Ahsay Backup

Ahsay Online Backup Restorer v8

User Guide for Windows

Ahsay Systems Corporation Limited

12 March 2021

A wholly owned subsidiary of
Ahsay Backup Software Development Company Limited
HKEx Stock Code: 8290

Copyright Notice

© 2021 Ahsay Systems Corporation Limited. All rights reserved.

The use and copying of this product is subject to a license agreement. Any other use is prohibited. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without prior written consent of Ahsay Systems Corporation Limited. Information in this manual is subject to change without notice and does not represent a commitment on the part of the vendor, Ahsay Systems Corporation Limited does not warrant that this document is error free. If you find any errors in this document, please report to Ahsay Systems Corporation Limited in writing.

This product includes software developed by the Apache Software Foundation (https://www.apache.org/).

Trademarks

Ahsay, Ahsay Cloud Backup Suite, Ahsay Online Backup Suite, Ahsay Offsite Backup Server, Ahsay Online Backup Manager, Ahsay A-Click Backup, Ahsay Replication Server, Ahsay BackupBox Firmware, Ahsay Universal Backup System and Ahsay NAS Client Utility, Ahsay Mobile are trademarks of Ahsay Systems Corporation Limited.

Amazon S3 is a registered trademark of Amazon Web Services, Inc., or its affiliates.

Apple and Mac OS X, macOS, and iOS are registered trademarks of Apple Computer, Inc.

Dropbox is a registered trademark of Dropbox Inc.

Google Cloud Storage, Google Drive, Google Authenticator, and Android are registered trademarks of Google Inc.

Wasabi Hot Cloud Storage is a registered trademark of Wasabi Technologies Inc.

Backblaze B2 Cloud Storage is a registered trademark of Backblaze Inc.

MariaDB is a registered trademark of MariaDB Corporation AB.

Lotus, Domino, and Notes are registered trademark of IBM Corporation.

Microsoft Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, OneDrive, OneDrive for Business, Microsoft Authenticator, and Microsoft Office 365 are registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle 11g, Oracle 12c, Oracle 18c, Oracle 19c, and MySQL are registered trademarks of Oracle Corporation.

Rackspace and OpenStack are registered trademarks of Rackspace US, Inc.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. www.redhat.com in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the U.S. and other countries.

Ubuntu is a registered trademark of Canonical Ltd.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

VMware ESXi, vCenter, and vSAN are registered trademarks of VMware, Inc.

All other product names are registered trademarks of their respective owners.

Disclaimer

Ahsay Systems Corporation Limited will not have or accept any liability, obligation or responsibility whatsoever for any loss, destruction or damage (including without limitation consequential loss, destruction or damage) however arising from or in respect of any use or misuse of reliance on this document. By reading and following the instructions in this document, you agree to accept unconditionally the terms of this Disclaimer and as they may be revised and/or amended from time to time by Ahsay Systems Corporation Limited without prior notice to you.

Revision History

Date	Descriptions	Type of modification
12 March 2021	Modified System Architecture diagram in Ch. 1.2; Modified features comparison table in Ch. 1.4; Reorganized and added Requirements in Ch. 3; Added Ch. 4 Limitations; Added login scenarios in Ch. 6; Reorganized Ch. 7	New / Modifications

Table of Contents

1 Overview 1

1.1 What is this software? 1

1.2 System Architecture 1

1.3 Why should I use AhsayOBR to restore backup data? 2

1.4 Features comparison between Client Backup Agent and AhsayOBR 3

2 About This Document 5

2.1 What is the purpose of this document? 5

2.2 What should I expect from this document? 5

2.3 Who should read this document? 5

2.4 Overview of the Document Content Structure 5

3 Prepare for Using AhsayOBR 6

3.1 Hardware Requirements 6

3.2 Software Requirements 6

3.3 Antivirus Exclusion Requirement 6

3.4 Upgrade VMware Tools Requirement 6

3.5 Encryption Key 7

3.6 Temporary Directory Requirement 7

3.7 Permissions 7

3.8 OpenDirect/Granular Restore 7

3.8.1 Windows Operating System 7

3.8.2 Available Spare Drive Letter 8

3.8.3 Network Requirements 8

3.8.4 Other Dependencies 8

4 Limitations 9

5 Download and Launch AhsayOBR 10

5.1 Download AhsayOBR 10

5.2 Launch AhsayOBR 12

5.2.1 Option 1: Online Installation 12

5.2.2 Option 2: Offline Installation 15

6 Start AhsayOBR 18

6.1 Login to AhsayOBR without 2FA 18

6.2 Login to AhsayOBR with 2FA enabled 20

7 Restore File Backup Sets 25

7.1 Restore Method 25

7.2 Normal Restore 25

7.3 OpenDirect Restore 36
8 Microsoft Hyper-V Guest VM Granular Restore 43
8.1 Requirements and Limitations 43
8.2 Start Granular Restore 43
9 VMware vCenter/ESXi Guest VM Granular Restore 51
9.1 Requirements and Limitations 51
9.2 Start Granular Restore 51
10 Contacting Ahsay 60
10.1 Technical Assistance 60
10.2 Documentation 60

1 Overview

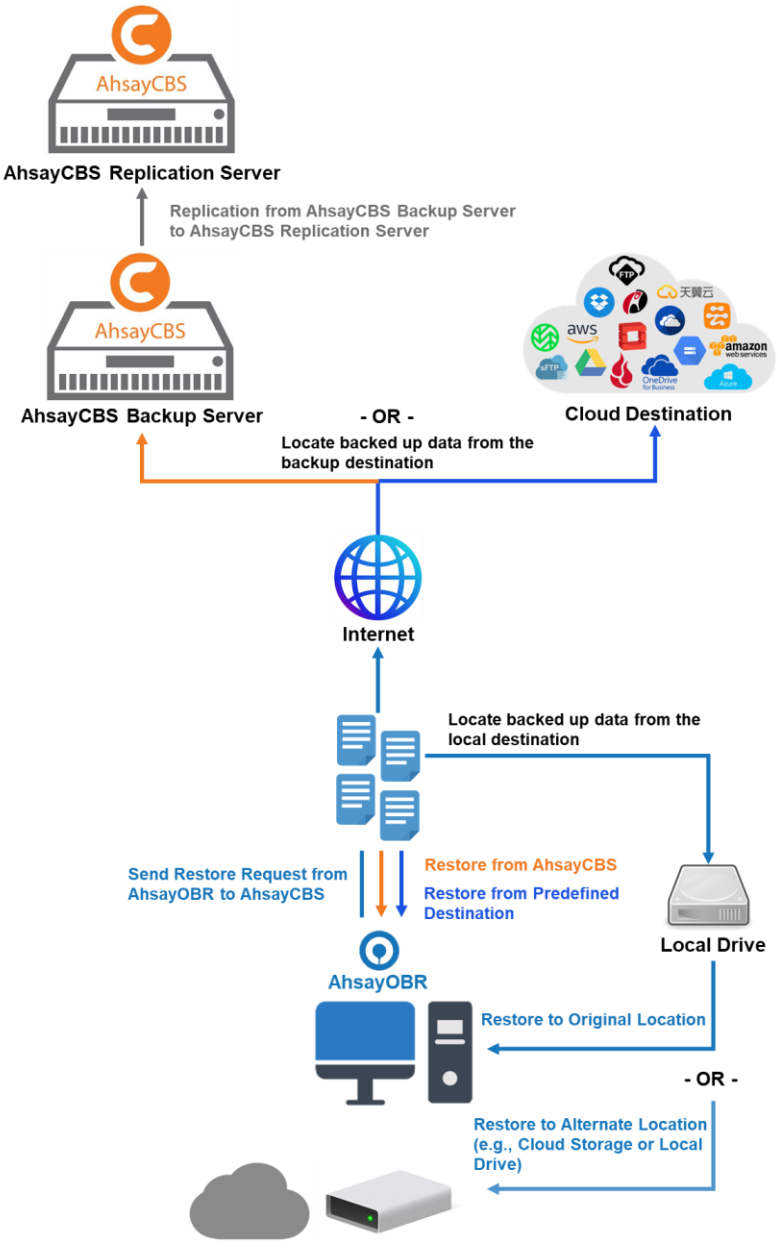
1.1 What is this software?

Ahsay brings you specialized restore software, namely Ahsay Online Backup Restorer (AhsayOBR), to provide a quick and secure solution for restoring your backup data anytime and anywhere. This software is designed specifically as a one-time restorer and is not served for performing backup and configuring any backup user settings. The software supports restoring data that is backed up with AhsayOBM or AhsayACB.

1.2 System Architecture

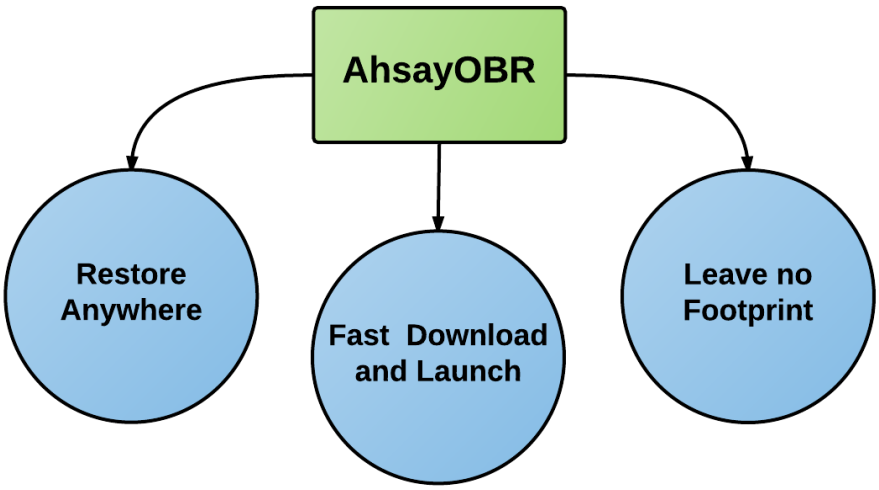
Below is the system architecture diagram illustrating the major elements involved in the process when you are using the AhsayOBR to restore data.

In this user guide, we will focus on information to get you started with using the software, as well as instructions on performing an end-to-end restore process.



*__Original location__ – the backed up data will be restored on the computer running the AhsayOBR under the same directory path as on the machine storing the backup source. For example, the backup source files are stored in C:\User\Downloads same as on the computer running the AhsayOBR.

1.3 Why should I use AhsayOBR to restore backup data?



Restore Anywhere

There may be times when you wish to restore your backed up data but have no access to the computer with the Client Backup Agent (AhsayOBM/AhsayACB) installed. AhsayOBR is exactly designed to cater to your needs under such circumstances.

You can now download and launch the AhsayOBR anytime and anywhere you like as long as you have a computer with a web browser installed and Internet connection.

Fast Download and Launch

Unlike a Client Backup Agent (AhsayOBM/AhsayACB) which is significantly larger in file size and takes longer time to install on your computer, AhsayOBR is a compact solution that can be downloaded and launched in a short period of time in just a few clicks.

Besides, the AhsayOBR is designed as a one-time restorer that will be removed from your computer completely after it is closed. All the restore log files or settings will also be removed from the computer altogether so you would not need to spend the time on uninstalling the software after you finished the restore.

Leave no Footprint

When you are trying to restore your backed up data remotely, the computer you use for restoring may not have the same level of security settings as the one you normally use for backup and restore onsite. Therefore, it may not be completely secure to install a Client Backup Agent (AhsayOBM/AhsayACB) to restore data because the backup agent will store information such as the backup user's personal info, backup set settings, backup/restore logs, etc. Using a Client Backup Agent for restore under such circumstances may pose potential threat to your personal and confidential information.

That is why the AhsayOBR is designed as a single-purpose restorer with high level of security protection and supporting Two-Factor Authentication (2FA). The restorer takes you right to the restore start point after login, where you can start performing a restore right away. It will also be removed completely after the restore is done, so you do not have to worry about leaving important information behind in the restore logs which could be viewed by a third party.

1.4 Features comparison between Client Backup Agent and AhsayOBR

While you can still download a Client Backup Agent (AhsayOBM/AhsayACB) to restore data, AhsayOBR gives a quick, direct and secure solution just for the data restore purpose. Below is a table comparing some major features of both tools, and the pros and cons of using them.

Feature	Tool	Pros	Cons
Installation	**AhsayOBR**	◉ No installation required ◉ Faster to launch	Required to launch every time you use
	Client Backup Agent	One-time installation	Larger installer size hence longer installation time
Run Direct Restore	**AhsayOBR**	N/A	Run Direct restore for VMware and Hyper-V servers is **NOT** supported, since AhsayOBR is not a Client Backup Agent and therefore NFS is not bundled along with the software. NFS is a mandatory item for performing Run Direct restore for VMware and Hyper-V servers.
	Client Backup Agent	Support Run Direct restore for both VMware and Hyper-V servers.	N/A
OpenDirect Restore	**AhsayOBR**	OpenDirect restore allows you to view and download individual files from a compressed or image file, without having to restore compressed file or image file first. OpenDirect restore gives you the flexibility to restore selective file(s) quickly, so it saves you time and effort to achieve your restore goal.	To ensure optimal restore performance, the backup of the files in an OpenDirect file backup set will **NOT** be encrypted and compressed, therefore, you may have to take these factors in consideration when selecting this restore option.
	Client Backup Agent		

Granular Restore	**AhsayOBR**	In some cases, you may only need to restore a few individual file(s) from the guest VM, therefore, granular restore gives you a fast, convenient, and flexible tool to restore selected file(s) from a guest VM quickly.	To make ensure optimal restore performance, the backup of the guest VM will **NOT** be encrypted and compressed, therefore, you may have to take this factor in consideration when using this restore method.
	Client Backup Agent		
Cross platform usage	**AhsayOBR**	Although both tools are available for use on various platforms, e.g., Windows, Mac, Linux, FreeBSD etc., cross platform restore is **NOT** recommended. For example, files backed up on Windows are not recommended to restore on a Mac/Linux/FreeBSD machine. Not supported on Synology DSM or QNAP QTS platforms.	
	Client Backup Agent		
Compatibility	**AhsayOBR**	N/A	Does not support restore of photos and videos backed up using Ahsay Mobile.
	Client Backup Agent	N/A	Support restore of backup set created by the same type of Client Backup Agent only. Example: backup set created on AhsayOBM can only be restored by AhsayOBM.

2 About This Document

2.1 What is the purpose of this document?

This document aims at introducing the AhsayOBR software and its features, providing all necessary information to download and launch the AhsayOBR software and instructions on performing restore.

2.2 What should I expect from this document?

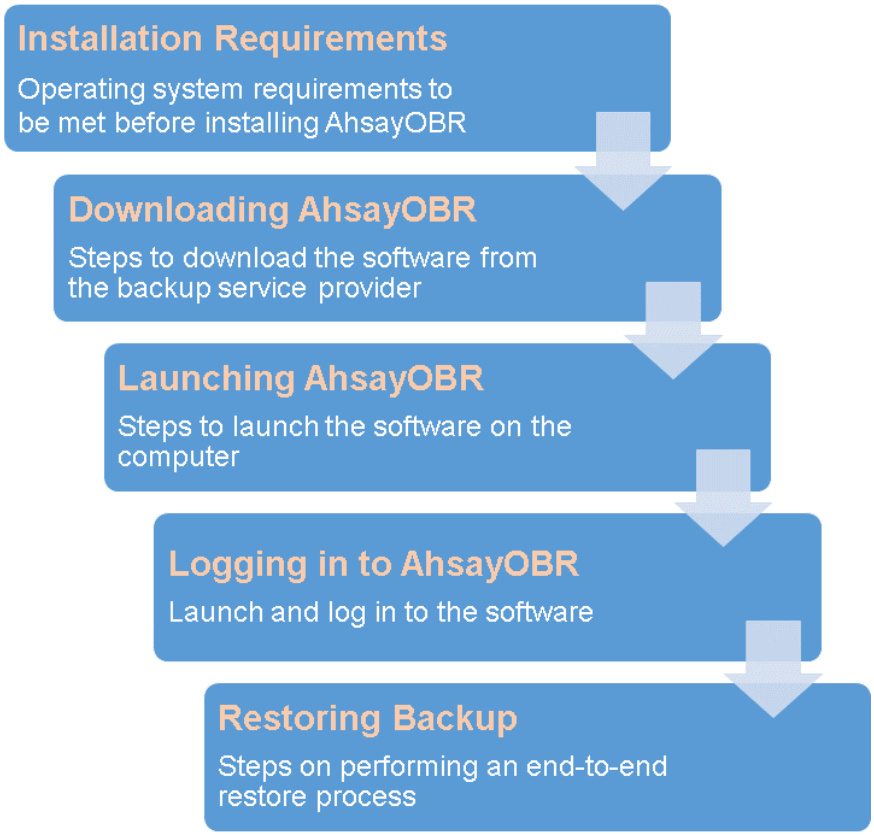
After reading through this documentation, you can expect to have sufficient knowledge to download and launch the AhsayOBR software, as well as to perform a restore

2.3 Who should read this document?

This document is intended for backup users who need to perform restore while having no access to their Client Backup Agent (AhsayOBM/AhsayACB) or for those who need to quickly recover file(s) on another machine or device with minimal effort.

2.4 Overview of the Document Content Structure

Below is a flow chart illustrating the major chapters this document will cover in sequence.



3 Prepare for Using AhsayOBR

3.1 Hardware Requirements

You can launch the AhsayOBR on a physical machine or on a virtual machine. The hardware requirements for launching AhsayOBR is the same as installing AhsayOBM.

Refer to the link below for details of the minimum and recommended hardware requirements:
FAQ: Ahsay Hardware Requirement List (HRL) for version 8.1 or above

Refer to the following article for the list of compatible operating system for OpenDirect and Granular Restore:
FAQ: Ahsay Software Compatibility List (SCL) for Granular and OpenDirect Restore (5250)

3.2 Software Requirements

Refer to the link below to see the list of the system requirements for software compatibility:
FAQ: Ahsay Software Compatibility List (SCL) for version 8.1 or above

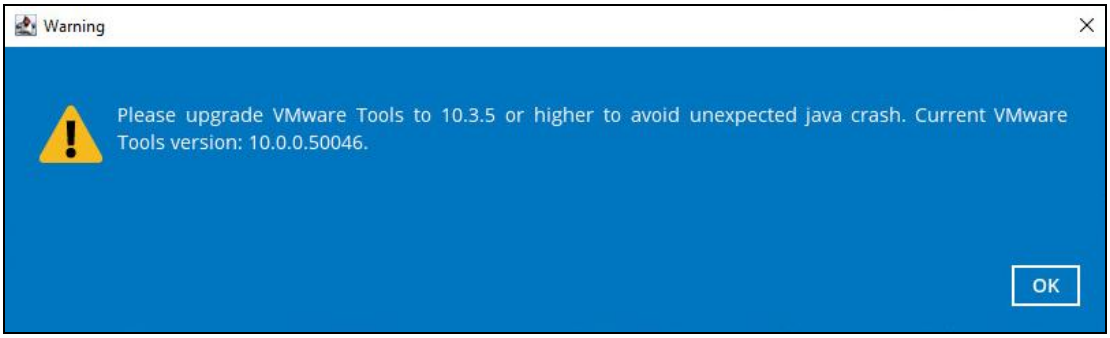
3.3 Antivirus Exclusion Requirement

To optimize performance of AhsayOBR on Windows, and to avoid conflict with your antivirus software, refer to the following KB article for the list of processes and directory paths that should be added to all antivirus software white-list / exclusion list:
FAQ: Suggestion on antivirus exclusions to improve performance of Ahsay software on Windows

3.4 Upgrade VMware Tools Requirement

To avoid unexpected java crash, if the Windows machine is a guest VM hosted on a VMware Host, then it is highly recommended that the VMware tools version installed on the guest VM must be 10.0.5 or above.

Below is the warning message that will be displayed if the version of the VMware Tools is less than 10.0.5.



NOTE

For more information about VMware Tools upgrade, refer to the following article:
https://wiki.ahsay.com/doku.php?id=public:5288_ahsayobc_crash_on_vm_with_vmware_tools_pre-10.0.5.

3.5 Encryption Key

If the backup set(s) are enabled with an encryption key, then the encryption key for the backup set(s) is required to successfully access and restore the data.

3.6 Temporary Directory Requirement

The temporary directory folder should have at least the same available size as the compressed or image file to be restored and should be located on a local drive to ensure optimal performance.

3.7 Permissions

The Windows login account used for installation and operation of the AhsayOBR client machine requires Administrator privileges.

3.8 OpenDirect/Granular Restore

3.8.1 Windows Operating System

AhsayOBR must be installed on a 32 bit or 64-bit Windows Operating System as libraries for OpenDirect only supports Windows platform.

Windows 7 SP1 or above	Windows 8	Windows 8.1
Windows 10	Windows 2008 R2 SP1 or above	Windows 2012
Windows 2012 R2	Windows 2016	Windows 2019

For MS Hyper-V, AhsayOBR must be installed on a 32 bit or 64-bit Windows Operating System as libraries for Hyper-V Granular Restore only supports Windows platform.

For VMware, AhsayOBR must be installed on a 64-bit Windows machine as libraries for Granular only supports 64-bit Windows operating system for VMware ESXi/VCenter.

AhsayOBR must be installed on the following Windows Operating Systems:

Operating System	MS Hyper-V Backup Set	VMware ESXi/vCenter Backup Set
Windows 7 SP1 or above	N\A	Compatible
Windows 8	Compatible	Compatible
Windows 8.1	Compatible	Compatible
Windows 10	Compatible	Compatible
Windows 2008 R2 SP1 or above	N\A	Compatible
Windows 2012	Compatible	Compatible
Windows 2012 R2	Compatible	Compatible
Windows 2016	Compatible	Compatible
Windows 2019	Compatible	Compatible

3.8.2 Available Spare Drive Letter

One spare drive letter must be available on the Windows machine for the OpenDirect/Granular restore process, as the compressed file or image (for OpenDirect restore) or VDDK virtual disk (for Granular restore) is mounted on Windows as a logical drive. AhsayOBR will automatically take the next available drive letter in alphabetical order for the compressed or image file or for the mounted virtual disk.

NOTES

- The Windows drive letters A, B, and C are not used by OpenDirect/Granular Restore.
- The assigned drive letter(s) will be released once you exit from AhsayOBR UI.

3.8.3 Network Requirements

The recommended minimum network speed is **at least 100Mbps download speed**.

The network bandwidth requirements will increase in proportion to the size of the guest VM, compressed file/image and or the incremental delta chain length to ensure optimal performance. Working with limited network bandwidth may severely affect the granular restore performance.

You can use an online network speed test website (e.g., www.speedtest.net) to get an idea of the actual bandwidth of the machine.

3.8.4 Other Dependencies

The following dependencies are restore-related and need to be installed on the AhsayOBR machine for OpenDirect/Granular restore to work. Absence of these elements will not affect the backup job but would cause the restore to fail.

- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
  https://www.microsoft.com/en-hk/download/confirmation.aspx?id=48145
- Microsoft Visual C++ 2015 Redistributable Update 3 RC
  https://www.microsoft.com/en-us/download/details.aspx?id=52685
- Update for Universal C Runtime in Windows
  https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows
  - Prerequisites for **Windows 8.1** or **Windows Server 2012 R2**
    - Install KB2919442
      https://support.microsoft.com/en-us/help/2919442/march-2014-servicing-stack-update-for-windows-8.1-and-windows-server-2012-r2

      Install KB2919355
      https://support.microsoft.com/en-us/help/2919355/windows-rt-8.1,-windows-8.1,-and-windows-server-2012-r2-update-april-2014
- Microsoft Security Advisory 3033929 for **Windows 7** and **Windows Server 2008 R2**
  https://technet.microsoft.com/en-us/library/security/3033929.aspx

4 Limitations

1. AhsayOBR is not supported on Synology DSM or QNAP QTS platforms.
2. AhsayOBR does not support restore of photos and videos backed up using Ahsay Mobile.
3. Enhanced Network Drive Support

   Not supported for “Restore Raw file” and “Restore to local computer” options.

