



PBMR for Windows

User Guide

Version 9.7.1 | July 2026

Contents

1. Legal	2
2. About this guide	3
2.1. Before you start	3
2.2. Backup process	4
2.3. Recovery process	4
3. Create the Bootable Recovery Environment	5
4. The PBMR Configuration Tool	6
4.1. Creating the configuration information	7
4.2. Backup of boot and hard-link files	8
4.3. Creating a PBMRcfg pre-script	8
5. Disaster Recovery Using PowerProtect Backup	11
6. Multi-Factor Authentication (MFA)	12
7. Restoring a System	13
7.1. File-Based recoveries	13
7.1.1. Booting the recovery environment	13
7.2. Begin the restore process	14
7.2.1. PBMR recovery environment main menu	15
7.2.2. Log file save path	17
7.2.3. Specify recovery details	18
7.2.4. Confirm volume layout	20
7.2.5. Select volumes to restore	21
7.2.6. Clone settings	22
7.2.7. Dissimilar hardware	23
7.2.8. Disk recovery status	24
7.2.9. Disk scaling	26
7.3. Recovery Environment Tools	27
7.3.1. Dissimilar hardware wizard	29
7.3.2. Load a driver	32
7.3.3. Copy log files	33
7.3.3.1. View logs	34
7.4. Configure Network	35
7.4.1. Configure NIC parameters	35
7.4.2. Assign static or DHCP IP settings	37
7.4.3. Map a network device	38
7.4.4. Unmap a network drive	39
7.4.5. Configure DNS servers	40
7.4.6. Configure network identification	41
7.5. Configure routing	42
7.5.1. IPv4 routes	42
7.5.2. Diagnostics	44
7.5.3. Reboot	45
7.5.4. Active Directory recoveries	46
7.6. Appendices	47
7.6.1. Storage space support	47
7.6.2. BIOS to UEFI conversion	48
8. Cristie Technical Support	50

Legal

Copyright © 2018–2026 Cristie Software Ltd. All rights reserved.

This software contains proprietary information belonging to Cristie Software Ltd. and is supplied under a licence agreement that restricts its use and disclosure. It is protected by copyright and other intellectual property laws. Reverse engineering, decompilation, or disassembly of the software is prohibited except where expressly permitted by applicable law.

The information contained in this document is subject to change without notice. While every effort has been made to ensure its accuracy, Cristie Software Ltd. makes no warranties, express or implied, regarding the completeness or accuracy of this document.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means - electronic, mechanical, photocopying, recording, or otherwise - without the prior written permission of Cristie Software Ltd.

Trademarks

The following are trademarks or registered trademarks of their respective owners:

- IBM Tivoli Storage Manager (TSM), AIX, and Tivoli - IBM Corporation
- IBM Storage Protect - IBM Corporation
- IBM Virtual I/O Server (VIOS) - IBM Corporation
- NetWorker and Avamar - Dell EMC
- vSphere, vCenter, and vCloud - VMware, Inc.
- Hyper-V and Azure - Microsoft Corporation
- Amazon Web Services (AWS) and Amazon Elastic Compute Cloud (EC2) - Amazon.com, Inc.
- Cohesity DataProtect - Cohesity, Inc.
- Rubrik - Rubrik, Inc.
- CloneManager® - Cristie Software Ltd.
- SysBack® - Cristie Software Ltd.
- Cristie Software Ltd. trademarks
- FSBlocker® - Cristie Software Ltd.
- PowerProtect Data Manager - Dell Technologies

PC-BaX, UBax, Cristie P4VM (Protect for VMs), Cristie Storage Manager (CSM), SDB, ABMR (Bare Machine Recovery for EMC Avamar), NBMR (Bare Machine Recovery for EMC NetWorker), TBMR (Bare Machine Recovery for Spectrum Protect/TSM), CBMR (Cristie Bare Machine Recovery), CoBMR (Bare Machine Recovery for Cohesity DataProtect), RBMR (Bare Machine Recovery for Rubrik), and CRISP (Cristie Recovery ISO Producer), PBMR (Bare Machine Recovery for Dell PowerProtect Data Manager)

About This Guide

This guide describes the key components of **Bare Machine Recovery for Dell PowerProtect Data Manager (PBMR)** and the disaster recovery process used to restore protected **Windows systems**. It provides instructions for **installing, configuring, and using PBMR**, together with reference information and advanced recovery procedures.

The procedures in this guide are based on **PBMR version 9.7.1**.

Before you start

To ensure that you can successfully recover a system, verify that the following prerequisites have been met before creating a backup:

- **PBMR** is **installed** on the protected system.
- `PBMRCfg.exe` has been run to generate the PBMR configuration.
- The generated PBMR configuration is included in a subsequent backup.
- A file-based backup is configured and completed.
- Compatible recovery media has been created and is available for use.
- Consult the [Cristie Product Support Matrix](#) to verify that your environment is supported before proceeding.

Volume Shadow Copy Service (VSS)

Enable **Windows Volume Shadow Copy Service (VSS)** for all volumes included in the backup.

VSS allows files that are open or in use at the time of backup to be captured consistently by the **PowerProtect Data Manager** backup process. This helps ensure that operating system files, application data, and other locked files are protected successfully.

By default, the **PowerProtect Data Manager backup** client enables VSS for:

- System State
- System Services

Depending on the applications being protected, additional VSS configuration may be required to ensure application data is backed up consistently.

Backup process

PBMR enables **bare machine recovery** directly from a **PowerProtect Data Manager**.

Before a recovery can be performed, the protected system must be prepared for recovery. This process consists of:

1. Install the required **PowerProtect Data Manager** and **PBMR components**.
2. **Run** `PBMRCfg.exe`
3. Create **bootable recovery media** using **CRISP**.
4. Perform **regular PowerProtect Data Manager backups**.

Once these steps have been completed, the system is ready to be recovered using the PBMR recovery environment.

The following chapters describe each stage of the preparation process in more detail.

Recovery process

In the event of a system failure, **PBMR** allows a protected system to be restored directly from a **PowerProtect Data Manager backup**.

Recovery is performed using a bootable WinPE-based recovery environment created with the **Cristie Recovery ISO Producer (CRISP)**.

The recovery environment can be:

- booted from USB media
- booted from CD/DVD media
- mounted directly within a virtual environment

The recovery process consists of five main stages:

1. Load the **PBMR configuration**.
2. Rebuild the **target storage layout**.
3. Restore operating system and application data from a **PowerProtect Data Manager backup**.
4. Perform **Dissimilar Hardware Recovery (DHR)**, if required.
5. **Boot** into the **recovered system**.

The following chapters describe each stage of the recovery process in more detail.

Create the Bootable Recovery Environment

The **PBMR** recovery environment is created using the **Cristie Recovery ISO Producer (CRISP)**.

CRISP generates a customised Windows Pre-installation Environment (WinPE) recovery image that is used to boot the target system and perform the recovery process.

WinPE Version Selection

CRISP supports the following WinPE environments:

- WinPE 10

CRISP Requirements

CRISP must be installed together with the appropriate **PBMR WinPE fileset** on the same host system.

A compatible **64-bit PowerProtect Data Manager** client installation package (.exe) must also be provided during the recovery media creation process.

For example:

PBMR-9.7.1.54181-for-PowerProtect20.1.0.0-pe10

Note:

- Only 64-bit PowerProtect Data Manager clients are supported.
- Recovery media must be created using the same PowerProtect Data Manager backup client version that was used to create the backup.

For example, backups created using PowerProtect Data Manager backup client version **20.1**, should be recovered using media created with the same client version.

CRISP can generate recovery media in the following formats:

- bootable ISO image
- bootable USB device

The generated media can be:

- written to CD/DVD media
- mounted directly in a virtual machine
- used to boot a physical system

Once booted, the recovery environment guides the recovery process.

Additional Options

Microsoft PowerShell can be included within the recovery environment if required.

This option must be selected when creating the recovery media.

For detailed instructions on installing and using CRISP, refer to the CRISP User Guide.

The PBMR Configuration Tool

The PBMRCfg utility collects and stores the system configuration information required during a PBMR recovery.

This information includes:

- disk and storage configuration
- operating system details
- storage controller information
- network adapter configuration
- network settings

The generated configuration is used during the recovery process to recreate the original system layout before data is restored.

Configuration Storage Location

Configuration information is stored by default in the following location:

```
C:\PBMRCFG
```

This location cannot be changed.

Running PBMRCfg

PBMRCfg (PBMRCfg.exe) is installed as part of the PBMR software and is typically located in:

```
C:\Program Files\Cristie\PBMR
```

The utility is a command-line tool and should be run as part of a **PowerProtect Data Manager** pre-backup script to ensure the configuration remains up to date.

Licensing

PBMR includes a 30-day trial period.

A valid BMR licence is required to continue using the utility after the trial period expires.

Logging

The result of each configuration capture is recorded in the **Windows Application Event Log**.

The following sections describe the configuration process in more detail.

Creating the configuration information

An initial PBMR configuration is created automatically during installation.

If required, you can create or update the configuration manually using the **Create Default Configuration** shortcut provided with PBMR. This creates a configuration using the default settings.

For advanced configuration options, run `PBMRCfg.exe` from a command prompt.

To display the available command-line options, run:

```
PBMRCfg.exe /?
```

or

```
PBMRCfg.exe /help
```

Format Additional Volumes During Recovery

By default, PBMR only marks the Windows volume for formatting during recovery.

If Windows is installed on a partition other than the first partition on the disk, both the boot partition and Windows partition are configured for formatting automatically.

Additional volumes can be specified using the `/format` option.

To format specific volumes during recovery:

```
PBMRCfg.exe /format D,E,F
```

To format all volumes on the system:

```
PBMRCfg.exe /format all
```

Volumes mounted to folders can also be specified:

```
PBMRCfg.exe /format D:\MountedVolume
```

For example:

```
PBMRCfg.exe /format D,D:\MountedVolume
```

Note:

Regardless of the configuration settings, the recovery environment allows partitions and volumes to be selected manually during the recovery process.

Configuration Storage

The generated configuration is stored in:

```
%SystemDrive%\PBMRCFG
```

This location **cannot** be changed.

Best Practice

The **PBMR configuration** should be updated before each **PowerProtect Data Manager backup**.

Cristie recommends running `PBMRCfg.exe` using the PowerProtect Data Manager **pre-script** feature available within the **protection** job's **Options** settings.

Backup of boot and hard-link files

Certain files required for system recovery are not included in the standard **PowerProtect Data Manager backup dataset**.

These include:

- boot files
- file hard-link objects

These components are essential for a successful bare machine recovery and must be captured separately.

Handling Locked Files

Some of these files may be in use when the backup runs and cannot be copied using standard file-based methods.

To ensure they are captured correctly, PBMRCfg.exe uses the **Windows Volume Shadow Copy Service** (VSS) to create a snapshot of the system. The required recovery files are then collected from the snapshot and included as part of the PBMR configuration data.

Procedure

1. From the Windows menu, search and select, **Create Default Configuration**.

```
=====
PBMR Configuration Utility Version 9.7 for x64
Copyright (C) 2009-2026 Cristie Software Limited
=====

Copying the EFI files ...
Successfully copied the EFI files
Created a snapshot of C:\ --> E:\
Searching for files missed under C:\Users ...
Searching for files missed under C:\Windows\ServiceProfiles ...
Searching for files missed under C:\Windows\WinSxS ...
Successfully copied the missed assembly directory
Searching for files missed under C:\Windows\System32 ...
Saving hard-link information ...
... progress 0%
```

Creating a PBMRCfg pre-script

PBMRCfg.exe can be configured to run automatically before a **PowerProtect Data Manager backup**.

