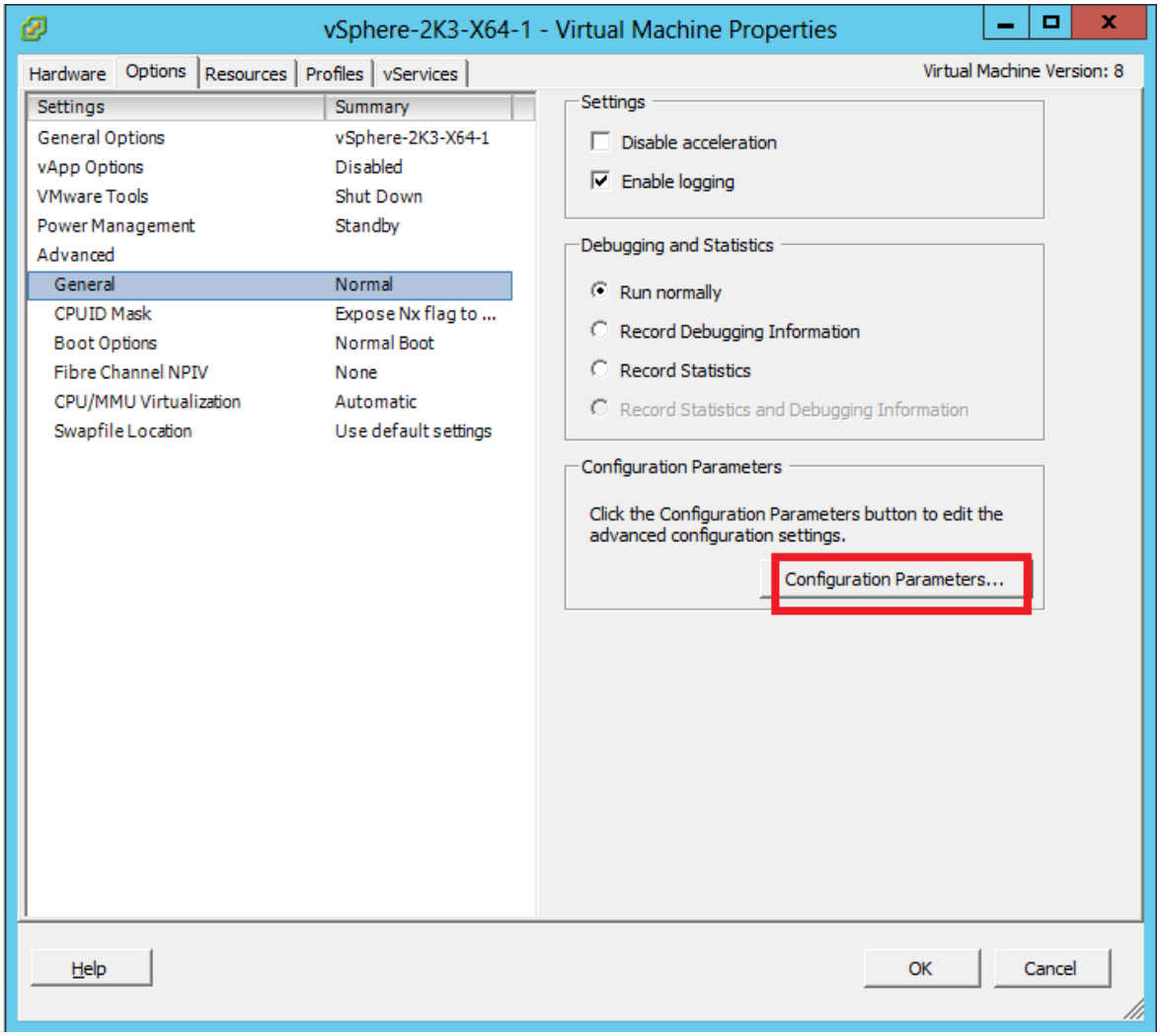


Fig. 1. Virtual Machine Properties.

