



DCS Online Backup Manager v8

Quick Start Guide for Windows

DCS Systems Corporation Limited

25 May 2021

Copyright Notice

© 2021 DCS 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 DCS 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, DCS Systems Corporation Limited does not warrant that this document is error free. If you find any errors in this document, please report to DCS Systems Corporation Limited in writing.

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

Trademarks

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

DCS 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 DCS Systems Corporation Limited without prior notice to you.

Revision History

| Date | Descriptions | Type of modification |
|-----------------|---|----------------------|
| 25 January 2021 | Updated Ch. 1.2 System Architecture; Added Ch. 1.3 Mobile Backup Server (MBS); Added Ch. 1.4 Two-Factor Authentication; Added Ch. 2.1 Requirements for DCS Mobile app; Updated Ch. 3.7 Firewall Settings; Added Ch. 3.8 Two-Factor Authentication Requirements; Added Ch. 3.9 Mobile Backup Requirements; Updated Ch 6.3 OBM Services; Added Ch. 6.4 Mobile Backup Server (MBS) Health Check and DCS Mobile app Connection Check; Added Ch. 7.1 Login to OBM without 2FA; Added Ch. 7.2 Login to OBM with 2FA using Android or iOS mobile device; Added Ch. 7.3 Login to OBM with 2FA using Twilio; Updated Ch. 8.1 Profile; Updated Ch. 8.1.5 Password; Updated Ch. 8.1.6 Authentication; Updated Ch. 8.1.7 Mobile Backup; Updated Ch. 8.1.8 Security Settings; Updated Ch. 8.3 Language; Added Ch. 13 Mobile Backup and Restore to OBM and Predefined Destinations; Added Appendix G: Example Registration of Time-base One-time Password (TOTP) Authenticator app in DCS Mobile app; | New / Modification |
| 29 January 2021 | Updated Ch. 7.2.1, 7.2.2, and 7.2.3 | Modifications |
| 25 March 2021 | Updated Ch. 7.2, 7.2.1 and 7.2.2 | Modifications |
| 7 April 2021 | Updated Ch. 10; Added sub-chapters for the detailed process diagrams in Ch. 10.1, 10.2, 10.2.1, 10.2.2 and 10.3 | New / Modifications |
| 30 April 2021 | Updated Ch. 8.6.3; Added new diagrams for the detailed process of Data Integrity Check (DIC) and updated screenshots for the Rebuild index option in Ch. 8.9.1; Updated description of Space Freeing Up in Ch. 8.9.2; Updated description of Delete Backup Data in Ch. 8.9.3; Added notes for Periodic Data Integrity Check (PDIC) in Ch. 10.1 | New / Modifications |
| 25 May 2021 | Added requirements in Ch. 3.10; Updated Ch. 6.1, 6.2.1 and Ch. 6.2.2; Updated screenshots of the Profile menu in Ch. 8.1.1 to 8.1.7; added | New / Modifications |

Mobile Backup in Ch. 8.8.3

Table of Contents

| | |
|--|----------|
| 1 Overview | 1 |
| 1.1 What is this software? | 1 |
| 1.2 System Architecture | 1 |
| 1.3 Mobile Backup Server | 1 |
| 1.4 Two-Factor Authentication | 3 |
| 2 Requirements for OBM on Windows | 4 |
| 2.1 Hardware Requirements | 4 |
| 2.2 Software Requirements | 4 |
| 2.3 Antivirus Exclusion Requirement | 4 |
| 2.4 Upgrade VMware Tools Requirement | 4 |
| 2.5 Temporary Directory Requirements | 5 |
| 2.6 Network Drive Requirements | 5 |
| 2.7 Firewall Settings | 5 |
| 2.8 Network Bandwidth | 5 |
| 2.9 Limitations | 5 |
| Enhanced Network Drive Support | 5 |
| 2.10 Best Practices and Recommendations | 5 |
| 3.12.1 Periodic Backup Schedule | 5 |
| 2.12.2 Set up of both Periodic and Continuous Backup Schedule | 6 |
| 2.12.3 Periodic Backup Schedule vs. Continuous Backup Schedule | 6 |
| 2.12.4 Temporary Directory Folder Location | 7 |
| 3 Get Started with OBM | 8 |
| 4 OpenDirect Restore | 9 |
| 4.1 What is OpenDirect Restore? | 9 |
| 4.2 Benefits of using OpenDirect Restore | 9 |
| 4.3 Requirements | 10 |
| 4.4.1 Supported Backup Modules | 10 |
| 4.4.2 License Requirements | 10 |
| 4.4.3 Backup Quota Storage | 10 |
| 4.4.4 Windows Operating System | 10 |
| 4.4.5 Available Spare Drive Letter | 10 |
| 4.4.6 Network Requirements | 11 |
| 4.4.7 Other Dependencies | 11 |
| 4.4.8 Permissions | 11 |

| | | |
|----------|--|-----------|
| 5 | Download and Install OBM | 12 |
| 6.1 | Download OBM | 13 |
| 6.2 | Install OBM | 14 |
| 6.2.1 | Online Installation using EXE online installer | 14 |
| 6.2.2 | Offline Installation using ZIP offline installer | 20 |
| 6.3 | OBM Services | 26 |
| 7 | Start OBM | 28 |
| 7.1 | Login to OBM without 2FA | 28 |
| 7.1.1 | Initial login to OBM with no 2FA and no Mobile Add-on Module | 28 |
| 8 | OBM Overview | 31 |
| 8.1 | Profile | 32 |
| 8.1.1 | General | 32 |
| 8.1.2 | Contacts | 34 |
| 8.1.3 | Time Zone | 36 |
| 8.1.4 | Encryption Recovery | 37 |
| 8.1.5 | Password | 37 |
| 8.1.6 | Authentication | 39 |
| 8.1.7 | Security Settings | 48 |
| 8.2 | Language | 49 |
| 8.3 | Information | 49 |
| 8.4 | Backup | 50 |
| 8.5 | Backup Sets | 50 |
| | Backup Set Settings | 50 |
| 8.6 | Report | 107 |
| 8.6.1 | Backup | 107 |
| 8.6.2 | Restore | 110 |
| 8.6.3 | Usage | 111 |
| 8.7 | Restore | 113 |
| 8.8 | Settings | 114 |
| 8.8.1 | Proxy | 114 |
| 8.8.2 | Windows Event Log | 116 |
| 8.9 | Utilities | 117 |
| 8.9.1 | Data Integrity Check | 117 |
| 8.9.2 | Space Freeing Up | 134 |
| 8.9.3 | Delete Backup Data | 137 |
| 8.9.4 | Decrypt Backup Data | 141 |
| 8.10 | Online Help | 145 |

| | |
|---|------------|
| 8.11 System Tray..... | 146 |
| 9 Create a Backup Set..... | 152 |
| 10 Overview on the Backup Process..... | 163 |
| 10.1 Periodic Data Integrity Check (PDIC) Process | 164 |
| 11 Run Backup Jobs | 165 |
| 11.1 Login to OBM..... | 165 |
| 11.2 Start a Manual Backup..... | 165 |
| 12 Restore Data | 169 |
| 12.1 Restore Method | 169 |
| 12.1.1 Traditional Restore | 169 |
| 12.1.2 OpenDirect Restore..... | 177 |
| 12.2 Restore Filter | 183 |
| 13 Contact DCS | 188 |
| 13.1 Technical Assistance | 188 |

1 Overview

1.1 What is this software?

DCS brings you specialized client backup software, namely OBM, to provide a comprehensive backup solution for protecting file(s) / folder(s) on your machine and extend protection to both Android and iOS mobile devices, with a wide variety of backup destinations (major cloud storage service providers, FTP/SFTP, local drive, etc.) of your choice.

1.2 System Architecture

Below is the system architecture diagram illustrating the major elements involved in the backup process among the backup machine OBM, DCS Mobile app and DCS CBS.

NOTE

The first mobile backup may take up a few hours to back up all the photos and videos from your device. Subsequent backups will take less time. Please do the following for the first mobile backup to prevent any interruption during backup process:

- For Android, disable screen lock or timeout
- For iOS, disable auto-lock
- Turn off all power saving modes
- Connect to power source

1.3 Mobile Backup Server

Starting with OBM v8.5.0.0, the Mobile Backup Server (MBS) will be utilized to handle mobile backup and restore of DCS Mobile app. It is an integral part of OBM.

System Diagram

The Mobile Backup Server (MBS) will be activated automatically when a mobile device installed with the DCS Mobile app is successfully registered for mobile backup with OBM. Afterwards, it will be automatically restarted whenever the OBM services is restarted or when the OBM machine is rebooted or powered on. The MBS will be deactivated when all mobile devices have deregistered from the mobile backup settings and the OBM services is restarted.

The MBS will use the following port ranges, **TCP Port:** 54000 to 54099, **UDP Port:** 54200 to 54299, **Protocol:** Http, for the request of DCS Mobile app.

The default TCP and UDP ports are **54000** and **54200**, if these ports are already in use by other applications or services, then the MBS will automatically acquire another port.

The actual TCP and UDP port can be seen on OBM when pairing a mobile device for mobile backup.

Photos and videos are stored either in mobile device's internal memory or SD Card. These are selected as backup source using the DCS Mobile app and will be backed up to the local destination of a DCS machine, that can be a Hard Drive, Flash Drive, and/or Network Drive in their ORIGINAL format unencrypted. For Android, photos and videos will retain all EXIF. While for iOS, photos and videos will retain most of the EXIF including, capture date, location, and lens.

If storage of photos and videos to a predefined destination is required, then this can be done using OBM to perform a secondary backup and restore of the photos and videos on the local drive to the predefined destination.

To backup and restore photos and/or videos from the DCS Mobile app to OBM then DCS CBS and/or Predefined Destination is a two-step process.

1st: Backup of photos and/or videos from DCS Mobile app to OBM local destination.

2nd: Create a File backup set using OBM, using the local backup destination as the backup source, and then backup this backup set to DCS CBS and/or Predefined Destination.

1.4 Two-Factor Authentication

New two-factor authentication implemented on OBM v8.5.0.0 onwards, to include support for TOTP (Time-based One-time Password) and Push notification authentication using the DCS Mobile app to provide additional security for the user login process. Since aside from logging in with just a username and password, if two-factor authentication is enabled for the account, there will be an added step that is needed to be able to login.

Upon initial login to OBM, you will have an option to setup two-factor authentication or skip the setup and do it later. If you continue the setup of two-factor authentication, it will be automatically enabled for your account. Several mobile devices may be added for authentication.

For logins with two-factor authentication enabled, you will be asked to select the method that you would like to use. This depends on the authenticator app used, you will either accept the login request in the DCS Mobile app or enter a one-time password generated in the third-party TOTP authenticator app such as Google Authenticator, Microsoft Authenticator, LastPass etc.

This illustrates the registration of mobile devices for Two-Factor Authentication.

- must be 12.0.0 or above.

2 Requirements for OBM on Windows

2.1 Hardware Requirements

Refer to the link below for details of the minimum and recommended requirements for installing OBM:

[FAQ: DCS Hardware Requirement List \(HRL\) for version 8.1 or above](#)

2.2 Software Requirements

Refer to the following article for the list of compatible operating systems and Hyper-V platforms:

[FAQ: DCS Software Compatibility List \(SCL\) for version 8.1 or above](#)

Refer to the following article for the list of compatible operating system for OpenDirect and Granular Restore:

[FAQ: DCS Software Compatibility List \(SCL\) for Granular and OpenDirect Restore](#)

2.3 Antivirus Exclusion Requirement

To optimize performance of OBM on Windows, and to avoid conflict with your antivirus software, refer to the following wiki article the list of processes and directory paths that should be added to all antivirus software white-list / exclusion list: https://wiki.DCS.com/doku.php?id=public:8014_suggestion_on_antivirus_exclusions

NOTE

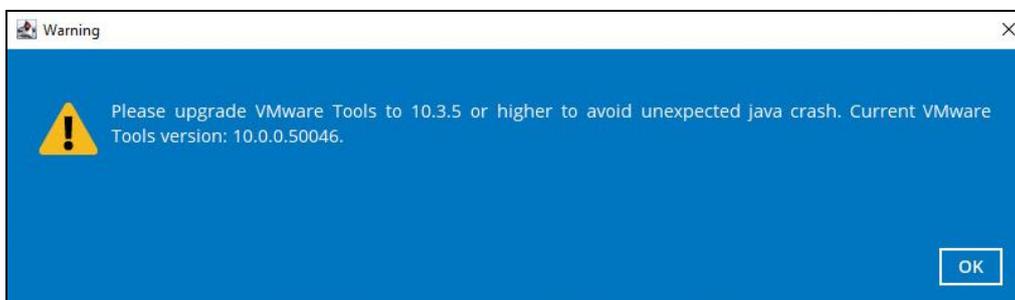
The bJW.exe process is automatically added to Windows Defender exclusion list for Windows 10 and 2016 / 2019, during installation / upgrade via installer or upgrade via AUA.

For mobile backups, the mobile backup destination must also be added to all antivirus software white-list / exclusion list.

2.4 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 the upgrade of VMware Tools, refer to this article https://wiki.DCS.com/doku.php?id=public:5288_DCS_obc_crash_on_vm_with_vmware_tools_pre-10.0.5.

2.5 Temporary Directory Requirements

The temporary directory is used for various purposes, such as storage of temporary spooled file (for database specific backup type in OBM), remote file list, local file list, temporary delta file and other files of temporary nature.

It is strongly recommended to use a local drive instead of a network drive to ensure optimal backup/restore performance.

2.6 Network Drive Requirements

The login accounts for network drives must have read and write access permission to ensure that backup and restore would be successful.

2.7 Firewall Settings

Make sure that your firewall settings allows network traffic through the following domain and/or ports:

- For OBM to function correctly must allow outbound connections to *.DCS .com via port 80 and 443.
- For mobile backup inbound / outbound network traffic must be allowed through the following default ports: HTTP port: 54000 and UDP port: 54200.

2.8 Network Bandwidth

10 Mbps or above connection speed.

2.9 Limitations

Enhanced Network Drive Support

- For network drives which have not been already setup or mapped in Windows.
- Temporary folder location is not supported with individual login credentials but can still be setup separately using existing Windows User Authentication login.
- It also does not support Pre-Backup and Post-Backup Commands.
- Not supported on “Restore Raw file” and “Restore to local computer” options.
- Not supported for mobile backup destinations.

2.10 Best Practices and Recommendations

3.12.1 Periodic Backup Schedule

The periodic backup schedule should be reviewed regularly to ensure the interval is sufficient to handle the data volume on the machine. Over time, data usage pattern may change on a production server, i.e., the number of new files created, the number of files which are updated/delete, new users may be added etc.

When using periodic backup schedules with small backup intervals such as backup every 1 minute, 2 minutes, 3 minutes etc. although the increased backup frequently

does ensure that changes to files are captured regularly which allows greater flexibility in recovery to a point in time.

Consider the following key points to efficiently handle backup sets with periodic backup schedule.

- Hardware – to achieve optimal performance, compatible hardware requirements is a must. Ensure you have the backup machine’s appropriate hardware specifications to accommodate frequency of backups,
 - so that the data is always backed up within the periodic backup interval
 - so that the backup frequency does not affect the performance of the production server
- Storage – ensure you have enough storage quota allocated based on the amount of new data and changed data you will backup.

Retention Policy – also make sure to consider the retention policy settings and retention area storage management which can grow because of the changes in the backup data for each backup job.

2.12.2 Set up of both Periodic and Continuous Backup Schedule

On a Windows platform, although it is possible to setup both Periodic backup schedule and Continuous backup schedules on a File backup sets, it is recommended to only use one schedule as only one schedule backup job can run at any one time.

For example, a backup job is started by the Periodic backup schedule and is running, if a Continuous backup is scheduled to run, the backup job will be skipped and vice versa.

2.12.3 Periodic Backup Schedule vs. Continuous Backup Schedule

The following table shows the comparison between a periodic and continuous backup schedule.

| Features | Periodic Backup Schedule | Continuous Backup Schedule |
|--|--------------------------|--|
| Will run whether or not a change on the backup source is made | ✓ | ✗ |
| Run Retention Policy after backup | ✓ | ✗ |
| Exclude system files from the backup | ✗ | ✓ |
| Only apply to files smaller than (MB) size | ✗ | ✓ |
| Exclude Filter | ✗ | ✓ |
| Supported on all operating systems (i.e. Windows, MacOS, Linux, FreeBSD, QNAP, and Synology) | ✓ | Only supported on Windows operating system |
| Supports all backup set types | ✓ | Only supports File Backup Sets |

2.12.4 Temporary Directory Folder Location

Temporary directory folder is used by OBM for storing backup set index files and any incremental or differential backup files generated during a backup job.

To ensure optimal backup/restoration performance, it is recommended that the temporary directory folder is set to a local drive with sufficient free disk space.

3 Get Started with OBM

This quick start guide will walk you through the following 6 major parts to get you started with using OBM.

Download and Install

Download and install OBM on your Windows machine

Launch the App

Launch and log in to OBM

Setup 2FA and/or Mobile Backup

Register mobile device for 2FA and/or mobile backup (optional)

Create a Backup Set

Create a backup set according to your preference

Run Backup Jobs

Run the backup job to backup data

Restore Data

Restore backed up data to your system

4 OpenDirect Restore

4.1 What is OpenDirect Restore?

OpenDirect restore is an additional restore options for restoring files from a Windows File backup set. The OpenDirect restore method makes use of the granular restore technology to make selective restore of individual files from a large compressed or image file, for example zip, RAR, ISO files, without the need to restore the compressed or image file first, to give you a fast and convenient file restore solution.

During the OpenDirect restore process, the files/folder can be viewed and/or copied from the Windows File Explorer on the Windows machine you are performing the restore. OpenDirect restore is only supported on File backup sets created and backed up using OBM on Windows platform with OpenDirect restore feature enabled.

IMPORTANT

OpenDirect restore requires an additional OpenDirect / Granular Restore add-on module license to work. Contact your backup service provider for further details.

4.2 Benefits of using OpenDirect Restore

Comparison between OpenDirect File Restore and Traditional File Restore

| OpenDirect Restore | |
|--|--|
| Introduction | |
| OpenDirect restore allows you to quickly access individual files from a large compressed or image file by viewing and/or copying files from the file explorer on the Windows you are performing the restore, without having to fully restore the whole compressed or image file first. | |
| Pros | |
| Restore of Entire Compressed File Not Required | As opposed to the traditional restore where you have to restore the entire compressed or image file first before you can access any individual file in it, 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. |
| Ability to Restore Selected Files | When restoring a large compressed or image file, sometimes, you may only need to restore individual file(s) out of the entire file, therefore, OpenDirect restore gives you the flexibility to restore selective file(s) quickly, so it saves you time and effort to achieve your restore goal. |
| Cons | |

| | |
|--------------------------------------|---|
| No Encryption and Compression | 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. |
|--------------------------------------|---|

| Traditional Restore | |
|---|--|
| Introduction | |
| The traditional restore method restores the entire compressed file or image file. Backed up data can only be accessed when complete restore is performed. | |
| Pros | |
| Backup with Compression and Encryption | Backup file(s) are compressed, therefore in smaller file size, and encrypted before being uploaded to the backup destination. |
| Cons | |
| Slower Recovery | As the entire compressed or image file must be restored before you can access any individual files, restore time could be long if the file size is large |

4.3 Requirements

4.4.1 Supported Backup Modules

OpenDirect restore is only supported on File backup sets created and backed up using OBM on Windows platform with OpenDirect restore feature enabled

4.4.2 License Requirements

An OpenDirect / Granular restore add-on module license is required per backup set for this feature to work. Contact your backup service provider for more details

4.4.3 Backup Quota Storage

As compression is not enabled for OpenDirect file backup sets, to optimize restore performance the storage quota required will be higher than non-OpenDirect file backup sets. Contact your backup service provider for details

4.4.4 Windows Operating System

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

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

4.4.5 Available Spare Drive Letter

One spare drive letter must be available on the Windows machine for the OpenDirect restore process, as the compressed file or image is mounted on Windows as a logical drive. OBM will automatically take the next available drive letter in alphabetical order for the compressed or image file.

NOTES

1. The Windows drive letters A, B, and C are not used by OpenDirect restore.
2. The OpenDirect restore assigned drive letter(s) will be released once you exit from OBM UI.

4.4.6 Network Requirements

Recommended minimum network speed is **at least 100Mbps download speed**.

The network bandwidth requirements will increase in proportion to the size of the 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

4.4.7 Other Dependencies

The following dependencies are restore-related. Therefore, they will be checked by OBM only when an OpenDirect restore is performed. 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-us/download/details.aspx?id=48145>
- Update for Universal C Runtime in Windows
<https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows>
- **For Windows 7 and Windows Server 2008 R2 only**
Microsoft Security Advisory 3033929
<https://technet.microsoft.com/en-us/library/security/3033929.aspx>

4.4.8 Permissions

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

5 Download and Install OBM

There are two installation modes of OBM, online installation and offline installation. Below is the table of comparison between online installation and offline installation.

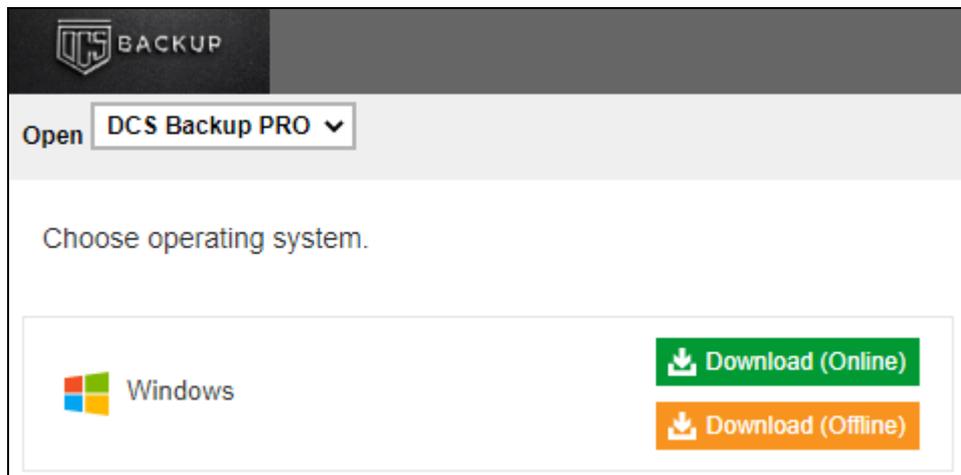
| | Online Installation | Offline Installation |
|--------------------------|--|--|
| Installation Time | <ul style="list-style-type: none"> ➤ Takes more time as it needs to download the binary and component files (80MB to 132MB depending on operating system) each time the installation is run. ➤ Online installer size is 6KB to 3.5MB depending on operating system as it contains only the initial installation package files. | <ul style="list-style-type: none"> ➤ 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 reused many times. ➤ Offline installer size is 50MB to 195MB depending on operating system as it contains all the necessary binary and component files. |
| Deployments | <ul style="list-style-type: none"> ➤ Suitable for single or small amount of device installations. ➤ 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. | <ul style="list-style-type: none"> ➤ Suitable for multiple or mass device installations. ➤ 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 need to update the product version after installation if an older offline installer is used. |

6.1 Download OBM

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



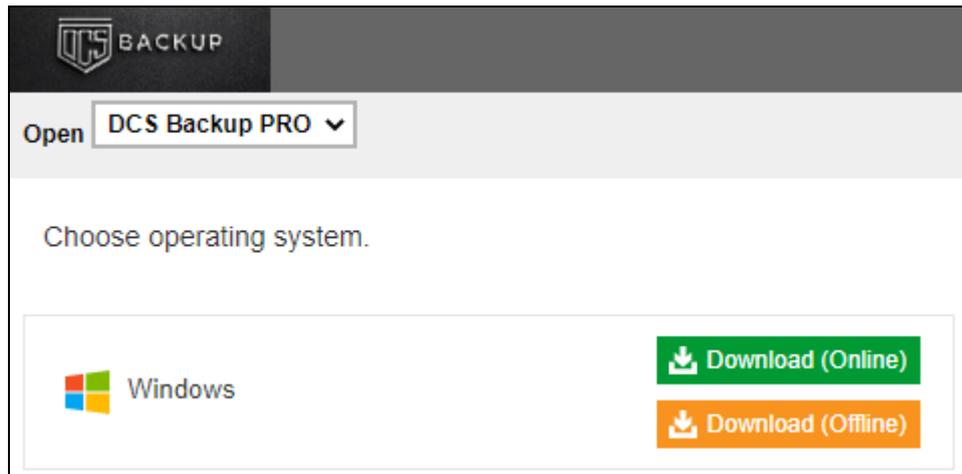
2. In the **Windows** section under the **OBM** tab of the download page, you can choose between two installation methods:
 - Online installation using EXE online installer
 - Offline installation using ZIP offline installer



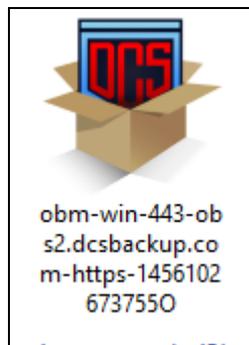
6.2 Install OBM

6.2.1 Online Installation using EXE online installer

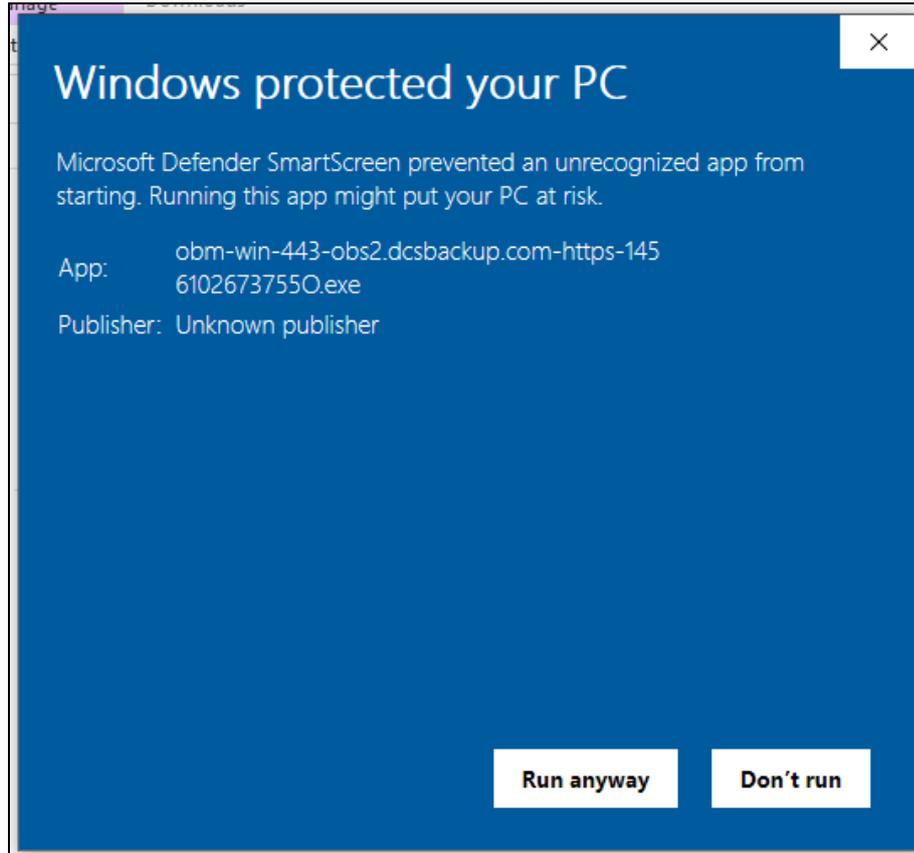
1. Go to the download page of your backup service provider's website and download the OBM EXE online installer.



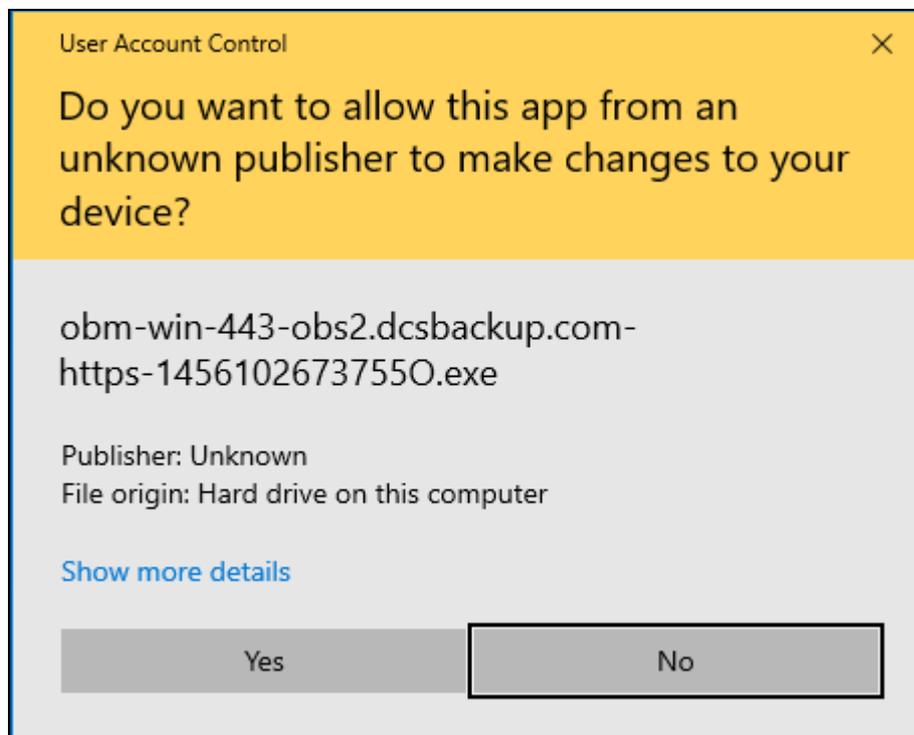
2. Double-click the icon of the OBM installation package .exe file you have downloaded.



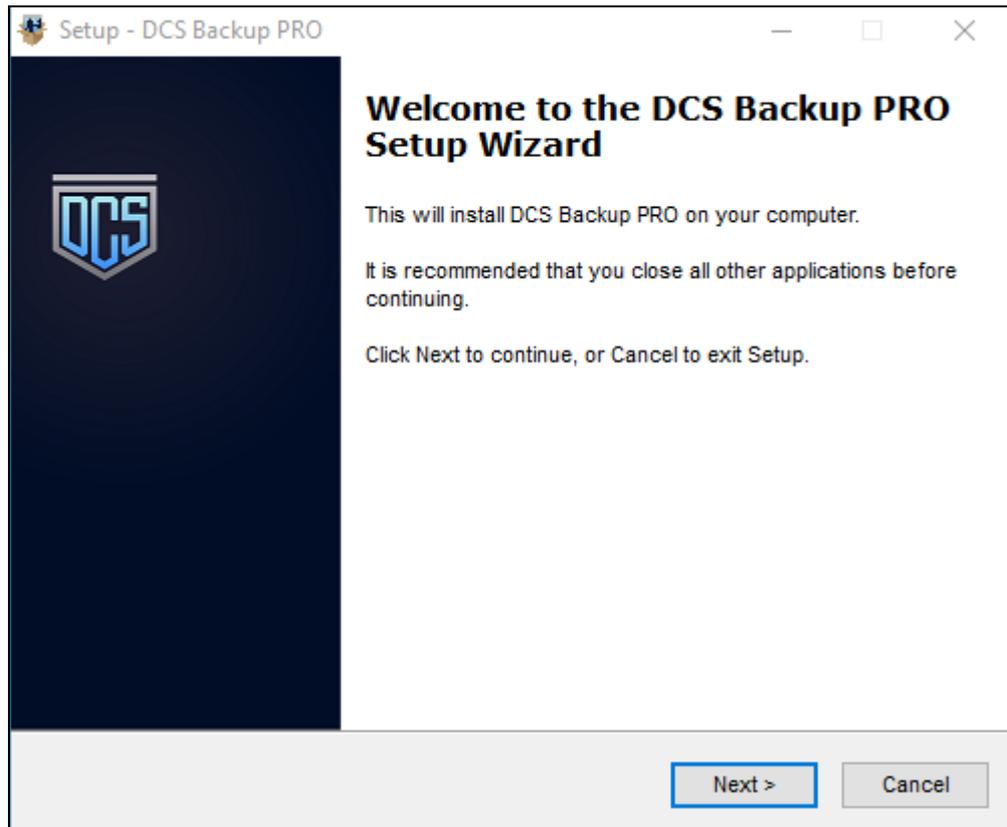
3. Click **Run Anyway** when you see this message.



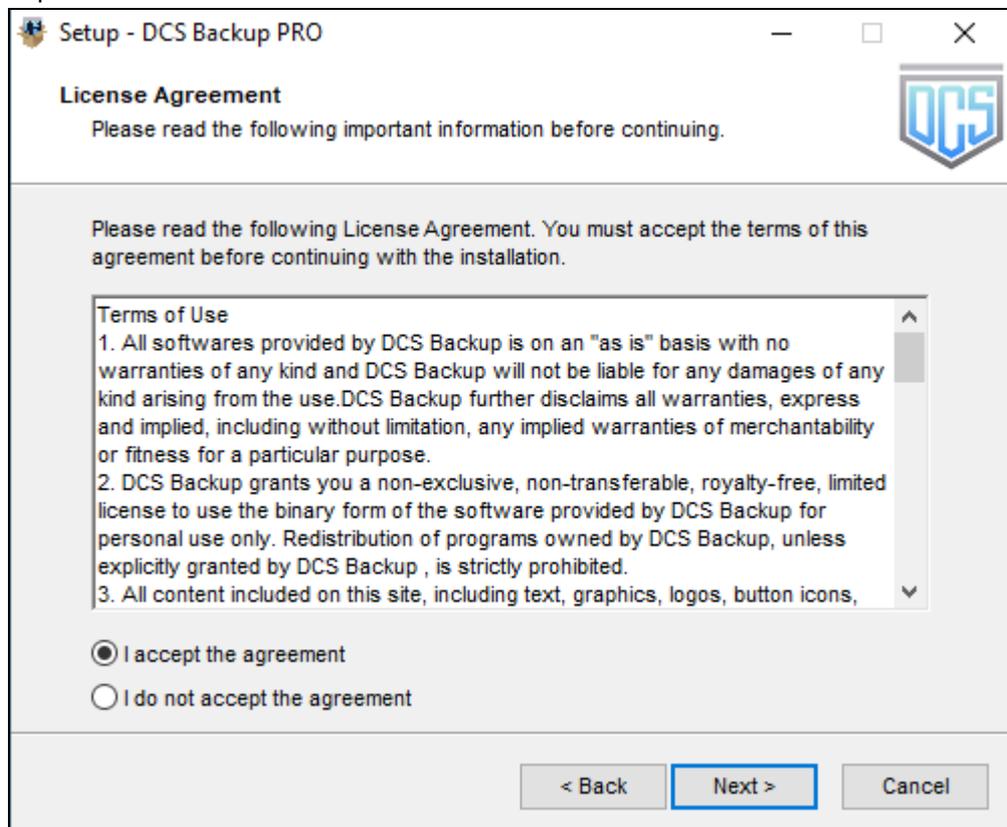
4. The following dialog box will appear only if User Account Control is enabled. Click **Continue** to start the installation.



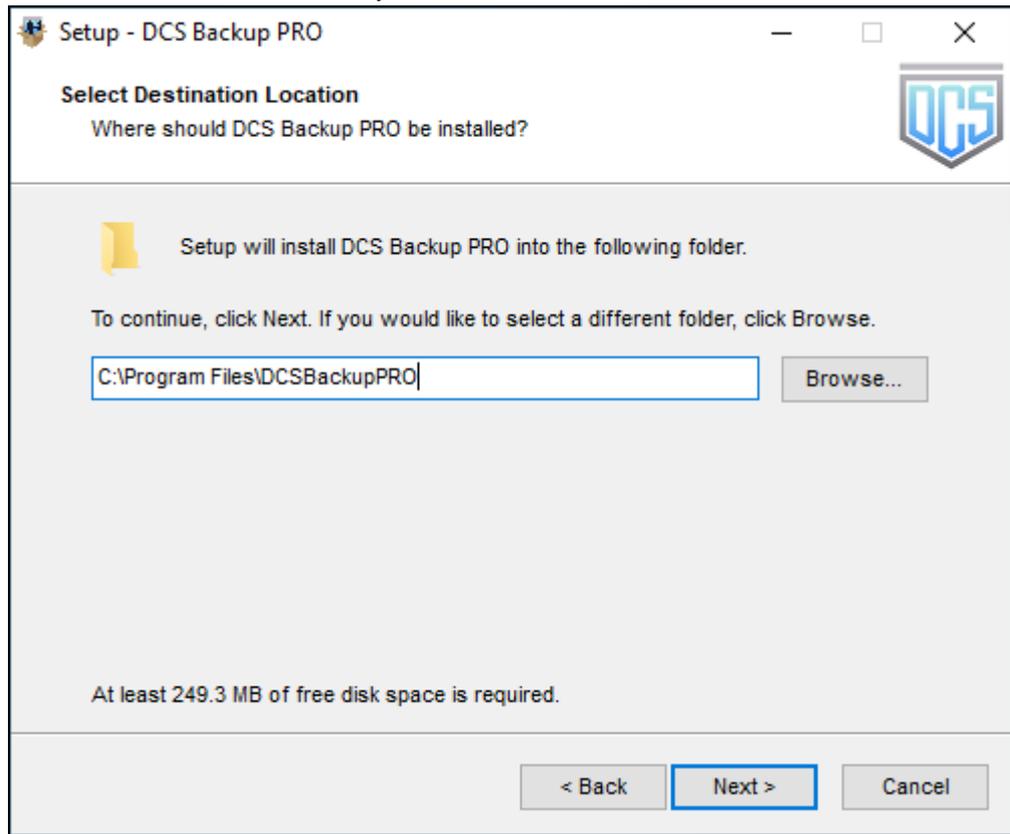
5. Click **Next** to continue.



6. Select **I accept the agreement** after reading the license agreement, then click **Next** to proceed.



7. Choose the installation directory. Then, click **Next** to continue.

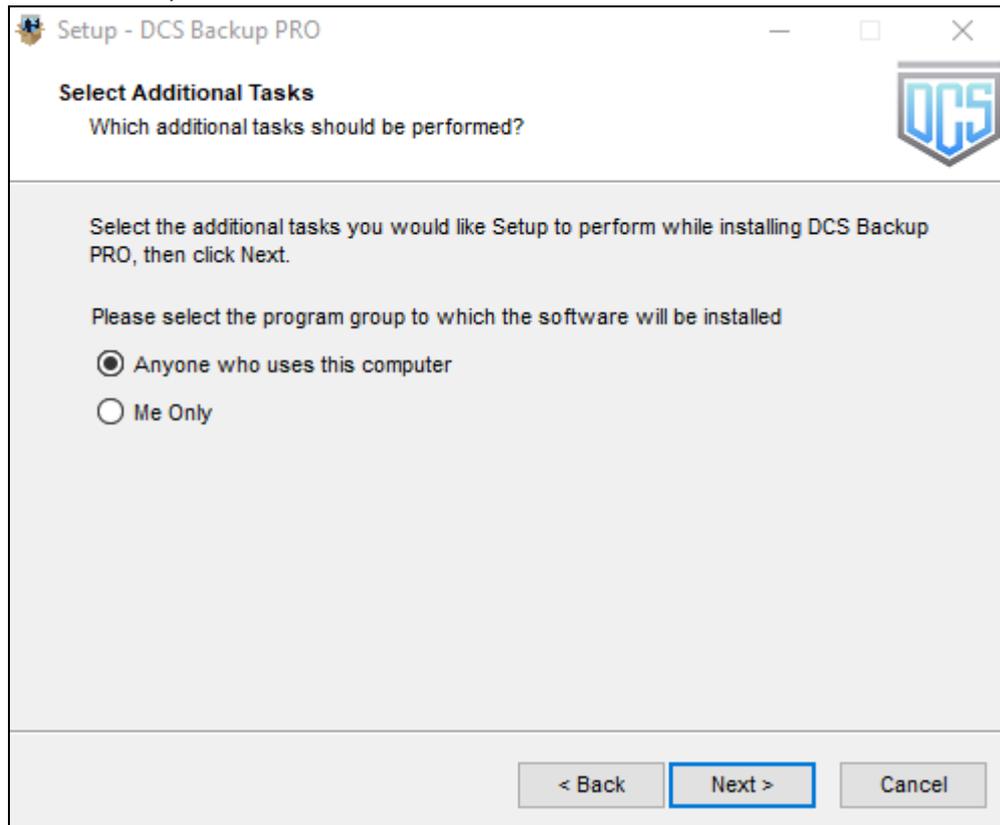


8. Select the program group to which the software will be installed. The default setting is “Anyone who uses this computer”. The following are the difference between the two settings:
- Anyone who uses this computer – the OBM System Tray icon will be available to all Windows users and backup notifications will be displayed on the Windows System Tray. For more information, please refer to [Chapter 8.11 System Tray](#).
 - Me Only – the OBM System Tray icon will not be available and backup notifications will not be displayed on the Windows System Tray.

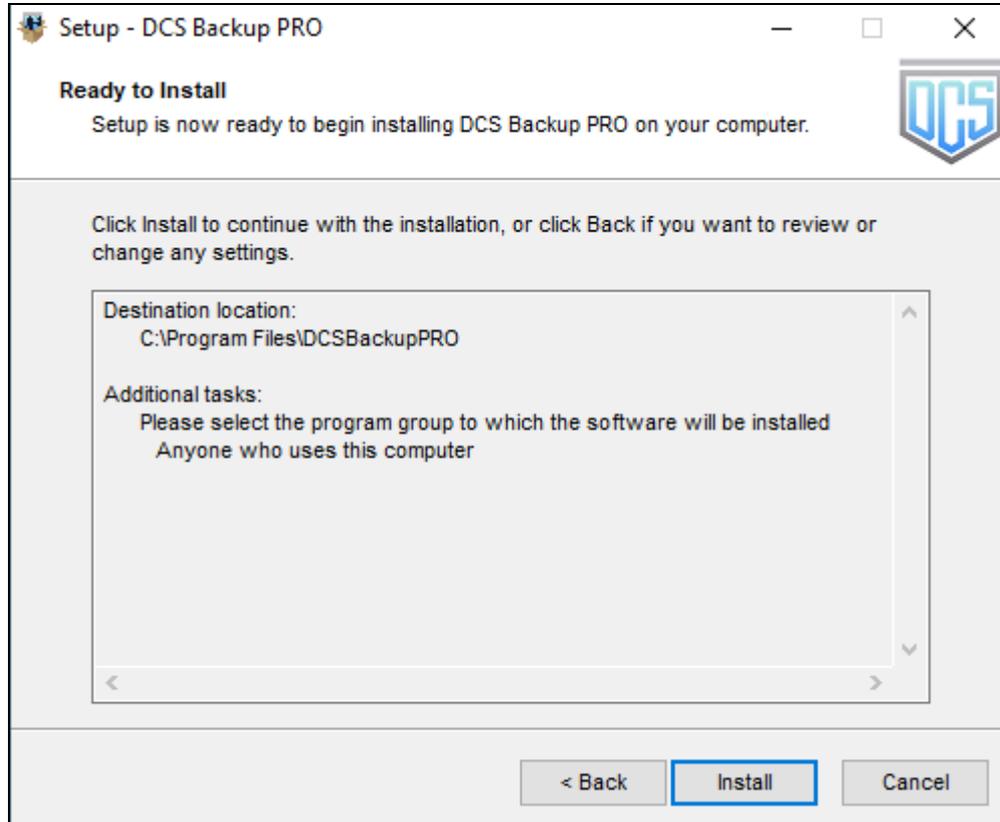
NOTE

Once the program group setting has been chosen and the installation completed; if you need to change the setting, this will require an uninstallation and re-installation of the application.