5 Download and Launch AhsayOBR

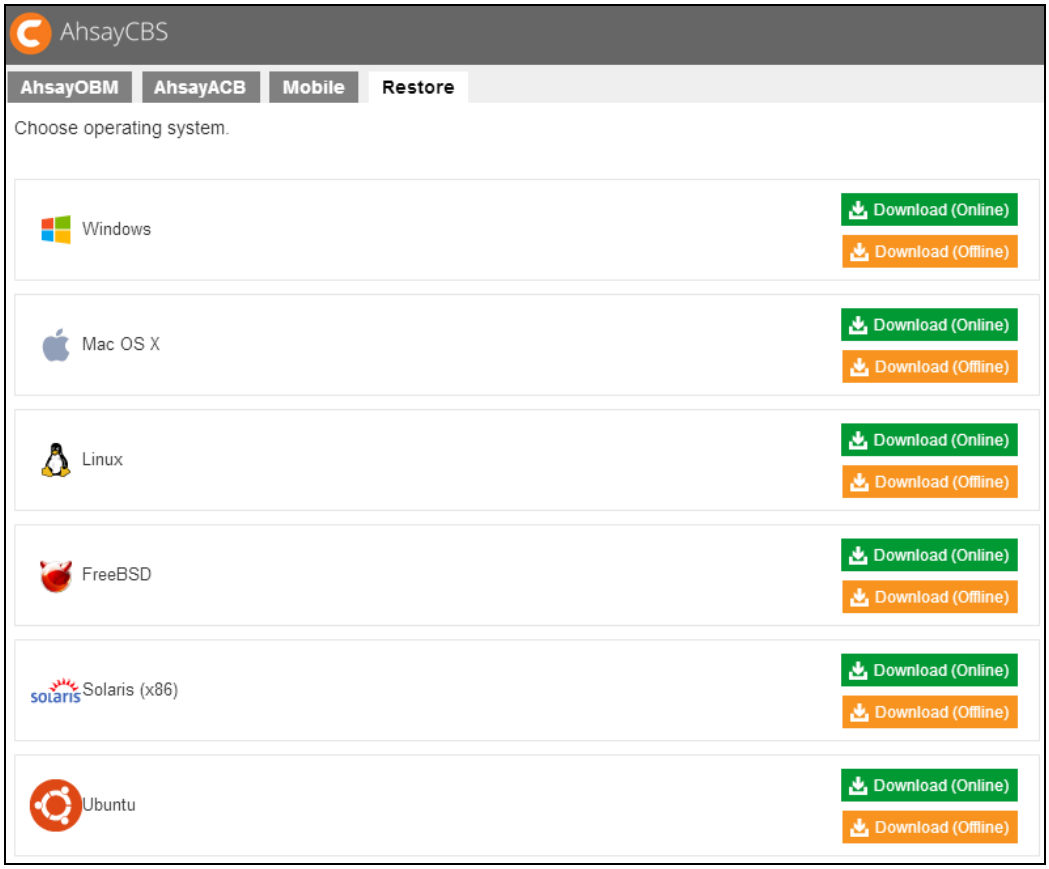
There are two installation modes for AhsayOBR: online installation and offline installation. Below is the table of comparison between online installation and offline installation.

	Online Installation	Offline Installation
Installation Time	➢ Takes more time as it needs to download the binary and component files (150MB to 272MB depending on operating system) each time the installation is run. ➢ Online installer size is 9KB to 2MB depending on operating system as it contains only the initial installation package files.	➢ Takes less time as all the necessary binary and component files are already available in the offline installer, and offline installer can be downloaded once but can be reused many times. ➢ Offline installer size is 150MB to 272MB depending on operating system as it contains all the necessary binary and component files.
Deployments	➢ Suitable for sites with fast and stable internet connection as internet connection is needed each time when an installation is run. ➢ A slow internet connection will result in longer installation time and interrupted, or unstable internet connection may lead to unsuccessful installation. ➢ Ensures the latest version of the product is installed.	➢ Suitable for client sites with metered internet connections as once the offline installer is downloaded, internet connection is not needed each time when an installation is run. ➢ May not be the latest version.

5.1 Download AhsayOBR

1. In a web browser, click the blue icon on the top right corner to open the download page for the AhsayOBR installation package file from your backup service provider's website.

2. In the **Restore** tab of the download page, choose the AhsayOBR installer for the appropriate operating system.

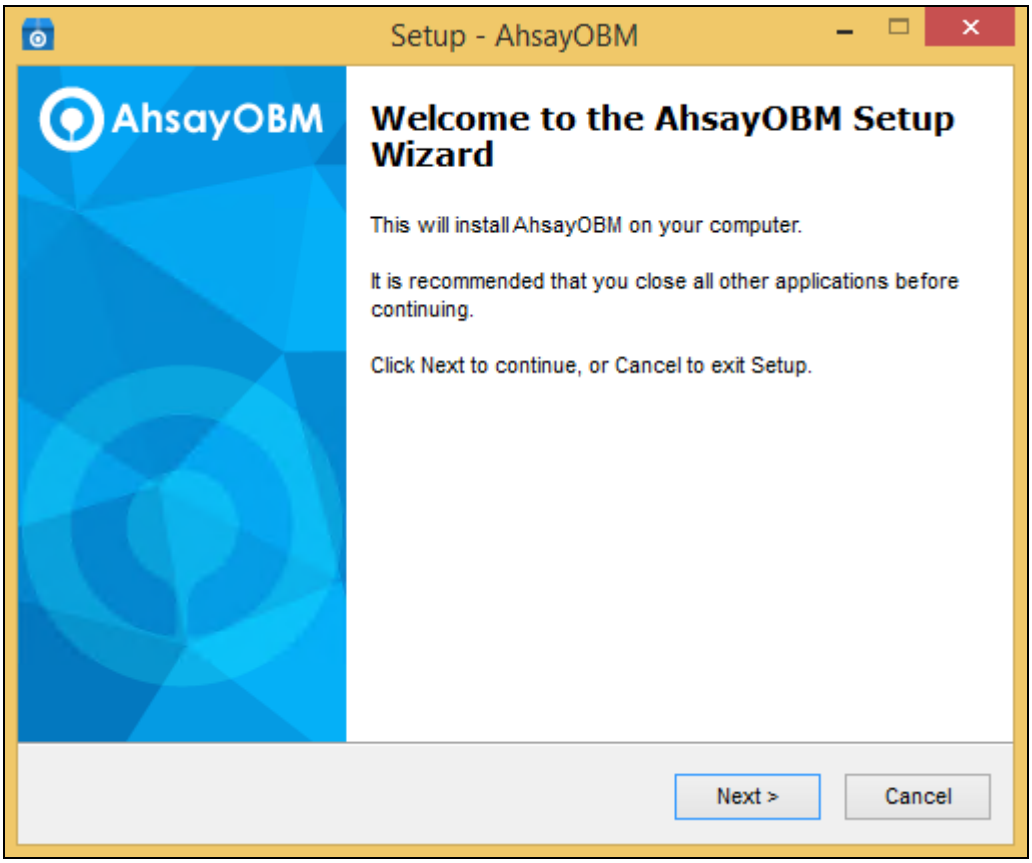


3. In the **Windows** section, click on the **Download (Online)** or **Download (Offline)** button to download the AhsayOBR installation package.

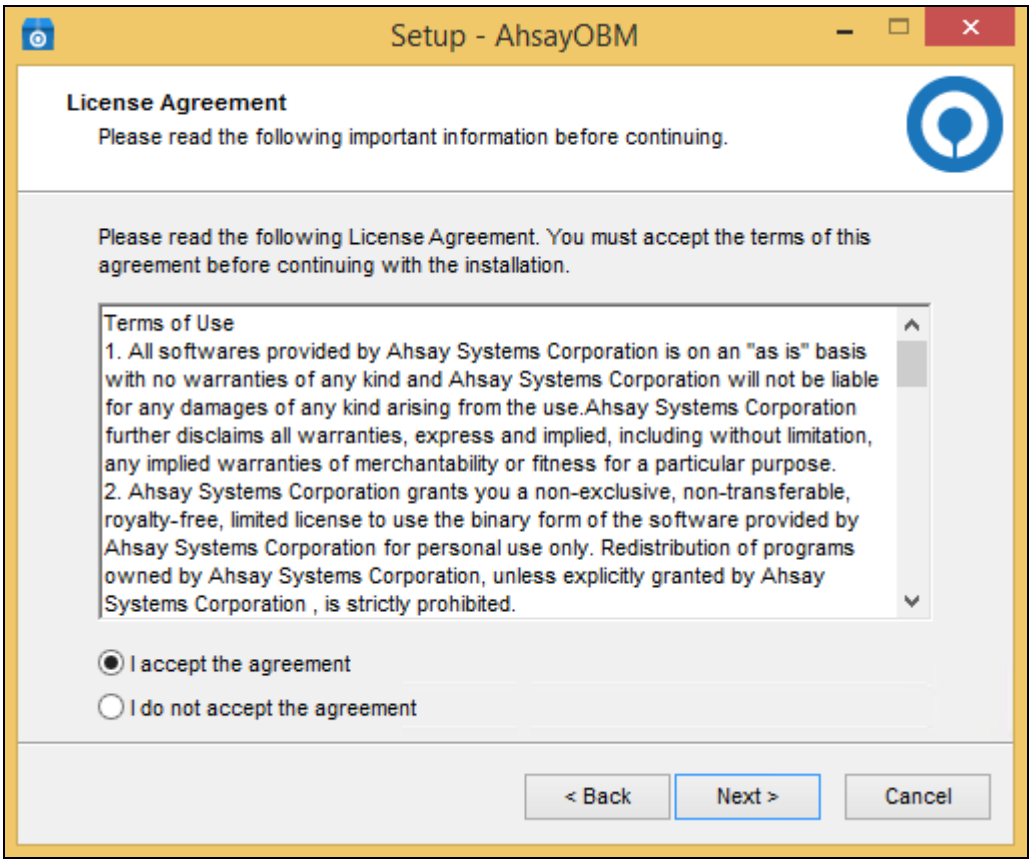
5.2 Launch AhsayOBR

5.2.1 Option 1: Online Installation

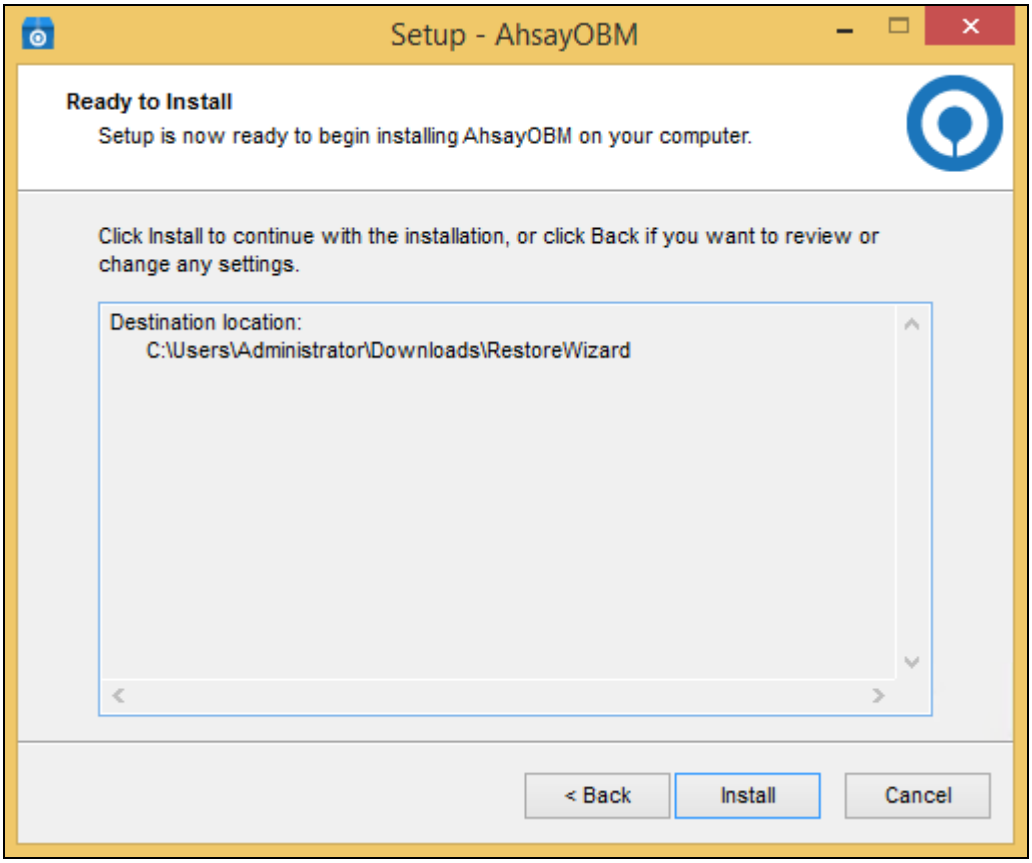
1. Launch the file you have downloaded from AhsayCBS. Refer to Ch. 5.1 Download AhsayOBR.
2. Click **Next** to proceed.



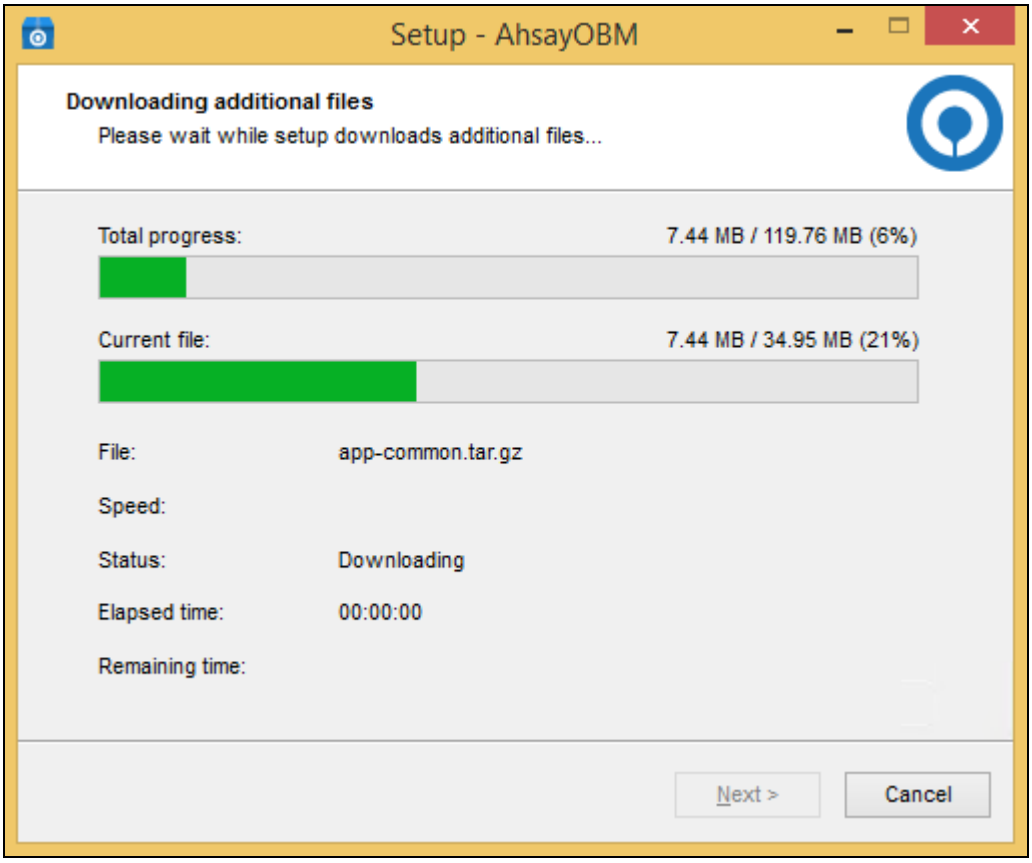
3. Select **I accept the agreement** after reading the license agreement. Then click **Next** to proceed.



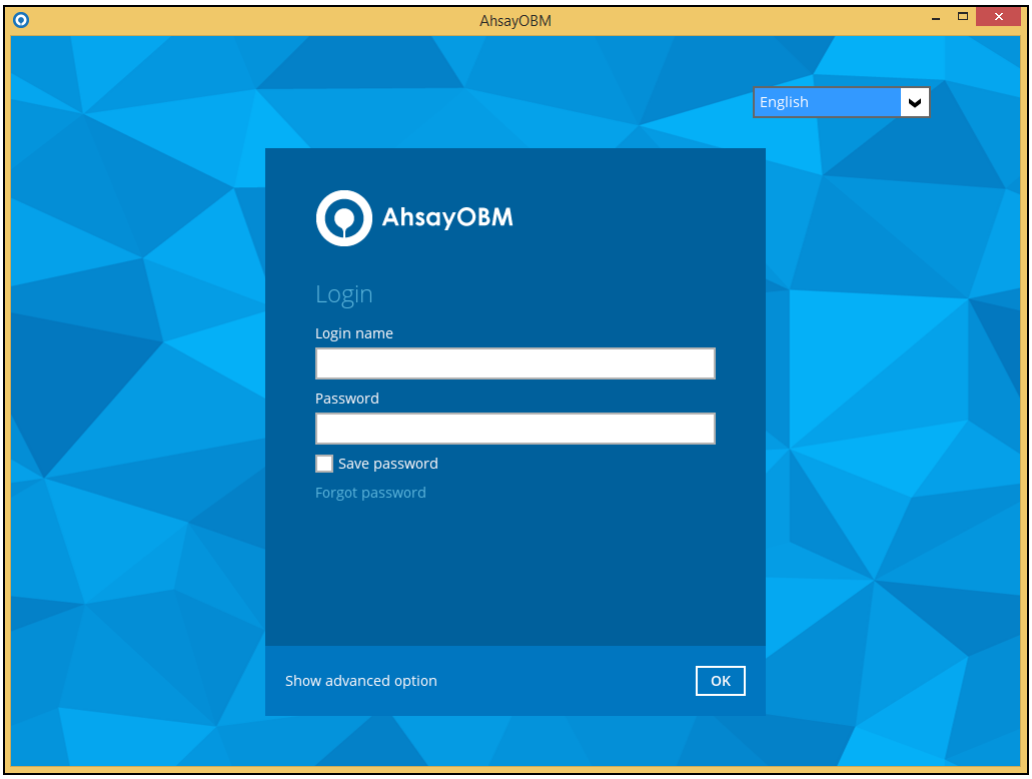
4. The installation will start after you click **Install**.



5. The component files will be downloaded first during installation.

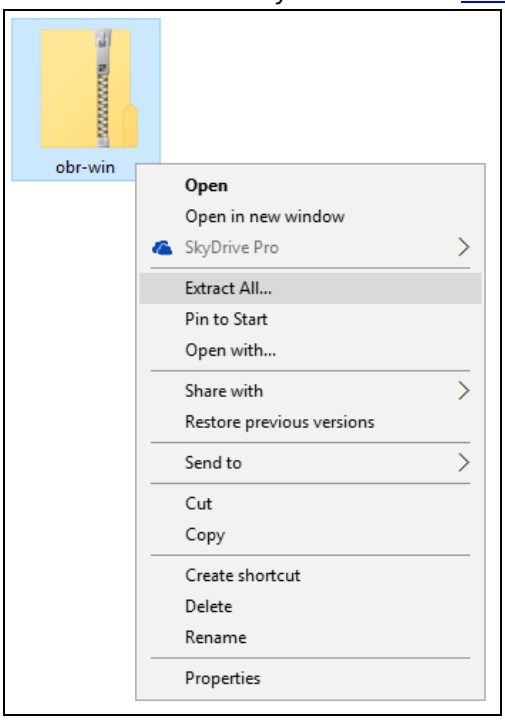


6. AhsayOBR will be displayed after a successful installation.

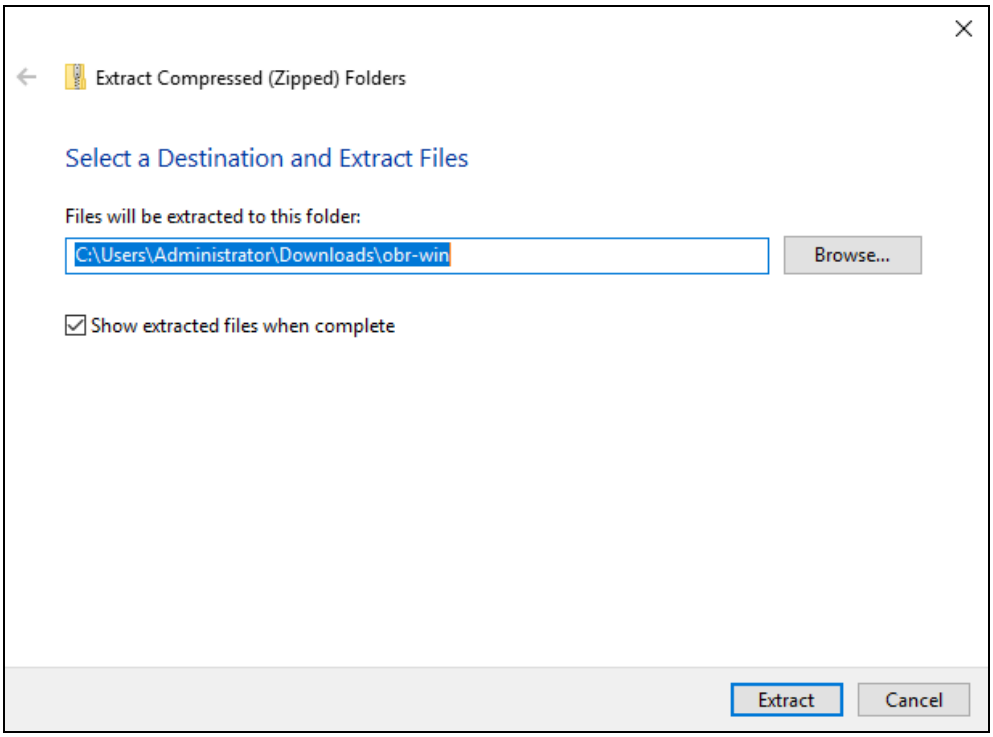


5.2.2 Option 2: Offline Installation

1. Extract the offline installation package file (obr-win.zip) that you have downloaded from AhsayCBS. Refer to Ch. 5.1 Download AhsayOBR.