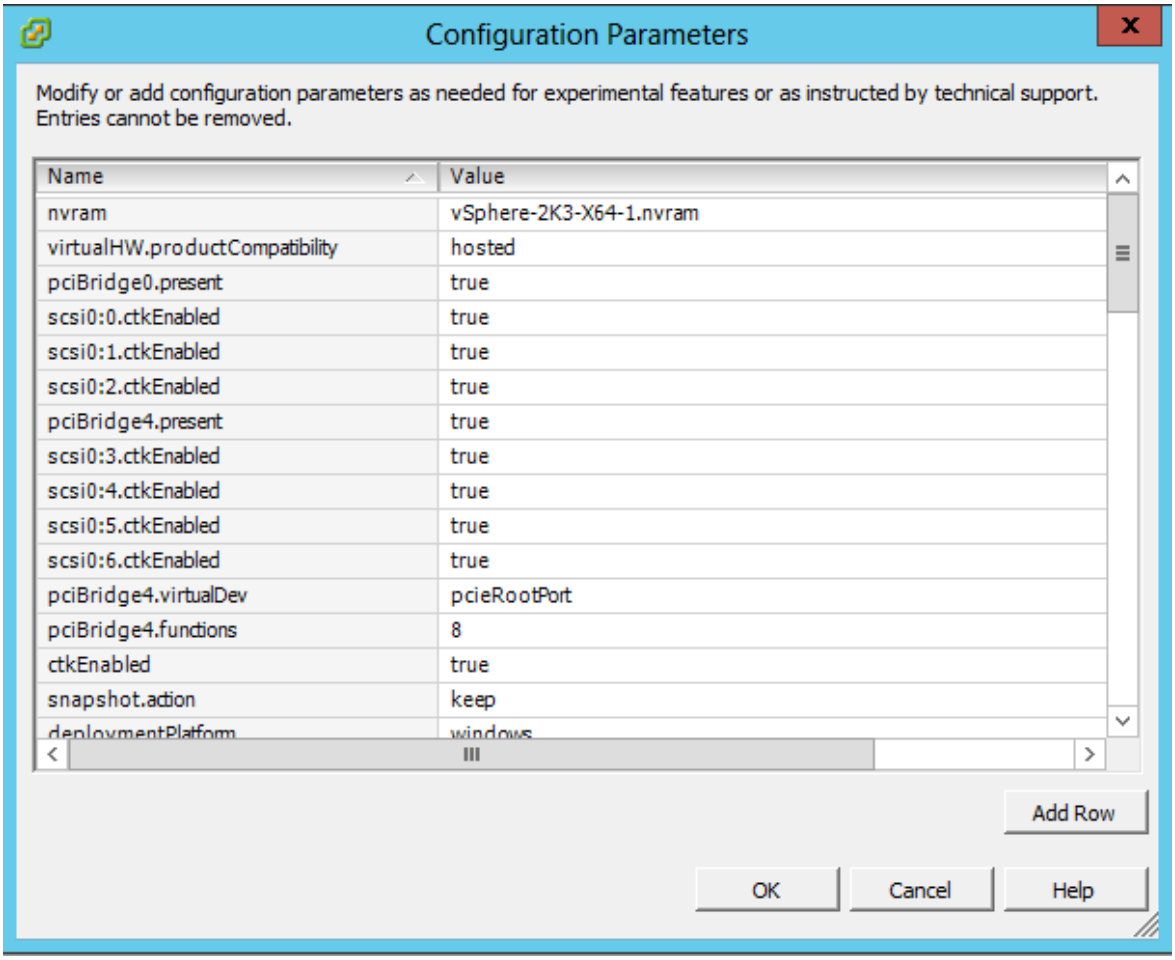


Fig. 2. Configuration Parameters.

2. scsi0:1.ctkEnabled, scsi0:2.ctkEnabled …. – The number of hard drives in VM will affect the number of entries that will be shown.

   scsi0:0.ctkEnabled – true (enable) or false (disable)

   ctkEnabled – true (enable) or false (disable)

   Make sure that all values are changed before clicking "OK". Select "OK" again. The VM will reconfigure.

3. Turn on the VM and log on to the machine. Do not power down before logging in. "Shut Down" after logging in, but do not "Restart".

4. Then right Click “VM”/ “Edit Settings” / “Options” / “Advanced/General” / “Configuration Parameters.” Change all scis0:X.ctkEnabled back to true. Select "OK". Select "OK" again.

5. Turn on the VM.

More info:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020128

The above is a temporary fix as it only fixes the corrupted CBT, but does not address the reason why it became corrupted in the first place. There are multiple reasons as to why this happens. A few will be addressed below. This is seen more frequently on vSphere 4.1. vSphere 5.0 and newer versions seem to be more stable.

Reasons for corruption:

1. Power failures and hard shut down while the VM is on.
2. Offline Storage vMotion will cause CBT tracking to be restarted.
3. VMs that have had their hardware version updated from version 4 to 7 or 8 will need to have the CBT reset.
4. Reverting a VM to an earlier snapshot. This has been fixed in vSphere 4.1 with update 3. vSphere 5.0 and later are not affected. More info on the fix can be found here: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1021607

UBQ000275: Single Mailbox Restore with Exchange 2013 Recovery DB

UBQ ID Number: UBQ000275
Last Modified: 2015-03-04

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 in Step 4 above..

7. Add the restored database to the Exchange mailbox server as a Recovery Database. This is performed using the Exchange Management Shell (EMS).
    - New-MailboxDatabase -Recovery -Name RESTORE1 -Server EXA2013 –EdbFilePath "C:\restore\Mailbox Database 1882717321.edb" -LogFolderPath "C:\Restore"

A new Recovery Database titled RESTORE1 will be created on server EXA2013 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

Mount the database using.

- Mount-Database "Database Name"

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:

New-MailboxRestoreRequest -SourceDatabase RecoveryDB -SourceStoreMailbox "UltraBac User1" -TargetMailbox UltraBac.User1 -AllowLegacyDNMismatch

Example #2 : Restoring a Inbox and all subfolders, to a different folder

This example restores 'UltraBac User2' mailbox content into a folder named "Restored Items":

In the Exchange Management Shell type:

New-MailboxRestoreRequest -SourceDatabase RecoveryDB -SourceStoreMailbox "UltraBac User2" -TargetMailbox UltraBac.User2 -TargetRootFolder "Restored Items" -IncludeFolders "#Inbox#/*"

Usefull Commands:

To verify the recovered database is mounted, run the following command;

- Get-MailboxDatabase -status "<Database Name>" | fl Mounted

To view the Mailboxes within the database, run the following command:

- Get-MailboxStatistics -Database '<Database Name>" -Recovery

To check the status of your Mailbox restore, run the following command:

- Get-MailboxRestoreRequestStatistics -Identity "<MailboxUser\RestoreRequestName>"