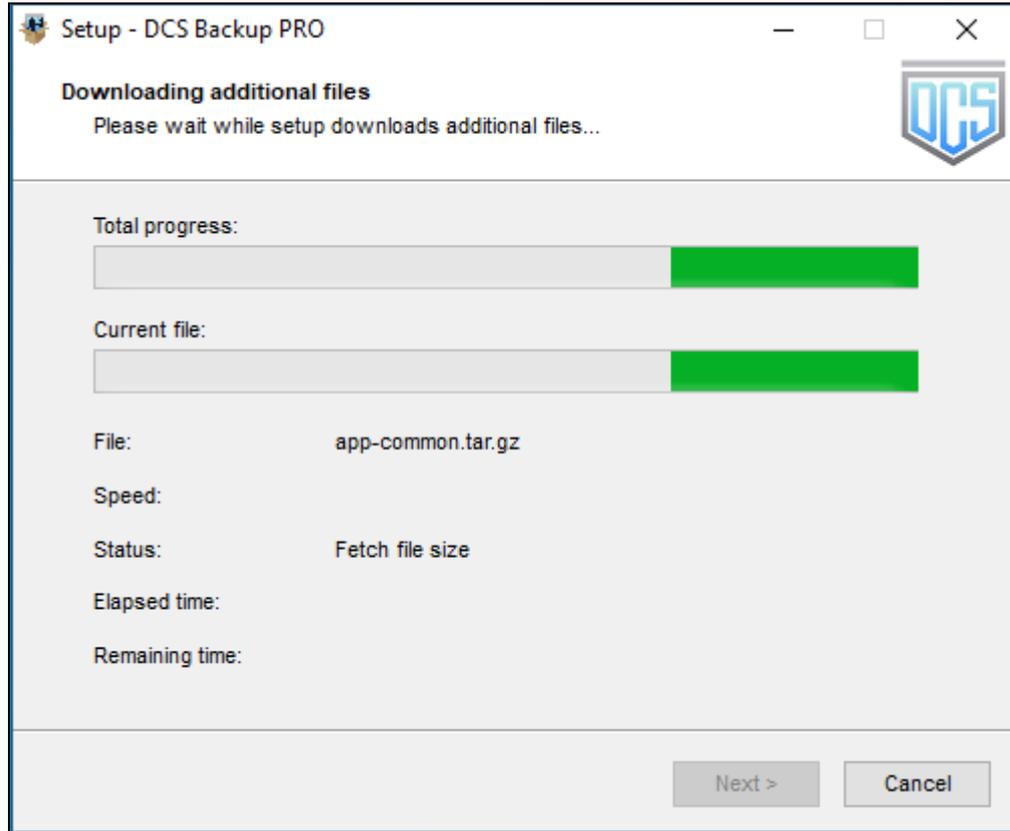
Click **Next** to proceed.



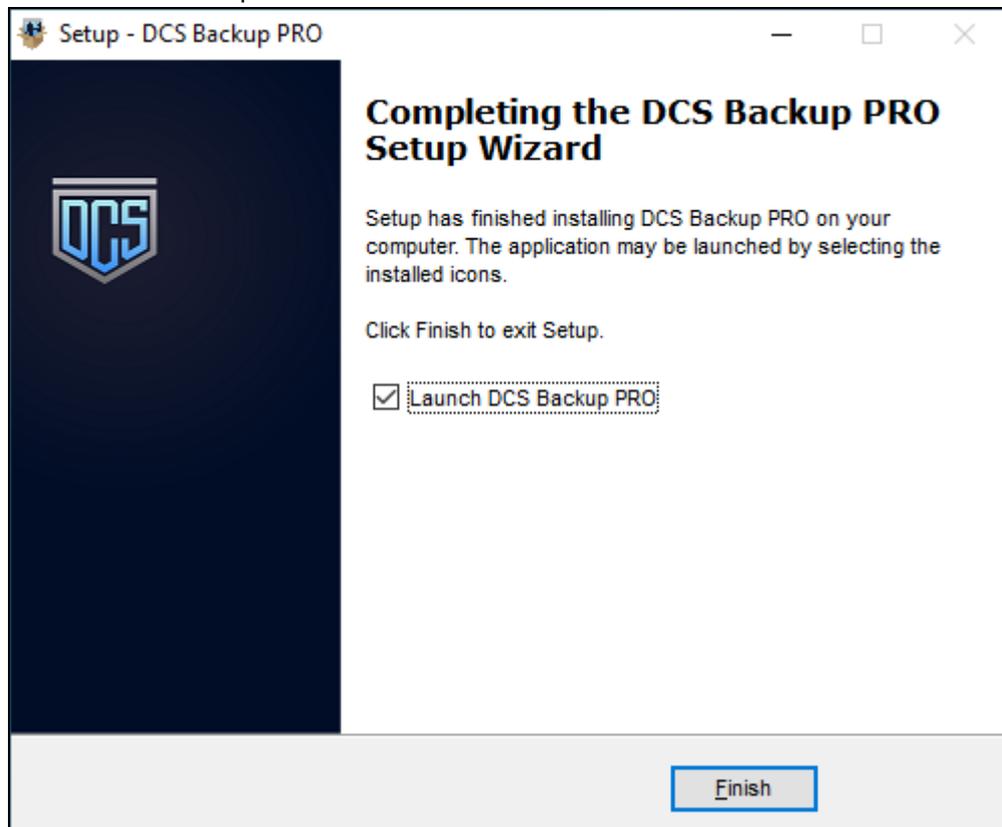
8. The installation will start after you click **Install**.



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

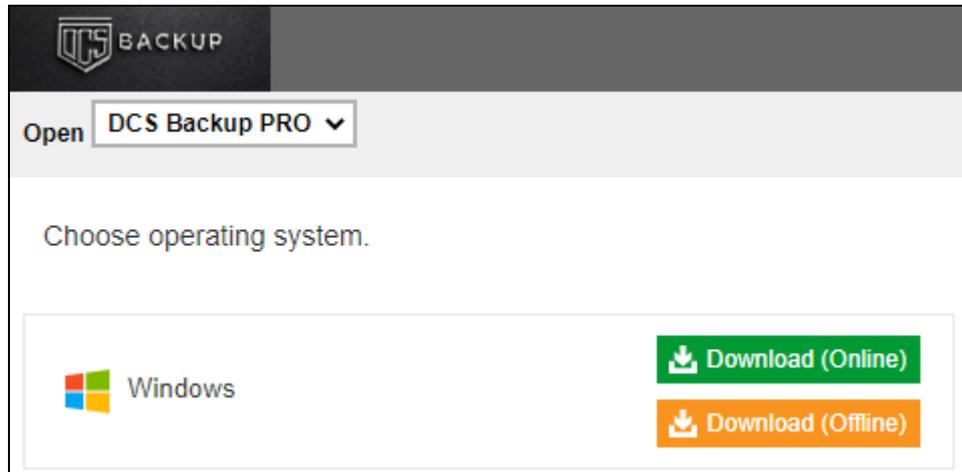


10. Click **Finish** to complete the installation.

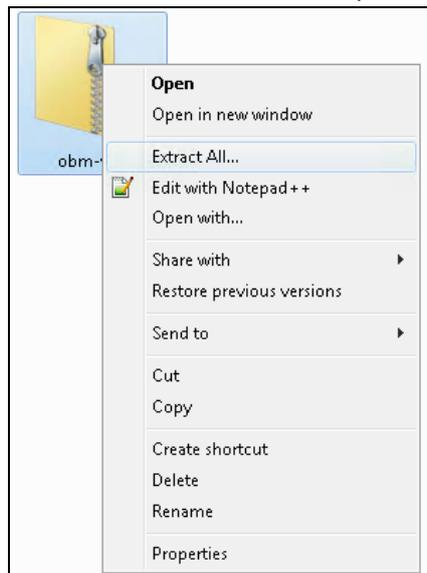


6.2.2 Offline Installation using ZIP offline installer

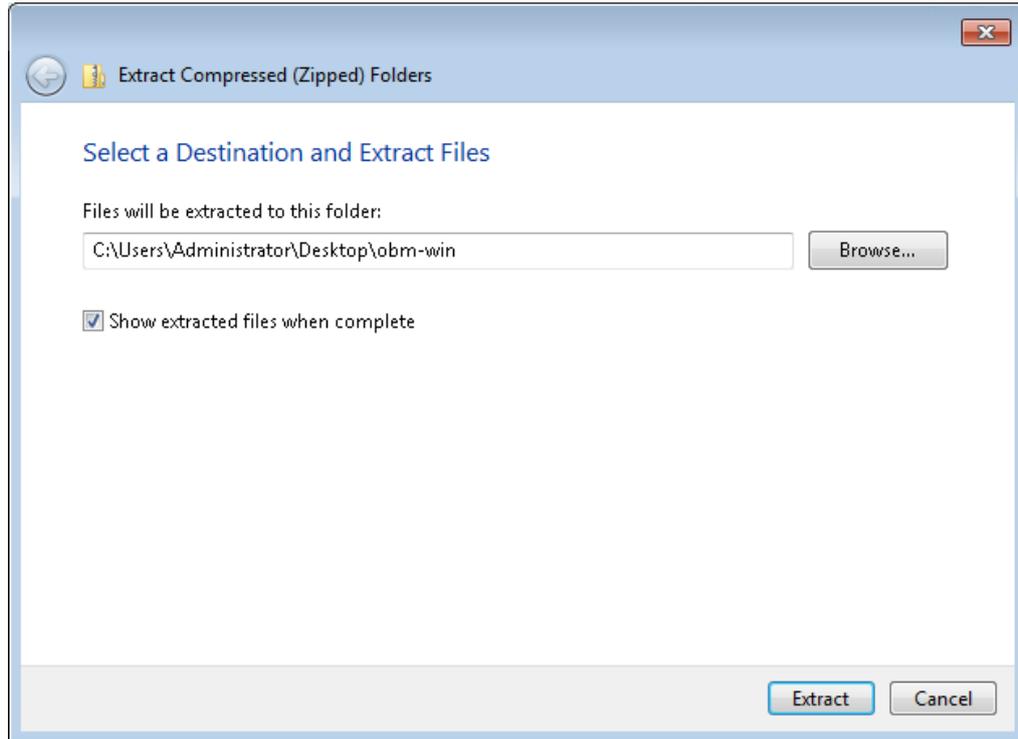
1. Go to the download page of your backup service provider's website and download the OBM ZIP offline installer.



2. Extract the offline installation package file (**obm-win.zip**) you have downloaded.



3. Select a destination and extract files.



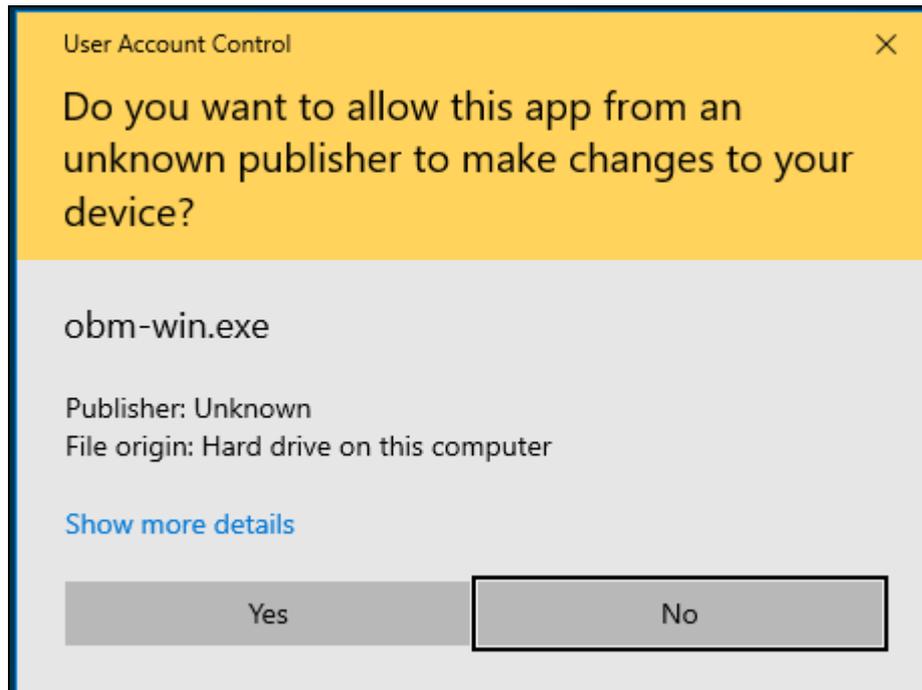
4. Launch the installer named **obm-win** you have extracted from the zip format file.



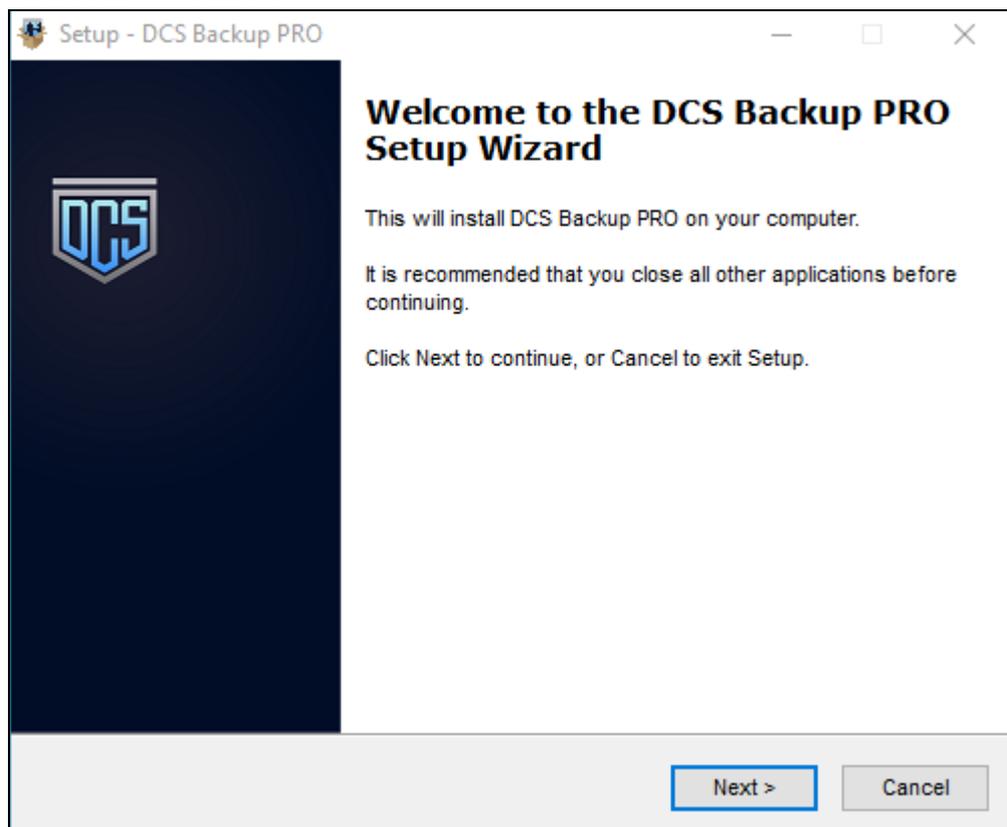
5. Click **Run** when you see this message.



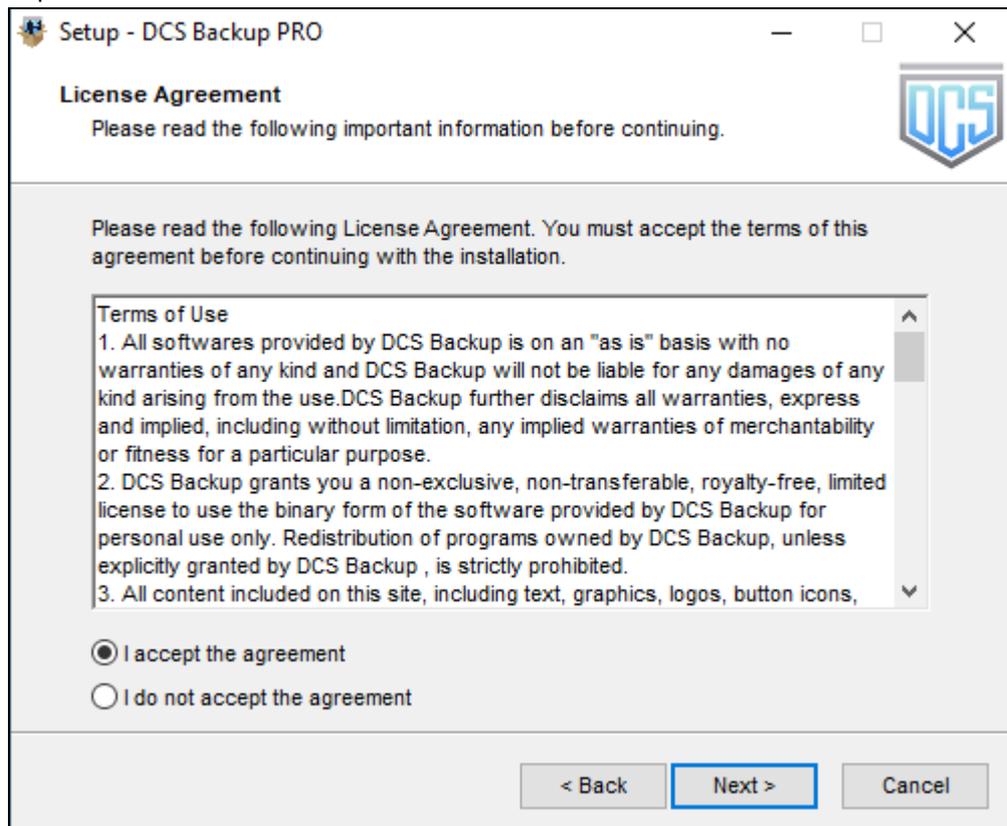
- The following dialog box will appear only if User Account Control is enabled. Click **Yes** to start the installation.



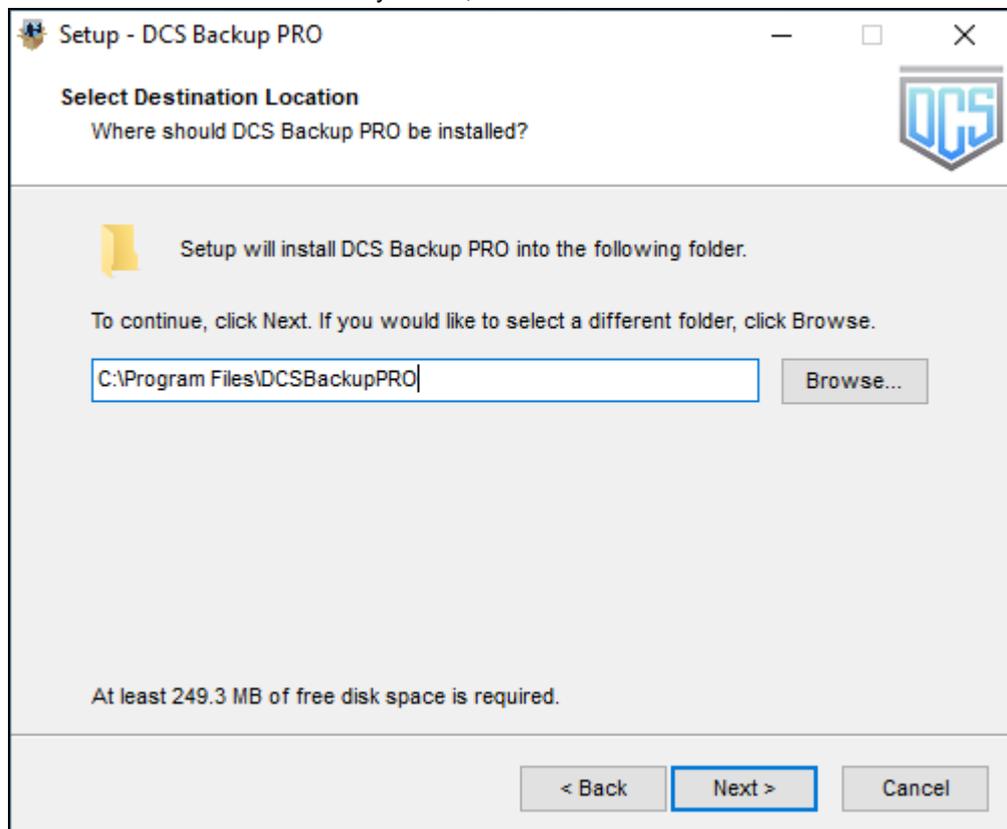
- Click **Next** to continue.



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



9. Choose the installation directory. Then, click **Next** to continue.



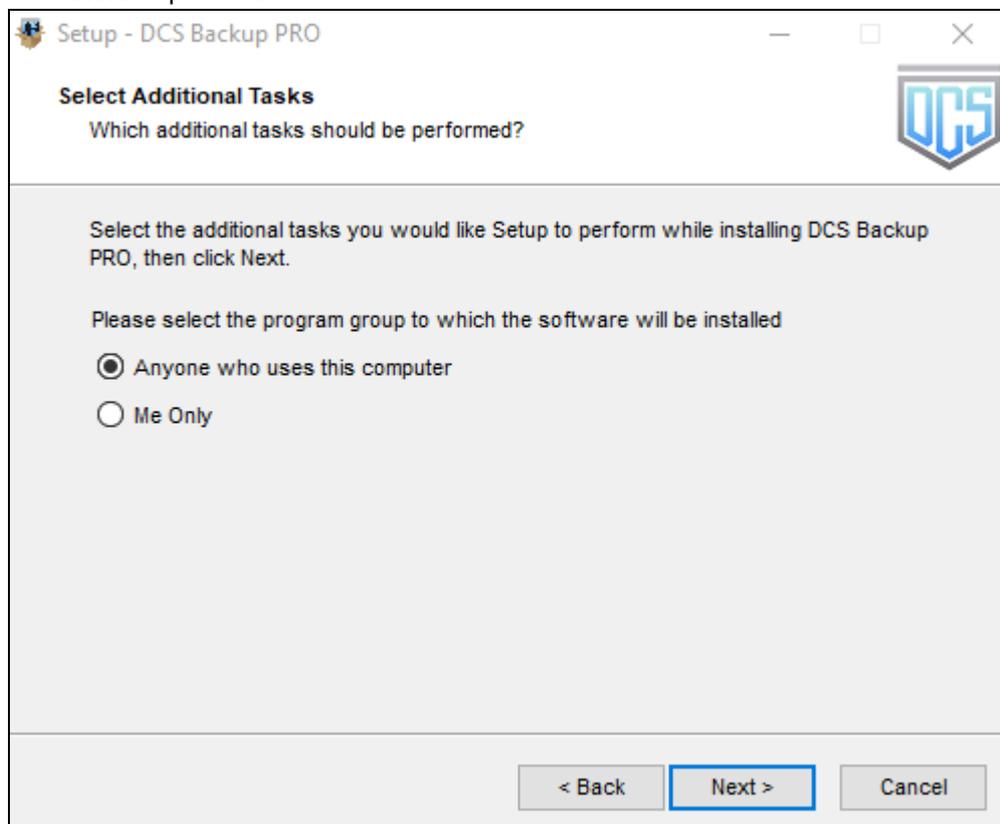
10. Select the program group to which the software will be installed. The default setting is “Anyone who uses this computer”. The following are the difference between the two settings:

- Anyone who uses this computer – the OBM System Tray icon will be available to all Windows users and backup notifications will be displayed on the Windows System Tray. For more information, please refer to [Chapter 8.11 System Tray](#).
- Me Only – the OBM System Tray icon will not be available and backup notifications will not be displayed on the Windows System Tray.

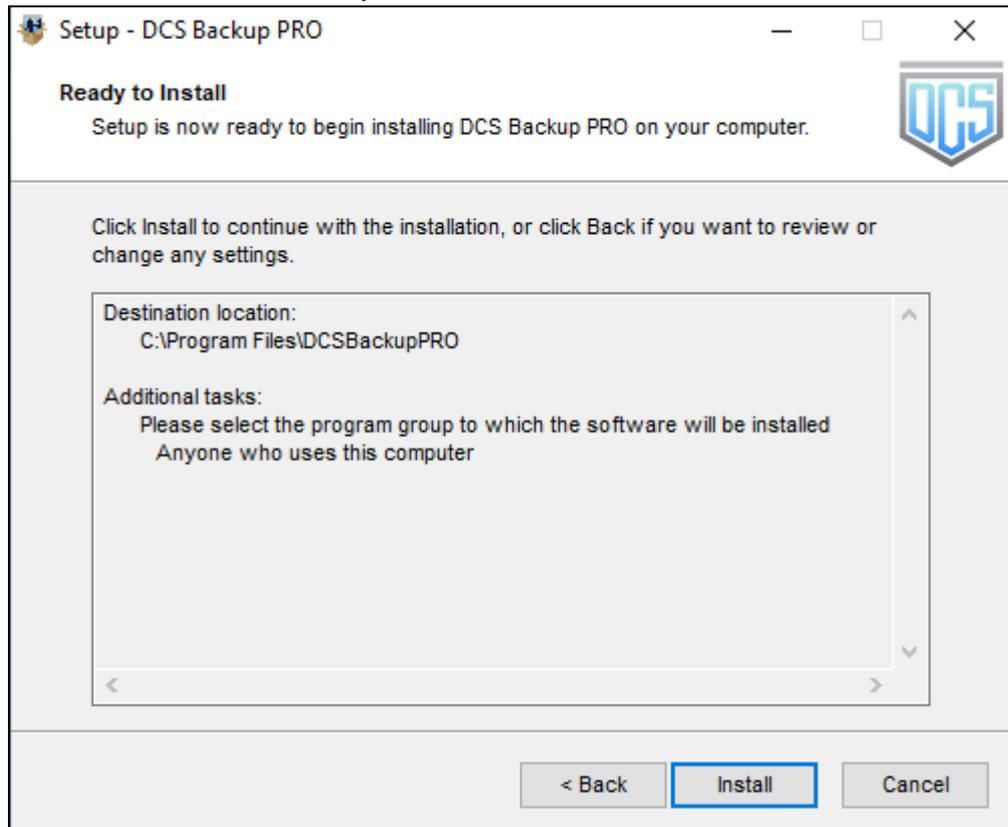
NOTE

Once the program group setting has been chosen and the installation completed; if you need to change the setting, this will require an uninstallation and re-installation of the application.

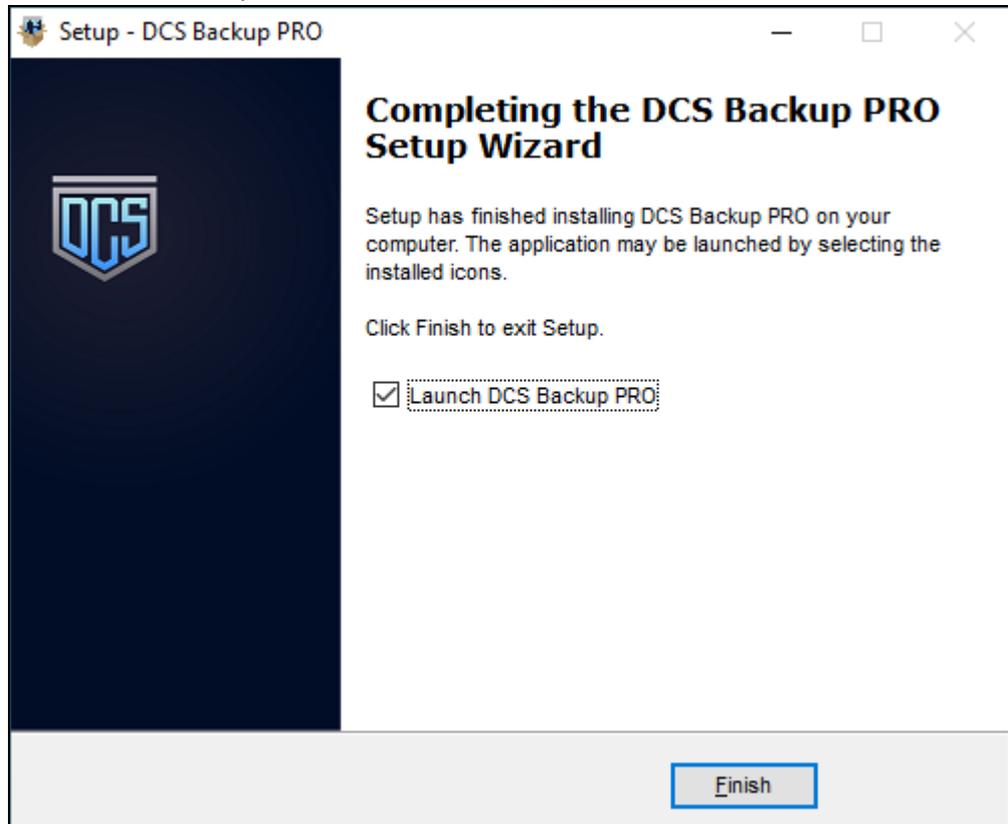
Click **Next** to proceed.



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



12. Click **Finish** to complete the installation.



6.3 OBM Services

The OBM Services is a key component which regulates and controls several important functions on OBM.

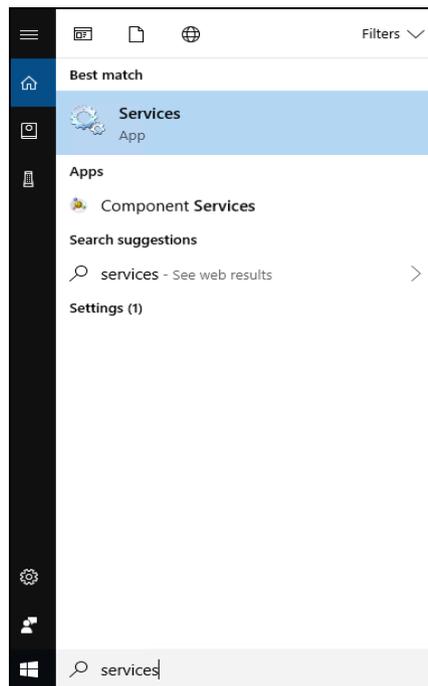
| Function | Description |
|---|---|
| Scheduled Backups | Ensures that backup jobs which are setup to run at a certain date and/or time are started. |
| Continuous Backups (Windows platform only) | Ensures that Continuous backups are run according to the backup interval. |
| Mobile Backup Server (MBS) | Ensures that registered mobile devices can perform backups to OBM. The MBS will be activated when a mobile device is registered for mobile backup on OBM. The MBS will be deactivated when all mobile devices have been deregistered from the mobile backup settings and the OBM services is restarted. |

Therefore, it is very important to ensure the OBM Services are running after:

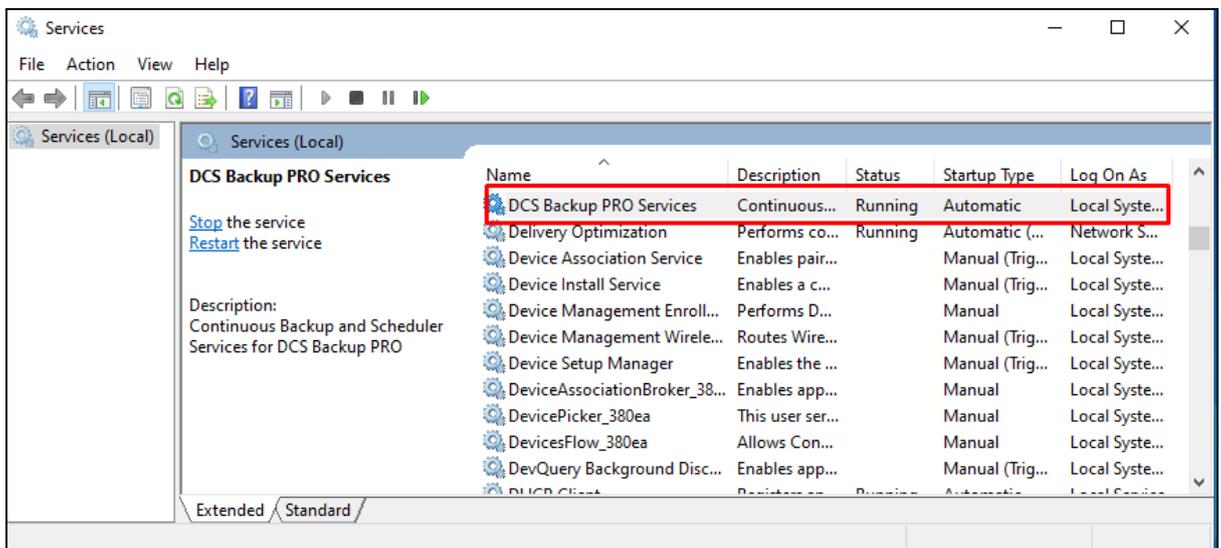
- ◉ a new OBM installation
- ◉ an OBM software update
- ◉ the machine was rebooted
- ◉ the machine is powered on
- ◉ the machine wakes up from hibernation or standby mode

Otherwise, all of the functions above will stop working.

To check if the OBM Scheduler Service is running properly on the local machine, go to start menu and search for **Services**.



Look for the **DCS Online Backup Manager Services** on the list. The **status** should be “Running”, and the **Startup Type** should be “Automatic”.



7 Start OBM

Starting with OBM v8.5.0.0, you will find two new features introduced with this latest version which are the Mobile Backup and Two-Factor Authentication. With these new features there are several scenarios that will be encountered for first time login if, Mobile Backup and/or Two-Factor Authentication are enabled on the user account. Login steps for the different scenarios will be discussed in this chapter.

7.1 Login to OBM without 2FA

To login to OBM without two-factor authentication, here are the three scenarios:

- ▶ [Initial login to OBM with no 2FA and no Mobile Add-on Module](#)
- ▶ [Initial login to OBM with no 2FA and with Mobile Add-on Module](#)
- ▶ [Subsequent login to OBM with no 2FA](#)

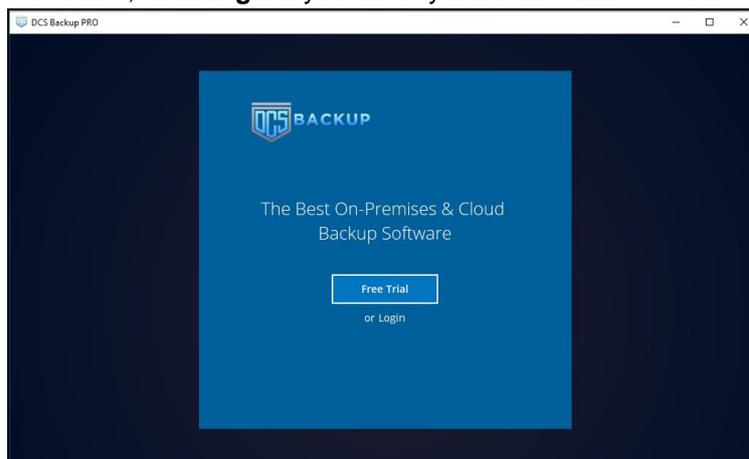
7.1.1 Initial login to OBM with no 2FA and no Mobile Add-on Module

When logging in to OBM for the first time pre-v8.5 login sequence, please follow the steps below:

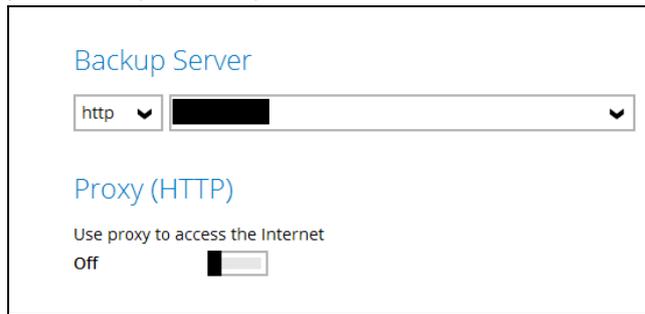
1. A shortcut icon of OBM will be available on your desktop after installation. Double-click the icon to launch the application.



2. The Free Trial Registration menu may be displayed when you login for the first time. If you want to create a free trial account please proceed to [Appendix E](#). Otherwise, click **Login** if you already have an OBM account.

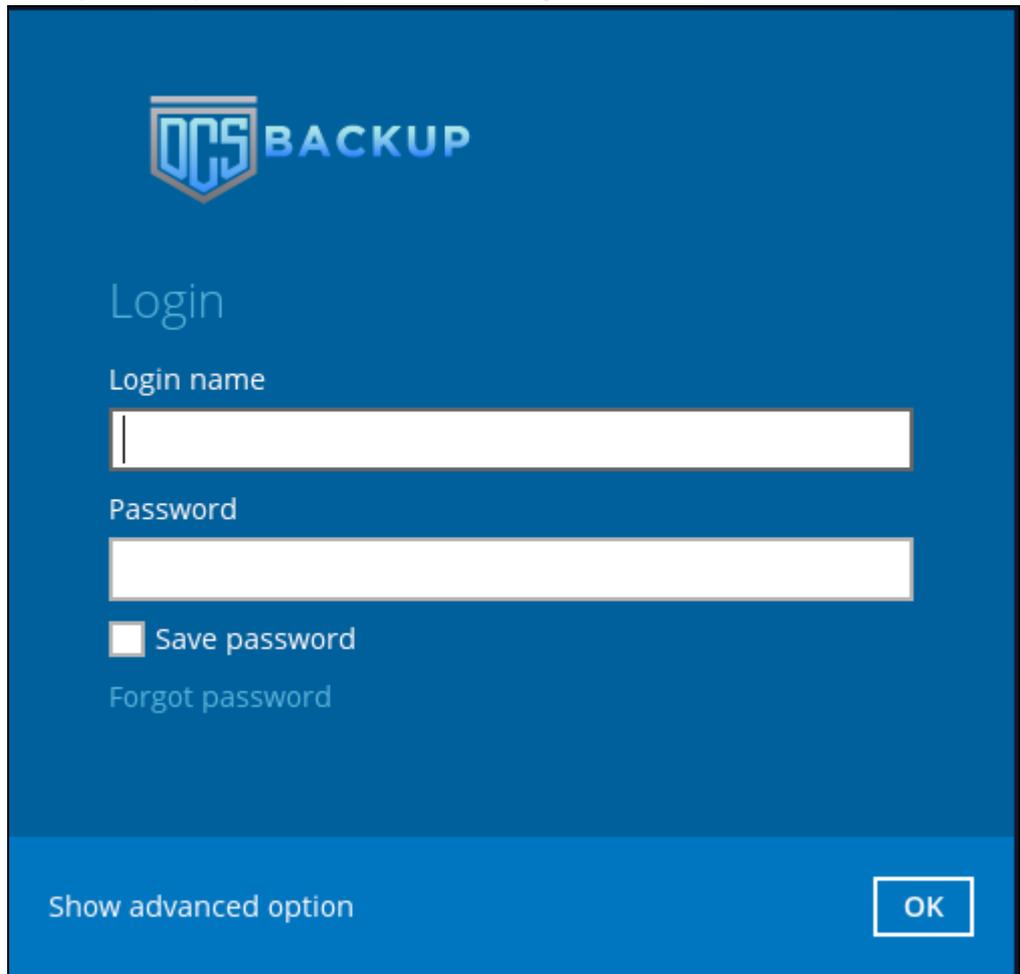


3. Click **Show advanced option** to enter the backup server settings provided by your backup service provider. Then, click **OK** to save the changes.



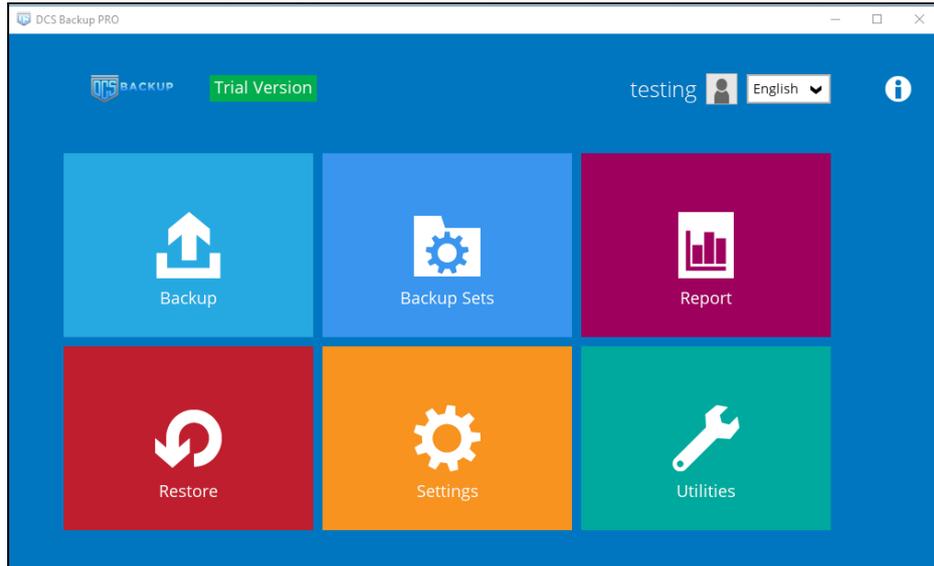
The screenshot shows a dialog box titled "Backup Server". It contains a dropdown menu with "http" selected and a redacted server address. Below this is a section for "Proxy (HTTP)" with a checkbox labeled "Use proxy to access the Internet" which is currently set to "Off".

4. Enter the login name and password of your OBM account provided by your backup service provider. Then, click **OK** to login.

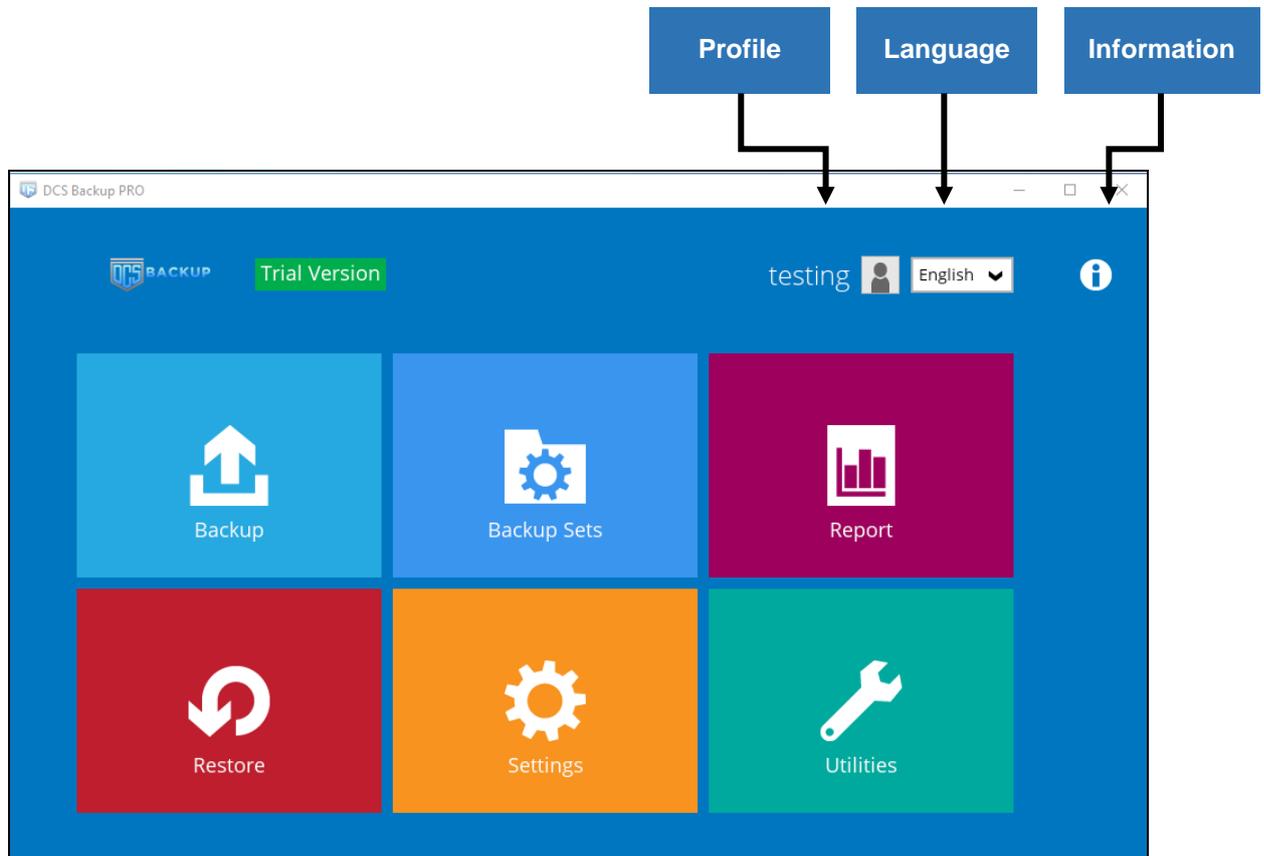


The screenshot shows the "OCS BACKUP Login" screen. It features the OCS Backup logo at the top. Below the logo is the word "Login". There are two input fields: "Login name" and "Password". Below the password field is a checkbox labeled "Save password" which is unchecked. There is a link for "Forgot password". At the bottom left, there is a link for "Show advanced option". At the bottom right, there is an "OK" button.

5. After successful login, the following screen will appear.



8 OBM Overview



OBM main interface has nine (9) icons that can be accessed by the user, namely:

- [Profile](#)
- [Language](#)
- [Information](#)
- [Backup](#)
- [Backup Sets](#)
- [Report](#)
- [Restore](#)
- [Settings](#)
- [Utilities](#)

8.1 Profile

The **Profile** icon shows the settings that can be modified by the user. The features that will be shown will depend on if the user accounts was using Twilio Two-Factor Authentication in prior to upgrading to v8.5.0.0 or above and continues to use Twilio.



There are seven (7) available features:

- ◉ [General](#)
- ◉ [Contacts](#)
- ◉ [Time Zone](#)
- ◉ [Encryption Recovery](#)
- ◉ [Password](#) (Only shown for backup accounts created prior to OBM v8.5.0.0 and using Twilio for two-factor authentication.)
- ◉ [Authentication](#)
- ◉ [Security Settings](#) (Only shown for backup accounts created prior to OBM v8.5.0.0 and using Twilio for two-factor authentication.)

8.1.1 General

The General tab displays the user's information.

