

A-Click Backup Manager v7

Microsoft System Backup and Restore Guide

Ahsay Systems Corporation Limited

14 September 2018

Copyright Notice

© 2018 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 (<http://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, Ahsay NAS Client Utility are trademarks of Ahsay Systems Corporation Limited.

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

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

Dropbox is registered trademark of Dropbox Inc.

Google Cloud Storage and Google Drive are registered trademarks of Google Inc.

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

Microsoft, Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, One Drive and One Drive for Business 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, Oracle 10g, Oracle 11g 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.

ShadowProtect is registered trademark of StorageCraft Technology Corporation.

VMware, ESX, ESXi, vCenter 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
28 Jul 2016	First Draft	New
3 Feb 2017	Added instructions and screen shots for Encryption key handling in Ch. 5.1	New
5 Apr 2017	Added Encryption Type option in Ch. 5.1 Create a MS Windows System Backup Set.	New
3 Nov 2017	Updated screen shot for Ch5.1	Modified
14 September 2018	Added requirement of Antivirus Exclusion for Ch.1.3; Updated Overview of backup process for Ch.6	New/ Modification

Table of Contents

Introduction.....	1
Overview	2
1 Requirements and Limitations.....	3
1.1 Hardware Requirement.....	3
1.2 Software Requirement	3
1.3 Antivirus Exclusion Requirement	3
1.4 Other Requirements and Limitations	3
2 Best Practice and Recommendation.....	5
3 Restore Consideration.....	7
4 Starting AhsayACB.....	8
4.1 Login to AhsayACB	8
5 Configuring a MS Windows System Backup Set	9
5.1 Create a MS Windows System Backup Set.....	9
6 Overview on the Backup Process	17
7 Running a Backup.....	18
7.1 Start a Manual Backup.....	18
7.2 Configure Backup Schedule for Automated Backup.....	19
8 Restore with a MS Windows System Backup Set.....	20
8.1 Login to AhsayACB	20
8.2 Restore the System Image	20
8.3 Recovering Your Server.....	24
8.3.1 Recover a Full System	25
Appendix	32
Appendix A Cloud Storage as Backup Destination.....	32
Appendix B Uninstall AhsayACB.....	33
Technical Assistance	34
Documentation	35

Introduction

The MS Windows System Backup module of AhsayACB provides you with a set of tools to protect your personal computers on Windows operating system platforms.

This includes an image-based / bare-metal backup feature, that leverages Microsoft's native Wbadmin command-line tool (<http://go.microsoft.com/fwlink/?LinkId=140216>), and recovery feature, to ensure that your computers are protected even if they are lost or destroyed entirely. The image can be recovered onto a new device if necessary.

Overview

This document contains information that are essential for understanding the MS Windows System backup and recovery process:

1. [Requirement and Limitation](#)
2. [Best Practice and Recommendation](#)
3. [Restore Consideration](#)
4. [Starting AhsayACB](#)
5. [Configuring a MS Windows System Backup Set](#)
6. [Overview on the Backup Process](#)
7. [Running a Backup](#)
8. [Restore with a MS Windows System Backup Set](#)

1 Requirements and Limitations

1.1 Hardware Requirement

Refer to the following article for the list of hardware requirements for AhsayACB: [FAQ: Ahsay Hardware Requirement List \(HRL\) for version 7.3 or above](#)

1.2 Software Requirement

Refer to the following article for the list of compatible Windows operating systems platforms: [FAQ: Ahsay Software Compatibility List \(SCL\) for version 7.3 or above](#)

1.3 Antivirus Exclusion Requirement

To optimize performance of AhsayACB on Windows, and to avoid conflict with your antivirus software, refer to the following KB article the list of processes and directory paths that should be added to all antivirus software white-list / exclusion list:
http://wiki.ahsay.com/doku.php?id=public:5352_suggestion_on_antivirus_exclusions

NOTE

For AhsayACB version 7.17 or above, the bJW.exe process is automatically added to Windows Defender exclusion list for Windows 10 and 2016, during installation / upgrade via installer or upgrade via AUA.

1.4 Other Requirements and Limitations

Ensure that the following requirements are met:

• AhsayACB Installation

Make sure that AhsayACB is installed on the computer to be backed up.

• Add-on Module Requirement

Make sure that the Windows System Backup add-on module is enabled for your AhsayACB user account. Contact your backup service provider for more details.

• Backup Quota Requirement

Make sure that your AhsayACB user account has sufficient backup storage quota assigned to accommodate the storage for the system backup. Contact your backup service provider for details.

• Latest Service Packs from Microsoft

Ensure that you have the latest service packs installed.

Updates to the Windows operating system improve its performance and resolve known issues with Windows Server Backup.

• Temporary Storage Location

Make sure that the storage location configure for the system image is set to a supported location.

Refer to the following KB article for details on the restriction:

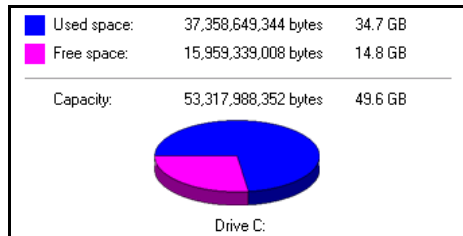
<https://forum.ahsay.com/viewtopic.php?f=196&t=16301>

❶ Disk Space Available in Temporary Storage Location

Make sure that there are sufficient disk spaces available in the storage location for the backup set.

For a system backup, it will typically require disk space of the total used size of all volumes selected for backup.

Note: *Used space, not free space of all volumes selected for backup.*



❷ Maximum Supported Disk Size

For Windows Vista / 7, source volumes with size greater than 2 TB (e.g. 2040 GB - 2 MB = 2088958 MB) are not supported.

This limitation is related to the .vhd file size limit.

Note: *This limitation does not apply to Windows 8 or newer releases of Windows.*

2 Best Practice and Recommendation

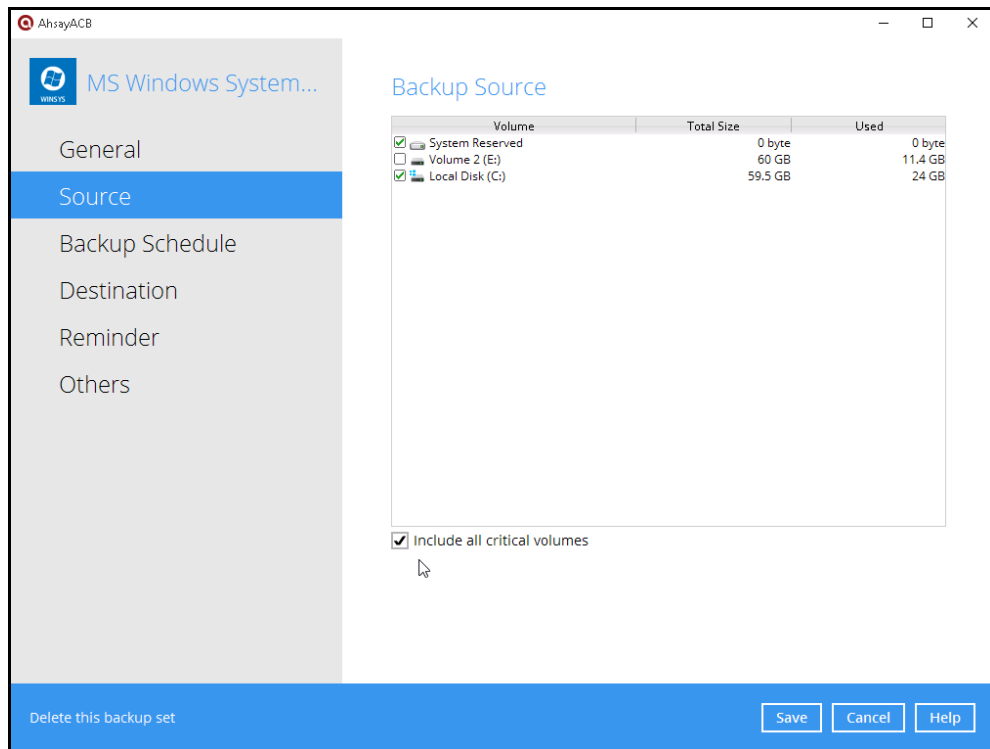
Please consider the following recommendations:

- It is recommended that the latest version of AhsayACB is installed on the computer to be backed up.

User should also stay up-to-date when newer version of AhsayACB is released. To get our latest product and company news through email, please subscribe to our mailing list via http://www.ahsay.com/jsp/en/home/subscribe_mail_list.jsp
- For best performance, It is recommended that the temporary storage location of a MS Windows System backup set is set to a supported local volume, and not to a network volume (e.g. to improve I/O performance).

The screenshot shows the AhsayACB configuration window for a 'MS Windows System Backup'. The 'General' tab is active in the sidebar. The main configuration area includes a 'Name' field set to 'MS Windows System Backup Set', an 'Owner' field set to 'Win10', and a dropdown menu for 'Specify the location where you want to store the system backup' currently set to 'Volume 2 (E:)'. Below this is a 'Windows User Authentication' section with fields for 'Domain Name (e.g. Ahsay.com) / Host Name' (csv2012.local), 'User name' (Administrator), and 'Password' (masked with dots). At the bottom of the window, there is a 'Delete this backup set' link and 'Save', 'Cancel', and 'Help' buttons.

- It is highly recommended to enable the **Include all critical volumes** option to select all critical volumes for backup automatically.



This will ensure that the backup image can be used for full-system / bare-metal recovery.

❶ **Memory setting**

For best performance, consider to increase the memory allocation setting for AhsayACB (Java heap space)

Refer to the following KB article for further instruction:

<https://forum.ahsay.com/viewtopic.php?f=206&t=14117>

❷ **Not a Replacement for File Backup**

An image-based / bare-metal backup should never be considered a replacement for a nightly data backup plan.

Firstly, image-based backups do not lend themselves easily to recovery of a single file. The nature of image-based backup requires a complete restore of the system image file, even if you only want to recover a single file.

❸ **System Recovery Plan**

Consider performing routine system recovery test to ensure your system backup is setup and performed properly. Performing system recovery test can also help identify potential issues or gaps in your system recovery plan.

For best result, it is recommended that you should keep the test as close as possible to a real situation. Often times when a recovery test is to take place, user will plan for the test (e.g. reconfiguring the test environments, restoring certain data in advance). For real recovery situation, you will not get a chance to do that.

It's important that you do not try to make the test easier.

3 Restore Consideration

Please consider the following before performing a restore:

- 1 **Windows Account Permission**

To perform a full-system recovery, the operating system account that you use, must be a member of the Backup Operators or Administrators group.

- 2 **Disk Size**

For recovery of operating system to a new hard disk, ensure that the disk that you restore to is at least the size of the disk that contained the volumes that were backed up, regardless of the size of those volumes within.

For example, if there was only one volume of size 100 GB created on a 1 TB disk during backup, then you should use a disk that is at least 1 TB when recovering.

- 3 **Caution on Recovery to Dissimilar Hardware**

This recovery method requires the restore target system to have similar hardware and the exact same boot type as the source system from which the backup was taken. Disk adapters are especially sensitive. If dissimilar hardware is used, the restored system might not be boot.

For example, if the system backup image was taken from a BIOS-based system, the recovery environment must be booted in BIOS mode.

- 4 **BitLocker Drive**

For computer with BitLocker Drive Encryption enabled, make sure to re-apply BitLocker Drive Encryption to the volume after a restore.

This will not happen automatically, it must be enabled explicitly.

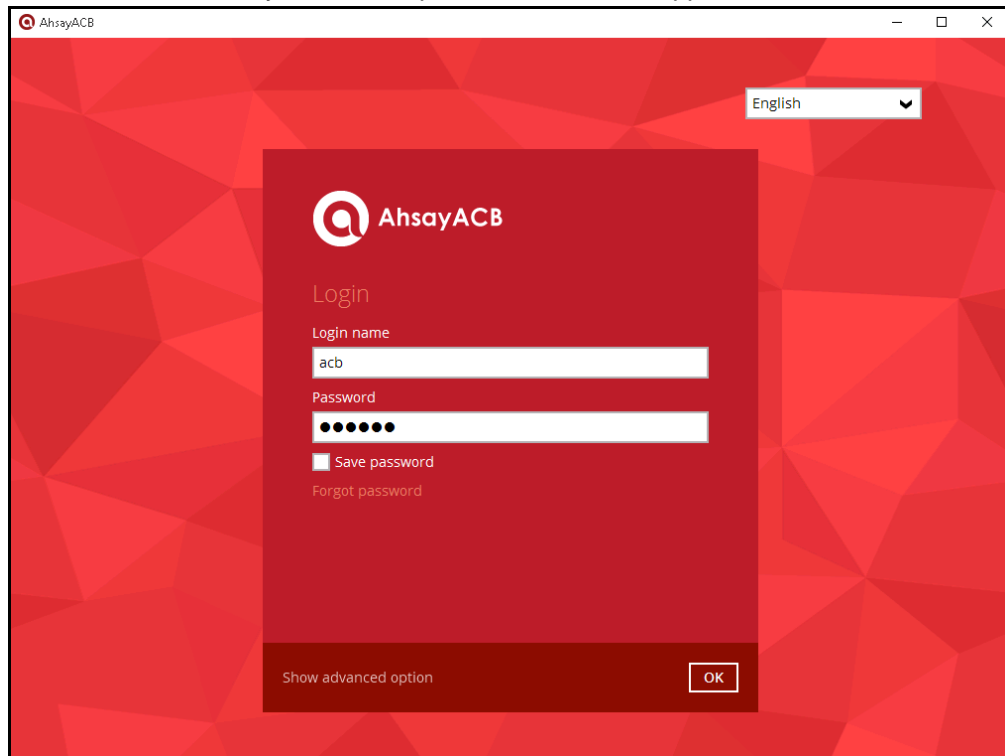
For instructions, refers to the following: <http://go.microsoft.com/fwlink/?LinkID=143722>

4 Starting AhsayACB

4.1 Login to AhsayACB

1. Login to the AhsayACB application user interface.

Double click the AhsayACB desktop icon to launch the application.