To restore a mailbox using the GUID, run the following command:

- New-MailboxRestoreRequest -SourceDatabase "<Database Name>" -SourceStoreMailbox "<MailboxGUID>" -TargetMailbox "<Target Mailbox Alias>" -AllowLegacyDNMismatch

NOTE: If you need to restore a mailbox and also want to restore the “deleted items” (deletions+purges+versions) you need to use the –AllowLegacyDNMismatch switch

To view the globally unique identifier (GUID) of each mailbox, run the following command:

- Get-MailboxStatistics -Database "<Database Name>" -Recovery | Format-List DisplayName, MailboxGUID

More Information:

See UltraBac User Manual: Exchange Agent
http://technet.microsoft.com/en-us/library/bb125218.aspx

UBQ000276: How to Boot a Windows Server Domain Controller into Directory Services Restore/Repair Mode

UBQ ID Number: UBQ000276
Last Modified: 2015-03-13

Summary:

NOTE: The information contained in this article was taken from a Dell knowledge base article. http://www.dell.com/support/article/us/en/19/SLN155833/EN

This document explains how to boot a Windows Server Domain Controller into Directory Services Restore/Repair Mode

Directory Services Repair Mode (DSRM, known as Directory Services Restore Mode in versions prior to Windows Server 2012) is an operating mode of a Windows Server domain controller (DC) that roughly equates to Safe Mode with Networking, but without Active Directory (AD) running. This mode is useful if there is a problem with the AD database that is preventing a DC from booting into normal mode. DSRM is used to restore AD from a backup.

Details:

To boot a Windows Server 2012 DC into DSRM locally:

1. Use one of the methods in this article to boot to the Advanced Boot Options menu.
2. Select **Directory Services Repair Mode** from the menu. The DC will boot into DSRM.

To boot a Windows Server 2012 DC into DSRM remotely:
Note: *The DC must be running and accessible via Remote Desktop.*

1. Establish a Remote Desktop session on the DC.
2. Open an elevated command prompt and type **bcdedit /set safeboot dsrepair**.
3. Reboot the DC. The Remote Desktop session will disconnect.
4. Wait a few minutes, then establish a new Remote Desktop session. The DC will be running in DSRM.
5. To reboot into normal mode, type **bcdedit /deletevalue safeboot** at an elevated command prompt and reboot the DC.

To boot a pre-Windows Server 2012 DC into DSRM locally:

1. Reboot the DC if it is running.
2. Press F8 immediately after the POST process completes to bring up the Advanced Boot Options menu.
3. Select **Directory Services Restore Mode** from the menu. The DC will boot into DSRM.

To boot a pre-Windows Server 2012 DC into DSRM remotely:
Note: *The DC must be running and accessible via Remote Desktop.*

1. Establish a Remote Desktop session on the DC.
2. **Windows Server 2008 and 2008 R2:** Open an elevated command prompt and type **bcdedit /set safeboot dsrepair**.
   Pre-Windows Server 2008: Run the **msconfig** utility and select **/SAFEBOOT** and **DSREPAIR** in the **BOOT.INI** tab. Click **OK.**
3. Reboot the DC. The Remote Desktop session will disconnect.
4. Wait a few minutes, then establish a new Remote Desktop session. The DC will be running in DSRM.
5. When you wish to reboot into normal mode, perform the following:
   Windows Server 2008 and 2008 R2: Type **bcdedit /deletevalue safeboot** at an elevated command prompt and reboot the DC.
   Pre-Windows Server 2008: Run **msconfig** and uncheck the **/SAFEBOOT** checkbox in the **BOOT.INI** tab. Click **OK** and reboot the DC.

More Information:

https://technet.microsoft.com/en-us/library/cc816897%28v=ws.10%29.aspx
https://technet.microsoft.com/en-us/library/cc794729%28v=ws.10%29.aspx

UBQ000277: Accessing the Advanced Boot Options Menu in Windows Server 2012

UBQ ID Number: UBQ000277
Last Modified: 2015-03-13

Summary:

NOTE: The information contained in this article was taken from a Dell knowledge base article. http://www.dell.com/support/article/us/en/19/SLN164148/ro

This document explains how to access the advanced boot options menu in Windows Server 2012/2012R2. This is replacement for the deprecated F8 boot option.

In previous versions of Windows Server, the preferred method of reaching the Advanced Boot Options menu was to press F8 immediately after the power-on self-test (POST) process completed. This often required numerous attempts and rapid pressing of the F8 key. Windows Server 2012 boots significantly more quickly than previous versions, making it all but impossible to press F8 at the correct time.

Details:

Method 1: Shift-Restart

1. Open the Power menu by normal means, such as via the Settings charm.
2. Hold down the Shift key and select Restart.



Fig. 1 - Shift Restart.

3. Select a reason for restarting the server and click Continue.

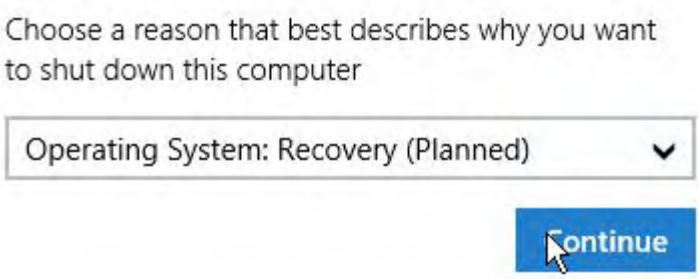


Fig. 2 - Choose reason for reboot.