Generating a fresh configuration ensures the recovery information remains up to date and reflects any changes to:

- disk configuration
- operating system updates
- hardware configuration

Configuring the pre-script consists of two steps:

1. Create the **script** on the **protected system**.
2. Adding the **script** to the PowerProtect Data Manager.
3. Assigning the **script** to a **protection policy**.

Procedure

Step 1: Create the script file

1. Open Notepad (Run as Administrator).
2. Paste the single-line command below:

```
@cd "%ProgramFiles%\Cristie\PBMR" && PBMRCfg.exe
```

3. Save the file as cristiePBMR.bat

Step 2: Add script to PowerProtect Data Manager

1. In **PowerProtect Data Manager**, navigate to **Protection** and select **Scripts**.

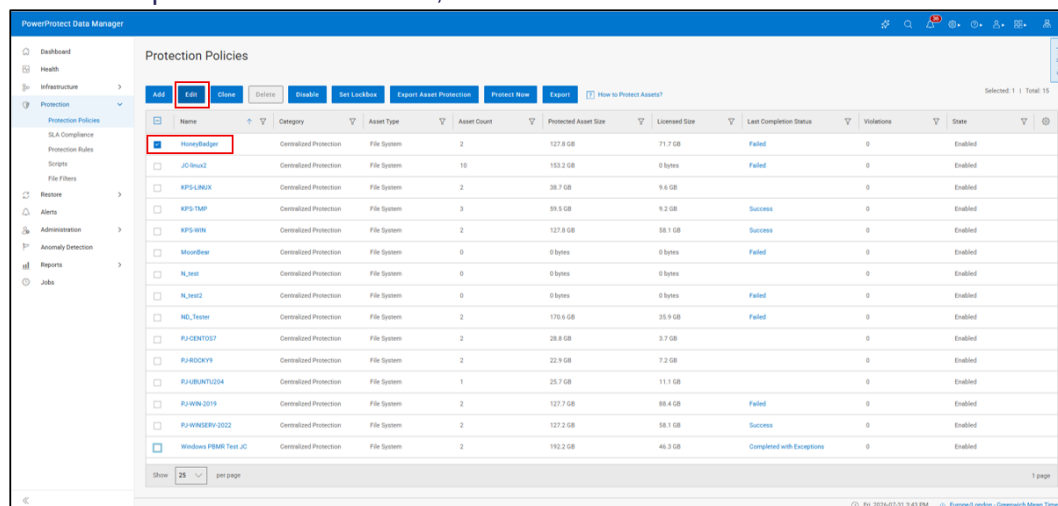


2. Click **Add**.
3. In the **Add Script** window click **Upload Script**.
4. **Navigate** and **select** the required **script**.
5. Enter the following details:
 - **Name:** Name of the script (it must be unique)
 - **Type:** Pre or Post script
 - **Compatibility:** Windows or Linux
 - **Description:** Brief description of what the script does (optional)
6. Click **Save**.

 A screenshot of the 'Add Script' dialog box. It includes an 'Upload Script' button, a text box for the script content, and fields for Name, Type, Compatibility, and Description. The 'Script Parameters' section is also visible, with an 'Add Parameter' button. The script content area shows 'PowerProtect Data Manager' on line 1.

Step 3: Assign script to protection policy

1. Within the **PowerProtect Data Manager** navigate to **Protection** and select **Protection Policies**.
2. Tick the required **Protection Job**, then click **Edit**.



3. Navigate to **Pre/Post-Script**.
4. Click **Add Script**, select the **uploaded script** from the list, then click **Apply**.
5. You now need to **configure the Timeout**.

Depending on the system configuration, PBMRcf g may take several minutes to complete, particularly on systems with large numbers of disks or complex storage layouts. Increase the script timeout value in the protection policy settings to allow PBMRcf g . exe to complete before the backup begins.

Pre/Post-Script (Optional)

Pre-script:

A maximum of two pre-scripts (one Windows-compatible script, and one non-Windows script) can be added.

Name: PowerProtectDataManager
Compatibility: Windows

+Add Script

If script fails ☐ Continue job ☒ Skip job

Note: If a timeout value for the script is not specified, hung jobs will continue to wait for a response from the script.

Timeout:*

6. Navigate to **Summary** to review the changes, then click **Finish**.

Note: If a timeout value for the script is not specified, hung jobs will continue to wait for a response from the script.

PowerProtect Backup for Disaster Recovery

PBMR allows a previously created **PowerProtect Backup** to be used for **bare machine recovery**.

Only file-based backups are supported.

To perform a recovery, the following conditions must be met:

1. A PBMR configuration must be created.
2. A **PowerProtect Backup** must be performed after the configuration has been created.

Once these steps have been completed, the backup can be used with the PBMR recovery environment to restore the protected system.

File-Based Backups

Ensure that Backup mechanism is set to File-Based Backup, **not Auto**, in the protection policy.

Edit Policy

Type
Purpose
Assets
File Filters
Objectives
Options
Summary

Options

Select additional options for this policy. Name: Windows PBMR Test JC | Type: File System | Purpose: Centralized Protection | Assets: 2

Advanced options

Disaster recovery options

- ☐ Back up system state files only
- ☒ Ignore missing system state files
- ☐ Exclude non-critical dynamic disks
- ☐ Ignore third-party services when identifying critical volumes

Note: These options apply only to disaster recovery objects.

Backup mechanism
File Based Backup

Troubleshooting
☐ Enable debug logs for troubleshooting purposes.

Step 6 of 7

Cancel Back Next

This setting is available within the **Additional Settings** section of the relevant Protection Group and ensures that system and locked files are included in the backup.

Note:

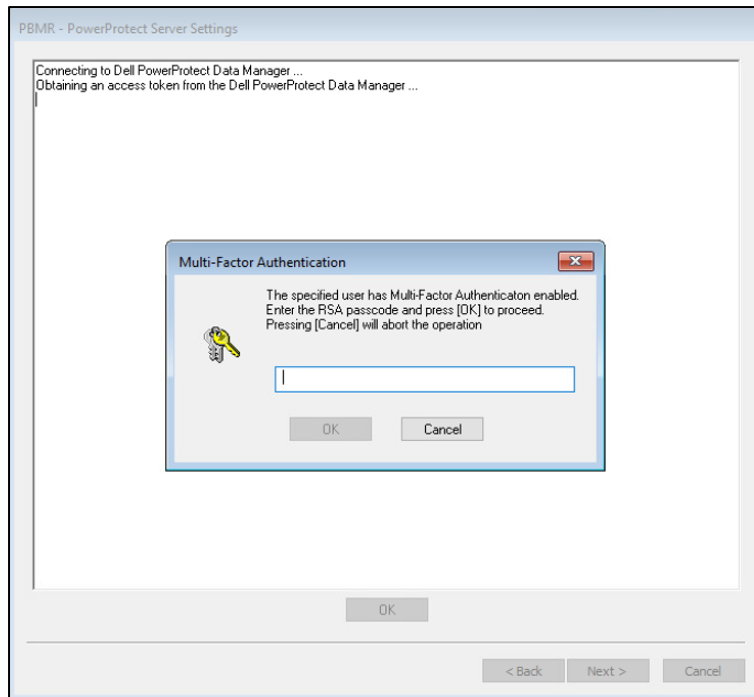
This guide does not describe how to create PowerProtect Backups. Refer to the PowerProtect Backups documentation for backup configuration and administration procedures.

Multi-factor Authentication

If PBMR is configured to use **Multi-factor Authentication** (MFA), you will be prompted to enter an **MFA code** during the **recovery process**.

Before performing a recovery, ensure that:

- an authenticator application is installed on a mobile device.
- the **PowerProtect Manager** server has been added to the authenticator application.



Common authenticator applications include:

- Microsoft Authenticator
- Google Authenticator

During recovery, enter the **MFA code** generated by the authenticator application when prompted.

Note:

MFA codes are only valid for a short period of time. If the code expires before it is entered, generate a new code and try again.

Restoring a System

This section describes the process of recovering a system using the **PBMR recovery environment**.

The recovery environment is created using CRISP and the appropriate PBMR WinPE files. For information on creating recovery media, see [Create the Bootable Recovery Environment](#).

The recovery environment can be booted on:

- the original system
- replacement hardware
- a virtual machine
- dissimilar hardware

Recovery Workflow

A typical PBMR recovery consists of the following stages:

1. **Boot** the **PBMR recovery environment** on the target system.
2. **Load** the **required PBMR configuration** and **connect** to the **PowerProtect Data Manager backup**.
3. **Restore** the **system** from the selected backup.
4. **Perform** any required post-recovery tasks, such as:
 - o updating the hostname
 - o modifying network settings
 - o performing Dissimilar Hardware Recovery (DHR)
5. **Boot** the **recovered system**.

The following sections describe each stage of the recovery process in more detail.

File-based recoveries

PBMR supports recovery from **file-based PowerProtect backups**.

The following sections describe the recovery process for file-based backups.

Booting the recovery environment

Boot the target system using the PBMR recovery media created with CRISP.

Depending on how the recovery media was created, this may be:

- a bootable USB device
- a bootable CD/DVD
- a mounted ISO in a virtual environment

If the recovery media was created with the default CRISP settings, a prompt similar to the following is displayed:

```
Press any key to boot from CD or DVD. _
```

The prompt is displayed only briefly before the system attempts to boot the installed operating system.

Note:

This prompt can be disabled when creating the recovery media. If disabled, the recovery environment will boot automatically.

For further information, refer to the CRISP documentation.

Driver Support

Additional drivers can be loaded after the recovery environment has started.

This is typically required when recovering systems that contain hardware not supported by the current WinPE environment, such as newer storage controllers or network adapters.

Ensure that the appropriate 64-bit drivers are used for the selected WinPE environment.

For more information, see **Load a Driver**.

Recovery Environment Startup

During startup, the WinPE environment loads the required storage and network drivers before launching the PBMR Recovery Environment.

Once the recovery environment has fully loaded, the recovery media can be removed if required.

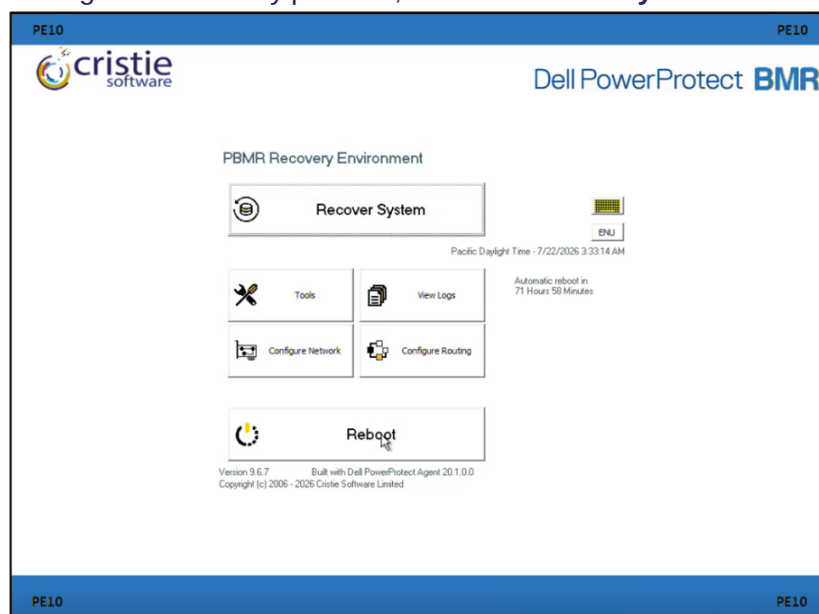
Note:

The Microsoft WinPE environment automatically restarts after 72 hours of continuous operation. This is a limitation of the Microsoft WinPE platform.

