Cristie Bare Machine Recovery

Technical Reference

For Windows

June 2007

Cristie Data Products Ltd
New Mill
Chestnut Lane
Stroud GL5 3EH
United Kingdom
Tel:+44(0)1453 847000
Fax:+44(0)1453 847001
cbmr@cristie.com

Cristie Data Products GmbH
Nordring 53-55

63843 Niedernberg
Germany
Tel: +49 (0) 60 28/97 95-0
Fax: +49 (0) 60 28/97 95 7-99
cbmr@cristie.de

Cristie Nordic AB
Gamla Värmdövägen 4

SE-131 37 Nacka
Sweden
Tel:+46(0)8 718 43 30
Fax:+46(0)8 718 53 40
cbmr@cristie.se

Cristie Data Products Ltd
New Mill
Chestnut Lane
Stroud
GL5 3EH
UK
+44 (0) 1453 847000
Internet E-Mail: cbmr@cristie.com
Website: http://www.cristie.com

Contents

1 Introduction

Cristie Bare Machine Recovery (CBMR) for Windows 2000/XP/Server 2003 is available as a single edition suitable for all platform types. It is also compatible with the 64-bit editions of Windows Server 2003 and Windows XP. You must have one of these Operating Systems correctly installed prior to proceeding with the installation of CBMR.

IMPORTANT:- Refer to the ReadmeEN.TXT file on the installation disk for any limitations and last minute updates. This readme file is also provided in French, German and Japanese versions.

To minimise the impact of a hard disk failure you need to have a restore strategy in place. CBMR allows you to recover both Windows 2000/XP/Server 2003 Workstations and Servers without first having to re-install the operating system or backup software. This reduces the recovery time significantly. All you need is disaster recovery media from which to boot your computer and a disaster recovery backup of the Windows 2000/XP/Server 2003 system.

Finally a full backup of the system can be restored using the backup features of CBMR or any other preferred Backup/Restore software.

Backups can be performed to a variety of different Backup Locations and media including IBM's Tivoli Storage Manager, tape, disk, network-attached storage etc. For simplicity, this manual will refer to Tape as the backup media throughout.

Note: CBMR no longer supports Windows NT.

1.1 How Cristie Disaster Recovery Works

CBMR makes the job of recovering a computer system running Windows 2000, XP or Server 2003 after a disaster (such as a major disk crash) much easier.

Configuration Information

The key is a set of files containing the system configuration. This includes information about the system, particularly about the hard disks, how they are partitioned, logical disk drive allocation, the network and storage adapters to use and so on.

Disaster Recovery Backup

You also need to make a special disaster recovery (DR) backup that contains essential files for the operation of your system and network (if relevant), such as the Windows and boot directories and registry. CBMR determines the minimum list of files to back up for you. Optionally, the media can also contain a backup of as many extra directories as you like. This is called the DR Backup. CBMR supports a wide range of Backup Locations such as SCSI, IDE, File Device, IBM Tivoli Storage Manager (TSM) Server and Cristie Storage Manager (CSM).

How the Recovery Works

CBMR uses a two stage DR process to recover any Windows 2000/XP/Server 2003 system. In the first stage, the emphasis is on bringing the essential operating system back up and running. In the second stage, all other disk partitions are formatted and the data restored, to bring the system back to the pre-disaster state.

Stage one of DR is carried out by using a Cristie recovery console based upon a standalone minimal version of either Linux or Windows PE. The provided DR Boot Media contains both kernels.

Stage two, is carried out by using the recovered Windows 2000/XP/Server 2003 operating system and the preferred backup/restore software to recover the remaining files and applications.

In the event of a disaster, the system is booted from the DR Boot Media, which uses the previously stored configuration information to rebuild the system. It re-partitions and then reformats the hard disk or disks if necessary, recovering the original partitioning.

It then restores the minimum files required to boot Windows from the backup media. It then reboots the machine to load Windows. If the Linux recovery console has been used, further formatting and restore will be carried out in Windows mode. This is not necessary if the Windows PE recovery console has been used to recover the system instead.

When it has finished, you can restore files from the latest regular backup tapes (say) to bring the system back as close as possible to how it was before the disaster.

2 What you need to do to use CBMR

CBMR can protect a system all the time, if setup and configured correctly. The following sections will explain this procedure.

2.1 Product Licensing

When first installed, CBMR may be used for a trial period of 30 days. During that period CBMR is fully functional. If the software is subsequently un-installed and later re-installed on the same system, the 30 day period continues from the date of the first installation.

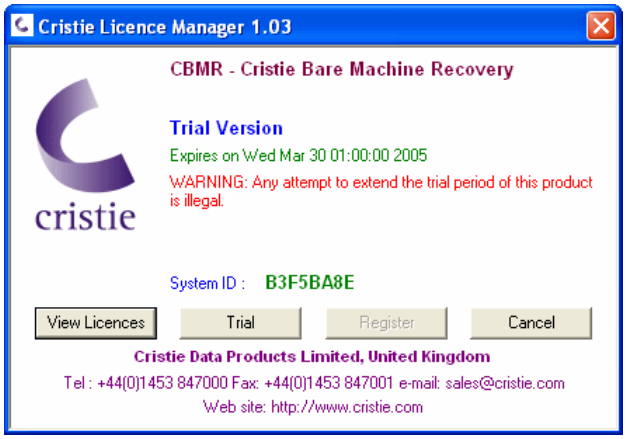
If you wish to use the software beyond the trial period you must register and purchase a license from Cristie. Alternatively, and in special circumstances, Cristie will normally extend the license period if you wish to trial the software beyond that period.

If you purchase the product, then a new license file and activation key will be sent to you.

The following sections discuss this is more detail.

2.1.1 Trial License

Unless a full license has already been purchased from Cristie and copied to the program folder, when starting CBMR for the first time, the following screen will be shown.



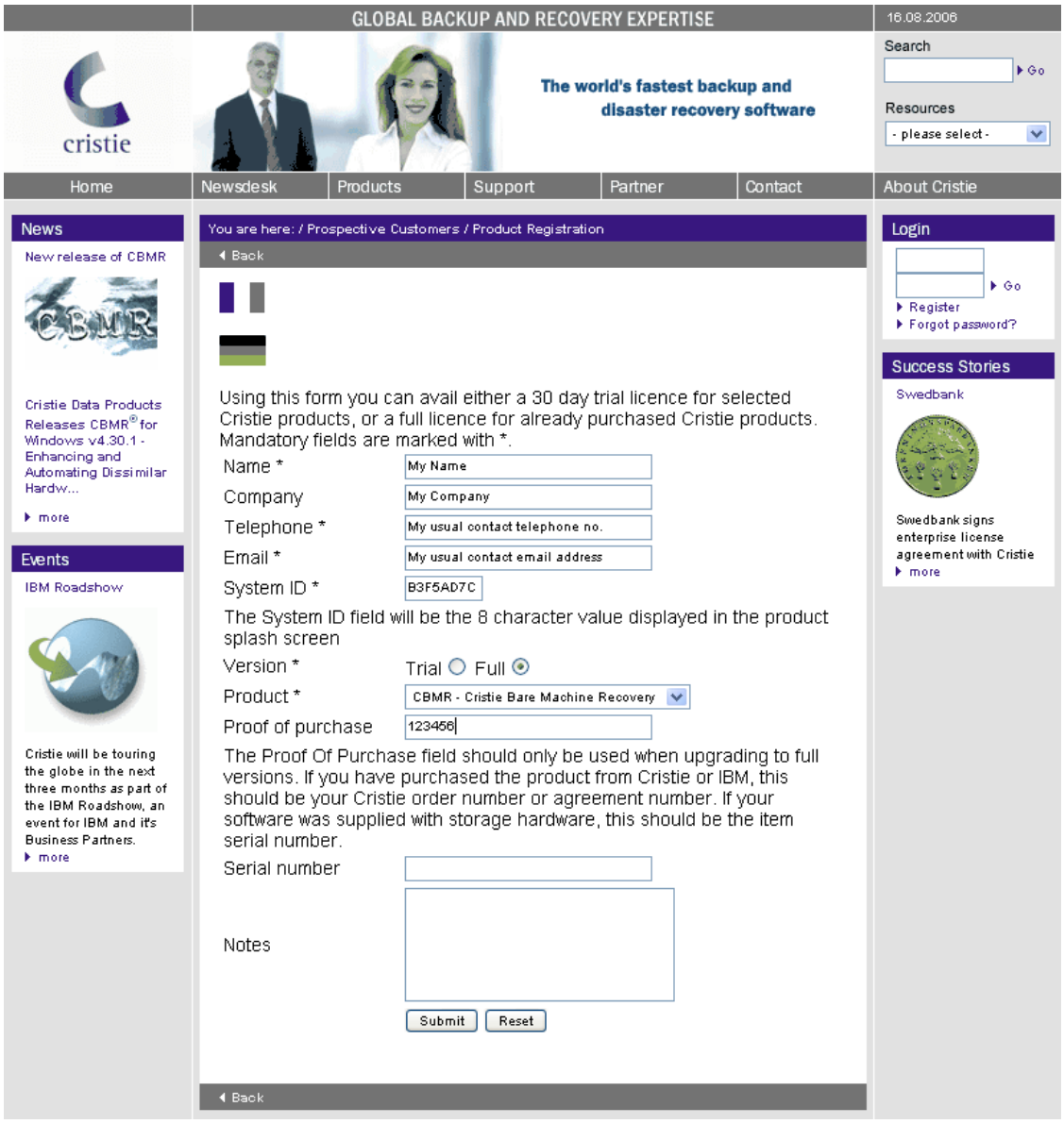
Select **Trial** to begin the CBMR trial period of 30 days. This dialog will be displayed every time the software is started until either the 30 day trial period expires or the Customer purchases and loads a valid license file.

2.1.2 Full License

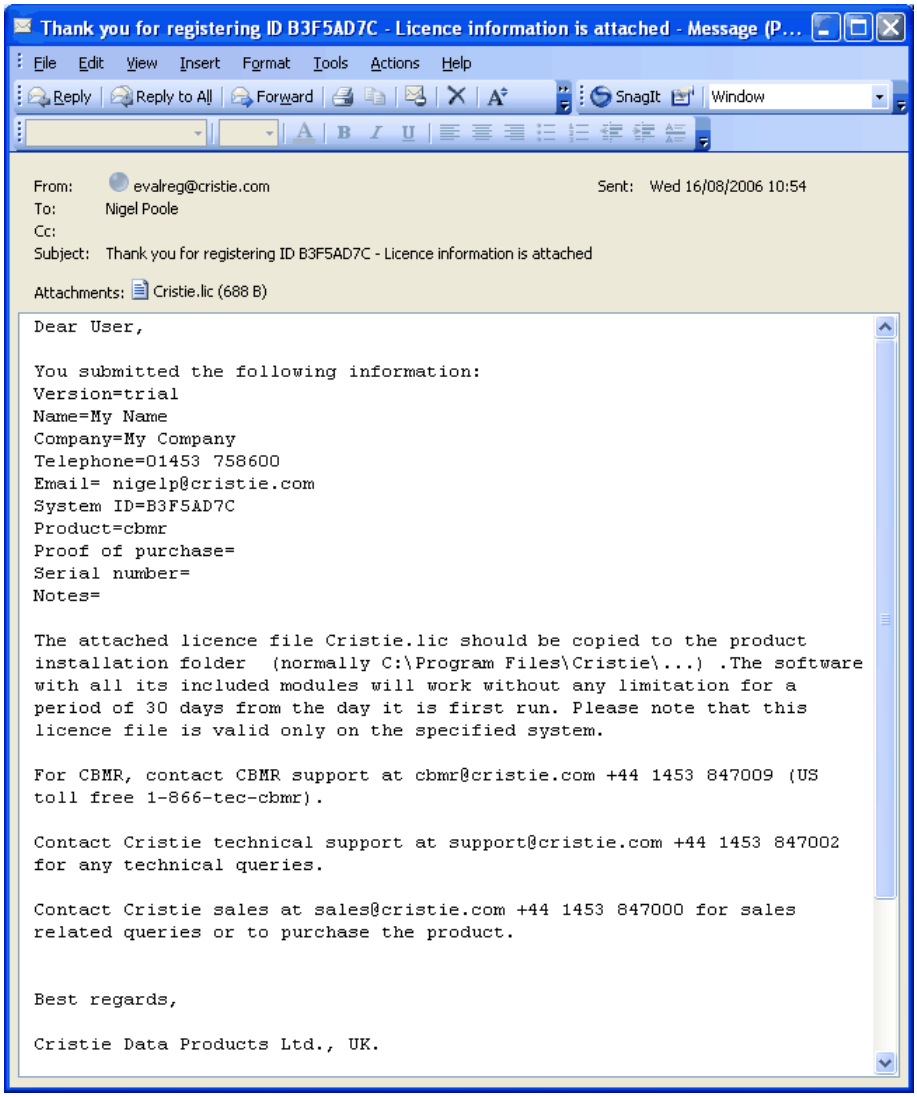
Before the trial period has expired and you have purchased CBMR, you will be sent a contract which contains the serial numbers that you are entitled to use. To upgrade from the trial licence to the full licence, you need to apply for an activation code via the web site. The process is identical to the registration for the Trial version except that you select the "**Full**" option at the appropriate place.

Before you can purchase the software you will need to register the product. This is done using the **Register** button in the License Manager utility. Make a note of the **System Id** shown in the License Manager for the system. This will then take you to the Cristie website page shown below. If necessary you can go straight to the registration page on the web site which you will find at **www.cristie.com/register**.

Please note that you have to be connected to the Internet to use this feature. Enter your Contract/Agreement No. as Proof of Purchase and the Serial No. of the licence that you wish to allocate to the specified System Id. Select Full as the license version.

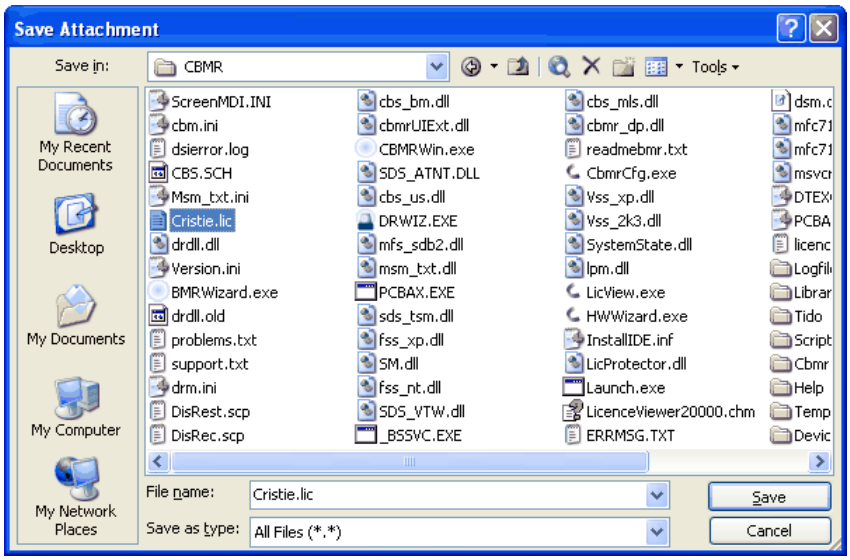


After you have completed the full registration of the product an email will be sent to you in the following form.

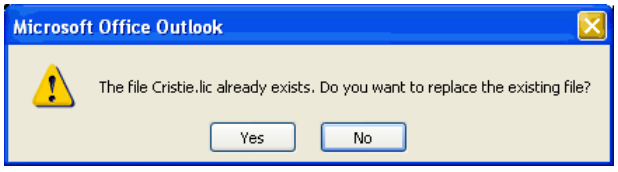


This email contains an attachment (Cristie.lic) which is a binary file. Make certain that your email server permits binary file attachments and does not remove the attachment or quarantine the email.

Once you have received the email with the attachment, you will need to copy the attached file from the email into the CBMR directory on your hard drive, which is normally located in "C:\Program Files\Cristie\CBMR". This can be done by "right clicking" on the attachment then selecting "Save As..." from the drop down menu. You will then have to select the CBMR folder . Alternatively simply "drag and drop" the file from the email to the folder.

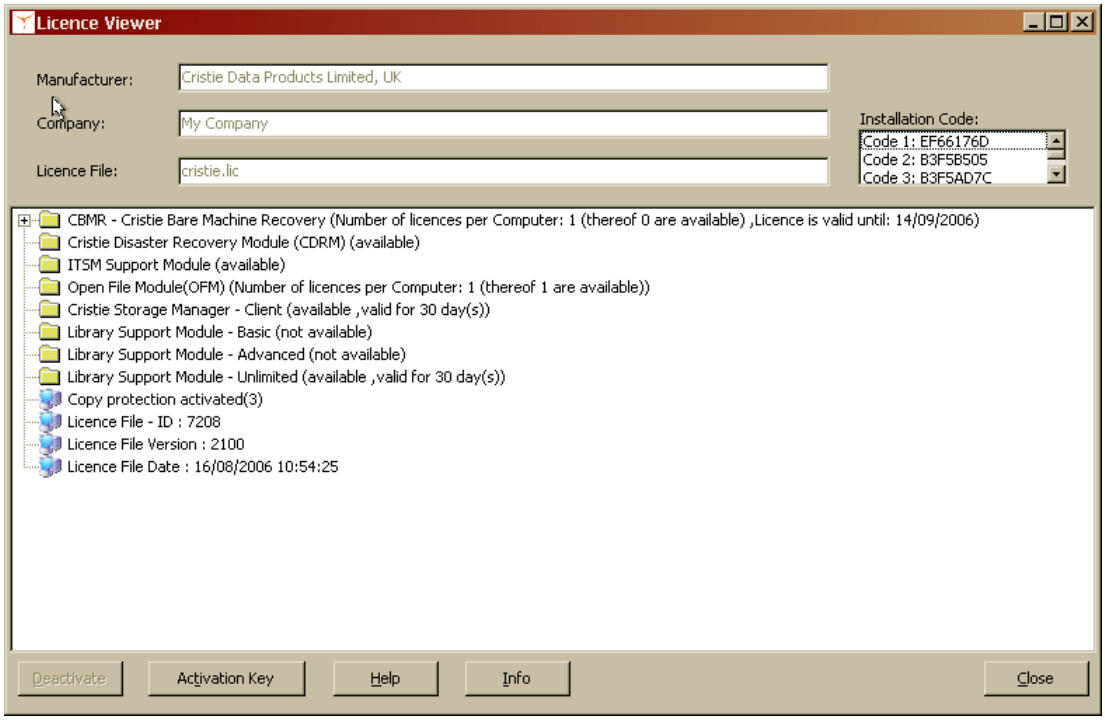


When you "paste" this file in to the CBMR folder a pop-up box will appear asking if you wish to over write the file. Click "**Yes**" to this message.



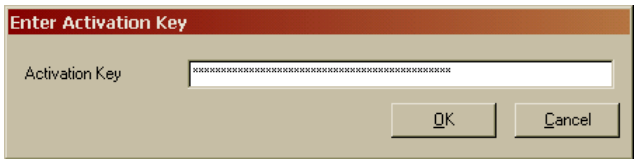
This license file will extend the trial licence period to a total of 45 days (from 30 days).

The final part of the activation process is processing the **Activation Key**. Entering this will fully enable CBMR functionality. The **Activation Key** will come as another email containing a text file attachment. Currently the validation of your registration request is handled manually so it may take two working days to issue it for a valid application. To apply the **Activation Key** click on the "**View licences**" button. This will then take you to the CBMR Licence Viewer.

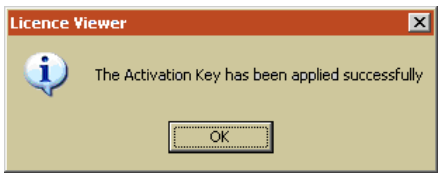


From this screen you are able to see all the licences held on this machine that relate to CBMR. To update your licence code you click on "**Activation Key**" this then will produce a pop up box.

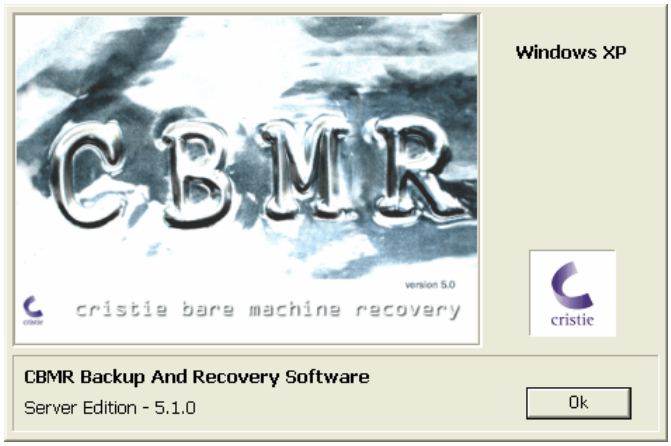
Then enter in the activation key that sales/ support has supplied (actual value not shown) and press **Ok**.



When a correct activation key has been entered the following dialog box is produced. This will confirm that the activation key has been applied successfully.



To check that the product is now fully activated, when you restart CBMR, the only dialog box shown is the initial splash screen (running on Windows XP in this example). The License Manager dialog will no longer be displayed.



Click "**Ok**" to enter CBMR or let the dialog timeout and the main CBMR opening dialog will be shown.

Further information may be found in the Cristie Knowledge Base at http://support.cristie.com/kb

2.2 CBMR (Cristie Bare Machine Recovery) Setup Steps

You must follow the procedure in the order listed below. CBMR can be used with or without a ITSM server. You may omit the steps involving the TSM server if you use CBMR with a directly attached Backup Location storage device (e.g. Tape).

1 Check TSM Client Version (page 11).

2 Install CBMR. (page 13)

3 Create a TSM Client node .

4 Configure CBMR (page 132).

5 Store machine configuration data (page 21).

6 Do regular system backups (page 31).

To perform a Bare Machine Recovery you must:

1 Boot up the machine to be restored from the CBMR CD-ROM (page 34).

2 Specify the location of the machine configuration data.

3 Perform a system recovery from CBMR.

4 Perform conventional data recovery from your backups.

2.2.1 Check TSM client version

It is important to check the version of the TSM Client installed on your machine. Versions supported by CBMR are:

TSM Client 4.2.1.32 onwards with a compatible TSM Server version.

If you are not using TSM, you should skip this step

2.2.2 Creating an TSM client node

This step is optional if TSM is not used in the recovery procedure. CBMR will connect to a TSM server as a client node and the machine's operating system files and other important files will be stored under a Filespace in the client node. If you need to create a Client node using the TSM Admin Client, refer to the TSM Administrator Guide for further information.

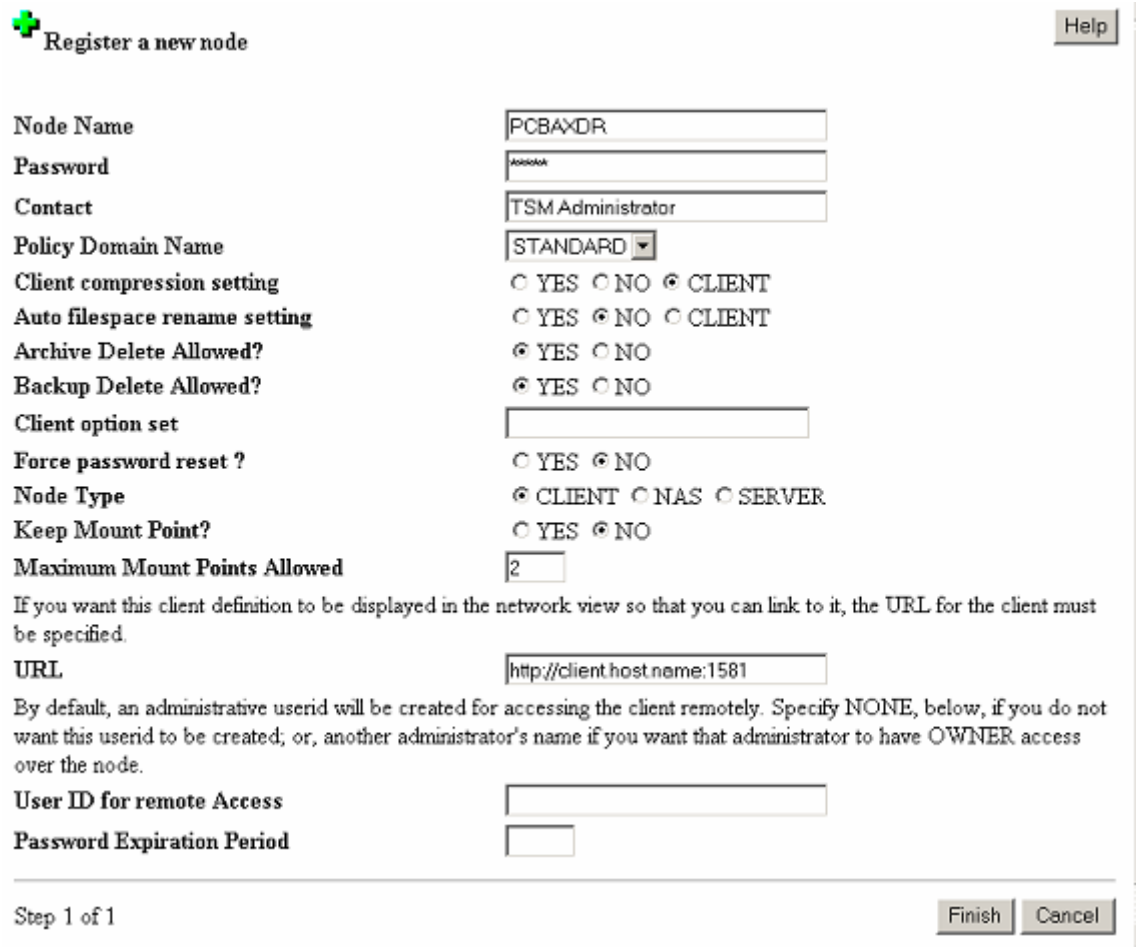
Creating a dedicated node via the TSM Admin client

To use the TSM module, you must enable CBMR to backup to the IBM Tivoli Storage Manager by creating a dedicated node via the TSM Admin client.

The settings required for the node are:

Archive Delete Allowed	YES
Backup Delete Allowed	YES
Client Compression setting	CLIENT
Force password reset	NO
Node Type	CLIENT

In addition, you must consider your password policy. If you specify a Password Expiration period, you will have to set the password in CBMR every time the password expires. Note that automatic password generation for the client nodes is supported in CBMR 5 and later.



Additional Configuration to Maintain Multiple Backup Versions

If it is required to hold more than 1 version of the DR backup in the same filespace then the node must be setup correctly to support this.

You must have a Management Class (MC), which contains a Backup Copy Group (BCG) and an Archive Copy Group (ACG).Your node needs to be registered to use the MC.

The parameters of the BCG of interest are

- Versions Data Exists = 2
- Versions Data Deleted = 1
- Retain Extra Versions = 30
- Retain Only Version = 60

In this example, there can be 2 versions of an object, the Versions Data Deleted attribute specifies the maximum number of different backup versions (1 in this case) retained for files and directories that you erased from your file system. This parameter is ignored as long as the file or directory remains in your file system.

The expiration date for the remaining versions is based on the retain extra versions and retain only version parameters. In the example, if there is more than one version and one is deleted, the deleted one will be kept for 30 days. The only remaining copy of the object will be retained for 60 days (that is AFTER you make it inactive).

If several versions of a DR backup are maintained in TSM, the Linux and WinPE recovery environments will allow you to choose a specific version to restore.

2.2.3 CBMR Installation and Removal

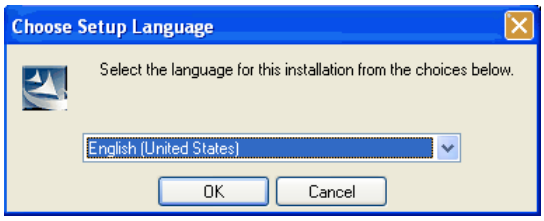
This section discusses a typical installation sequence of CBMR. Note that all example dialogs are shown in English.

Install CBMR

When you insert the CD into a drive that will Autoplay, the following menu is displayed.

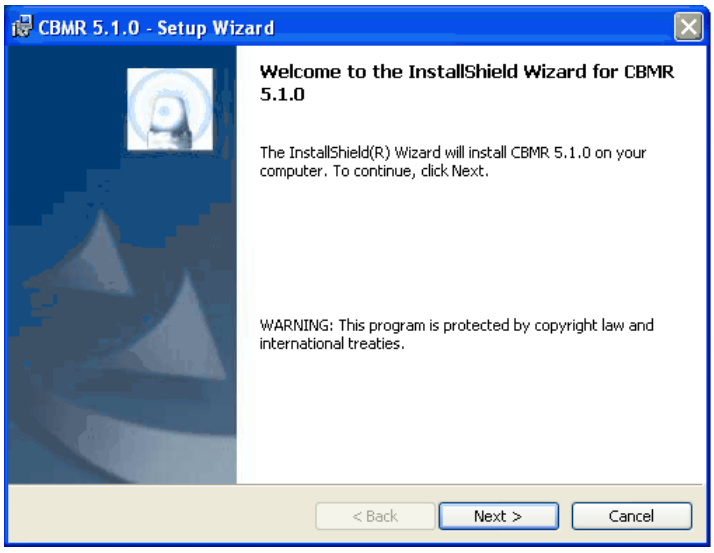
You install CBMR by clicking on Install CBMR. This starts `SetupCBMR5.exe` on the CD, so if AutoPlay is disabled for your CD-ROM drive, double click on `SetupCBMR5.exe` to launch it manually.

Similarly if you want to install the Desktop version of CBMR click on Install CBMR Desktop to start `SetupCBMR5dt.exe` on the CD, or double click on `SetupCBMR5dt.exe` to launch it manually.

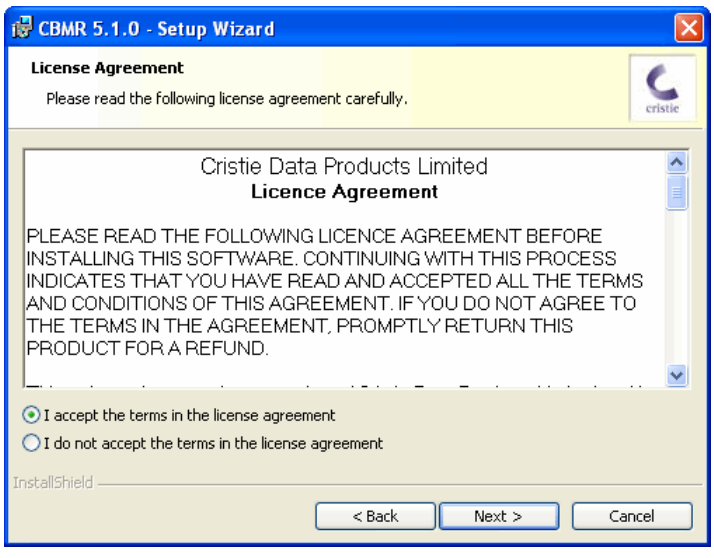


The first dialog presented enables the User to select the installation language. The default language will be the current default language installed in the target Windows system. The available languages are English, French, German and Japanese.

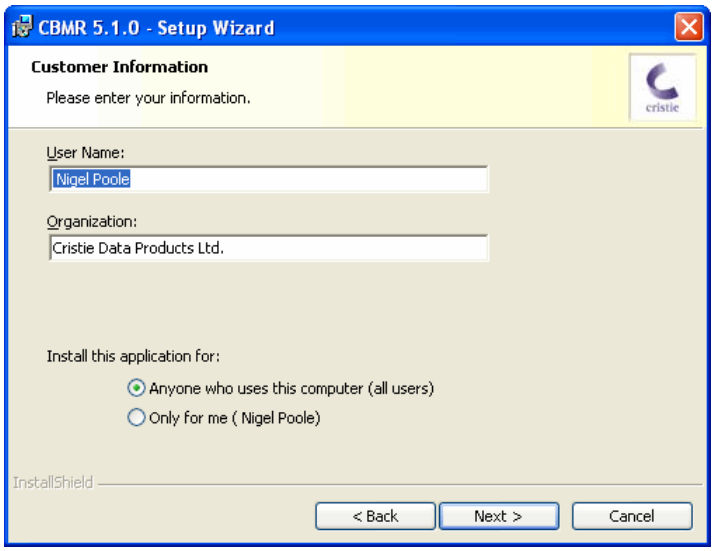
The Welcome message will then be displayed in the selected language.



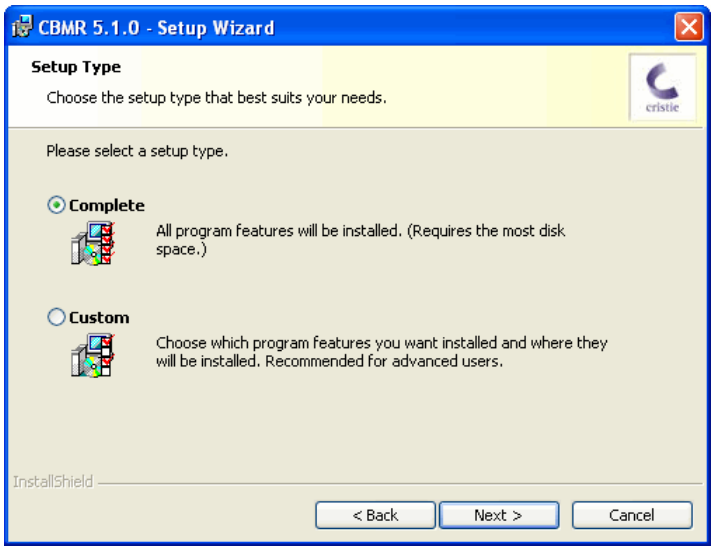
Selecting Next> results in the display of the Cristie Licence agreement.



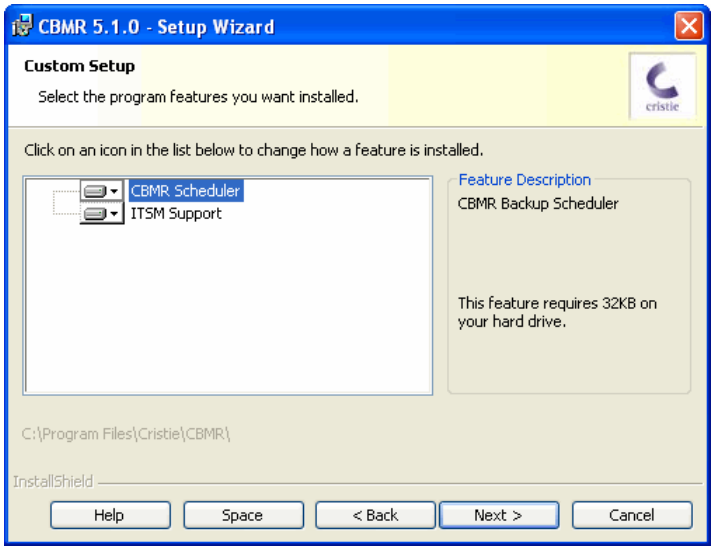
Accept the license agreement and press Next>.



Confirm the User information and press Next>.

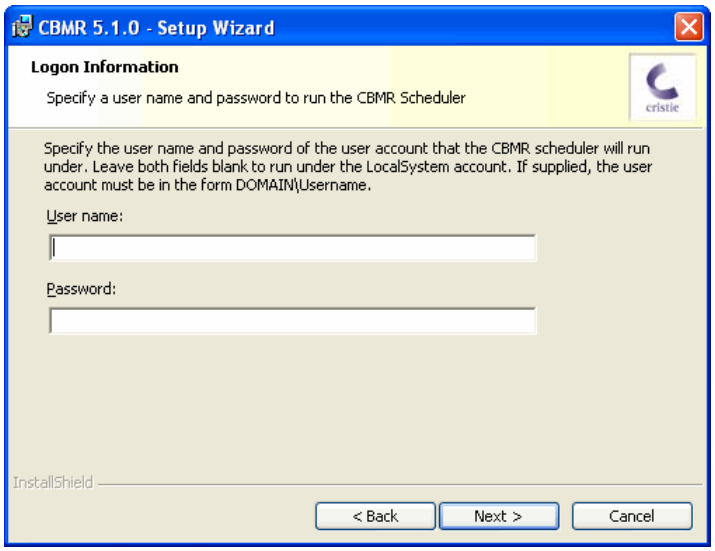


Choose either Complete to install all optional components for the platform or Custom to install only selected items.

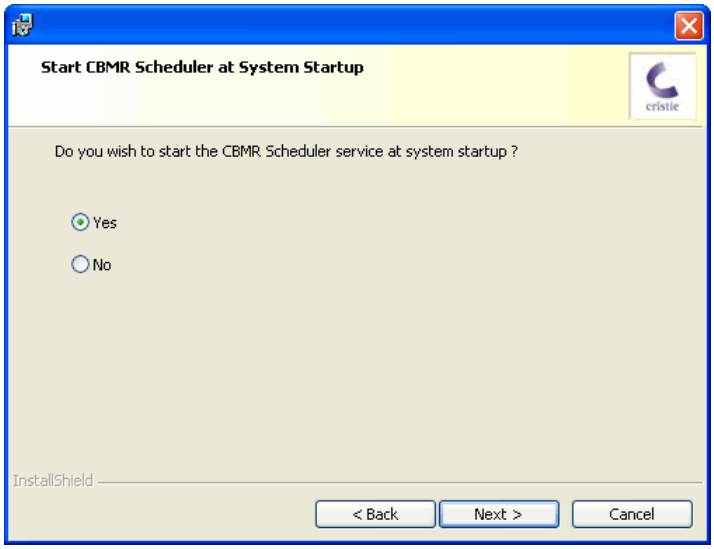


In the Custom installation, if you had the TSM Client already installed on your system, the TSM Support option will be displayed and selected. If you wish to use CBMR without TSM you may deselect it here. Choose Next> and you will see the final confirmation dialog. Select Install to proceed with the selected installation, or <Back to adjust previously chosen settings.

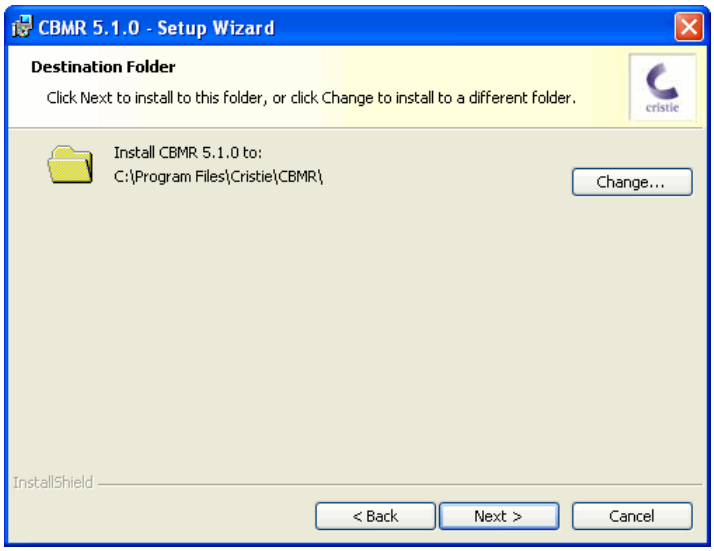
Provided that you have chosen to use the CBMR Scheduler you will be asked to provide a User name and Password. Normally you leave this blank and the service will be installed to login using the default System Account. If you do specify a user account, then it must have Administrator privileges. Click on Next> to continue.



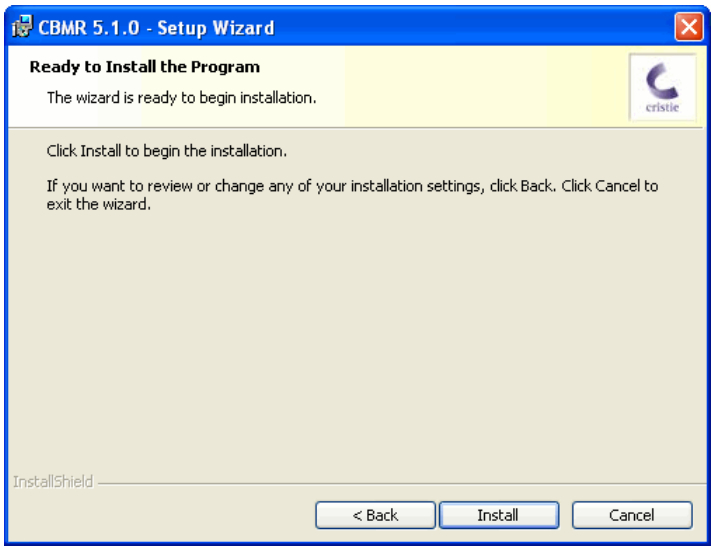
After the login details you will be asked if you want the service to be started whenever the machine boots.



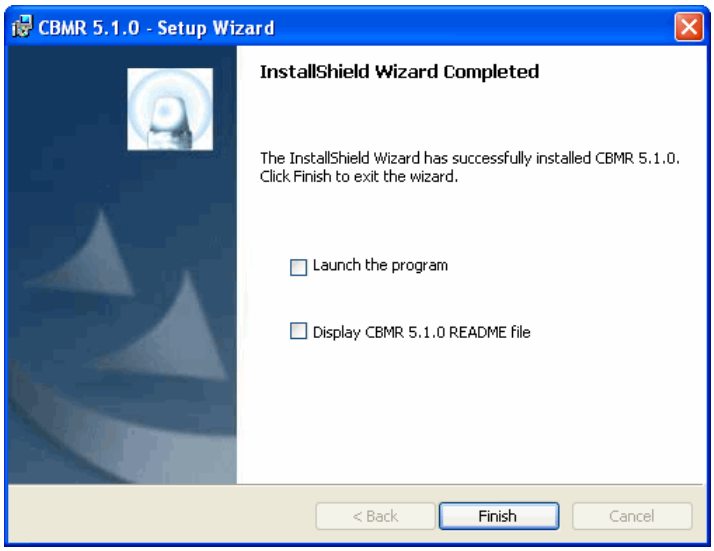
Click Next>to select the CBMR installation folder.



Click Next> and you have completed the installation parameters.



Finally you can begin the installation by clicking on Install.



Successful completion results in the dialog above. Press Finish to complete the installation. A re-boot will be required when installing CBMR on Windows 2000 systems to install the OFM drivers.

Note Windows NT is no longer supported in this version of CBMR.

Upgrade Install of CBMR

If an existing version CBMR 4.x.x or PC-BaX 4.11/4.30.1 is detected during the installation sequence it will be first uninstalled. During the upgrade sequence the following items will be retained:

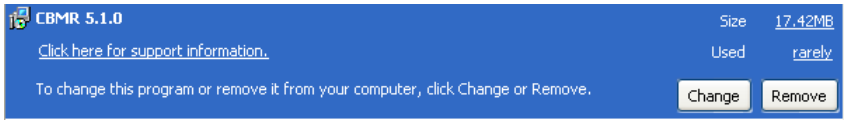
1. CBMR licence file (not for CBMR version 4.10 where a new licence file must be obtained from Cristie). PC-BaX upgrades will also require a new license file.
2. Defined backup locations (storage devices)
3. Default backup location setting
4. User specified file and folder backup exclusions

Note: The upgrade sequence may require several re-boots. These must never be cancelled, so always select to re-boot when prompted.

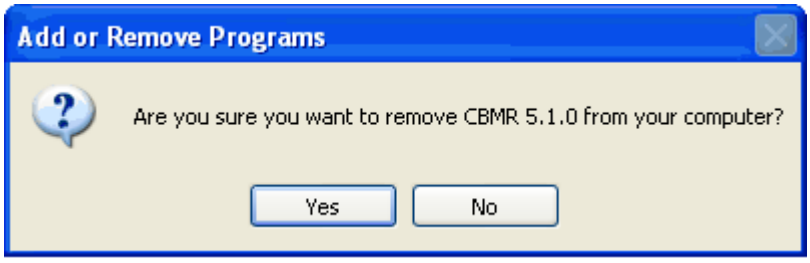
An upgrade of CBMR 5.x.x does not require an uninstallation. The upgrade process will simply replace the changed program files. All existing configuration files will be retained in this case.

Remove CBMR

From the Start menu, select the *Control Panel* dialog. Select *Add/Remove Programs* and select the **Remove** button for CBMR.



Select **Remove** to uninstall CBMR. A confimation dialog is displayed. Select **Yes** to proceed and complete the removal.



Note: The example dialog shown is in English, but if a different installation language was selected when CBMR was installed, the Program Maintenance dialog will be shown in the same selected language.

3 The Disaster Recovery Boot Phase

In the event of a disaster, having previously taken a backup of the system and stored the configuration information, Linux or Windows PE mode DR enables you to restore your system to the state at the last backup.

The CBMR recovery console (supplied in both Linux and Windows PE form) is supplied on CD-ROM and, if your machine supports bootable CD-ROMs (most PCs do), then this is the most convenient way to boot the DR module. If the system does not support bootable CD-ROMs you can boot from the network. The WinPE DR environment can be network booted from a RIS server. The supplied Cristie document CBMR WinPE DR RIS Network Boot provides details on how to set this up.

For those users familiar with earlier versions of CBMR (i.e. prior to version 5), the Linux based recovery mode may be preferred. However, the new Windows PE option offers several advantages namely:

- a familiar Windows GUI
- the ability to selectively choose which disks/partitions are going to be recovered
- the ability to inject new mass storage drivers during the boot process for dissimilar recovery
- all variations of dynamic disks are supported (i.e. mirrored, spanned, striped and RAID-5)
- NTFS volumes/partitions are created natively (i.e. no need to convert to NTFS after a reboot as with the Linux DR console)
- the restored backup contains the original file security information

4 The CBMR Configuration Wizard

Configuration information can be stored in the following locations:

- Floppy disk
- Network share
- Local folder
- Locally attached USB pen drive
- Collocated with the DR backup

Depending on your deployment strategy, you may choose any one of the above.

As part of this process the details about the hard disks, operating system, storage and network adapter, network settings and the Backup Location to use will be queried and stored. You can override some of these details if you wish.

This phase of the Setup comprises the following stages:

1 Specify where the DR configuration is to be stored.

2 Specify a Backup Location to hold the DR backup

3 Select the disk volumes to be restored and formatted during the recovery process.

The next sections discuss these stages in more detail.

4.1 Setting up the Configuration Parameters

The configuration information can be stored either:

- on a floppy
- on a local folder
- locally attached USB pen drive
- on the network
- collocated with the DR backup

If it is stored in a network share, the DR system will need to know the authentication details to gain access.

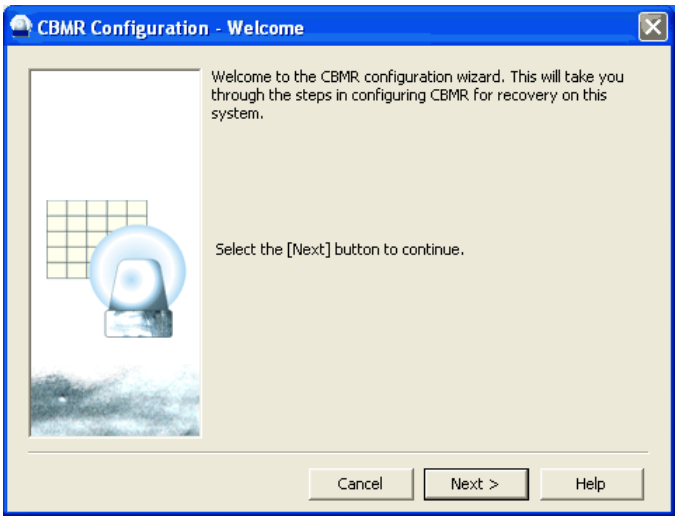
In the CBMR main window, click on Setup Disaster Recovery Configuration:

First, you will be offered the choice of where to store your configuration parameters. This can be stored as part of the DR backup itself or any local Backup Location (floppy, USB disk, network share etc.).

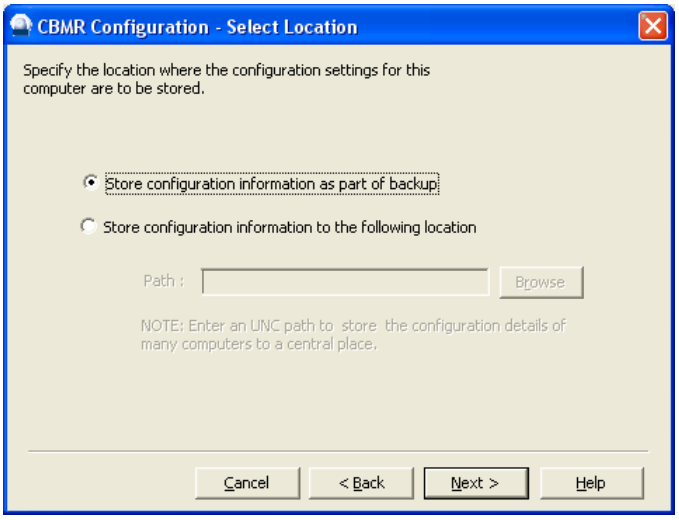
4.1.1 Storing the Configuration Information with the Backup

1 In the CBMR main window, click on Setup Disaster Recovery Configuration option.

1 The CBMR Configuration - Welcome page will appear.

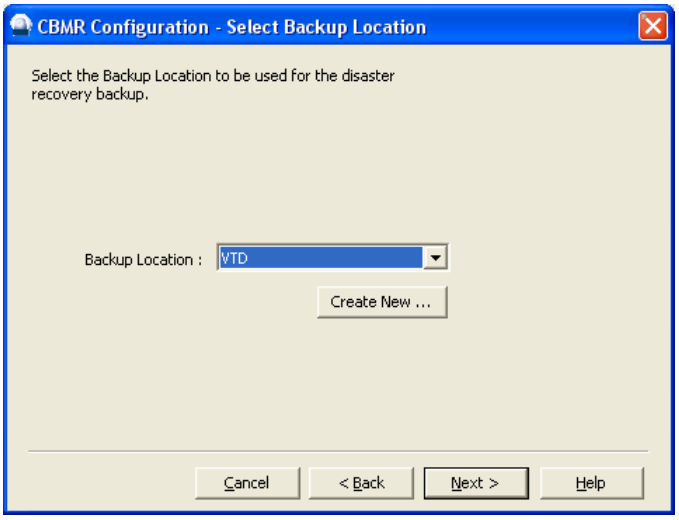


2 Click on **Next>** and the CBMR Configuration - Select Location page will appear.

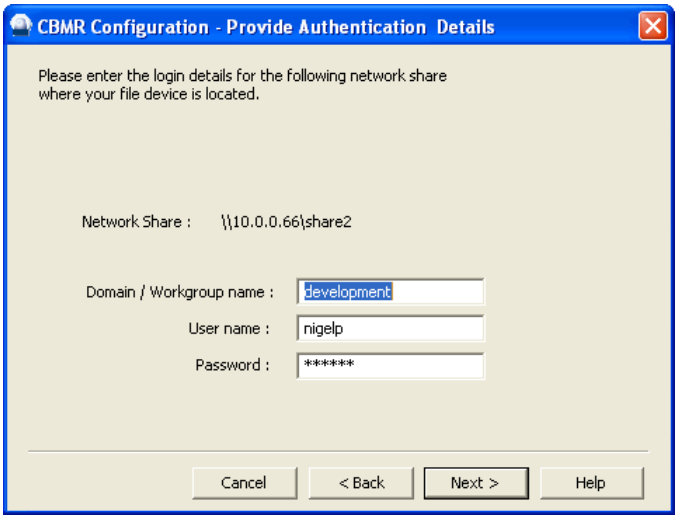


3 Select the **Store configuration information as part of backup.**

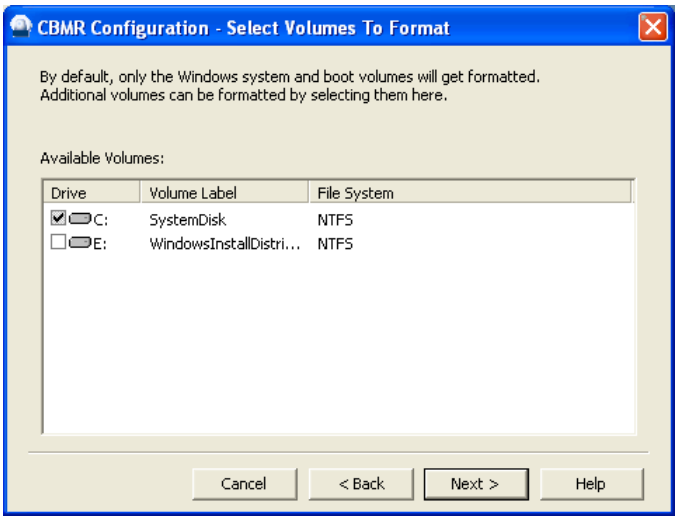
4 Press **Next>** and you will now be prompted to select a **Backup Location** for the DR backup and configuration.



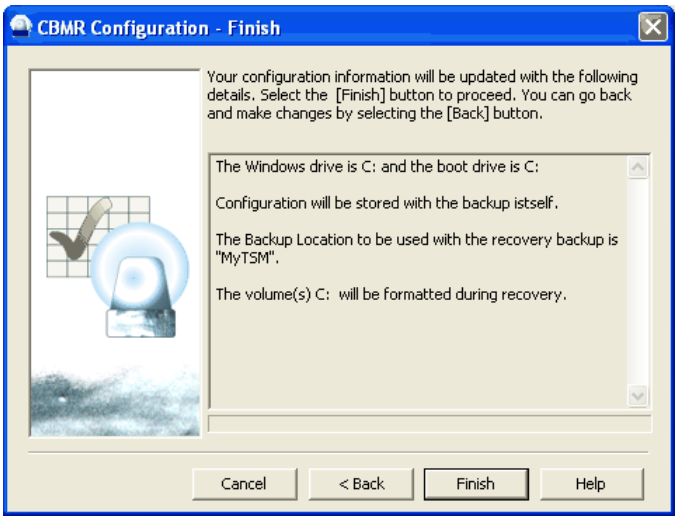
5 If a VTD is chosen as a Backup Location and it resides on a remote share, the CBMR Configuration - Provide Authentication Details page will be shown to allow the network authentication details to be specified.



6 The CBMR Configuration - Select Volumes to Format page will help you to select the disks and partitions which should be formatted during a recovery.



7 Click on **Next>** to confirm the disks/partitions for formatting.



8 Finally click **Finish** to save the setting. When a DR backup is run, the configuration information will be stored to a folder on the Windows drive named CBMRCFG and this folder will be automatically included with the backup. This folder should neither be removed manually nor its attributes or contents changed.