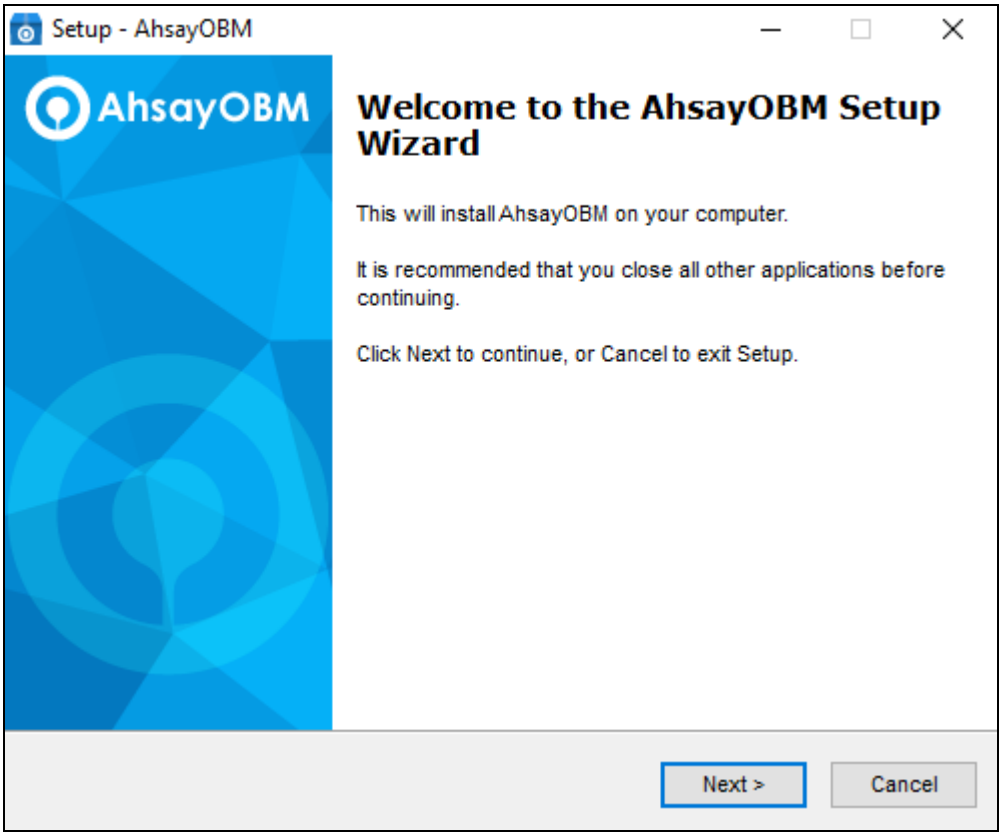


2. Select a destination where the files will be extracted, then extract the files.

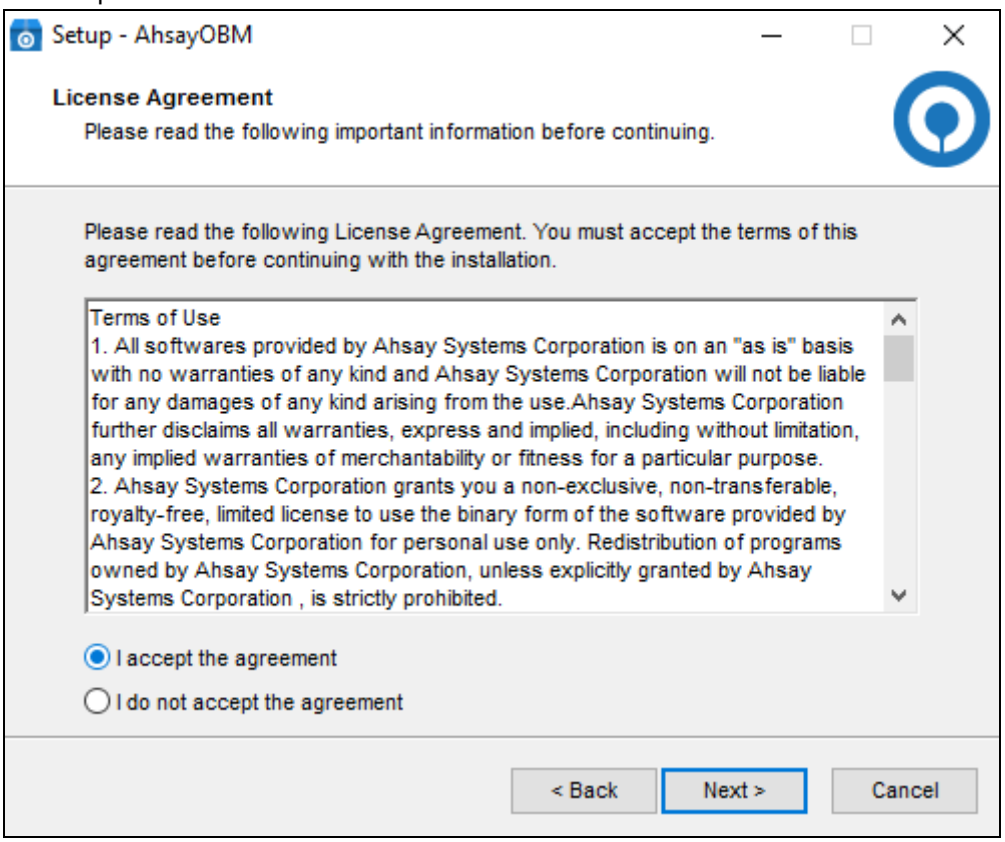


3. Launch the installer you have extracted from the zip format file.

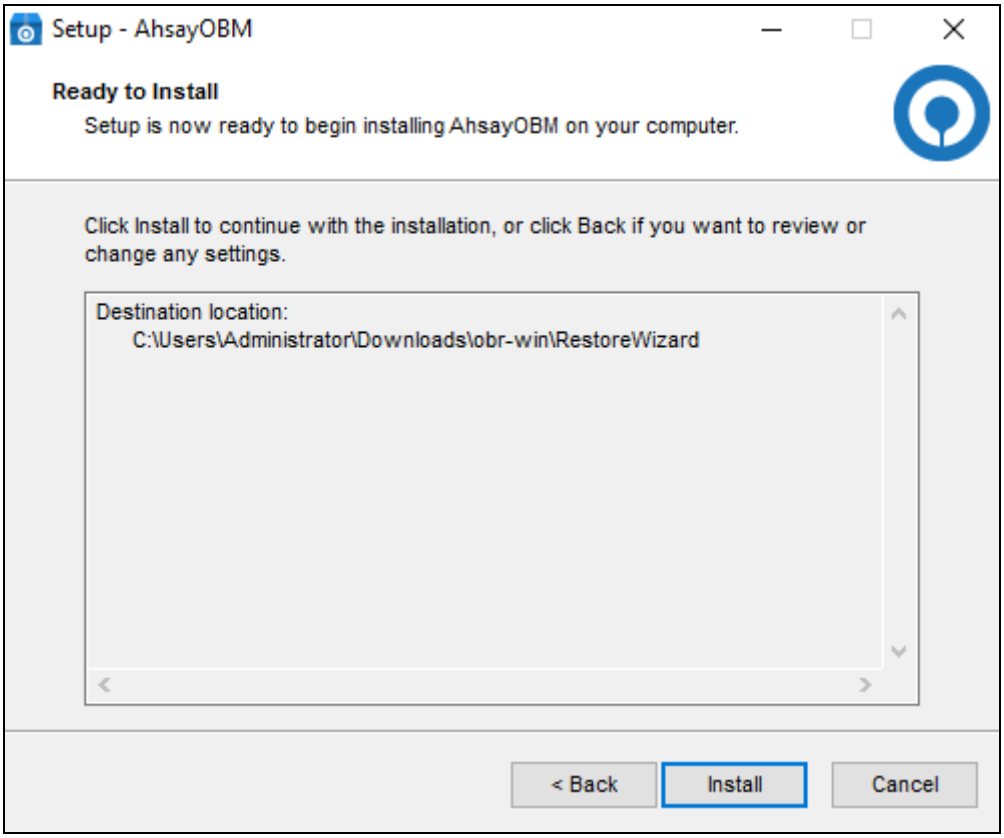
4. Click **Next** to proceed.



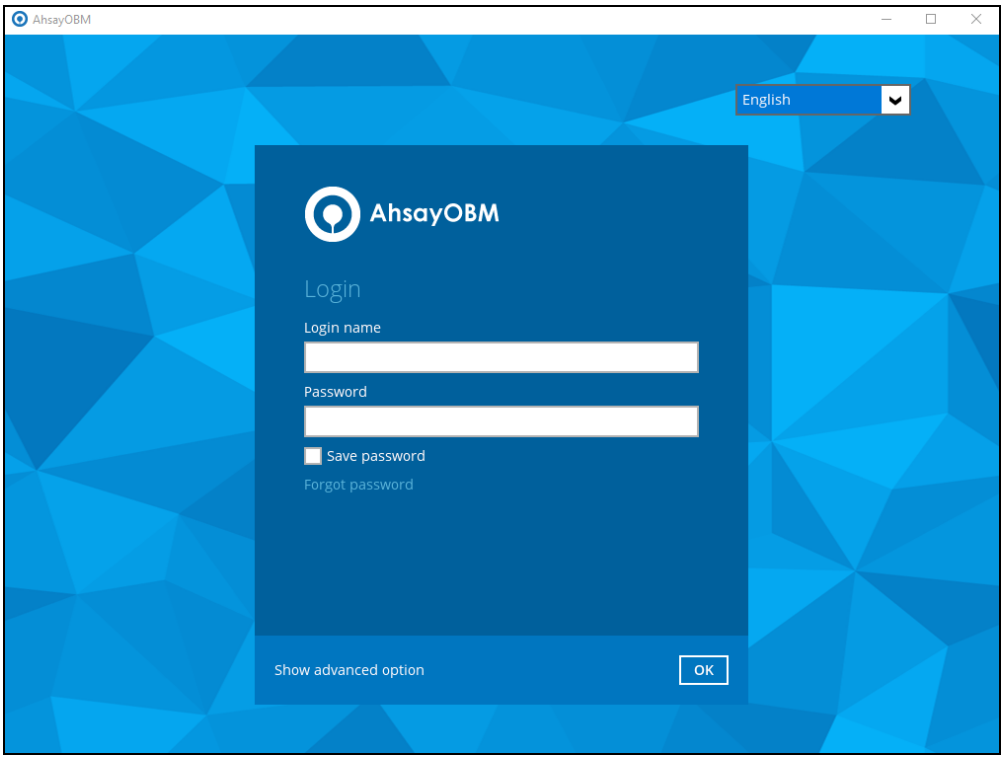
5. Select **I accept the agreement** after reading the license agreement. Then click **Next** to proceed.



6. The installation will start after you click **Install**.



7. AhsayOBR will be displayed after a successful installation.

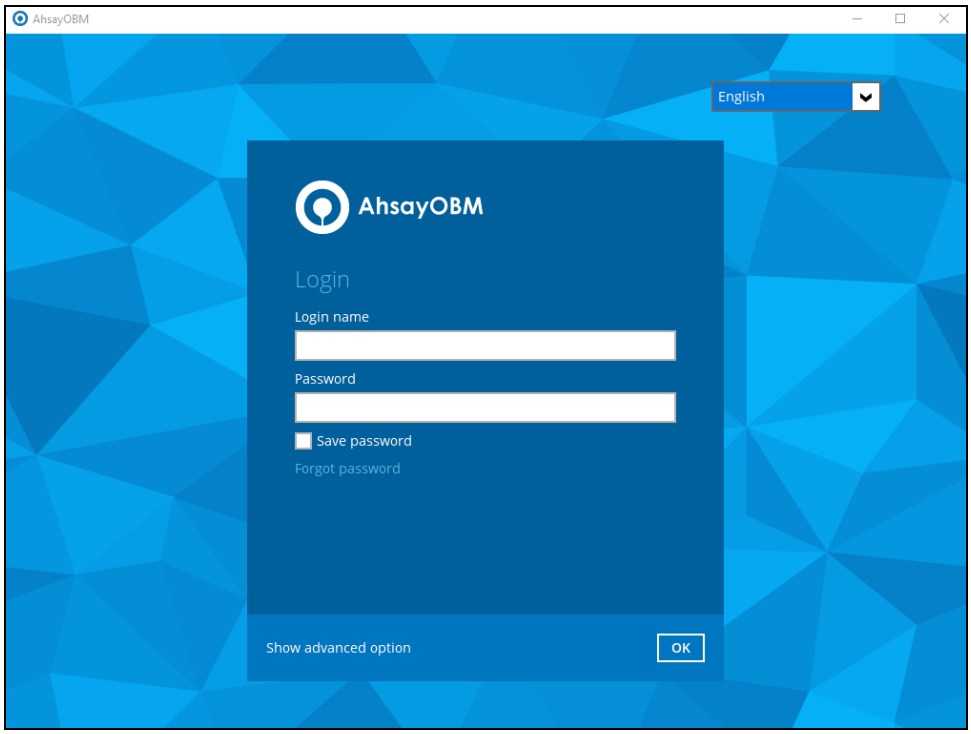


6 Start AhsayOBR

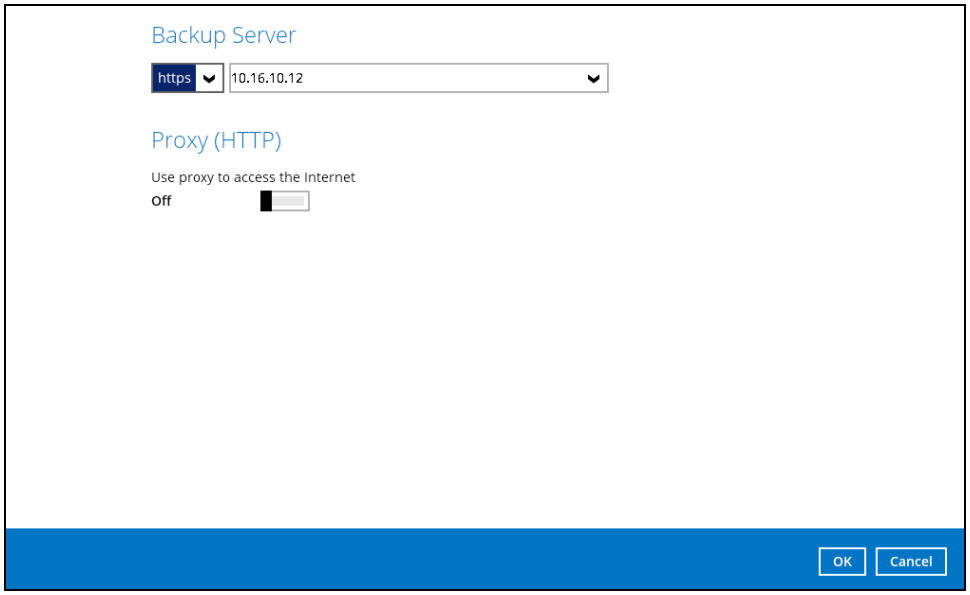
Starting with AhsayOBR v8.5.0.0, Two-Factor Authentication (2FA) is introduced to provide high level of security protection to the backup data that will be restored. With this new feature, there are several scenarios that will be encountered for first time login. Login steps for the different scenarios will be discussed in this chapter.

6.1 Login to AhsayOBR without 2FA

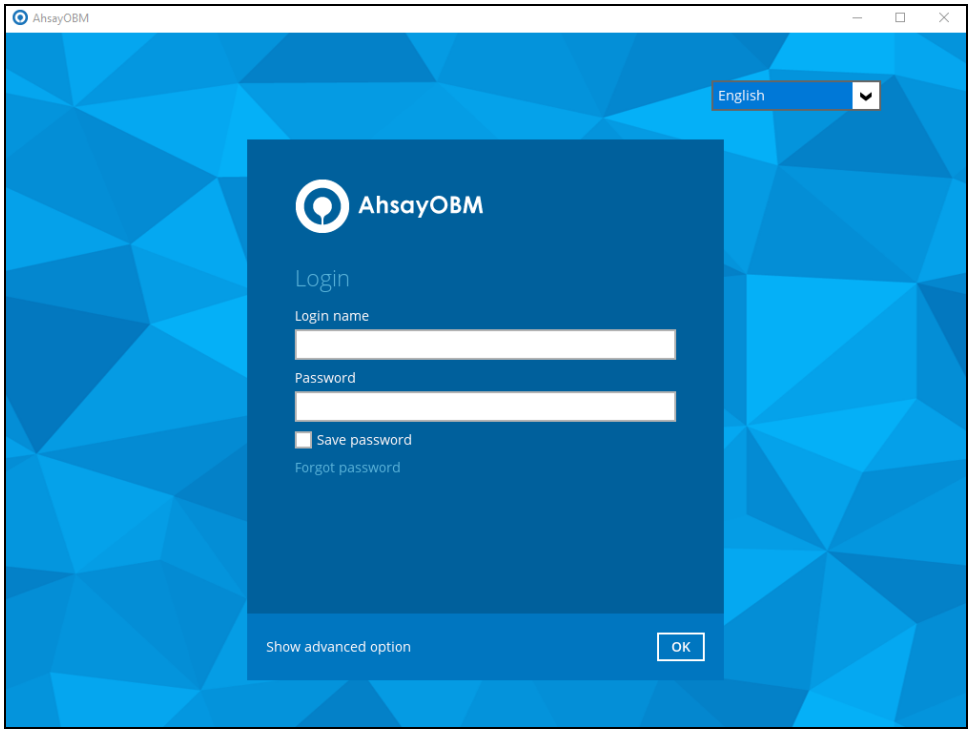
1. The AhsayOBR will launch automatically, and you will see the following screen. Click **Show advanced option** to configure the network settings.



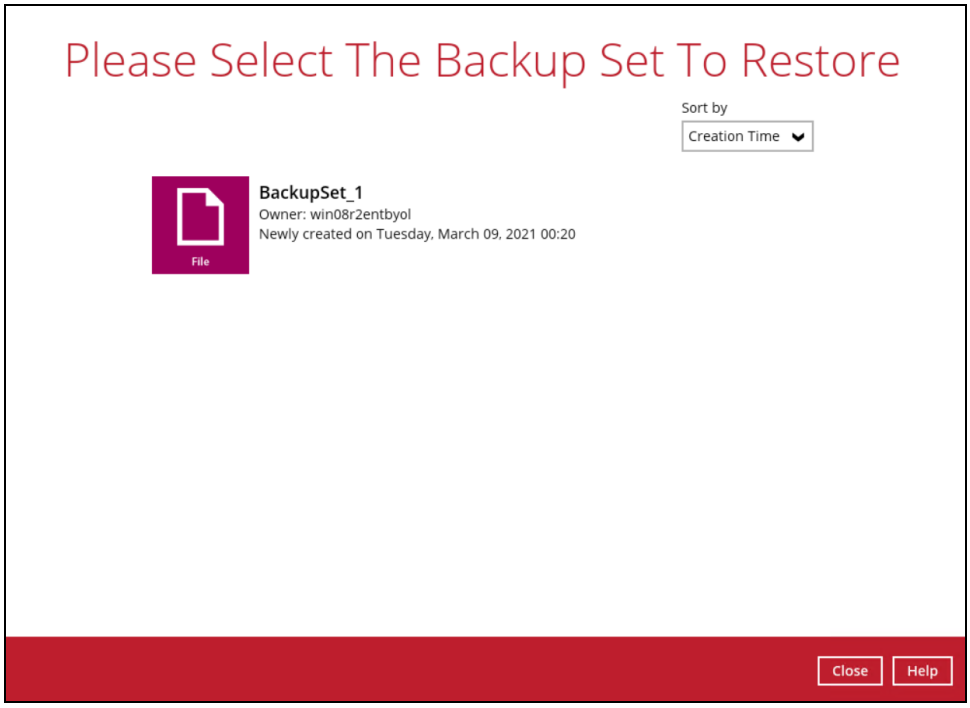
2. Enter the Backup Server address provided by your backup service provider. If you need to use proxy to access the Internet, enable the Proxy feature and fill in the relevant information. Click **OK** when you are done with the settings.



3. Enter the login name and password of your Client Backup account, then click **OK** to log in.

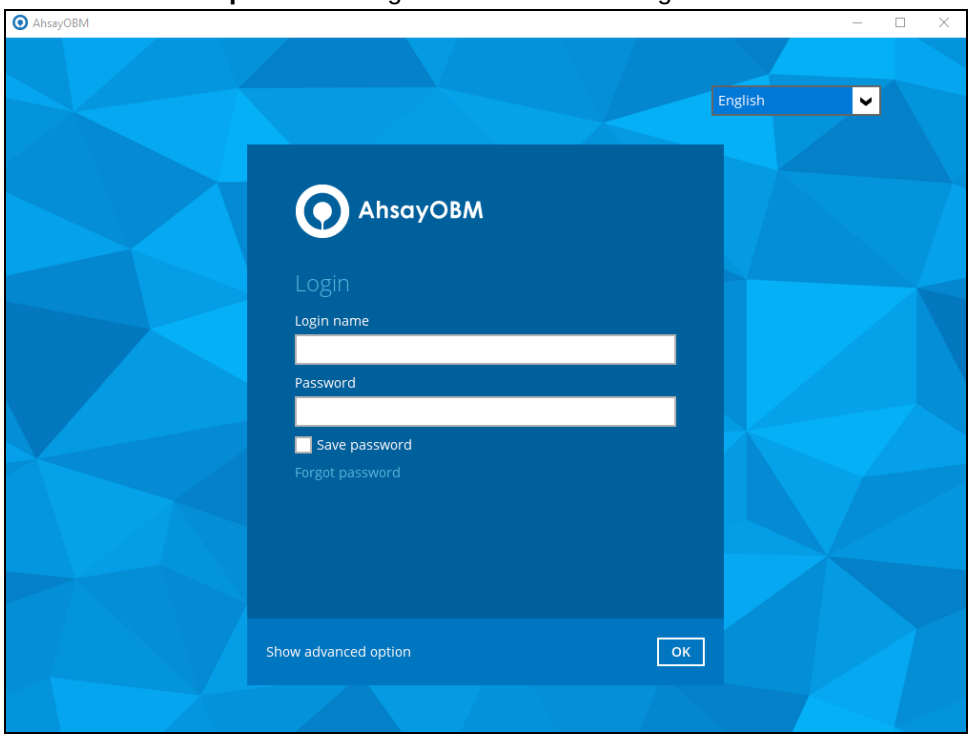


4. After a successful login, the available backup set(s) for restore will be displayed.

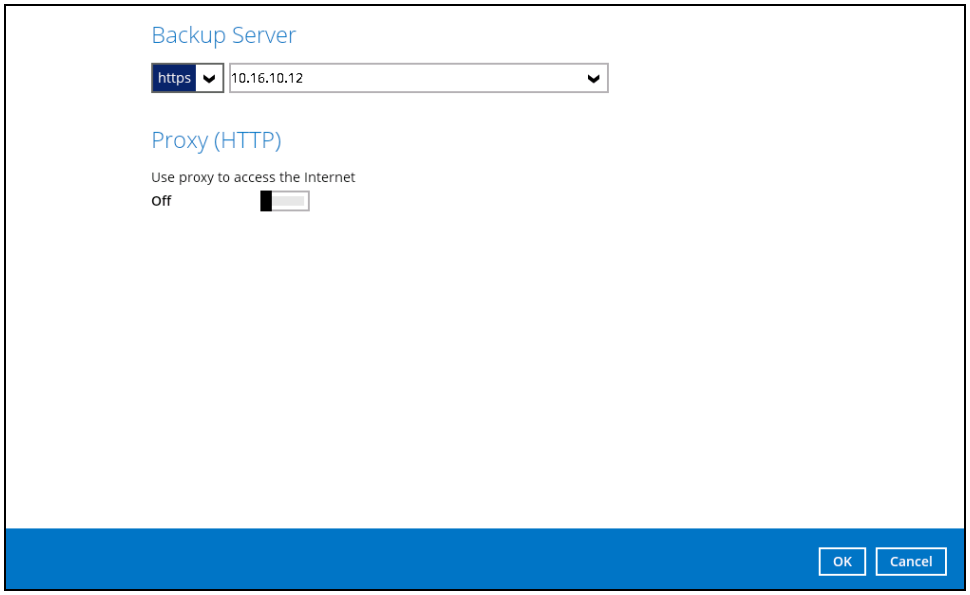


6.2 Login to AhsayOBR with 2FA enabled

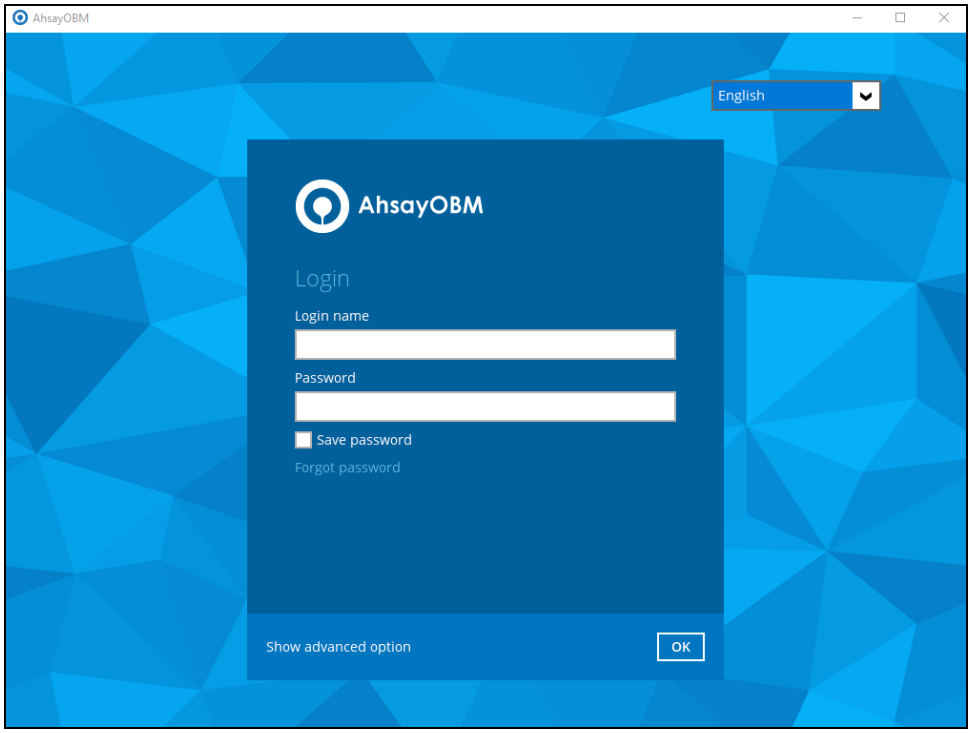
1. The AhsayOBR will launch automatically, and you will see the following screen. Click **Show advanced option** to configure the network settings.