A screenshot of a web application interface. On the left is a vertical sidebar with a "Profile" header and a list of tabs: "General" (highlighted in blue), "Contacts", "Time Zone", "Encryption Recovery", and "Authentication". The main content area is titled "User Information" and contains two fields: "Login name" with the value "WindowsTestAccount" and "Display name" with an empty text input box. At the bottom right of the main area are three buttons: "Save", "Cancel", and "Help".

| Control | Description |
|---------------------|---|
| Login name | Name of the backup account. |
| Display name | Display name of the backup account upon logging in to the DCS CBS User Web Console. |

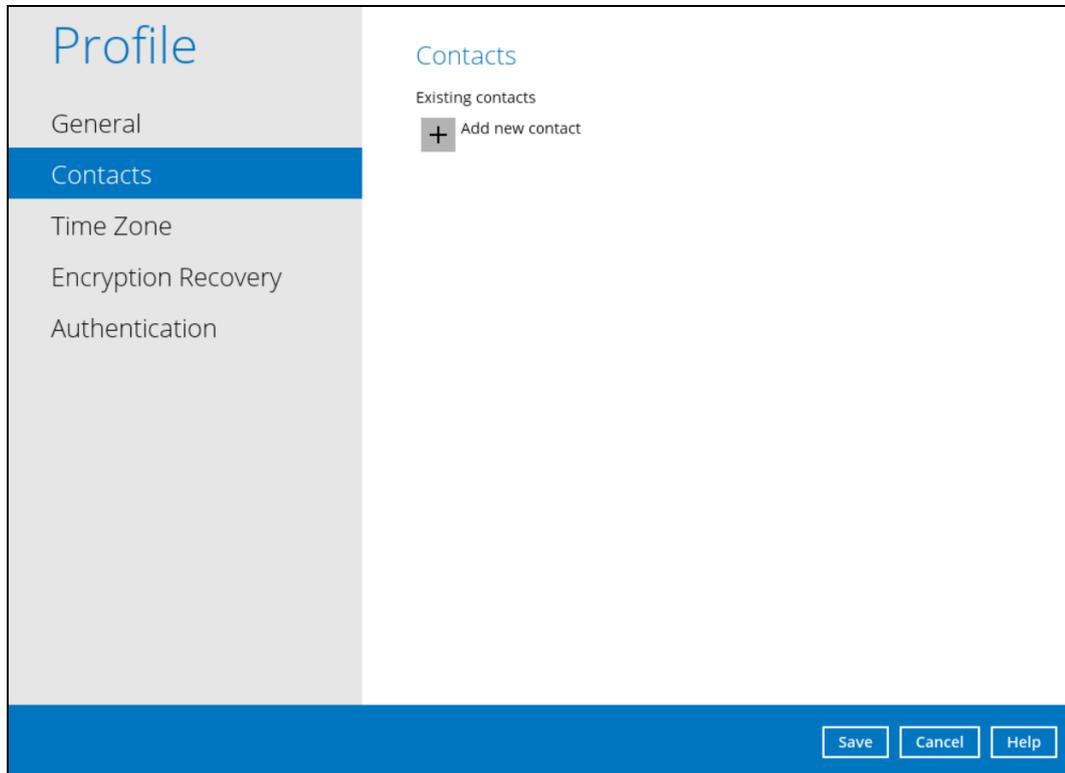
This will be the General tab for old backup account using Twilio for two-factor authentication.

The screenshot shows a 'Profile' page with a left-hand navigation menu and a main content area. The 'General' tab is selected in the menu. The 'User Information' section includes fields for 'Login name' (WindowsTestAccount) and 'Display name' (empty). The 'Last Successful Login' section displays the following information: Time: 10/09/2020 17:53 (CST), IP address: 180. [redacted] 31, Phone number (MFA): 63- [redacted], and Browser / App: Windows / Chrome. At the bottom right, there are 'Save', 'Cancel', and 'Help' buttons.

| Control | Description |
|---------------------------|---|
| Login name | Name of the backup account. |
| Display name | Display name of the backup account upon logging in to the DCS CBS User Web Console. |
| Time | The date and time the user last logged in. |
| IP address | The IP address used to login. |
| Phone number (MFA) | The phone number where sms authentication will be sent when 2FA is enabled. |
| Browser / App | The browser or app used to login in to DCS CBS User Web Console or OBM. |

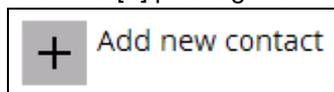
8.1.2 Contacts

This refers to the contact information of the user. You can also add multiple contacts or modify existing contact information. Having this filled in will help in sending backup and daily reports and even recovered backup set encryption key in case it was forgotten or lost.



To add a new contact, follow the instructions below:

1. Click the [+] plus sign to add a new contact.



2. Complete the following fields then click the [OK] button to return to the main screen.
 - Name
 - Email
 - Address
 - Company
 - Website
 - Phone 1
 - Phone 2

Profile | **Contacts**

New Contact

Name

Email

Send me encrypted email (S/MIME)

Address

Company

Website

OK Cancel

3. Click the [Save] button to store the contact information.

Profile

General

Contacts

Time Zone

Encryption Recovery

Authentication

Contacts

Existing contacts

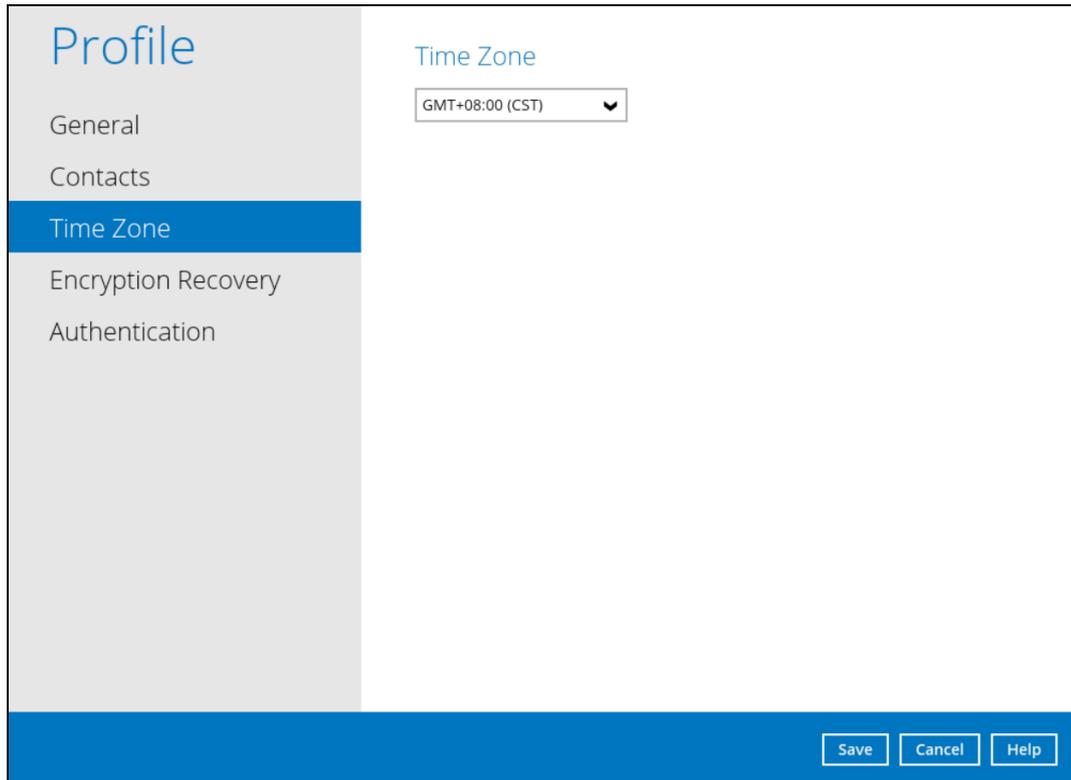
samplename
sample_email@mail.com

Add

Save Cancel Help

8.1.3 Time Zone

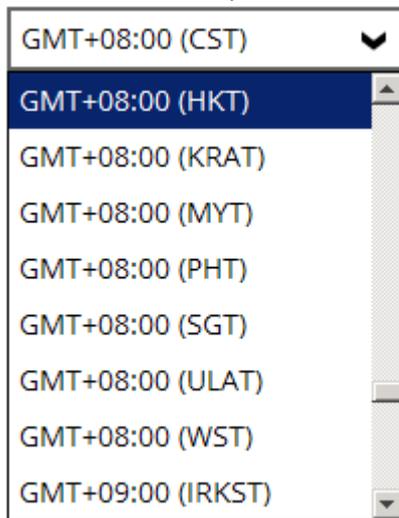
The time zone indicated.



The screenshot shows a web interface for profile settings. On the left is a navigation menu with the following items: Profile, General, Contacts, Time Zone (highlighted in blue), Encryption Recovery, and Authentication. The main content area is titled 'Time Zone' and contains a dropdown menu currently set to 'GMT+08:00 (CST)'. At the bottom right of the interface are three buttons: 'Save', 'Cancel', and 'Help'.

To modify the time zone, follow the instructions below:

1. Select from the dropdown list.



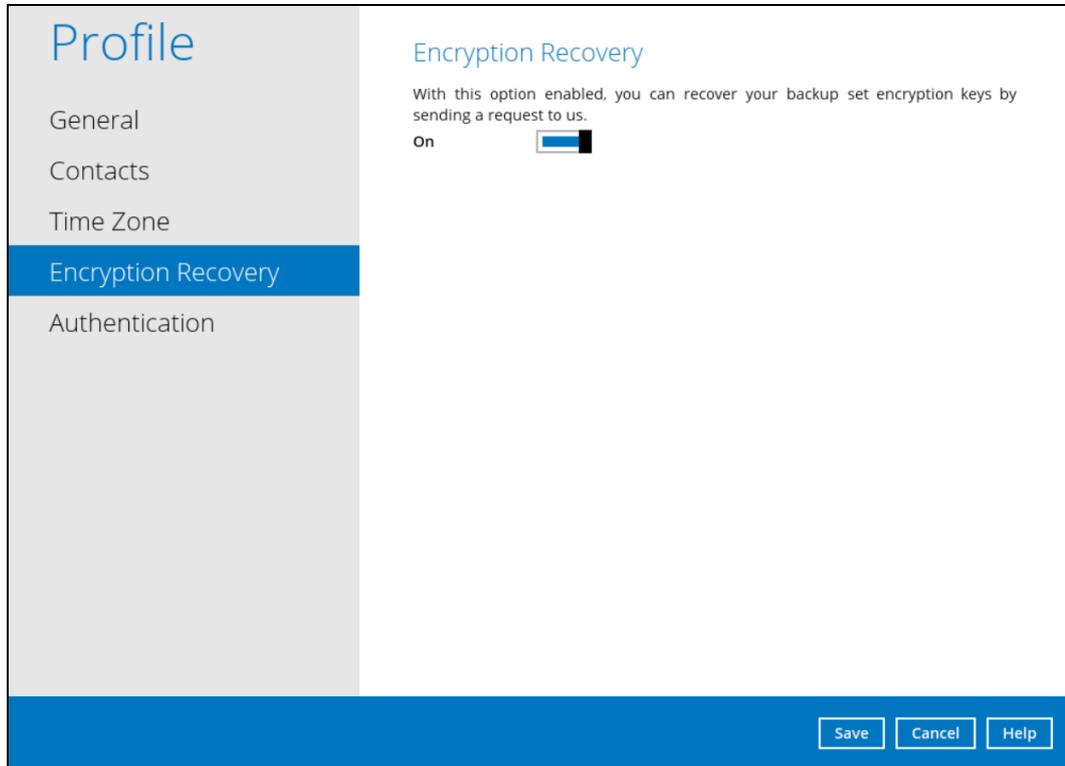
The screenshot shows the dropdown menu expanded, displaying a list of time zone options. The current selection is 'GMT+08:00 (CST)'. The list includes: GMT+08:00 (HKT), GMT+08:00 (KRAT), GMT+08:00 (MYT), GMT+08:00 (PHT), GMT+08:00 (SGT), GMT+08:00 (ULAT), GMT+08:00 (WST), and GMT+09:00 (IRKST).

2. Click the [Save] button to save the updated time zone.

8.1.4 Encryption Recovery

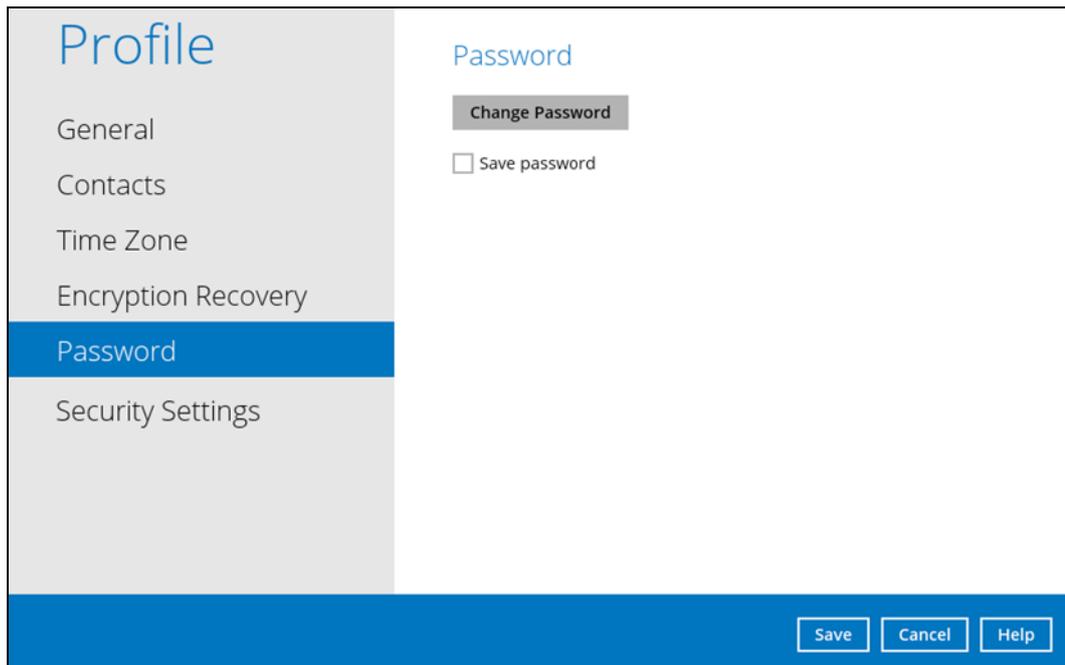
Backup set encryption key can be recovered by turning this feature on.

NOTE: This option may not be available. Please contact your backup service provider for more details.



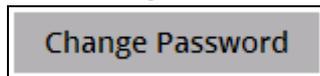
8.1.5 Password

Login password can be modified anytime. Tick the [Save Password] box to bypass the password entry upon opening the OBM.



To modify the password, follow the instructions below:

1. Click [Change Password].



2. Enter the current password, then click [Next].

A screenshot of a web application interface. At the top, there is a dark grey header with the word "Profile" on the left and "Password" on the right. Below the header, the main content area is white and contains the title "Change Password" in blue. Underneath the title, the text "Please confirm current password" is displayed above a single text input field. At the bottom of the white area, there is a blue horizontal bar containing two buttons: "Next" and "Cancel". Below this bar, a dark grey footer contains three buttons: "Save", "Cancel", and "Help".

3. Enter the New Password and re-enter, then click the [OK] button to return to the main screen.

A screenshot of the same web application interface as in the previous step. The main content area is white and contains the title "Change Password" in blue. Below the title, the text "New Password" is displayed above a text input field. Underneath that, the text "Re-enter password" is displayed above another text input field. At the bottom of the white area, there is a blue horizontal bar containing two buttons: "OK" and "Cancel". Below this bar, a dark grey footer contains three buttons: "Save", "Cancel", and "Help".

4. Click the [Save] button to store the updated password.

8.1.6 Authentication

You can use the Authentication function to:

- ◉ Change the [“Password”](#).
- ◉ Enable or disable the [“Two-Factor Authentication”](#).
- ◉ Add one or more device(s) registered for Two-Factor Authentication (2FA).

NOTE

Please refer to the [DCS Mobile App User Guide for Android and iOS – Chapter 6.3.1](#) for the detailed step-by-step procedure.

- ◉ [Remove one or more device\(s\)](#) registered for Two-Factor Authentication (2FA).
- ◉ View details of the [“Last Successful Login”](#) for Password Lock and Two-Factor Authentication (2FA).

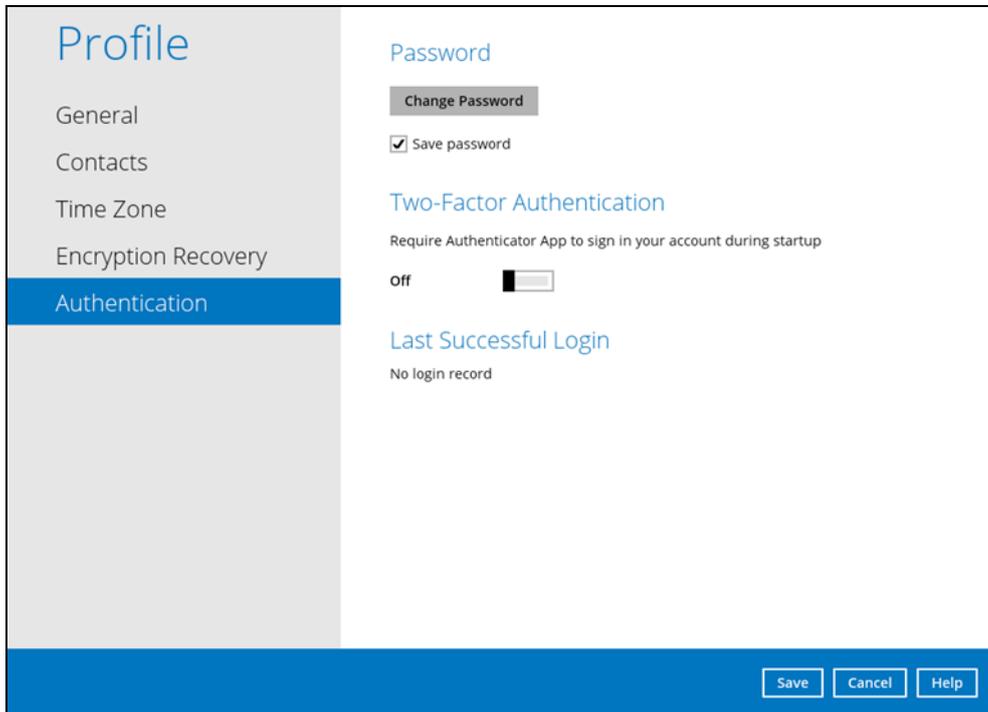
NOTE

For Two-Factor Authentication (2FA), you can register your mobile device on both DCS Mobile app and a third-party authenticator apps (e.g., Authy, Duo, Google Authenticator, Microsoft Authenticator, and LastPass Authenticator).

The screenshot displays the 'Profile' settings page in the DCS Mobile App. On the left, a navigation menu lists 'General', 'Contacts', 'Time Zone', 'Encryption Recovery', and 'Authentication' (which is highlighted in blue). The main content area is divided into three sections: 'Password', 'Two-Factor Authentication', and 'Last Successful Login'. The 'Password' section includes a 'Change Password' button and a 'Save password' checkbox. The 'Two-Factor Authentication' section shows the option 'Require Authenticator App to sign in in your account during startup' is currently 'off'. The 'Last Successful Login' section indicates 'No login record'. At the bottom right, there are three buttons: 'Save', 'Cancel', and 'Help'.

Password

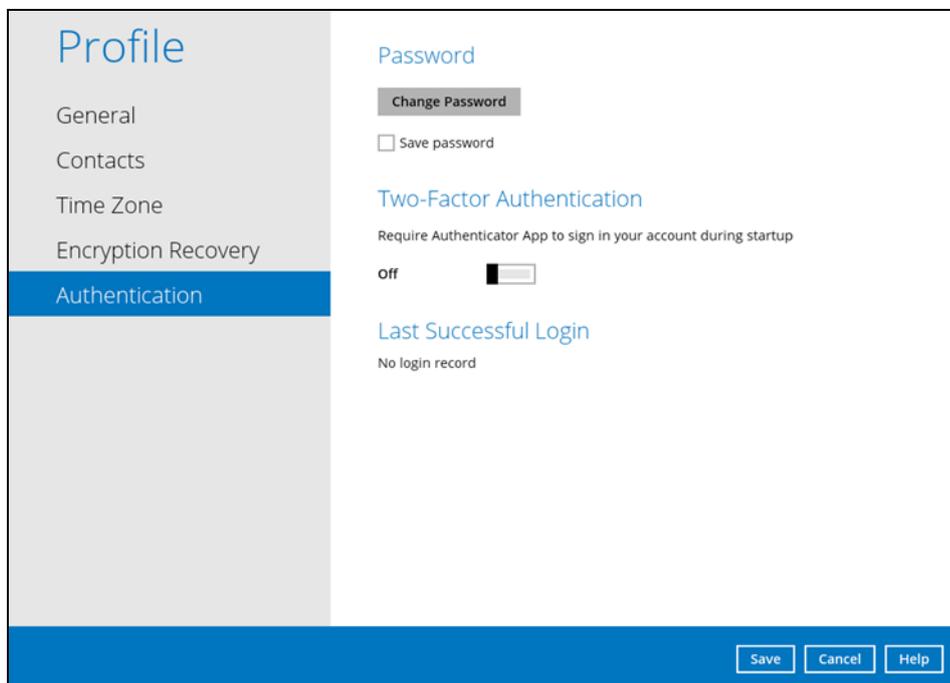
Login password can be modified anytime. Tick the **Save Password** box to bypass the password entry upon opening the OBM.



The screenshot shows the 'Profile' page with the 'Authentication' section selected. Under the 'Password' heading, there is a 'Change Password' button and a checked 'Save password' checkbox. Below this, the 'Two-Factor Authentication' section is visible, with a toggle switch set to 'off'. The 'Last Successful Login' section shows 'No login record'. At the bottom right, there are 'Save', 'Cancel', and 'Help' buttons.

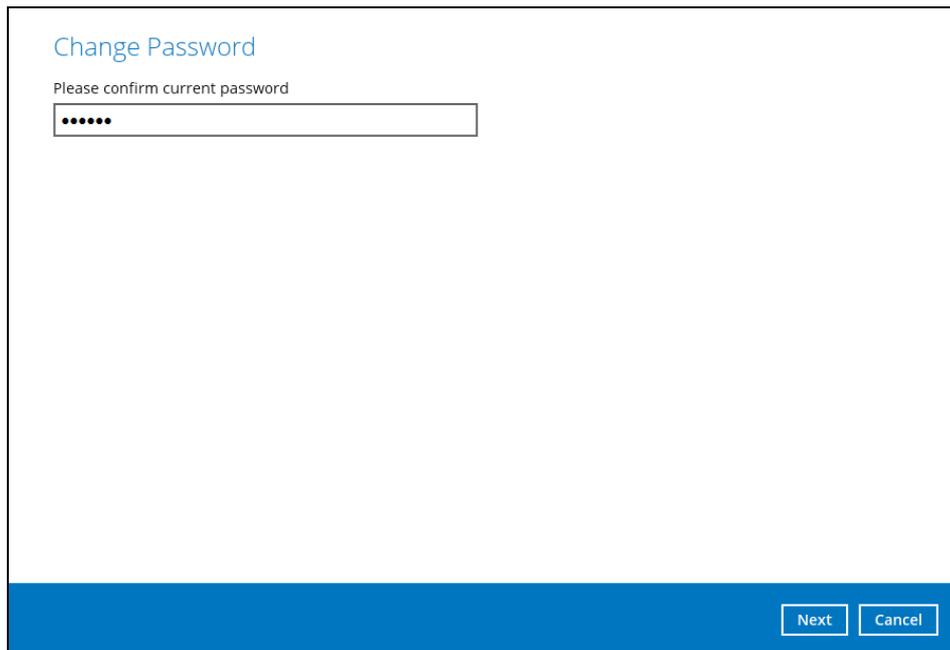
To change the password, follow the instructions below:

1. Click the **Change Password**.



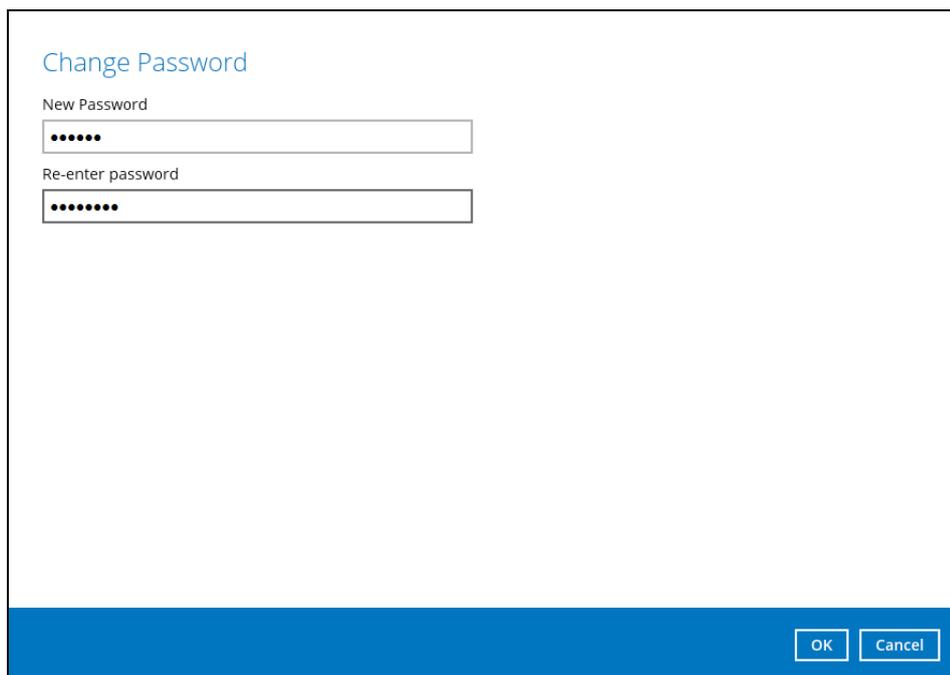
This screenshot is identical to the previous one, but the 'Change Password' button is highlighted with a grey background, indicating it is the next step in the process.

2. Enter the current password.



The screenshot shows a dialog box titled "Change Password". Below the title, it says "Please confirm current password". There is a single text input field containing six black dots. At the bottom right of the dialog, there are two buttons: "Next" and "Cancel".

3. Enter the new password and re-enter it for authentication purposes. Click **OK** to return to main screen.



The screenshot shows the same "Change Password" dialog box. Below the title, it says "New Password". There is a text input field containing six black dots. Below that, it says "Re-enter password". There is another text input field containing six black dots. At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

4. Click **Save** to store the settings.

The screenshot shows a user profile settings page. On the left is a navigation menu with the following items: Profile, General, Contacts, Time Zone, Encryption Recovery, and Authentication (which is highlighted in blue). The main content area is titled 'Authentication' and contains three sections: 'Password' with a 'Change Password' button and a 'Save password' checkbox; 'Two-Factor Authentication' with the text 'Require Authenticator App to sign in your account during startup' and a toggle switch set to 'Off'; and 'Last Successful Login' with the text 'No login record'. At the bottom right of the page are three buttons: 'Save', 'Cancel', and 'Help'.

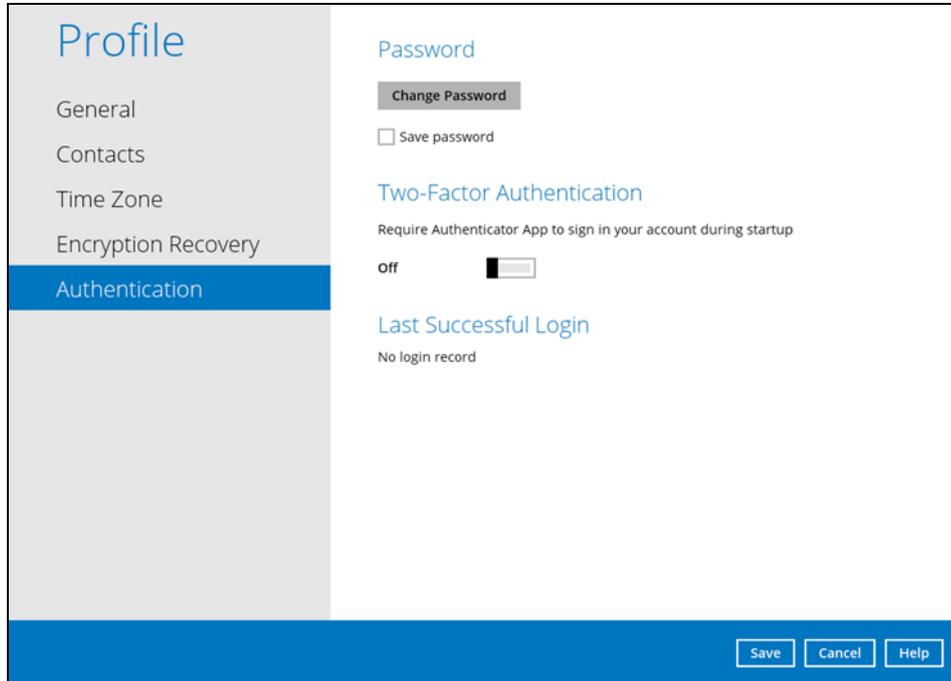
Two-Factor Authentication

To enable the two-factor authentication feature, follow the instructions below:

NOTE

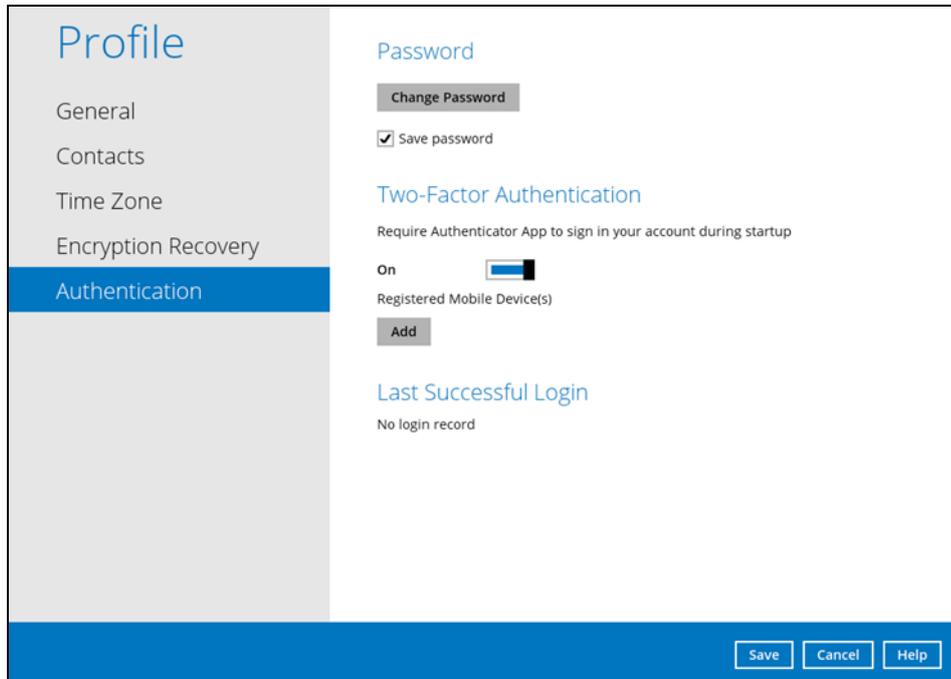
The DCS Mobile app or a third-party authenticator apps is needed for 2FA.

1. Go to **Settings > Authentication > Two-Factor Authentication**.



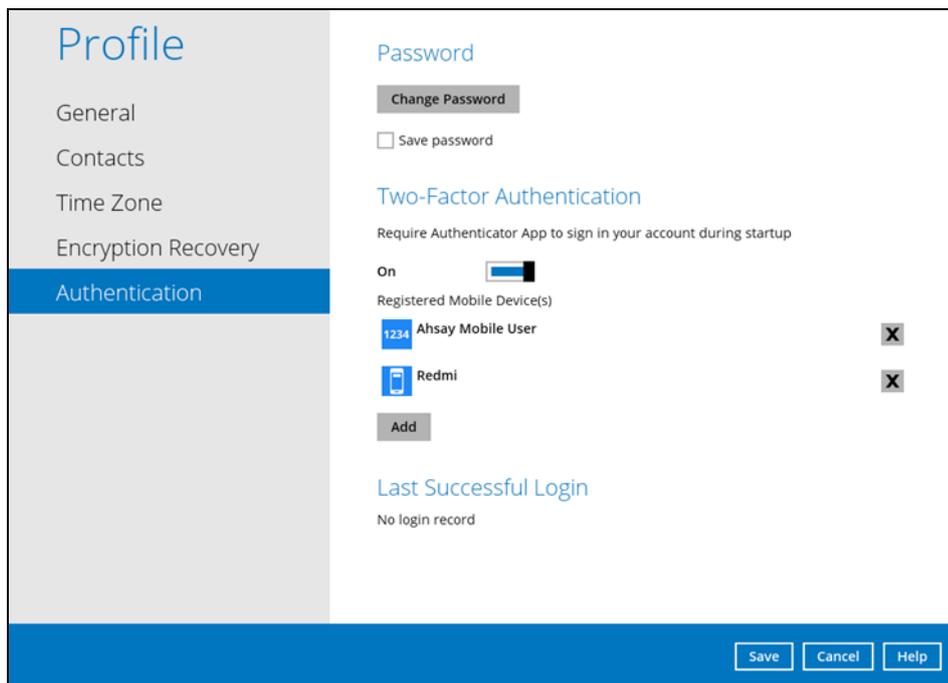
2. Swipe lever to the right to turn it on.

For the detailed step-by-step procedure on how to add a mobile device, please refer to [DCS Mobile App User Guide for Android and iOS – Chapter 6.3.1](#)

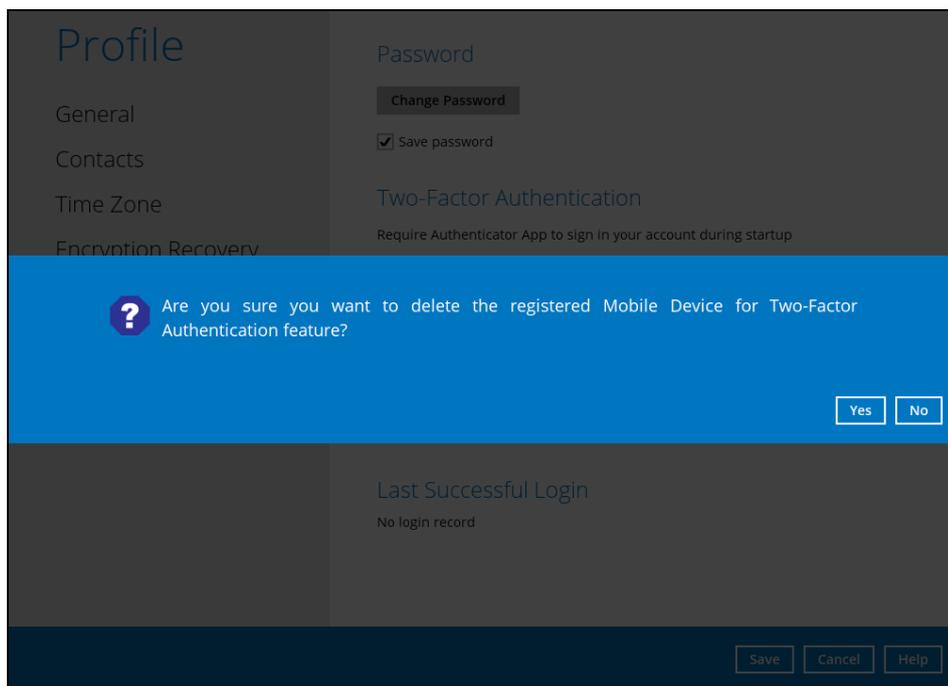


To remove a mobile device, follow the instructions below:

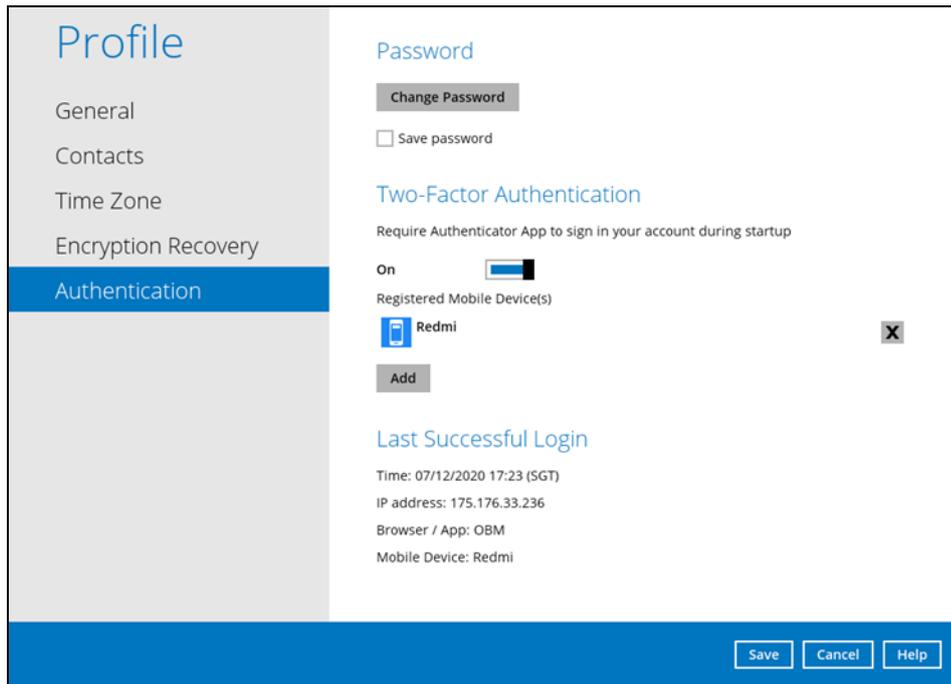
1. Click the **[X]** button on the left side of the registered mobile device.



2. A confirmation message will appear, click **Yes** to proceed. Otherwise, click **No**.



3. Mobile device is successfully removed.

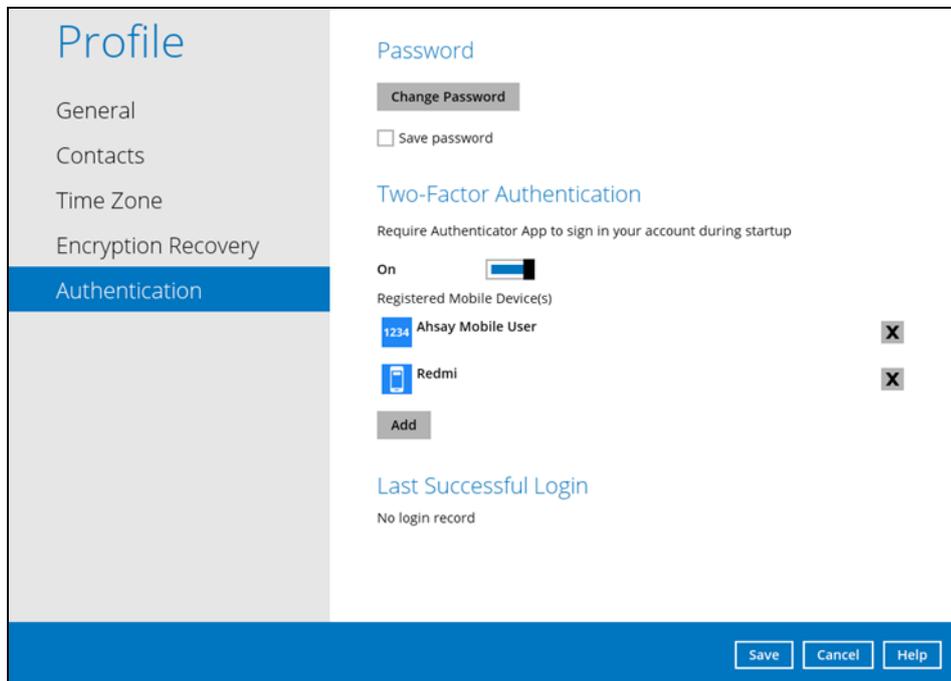


To disable the two-factor authentication feature, follow the instructions below:

NOTE

Sliding the switch to right hand side will only turn off the two-factor authentication but it will not automatically delete the registered mobile device(s) for Two-Factor Authentication. If you need to delete the registered mobile device(s), this must be done manually first before disabling Two-Factor Authentication

1. Swipe the lever to the left to turn it off.



2. Click **Save** to save the settings.

Profile

- General
- Contacts
- Time Zone
- Encryption Recovery
- Authentication**

Password

[Change Password](#)

Save password

Two-Factor Authentication

Require Authenticator App to sign in your account during startup

off

Last Successful Login

No login record

[Save](#) [Cancel](#) [Help](#)

Last Successful Login

Displays the Date, Time, IP address, and Browser / App the user last logged in and the registered Mobile Device.

- ▶ Time – the date and time the user last logged in.
- ▶ IP address – the IP address used to login.
- ▶ Browser / App – the browser or app used to login to DCS CBS User Web Console or OBM.
- ▶ Mobile Device – the name of the device used for authentication when 2FA is enabled.

The screenshot shows the 'Profile' page with the 'Authentication' tab selected. The 'Last Successful Login' section displays the following information:

- Time: 07/12/2020 17:23 (SGT)
- IP address: 175.176.33.236
- Browser / App: OBM
- Mobile Device: Redmi

At the bottom of the page, there are three buttons: 'Save', 'Cancel', and 'Help'.

Below is the screenshot If there is no login record yet.

The screenshot shows the 'Profile' page with the 'Authentication' tab selected. The 'Last Successful Login' section displays the following information:

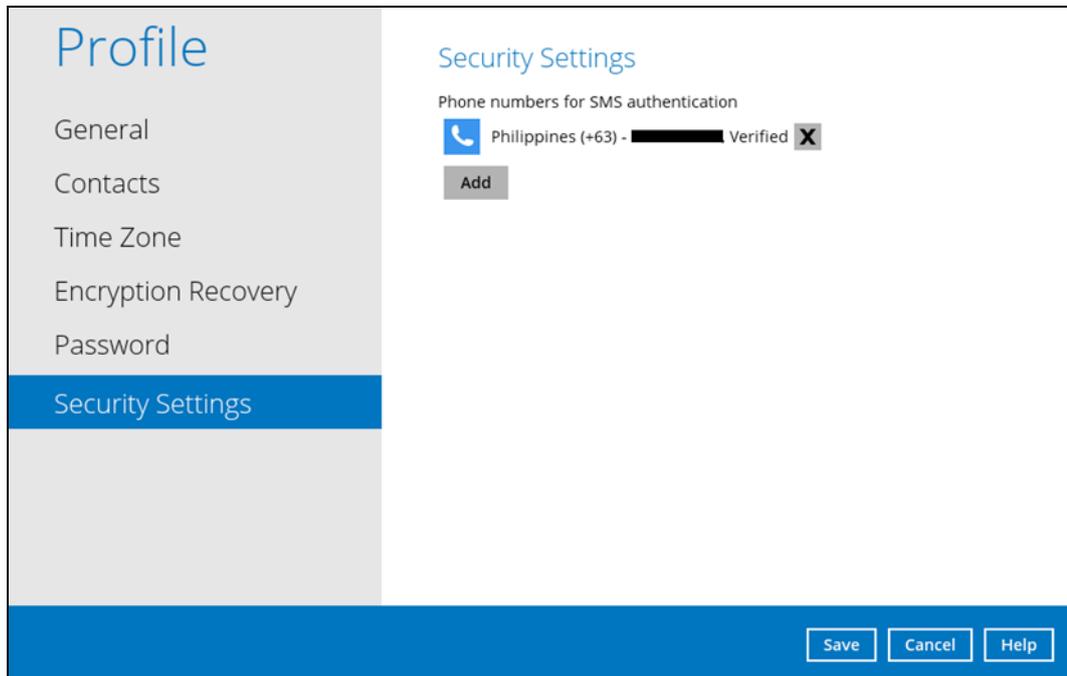
- No login record

At the bottom of the page, there are three buttons: 'Save', 'Cancel', and 'Help'.

8.1.7 Security Settings

The **Security Settings** option is for backward compatibility with Twilio Two-Factor Authentication. It will only be visible if Twilio Two-Factor Authentication was enabled on the user account on pre-v8.5.0.0 OBM versions.