When startup is complete, the PBMR Recovery Environment is displayed.

Begin the restore process

To begin the recovery process, select **Recover System** from the **PBMR Recovery Console**.



PBMR recovery environment main menu

When the system boots into the **PBMR recovery environment**, the main menu is displayed.

Network Configuration

Before starting the restore, you can configure:

- Network settings
- Network routing

Use the relevant icons on the main menu to open these options.



Reboot Timer

A countdown timer is displayed on the screen, this shows how long remains before the recovery environment automatically restarts.



This is a standard limitation of the **Microsoft WinPE environment**.

Locale and Keyboard Settings

The Locale option allows you to configure regional settings for the recovery environment.

Using this option you can adjust:

- Date and time format
- Keyboard layout

The locale icon shown depends on the system locale used when the recovery media was created with CRISP. For example, if the recovery ISO was built on a system using a UK locale, the corresponding locale icon will be displayed:

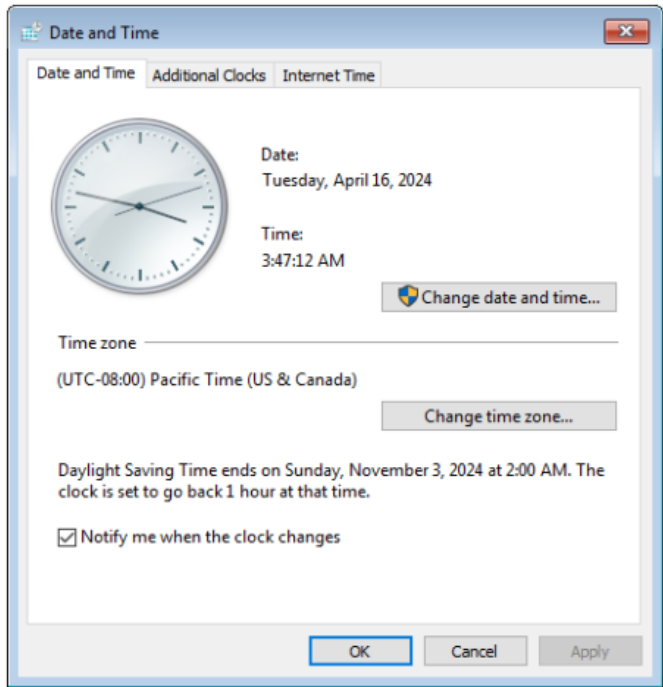


Changing the locale does not change the display language, which remains English.

Date, Time and Time Zone

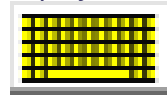
The **Date**, **Time** and **Time Zone** settings can also be configured from the **recovery environment**.

The **Additional Clocks** and **Internet Time** options are available, allowing the system time to be synchronised with an NTP server if required.

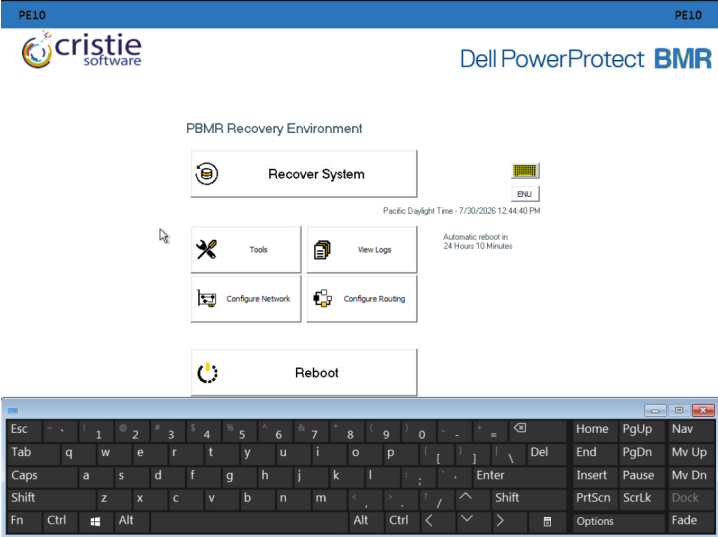


On-Screen Keyboard

If keyboard input is unavailable (for example, due to missing drivers), an on-screen keyboard can be displayed.



Click the **keyboard icon** to open the on-screen keyboard. The keyboard will appear at the bottom of the screen and will follow the currently selected locale layout.



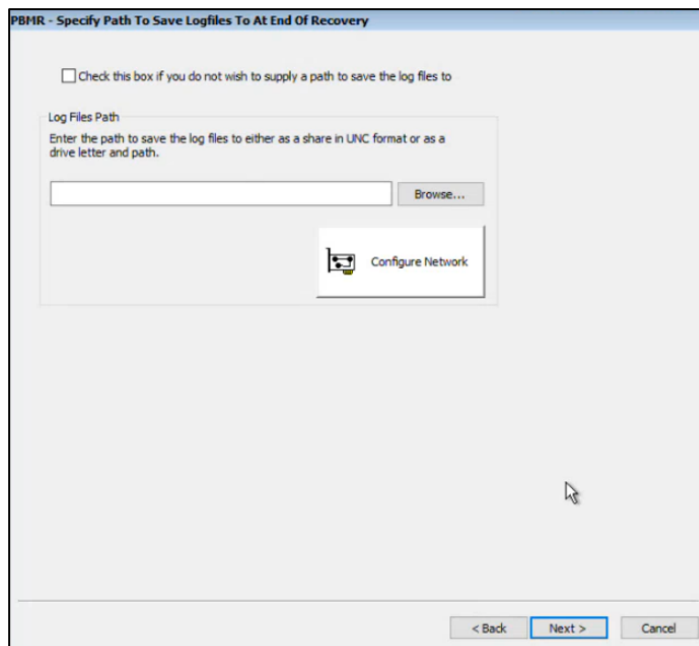
Log file save path

Before starting the restore process, you should configure a location where the recovery log files will be saved.

The log files can be saved to:

- a **network location**, or
- **removable media** such as a USB flash drive

Once configured, the log files will be automatically saved at the end of the restore process without further user interaction.

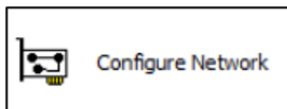


Saving Logs to a Network Location

Procedure

To save the log files to a network share:

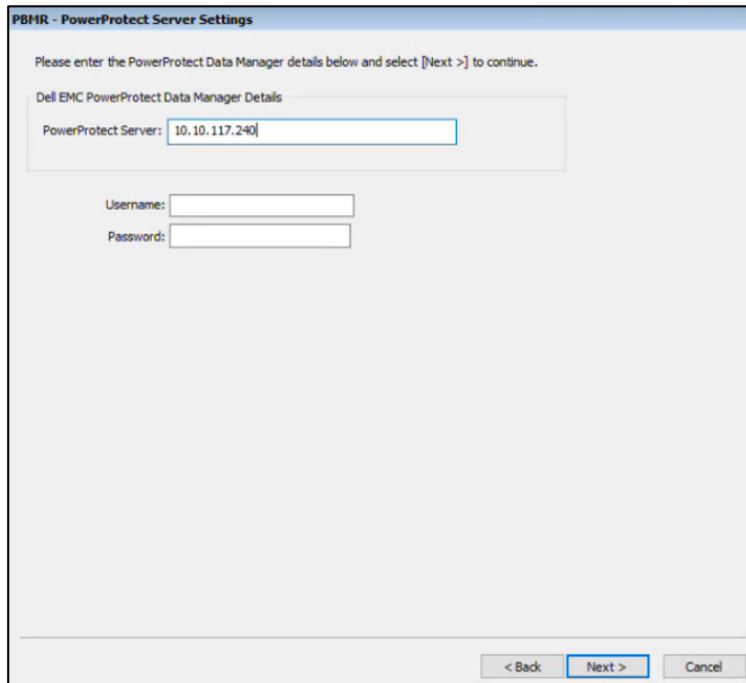
1. Use the **Configure Network** option to connect to the desired network location.



2. Click **Browse** to select the folder where the log files will be stored.
3. Click **Next** to continue to the next step.

Specify recovery details

In this section, we demonstrate how to specify the **PowerProtect server** and select the **recovery point** to restore from.

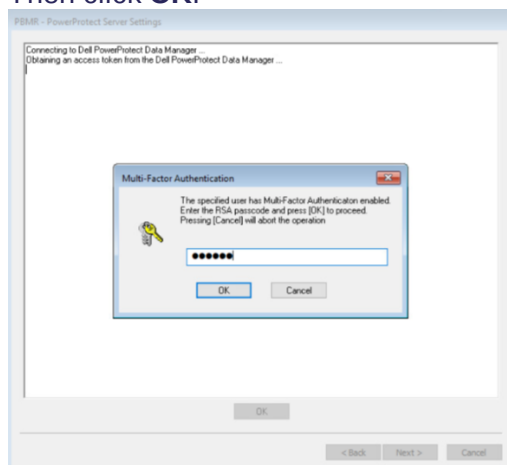


The screenshot shows the 'PBMR - PowerProtect Server Settings' dialog box. It contains the following fields and controls:

- PowerProtect Server:** A text box containing the IP address '10.10.117.240'.
- Username:** An empty text box.
- Password:** An empty text box.
- Navigation buttons:** '< Back', 'Next >', and 'Cancel' buttons at the bottom right.

Procedure

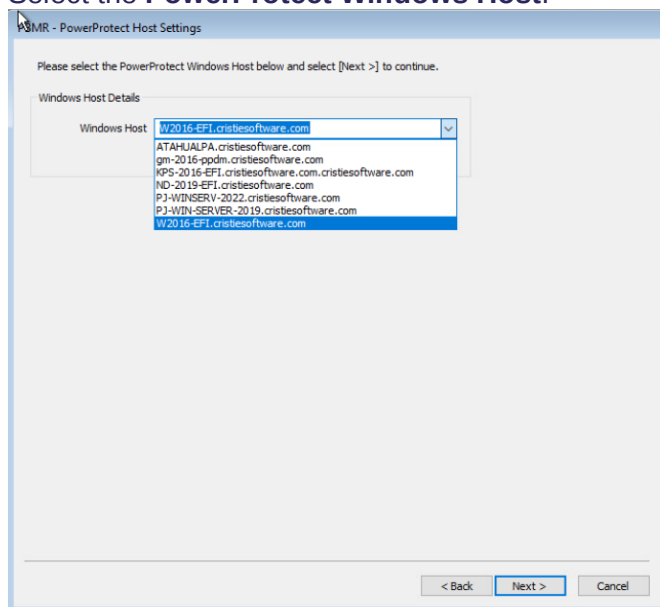
1. Enter the **PowerProtect server IP address** (IPv4 format)
2. In **Registered Source**, enter:
 - The IPv4 address, or
 - The hostname of the source
 - This must match the value used when the source was originally registered with the server.
3. Enter a **Tenant ID** if required.
4. **Optional:** If **Multi-Factor Authentication (MFA)** is enabled on the **PowerProtect** server, enter the **MFA code** generated by the authenticator application when prompted. Then click **OK**.