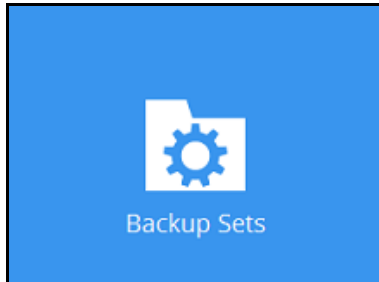


2. Enter the **Login name** and **Password** of your AhsayACB account.
3. Click **OK** afterward to login to AhsayACB.

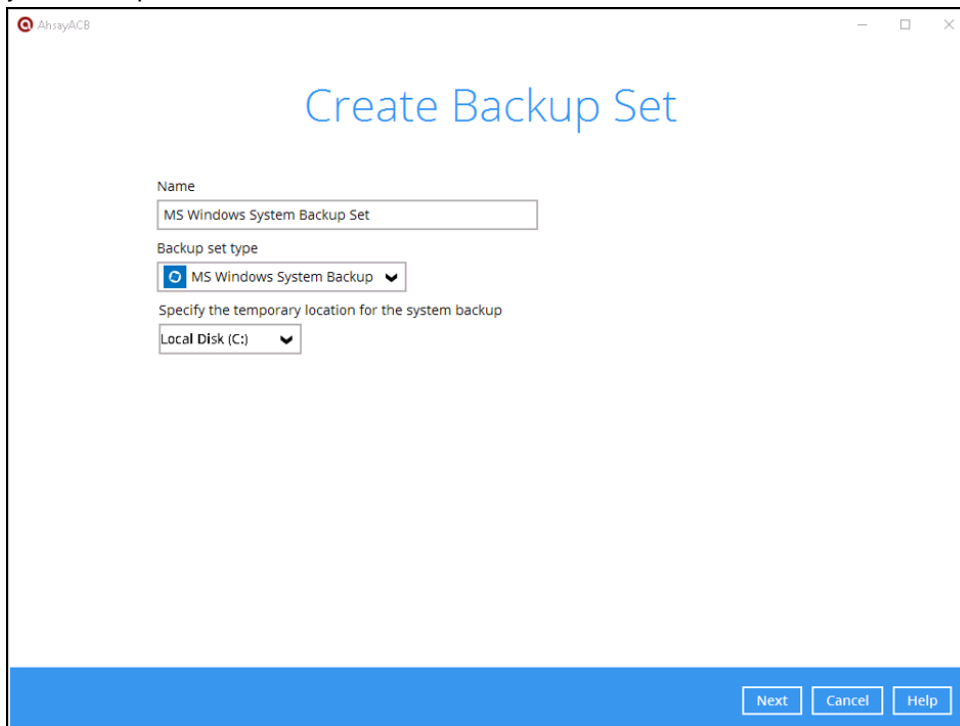
5 Configuring a MS Windows System Backup Set

5.1 Create a MS Windows System Backup Set

1. In the AhsayACB main interface, click **Backup Sets**.



2. Create a MS Windows System backup set by clicking the “+” icon next to **Add new backup set**.
3. Select **MS Windows System Backup** as the **Backup set type**; then enter a **Name** for your backup set.

A screenshot of a Windows-style dialog box titled 'Create Backup Set'. The dialog has a white background and a blue header bar. It contains three input fields: a text box for 'Name' with the value 'MS Windows System Backup Set', a dropdown menu for 'Backup set type' with 'MS Windows System Backup' selected, and a dropdown menu for 'Specify the temporary location for the system backup' with 'Local Disk (C:)' selected. At the bottom right, there are three buttons: 'Next', 'Cancel', and 'Help'.

4. Select the location where you would like to store the system image before generating the backup data.

Select a local volume from the dropdown menu. Click **Next** to proceed.

AhsayACB

Create Backup Set

Name
MS Windows System Backup Set

Backup set type
☒ MS Windows System Backup

Specify the temporary location for the system backup
Local Disk (C:) ▼
Local Disk (C:)
Volume 2 (E:)

Next Cancel Help

-OR-

Enter the UNC path to a network volume that is accessible to the client computer. Click **Next** to proceed.

AhsayACB

Create Backup Set

Name
MS Windows System Backup Set

Backup set type
☒ MS Windows System Backup

Specify the temporary location for the system backup
\\unc_path\\share ▼

Next Cancel Help

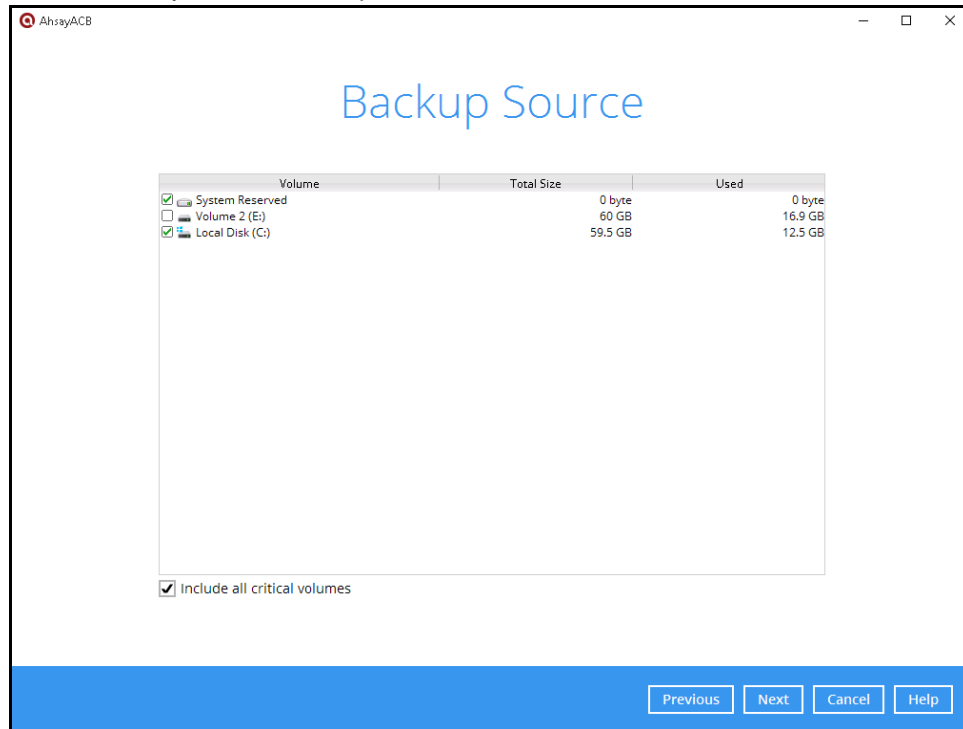
Note: Make sure that the storage location configure for the system image is set to a supported location.

Refer to the following KB article for details on the restriction:

<https://forum.ahsay.com/viewtopic.php?f=196&t=16301>

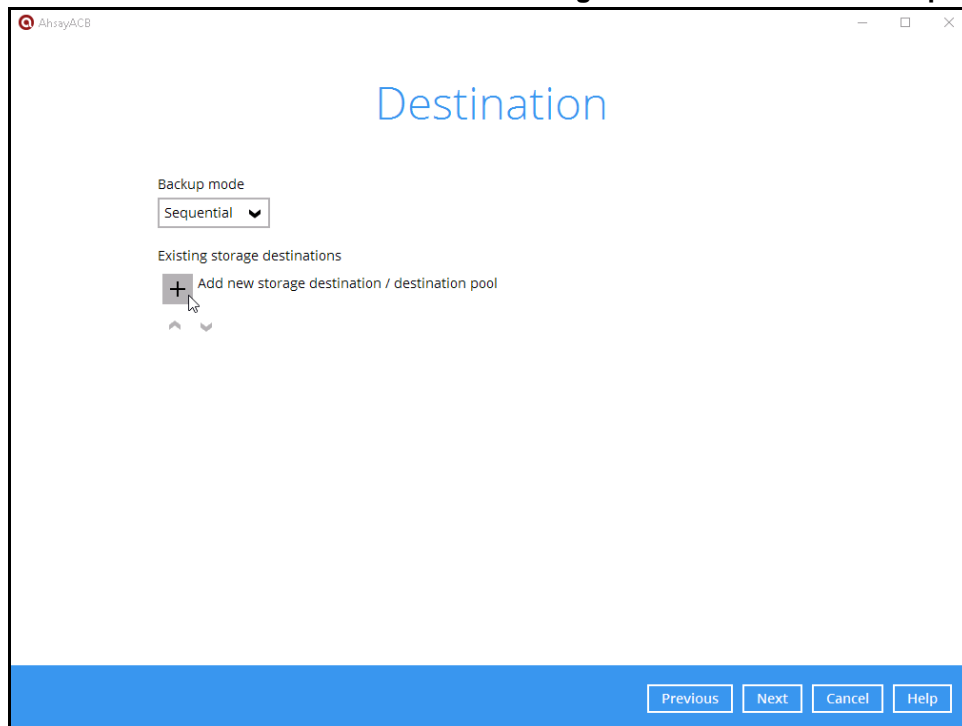
5. In the Backup Source menu, select the volume(s) which you would like to backup.

Enable the **Include all critical volumes** option to select all critical volumes for backup automatically. This will ensure that the backup image can be used for full-system / bare-metal recovery. Click **Next** to proceed.



6. In the Schedule menu, configure a backup schedule for backup job to run automatically at your specified time interval. Click **Add** to add a new schedule, then click **Next** to proceed afterward.

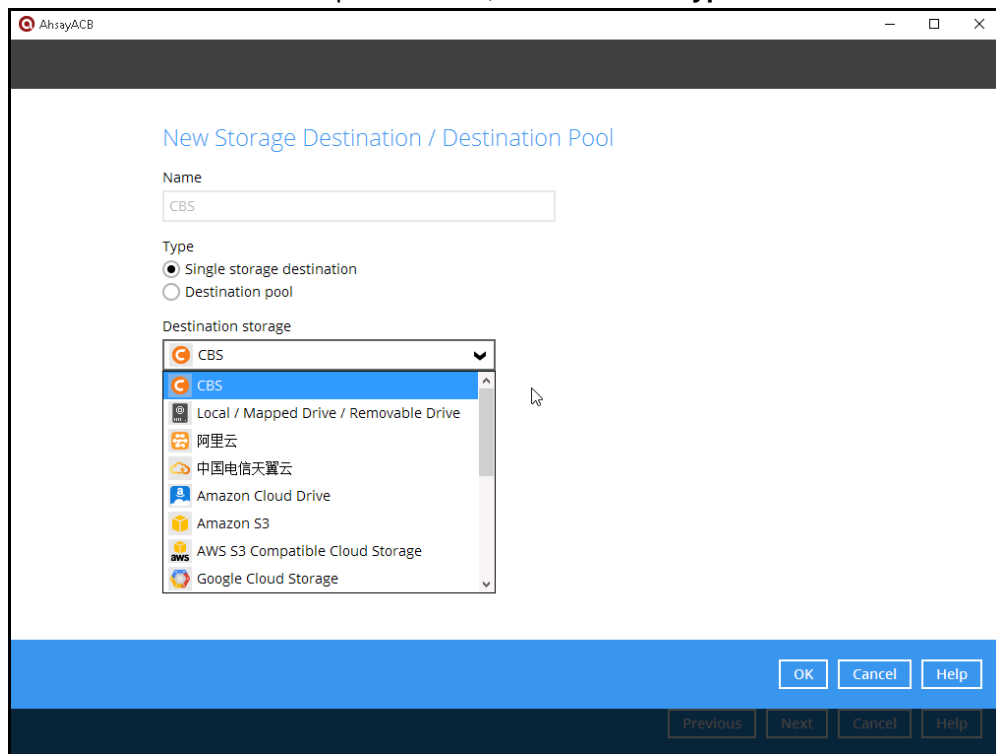
7. In the Destination menu, select a backup destination where the backup data will be stored. Click the “+” icon next to **Add new storage destination / destination pool**.