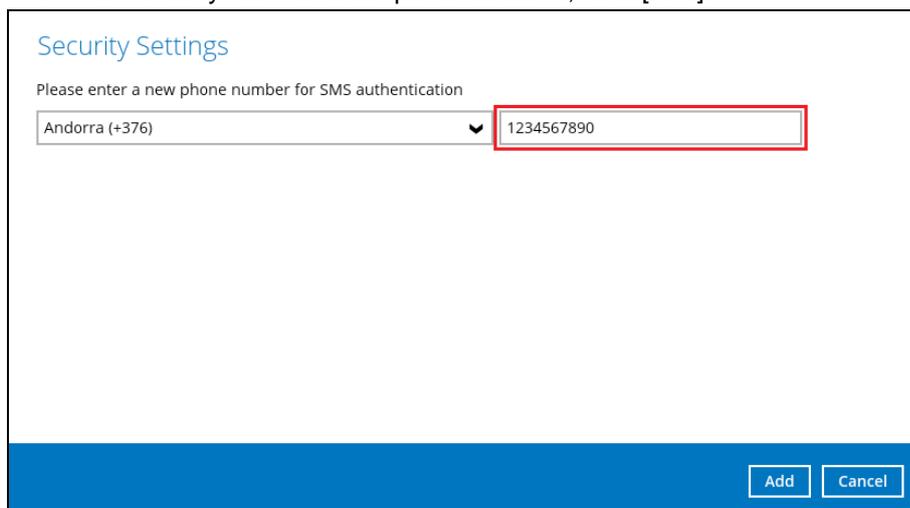
Phone numbers that will be used for sending sms authentication will be listed here and will show the status if it is verified or not. You can also add phone numbers here that can be used for sending the sms authentication.



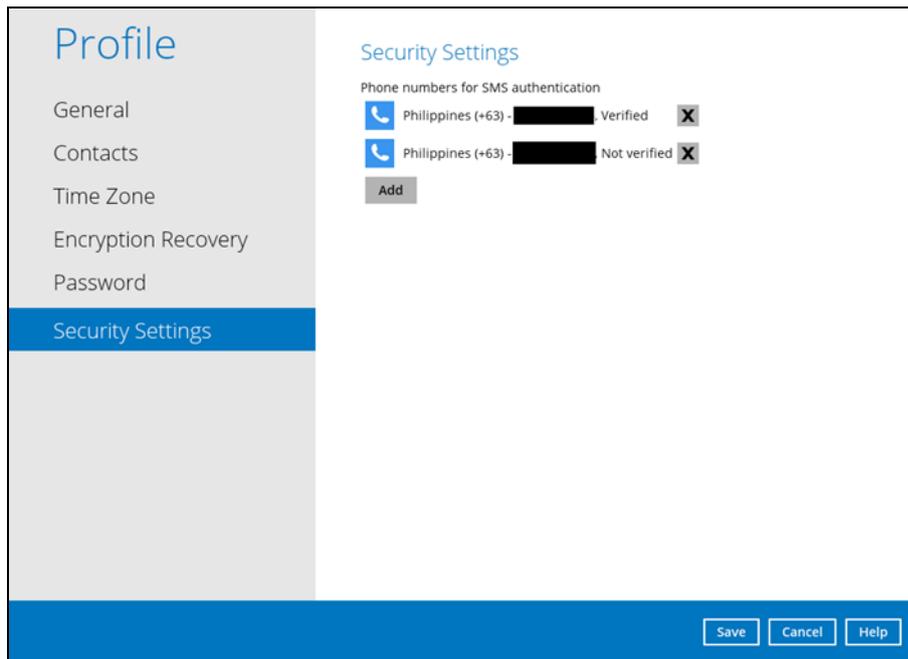
1. Click [Add].



2. Select the country and enter the phone number, click [Add].

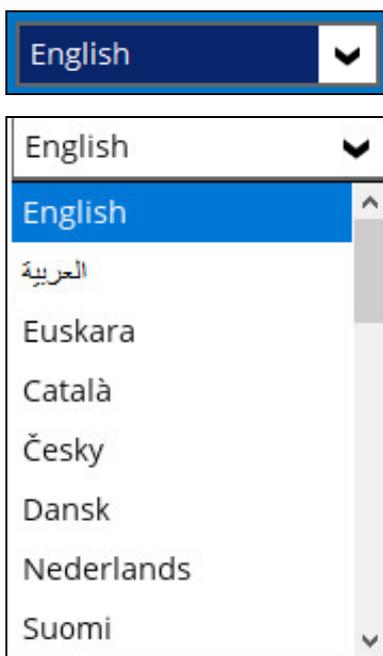


3. Click the [Save] button to save the phone number.



8.2 Language

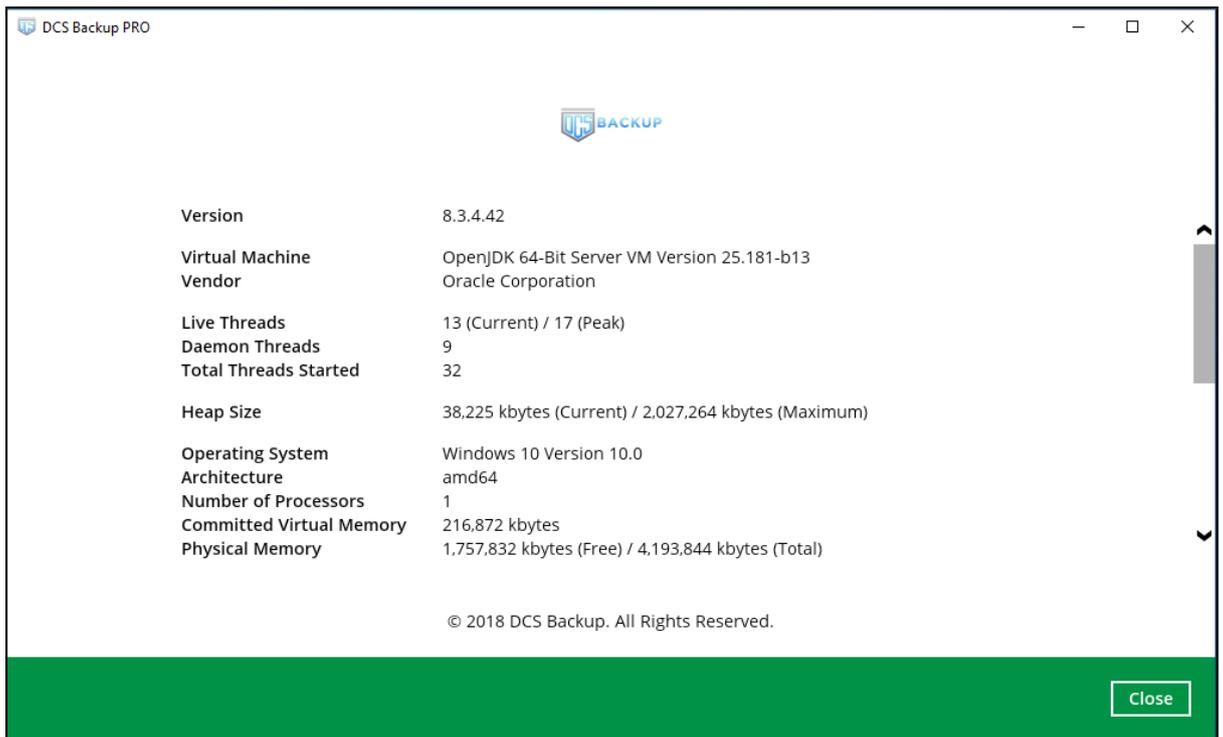
The list of available languages depends on the backup service provider.



8.3 Information

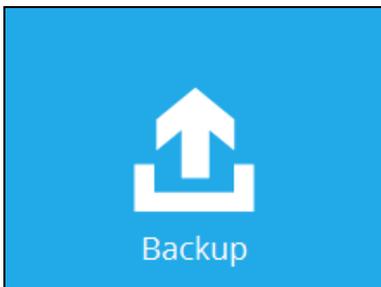
The **Information** icon displays the product version and system information of the machine where the OBM is installed.





8.4 Backup

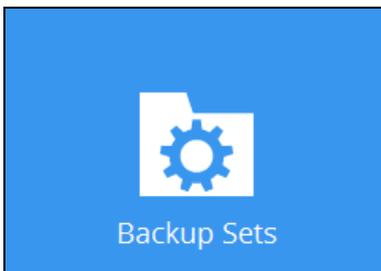
This feature is used to run the backup set/s.



To start backing up, follow the instructions on [Chapter 11 Run Backup Jobs](#)

8.5 Backup Sets

A backup set is a place for files and/or folders of your backed up data. This feature allows the user to select files individually or an entire folder to backup. It is also used to delete backup set/s.



To create or modify a backup set, follow the instructions on [Chapter 9 Create a Backup Set](#)

Backup Set Settings

Below is the list of configurable settings under a Backup Set:

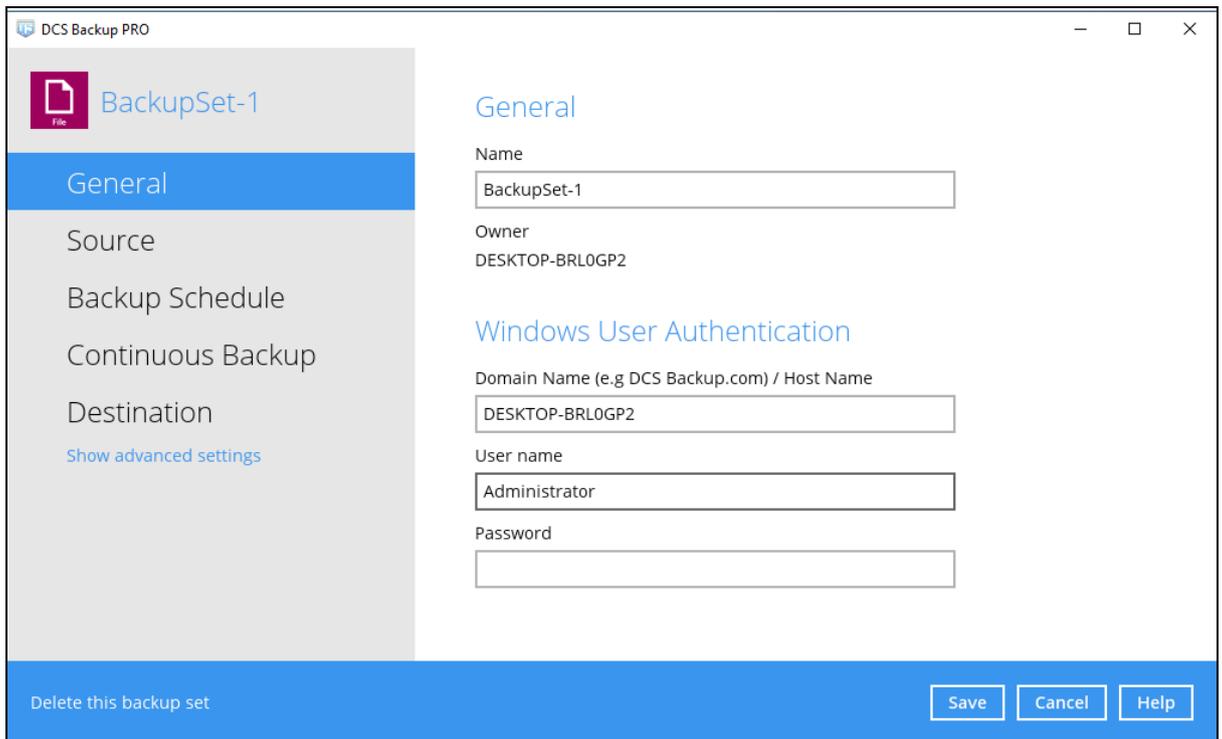
- [General](#)
- [Source](#)
- [Backup Schedule](#)
- [Continuous Backup](#)
- [Destination](#)

(Advanced settings)

- [In-File Delta](#)
- [Retention Policy](#)
- [Command Line Tool](#)
- [Reminder](#)
- [Bandwidth Control](#)
- [Others](#)

General

This feature allows the user to modify the backup set name and manage the Windows User Authentication login credentials in the backup set.



The screenshot shows the 'General' settings window for a backup set named 'BackupSet-1'. The window has a sidebar on the left with a 'General' tab selected. The main area contains the following fields:

- Name:** BackupSet-1
- Owner:** DESKTOP-BRLOGP2
- Windows User Authentication:**
 - Domain Name (e.g DCS Backup.com) / Host Name:** DESKTOP-BRLOGP2
 - User name:** Administrator
 - Password:** (empty field)

At the bottom of the window, there is a 'Delete this backup set' link on the left and 'Save', 'Cancel', and 'Help' buttons on the right.

Backup Set Name

To modify the name of a backup set, follow the steps below:

1. In the Name field, enter a new backup set name.

General

Name

Owner

w2k16R2-std

2. Click the [Save] button to save the updated backup set name.

The screenshot shows the 'DCS Backup PRO' application window. On the left is a navigation pane with a 'BackupSet-1' header and a list of settings: 'General' (selected), 'Source', 'Backup Schedule', 'Continuous Backup', and 'Destination'. Below these is a link for 'Show advanced settings'. The main area is titled 'General' and contains the following fields: 'Name' (BackupSet-1), 'Owner' (DESKTOP-BRLOGP2), 'Windows User Authentication' section with 'Domain Name (e.g DCS Backup.com) / Host Name' (DESKTOP-BRLOGP2), 'User name' (Administrator), and 'Password' (empty). At the bottom, there is a blue bar with a 'Delete this backup set' link and three buttons: 'Save', 'Cancel', and 'Help'.

NOTE

In assigning a backup set name, make sure that it does not have an identical name.

Windows User Authentication

To successfully perform backup and restore operations, OBM requires both read and write permission to all the files/folders selected in the backup source.

The Windows User Authentication login credentials are used by the OBM to ensure it has sufficient permission to access files and/or folders selected in the Backup Source, the temporary folder location, and the backup destination if it is a network drive accessible from backup machine via LAN, especially when running scheduled backup jobs, as the default Windows account used by the OBM scheduler service is a local system account which does not have access to network resources.

Windows User Authentication

Domain Name (e.g DCS Backup.com) / Host Name

User name

Password

- If files and/or folders selected are located on network drive(s), the login credentials for the Windows User Authentication must have permission to access network resources, (e.g. an administrator account).
- If the machine is a file server shared by multiple users, then the OBM will require login credentials with read/write permissions to access all the selected files and/or folders in the backup source (e.g., an administrator account).

| Field | Description |
|--------------------|--|
| Domain Name | The domain or host name of the machine. |
| Username | Login username used by the OBM to access files and/or folders selected in the backup source. |
| Password | Login password used by the OBM to access files and/or folders selected in the backup source. |

Source

This feature allows the user to select files and/or folders in the backup source to back up.

There are three (3) different ways to select files and/or folders to back up:

| Option | Description |
|-------------------------------|--|
| Quick or Shortcut | This allows the user to back up files and/or folders in the selected backup source entirely. |
| Filter | This allows the user to select or exclude files and/or folders from the backup job. |
| Advanced Backup Source | This allows the user to select files and/or folders individually to back up. |

Option 1: Quick or Shortcut

This option allows the user to quickly select a backup source to be backed up.

Backup Source

Select the files and folders that you want to backup

Desktop

My Documents

Favorites

Outlook

Windows Live Mail

If any of the following backup source is selected and the [Backup Schedule](#) is enabled, the Windows User Authentication will prompt the user to enter the login password. To select a backup source without entering the login password, the backup schedule must be disabled.

| | |
|-------------------|---|
| Desktop |  |
| My Documents |  |
| Favorites |  |
| Outlook |  |
| Windows Live Mail |  |

Windows User Authentication

Domain Name (e.g DCS Backup.com) / Host Name

User name

Password

NOTE

During the creation of backup set, if this type of backup source (Quick or Shortcut) is selected and the Schedule is set to "on", the Windows User Authentication screen will be displayed. You will

need to enter the login password, otherwise, the creation of backup set will not continue.

To know the locations of the folder(s) that will be backed up for each selected backup source, refer to the following table:

| Backup Source | | Description |
|-------------------|---|--|
| Desktop |  | If Desktop is selected, all files and/or folders in the following location will be backed up: <i>%UserProfile%\Desktop</i> |
| My Documents |  | If Documents is selected, all files and/or folders located in the following location will be backed up: <i>%UserProfile%\Documents</i> If the Follow Link is enabled, all files and/or folders located in the following locations will also be backed up: <i>%UserProfile%\Music</i> <i>%UserProfile%\Pictures</i> <i>%UserProfile%\Videos</i> NOTE: The Follow link is enabled by default. |
| Favorites |  | If Favorites is selected, all files and/or folders located in the following location will be backed up: <i>%UserProfile%\Favorites</i> |
| Outlook |  | If Outlook is selected, all files and/or folders located in the following location will be backed up: <i>%UserProfile%\AppData\Local\Microsoft\Outlook</i> |
| Windows Live Mail |  | If Windows Live Mail is selected, all files and/or folders located in the following location will be backed up: <i>%UserProfile%\AppData\Local\Microsoft\Windows Live Mail</i> |

To select files and/or folder to back up using the Quick or Shortcut option, follow the steps below:

1. Select a backup source.

Backup Source

Select the files and folders that you want to backup

 Desktop

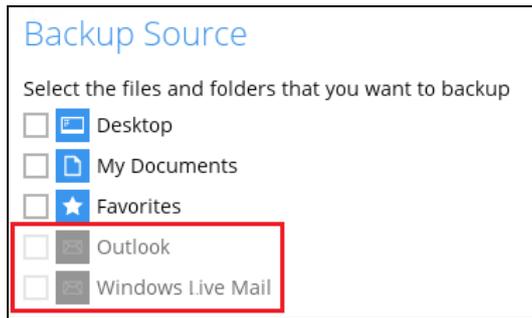
 My Documents

 Favorites

 Outlook

 Windows Live Mail

2. The Outlook and Windows Live Mail will be disabled if they were not installed on the machine.



3. Click the [Save] button to store the selected backup source.

Option 2: Filter

The Filter Backup Source is an alternative way to select a backup source which does not require Windows User Authentication login password even if the backup schedule is enabled unless the filter backup source is located on a network drive.

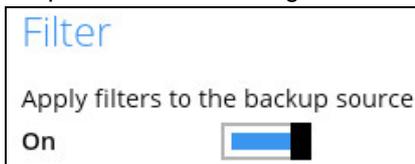


The following options in the filter backup source does not require Windows User Authentication login password:

| | |
|----------------------|--|
| All hard disk drives | Apply this filter to all files/folders in <input type="radio"/> All hard disk drives |
| Specific folder | <input checked="" type="radio"/> This folder only (Input local / network address or click [Change]) <input type="text"/> <input type="button" value="Change"/> <input type="checkbox"/> This share requires access credentials |

To select files and/or folders to back up using the Filter Backup Source, follow the steps below:

1. Swipe the lever to the right to turn on the filter setting.



2. Click the [Add] button to create filter.

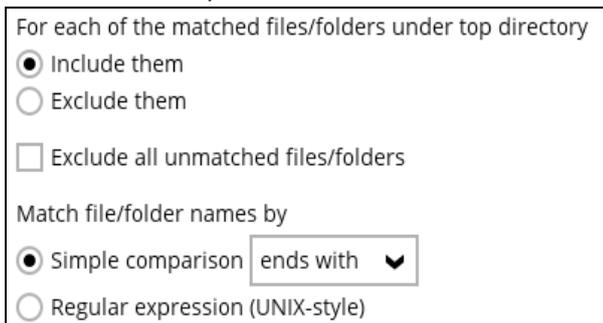


3. Assign a desired name to the backup filter.



The screenshot shows a dialog box titled "New Backup Filter". It has a "Name" label and a text input field containing "Filter-1".

4. Select from the options below.



The screenshot shows a dialog box with the following options:
For each of the matched files/folders under top directory
 Include them
 Exclude them
 Exclude all unmatched files/folders
Match file/folder names by
 Simple comparison
 Regular expression (UNIX-style)

- In this example, all files and/or folders that end with the letter 'X' will be included to the backup job. You can add multiple patterns here.

Existing patterns to match

- Select whether you would like to apply the filter to all files and/or folders in all hard disk drives or to a specific folder only. If 'This folder only' is selected, click the [Change] button to select the specific folder or input the local / network address that you would like to apply the filter to.

Apply this filter to all files/folders in

All hard disk drives

This folder only (Input local / network address or click [Change])

This share requires access credentials

Apply to

File Folder

- If 'This share requires access credentials' is checked, enter the User name and Password of the local or network drive. This checkbox will only be enabled if a local or network address is detected.

This share requires access credentials

User name (e.g. domain\username)

Password

- Click the [OK] button to save the created filter, then click the [Save] button to save the settings. Once you run a backup, all files and/or folders that match the applied filter will be backed up.
- Multiple backup filters can be created by clicking the [Add] button.

Existing filters

 **Filter-1**
/Users/admin/Desktop

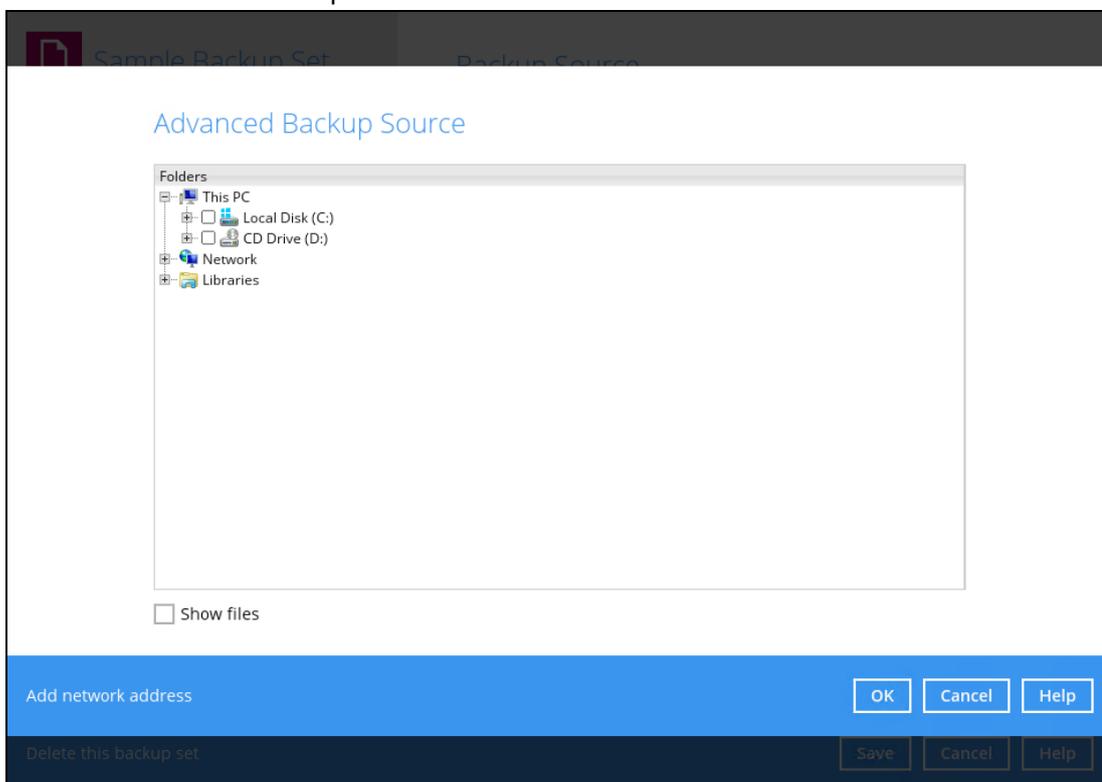
 **Filter-2**
/Users/admin/Documents

NOTE

For more details about backup source file filtering, please refer to **Chapter 4.1 Create a backup set with filter** in the [DCS Online Backup Manager v8 Backup Source File Filter Guide](#).

Option 3: Advanced Backup Source

The Advanced Backup Source is another way to select a backup source which does not require Windows User Authentication login password even if the backup schedule is enabled unless the advanced backup source is located on a network drive.



The following table shows the list of options in the Advanced Backup Source which require and does not require Windows User Authentication login password:

| Advanced Backup Source | | Description |
|------------------------|---|---|
| Local Disk |  | Does not require Windows User Authentication login password. |
| Network drive |  | Requires Windows User Authentication login password. For network drive/s, you will need to enter the login credentials which has permission to access network resources in order to back up selected files and/or folders. |
| Libraries |  | Does not require Windows User Authentication login password. NOTE: This type of backup source may not be supported on other versions of Windows. This feature is not supported on: Windows 10 Windows 8.1 |

| | | |
|----------------------------|---|--|
| | | <p>Windows 8 and Windows Server 2012 R2</p> <p>Supported on:</p> <p>Windows 7</p> <p>Windows Server 2016 and Windows Server 2008 R2</p> |
| Add network address |  | Requires Windows User Authentication login password. For network drive/s, you will need to enter the login credentials which has permission to access network resources in order to back up selected files and/or folders. |

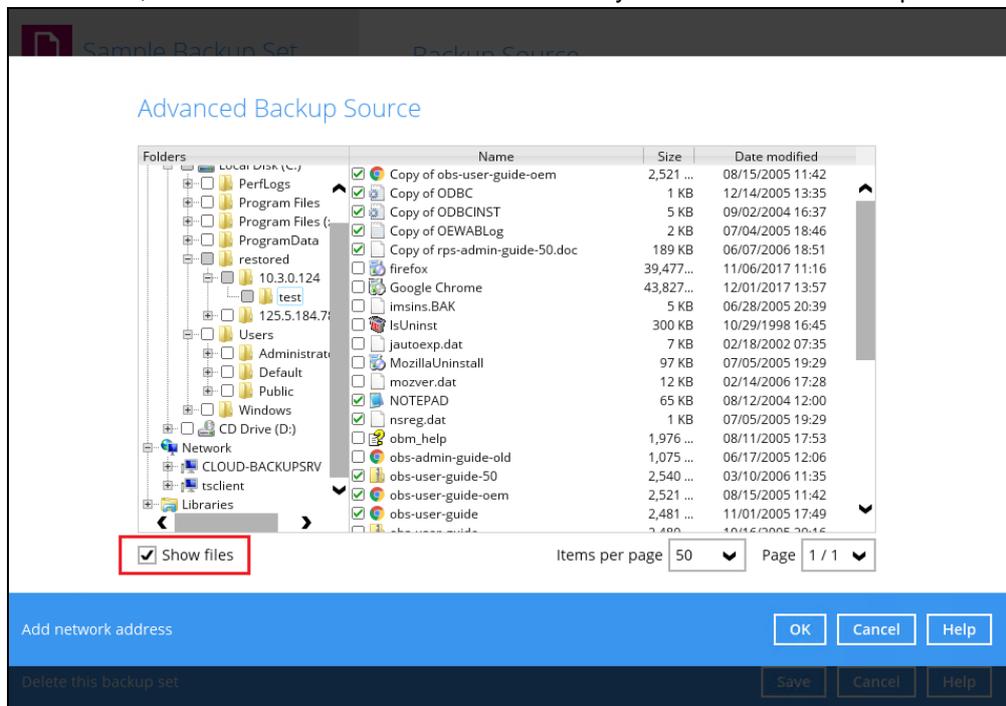
To select files and/or folders using the Advanced Backup Source, follow the steps below:

1. In the Source window, select 'I would like to choose the files to backup'.



2. There are two (2) ways to select files and/or folders, one is when the files and/or folders are located in the local machine and another way is when the files and/or folders are located in the network.

- In the Advanced Backup Source window, select 'Show files' to display the files inside each folder, then select the files and/or folders that you would like to back up.



- 1 If the files and/or folders are located in a network drive, click the 'Add network address' link. Enter the network address.

Network Address

Input the details of network address, and click [OK] to proceed.

Network address (e.g. \\servername.domain\path)

This share requires access credentials

If access credentials are required to access the network, then check the "This share requires access credentials" checkbox. The checkbox will only be enabled once the network address is entered. Enter the User name and Password of the network drive and click the [OK] button.

This share requires access credentials

User name (e.g. domain\username)

Password

By default all the files inside the folder in the network drive is selected for backup. But there is still an option to deselect files that you do not want to be included in the backup.

Advanced Backup Source

| Folders | Name | Size | Date modified |
|---|---|------------------|------------------|
| This PC | <input checked="" type="checkbox"/> AhsayACB_UserGuideforWindows_versi... | 15 KB | 07/10/2018 17:24 |
| | <input checked="" type="checkbox"/> AhsayCBS_version7_UserGuide | 15 KB | 07/10/2018 17:24 |
| | <input checked="" type="checkbox"/> AhsayCloudFileBackupSolution_v10.pptx | 39 KB | 03/18/2019 15:06 |
| | <input checked="" type="checkbox"/> AhsayCloudFileBackupSolution_v7.pptx | 39 KB | 03/18/2019 15:06 |
| | <input checked="" type="checkbox"/> AhsayCloudFileBackupSolution_v8.pptx | 39 KB | 03/18/2019 15:06 |
| | <input checked="" type="checkbox"/> AhsayCloudFileBackupSolution_v9.pptx | 39 KB | 03/18/2019 15:06 |
| | <input checked="" type="checkbox"/> AhsayOBM_version7_QuickStartGuide | 15 KB | 07/10/2018 17:24 |
| | <input checked="" type="checkbox"/> AlertMessageFive | 3 KB | 02/28/2019 12:10 |
| | <input checked="" type="checkbox"/> AlertMessageFour | 3 KB | 02/28/2019 12:10 |
| | <input checked="" type="checkbox"/> AlertMessageOne | 3 KB | 02/28/2019 12:10 |
| <input checked="" type="checkbox"/> AlertMessageThree | 3 KB | 02/28/2019 12:10 | |
| <input checked="" type="checkbox"/> AlertMessageTwo | 3 KB | 02/28/2019 12:10 | |
| Network | <input checked="" type="checkbox"/> BackupSet_2015 | 15 KB | 07/10/2018 17:24 |
| | <input checked="" type="checkbox"/> BackupSet_2016 | 15 KB | 07/10/2018 17:24 |
| | <input checked="" type="checkbox"/> BackupSet_2017 | 15 KB | 07/10/2018 17:24 |
| | <input checked="" type="checkbox"/> BackupSet_2018 | 15 KB | 07/10/2018 17:24 |
| | <input checked="" type="checkbox"/> BackupSet_2019 | 15 KB | 07/10/2018 17:24 |
| | <input checked="" type="checkbox"/> BackupSolution | 8 KB | 12/17/2018 14:27 |
| | <input checked="" type="checkbox"/> File snapshot testing | 8 KB | 12/17/2018 14:27 |
| | <input checked="" type="checkbox"/> File snapshot testing1 | 8 KB | 01/15/2019 10:12 |
| | <input checked="" type="checkbox"/> File snapshot testing2 | 8 KB | 01/15/2019 10:12 |
| | <input checked="" type="checkbox"/> File snapshot testing3 | 8 KB | 01/15/2019 10:12 |

Show files Items per page 50 Page 1 / 1

Add network address

Delete this backup set

NOTE

- There must be a specific folder that is shared in the network drive that will be entered in the network address e.g. \\125.5.184.23\Share
- Temporary folders location are not supported for individual login credentials but can still be setup separately using existing Windows User Authentication login.

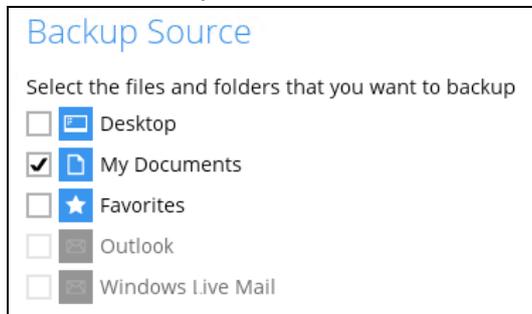
3. Click the [OK] button to save the selection, then click the [Save] button to store settings.

In selecting files and/or folders to back up, the three (3) options can be used simultaneously. For more details, please refer to the example scenarios below:

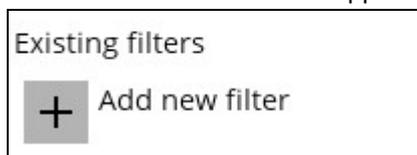
Scenario 1 (Quick or Shortcut + Filter)

You can use the quick or shortcut option and apply filter to the selected backup source at the same time. To use this type of combination, follow the steps below:

1. Choose a backup source.



2. Create a filter which will be applied to the backup source.



New Backup Filter

Name
Filter-1

For each of the matched files/folders under top directory

- Include them
- Exclude them

Exclude all unmatched files/folders

Match file/folder names by

- Simple comparison ends with ▼
- Regular expression (UNIX-style)

Existing patterns to match

X

Add

Apply this filter to all files/folders in

- All hard disk drives
- This folder only (Input local / network address or click [Change])

OK Cancel Help

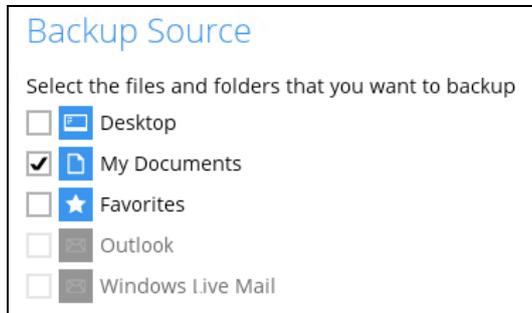
Delete this backup set Save Cancel Help

3. Click the [OK] button to save the created filter, then click the [Save] button to store settings.

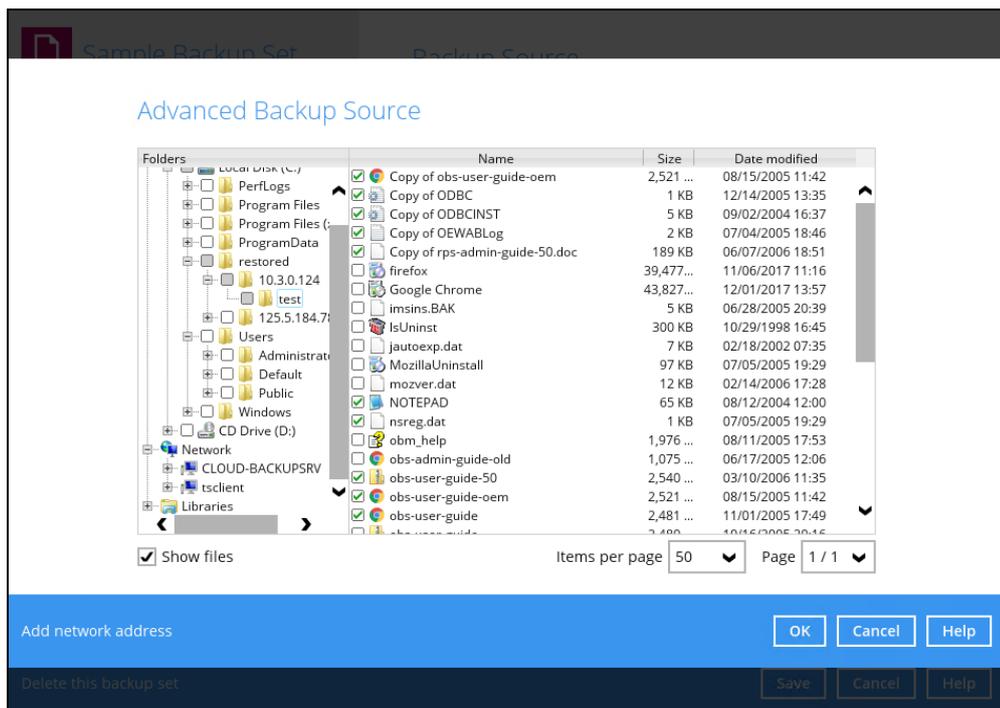
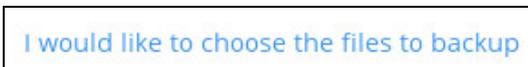
Scenario 2 (Quick or Shortcut + Advanced Backup Source)

You can use the quick or shortcut option and select files and/or folders in the advanced backup source at the same time. To use this type of combination, follow the steps below:

1. Choose a backup source.



2. In the source window, click 'I would like to choose the files to backup' and select the files and/or folders that you would like to back up. Or click 'Add network address' to backup files and/or folders located in a network drive.

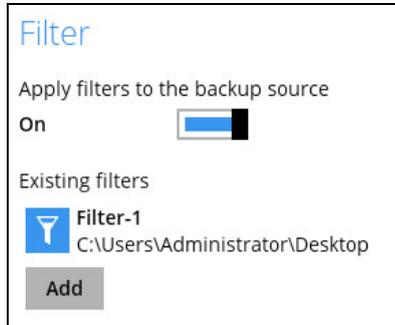


3. Click the [OK] button to save the selection, then click the [Save] button to save settings.

Scenario 3 (Filter + Advanced Backup Source)

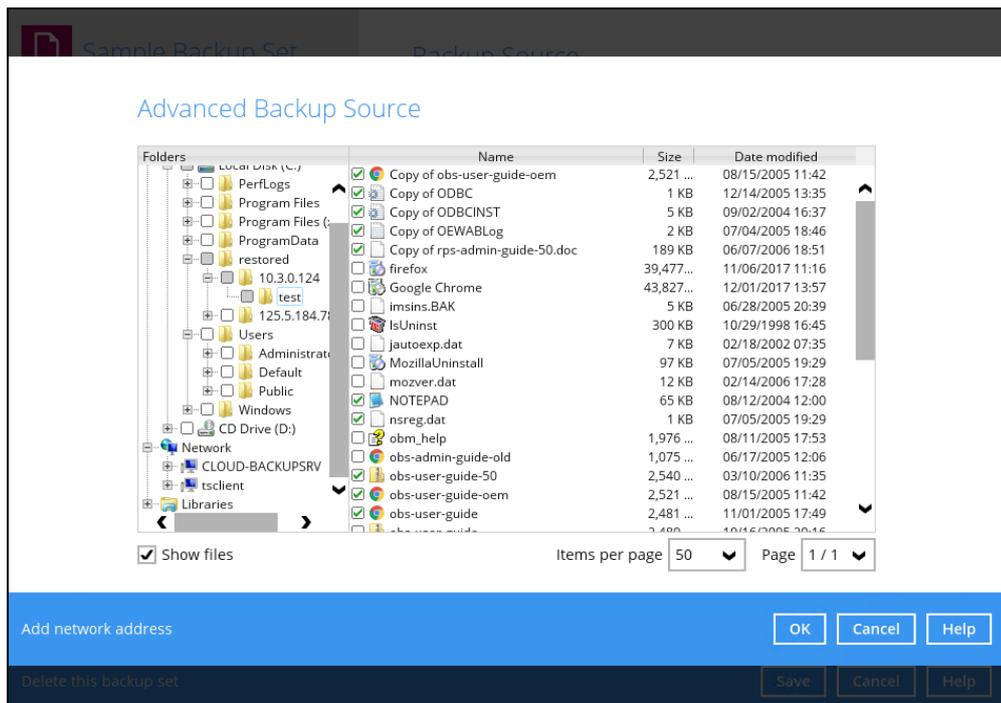
You can use the filter backup source and select files and/or folders in the advanced backup source source at the same time. To use this type of combination, follow the steps below:

1. Create a filter.



2. In the source window, click 'I would like to choose the files to backup' and select the files and/or folders that you would like to back up. Or click 'Add network address' to backup files and/or folders located in a network drive.

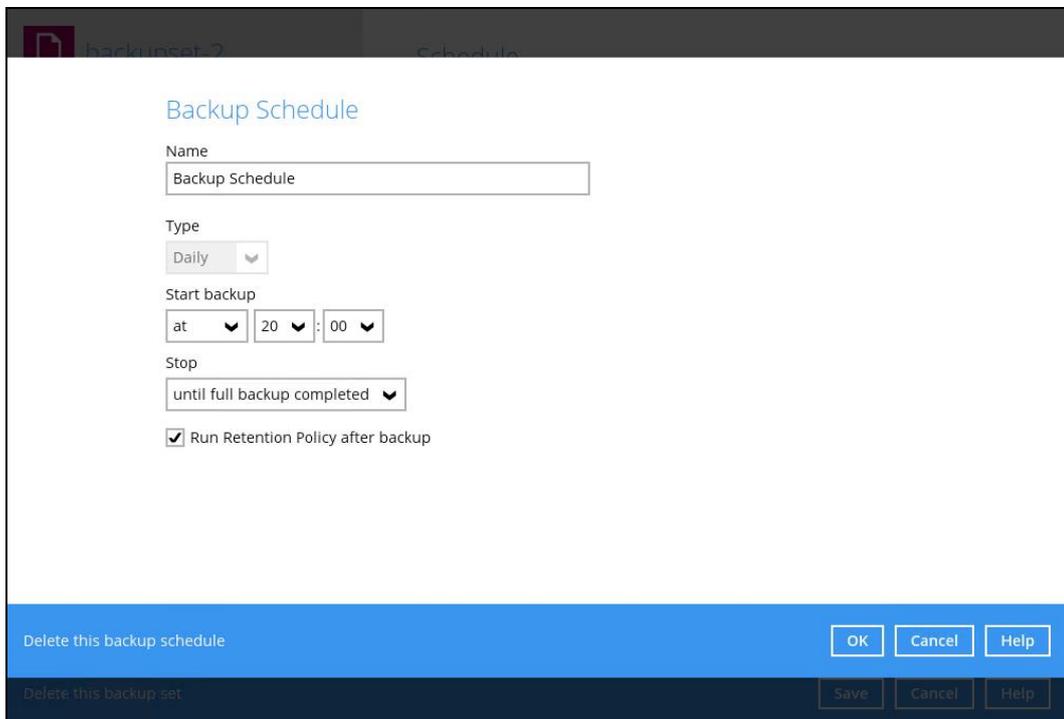
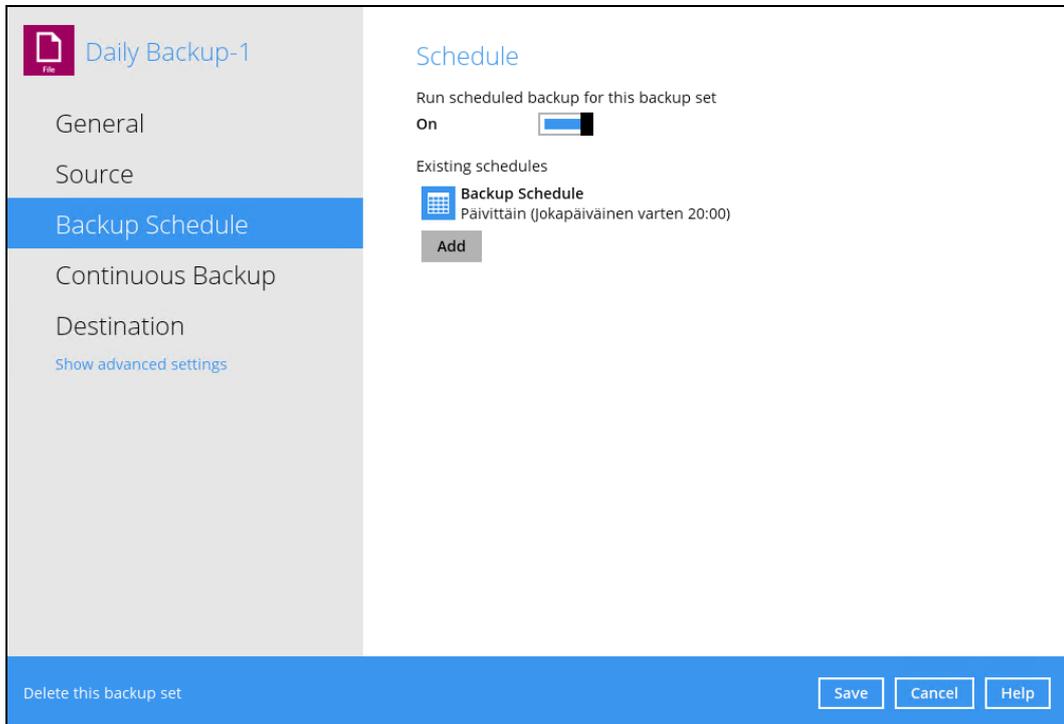
I would like to choose the files to backup



3. Click the [OK] button to save the selection, then click the [Save] button to store settings.

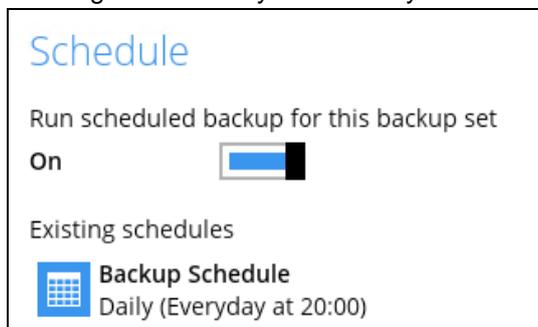
Backup Schedule

This feature allows the user to assign a backup schedule for the backup job to run automatically.