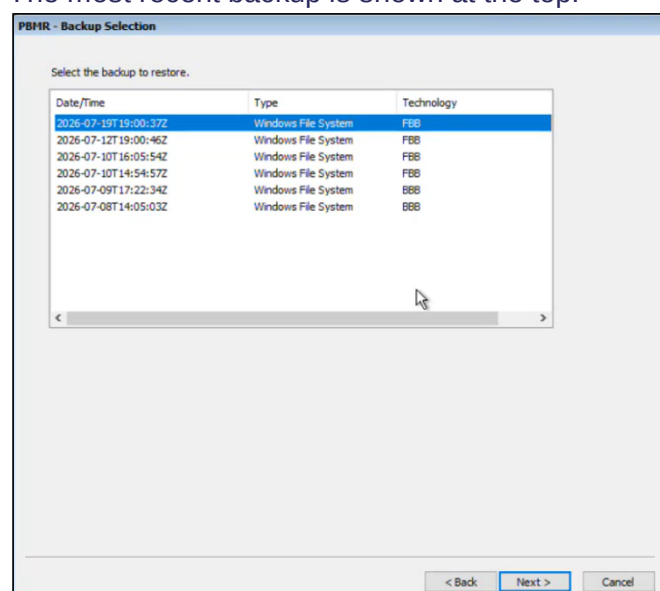
The screenshot shows a 'Multi-Factor Authentication' dialog box overlaid on the 'PBMR - PowerProtect Server Settings' dialog. It contains the following elements:

- Message:** 'The specified user has MultiFactor Authentication enabled. Enter the RSA passcode and press [OK] to proceed. Pressing [Cancel] will abort the operation.'
- Input field:** A text box containing a masked passcode represented by eight dots.
- Buttons:** 'OK' and 'Cancel' buttons.

5. Select the **PowerProtect Windows Host**.



6. Select the **recovery point** from the list.
The most recent backup is shown at the top.

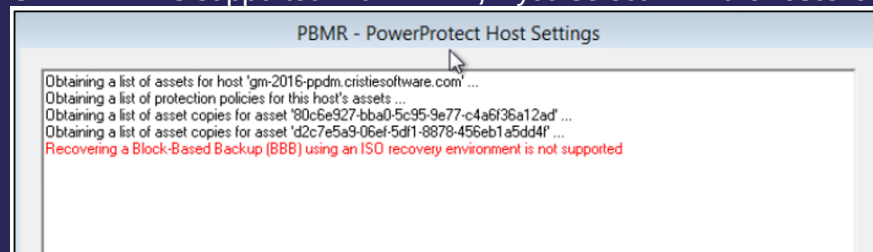


Note:

FBB: File-Based back up

BBB: Block-Based back up

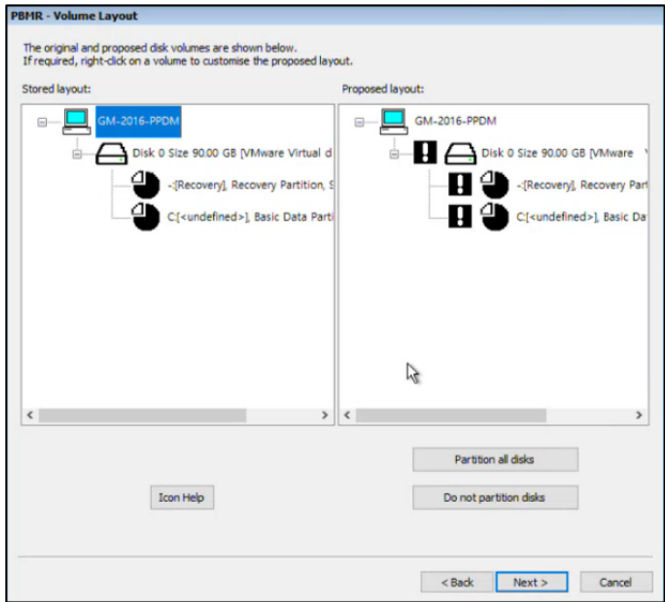
ONLY FBB is supported with **PBMR**, if you select **BBB** the **restore** will fail.



7. Click **Next** to proceed.

Confirm volume layout

The confirm **Volume Layout** step displays the disk and partition layout that will be created during recovery.



- The left-hand pane shows the original source disk layout captured in the backup.
- The right-hand pane shows the proposed layout for the target system.

Review the proposed disk mapping and partition layout before continuing.

Disk and partition indicators

The icons next to each disk and partition indicate how they will be handled during recovery:

Icon	Type	Description
	Tick icon	The disk or partition will be left unchanged.
	Exclamation mark	The disk or partition will be formatted.
	Mixed indicator (black/white exclamation)	At least one partition on the disk will be formatted.
	Empty box	The disk will be ignored during recovery.

Disk types

Use the Icon Help in the interface to display a summary of these indicators.

Modifying disk layout

If required, you can modify the proposed recovery layout before continuing.

Available options include:

- enabling or disabling disk partitioning
- enabling or disabling partition formatting
- modifying partition labels
- adjusting partition sizes where supported

You can also choose to ignore specific target disks during the recovery process.

Once the disk and partition layout has been verified, click **Next** to continue.

No changes are made to the target disks until the recovery proceeds beyond this stage.

Note:

System partitions required for a successful recovery cannot be removed or configured incorrectly. PBMR validates the configuration and displays an error if an invalid layout is selected.

Select volumes to restore

In this step, select the volumes you want to restore.

Each volume typically represents a disk partition.

Notes:

- The system and boot partitions are always restored by default
- These cannot be deselected, even if they are located on separate partitions

Select Volumes

- Tick the **volumes** you want to include in the restore
- Alternatively, click **Select All** to restore all volumes

PBMR - Select Volumes to Restore

At least one System and one Boot partition must be selected in order to recover your machine. This may be the same partition. You can select additional drives to be restored by ticking the check box next to the drive.

Drive Letter	Boot	System	Name	File System
☒ C:	Yes		C:\	NTFS

Select All Deselect All

< Back Next > Cancel

- Click **Next** to proceed to the next step.

Clone settings

The **Clone Settings** step allows you to review and modify the hostname and network configuration that will be applied to the recovered system.

You can:

- retain the original hostname and IP configuration
- assign a new hostname
- configure static IP addresses
- enable DHCP for individual network interfaces

Network adapters that are currently connected to a network are identified as Operational.

Note:

The Use DHCP option indicates how the network adapter was configured on the source system:

- selected = DHCP was used
- cleared = a static IP address was used

If no changes are required, leave the default values and click Next to continue.

When recovering to a system with different hardware, PBMR may detect devices that require additional drivers.

If dissimilar hardware is detected, the Dissimilar Hardware dialog is displayed before the recovery begins.

If additional hardware configuration is required, an additional dialog will be displayed before the recovery begins.

After reviewing the **Clone Settings**, click **Finish** to start the recovery.

Dissimilar hardware

During the recovery process, PBMR checks whether the target system contains hardware that was not present in the original system.

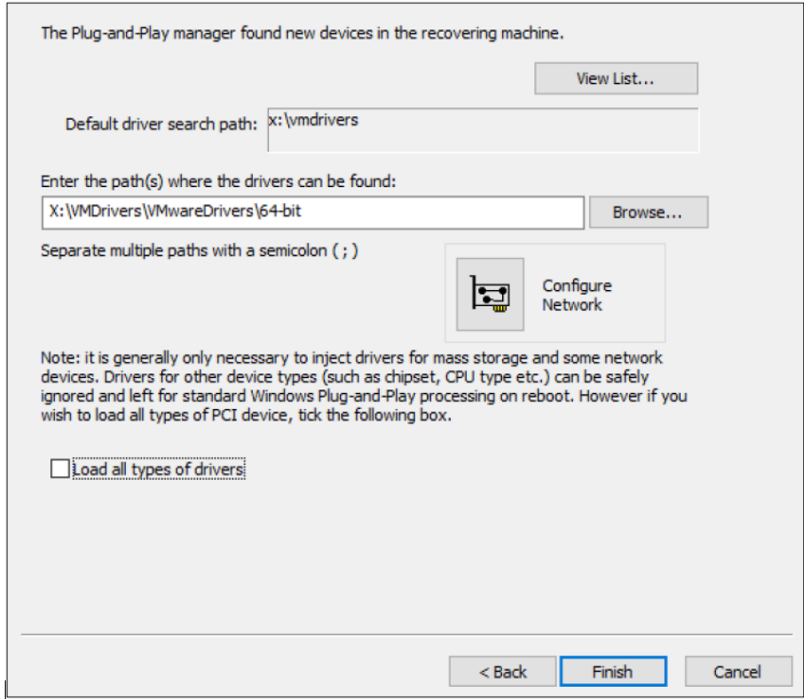
If new hardware is detected, the **Dissimilar Hardware dialog** is displayed, allowing additional drivers to be supplied before the recovery begins.

Specify one or more locations that contain the required driver files.

These locations can be:

- local storage devices (such as USB drives)
- network shares

If required, use **Map Network Drive** to connect to a network share.

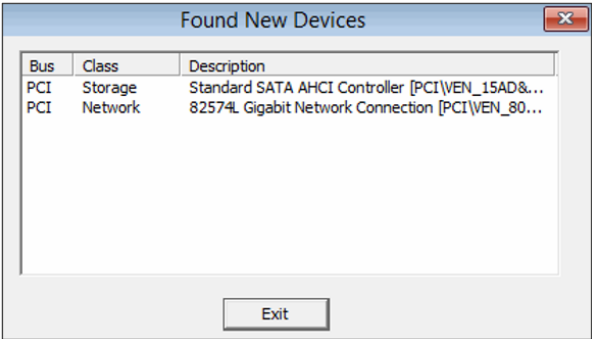


Note:

Any specified locations must be accessible from the recovery environment.

Procedure

1. Click **View List** to display the devices that require drivers. This helps identify which drivers need to be provided.



2. Ensure the specified locations contain the appropriate 64-bit drivers for the target system. During recovery, PBMR searches the configured locations and automatically injects any required drivers into the recovered operating system.

By default, PBMR searches for:

- mass storage drivers
- network drivers

The Load all types of drivers option extends the search to include additional device types such as graphics, USB, and chipset drivers.

In most cases, this option is not required and is not recommended.

3. When ready, click **Finish** to continue the recovery.

Important:

If a required storage driver is not available, the recovery may complete successfully but the recovered system may fail to boot.

Disk recovery status

Once the recovery starts, PBMR prepares the selected disks and begins restoring data.

Disk preparation

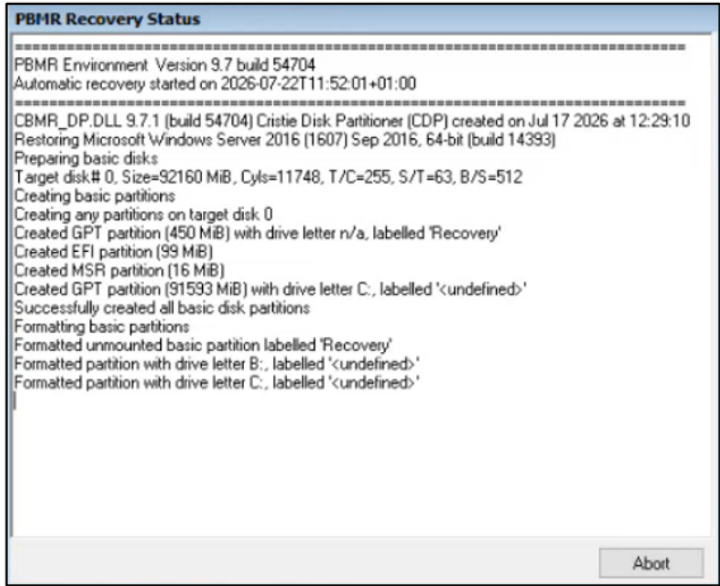
Before any data is restored, the target disks are prepared. This includes:

- Mapping the original disk layout to the target system
- Removing existing partitions
- Clearing any dynamic disk configuration
- Recreating the required partitions
- Converting to dynamic disks (if required)
- Formatting partitions
- Creating mount points
- Marking bootable volumes as active

After disk preparation, the restore process begins.