2. Enter the Backup Server address provided by your backup service provider. If you need to use proxy to access the Internet, enable the Proxy feature and fill in the relevant information. Click **OK** when you are done with the settings.

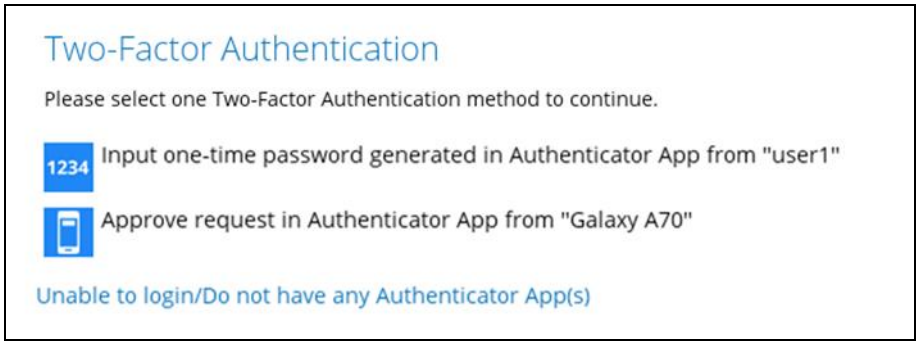


3. Enter the login name and password of your Client Backup account, then click **OK** to log in.



4. If the 2FA setup is enabled, the following screen will be displayed. Select the authentication method to continue with the login.

   Example: the AhsayOBM/AhsayACB user account is setup with 2FA using Ahsay Mobile Authenticator on a Mobile device called “Galaxy A70” and a third party TOTP Authentication app such as Google Authenticator, Microsoft Authenticator, LastPass etc.

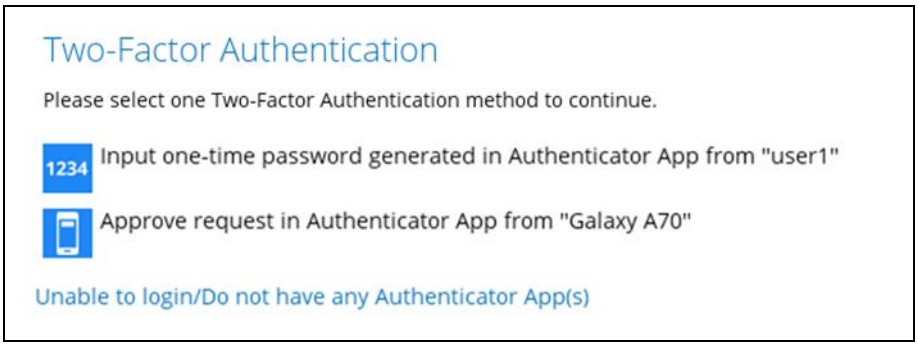


   There are two authentication method to choose from which are:

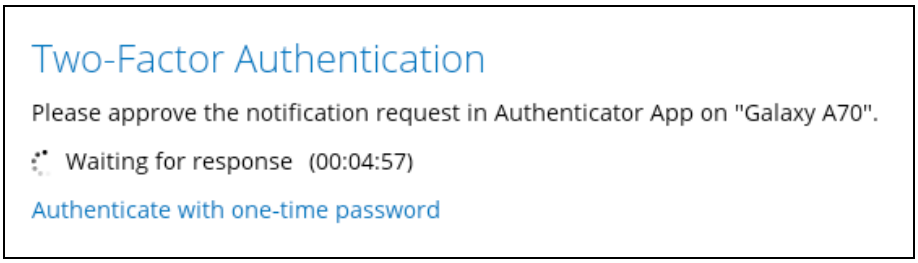
   - Ahsay Mobile Authenticator
   - TOTP Authentication App

   If **Ahsay Mobile** will be used as authenticator, follow the steps below to log in.

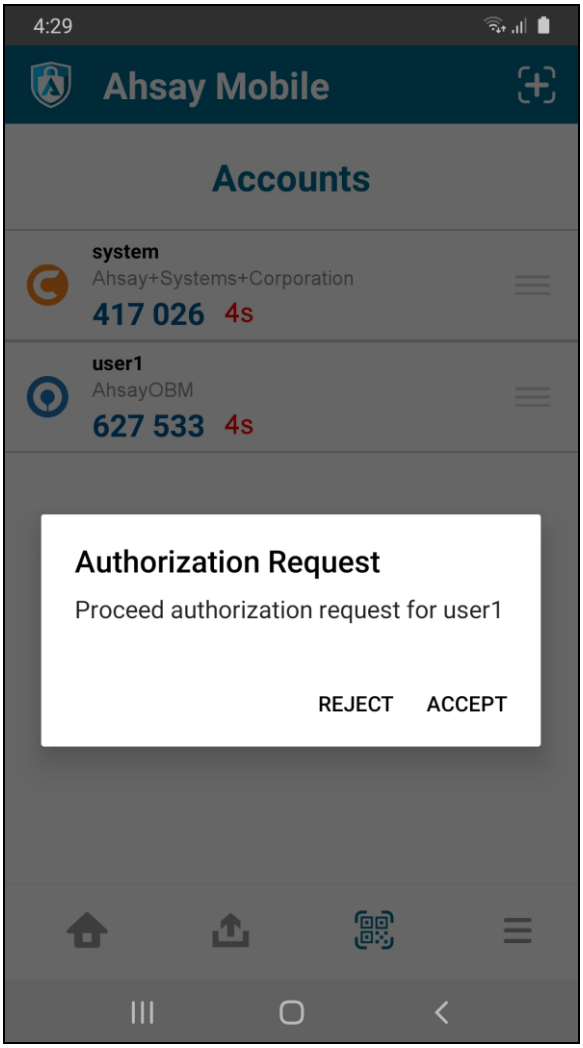
   i. Click **Approve request in Authenticator App** to proceed with the login.



   ii. Accept the authorization request sent to your device.

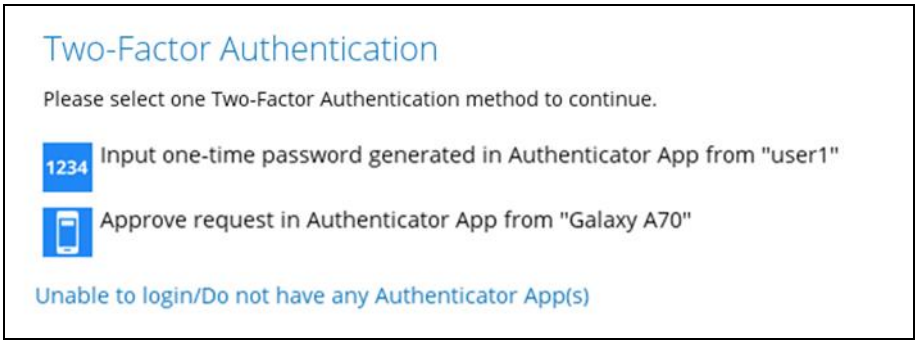


This is a sample of the authorization request sent to Ahsay Mobile.

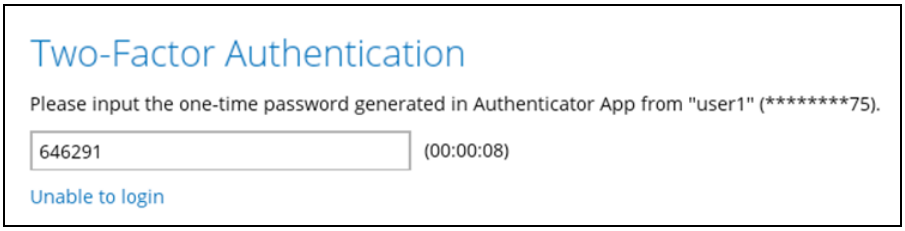


If a third-party **TOTP Authenticator App** will be used, follow the steps below to log in.

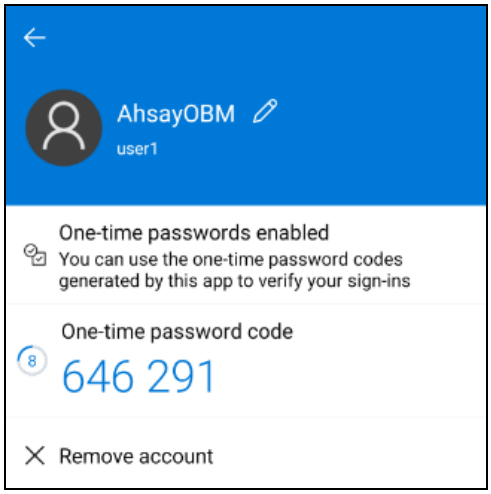
i. Click **Input one-time password generated in Authenticator App** to proceed with the login.



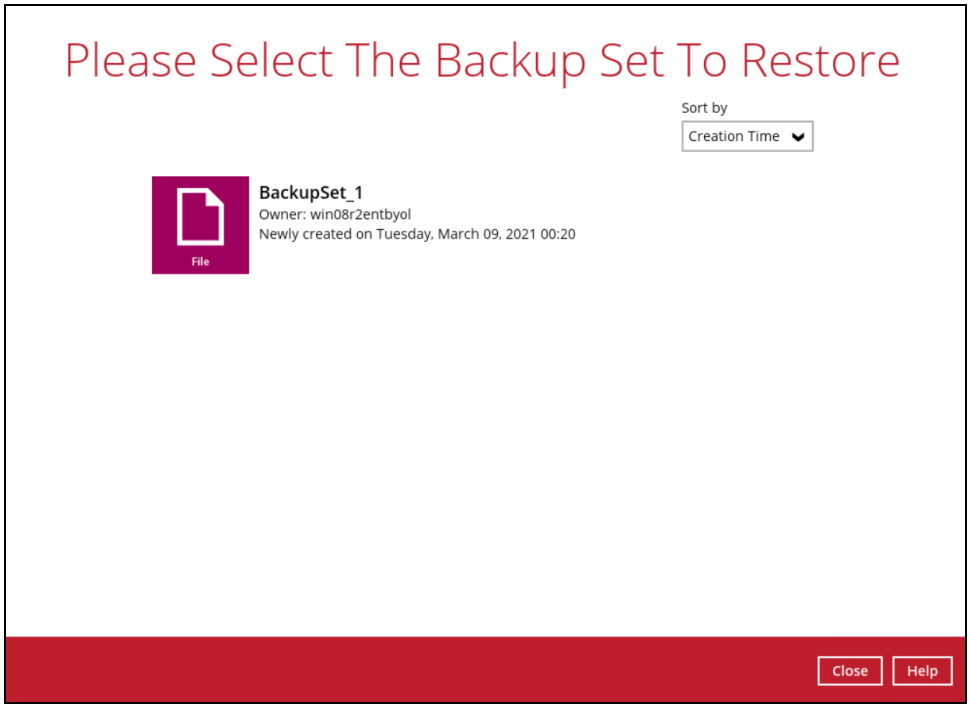
ii. Enter the one-time password that is generated by the app and click **Next**.



This is a sample of the one-time password generated in the third-party Authenticator App Microsoft Authenticator.



5. After a successful login, the available backup set(s) for restore will be displayed.



7 Restore File Backup Sets

7.1 Restore Method

There are two restore methods available in AhsayOBR:

- **Normal Restore** (File backup set restore without OpenDirect)
- **OpenDirect Restore** (open backup data directly without restoration)

  OpenDirect restore only applies to File backup sets with OpenDirect feature enabled.

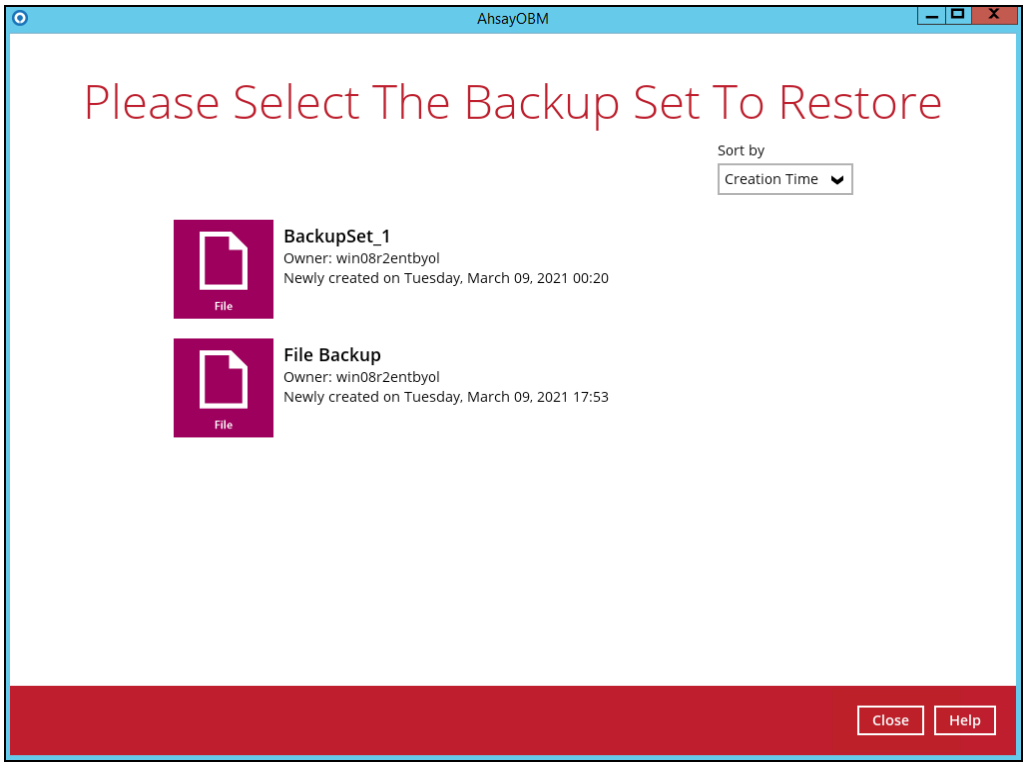
7.2 Normal Restore

The following is a typical end-to-end process for a file normal restore. The actual steps may slightly vary depending on the module you are restoring.

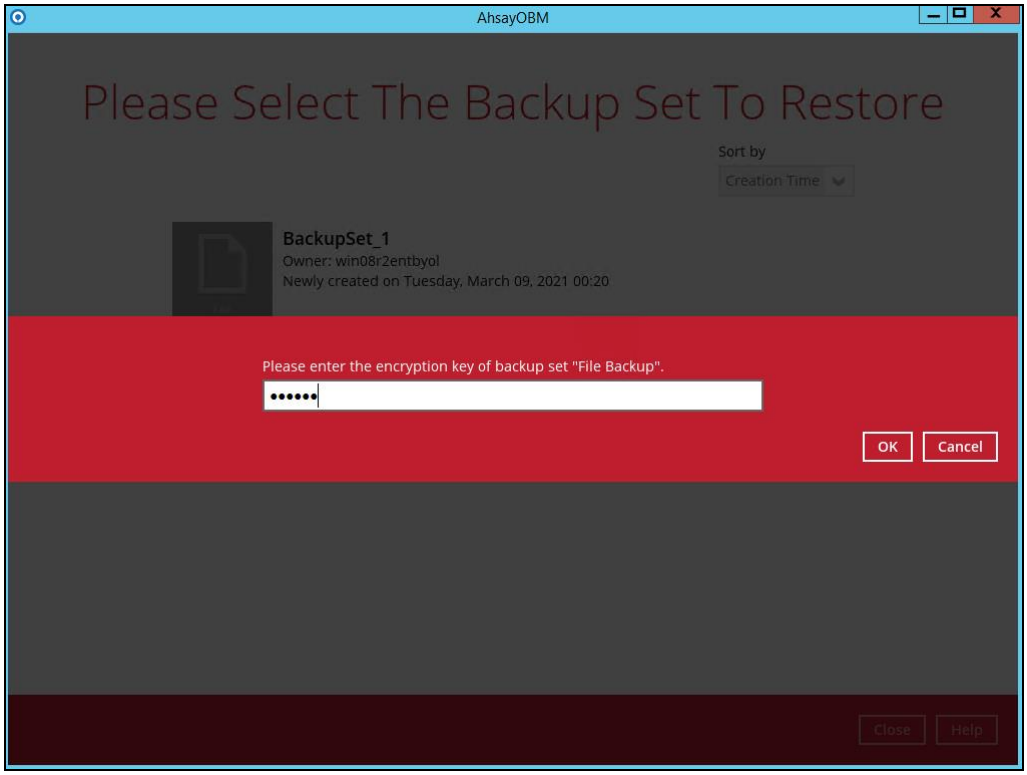
IMPORTANT

- AhsayOBR can be used to restore data that is backed up with AhsayOBM or AhsayACB.
- Clicking **Cancel** then **Yes** at any point during the steps below will close the software completely. If you wish to use it after the software is closed, you will have to launch it again according to the instructions in Ch. 5.2 Launch AhsayOBR.

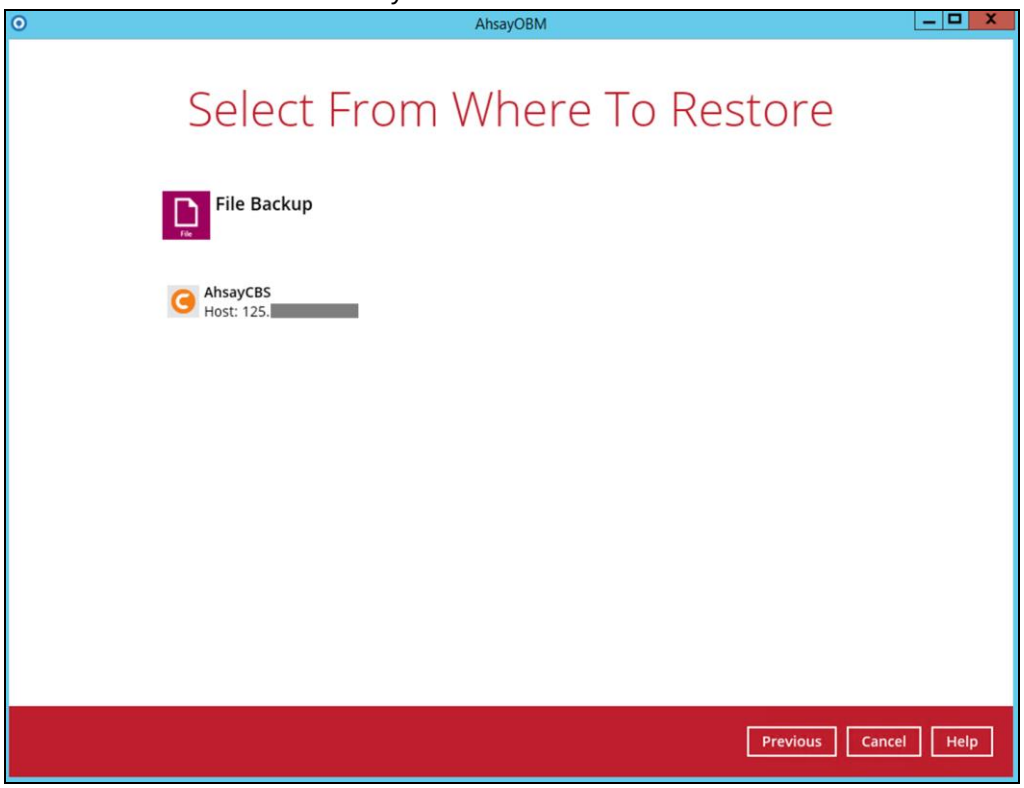
1. After logging in to your backup account, the available backup set(s) for restore will be displayed. Click on the backup set that you would like to restore.



2. Enter the encryption key of the selected backup set, then click **OK** to proceed.



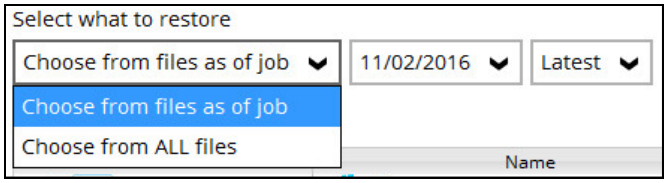
3. Click on the location from where you would like to restore the data from.

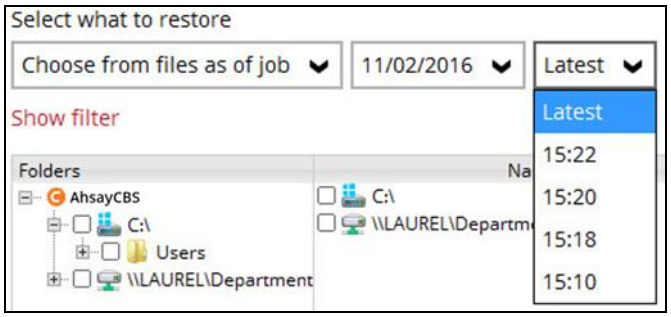


4. Select to restore files from a specific backup job, or from all files available, then select the files or folders that you would like to restore.

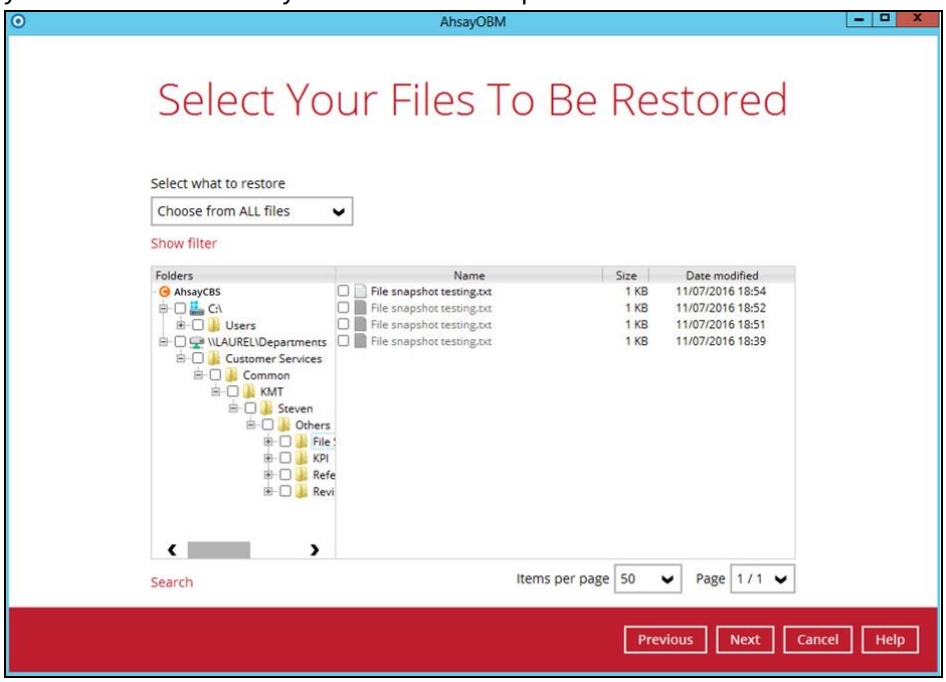
   There are two options from the **Select what to restore** drop-down menu:

   - **Choose from files as of job** – this option allows you to select a backup version from a specific date and time to restore.



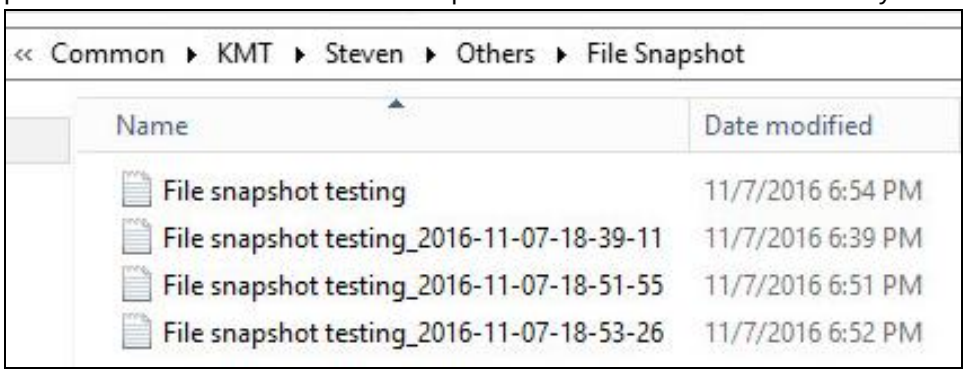


   - **Choose from ALL files** – this option allows you to restore all the available backup versions for this backup set. Among all the available backup versions, you can even select only some of the backup versions of a file to restore.