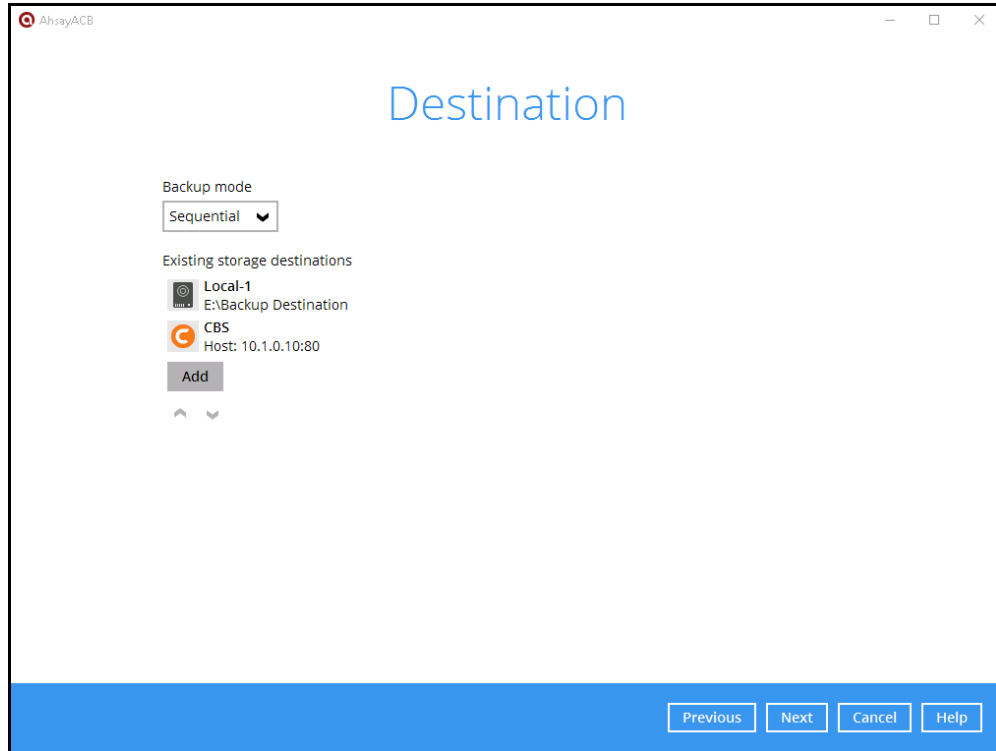
Note: For more details on Backup Destination, refer to the following KB article for details:
<https://forum.ahsay.com/viewtopic.php?f=186&t=14049>

For more details on configuration of cloud storage as backup destination, refer to the [Appendix](#) section in this guide.

8. Enter a **Name** for the backup destination, and select the **Type** and **Destination storage**.

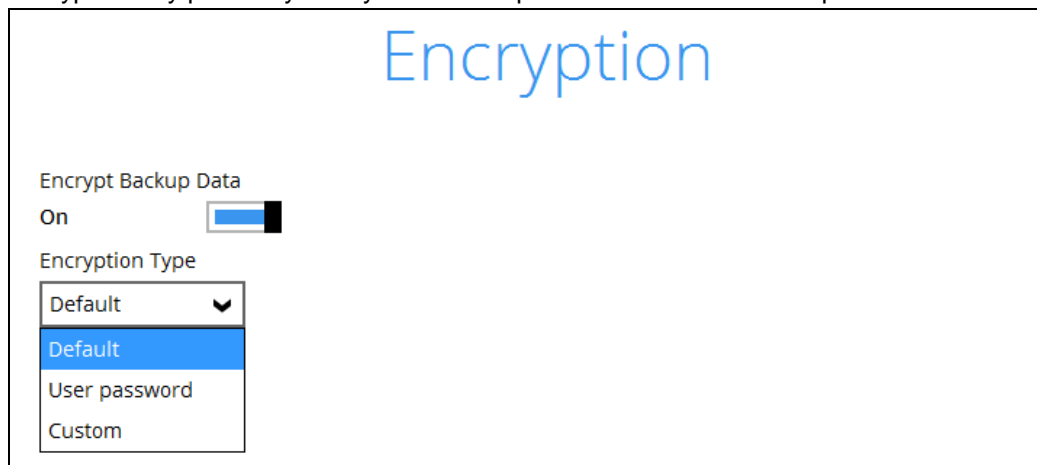


9. Continue by adding another destination for the backup set, or click **Next** to proceed.



Note: Multiple backup destinations can be configured for a single backup set.

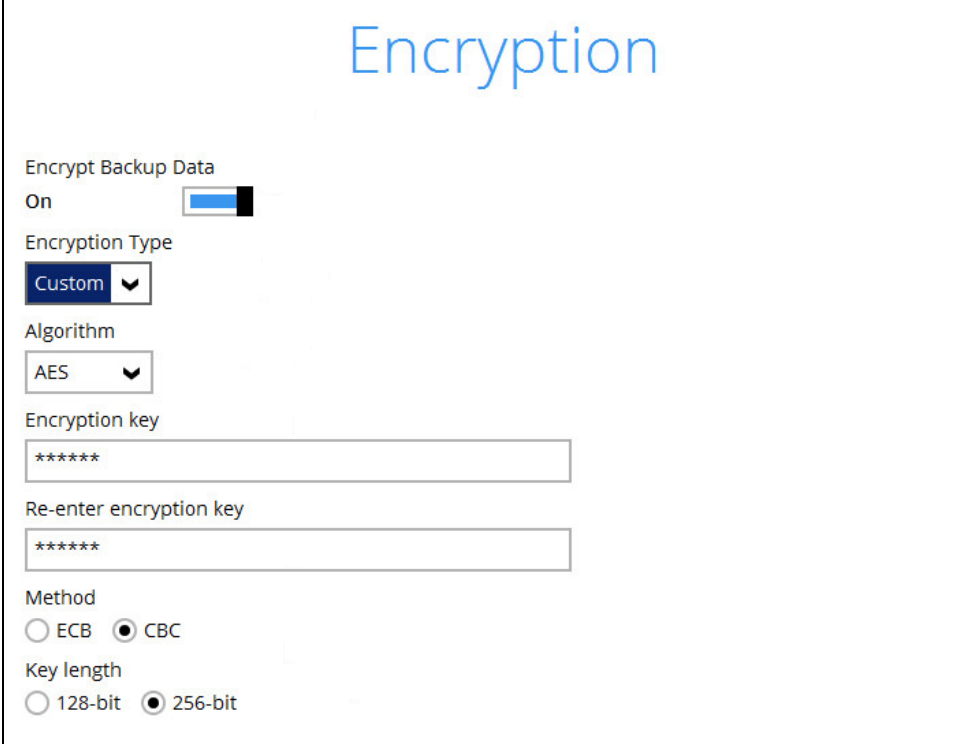
10. In the Encryption window, the default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides the most secure protection.



You can choose from one of the following three Encryption Type options:

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your AhsayACB at the time when this backup set is created. Please be reminded that if you change the AhsayACB login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.

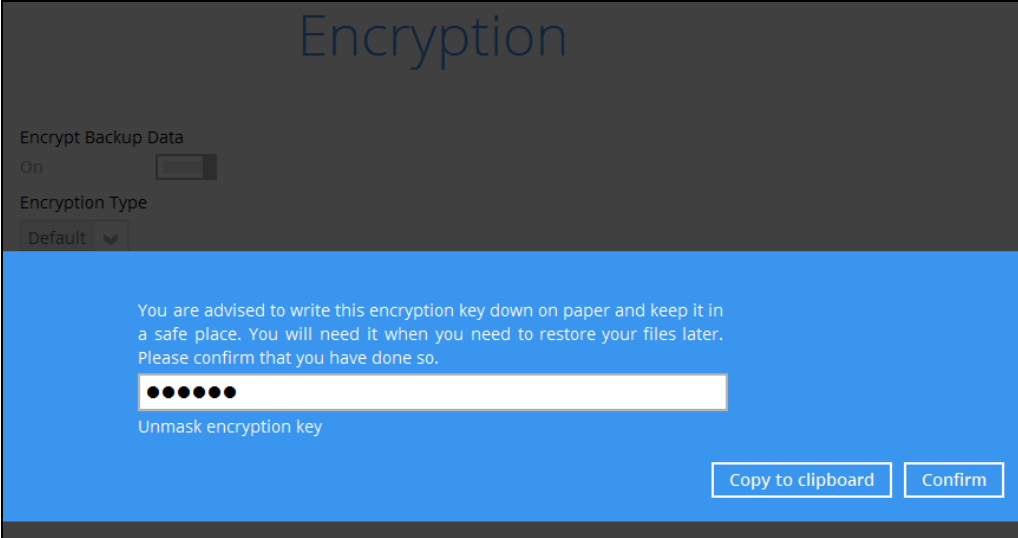
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.



Note: For best practice on managing your encryption key, refer to the following KB article. <https://forum.ahsay.com/viewtopic.php?f=169&t=14090>

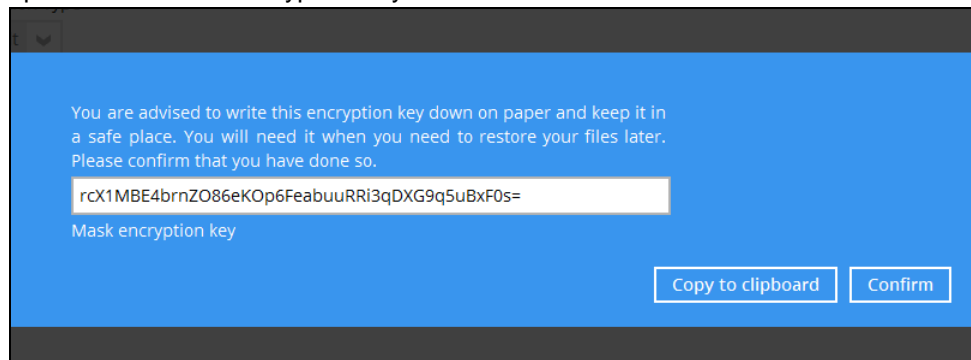
Click **Next** when you are done setting.

11. If you have enabled the Encryption Key feature in the previous step, the following pop-up window shows, no matter which encryption type you have selected.



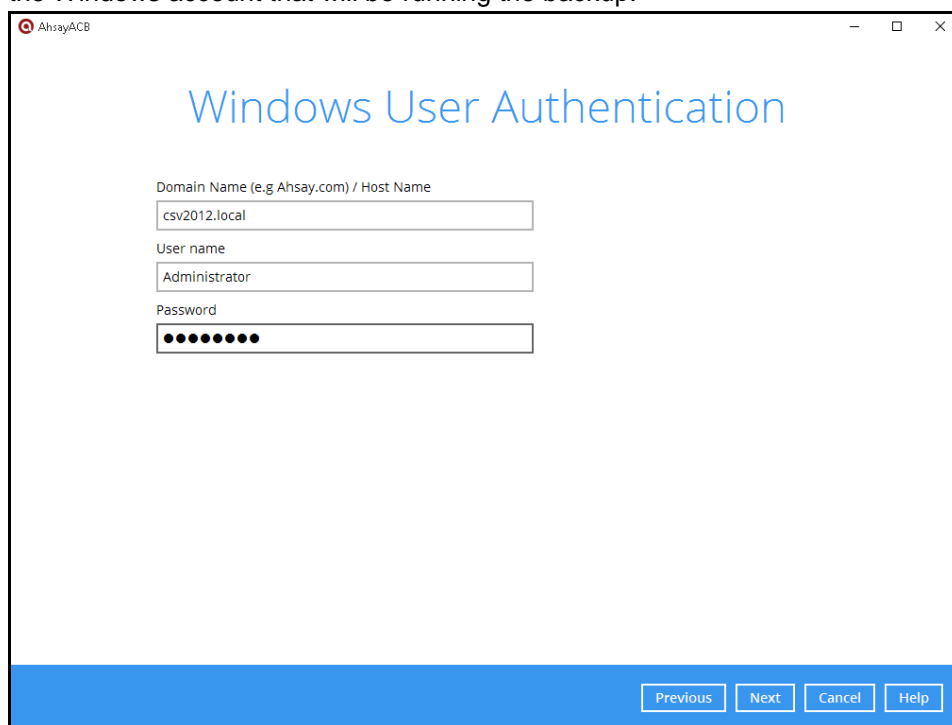
The pop-up window has the following three options to choose from:

- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.
- **Confirm** – Click to exit this pop-up window and proceed to the next step.