NOTE: If you choose this option you will need to manually specify the Backup Location during the recovery procedure.

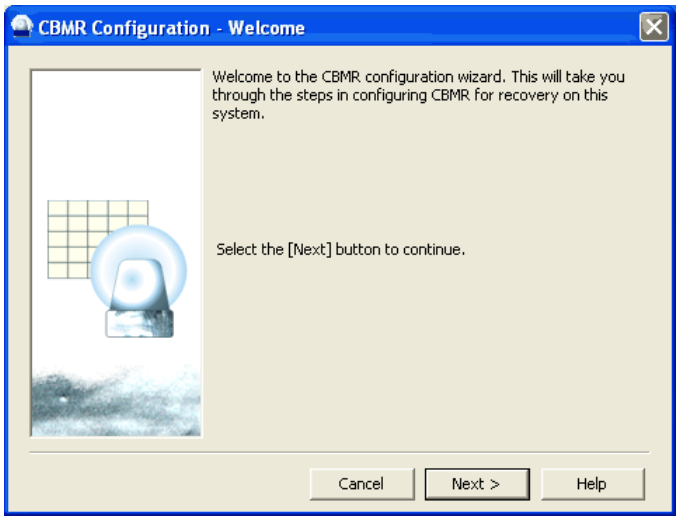
4.1.2 Storing the Configuration Information in a Specific Location

This can be useful if:

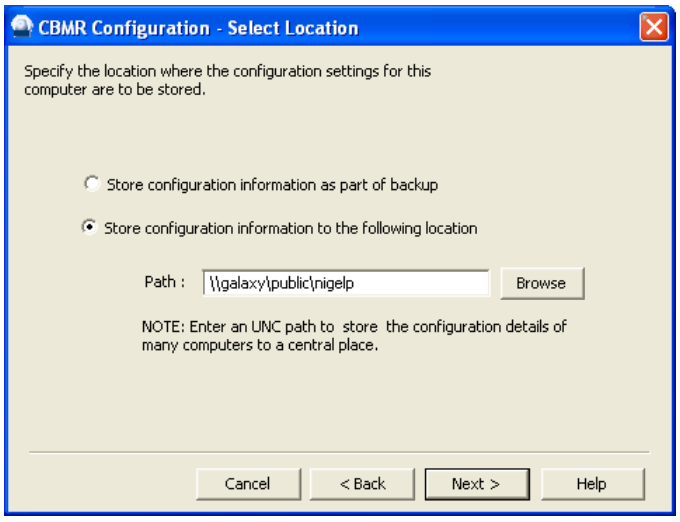
- You do not have a floppy or another locally attached drive.
- A number of similar computers are connected to a network.

In the CBMR main window, click on the Setup Disaster Recovery Configuration option.

The CBMR Setup Configuration Wizard Welcome will appear.



Click on **Next>** and the CBMR Configuration - Select Location page will appear.



1 Select the Store configuration information in the following location radio button.

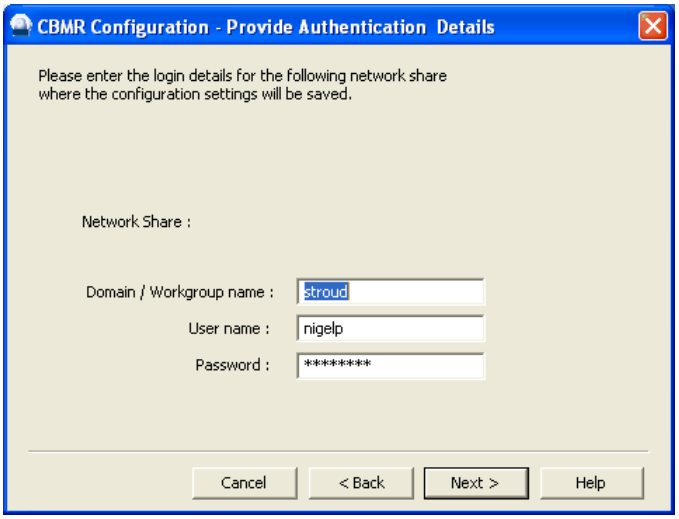
2 If the configuration is to be stored on a local drive such as a floppy or USB disk either use the **Browse** button to navigate to the folder or specify the path like:

- A: (root folder on a floppy)
- F:\Configs (folder on a locally attached USB disk)

Saving the configuration to a network share requires a full UNC path to be entered, such as:

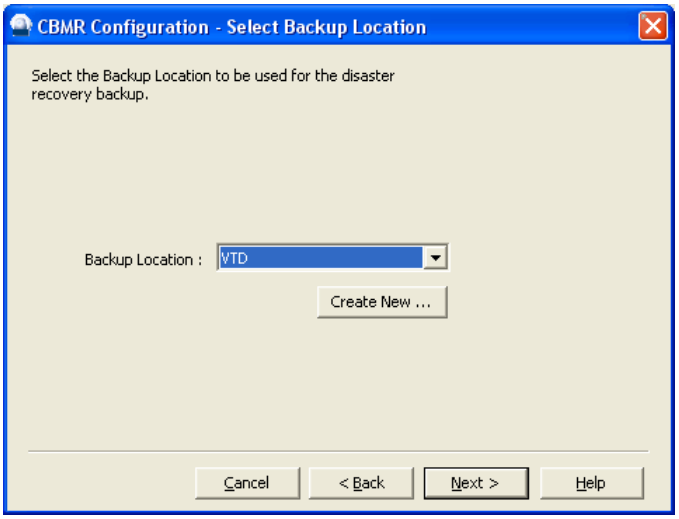
- \\Galaxy\CBMR\Configs

To gain access to the network share you may be required to enter your network credentials. Specify your network Domain or Workgroup and a valid network Username and Password.

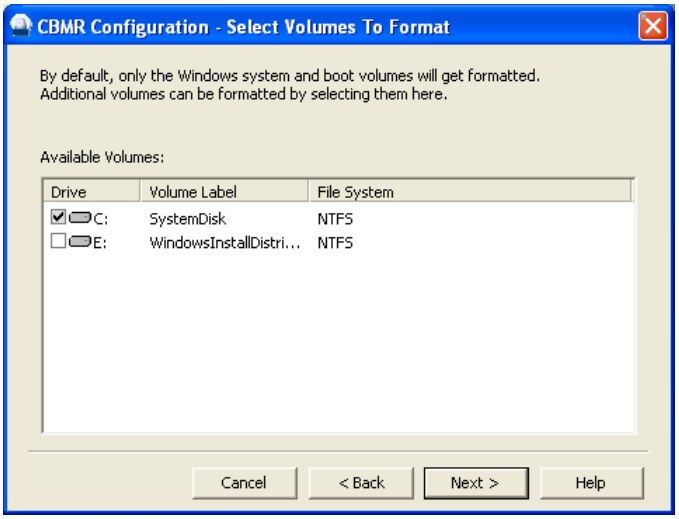


3 Whether the configuration is stored on a network share or on a local drive, the selected folder must currently exist.

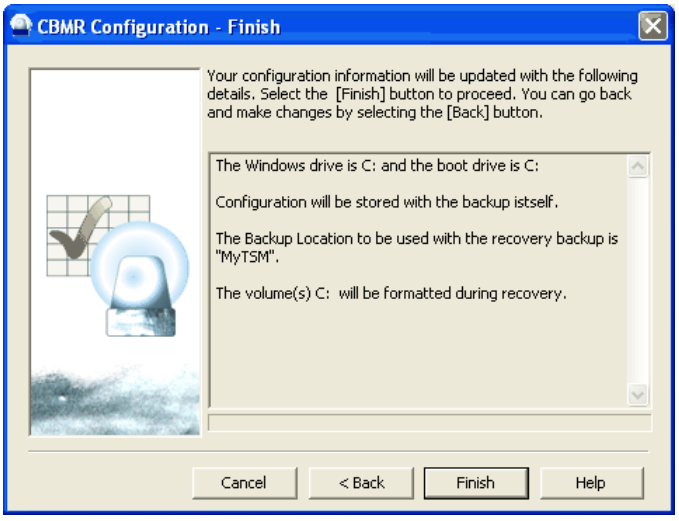
4 Press **Next>** and you will now be prompted to select a Backup Location for the DR backup and configuration.



5 The CBMR Configuration - Select Volumes to Format page will help you to select the disks and partitions which should be formatted during a recovery.



6 Click on **Next>** to confirm the disks/partitions for formatting.

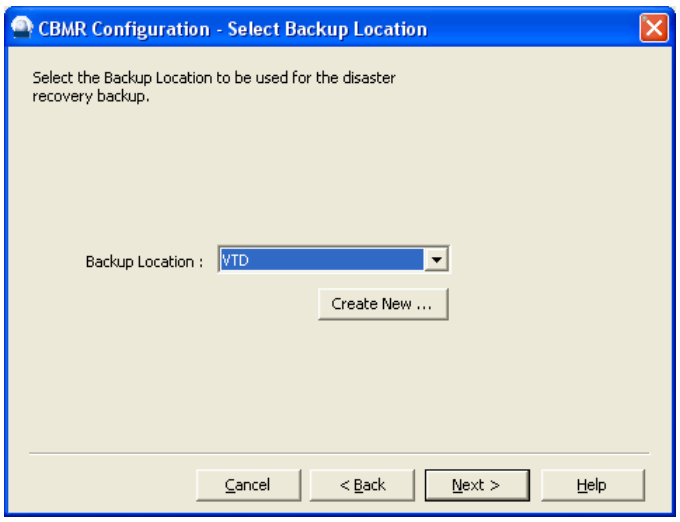


7 Finally click **Finish** to save the configuration to the selected location.

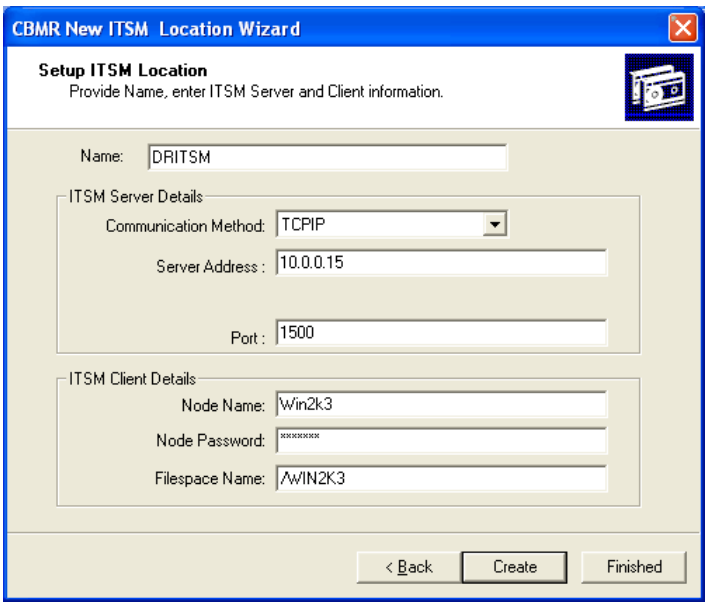
NOTE: If a UNC path is specified for the configuration location, the same path can be used for all the computers in the workgroup as individual system's configuration will be stored under a folder named after the system's NetBIOS name.

4.2 Choosing a DR Backup Location

After choosing a location for the configuration, you will then be asked to select a Backup Location for the DR backup.



1 The drop down control will list all the existing Backup Locations. If you wish to create a new Backup Location just for the DR backup, select **Create New...** which will show the New Backup Location Wizard.

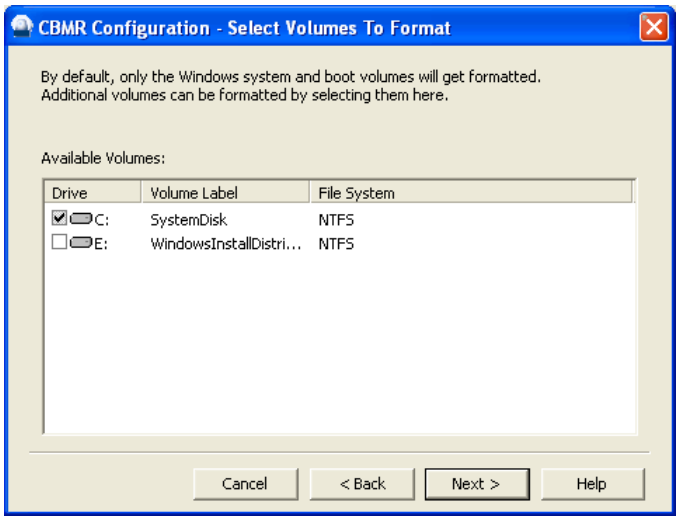


In the example above, a new ITSM Backup Location is being created. Select **Create** to create the new Backup Location. Once done, select **Finished** and the control will return to the Select Backup Location page.

2 Press **Next>** and you will now be prompted to select the disk options for the DR backup and configuration.

4.3 Selecting Volumes To Format

The "CBMR - Select Volumes to Format" page allows you to select the volumes and partitions which should be formatted by the Recovery Console as part of the recovery procedure.

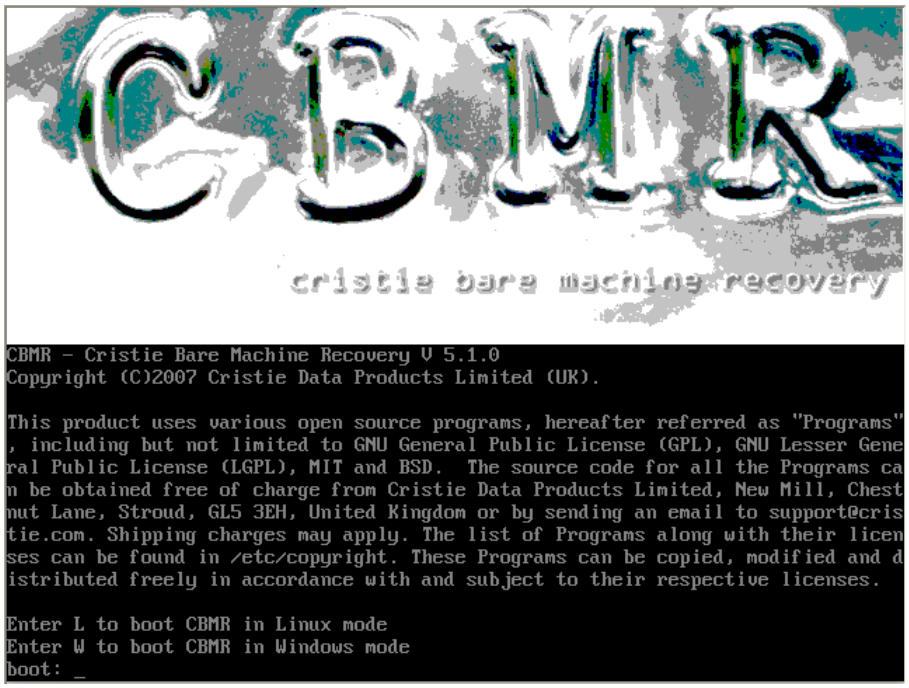


The Windows boot and system partitions will be selected by default and you cannot exclude them. All other volumes and partitions can be selected or de-selected by clicking on the selection box which toggles the current selection.

1 Select **Next>** when you have finished your selections.

4.4 Booting the DR Console from CD-ROM

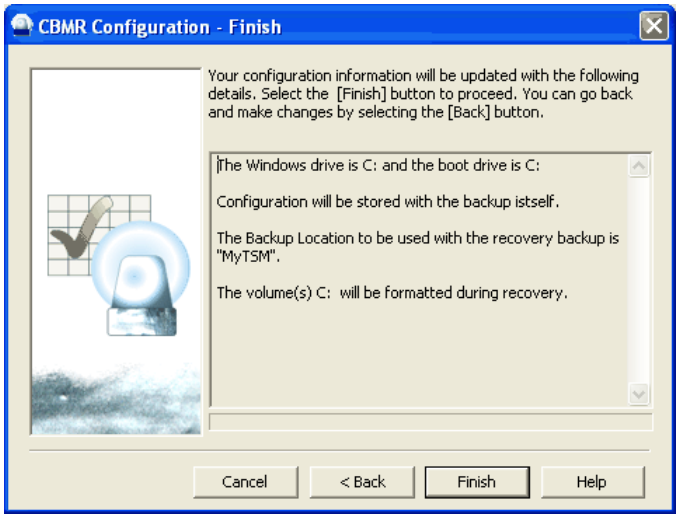
Insert the bootable DR CD-ROM and reset the machine. You will be initially prompted to choose a DR environment - Linux or WinPE.



Choose the appropriate recovery mode. Both environments are compatible with the configuration file and DR backup.

4.5 DR Setup - Finish Dialog

You have almost completed the DR Configuration setup. (The location for the configuration may be a floppy disk, a network share, a local folder or collocated with the DR backup itself)



All of the configuration selections are shown in the scrollable window.

Check that all your selections are correct.

1 If you need to modify any of these settings choose the **<Back** button and modify your selection.

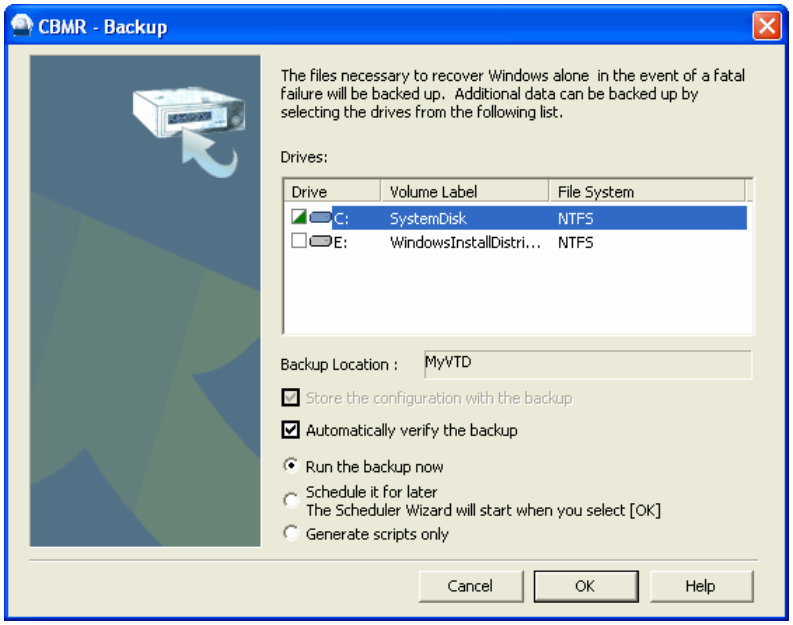
2 If you are happy with the selection choose the **Finish** button and the DR Setup will add your system configuration data to the configuration location of your choice.

5 Creating a Disaster Recovery Backup

1 For locally attached physical Backup Locations (i.e. non-ITSM), insert a clean tape in the tape drive or ensure there is enough space on the backup disk.

2 Click on the Run or Schedule Disaster Recovery Backup icon in the CBMR main window.

The CBMR - Backup Wizard appears. The selected Backup Location is shown and all the settings used for the backup are those that are currently specified for the CBMR application.



1 Select the drive or drives you want to backup.

The window shows all the available hard disk drives. You can select all, some or none.

Whatever you choose, the Windows 2000/XP/Server 2003 - folder, Registry and CBMR folder will always get backed up and additionally in Windows 2000 and above, the "Documents and Settings" directory.

2 The Automatically verify the backup check box will be checked by default which will check the integrity of the DR backup. This is independent of the program default settings. This can be turned off by clearing this box. However, this is not recommended.

3 Select Run the backup now radio button if you wish to run the DR backup on pressing the OK button or select the Schedule it for later radio button if you wish to schedule it either using CBMR Scheduler or Windows Scheduler depending on the default settings.

4 Select Generate scripts only if you wish to prepare a script (disrec.scp) for scheduling the DR backup.

NOTE: It is not possible to run a DR backup until the DR configuration has been setup and saved at least once.

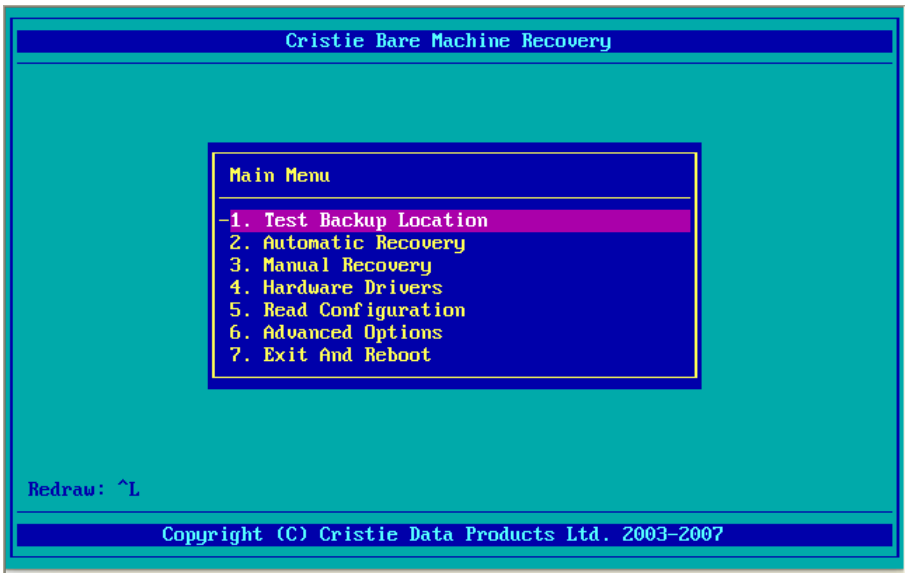
5.1 Testing the Backup Location Using Linux Mode Recovery

NOTE:- Before storing your Disaster Recovery Disk and the DR Backup tape it is important to check that the Disaster Recovery works and the Backup Location is accessible. You only need to test that you can connect to the backup data. The description below is a summary of the process which is described in more detail in the section on Restoring your System.

Insert the Disaster Recovery CD in your CD-ROM drive and reboot your computer from CD. Follow the on-screen instructions and boot the Linux Recovery Console.

5.1.1 Linux DR Console

If successful, Linux DR Console will start.



Ensure that your Backup Location is accessible and, if using tape, that it is switched on and has the DR Backup tape inserted.

Using a configuration floppy

1 Select option 1, Test Backup Location.

A screen message will advise you to insert the DR Configuration disk and the program will ask you for the Media Password, Enter the password if you are using one and then the program will check that a connection can be made to the Backup Location and that a valid tape header can be accessed.

2 Now you can EXIT AND REBOOT the machine (option 7). Make sure the disaster recovery tape is clearly labelled.

Using a configuration file on the network

If you have kept the network details on the configuration floppy

1 Select option 5 (READ CONFIGURATION).

2 Select option 3 (SELECT CONFIGURATION FROM REMOTE SHARE) from the READ CONFIGURATION menu.

3 Select the Copy Files option to copy the configuration files from the network server to the floppy.

With no configuration floppy available or collocated with the DR backup

1 Select Option 5 (READ CONFIGURATION).

2 Select option 2 (SETUP REMOTE SHARE) from the READ CONFIGURATION menu. Then provide the network location of the local machine and the network server where the files are stored.

3 Select the Copy Files option to copy the configuration file from the network server to the local machine.

NOTE: Store the DR System CD or disks and the DR backup tape in a safe location. It is a good idea to keep more than one copy and store them in different locations.

6 Restoring your System

If the situation arises where you need to recover your system, you have all the necessary information on the DR System CD, the DR Configuration Disk (or file) and the DR Backup to get your system up and running in minimal time. The restore process requires little user intervention.

6.1 Linux Based Disaster Recovery Console

1 After the system has booted into Linux mode, the following prompt will appear

```
Press 'f' to use CBMR configuration floppy disk
Press 'u' to use CBMR configuration USB device
Press ENTER otherwise
```

Configuration information on floppy

1 If your configuration information is stored on a floppy disk press **f** and then the ENTER key.

The following prompt will appear

```
Please insert CBMR configuration media and press ENTER [/dev/fd0]
```

2 Insert the floppy disk labelled Cristie DR Configuration disk and press **ENTER**.

Configuration information on USB device

1 If your configuration information is stored on a USB device (such as a USB disk) press **u** and then the **ENTER** key.

The following prompt will appear

```
Please insert CBMR configuration media and press ENTER [/dev/sda]
```

2 Insert the device and press **ENTER**.

3 Drivers will be autoloaded.

Configuration information on remote fileserver

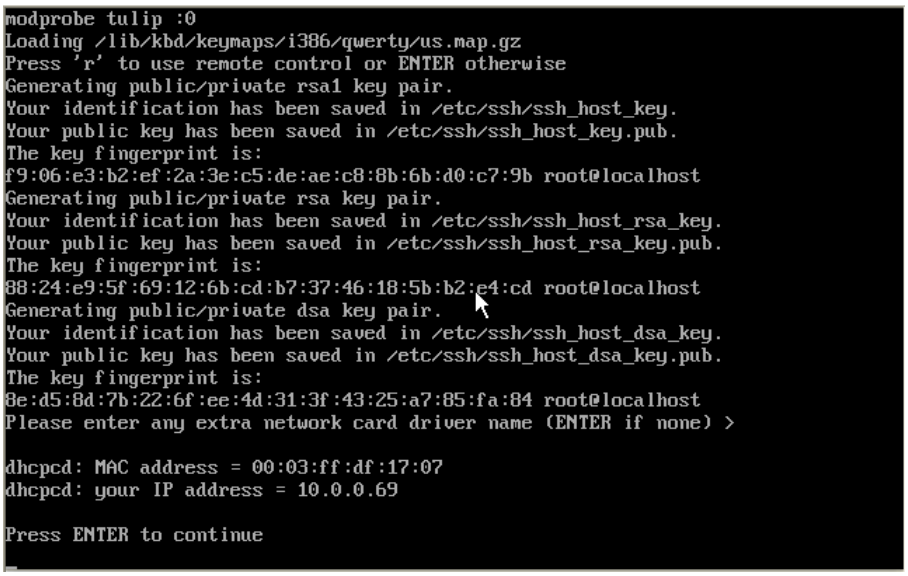
If you have stored the location and network details for the remote fileserver on floppy (checked the Update Floppy Disk box on the Settings File Location dialog) then options are provided on the main Console menu to retrieve this.

Remote Control

Finally the following prompt will appear

```
Press 'r' to use remote control or ENTER otherwise
```

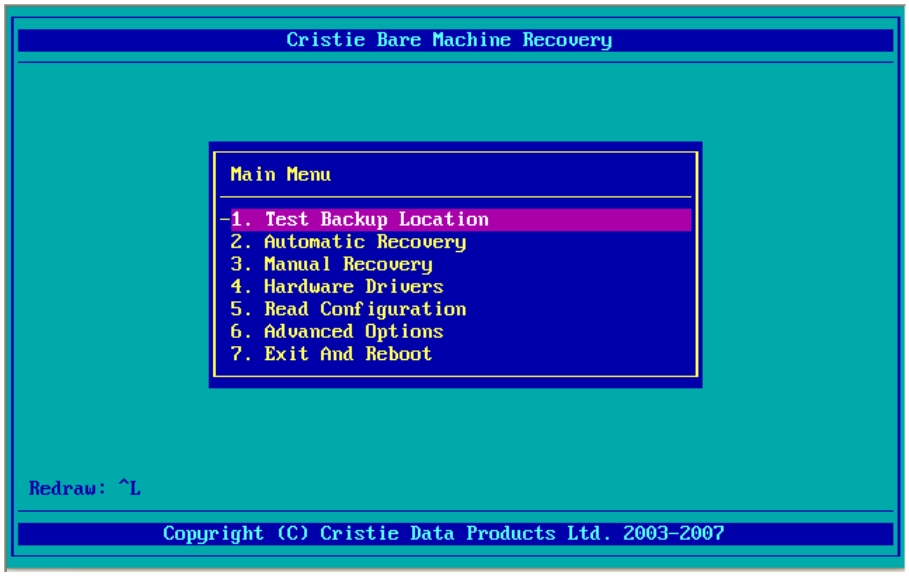
1 Press '**r**' if the remainder of the recovery process is to be performed from a remote location. This will then display information required to support a remote connection to the recovering system.



2 Otherwise press **ENTER** to continue and display the main Linux based BMR Console.

6.1.1 Linux Based Disaster Recovery Console Main Menu

When you boot the Linux DR environment, you will see the Disaster Recovery Console Main Menu as below.



1 Test Backup Location (page 36) allows you to check that the DR Backup Location is accessible.

2 Automatic Recovery (page 37) restores the system using the parameters provided on the configuration floppy.

3 Manual Recovery (page 37) allows you to perform the recovery step-by-step. This is for experienced Linux users.

4 Hardware Drivers (page 40) allows you to load the correct drivers for your hardware if you restore your system to a different hardware than the original one.

5 Read Configuration allows you to to set up the location of the system configuration if located on a network share or collocated with the backup itself.

6 Advanced Options (page 52) require a knowledge of both the Windows 2000/XP/Server 2003 and the Linux operating system. The options are supplied in order that Cristie Technical support can better assist you, should recovery problems exist.

7 Exit And Reboot will exit the recovery console and reboot the machine. You will be prompted to remove the CD and any USB or floppy media.

6.1.2 Test Backup Location Access Option

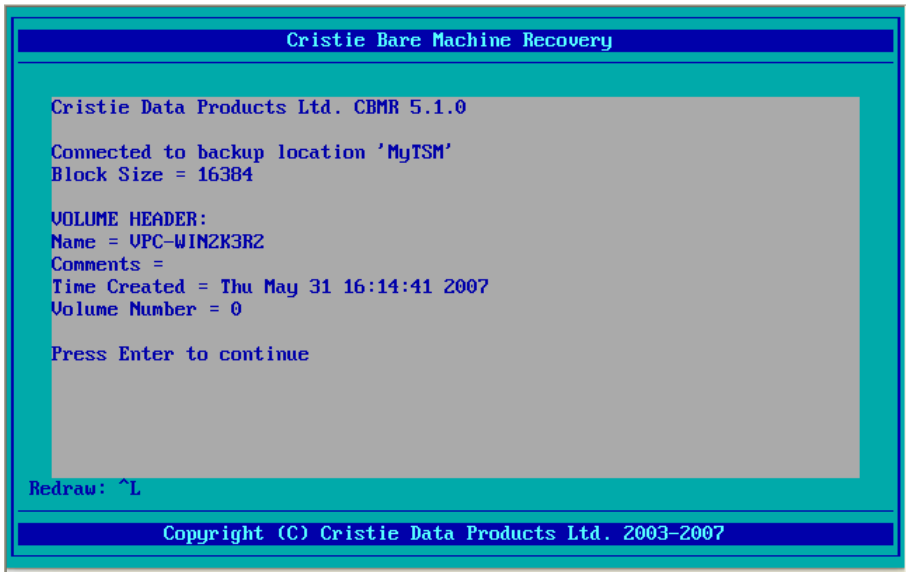
This option allows you to confirm that backup location is accessible without making any changes to the system being recovered. This is normally the first thing to do when presented with the DR console. When you select this option, the DR system uses the driver information saved in the Configuration file to attempt to read the volume header on the media at the backup location and display the results on screen.

If the configuration file is held on a remote fileserver, you must first select the Read Configuration option to select the location of the configuration and to copy the configuration file to the local machine.

If you have not saved the server configuration details to a configuration floppy, you must set up the server configuration details before you can copy the file.

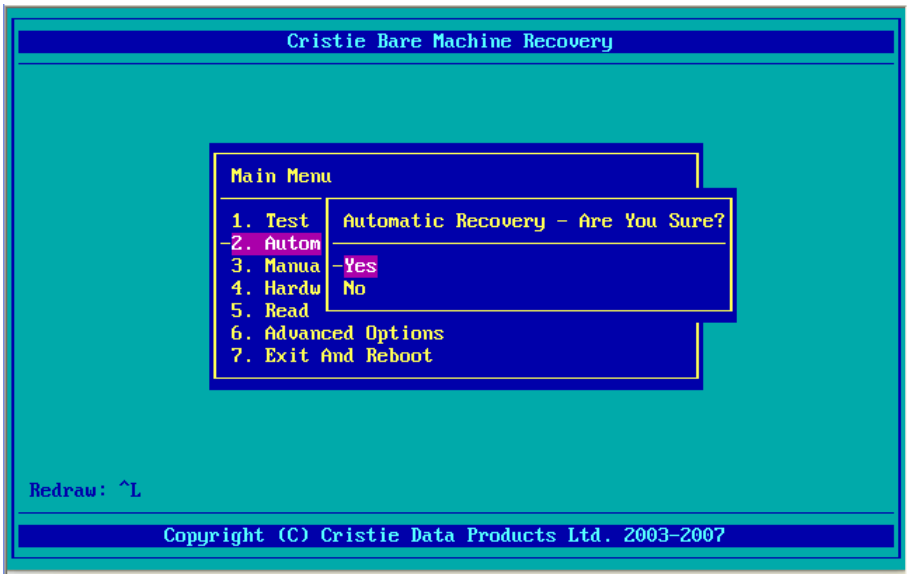
Selecting the Test Backup Location Access option and after a wait of a few seconds you should see

- a message with some information about the backup location
- the volume header name, comments and creation time.



If all this information is displayed correctly then the program has successfully accessed the backup location. If there was a problem with accessing the backup location an error message will be displayed.

6.1.3 Automatic Recovery Option



This is the usual method for recovering a machine to its previous state. It consists of 4 stages of recovery which are described in the manual recovery sections. To invoke automatic recovery, select the menu item and answer **Yes** to the Are You Sure dialogue box. The program will go through each of the 4 stages and ask the user to remove the boot media (floppy disk, CD-ROM or both) at the end. After this is completed, the machine will reboot and Windows will take over to restore any remaining files and information.

6.1.4 Manual Recovery Option

If the "Automatic Recovery" option does not work, or if you want to re-arrange the partitions on the recovered system then it will be necessary to perform a "Manual Recovery"

When the "Manual Recovery" option is selected a further menu appears:-

This enables you to manually Partition, Format and Restore your computer system. It is advisable to have a good working knowledge of the Windows 2000/XP/Server 2003 disk architecture before selecting these options.

When the "**Restore**" option is selected then everything contained in the backup will be restored. This could have been a full backup or a minimal DR backup).

NOTE: None of the other drives will be restored at this point. Other drives can be restored manually using CBMR in Windows mode after the initial restore has been completed.

Manual Recovery: Automatically Partition Option

This stage of recovery creates the machine's partition table. The existing partition table will be overwritten. If the hard disk geometry is not the same as the geometry written to the configuration file (eg if a new hard disk had been installed after a failure), the partitions will be resized in the same ratios as they were on the old hard disk.

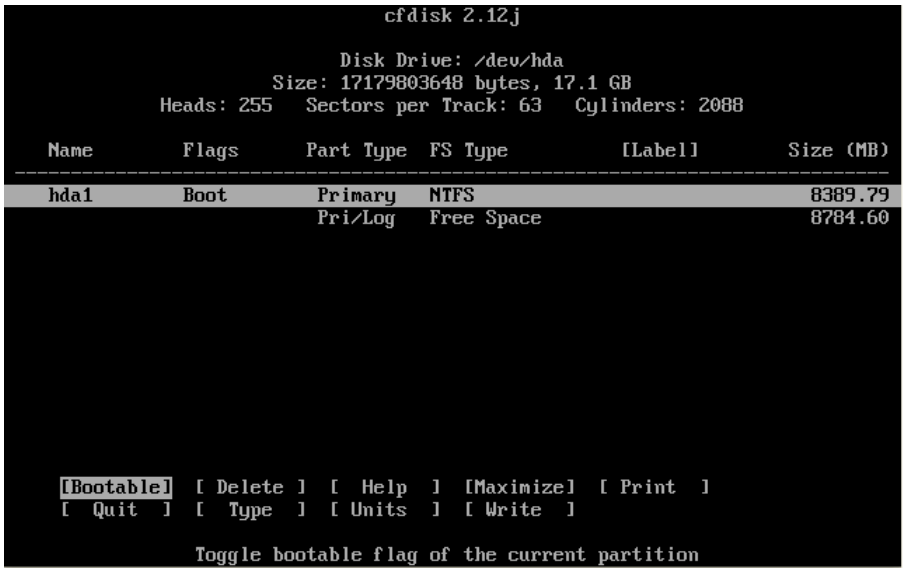
It is, however, possible to opt out if this is not desired. This will work for hard disks that are both bigger and smaller than the original (but the user should bear in mind that if using a smaller hard disk there may be insufficient space to restore all the files).

If more hard disks are found than were recorded in the configuration file, they will not be partitioned, the user should partition them manually at a later stage. Note that Windows NT boot and system partitions will be resized to a maximum of 4GB in order to use FAT16 file system on them. This does not affect Windows 2000/XP/Server 2003 boot and system partitions.

Manual Recovery: Manually Partition Option

This option is useful if you want to create the partitions manually. On selecting this option, available hard disks will be displayed in a menu.

On selecting a disk, a simple utility cfdisk will be launched for that disk which will enable you to partition the disk. The utility cfdisk is very similar to the DOS utility fdisk but only more advanced. A typical screen is as shown below.



Once all the partitions are created, exit cfdisk by selecting [Quit].

Manual Recovery: Format Option

This stage of recovery formats all the partitions that are required to bring up the Windows operating system. This will be either one or two partitions depending on how Windows was installed. Note that Linux mode DR does not support writing to NTFS partitions so all NTFS partitions are created as FAT16 for Windows NT and FAT32 for Windows 2000/XP/Server 2003. Conversion back to NTFS is done by Windows at a later stage. Partitions that are not required for restoring the Windows operating system are not formatted at this stage, this is done at a later stage in Windows.

Manual Recovery: Setup Network Option

Allows you to start the network if not already started. IF DHCP is configured then it will be used to provide an IP address and network mask.

Manual Recovery: Restore Option

This stage of recovery restores files from the backup media onto the hard disk. All the files backed up as part of the DR backup will be restored. A list of files and directories being restored will scroll up the screen as they are read from the media and written to disk. Files and directories which are skipped will be prefixed with a minus sign (-).

Manual Recovery: Setup New Hardware Option

Option not implemented yet.

Manual Recovery: Make Bootable Option

This last stage of recovery makes the recovered hard disk bootable ready for Windows to take over.

6.1.5 Hardware Drivers

This option allows you to load various drivers for the new hardware (SCSI and RAID controllers, network adapters etc.). This is required only when the destination hardware is different than the original hardware (dissimilar hardware restore).

1 Load Modules (page 40)allows you to load modules(drivers).

2 Unload Modules (page 41) allows you to unload already loaded drivers.

3 List Loaded Modules (page 42) lists the loaded modules.

4 System Details (page 42) lists various system configuration details.

5 Skip Hard Disks (page 43) allows you to skip some hard disks from the restore process.

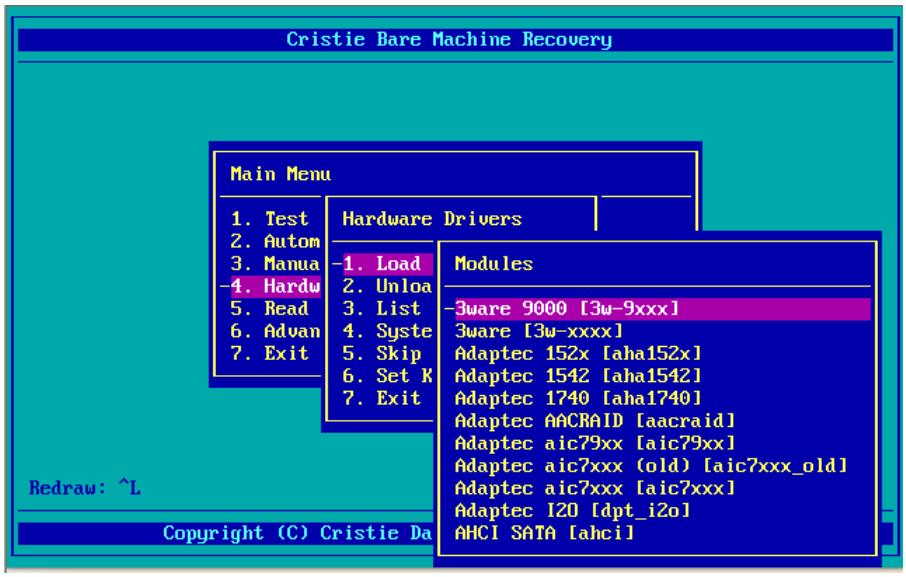
6 Set Keyboard Driver (page 44) allows you to select a keyboard layout.

7 Exit will take you back to the main menu.

Load Modules

Linux mode DR uses modules to access the hardware. This option is used to load modules(drivers) for new hardware. On selecting this option the following menu will be displayed.

On selecting Storage Modules, a list of supported SCSI and RAID modules will be listed. Selecting a module will result in DR loading the module.If you load an incorrect module, an error message will be displayed.



On selecting Network Modules and Other Modules, the appropriate modules will be listed from which you can select the one you need.

NOTE: Loading an incorrect module will not give an error message always. It is possible for an incorrect module to load correctly though it will not function properly. Some modules may take quite a long time to report a failure. If your hardware is not listed, contact Cristie Support for a driver.

Unload Modules

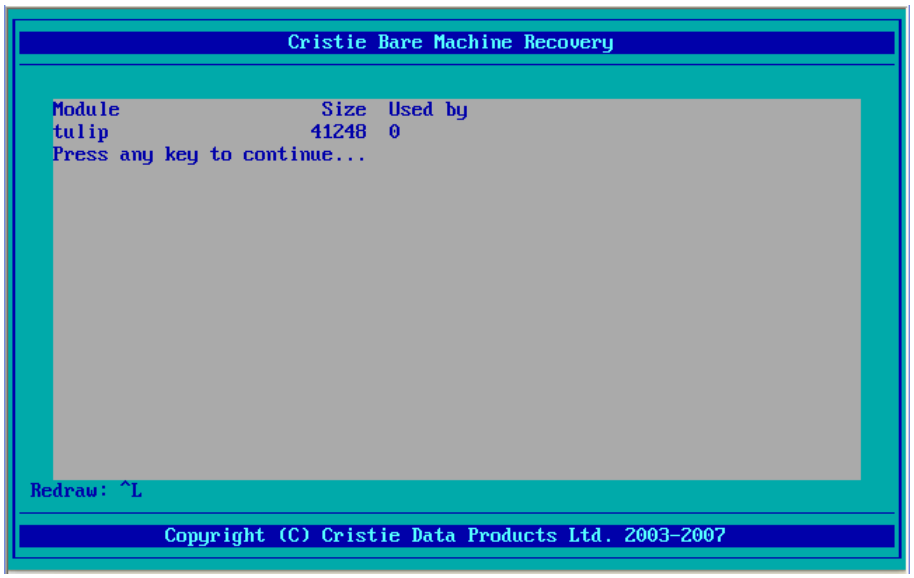
This option allows you to unload modules which are not needed for the restore or which may interfere with the restore operation if left loaded.

On selecting this option, all the loaded modules will be listed in a menu.

Selecting a module from the list will unload the module. If a module cannot be unloaded, a message will be displayed explaining why.

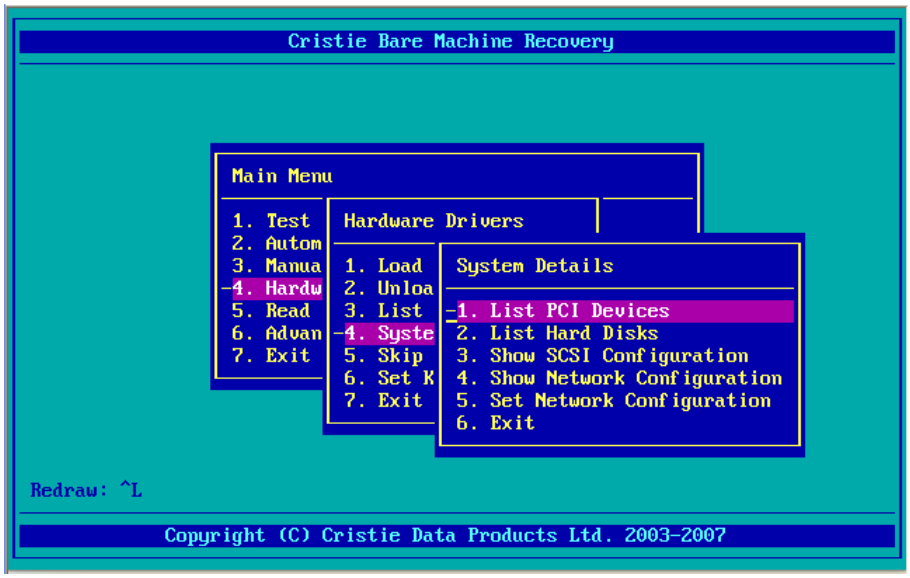
List Loaded Modules

This option shows a list of successfully loaded SCSI, RAID and network modules.



System Details

This option shows various system configuration details like the installed PCI devices, hard disks, SCSI and network configuration.



1 List PCI Devices will list all the installed PCI devices and their description. Useful to find the correct driver without opening the cover of the machine.

2 List Hard Disks will list the available hard disks on the system.

3 Show SCSI Configuration will show the available SCSI hosts and targets on the system.

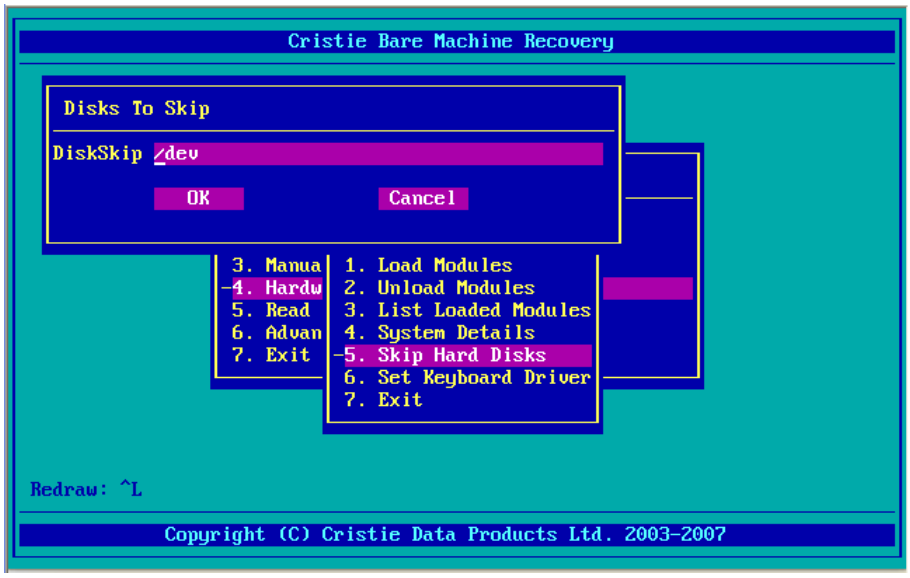
4 Show Network Configuration will show the network instances, their IP address bindings and the routing table entries.

5 Set Network Configuration will allow the network interface speed and duplex settings to be changed.

6 Exit will take you back to the Hardware Drivers menu.

Skip Hard Disks

This option allows you to skip hard disks from the recovery process. At times it may be necessary to completely ignore a connected hard disk from the recovery process.



You can enter a full path to the hard disk or a wild card pattern. In the above example, the first SCSI hard disk will be ignored from the recovery process. If you want to ignore all the SCSI hard disks you can enter '/dev/sd*'.

Set Keyboard Driver

This option allows you to select the desired keyboard layout during the Linux mode recovery.

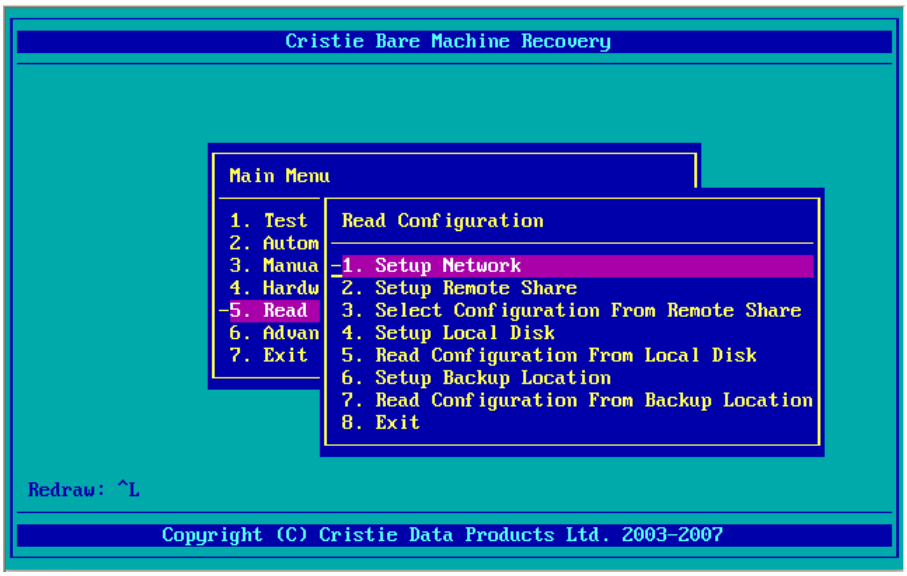
Supported layouts are as follows:

Option	Description
fr	French
sv	Swedish
uk	English (United Kingdom)
us	English (United States)
de	German
sg	Swiss German

6.1.6 Read Configuration

Select the Read Configuration options to setup the location of the system DR recovery configuration or to set the network settings for the recovering machine.

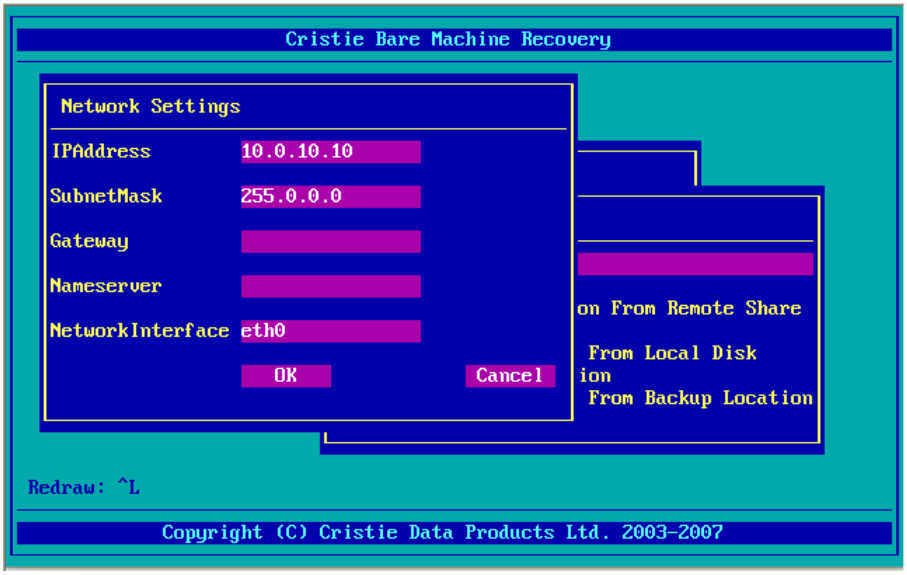
Note that the configuration may be held on a local disk (floppy or USB disk), network share or collocated with the backup.



The following sections explain each option in more detail.

Setup Network

Use this menu option to setup the local network interface settings for the recovering machine.



IPAddress

This should be set to the local IP address to be used for the local network interface setup for connecting to the share containing the machine configuration. Note that this IP address need not be the same as the permanent IP address for this machine, and a single address could be used for many machines, providing that they are not used at the same time. This field can take the value DHCP if a DHCP server is to be used.

SubnetMask

This field specifies the subnet mask for the network interface. This field can take the value DHCP if a DHCP server is to be used.

Gateway

This field specifies the gateway to be used to connect to the remote share. If no gateway is required this field can be left blank. This field can take the value DHCP if a DHCP server is to be used.

Nameserver

This field specifies the nameserver to be used for hostname lookup. If hostname lookup is not required this field can be left blank.

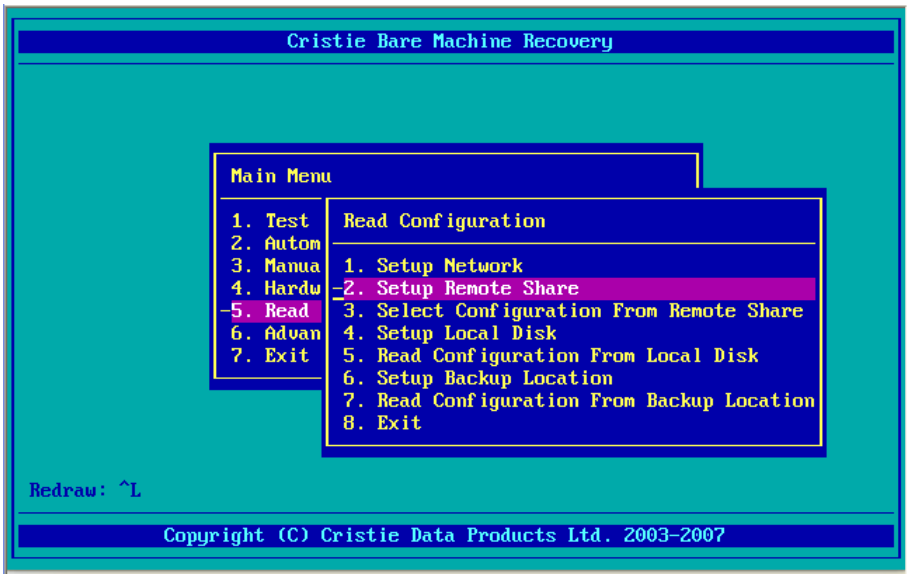
Network Interface

This field specifies the network interface which should be used to connect the remote share. This will take values like eth0, eth1 etc., where eth0 refers to the first ethernet adapter. If this is left blank, the first available interface will be used.

Once you click on **OK**, the software will attempt to assign the specified IP address to the interface. You can check this if necessary by switching to another BASH shell (`<Alt><F2>`) and typing `ifconfig`. This will show you if an IP has been assigned to the interface and you may also use the `ping` command from here to test connectivity. Return to the GUI by pressing `<Alt><F1>`.