   Below is an example showing all the available backup versions of the **File snapshot testing.txt** file. The latest version is shown in solid black color and all the previous versions are shown in grey color. You can identify the file version from the **Date modified** column.

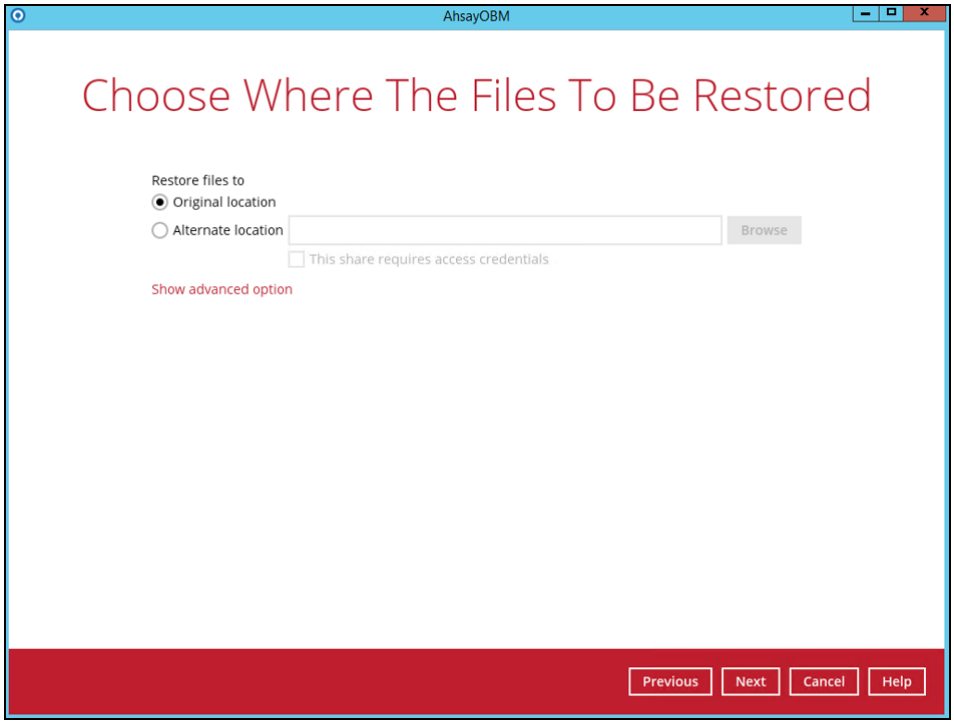
When the restore is done, you will see all the selected backup versions in the restore destination. The latest backup version has the file name as the original file, while the previous versions have the time stamps added to their file names for easy identification.



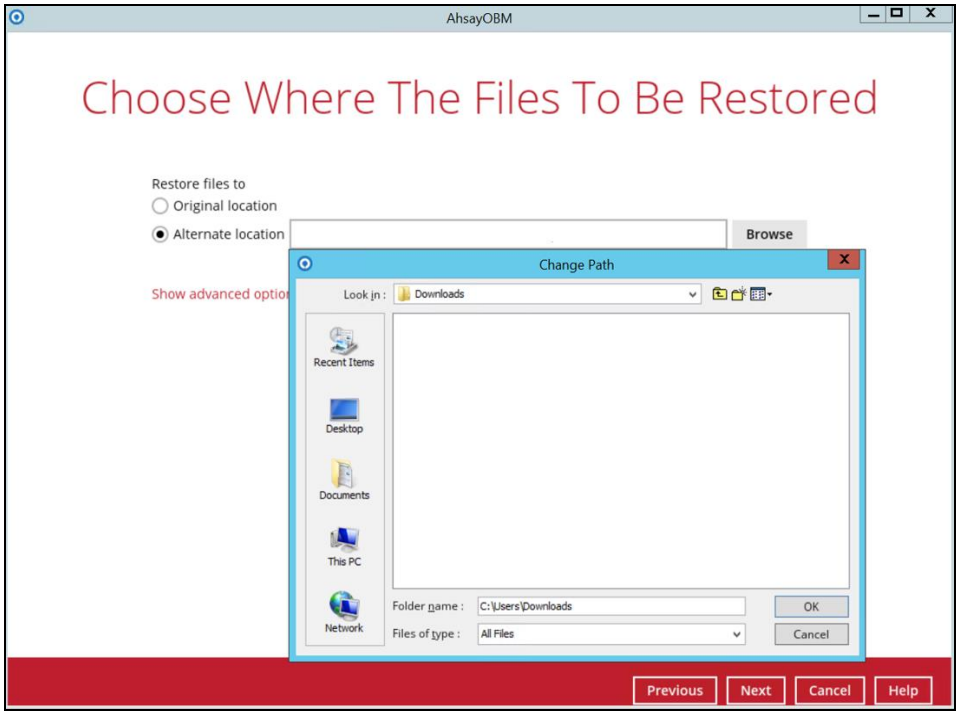
5. Click **Next** to proceed when you are done with the selections.

6. Select to restore the files to their **Original location**, or to an **Alternate location**, then click **Next** to proceed.

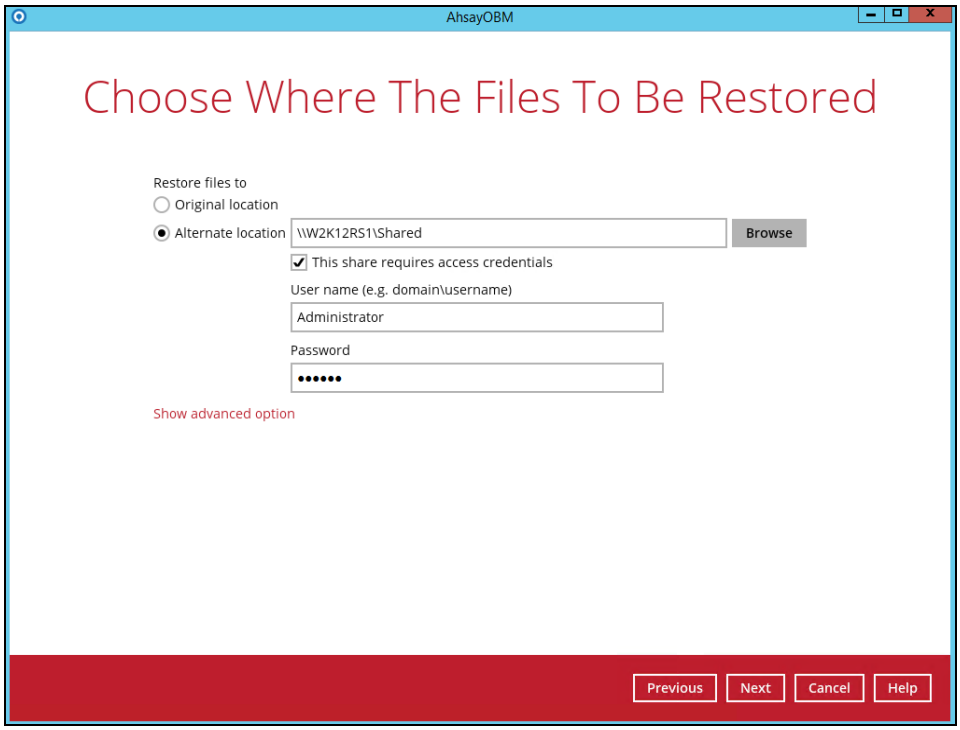
   - **Original location** – the backed up data will be restored to the computer running the AhsayOBR under the same directory path as on the machine storing the backup source. For example, the backup source files are stored in C:\User\Downloads same as on the computer running the AhsayOBR.



- **Alternate location** – you can choose to restore data to an alternate location on the computer where AhsayOBR is running. Click **Browse** to choose a location, then click **OK** to select.

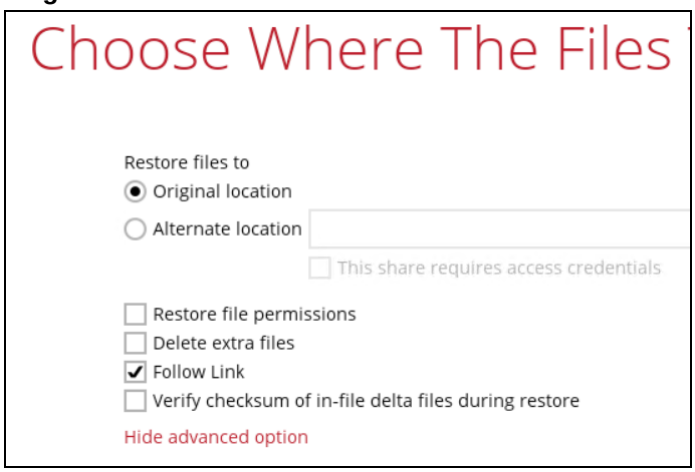


Alternatively, you may also choose to restore data to an unmapped network share.

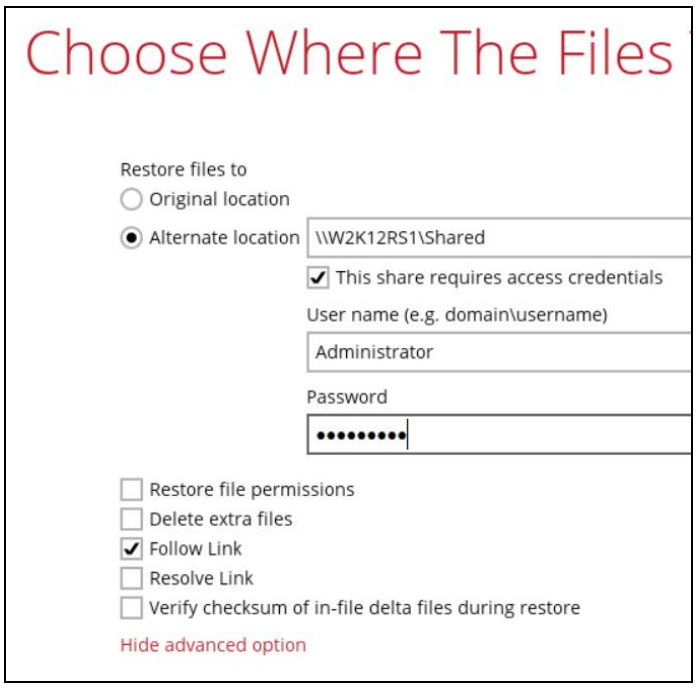


7. Click **Show advanced option** to configure other restore settings:

- **Original location**



- **Alternate location**



  - **Restore file permissions**

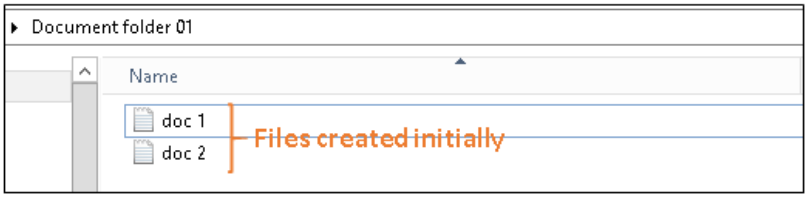
    By enabling this option, file permissions of the operating system files will be restored. File permission defines, for example, the right to view or change a file by the system owner/group/individual. If file permission is not restored properly, there is a potential risk that the restored data could be viewed by group/individual who is not supposed to have the access to.

  - **Delete extra files**

    By enabling this option, the restore process will attempt to synchronize the selected restore source with the restore destination, making sure the data in the restore destination is exactly the same as the restore source. Any data created after backup will be treated as "extra files" and will be deleted from the restore source if this feature is enabled.

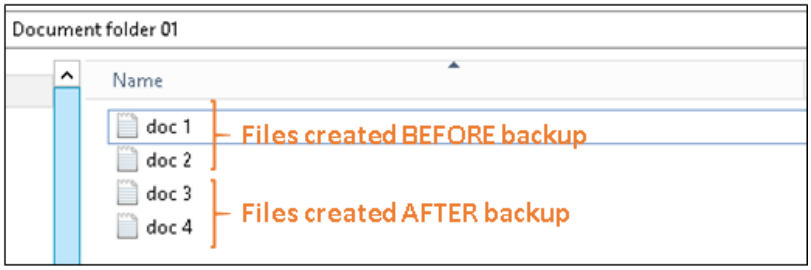
Example:

i) Two files are created under the **Document folder 01**, namely doc 1 & doc 2.



ii) A backup is performed for folder **Document folder 01**.

iii) Two new files are created, namely doc 3 & doc 4.



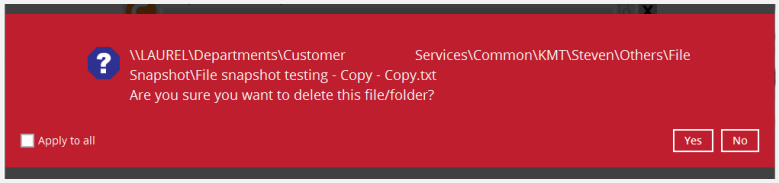
iv) A restore is performed for the **Document folder 01**, with **Delete extra files** option enabled.

v) Since doc 3 & doc 4 have never been backed up, therefore, they will be deleted from **Document folder 01**, leaving only the two files that have been backed up.

WARNING

Please exercise extra caution when enabling this feature. Consider what data in the restore source has not been backed up and what impact it would cause if those data were deleted.

Prior to the data restore and synchronization, a warning message shows as the one shown below. Clicking **Yes** will delete the “extra file”. You can check the **Apply to all** option to confirm deleting all the “extra files” at a time.



- **Follow Link (Enabled by default)**

  When this option is enabled, not only the symbolic link or junction point will be restored, the directories and files that the symbolic link or junction point links to will also be restored.

  The table below summarizes the behaviors when a restore is performed with different settings.

Follow Link	Restore to	Behavior
Enabled	**Original location**	Symbolic link or junction point is restored to the original backup location. Target directories or files are also restored to the original backup location.
	Alternate location	Symbolic link or junction point is restored to the location specified. Target directories or files are also restored to the alternate location specified.
Disabled	**Original location**	Symbolic link or junction point is restored to the original backup location. Target directories or files are NOT restored to the original backup location.
	Alternate location	Symbolic link or junction point is restored to the location specified. Target directories or files are NOT restored to the alternate location specified.

- **Resolve Link (Only applicable for restoring to Alternate Location)**

  This option must be used in conjunction with the **Follow Link** option. When this option is enabled, the symbolic link or junction point, as well as the directories and files that the symbolic link or junction point links to will also be restored in the alternate location you have chosen. This means that the symbolic link or junction will point to the alternate location instead of the original location.

  The table below summarizes the behaviors when a restore is performed with this option turned on and off.

Resolve Link	Behavior
Enabled	Symbolic link or junction point is restored to the alternate location specified, with its target directories and files also restored to the same location in their relative path. Target of the link or junction is updated to the new relative path. In other words, the link or junction now points to the new alternate location.
Disabled	Symbolic link or junction point is restored to the alternate location specified, with its target directories and files also restored to the same location in their relative path. However, target of the link or junction is NOT updated to the new relative path. In other words, the link or junction still points to the original location.

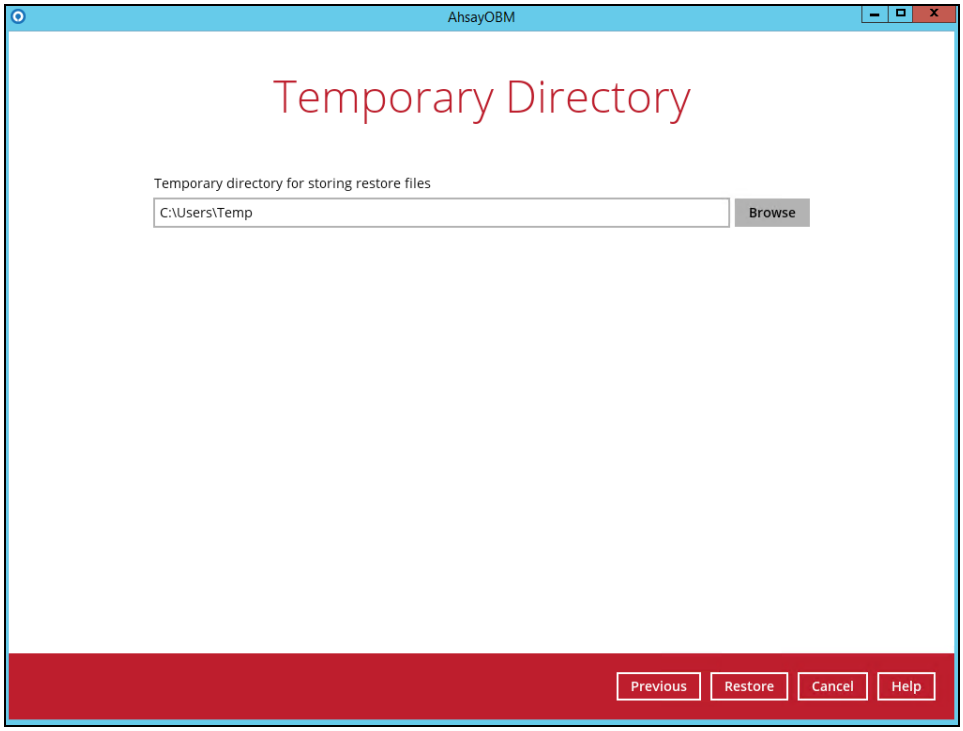
- **Verify checksum of in-file delta files during restore**

  By enabling this option, the checksum of in-file delta files will be verified during the restore process. This will check the data for errors during the restore process and create a data summary of the in-file delta files which will be included in the report.

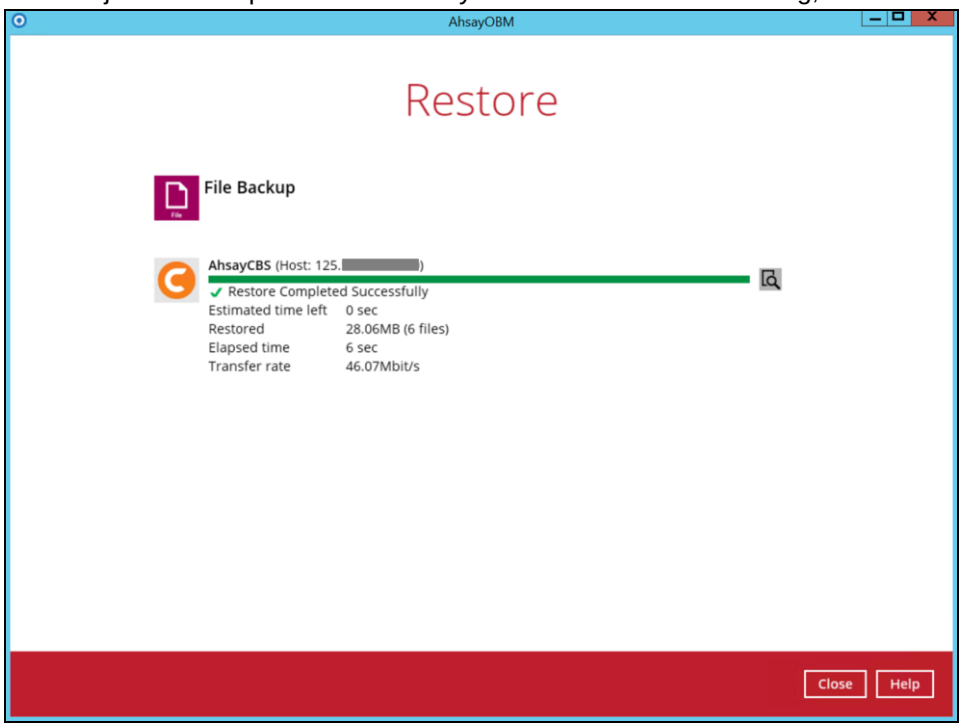
8. Once done with the restore settings, click **Next** to proceed.
9. Select the temporary directory for storing temporary files, such as delta files when they are being merged.

   By default, the temporary files are stored under the temporary directory of the user profile directory. However, there is a chance that the same directory path does not exist in the computer you are running the AhsayOBR. In that case, you will have to click **Browse** to define a new location for storing the temporary files. Otherwise, you will not be able to perform a restore.

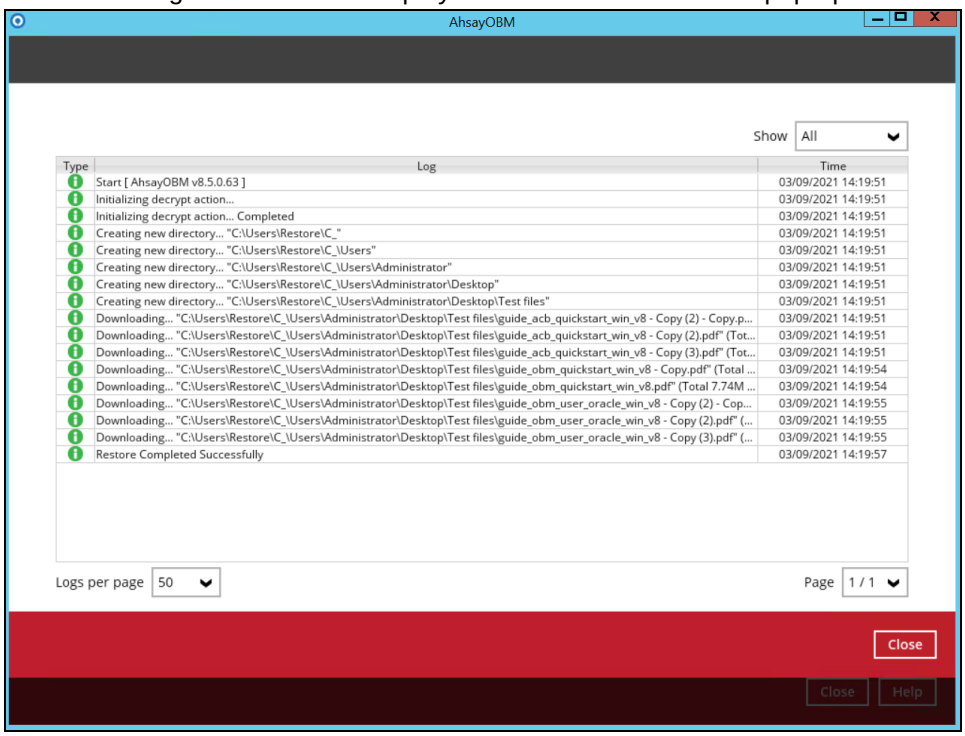
   Once the temporary directory is configured, click **Restore** to start the restore



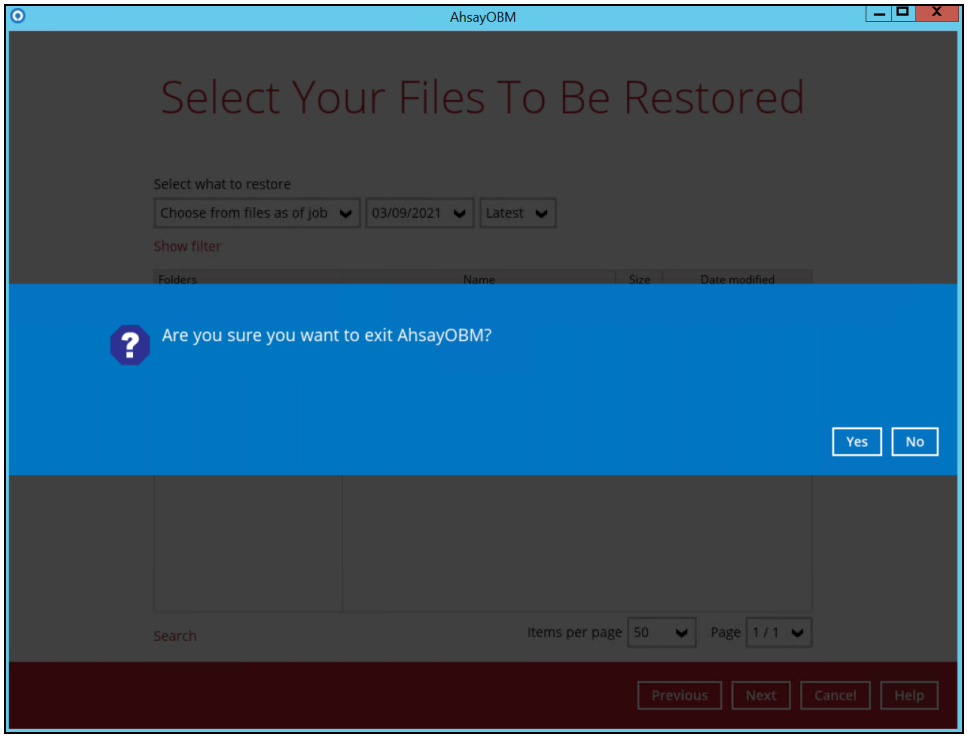
10. Restore job has completed successfully. To check for the restore log, click the icon.