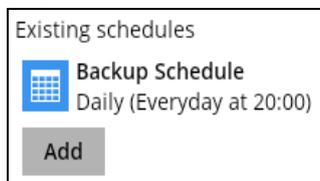


To configure a backup schedule, follow the steps below:

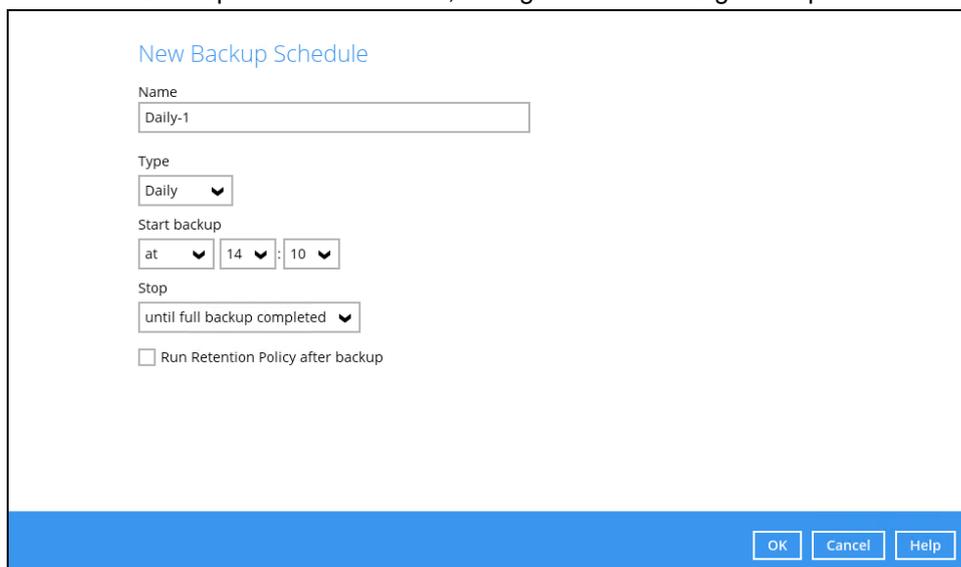
1. Swipe the lever to the right to turn on the backup schedule setting. The backup schedule is configured as “Daily at 20:00” by default.



2. Select an existing backup schedule to modify or click the [Add] button to create a new one.



3. In the New Backup Schedule window, configure the following backup schedule settings.



- **Name** – the name of the backup schedule.
- **Type** – the type of backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom.

- ⦿ **Daily** – the time of the day or interval in minutes/hours when the backup job will run.

New Backup Schedule

Name

Type

Start backup
 at :

Stop

Run Retention Policy after backup

- ⦿ **Weekly** – the day of the week and the time of the day or interval in minutes/hours when the backup job will run.

New Backup Schedule

Name

Type

Backup on these days of the week
 Sun Mon Tue Wed Thu Fri Sat

Start backup
 at :

Stop

Run Retention Policy after backup

- ⦿ **Monthly** – the day of the month and the time of that day which the backup job will run.

New Backup Schedule

Name

Type

Backup on the following day every month
 Day
 First

Start backup at
 : on the selected days

Stop

Run Retention Policy after backup

- **Custom** – a specific date and the time of that date when the backup job will run.

New Backup Schedule

Name: Custom-1

Type: Custom

Backup on the following day once: 2019 December 31

Start backup at: 23 : 59

Stop: until full backup completed

Run Retention Policy after backup

- **Start backup** – the start time of the backup job.
 - **at** – this option will start a backup job at a specific time.
 - **every** – this option will start a backup job in intervals of minutes or hours.

Start backup: every 1 minute

Stop: until full backup completed

Run Retention Policy after backup

Start backup: every 1 minute

Stop: until full backup completed

Run Retention Policy after backup

Here is an example of a backup set that has a periodic and normal backup schedule.

New Backup Schedule

Name: Weekly-1

Type: Weekly

Backup on these days of the week: Sun Mon Tue Wed Thu Fri Sat

Start backup: every 4 hours

Stop: until full backup completed

Run Retention Policy after backup

Figure 1.1

New Backup Schedule

Name: Weekly-2

Type: Weekly

Backup on these days of the week: Sun Mon Tue Wed Thu Fri Sat

Start backup: at 21 : 00

Stop: until full backup completed

Run Retention Policy after backup

Figure 1.2

Figure 1.1 – Periodic backup schedule runs every 4 hours from Monday – Friday during business hours

Figure 1.2 – Normal backup schedule runs at 21:00 or 9:00 PM on Saturday and Sunday on weekend non-business hours

- **Stop** – the stop time of the backup job. This only applies to schedules with start backup “at” and is not supported for periodic backup schedule (start backup “every”)
 - **until full backup completed** – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.
 - **after (defined no. of hrs.)** – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

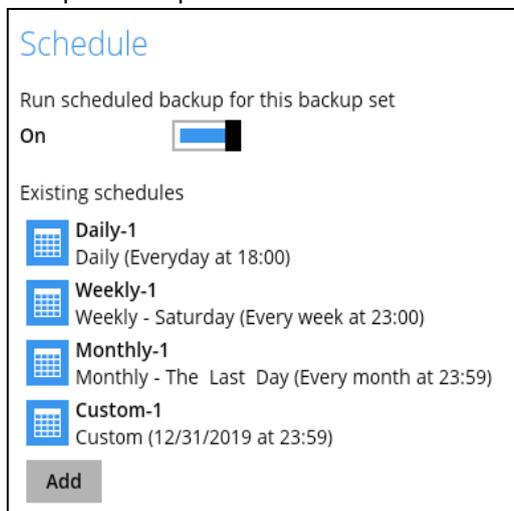
The number of hours must be enough to complete a backup of all files in the backup set. For small files in a backup, if the number of hours is not enough to back up all files, then the outstanding files will be backed up in the next backup job. However, if the backup set contains large files, this may result in partially backed up files.

For example, if a backup has 100GB file size which will take approximately 15 hours to complete on your environment, but you set the “stop” after 10 hours, the file will be partially backed up and cannot be restored. The next backup will upload the files from scratch again.

The partially backed up data will have to be removed by running the [Data Integrity Check](#).

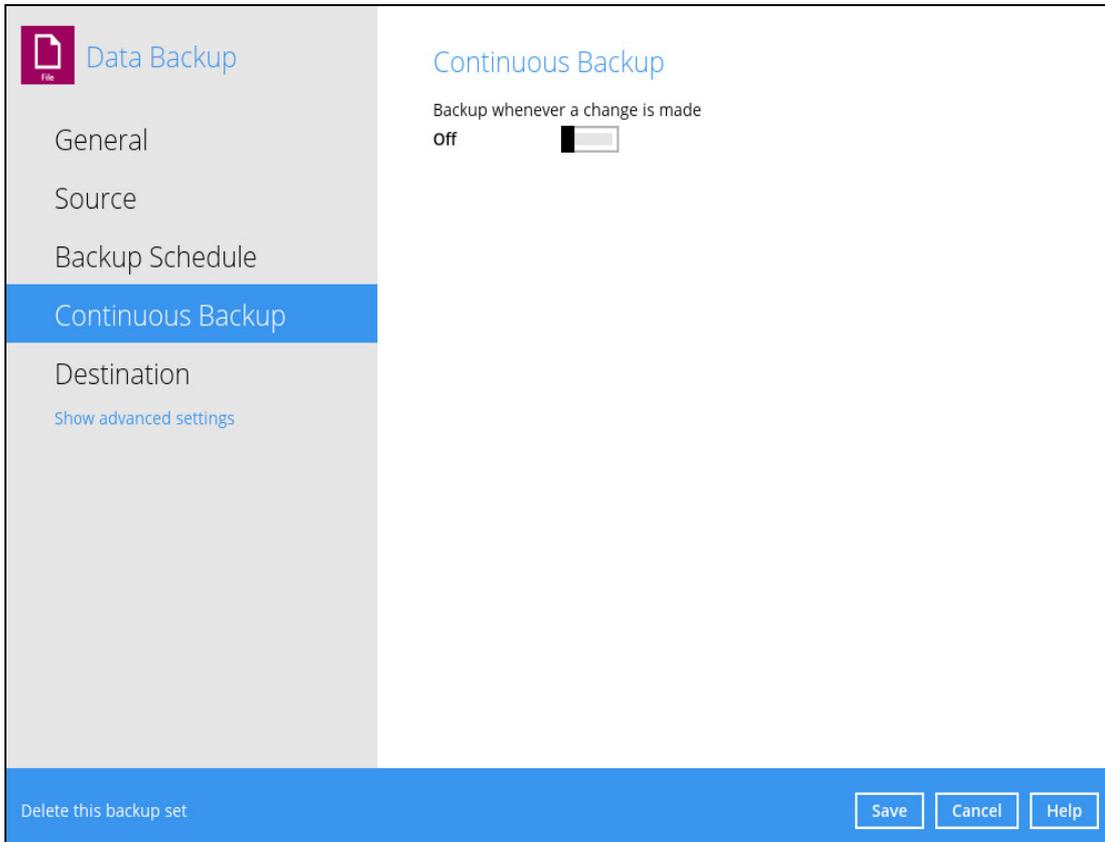
As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.

- **Run Retention Policy after backup** – if enabled, the OBM will run a retention policy job to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job.
4. Click the [OK] button to save the configured backup schedule settings.
 5. Click the [Save] button to save settings.
 6. Multiple backup schedules can be created.



Continuous Backup

This feature provides backup for selective data whenever a change is made. This feature is disabled by default.

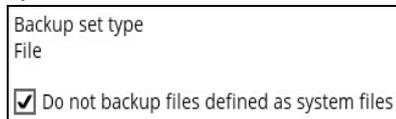


To enable the continuous backup, follow the steps below:

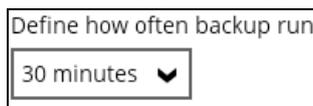
1. Swipe the lever to the right to turn on the continuous backup setting.



2. It is recommended to select this option to avoid backing up files that are marked as system files.



3. Define how often the continuous backup job will run. The backup time interval can be set from 1 minute to 12 hours.



- This applies the continuous backup on small regular update files. The file size can range from 25MB to unlimited MB.

Only apply to files smaller than
4096 MB

NOTE

For large file size, the continuous backup may not run with a short time interval. You may need to adjust the continuous backup time interval (in step 3).

- This allows the user to create an exclude filter to exclude files and/or folders from the backup job. Click the [Add] button to create an exclude filter.

Exclude Filter

Existing Exclude Filters

+ Add new exclude filter

- If an exclude filter is created, click the [OK] button to save the created exclude filter, then click the [Save] button to save the configured continuous backup settings.

NOTE

Only File backup sets on Windows operating system will support Continuous Backup Schedule on v8.3.4.0 (or above)

All v7 and pre-v8.3.4.0 Windows non-File backup sets with Continuous Backup Schedules will be automatically converted to periodic backup schedules after upgrading to v8.3.4.0 (or above)

Destination

This feature allows the user to select a backup mode and add an additional storage destination.

There are two (2) different types of backup mode:

| Backup mode | Description |
|-------------------|--|
| Sequential | This is the configured backup mode by default. This backup mode will run a backup job to each backup destination one by one. |
| Concurrent | This backup mode will run a backup job to all backup destinations simultaneously. |

Comparison between Sequential and Concurrent Backup mode

| Backup mode | Pros | Cons |
|-------------------|--|--|
| Sequential | <ul style="list-style-type: none"> ➤ Takes less resources in the local machine (e.g., memory, CPU, bandwidth, etc.) to complete a backup job. | <ul style="list-style-type: none"> ➤ Backup job is slower than in concurrent mode since the backup job will upload the backup data to the selected backup destinations one at a time. |
| Concurrent | <ul style="list-style-type: none"> ➤ Backup job is faster than in Sequential mode. ➤ Maximum number of concurrent backup destinations can be | <ul style="list-style-type: none"> ➤ Requires more resources in the local machine (e.g. memory, CPU, bandwidth, etc.) to complete a backup job. |

| | | |
|--|-------------|--|
| | configured. | |
|--|-------------|--|

To modify the backup mode, follow the steps below:

1. Go to Backup Sets, then choose a backup set.
2. Select the [Destination] tab in the backup set settings.
3. Click the drop-down button to select a backup mode.

Destination

Backup mode

Sequential ▼

4. If “Concurrent” is selected, click the drop-down button to select the no. of maximum concurrent backup destination.

Maximum concurrent backup destinations

2 ▼

5. Click the [Save] button to save the selected backup mode.

To add a new storage destination, follow the steps below:

1. Click the [Add] button.

Existing storage destinations

DCS Backup CBS

Add

^
v

2. Click the drop-down button to select a backup destination.

New Storage Destination / Destination Pool

Name

DCS Backup CBS

Destination storage

DCS Backup CBS ▼

DCS Backup CBS

Local / Mapped Drive / Network Drive / Removable Drive

3. If the Local / Mapped Drive / Network Drive / Removable Drive is selected, click the [Change] button to select a new storage destination or input the local or network address. Check 'This share requires access credentials' if required then click the [Test] button to validate access to it.

The screenshot shows a dialog box titled "Destination storage". At the top, there is a dropdown menu with the text "Local / Mapped Drive / Network Drive / Removable Drive". Below this is a text input field labeled "Path (Input local / network address or click [Change])" containing the text "\\10.3.0.124\test", with a "Change" button to its right. A checkbox labeled "This share requires access credentials" is checked. Below the checkbox is a text input field for "User name (e.g. domain/username)" containing the text "admin". Another text input field for "Password" contains several dots. At the bottom left of the dialog is a "Test" button.

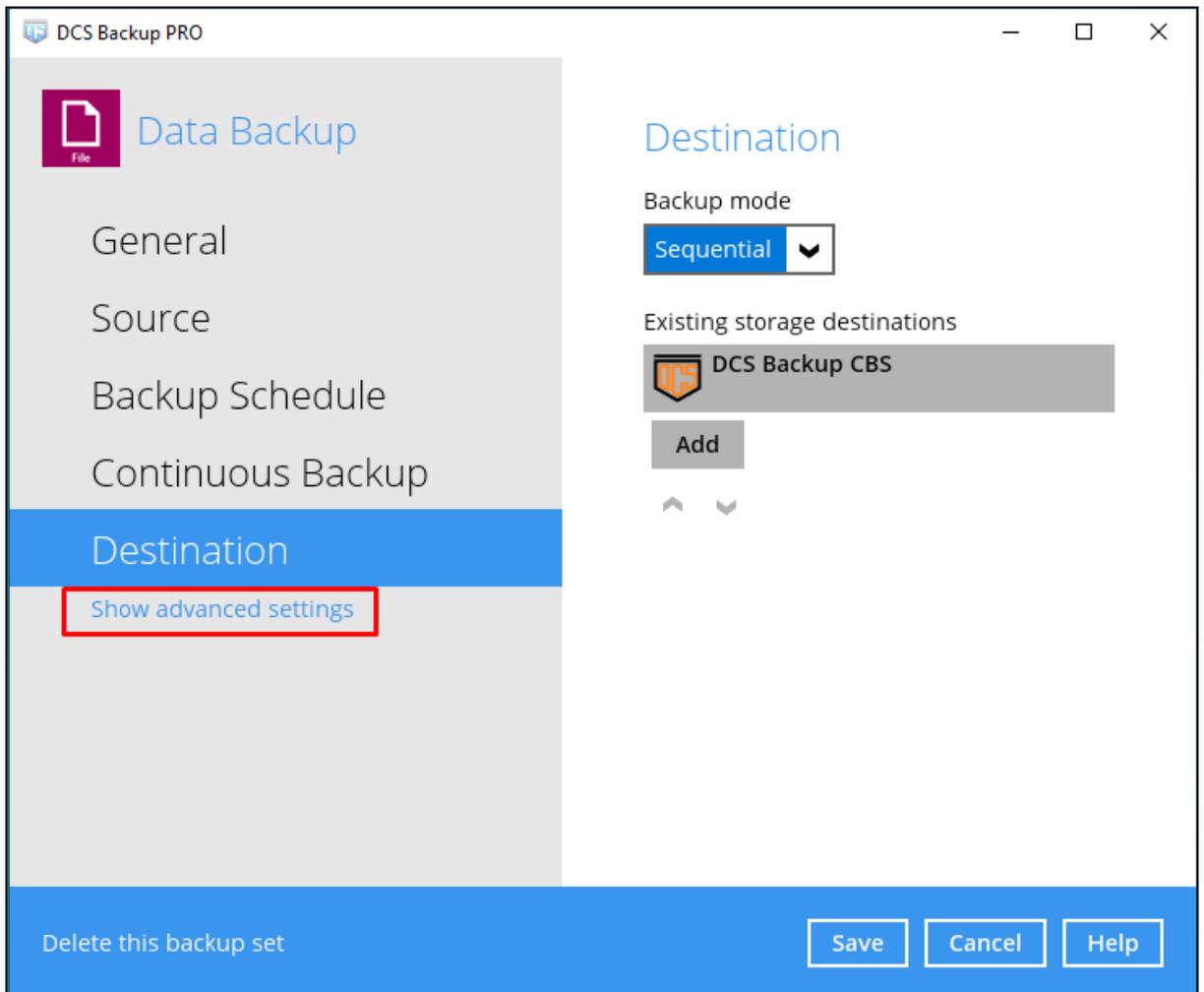
4. If there is an added storage destination, click the [OK] button to save the added one. Then click the [Save] button to save the updated backup mode and the added storage destination.

NOTE

The error below will appear if 'This share requires access credentials' is not checked and access credentials are setup in the storage destination.

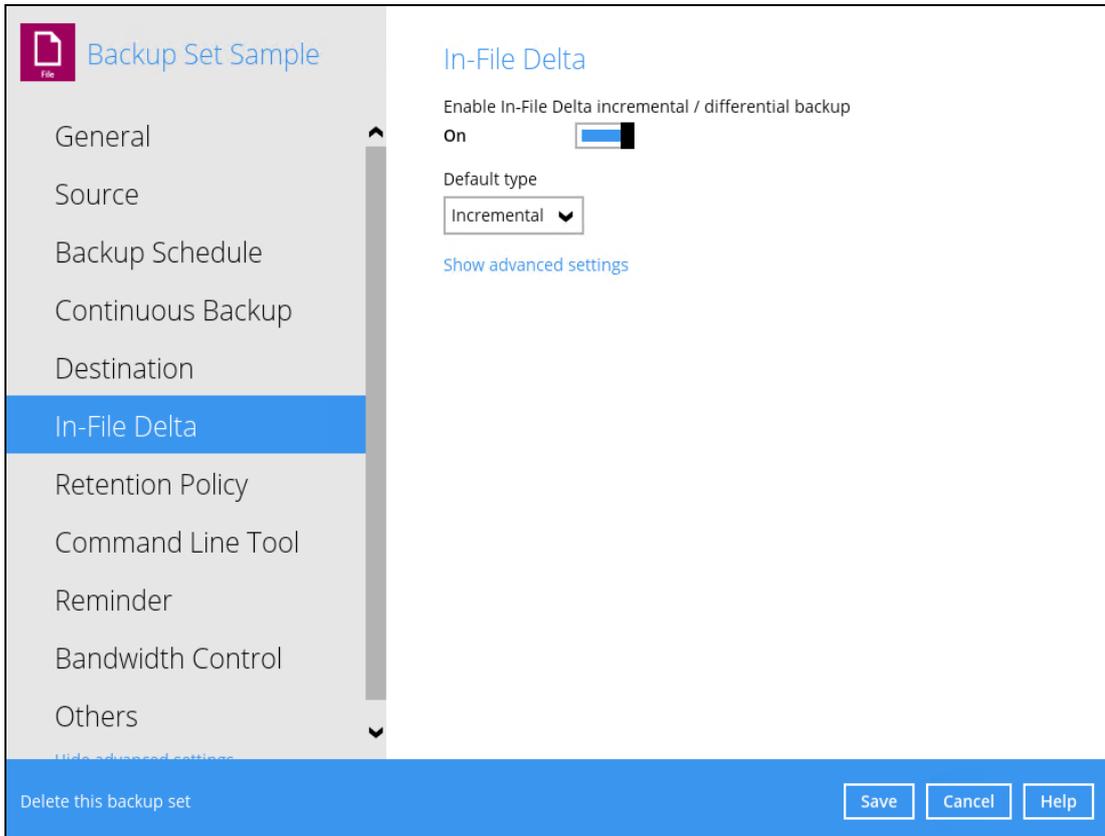
The screenshot shows an error message dialog box with a blue background. On the left side, there is a red circle with a white 'X' icon. To the right of the icon, the text reads "[Exception] Access is denied due to invalid credentials". In the bottom right corner of the dialog, there is an "OK" button.

Select **Show advanced settings** to modify the In-File Delta, Retention Policy, Command Line Tool, Reminder, Bandwidth Control, and other configurable items.



In-File Delta

In-file delta technology is an advanced data block matching algorithm which is capable to pick up the changes (delta) of file content between two files.



There are two (2) default types of In-File Delta:

| In-File Delta Type | Description |
|---------------------|---|
| Differential | The delta is generated by comparing with the last uploaded full file only. Delta generated with this method will grow daily and uses more bandwidth. |
| Incremental | This is the configured In-file delta by default. The delta is generated by comparing with the last uploaded full of delta file. Delta generated with this method is smaller and uses the least bandwidth. |

Comparison between Incremental and Differential In-File Delta

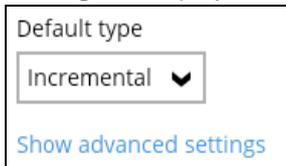
| In-File Delta Type | Pros | Cons |
|---------------------|--|--|
| Differential | <ul style="list-style-type: none"> ➤ Backup speed is faster than Full backup. ➤ Restoration is faster than data backup with Incremental In-File Delta. <p>Less storage space is need than a Full backup.</p> | <ul style="list-style-type: none"> ➤ Backup process is slower than Incremental In-File Delta backup. ➤ Restoration is slower than data backup with Full backup. |
| Incremental | <ul style="list-style-type: none"> ➤ Backup process is fastest among all three (3) types; Full, Differential, and Incremental ➤ Least storage space is required. | <ul style="list-style-type: none"> ➤ Restoration is slowest among all three (3) types; Full, Differential, and Incremental. ➤ For restoration, the full file and all deltas that does not chain up to the required point-in-time may result to broken delta chain. |

To configure the In-File Delta settings, follow the steps below:

1. Swipe the lever to the right to enable the In-File Delta.



2. Click the drop-down button to choose an In-File Delta type, then click **Show advanced settings** to display all configurable items.



3. Click the drop-down button to specify the In-File Delta block size. This is configured as "Auto" by default.



4. Click the drop-down button to select how much of the file size (MB) the In-File Delta logic will apply to. By default, the In-File Delta logic is configured to apply to files larger than 25 MB.



- A full file will be uploaded when either of these conditions is met. This setting can also be configured.

Upload full file when either of these conditions is met

Number of deltas is over

Delta ratio (delta file size / full file size) is over

Failed to generate delta file

- This allows the user to configure a different In-File Delta setting to override the default In-File Delta.

- Weekly variations** – for example, you set Sunday to perform a full backup, for the rest of the week, a backup based on the default In-File Delta will be run.

Weekly variations for overriding default type

| | | | |
|------------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|
| <input type="checkbox"/> Sunday | <input type="text" value="Full"/> | <input type="checkbox"/> Thursday | <input type="text" value="Full"/> |
| <input type="checkbox"/> Monday | <input type="text" value="Full"/> | <input type="checkbox"/> Friday | <input type="text" value="Full"/> |
| <input type="checkbox"/> Tuesday | <input type="text" value="Full"/> | <input type="checkbox"/> Saturday | <input type="text" value="Full"/> |
| <input type="checkbox"/> Wednesday | <input type="text" value="Full"/> | | |

- Yearly variations** – for example, you set a particular day in January to perform a full backup, for the rest of the year, a backup based on the default In-File Delta will be run.

Yearly variations for overriding default type and weekly variations

| | | | |
|-----------------------------------|-----------------------------------|------------------------------------|-----------------------------------|
| <input type="checkbox"/> January | <input type="text" value="Full"/> | <input type="checkbox"/> July | <input type="text" value="Full"/> |
| <input type="checkbox"/> February | <input type="text" value="Full"/> | <input type="checkbox"/> August | <input type="text" value="Full"/> |
| <input type="checkbox"/> March | <input type="text" value="Full"/> | <input type="checkbox"/> September | <input type="text" value="Full"/> |
| <input type="checkbox"/> April | <input type="text" value="Full"/> | <input type="checkbox"/> October | <input type="text" value="Full"/> |
| <input type="checkbox"/> May | <input type="text" value="Full"/> | <input type="checkbox"/> November | <input type="text" value="Full"/> |
| <input type="checkbox"/> June | <input type="text" value="Full"/> | <input type="checkbox"/> December | <input type="text" value="Full"/> |

This allows the user to specify which day of the selected months in yearly variations the backup job will be run. (e.g., First of January, March, May...)

Day of the selected months in yearly variations

Day

First

- Click the [Save] button to save the modified In-File Delta settings.

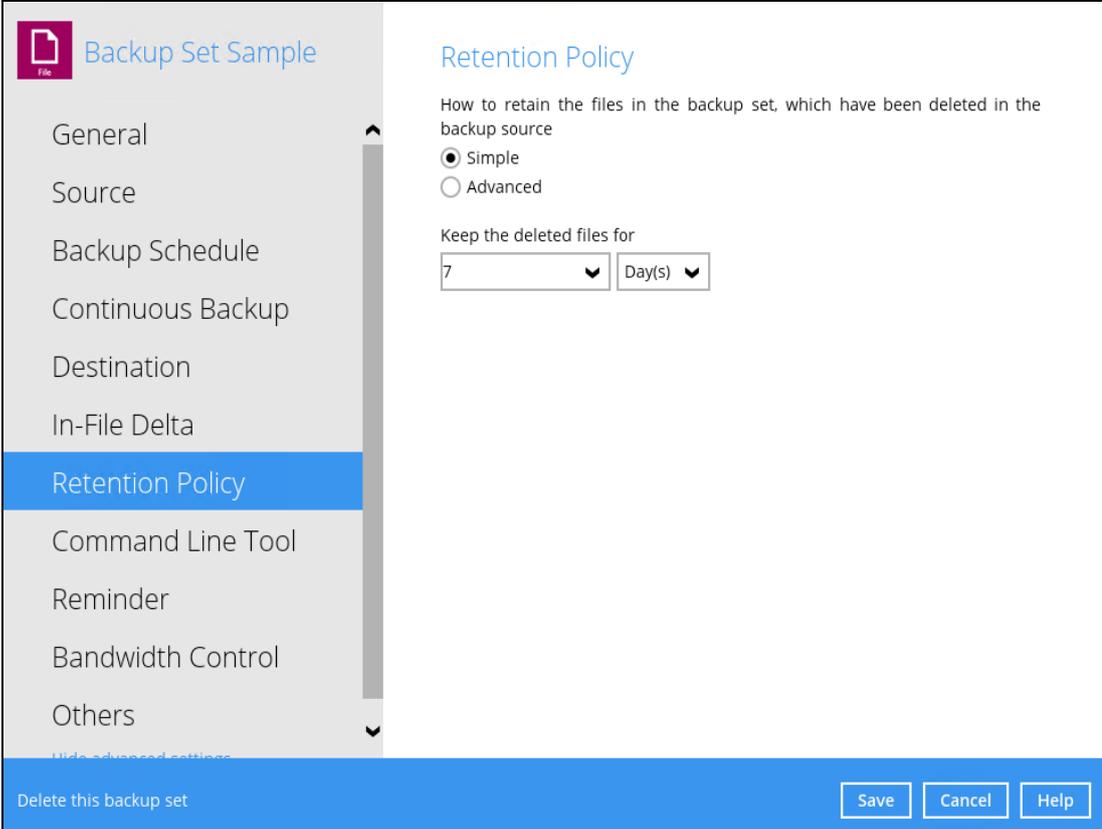
Retention Policy

When the OBM identifies files and/or folders that are deleted, updated, or with updated permission/attributes during a backup job, these files and/or folders will then be moved from the data area to the Retention area.

Retention area is a place used as a temporary destination to store these files (deleted, updated, or with updated permission/attributes during a backup job). Files and/or folders in the retention area can still be restored.

The **Retention Policy** is used to control how long these files remain in the retention area when they are removed which can be specified in the number of days, weeks, months, or backup jobs. Retained data within all backup destinations (e.g., DCS CBS, local drive, SFTP/FTP, and cloud storage) are cleared by the retention policy job.

The default Retention Policy setting for a File Backup Set is 7 days, but the appropriate Retention Policy setting depends on individual, contractual, or regulatory requirements.



The screenshot shows a configuration window titled "Backup Set Sample" with a sidebar menu on the left. The "Retention Policy" option is selected and highlighted in blue. The main content area is titled "Retention Policy" and contains the following settings:

- How to retain the files in the backup set, which have been deleted in the backup source:
 - Simple
 - Advanced
- Keep the deleted files for:
 - 7 (selected in a dropdown menu)
 - Day(s) (selected in a dropdown menu)

At the bottom of the window, there is a blue bar with the text "Delete this backup set" on the left and three buttons: "Save", "Cancel", and "Help" on the right.

NOTE

There is a trade-off between the retention policy and backup destination storage usage. The higher the retention policy setting, the more storage is used, which translates into higher storage costs.

There are two (2) different types of Retention Policy:

| Type | Description |
|-----------------|---|
| Simple | A simple retention policy is a basic policy where the retained files (in the retention area) are removed automatically after the user specifies the number of days or backup jobs. |
| Advanced | An advanced retention policy defines a more advanced and flexible policy where the retained files (in the retention area) are removed automatically after a combination of user defined policy. |

Comparison between Simple and Advanced Retention Policy

| Control | Simple | Advanced |
|--------------------------|--|---|
| Backup Jobs | Can keep the deleted files within 1 to 365 backup job(s) | Not applicable |
| Days | Can keep the deleted files within 1 to 365 day(s) | Can keep the deleted files within 1 to 365 day(s) |
| Type | Not applicable | <ul style="list-style-type: none"> ➤ Daily ➤ Weekly ➤ Monthly ➤ Quarterly ➤ Yearly ➤ Custom |
| User-defined name | Not applicable | Applicable |

WARNING

When files and/or folders in the retention area exceed the Retention Policy setting, they are permanently removed from the backup set and cannot be restored

To configure a **Simple Retention Policy**, follow the steps below:

1. Go to Backup Sets, then select a backup set.
2. Click the [Retention Policy] tab in the Backup Set Settings.
3. Select [Simple] from the options, then click the drop-down button to define the number of day(s) or job(s) which the deleted files will be retained. This is configured as seven (7) days by default.

Retention Policy

How to retain the files in the backup set, which have been deleted in the backup source

Simple
 Advanced

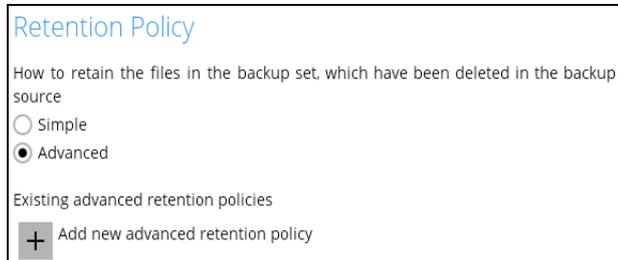
Keep the deleted files for

▼ Day(s) ▼

4. Click the [Save] button to save the configured retention policy settings.

To configure an **Advanced Retention Policy**, follow the steps below:

1. Go to Backup Sets, then select a backup set.
2. Click the [Retention Policy] tab in the Backup Set Settings.
3. Select [Advanced] from the options, then click the [Add] button to create.



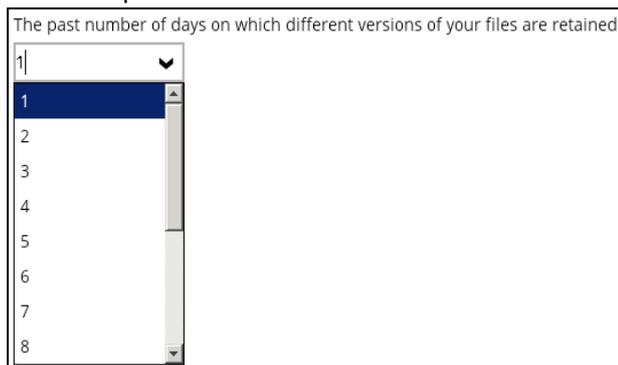
4. Assign a desired name to the retention policy.



5. Click the drop-down button to display the retention type, then select one.



6. Click the drop-down button to specify the period on which the deleted files will be kept in the backup set.



7. Click the [OK] button to save the configured advanced retention policy, then click [Save] to save the settings.

For further details about how to configure an advanced retention policy for each type (Daily, Weekly, Monthly, Quarterly, Yearly), refer to the examples below:

- **Example no. 1:** To keep the retention files for the last seven (7) days:

Name
Daily-1

Type
Daily

The past number of days on which different versions of your files are retained
7

- **Example no. 2:** To keep the retention files for the last four (4) Saturdays:

Name
Weekly-1

Type
Weekly

The days within a week on which different versions of your files are retained
 Sun Mon Tue Wed Thu Fri Sat

The number of weeks to repeat the above selection
4

- **Example no. 3:** To keep the retention files for the 1st day of each month for the last three (3) months:

Name
Monthly-1

Type
Monthly

The day within a month on which different versions of your files are retained
 Day 1
 First Sunday

The number of months to repeat the above selection
3

- **Example no. 4:** To keep the retention files for the 1st day of each quarter for the last four (4) quarters:

Name
Quarterly-1

Type
Quarterly

The day within a quarter on which different versions of your files are retained
 Day 1
 First Sunday

Months of quarter
January, April, July, October

The number of quarters to repeat the above selection
4

- **Example no. 5:** To keep the retention files for the 1st day of each year for the last seven (7) years:

| |
|--|
| Name |
| <input type="text" value="Yearly-1"/> |
| Type |
| <input type="button" value="Yearly"/> |
| The day within a year on which different versions of your files are retained |
| <input checked="" type="radio"/> January |
| <input checked="" type="radio"/> Day 1 |
| <input type="radio"/> First Sunday |
| <input type="radio"/> Sunday of Week 1 |
| The number of years to repeat the above selection |
| <input type="text" value="7"/> |

NOTE
Multiple advanced retention policy can be created.

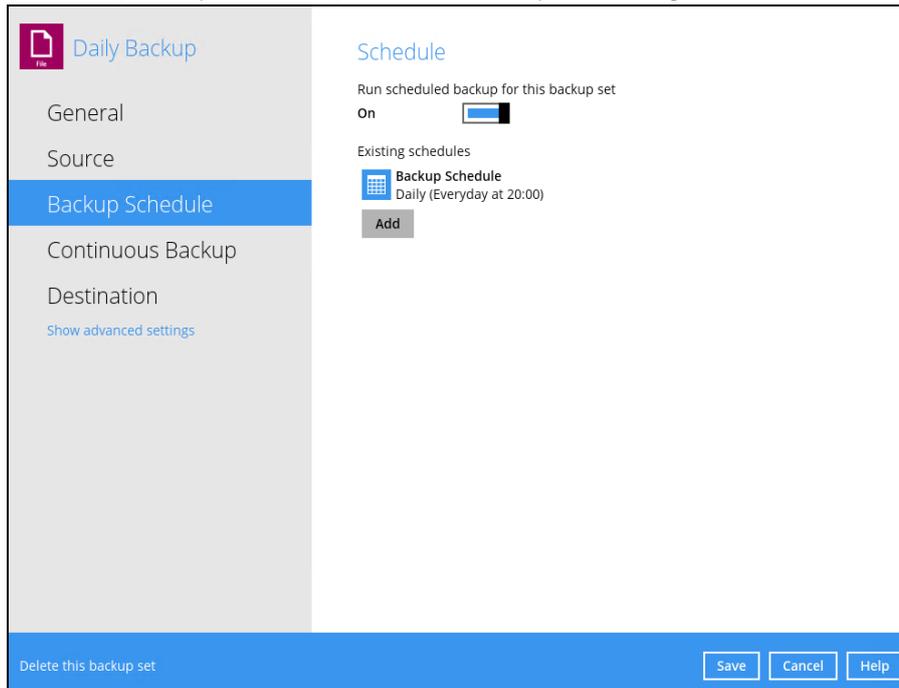
There are three (3) ways to run the Retention Policy:

- Backup Scheduler
- Manual Backup
- Space Freeing Up

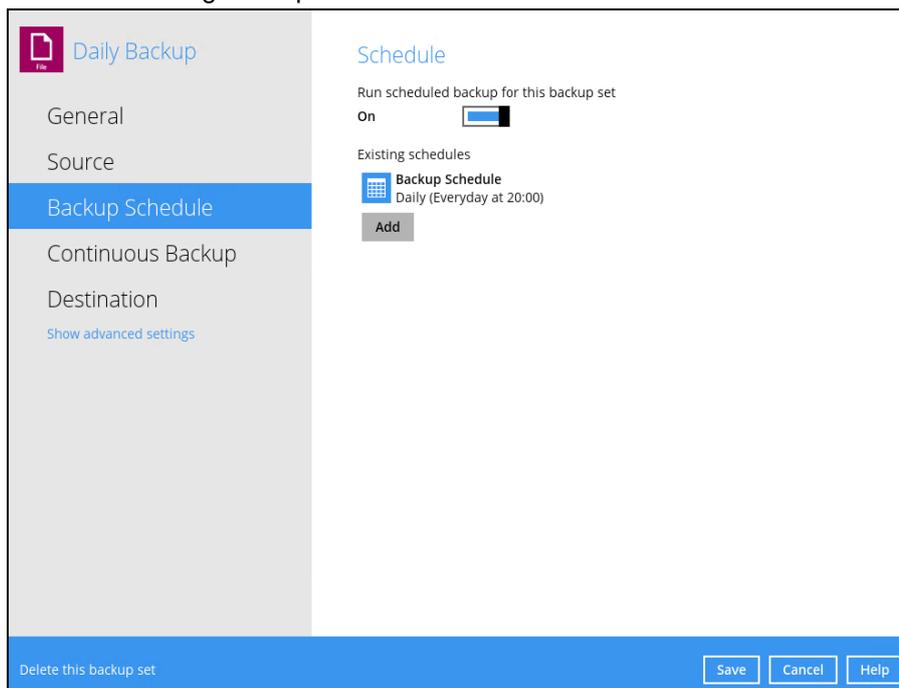
Backup Scheduler (Recommended)

To run a retention policy job after a scheduled backup job, follow the steps below:

1. Click the [Backup Schedule] tab in the backup set settings.



2. Select an existing backup schedule or add a new one.



3. In the Backup Schedule window, select 'Run Retention Policy after backup' to run a retention policy job after a scheduled backup job.

Backup Schedule

Name
Backup Schedule

Type
Daily

Start backup at
20 : 00

Stop
until full backup completed

Run Retention Policy after backup

Delete this backup schedule

Delete this backup set

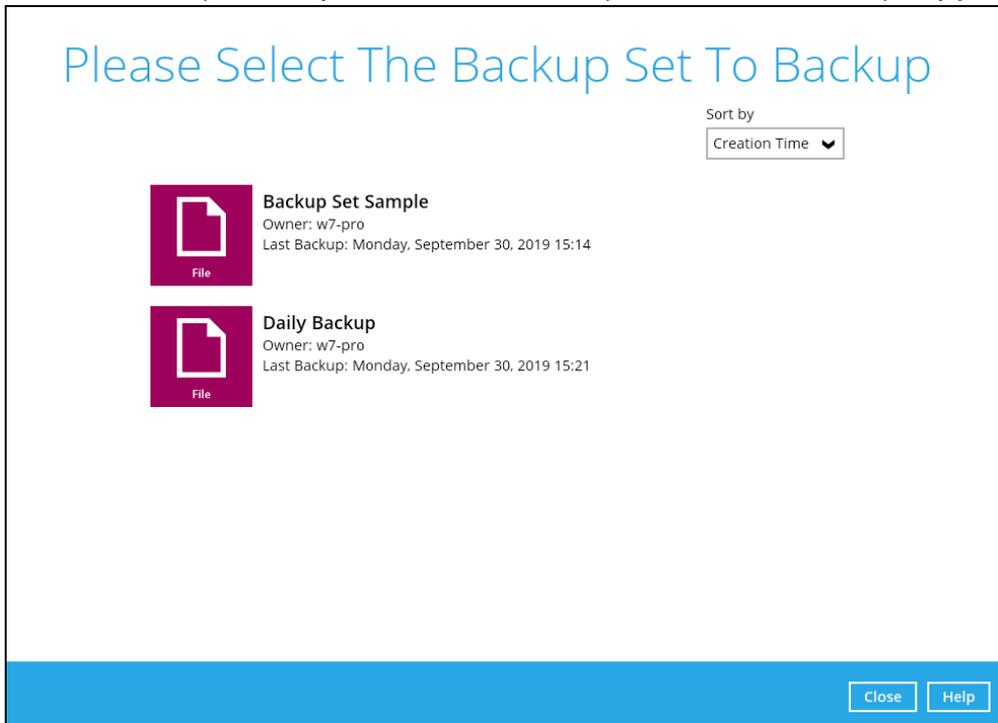
Manual Backup

To run a retention policy job after a manual backup, follow the steps below:

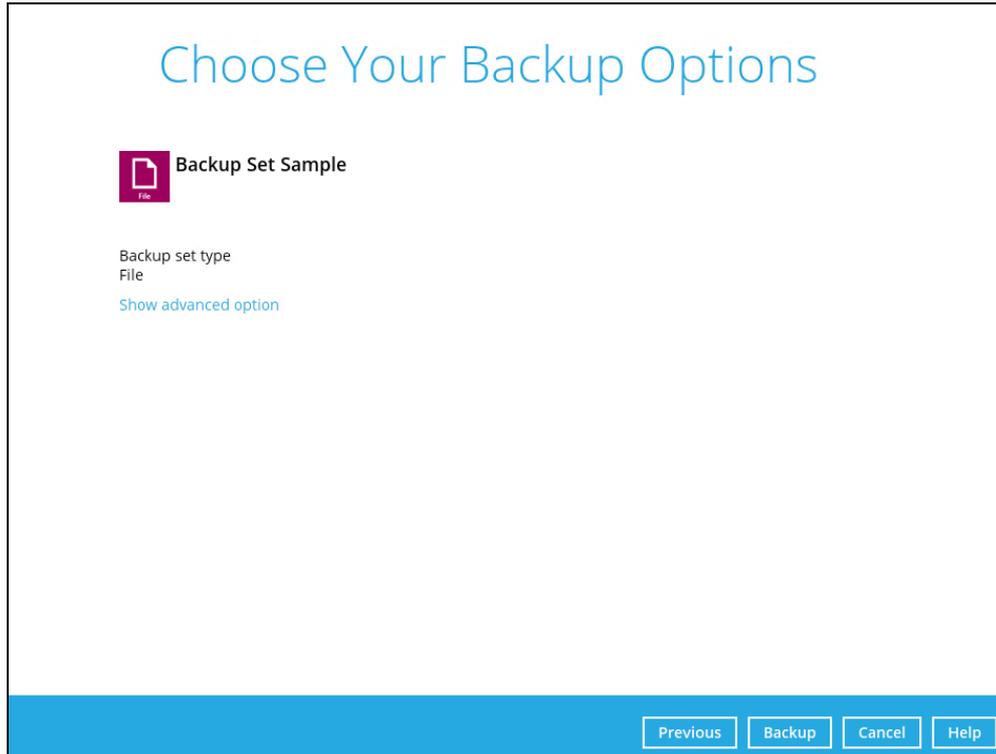
1. Click the **Backup** icon in the OBM main interface.



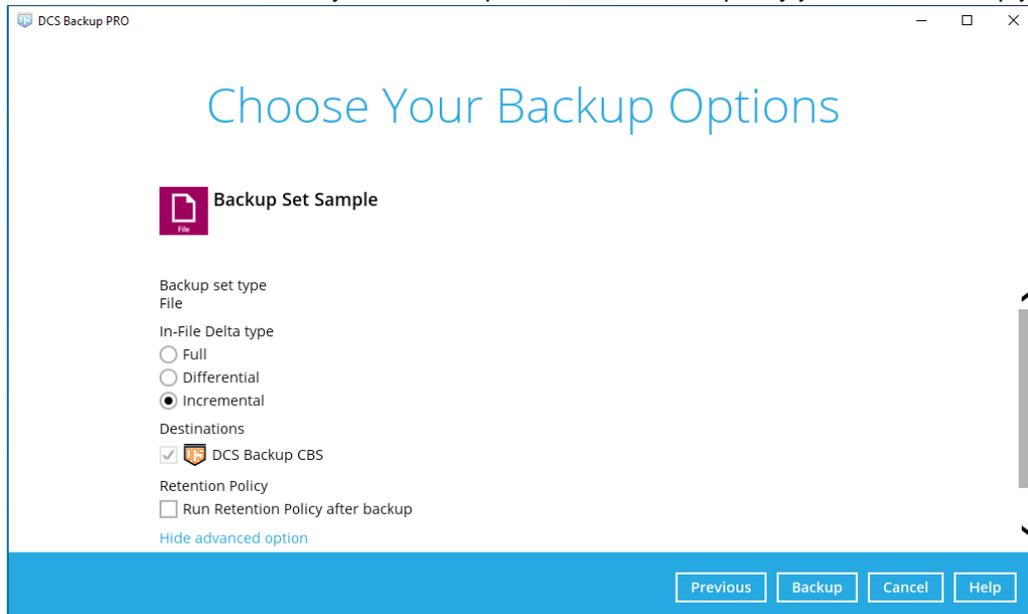
2. Select the backup set that you would like to back up and run the retention policy job on.



3. Click **Show advanced option** to display other settings.



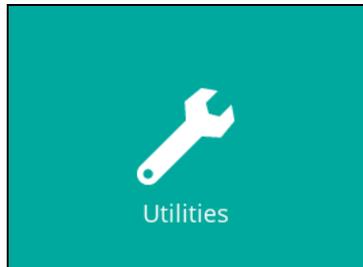
4. Select 'Run Retention Policy after backup' to run a retention policy job after a backup job.