Configuration on Remote (Network) Share

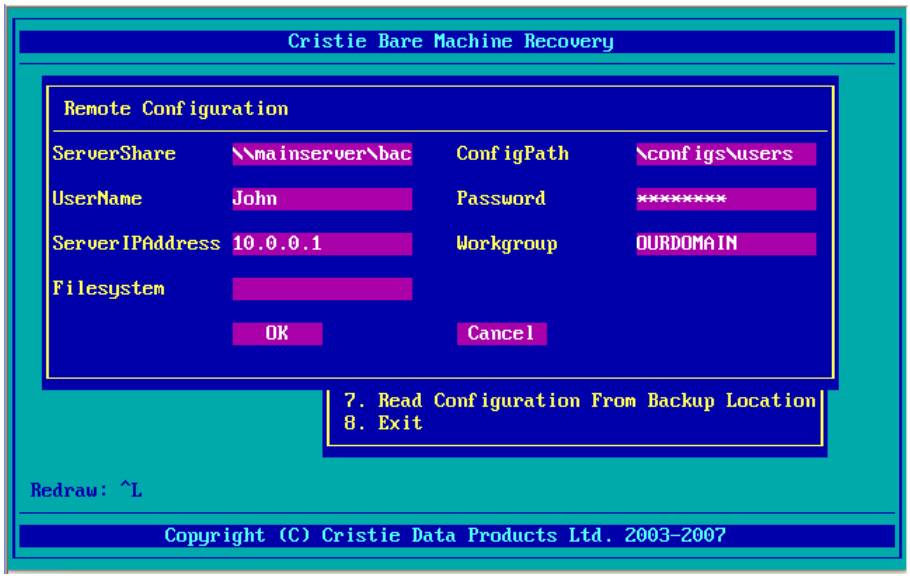
In order to use configuration information located on a remote share first setup access to the network share itself and then select the desired configuration from the share (there may be more than one).



- Setup (page 47)
- Select Configuration (page 49)

Setup Remote Share

First you may need to set Local IP settings. Use the **Setup Network** menu option to do this.



ServerShare

This field should contain the server share name which contains configuration information. The share name should be of the form `\\<hostname>\<share>`. The hostname can be specified rather than using an IP address as this is specified elsewhere.

ConfigPath

The path under the share where the configuration information is stored. This path should start with \

UserName

A username which has read access to the share containing configuration information.

Password

The password corresponding to the above username. Note that the password field will not be displayed on screen.

ServerIPAddress

This field should contain the IP address of the server which holds the configuration information.

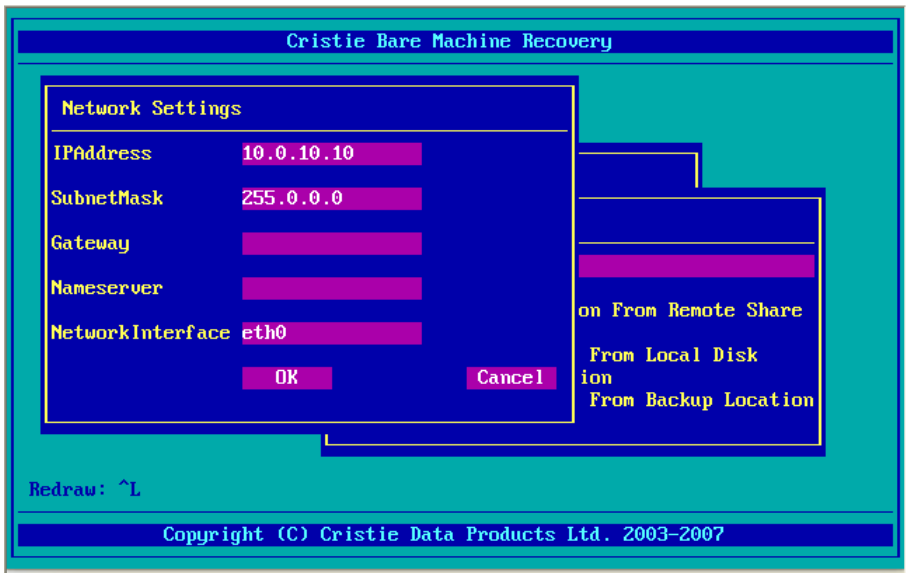
Workgroup

This field should contain the workgroup or domain name for the server containing the network configuration.

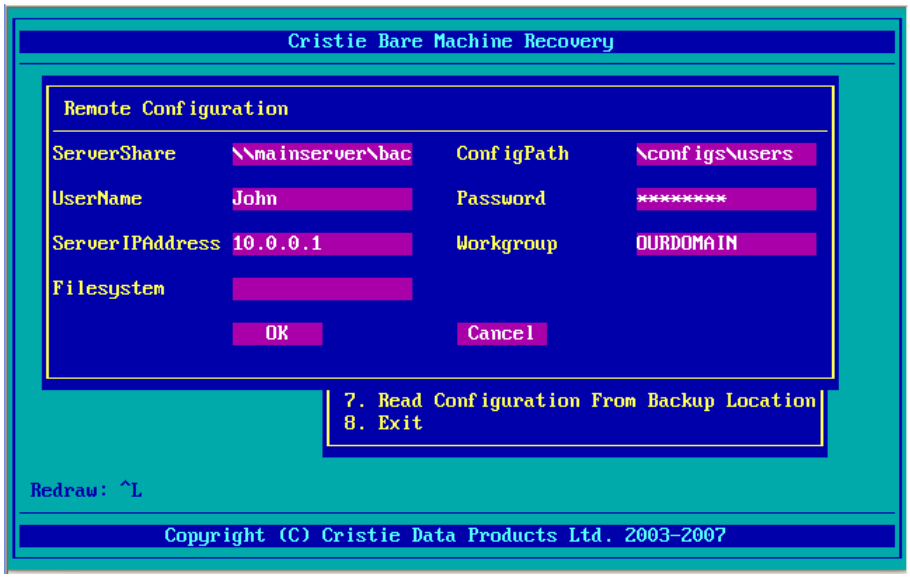
Example form

Say we have a system we need to recover with hostname `mypc` and IP address `10.0.10.10`. The configuration information is stored in `\\mainserver\backups\configs\users`. The server `mainserver` has IP address `10.0.0.1`. Both machines are members of domain `OURDOMAIN` and are on the same subnet (mask `255.0.0.0`). User `john` with password `hello` has read access to the share containing the configuration information. We are not using DHCP on this network. The forms should be filled out as follows:

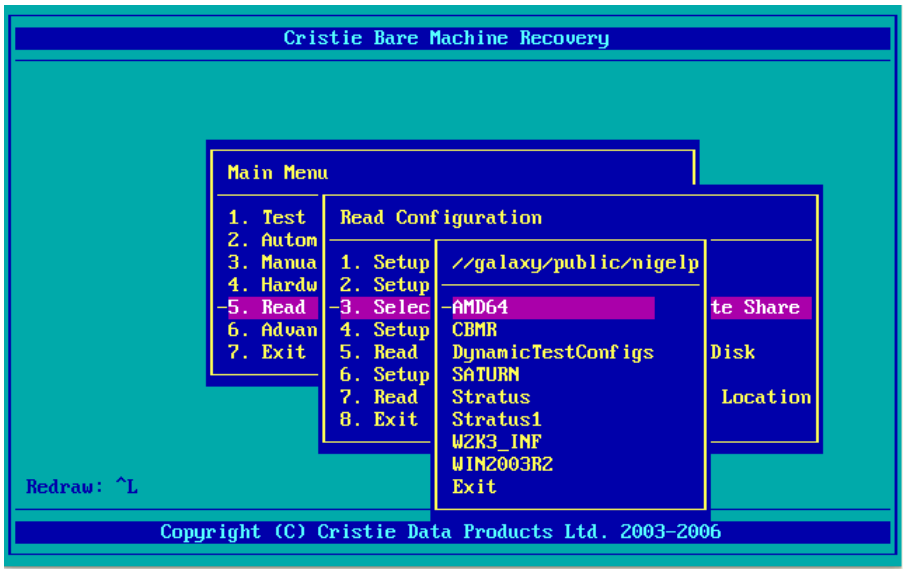
IPAddress: 10.0.10.10
SubnetMask: 255.0.0.0
GatewayIP: <blank>
ServerIPAddress: 10.0.0.1



ServerShare: \\mainserver\backups
ConfigPath: \configs\users
UserName: john
Password: hello
ServerIPAddress: 10.0.0.1
Workgroup: OURDOMAIN



Select Configuration from Remote Share

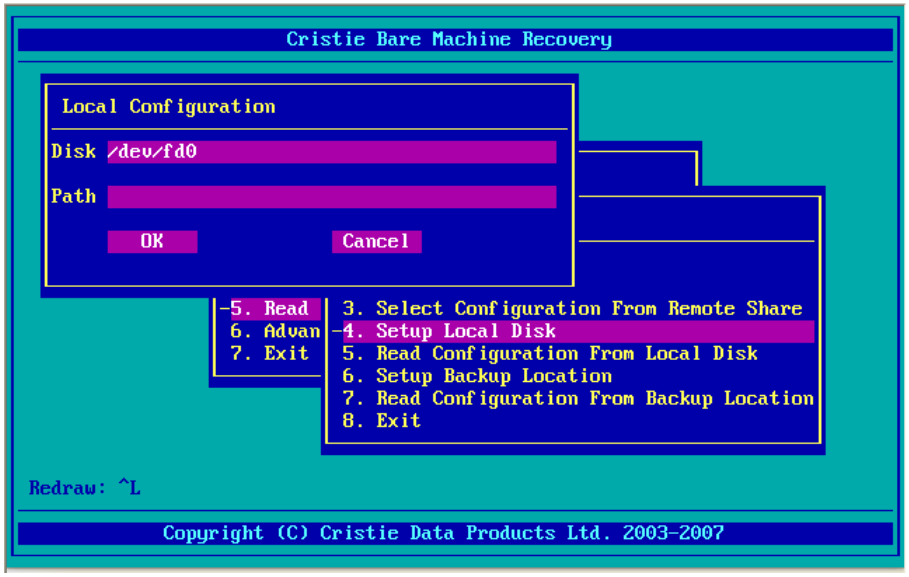


This option will give the user a menu based on available remote configurations. The user should choose the correct configuration for the hostname of his system. Note that an incorrect choice of configuration may not work on the user's system.

The system drivers and other configuration details will then be copied to the local system from the remote server share.

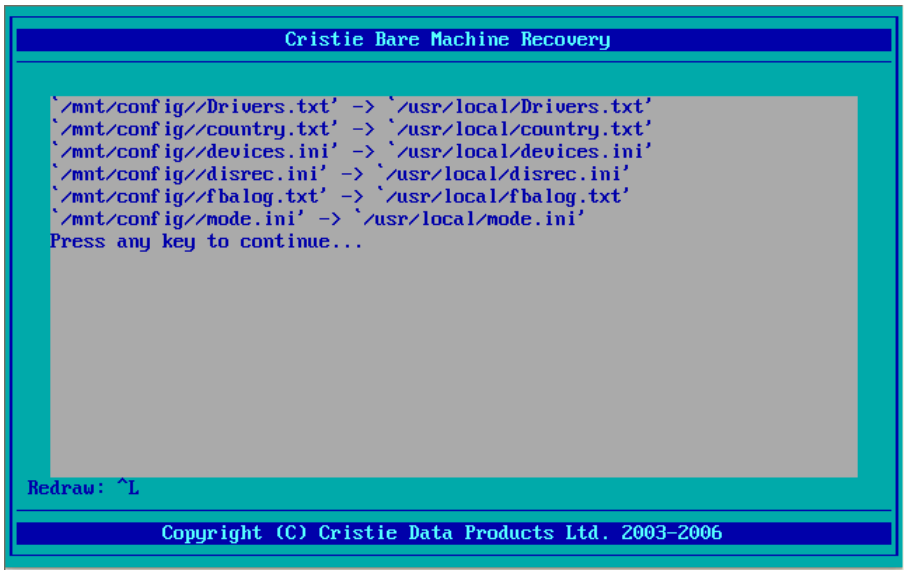
Setup Local Disk

If the configuration is held on a local disk (not already specified), use this menu option to define the device and path of the configuration.



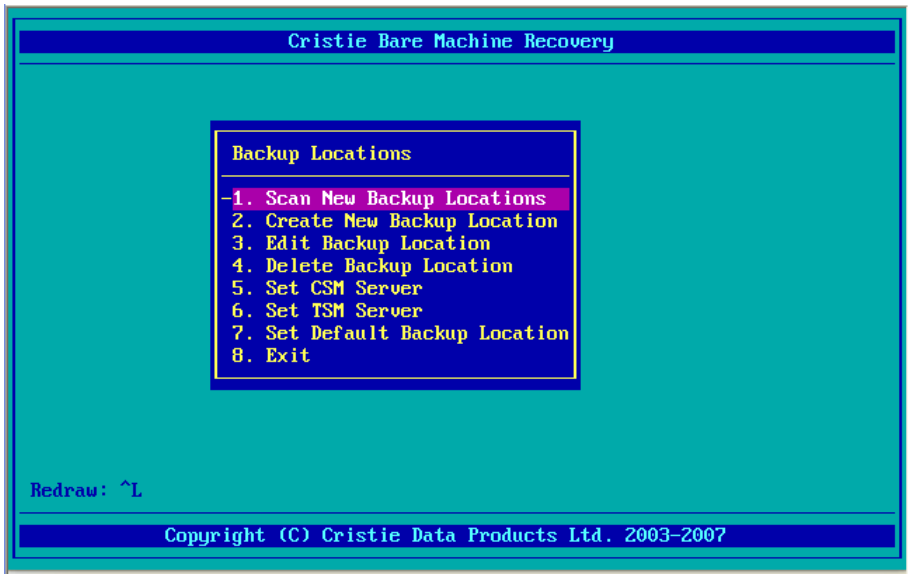
Read Configuration From Local Disk

Allows the configuration to be read from a local disk such as floppy or USB disk. After reading the configuration the following is displayed (files have been copied to local workspace):



Setup Backup Location

This option allows you to select a Backup Location for the restore operation and to update the password for the ITSM client node.



1 Scan New Backup Location will attempt to locate any directly attached devices like SCSI tape or Autoloaders. It will not detect TSM devices.

2 Select Location will allow you to select a Backup Location for restore. By default the location stored in the configuration file Disrec.ini file will be used for the restore. This is useful if you maintain different versions of data under different locations.

3 Update Password will allow you to update the TSM Backup Location with a new password. It is possible you periodically change the password to your TSM client node. In this case the original password stored with the configuration information file Devices.ini will no longer valid. Using this option, it is possible to update the password.

NOTE: Passwords are always encrypted using Cristie's proprietary encryption algorithm before storing.

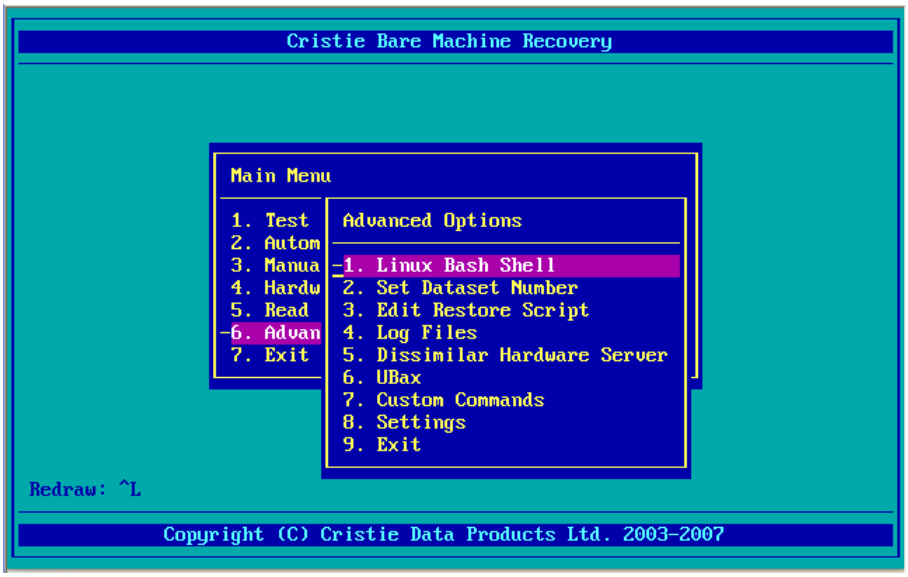
Read Configuration From Backup Location

Once the Backup Location has been created, select option 7 to read the configuration from the designated backup device setup from option 6.

This will result in the backup being accessed to retrieve the configuration details. You may be prompted for a password if the backup is password protected.

6.1.7 Advanced Options

There are several advanced options available from the DR console. As the name suggests, this is for users who have some fluency in the Linux operating system and the internals of how CBMR DR works.



1 Linux Bash Shell gives you a bash shell

2 Set Dataset Number allows you to set a dataset for recovery purposes.

3 Edit Restore Script allows you to edit the final script to include and exclude files.

4 Log Files allows you to view and store various log files created by DR.

5 Dissimilar Hardware Server starts a server process so that various Windows drivers can be installed from another Windows workstation running on the same network.

6 UBax provides a direct link to UBax - the underlying backup/restore engine used by CBMR for Linux

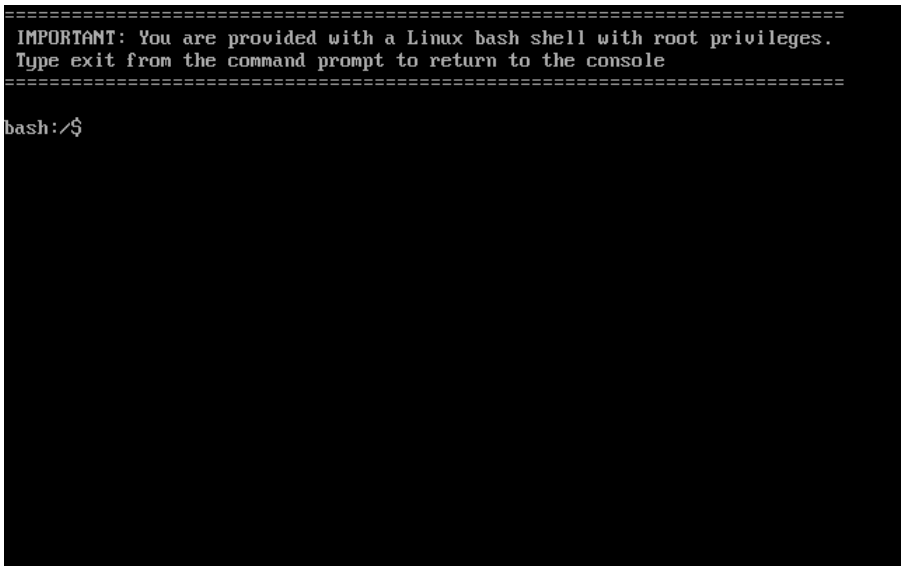
7 Custom Commands allows you to select custom commands and scripts.

8 Settings will allow you to modify disrec.ini, remote.ini, devices.ini. This is recommended for advanced Users only.

9 Exit will take you back to the main menu.

Bash Shell

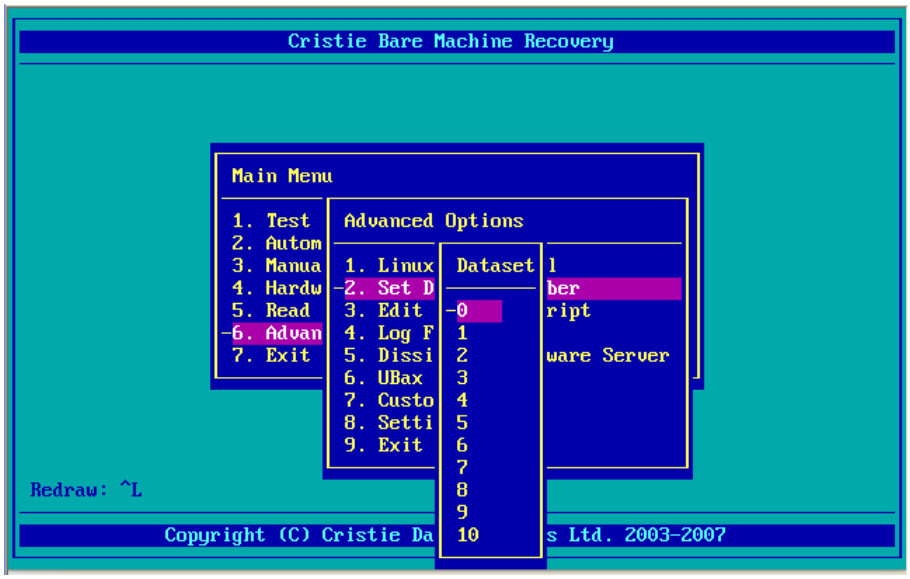
This option provides the user with a Linux 'bash' shell in which to execute commands. This option should be used by experts only.



To exit the shell, type `exit` and return to the menu.

Set Dataset Number

This option is used to set the number of the dataset to restore from. By default this is set to the first dataset (number 0). Selecting a number from the menu will change the dataset number in the script used to restore files.



Edit Restore Script

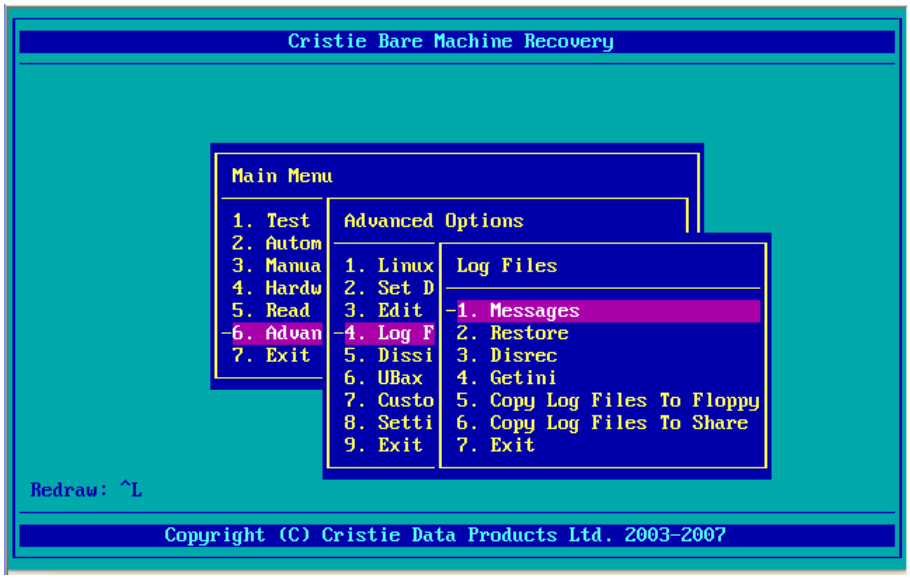
This option allows you to edit the Backup Selection script used to restore files to allow you to remove or add files to be restored at Linux mode DR stage.

```
: Disaster recovery script
: ====Generated by PC-BaX Disaster recovery module. Do not edit!=====
: Build Dec 15 2004 10:17:01
:
Mode=RESTORE
LogFile = LiRest.log
:
Drive = C:
SNumber = 0
:
\ntldr
\NTDETECT.COM
\boot.ini
\BOOTSECT.DOS
\NTBOOTDD.SYS
\Documents and Settings\*.* /SubDirs
\Dokumente und Einstellungen\*.* /SubDirs
\WINNT\*.* /SubDirs
\Program Files\Cristie\CBMR\*.* /SubDirs
~
~
~
~
~
"/usr/local/DisRec.rsf" 19L, 391C
```

The format of scripts is beyond the scope of this document.

Log Files

This option allows you to view various log files created during recovery. These files will be shown on the screen, one screen at a time. It is also possible to copy these files to a floppy so that these can be sent to the Cristie Technical Support in case of an issue.



1 Message will show general messages.

2 Restore will show the messages created by Lirest program. Lirest is responsible for restoring files from the DR backup.

3 Disrec will show the messages created by the Disrec program. Disrec is responsible for hard disk preparation like partitioning, formatting, making it bootable etc.

4 Getini will show the messages created by the Getini program. Getini is responsible for accessing the configuration information stored on a network.

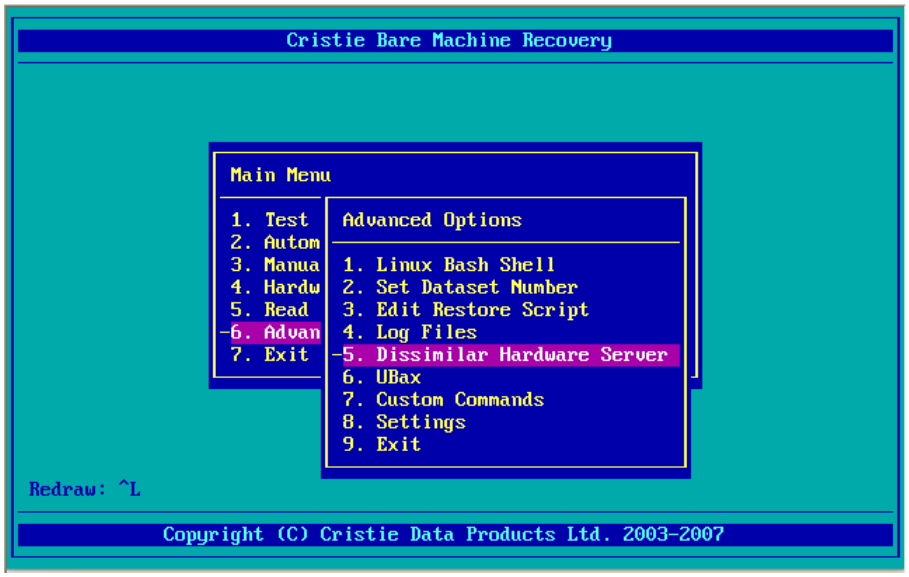
5 Copy Log Files To Floppy will copy all the files to a floppy drive so that these files can be sent to Cristie Technical Support.

6 Copy Log Files To Share as an alternative to the above, will copy all the files to a configured remote network share. This may be more convenient if the system has no floppy drive.

7 Exit will take you back to the Advanced Options menu.

Dissimilar Hardware Server

This option starts the necessary server service so that the Windows mode drivers can be installed in the just recovering Windows system using the Dissimilar Hardware Wizard from another Windows workstation running on the same network.



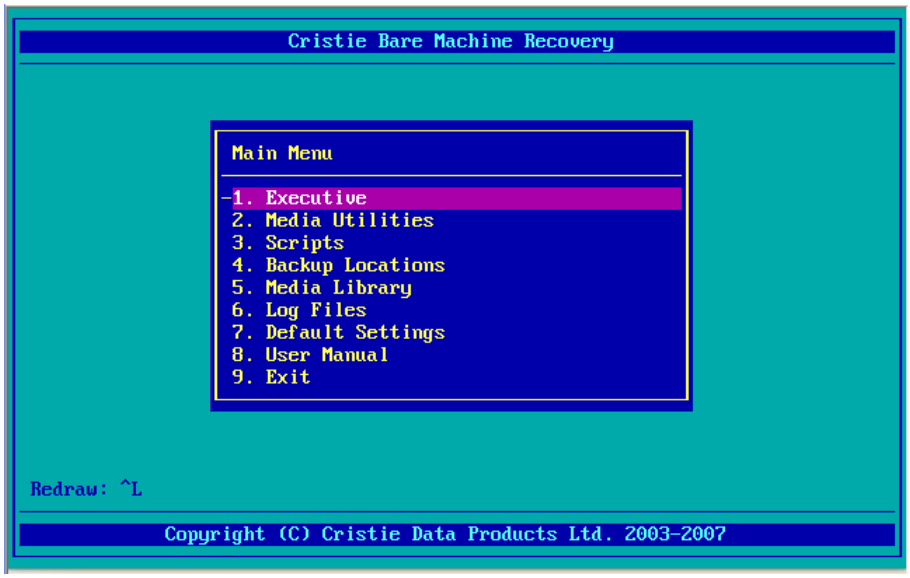
On selecting this option, the active ethernet interfaces and the assigned IP addresses will be displayed.

```
disrec v5.00-0 (c) Cristie Data Products Ltd. 2004-2006
SIOCADDRT 2 eth0 10.0.0.83: Network is unreachable
SIOCADDRT 4 eth0 127.0.0.0: Network is unreachable
Use dissimilar hardware wizard from a Windows 2000 or above
machine to connect to this machine.
The IP address details for this machine are shown here:

eth0      Link encap:Ethernet  HWaddr 00:03:FF:DF:17:07
          inet addr:10.0.0.83  Bcast:1.0.0.0  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17926 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1007 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4527196 (4.3 MiB)  TX bytes:96643 (94.3 KiB)
          Interrupt:11 Base address:0x8000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3084 (3.0 KiB)  TX bytes:3084 (3.0 KiB)

Press any key to continue_
```

Pressing any key from this screen will stop the server.

UBax

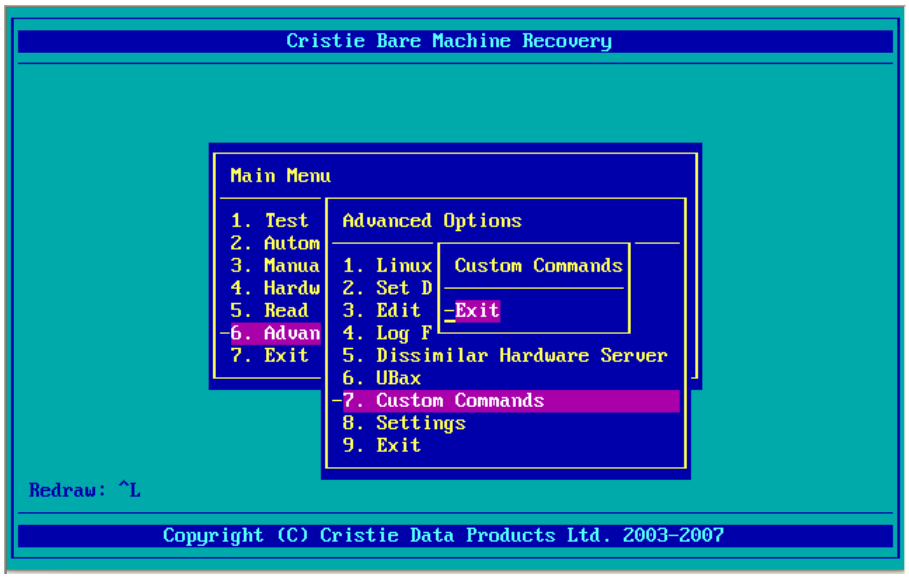
Provides a direct interface to the CBMR for Linux based backup/restore engine. This is used by DR to recover the backup during the Windows based setup.



Refer to the User Manual for further Help on UBax.

Custom Commands

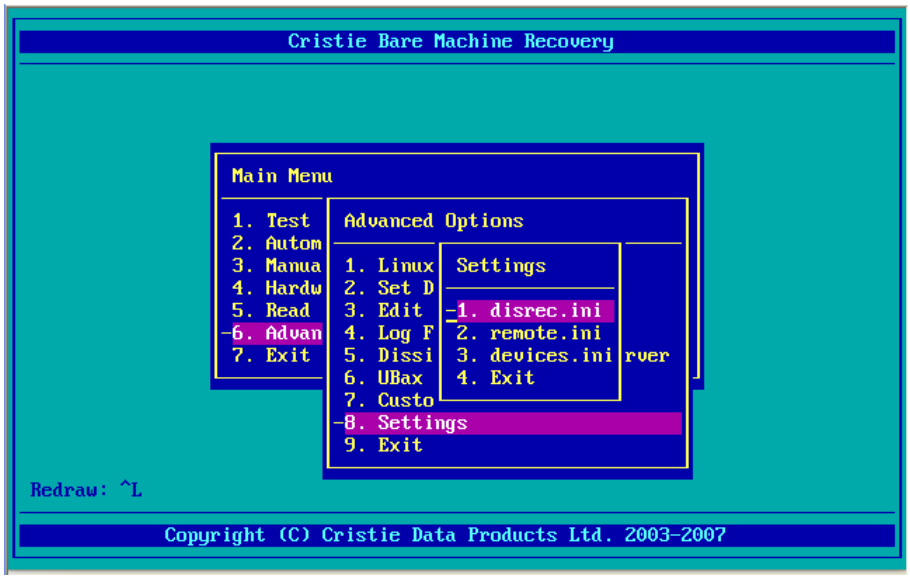
This option will list various command from the \bin folder from the configuration floppy or from the configuration network folder.



This is for advanced customization only, enabling users to run their own Linux shell scripts and utilities.

Settings

Allows some of the CBMR system files to be edited. This is for advanced Users only.



6.2 Linux Disaster Recovery Limitations

The Linux based DR has some limitations on the types of system it can recover.

When recovering a Windows NT4 system with a boot partition greater that 4GB, the boot partition will be resized to 4GB. This does not apply to Windows 2000 or other systems.

Windows dynamic disks are not supported. Use the Windows PE DR environment instead.

6.3 Dissimilar Hardware Support

CBMR can restore a Windows system to the same or similar hardware as well as to a hardware with significant changes. The dissimilar restore capability makes CBMR a deployment or server migration tool as well as a disaster recovery tool. It has to be noted that Microsoft Windows is a complex operating system which has its own hardware dependencies and limitations.

6.3.1 Overview

This document discusses various issues involved in recovering a Windows server or workstation using CBMR version 5.0.0 for Windows . The original machine may have been configured for a very different set of hardware to the machine to which you are recovering. The ability to recover to different hardware is becoming an increasingly important feature in any disaster recovery software. This is due to the fact that hardware is superseded very quickly. So it may not be practical to find an exact replacement for a server or a failed component.

Over a period of time our dissimilar hardware support has evolved and with the latest release, a new Plug-and-Play manager is incorporated which will prompt for the correct driver for the new hardware. With a little knowledge of drivers for motherboard resources, it is also possible to change any aspect of Windows by using the Manual Driver Install option. The rest of the document will explain the steps used in CBMR to recover a Windows system to a different machine.

6.3.2 Hardware differences

Almost all hardware components can be different in a new system. From the CBMR point of view the following are considered different if:

One or more new hard disks are added or removed from the system.

One or more hard disk is replaced with a bigger or smaller capacity disk.

Network adapters are changed.

Mass Storage Controllers like SCSI/RAID are changed.

Motherboard is different.

One or more CPUs are added or removed. The CPU could also be a different model.

6.3.3 Current Support

CBMR addresses the different hardware dissimilarity situations as follows:

a One or more new hard disks are added or removed from the system

If more disks are added, they need to be partitioned and formatted manually using Windows disk management tools.

b One or more hard disk is replaced with a bigger or smaller capacity disk.

The disks may be scaled up or down in proportion to the original disk layout.

c Network Adapters are changed.

The drivers will be loaded automatically and can be selected manually in the Linux mode recovery. Windows drivers will be installed automatically if they are PnP capable.

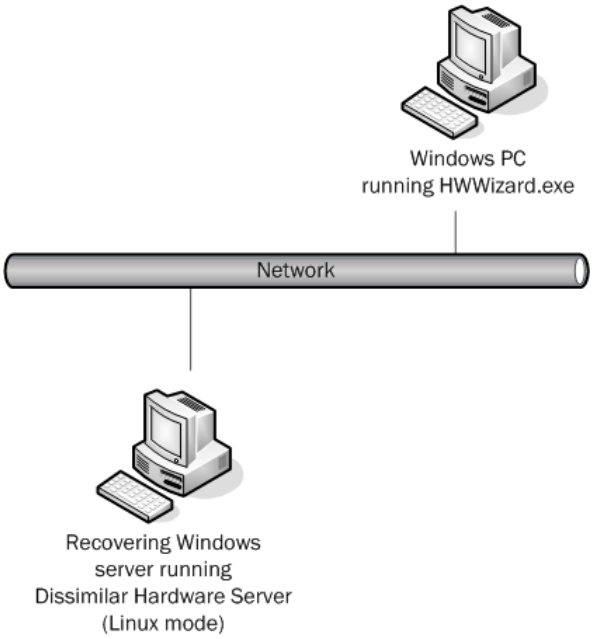
d Mass Storage Controllers like SCSI/RAID are changed.

The correct drivers must be installed using a Cristie utility HWWizard.exe which must be run from a networked Windows system when using Linux DR or run locally when run using WinPE DR.

6.3.4 Linux Based Recovery: How does it work?

The following discussion relates to a dissimilar recovery using the Linux recovery environment.

In a dissimilar hardware situation, the original Windows operating system as restored from the backup may not and mostly will not have the necessary drivers to access the newly installed hardware. It is possible to inject the drivers into the recovering machine using the CBMR tools. This is achieved by accessing the just-recovering system's resources from another Windows 2000 or newer machine running on the same network and by running the utility HWWizard.exe. HWWizard.exe can be found in the CBMR installation folder and also on the CBMR installation CD-ROM. This is the client side of a client-server utility. The server side of the utility is contained in the CBMR installation CD-ROM and which can be accessed from a menu option after booting from the CD-ROM. A section about how to use this utility can be found later in this document.



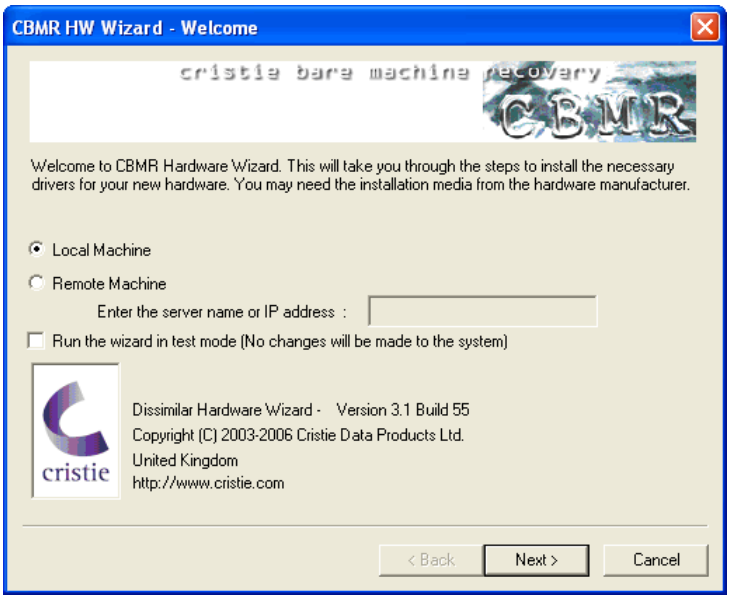
The necessary drivers to access the hardware in Linux mode will be loaded automatically. After this, automatic or manual recovery should be used to partition and format the hard disks and to restore the system files. When this has been done and just before restarting the system, Dissimilar Hardware Server should be started via the Advanced Options. This will make the system's resources available on the network. By running HWWizard.exe from another Windows machine, the new drivers should be installed from the manufacturers installation media or from a network share. The Plug-and-Play feature will enable anyone to install the correct drivers without prior knowledge of what hardware is installed in the new system.

6.3.5 Using HWWizard and the Linux Based DR Console

HWWizard is a comprehensive utility which will install new files and drivers to a just-recovering Windows system. This is a Win32 application and should be run from a Windows 2000 or newer system because it uses some newer Windows components. This utility should always be run on Windows 2000 or newer installation. As there have been changes in the registry editor between Windows 2000 and 2003, you should use a Windows 2003 machine to recover a Windows 2003 machine. HWWizard should also be run in an account with Administrative rights to the local machine.

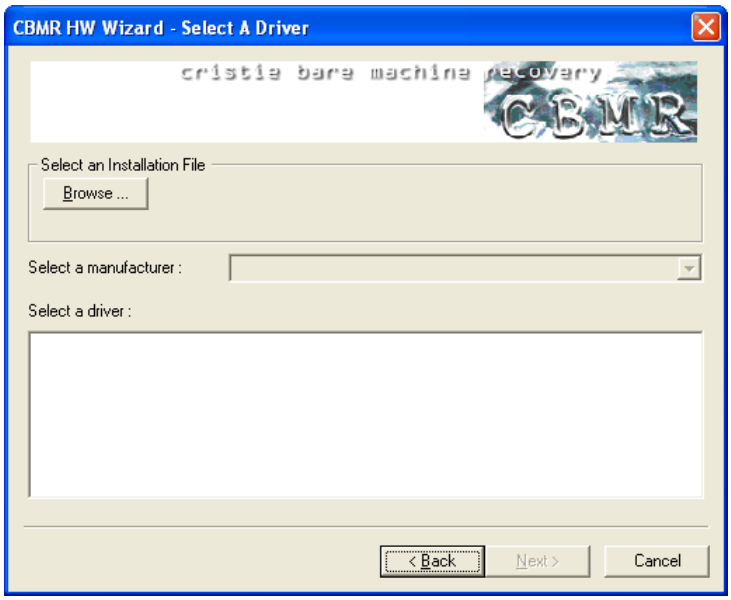
The HWWizard will also allow 64-bit drivers to be 'pushed' to the recovering system. Ensure you have the correct drivers for the target system (i.e. 32 or 64-bit).

On invoking HWWizard.exe from a Windows machine, the Welcome screen will be displayed which is shown below:

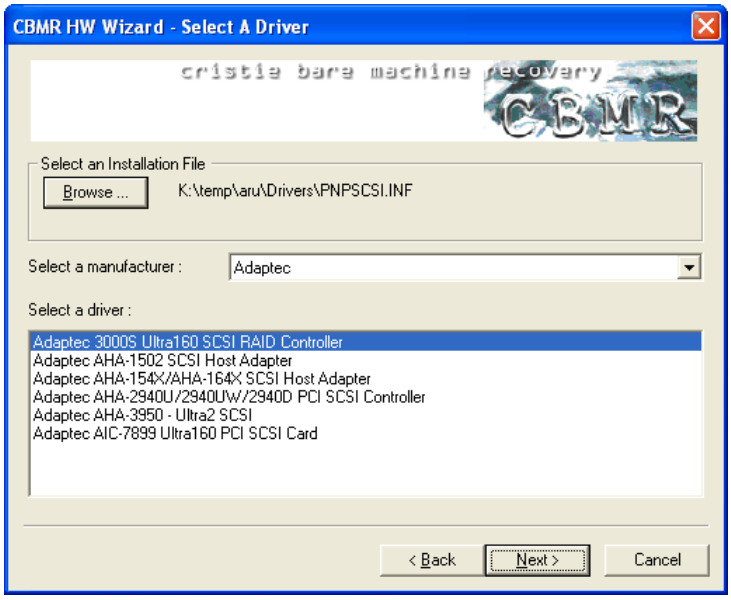


The welcome screen will accept the IP address or the NetBIOS name of the just-recovering system. On selecting **Next>**, the wizard will connect to the just-recovering system and will show the Select A Driver screen. If you get an Authentication screen, enter the pre-defined user ID pcbax and password pcbax and select **OK**.

NOTE: It is possible to run this utility in *test* mode which will not connect to a server and hence no update will take place. In this mode, the driver installation script will be parsed and any errors will be reported. It will create a log file Wizard.log in the current folder. This will also create a file Driver.txt in *test* mode. Both these files should be sent to Cristie when asking for support.

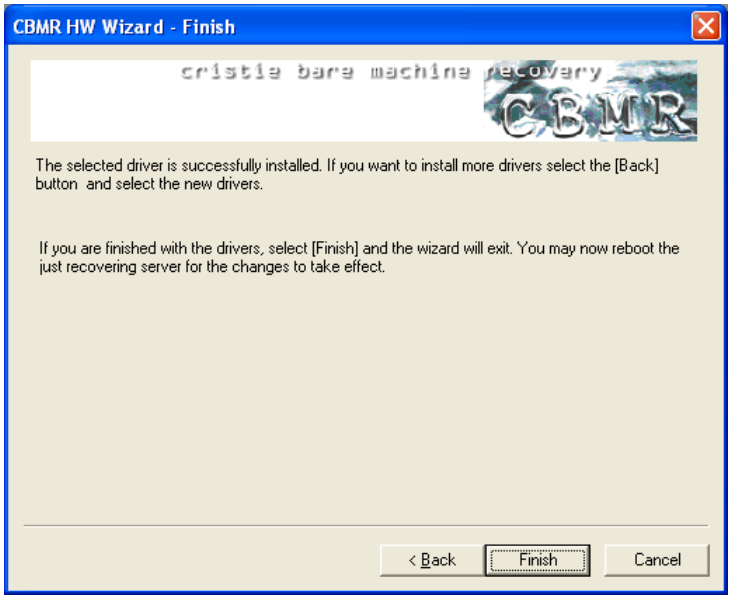


Select the **Browse** button and select the correct INF file for the SCSI/RAID controller you are installing. This will list the manufacturers and the drivers contained in the INF file. A screen shot showing Comaq (now HP) SCSI drivers is shown below.



Once you have highlighted the required driver, select **Next>**. This will show a confirmation dialog. Selecting **Yes** from the confirmation dialog will copy the files across and make the necessary registry changes to the just-recovering system. If it can't find the necessary files on the installation location, it will prompt you for the files.

Upon successful installation, you will get the following **Finished** Screen. You can quit the wizard by pressing the **Finish** button. If you wish to install more drivers, you can select **<Back** and install more drivers.

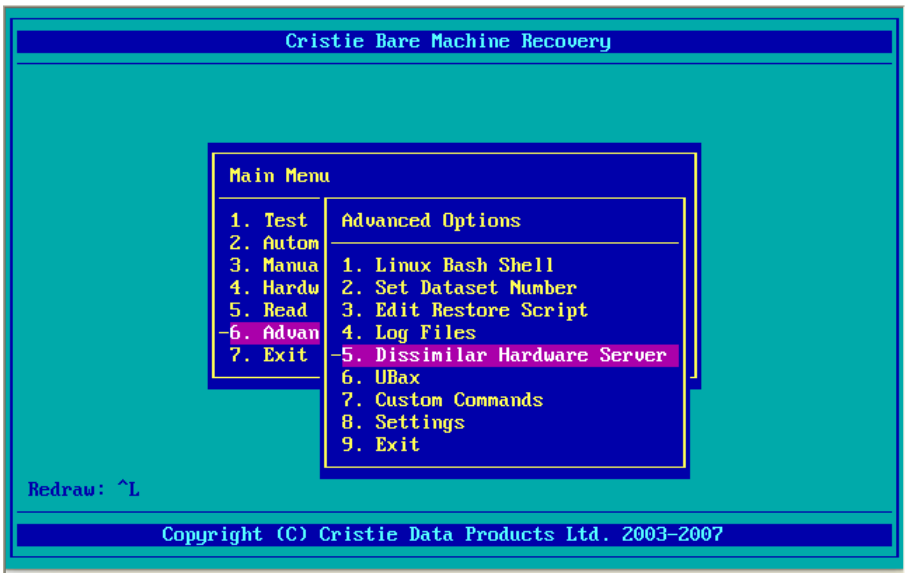


You can install as many drivers as you wish without rebooting either of the systems! Once the drivers are installed, you should exit from the CBMR Recovery Console of the just-recovering system and reboot. Now Windows will boot from the (possibly new) hard disks and the recovery will continue in Windows mode.

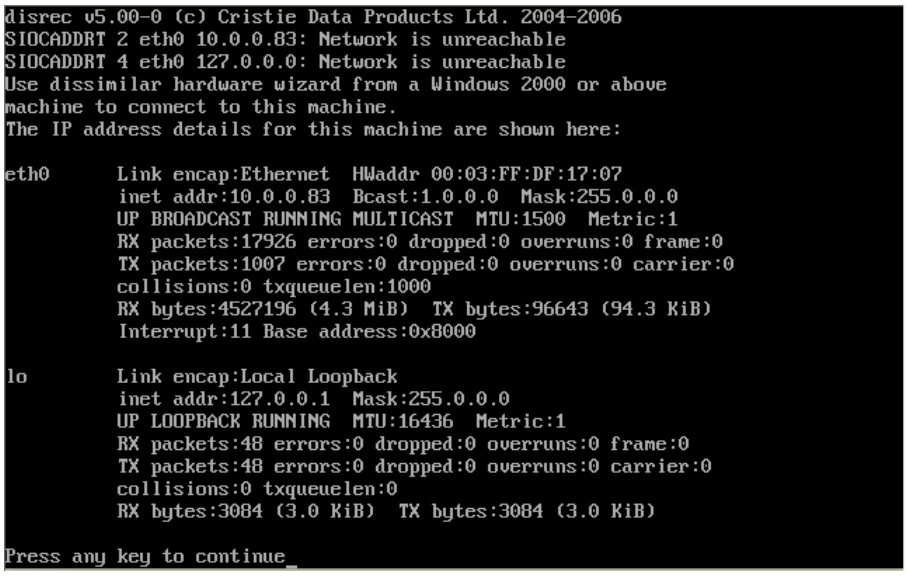
For some reason, if you get a system crash with a blue screen, check that you have installed the correct drivers. New drivers can be installed by booting from the CBMR CD-ROM, starting the Dissimilar Hardware Server and by running HWWizard from another Windows machine on the same network.

Starting dissimilar hardware server

Before running this wizard, you must have completed the Linux mode of recovery and started the Dissimilar Hardware Server from the Advanced Options of the CBMR recovery console from the just-recovering system.

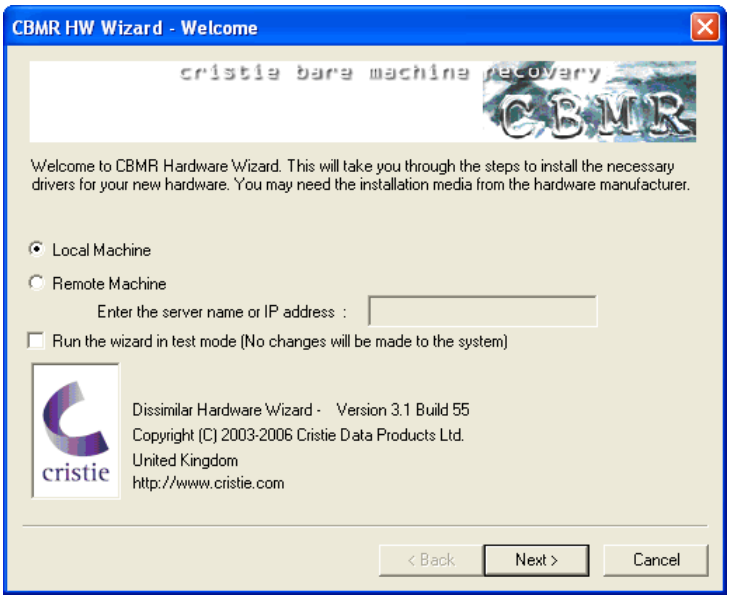


If the network is configured correctly, you will get the following screen listing the ethernet interfaces and their corresponding IP address assignments.



Connecting to the recovering machine

On invoking HWWizard.exe from a Windows machine, the Welcome screen will be displayed which is shown below:

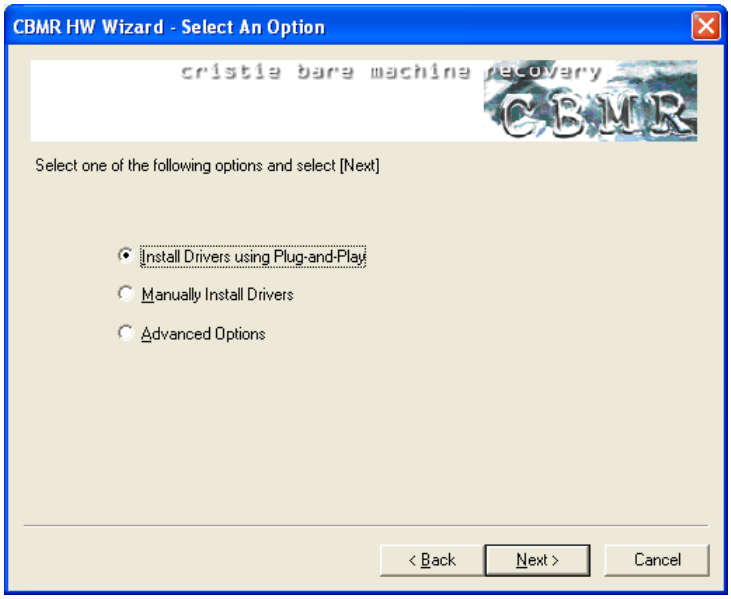


The welcome screen will accept the IP address or the NetBIOS name of the just-recovering system. On selecting **[Next]**, the wizard will connect to the just-recovering system and will show the Select An Option screen. If you get an Windows Authentication screen, enter the pre-defined user ID pcbax and password pcbax and select **[OK]**.

NOTE: It is possible to run this utility in *test* mode which will not connect to a server and hence no update will take place. In this mode, the driver installation script will be parsed and any errors will be reported. It will create a log file Wizard.log in the current folder. This will also create a file Driver.txt in *test* mode. Both these files should be sent to Cristie while asking for support.

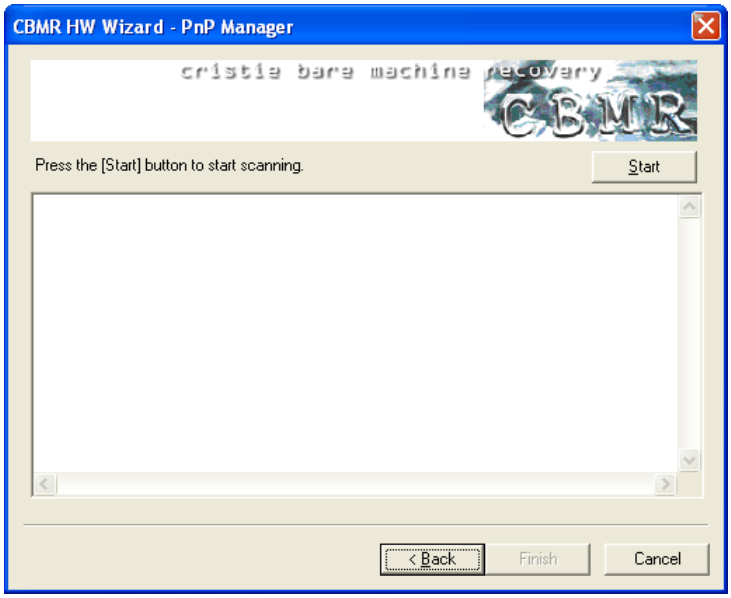
Automatic driver installation using plug-and-play

On successfully connecting to a just-recovering machine, the Select An Option screen will be displayed which is shown below.