A progress window is displayed showing:

- Recovery progress (progress bar)
- Amount of data restored
- Time elapsed
- Throughput



Recovery phases

The recovery runs in stages:

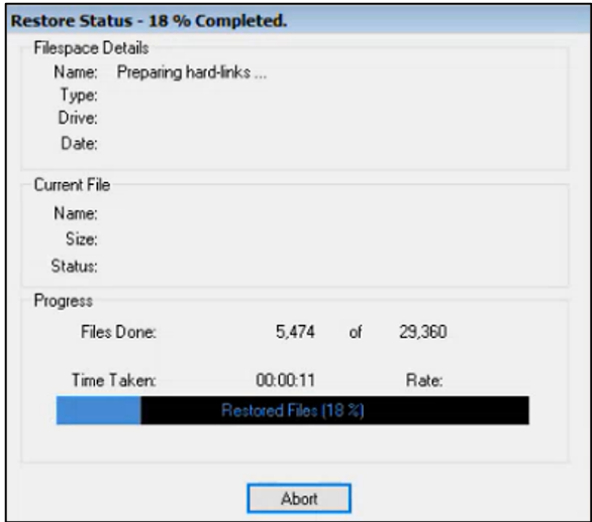
- 1. **Volume restore:** Each selected volume is restored, including System State.
- 2. **Hard link restore:** File system hard links are restored after the main data.

Recovery time

Recovery duration depends on the size of the backup and the performance of the source and target systems.

Interrupting the recovery

You can select **Abort** to stop the recovery process.



Important:
Aborting the recovery may leave disks or partitions in an inconsistent state, which could make them unusable.

Errors and Logs

Any recovery errors are displayed in the progress window.

After the recovery completes, review the recovery logs to identify and troubleshoot any issues

Final checks

At the end of the recovery process, PBMR verifies:

- that the required boot files are present.
- whether any additional hardware drivers are required.

Click **Finish** to return to the **recovery environment** main menu.

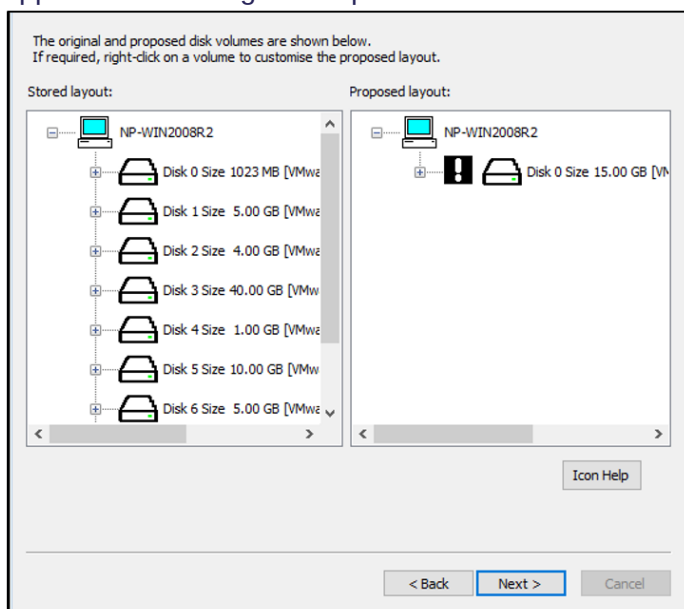
Before rebooting, you may wish to:

- review the recovery logs.
- copy the logs to a local device or network location.

If a log file path was configured earlier, logs will be saved automatically.

Disk scaling

When recovering to a system with fewer or smaller disks than the original system, PBMR automatically applies disk scaling where possible.



How disk scaling works

During recovery, PBMR attempts to restore as much of the original disk layout as possible using the available target disks.

Partition sizes are adjusted based on:

- the original partition size
- the amount of data stored within the partition

For example, if the original system contains multiple disks and the target system contains only a single disk, PBMR prioritises the recovery of essential volumes, such as the boot volume, and scales the remaining partitions accordingly.

Considerations

- Complex disk configurations, such as mirrored dynamic volumes, may require manual adjustment.
- If only a single target disk is available, mirrored volumes may be restored as a non-mirrored configuration.
- The Volume Layout screen displays only disks and partitions that can be modified.
- When recovering to larger disks, partition sizes remain unchanged by default.

Expanding partitions

When recovering to larger disks, partition sizes can be increased manually.

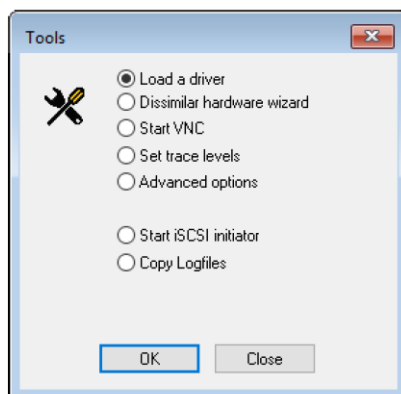
To modify a partition:

1. **Right-click** the partition.
2. Select **Modify**.
3. Specify the required partition size.

Recovery environment tools

Several tools are available within the PBMR Recovery Environment to assist with recovery, troubleshooting, and system configuration.

These tools can be accessed from the **Tools menu**.



Available tools

The following options are available:

Tool	Description
Load a Driver	Allows you to load additional mass storage or network drivers into the running WinPE environment. Use this if required hardware is not detected automatically. This should be done before starting the recovery process.
Dissimilar Hardware Wizard	Allows drivers to be injected into the recovered system when restoring to different hardware. This step is normally handled automatically during recovery and does not usually need to be run manually.
Start VNC	Starts a VNC server within the recovery environment, allowing remote access. - The system IP address will be displayed when the service starts - This IP is required to connect using a VNC client
Set Trace Levels	Allows you to adjust the level of logging detail for the recovery process.
Advanced Options	Provides additional configuration options. Important: Only use this option when instructed by Cristie Support.
Start iSCSI Initiator	Starts the iSCSI initiator service. Contact Cristie Support for guidance before using this feature.
Copy Log files	Creates a compressed archive of recovery log files and allows you to copy them to: - A local device (for example, USB) - A network share

Notes:

- VNC sessions are password protected. If remote troubleshooting is required, Cristie Support will provide the necessary connection details and password.
- Increasing trace levels may impact recovery performance and should only be used for troubleshooting purposes.

Dissimilar hardware wizard

The **Dissimilar Hardware Wizard** (DHW) is used when restoring a system to hardware that differs from the original system.

In most cases, PBMR automatically detects new hardware during recovery and injects any required drivers.

Use this wizard if:

- Driver injection did not complete successfully.
- Additional drivers need to be installed manually.

Driver requirements

In most recovery scenarios, only the following drivers are required:

- Mass storage drivers
- Network drivers

In some environments, additional drivers may also be required.

Note:

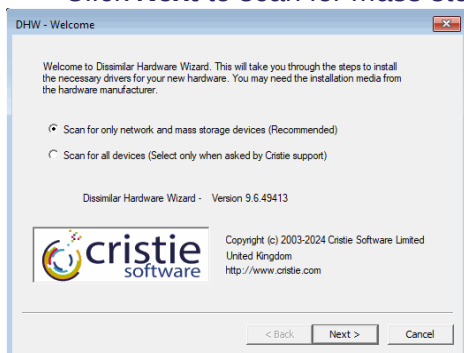
Hardware Abstraction Layer (HAL) changes must be handled manually.

Automatic driver installation

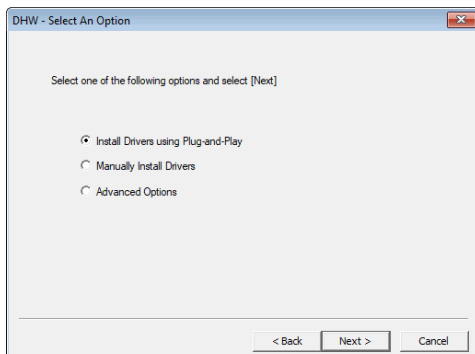
Procedure

1. When the wizard starts, you can choose how devices are scanned:

- Select ***Scan for all devices if instructed by Cristie Support***
- Click **Next** to scan for mass storage and network devices only (recommended)



2. Select **Install Drivers** using **Plug-and-Play** to begin automatic detection, click **Next**.



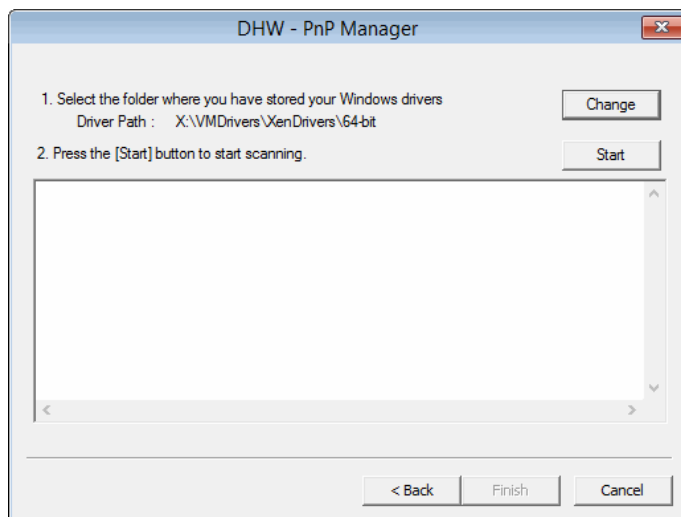
3. If the required drivers are not located automatically:

- Click **Change**.
- Specify the location of the driver files.
Driver files can be located on:

- o local storage
- o USB devices
- o CD/DVD media
- o network shares

For each detected device, review the suggested driver and click Install if appropriate.

- Click **Start** to begin scanning.



The wizard continues until all detected devices have been processed.