4. Windows will shut down. At the Choose an option screen, select Troubleshoot.



Fig. 3 - Choose Troubleshoot option.

5. Select Startup Settings on the Advanced options screen, then click Restart.

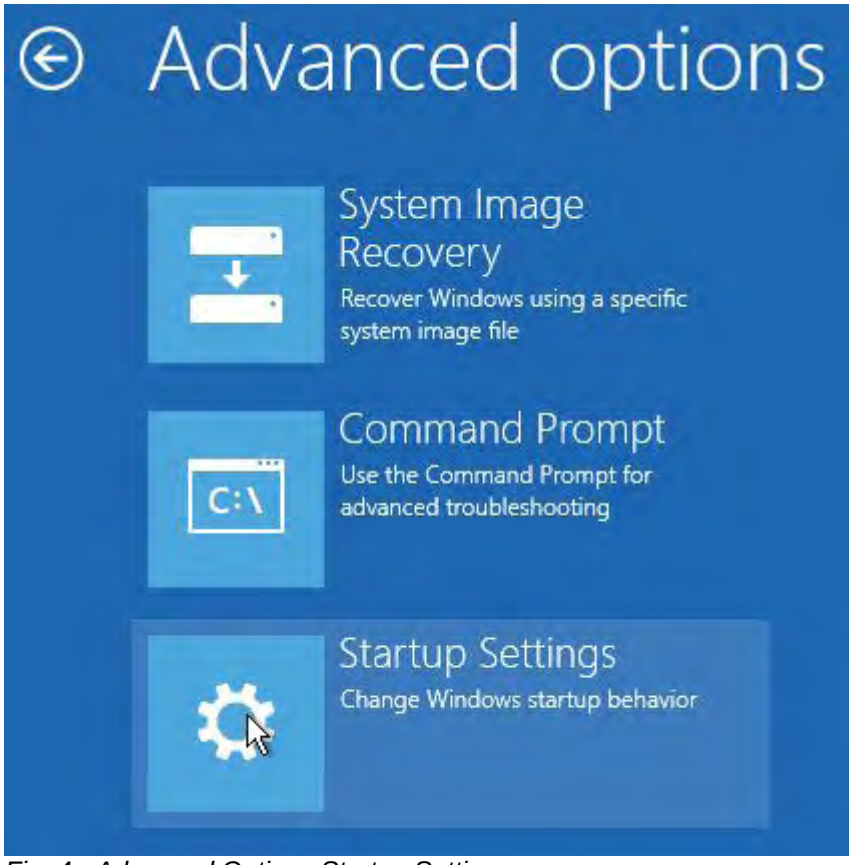


Fig. 4 - Advanced Options Startup Settings.

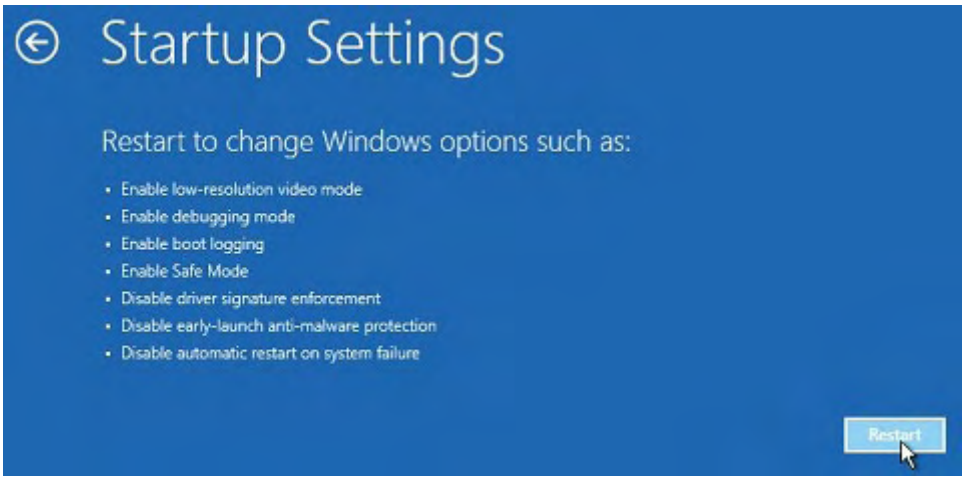


Fig. 5 - Click restart.