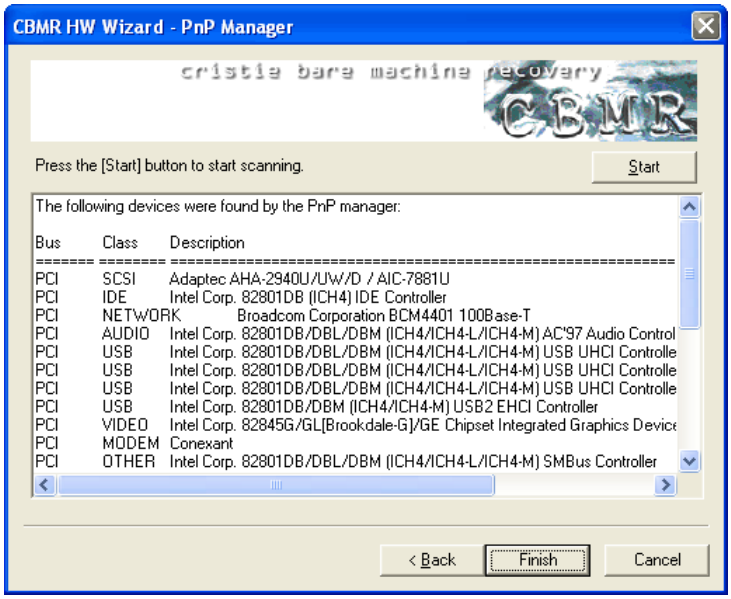


From the Select An Option screen, select the 

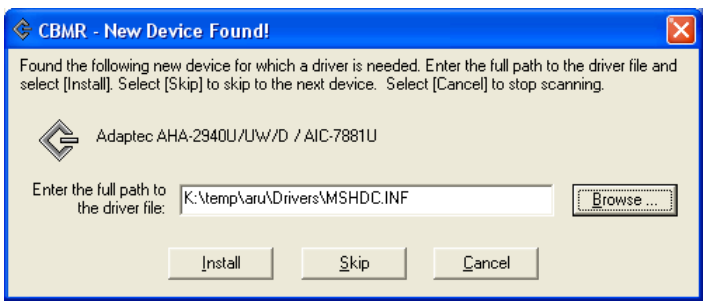
button followed by the **[Next]** button. The PnP Manager screen will be displayed which is shown below.



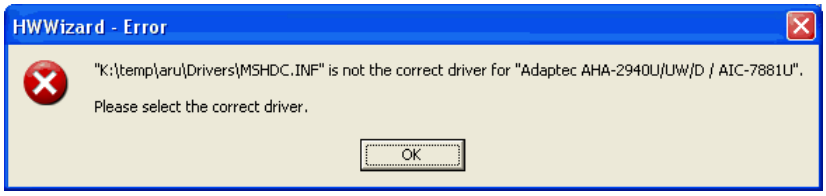
Select the **[Start]** button to start the PCI bus scanning. It will scan all the PCI buses for connected PCI devices. The devices will be listed in the screen. A sample screen is shown below.



During the PCI bus scanning, if HWWizard encounters a device for which there is no corresponding Windows driver, a New Device Found! dialog will be displayed. A sample screen is shown below.



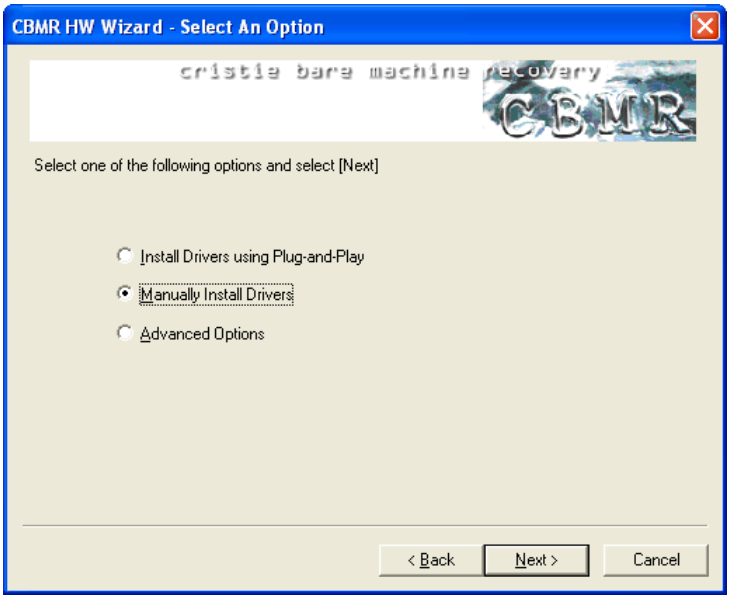
You must enter the correct .INF file including the path directly or by selecting the **[Browse]** button. On selecting the [Install] button, if there is a matching driver, it will be installed and a message will be added in the display area of the PnP Manager screen. An error message similar to the following will be displayed if an incorrect .INF file is specified.



Once the drivers are installed, select the **[Finish]** button to exit the wizard.

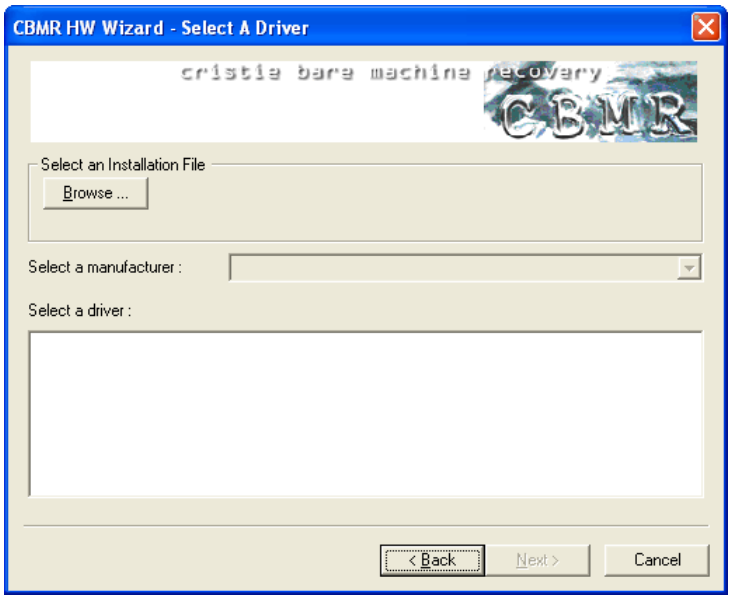
Manual driver installation

On successfully connecting to a just-recovering machine, the Select An Option screen will be displayed which is shown below.

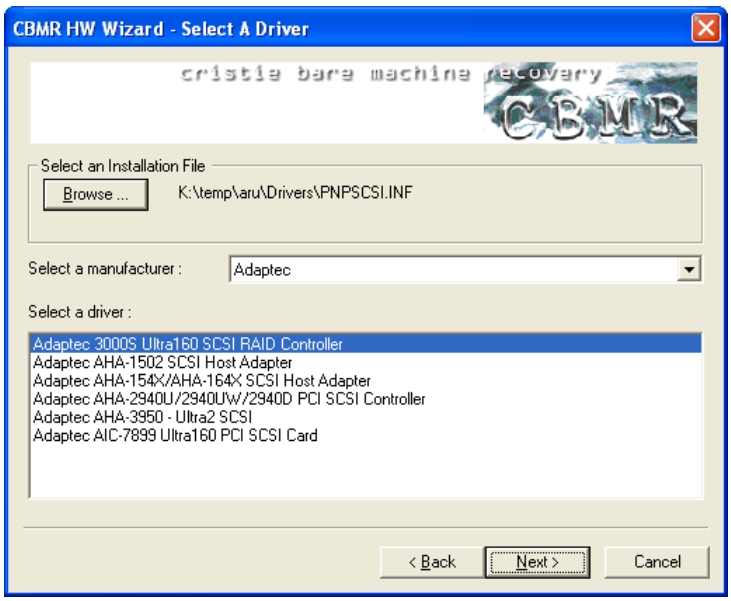


From the Select An Option screen, select the 

button followed by the **[Next]** button. The Select A Driver screen will be displayed which is shown below.

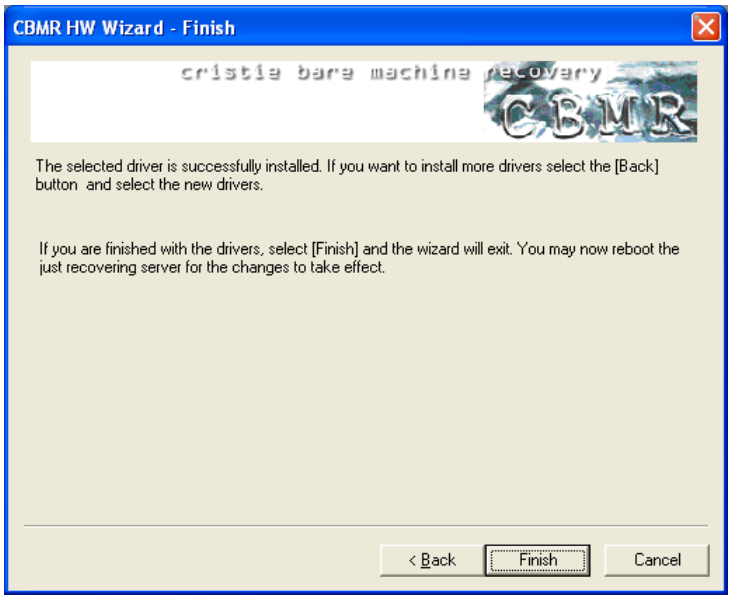


Select the **[Browse]** button and select the correct INF file for the SCSI/RAID/NIC controller you are installing. This will list the manufacturers and the drivers contained in the INF file. A screen shot showing Adaptec drivers is shown below.



Once you have highlighted the required driver, select **[Next]**. This will show a confirmation dialog. Selecting **[Yes]** from the confirmation dialog will copy the files across and make the necessary registry changes to the just-recovering system. If it can't find the necessary files on the installation location, it will prompt you for the files.

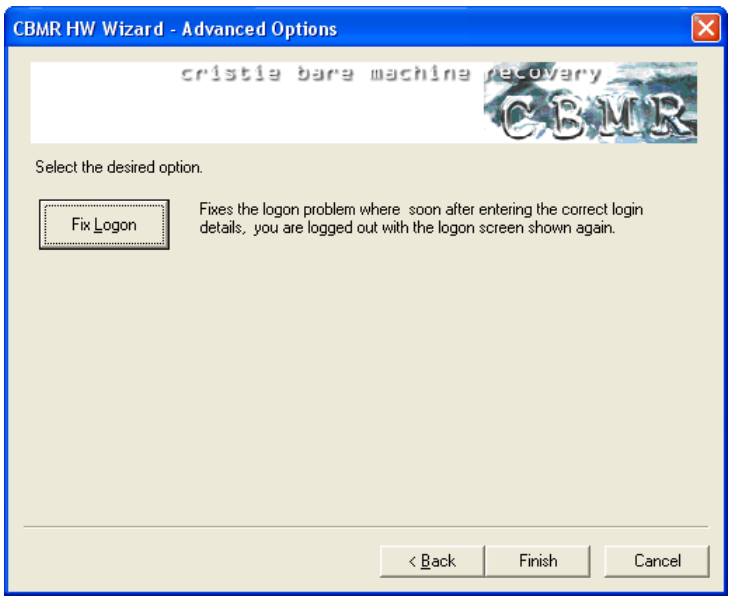
Upon successful installation, you will get the following Finished Screen. You can quit the wizard by pressing the **[Finish]** button. If you wish to install more drivers, you can select **[Back]** and install more drivers.



You can install as many drivers as you wish without rebooting either of the systems!

Advanced Options

Advanced Options let you do operations on the server other than installing drivers. On selecting this, the following screen will be presented.



Currently **[Fix Logon]** is the only option available. More options will be added later.

After the Linux mode restore, some times it may not be possible to login to the system. Either the system will log you out immediately after entering the correct credentials or you may get an error like the following if Citrix Presentation Server is installed.

In this case, **[Fix Logon]** will make necessary changes to the system registry so that you can logon to the system successfully. Upon successful completion, you will get the following message.

You should exit the wizard and restart the recovering machine. Now you should be able to logon normally using the local Administrator account and complete the restore process.

NOTE: It is important you must close the wizard by selecting the **[Finish]** button before rebooting the recovering machine. Otherwise, all your changes will be lost.

Rebooting after installing the drivers

Once the necessary drivers are installed, you should exit from the HWWizard and CBMR Recovery Console of the just-recovering system and reboot. Now Windows will boot from the (possibly new) hardware. The Windows mode recovery will continue.

For some reason, if you get a system crash with a '*Blue Screen Of Death*' (BSOD), check that you have installed the correct drivers for your SCSI/RAID controllers and repeat the steps as necessary to install the correct drivers. If there is a later version of driver available from the hardware vendor, try it first before seeking support.

6.3.6 Important point to note

Care must be taken **not to restore the Windows registry** from any previous backups until a new backup of the registry is made. Otherwise, the newly installed drivers will be lost and the system will crash on the next reboot. If this happens you will need to start the recovery all over again, doubling the recovery time.

6.3.7 Tested configurations

The following table contains a list of servers on which CBMR is tested. It doesn't mean that CBMR does not support other server configurations. We are continuously testing it on other popular server configurations and will update this section. In the mean time, if you tried it successfully on a configuration which is not listed here, please send an e-mail with the server details to cbmr@cristie.com (mailto:cbmr@cristie.com) so that we can include your server configuration in this list.

Source Server	Target Server	Operating System(s)

Compaq ProLiant DL360 G2 (Smart Array 2 RAID Controller)	DELL PowerEdge 2450 (Perc2 RAID controller)	Windows 2000 Server with Citrix Windows 2000 Advanced Server Windows Server 2003 Enterprise
Compaq PL3000 with 2 CPUs (Smart Array 3200 RAID Controller)	IBM X345 using integrated LSI controller	Windows 2000 Server
DELL PowerEdge 2450 (Perc2 RAID controller)	Compaq Proliant DL360 G2 (Smart Array 2 RAID Controller)	Windows 2000 Server with Citrix Windows 2000 Advanced Server Windows Server 2003 Enterprise Windows NT4
IBM Netfinity 5500	VMWare Server ESX 2.1	Windows 2000
Windows on IDE disk	Windows on SCSI Disk Symbios logic LSI120160	Windows 2000 Server Windows 2000 Advanced Server Windows Server 2003 Enterprise Windows XP
Windows on IDE disk	Windows on SCSI Disk Adaptec AHA-29160	Windows 2000 Server Windows 2000 Advanced Server Windows Server 2003 Enterprise Windows XP
Windows on IDE disk	VMware Server ESX 2.5	Windows 2000 Server
Windows on SCSI Disk Symbios logic LSI120160	Windows on SCSI Disk Adaptec AHA-29160	Windows 2000 Server Windows 2000 Advanced Server Windows Server 2003 Enterprise Windows XP

Windows on SCSI Disk Adaptec AHA-29160	Windows on SCSI Disk Symbios logic LSI120160	Windows 2000 Server Windows 2000 Advanced Server Windows Server 2003 Enterprise Windows XP
HP NetServer RAID 5	VMware GSX Server 2.5	Windows 2000 Advanced Server (PDC)
HP NetServer RAID 5	IBM Server x335 Fusion MPT	Windows 2000 Advanced Server (PDC)
VMware GSX Server 2.5	IBM Server x335 Fusion MPT	Windows 2000 Advanced Server (PDC)
Siemens Nixdorf Primargy 360	IBM X-Series 235	Windows NT4 (SP6a)
Siemens Nixdorf Primargy 460	IBM X-Series 235	Windows NT4 (SP6a) running MS Exchange 5.5 (SP4)

6.3.8 Current limitations

A Windows 2000 or newer machine running on the same network is required.

Recovering to systems with different CPUs and motherboards can not be done automatically. The necessary drivers should be installed from the Windows installation media using the manual driver installation feature of HWWizard.exe.

6.3.9 Future development

CBMR is in continuous development to incorporate newer features. Most of them are due to popular customer feedback.

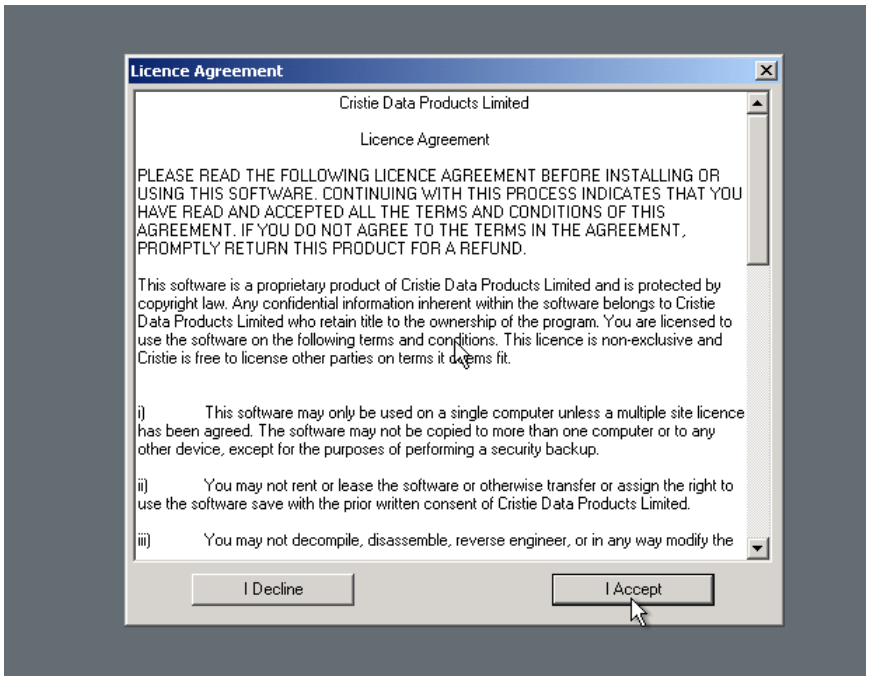
6.3.10 Conclusion

We at Cristie are committed to provide world class recovery software and support for Windows, Linux, HP-UX, and Solaris systems. We listen to our customers always and most of the features are customer driven. If you have any suggestion in any aspect of this product, please contact Cristie by e-mail (cbmr@cristie.com (mailto:cbmr@cristie.com)). We will value your suggestion.

6.4 WinPE Based Disaster Recovery Console

If the WinPE DR Console is selected, then a Windows installation-like boot procedure is started. Early on in this process you will be prompted to optionally inject new Mass Storage (disk) drivers if required (this will be useful during dissimilar recovery) by pressing F6. Ignore this option if no new drivers are required.

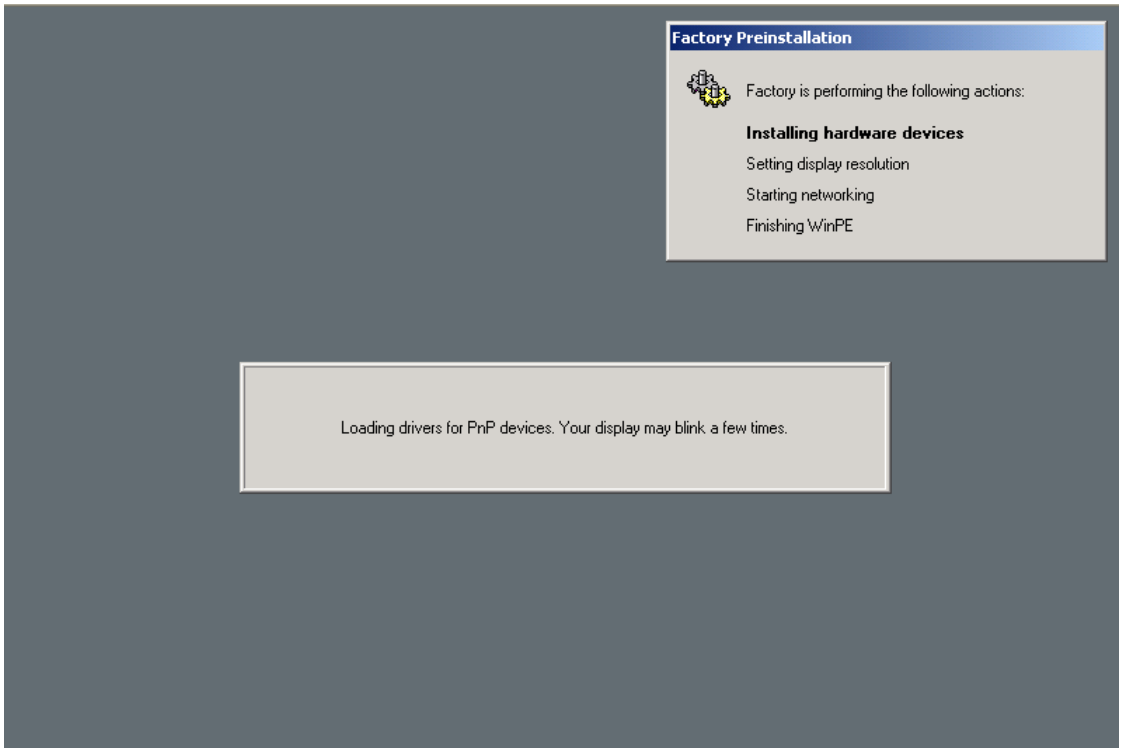
Upon successful boot the following licence Agreement will be displayed.



Press **I Accept** to continue. Selecting **I Decline** will reboot the system. You must agree to the Licence Terms and Conditions to perform a Disaster Recovery.

Note that the DR Console will automatically reboot 24 hours after starting. This is an operating feature of the Microsoft Windows PE environment.

The DR console will then run a **Plug and Play** sequence to determine the installed devices - in particular the Mass Storage devices and Network Adapters. At this point the screen may blink a few times whilst the Display Adapter is detected.



When this sequence completes the **CBMR Recovery Console** will be shown.

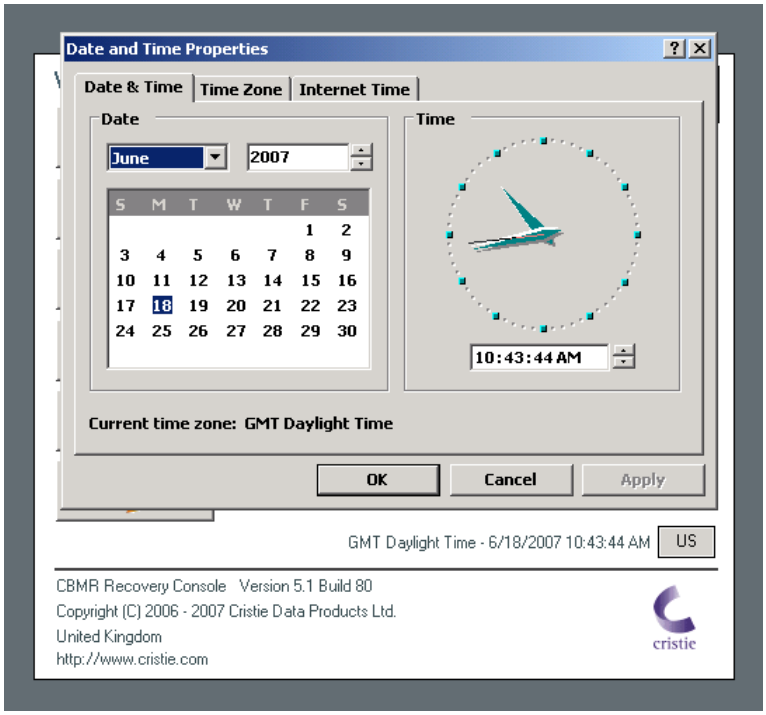
6.4.1 WinPE Based Disaster Recovery Console Main Menu

When you boot the WinPE DR environment, you will see the Recovery Console Main Menu as below.

You may configure the displayed date/time and the keyboard layout, by pressing the 

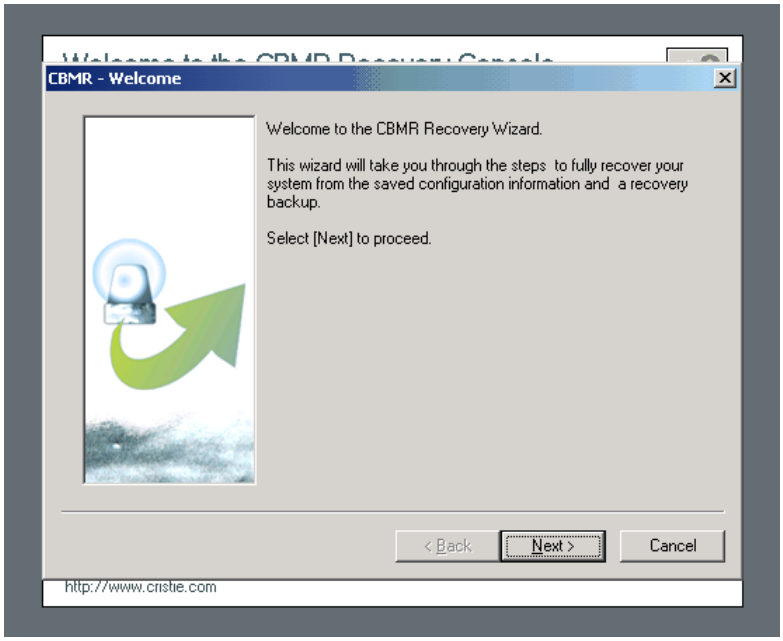
icon.

By default the standard display uses US layout, but this may be changed to one of the listed alternatives. Select Date, Time and Time Zone to configure the locale.



6.4.2 Start Automatic Recovery Wizard

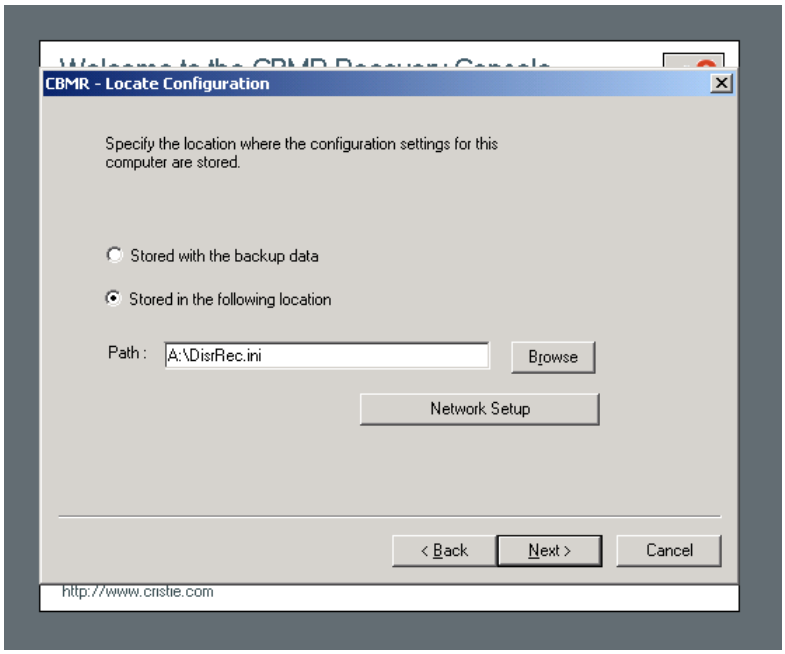
Select this option to commence a automatic DR sequence.



Press **Next>** to proceed to the first step of the sequence. Press **Cancel** to abort the recovery sequence at this point or **Help** to display context sensitive help.

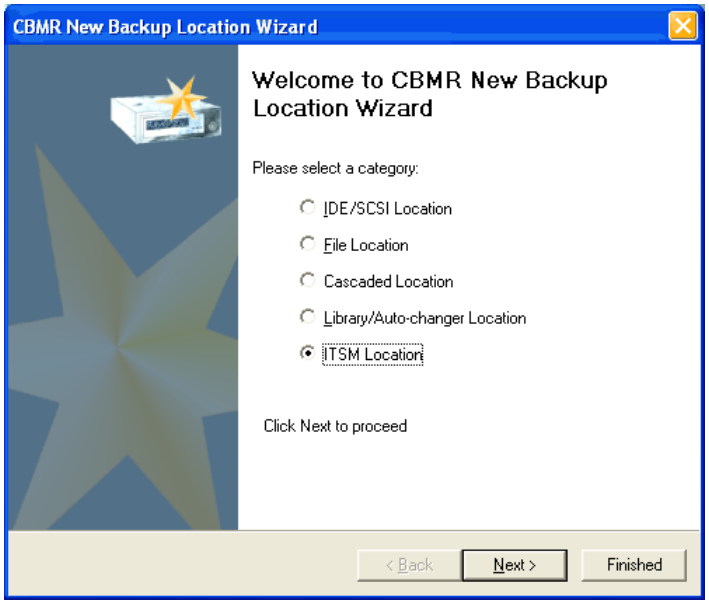
Locate Configuration

The first step of the recovery identifies the location of the System configuration details required for successful recovery.

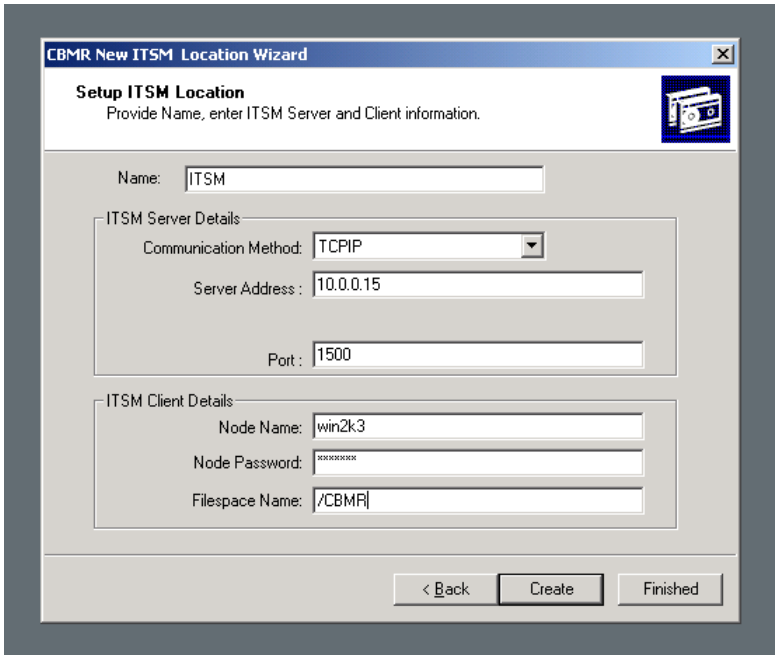


Stored with the backup data

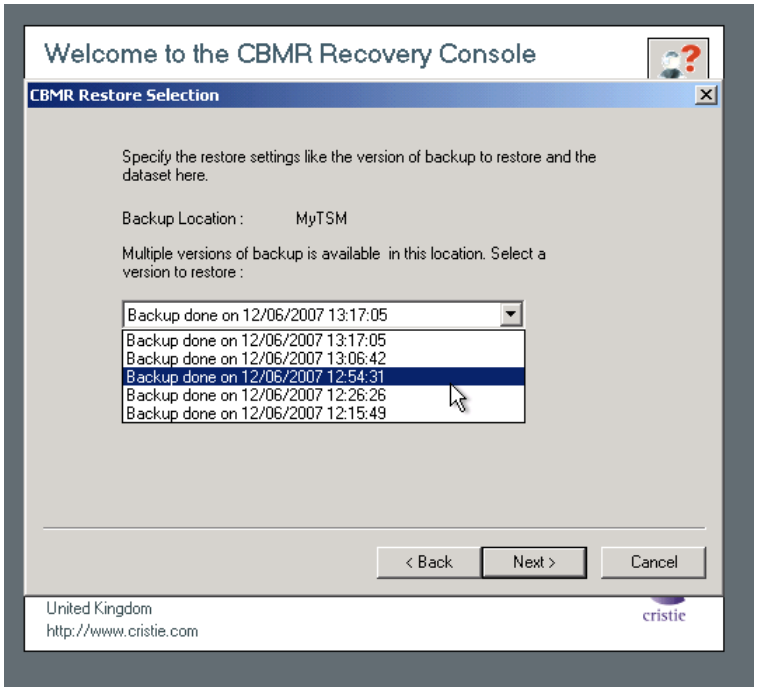
If the configuration settings were collocated with the DR backup itself, select this option. You will be required in the next step to identify the source of the backup by creating a temporary **Backup Location**.



Select **Next>** and setup the Location details. The example shows a temporary ITSM Location being defined. This will exist for the duration of the recovery.



Note that it is possible to change the temporary Location's details by selecting **Modify** on the menu. If the backup location resides on TSM it may be that there are several versions of the DR backup available.



Select the version appropriate to the recovery required. If the configuration is contained within the backup, it will be extracted from the selected version.

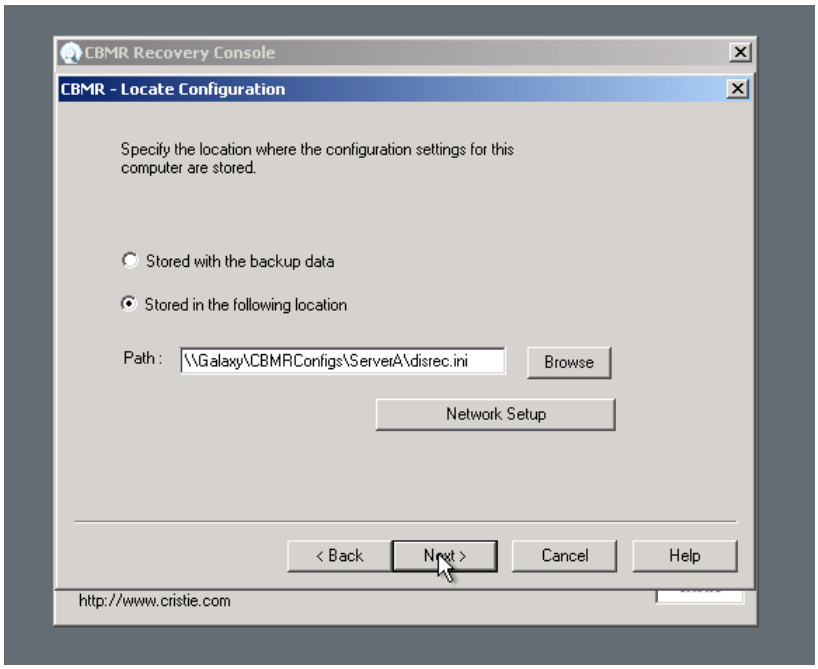
Stored in the following location

The example shown at the start of this topic will retrieve the configuration from the local floppy disk. A USB disk would be identified in the same way.

Note 1: USB devices must be connected to the system and powered (if required) BEFORE booting the Windows PE recovery environment. This is a restriction of Windows PE.

Note 2: The configuration filename disrec.ini must be appended to the path name.

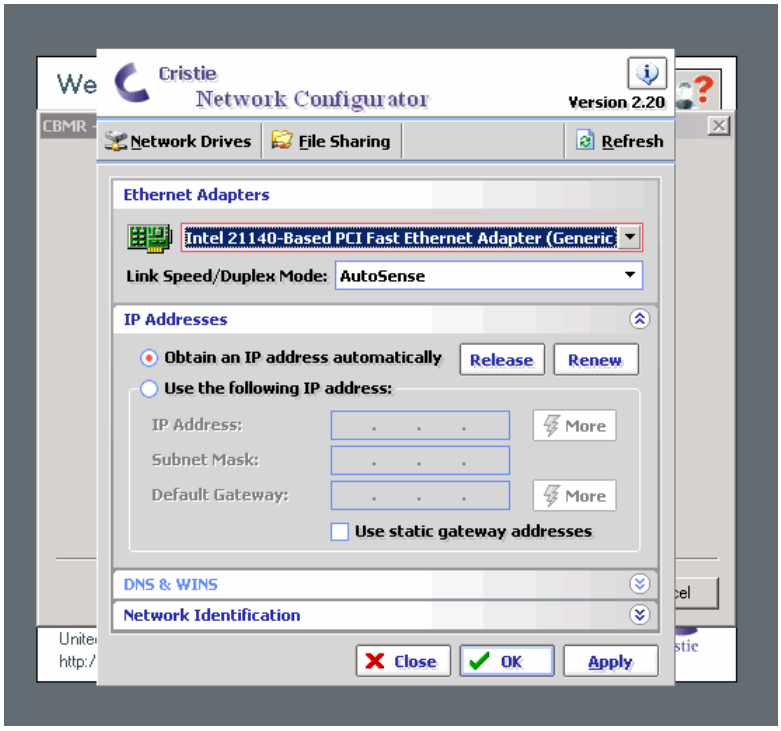
If the configuration is held on a network share use the following syntax in the **Path** field:



Network Setup

If the configuration is maintained on a remote network share then the network must be operational. Select this option to start the **Network Configurator** , http://www. tool. Configure the required network adapter from the drop down list and configure the IP settings accordingly.

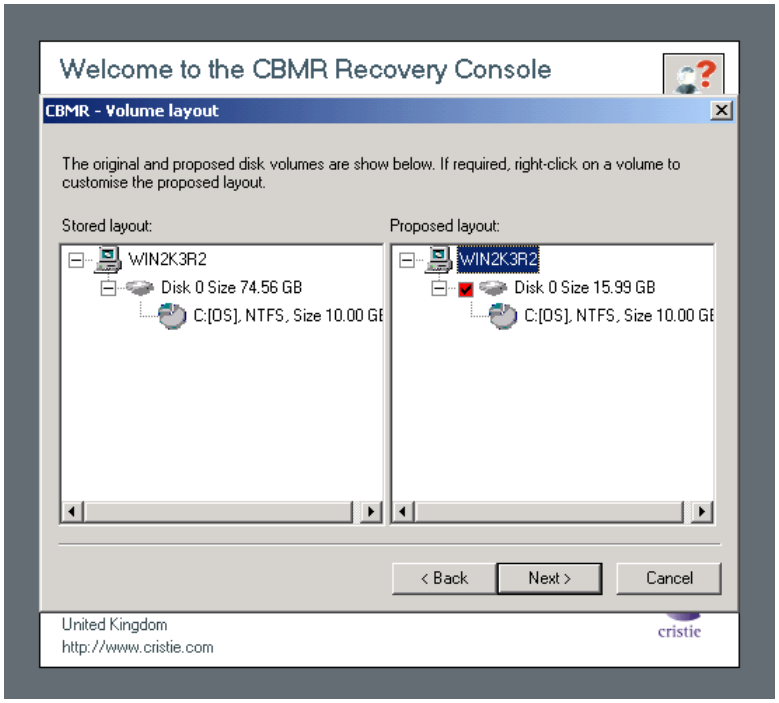
This saves having to navigate back to the DR Console Main Menu where the same function is provided.



Press **Close** to complete the Network Configurator dialog and then **Next>** to proceed with the next step in the recovery sequence.

Confirm Volume Layout

The next step in the automatic recovery shows a list of the disks and partitions to be recovered.



The left-hand panel of the display shows the original disk layout and partitions. The right-hand panel shows how the recovered disks will be partitioned after the recovery.

A red tick box next to a disk on the right-hand panel signifies that at least one partition on the disk will be re-formatted.

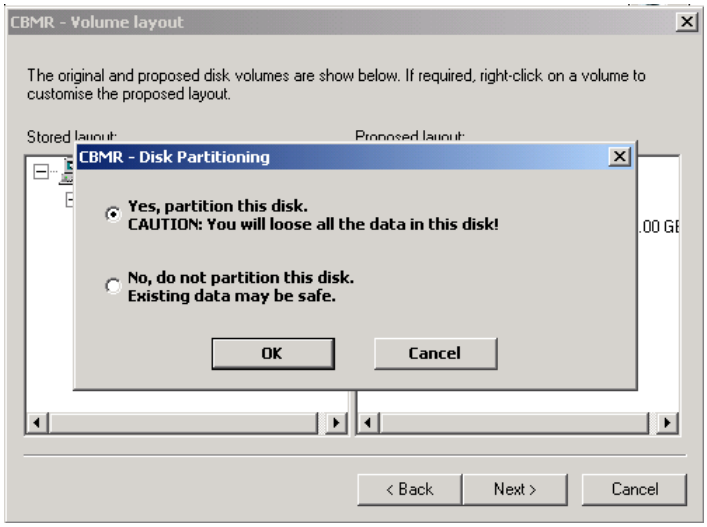
A green tick box signifies that the disk and its underlying partitions will be left intact.

When the recovery is to the original system the contents of both panels will look similar if the number of disks is the same. Possibly the disk sizes will be different (as in the above example).

When performing a recovery to a dissimilar system the disk mapping can be much more complex. Some of the criteria used to judge the disk mapping match are:

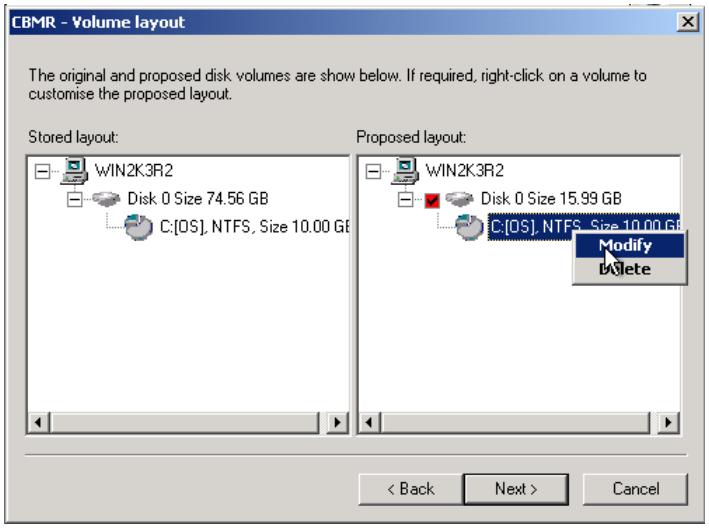
- disk geometry (tracks, cylinders and sectors)
- disk capacity
- if currently formatted, the disk signature

You may right-click on any disk shown in the right-hand panel to select whether the disk will be formatted or not.



Any attempt to turn off formatting incorrectly will result in this error.

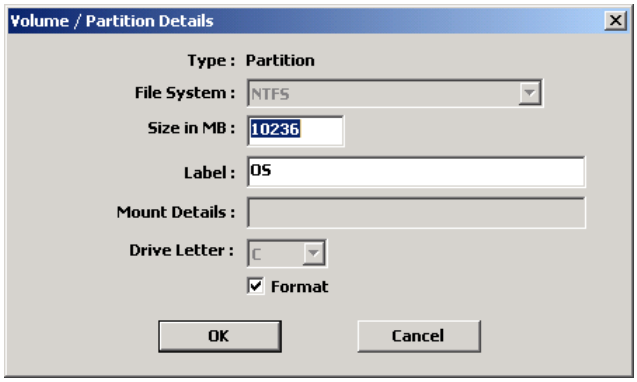
You may also right-click on a partition to allow you to selectively modify the partition parameters or to remove it altogether.



You may **Modify** the following partition parameters:

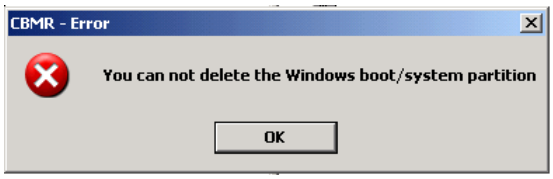
- size in MB
- label
- format (yes/no)

The screenshot below shows this.



Select **Delete** to remove the partition completely.

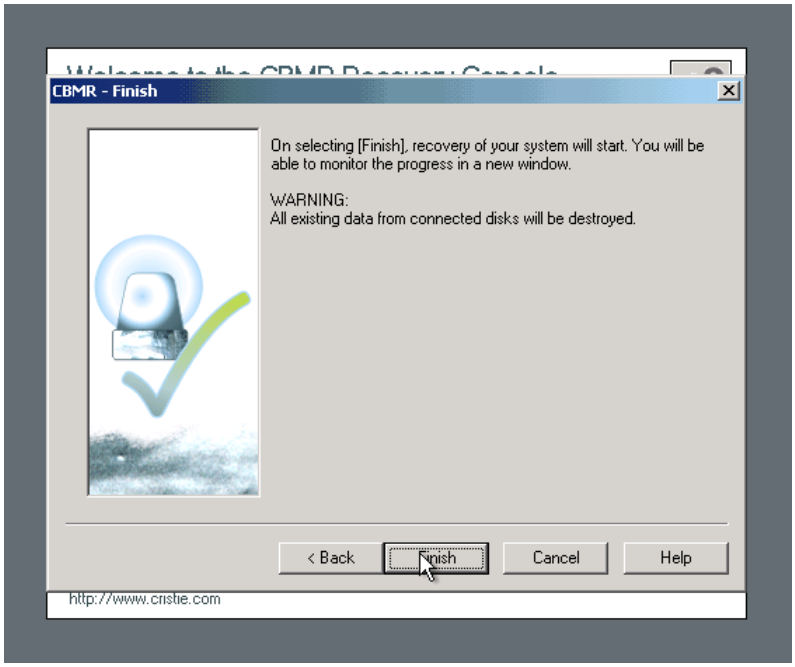
If you attempt to either not format or delete a Windows system partition, an error such as this will be displayed.



At this stage nothing has happened to the disks. Press **Next>** to continue with the recovery.

Proceed With The Recovery

Before continuing with the actual recovery a final warning screen is displayed.

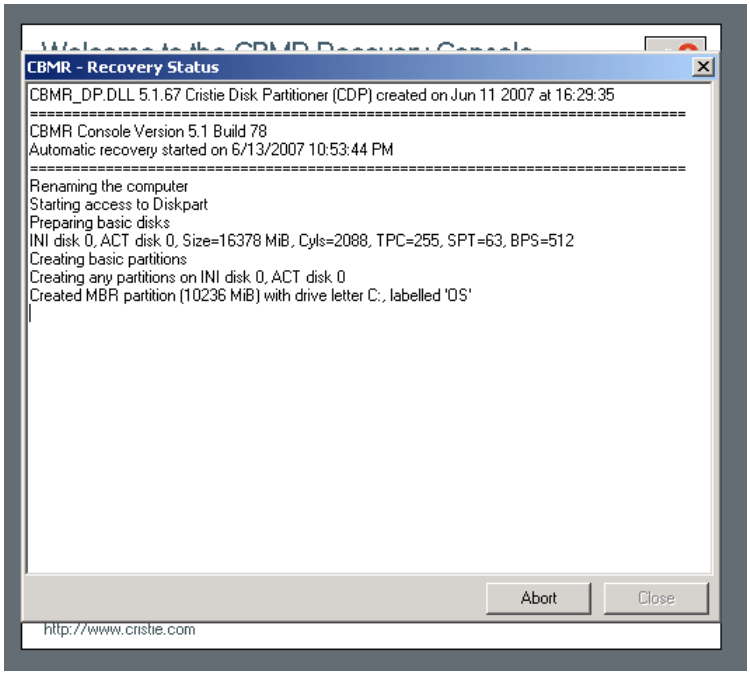


If you are happy with the recovery configuration, press **Finish**. This will commence the actual recovery.

Note: This procedure will completely destroy any existing data on the disks selected for recovery. Disks or partitions tagged as *no format* will however be retained.

Disk Recovery Sequence

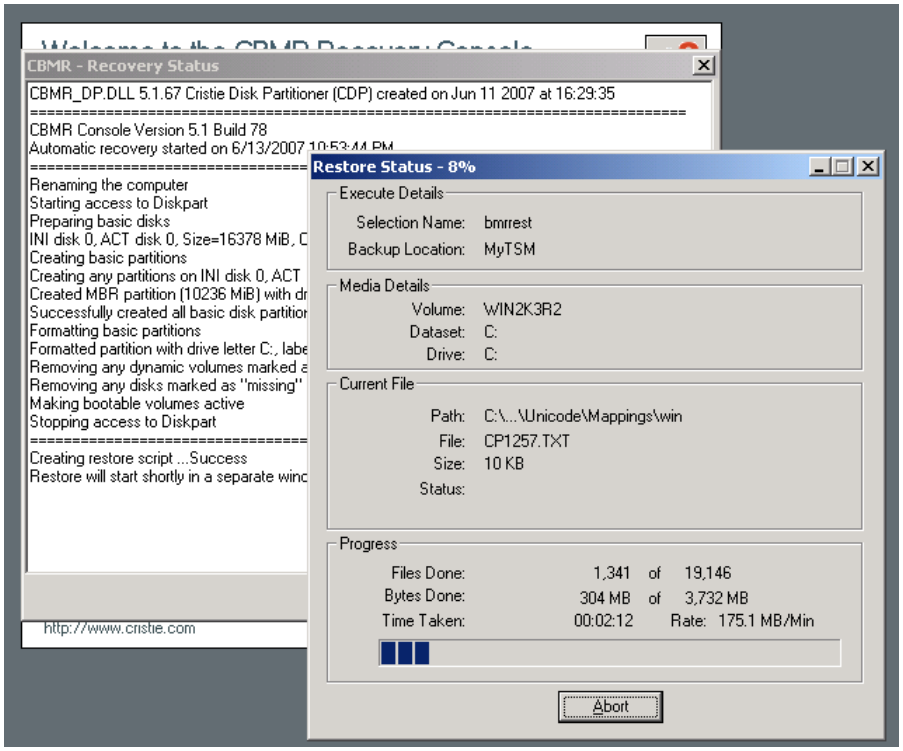
The recovery sequence begins by preparing the disk selected for the recovery.



This involves:

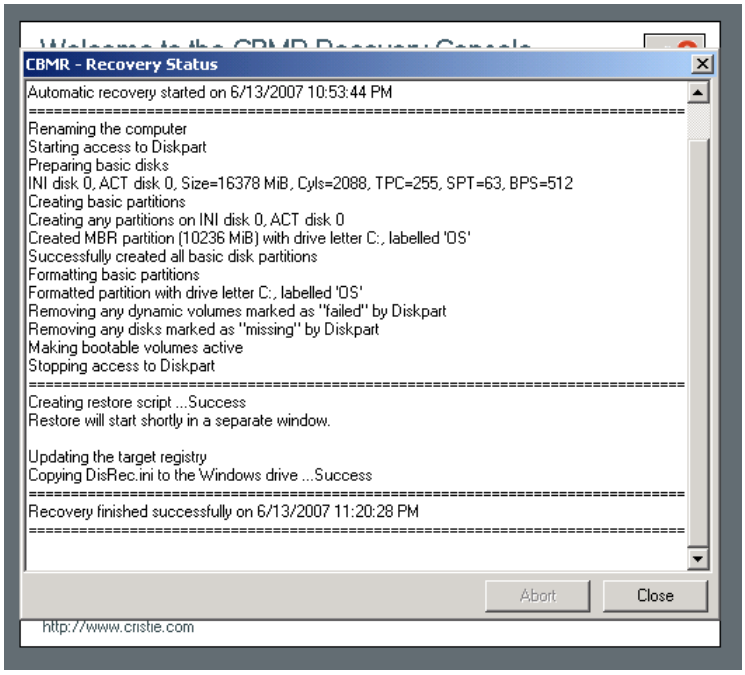
- disk mapping original layout to new
- cleaning (removing any existing disk partitions)
- removing any existing dynamic volume databases
- re-creating the partitions
- converting to dynamic volumes if required
- formating to the required partition type.

The next step is to recover the backups to the target disks/partitions. A new window appears containing the restore status of recovered files and a progress bar which indicates how much of the backup has been restored.. This display also shows the recovery statistics in terms of time, size and throughput.



This process may take some minutes if the backups are large. You may select the **Abort** button to terminate the file recovery process, but this may leave the disk or partition in an unpredictable state which may be unusable.

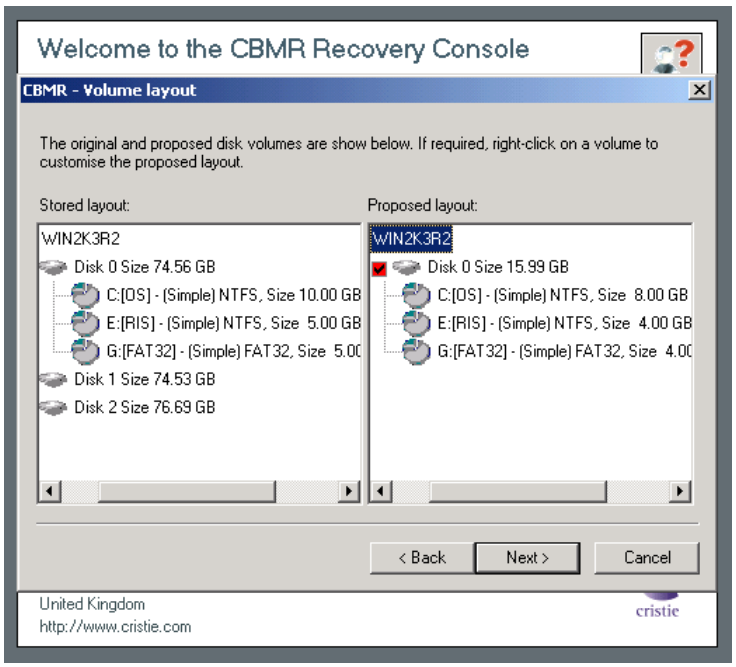
If any errors occur during the recovery, an error message will be shown in the window. Refer to the logs post recovery to establish the cause of any error.



Press **Close** to return to the Recovery Console main menu. At this point you may want to view the recovery logs and perhaps copy the logs to a local device or remote share before selecting to reboot.

Disk Scaling

In situations where the target system has fewer or smaller disks than the original system, disk scaling will come into effect. For example,



The above example shows a recovery from an original system with 3 physical disks to a target system with only 1 disk. The target disk is also much smaller than the original disks.

In this case CBMR will select as many disks to recover as possible (in this case only 1 disk - the boot disk). In addition it will scale the partitions down in proportion to their original size and occupancy. This can be complicated by having say mirrored dynamic volumes when the mirror will need to be broken - if only 1 disk exists on the target (or it has been tagged as not to modify).

Note 1: The Volume Layout dialog will only show disks in the left hand panel that can be recovered.

Note 2: During a recovery to a system with larger disks the partition sizes will remain the same as the original by default. However, in this case, it is possible to increase partition size during the recovery by right-clicking on the partition icon and selecting Modify.