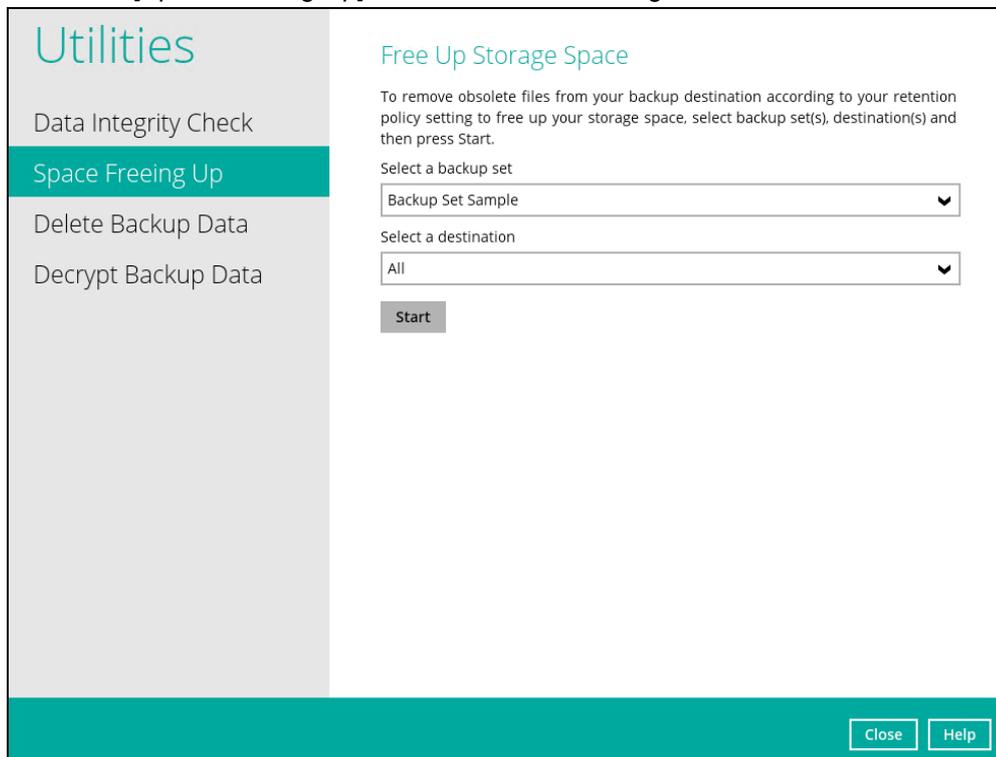
Space Freeing Up

To run a retention policy job manually via backup client interface, follow the steps below:

1. Click the **Utilities** icon in the OBM interface.

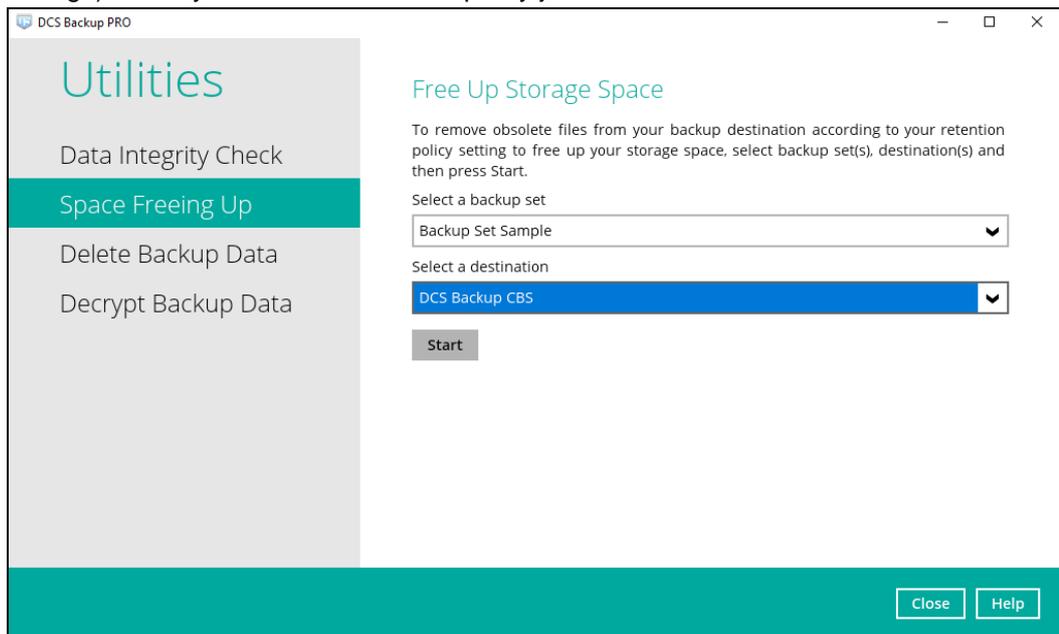


2. Select the [Space Freeing Up] tab in the Utilities settings.



The screenshot shows the 'Utilities' settings window. On the left is a sidebar with the following options: 'Data Integrity Check', 'Space Freeing Up' (highlighted in teal), 'Delete Backup Data', and 'Decrypt Backup Data'. The main content area is titled 'Free Up Storage Space' and contains the following text: 'To remove obsolete files from your backup destination according to your retention policy setting to free up your storage space, select backup set(s), destination(s) and then press Start.' Below this text are two dropdown menus: 'Select a backup set' with 'Backup Set Sample' selected, and 'Select a destination' with 'All' selected. A 'Start' button is located below the dropdowns. At the bottom right of the window are 'Close' and 'Help' buttons.

3. Select the corresponding backup set and destination (e.g. DCS CBS, local drive, cloud storage) where you want the retention policy job to run on.



4. Click the [Start] button to run the retention policy job.

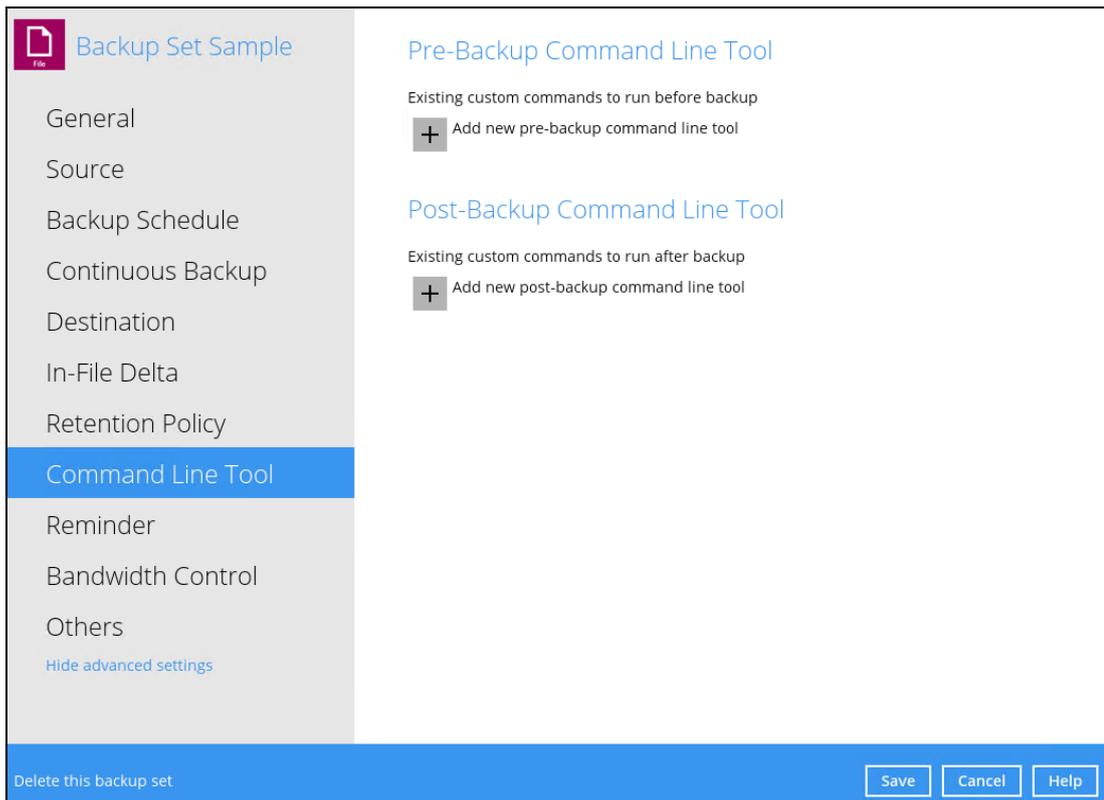
NOTE

For more details about Space Freeing Up, please refer to [Space Freeing Up](#) in **Chapter 8 OBM Overview**.

Command Line Tool

This feature allows the user to configure a pre-backup or post backup command which can be: an operating system level command, a script or batch file, or third-party utilities to run before and/or after a backup job.

e.g., Connecting to a network drive and disconnecting a network drive, stopping a third-party database (not officially supported by DCS) to perform a cold backup, and restarting a third-party database after a backup.



Requirements and Best Practices

Error and Exception Handling

Each pre-backup command or batch file should have an error and exception handling. If a pre-backup command contains an error, although an unhandled error may not hinder the backup job process, and the backup job is successful, it will result to a status indicating completed backup with warning(s). For more details about backup report status, please refer to [Backup Reports](#) in **Chapter 8 OBM Overview**.

Command or Batch File Compatibility

Make sure that each command (pre-backup and post-backup) are tested thoroughly before including them to the backup job.

Scheduled Backup

If the scheduled backup job is set to stop after x no. of hours, make sure that the duration of the running backup job will not be affected. You may need to adjust the number of hours in the backup schedule configuration. Please refer to [Backup Schedule](#) for more details.

Pre-backup Command Limitation

A Windows reboot or shutdown must not be used in the pre-backup command. Otherwise, the machine will shut down immediately that will result to a status indicating “Backup not yet finished”, which can be viewed in the DCS CBS User Web Console. Please refer to [DCS CBS Backup Reports](#) for more details.

Post-backup Command Recommendation

It is recommended to include a timeout for a post-backup command to shut down the machine. The timeout must be adjusted until when the OBM sends the backup job status to the DCS CBS.

In this example, the configured post-backup command is to shut down the machine that has a timeout set to ninety (90) seconds. The machine will shut down automatically after the specified time.

Post-Backup Command Line Tool

Name

Working Directory

Command

This is to ensure that the OBM has enough time to complete the backup process in order to send the backup job status to the DCS CBS before the machine shuts down. See screenshot below:

The screenshot displays a backup log with columns for Type, Log, and Time. The log entries show the backup process, including file copying, shadow copy deletion, and the execution of the post-backup command 'shutdown /s /t 90'. The log ends with 'Backup Completed Successfully' at 09/05/2019 12:05:59.

| Type | Log | Time |
|------|---|---------------------|
| [i] | [New File]... 53% of "C:\Users\Administrator\Desktop\New folder\photo-1493246507139-91e8fad9978e.jpg" | 09/05/2019 12:05:54 |
| [i] | [New File]... 65% of "C:\Users\Administrator\Desktop\New folder\photo-1493246507139-91e8fad9978e.jpg" | 09/05/2019 12:05:54 |
| [i] | [New File]... 76% of "C:\Users\Administrator\Desktop\New folder\photo-1493246507139-91e8fad9978e.jpg" | 09/05/2019 12:05:54 |
| [i] | [New File]... 88% of "C:\Users\Administrator\Desktop\New folder\photo-1493246507139-91e8fad9978e.jpg" | 09/05/2019 12:05:54 |
| [i] | [New File]... 100% of "C:\Users\Administrator\Desktop\New folder\photo-1493246507139-91e8fad9978e.jpg" | 09/05/2019 12:05:54 |
| [i] | Total New Files = 35 | 09/05/2019 12:05:55 |
| [i] | Total New Directories = 5 | 09/05/2019 12:05:55 |
| [i] | Total New Links = 0 | 09/05/2019 12:05:55 |
| [i] | Total Updated Files = 0 | 09/05/2019 12:05:55 |
| [i] | Total Attributes Changed Files = 0 | 09/05/2019 12:05:55 |
| [i] | Total Deleted Files = 0 | 09/05/2019 12:05:55 |
| [i] | Total Deleted Directories = 0 | 09/05/2019 12:05:55 |
| [i] | Total Deleted Links = 0 | 09/05/2019 12:05:55 |
| [i] | Total Moved Files = 0 | 09/05/2019 12:05:55 |
| [i] | Deleting Shadow Copy snapshot for volume "\?\Volume{d8b4117e-f9e7-11e6-9e11-806e6f6e6963}\" | 09/05/2019 12:05:56 |
| [i] | Deleting Shadow Copy snapshot for volume "C:\" | 09/05/2019 12:05:56 |
| [i] | Saving encrypted backup file index to 1567656180789/blocks at destination AhsayCBS... | 09/05/2019 12:05:57 |
| [i] | Saving encrypted backup file index to 1567656180789/blocks/2019-09-05-12-05-38 at destination AhsayCBS... | 09/05/2019 12:05:57 |
| [i] | Start running post-commands | 09/05/2019 12:05:58 |
| [i] | [Post-Backup-1] shutdown /s /t 90 | 09/05/2019 12:05:58 |
| [i] | Finished running post-commands | 09/05/2019 12:05:59 |
| [i] | Deleting temporary file C:\Users\Administrator\temp\1567656180789\OBS@1567656260848 | 09/05/2019 12:05:59 |
| [i] | Backup Completed Successfully | 09/05/2019 12:05:59 |

Logs per page: 50 Page: 2 / 2

Close

NOTE

For more details about detailed backup report, please refer to [Backup Reports](#) in **Chapter 8 OBM Overview**.

There are three (3) fields in the command line tool:

| Field | Description |
|--------------------------|--|
| Name | The user-defined name of the pre-backup or post-backup command. |
| Working Directory | The location in the local machine which the pre-backup or post-backup command will run at, or the location of the command or created batch file. |
| Command | The pre-backup or post-backup command which can be defined as a native command or command to execute a batch file, command, or a VBScript (exclusively for Windows). |

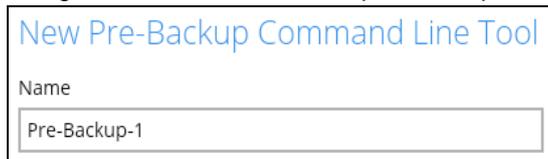
Pre-backup Command

A pre-backup command is used to execute an action or process before the start of a backup job. To create a pre-backup command, follow the steps below:

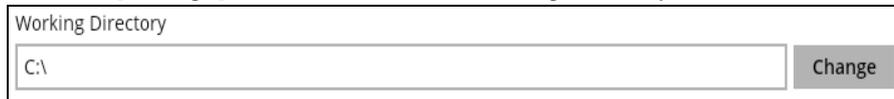
1. Click the [Add] button.



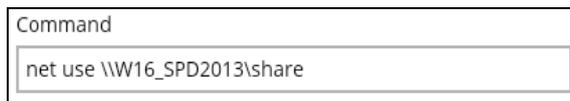
2. Assign a desired name to the pre-backup command.



3. Click the [Change] button to locate the working directory of the command.

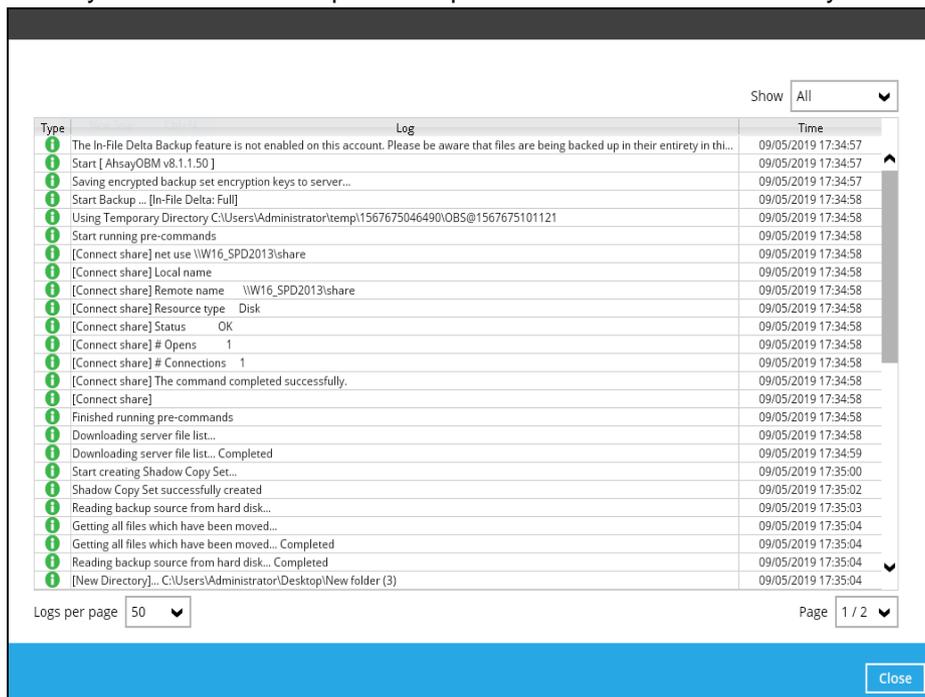


4. Input a command to be run before a backup job. In this example, the pre-backup command will connect to a network drive before the backup process.



5. Click the [OK] button to save the created pre-backup command, then click the [Save] button to save settings.

6. Once the backup job is complete, click the  button to display the backup report log where you can check if the pre-backup command has run successfully.



Post-backup Command

A post-backup command is used to execute an action or process after a backup job. To create a post-backup command, follow the steps below:

1. Click the [Add] button.



Post-Backup Command Line Tool

Existing custom commands to run after backup

+ Add new post-backup command line tool

2. Assign a desired name to the post-backup command.

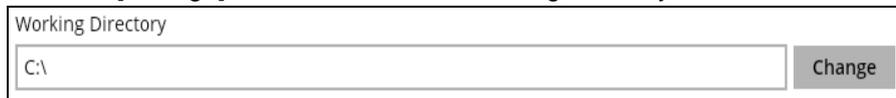


New Post-Backup Command Line Tool

Name

Post-Backup-1

3. Click the [Change] button to locate the working directory of the command.

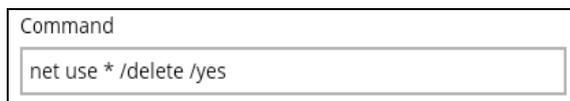


Working Directory

C:\

Change

4. Input a command to be run after a backup job. In this example, the post-backup command will disconnect a network drive after the backup process.



Command

net use * /delete /yes

5. Click the [OK] button to save the created post-backup command, then click the [Save] button to save the settings.

6. Once the backup job is complete, click the  button to display the backup report log where you can check if the post-backup command has run successfully.

Show All ▼

| Type | Log | Time |
|---|---|---------------------|
|  | Total New Files = 20 | 09/05/2019 17:44:13 |
|  | Total New Directories = 5 | 09/05/2019 17:44:13 |
|  | Total New Links = 0 | 09/05/2019 17:44:13 |
|  | Total Updated Files = 0 | 09/05/2019 17:44:13 |
|  | Total Attributes Changed Files = 0 | 09/05/2019 17:44:13 |
|  | Total Deleted Files = 0 | 09/05/2019 17:44:13 |
|  | Total Deleted Directories = 0 | 09/05/2019 17:44:13 |
|  | Total Deleted Links = 0 | 09/05/2019 17:44:13 |
|  | Total Moved Files = 0 | 09/05/2019 17:44:13 |
|  | Deleting Shadow Copy snapshot for volume "\\?\Volume{d8b4117e-f9e7-11e6-9e11-806e6f6e6963}\\" | 09/05/2019 17:44:13 |
|  | Deleting Shadow Copy snapshot for volume "C:\" | 09/05/2019 17:44:13 |
|  | Saving encrypted backup file index to 1567676544679/blocks at destination AhsayCBS... | 09/05/2019 17:44:14 |
|  | Saving encrypted backup file index to 1567676544679/blocks/2019-09-05-17-43-58 at destination AhsayCBS... | 09/05/2019 17:44:14 |
|  | Start running post-commands | 09/05/2019 17:44:15 |
|  | [Post-Backup-1] net use * /delete /yes | 09/05/2019 17:44:15 |
|  | [Post-Backup-1] You have these remote connections: | 09/05/2019 17:44:15 |
|  | [Post-Backup-1] | 09/05/2019 17:44:15 |
|  | [Post-Backup-1] \\W16_SPD2013\share | 09/05/2019 17:44:15 |
|  | [Post-Backup-1] Continuing will cancel the connections. | 09/05/2019 17:44:15 |
|  | [Post-Backup-1] | 09/05/2019 17:44:15 |
|  | [Post-Backup-1] The command completed successfully. | 09/05/2019 17:44:15 |
|  | [Post-Backup-1] | 09/05/2019 17:44:15 |
|  | Finished running post-commands | 09/05/2019 17:44:15 |
|  | Deleting temporary file C:\Users\Administrator\temp\1567676544679\OBS@1567676569092 | 09/05/2019 17:44:15 |
|  | Backup Completed Successfully | 09/05/2019 17:44:15 |

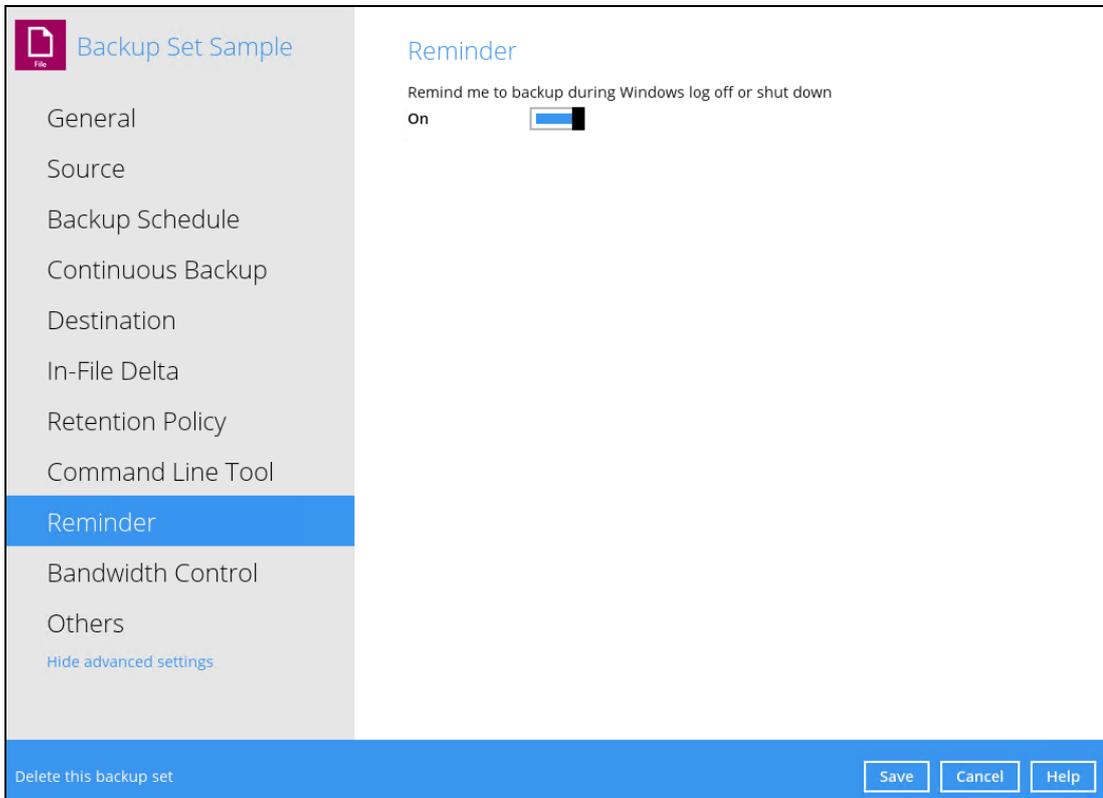
Logs per page 50 ▼
Page 3 / 3 ▼

Close

NOTE
Multiple commands (pre-backup and post-backup) can be created in the Command Line Tool

Reminder

This feature is enabled by default. When enabled, a backup confirmation dialog box will prompt the user to run a backup job during Windows log off, restart or shut down.



To enable the Reminder setting, follow the steps below:

1. Go to Backup Sets, then select a backup set.
2. Choose the [Reminder] tab in the backup set settings.
3. Swipe the lever to the right to turn on the reminder.
4. Click the [Save] button to save settings.

NOTES

1. This feature is not supported on Windows 10, Windows Server 2016, and Windows Server 2019.
2. The dialog box will only appear if there is a backup set with enabled Reminder setting.
3. The dialog box will only be displayed for four (4) seconds.
4. If there are multiple backup sets displayed, you cannot select one (1) backup set to back up. It is recommended to only enable the Reminder setting for the backup sets you regularly back up.

For more detailed examples of the reminder feature, please refer to [Appendix D: Example Scenarios for the Reminder](#).

Bandwidth Control

This option allows the user to limit the amount of bandwidth used by backup traffic between specified times. This feature is configured as disabled by default.

Daily Backup~2

Bandwidth Control

Limit the transfer rate when performing backup and restore tasks

off

General

Source

Backup Schedule

Continuous Backup

Destination

In-File Delta

Retention Policy

Command Line Tool

Reminder

Bandwidth Control

Others

[Hide advanced settings](#)

[Delete this backup set](#) [Save](#) [Cancel](#) [Help](#)

There are two (2) different modes in assigning a bandwidth control:

| Bandwidth Control Type | Description |
|------------------------|--|
| Independent | Each backup and restore has its assigned bandwidth. |
| Share | All backup and restore operations are sharing the same assigned bandwidth. |

NOTE

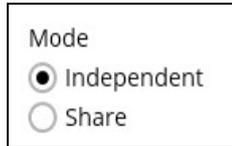
Share mode does not support performing backup job on multiple destinations concurrently.

To enable the bandwidth control setting, follow the steps below:

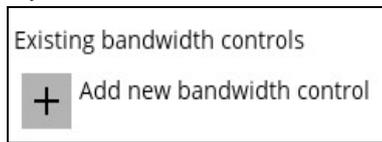
1. Swipe the lever to the right to turn on the bandwidth control.



2. Select a bandwidth control mode.



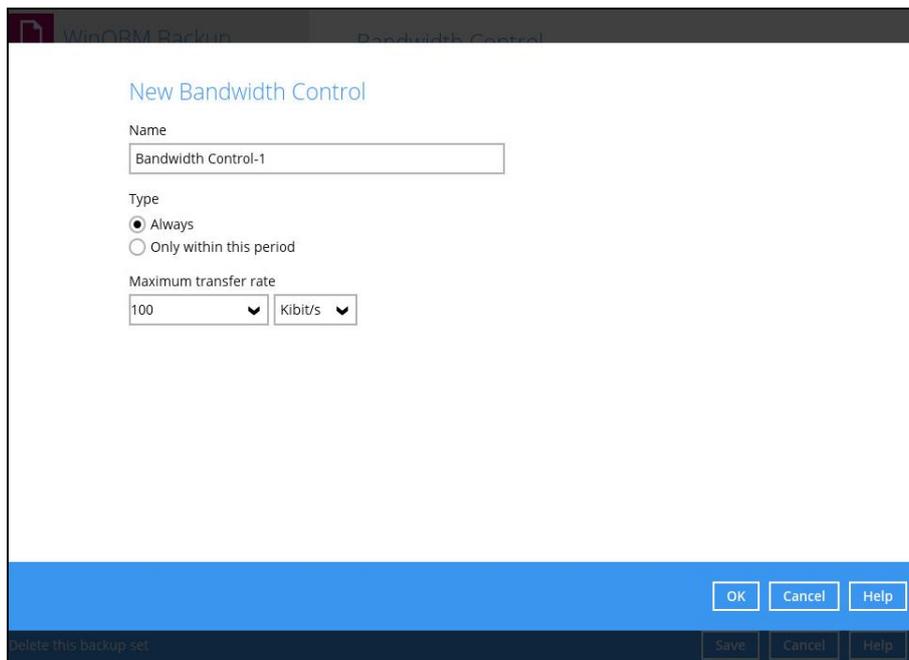
3. If you want to add a modified bandwidth control, click the [Add] button.



4. Complete the following fields:

- Name
- Type
- Maximum transfer rate

| Field | Description |
|------------------------------|--|
| Name | The name of the bandwidth control set. |
| Type | The type of enforced bandwidth control period. |
| Maximum Transfer rate | The maximum bandwidth used. |

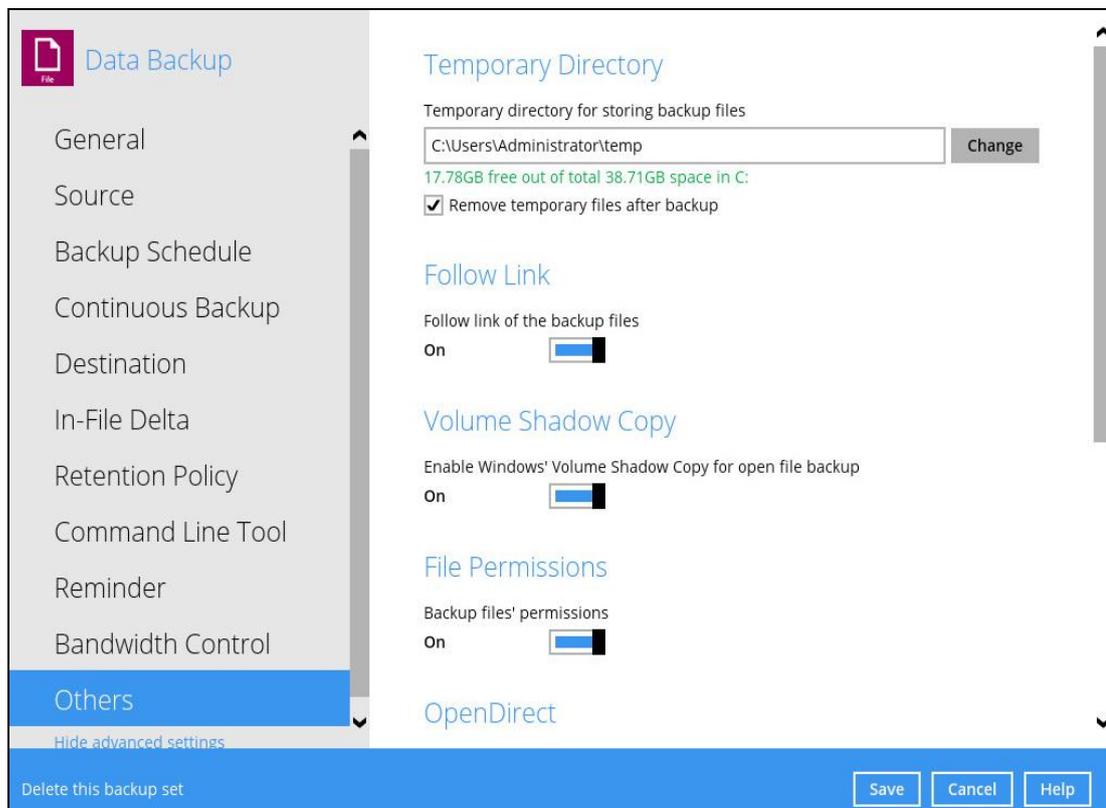


5. Click the [OK] button to save the created bandwidth control set, then click the [Save] button to save settings.

Others

Below is the list of other configurable options under the advanced backup set settings:

- [Temporary Directory](#)
- [Follow Link](#)
- [Volume Shadow Copy](#)
- [File Permissions](#)
- [OpenDirect](#)
- [Compressions](#)
- [Encryption](#)



Temporary Directory

The OBM uses the temporary directory for both backup and restore operations.

For a **backup job**, it is used to temporarily store:



- Backup set index files. An updated set of index files is generated after each backup. The index files are synchronized to each individual backup destination at the end of each backup job.
- Incremental/Differential delta files generated during backups.

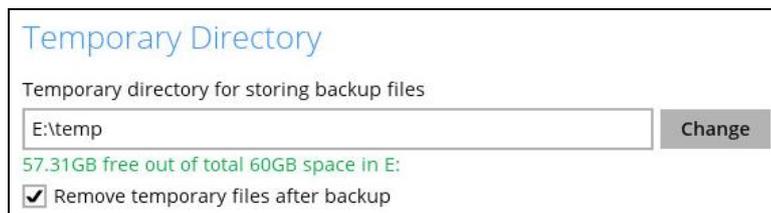
For a **restore job**, it is used to temporarily store:

- Full and Incremental/Differential delta files retrieved from the backup destination.
- Merging of the Full and Incremental/Differential delta files as part of the restore process.

| NOTES | |
|-------|--|
| 1. | For best practice, the temporary directory should be located on a local drive for optimal backup and restore performance. |
| 2. | It should not be located on: <ul style="list-style-type: none">○ Windows System C:\ drive, as the C:\ drive is used by Windows and other applications. There will be frequent disk I/O activity which may affect both backup and restore performance.○ A network drive, as it could affect both backup and restore performance. |
| 3. | It is recommended to select the 'Remove temporary files after backup' option on the backup set to keep the temporary drive clear. |

To change the temporary directory, follow the steps below:

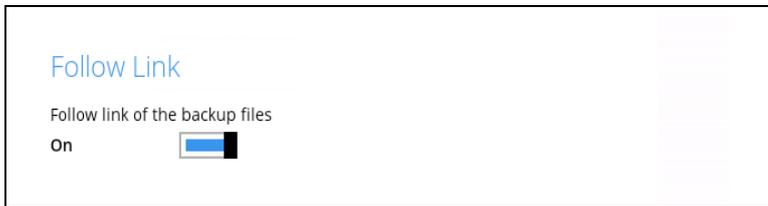
1. Click the [Change] button to select a directory path for storing temporary data.



2. Click the [Save] button to save settings.

Follow Link

This feature allows the user to enable or disable the follow link which defines the NTFS junction or symbolic link during a backup job. This option is enabled by default.



NOTE

Applicable for File Backup Sets only.

Volume Shadow Copy

This feature allows the OBM to use the Windows Volume Shadow Copy service to create a snapshot of the selected files and/or folders on the local drive(s) of the machine, so that the OBM can continue to back up files even if they are opened and/or have been updated by the user. This feature is enabled by default.



WARNING

1. To use the Volume Shadow Copy, the license module must first be enabled on your backup user account. Otherwise, just enabling this setting on the OBM will not activate this feature and can result in possible backup errors if the backup job encounters an open file. Please contact your backup service provider for more details.
2. Volume Shadow Copy does not support open file backups on network drives.

File Permissions

This option defines whether to back up operating system file permission of the data selected as backup source. This option is enabled by default.



NOTE

Applicable for File Backup Sets only.

OpenDirect

This feature is used to add additional restore options in restoring files from a File Backup Set. This feature can only be enabled during the creation of backup set. For more details about OpenDirect Restore, please refer to [Chapter 5 OpenDirect Restore](#).

OpenDirect

Support of opening backup data directly without restoration

off

WARNING

1. To use this feature, the OpenDirect license module must first be enabled with the correct number of modules on your user account. If you enable this setting on the OBM without an OpenDirect license, or your account does not have enough OpenDirect licenses, then your backup job will not run. Please contact your backup service provider for more details.
2. When OpenDirect is enabled, to optimize restore performance, both compression and encryption will be disabled for this backup set. Therefore, it is not recommended to assign your backup destination on a cloud or on an offsite location.
3. Once the OpenDirect is enabled and the setting is saved, it cannot be disabled without re-creating the backup set.

Compressions

This feature is used to enable the compression of data during a backup job. When the compression is enabled, the OBM will compress all files before it is backed up to the backup destination(s). Newly created backup sets are configured to use Fast with optimization for local by default.

Compressions

Select compression type

Fast with optimization for local

There are four (4) different data compression types:

- No Compression
- Normal
- Fast (Compressed size larger than normal)
- Fast with optimization for local

NOTE

The compression type can be changed anytime even after a backup job. The modified compression type will be applied on the next run of a backup.

Encryption

This feature allows the user to view the current encryption settings. The encryption settings can only be enabled or disabled during the creation of backup set.

| Encryption | |
|---------------------------------------|----------|
| Encryption key | •••••• |
| Unmask encryption key | |
| Algorithm | AES |
| Method | CBC |
| Key length | 256 bits |

To view the encryption key of the backup set, follow the steps below:

1. Go to Backup Sets, then select a backup set.
2. Click the [Others] tab in the backup set settings.
3. In the Encryption, select 'Unmask encryption key' to display the encryption key of the backup set.

| Encryption | |
|---------------------------------------|----------|
| Encryption key | •••••• |
| Unmask encryption key | |
| Algorithm | AES |
| Method | CBC |
| Key length | 256 bits |

| Encryption | |
|-------------------------------------|---------------|
| Encryption key | AbcDefGhi1234 |
| Mask encryption key | |
| Algorithm | AES |
| Method | CBC |
| Key length | 256 bits |

NOTE

For more details about encryption settings, please refer to step no. 13 in [Chapter 9 Create a Backup Set](#).

8.6 Report

This feature allows the user to view the backup and restore reports.



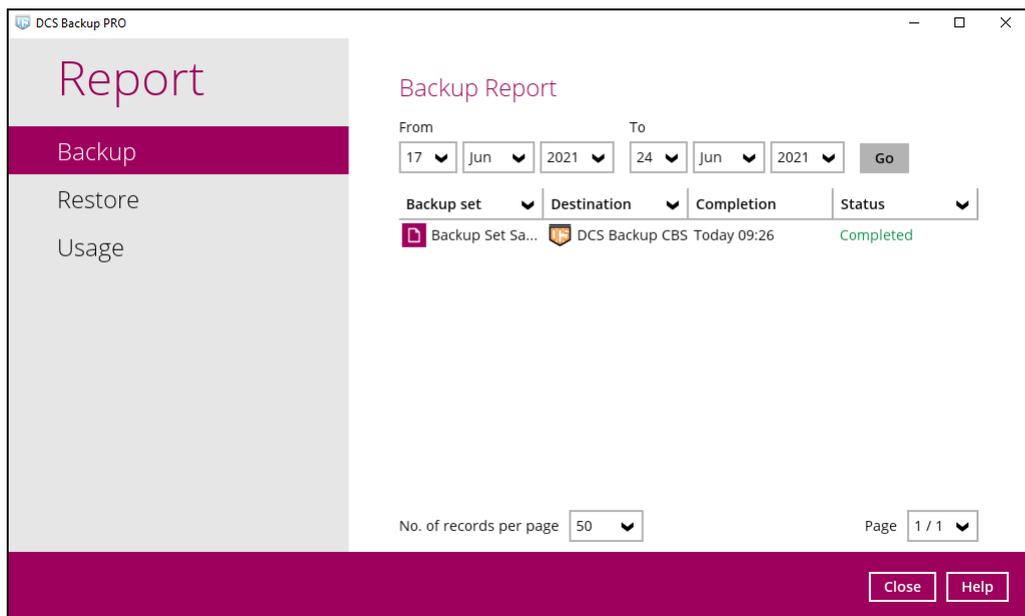
There are three (3) functions available for this feature:

- Backup
- Restore
- Usage

8.6.1 Backup

This shows the backup reports. There are four (4) filters that can be applied on this feature:

- Date
- Backup Set
- Destination
- Status



You can filter and view the backup report using the Date filter.

You can filter and view the backup report using the Backup set filter.

You can filter and view the backup report to your selected storage location using the Destination filter.

You can filter and view the backup report with the same status using the Status filter.

To view the backup log, follow the instructions below:

1. Select and click the backup report, then click the [View log] button.

The screenshot shows the DCS Backup PRO application window. On the left is a sidebar with a 'Report' section containing 'Backup', 'Restore', and 'Usage'. The main window displays a 'Backup Report' for the date 06/24/2021 at 09:25. The report details include: Time (Today 09:25 - 09:26 (PST)), Status (Completed successfully), New files (17 [1.6MB/2.3MB (27%)]), Updated files (0), Attributes Changed Files (0), Moved files (0), and Deleted files (0). A 'View log' button is located at the bottom of the report area. Below the report, there are filters for 'Backup set', 'Destination', 'Completion', and 'Status', along with a 'No. of records per page' dropdown set to 50 and a 'Page 1 / 1' indicator. 'Close' and 'Help' buttons are at the bottom right.

2. Backup set, Destination, Log Date and Time, and Status can also be filtered as well as the number of logs per page.

Report

Backup Report

Backup set

Destination

Log

Show

| Type | Log | Time |
|------|---|---------------------|
| | Start [Windows Server 2008 R2 (w2k8r2-std), AhsayOBM v7.17.0.50] | 07/23/2019 13:16:08 |
| | Saving encrypted backup set encryption keys to server... | 07/23/2019 13:16:08 |
| | Start Backup ... [In-File Delta: Full] | 07/23/2019 13:16:10 |
| | Using Temporary Directory C:\Users\Administrator\temp\156385893767210BS@1563858951806 | 07/23/2019 13:16:10 |
| | Start running pre-commands | 07/23/2019 13:16:10 |
| | Finished running pre-commands | 07/23/2019 13:16:10 |
| | Downloading server file list... | 07/23/2019 13:16:10 |
| | Downloading server file list... Completed | 07/23/2019 13:16:10 |
| | Start creating Shadow Copy Set... | 07/23/2019 13:16:11 |
| | Shadow Copy Set successfully created | 07/23/2019 13:16:14 |
| | Reading backup source from hard disk... | 07/23/2019 13:16:14 |
| | [New Directory]... C:\ | 07/23/2019 13:16:16 |
| | [New Directory]... C:\Users | 07/23/2019 13:16:16 |
| | [New Directory]... C:\Users\Administrator | 07/23/2019 13:16:16 |
| | [New Directory]... C:\Users\Administrator\Documents | 07/23/2019 13:16:16 |
| | [New Directory]... C:\Users\Administrator\Music | 07/23/2019 13:16:16 |
| | Reading backup source from hard disk... Completed | 07/23/2019 13:16:16 |
| | [New File]... 100% of "C:\Users\Administrator\Documents\AhsayACB_UserGuideforWindows_version7.docx" | 07/23/2019 13:16:16 |
| | [New Directory]... C:\Users\Administrator\Pictures | 07/23/2019 13:16:16 |
| | [New Directory]... C:\Users\Administrator\Videos | 07/23/2019 13:16:16 |
| | [New File]... 100% of "C:\Users\Administrator\Documents\AhsayCBS_version7_UserGuide.docx" | 07/23/2019 13:16:16 |

Logs per page

Page

Close

Close

Help

8.6.2 Restore

This shows the restore reports. There are four (4) filters that can be applied on this feature:

- Date
- Backup Set
- Destination
- Status

The screenshot displays the 'Restore Report' window in DCS Backup PRO. On the left is a navigation menu with 'Report', 'Backup', 'Restore' (highlighted), and 'Usage'. The main area shows a date range filter (From: 17 Jun 2021, To: 24 Jun 2021) and a table of reports. The table has columns for Backup set, Destination, Job, and Status. A single report is shown with the following details:

| Backup set | Destination | Job | Status |
|-------------------|----------------|------------------|------------------------|
| Backup Set Sample | DCS Backup CBS | 06/24/2021 09:28 | Completed successfully |

Additional details for the selected report:

- Time: Today 09:28 - 09:28 (PST)
- Status: Completed successfully
- Downloaded files*: 0
- * Unit = No of files (Download size)

At the bottom, there is a 'View log' button, a 'No. of records per page' dropdown set to 50, and a 'Page 1 / 1' indicator. The footer contains 'Close' and 'Help' buttons.

You can filter and view the restore report using the Date filter.

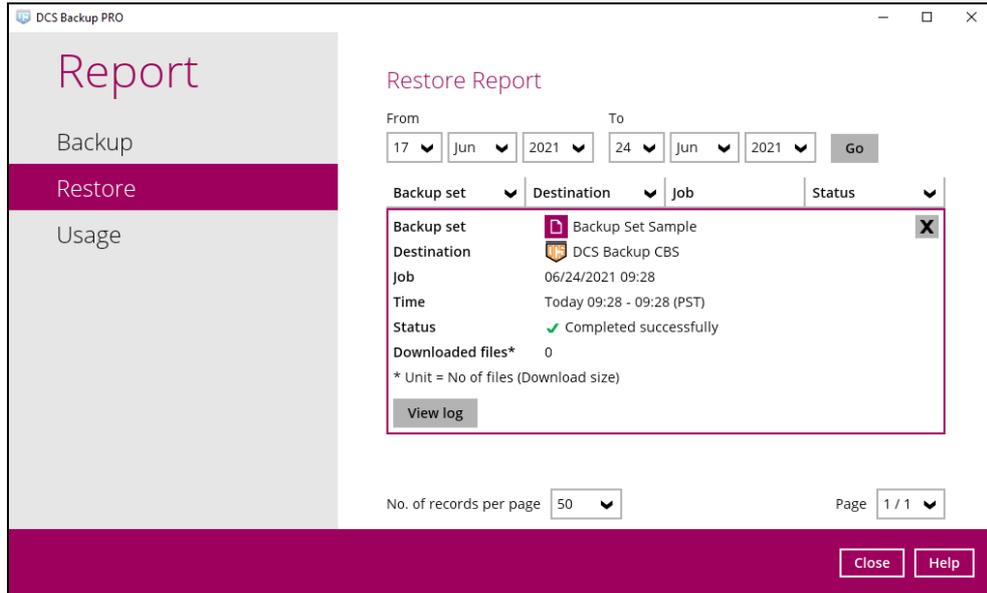
You can filter and view the restore report using the Backup set filter.