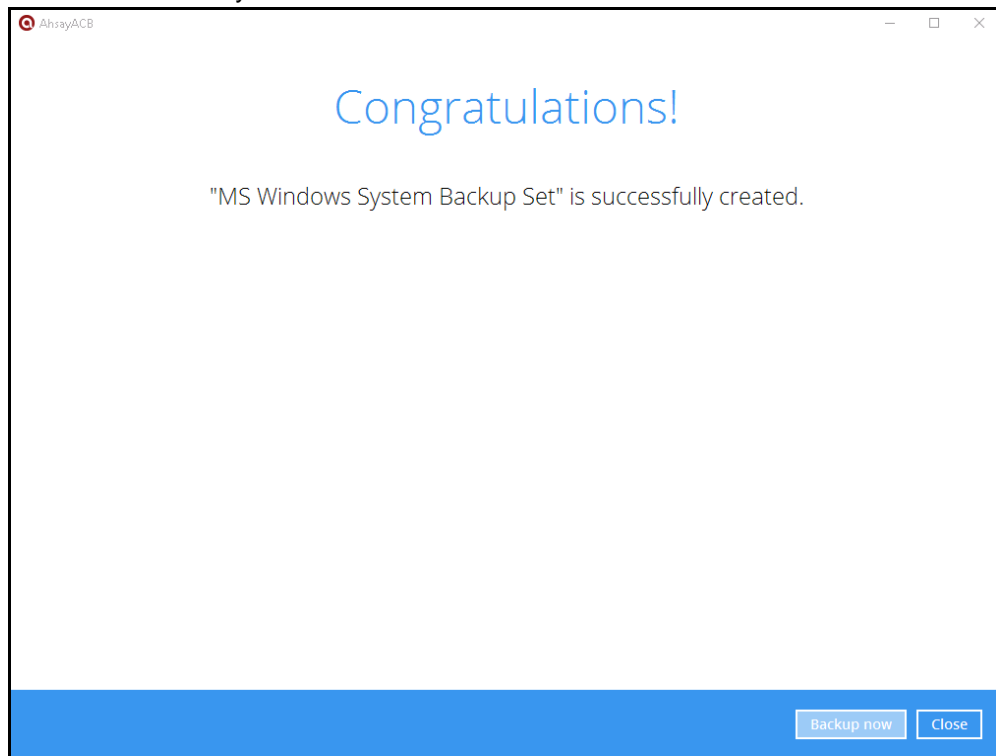
12. Enter the **Domain Name / Host Name** of the computer, **User Name** and **Password** of the Windows account that will be running the backup.



Note: This menu will only be displayed if a backup schedule is configured in the previous step.

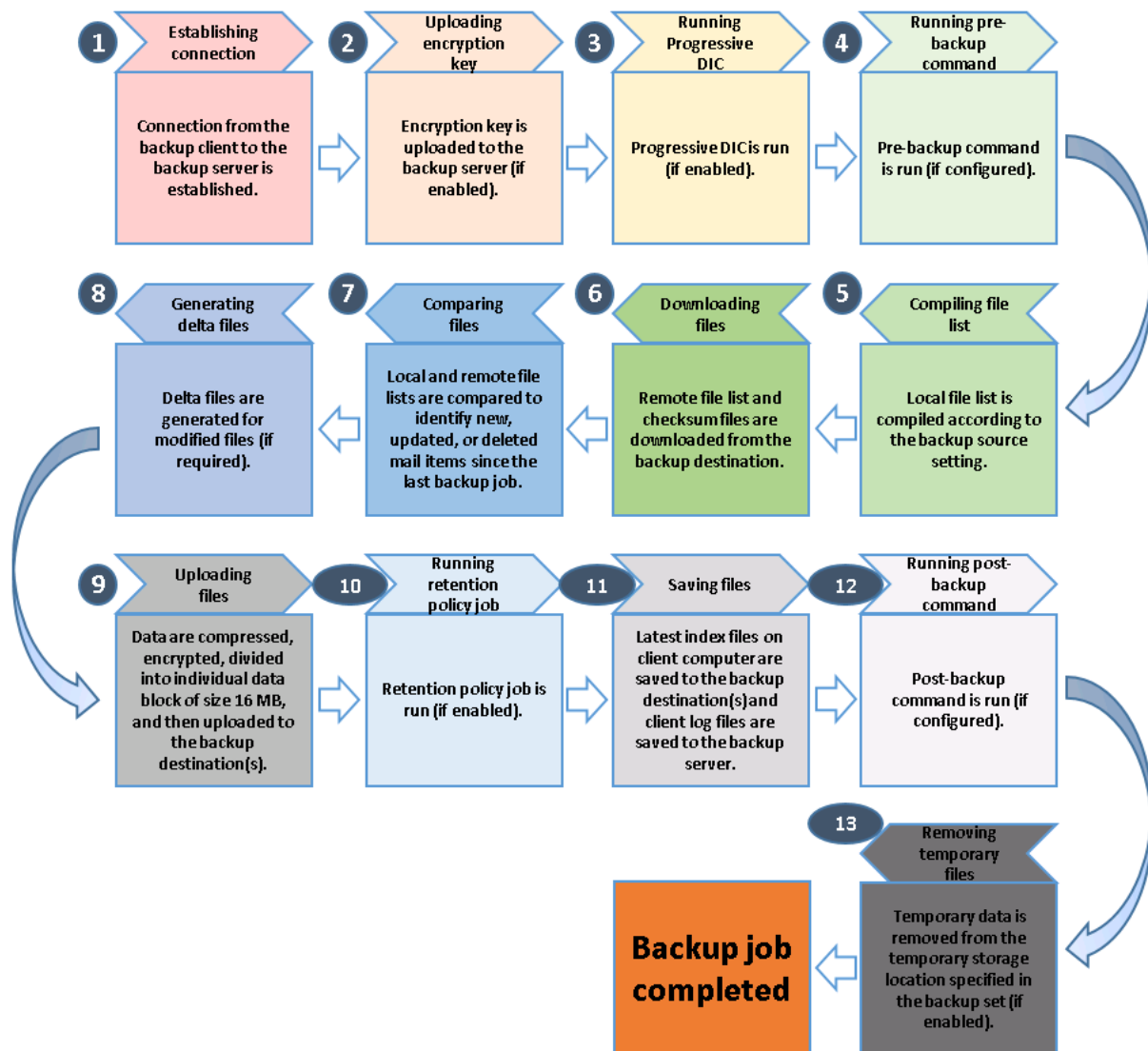
13. Click **Next** to create the backup set.

14. The following screen is displayed when the new MS Windows System backup set is created successfully.



6 Overview on the Backup Process

The following steps are performed during a MS Windows System backup job.



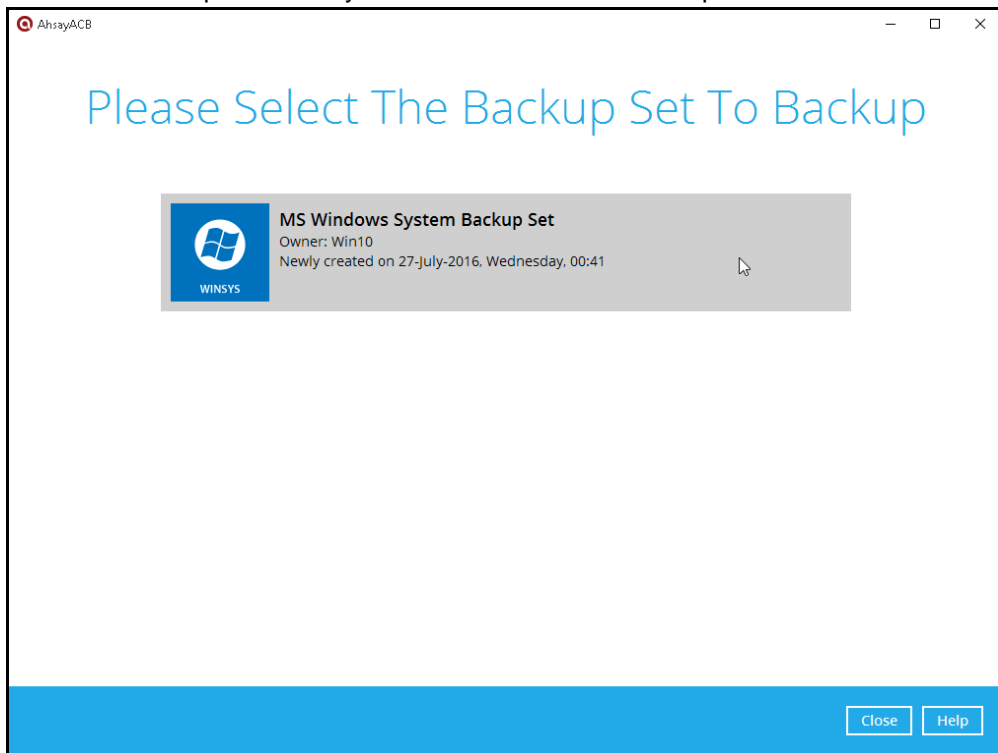
7 Running a Backup

7.1 Start a Manual Backup

1. Click the **Backup** icon on the main interface of AhsayACB.



2. Select the backup set which you would like to start a backup for.



3. If you would like to modify the In-File Delta type, Destinations and Retention Policy Settings, click **Show advance option**.
4. Click **Backup** to start the backup.

7.2 Configure Backup Schedule for Automated Backup

1. Click the Backup Sets icon on the AhsayACB main interface.



2. Select the backup set that you want to create a backup schedule for.
3. Click **Backup Schedule**, then create a new backup schedule by clicking **Add**.
4. Configure the backup schedule settings, then click **OK** to proceed.
5. Click **Save** to confirm your settings.

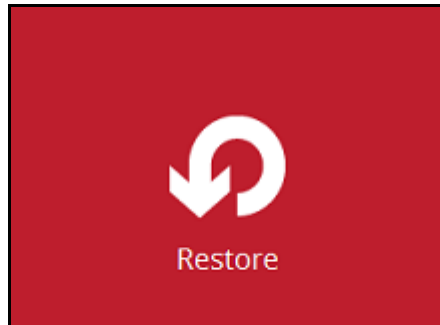
8 Restore with a MS Windows System Backup Set

8.1 Login to AhsayACB

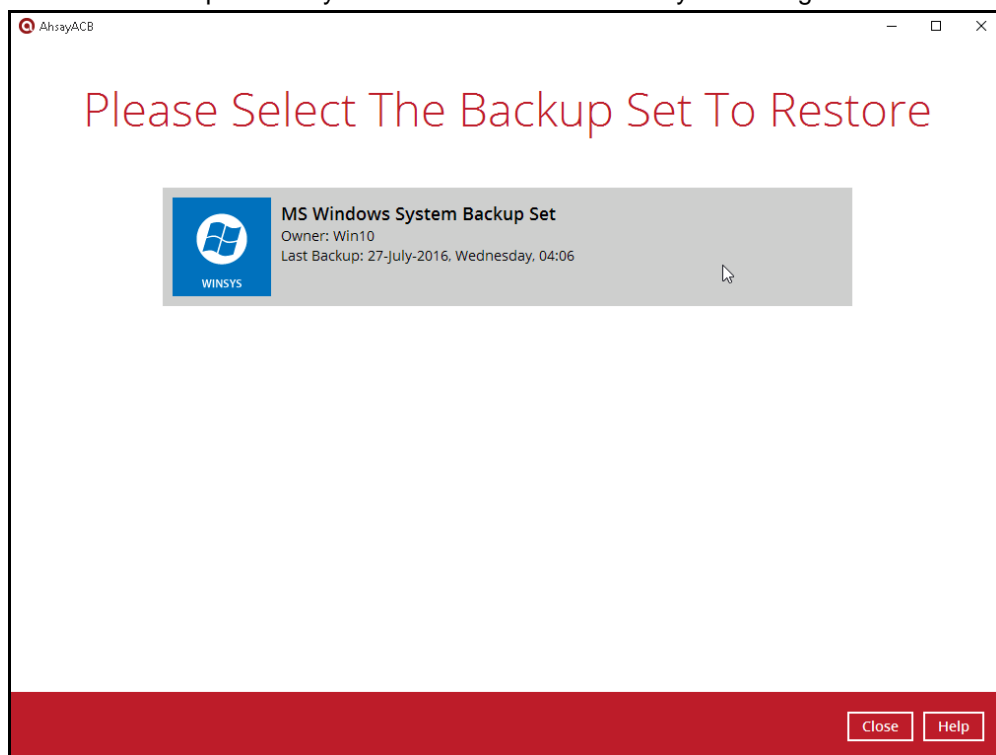
Login to the AhsayACB application according to the instruction provided in the chapter on [Starting AhsayACB](#).