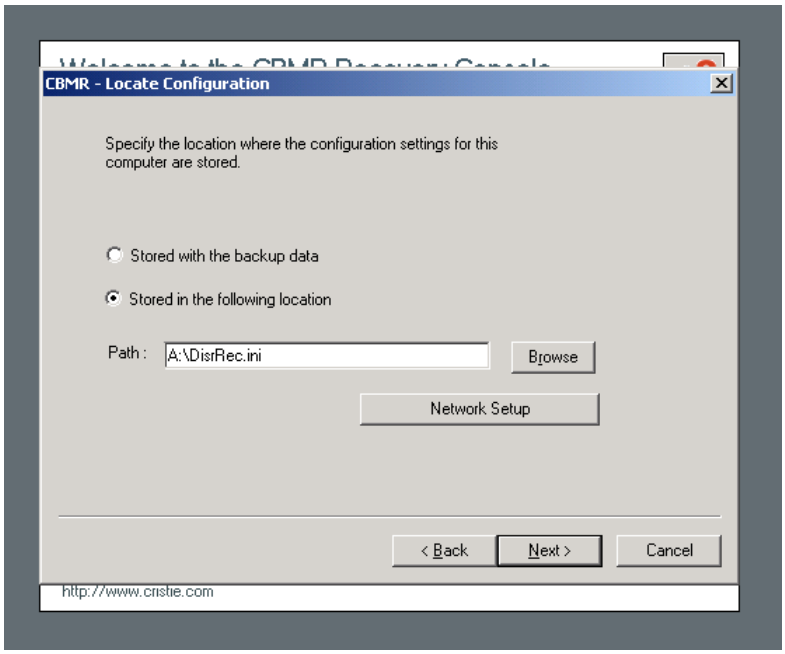
6.4.3 Start Manual Recovery Sequence

Select this option to commence a manual DR sequence. This option will stop after each step in the DR sequence allowing the DR to be aborted or the step to be repeated with different parameters.

Locate Configuration

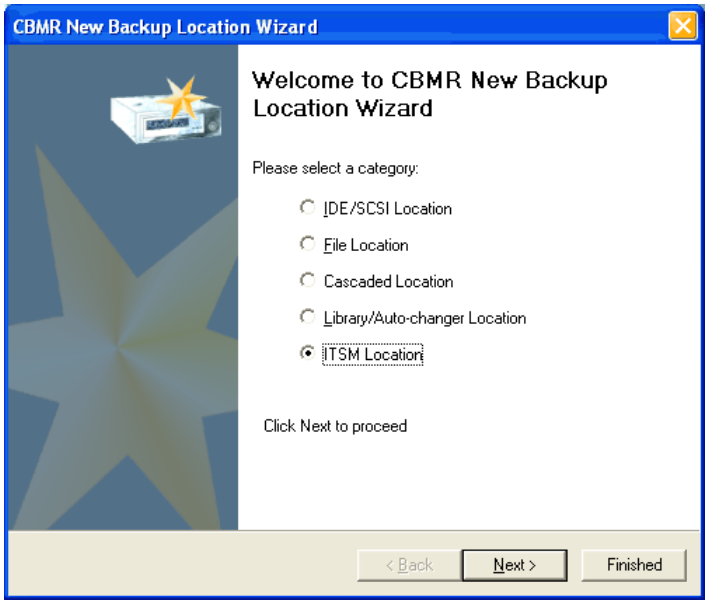
The first step of the manual DR sequence is to provide the location of the DR configuration.

Press **Next>** to continue to:

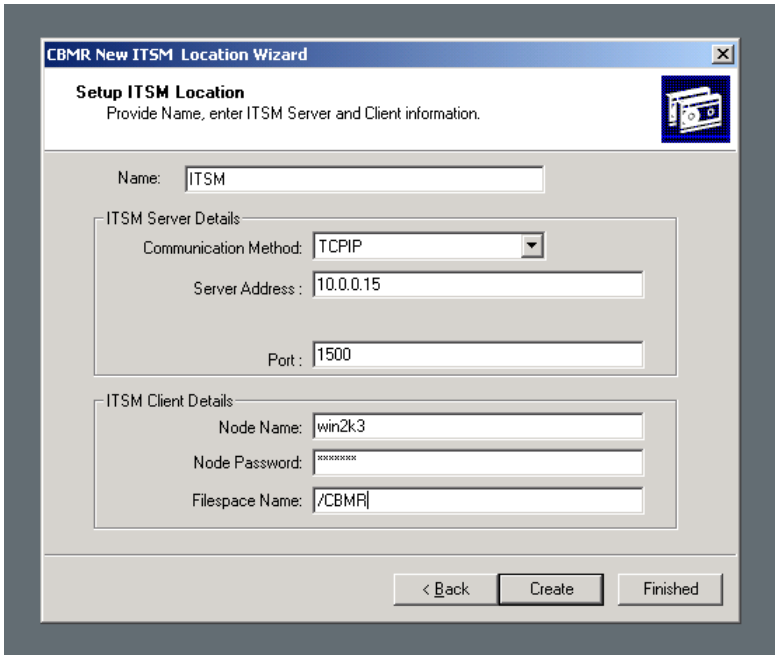


Stored with the backup data

If the configuration settings were collocated with the DR backup itself, select this option. You will be required in the next step to identify the source of the backup by creating a temporary **Backup Location**.



Select **Next>** and setup the Location details. The example shows a temporary ITSM Location being defined. This will exist for the duration of the recovery.



Note that it is possible to change the temporary Location's details by selecting **Modify** on the menu.

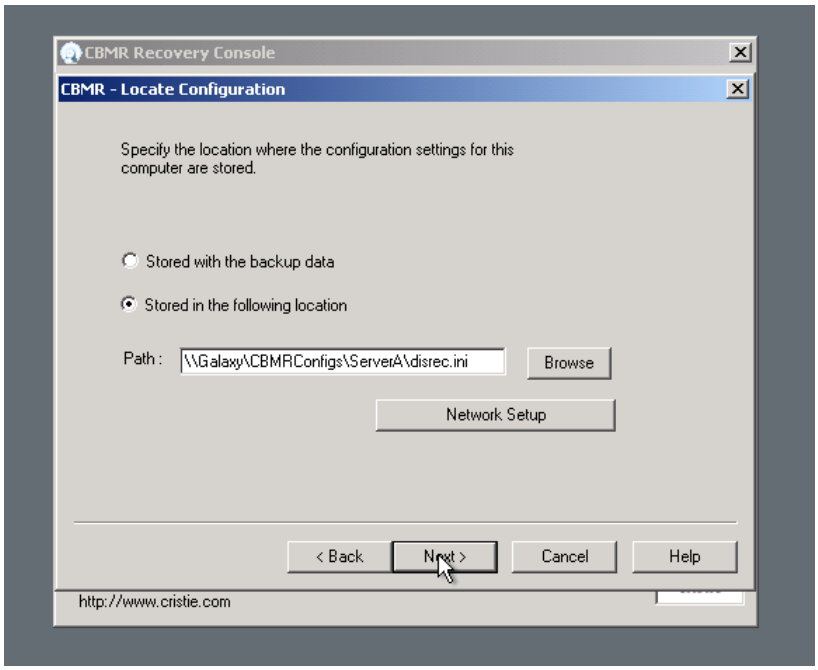
Stored in the following location

The example shown above will retrieve the configuration from the local floppy disk. A USB disk would be identified in the same way.

Note 1: USB devices must be connected to the system and powered (if required) BEFORE booting the Windows PE recovery environment. This is a restriction of Windows PE.

Note 2: The configuration filename disrec.ini must be appended to the path name.

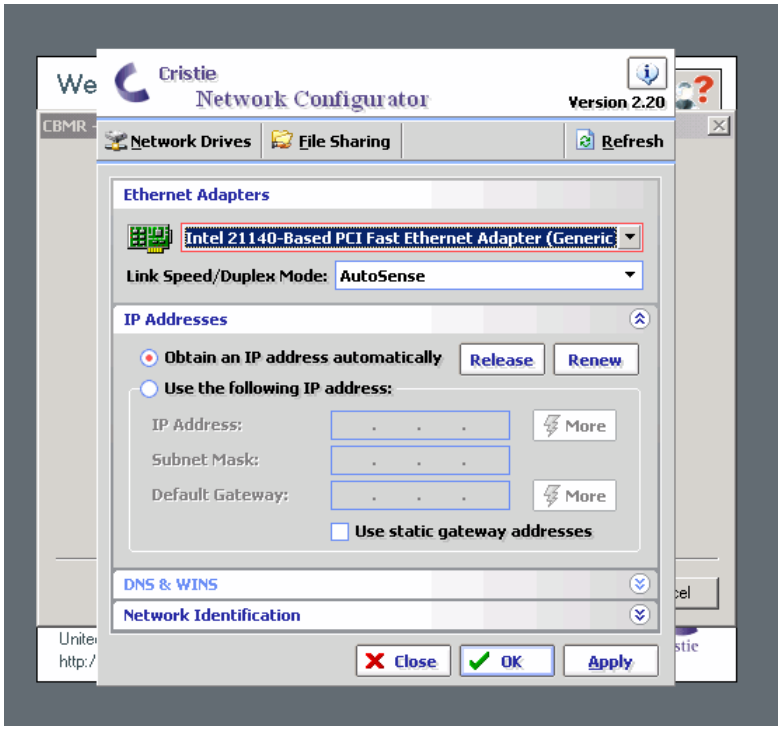
If the configuration is held on a network share use the following syntax in the Path field:



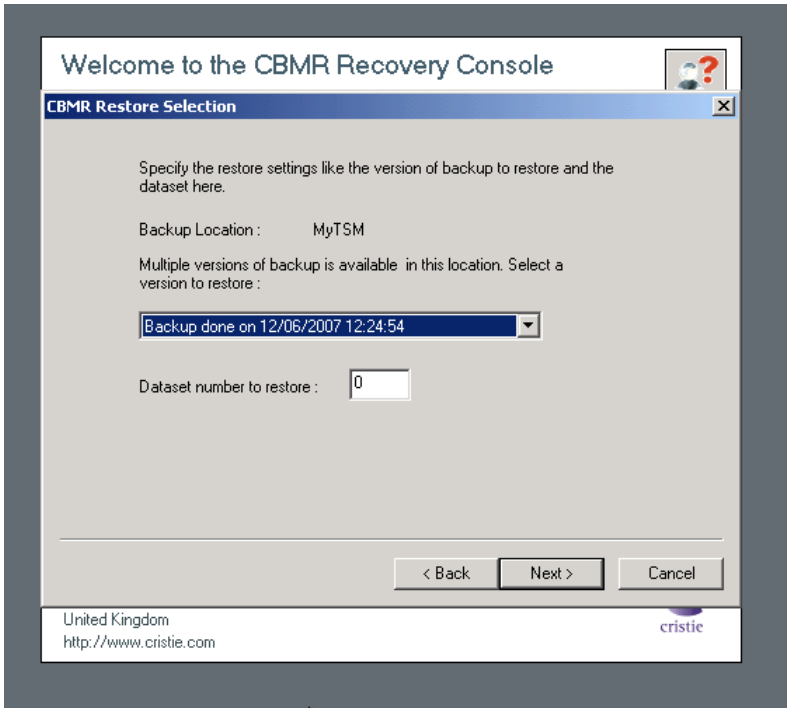
Network Setup

If the configuration is maintained on a remote network share then the network must be operational. Select this option to start the Network Configurator tool. Configure the required network adapter from the drop down list and configure the IP settings accordingly.

This saves having to navigate back to the DR Console Main Menu where the same function is provided.



Press **Close** to complete the Network Configurator dialog and then **Next>** to proceed with extracting the configuration from the selected location.

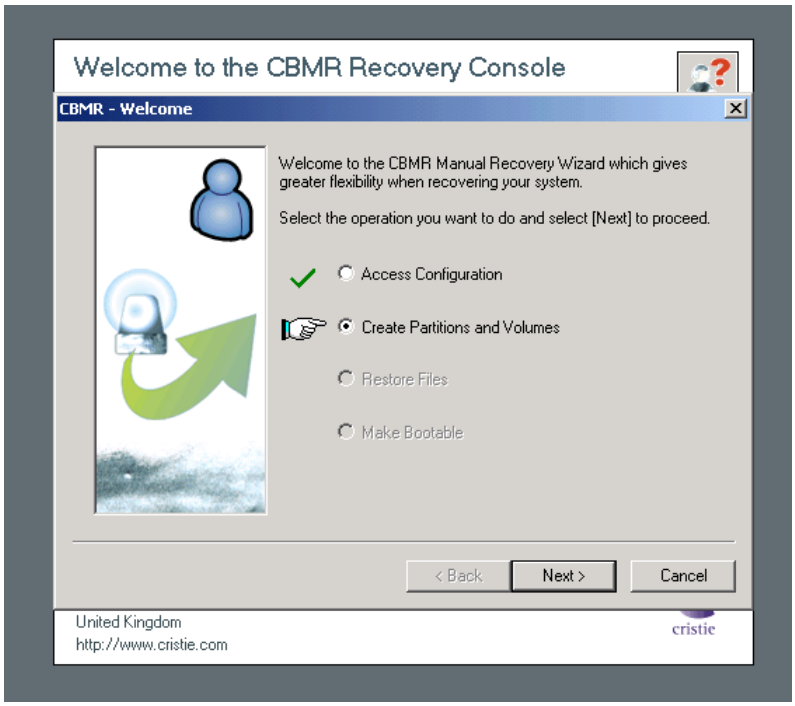


Successful extraction of the configuration is confirmed with the following dialog:

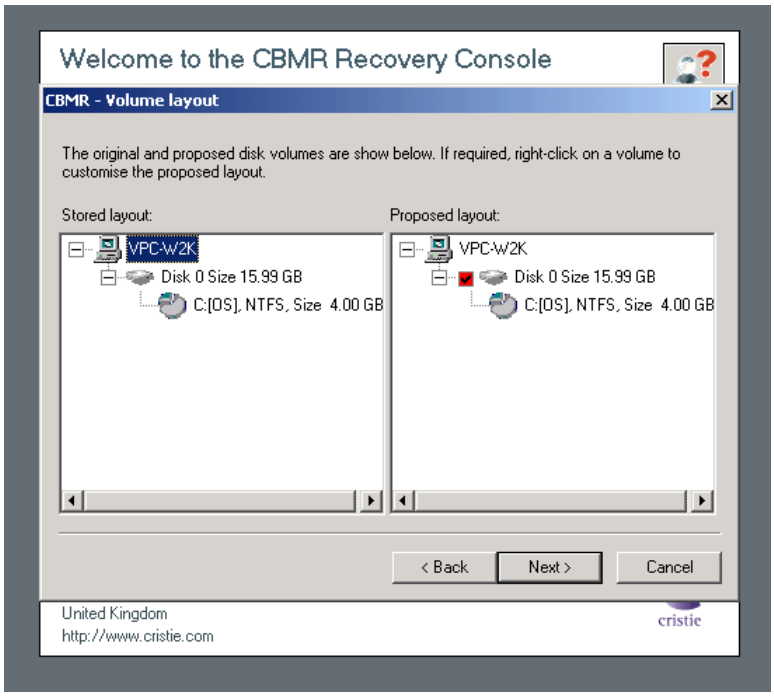
Select **Finish** and control returns to the next step in the Manual Recovery sequence.

Create Partition and Volumes

The next step of the manual recovery process is to configure the target disk partitions and volumes.



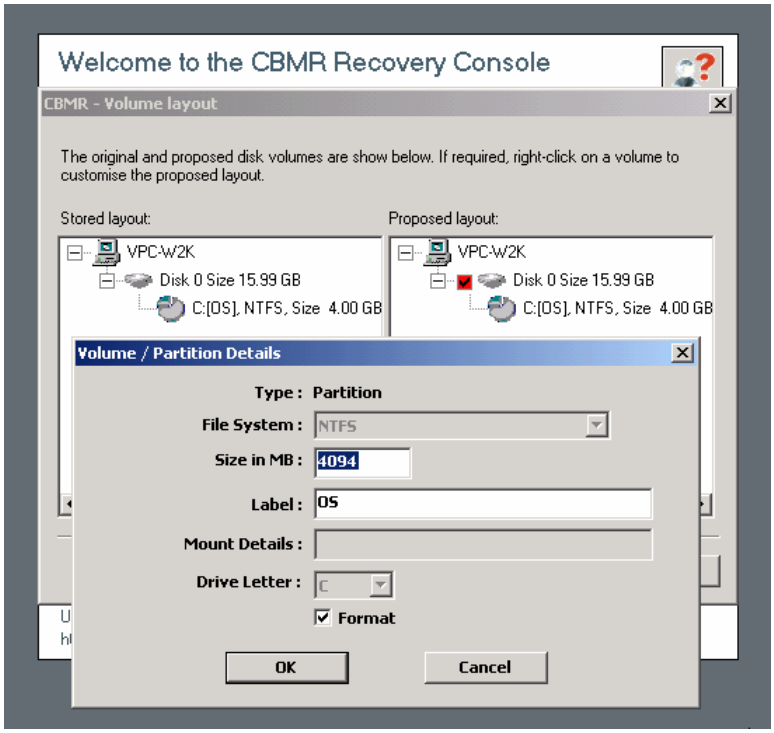
Select Next> to display the Volume Layout dialog.

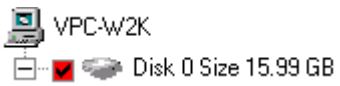


This screen shows the original disk layout against that of the target system. Naturally the target disk layout could be very different to the original. CBMR will attempt to match the disks using its own in-built criteria. Some of the criteria used to judge the match are:

- disk geometry (tracks, cylinders and sectors)
- disk capacity
- if currently formatted, the disk signature

However, it is possible to change the partition size or opt to tag/untag whether or not a partition should be formatted. To do this right click on the the disk icon and the following configuration dialog is displayed.





The indicator shown next to the disk icon indicates whether that disk will be left intact or not. A red tick indicates that the disk will be re-partitioned and/or formatted. A green tick indicates that the disk will be left intact.

Disks and partitions are discussed in more detail in the Automatic Recovery - Recovery Details section.

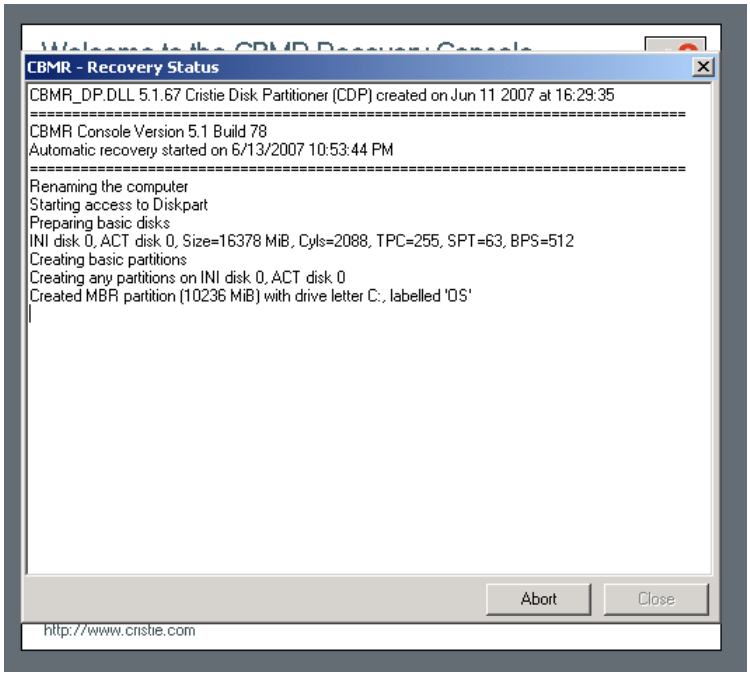
Press **<Back** to return to the previous step, **Next>** to commence the active part of this step or **Cancel** to abort.

Before continuing with the actual recovery a final warning screen is displayed.

If you are happy with the recovery configuration, press **Finish**. This will commence the actual recovery.

Note: This procedure will completely destroy any existing data on the disks selected for recovery. Disks or partitions tagged as *no format* will however be retained.

The Create Partitions and Volumes step begins by preparing the disk selected for the recovery.



This involves:

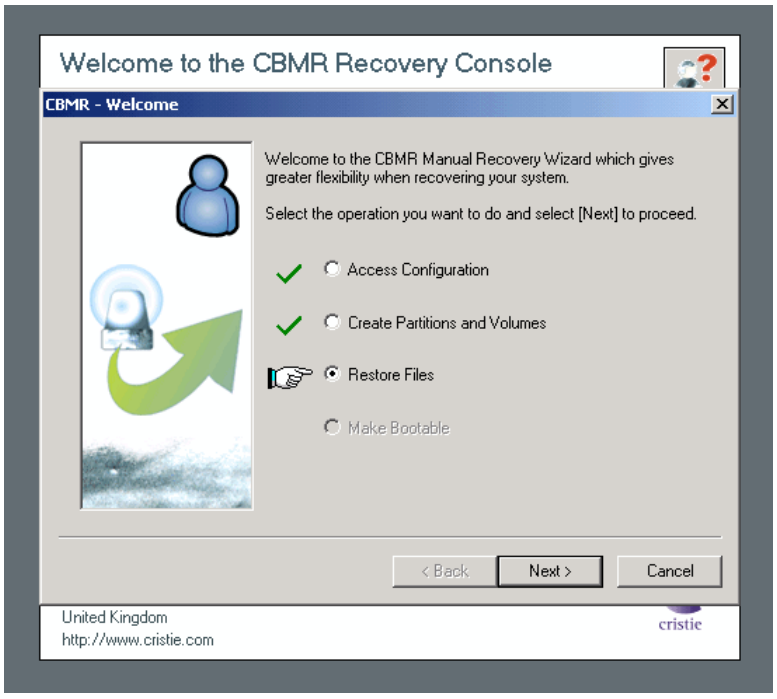
- disk mapping original layout to new
- cleaning (removing any existing disk partitions)
- removing any existing dynamic volume databases
- re-creating the partitions
- converting to dynamic volumes if required
- formating to the required partition type.

The next step is to recover the backups to the target disks/partitions. A new window appears containing the restore status of recovered files and a progress bar which indicates how much of the backup has been restored.. This display also shows the recovery statistics in terms of time, size and throughput.

Press **Next>** to continue with the recovery.

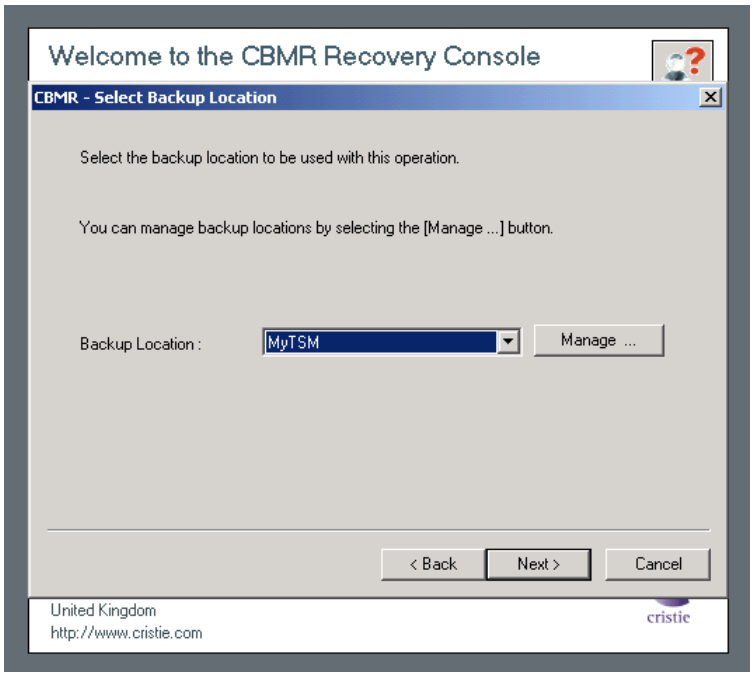
Restore Files

The next step of the manual recovery process is to restore the DR backup files.

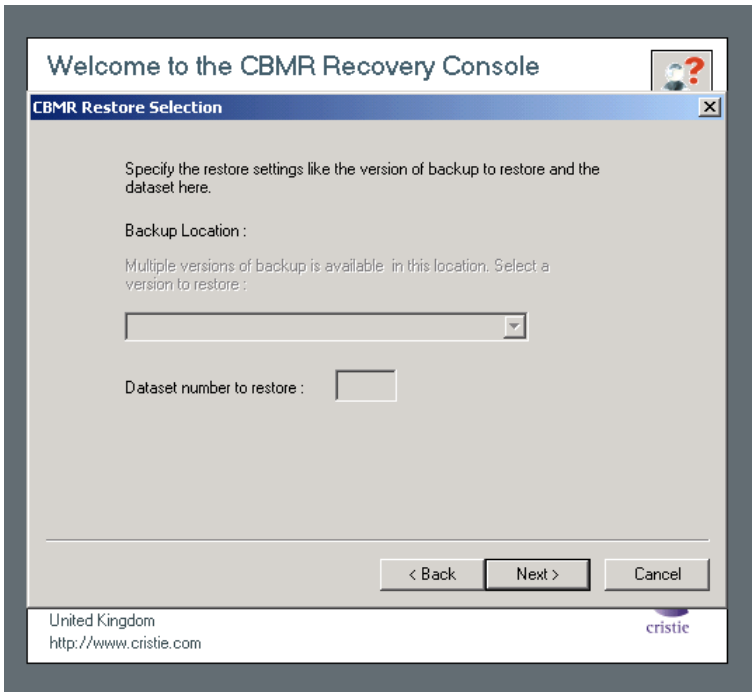


Press **Next>** to commence the restore of the backups to the target disks/partitions.

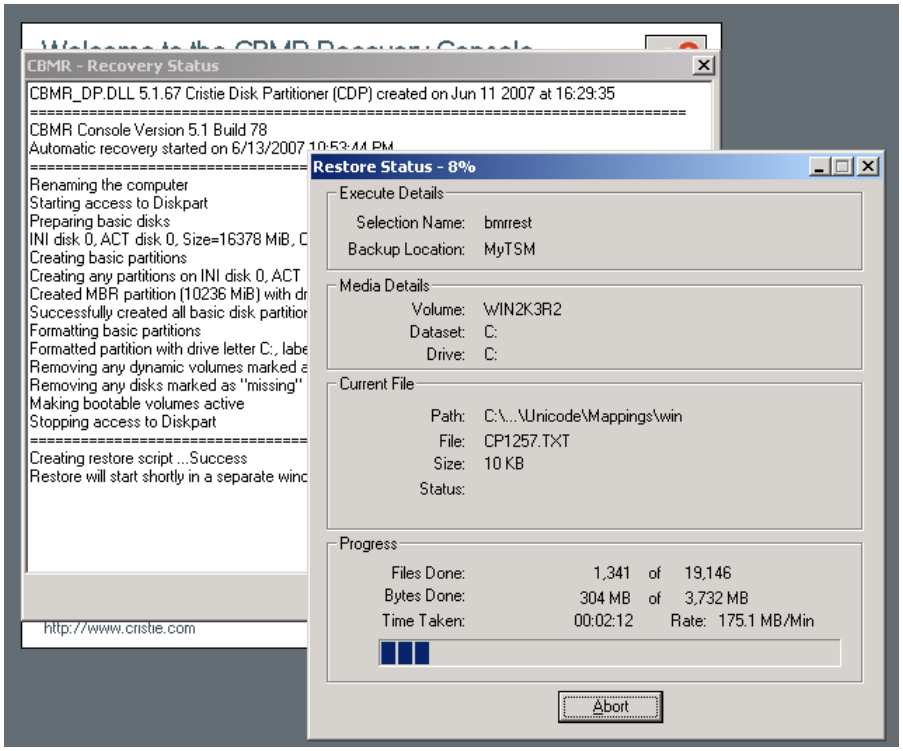
A new dialog window opens to allow the location of the backup itself to be selected.



Select the Location and press **Next>** to continue. You will then be prompted to select the backup version if the Location selected supports versioning (currently only TSM).



Finally, a new window appears containing the restore status of recovered files and a progress bar which indicates how much of the backup has been restored.. This display also shows the recovery statistics in terms of time, size and throughput.



This process may take some minutes if the backups are large. You may select the **Abort** button to terminate the file recovery process, but this may leave the disk or partition in an unpredictable state which may be unusable.

If any errors occur during the recovery, an error message will be shown in the window. Refer to the logs post recovery to establish the cause of any error. When the restore files step completes the following dialog is displayed.

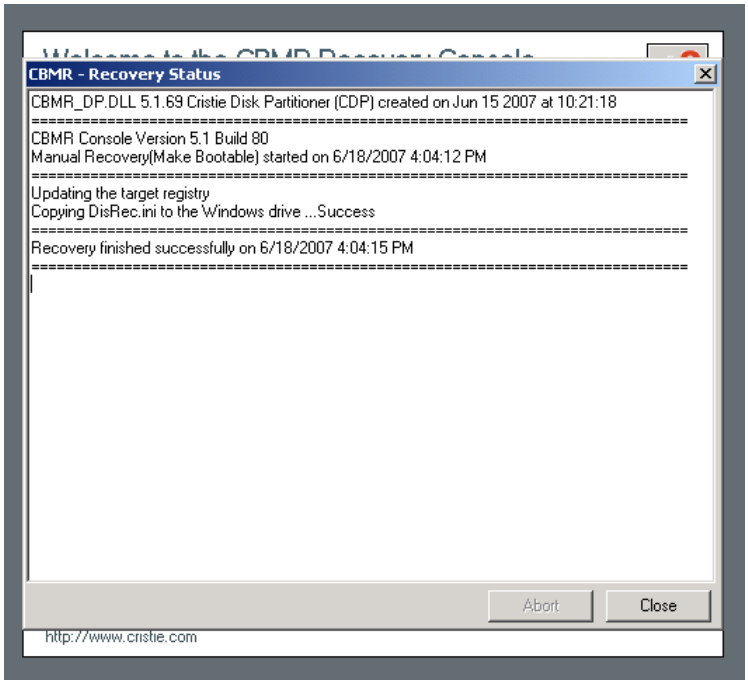
Select **Finish** and control returns to the next step in the Manual Recovery sequence.

Make Bootable

The final step in the manual recovery sequence is to make the original disk 'bootable'. This involves re-creating the MBR of the boot disk and modifying the registry with the new disk GUID.

Press **Next>** to commence the make bootable step..

A new dialog window opens summarising the success or failure of the operation..



Press **Close** to complete the step and return to the Manual Recovery Wizard.

6.4.4 Tools

There are a few tools that can assist with the recovery process. The are all collected under this command button.

The options available are

- Configure the network
- Dissimilar Hardware Wizard
- Setup Backup Locations

Selecting Configure the network will start the Cristie Network Configurator tool. This provides extensive facilities to configure network during the DR process.

The Dissimilar Hardware Wizard will allow drivers to be injected into the recovered system when the target hardware has different devices from the original (e.g. RAID controllers).

Setup Backup Locations will allow the creation of a pseudo device defining the location of the backup (and the configuration if it is collocated with the backup). This could for example be TSM, tape or a VTD.

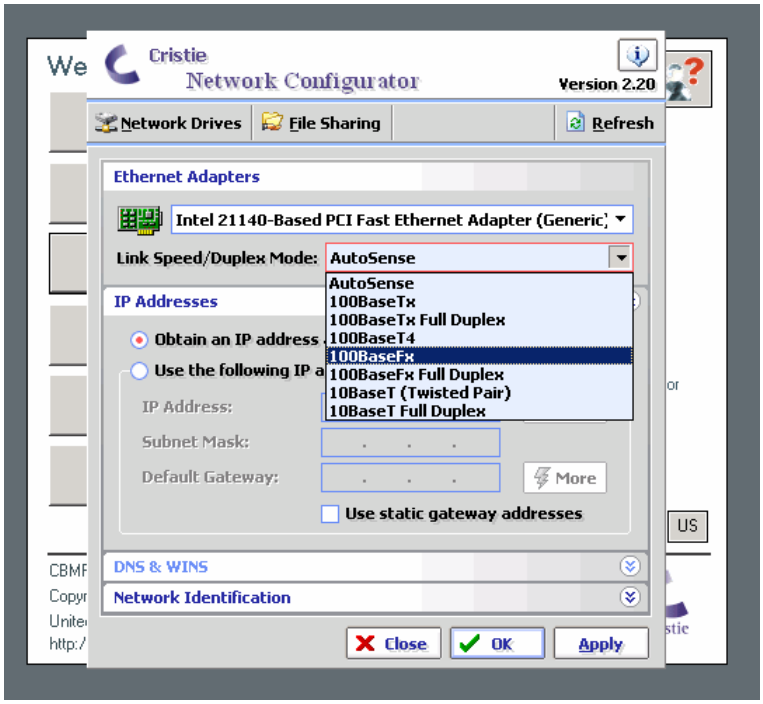
Cristie Network Configurator Tool

This is a very powerful tool that provides extensive facilities to configure the network during the recovery process. It offers the following features:

- supports multiple NICs
- configure individual NIC parameters for duplex mode and link speed
- the ability to select DHCP allocated or static IP addresses
- the ability to setup DNS and WINS server IP addresses
- the ability to setup the Network Identification of the recovering system.
- allow file shares to be set on the recovering system.
- map/unmap network drives.

Configure NIC Parameters

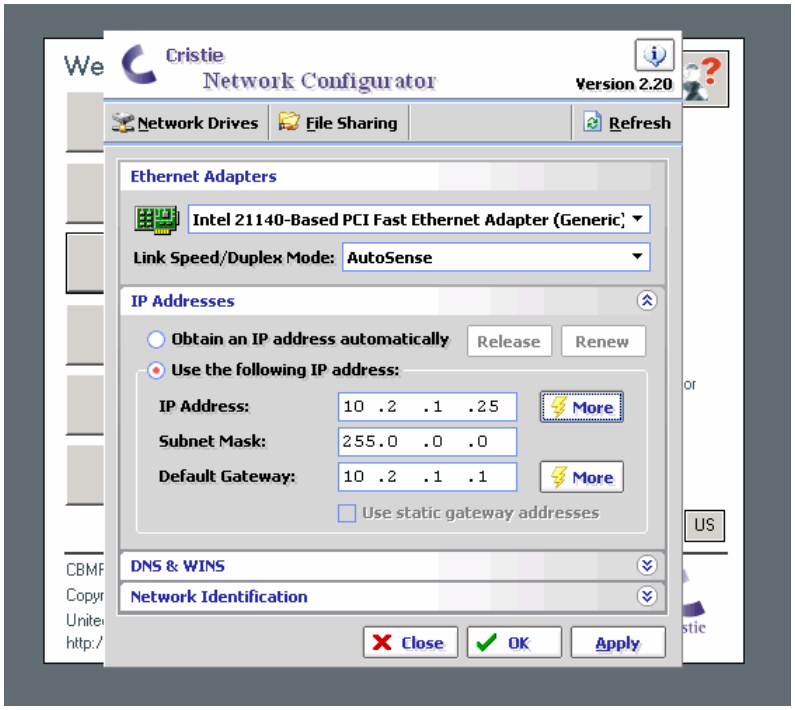
It is possible to change both the link speed and duplex mode for any NIC detected on the recovering target system. Simply choose the NIC from the drop down box and select the desired mode. *Autosense* is the default.



Assign Static or DHCP IP Settings

Normally the WinPE DR environment will start with DHCP enabled and active. However, if a static IP is required use the IP Addresses option to manually configure.

First choose the network adapter from the drop down list.

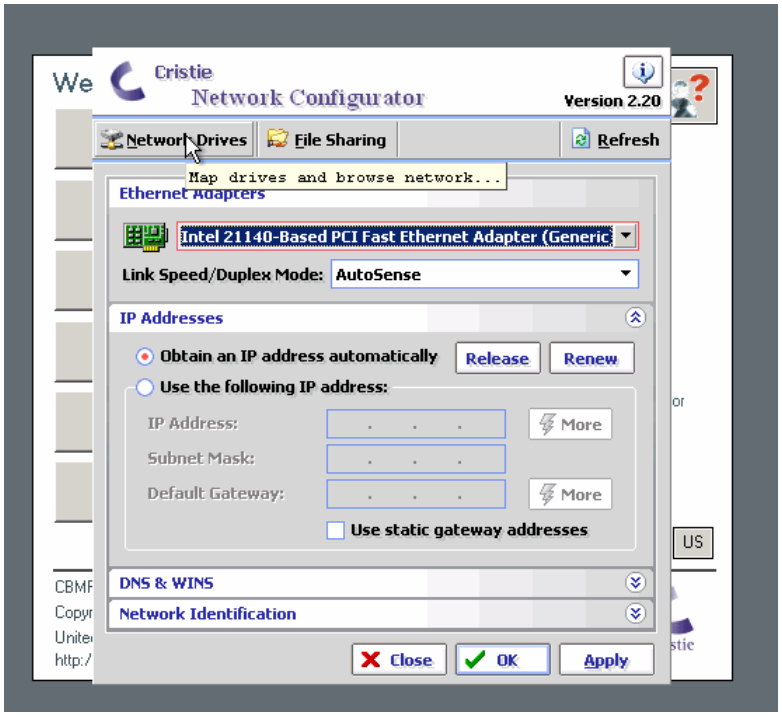


Select the Static radio button and set the IP address, subnet mask and gateway IP address. Click on **Apply** to confirm the settings for the selected adapter.

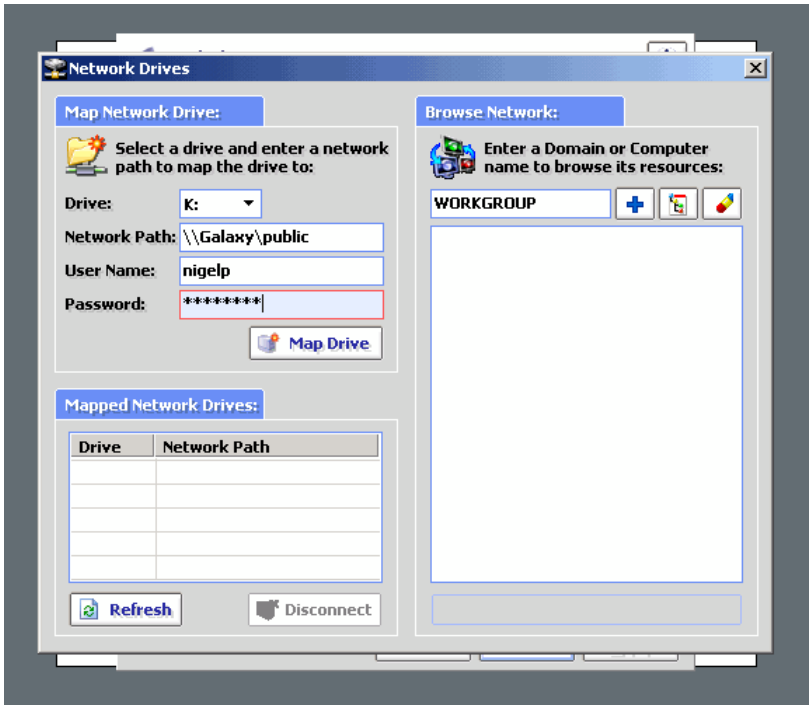
This feature will also allow the DHCP lease to be released or renewed, as required.

Map a Network Drive

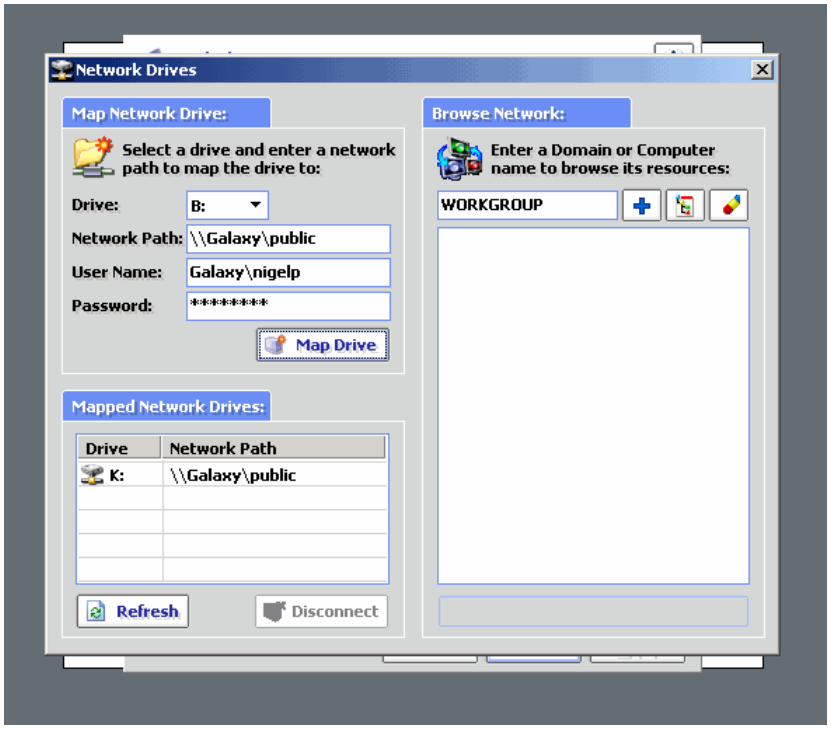
In order to simplify access to network resources, the Network Configurator allows you to map a network drive to a network share.



Start the Network Configurator from the Tools menu and select the **Network Drives** button.



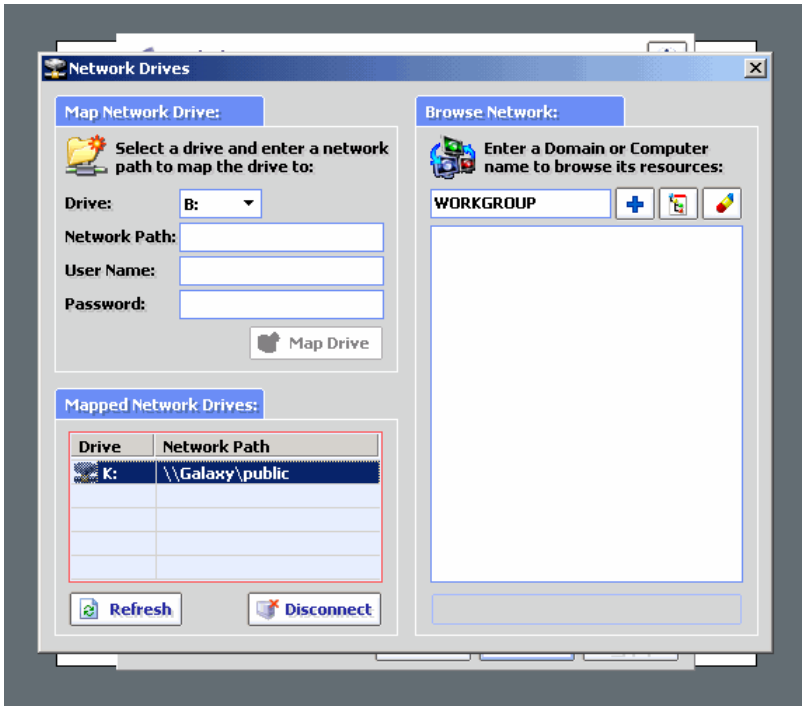
Select the drive letter that you wish to allocate from the **Drive** drop-down box and type in the share name that you wish to associate with it. Also specify the network credentials to be used to access the share. Press **Map Drive** to confirm the share operation. If successful the share will be added to the Mapped Network Drives table (see below).



Press the  icon on the top right of the dialog window to return to the Network Configurator main menu.

Disconnect Network Drives

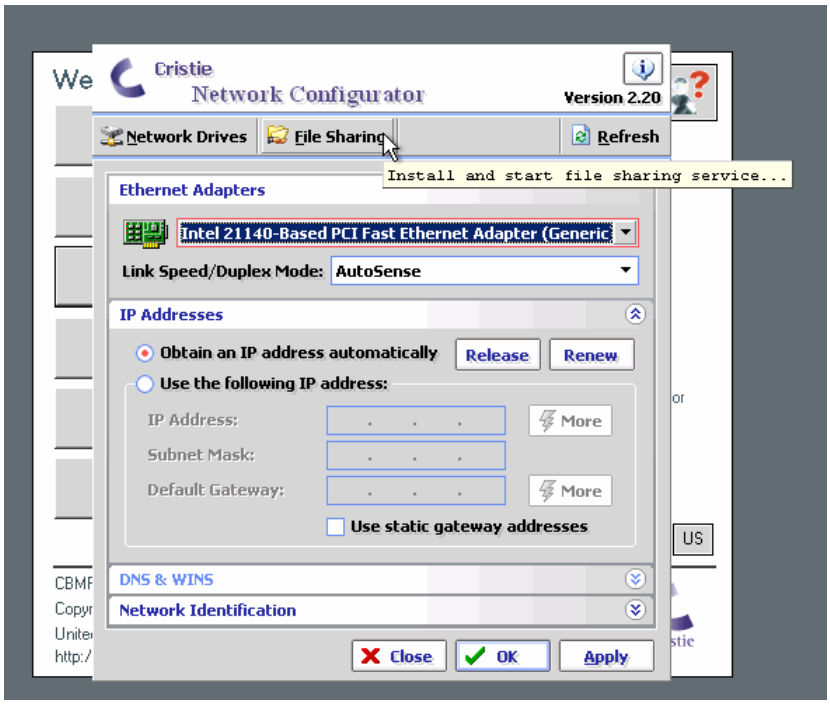
If you need to disconnect a mapped drive for any reason, this option allows you to do this.



Just highlight the drive that you wish to disconnect from the **Mapped Network Drives** list and then click **Disconnect**. The mapped drive is removed from the list to confirm the operation.

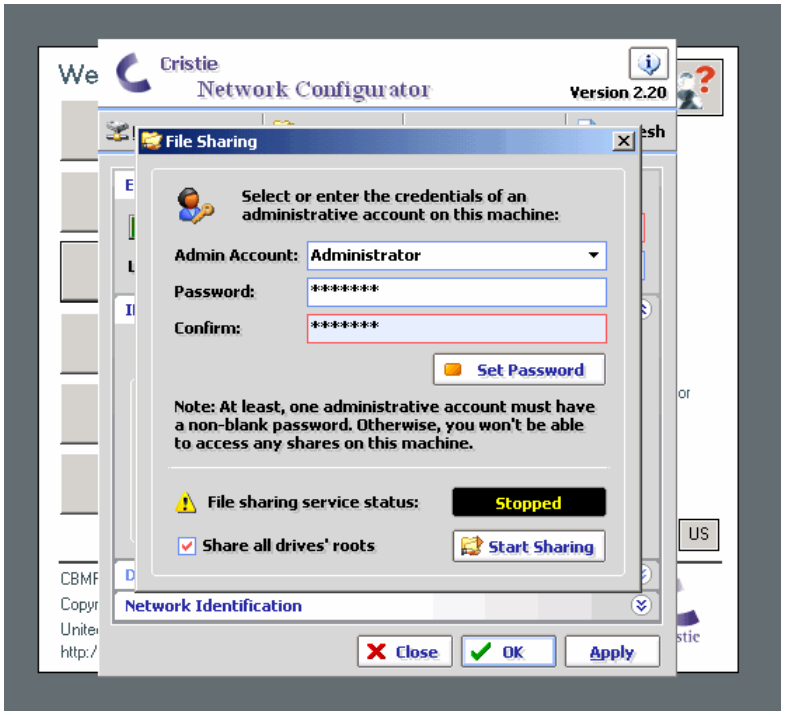
Local File Sharing

It is possible to allow local drives to be shared on the network using the **File Sharing** feature of the **Network Configurator**.

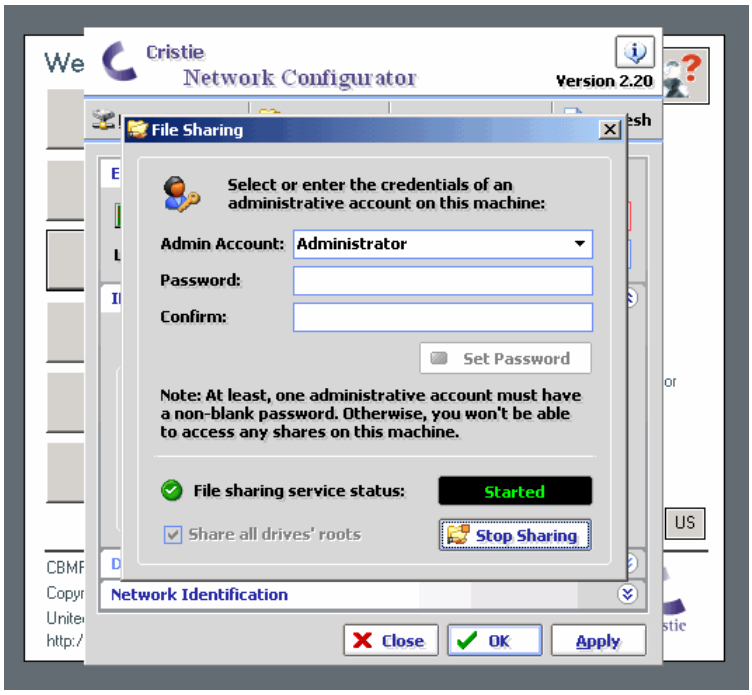


This gives you remote read/write access to any of the drives in the WinPE environment (including any of the recovered drives).

A two step process is required to enable this feature. First you must setup some remote access credentials. If users elsewhere on the network have these credentials then they may access the configured drives. Make sure you specify a non-blank password.



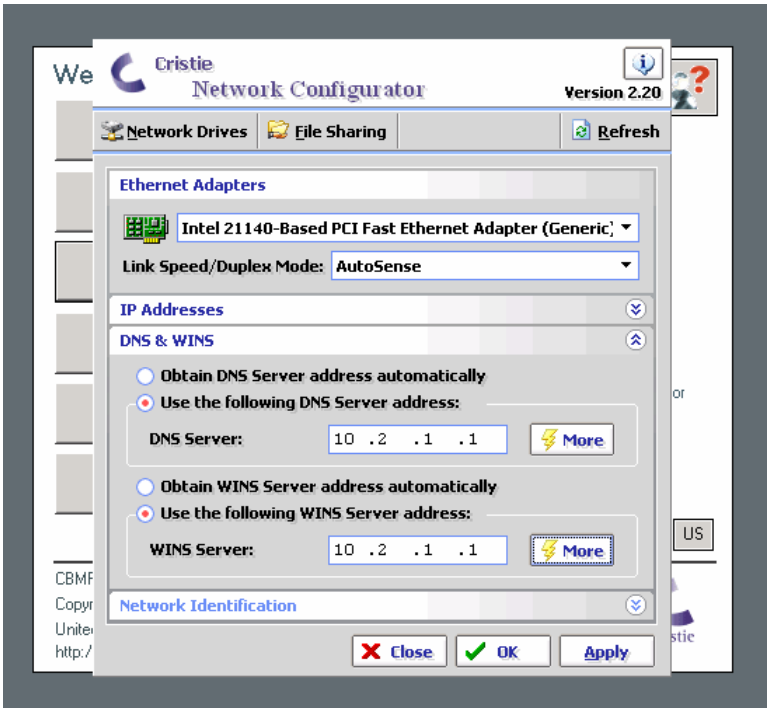
Next start the file sharing service by clicking the **Start Sharing** button.



Click on the  icon to exit this dialog and return to the main **Network Configurator** menu.

Setup DNS And WINS Servers

Using this option allows DNS and WINS server IP addresses to be set for the WinPE environment.



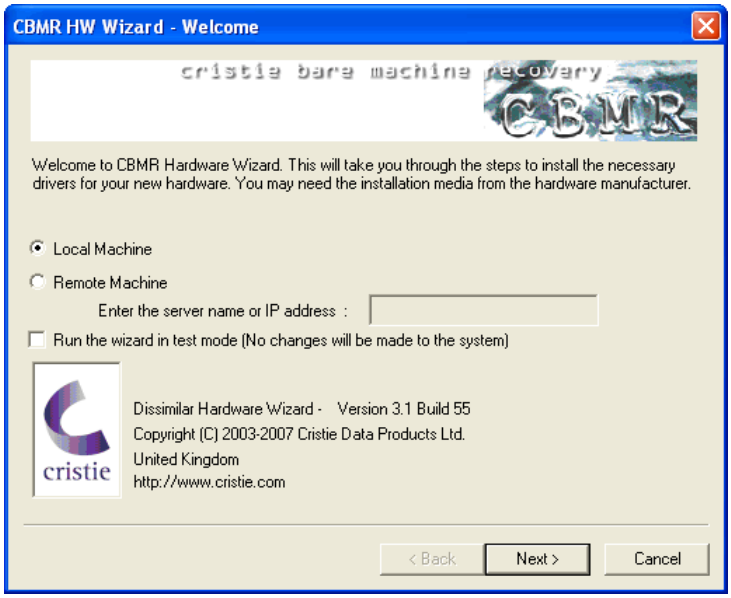
Setup Network Identification

It is possible to setup the Network Identification of the recovering system. This allows the WinPE hostname and workgroup to be changed during a DR session. These details are transient and only apply while the WinPE DR session is running. They are not applied to the recovering system when it reboots after the DR session.

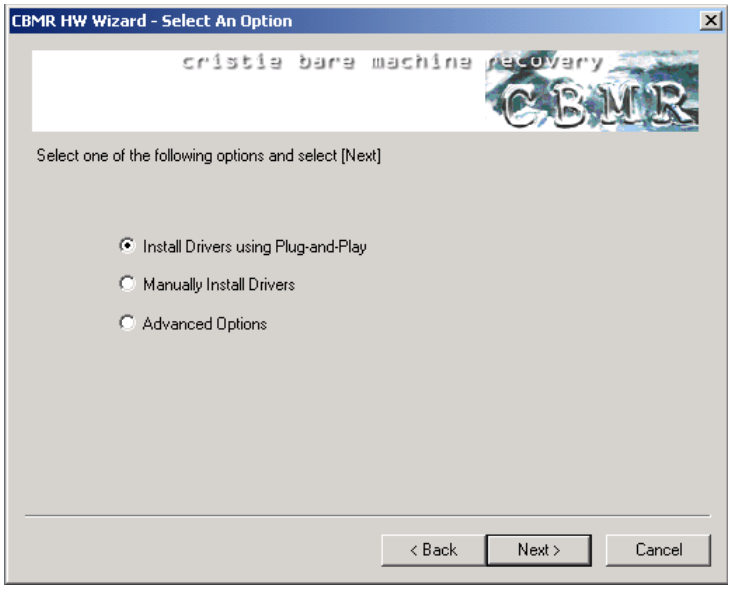
Dissimilar Hardware Wizard

The Dissimilar Hardware Wizard can be used to load Windows drivers onto the recovering machine. It is only necessary to load the drivers for the hard disk and the CPU/HAL. Drivers for the hard disks can be determined by Plug-and-Play (PnP) and may be readily identified. However changes required in the CPU model via a change in HAL, cannot yet be determined by PnP; these need to be loaded manually.

In the Windows PE environment you only connect to the **Local Machine**. The same wizard is also used remotely for Linux mode recovery.