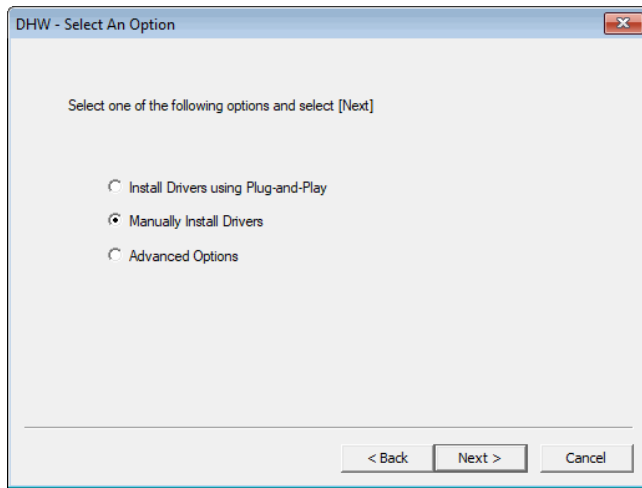
Manual driver installation

Manual installation may be required for:

- HAL changes
- Drivers that are not detected automatically

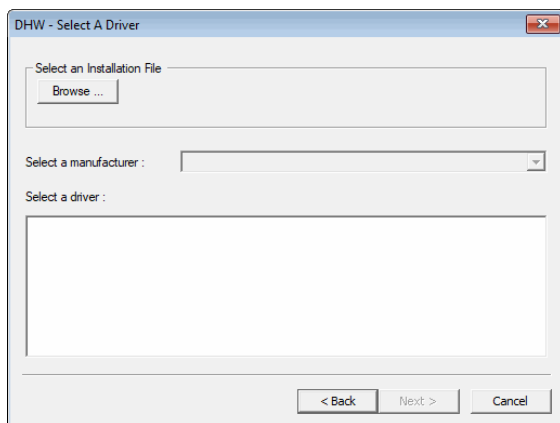
To install a driver manually:

1. Select **Manually Install Drivers**
2. Click **Next**



3. Click **Browse**.

Navigate to the folder containing the required driver .inf file.
This can be a local path or network share.

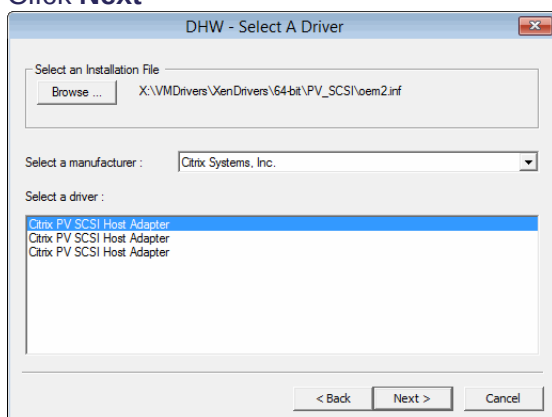


4. Select the **required driver**. Drivers are grouped by manufacturer.
Drivers are typically supplied as:

- .inf files
- .sys files

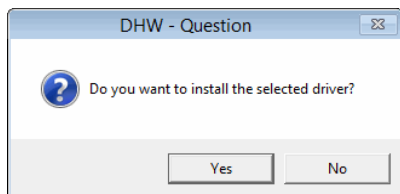
The .inf file contains the information required to install the associated driver files.

5. Click **Next**



6. The wizard will:

- Identify required files
- Allow you to confirm or change the source location



7. Once complete:

- You can install additional drivers, or
- Click **Finish** to exit the wizard

Load a driver

Use **Load a Driver** to add additional mass storage or network drivers to the WinPE recovery environment.

This option is typically used when the recovery environment does not include native support for the required hardware.

When to use this

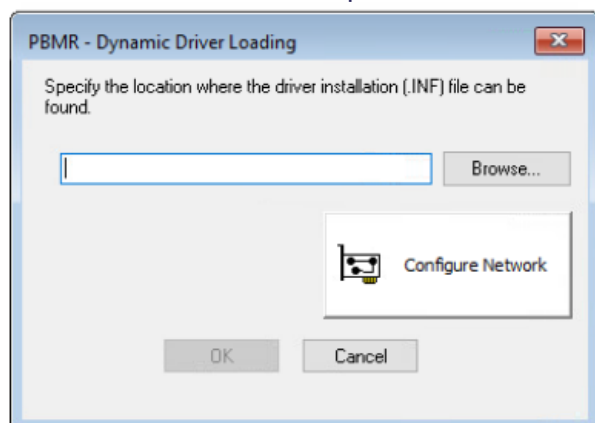
Use this option if:

- No disks are detected during recovery
- Network interfaces are not available
- Required hardware is not recognised

For example, if no storage devices are displayed, a mass storage driver may need to be loaded before recovery can continue.

Procedure

1. Select **Load a Driver** from the **Tools** menu.
2. **Browse** to the location of the **driver** .inf file.
3. **Select** the **driver** and complete the installation.



Driver location

Driver files can be loaded from:

- A USB storage device
- CD/DVD media
- Network share

If the driver is stored on a network location, configure network connectivity before attempting to load the driver.

Driver files

The selected driver package must include the required driver files.

Typically:

- .inf files contain the driver configuration
- .sys files contain the driver binaries

Ensure all associated files are available in the same location.

Confirmation

A confirmation message is displayed when the driver has been loaded successfully.

Copy log files

Use **Copy Log files** to save recovery logs before exiting the WinPE recovery environment.

Recovery logs created within WinPE are temporary and will be lost when the recovery environment is closed.

When to use this

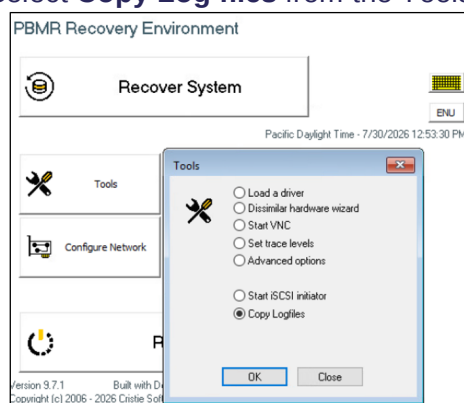
Use this option if you need to:

- Retain logs for troubleshooting
- Share logs with Cristie Support
- Keep a record of the recovery process

The steps below demonstrate how to copy the log files.

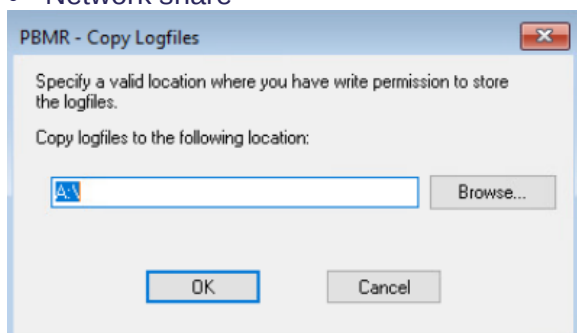
Procedure

1. Select **Copy Log files** from the Tools menu.



2. Choose a destination location:

- Local device (for example, USB)
- Network share



3. If copying to a network location:

- Use the **Cristie Network Configurator** to configure access.
- Map the required network share.
- Copy the log files to the mapped location.

All recovery logs are collected into a single ZIP archive, making them easy to store or share with Cristie Support.

Example destination:

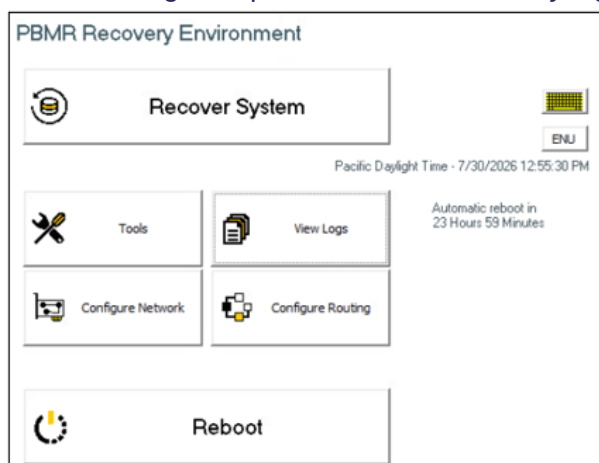
`Q:\<User>\LOGs`

Notes:

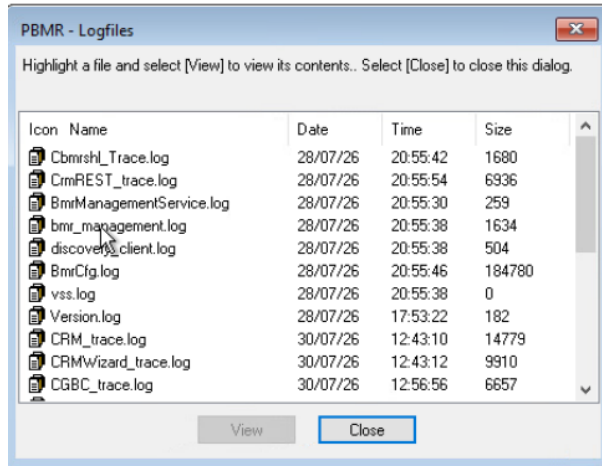
- Recovery logs are also saved to the recovered system following a successful recovery.
- These logs are stored within the PBMR installation folder under the **Temp** directory.

View logs

Use View Logs to open and review recovery log files directly within the WinPE recovery environment.



Log files are primarily intended for troubleshooting and diagnostic purposes and may be requested by Cristie Support when investigating recovery issues.



Note:

- Most logs are intended for diagnostic use.
- Cristie Support may request specific log files when investigating recovery issues.

Configure network

The **Cristie Network Configurator** allows network settings to be configured within the recovery environment.

The tool supports:

- multiple network interfaces (NICs)
- DHCP and static IPv4 configuration
- DNS server configuration
- NIC settings such as duplex mode and link speed
- network identification settings
- access to network file shares
- mapping and unmapping network drives

When to use this

Use the **Network Configurator** when you need to:

- access backups stored on a network location
- connect to network shares for drivers or log files
- configure network connectivity during the recovery process

The following sections describe the available network configuration options in more detail.

Configure NIC parameters

The **Network Configurator** allows you to modify network adapter (NIC) settings during recovery.

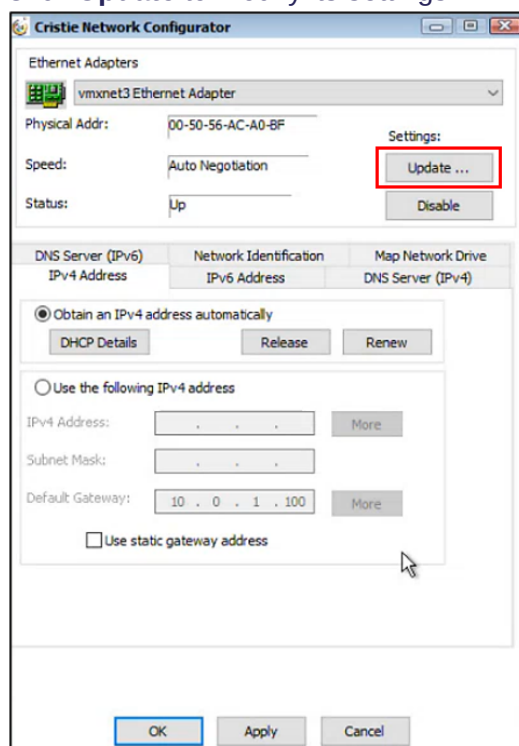
Supported settings may include:

- link speed
- duplex mode
- other hardware-specific adapter properties

Modifying NIC settings

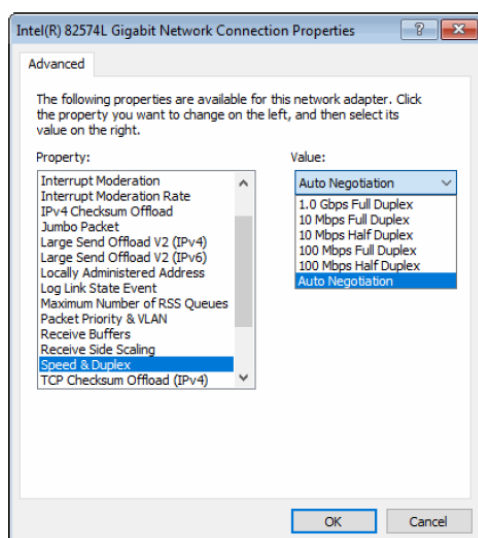
Procedure

1. Choose the required **NIC** from the drop-down list (Multiple NICs may be available)
2. Click **Update** to modify its settings.