8.2 Restore the System Image

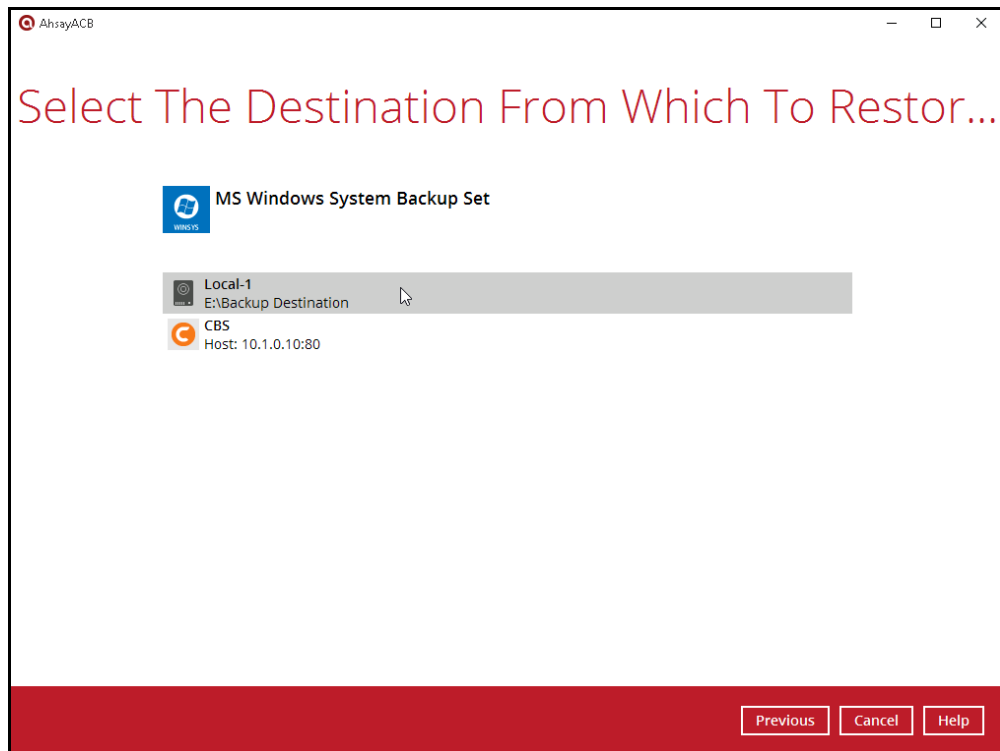
1. Click the **Restore** icon on the main interface of AhsayACB.



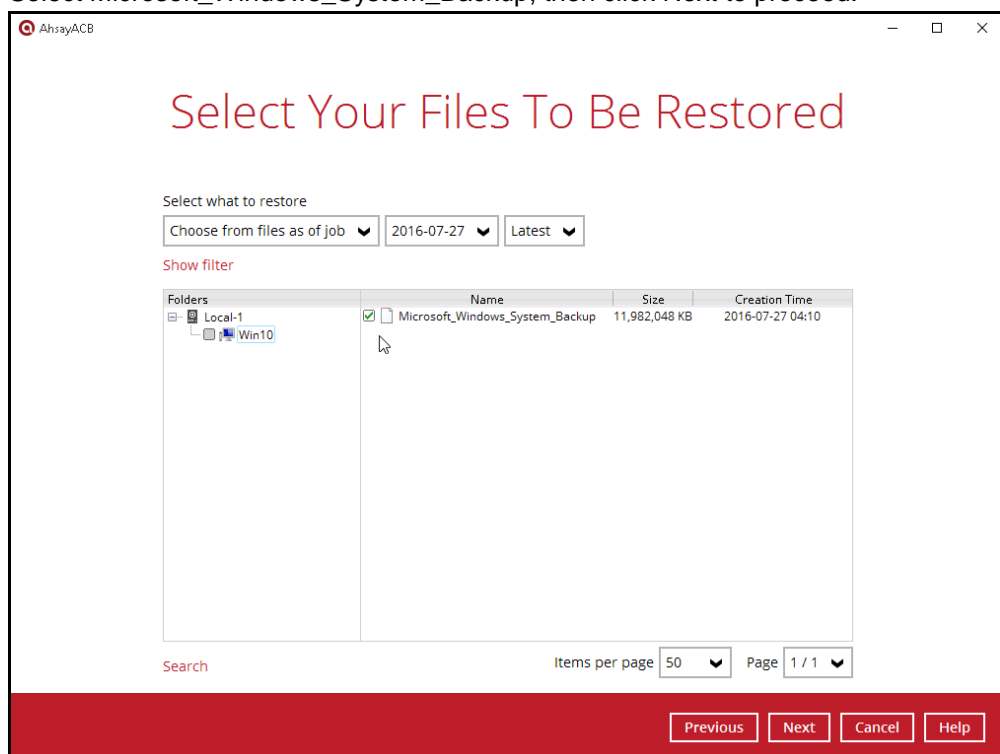
2. Select the backup set that you would like to restore the system image from.



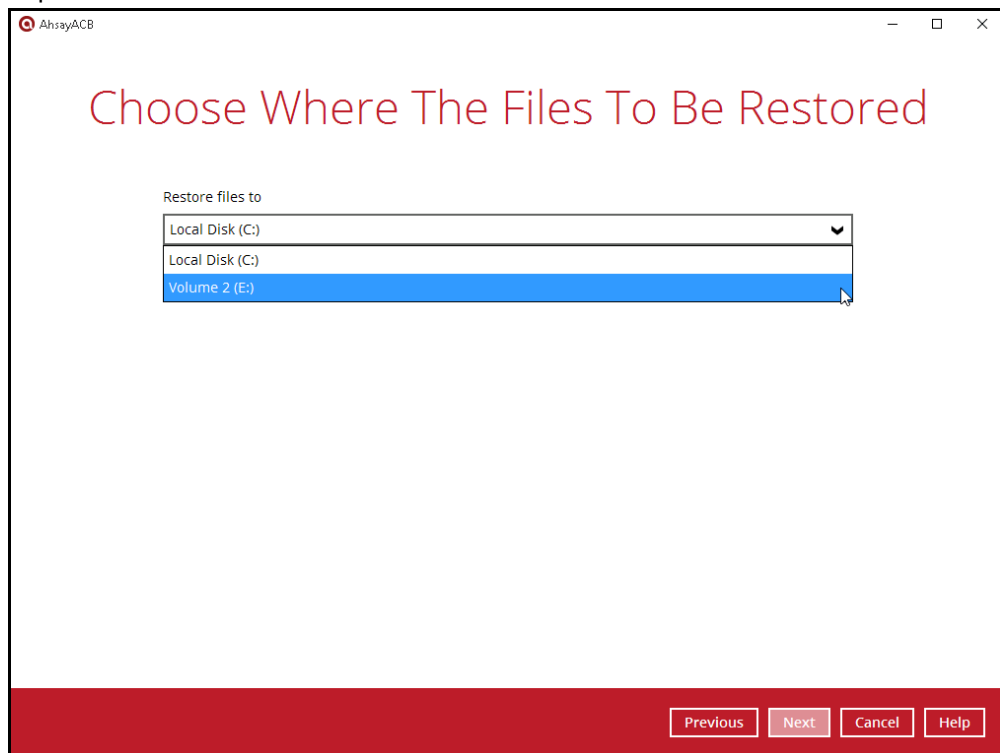
3. Select the backup destination that contains the system image that you would like to restore.



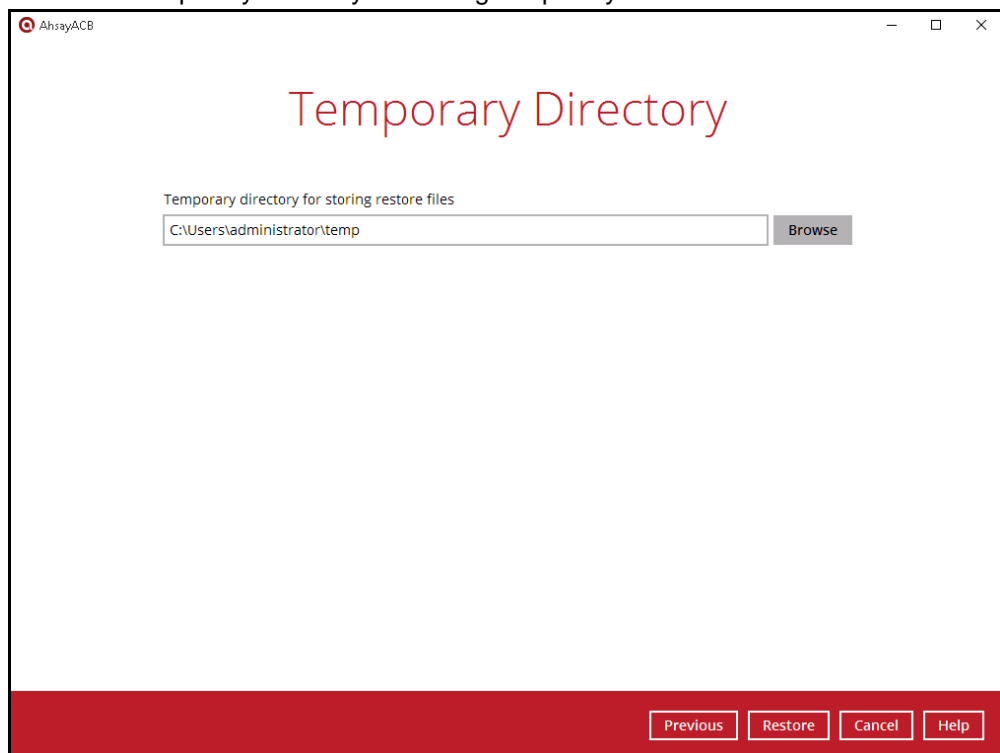
4. Select to restore from a specific backup job, or the latest job available from the **Select what to restore** drop down menu.
5. Select Microsoft_Windows_System_Backup, then click Next to proceed.



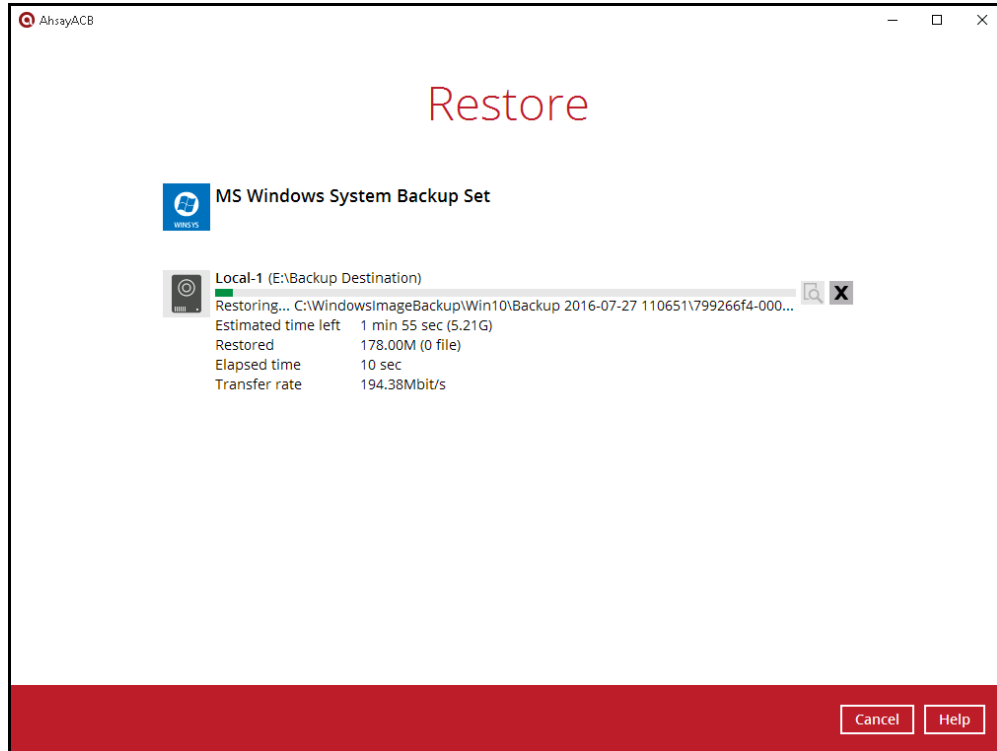
6. Select to restore the system image to a local volume or to a removable drive. Click **Next** to proceed.