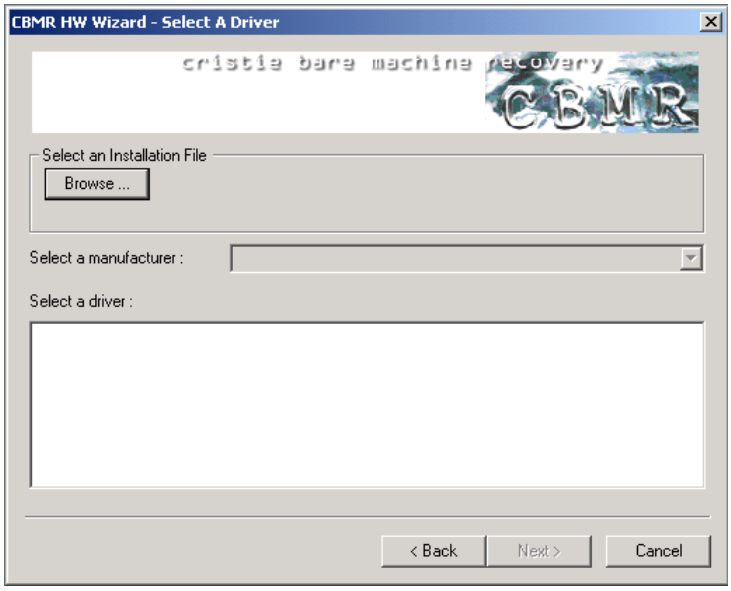


So to install drivers for hard disks, select the Plug-and-Play option.

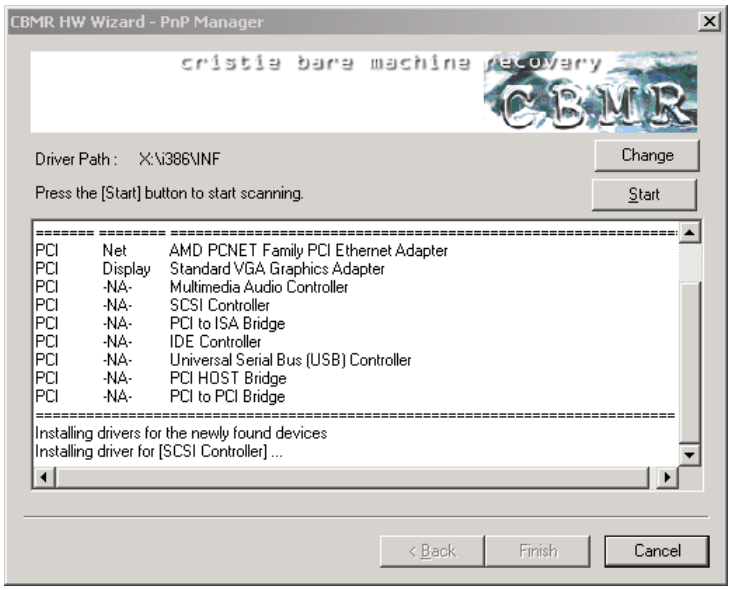


Plug-and-Play

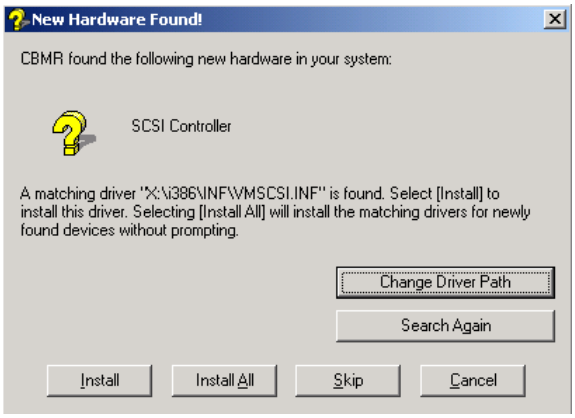
The window appears empty to start with. The set of drivers located on the recovery CD is the default choice. It is possible to change this to a network share or another CD with the **Change** command button. Begin the PnP driver detection by clicking **Start**.



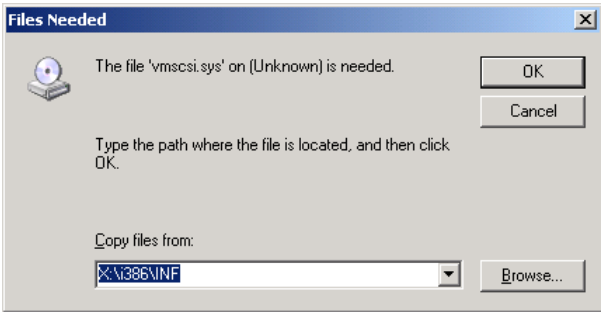
The process checks the devices that it can detect and when it finds one that does not have a driver loaded, it will offer to install it.



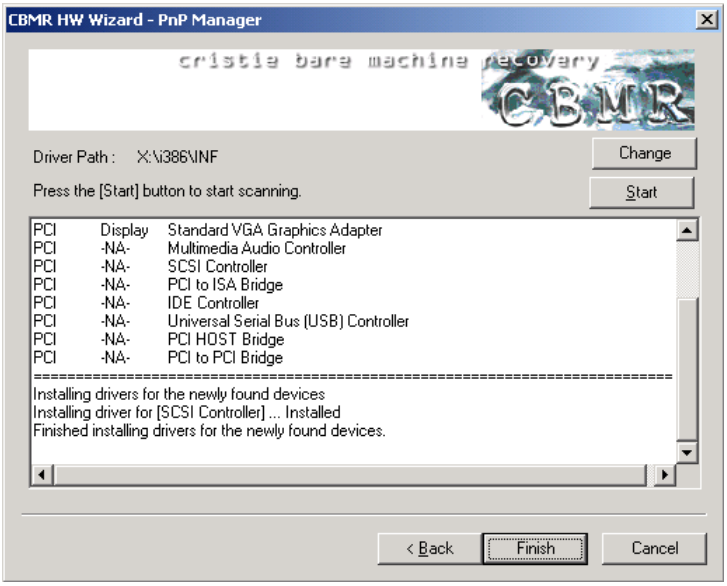
The wizard identifies the source of the Windows drivers. You may change the path to these .inf files and click **Search Again** to make it use the new path. Once you are satisfied that the path is correct click on **Install** and the driver will be installed.



Drivers are usually .sys files. The .inf files define which driver files need to be loaded for a given device. You may need to confirm the location of the driver files for each device, or possibly find the path where they are stored. When you have the correct path, click on **OK** and the wizard will look for more.

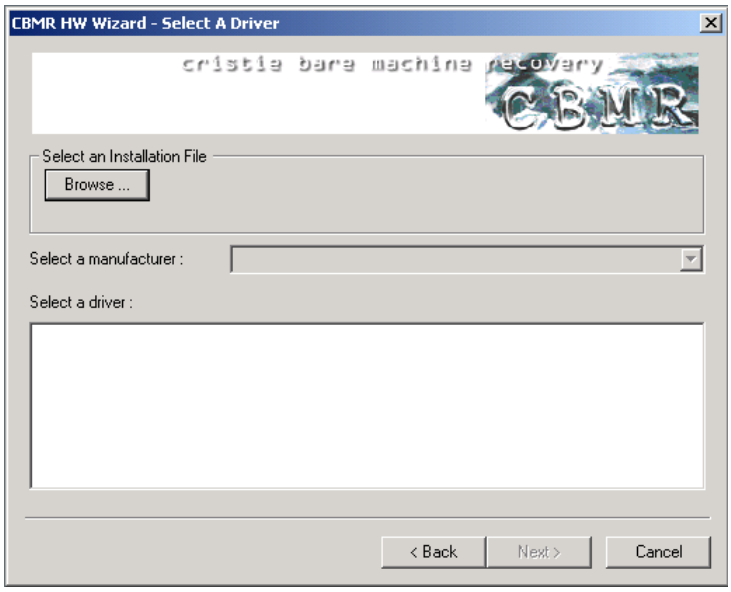


Once all of the drivers of the detected devices have been processed, the wizard will indicate that the installation has finished. Click on **Finish** to proceed.

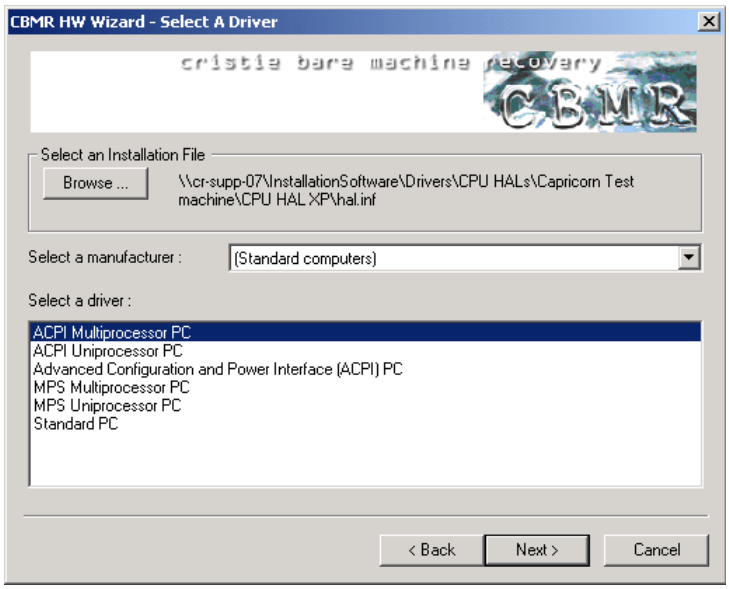


Manual Installation

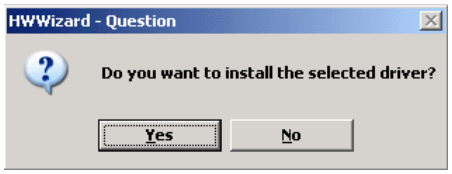
Normally you would only manually install a driver for a CPU/HAL change. Select **Browse**.



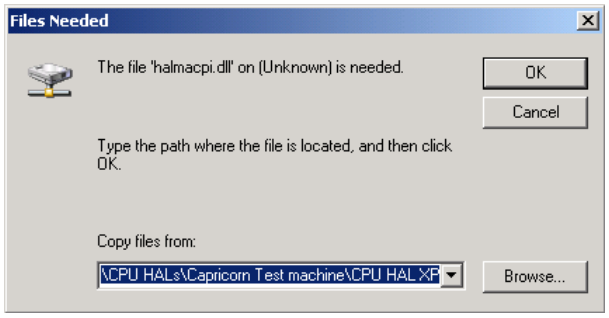
Find the driver that you need by browsing to the appropriate folder that holds the .inf file for the driver you wish to load. If you need to load the driver from another machine, then you can browse to a share on that machine and then to the appropriate folder.



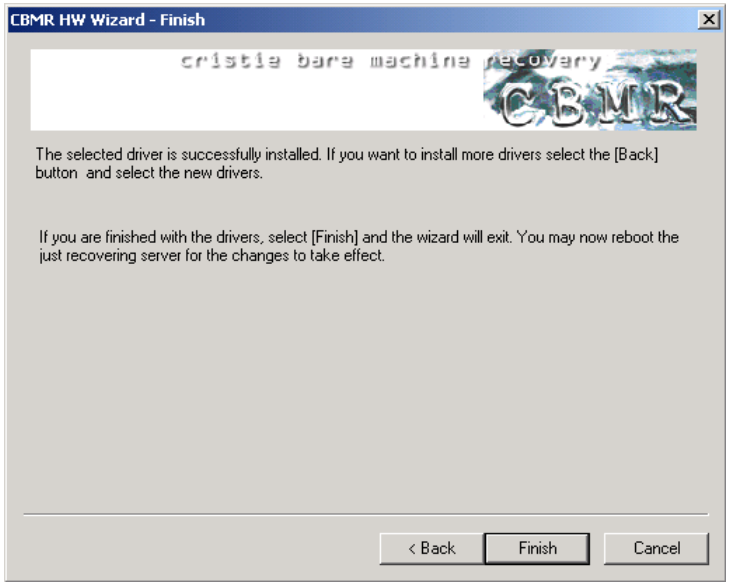
The wizard allows you to select drivers that are grouped by manufacturer. Select the actual driver that you wish to install and click **Next>**.



After you confirm the selection, the wizard determines which files need to be installed. You are given the opportunity to change the location from which they are loaded.

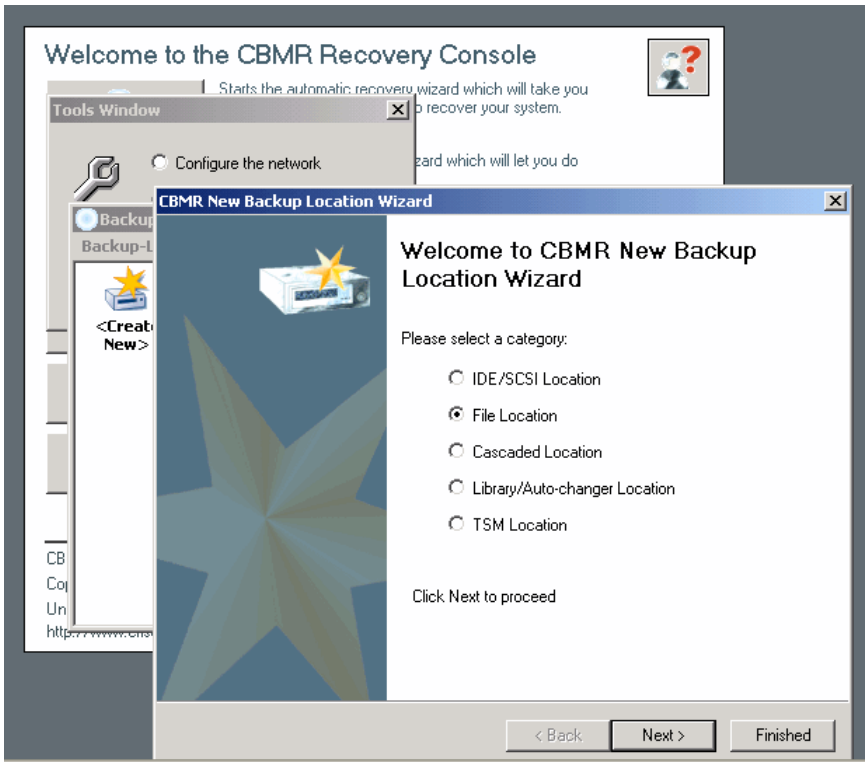


When the drivers have been installed, the wizard allows you to go back and do another one or finish the process.



Setup Backup Locations

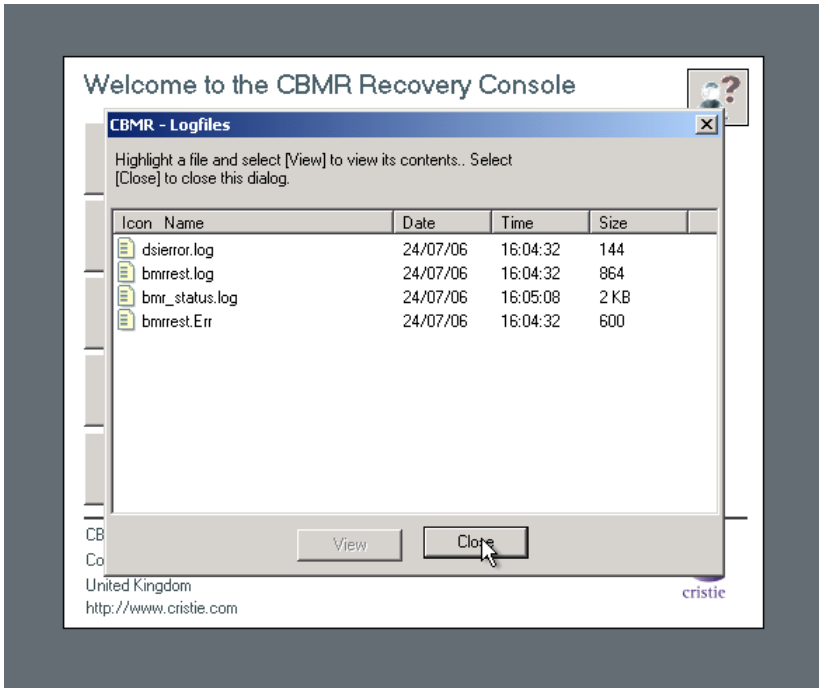
Starts the Create Backup Location wizard allowing the location of the backup to be defined.



Select the device category from the list and enter all the parameters required to define the location. Refer to Locate Configuration , http://www. for further discussion.

6.4.5 Show Log and Error Reports

This main menu option allows the log files produced during the recovery to be viewed using notepad. Normally viewing this information is only required to diagnose a problem with the recovery.



dsierror.log - ITSM interface log information

bmrest.log - backup restore summary information, e.g number of files restored, skipped, time taken etc.

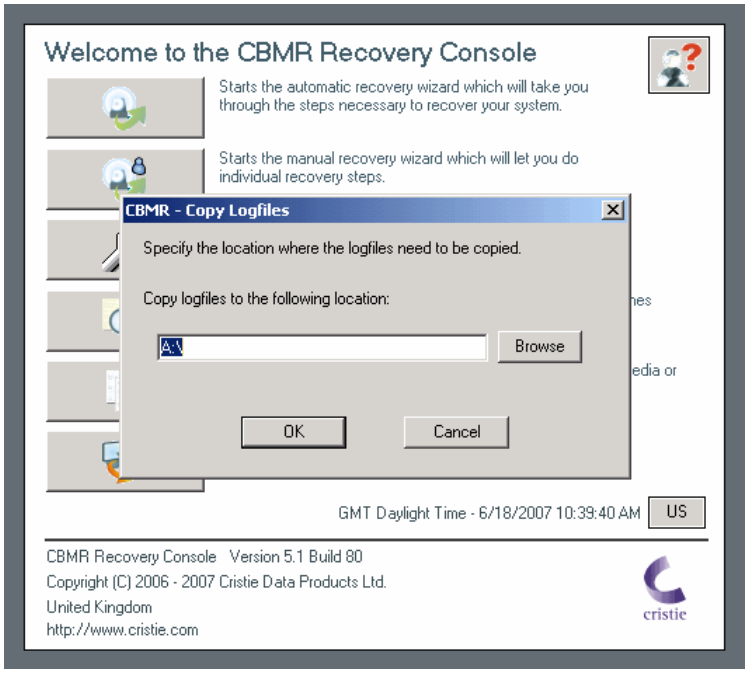
bmrest.err - log of errors encountered during the backup restore.

bmr_status.log - restored disk and registry configuration log, e.g. disks/partitions created summary etc.

setupapi.log - contains a summary of the PlugNPlay devices detected by WinPE as it boots. Useful for diagnosing WinPE driver problems.

6.4.6 Copy Log and Error Report Files

Since all log and error files generated during the recovery are only transitory (i.e. they are lost as soon as the Windows PE environment exits), this option allows you to copy the to a local device or remote network share for permanent record. Use the Cristie Network Configurator Tool , http://www. to setup a network share.

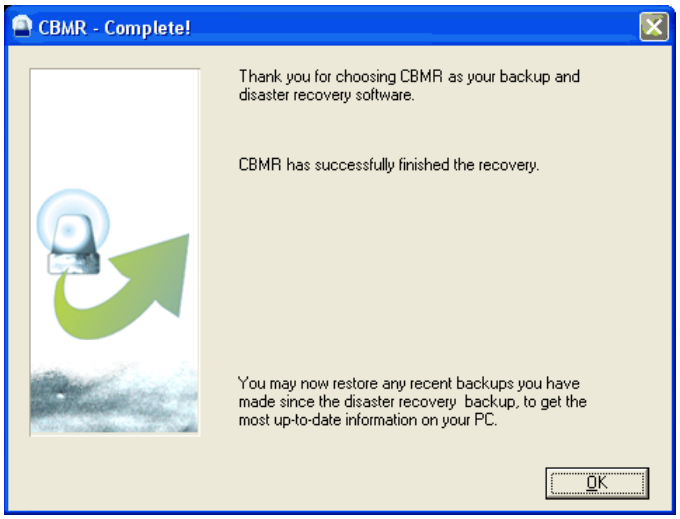


The example shows files being copied to a local floppy drive.

6.4.7 Close Recovery Console and Reboot

After a successful recovery, select this option to exit the Windows PE environment and boot the recovered system.

Press **Yes** to the restart confirmation warning or **No** to continue running the DR console. If you choose to reboot the recovered Windows system will start.



The above dialog is displayed when the recovered system re-starts and shows the successful completion of the Disaster Recovery.

7 CBMR In More Detail

The Cristie Cristie Bare Machine Recovery software is a fully featured 32 bit multi-threaded disaster recovery and backup software package for all users of Windows 2000, Server 2003 and XP (including 64-bit versions).

Unless indicated otherwise the information in this document applies to all versions of the software.

Cristie Bare Machine Recovery offers:

Optimum system performance with minimum use of system resources. For example, Quick File Access (QFA) tape indexing which allows high speed retrieval of individual files, appended backups, backups run as a background process.

Multiple drive support. CBMR supports a wide range of Backup Locations including AIT, DLT, DAT, SLR, LTO tape drives and library, autochanger systems. the File Device or Virtual Tape Device driver allows backup to hard disks, network drives and a variety of removable disk drives.

A Scheduler tool allowing automated unattended backups.

A Backup Catalogue, which is a collection of summary information on each backup volume. This provides a quick method of locating data without having to access different Backup Locations or load numerous media until you find the data you require.

7.1 On-line Help

CBMR includes a comprehensive on-line Help facility.

Help is available:

- from the Help push button 

- using the F1 key. Help information is displayed for the currently selected operation.
- from the Help top bar menu.
- using the Table of Contents, Index or the Search facility to locate the topic you are interested in.

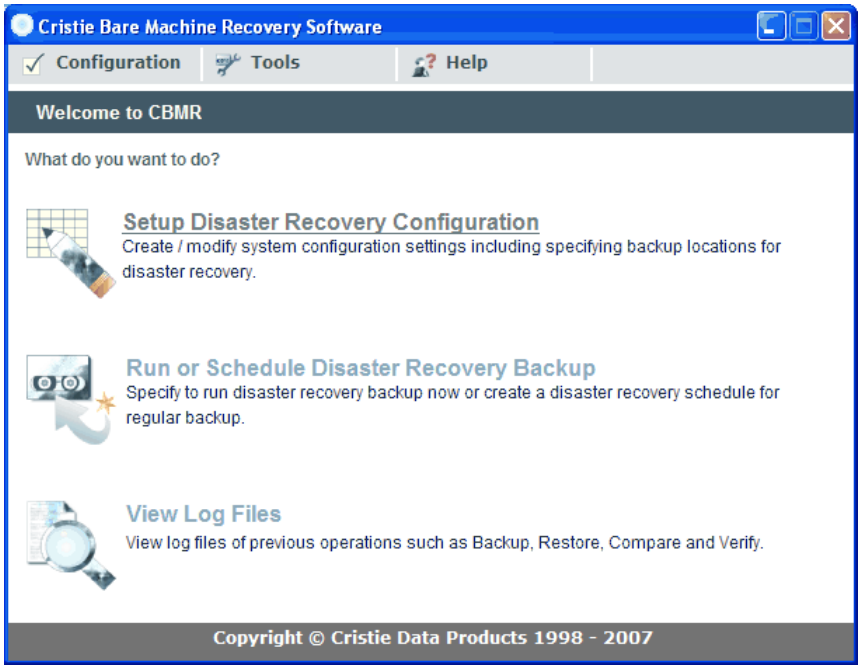
7.2 CBMR User Interface

The CBMR main workspace is where most CBMR windows are opened. The main dialog shows the most frequently used functions of CBMR. In addition a menu bar runs along the top providing drop-down options for further more advanced features.

A wizard is defined for each of the main tasks such as setting up the system recovery information, creating or running a backup, managing backup locations, maintaining a catalogue of backups and defining the default options.

7.2.1 CBMR Setup Disaster Recovery Configuration

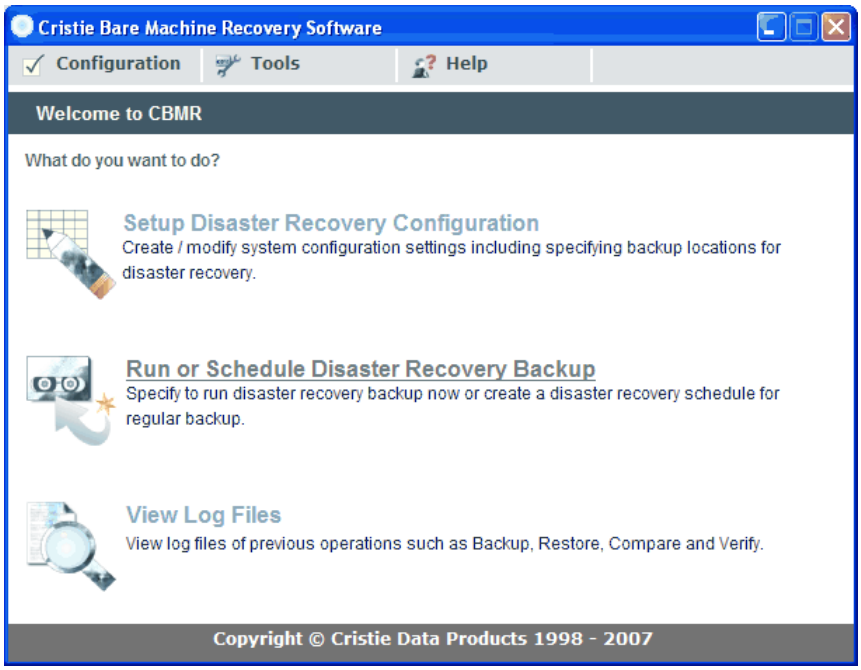
To invoke, click on Setup Disaster Recovery Configuration from the CBMR main window.



Selecting this option allows the system configuration to be created and saved to a User specified location. Note that this could optionally be collocated with the Disaster Recovery backup itself.

7.2.2 CBMR Run or Schedule Disaster Recovery Backup

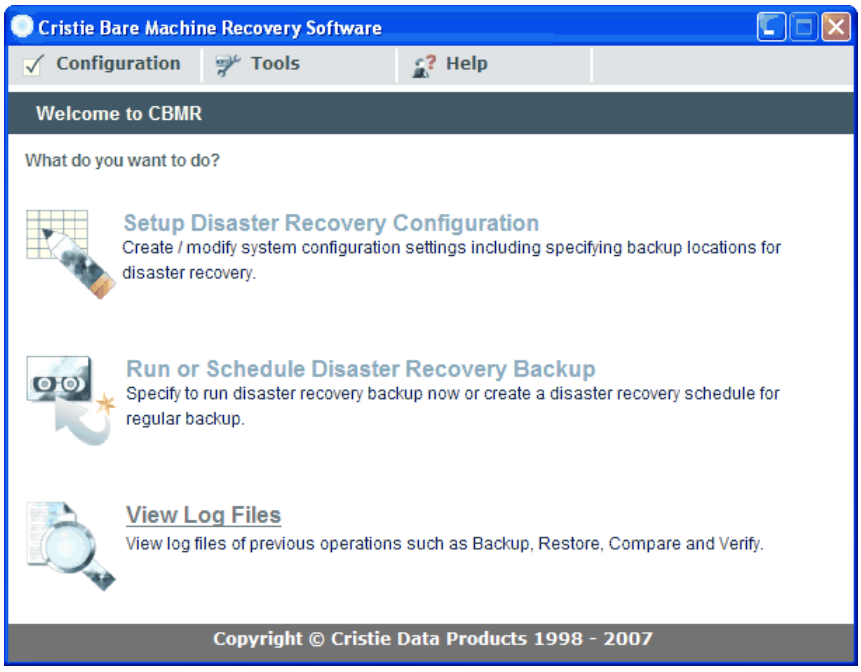
To invoke, click on Run or Schedule Disaster Recovery Backup from the CBMR main window.



7.2.3 Log Files

When a backup or restore operation is performed, progress messages can be stored in a log file. The level of information stored and the name of the log file is set in Backup Selection script properties (for backups) and in the options dialog (for Restore, Compare and Verify operations).

To view existing log files select View Log Files from the main CBMR menu.



If you request a log file to be created, the file is automatically saved and can be viewed using this option.

You can view or delete existing log files.

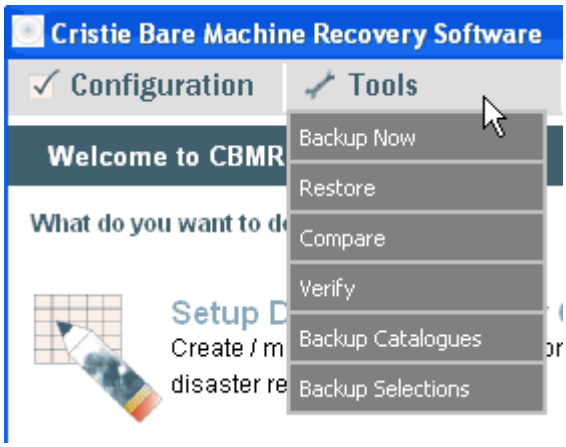
Please note that there will be no log files present unless you have previously run a Backup, Restore, Compare or Verify which requests one to be created.

Cristie's Support personnel may ask for a CBMR version log to help in diagnosing problems with your CBMR installation. This is a text file containing a list of components and their corresponding version nos. To do this select Log Version Details from the main Help menu.

A file called version.log is created and can be viewed using the View Log Files option as before.

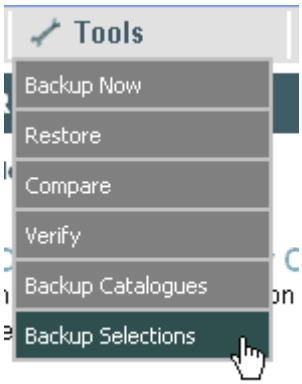
7.2.4 CBMR Tools

The CBMR Tools presents the Backup Now, Restore, Compare, Verify, Backup Catalogues and Backup Selections functions. These are the main tasks that you will perform when maintaining your backup routines.



7.2.5 CBMR Backup Selection Tool

The Backup Selection tool contains scripts for performing regular backup jobs. To view the backup selections, click on the Tools drop-down menu and select Backup Selections.



All saved scripts are created by this tool.

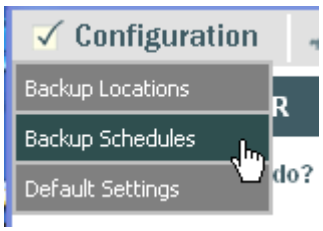
A backup selection script defines the files and folders that will be backed up, along with various options such as the Backup Location on which the backup will be stored, the detail that will be saved in the backup catalogue, and the amount of information that will be stored in the backup catalogue. Essentially, a backup selection script defines the What and the How of a backup.

CBMR is supplied with a pre-defined script called system.scp. This script will backup all the files on Drive C: to the default backup location.

You can modify the system.scp script to suit your backup job or you can use the options in 'Create New Backup Selections' to create your own scripts.

7.2.6 Scheduler

To invoke the Backup Schedules configuration tool, click on the Configuration drop-down menu and select Backup Schedules.



From here you can control existing scheduled jobs (Hold, Release, Run, Delete, Modify) or create new ones.

The Scheduler is a simple way of maintaining your Backup regime. Once you have created the backup selection scripts (...what needs to be backed up and how), and created schedules for them, the scheduler will simply carry on and do the work without further intervention.

If Backup Scripts define the What and the How of a backup, then Schedules define the When.

CBMR supports two services for running scheduled jobs: the CBMR Scheduler Service and the Microsoft Windows Task Scheduler service. Both provide the facility to schedule jobs for unattended running. The Microsoft Windows Task Scheduler service allows more flexible schedules to be configured but the CBMR scheduler service is more tightly integrated into CBMR.

The Default Settings option can be used to configure whether the Scheduled Jobs tool displays jobs scheduled through the Windows Task Scheduler service or the CBMR Scheduler service.

7.2.7 Backup Catalogue

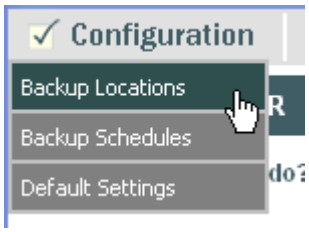
The Backup Catalogue is a list of previous backups (backup volumes). To view the catalogue, click on the Tools drop-down menu and select Backup Catalogue.

Each time a backup is performed, a new Volume can be created in the Backup Catalogue. A Backup Catalogue entry holds a list of the files and folders backed up. This catalogue can be browsed and queried, allowing you to find the location of backed up data without having to load tapes (if relevant).

The Backup Catalogue tool displays existing backups. You can view the catalogue entries, search for individual entries, create new ones or delete existing entries.

7.2.8 Backup Locations

To invoke the Backup Locations configuration tool, click on the Configuration drop-down menu and select Backup Locations.



A Backup Location reprsents any physical device you use to backup your data. For example, a tape streamer, an autochanger or tape library, or a Virtual Tape Device, IBM Tivoli or Cristie Storage Manager device.

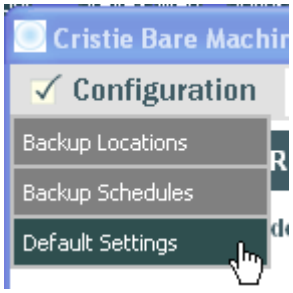
The Backup Location Configuration option holds details of all the Backup Locations currently configured within CBMR. Locations can be deleted, queried, backed up to and restored from using the Backup Location Tool. At least one Backup Location must be configured within CBMR.

When CBMR first starts, no Backup Locations will be configured.

Backup, Restore, Compare, Verify and Media Utilities will all automatically use the default backup location unless otherwise directed.

7.2.9 CBMR Default settings window

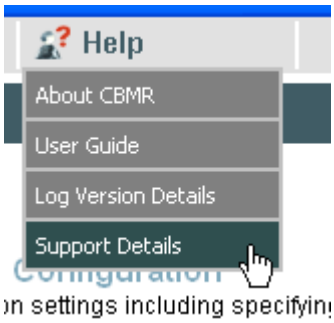
CBMR has a range of defaults which can be adjusted with Default Settings configuration. These include a set of rules which direct CBMR during a backup. For example, what actions apply to a Backup (Append/Overwrite, compression on/off, Save Security Information and so on). To invoke this option select the Default Settings option from the Configuration drop-down menu.



This takes you directly to the Default Settings property sheet. Default settings relating to backup are used by all backups unless you specify otherwise in the individual backup location script's properties.

7.2.10 Support

Click on the Help drop-down menu and select Support Details to display the contact numbers for Cristie Data Products should you have any enquiries or need help with your CBMR package.



Selecting Support Details displays a text document called support.txt (located in C:\Program Files\Cristie\CBMR) which you can change to suit your own requirements. For example, you could edit the file to display your company's technical support contacts.

Technical Support

The Support window lists the contact numbers for Cristie Data Products Limited. If you have any queries or problems concerning your Cristie Bare Machine Recovery product contact Cristie Technical Support. Please make sure you have the following information available for the person dealing with your call:

- CBMR Version Number
- Windows OS and Version Number
- Backup location type and Model Name if appropriate (e.g. SCSI tape device)
- Backup location device Serial Number if appropriate
- Backup location device connection type (Parallel, SCSI, USB)
- Any error message information (if appropriate)
- Description of when the error occurs.

Cristie Data Products Limited are continually expanding their product range in line with the latest technologies. Please contact the Cristie Sales Office for the latest product range. Should you have specific requirements for data storage and backup devices then Cristie's product specialists can provide expert advice for a solution to suit your needs.

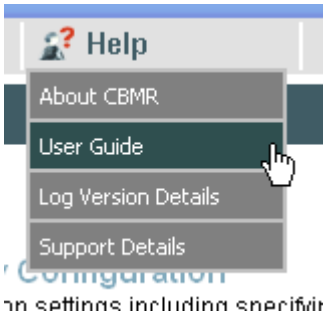
7.2.11 Contact Numbers

Cristie Data Products Limited (UK Office)	
Technical Support	+44 (0)1453 847009
Technical Support Fax:	+44 (0)1453 847003
Sales	+44 (0)1453 847000
Sales Fax	+44 (0)1453 847001
Email	cbmr@cristie.com

Web Page	www.cristie.com

7.2.12 User Manual

To display the CBMR User Guide, click on the Help drop-down menu and select User Guide.



This will display the contents of the User Guide.

8 Getting Started with CBMR

CBMR allows you to backup any data on your system to any Backup Location (except CD-writers) attached to your computer or network. You can then examine the content of the backup and restore any desired files/directories.

To use CBMR you must:

1 Install the software.

2 Set up the Backup Location storage device(s (page 132)).

3 Set up Backup Selection scripts to do appropriate backups (page 147).

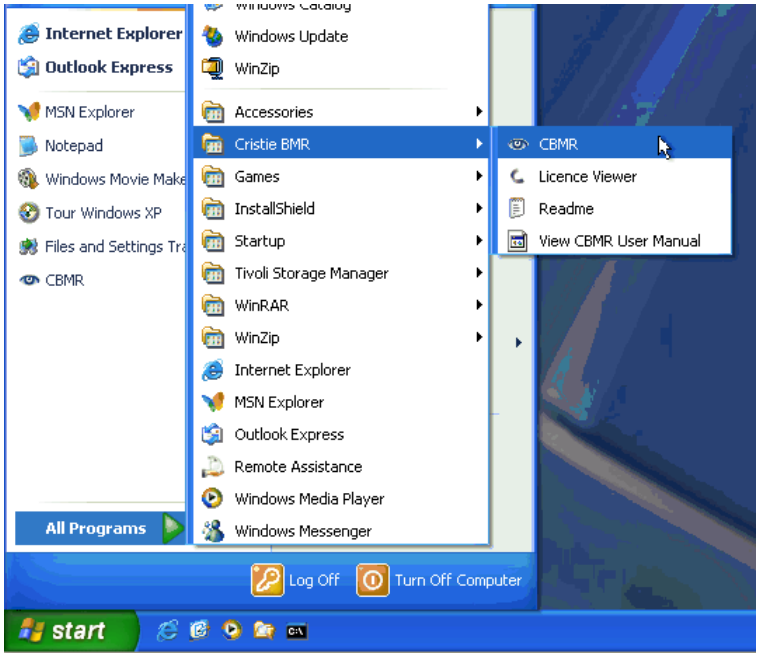
If you wish, you can also set up the scheduler (page 159) to perform the backups.

You can then

- Perform a regular cycle of backups (page 170) using the Scheduler.
- Find data that you have backed-up, using the Backup Catalogue Utility (page 165).
- Restore data from the backups.

8.1.1 Running CBMR

When the software is successfully installed CBMR is available from the Programs menu in the Start popup. The example below shows CBMR about to be started.



A shortcut 

to CBMR is also created on the desktop during installation . CBMR may also be started by clicking on this shortcut.

8.1.2 Configuring CBMR

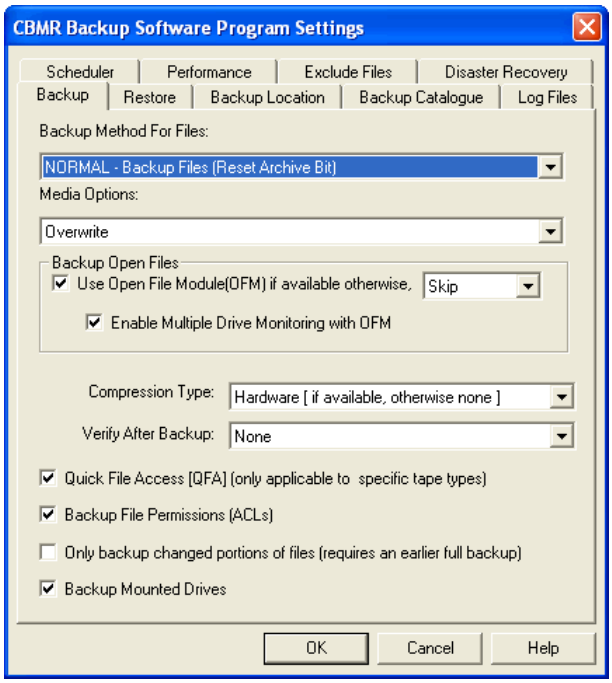
CBMR is supplied ready to use, with program settings already defined. However, you should check the program defaults to ensure that they are appropriate to your Disaster Recovery or Backup and Restore requirements.

All the information is contained in property pages. Each page is dedicated to a different section of the configuration making it easy to locate a particular area if you need to make changes.

The default program settings, once defined, will generally remain unchanged. If you want to apply different rules for a particular job then you can modify the settings from within the Backup Selection script and these will apply only to the current script.

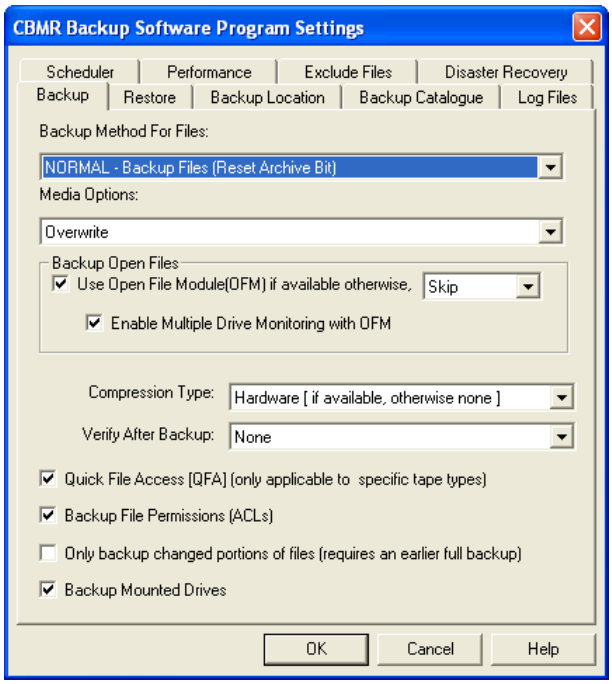
Default Settings Configuration

To invoke the **Default Settings** configuration, select it from the Configuration toolbar. If the Default Settings configuration is invoked from a wizard or other tool, CBMR opens the relevant page. For example, if you are in the **Backup Catalogue** the Backup Catalogue tab is displayed; if you are in **Backup Location** the Backup Location tab is displayed.



Backup Properties

This page allows you to set the default actions which will apply during a backup. The defaults can be over-ridden in the properties for individual backup selection scripts.



Backup Method For Files

There are 4 pre-configured backup methods to choose from.

NORMAL - Backup Files (Reset Archive Bit)

The Normal selection will backup all the selected files and reset the archive bit.

COPY - Backup Files

The Copy selection will backup all the selected files without affecting the archive bit.

DIFFERENTIAL - Backup Changed Files

The Differential selection will backup all files that have changed or are new since the last Normal or Incremental backup. The backup will not affect the archive bit.

INCREMENTAL - Backup Changed Files (Reset Archive Bit)

The Incremental selection will backup all files that have changed or are new since the last Normal or Incremental backup. The backup will reset the archive bit.

Media Options

The media options control the way that data is written to the media.

Overwrite. If overwrite is selected the backup will start at the beginning of the media overwriting any existing data.

Overwrite media with the same label, append otherwise. Selects overwrite only if the media label matches with the requested media, otherwise the data will be appended to the media.

Overwrite media with the same label, fail otherwise. Selects overwrite only if the media label matches with the requested media, otherwise the operation fails and no data will be written to the media.

Append, overwrite if not appendable. Selects append, but if the media is blank or the media contains a non CBMR data set and therefore cannot be appended, the media is overwritten.

Append to media with the same label, fail otherwise. Selects append only if the media label matches with the requested media, otherwise the operation fails and no data will be written to the media.

Backup Open files. By selecting this option, CBMR will use OFM if installed and running, while backing up open files. If OFM is not installed or the option is not selected then the option to Automatically retry the open file, Skip the open file or Ask the user what to do can be selected from the list box. If the OFM is in use then a further option is available to enable multiple-drive monitoring. Note that OFM is only used on Windows 2000 platforms.

Compression Type The type of data compression can be selected to be:-

None Data is not compressed.

Software Data compression will be performed by the CBMR software before the data is written to the Backup Location.

Hardware compression (if available, otherwise none) This option will attempt to make the Backup Location perform the data compression. If compression is not available on the hardware, the data will remain uncompressed.

Hardware compression (if available, otherwise Software) By preference, data compression will be performed by the hardware if it is possible, otherwise compression will be done by CBMR software.

Verify After Backup Checks the validity of the recorded media.

None Does not perform any checks

Check Integrity alone After finishing the backup, the media will be scanned from the beginning to end, ensuring it is readable.

Byte By Byte comparison After finishing the backup, each file on the media will be compared against its disk counterpart and the differences reported.

Quick File Access (QFA)

This option, if ticked will provide rapid access to files during a restore operation. (Not all drives support this option.)

Save File Permissions (ACLs)

Select this option (ticked) if you want the security information (access control data) associated with directories and files as well as the data included in the backup. If the option is not ticked then only the data is included.

The user who is logged on must have the appropriate '*Right*' to request security information to be backed up. Please check with your System Administrator that your user account has been included in the Backup Operators group.

If this option is enabled then all the security details (access control data) are included in the backup as well as the data.

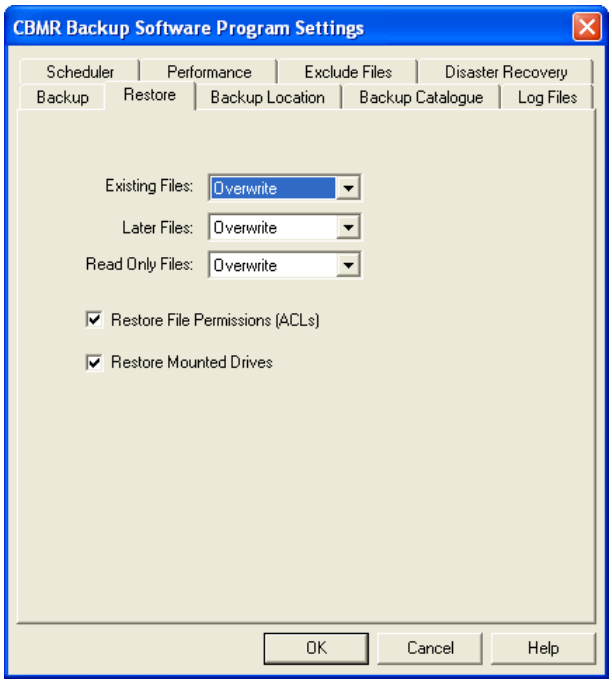
Only backup changed portions of files

When changes are made to large databases files these are usually very localised. That is, only certain portions of the files keep changing. It is sufficient to only backup the changes as long as the most recent version of the file can be reconstructed with the original version and the changes. This saves lots of time and media space but is very processor intensive.

Caution should be used when using this option since the original file backup and all the fragments of the file are needed when restoring file.

Restore Properties

This page allows you to set the default actions which will apply during a Restore job. The defaults can be over-ridden when performing individual restores.



Existing Files If any files being restored already exist on disk then you can direct CBMR to respond in one of the following ways:

- Skip any file it encounters which already exists.
- Ask whether it should overwrite or skip the file.
- Overwrite the existing file with the file from the backup.

Later Files If any files being restored are found to be later versions than those already existing on disk then you can direct CBMR to respond in one of the following ways:

- Skip any file it encounters which are later versions.
- Ask whether it should overwrite or skip the file.
- Overwrite the file on disk with the later version from the backup.

Read Only Files If any read only files being restored already exist on disk then you can direct CBMR to respond in one of the following ways:

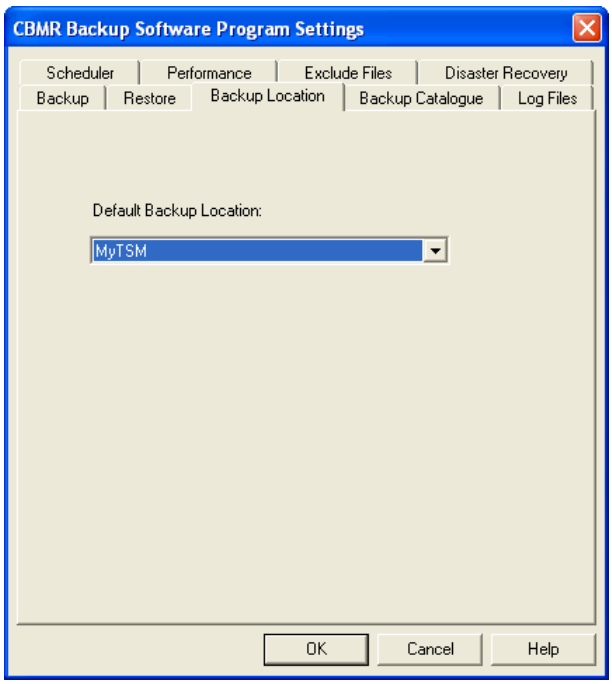
- Skip any read only file it encounters which already exists on disk.
- Ask whether it should overwrite or skip the file.
- Overwrite the file on disk with the file from the backup.

Restore Security Info: (CBMR for Windows NT installations only) If this option is ticked CBMR will restore the security information associated with directory files included in the restore. If the option is not ticked then only the data is restored.

NOTE: You must be logged on the computer as a user account with the appropriate rights to restore security data.

Backup Location Properties

This page allows you to select a default backup location for all future Backup, Restore, Compare and Verify operations. The selection will show all configured Backup Locations. CBMR will always use the default location for Backup, Restore, Compare and Verify jobs initiated from the Executive window.



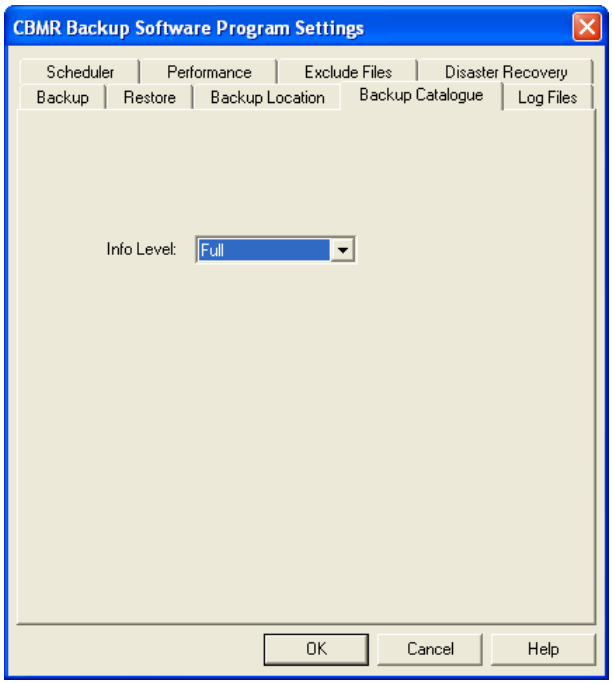
If you need a location which does not appear in the list then you need configure it using Create New Backup Location in the *Backup Locations* folder.

Note: If necessary you can assign a different Backup Location from within the Backup Selections script to be used for a particular job. This does not affect the default.

Restore, Compare and Verify jobs can be run on a non-default location by selecting another backup location in the *Backup Locations* dialog and selecting Restore / Compare / Verify... from its context menu.

Backup Catalogue Properties

This page allows you to define the level of information which is recorded in the Backup Catalogue when a backup is run.

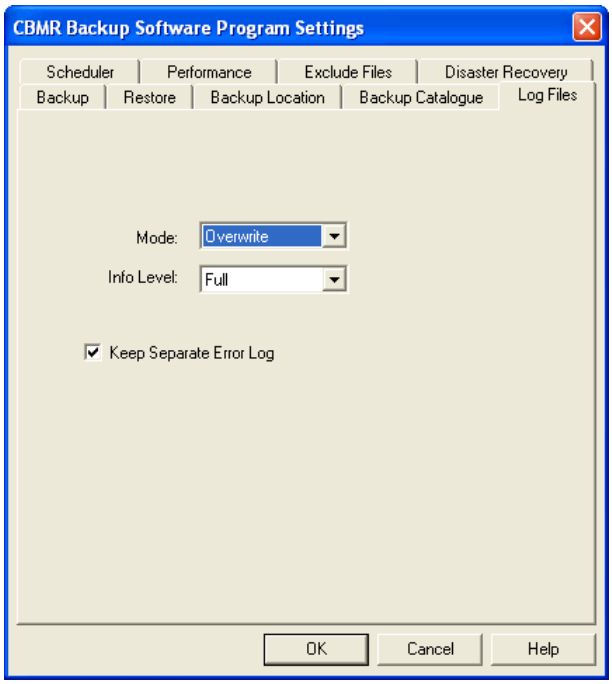


There are four different levels:

1. Full - Media and Dataset headers, Directories plus File information. (This level of detail will use a significant amount of disk space.)
2. Partial - Media and Dataset headers plus Directories.
3. Brief - Media and Dataset headers only.
4. None - No details of the backup are recorded in the Backup Catalogue.

Log File Properties

Log files are a useful source of information and will list any error messages. Log file information can be important if problems have occurred.



The following options are available:

Mode - Overwrite/Append

If **Overwrite** is set, then each time the log file is created it overwrites the existing one.

If **Append** is set, then each log file is appended to the previous one.

Info Level - Full/Partial/Brief/None

A **Full** logfile contains a list of all files, errors (if any) and statistics.

A **Partial** log file contains sub-directories, errors (if any) and statistics.

A **Brief** log file contains errors (if any) and statistics.

If **None** is selected then no log file is created.

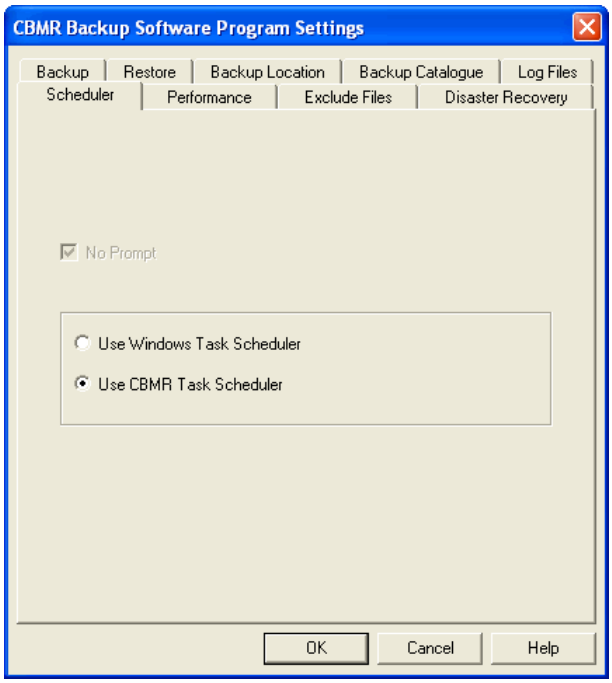
Keep Separate Error Log

If this option is ticked, an additional log file is created which lists errors only. Similar to the other log files, it takes the name of the current operation but with an extension of .err E.g. **backup.err**

Errors will still be written to the Full, Partial or Brief log file if you have requested one of these.