You can filter and view the restore report to your selected storage location using the Destination filter.

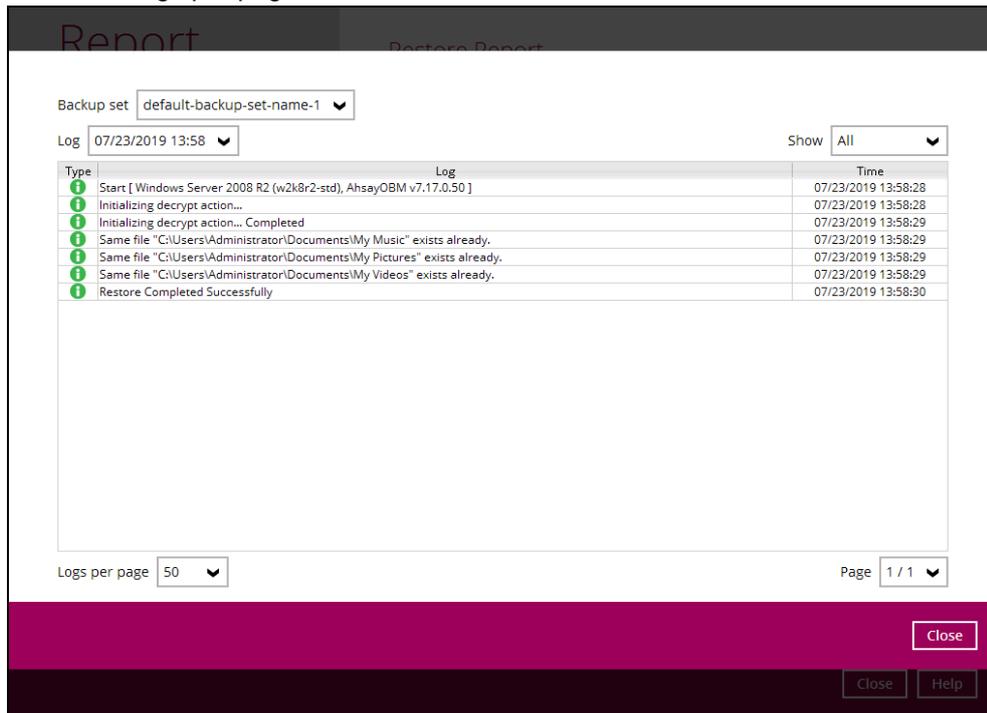
You can filter and view the restore report with the same status using the Status filter.

To view the restore log, follow the instructions below:

1. Select and click the restore report, then click the [View log] button.

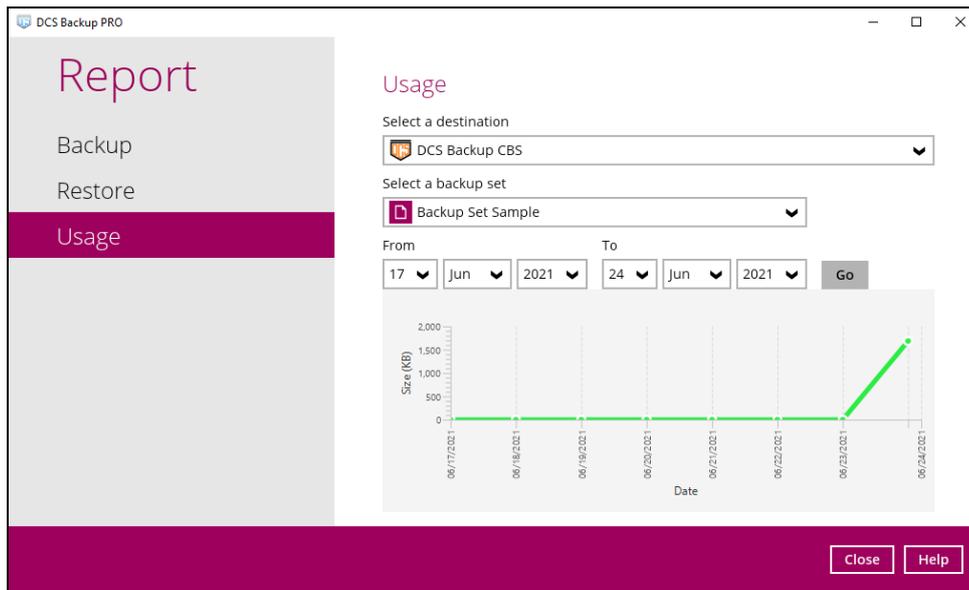


2. Backup set, Log Date and Time, and Status can also be filtered as well as the number of logs per page.



8.6.3 Usage

This allows the user to view the storage and usage information in a graphical view for each backup set and backup destination by date.



- Storage statistics

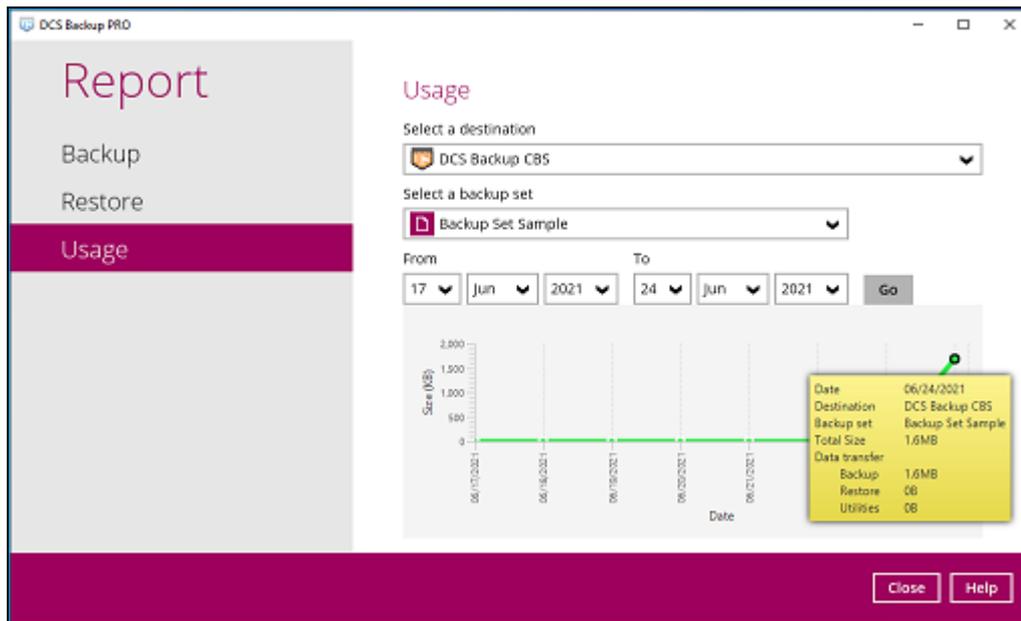
Total Size: displays the total amount of backed up data on the backup destination

The storage statistics of a backup set is updated every time the following functions are run:

1. Backup job
2. [Periodic Data Integrity Check \(PDIC\)](#)
3. [Data Integrity Check \(DIC\)](#)
4. [Space Freeing Up](#)
5. [Delete Backup Data](#)

Example:

The data transfer statistics will pop up when mouse pointer moves over a specific date.



- Data Transfer statistics:
 - **Backup:** displays the amount of data transferred to the backup destination for backups
 - **Restore:** displays the amount of data transferred from the backup destination for restores
 - **Utilities:** displays the amount of data transferred from the backup destination, when a Data Integrity Check (DIC) is run with the "Run Cyclic Redundancy Check (CRC) during data integrity check" option selected

8.7 Restore

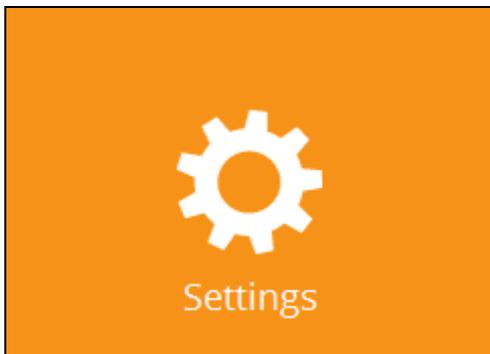
This feature is used to restore backed up files to its original or alternate location.



To restore backed up files, follow the instructions on [Chapter 12 Restore Data](#).

8.8 Settings

This feature allows the user to enable the **Proxy Settings** and **Windows Event Log**.



There are three (3) functions available for this feature:

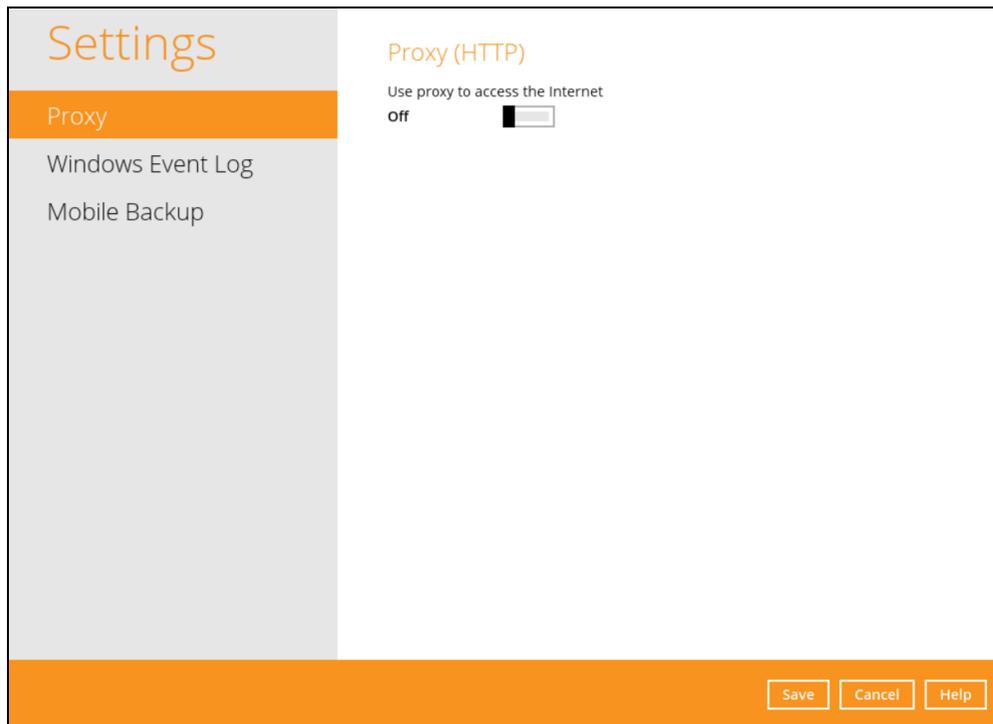
- ⦿ Proxy
- ⦿ Windows Event Log
- ⦿ Mobile Backup

8.8.1 Proxy

When this feature is on, OBM will use a proxy to gain access to the internet.

To enable the Proxy Settings, follow the instructions below:

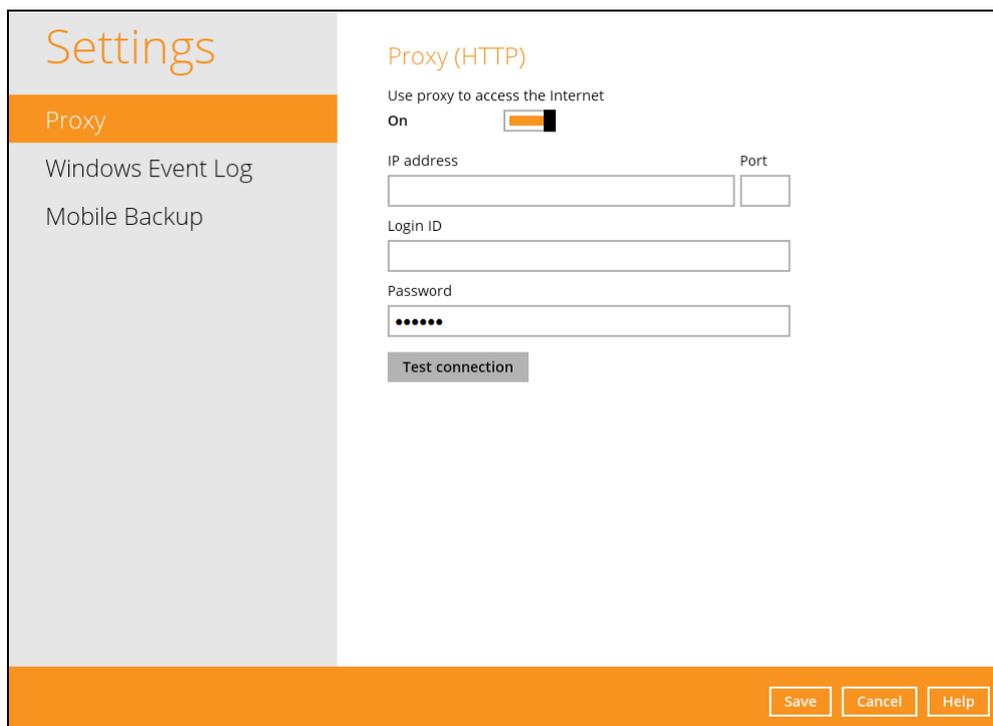
1. Slide the lever to the right to turn it on.



NOTE: Mobile Backup is available if the mobile add-on module is enabled on the user profile. Please contact your backup service provider for details.

2. Complete the following fields:

- IP address
- Port
- Login ID
- Password



3. Click the [Test Connection] button to validate the connection.
4. Click the [Save] button to store the settings.

8.8.2 Windows Event Log

When this feature is on, all OBM system log information will be written under **Applications and Services Logs**. User may access them through **Windows event viewer** in the local machine.

Settings

Proxy

Windows Event Log

Mobile Backup

Windows Event Log

Write AhsayOBM's logs to Windows Event Log. It will be placed under the "AhsayOBM" application log. Activities of backup, restore, and triggered utilities will be logged

On

Event level

error warning Info

Event sources

| | |
|---|--|
| <input type="checkbox"/> Profile | <input type="checkbox"/> Service (CDP & Scheduler) |
| <input type="checkbox"/> Login / Logout | <input type="checkbox"/> Software Update |
| <input type="checkbox"/> Backup | <input type="checkbox"/> Report |
| <input type="checkbox"/> Restore | <input type="checkbox"/> Utilities |

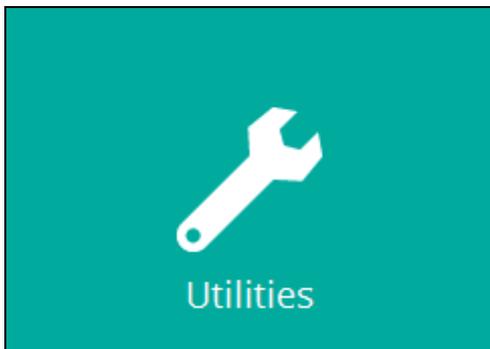
Save Cancel Help

NOTE: This feature is only applicable for Windows OS.

Mobile Backup is available if the mobile add-on module is enabled on the user profile. Please contact your backup service provider for details.

8.9 Utilities

This allows the user to perform quality check on the backed up data, free up storage from obsolete files, delete, and decrypt backed up data.



There are four (4) options available for this feature:

- Data Integrity Check
- Space Freeing Up
- Delete Backup Data
- Decrypt Backup Data

8.9.1 Data Integrity Check

The Data Integrity Check (DIC) is used to identify the data in the backup set that has index-related issues, remove any corrupted file(s) from the backup destination(s) to ensure the integrity of the backup data and its restorability, and update the storage statistics.

For an efficient management of overall storage size of the backup destination(s), the data integrity check job will perform check for the backup destination(s) to remove old index files that are more than ninety (90) days old in the backup job folder(s).

There are four (4) options in performing the Data Integrity Check:

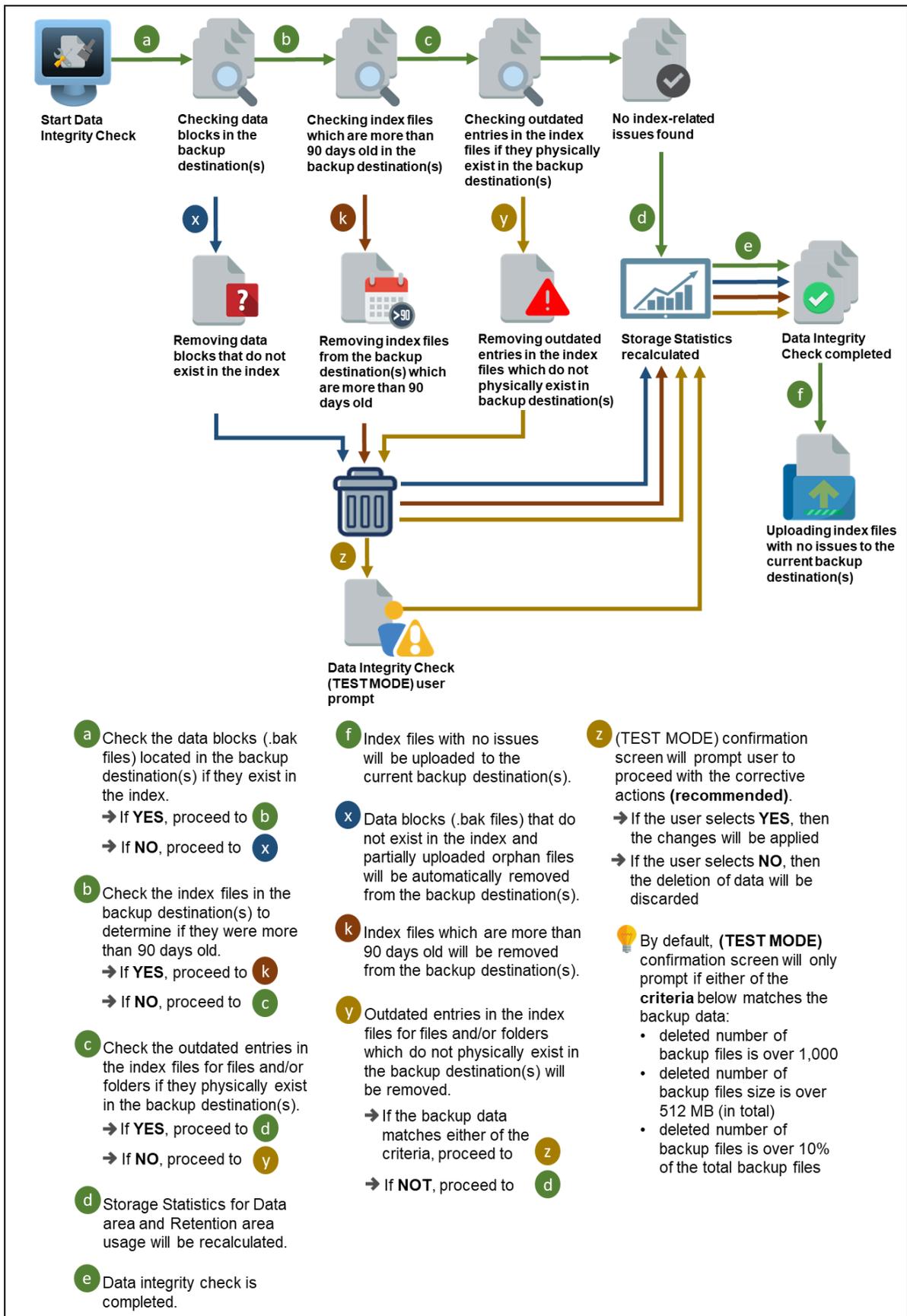
| | |
|--|---|
| Option 1 <input type="checkbox"/> Run Cyclic Redundancy Check (CRC) during data integrity check <input type="checkbox"/> Rebuild index Start | For checking of index and data. |
| Option 2 <input checked="" type="checkbox"/> Run Cyclic Redundancy Check (CRC) during data integrity check <input type="checkbox"/> Rebuild index Start | For checking of index and integrity of files against the checksum file generated at the time of the backup job. |
| Option 3 | For checking and rebuilding of index. |

| | |
|---|--|
| <input type="checkbox"/> Run Cyclic Redundancy Check (CRC) during data integrity check <input checked="" type="checkbox"/> Rebuild index <input type="button" value="Start"/> | |
| <p>Option 4</p> <input checked="" type="checkbox"/> Run Cyclic Redundancy Check (CRC) during data integrity check <input checked="" type="checkbox"/> Rebuild index <input type="button" value="Start"/> | <p>For checking of index, integrity of files against the checksum file generated at the time of the backup job, and rebuilding of index.</p> |

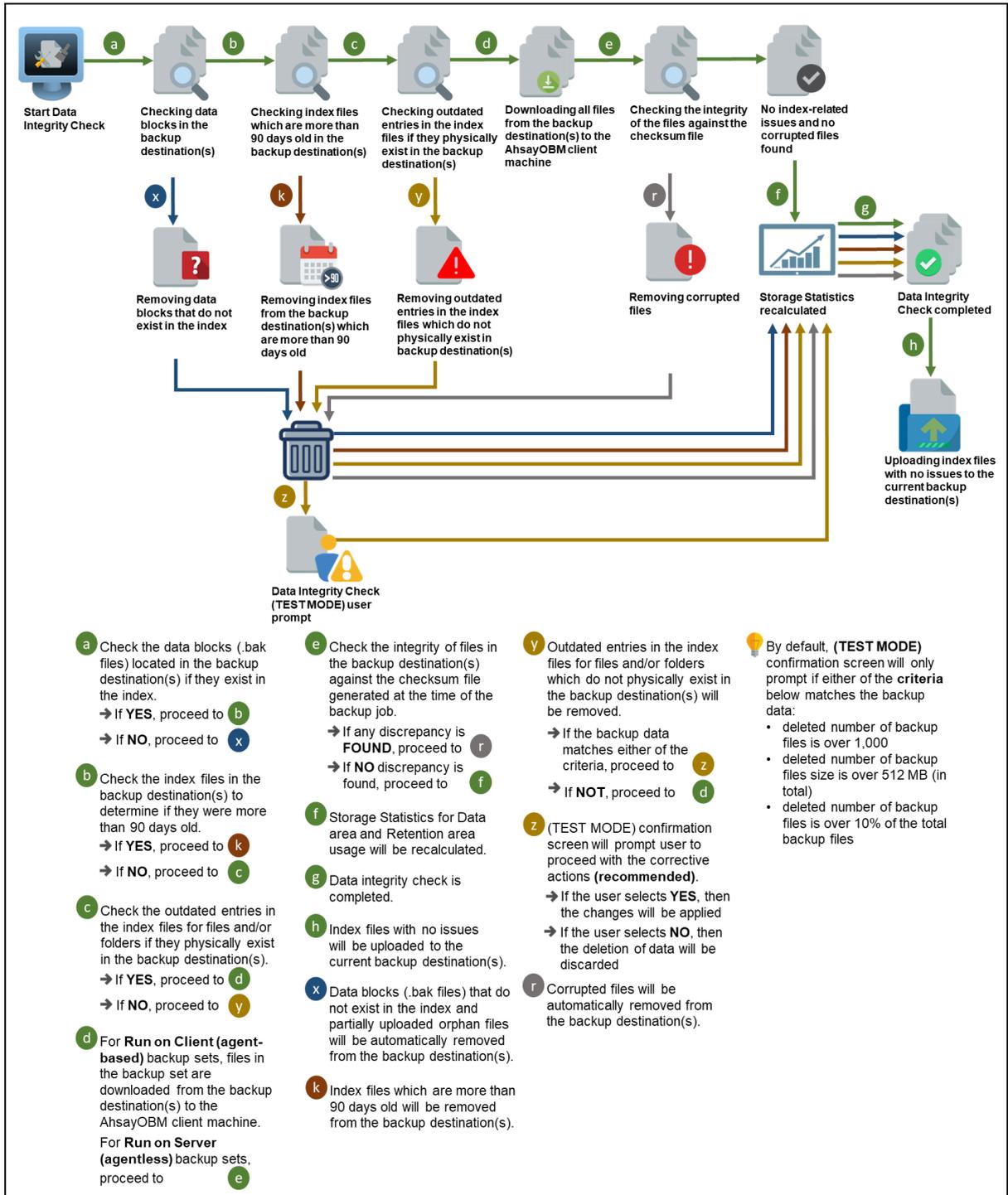
The following diagrams show the detailed process of the Data Integrity Check (DIC) in four (4) modes:

- **Option 1**
Disabled Run Cyclic Redundancy Check (CRC) and Rebuild index - **(Default mode)**
- **Option 2**
Enabled Run Cyclic Redundancy Check (CRC) and Disabled Rebuild index
- **Option 3**
Disabled Run Cyclic Redundancy Check (CRC) and Enabled Rebuild index
- **Option 4**
Enabled Run Cyclic Redundancy Check (CRC) and Rebuild index

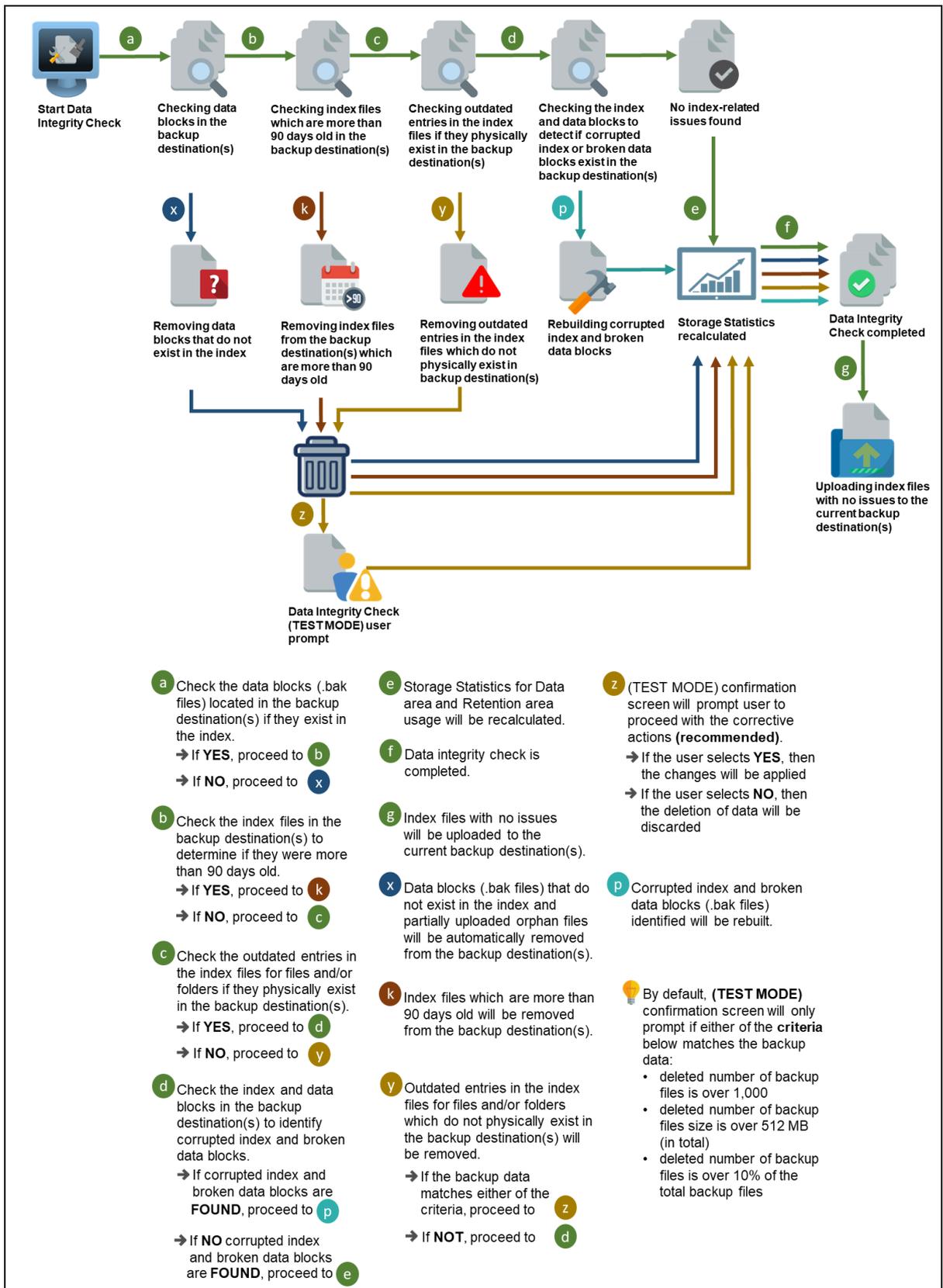
Option 1 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) and Rebuild index DISABLED (Default mode)



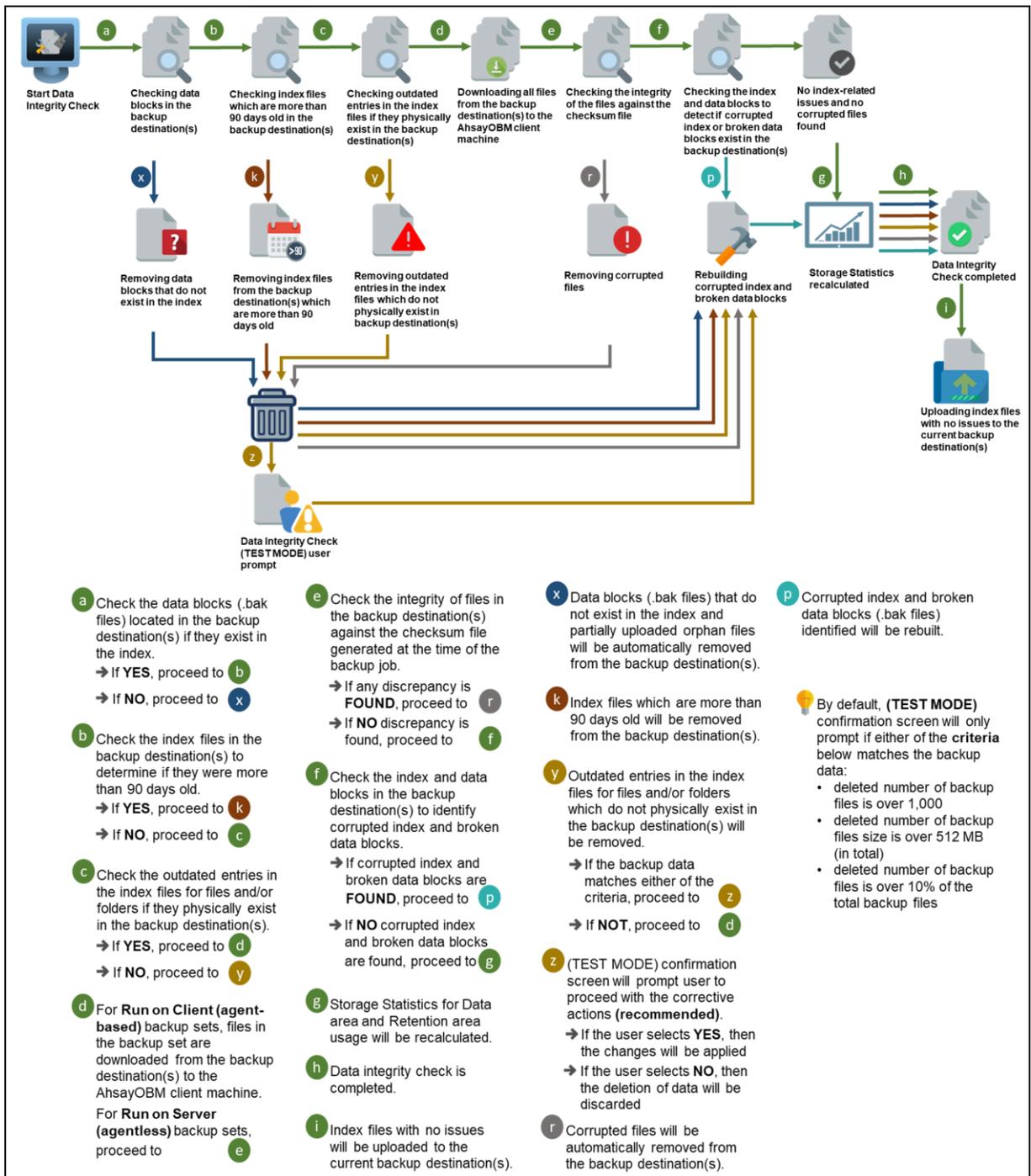
Option 2 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) ENABLED and Rebuild index DISABLED



Option 3 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) DISABLED and Rebuild index ENABLED



Option 4 - Data Integrity Check (DIC) Process with Run Cyclic Redundancy Check (CRC) and Rebuild index ENABLED



Utilities

Data Integrity Check

Space Freeing Up

Delete Backup Data

Decrypt Backup Data

Data Integrity Check

Perform health check for your backed up data to ensure the data integrity and restorability

Select a backup set

All

Run Cyclic Redundancy Check (CRC) during data integrity check

Rebuild index

Start

Close

Help

NOTES

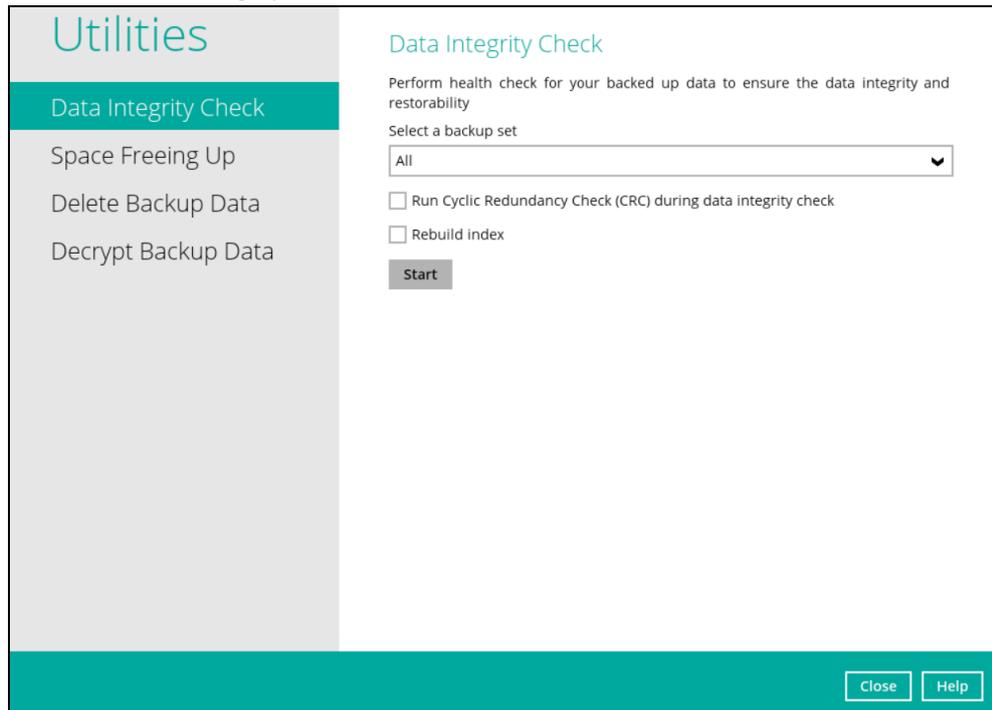
1. Data Integrity Check CANNOT fix or repair files that are already corrupted.
2. Data Integrity Check can only be started if there is NO active backup or restore job(s) running on the backup set selected for the DIC job. As the **backup, restore** and **data integrity check** are using the same index for read and write operations. Otherwise, an error message will be displayed in the post-DIC to indicate that the data integrity check is completed with error(s) and had skipped a backup set with an active backup job.

The following screenshot is an example of a Data Integrity Check completed with error(s). A Data Integrity Check is run on a backup set with an active backup job running which resulted the Data Integrity Check to stop with error(s). Clicking the **View log** button will display the details of the Data Integrity Check job error(s).

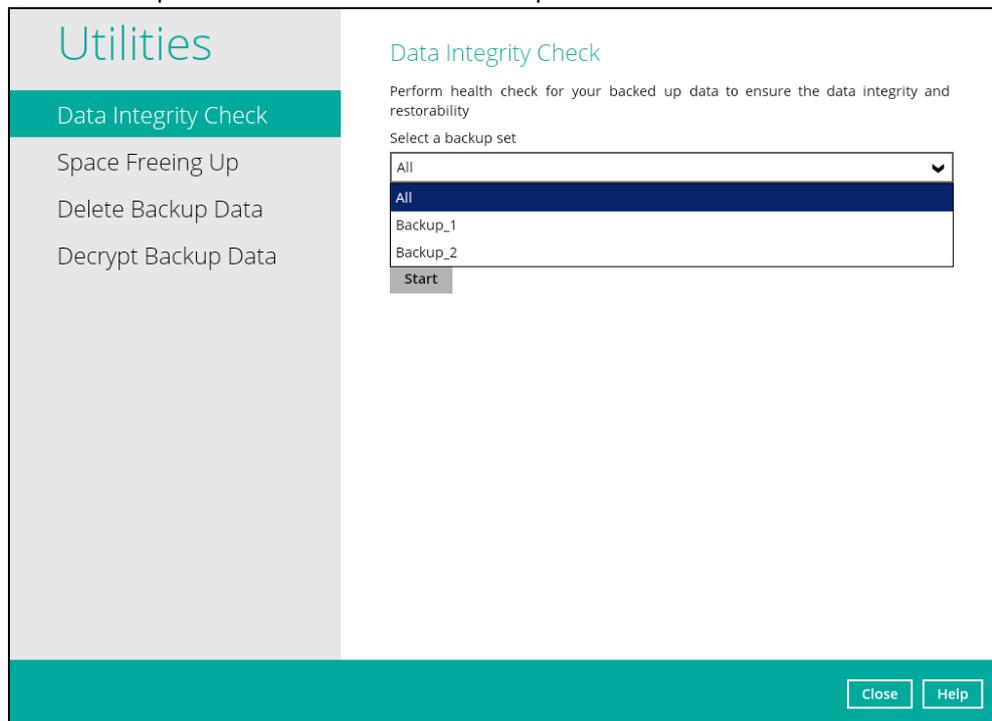
| Type | Log | Time |
|------|--|---------------------|
| i | Start [AhsayOBM v8.5.0.126] | 14/04/2021 10:59:35 |
| i | Start data integrity check on all backup sets, crc disabled, rebuild index disabled | 14/04/2021 10:59:35 |
| x | Skipped Backup Set = "default-backup-set-name-1". Reason = "Backup job "default-backup-set-name-1" is still running." | 14/04/2021 10:59:35 |
| i | Start processing data integrity check on backup set= "default-backup-set-name-2" destination= "AhsayCBS" | 14/04/2021 10:59:35 |
| i | Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1618369079628\OBS@1618369104630..." | 14/04/2021 10:59:37 |
| i | INT_CHECK_VACUUM_INDEX | 14/04/2021 10:59:37 |
| i | INT_CHECK_VACUUM_INDEX... Completed | 14/04/2021 10:59:37 |
| i | Existing statistics of backup set= "default-backup-set-name-2" destination= "AhsayCBS": Data area compressed size: 13.57MB... | 14/04/2021 10:59:38 |
| i | Recalculated statistics of backup set= "default-backup-set-name-2" destination= "AhsayCBS": Data area compressed size: 13.5... | 14/04/2021 10:59:38 |
| i | The statistics of backup set= "default-backup-set-name-2" destination= "AhsayCBS" is correct. | 14/04/2021 10:59:38 |
| i | Saving the integrity check result. | 14/04/2021 10:59:38 |
| i | Saving encrypted backup file index to 1618369079628\blocks at destination AhsayCBS... | 14/04/2021 10:59:39 |
| i | Data integrity check on backup set= "default-backup-set-name-2" destination= "AhsayCBS" is completed | 14/04/2021 10:59:40 |
| x | Skipped Backup Set = "default-backup-set-name-1". Reason = "Backup job "default-backup-set-name-1" is still running." | 14/04/2021 10:59:41 |
| x | Finished data integrity check with error on all backup sets, crc disabled, rebuild index disabled | 14/04/2021 10:59:41 |
| i | Completed data integrity check on all backup sets, crc disabled, rebuild index disabled | 14/04/2021 10:59:41 |

To perform a Data Integrity Check, follow the instructions below:

1. Go to the Data Integrity Check tab in the Utilities menu.



2. Click the drop-down button to select a backup set.



3. Click the drop-down button to select a backup destination.

Utilities

Data Integrity Check

Space Freeing Up

Delete Backup Data

Decrypt Backup Data

Data Integrity Check

Perform health check for your backed up data to ensure the data integrity and restorability

Select a backup set

Backup_2

Select a destination

All

All

AhsayCBS

Run Cyclic Redundancy Check (CRC) during data integrity check

Rebuild index

Start

Close Help

4. Unchecked Run Cyclic Redundancy Check (CRC) and Rebuild index options is the default setting of data integrity check.

Utilities

Data Integrity Check

Space Freeing Up

Delete Backup Data

Decrypt Backup Data

Data Integrity Check

Perform health check for your backed up data to ensure the data integrity and restorability

Select a backup set

Backup_2

Select a destination

AhsayCBS

Run Cyclic Redundancy Check (CRC) during data integrity check

Rebuild index

Start

Close Help

Run Cyclic Redundancy Check (CRC)

When this option is enabled, the DIC will perform check on the integrity of the files on the backup destination(s) against the checksum file generated at the time of the backup job.

If there is a discrepancy, this indicates that the files on the backup destination(s) are corrupted and will be removed from the backup destination(s). If these files still exist on the client machine on the next backup job, the OBM will upload the latest copy of the files.

However, if the corrupted files are in the retention area, they will not be backed up again as the source file has already been deleted from the client machine.

The time required to complete a data integrity check depends on the number of factors such as:

- number of files and/or folders in the backup set(s)
- bandwidth available on the client computer
- hardware specifications of the client computer such as, the disk I/O and CPU performance

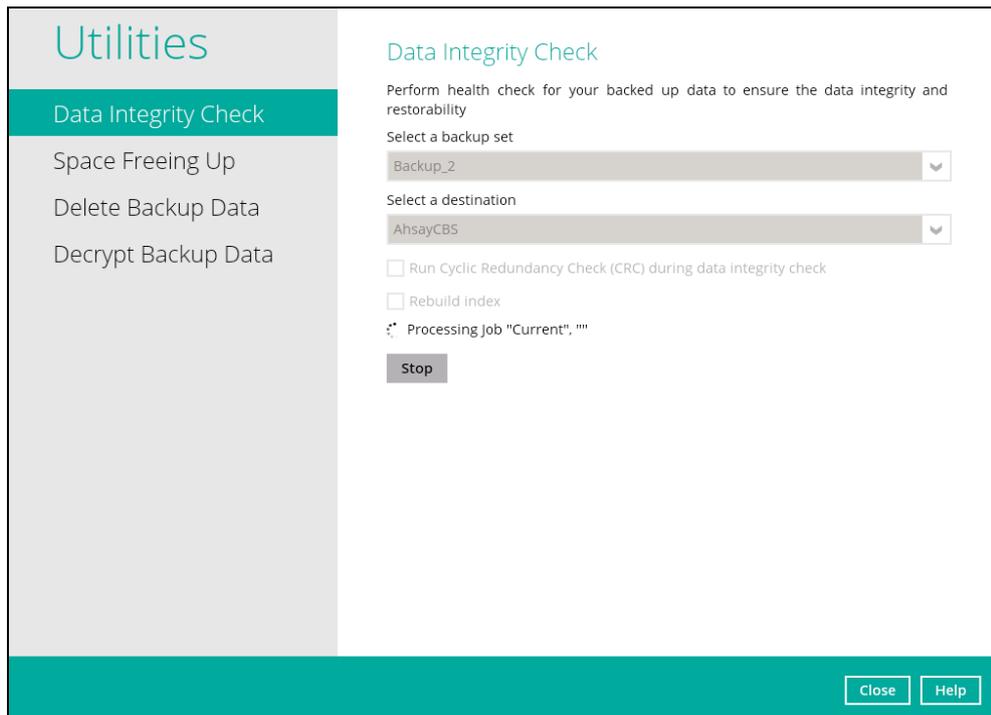
NOTES

1. For user(s) with metered internet connection, additional data charges may be incurred if the Cyclic Redundancy Check (CRC) is enabled. As CRC data involves downloading the data from the backup destination(s) to the client machine in order to perform this check.
2. To find out how much data is downloaded from the backup destination(s) for the CRC check, please refer the value for **Utilities** in the [Data Transfer statistics](#) on chapter 8.6.3.