6. The server will POST and boot into the Advanced Boot Options menu.

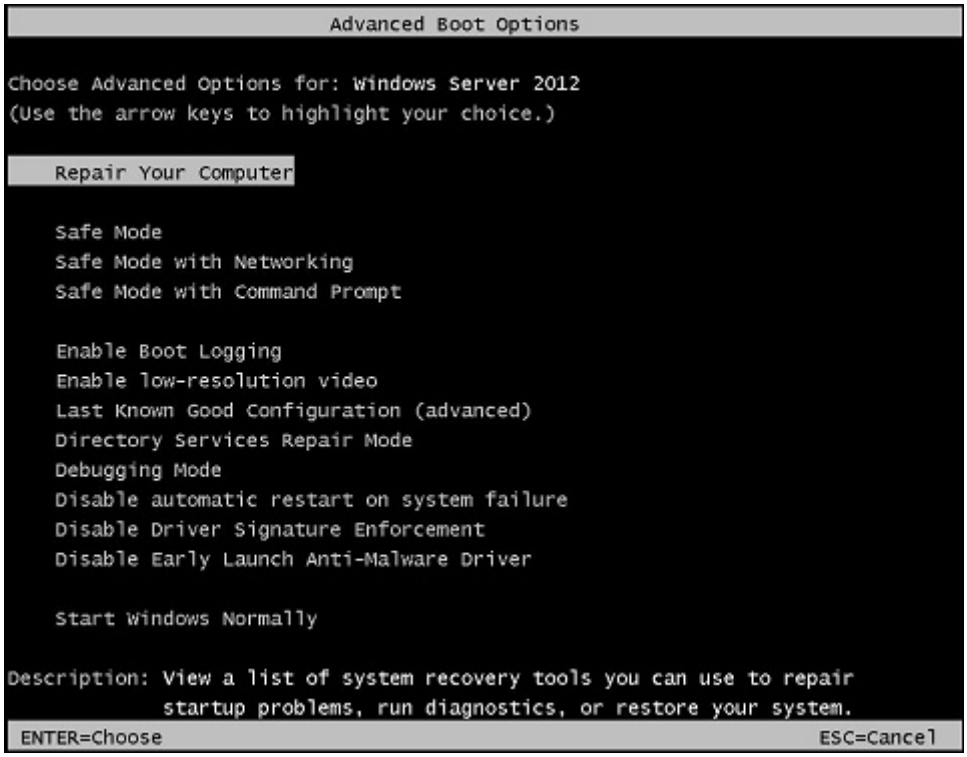


Fig. 6 - Advanced Boot Options - DSRM.

Method 2: Shutdown.exe /r /o

1. Open an elevated command prompt on the server.
2. Type shutdown /r /o to restart Windows.



Fig.6 - Elevated command prompt

NOTE: The /o switch is new in Windows Server 2012 and can only be used in conjunction with the /r switch.

3. The server will boot to the Choose an option screen. Follow steps 4-6 above to access the Advanced Boot Options menu.

UBQ000278: Configuring UltraBac Deduplication Server

UBQ ID Number: UBQ000278
Last Modified: 2015-10-22

Minimum System Requirements:

> NOTE: Machine must NOT have any other UltraBac Software components installed. It is highly recommended that the deduplication server should be dedicated explicitly as a deduplication server.

- 16GB RAM (32GB recommended, 64GB if using block store)
- Windows Server 2008R2 (2012R2 recommended)
- Microsoft .NET Framework 4.5
- 128GB Primary Drive
- If file store enabled: 100GB - 1TB Database Drive (RAID 6 or 5 recommended)
- If block store enabled: ~5% of total data size backed up

Configuring deduplication server:

After installing the UltraBac Deduplication Server, use the Start Menu to open “Configure UltraBac Deduplication Server.”

You will see a screen similar to this one:

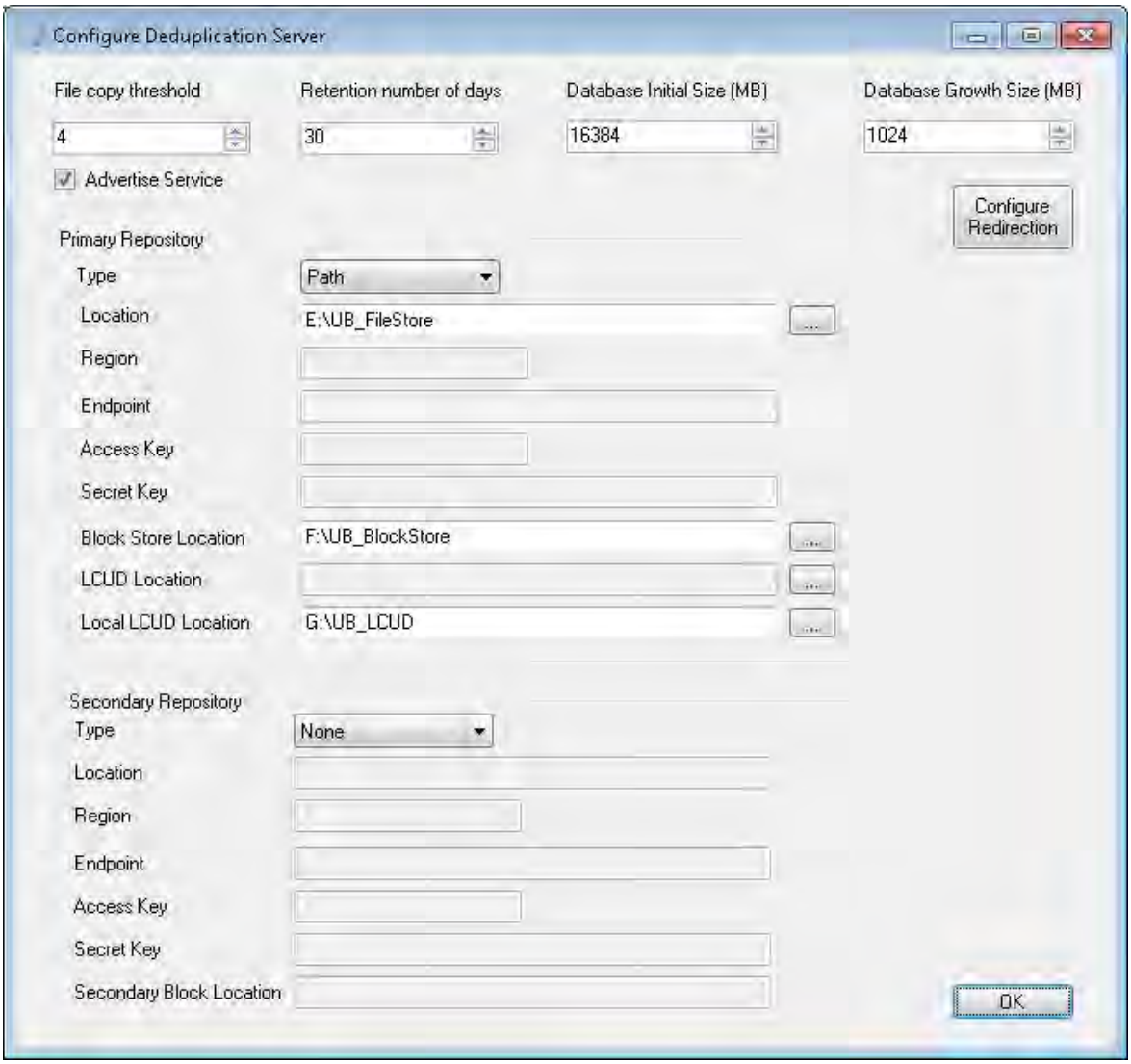


Fig. 1 - Configuring Database(s).

NOTE: By design, the service “UltraBac Deduplication Server” is not started after installation because it first needs to be configured. Once the service has been configured with this utility, use Service Control Manager to start the service. Note that any subsequent changes made to the configuration will require the service to be restarted.

- File copy threshold – How many times a file must be “seen” by the server before it is considered “common” and put in the file store. (Multiple copies of the same file from the same computer will only be seen once. The name of the file is not important, only the file contents are used to determine if the file is common.)
- Retention number of days – The number of days a file has to reach the “File copy threshold” and be considered “common” after first being “seen” by the server. If it fails to reach the threshold then it will be treated as a “locally unique” file to the computer(s) it was found on. This information is cached locally on each of the client computers, so they will not query the server again for this file. Set the value higher to increase the chance of more common files being discovered, but at the cost of the database size.

- Database Initial Size (MB) – If you are only enabling the file store then it is recommended to set this value to at least 8000 MB. If you are enabling the block store then this should be set to at least 20,000 MB. If you are enabling both then the minimum should be 28,000 MB. If the database does not exist, this sets the size of the database when it is created in the "gcfosdb" directory off of the main deduplication server's installation path (usually "c:\Program Files\UltraBac Software\UltraBac Deduplication Server\").
- Database Growth Size (MB) – The amount to extend the database when full. It is recommended to set this value to 20 to 25% of the initial size.
- Advertise Service – Allows clients to auto-discover the duplication server. This uses UDP protocol on port 1910 (IANA assigned to UltraBac Software). If this feature is not enabled, then each backup server will need to be configured with the IP/Name of the deduplication server in the registry.
- Configure Redirection – Used when connecting to UltraBac's global file repository hosted in AWS.

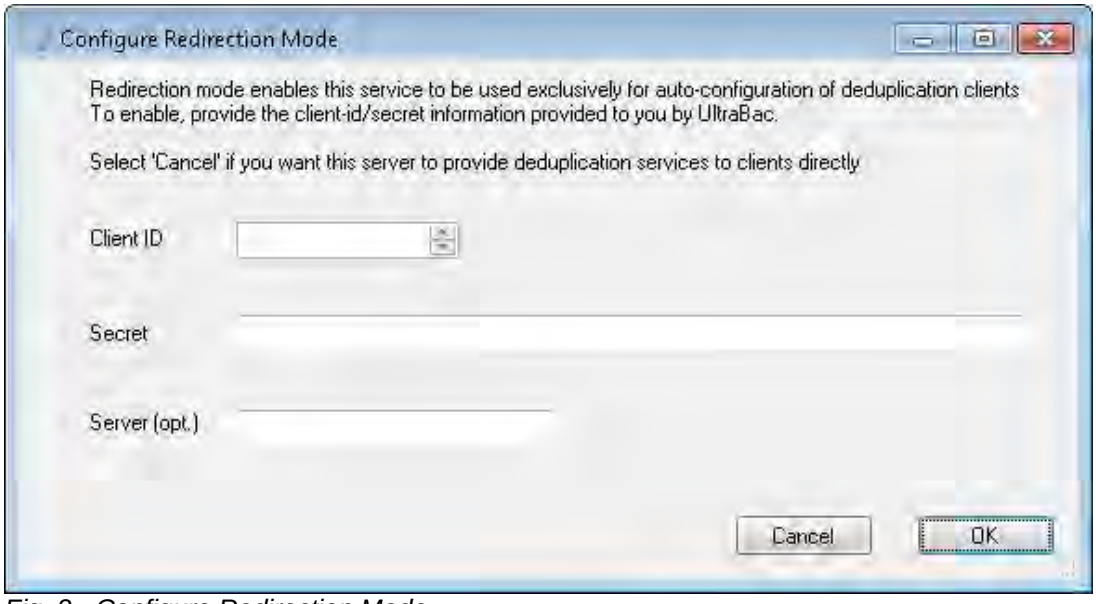


Fig. 2 - Configure Redirection Mode.