3. The NIC properties window allows you to adjust available settings.
To change speed or duplex settings:

- Select the relevant **Property** (e.g.Speed/Duplex)
- Choose the required value from the **Value** drop-down list.



Note:

The available options depend on the network adapter installed in the system. In most environments, Auto Negotiation is the recommended setting.

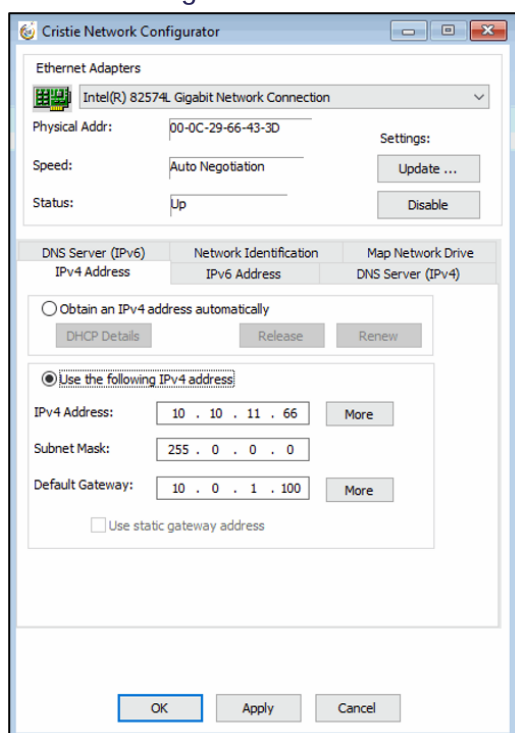
Assign static or DHCP IP settings

By default, the WinPE recovery environment uses DHCP to obtain an IP address automatically. If required, you can configure a static IP address as described below.

Configure IP Settings

Procedure

1. Select the required network adapter from the drop-down list.
2. Choose one of the following options:
 - Use DHCP to obtain an IP address automatically.
 - Use the following IP address to configure a static address.
3. If using a static configuration, enter:
 - IP address
 - Subnet mask
 - Default gateway
4. Click **Apply** to save the changes.
5. **Optional:** Select **More** to access additional network configuration options. These include:
 - adding additional IP addresses to the selected adapter
 - releasing the current DHCP lease
 - renewing the current DHCP lease

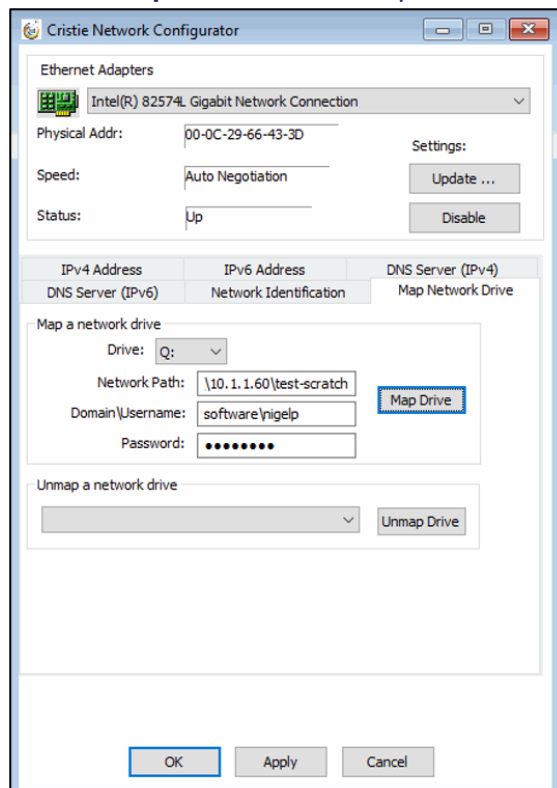


Notes:

- Selecting a static IP address automatically disables DHCP for the selected adapter.
- Ensure the correct network adapter is selected before applying any changes.

Map a network device

Use the **Map Network Drive** option to access shared network resources during recovery.



Map a drive

Procedure

1. Open the **Cristie Network Configurator** from the **Tools** menu.
2. Select the **Map Network Drive** tab.
3. Choose a **Drive** from the Drive drop-down list.
4. Enter the **network share path**.
5. Enter the required **network credentials**.
6. Click **Map Drive**.

Network share paths

Network shares can be specified using either:

- Hostname (e.g. \\server\share)
- IPv4 address (e.g. \\192.168.1.10\share)

When the mapping is successful, the drive becomes available within the recovery environment and is listed in the **Unmap Network Drive** tab.

Note:

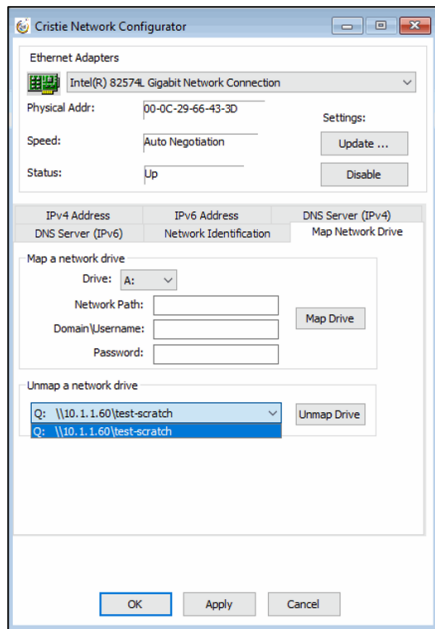
- Ensure network connectivity has been configured before mapping a drive.
- Verify that the supplied credentials have permission to access the network share.

Unmap a network drive

Use the **Unmap Network Drive** option to remove a previously mapped network drive from the recovery environment.

Procedure

1. Open the **Cristie Network Configurator** from the **Tools** menu.
2. Select the **Unmap Network Drive** option.
3. Choose the **drive to remove** from the drop-down list
4. Click **Unmap Drive**.



5. Once the drive is unmapped:
 - It will be removed from the list
 - It will no longer be accessible from the system

Notes:

- Ensure the drive is not currently in use before removing it.
- Removing a mapped drive does not affect the underlying network share.

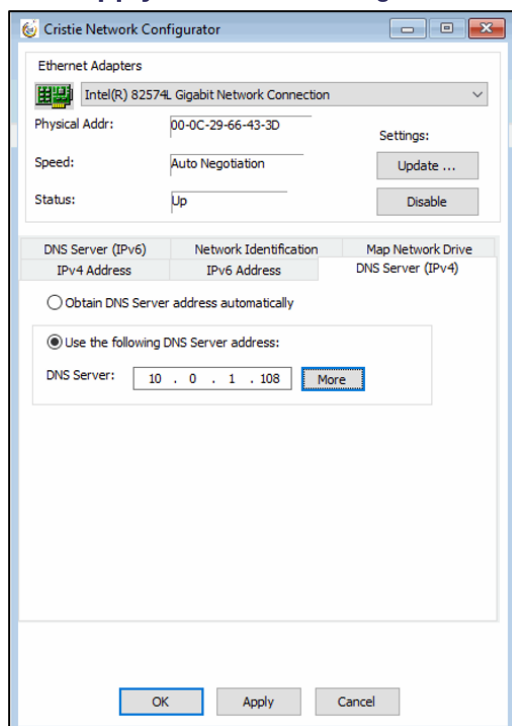
Configure DNS servers

By default, DNS server settings are assigned automatically when the WinPE recovery environment starts. If required, you can configure DNS server addresses manually.

Configure DNS servers

Procedure

1. Select **Use the following DNS server address**.
2. Enter the required **DNS server IP address**.
3. Click **Apply** to save the configuration.



4. **Optional:** Click **More** to add additional **DNS server addresses**.

Notes:

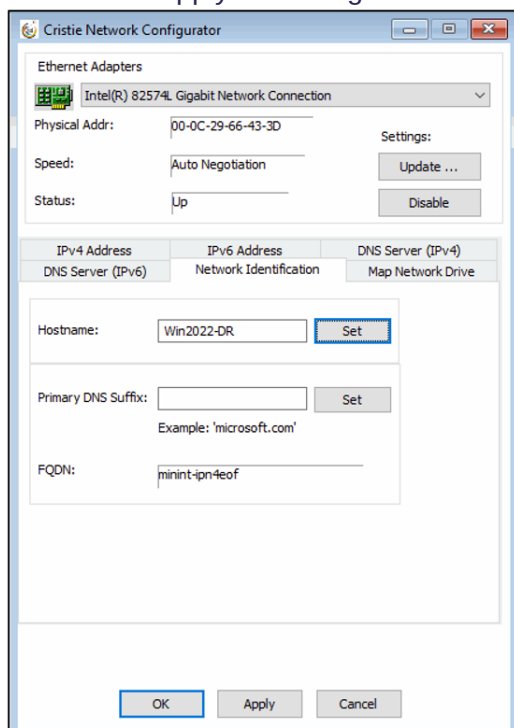
- WINS servers are not supported.
- Ensure the DNS server configuration is correct when accessing network resources using hostnames rather than IP address.

Configure network identification

Use the **Network Identification** tab to modify the **hostname** and **Primary DNS suffix** used by the **WinPE** recovery environment.

Procedure

1. Select the **Network Identification** tab.
2. Enter the required **Hostname**, then click **Set**.
3. Configure the **Primary DNS suffix** if required, then click **Set**.
4. Click **Set** to apply the change.



Notes:

- These settings apply only to the current WinPE recovery session.
- They are not applied to the recovered operating system.
- Any changes are lost when the recovery environment is closed or restarted.

Configure routing

The **Cristie Route Configurator** allows you to manage network routing within the recovery environment. This can be useful when access to backups, network shares, or other resources requires specific routing configuration.

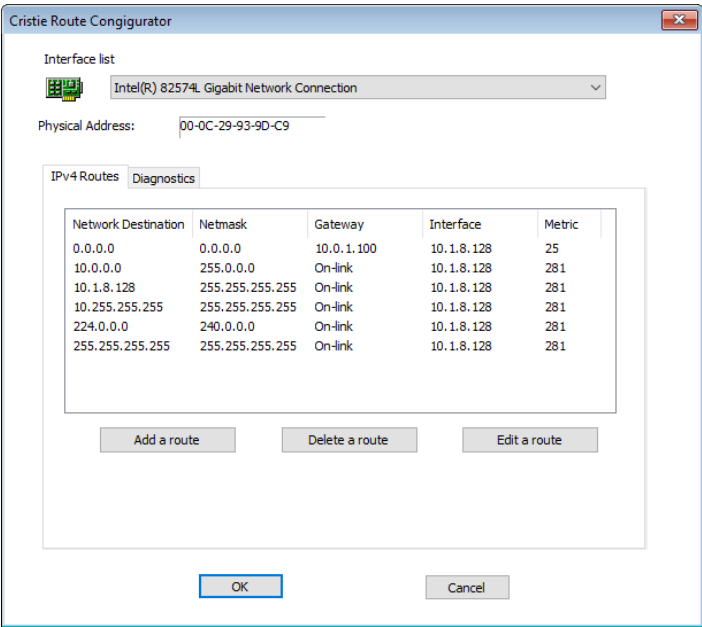
Feature	Description
Multiple NIC support	Configure routing across multiple network interfaces
Route management	Add, modify, or delete network routes
IPv4 support	Configure routing using IPv4 addresses
Diagnostics tools	Run ping and tracer tests to verify connectivity

Note:

- Only IPv4 routing is supported.
- IPv6 routing is not supported in the WinPE recovery environment.