CBMR Scheduler Properties

The CBMR Scheduler tool can be configured to use one of two scheduling services: the Windows Task Scheduler service or the CBMR Scheduler service. The Windows Task Scheduler service allows more flexible schedules to be configured but is not as tightly integrated into CBMR as the CBMR Scheduler service.



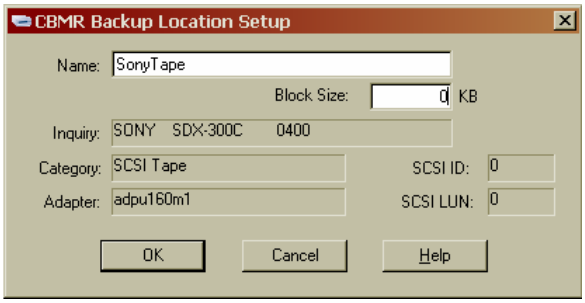
You can request the scheduler to issue a prompt before it begins a scheduled backup. This can be useful if you need to put a job on hold, cancel a job, check the schedule and so on.

Performance Page

CBMR has control over some performance related parameters like the number and size of read/write buffers. The basic unit of data which can be read or written to the tape, called a block, is determined by CBMR depending on the Backup Location device and media type in use. Most recent tape drive manufactures recommend bigger block sizes for better performance. As a result, in version 4 the following configurable parameters were introduced.

Tape Block Size

It is possible to set individual block sizes for each Backup Location used by CBMR. This could be done using the Backup Locations dialog.

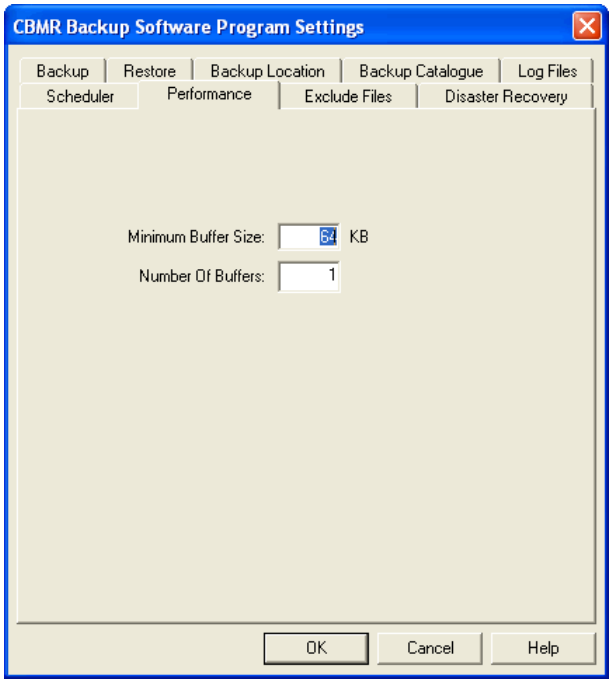


Minimum Buffer Size

The minimum buffer size can be set using the **Default Settings** property sheet, **Performance** page. This only sets the minimum buffer size. It is guaranteed that a buffer size, over this limit will be used. The buffer size should be in multiples of the tape block size in use. Since it is possible to set block sizes individually for locations, CBMR will calculate the next integral multiple block size over this limit.

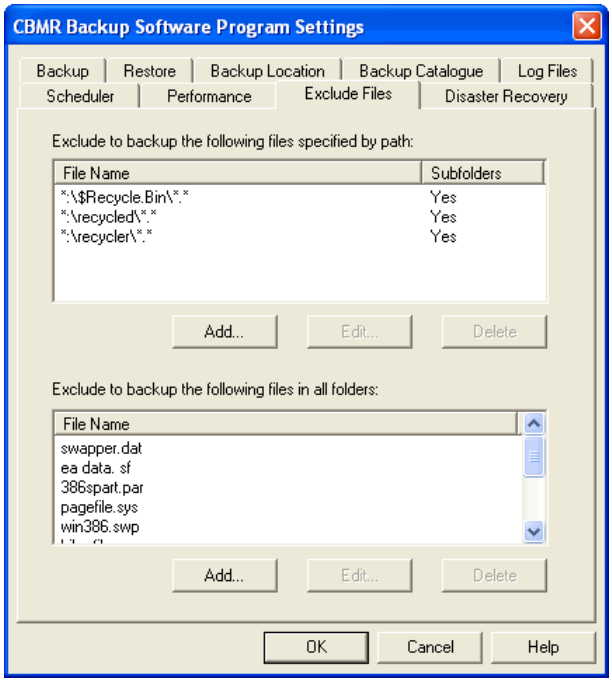
Number of Buffers

At least one buffer is required for any read/write operation. Increasing the number of buffers will increase the performance of the locations with high latency. This depends on the system configuration, location in use and the load on the system at the time of the backup. It is recommended to test with different values on a test backup.



Exclude Files

Allows selected groups of files or folders to be excluded from *all* backups.

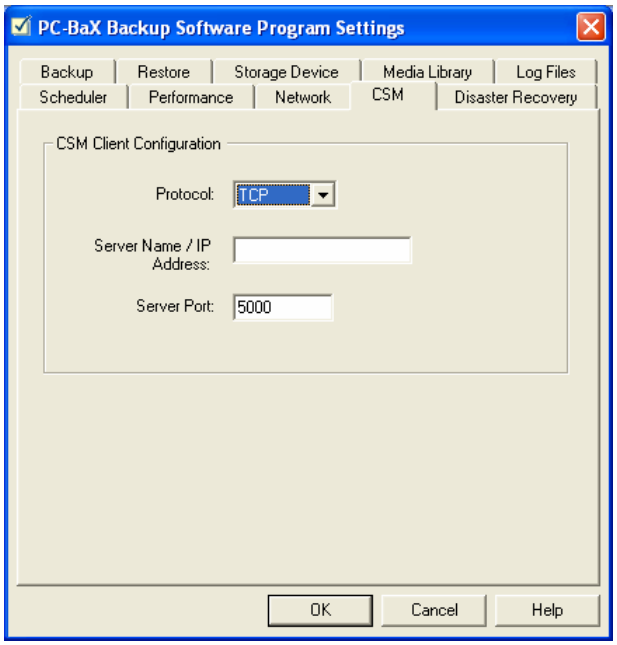


The upper section allows files and folders to be excluded from a backup using the wildcard characters * or ?. The wildcard characters are accepted for drive and filename, but not for the path. For example, *:*.avi will exclude all files with the extension AVI from a backup.

The lower section allows specific named files to be excluded from a backup. Note all files with the specified name regardless, on which drive or in which folder they reside, will be excluded from the backup. Wildcards are not accepted in this case.

CSM Properties Page

If the Cristie Storage Manager Client is installed on your system, the CSM Properties Page displays the options for connecting to a CSM Server.



Protocol

The method of communication to use. Currently, the only supported method is TCP/IP.

Server Name / IP Address

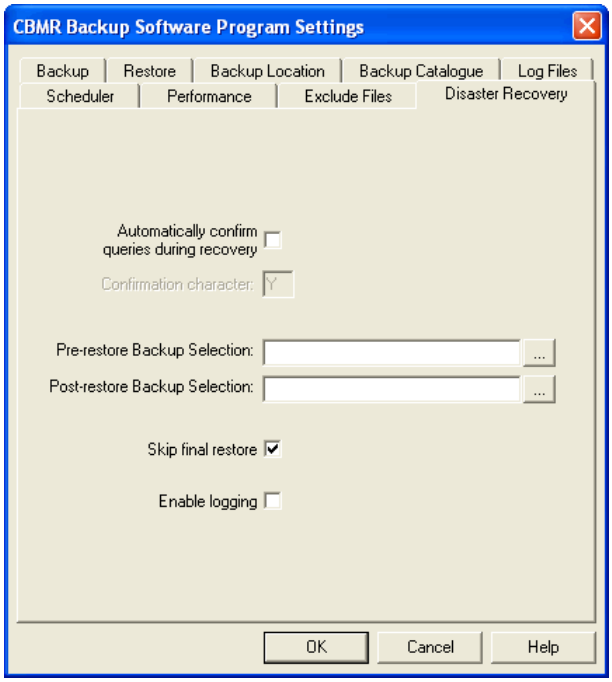
The host name of the CSM server or the IP address in dotted decimal form.

Server Port

The TCP port at which the CSM server is listening for client requests.

Disaster Recovery Properties Page

This page allows various default settings for Disaster Recovery to be configured.



Automatically confirm queries during recovery

During the disaster recovery process, the system will prompt for confirmation to perform some actions. If you would like the Disaster Recovery module to confirm these prompts for you, check this box.

Confirmation Character

The default confirmation character is normally correct for the installed language. If your system uses a different character for confirming command line prompts, change this setting to match. Only relevant when performing Linux based Disaster Recovery.

Pre-restore script / Post-restore script

There may be a requirement to run custom commands before or after a disaster recovery restore operation. These commands should be entered into a windows '.cmd' file which can be linked to using these settings.

Skip final restore

If the final, post-recovery, restore should not be automatically run, select this option. The final restore can be manually run using the DR scripts.

Enable logging

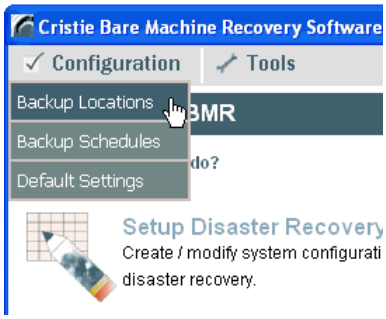
This option configures the disaster recovery restore process to log status messages.

8.1.3 Configuring Backup Locations

To use a Backup Location within CBMR, you must first configure it. The configuration process allows you to give a custom name to your location, as CBMR is capable of finding all the directly attached locations automatically (not ITSM however).

CBMR must have at least one location configured in order to operate and backup data.

Configured locations are listed in the Backup Locations option selected from the Configuration toolbar.



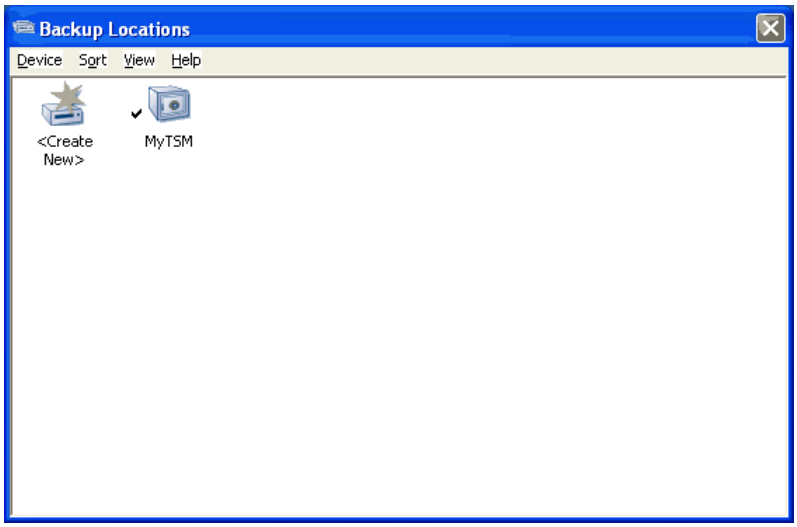
CBMR can use a variety of different backup locations.

These include:

1. SCSI tape drives like DAT, DLT and SLR.
2. IDE tape drives like TRAVAN drives.
3. File locations like removable optical disks or files on a networked disk-drive.
4. All of the above locations cascaded to operate in sequence avoiding media change requests.
5. Library/Auto-Changers configured from Tape drives and Robotics/Media Handler mechanisms.
6. IBM TSM Server (With the Cristie ITSM Client Module).
7. Cristie Media Server CMS (With the Cristie Media Client Module).

Backup Locations

All the configured backup locations in CBMR are listed in the **Backup Locations** configuration. This is a one stop solution to create, modify and delete Backup Locations.



The Locations top bar menu contains options to:

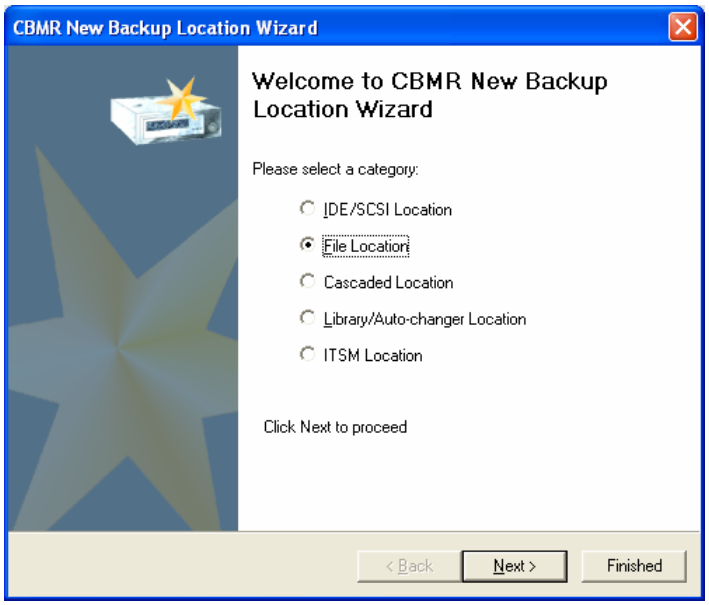
- View the **Settings**... for the selected location
- Run a **Backup**, **Restore**, **Compare** or **Verify** on the selected location
- **Delete** the location
- Run Media Utilities
- Set the location to be the default location when running a Backup/Restore etc. (**Set as Default Location**)

The **Sort** top bar menu allows you to arrange the backup locations in alphabetic sequence (**Sort by Name**) or in date created sequence (**Sort by Category**)

Note: If the **Details** view is displayed you can also sort the entries by clicking the relevant column heading.

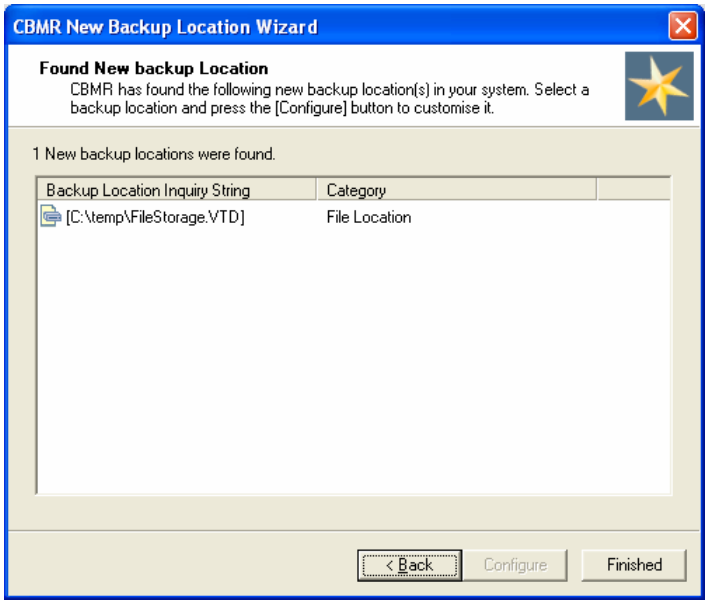
New Backup Location

Selecting the **New** menu option or double clicking the **Create New** icon will invoke the New Backup Location wizard. The wizard allows you to configure various types of backup location.



New Backup Location Wizard/Listing New Backup Location Found Dialog

If you let the CBMR wizard search automatically, the New Backup Location wizard will list the location devices that are directly attached to the system but yet to be configured. It displays the Inquiry string of each location which is read from the device firmware and also the category of the backup location.



The categories can be

- SCSI tape
- IDE tape
- Media Handler/Robotics
- File Device

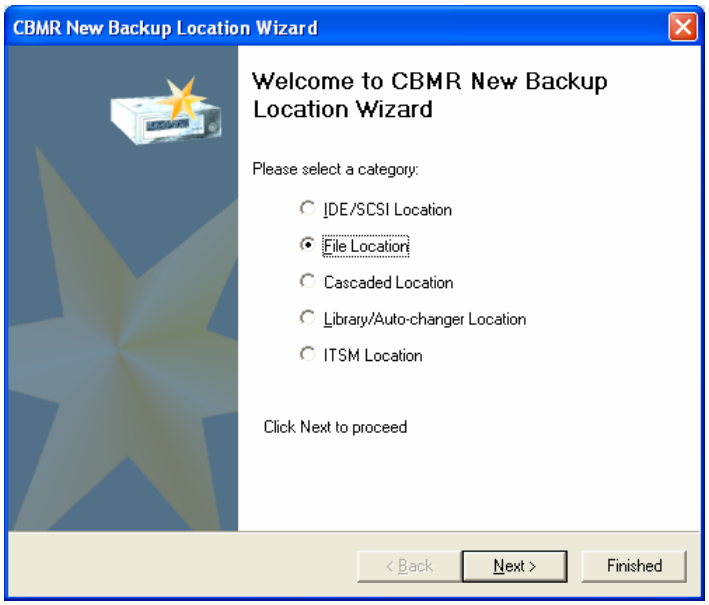
Select an entry and press the [Configure] button (or double click the entry) to add this Backup Location to CBMR's known locations list. You will then be provided with the appropriate configuration dialog.

Note: The locations under the following categories, SCSI Tape, IDE Tape and Media Handler/Robotics should always be scanned by CBMR automatically. The locations under the following categories Cascaded Location and Library/Auto-changer should always be created manually.

New Backup Location Wizard

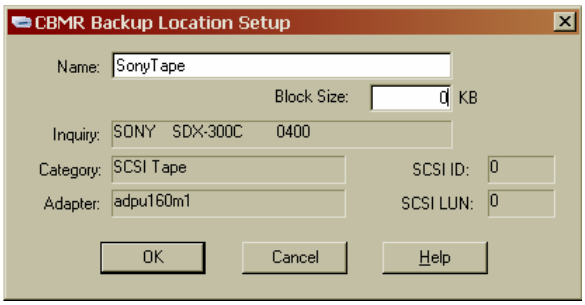
Some backup location types can be automatically found and configured by CBMR

If the selected backup location type can be found by CBMR then the following dialog is presented.



SCSI/IDE Backup Location Setup

SCSI/IDE backup location devices can be configured using the SCSI/IDE backup location Setup dialog. In this only the Name and the Block Size fields are editable and all other fields are for display only.



The various screen fields and their purpose are listed below.

Field	Description
Name	The friendly name of the backup location. Any valid character sequence upto 79 characters is acceptable. The name should be unique and you cannot specify the name of an existing backup location.
Block Size	The size of the tape blocks in kilobytes. Bigger block sizes will give better performance on newer tape drives. However, if you are not sure about it, set it to 0 and CBMR will decide the appropriate block size for the device.
Inquiry	The device specific SCSI/IDE Inquiry string returned from the device. May be useful to find the firmware revision of the device etc.
Category	The category of the Backup Location. The following categories are currently supported: *SCSI Tape* *IDE Tape* *Robotics/Media Handler* *File Device(VTD)* *ITSM Module (if installed)* *Cascaded Device*
Adapter	The name of the Adapter or SCSI Port. On Windows 2000, XP and Server 2003, it will give you the name of the SCSI miniport driver with a running serial number. On Windows NT 3.51, 4.x, it will be of the form ScsiPortx, where x will be 0, 1, ...
SCSI ID	The SCSI ID or Drive number of the device.
SCSI LUN	The SCSI Lun of the device and it will be 0 for IDE devices.

Pressing OK will save the Backup Location details and Cancel will discard the changes you have made. Pressing Help will display this topic.

Virtual Tape Device (VTD) Backup Location

This is a special CBMR file that can be used to emulate a tape on a disk drive. The file can be located on a removable disk, a local fixed disk or located on a remote server share. A File backup location can be created using the Create Backup Location dialog in xubax or gubax. It is possible to specify a size limit on the file itself, in which case, on reaching the specified size, an end of media condition will be created.

It is not a good idea to place the VTD file on a local disk that will be destroyed during a DR operation!

Cascaded Backup Location Setup

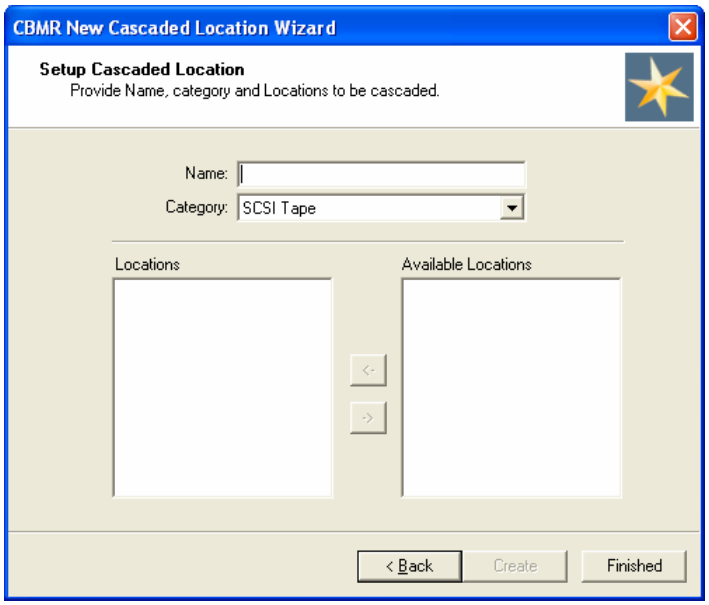
Cascaded backup location in CBMR are special Backup Locations which allow you to cascade two or more similar Backup Locations. Cascaded locations can be regarded as a simple library device, which eliminate the need for a media change on encountering a end-of-media condition on a device. If you have two identical tape devices attached to your system and your backup requires 2 media, you can cascade the 2 devices. The backup will continue on device 2 on reaching the end of tape in device 1.

You can setup a Cascaded Backup Location using the Cascaded Backup Location Setup dialog.

The order of the backup locations in the chain is important as the first location in the list will be accessed first.

You can double click on any location to remove it from the list and add it to the other list.

You can drag and drop using the mouse to re-arrange the locations in the Locations list.



The screen fields with their description are explained below.

Field	Description
Name	The friendly name of the backup location. Any valid character sequence upto 79 characters is acceptable. The name should be unique and you cannot specify the name of an existing backup location.
Category	Gives you a list of location categories in which cascading is permitted. Cascading is allowed in the following Backup Location categories. SCSI Tape IDE Tape File Device Changing the category will list the available locations for that category and you will loose any previous selections.
Locations	Gives you a list of backup locations configured under the selected category. Highlight a location and press the [->] button to remove a location from the chain.
Available Locations	Gives you a list of available locations under the selected category. Highlight a location and press the [<-] button to add it to the chain.

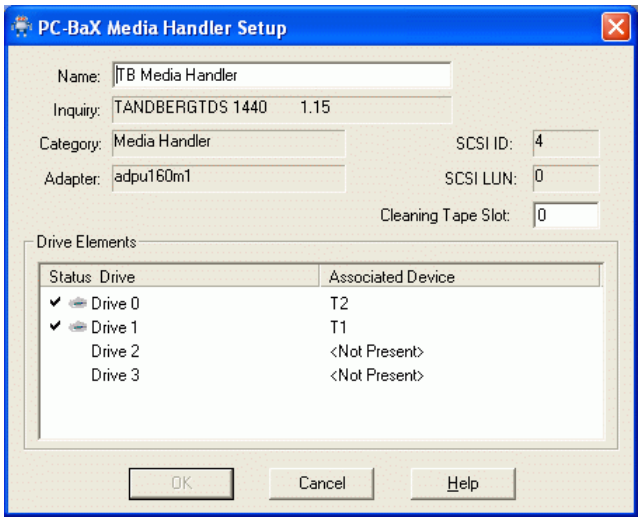
Pressing OK will save the location and Cancel will discard the changes you have made. Pressing Help will display this topic.

Note: Though CBMR does not prevent you from cascading dissimilar backup location devices, for example, a DAT drive to an AIT drive, the backup operation will fail while trying to access the next backup location.

Robotics/Media Handler Setup

"Robotics" is the transport mechanism which moves the media in and out of drives and slots in a tape library device. Each drive in a library is a SCSI device by itself, which should be configured prior to this configuration. You have to make a simple association of the Drive in the library to the SCSI device. This is required because the Drive and the Robotics can be on different SCSI buses or even on different SCSI Adapters. Note that this is a one time setup for a Library backup location.

A Robotics device can be configured using Robotics/Media Handler Setup dialog.



The various screen fields and their purpose are listed below.

Field	Description
Name	The friendly name of the backup location. Any valid character sequence up to 79 characters is acceptable. The name should be unique and you cannot specify the name of an existing backup location.
Inquiry	The device specific SCSI/IDE Inquiry string returned from the device. May be useful to find the firmware revision of the device etc.
Category	The category of the Backup Location. It will be Media Handler in this case.
Adapter	The name of the Adapter or SCSI Port. On Windows 2000, XP and Server 2003, it will give you the name of the SCSI miniport driver with a running serial number. On Windows NT 4.x, it will be of the form ScsiPortx, where x will be 0, 1, ...
SCSI ID	The SCSI ID or Drive number of the device.
SCSI LUN	The SCSI Lun of the device and it will be 0 for IDE devices.
Cleaning Tape Slot	Specify the Cleaning Tape Slot of the library, if any.
Drives	Lists all the drives in the library/changer. The Status of the drive is shown using a tape icon. The drives are listed numerically and by the allocated Association that you have set.

Pressing OK will save the Backup Location details. Pressing Help will invoke this topic.

IMPORTANT: In order to configure a Robotics device, the corresponding Library hardware should be connected and online.

Be sure to choose the correct drives for the hardware. CBMR cannot know which drives are associated with the Robotics.

Once a Robotics device is configured successfully, you have to create a Library backup location, which will use this Robotics device, during backup and other media operations. Refer to Library Backup Location Setup (page 139) for further details. A library backup location can only be created manually.

Library Backup Location Setup

A Library backup location in CBMR consists of a drive, a robotics and one or more slots. It may be all or part of a physical library or autochanger. Before setting up a library backup location, you must set up the individual components:

- setting up robotics (page 138) (not required for autochangers)
- setting up the SCSI drives (page 135)

Each library device consists of any number of available slots. Slots may not be shared between libraries, but drive devices can. For instance, if you have a library with a single drive and 20 slots, you could use the first 10 slots for Manufacturing backup and the next 10 slots for Marketing backup.

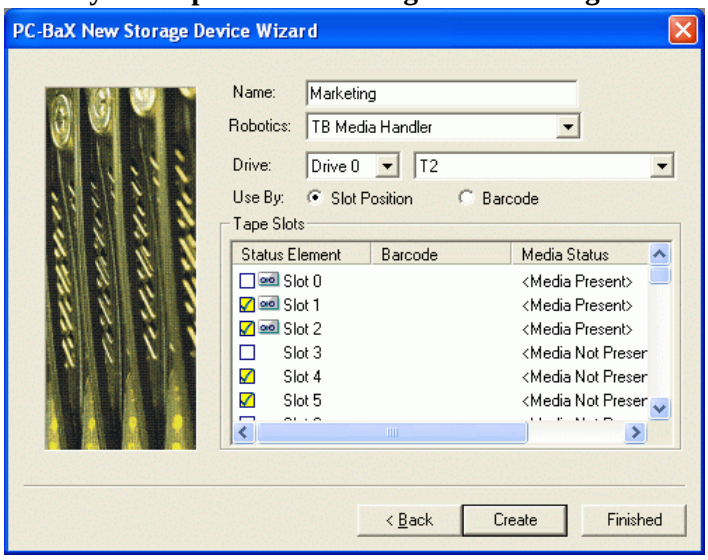
In this case you will create one backup location with name **Manufacturing** with slots 0 through 9 selected and another with name **Marketing** with slots 10 through 19 selected.

With a single device shared between two libraries, you cannot perform the Manufacturing and Marketing backups simultaneously. If you have two 2 drives available, each library could have its own drive, and they can be backed up in parallel.

The slots of a library device need not be contiguous. You can have slots 0, 2, 4, 5 etc. in a device configuration. In this case the backup will continue from Slot 0 to 2 etc.

You **must have media in all the selected slots** of a library device in order to use it.

Library Backup Location Configuration Dialog



This dialog allows you to configure the Library/Auto-loader backup location. You will specify the Elements or Slots, which will be used interchangeably in CBMR, in this dialog.

You have to enter a friendly and unique name to the Library configuration. Single click on the box next to the slot to include that slot with this library configuration.

It is possible to select or deselect multiple slots quickly by using the Ctrl and Shift keys while highlighting the rows. A single click on any box will then select or deselect the whole selection.

You must select at least one slot for each library.

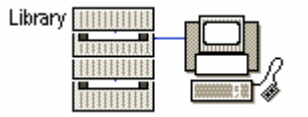
The screen fields are as follows:

Field	Description
Name	The friendly name of the backup location. Any valid character sequence up to 79 characters is acceptable. The name should be unique and you cannot specify the name of an existing backup location.
Robotics	Gives you a list of all configured Robotics devices. Select the Robotics you want to use with this definition. Changing the Robotics automatically displays the Drive and Slots of the selection.
Drive	The available drives in the Robotics will be listed here. Select the drive you want to use with this Backup Location definition.
Use by: Slot Position	When "Use by Slot Position" is selected the Media is shown ordered by Slot number. The bar code associated with each media is also shown.
Use by: Barcode	When "Use by Barcode" is selected the Media is shown ordered by Barcode. The Barcodes order can be changed by dragging and dropping the Barcodes into the required positions.
Tape Slots	Gives you a list of all available Tape slots within the library. It also displays whether a media is present in the slot, the barcode of the media, if your device supports one. Click on the box on the left of the element to select or deselect it. You must have at least one element selected in order to use the library.

Pressing OK will save the Backup Location and Cancel will discard the changes you have made. Pressing Help will display this topic.

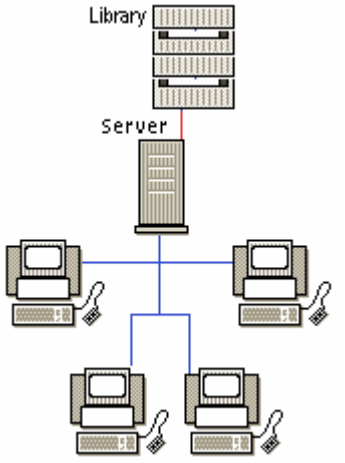
Library Backup Location examples

Isolated tape library example



This simple system consists of a workstation connected to a local tape library. The library consists of two SCSI drives and a robotic media handler

Simple tape library network example



This simple system consists of four workstations connected to a server. The server is connected to a local 10-slot tape library.

You could either:

- User Cristie Storage Manager to make the tape library accessible across the whole network. You could then create a separate library device for each workstation (using a dedicated tape slot), and back the workstation up to that device. The procedure would then be the same as backing up to an isolated tape library (page 141)

  or

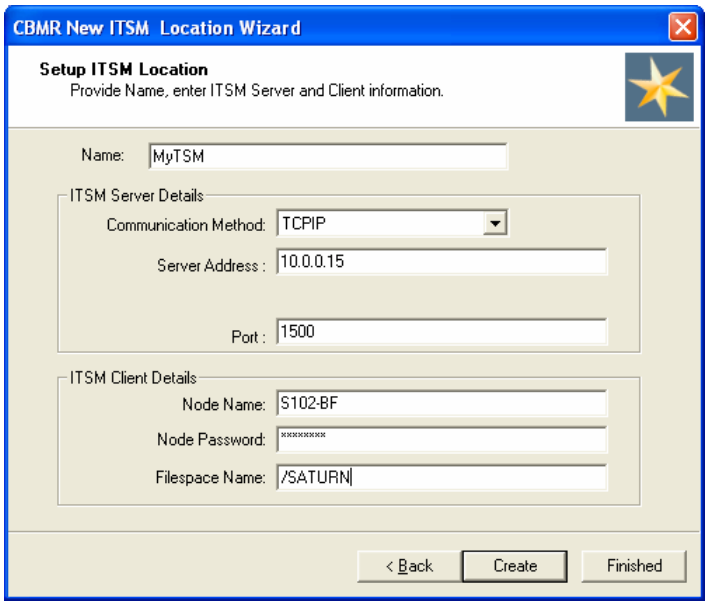
- Back the workstations up to the server (as in the simple network example) and then back the server up to the tape library (as in the isolated tape library example (page 141)).

In this case you could either:

- Create a single library backup location for the tape library and then back the server up to it.
- Create separate library backup locations for each workstation and the server in the tape library, and then back the appropriate areas of the server to the specified library backup location.

TSM Backup Location Setup

CBMR TSM Backup Location Setup dialog will enable you to define the TSM client options that CBMR should use to access the TSM server.



The various values which you can set using this dialog are listed below:

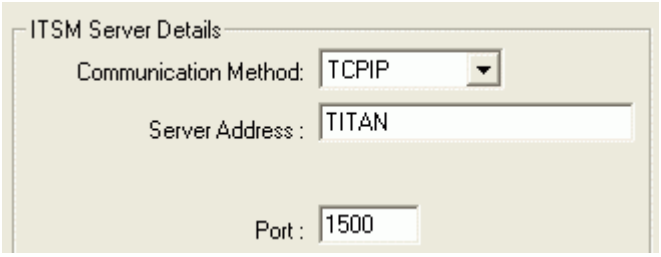
Field	Description
Name	The friendly name of the backup location. Any valid character sequence up to 79 characters is acceptable. The name should be unique and you cannot specify the name of an existing backup location.

TSM Server Details:

Here is where you specify the communication method to be used to access the TSM server. The displayed options correspond to the currently supported options by the TSM server. The possible value combinations are listed below:

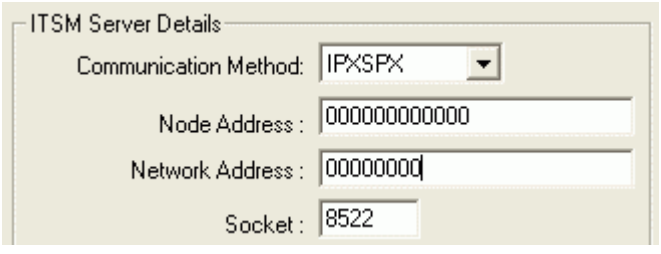
Communication Method	The method of communication to use. The possible selections are : TCPIP - to use TCP/IP IPXSPX - to use IPX/SPX NETBIOS - to use NetBIOS NAMEDPIPE - to use Named Pipes

TCPIP:



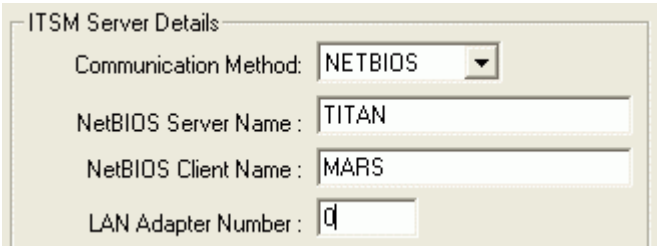
Server Address	The host name of the TSM server or the IP address in dotted decimal form.
Port	The TCP port at which the TSM server is listening for client requests.

IPXSPX:



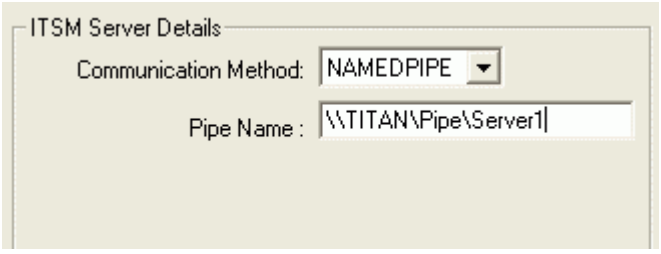
Node Address	Enter the IPX/SPX node address for the TSM server.
Network Address	Enter the IPX/SPX network address for the TSM server.
Socket	Enter the socket number for the TSM server.

NETBIOS:



NetBIOS Server Name	Enter the NetBIOS server name for the ITSM server.
NetBIOS Client Name	Enter the TSM client name.
LAN Adapter Number	Enter the LAN adapter number.

8.1.4 NAMEDPIPE:



Name Pipe Name	Enter the Named Pipes server pipe name.

TSM Client Details:

Here is where you will specify the name of the client node which will be used by CBMR. The node might have a password associated with it. You will also enter the name of the filespace to use. The filespace name must start with a '/'. If you haven't specified a '/' it will be added automatically.

If only single version DR backups are going to be used, the client node should be created before using TSM Administrator utilities and it must have the Backup Delete Allowed and Archive Delete Allowed set to Yes.

If backup versions are going to be used, the Node Policy domain used must be configured to use a 'versioning' copy policy.

Node Name	Enter the node name which must have been created prior to invoking this dialog.
Node Password	Enter the node password, if any. Leave it blank for no password.
Filespace Name	Enter the name of the filespace which should start with /. If this doesn't exist before, it will be registered.

Once a TSM backup location is successfully created, try to create a new header using the media utilities. If it succeeds, congratulations and your location is ready to go. If it fails, the appropriate message will tell you what is wrong.

Setting Up a Versioning Node

To set up a TSM Node to allow multiple versions of the a DR backup to be stored, follow the following steps:

1 Define a Management Class (MC), which contains a Backup Copy Group (BCG) and an Archive Copy Group (ACG).

2 Register your node needs to be registered to use the MC.

The parameters of the BCG to be considered are

- Versions Data Exists 2
- Versions Data Deleted 1
- Retain Extra Versions 30
- Retain Only Version 60

In this example, there can be 2 versions of an object. If there is more than one version and you've deleted one of them, then the deleted one will be kept for 30 days, the only remaining copy of the object will be retained for 60 days (AFTER you make it inactive).

These parameters should be set according to your preferred use of TSM.

Set a Default Backup Location

You can make any backup location the default location which will be used in Backup/Restore/Compare/Verify jobs. The Executive window Restore, Compare and Verify always use the default backup location.

1 Select a backup location.

2 Select Set as Default Backup Location from the Location top bar menu (or right mouse context menu).

The new default will be reflected in the *Backup Location* page of the Default Settings dialog.

NOTE: Individual backup selection scripts can be configured to use the default backup location. By changing the default location, individual scripts will use the new location without the need to edit individual scripts.

Deleting a Backup Location

Highlight the location to be deleted in the Backup Locations dialog, and press the <Delete> key on your keyboard. Alternately you can use the Delete menu option from the Backup Location menu.

You will be prompted to confirm the delete operation. It is possible to delete multiple locations by selecting several locations using the Shift and Ctrl keys while making the selection.

Viewing Existing Backup Location Settings

Highlight the location from the Backup Location dialog.

1 Either select the Settings option from the Backup Location menu or double click the corresponding entry.

This will bring the corresponding setup dialog where you can view and edit the parameters.

8.1.5 Setting up CBMR for Routine Operations

Although CBMR is designed to offer a high degree of flexibility and ease of use there may be times when you just want to configure the software to run simple routine backups with the minimum of user intervention. This section summarises the steps you can take to achieve this.

CBMR provides a number of features that should enable you to set up the system in the way that best suits you.

Scheduling routine backups

Adding jobs to the Scheduler list is an easy way of automating DR backup. The CBMR Scheduler offers a comprehensive time/date setup and the choice of running with Backup Selection scripts or for even greater flexibility, command files.

Customising the User Interface

You can simplify the appearance of CBMR by hiding some of the options, for example, *Backup Locations* and *Default Settings* in the Configuration drop-down menu. The pcbax.ini file can be edited to remove any of the main window objects. The list of variables in the pcbax.ini file controls what appears on the CBMR launch panel. All the variable names are relevant to their function so it is easy to decide which you need to change if required.

To hide an object, set the appropriate '*Showxxx*' value to zero. For example, to hide the *Backup Locations* object, set

ShowBackupLocations = 0

8.2 Introduction to Backing up Data

The purpose of a backup is:

- to minimise the effect of lost data be it due to human error or machine error
- maintain an archive copy.

One of the main tasks in creating a backup is ensuring that there is an up-to-date copy of all data. This does not mean backing up every file every time. Although a complete and full backup is necessary, in between times a selective backup is enough to ensure that all data is secure up to the last backup.

Backing up your data using CBMR is very easy

- Create some Backup Selection scripts to cover the routine jobs such as a full weekly backup, a daily incremental backup and so on.
- Pick the appropriate Backup Selection script and set the Backup in motion.

You can also set up the Scheduler to run the jobs automatically at the set times.

8.2.1 Introduction to Backup Schedules and Backup Selection Scripts

Backup Schedules and Selection scripts are used to define a set of instructions relating to a Backup. The scripts contain the data tagged for backup, the rules to follow during the operation, and header information. Existing scripts can be viewed, modified or deleted as requirements change. The scripts can be temporary and used for a one off job, or can be saved and used as and when required. Once saved you can view, modify or delete them as your requirements change.

Once you have established some backup routines and know what you need to backup and when, it is a good idea to create a range of scripts covering all the routine backup jobs.

CBMR is supplied with a pre-defined script called 'Backup all files on system [Boot] drive'.

From the main Backup Schedules drop-down menu you can change the View (icons, list or details display) and Sort by name/date. Also, from the Jobs menu you can perform all the routine tasks such as Modify an existing schedule, Run a selected schedule, Delete a schedule, create a new schedule (Create New) and access the Default Settings.

If the Details view is displayed you can also sort the entries in Description, File Name or Date/Time sequence by clicking in the appropriate column heading.

Creating a Backup Schedule

To create a new DR backup schedule/script, select the Run or Schedule Disaster Recovery Backup option from the main menu.

- from the Tool top bar menu in the Backup Selections tool

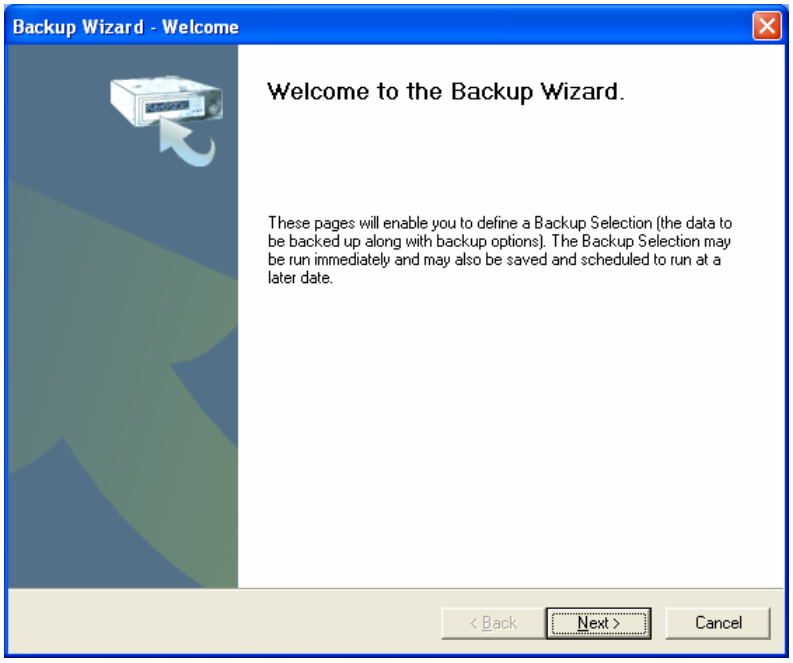
  or

- double click the Create New icon in the Backup Schedules drop-down menu.

  or

- double click the Backup Now option in the Tools drop-down menu.

Any one of these methods will invoke the Backup wizard. This will take you through the steps required to create the new Backup Selection script.



Viewing Existing Backup Selection Scripts

To display existing Backup Selection scripts, click on the Backup Selection button on the toolbar or select Backup Selections from the Tools top menu.

The View top bar menu provides different display options. Large/Small icons, a List or a Detailed view. The Details View provides some extra information about the scripts. It details the name (the entry in the *Description* line), the filename (the entry in the *File* line) and the date/time created.

The Sort top bar menu allows you to arrange the scripts in alphabetic sequence (Sort by Name) or in date sequence (Sort by Date). When in Details view, you can also sort the scripts by clicking in the column headings.

The Script top bar menu contains all the operations you might perform on a script. For example, Modify, Delete, Create New.

There is a pre-defined script supplied with CBMR called 'Backup all files on system [Boot] drive' (filename - system.scp). When you run this script the system identifies which drive the Operating System was booted from and backs up all the files on that drive. This means that, should there be a need to recover the system you have a copy of all your system files.

Modifying an Existing Selection Script

1. Open the Backup Selections tool
2. Double-click the script you want to change or highlight it (single-click) and select Modify from the Script top bar menu.
3. Make the changes to the selections (file changes/Backup options etc.).
4. Select Save from the top bar menu and press OK to close the script window.
5. If you decide you do not want to save the changes you have just made then press Cancel button.

Deleting a Backup Selection Script

1 Open the Backup Selections tool.

2 Highlight the Backup Selection script you want to remove (single mouse click on the relevant script).

3 Select Delete from the Backup Selection Scripts top bar menu or press the Delete key.

Backup Selection Script Properties

The Backup Selection Script property sheet allows you to define all the details which should apply for this particular backup. You can create as many different backup scripts as you need to cover all backup situations.

8.2.2 Running a Backup Using an Existing Selection Script

From the Backup Selections tool you can highlight a script and select Run from the Script top bar menu.

or

Double click on the script to view/modify it and then press the Backup button.

or

From the CBMR tool select Backup Using Existing Script from the Tool top bar menu. This will open the Backup Selections tool. Double-clicking on a script will then run it. Once the script has finished, the Backup Selections tool will also close.

When editing a Backup Selection script, the Estimate button (which also available from the Tool top bar menu) will estimate the size of the backup you have defined: the number of files and the size in Bytes). This could be useful if you need to know in advance how much capacity you require for this backup or estimate how long the job will take to run.

The Backup Status window displays a running report on how the backup is progressing. The information is divided into three headings:

Media Details - shows the header information.

Current File - details of the file currently being written to the backup.

Progress - how many files have been backed up, time taken and so on.

8.2.3 Dataset Settings

A dataset is created for each drive that is backed up on the volume. If you do not provide dataset header settings, CBMR will automatically assign the drive letter as the default header.

(In the CBMR Enterprise Edition, the default header is the UNC path.)

You can password protect a dataset. This provides increased security of data BUT make sure you can remember the password. You will be prompted for the password at any future access. There is no bypass procedure and if the password is lost or forgotten, the data will be inaccessible.

When you do a Restore, Compare or Verify, CBMR displays the first dataset. Any remaining ones are listed when you select Next or All.

Dataset Details

Select the Settings button under *Dataset* on the right of the window, the Dataset Info dialog is displayed. (The Dataset Info option in the top bar Select window performs the same function.) Notice that the selected drive is identified in the window banner.

Name	Type a name to identify the dataset or accept the default name (drive name)
Comment	The field allows for a brief description of the backup.
Password	The data can be made more secure by attaching a password to it. Always choose a password which you can remember easily. See note below.
Save Security Info	You can accept the <Use default>, that is the value define in Default Settings or select Yes/No which will apply to this backup script only. If Save Security Info is enabled then all the security details are included in the backup in addition to the data. This option is only applicable if you have the appropriate user account *'Rights'* to back up security information.

NOTE: A Password is a useful security measure but you should be aware of the implications. If a backup is password protected then the password will be requested before the data can be accessed. If you forget the password then there is no by-pass procedure and the data will be lost.

Estimate Backup Size window

The Estimate Backup Size option in the Selections top bar menu displays a window containing an estimate the size of the backup you have defined (the number of files and the size in Bytes). This could be useful if you need to know in advance how much capacity you require for this backup or estimate how long the job will take to run.

8.2.4 Specifying a Backup Catalogue Entry

Before you create a backup you need to specify a level of information to be recorded in the catalogue.

There is a *Backup Catalogue* page in the Default Settings properties. From here you can specify just how much information you want to store or indeed if you want the backup added to the catalogue.

There are four levels of information (Brief, Partial, Full, None). There is a trade-off of space versus level of information. There is no typical setting; which level you use depends on your own requirements. You can change the level at any time if you change your mind about how much information you need to keep.

You can either change the default setting or modify a particular Backup Selection script which will then apply from the next backup or you can modify the Catalogue information level from within the Backup Catalogue window.

Brief	Volume and Dataset headers. This is a minimal level of information and takes up little space.
Partial	Volume, Dataset and Directory details.
Full	All the above plus File information. This will be significantly larger than Brief or Partial entries.
None	Select 'None' if you do not want this particular backup recorded in the catalogue.

8.2.5 CBMR Log Files Overview

Log files are a record of completed CBMR operations. You can check the content and determine whether the job was successful. A logfile can be a useful source of information if a problem occurs.

You can request a log file to be created during a Backup, Restore, Compare, Verify and by the Scheduler. The files are named according to the operation (Backup.log, Restore.log and so on) and stored in the CBMR directory. If a Backup.log, Restore.log etc. already exists then logging information is appended to the relevant file for each subsequent operation.

The file can grow rapidly. If you need to retain the information save it to a new name. (Save as... is available from the File menu (in Notepad) when you View the logfile.) If not, delete it and a new file will be created next time the operation is carried out.

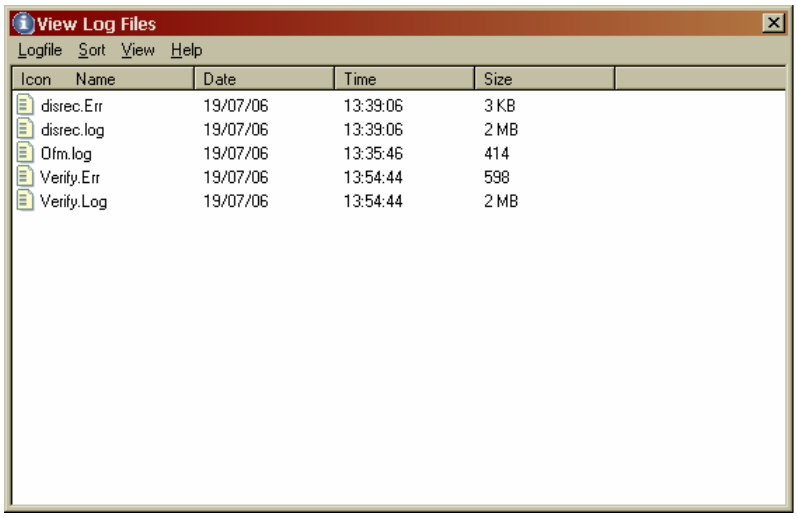
The View top bar menu allows you to control the log files display window. The files can be displayed as large/small icons, as a list or as a detailed listing which includes date, time and size details.

The Sort top bar menu allows you to sort the files in alphabetic sequence (Sort by Name), in date (Sort by Date) or in size sequence (Sort by Size).

NOTE: In the Details view you can click in the relevant column heading to sort the display in Name, Size or Date/Time sequence.

Managing Log Files

The View Log Files main menu option allows you to control the log files display window. The files can be displayed as large or small icons, a list or as a detailed listing which includes date, time and size details as shown in a sample screen below.



The Sort top bar menu options sorts the files in alphabetic sequence (Sort by Name), in date (Sort by Date) or in size sequence (Sort by Size).

NOTE: If the Details view is displayed you can also sort the entries in Name, Date, Time or Size sequence by clicking in the relevant column heading.

Default Settings for a Log File

Log Files are controlled from the Default Settings. Select the Default settings... option from the Logfile top bar menu. This takes you directly to the log file property page. You can request:

Full	Contains a complete file listing, errors (if any) and statistics.
Partial	Contains only errors and statistics.
None	No log file is created.

The default log file settings can be overridden by changing the *Logfile Setting*s from within a Backup Selection script's Backup Options page.

Viewing a Log File

- Highlight the relevant logfile in the Log Files window and select View Logfile from the Logfile top bar menu

  or

- Double click on the required logfile.

The logfile will be opened using the Windows Notepad application. If you want a printed copy of the file; select the Print file... option from the File menu (in Notepad).

Deleting a Log File

1 Open the Logfiles tool

2 Highlight the relevant logfile (single mouse click).

3 Select Delete from the Logfile top bar menu

You are prompted to confirm the delete action.

8.2.6 Start Backup

When you have defined the Backup Selection script you can run it immediately by selecting the Backup button.

The Backup Status window keeps you informed about how the backup is progressing.

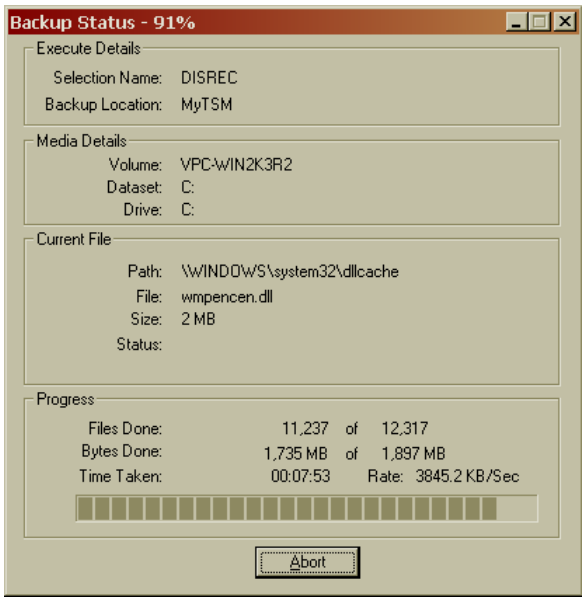
You will get a format warning message if the loaded tape has been recorded in a different format from CBMR. You are prompted to overwrite the tape Yes/No?

Select 'No' and the backup is aborted; select 'Yes' and the tape will be treated as a new piece of media (a new media header is created and existing data overwritten).

NOTE: There is an Estimate Backup Size option in the Selections top bar menu which will detail the size of the backup you have defined. This could be useful if you need to know in advance how much capacity you require for this backup.

Status Window

While a Backup (Restore, Compare or Verify) is running, a status window is displayed.



This displays:

Execute Details - Volume dataset name being recovered and the Backup Location name.

Media Details - shows the header information: Volume, Dataset and Drive.

Current File - details of the file currently being written to the backup.

Progress - a running count of files backed up, bytes done and time taken.

When the job is complete a statistics window is displayed which gives you an immediate report on the job.

The Detach button only appears on the Backup Status screen if the job has been initiated from the scheduler. Pressing the Detach button causes the job to run as a background process with no user console interaction.

If you want to attach to a job which is running in detached mode: run CBMR, open the CBMR Backup Schedules tool, select the 'running job' and select Attach from the Jobs top bar menu (or double click the 'running' job) to open the Backup Status window.