  - Client ID – A unique identifier that is associated with the "Secret" key. Provided by UltraBac Software.
  - Secret – A key that is used in conjunction with the "Client ID." Provided by UltraBac Software.
  - Server (opt.) – Leave blank unless provided a server name or IP by UltraBac Software.

Repositories

There are two repositories – a primary and a secondary. When a secondary is configured, everything written to the primary is duplicated onto the secondary. In the event that the primary is not available, any restore/retrieve request will automatically failover to the secondary for retrieval. If you do not wish to enable file-level deduplication, set the primary repository type to "None". (Then see below regarding "Block Store Location" to enable block-level deduplication.) To enable file-level deduplication you must define the primary repository. The type may be set to Path, S3, Azure, or OpenStack.

Primary Repository

- Type
  - None – Disables file level deduplication.

    - Path – Store “common” files in the path specified. Ensure that there is plenty of disk space available as potentially thousands of files will be stored in that location.
        - Location – Local or remote path to store “common” files.
    - S3 – Store “common” files in a Amazon S3 bucket location.
        - Location – Bucket name. If bucket is not found, it will attempt to create it.
        - Region – Geographical location to store data in.
        - Endpoint – A URL that identifies a host and port as the entry point for a Web service. The Endpoint may be left blank if the region has been defined, otherwise you can name an explicit region specific endpoint or the generic endpoint, for example http(s)://s3.amazonaws.com.
        - Access Key – A unique identifier that is associated with the “Secret Key.”
        - Secret Key – A key that is used in conjunction with the “Access Key” ID.
    - Azure – Store “common” files in a Microsoft Azure Blob Storage location.
        - Location – The “Container” name to use for storing “common” files. Name must already exist.
        - Region – Also known as an ‘Affinity Group’. Geographical location to store data in.
        - Access Key – Account Name, a unique identifier that is associated with the “Secret Key.”
        - Secret Key – Account Key, a key that is used in conjunction with the “Access Key” ID.
    - Openstack – Store “common” files in an Openstack based cloud provider location.
        - Location – The “Container” name to use for storing “common” files. It will be created if it does not exist.
        - Region – Geographical location to store data in.
        - Endpoint – A URL that identifies a host and port as the entry point for a Web service.
        - Access Key – A unique identifier that is associated with the “Secret Key.” There are two styles of authentication that OpenStack uses, one with a “project” setting and one without. If your provider requires a tenant number or account number provided alongside another identification, then it is likely using a project-style authentication (e.g. NephoScale or HP). If that is the case, then use the “[project]:[id]” format, e.g.: “128542:mycompanyaccount”.
        - Secret Key – A key that is used in conjunction with the “Access Key” ID. Openstack refers to this as an “API Key.”
- Block Store Location – Must be a local or remote path to store “common” disk blocks. Leave the field blank to disable block-level deduplication. Note that this will drastically increase the storage requirements. For performance, the software currently enforces that the block store is not stored in the cloud. However, a lazy migration occurs from the local/remote path to the cloud if you enable “Secondary Block Store Location” below.
- LCUD Location – “Local Common Unique Database.” Enabled only when using a cloud provider for the file deduplication database. Specify a path relative to the “Location” path specified above. This is a secondary storage location of LCUD files.
- Local LCUD Location – Local disk path to store list of files determined to be unique to the computer. Client will not attempt to query the server for files in this list.

Secondary Repository

This is optional. When enabled (repository type is not “None”) all data written to the primary repository is duplicated to the secondary repository. The fields: “Location,” “Region,” “Endpoint,” “Access Key,” and “Secret Key” all work as described above for the primary repository. The “Secondary Block Location” field will only become available if the primary “Block Store Location” is used. If using a cloud location for the secondary repository, this field is relative to the “Location” field.