The restore log window will be displayed. Click **Close** to exit the pop-up window.



11. After restoring, click the **close** button to exit the AhsayOBR, then click **Yes**. This will completely uninstall the software. If you wish to use it again, you will have to launch it again according to the instructions in Ch. 5.2 Launch AhsayOBR.



7.3 OpenDirect Restore

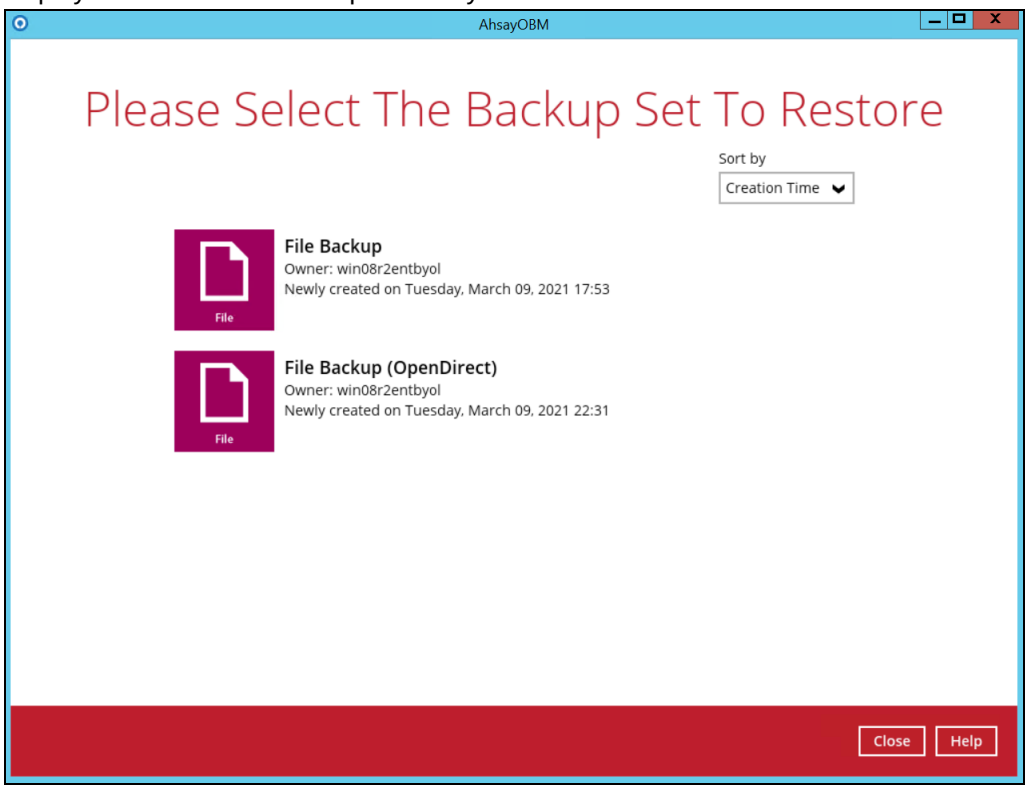
This restore method applies to backup sets created with OpenDirect restore enabled only.

IMPORTANT

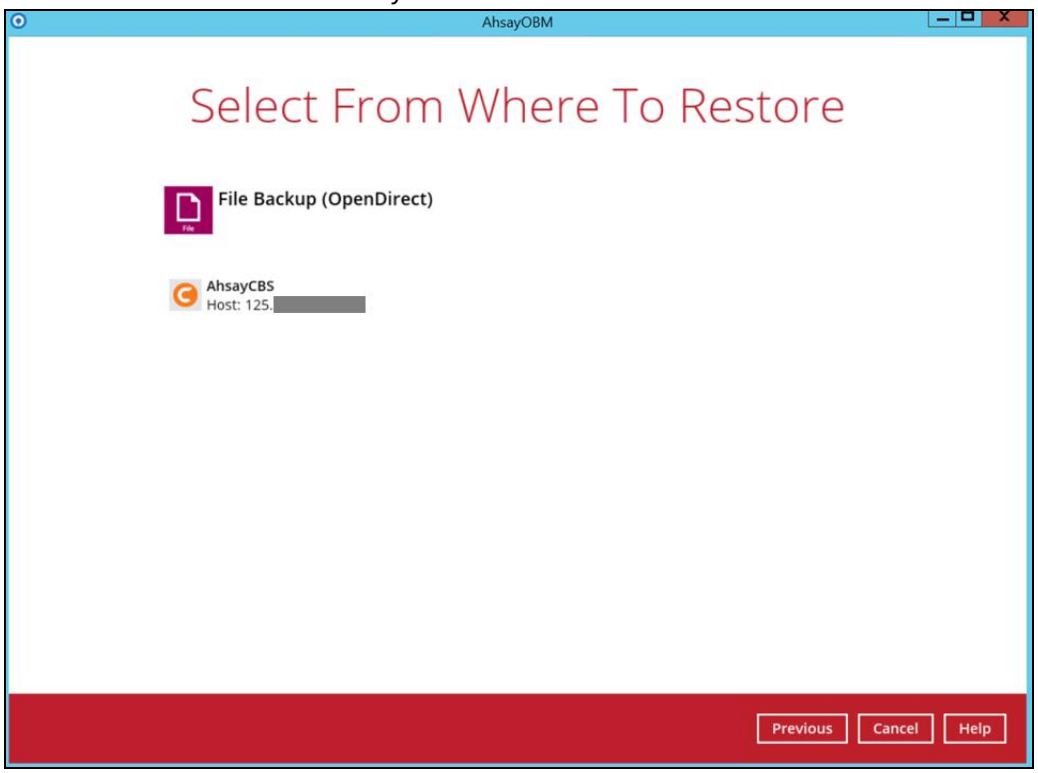
Before you proceed with the OpenDirect Restore, ensure that the following dependencies are fulfilled. Failure to do so may cause the restore to fail.

- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
  https://www.microsoft.com/en-hk/download/confirmation.aspx?id=48145
- Microsoft Visual C++ 2015 Redistributable Update 3 RC
  https://www.microsoft.com/en-us/download/details.aspx?id=52685
- Update for Universal C Runtime in Windows
  https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows
  - Prerequisites for **Windows 8.1** or **Windows Server 2012 R2**
    - Install KB2919442
      https://support.microsoft.com/en-us/help/2919442/march-2014-servicing-stack-update-for-windows-8.1-and-windows-server-2012-r2
    - Install KB2919355
      https://support.microsoft.com/en-us/help/2919355/windows-rt-8.1,-windows-8.1,-and-windows-server-2012-r2-update-april-2014
- Microsoft Security Advisory 3033929 for **Windows 7** and **Windows Server 2008 R2**
  https://technet.microsoft.com/en-us/library/security/3033929.aspx

1. After logging in to your backup account, the available backup set(s) for restore will be displayed. Click on the backup set that you would like to restore.

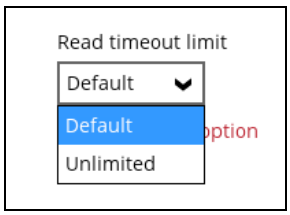


2. Click on the location from where you would like to restore the data from.



3. From the two available restore modes, select the option **Open backup data directly without restoration (OpenDirect)**. Click **Show advanced option** to display the other restore settings.

Read timeout limit defines the duration when the OpenDirect restore session will be disconnected if there is no response from the mounted compressed or image file.



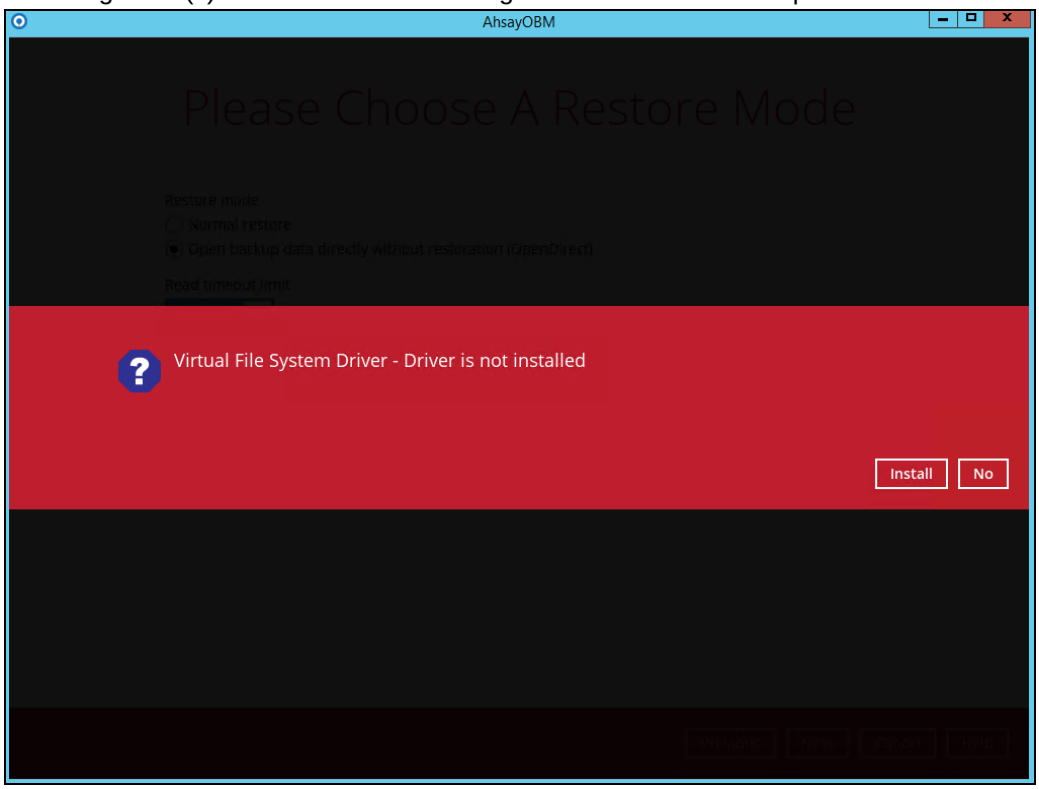
- **Default** – This setting is suitable for compressed or image file located on a local, removable, or network drive. The timeout value is 15 seconds.
- **Unlimited** – The connection will not have a timeout when this option is selected. This setting is recommended under the following usage:
  - Backup destination is a cloud storage.
  - AhsayCBS over the Internet.
  - A large compressed or image file with large incremental delta chain.

NOTE

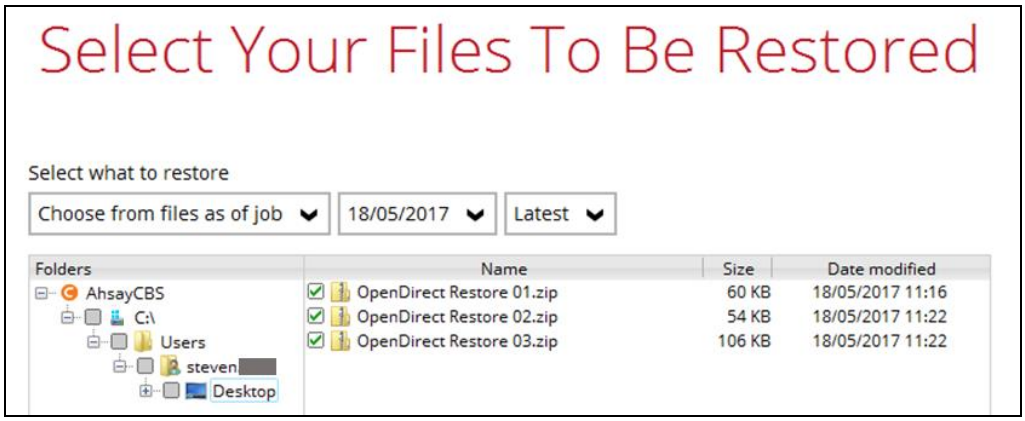
If in doubt or unsure about the compressed or image file size or network stability, it is recommended to use **Unlimited**.

Click **Next** once done with the selection.

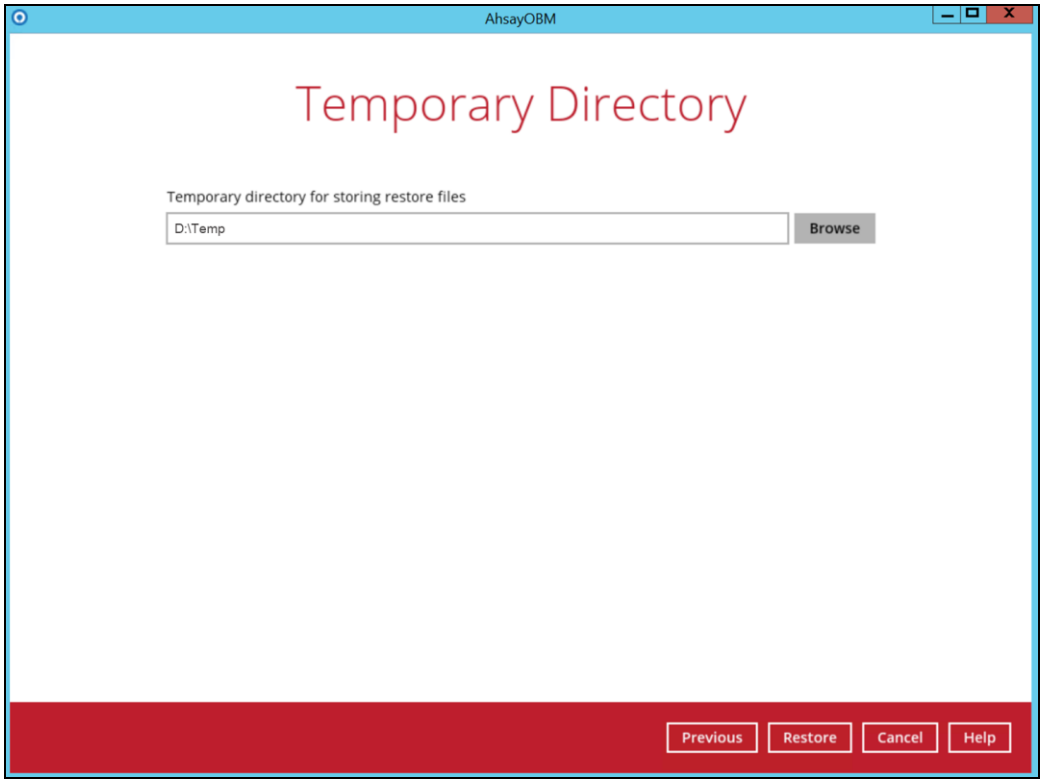
4. The following screen will be displayed when the OpenDirect restore for the backup set on the AhsayOBR machine will be performed for the first time. Click **Install** to confirm mounting of file(s) on the machine. Clicking **No** will exit the restore process.



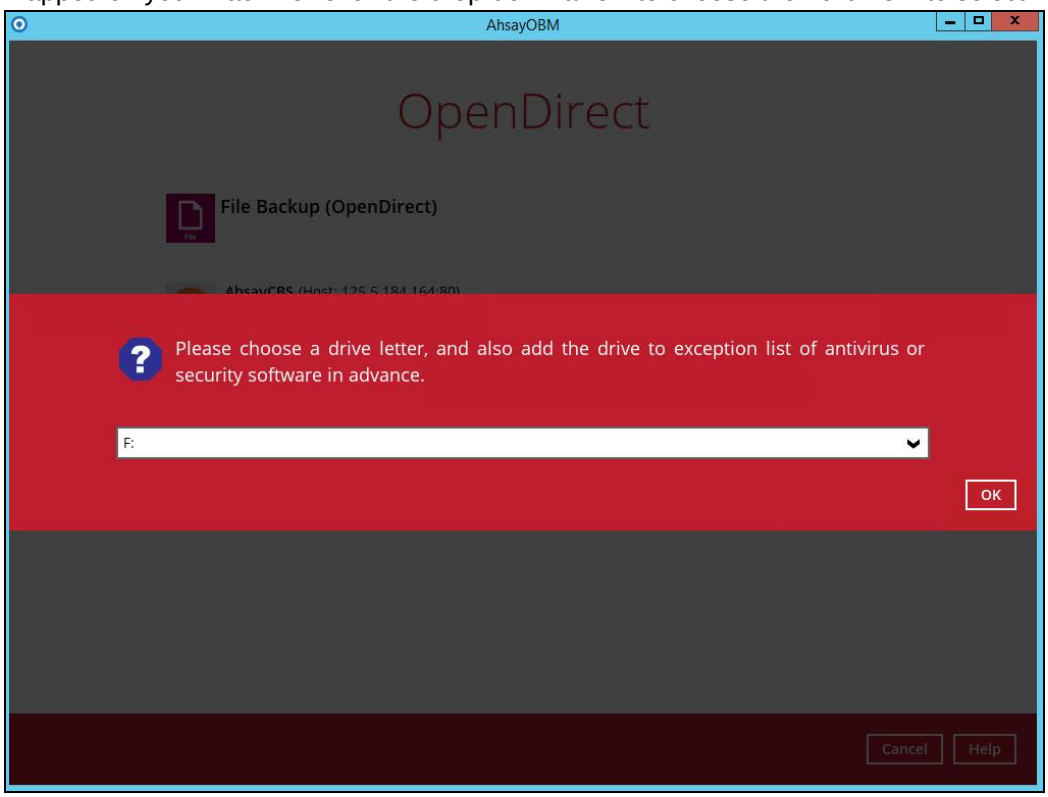
5. Select to restore files from a specific backup job, or from all files available, then select the files or folders that you would like to restore.



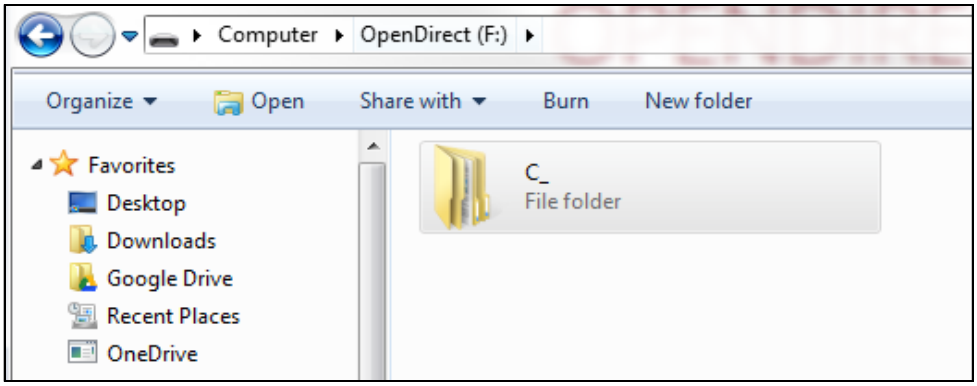
6. Select a temporary directory for storing restore files, then click **Restore** to start the restore process.



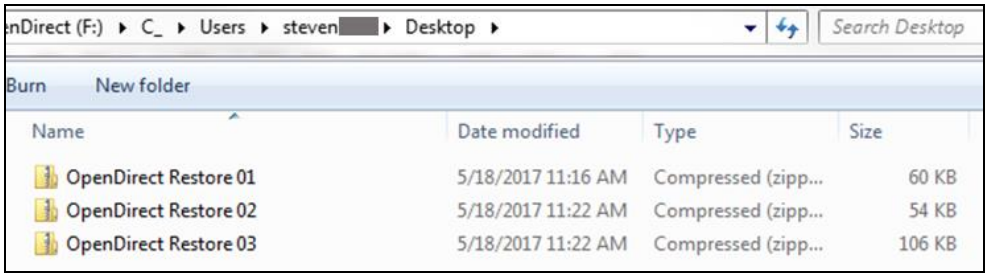
7. You will be prompted to select a drive letter where you wish the mounted files to be mapped on your machine. Click the drop-down arrow to choose then click **OK** to select.



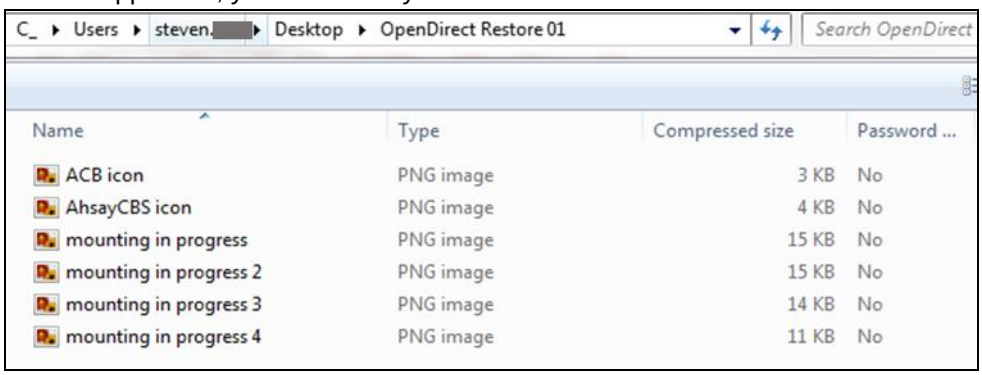
8. The selected drive letter will be mapped and prompted in the Windows Files Explorer with the files you wish to restore.



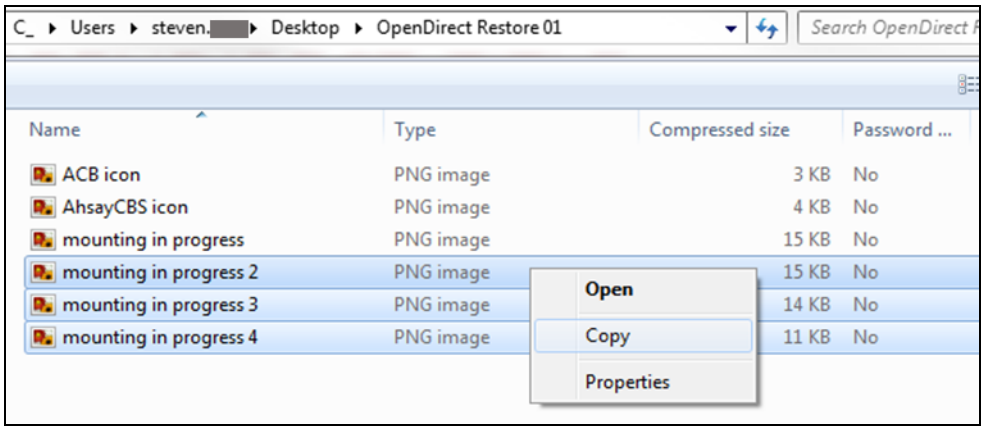
9. You can now click on the files to view them directly from here, which will be in read-only mode.



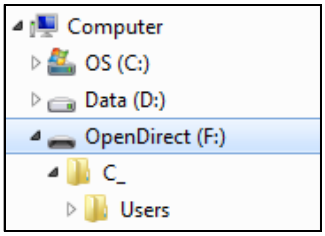
If it is a zipped file, you can directly click on it to see all the individual files inside.