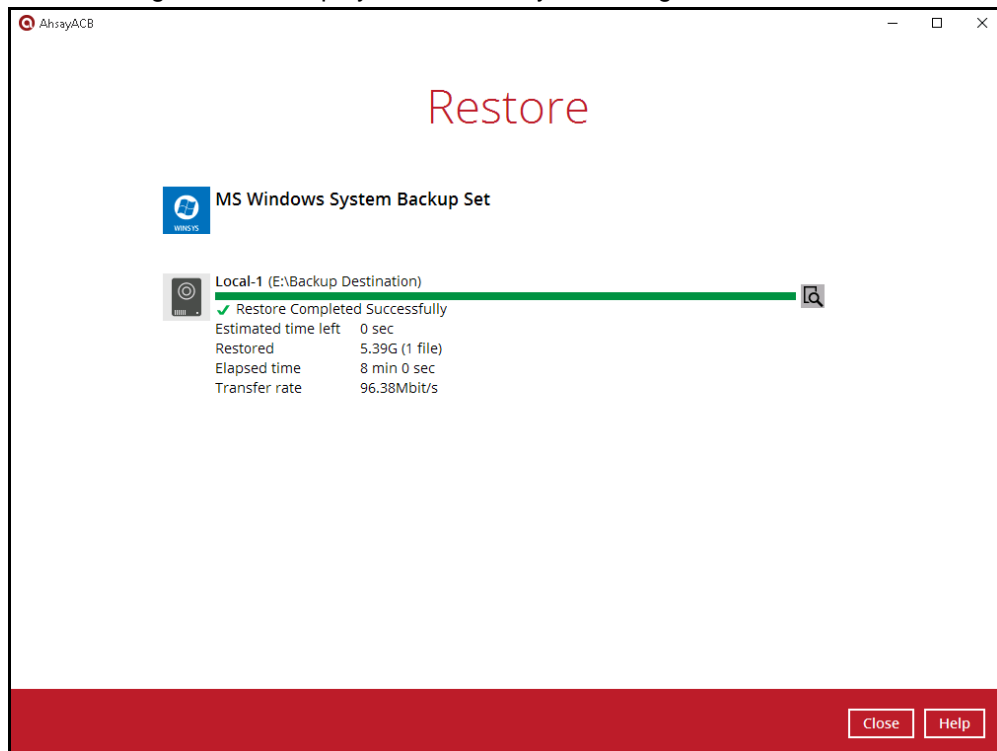
7. Select the temporary directory for storing temporary files.



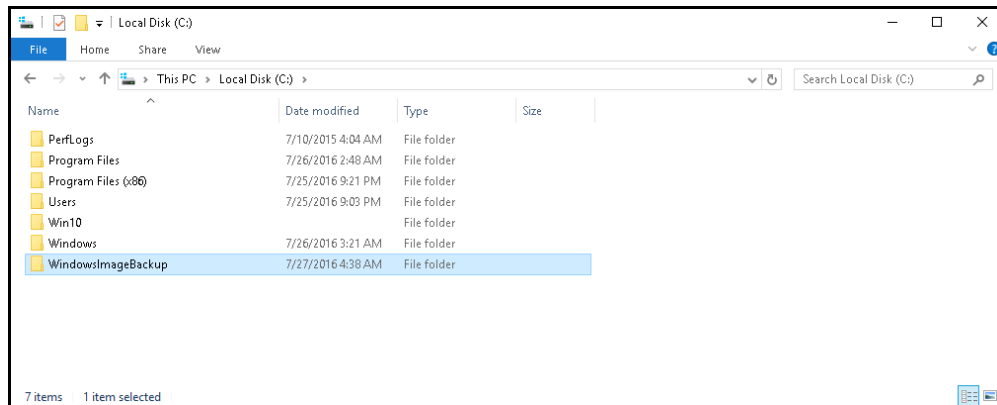
8. Click **Restore** to start the restoration.



9. The following screen is displayed when the system image files are restored successfully.



10. The restored system image files are stored in the **WindowsImageBackup** folder in the restore location.



Important: In addition to the system image files, the **WindowsImageBackup** folder includes catalog files that contain information about all backups in there up to the current backup, and MediaId, that contains the identifier for the backup storage location.

This information is required to perform a recovery. Do not alter the directory structure or delete any file / folder within the **WindowsImageBackup** folder.

11. Copy the **WindowsImageBackup** folder with its content to the server that you want to perform the restore for, or copy the folder to a network drive that is accessible to the server that you want to perform the restore for.

WindowsImageBackup folder must be stored at the root level of a volume (e.g. top-most level), unless you are copying the folder to a network drive.

12. Continue to the next section of the guide.

8.3 Recovering Your Server

You can recover perform a full-system (bare-metal) with the following tools:

Tool	What you can recover
Advanced startup option (in safe mode)	Full system recovery.
Advanced startup option (Windows installation media)	Full system recovery.

Note: You can also perform the above tasks using `wbadmin` command. For the syntax of the command, refer to the following: <http://go.microsoft.com/fwlink/?LinkId=140216>

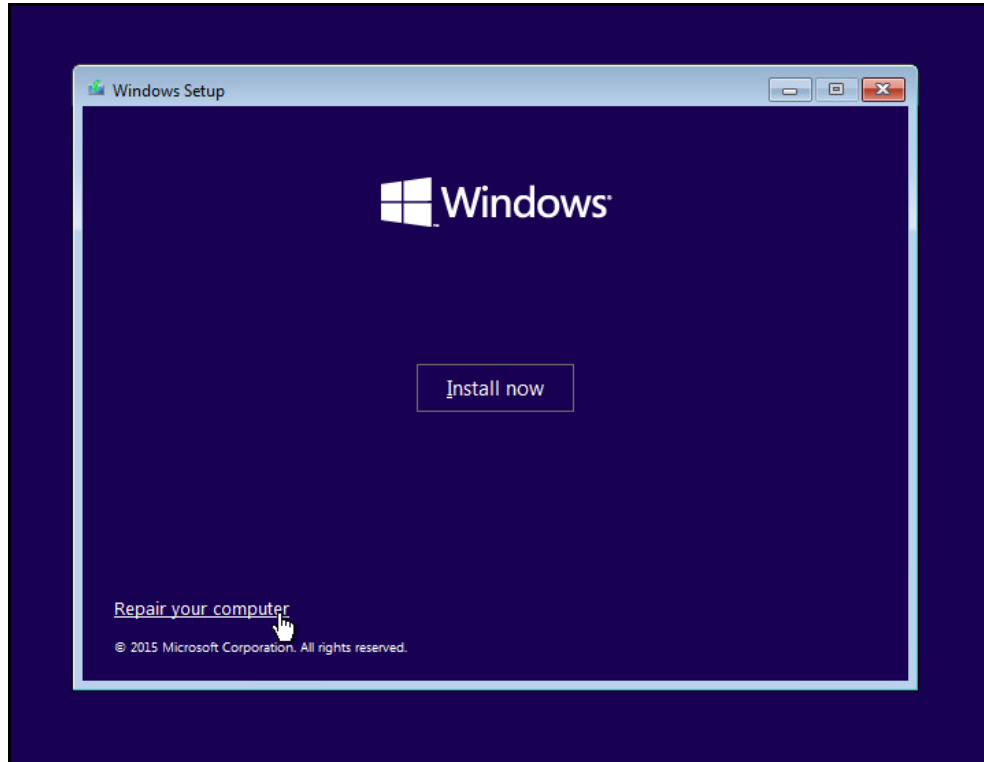
8.3.1 Recover a Full System

You can recover a full system using the advanced startup option by:

- ▶ **Booting from a Windows installation media**

Insert the installation media that has the same architecture of the system that you are recovering, and restart your computer. Press the required key to boot from the disc.

When you see the **Windows Setup** page, click **Next**, then click **Repair your computer**.

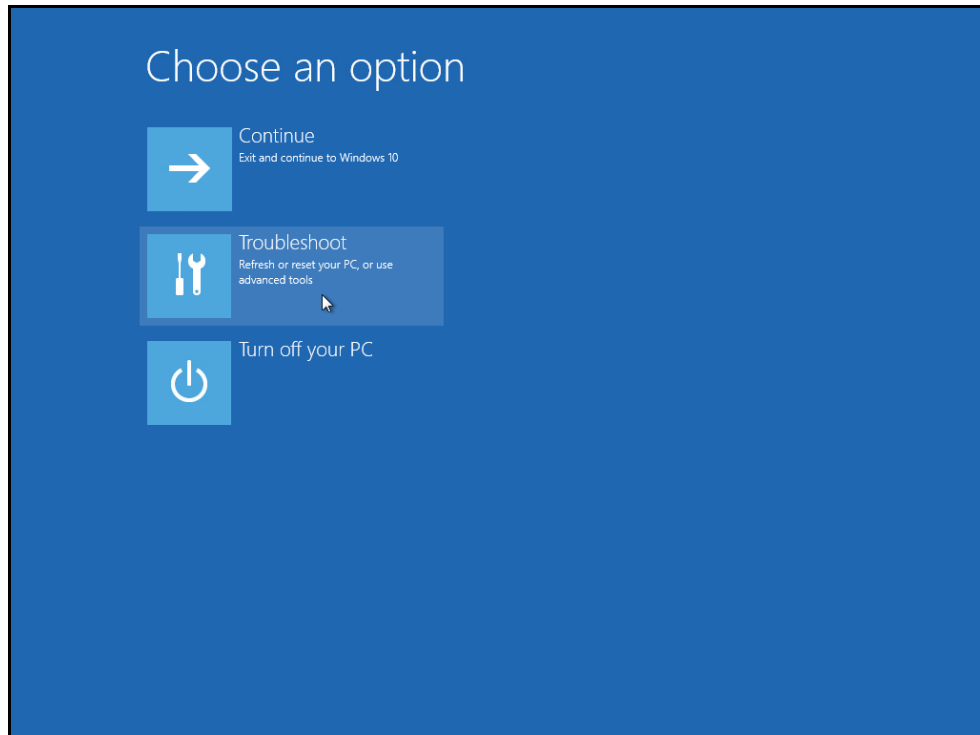


- ▶ **Starting Windows in safe mode**

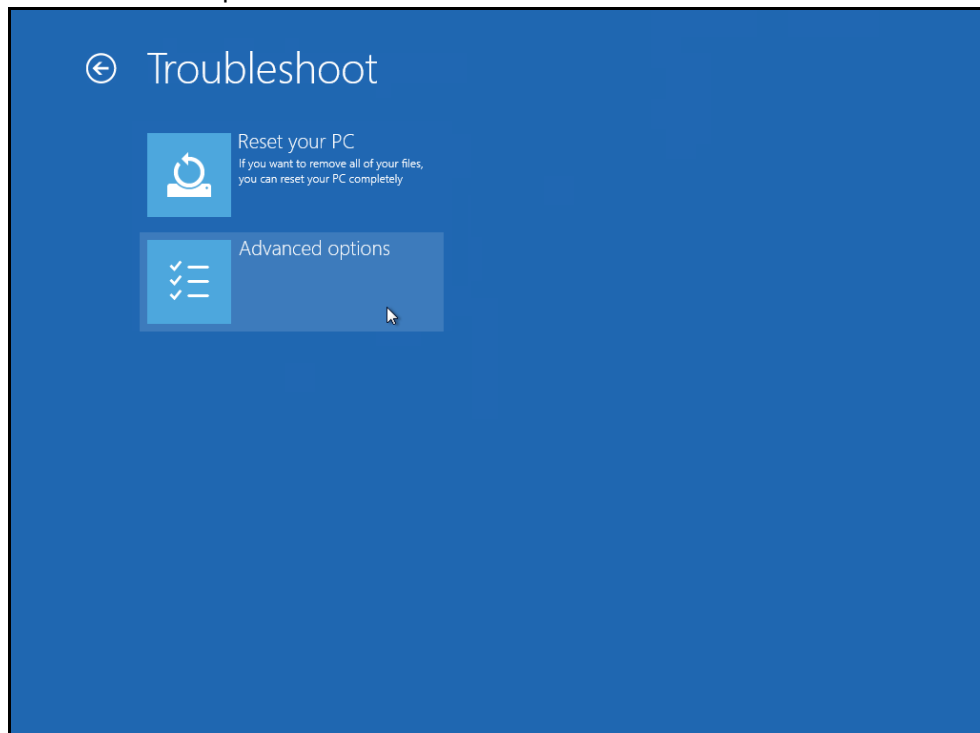
Press the **Power** button at the Windows login screen. In the Start menu or in the Setting screen, press and hold the SHIFT key on the keyboard and click **Restart**.

Once you are in the Startup Option menu, perform the following steps.