IPv4 routes

Use this tab to manage **IPv4 network routes** during the recovery process.



Procedure

1. Select the required **network interface** from the drop-down list
2. Enter the following details:
 - Network
 - Netmask
 - Gateway
 - Metric

3. Click **Save** to add the route or **Cancel** to discard

Network Destination: 10 . 10 . 1 . 1

Netmask: 255 . 255 . 0 . 0

Gateway: 10 . 0 . 1 . 100

Interface: 10 . 1 . 8 . 214

Metric: 32

Click 'Save' to add this route, or 'Cancel' to not add this route

Save Cancel

4. To **Edit a Route**:

- Select the **route** from the list.
- Click **Edit** a route
- Modify the following fields:
 - o Gateway
 - o Metric
- Click **Save** to apply changes or **Cancel** to discard.

Network Destination: 10 . 1 . 8 . 214

Netmask: 255 . 255 . 255 . 255

Gateway: 0 . 0 . 0 . 0

Interface: 10 . 1 . 8 . 214

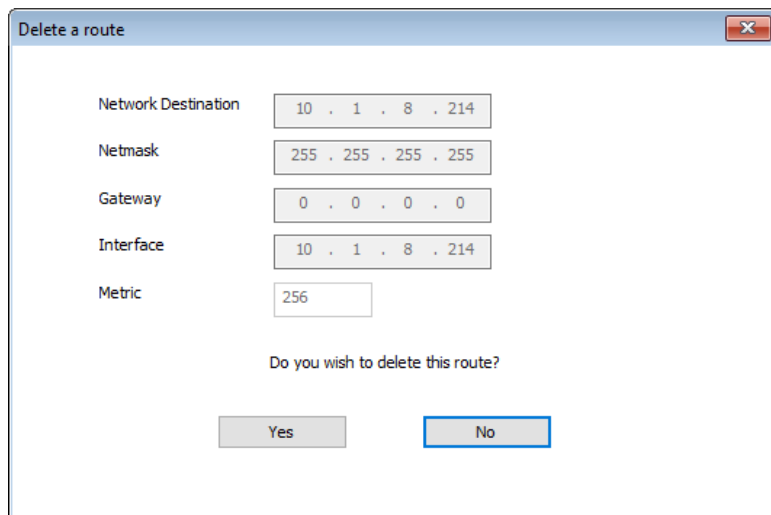
Metric: 256

Click 'Save' to change this route, or 'Cancel' to not change this route

Save Cancel

5. To **Delete a Route**

- **Select** the **route** from the list
- Click **Delete** a route
- **Confirm** the action:
 - o Click **Yes** to delete
 - o Click **No** to cancel



Delete a route

Network Destination: 10 . 1 . 8 . 214

Netmask: 255 . 255 . 255 . 255

Gateway: 0 . 0 . 0 . 0

Interface: 10 . 1 . 8 . 214

Metric: 256

Do you wish to delete this route?

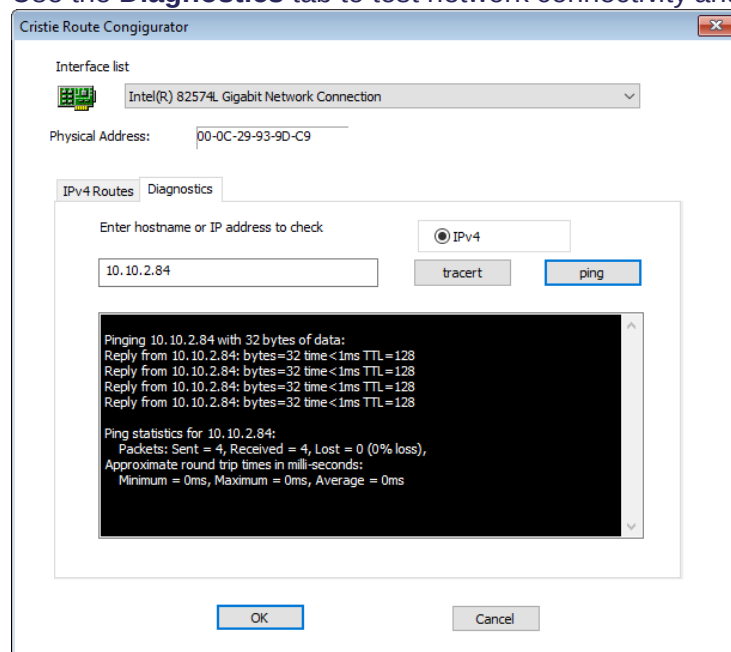
Yes No

Notes:

- Only the **Gateway** and **Metric** values can be modified when editing an existing route.
- Ensure the correct network interface is selected before adding, editing, or removing routes.

Diagnostics

Use the **Diagnostics** tab to test network connectivity and verify routing within the recovery environment.



Cristie Route Configurator

Interface list: Intel(R) 82574L Gigabit Network Connection

Physical Address: 00-0C-29-93-9D-C9

IPv4 Routes Diagnostics

Enter hostname or IP address to check: 10.10.2.84

☒ IPv4

tracert ping

Pinging 10.10.2.84 with 32 bytes of data:
 Reply from 10.10.2.84: bytes=32 time<1ms TTL=128
 Reply from 10.10.2.84: bytes=32 time<1ms TTL=128
 Reply from 10.10.2.84: bytes=32 time<1ms TTL=128
 Reply from 10.10.2.84: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.2.84:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in mill-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

OK Cancel

Run diagnostic tests

Procedure

1. **Select** the required **network interface** from the drop-down list
2. Enter the hostname or IPv4 address of the target system.
3. You can then run the following tests:
 - **Ping**: Checks basic network connectivity to the target
 - **Tracert**: Displays the route taken to reach the target
4. Choose one of the following to run diagnostics:
 - Click **Ping** to test connectivity
 - Click **Tracert** to analyse the network path
5. **Review** the results.
6. Click **OK** to close the Diagnostics window.

Note:

- Both hostnames and IPv4 addresses can be used as targets.
- Use Ping to confirm connectivity.
- Use Tracert to identify routing issues or network path problems.

Reboot

After a successful recovery, select **Reboot** to exit the recovery environment and start the recovered system.

Procedure

1. Click **Reboot**.
2. Confirm the action when prompted:
 - Click **Yes** to restart the system
 - Click **No** to return to the recovery console

Important:

- Ensure the system is configured to boot from the OS disk.
- The system may still be set to boot from the PBMR recovery media (CD/DVD or USB)
- Remove recovery media if required before rebooting.
- The system will boot into the recovered operating system.

Active Directory recoveries

PBMR supports the recovery of **Active Directory Domain Controllers** without requiring additional intervention during the recovery process.

Restore behaviour

During recovery:

- For **file-based backups**, **System State data** is restored if it has been backed up separately. Otherwise, it is restored as part of the file system recovery.

PBMR also automatically adjusts:

- System State components where required.
- boot configuration settings to account for hardware differences.

Post-recovery process

After the recovery completes, the **Domain Controller** recovery process continues automatically.

1. The system boots into **Directory Services Restore Mode (DSRM)**.
2. PBMR performs the required **cleanup** tasks to **reintegrate** the **Domain Controller** into the domain.
3. The system **reboots** automatically.
4. Following the **second reboot**, the **Domain Controller** should return to **normal operation**.

Important:

- Allow the recovery process to complete both reboot cycles without interruption.
- **Do not:**
 - o log in to DSRM
 - o perform manual Active Directory recovery steps

Although Microsoft documentation may describe manual intervention during certain Active Directory recovery scenarios, this is not required for PBMR recoveries and may interfere with the automated recovery process.

Completion

Once the automatic recovery process has finished and the second reboot has completed, the **Domain Controller** should be fully **operational**.

Appendices

This section provides additional reference information to support the use of PBMR. It includes supplementary guidance for specific features and configurations that may require additional consideration during backup and recovery.

Storage space support

PBMR supports the recovery of the following operating systems:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows 10

Important:

Storage Pool configurations must be manually reconfigured during recovery.

PBMR preserves:

- Storage Pool names
- Physical disk information
- Virtual disk information

However, the mapping between physical and virtual disks is not retained and must be configured manually during the recovery process.

Backup requirements

To ensure successful recovery:

- No additional backup configuration is required.

Special scenarios

iSCSI Disks

- Use the **iSCSI Initiator tool** within the recovery environment to reconnect the required storage before starting the recovery.

USB Disks

- The disks must also be configured as **Not Removable** in Windows Device Properties. Otherwise, they will not be available during Storage Pool configuration.

Virtual /Cloud Environments

- Where appropriate, physical iSCSI or USB disks can be represented using virtual disks on the target system.

BIOS to UEFI conversion

PBMR supports automatic conversion between legacy BIOS (MBR) and UEFI (GPT) boot configurations during recovery.

Supported conversion paths include:

- Legacy BIOS (MBR) to UEFI (GPT)
- UEFI (GPT) to legacy BIOS (MBR)

Converting from BIOS to UEFI

When converting from BIOS to UEFI:

- An EFI system partition is automatically created on the target disk
- Required boot files are added to this partition
- The target disk is converted to GPT format, regardless of the original disk type

Requirements

- The target environment must support UEFI boot
- Supported environments include:
 - o Physical machines
 - o VMware Workstation™
 - o VMware vSphere™

Post-Recovery Configuration

After recovery, you may need to:

- Create a new UEFI boot entry.
- Update the boot configuration within the system firmware or virtual machine setting.

Supported Scenarios

PBMR supports BIOS to UEFI conversion for a range of storage layouts, including:

- Split boot configurations
 - o Boot and System partitions on different disks.
 - o Separate Boot/System partitions on the same disk.
- Dynamic disk boot volumes, for example, mirrored dynamic disks.
These configurations will be preserved during recovery, with conversion to GPT if required.

UEFI to BIOS conversion

PBMR can also convert a UEFI-based system to legacy BIOS.

During the conversion:

- GPT disks are converted to MBR.
- The EFI partition is removed.

Notes:

- Boot mode conversion is performed automatically during recovery.
- Ensure the target system firmware is configured for the required boot mode before starting the recovered system.

Cristie Technical Support

Contact Numbers - Cristie Software (UK) Limited

Technical Support: +44 (0) 1453 847 009

Toll-Free US Number: 1-866-TEC-CBMR (1-866-832-2267)

Cristie Support links

Forum: forum.cristie.com

Web: www.cristie.com

Emails

Sales Enquiries: sales@cristie.com

Support: support@cristie.com

Address

Cristie Software Ltd,
New Mill,
Chestnut Lane,
Stroud,
GL5 3EW,
UK

Support Hours

Monday to Friday

5:00 AM - 5:00 PM Eastern Time

Out-of-Hours support available to customers with a valid Support Agreement - Severity 1 issues* only
UK Bank Holidays** classed as Out-of-Hours - Severity 1 issues only.

*Severity 1 issues are defined as: a production server failure, cannot perform recovery or actual loss of data occurring.

**For details on dates of UK Bank Holidays, please see www.cristie.com/support/

Note: Cristie Software Ltd. are continually expanding their product range in line with the latest technologies. Please contact the Cristie Sales Office for the latest product range.