Index

A
Active Directory ... 5, 11, 205, 223, 228, 523, 525
Add Device 48, 148, 283, 316, 409
Add New Event 122
Add New Holiday.....11
Advanced Driver Options 148
Advanced Encryption Standard (AES).....11, 460
After Copy Options.....62
Agents 5, 11, 30, 34, 205, 217, 221, 245, 266, 275, 283, 316, 442, 450
Archive Bit 112, 205, 217, 400
Authoritative System State Restore 223, 228
Autoloader Library.....79
Autoloader Support 148
Automatic Cleaning 79
B
Backup Account Permissions 434
Backup Commands.....134
Backup Migration 68
Backup Output Files.....441
Backup Path11, 34, 48, 245, 393, 441, 450, 488, 493
Backup Set Basics 98
Bare Metal Recovery (BMR) 148, 316
Before/After Jobs 11, 125, 205
C
Centralized Management.....366
CIFS Backup Path.....493
CIFS Share 48
Command Line Backup/Restore 385
Command Line Functionality 134, 385
Common Backup Errors Explained.....448
Continuous Image Protection (CIP) 138, 148, 189, 192
Copying Restore Logs.....148
D
Defining a Disk (BackupPath) Storage Device48, 112, 393
Device Selection 48, 148, 391, 393
Differential Backups 138, 198, 205, 217, 266, 275, 400
Directory Services Restore 205, 223, 228
Disaster Recovery Agent 138, 148, 189, 192, 198, 203, 221, 390, 445
Disk Storage Device Properties 48, 393
E
Email Notification 112, 428, 510
Enable Single File Restore.....138
Encrypting Backup Data.....11, 460
Errors During Backup.....501
ESX/ESXi 192, 245, 512
Event Frequency.....112
Event Time Options 112
Exchange 5, 30, 98, 275, 457, 472, 475, 486, 492, 494, 506
Express index 62, 127
F
File-by-File Agent.....205, 217, 221, 523, 525
Freeze All Drives.....138, 205, 221
FTP Device 48, 148
G
General Options.....11
H
Hewlett-Packard LTO Ultrium devices.....48, 473
Holiday Options.....11
HP StorageWorks D2D Backup Systems 48, 488
I
IBM Tivoli 48
Image Agent.5, 98, 138, 148, 189, 192, 198, 221
Image Backup ...5, 127, 138, 148, 189, 192, 198, 203, 221, 390, 450
Image Restore Options ..138, 148, 198, 445, 450
Import License 30
Importing Managed Machines list.....507
Incremental Backup 138, 198, 217, 245, 275, 400, 506, 512
Incremental/Differential VHD Files.....189
Incremental/Differential VMDK Files.....192
Installation.....5, 283, 316
ISCSI.....245, 476
L
Library Configuration 62, 79, 102, 431
License Components 30, 442
Licensing.....5, 30
Linux Agent Options 283, 316
Locked File Backup Agent 138, 205, 221, 448
Log File Options.....11
M
Managed Machines List.....11, 507
Management Console.....11, 34, 148
Master Boot Record (MBR) ...138, 148, 390, 450
Media Builder.....377
Media Library 34, 62, 79, 102, 148, 414, 431, 455
Media Library Controls.....79
Media Limit MB 48, 393
Media Options.....11, 79, 460
Media Pool.....62, 79, 455
Medium Changer Driver Unloading 431
Minimum System Requirements.....1
MySQL 92, 464

N
Network Configuration.....148, 316
Non-Authoritative System State Restore 223, 228
Non-UltraBac Specific Registry Keys.....428
Non-VSS Exchange Backup Restore 494
O
OpenSUSE.....283, 316
P
Partition/Disk Restore 138, 316
Permissions Issues 412
PersistentTargets 476
Public Folder Stores.....275
Publish License Servers.....11
Purge Logs After 11
R
RAID.....138, 148, 203
Raw Disk Mappings 245
Rebuild Index 34, 127, 148
Recovery Storage Group 275, 457, 494
Red Hat Enterprise Linux.....283, 316
Remote Administration.....34
Remote Device.....48, 79, 148
Remote Installer 5, 34
Remote Local Server Agent.....442
Reporting Console 421
Reset License 30
Resize Partition 148, 198
Restore Basics 127
Restore Commands 134, 385, 450
Restore Destination Path 138
Restore Logs.....426
Restore MBR.....148, 316
Root Certificates.....1, 5
S
Samba.....393, 412
Save Backup Set.....34
Scheduled Backups 11, 34, 79, 98, 102, 112, 122, 125, 203, 390, 391, 393, 400
Scheduled Events 34, 122
Scheduler 11, 34, 102, 122, 134, 441
Scripted Install.....5
SCSI/CRC Problems.... 148, 203, 406, 409, 431, 448
Secure FTP (SFTP) 48
Select Storage Device.....48, 391, 393
Set License Server.....5, 30
Show Hidden Devices.....221
Single File Restore.....138
Single Server License 442
Slot Based Library.....79, 431
SMTP 34, 112, 398, 428
Solaris Client.....429
SQL 266, 438
SQL Agent.....266, 438, 510
SQL Backup/Restore 266
Static Mirror Image Backup/Recovery 48, 138, 148, 203, 397
Storage Device Manager 11, 48, 148
Storage Device Options.....102, 112
Storage Driver.....148
Storage Media.....11, 62, 79, 112, 127, 148, 203, 385, 390, 391, 460
SUSE Linux Enterprise Server 283, 316
System State.....112, 205, 223, 228
T
Tivoli.....48, 148, 391
TSM Client 48, 148
Typical SCSI Problems.....409
Solving.....409
U
UBDR.....148, 426, 450, 504
UBDR Gold Advanced Tools 148, 445
UBQ000092 409
UBQ000234 448
UltraBac Agents.....5, 34
UltraBac Database.....5, 92, 127, 464
UltraBac Disaster Recovery.....48, 148, 390
UltraBac Management Console....5, 11, 34, 138, 148
UltraBac Medium Changer 79, 431
UltraBac Specific Registry Keys 428
UltraCopy.....34, 62
UltraVue.....11, 34
Unattended Installation.....443
Uninstall UltraBac 5
UNIX/Linux.....283, 316
Unknown Medium Changer 414
Upgrading UltraBac.....30, 510
UX Agent (File-by-File) 283
Ux Image Agent 316
V
VHD Files.....189
View Backup Set Properties 34, 125
View Events 34, 79, 102, 122
View Media Index.....385
View Restore Logs.....34
View Verify Logs 34
Viewing Scheduled Backups 122
Virtual Disk Agent 189, 192
Virtual Disk Options 189, 192
VMDK Files.....192
Volume Shadow Copy Service 205, 221, 275
vSphere Agent 245
VSphere Agent CBT Troubleshooting 512
W
Windows Automated Installation Kit 476
Windows Logo Warning.....5
Wipe MBR.....148, 445
Workgroup 5, 11, 148, 412, 436, 450
Writing to VHD 138, 189
Writing to VMDK 138, 192

Y

YaST 283, 316