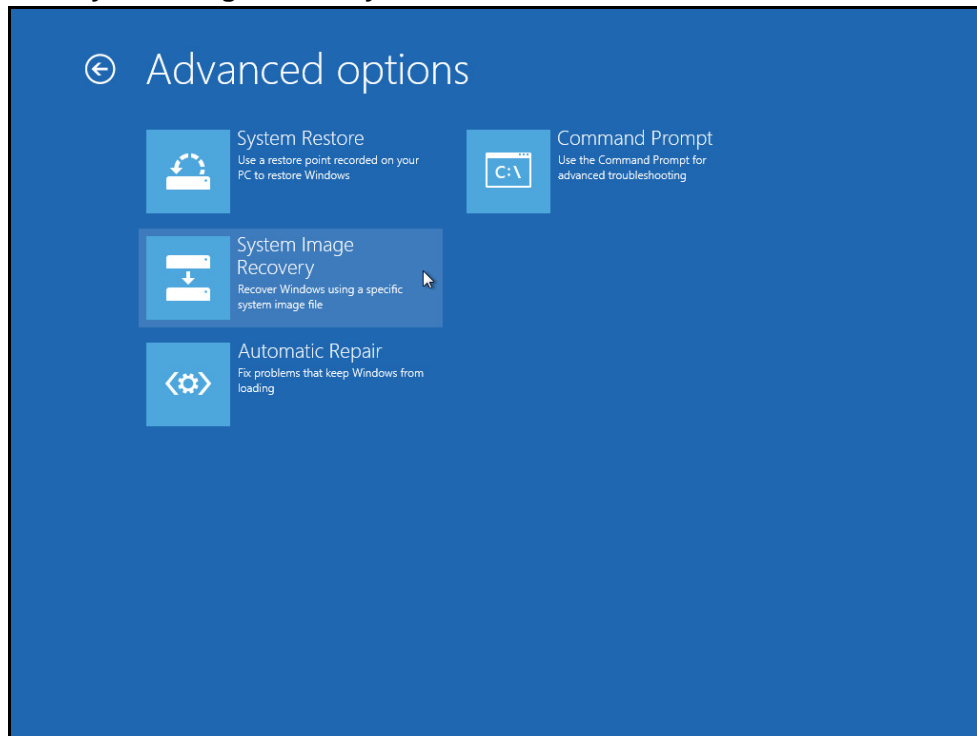
1. Click **Troubleshoot**.



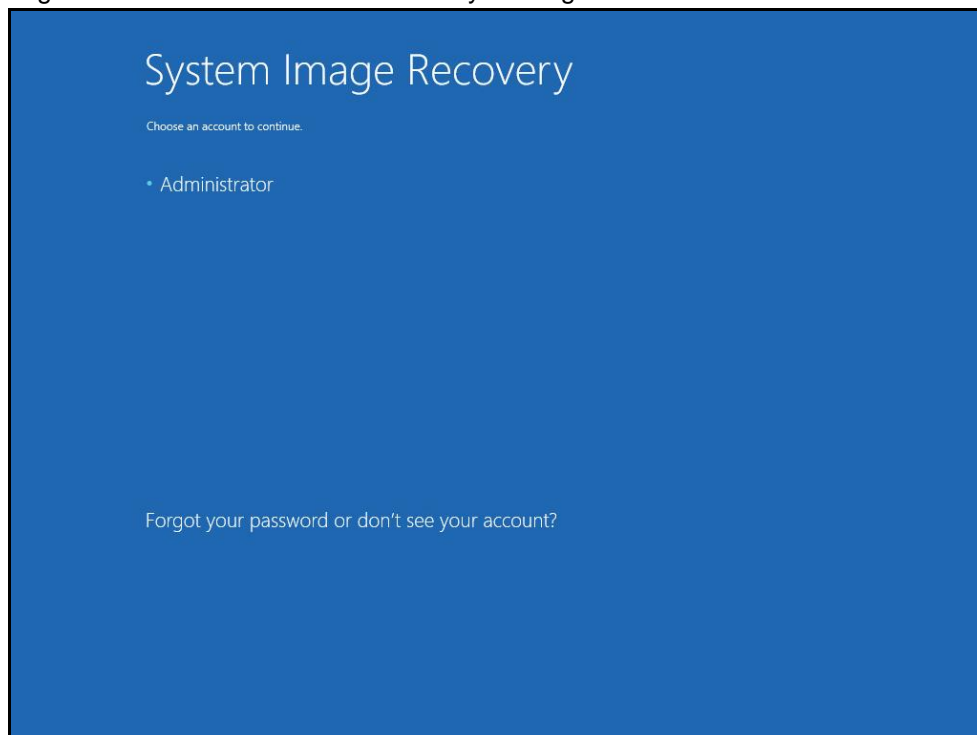
2. Click **Advanced options**.



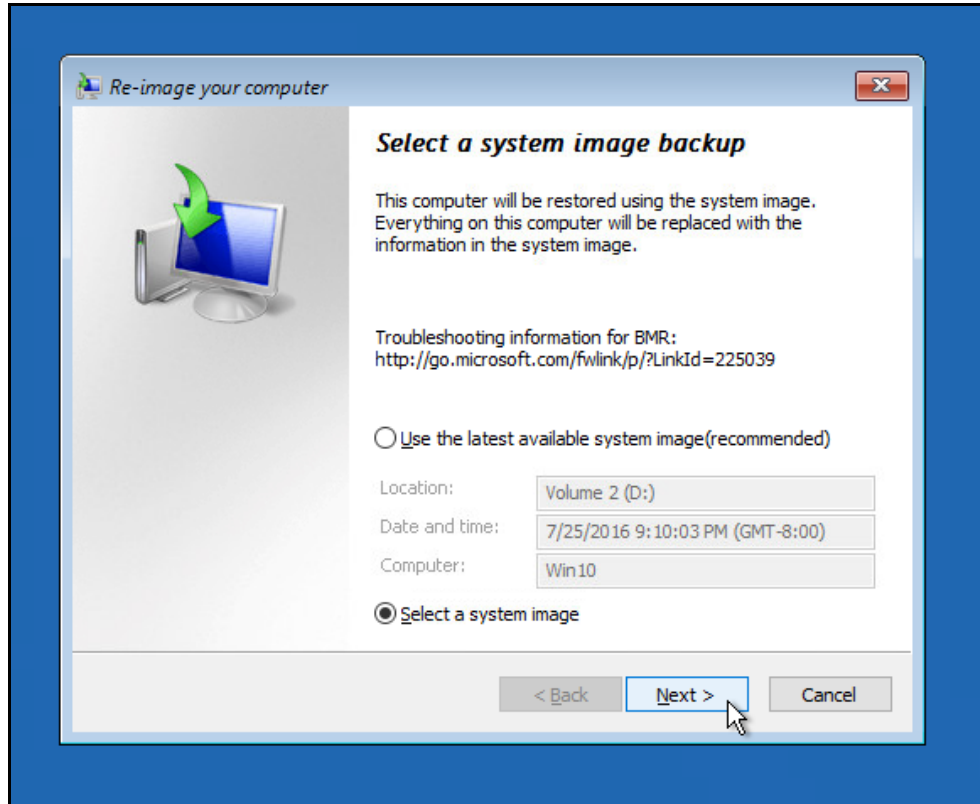
3. Click **System Image Recovery**.



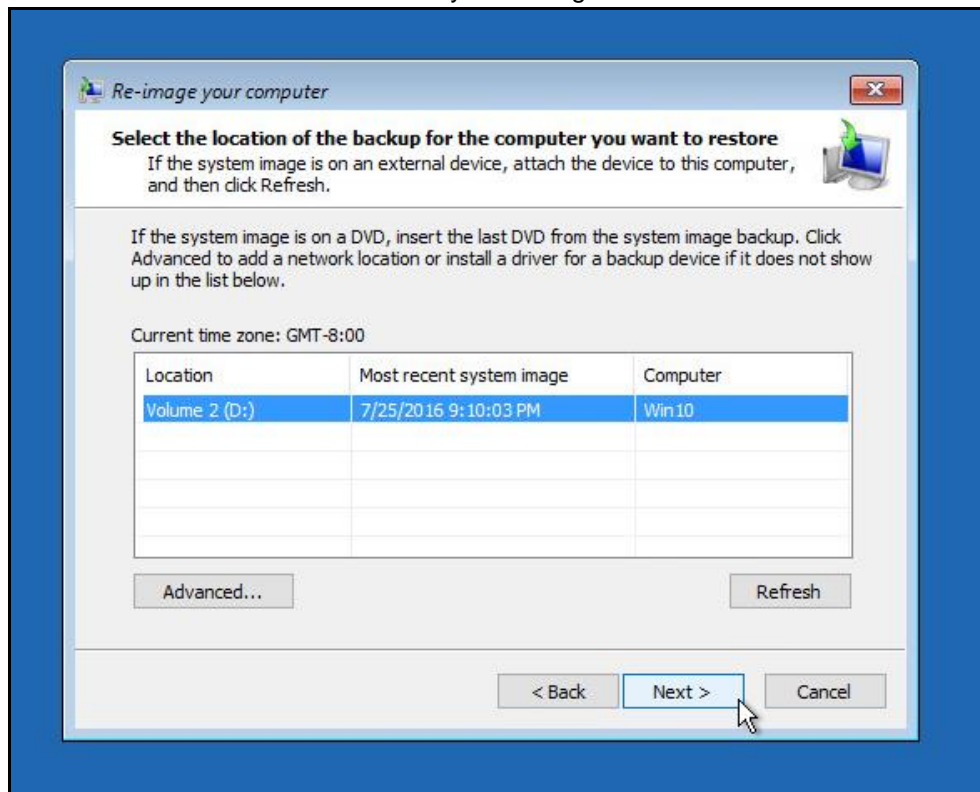
4. Log in with an administrative account by clicking on **Administrator**.



5. Click **Select a system image**, then click **Next**.



6. Select the location that contains the system image to restore from.



If you do not see the image available, then

- Click **Advanced**, and install the required driver for the removable drive to be accessed, if the system image was copied to a removable drive attached to the server.

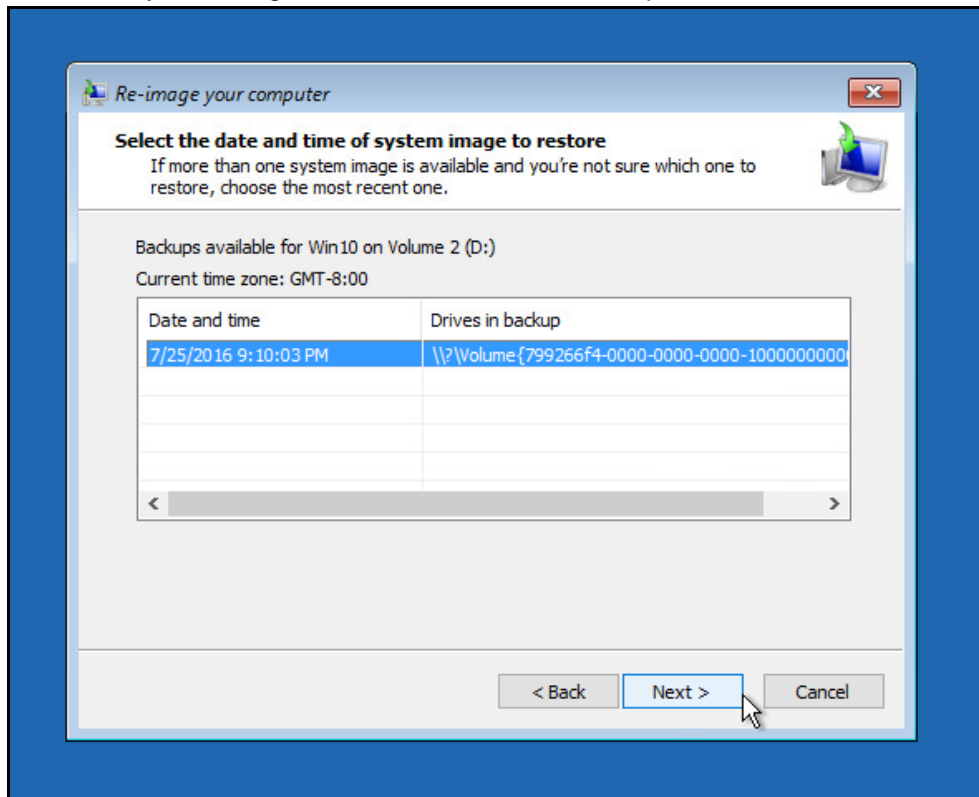
To install a driver, the driver must be located on the local system. You cannot install a driver from the network.

- Click **Advanced**, and browse to the remote shared folder which contains the system image, if the system image was copied to a network path.