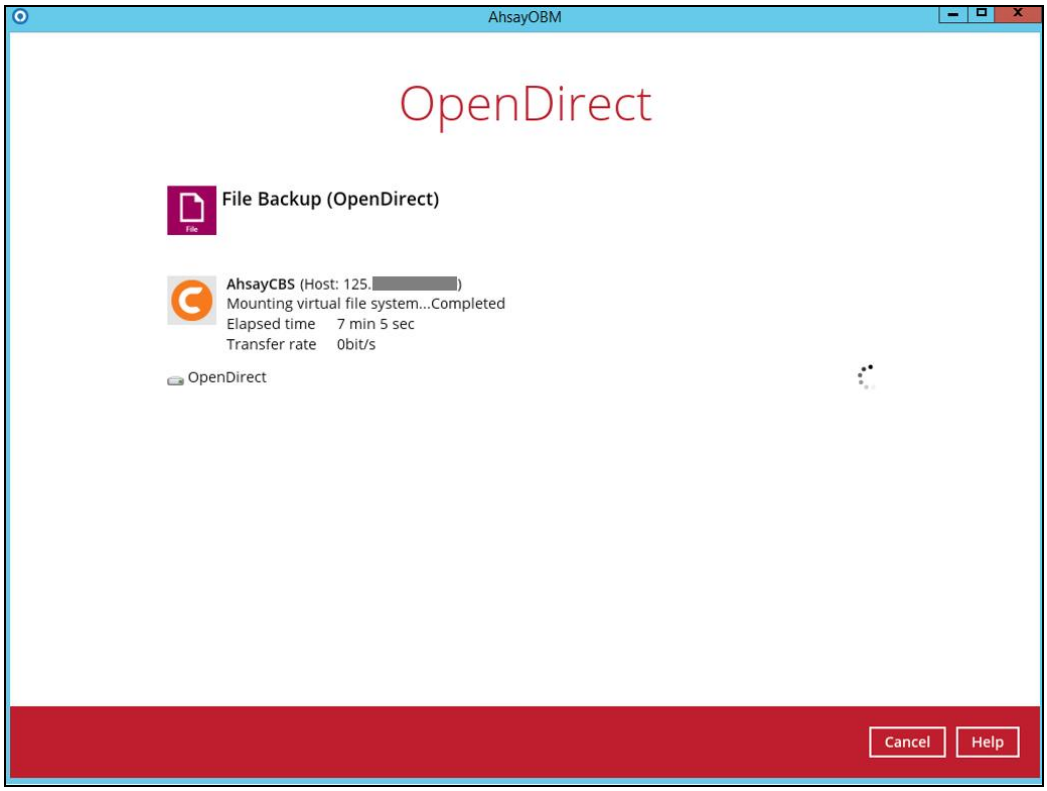
You may also copy individual file(s) you wish to restore to your local machine.

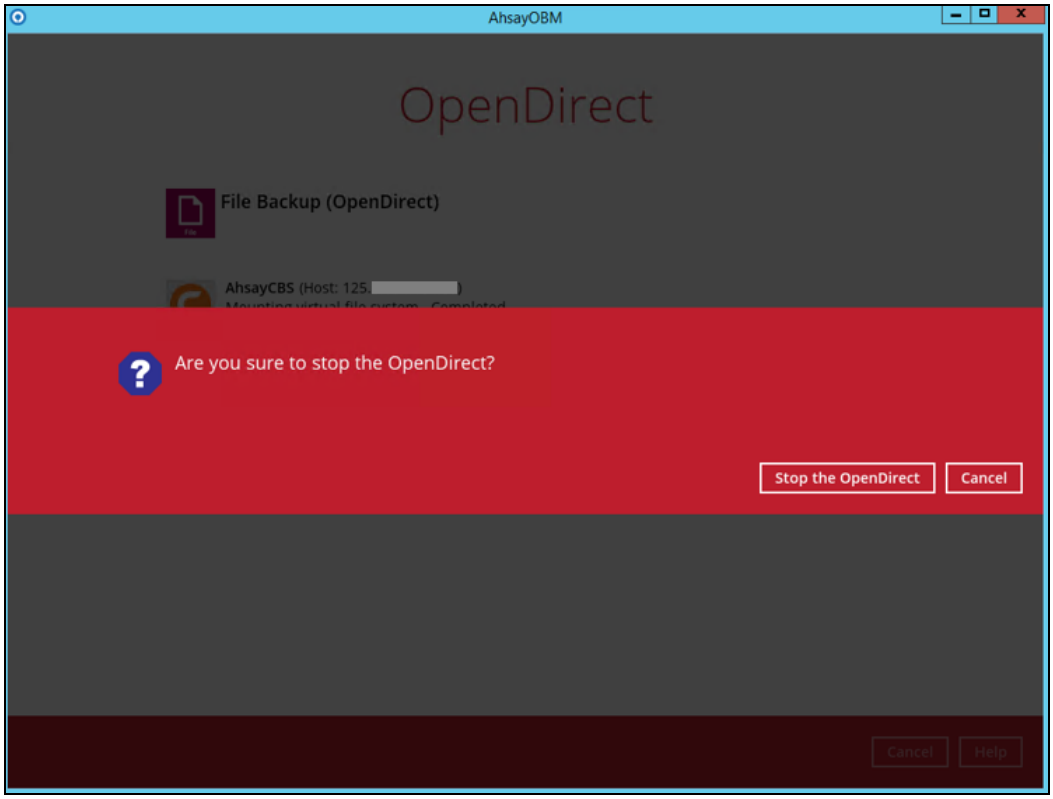


10. The mounted drive letter cannot be ejected from the Windows File Explorer, it will only be closed when you exit AhsayOBR.



11. When you have finished restoring the necessary files, you can go back to AhsayOBR to **Cancel** and **Stop the OpenDirect**.





IMPORTANT

1. As a result of the limitation of the virtual file system library, the mapped drive will only be unmounted from your machine when you exit AhsayOBR. In other words, each OpenDirect restore session on AhsayOBR can only be mounted and unmounted once.
2. **OpenDirect restore** of file backup sets:
   - Will not show up on the **Restore Status** tab in **Live Activities** of the backup service provider AhsayCBS. **Restore Status** tab in **Live Activities** only applies to the restore performed directly through AhsayOBR.
   - Will not generate restore reports or report email on backup service provider AhsayCBS.
   - Will not generate restore log on AhsayOBR.

8 Microsoft Hyper-V Guest VM Granular Restore

IMPORTANT

Before you proceed with the Granular Restore, ensure that the following dependencies are fulfilled. Failure to do so may cause the restore to fail.

- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
  https://www.microsoft.com/en-hk/download/confirmation.aspx?id=48145
- Microsoft Visual C++ 2015 Redistributable Update 3 RC
  https://www.microsoft.com/en-us/download/details.aspx?id=52685
- Update for Universal C Runtime in Windows
  https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows
  - Prerequisites for **Windows 8.1** or **Windows Server 2012 R2**
    - Install KB2919442
      https://support.microsoft.com/en-us/help/2919442/march-2014-servicing-stack-update-for-windows-8.1-and-windows-server-2012-r2
    - Install KB2919355
      https://support.microsoft.com/en-us/help/2919355/windows-rt-8.1,-windows-8.1,-and-windows-server-2012-r2-update-april-2014
- Microsoft Security Advisory 3033929 for **Windows 7** and **Windows Server 2008 R2**
  https://technet.microsoft.com/en-us/library/security/3033929.aspx

8.1 Requirements and Limitations

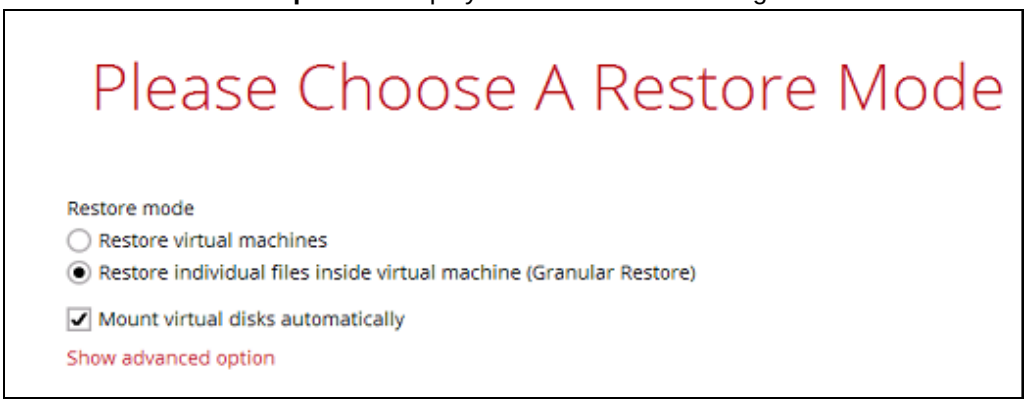
1. Granular restore does not support the mounting of virtual disks, for example if the disk itself is encrypted using Windows Bitlocker or other third-party security features.
2. Granular restore does not support the restore of folders or files on a virtual disk if the files/folders are encrypted. For example, if the “Encrypt contents to secure data” is selected in Advanced attributes.
3. The mounting of Linux/Unix file systems from virtual disk file is currently not available due to limitations of the file system drivers.
4. Granular restore can only be performed on one guest VM at a time.

8.2 Start Granular Restore

1. After logging in to your backup account successfully, you should see a screen showing all the available backup sets for restore. Select the backup set that you would like to restore data from.

2. Select the backup destination that contains the guest VM that you would like to restore.

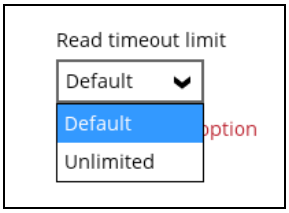
3. Select to the Restore individual files in virtual machine (Granular Restore) option. Click **Show advanced option** to display the other restore settings.



NOTE

The **Mount virtual disks automatically option** is selected by default. If the guest VM contains a multiple virtual disk and you only require the restore of files from a single or certain virtual disk(s), then unselect this option to speed up the virtual disk mounting. Otherwise, Granular Restore will connect and mount all available virtual disks and this process could take longer.

Read timeout limit defines the duration when the Granular Restore session will be disconnected if there is no response from the mounted virtual machine.

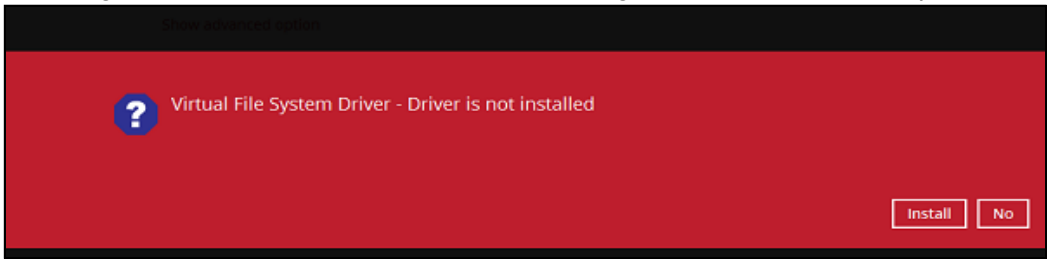


- **Default** – This setting is suitable for guest VMs located on a local, removable, or network drive. The timeout value is 15 seconds.
- **Unlimited** – The connection will not have a timeout when this option is selected. This setting is recommended under the following usage:
  - Backup destination is a cloud storage.
  - AhsayCBS over the Internet.
  - A large guest VM or guest VM with large incremental delta chain.

> **NOTE**
>
> If in doubt or unsure about the guest VM size or network stability, it is recommended to use **Unlimited**.

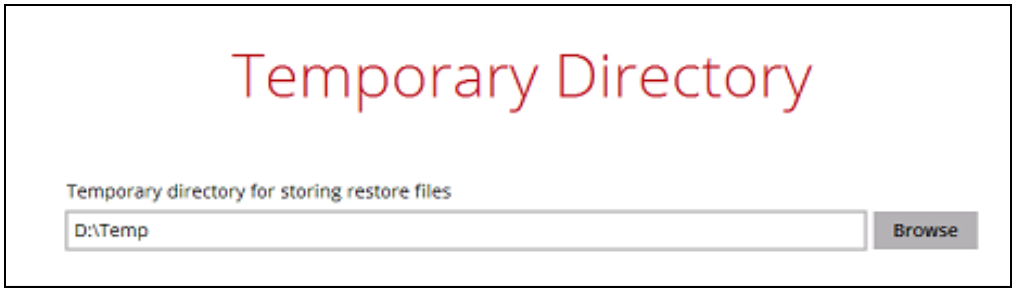
Click **Next** once done with the selection.

4. The following screen will be displayed when the Granular restore for the backup set on the AhsayOBR machine will be performed for the first time. Click **Install** to confirm mounting of the virtual disk on the machine. Clicking **No** will exit the restore process.



5. Select the virtual machine that you would like to perform Granular Restore for, then click **Next** to proceed.

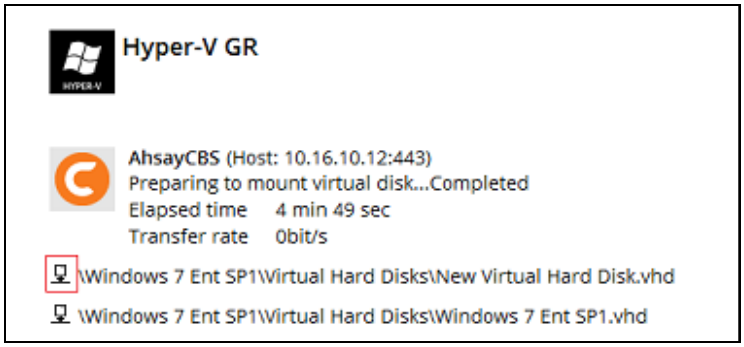
6. Select a temporary directory for storing restore files, then click **Restore** to start the Granular restore process.



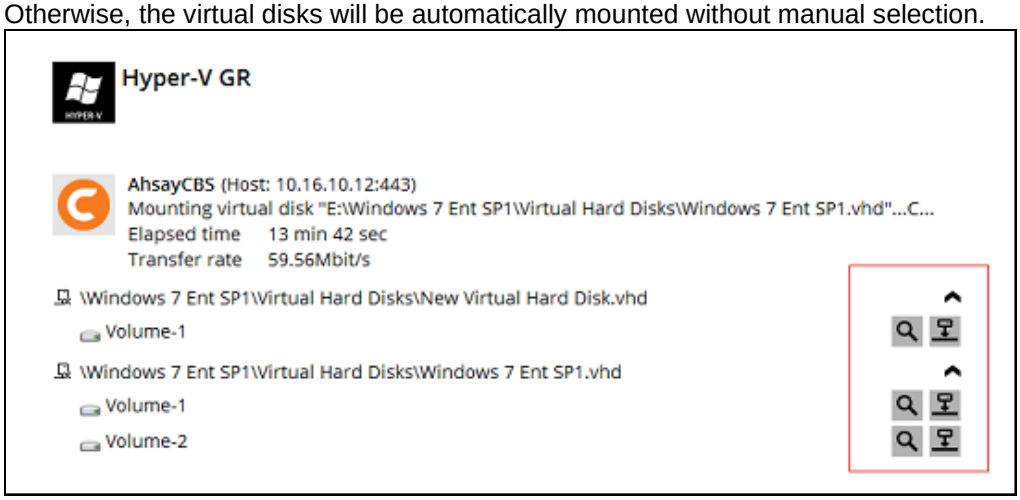
7. When the virtual disk(s) are in the process of being prepared for mounting on the AhsayOBR machine, you will see the following screen.

Please wait as the process could take some time depending on the size of the virtual disk, network bandwidth, and storage location.

8. If the **Mount virtual disks automatically** option is unselected, then click on the disk icon to mount the virtual disk you wish to restore files from.



Otherwise, the virtual disks will be automatically mounted without manual selection.



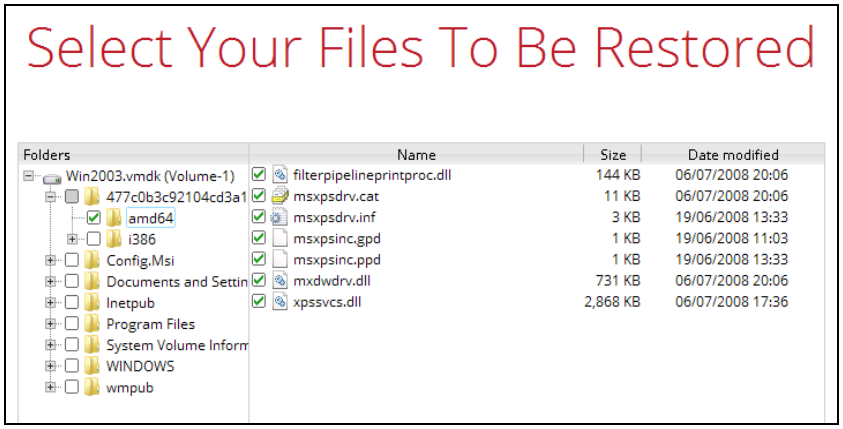
There are two options to restore individual files from here.

Option 1: Restore Using AhsayOBR File Explorer

This method allows you to use the file explorer in AhsayOBR to browse through the files from the backup up image mounted and select those you wish to restore.

i. Click the icon to browse the files in the mounted backup image. If there are multiple volumes in the guest VM, you can only select one volume to restore indidual files at a time.

You will then see a file explorer menu as shown below. Select the file(s) you wish to restore, then click **Next** to proceed.

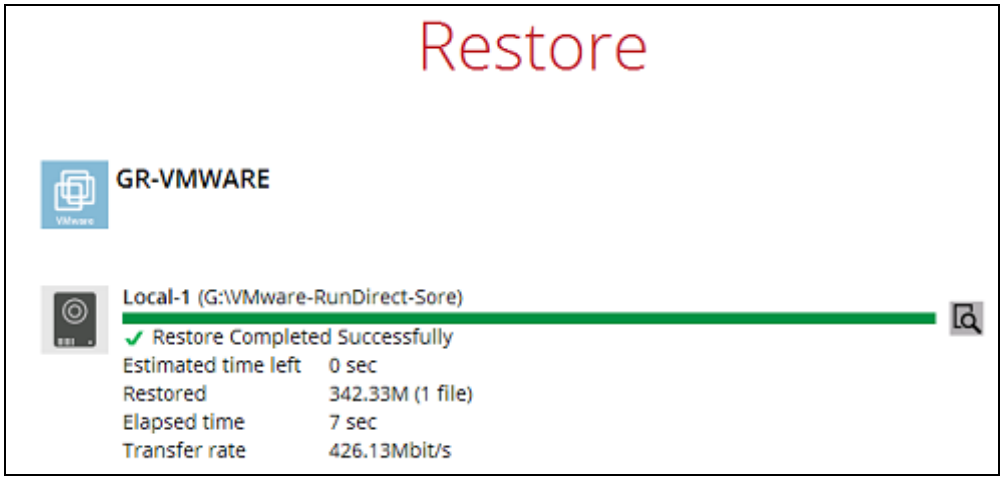


NOTE

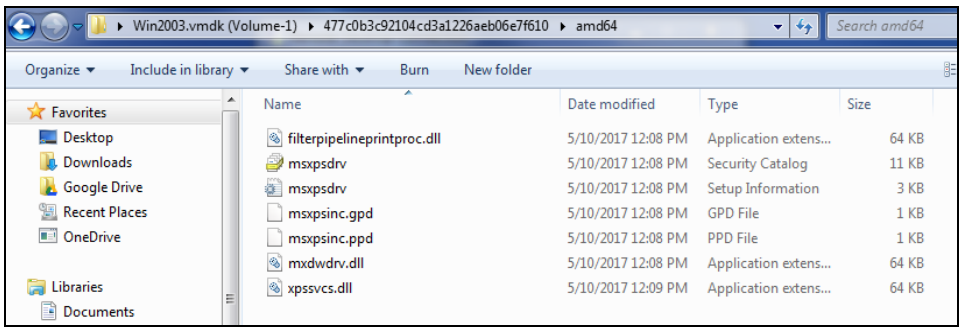
Some system folder(s)/file(s) (e.g., System Volume Information) are only shown in the AhsayOBR File Explorer and will be not restored. Therefore, those folder(s)/file(s) will not be shown in the mapped drive shown in **step iv** below.

ii. Select a path where you wish the files to be restored to, then click **Restore**.

iii. The following screen shows when the selected files have been restored to the defined destination.



iv. Open the defined restore path and you should be able to see the files being restored there.



Option 2: Restore Using Windows File Explorer

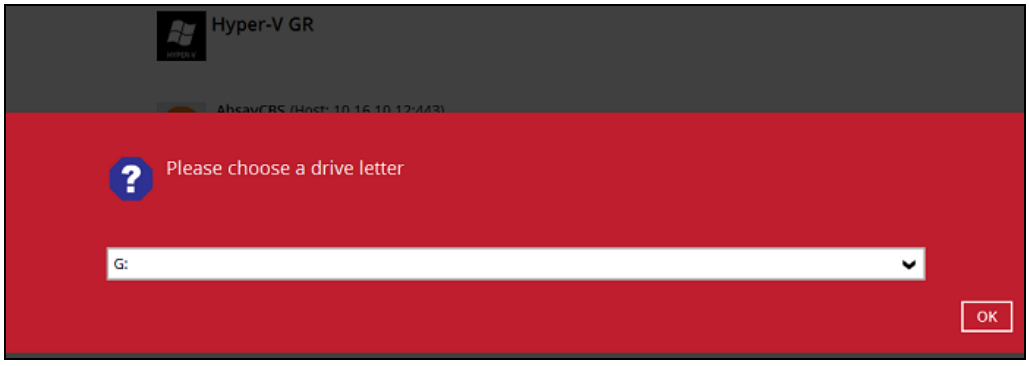
This method allows you to browse through the files from the mounted virtual disk through the Windows File Explorer on the machine where you AhsayOBR is installed.

NOTES

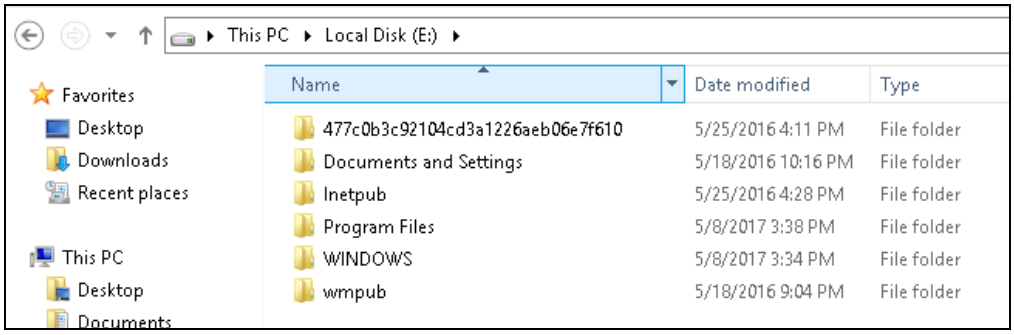
Granular restore of Hyper-V backup sets performed using Windows File Explorer:

1. Will not show up on the [**Restore Status**] tab in **Live Activities** of the backup service provider AhsayCBS.
2. Will not generate restore reports on backup service provider AhsayCBS.
3. Will not generate restore log on AhsayOBR.

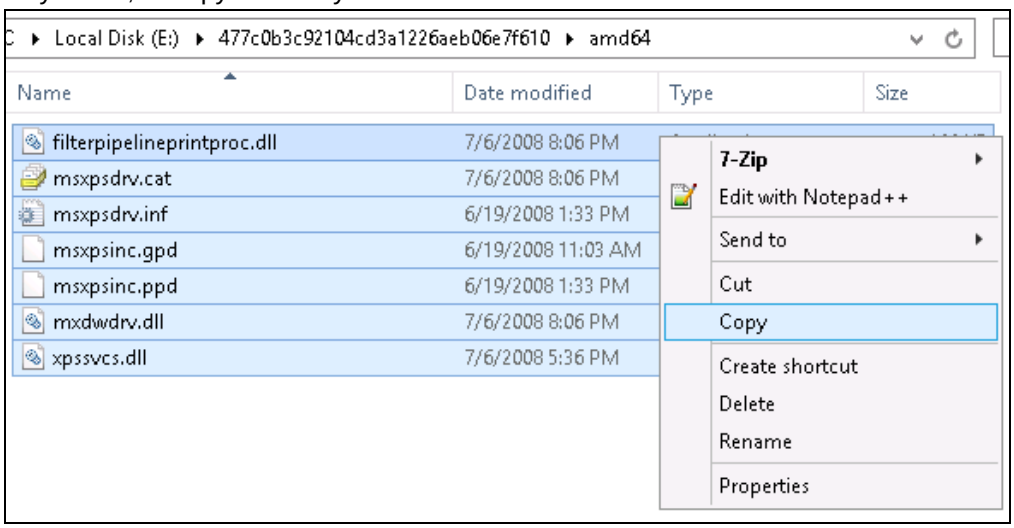
i. Click and then you will be prompted to select a driver letter where you wish the mounted image to be mapped on your machine, click **OK** when you have finished selection.



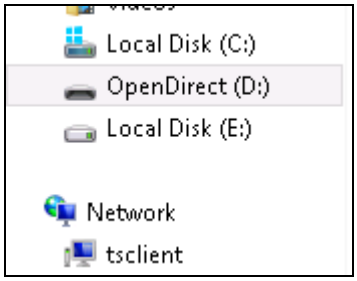
ii. The selected drive letter will be mapped and prompted in the Windows Files Explorer with the files you wish to restore.



iii. You can now click on the files to view them directly from here, which will be in read-only mode, or copy them to your local machine.



iv. The mounted drive letter cannot be ejected from the Windows File Explorer, it will only be closed when you exit AhsayOBR.



v. When you have finished restoring the necessary files, you can go back to AhsayOBR and click on **Cancel**.

vi. Then click on **Stop the granular restore** to unmount the virtual disk(s).