8.2.7 Aborting a Backup

If you need to stop the backup there is an Abort option in the CBMR Backup Status window (the window displayed when the backup starts running) which allows you to stop the operation. However, CBMR begins to process the first command it receives, which is Start, before it receives and can process the Abort command and as a result the header details are written before the operation stops. If the backup selections script requests overwrite rather than append then existing data will be overwritten.

8.2.8 Verify and Compare

Restore, Verify and Compare are related functions which use a common interface. These commands are accessible from the Tools drop-down menu.

Verify and/or Compare should be run after every backup to make sure that the tape is in good condition, the read/write heads are clean and the data has been reliably recorded.

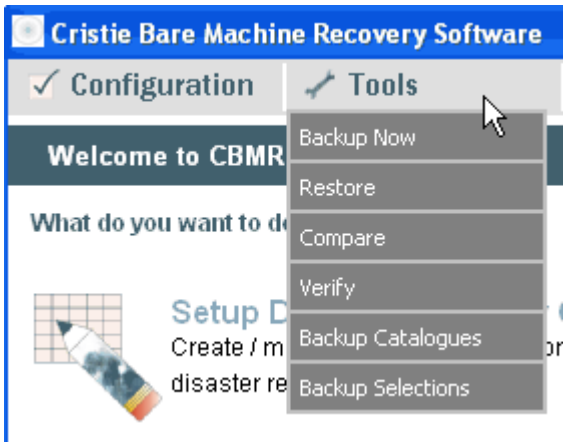
Verify checks that the data can be read back from tape, it will not check the data for accuracy.

Compare checks for data accuracy. The program performs a byte by byte comparison of the backed up data on the tape with the source data on disk. For this reason it will take considerably longer to complete than a Verify.

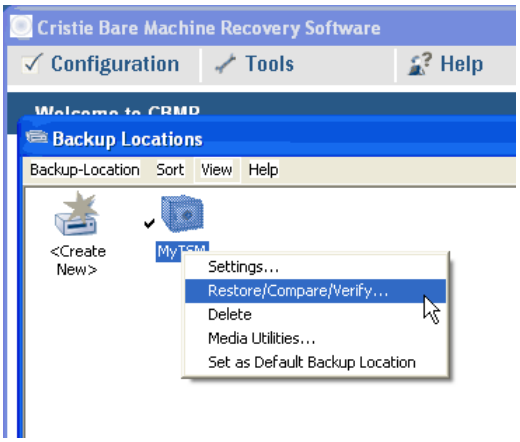
You are recommended to run both programs when you use CBMR for the first time, to ensure that the software and the Backup Location storage devices are working correctly.

Verify and Compare Programs

The Restore, Verify and Compare programs can be run from the CBMR Tools drop-down menu (click the Restore, Verify or Compare icon)



or from the Locations top bar menu in the Configuration *Backup Locations* option.



If running from the drop-down Tools menu, the first step is to choose whether to access the data via the Backup Catalogue or directly via the Backup Location.

If you are checking the backup immediately after it has completed then you will probably access the data via the Backup Location. If you want to check an earlier backup and you are not sure where the data is located then using the Backup Catalogue is the quickest option.

Verify and Compare dialog

The Compare and Verify programs each present a similar screen display. The window opens with the top level tape icon and first dataset displayed. The other screen features are described below.

The Scan options are used to scan the tape and display each dataset in turn. Each time you click on the Next button the next dataset on the tape is displayed until no more datasets are found. Alternatively, you can display the complete structure in one step by selecting All.

You can confirm the tape that is loaded by checking the media header details. Highlight the top level (root) tape icon and select the Show details... button. Similarly, pressing the Show details... button when a dataset is selected will display the dataset header details.

You can also display Header details by double clicking on the root icon (Media header) or individual datasets (Dataset header).

Tag or untag files and directories as required.

To begin a Restore, Verify or Compare operation, click the appropriate button at the top of the window.

CBMR displays a progress report and will warn you if any problems occur. The window title reflects which program is running (*Restore, Compare Status* or *Verify Status*).

A Statistics window is displayed when the job is completed. This information is written to the relevant log file (restore.log, compare.log or verify.log) if one has been requested.

Redirecting files has no purpose in a VERIFY or COMPARE job.

Introduction to Compare

Compare is different from Verify in that it performs a byte by byte comparison of the backed up data on the tape with the source data. For this reason it will take considerably longer to complete.

You are recommended to run Compare:

1 When you first use CBMR to do a backup, to ensure that the software and the Backup Locations are all working correctly.

2 Periodically to ensure the continued accuracy of your backups.

Introduction to Verify

It is good sense to verify your data after a backup to ensure that it can be restored. Verify checks the data for readability; it does not guarantee its accuracy.

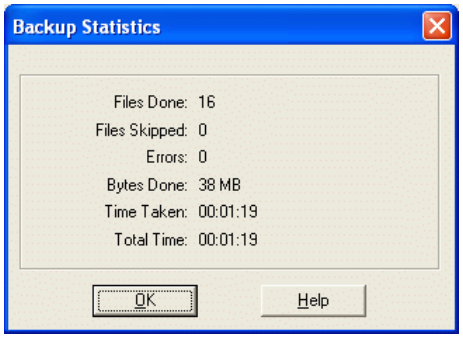
Verify should be run after every backup to make sure that the tape is in good condition and the read/write heads are clean.

You are recommended to run Verify :

1 When you first use CBMR to do a backup, to ensure that the software and the Backup Locations are all working correctly.

2 Periodically to ensure the continued accuracy of your backups.

8.2.9 Statistics Report



When a backup job is completed, a Statistics window is displayed which gives you an immediate report on how many files have been backed up, skipped, errors encountered (if any) and so on. These statistics will be written to the relevant log file (provided a log file has been requested in the Default Settings). For example, backup.log for a Backup job, restore.log for a Restore job).

8.3 Restoring Files - General

Maintaining an efficient backup routine is useless unless the data can be restored correctly. A restore routine for day to day files plus for disaster recovery situations is just as important as a backup routine. You are recommended to run practice restores to a spare drive to ensure that you are confident using the Restore program BEFORE you need to do it in a 'real' situation. Also it is good sense to run restores periodically to check that data is being correctly restored without errors. It is possible for hardware errors to occur which are not immediately obvious but which may corrupt the data.

Restoring data means that files are written from the backup media to the disk.

There are a number of ways of restoring files:

- The Restore Wizard can be run by selecting Restore from the Tools menu. This will guide you through the restore process.
- The media in a specific Backup Location can be browsed by highlighting it in the Backup Locations Tool and selecting Restore / Compare / Verify. Data can then be selected and restored.
- A Backup Catalogue Volume can be browsed by highlighting it in the Backup Catalogue Tool and selecting Open from the top menu bar.

8.3.1 Restoring From the Backup Catalogue

If you click on Use Backup Catalogue then the screen displays a listing of the Backup Catalogue contents.

Use the Backup Catalogue options to view the catalogue information and make your selection.

Before the operation takes place CBMR checks the Backup Location and the media header selected from the Catalogue against the connected location and the loaded media. If either items conflict then an error message is displayed and you are prompted to correct the situation.

Please refer to the section on Restoring Registry Files (page 158).

8.4 Windows Registry - General

The registry is a hierarchical structured collection of settings that control the operation of virtually all of the components within a Windows system. This includes the operating system, applications and user preferences.

It is very important that you make regular backups of the registry and understand how to restore it should a disaster occur.

Important notes

1. To backup or restore the registry you must be logged on to the system as a user with *Administrator Rights*.
2. After restoring the registry there are some files in the \pcbax\temp directory on the system drive which will be locked and cannot be deleted. However, after the system is rebooted the registry replacement takes effect and these files can be deleted. It is now safe to delete all the files in the \pcbax\temp directory.
3. If you do not specify the Restore Registry option then none of the active registry files will be restored and a 'File is locked' warning will be issued for each file. Enabling the Restore Registry option informs CBMR to replace the existing registry files and causes it to perform special processing on these files.

4 A full backup of the system drive will also contain the registry files (assuming the user had sufficient *Right*s for this). The important point here is that if you wish to restore an entire system drive but do not want the registry to be restored then this is possible by tagging all files but not selecting the Restore Registry option. Likewise, if you do want all files and the registry restored, tag all files and select the Restore Registry option - there is no need to restore the registry dataset separately.

5 The dataset containing the registry files is a standard dataset containing ordinary file images. The registry is not backed up as any special data type. This is done to facilitate disaster recovery operations and also to allow advanced users to be able to restore individual user profiles.

8.4.1 Structure of the Registry

The registry is composed of many files and the names of these are dependent on the version of operating system that is running.

Most of the files are normally located within the system32\config directory below the main Windows System directory.

User Profiles

User profiles are automatically mapped to the registry when a user logs on to the system. At this point the file(s) that hold the user profile information are locked and become unavailable for normal file backup. Active user profiles can only be accessed using the registry API functions.

8.4.2 How it is backed up?

CBMR provides the user with a simple and easy to use method of backing up the registry files by showing the registry as a separate resource that can be selected along with the available drives.

If this resource is selected a separate dataset will be created containing all of the files that comprise the registry. In addition all user profiles are backed up into this dataset, this includes both active and inactive profiles.

8.4.3 Restoring

Restoring the registry needs to be given careful consideration because any changes that have been made since the registry was backed up will be lost. For example, any application installed since the backup will no longer be known to the system.

If it is necessary to restore a registry, for example due to a registry corruption, the following steps should be taken:

1 Tag all files in the registry dataset containing the most recent copy of the registry.

2 Ensure that the Restore Registry option is checked in the Restore Options dialog. (Restore Options button in the Restore window.)

3 Start the restore.

4 When the restore has completed the system MUST be rebooted to enable the registry change to take effect.

The reason for having a Restore Registry option that must be used in addition to selecting the data, is to force a separate and specific request to restore the registry. This prevents an accidental restore which is an irreversible process that may have severe consequences.

8.5 Scheduler Overview

The CBMR Scheduled Jobs tool allows you to set up jobs to run automatically and is a trouble free way of maintaining your Backup regime. Once you have defined the jobs (...what needs to be backed up and when) and added them to the jobs list the scheduler will simply carry on and do the work without further intervention from you.

The CBMR Scheduled Jobs tool does not require any complex command statements; the property pages provide an easy to use interface enabling you to create new jobs and add them to the jobs list, update jobs or remove out-of-date jobs.

CBMR can use its own scheduling service or the Task Scheduler service provided with Windows. Which service is used depends on an option in the Scheduler page of the Default Settings tool. The service that CBMR is using will affect the dialogs and wizards that are presented to create and edit scheduled jobs.

The Windows Task Scheduler allows more flexible schedules to be set up (for instance 'every 10 minutes from 09:00 for 1 hour every Mon, Wed of every 2 weeks"). However, Windows Task Scheduler is not integrated as tightly into CBMR.

NOTE: To configure which scheduling service is used by CBMR, go to the Scheduler page of the Default Settings menu option.

8.5.1 Multiple Backups

You can easily maintain a daily, weekly and monthly backup routine by creating a job for each backup and adding it to the schedule list.

You can use the same Backup Selection script or command file for several jobs but each must have different time/date parameters. CBMR will not allow two jobs of the same specification to be created.

8.5.2 Operating the Scheduler

The Scheduler tool is accessed by:

Selecting the Backup Schedules menu option on the main CBMR Toolbar

or

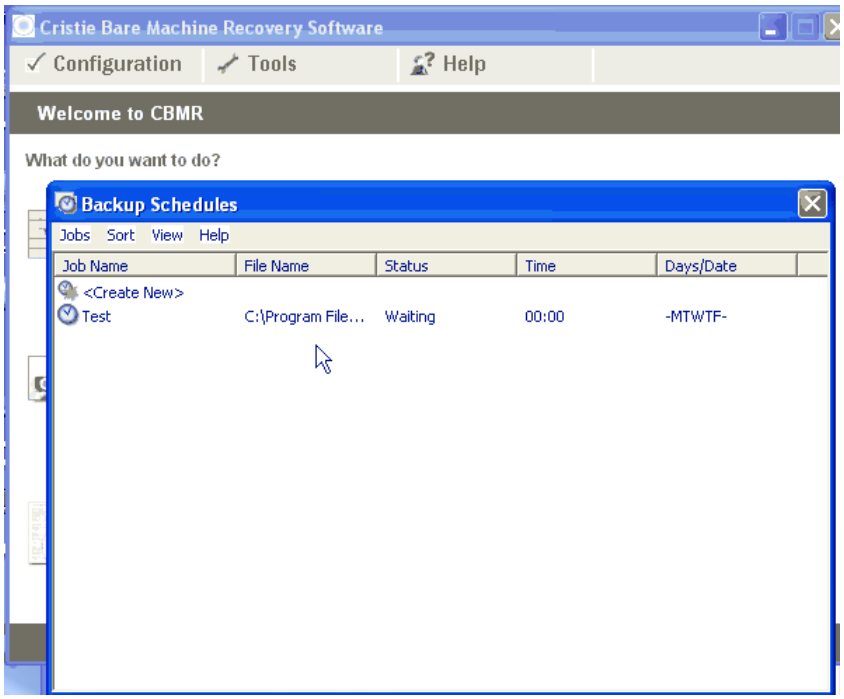
1 selecting the Backup Schedules option from the Configuration menu

The CBMR Scheduler tool allows you to manage scheduled jobs. Jobs are scheduled either through the *CBMR Scheduler service* or the *Windows Task Scheduler service*. Which service is used is configured through the *Default Settings* tool. All scheduled jobs for the configured scheduler service are listed.

The top bar Jobs menu contains all the scheduler related tasks such as creating a job, modifying an existing job, putting a job on hold and attaching to a scheduled job.

Similar to other windows you can Sort the job list and change the View (large/small icons, a list or details). The Details view allows you to monitor the state of jobs. It shows you the most information about a job (status, run time and the Days/Date).

The icon representation will identify the status of a job. For example a scheduled job will have a plain clock icon, a running job will have a tick superimposed on the clock and a job requiring user intervention will have a warning symbol superimposed.



Scheduler Window

The Schedule dialog contains all the fields required to define a job to be scheduled to run at a particular time. This window may contain an existing schedule with all the fields defined or if you have selected the <Create New Job> icon (or the Create New option in the Jobs menu/context menu) the fields will be blank.

If the Scheduler tool is using the Windows Task Scheduler service, then the Schedule dialog will be a property sheet with 3 pages. The first page details the job that will be run, the second page details the times that the job will be run and the third page details various advanced settings such as how long the job will be allowed to run.

NOTE: To configure which scheduling service is used by CBMR, go to the Scheduler page of the Default Settings tool.

8.5.3 Creating a New Scheduled Job

1 Click on Run or Schedule Disaster Recovery option on the main menu (or select Backup Schedules from the Configuration drop-down menu).

2 Double click on the 'Create New Job' icon in the Scheduler tool or New Job from the Jobs top bar menu.


<Create New>

3 If the Scheduled Jobs tool is using the CBMR Scheduler service, then the Schedule dialog will be displayed. Enter the job details and press the OK button. The new job will be added to the schedule list.

The Scheduler dialog contains all the details you need to define for a job to be scheduled to run at a particular time. This window may contain a schedule which you may want to modify or the details are blank when you select the <Create New Job> icon (or the *Create New* option in the Jobs menu/context menu).

1 If the Scheduled Jobs tool is using the Windows task Scheduler service, the the New Task wizard will be displayed. Enter the required details on each page of the wizard. The new job will be added to the schedule list.

NOTE: To configure which scheduling service is used, go to the Scheduler page of the Default Settings tool.

Program Title

Enter a descriptive name for the job. This name will appear in the job list.

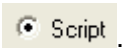
Program

You can choose to run a job with a Backup Selection script file or a command file. CBMR works quite happily with both so it is a matter of what best suits your way of working.

Type the full path and script name or command file name.

If you are not sure what to enter in this field, use the Find... button to select a script or to locate and specify a command file.

Using a Backup Selection script

To use a script, select the Script radio button 

. Pressing the Find... option displays a list of available scripts.

Using a command file

There are some benefits in using a command file. For example, you could include several scripts which would run one after the other (as opposed to using the script file option where only one job can run at a time).

To use a command file, select the Cmd file radio button 

. Pressing the Find... option with the command file option opens the 'Select File To Run' window. From here locate the command file and select the Open button.

Day/Date To Run Program

In this section of the window you can set when you want the job to run. There are several options you can set here.

'Weekdays' (Monday to Friday are ticked in the list)

'All days' (Sunday through to Saturday is ticked)

A job can be run on a weekly basis. For example, to run a job every Thursday, tick the Thursday box, set the time option and set the Repeat option (box ticked).

A job can be run on a monthly basis. For example, you could select Monday and Monthly plus the Time setting and set the Repeat option (box ticked). This means that the job would run on the first Monday of the month at the time set. (In actual fact the program runs on the first Monday it encounters. So, if your machine was switched off over the first two weeks of the month the job would then run on the first Monday encountered after you switch it back on.)

A job can be set to run on a particular date. When the Date box is ticked press the Set... button to display the calendar. Select the date you require, the current date is the default. The arrows at the top of the calendar allow you to change Month and Year.

> changes the month forward >> changes the year forward

< changes the month backward << changes the year backward

If the Repeat box is checked when a Date is set, the date automatically increments to the next day after the job has run.

Time To Run Program

The time is set by selecting the up/down arrows next to the Hour and Minute boxes.

Options

You can run a job on a regular basis by setting the Repeat option (the box is ticked when active). When this box is ticked, the job will be repeated until you cancel the Repeat option. For example, if a job is scheduled to run on Monday at 8.0am then, with the Repeat option set, this job will run every Monday at 8.0am until you cancel the Repeat setting.

If the Repeat option is not checked for a particular job then the job will disappear from the scheduled jobs list after it has run.

Run Detached

You can run a job as a background process while you continue to work in other applications. When the Run detached button is ticked the job will run as a detached process.

8.5.4 Attaching/Detaching Jobs

If you want to check on the progress of a scheduled job which is running, selecting the Attach option from the Jobs top bar menu (or double clicking on the tape icon) will open the Backup Status window.

Pressing the Detach button in the status window returns you to the Scheduler jobs window.

8.5.5 Changing an Existing Job

1 Click on the Configuration *Backup Schedules* drop-down menu option.

2 Open the job details by double clicking the relevant job or select Open from the Jobs top bar menu.

3 Make the appropriate changes to the job details and press the OK button.

Putting a Job on Hold

You may need to hold back a routine backup, for example, people are working late and you don't want the backup to run until everyone has finished with the system.

1 Select one or more jobs in the Scheduled Jobs tool.

2 Select Hold\Selected from the Jobs top bar menu. You can also apply 'hold' to all jobs by selecting Hold\All.

The job(s) will not run until released.

The icon representation will change to identify the status of the job

If a detailed view of the Scheduled Jobs tool is displayed (View / Details) you will see the job status (Held, Waiting or Running).

Releasing a 'Held' Job

1 Select the job(s) that are on hold.

If you display the detailed view of the Scheduled Jobs tool (View / Details) you will see exactly what status each job is at (Held, Waiting or Running).

2 Select Release\Selected from the Jobs top bar menu. You can also apply 'Release' to all jobs by selecting Release\All.

Deleting a Job

1 Select job(s) from the scheduled jobs list.

2 Select Delete Selected from the Jobs top bar menu. You are prompted to confirm the delete action.

Running a Job Immediately

If you need to run an ad hoc job or test a job you have set up then select the Run option and the job will run straight away. This will not affect any time/date parameters that you have already defined. If you have set the job to run nightly at 10 o'clock, it will still do so.

8.5.6 System dependent information

The Scheduler Service (Windows 2000/XP/2003 Only)

CBMR can schedule jobs to run with no user interaction. These jobs are configured to be executed by a special type of program known as a service. The main reason for this is to allow scheduled backups to run even when a user is not logged on to the system.

What are Windows Services ?

Windows 2000/XP/2003 services are a special class of program that are installed and controlled by the Windows Service Manager. The Service Manager can be accessed from the control panel allowing services to be started, stopped and also have their properties modified.

One of the most important points to remember is that services should not, and in most cases cannot, directly interact with the current users console.

CBMR can be configured to use one of two scheduling services: its own CBMR Scheduler Service or the Windows Task Scheduler Service. To select which service to use, go to the Scheduler page of the Default Settings tool.

CBMR Scheduler Service

The CBMR Scheduler service is automatically installed, if requested, during the CBMR installation process. By default it will log on to the system using a special account known as a 'Local System Account'. If required you may change the log on account name using the Service Control Manager, accessed using the Control Panel. One possible reason for this would be to control specific security issues that you may want to setup for a Backup Operator user or group and want the scheduler assigned to this profile.

As mentioned previously the scheduler will not normally interact with the current user console, however, if you particularly need this capability you can set the 'interact with desktop' setting for the service using the Service Control Manager. It must be noted, however, that this would not normally be done.

In order to view a scheduled backup, the CBMR command line program (pcbax.exe) provides an option (/d) that indicates to the program that it is running 'detached' and should communicate status information to an external program via a defined IPC (Inter Process Communication) mechanism rather than directly to the current console. The CBMR program will automatically add this parameter when scheduling a Backup Selection script.

When a backup is running with this option specified, it is possible to run CBMR and attach to this job (through the Scheduled Jobs tool) to view the status and provide any user interaction required.

After attaching to the job the status screen will be the same as for a backup that is run interactively from within CBMR.

Windows Scheduled Tasks Service

Microsoft Windows provides its own scheduling service, called the Windows Task Scheduler. CBMR jobs can be configured to run under the control of the Windows Task Scheduler. These jobs run in a similar manner to those running from the CBMR Scheduler service. However, they also require one more option (/ts:*JobName*) where JobName is the name of the Windows Task Scheduler job. Again, the CBMR program will automatically add this parameter when scheduling a scrip.

The Windows Scheduled Task Service has the advantage that much more flexible schedules can be created in it. However it is not as tightly integrated into CBMR as is CBMR's own scheduling service.

8.5.7 Using Batch Files (Windows 2000/XP/2003)

There are many occasions when other operations are required for a backup in addition to the actual backup process itself. For example, copying the log file to a specific location, parsing the log file, e-mailing status etc. When additional commands are required you can create a batch file to perform the backup job and specify this as the job to be run by the scheduler.

When running a batch file it is important to remember that if you want to attach to a running job to interact with it or view the status, you will need to specify the /d option as one of the parameters on the CBMR command line. In addition, if you are using the Windows Task Scheduler service instead of the CBMR Scheduler service, you must also specify the /ts:task.job option where task.job should be replaced with the name of the Windows Task Scheduler job.

For example to run a Backup Selection script called *weekly.scp* the following batch file could be used:

```
rem start of batch file
rem other commands can go here
rem remember the /d option to specify detached mode (and, if
rem using the Windows task scheduler, the /ts: option to
rem specify the task this batch file belongs to)!
pcbax weekly /b /d /ts:weekly.job
rem other commands can go here
rem end of batch file
```

Note: If you do not specify the /d option (and, if using the Windows Task Scheduler, /ts: option), or if you run a program other than pcbax.exe then you will not be able to attach to the job to view the status. The scheduler will run the program and will indicate that the program is waiting, running etc. from the job folder but attempting to attach to the job will result in an error indicating that CBMR was unable to attach to the job.

8.6 Backup Catalogue - General

A Backup Catalogue has two major advantages:

- It is quick and easy to locate data on a backup.
- It allows you to keep more information about a backup than is possible on the backup media and you have instant access to the contents of the selected volume.

Using the Backup Catalogue you can view any volume (Volume top bar menu) without having to connect a Backup Location or load the media. This can be a considerable time saver if you are searching for a directory or files and you are not sure on which volume they are stored (Search top bar menu), especially if you take into account a large organisation where there may be a large number of volumes retained.

The View top bar menu provides different display options. Large/Small icons, a List or a Detailed view. The Details View provides some extra information about the volume. It details the volume name, the date/time created, the tape format type (currently SDB) and an ID (this is a number assigned internally to the volume).

The Sort top bar menu allows you to arrange the catalogue entries in alphabetic sequence (Sort by Name) or in date sequence (Sort by Date).

NOTE: In the Details view you can also click in the relevant column heading to sort the entries in Name, Date or Time sequence.

The New option allows you to create a catalogue entry. For example, you may have some backup volumes for which no catalogue entry was created at the time of the backup.

The Backup Catalogue appears on the main CBMR Tools menu option.

8.6.1 Viewing the Catalogue Contents

You can access the Backup Catalogue contents either by selecting the Backup Catalogue icon or selecting Restore, Compare or Verify from the CBMR Tools menu and selecting the Use Backup Catalogue option.

At this point you have not committed to a particular volume or Backup Location, you are merely viewing the entries in the catalogue listing. Similar to other displays e.g. Backup Location scripts, the view can be as an Icon or a detailed listing (View top bar menu). The detail includes Volume name, date and time the backup was created and the format. The Details display can be sorted by Name, Date and Time.

8.6.2 Information stored about the backup

Each backup is stored as a volume. There is one volume available per media (tape, file etc), Details about the backup volume are stored as the Media Header. Access to a volume may be locked with a password

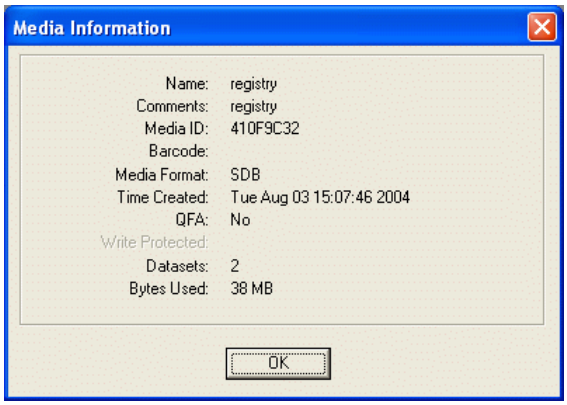
Each drive backed-up within a volume is known as a dataset. Details about the drive are stored as a Dataset Header. Access to a dataset may be locked by a password.

The Media and Dataset headers can be viewed through the Backup Catalogue. The amount of information about the files and directories stored within a dataset is defined when the backup is made.

Displaying Media Header Details

Select the Media Header... option from the top bar Backup Catalogue Volume menu.

The *Media Information* window shows all the available information for the selected volume.



Even if your volume is unnamed you will get other details such as the date and time created which may give you a clue as to which volume you need. However, it is recommended that all backups are given a meaningful name which provides an indication to the contents.

Name:	User-defined
Comments:	User-defined
Media ID	Set by system
Media Format	
Time created	Set by system
QFA	Quick file access. Defined by user at backup. Dependent on media
Write protected	Defined by media
Datasets	Number of datasets within volume
Bytes used	Size of backup in bytes

Show Dataset Details

The Dataset Header... option in the top bar Item menu provides detailed information about the selected dataset. The information should help you identify a backup and decide if it is the one you want.

Name:	User-defined
Comments:	User-defined
Time created	Set by system
Barcode:	(From barcode label on media)
Resource	
Compression:	Defined by user at backup
Software version:	CBMR software version used to create it
Size:	Size of backup in bytes
Catalogue Info level:	Set by user at backup
Backup Location:	Backup Location holding the backup datasets

8.6.3 Modifying the Level of Catalogue Information

You can change the level of information held by the Backup Catalogue. Select the Change Info Level option from the top bar Volume menu in the Backup Catalogue tool.

The Current Info Level: tells you the information level of the selected volume. (The 'Current Info Level:' will be 'None' if you are creating a new entry.)

If you want to down-grade the level of information, for example from 'Full Information' to 'Headers and Directories' or 'Headers Only' then just click on the required option. You are given the opportunity to cancel the action.

However, if you are up-grading the information level then you need the media loaded so that the relevant information can be read from the media and written to the catalogue entry. You will be prompted to select a Backup Location to use. When you select the Backup Location storage device to use for this operation, CBMR checks the location, compares the media header with the selected header in the catalogue entry and if correct proceeds with the upgrade. You will be prompted to connect the correct location or insert correct volume if either does not agree with your selection.

You are informed when the update is complete.

Select Required Info Level

You can choose to store any one of three levels of information. The current level will be 'None' if this is a new volume or, if you are modifying a Catalogue entry the existing level will be quoted (which of course could also be 'None' if that is what is defined in the backup selections script).

The levels of information are as follows;

'Headers Only' Volume and Dataset headers. This is a minimal level of information and takes up little space.

'Headers and Directories' Volume, Dataset and Directory details.

'Full Information' All the above plus File information. This will be significantly larger than Brief or Partial entries.

8.6.4 Creating a New Catalogue Volume

You can add new volumes to the Backup Catalogue. For example, if a backup job specified no entry in the Backup Catalogue at the time it was run or Backups which were created prior to using CBMR.

CBMR is compatible with Cristie's SDB Backup and Recovery Software.

1. Insert the media into the Backup Location storage device.
2. Select New from the top bar Backup Catalogue menu.
3. You are prompted to select a Backup Location storage device and define the level of information you wish to record.
4. Select OK when the operation is complete; the entry is added to the catalogue listing.

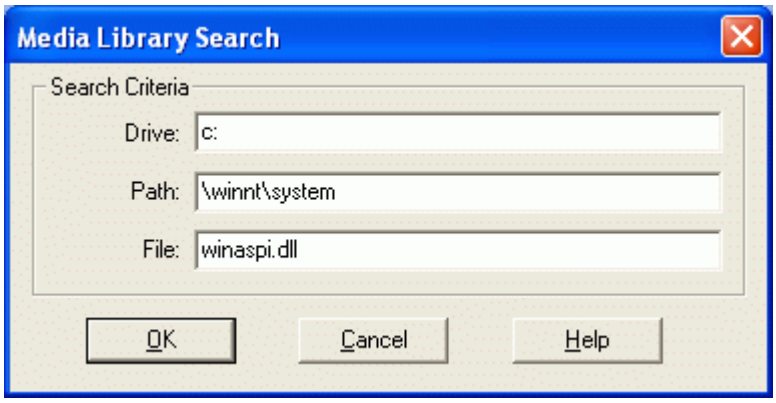
8.6.5 Deleting a Volume From the Catalogue

Select the Delete Selected Volumes option from the top bar Backup Catalogue Volume menu. You are given the opportunity to cancel the action or to continue. This is only deleting a catalogue entry and has no bearing on the actual data.

8.6.6 Searching the Backup Catalogue

Select the Backup Catalogue top bar Search option to display the search menu. You have the option of searching All Volumes or Selected Volumes. You can make a multiple selection by pressing the shift key while clicking on the each line in turn.

You must provide some parameters to direct the search; how specific you are refines or widens the search field.



If you do not supply a full path then all occurrences of the search object will be listed in time order with the most recent at the top of the list.

You can search for an individual file but obviously you must have the 'Full' level of information on this volume otherwise there will be no file details to search.

If you want to locate an individual file you must enter the full file name, wildcards (E.g. *. doc, pcbax.*) are not accepted.

8.6.7 Restoring Data via the Backup Catalogue

You can initiate a Restore, Compare or Verify operation from the Backup Catalogue Volume window by selecting Restore / Compare / Verify from the Volume top bar menu or by pressing the appropriate button.

You can also select Restore, Compare or Verify from the CBMR Tools menu which will start the Restore/Compare/Verify Wizard. This will give you the option of using the Backup Catalogue or the Backup Location to select the data you are interested in.

8.6.8 Backup Location Search

This window allows you to search the Backup Catalogue.

You can search for an individual file but obviously you must have the 'Full' level of information on this volume otherwise there will be no file details to search. Wildcards (E.g. *. doc, pcbax.*) are accepted.

If you do not supply a full path then all occurrences of the search object will be listed in time order with the most recent at the top of the list.

Backup Location Entry Information

This window displays information about the selected entry resulting from a search operation.

Details about the volume, the dataset and the specific entry are shown. This information is a useful checking option before you actually restore the data.

Backup Location Search Results

This window displays the results of the Search operation. Select View Information from the Options menu to display detailed information about the selected volume.

When you have found the data you want to restore you can set the Restore program in action using the Start option in the top bar Options menu.

8.6.9 Select Backup Location to Use

This window is displayed when you press the 'Select the Location to Use' button when updating the Catalogue information or when you want to create a new entry.

This window lists all the configured locations.

Select the Backup Location storage device currently connected to your system.

If you want to use a location which is not listed then you need to open the Backup Location (page 133)menu option and define its properties. The new location will be included in the list.

CBMR now checks the location, compares the media header with the selected header in the catalogue entry and if correct proceeds with the upgrade. You will be prompted to connect the correct location or insert correct volume if either does not agree with your selection.

Select the Location to Use for this Operation

This window prompts you to select a Backup Location to use. For example, if you are upgrading the catalogue information level then you need the original data loaded so that the relevant information can be read from the media and written to the catalogue entry. You are prompted to select :

the location used to write the data.

the location defined as the default.

pick one from the list of configured locations.

Both the original Backup Location and the default location will be identified below the relevant buttons.

CBMR now checks the location, compares the media header with the selected header in the catalogue entry and if correct proceeds with the upgrade. You will be prompted to connect the correct location or insert the correct volume if either does not agree with your selection.

8.7 Backup Strategy - General

Backing up data to a data cartridge is a convenient and secure means of ensuring vital information can be retrieved in the event of a disaster. A disaster in this instance does not necessarily mean a major earthquake or such like. Loss of data can be due to relatively common occurrences like accidental deletion, data corruption, software/hardware failure, power failure (even minimal) or theft of equipment. If you consider the effect of losing a complete weeks data or even a day or two then you can appreciate the importance of backing up your data. Also, most companies are legally required to keep data for a period of years and therefore an efficient archive and retrieval procedure releases expensive hard disk space for working data.

The backup routine you employ depends on several factors: how often does the data change, how valuable is the data (time and money invested in it), how much time can be allotted to carrying out the backup. Remember that the scheduling option in CBMR provides for unattended backups. There are several established backup strategies and you can use the one which suits your working practices best or use one as a basis for developing your own pattern.

Points to Consider

- Identify the backup needs of your company and create a suitable backup regime.
- Once established maintain the routine. (Make use of the CBMR automated routines.)
- Identify the backups with meaningful titles so that you can restore your files quickly and with the appropriate version of the data.
- Follow the maintenance procedures for your tapes and drive (tape storage, drive head cleaning etc.).
- Store tapes in a secure location and maintain copies off-site in case of theft, fire or flood damage.

8.7.1 Examples of Backup Routines

If you maintain efficient backup procedures you should always be able to recover any lost data with minimum effort whether it is due to external causes, a fatal malfunction during a backup or just a routine retrieval of archived data. Always use meaningful descriptive labels so that tapes can be identified quickly and without confusion. ('Fred's Backup' may not be very helpful when the system has crashed and an entire department want their data restored asap!)

There are three typical Backup routines described here but ultimately you need to instigate a routine which best suits your company requirements.

For specialist advice on backup strategies and how best to secure your data please contact Cristie Data Products.

8.7.2 Three Week Backup Cycle

The most basic backup provides three weeks of data.

On the first working day of the week, a complete backup of all files is carried out. On subsequent days of the working week, newly created files and modified files are backed up.

This procedure is followed for 3 weeks and on the fourth week the first weeks tapes are re-used, then the second weeks and so on in a continual cycle.

Reasonably small computer systems would allow the one full backup and four partial backups to be stored on one volume, therefore only requiring three volumes.

8.7.3 Twelve Week Backup Cycle

This backup regime allows you to recover data from up to 12 weeks ago. This pattern is more suitable for larger systems, for systems where there are frequent file changes or systems which require a longer data history.

Volumes should be labelled as follows:

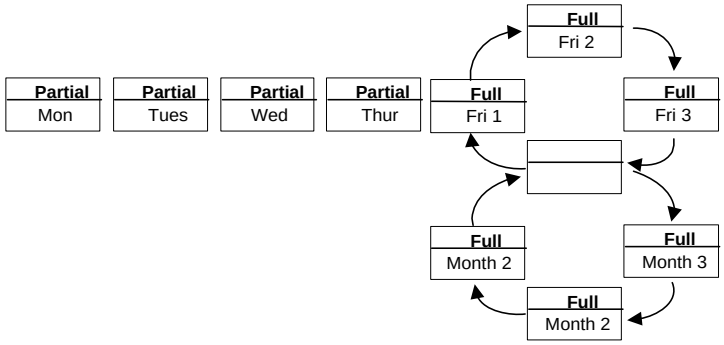
Monday, Tuesday, Wednesday, Thursday

Friday 1, Friday 2, Friday 3

Month 1, Month 2, Month 3

The Friday 1-3 and Month 1-3 volumes are used for full backups, the others for partial backups (new and modified files only). 'Month' is not strictly accurate; the volumes are used every four weeks.

The following diagram illustrates how the tapes are used:



Twelve Week Cycle

Again, depending on the amount of date to be backed up, this method can use as little as 10 volumes.

8.7.4 Three Year Archive

This is a comprehensive Backup cycle which will provide three years of data. A time span of this nature must be considered where legal requirement calls for data to be kept for a number of years, for example accounts information.

Each year, a full backup is taken of all data and archived.

Each month, a full backup is taken. The monthly tapes are re-used on the corresponding month of the following year.

A weekly backup is taken on an appointed day each week (typically the first working day). The weekly tapes are re-used on the corresponding weeks of the following month. (Again, the month is regarded as a four week cycle.)

Daily backups are taken and the tapes reused on corresponding days the following week.

The monthly, weekly and daily tapes should be kept in a fireproof safe. The yearly backup should be stored off-site.

You now have substantial coverage should you need to recover data. There is data for each individual day plus weekly and monthly and annual backups.

8.8 Running CBMR from the Command-line

CBMR can be run as a console based application using the program pcbax.exe.

In a command window change directory to where CBMR is located.

At the prompt, type: pcbax /? for a list of commands and description of usage.

Usage:

pcbax <script> <mode>[options] ....<script> (omit the .scp extension) is any Backup Selection script contained in the \pcbax\scripts directory

pcbax /ds:n [options] .... restores all files in dataset *n* where *n* is the number of the dataset. The first dataset is 0 and is the default if a number is not supplied. For example: pcbax /ds:2 Restores the files in the third dataset.

This provides a quick way to restore all the files within a dataset without needing to specify a Backup Selection script.

pcbax /cl:<media name> ....checks that the correct media is loaded in the Backup Location.

pcbax /cw .....checks if the media is write protected.

pcbax [<script>] /cmh .....creates a new header.

pcbax /sms .....shows media status.

pcbax /smh .....shows media header

<Modes> are:

/b Backup

/r Restore

/c Compare

/v Verify

[options] are:

/sd: <*device*> Where *device* is the name of the Backup Location storage device you wish to use to override the default location OR the location specified in the Backup Selections script.

/h Disables screen output.

/s shows statistics during backup in place of file names.

/p:<media password> This password overrides any script specified password.

/unload Unloads media at end of operation.

/registry Replaces registry files if found during restore.

/erase Performs a security erase on the media.

/retension Performs a retension operation on the supported location/media.

/initialise Performs a partition operation on the supported location/media.

8.8.1 pcbax.exe Command Line Options

CBMR can be run as a console based application using the program pcbax.exe.

In a command window change directory to where CBMR is located.

At the prompt, type: pcbax /? for a list of commands and description of usage.

8.8.2 Usage:

pcbax <script> <mode>[options] ....<script> (omit the .scp extension) is any Backup Selection script contained in the \pcbax\scripts directory

pcbax /ds:n [options] .... restores all files in dataset *n* where *n* is the number of the dataset. The first dataset is 0 and is the default if a number is not supplied. For example: pcbax /ds:2 Restores the files in the third dataset.

This provides a quick way to restore all the files within a dataset without needing to specify a Backup Selection script.

pcbax /cl:<media name> ....checks that the correct media is loaded in the Backup Location.

pcbax /cw .....checks if the media is write protected.

pcbax [<script>] /cmh .....creates a new header.

pcbax /sms .....shows media status.

pcbax /smh .....shows media header

pcbax [<script>] /scan .....scan media into library

<Modes> are:

/b Backup

/r Restore

/c Compare

/v Verify

[options] are:

/sd: <*device*> Where *device* is the name of the Backup Location storage device you wish to use to override the default location OR the location specified in the Backup Selections script.

/ver:<date> The backup version as of <date> to use where <date> should be in the form "DD/MM/YYYY-HH:MM:SS".

/h[s][q] Disables screen output except [s] - always show stats and [q] always show questions. If questions arise and /h is in effect, a USER ABORT is assumed.

/s shows statistics during backup in place of file names.

/p:<media password> This password overrides any script specified password.

/unload Unloads media at end of operation.

/registry Replaces registry files if found during restore.

/erase Performs a security erase on the media.

/retension Performs a retension operation on the supported location/media.

/initialise Performs a partition operation on the supported location/media.

/ts:<ScheduleName> identifies the Windows Scheduler task. If CBMR is being run from the Windows Scheduler as opposed to the CBMR Scheduler Service, then this parameter is required to enable the CBMR graphical user interface to communicate with the scheduled job while it is running. <ScheduleName> must be replaced with the exact name of the Windows Scheduler job (including the .job extension).

8.8.3 CBMRwin.exe Command Line Options

CBMRwin.exe is the graphical based application. You can run some command line options with the GUI version.

In a command window change directory to where CBMR is located.

At the prompt, type: CBMRwin /? for a list of commands and description of usage.

8.8.4 CBMRCfg.exe Command Line Options

This program allows the system configuration to be created on the command line.

In a command window change directory to where CBMR is located.

At the prompt, type: cbmrcfg.exe /? for a list of commands and description of usage.

Usage: CBMRCFG.EXE [options]

Options are:

/help or /? - Show usage

/sd {device} - Use device specified instead of the default device

/out {backup|<valid local or UNC path>} - Store configuration in this location

backup - Store the configuration with the backup

/volatile - Do not remember the changes. Changes will be remembered by default

/scripts - Creates the scripts DISREC.SCP and DISREST.SCP

Existing scripts will be always overwritten!

8.8.5 Information required to access the configuration share

/cfguser <login ID> - Enter as Domain\Username

/cfgpwd <password> - Password

8.8.6 Information required to access a file device

/devuser <login ID> - Enter as Domain\Username

/devpwd <password> - Password

8.8.7 CBMR Configuration Files

The following configuration files are used by the CBMR software.

PCBAX.INI

This file contains the name of the default Backup Manager to connect to (currently this can only be the local one). Also in this file are options to select the preferred user level (0 or 1) and options to disable any of the objects in the main container window.

CBM.INI

This file contains the default settings for the Backup Manager. These settings are maintained by the CBMR.exe program. The settings in this file are used by the CBMR.exe and pcbax.exe programs for Backup/Restore/Compare/Compare and Verify operations.

USERSHAR.INI

This is an editable text file is used to define user defined shares.

USERINFO.INI

This is an encrypted file containing user names and passwords.

DTEXC.INI

This is an editable text file which may be used to exclude any desktop resource by name.

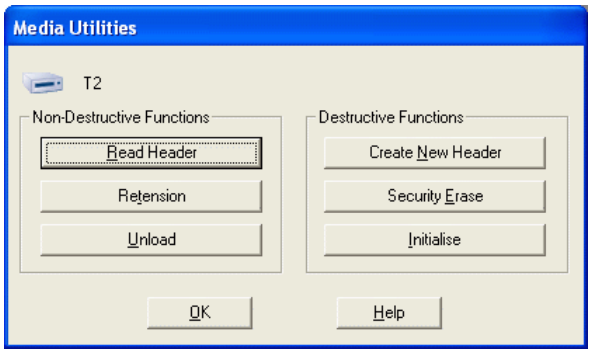
8.9 Media Utilities

CBMR provides a number of media maintenance utilities such as retensioning, initialising or erasing a tape.

Not all options are applicable to every Backup Location type; a message will be displayed if you select an option which is not relevant to the connected location.

Select the *Backup Locations* option from the Configuration drop down menu option in the CBMR main menu. Right-click on the Backup Location and select Media Utilities...

8.9.1 Media Management



The utilities in this window allow you to carry out maintenance tasks on the media. Notice that the utilities are divided into Non-Destructive and Destructive functions. The non-destructive functions do not have any affect on the data stored on the media. The destructive functions will destroy any data currently stored on the media.

The window is divided into two sections. These are *Non Destructive Functions,* which do not affect the data stored on tape, and *Destructive Functions* which will destroy the data. The connected location is identified in the top left hand corner of the window.

8.9.2 Non Destructive Functions

Read Header	CBMR scans the media and displays the header information.
Retension	Removes any slackness in the tape by fast forwarding to the end and rewinding back to the beginning.
Unload	Causes the media to be ejected when the backup is complete. Only applies to 'soft load' locations.

8.9.3 Destructive Functions

Create New Header	Creates a new media header for the volume currently loaded in the location. All existing data will be lost
Security Erase	Completely and irrevocably erase all data from the tape.
Initialise	Initialise prompts for a new media header and as far as the software is concerned this is now a new piece of media. This option only applies to DAT tapes and you will be advised of this if you use it on other formats.

8.9.4 Read Header

CBMR scans the media loaded in the connected Backup Location and displays the header information which was recorded during Backup. The information is for viewing only; you cannot add, delete or change any details.

8.9.5 Retension

This option is only applicable to magnetic tape media. When a tape is retensioned it simply means that it is wound from end to end and back to the beginning again in order to remove any slackness in the tape and ensures that it is evenly wound on the spool and will feed past the read and write heads smoothly.

A tape should be retensioned:

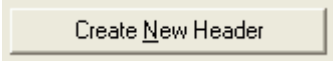
if it is new - This will ensure that any loose particles left from the manufacturing process are dislodged.

if left in storage for a period of time - When a tape is not used for a long time there is the possibility of print-through which means that the magnetic orientation of particles on one layer of tape affect those on the adjacent layer and so causing data corruption.

8.9.6 Unload

This option will eject the media from all 'soft load' Backup Locations such as DAT drives.

8.9.7 Create New Header



This option will allow you to create a new media header for the media currently loaded in the Backup Location. You can use this option to remove or change a password protected backup.

8.9.8 New Media Header

This window allows you to create a new Media Header for the media currently stored in the Backup Location.

Name - Enter a meaningful name which identifies the volume contents.

Comments - This field allows you to provide more information about the volume. It is not essential but can be useful if you are viewing a volume at a later date.

Password - A password will secure the volume against unauthorised access. Make sure it is a password you will remember at a later date because there is no by-pass procedure and the data will be unrecoverable if you cannot remember what the password is.

You have the opportunity to Cancel this operation if you change your mind.

8.9.9 Security Erase

Only use this option if you want to totally and irrevocably erase all data from the media. This may be required if the media contained highly sensitive information. This operation takes a considerable length of time to complete especially for high capacity media because data is erased byte by byte.

8.9.10 Initialise

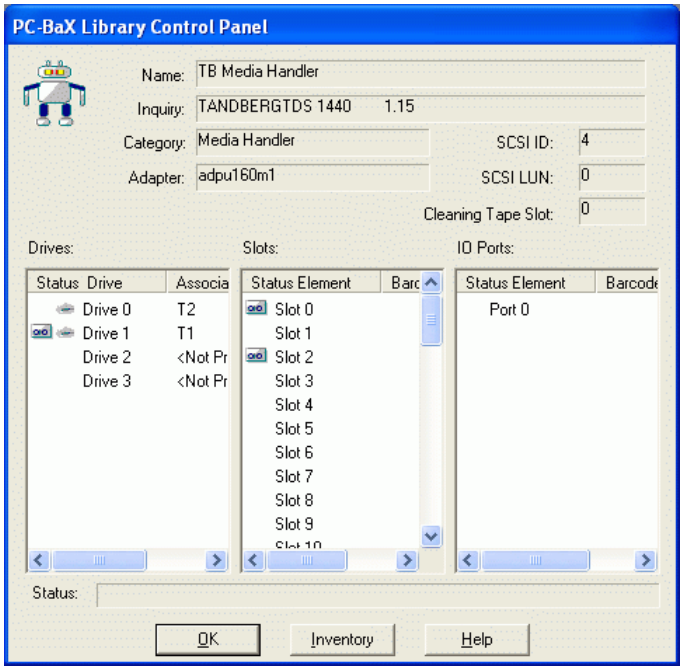
This option only applies to DAT tapes. You will be advised of this if you try to run it on other media types. When you initialise media you are prompted to enter a media header name and as far as the software is concerned this is now a new, blank piece of media.

You can use the Initialise utility to re-use old media where the stored data is no longer required.

8.9.11 Library Control Panel

CBMR Library Control Panel is an advanced utility for the tape library. Contrary to the notion of associating one drive for every logical library configuration, it is possible to work with the library as a whole and it gives a birds-eye view of the total inventory. If the media are fitted with barcodes and the library is capable of reading them, you will know exactly where each media is. It is also possible to import and export media on the fly, without even opening the library door!

This can be invoked by selecting the Media Utilities menu option for a Media Handler device.



The presence of a tape icon in the drive status indicates that there is a media in that location.

The Media Handler/Robotics device must have been configured earlier, i.e. SCSI devices are associated with its drives.

Importing Media

To import media to an empty slot or an empty drive, click an IO port slot using the left mouse button and drag it to the desired drive, holding the left mouse button. The valid locations which can accept a media will be highlighted automatically. Once you have highlighted the desired drive or slot, release the left mouse button.

If there is already a media in the IO port it will be moved to the specified drive or slot. If there is no media in the IO port, it will be extended and wait for a media to be placed. The default timeout is 20 seconds. Once a media is placed, it will be moved to the specified location. An inventory will be performed.

Exporting Media

Media from drives and slots can be exported by dragging them and dropping in one of the IO ports. The IO port will be extended and wait for about 20 seconds. After that the IO port will be retracted and an inventory will be done.

Inventory

An inventory can be done by pressing the [Inventory] button. After an inventory operation, the drives, slots and IO ports on screen will reflect the exact status as seen by CBMR.

9 Glossary of Terms

Adapter definition

An adapter is required to provide a connection between the computer and the device. This may be the parallel adapter which normally connects the printer to the computer in which case the printer is attached to the back of the drive. Alternatively, the drive may be connected to an adapter card or ASPI.

Archive bit

The archive bit is automatically set by the operating system whenever a file is created or modified. If the 'Reset Archive Bit' option is enabled then the flag is cleared when the file is backed up. It will be set again by the operating system when the file is next modified.

ASPI

ASPI (Advanced SCSI Programming Interface) is a standard SCSI software interface linking host adapters to SCSI device drivers. ASPI allows multiple devices to be connected to the one host adapter. This keeps costs down and frees up internal slots.

Backup Selections (Scripts) Definition

A list of drives, folder and files to be backed up or restored. Held in a 'script' file for repeated use.

The list may include or exclude certain selections. The selection script file also contains encrypted passwords for volume header and datasets. CBMR is provided with a standard script for performing a full DR backup called CBMR.SCP.

CBMR

The Cristie Bare Machine Recovery product.

Compression

Almost all data exhibits redundancy in the form of repetition. Redundancy of this sort when transferring data is purely wasteful. Data compression is a means of reducing this waste.

Data compression allows the drive to store more data on the same length of tape. In ideal conditions the ratio can be as much as 2:1 or higher.

Data compression also aids performance in that it allows the drive to match the performance of higher transfer rate systems more closely.

Data compression can be performed in 2 ways.

Hardware compression is performed by the backup hardware, this takes the load off the PC but still requires the whole uncompressed data to be transferred over the interface to the backup location.

Software compression is performed by the PC before sending the data to the backup location. This puts extra overhead on the PC in order to compress the data, but it provides less data be transferred over the interface to the backup location.

Dataset header

Each drive backed up is contained in its own dataset on the backup media. The dataset header is information written at the beginning of the backup.

Driver

A device driver is a program which allows a device to communicate with the operating system. Each device must have the correct driver installed to allow the device to operate.

Domains

In the Windows NT environment a domain is a collection of computers which share a common domain database and security policy. The domain name is a unique name by which the domain is known to the network.

DR (Disaster Recovery)

A reference to Disaster Recovery. Also considered to be an abbreviation for the Cristie Disaster Recovery software.

Locked Files

You can have a situation where a backup is halted because a locked or open file has been encountered. Locked or open files are files which are being used by another application at the time the backup is taking place. CBMR cannot back up these files unless the Open File Module (OFM) is installed or VSS is used on Windows XP/2003 systems. If you are not using the OFM then it is good practice to close down other Windows applications during a backup. OFM is only required for Windows 2000 systems.

Media header

Information written at the beginning of the media. E.g. Name, Date and Time created, whether the data is password protected. This information may be useful at a much later date if you are trying to locate a backup.

Open File Module (OFM) for CBMR

For Windows 2000 systems, OFM (Open File Module) allows for the safe backup of files that are used by other applications like email and database servers. On Windows 2000 CBMR includes OFM by default and no additional configuration is necessary for this. For Windows XP/2003 systems the VSS open file manager is used instead. VSS is provided by Microsoft as an integral part of these Operating Systems.

PC-BaX

The Backup and Recovery Software from Cristie, which forms the backup/restore engine of CBMR.

QFA

Quick File Access (QFA) is a facility on some tape drives which enables rapid access to files during Restore. The tape is divided into two areas: a catalog area and a data area. The catalog area at the start of the volume stores directory information which points to the data area where the actual data is stored. During Restore the program locates the file entry in the catalog and goes straight to the correct point in the data section.

During backup the directory catalog is written first therefore in a situation where a backup extends over multiple tapes the first tape (containing the directory catalog) must be used to start a Restore.

SCSI ID

Each SCSI device on the chain must have a unique address which the system uses to communicate with that device. The address is represented by the SCSI ID number. The SCSI ID also determines priority when two or more devices attempt to use the bus at the same time.

Volume Shadow Copy Service (VSS)

The Volume Shadow Copy Service provides the backup infrastructure for the Microsoft Windows XP and Microsoft Windows Server 2003 operating systems, as well as a mechanism for creating consistent point-in-time copies of data known as shadow copies. CBMR makes use of this technology.

Windows Pre-Installation Environment (WinPE)

The Microsoft Windows Pre-installation Environment (Windows PE or WinPE) is a powerful replacement for the Microsoft MS-DOS operating system in OS deployment processes, test and diagnostic tools development, and system recovery processes. Windows PE is a minimal Windows system that provides limited services based on the Windows XP Professional and the Windows Server 2003 kernels. It also provides the minimal set of features required to run Windows Setup, access and install operating systems from the network, script basic repetitive tasks, and validate hardware.

Cristie is fully licensed by Microsoft to deploy its DR console software based upon Windows PE.

10 Index

A

B

C

D

E

S

T

U

V

W