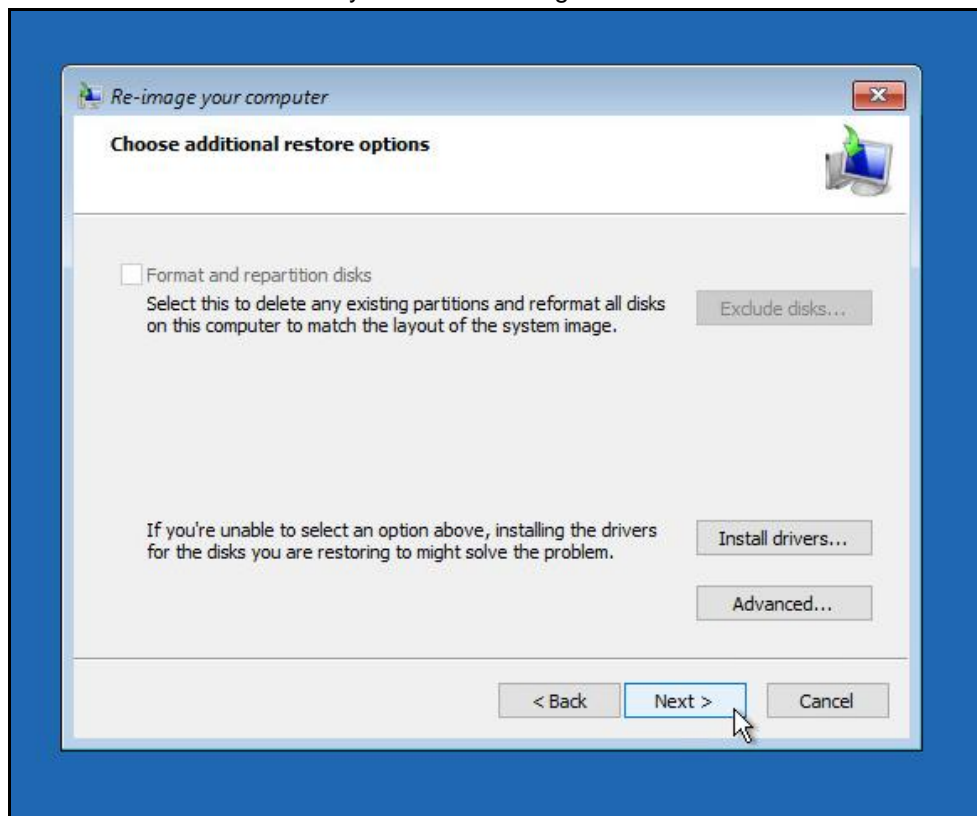
For domain environment, if the backup storage location is on a computer that is a member of that domain, then the computer containing the storage location should be on the IPsec boundary, to be accessible by non domain computer.

When a computer boots into Windows Recovery Environment, it becomes a non domain computer, therefore, cannot access the usual network shares. Only those computers that allow non domain computers to access the share can be used as a backup storage location in this way.

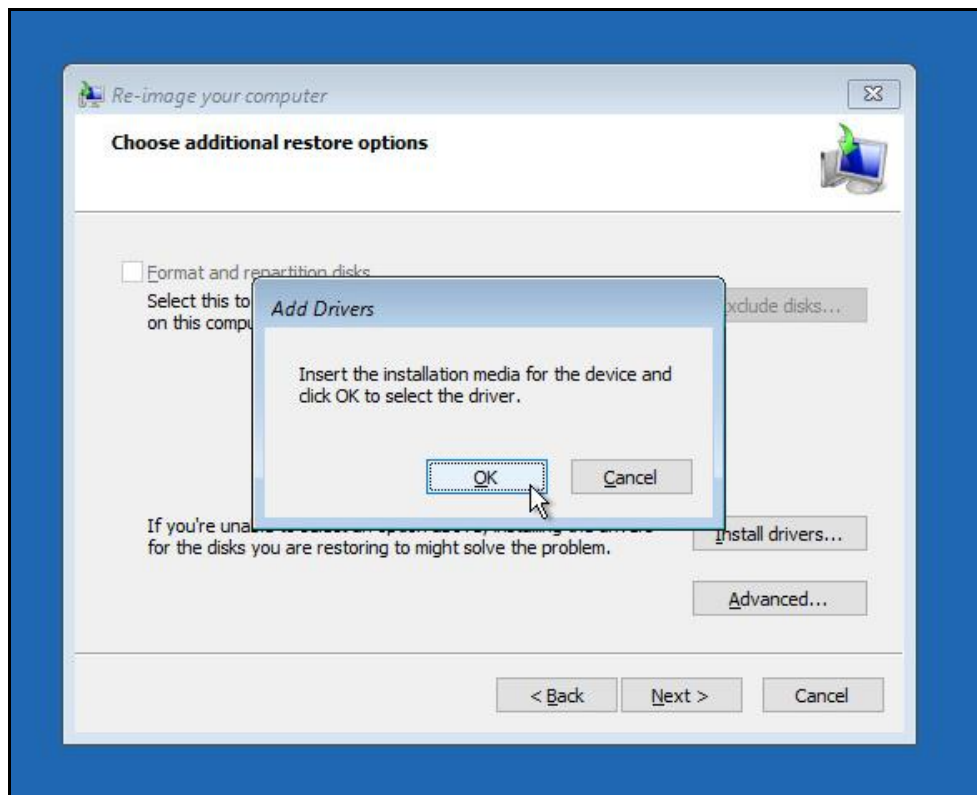
7. Select the system image to restore, then click **Next** to proceed.



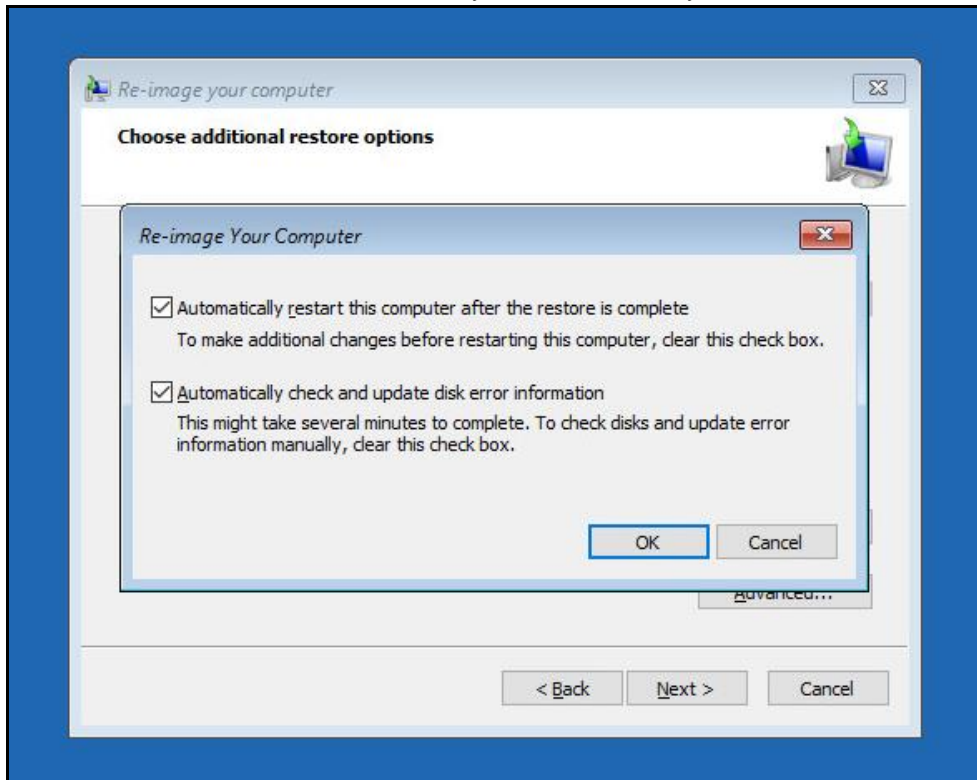
- On the **Choose additional restore options** page, click **Install drivers** to install device drivers for the hardware that you are recovering to.



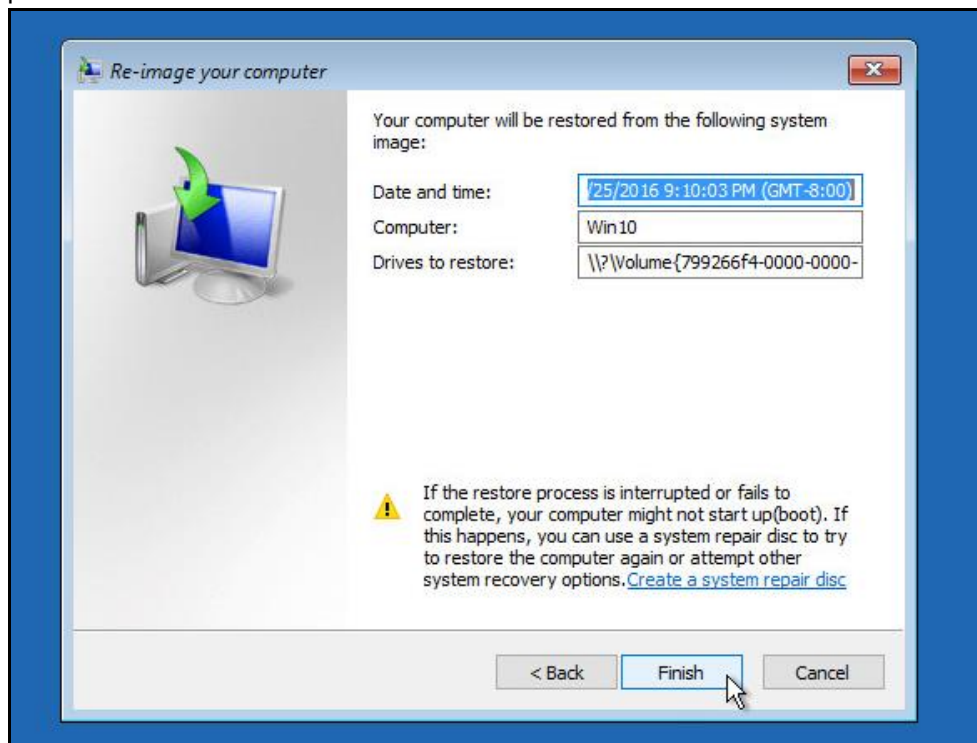
Click **OK** to add drivers.



Click **Advanced** to specify whether the computer is automatically restarted and the disks are checked for errors immediately after the recovery.



9. Confirm the details for the restoration, and then click **Finish** to start the recovery process.



Important: Do not interrupt the restore process.

The recovery will succeed as long as all the critical volumes (e.g. volumes containing operating system components) are recovered.

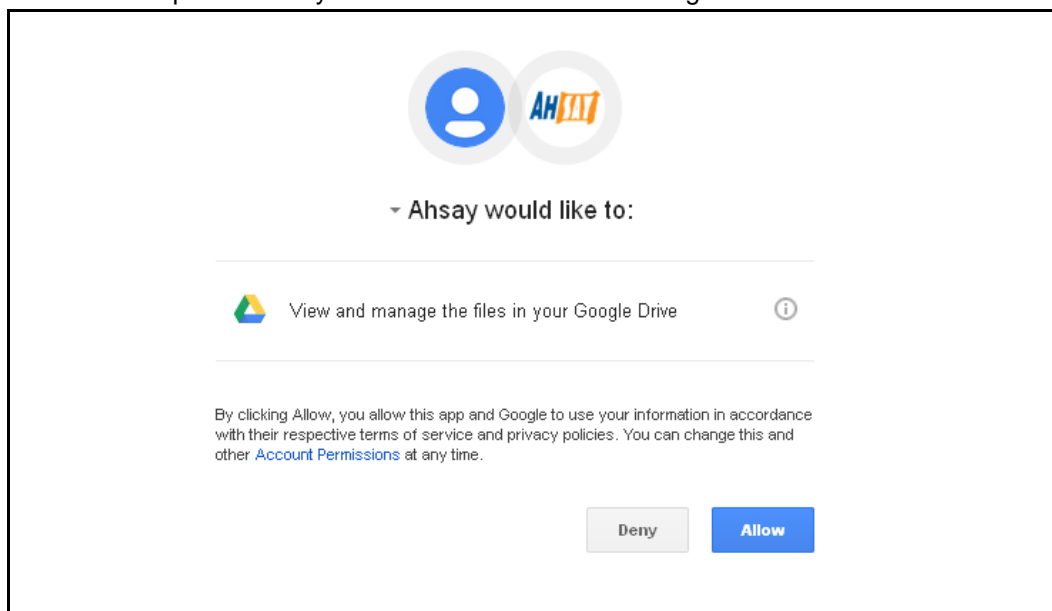
Appendix

Appendix A Cloud Storage as Backup Destination

For most cloud storage provider (e.g. Dropbox, Google Drive ... etc.), you need to allow access AhsayACB to access the cloud destination. Click OK / Test, you will be prompted to login to the corresponding cloud service.

Important: The authentication request will be opened in a new tab / window on the browser, ensure that the pop-up tab / window is not blocked (e.g. pop-up blocker in your browser).

Click Allow to permit AhsayACB to access the cloud storage:



Enter the authentication code returned in AhsayACB to complete the destination setup.

Note: A backup destination can be set to a supported cloud storage, backup server, FTP / SFTP server, network storage, or local / removable drive on your computer.

Multiple backup destinations can be configured for a single backup set. In fact it is recommended for you to setup at least 2 backup / destinations for your backup set.

For more details on backup destination, for example which cloud service providers are supported, destination type, or limitation, you can refer to the following KB article:

<https://forum.ahsay.com/viewtopic.php?f=169&t=14049>

Appendix B Uninstall AhsayACB

Refer to the Appendix of the AhsayACB Quick Start Guide for the corresponding operating system for details on how to uninstall AhsayACB:

https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_downloads_documentation_guides

Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the following website:

<https://www.ahsay.com/jsp/en/contact/kbQuestion.jsp>

Also use the Ahsay Knowledge Base for resource such as Hardware Compatibility List, Software Compatibility List, and other product information: <https://forum.ahsay.com>

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/jsp/en/contact/kbQuestion.jsp>

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