IMPORTANT

Due to the limitation of the virtual file system library, the mounted virtual disks will only be unmounted from your machine when you exit AhsayOBR.

9 VMware vCenter/ESXi Guest VM Granular Restore

IMPORTANT

Before you proceed with the Granular Restore, ensure that the following dependencies are fulfilled. Failure to do so may cause the restore to fail.

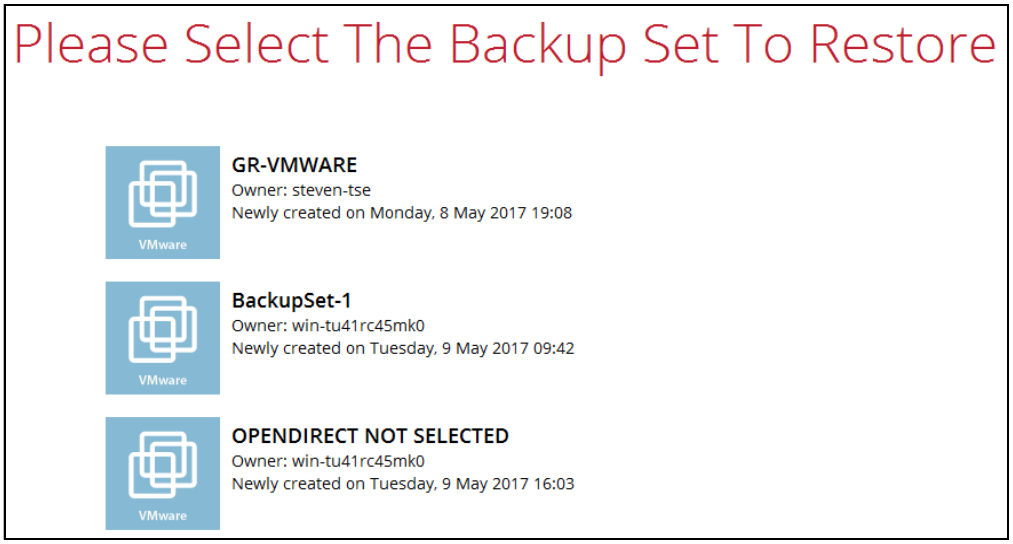
- Microsoft Visual C++ 2015 Redistributable (x86) / (x64)
  https://www.microsoft.com/en-hk/download/confirmation.aspx?id=48145
- Microsoft Visual C++ 2015 Redistributable Update 3 RC
  https://www.microsoft.com/en-us/download/details.aspx?id=52685
- Update for Universal C Runtime in Windows
  https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows
  - Prerequisites for **Windows 8.1** or **Windows Server 2012 R2**
    - Install KB2919442
      https://support.microsoft.com/en-us/help/2919442/march-2014-servicing-stack-update-for-windows-8.1-and-windows-server-2012-r2
    - Install KB2919355
      https://support.microsoft.com/en-us/help/2919355/windows-rt-8.1,-windows-8.1,-and-windows-server-2012-r2-update-april-2014
- Microsoft Security Advisory 3033929 for **Windows 7** and **Windows Server 2008 R2**
  https://technet.microsoft.com/en-us/library/security/3033929.aspx

9.1 Requirements and Limitations

1. Granular restore does not support the mounting of virtual disks, for example if the disk itself is encrypted using Windows Bitlocker or other third-party security features.
2. Granular restore does not support the restore of folders or files on a virtual disk if the files/folders are encrypted. For example, if the “Encrypt contents to secure data” is selected in Advanced attributes.
3. The mounting of Linux/Unix file systems from virtual disk file is currently not available due to limitations of the file system drivers.
4. Granular restore can only be performed on one guest VM at a time.

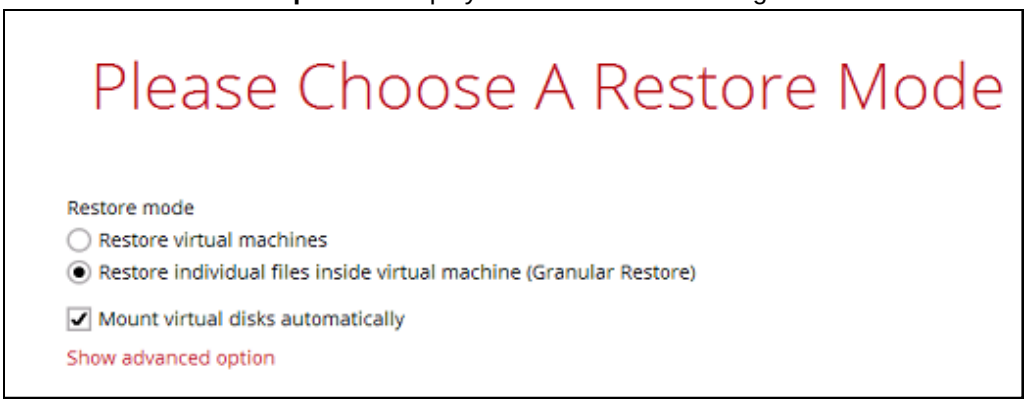
9.2 Start Granular Restore

1. After logging in to your backup account successfully, you will see a screen showing all the available backup sets for restore. Select the backup set that you would like to restore data from.



2. Select the backup destination that contains the VM that you would like to restore.

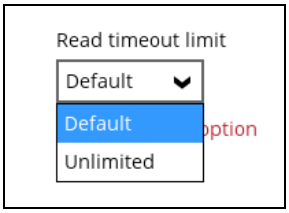
3. Select the **Restore individual files in virtual machine (Granular Restore)** option. Click **Show advanced option** to display the other restore settings.



NOTE

The **Mount virtual disks automatically option** is selected by default. If the guest VM contains a multiple virtual disk and you only require the restore of files from a single or certain virtual disk(s), then unselect this option to speed up the virtual disk mounting. Otherwise, granular restore will connect and mount all available virtual disks and this process could take longer.

Read timeout limit defines the duration when the Granular Restore session will be disconnected if there is no response from the mounted virtual machine.

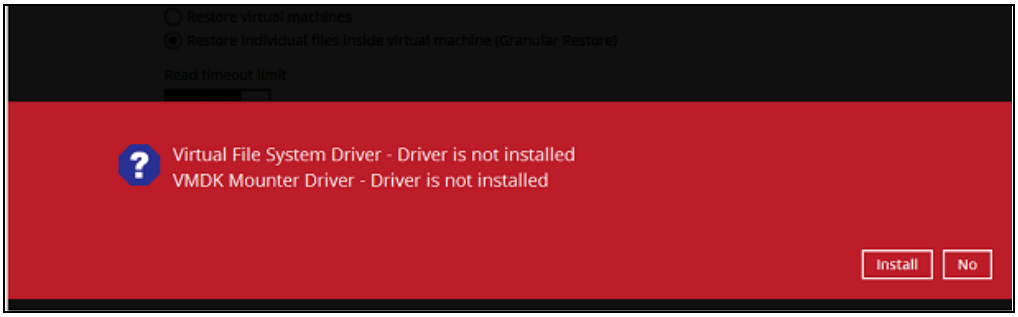


- **Default** – This setting is suitable for guest VMs located on a local, removable, or network drive. The timeout value is 15 seconds.
- **Unlimited** – The connection will not have a timeout when this option is selected. This setting is recommended under the following usage:
  - Backup destination is a cloud storage.
  - AhsayCBS over the Internet.
  - A large guest VM or guest VM with large incremental delta chain.

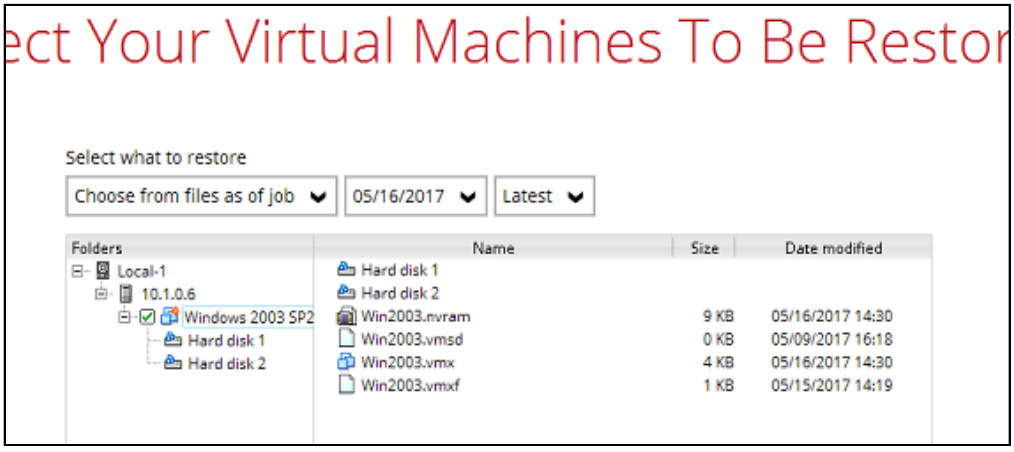
> **NOTE**
>
> If in doubt or unsure about the guest VM size or network stability, it is recommended to use **Unlimited**.

Click **Next** once done with the selection.

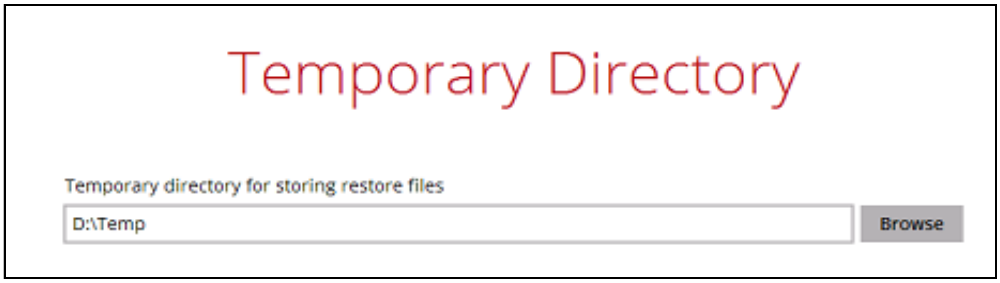
4. The following screen will be displayed when the Granular restore for the backup set on the AhsayOBR machine will be performed for the first time. Click **Install** to start the installation of drivers on the machine. Clicking **No** will exit the restore process.



5. Select the virtual machine that you would like to perform granular restore for, then click **Next** to proceed.



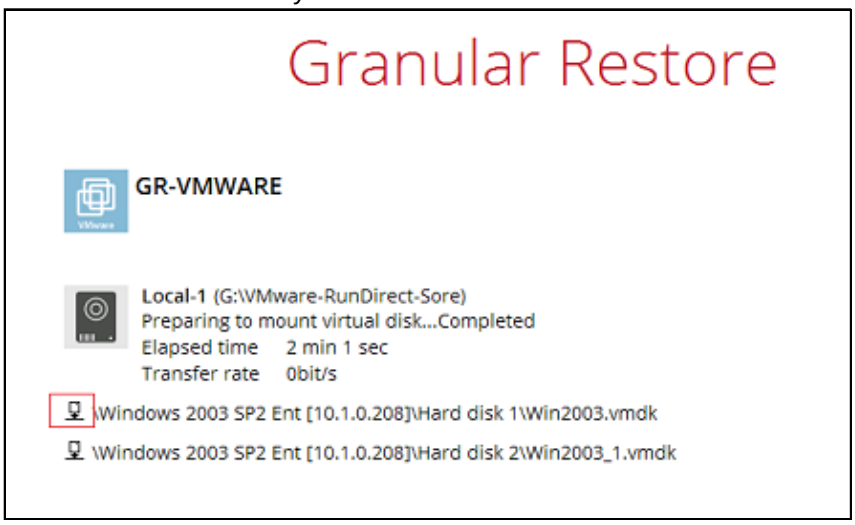
6. Select a temporary directory for storing restore files, then click **Restore** to start the Granular restore process.



7. When the virtual disk(s) are in the process of being prepared for mounting on the AhsayOBR machine, you will see the following screen.

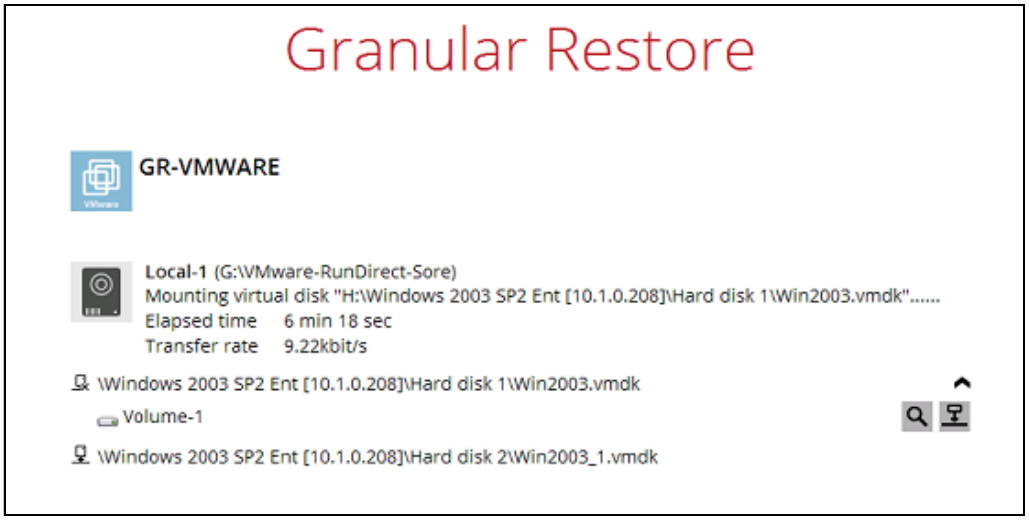
Please wait as the process could take some time depending on the size of the virtual disk, network bandwidth, and storage location.

8. If the **Mount virtual disks automatically** option is unselected, click on the disk icon to mount the virtual disk you wish to restore files from.



Otherwise, the virtual disks will be automatically mounted without manual selection.

9. When the virtual disk are mounted, you will see the following screen showing the information of the mounted virtual disk with the available volume shown.

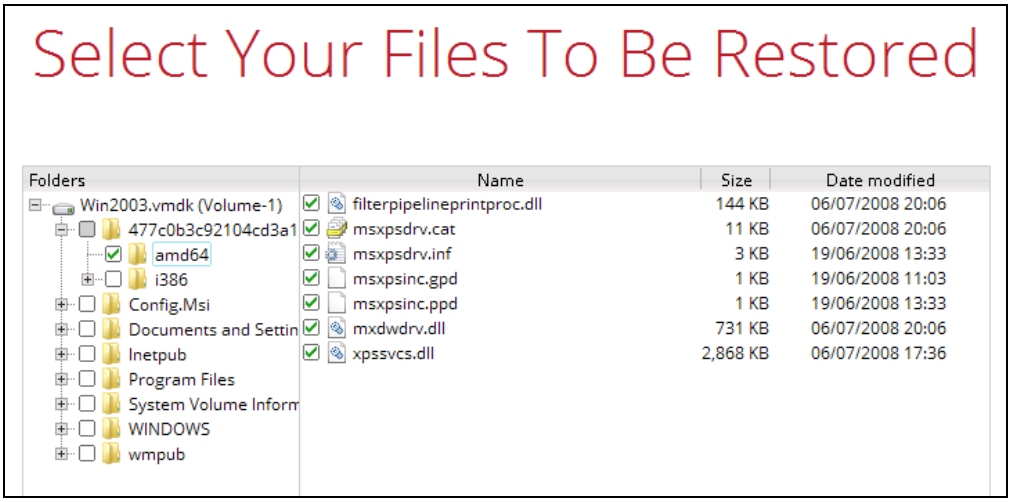


Option 1: Restore Using AhsayOBR File Explorer

This method allows you to use the file explorer in AhsayOBR to browse through the files from the backup up image mounted and select those you wish to restore.

i. Click the icon to browse the files in the mounted backup image. If there are multiple volumes in the guest VM, you can only select one volume to restore indidual files at a time.

You will then see a file explorer menu as shown below. Select the file(s) you wish to restore, then click **Next** to proceed.

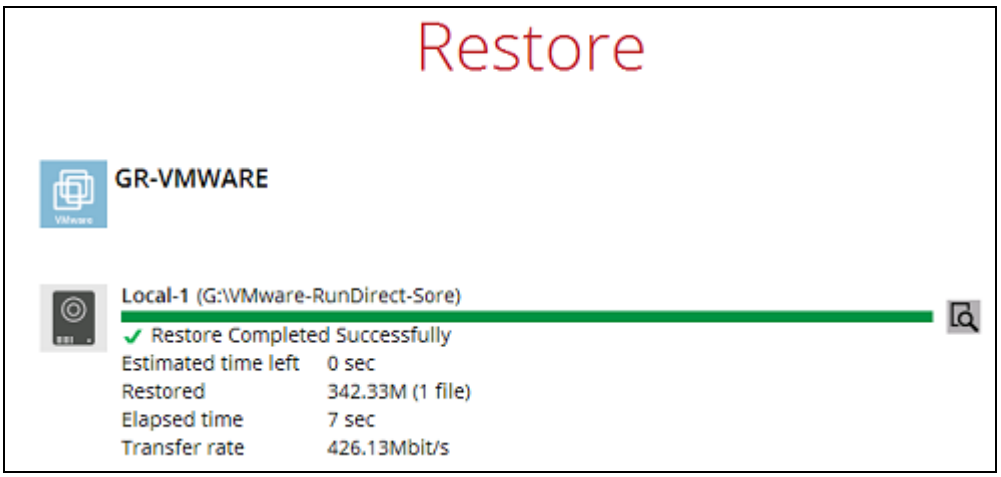


NOTE

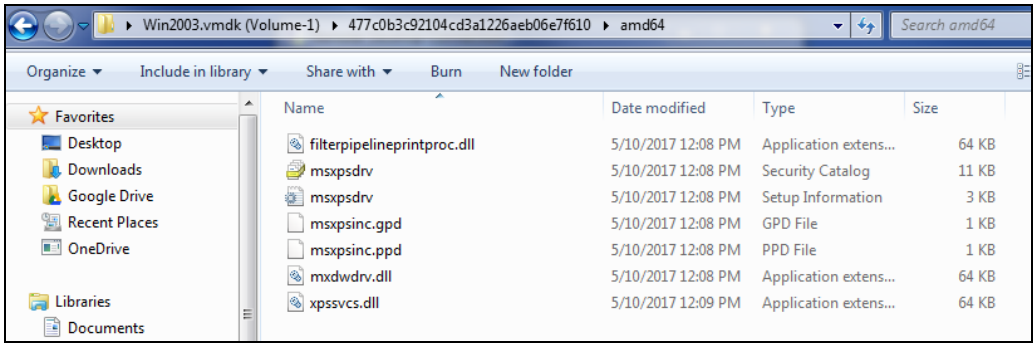
Some system folder(s)/file(s) (e.g., System Volume Information) are only shown in the AhsayOBR File Explorer and will be not restored. Therefore, those folder(s)/file(s) will not be shown in the mapped drive shown in **step iv** below.

ii. Select a path where you wish the files to be restored to, then click **Restore**

iii. The following screen shows when the selected files have been restored to the defined destination.



iv. Open the defined restore path and you should be able to see the files being restored there.



Option 2: Restore Using Windows File Explorer

This method allows you to browse through the files from the mounted virtual disk through the Windows File Explorer on the machine where you have AhsayOBR installed on.

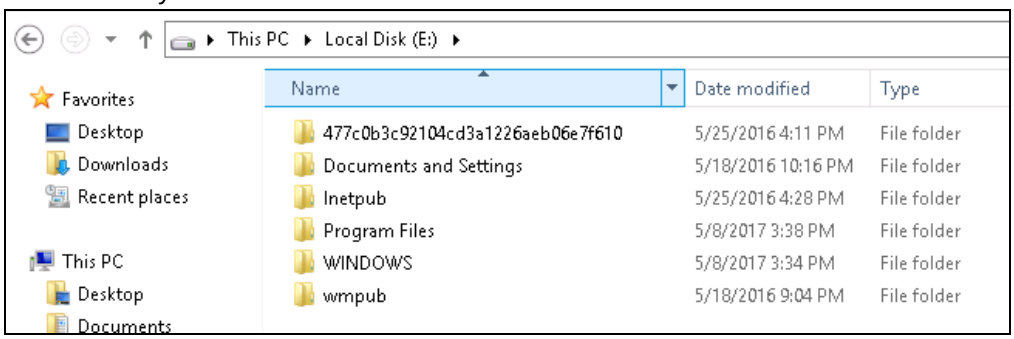
NOTES

Granular restore of Hyper-V backup sets performed using Windows File Explorer:

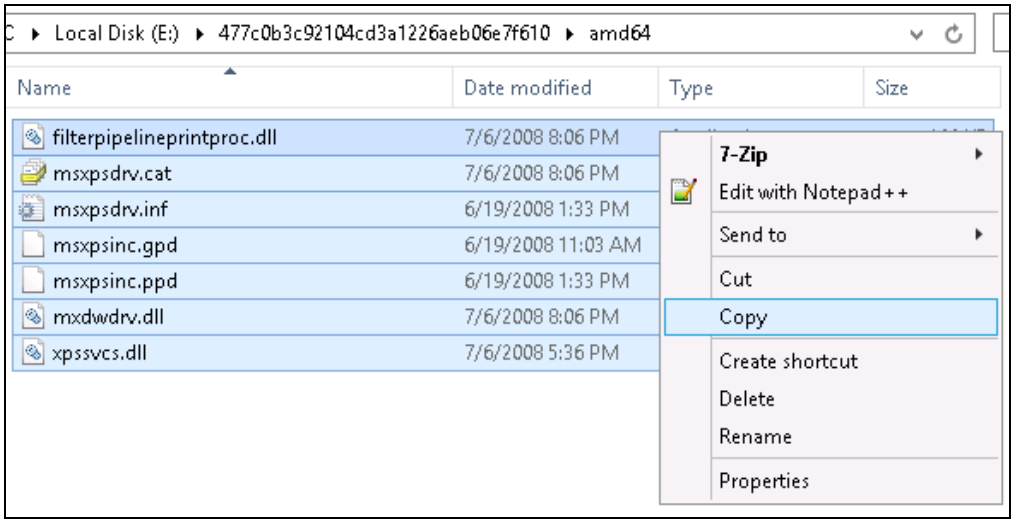
1. Will not show up on the [**Restore Status**] tab in **Live Activities** of the backup service provider AhsayCBS.
2. Will not generate restore reports on backup service provider AhsayCBS.
3. Will not generate restore log on backup service provider AhsayCBS.

i. Click and then you will be prompted to select a driver letter where you wish the mounted image to be mapped on your machine, click **OK** when you have finished selection.

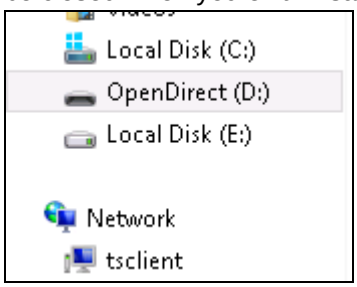
ii. The selected drive letter will be mapped and prompted in the Windows Files Explorer with the files you wish to restore shown.



iii. You can now click on the files to view them directly from here, which will be in read-only mode, or copy them to your local machine.



iv. The mounted drive letter cannot be ejected from the Windows File Explorer, it will only be closed when you exit AhsayOBR.



v. When you have finished restoring the necessary files, you can go back to AhsayOBR and click on **Cancel**.

vi. Then click on **Stop the granular restore** to unmount the virtual disk(s).

IMPORTANT

Due to the limitation of the virtual file system library, the mounted virtual disks will only be unmounted from your machine when you exit AhsayOBR.

10 Contacting Ahsay

10.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the Partner Portal: https://www.ahsay.com/partners/

Also use the Ahsay Wikipedia for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:
https://wiki.ahsay.com/

10.2 Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_downloads_documentation_guides

You can send us suggestions for improvements or report on issues in the documentation by contacting us at:
https://www.ahsay.com/partners/

Please specify the specific document title as well as the change required/suggestion when contacting us.