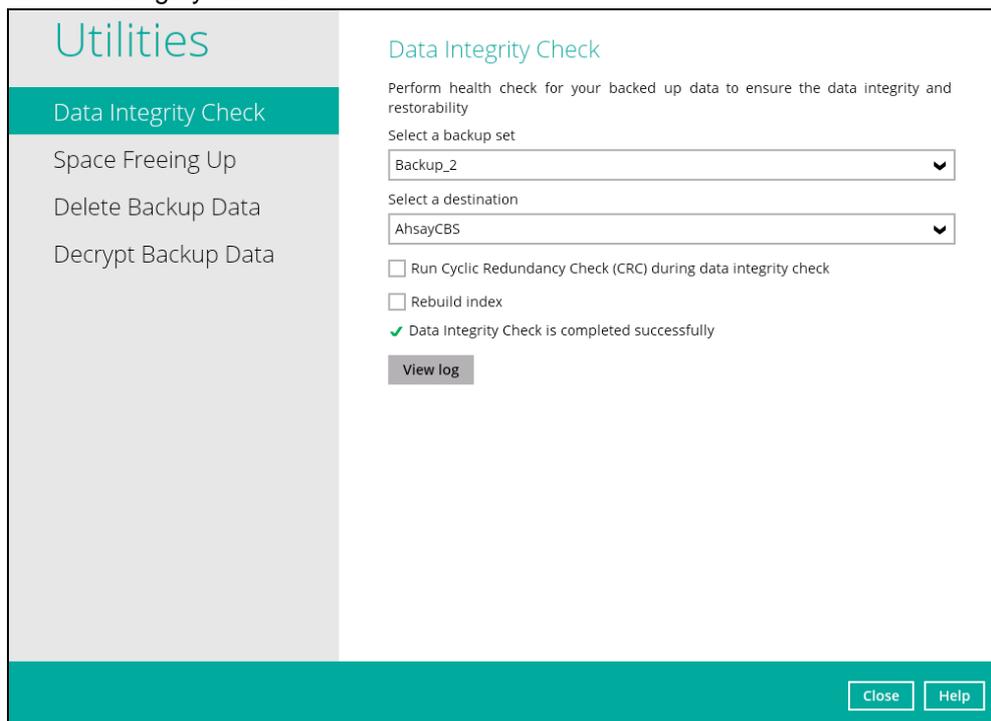
Rebuild index

When this option is enabled, the data integrity check will start rebuilding corrupted index and/or broken data blocks if there are any.

5. Click the [Start] button to begin the Data Integrity Check.
6. Data Integrity Check will start running on the selected backup set(s) and backup destination(s).



7. Once the DIC is completed, click the **View log** button to check the detailed process of the data integrity check.



8. The detailed log of data integrity check process will be displayed.

Utilities Data Integrity Check

Log 14/04/2021 11:33 Show All

| Type | Log | Time |
|------|---|---------------------|
| i | Start [AhsayOBM v8.5.0.126] | 14/04/2021 11:33:17 |
| i | Start data integrity check on backup set "Backup_2(1618369079628)", "AhsayCBS(1618369104630)", crc disabled, rebuild inde... | 14/04/2021 11:33:17 |
| i | Start processing data integrity check on backup set= "Backup_2" destination= "AhsayCBS" | 14/04/2021 11:33:17 |
| i | Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1618369079628\OBS@1618369104630..." | 14/04/2021 11:33:18 |
| i | INT_CHECK_VACUUM_INDEX | 14/04/2021 11:33:18 |
| i | INT_CHECK_VACUUM_INDEX... Completed | 14/04/2021 11:33:18 |
| i | Existing statistics of backup set= "Backup_2" destination= "AhsayCBS": Data area compressed size: 13.57MB, Data area unco... | 14/04/2021 11:33:19 |
| i | Recalculated statistics of backup set= "Backup_2" destination= "AhsayCBS": Data area compressed size: 13.57MB, Data area u... | 14/04/2021 11:33:19 |
| i | The statistics of backup set= "Backup_2" destination= "AhsayCBS" is correct. | 14/04/2021 11:33:19 |
| i | Saving the integrity check result. | 14/04/2021 11:33:19 |
| i | Saving encrypted backup file index to 1618369079628/blocks at destination AhsayCBS... | 14/04/2021 11:33:20 |
| i | Data integrity check on backup set= "Backup_2" destination= "AhsayCBS" is completed | 14/04/2021 11:33:21 |
| i | Finished data integrity check on backup set "Backup_2(1618369079628)", "AhsayCBS(1618369104630)", crc disabled, rebuild i... | 14/04/2021 11:33:21 |
| i | Completed data integrity check on backup set "Backup_2(1618369079628)", "AhsayCBS(1618369104630)", crc disabled, rebuild... | 14/04/2021 11:33:21 |

Logs per page 50 Page 1 / 1

Close

Close Help

The following options can be used for further viewing of the detailed DIC log:

- Log filter
- Show filter
- Logs per page
- Page

Utilities Data Integrity Check

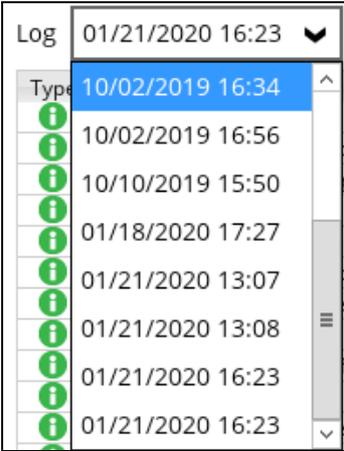
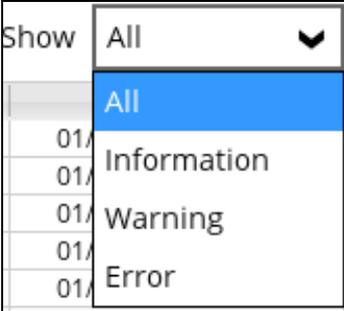
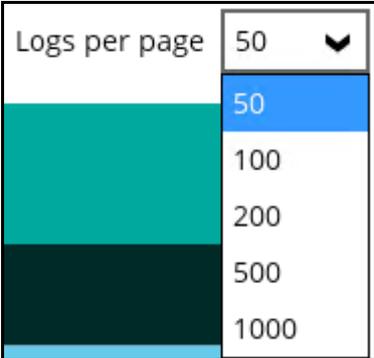
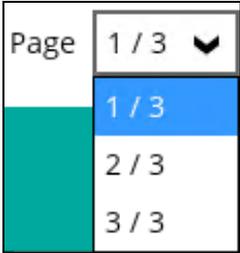
Log 14/04/2021 11:33 Show All

| Type | Log | Time |
|------|---|---------------------|
| i | Start [AhsayOBM v8.5.0.126] | 14/04/2021 11:33:17 |
| i | Start data integrity check on backup set "Backup_2(1618369079628)", "AhsayCBS(1618369104630)", crc disabled, rebuild inde... | 14/04/2021 11:33:17 |
| i | Start processing data integrity check on backup set= "Backup_2" destination= "AhsayCBS" | 14/04/2021 11:33:17 |
| i | Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1618369079628\OBS@1618369104630..." | 14/04/2021 11:33:18 |
| i | INT_CHECK_VACUUM_INDEX | 14/04/2021 11:33:18 |
| i | INT_CHECK_VACUUM_INDEX... Completed | 14/04/2021 11:33:18 |
| i | Existing statistics of backup set= "Backup_2" destination= "AhsayCBS": Data area compressed size: 13.57MB, Data area unco... | 14/04/2021 11:33:19 |
| i | Recalculated statistics of backup set= "Backup_2" destination= "AhsayCBS": Data area compressed size: 13.57MB, Data area u... | 14/04/2021 11:33:19 |
| i | The statistics of backup set= "Backup_2" destination= "AhsayCBS" is correct. | 14/04/2021 11:33:19 |
| i | Saving the integrity check result. | 14/04/2021 11:33:19 |
| i | Saving encrypted backup file index to 1618369079628/blocks at destination AhsayCBS... | 14/04/2021 11:33:20 |
| i | Data integrity check on backup set= "Backup_2" destination= "AhsayCBS" is completed | 14/04/2021 11:33:21 |
| i | Finished data integrity check on backup set "Backup_2(1618369079628)", "AhsayCBS(1618369104630)", crc disabled, rebuild i... | 14/04/2021 11:33:21 |
| i | Completed data integrity check on backup set "Backup_2(1618369079628)", "AhsayCBS(1618369104630)", crc disabled, rebuild... | 14/04/2021 11:33:21 |

Logs per page 50 Page 1 / 1

Close

Close Help

| Control | Screenshot | Description |
|---------------|---|---|
| Log filter |  | This option is used to display the logs of the previous data integrity check jobs. |
| Show filter |  | This option is used to sort the data integrity check log by its status (i.e., All, Information, Warning, and Error). With this filter, it will be easier to sort the DIC logs by its status especially for longer data integrity check logs. |
| Logs per page |  | This option allows user to control the displayed number of logs per page. |
| Page |  | This option allows user to navigate the logs to the next page(s). |

Data Integrity Check Result

There are two possible outcomes after the completion of a data integrity check:

- Data Integrity Check is completed successfully with no data corruption or index-related issues detected;

- Corrupted data (e.g. index files, checksum files and/or broken data blocks) has been detected

The screenshot below shows an example of a data integrity check log with NO data corruption or index-related issues detected.

The screenshot shows the 'Data Integrity Check' utility interface. At the top, there is a 'Log' dropdown set to '14/04/2021 11:33' and a 'Show' dropdown set to 'All'. Below this is a table with columns 'Type', 'Log', and 'Time'. The log entries are as follows:

| Type | Log | Time |
|---|-----|---------------------|
| Start [AhsayOBM v8.5.0.126] | | 14/04/2021 11:33:17 |
| Start data integrity check on backup set "Backup_2(1618369079628)", "AhsayCBS(1618369104630)", crc disabled, rebuild inde... | | 14/04/2021 11:33:17 |
| Start processing data integrity check on backup set= "Backup_2" destination= "AhsayCBS" | | 14/04/2021 11:33:17 |
| Download valid index files from backup job "Current" to "C:\Users\Administrator\temp\1618369079628\OBS@1618369104630... | | 14/04/2021 11:33:18 |
| INT_CHECK_VACUUM_INDEX | | 14/04/2021 11:33:18 |
| INT_CHECK_VACUUM_INDEX... Completed | | 14/04/2021 11:33:18 |
| Existing statistics of backup set= "Backup_2" destination= "AhsayCBS": Data area compressed size: 13.57MB, Data area unco... | | 14/04/2021 11:33:19 |
| Recalculated statistics of backup set= "Backup_2" destination= "AhsayCBS": Data area compressed size: 13.57MB, Data area u... | | 14/04/2021 11:33:19 |
| The statistics of backup set= "Backup_2" destination= "AhsayCBS" is correct. | | 14/04/2021 11:33:19 |
| Saving the integrity check result. | | 14/04/2021 11:33:19 |
| Saving encrypted backup file index to 1618369079628/blocks at destination AhsayCBS... | | 14/04/2021 11:33:20 |
| Data integrity check on backup set= "Backup_2" destination= "AhsayCBS" is completed | | 14/04/2021 11:33:21 |
| Finished data integrity check on backup set "Backup_2(1618369079628)", "AhsayCBS(1618369104630)", crc disabled, rebuild i... | | 14/04/2021 11:33:21 |
| Completed data integrity check on backup set "Backup_2(1618369079628)", "AhsayCBS(1618369104630)", crc disabled, rebuil... | | 14/04/2021 11:33:21 |

At the bottom of the log area, there are controls for 'Logs per page' (set to 50) and 'Page' (set to 1 / 1). A 'Close' button is located at the bottom right of the log area.

If any index-related error(s) or data corrupted item(s) is found, the (TEST MODE) confirmation screen will be displayed.

The screenshot shows the 'Data Integrity Check' utility interface with a warning message. The message reads: "The result of data integrity check (TEST MODE) is as follow. No actions are performed yet. Data corrupted items, checksum incorrect items and index broken data blocks will be deleted. Are you sure you want to continue?". Below the message, it shows 'Backup set: Backup_1' and a table with the following data:

| Destination | Items found in index | Data corrupted items | Index broken data blocks | Statistics |
|-------------|----------------------|----------------------|--------------------------|------------|
| AhsayCBS | 11 (45.7MB) | 6 (45.7MB) | 2 (26.6KB) | Incorrect |

Below the table, there is a note: "* File count (File size)". At the bottom right of the confirmation screen, there are three buttons: 'Yes', 'No', and 'View log'. A 'Close' button is located at the bottom right of the utility interface.

This is to inform the user of the following details:

- Backup set that contains an error
- Backup Destination
- Items found in index

- Data corrupted items
- Index broken data blocks
- Statistics (i.e. Correct or Incorrect)

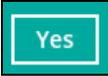
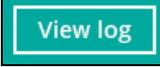
Test Mode confirmation

The (TEST MODE) confirmation screen will ONLY appear if either of the **criteria** below matches the backup data during the data integrity check process:

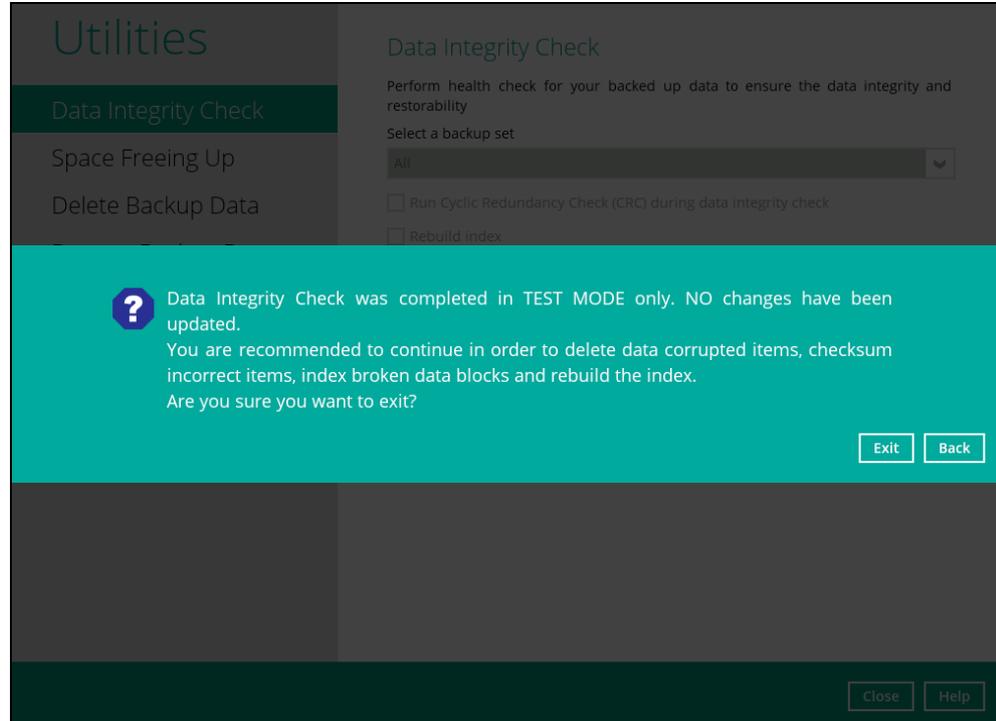
- deleted number of backup files is over 1,000
- deleted number of backup file size is over 512 MB (in total)
- deleted number of backup files is over 10% of the total backup files

Otherwise, the Data Integrity Check job will **automatically** take corrective actions.

There are three (3) options on the (TEST MODE) confirmation screen:

| Control | Screenshot | Description |
|-----------------|--|---|
| Yes |  | Corrupted data (e.g. index files, checksum files and/or broken data blocks) will be deleted and storage statistics will be updated. |
| No |  | No action(s) will be taken and a message will prompt. |
| View log |  | The detailed log of the data integrity check process will be displayed. |

Clicking **No** will display the following screen:



If the **[Exit]** button is clicked, the data integrity check result will be discarded.

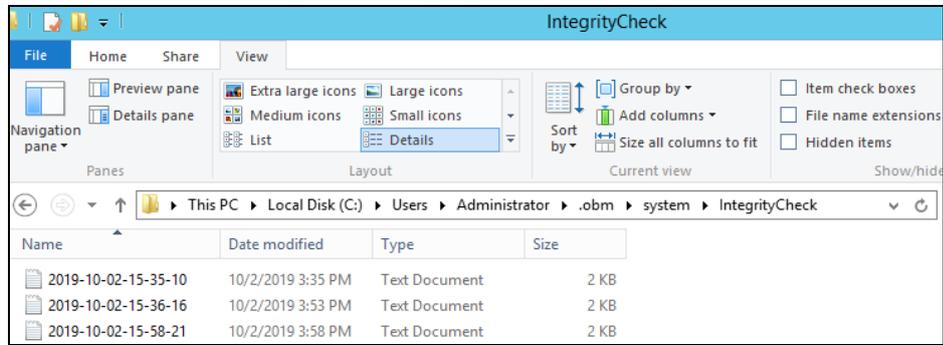
If the **[Back]** button is clicked, it will go back to the (TEST MODE) confirmation screen.

NOTES

1. It is strongly recommended to apply corrective actions when the (TEST MODE) confirmation screen pops up (clicking the **Yes** button). This is to ensure that the remaining corrupted file(s) will be removed from the backup destination(s), therefore on the next backup job, these files are backed up again if they are still present on the client machine. However, if the corrupted files are in retention area, then they will not be backed up again as the source file has already been deleted from the client machine.
2. If the DIC detects data blocks (.bak files) in the backup destination(s) that do not have related index entries, then these physical data blocks will be **automatically** removed from the backup destination(s) without the (TEST MODE) prompt.

Aside from viewing the Data Integrity Check logs directly on OBM client, they can also be viewed on the file system of the OBM client machine. For OBM on Windows, the DIC logs are located in the following directory:

%UserProfile%\obm\system\IntegrityCheck

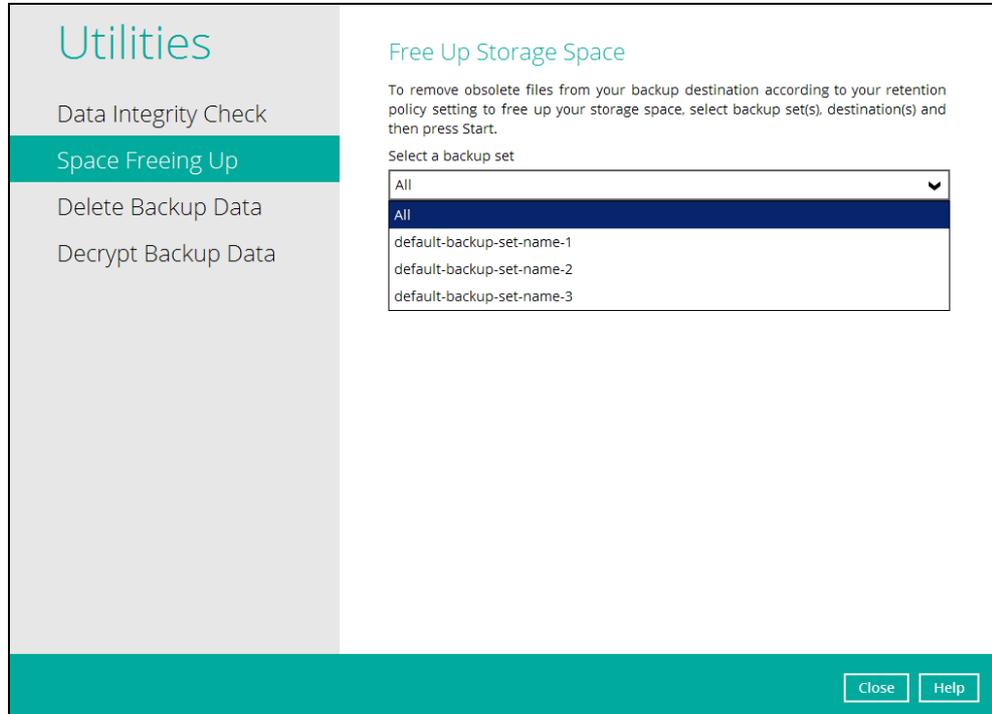


8.9.2 Space Freeing Up

This feature is used to remove obsolete file(s) from your backup set and destination (manually start retention policy). After the Space Freeing Up job is completed, the storage statistics of the backup set(s) are updated.

To perform Space Freeing Up, follow the instructions below:

1. Select a backup set from the drop-down list.



If you select a specific backup set, then you will also have to select a specific destination or all destinations.

Free Up Storage Space

To remove obsolete files from your backup destination according to your retention policy setting to free up your storage space, select backup set(s), destination(s) and then press Start.

Select a backup set

Backup Set Sample

Select a destination

DCS Backup CBS

Start

Close Help

If you select All backup sets, then there is no need to select a destination.

Utilities

Data Integrity Check

Space Freeing Up

Delete Backup Data

Decrypt Backup Data

Free Up Storage Space

To remove obsolete files from your backup destination according to your retention policy setting to free up your storage space, select backup set(s), destination(s) and then press Start.

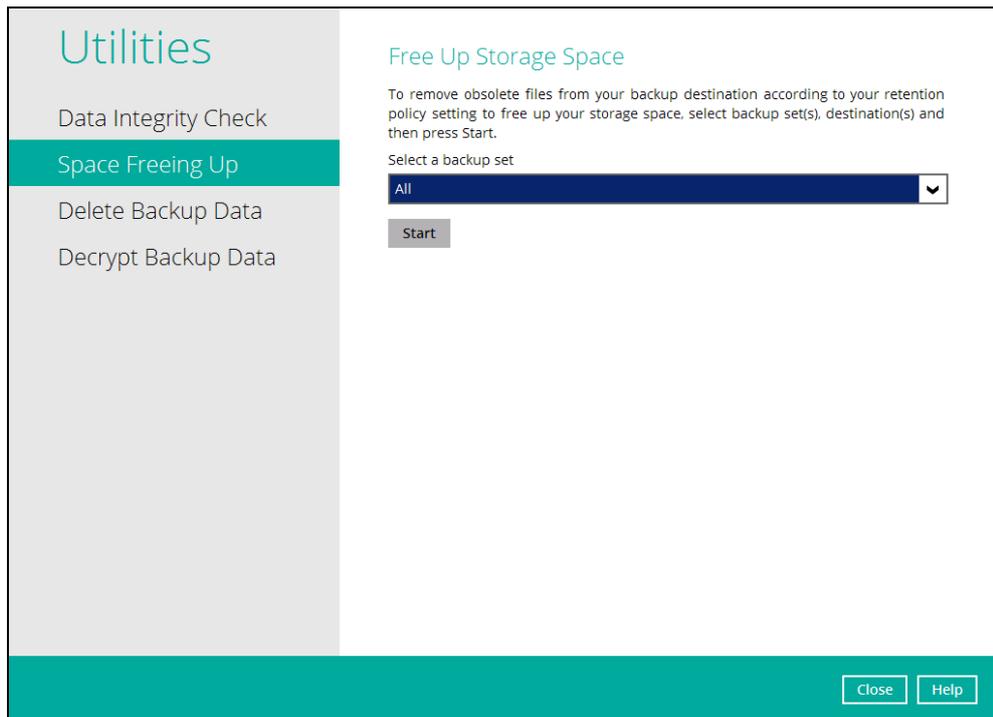
Select a backup set

All

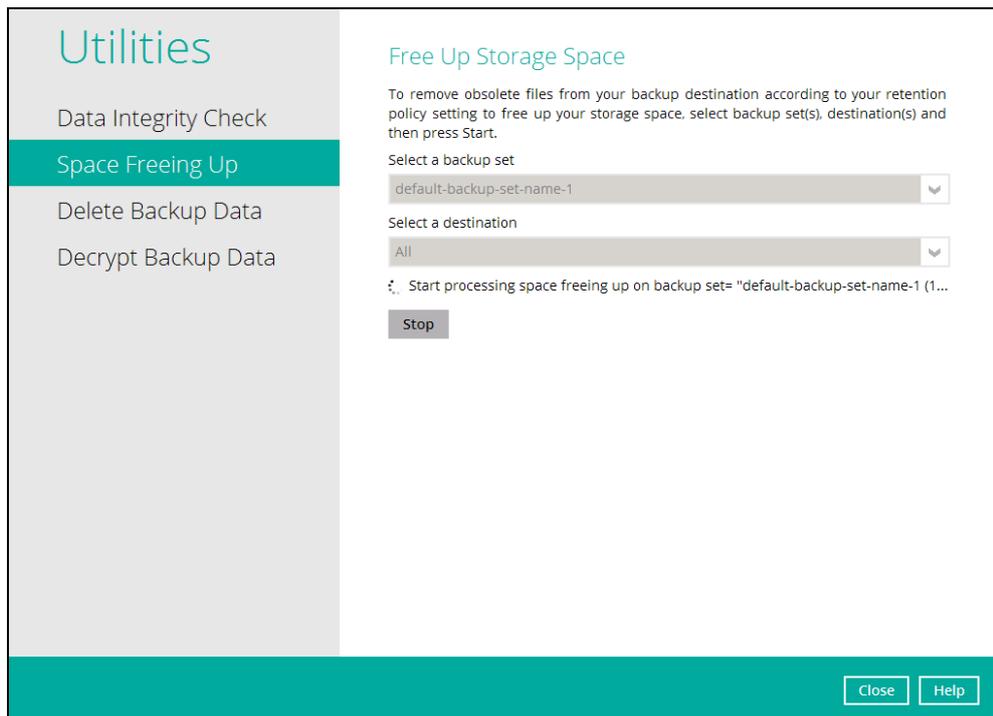
Start

Close Help

2. Click the [Start] button to perform space free up.



- Space freeing job will start running on the selected backup set(s) and backup destination(s).



- The status will be shown once completed. Click the [View log] button to see the detailed report of the space freeing up job.

Utilities

- Data Integrity Check
- Space Freeing Up**
- Delete Backup Data
- Decrypt Backup Data

Free Up Storage Space

To remove obsolete files from your backup destination according to your retention policy setting to free up your storage space, select backup set(s), destination(s) and then press Start.

Select a backup set

Select a destination

✓ Space freeing up is completed successfully

[View log](#)

[Close](#) [Help](#)

Log Show

| Type | Log | Time |
|--------|--|---------------------|
| Start | Start space freeing up on backup set "default-backup-set-name-1(1563858937672)" all destination | 07/23/2019 15:15:33 |
| Start | Start processing space freeing up on backup set="default-backup-set-name-1 (1563858937672)" destination="AhsayCBS (15... | 07/23/2019 15:15:33 |
| Save | Saving encrypted backup file index to 1563858937672/blocks at destination AhsayCBS... | 07/23/2019 15:15:35 |
| Space | Space freeing up on backup set="default-backup-set-name-1 (1563858937672)" destination="AhsayCBS (1563858951806)" i... | 07/23/2019 15:15:37 |
| Finish | Finished space freeing up on backup set "default-backup-set-name-1(1563858937672)" all destination | 07/23/2019 15:15:37 |

Logs per page Page

[Close](#) [Close](#) [Help](#)

8.9.3 Delete Backup Data

This feature is used to permanently delete backed up data from a backup set(s), destination(s), backup job, or delete all backed up data. After the data is deleted, the storage statistics of the backup set(s) are updated.

To perform deletion of backup data, follow the instructions below:

- Select a backup set from the drop-down list.

Utilities

- Data Integrity Check
- Space Freeing Up
- Delete Backup Data
- Decrypt Backup Data

Delete Backup Data

Delete backed up data of a specific backup set from a specific destination. This action will physically delete the selected data regardless the defined retention policy. Therefore, make sure you know what you are deleting and NO undo will be available afterward.

Select a backup set

All

All

Sample Backup Set 02

Sample Backup Set 01

Close
Help

NOTE: This will only delete the backed up files in a backup set(s) and destination(s), but the backup set and destination will remain.

If you select a specific backup set, then you will also have to select a specific destination or all destinations.

Utilities

- Data Integrity Check
- Space Freeing Up
- Delete Backup Data
- Decrypt Backup Data

Delete Backup Data

Delete backed up data of a specific backup set from a specific destination. This action will physically delete the selected data regardless the defined retention policy. Therefore, make sure you know what you are deleting and NO undo will be available afterward.

Select a backup set

Sample Backup Set 01

Select a destination

All

All

AhsayCBS

Close
Help

If you select **All** backup sets, then there is no need to select a destination.

Delete Backup Data

Delete backed up data of a specific backup set from a specific destination. This action will physically delete the selected data regardless the defined retention policy. Therefore, make sure you know what you are deleting and NO undo will be available afterward.

Select a backup set
Backup Set Sample

Select a destination
DCS Backup CBS

Select what to delete
Delete all backed up data

Delete

Close Help

2. If you choose to delete **All** backup set(s), the following message will be displayed. By clicking **Yes**, all backed up files from the selected backup set(s) and destination(s) will be deleted.

Utilities

- Data Integrity Check
- Space Freeing Up
- Delete Backup Data**
- Decrypt Backup Data

Delete Backup Data

Delete backed up data of a specific backup set from a specific destination. This action will physically delete the selected data regardless the defined retention policy. Therefore, make sure you know what you are deleting and NO undo will be available afterward.

Select a backup set
All

Delete

Delete all backup set files?

Yes No

Close Help

If you select a specific backup set, you will have an option to choose a destination.

If you select a specific destination, there are two (2) available options for the type of files you wish to delete.

- Delete all backed up data
- Choose from ALL files

Delete Backup Data

Delete backed up data of a specific backup set from a specific destination. This action will physically delete the selected data regardless the defined retention policy. Therefore, make sure you know what you are deleting and NO undo will be available afterward.

Select a backup set

Backup Set Sample ▼

Select a destination

DCS Backup CBS ▼

Select what to delete

Delete all backed up data ▼

Delete

Close Help

Delete all backed up data

If you choose this option, the following message will be displayed. By clicking **Yes**, all backed up data from the selected backup set(s) and destination(s) will be deleted.

DCS Backup PRO

Utilities

Data Integrity Check

Space Freeing Up

Delete Backup Data

Delete backed up data of a specific backup set from a specific destination. This action will physically delete the selected data regardless the defined retention policy. Therefore, make sure you know what you are deleting and NO undo will be available afterward.

Select a backup set

?

Delete all files (Backup Set Sample - DCS Backup CBS)?

Yes No

Close Help

Choose from ALL files

If you choose this option, you can select to delete any file(s) in the backup set.

Delete Backup Data

Delete backed up data of a specific backup set from a specific destination. This action will physically delete the selected data regardless the defined retention policy. Therefore, make sure you know what you are deleting and NO undo will be available afterward.

Select a backup set

Backup Set Sample

Select a destination

DCS Backup CBS

Select what to delete

Choose from ALL files

| Folders | Name | Size | Date modified |
|---|---|------|---------------|
| DCS Backup CBS | <input checked="" type="checkbox"/> C:\ | | |
| <input checked="" type="checkbox"/> C:\ | | | |
| <input checked="" type="checkbox"/> Users | | | |

Close Help

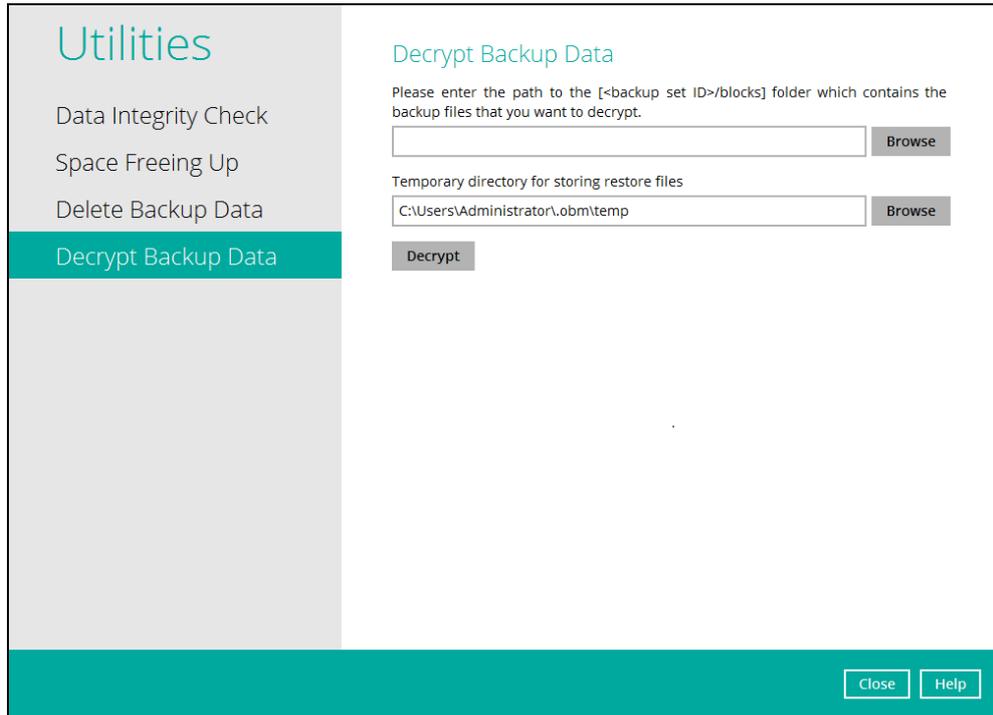
3. Click the [Delete] button, then click [Yes] to start the deletion of files.
4. Files are successfully deleted.

8.9.4 Decrypt Backup Data

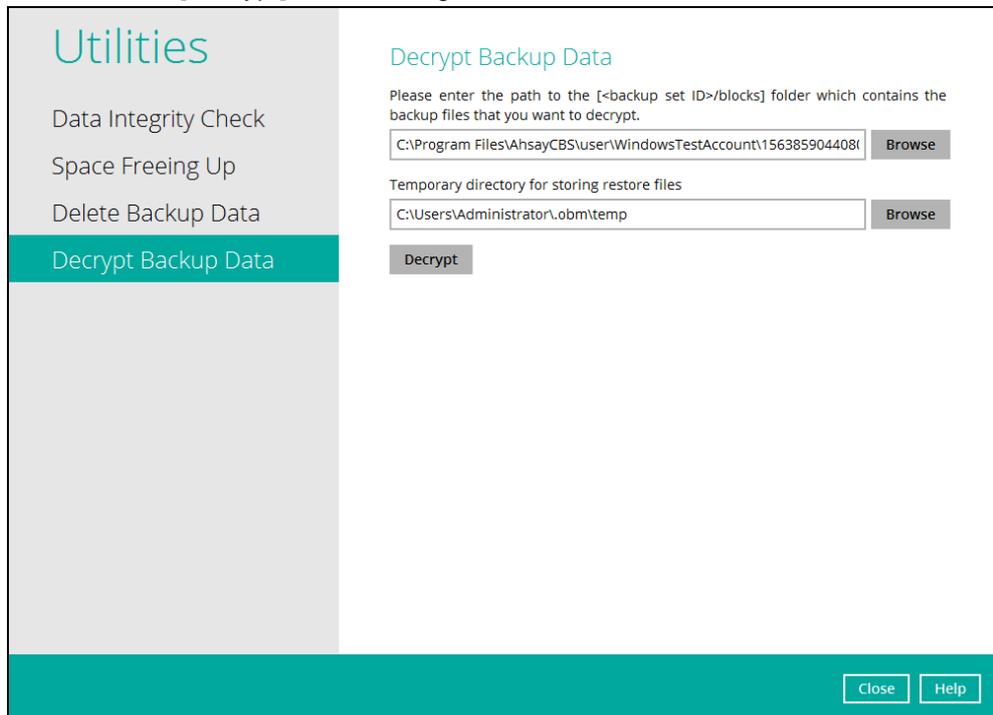
This feature is used to restore raw data by using the data encryption key that was set for the backup set.

To perform decryption of backup data, follow the instructions below:

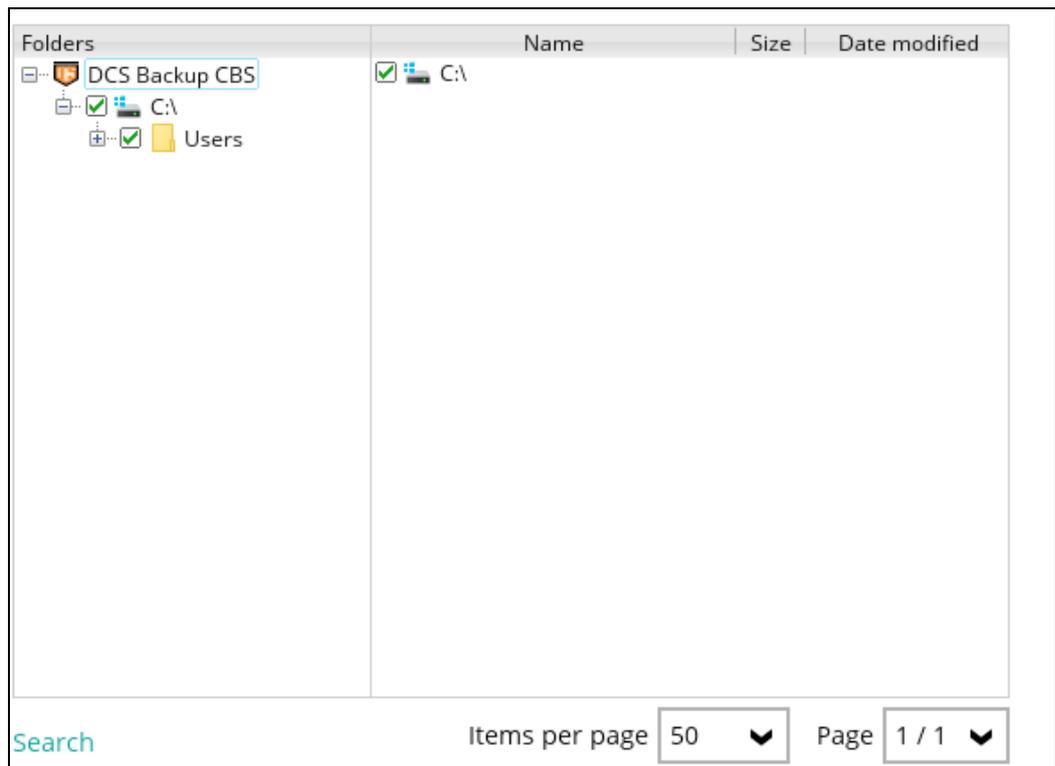
1. Click the [Browse] button to locate the path of the backup set ID / blocks folder.



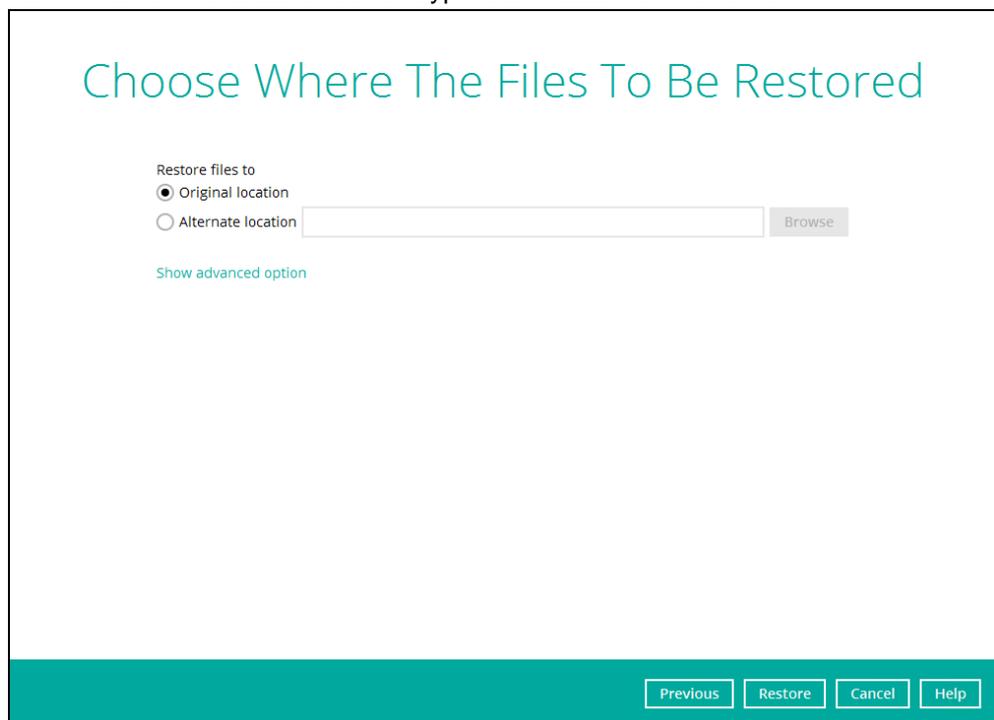
2. Click the [Browse] button to re-select the temporary folder for the decrypt process. Then click the [Decrypt] button to begin.



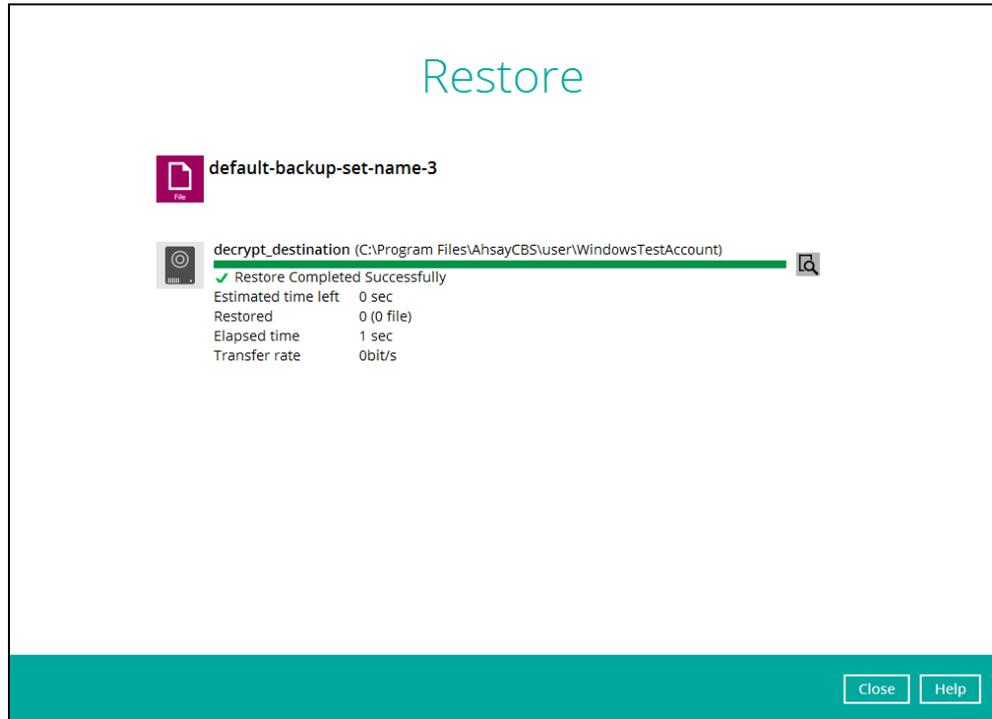
3. Select files to be decrypted.



4. Choose the location where the decrypted files will be restored to.

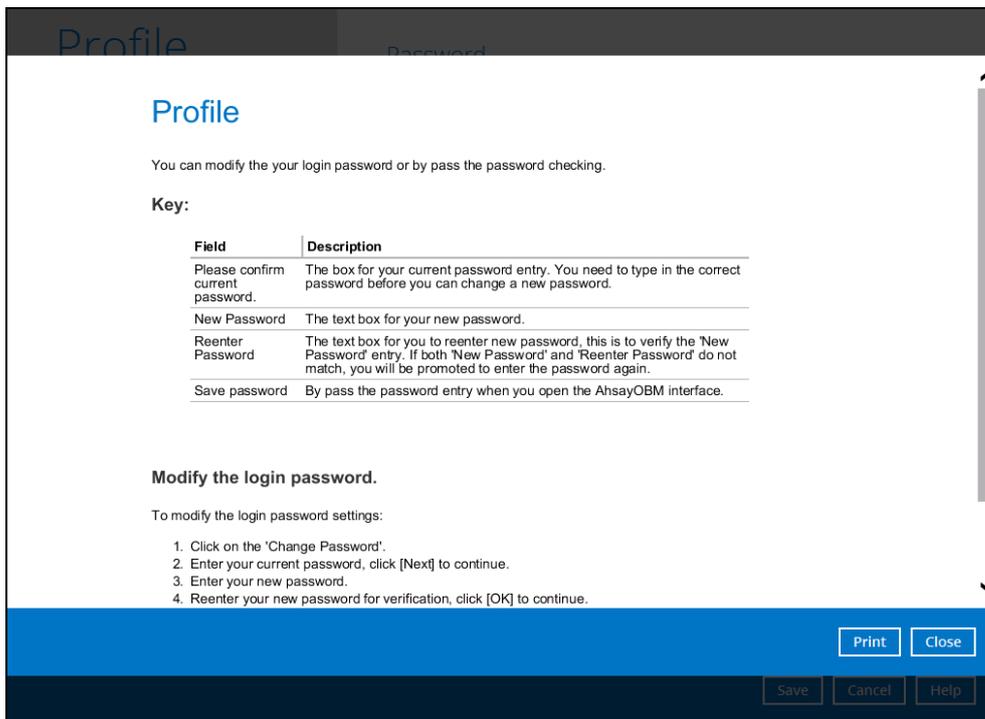
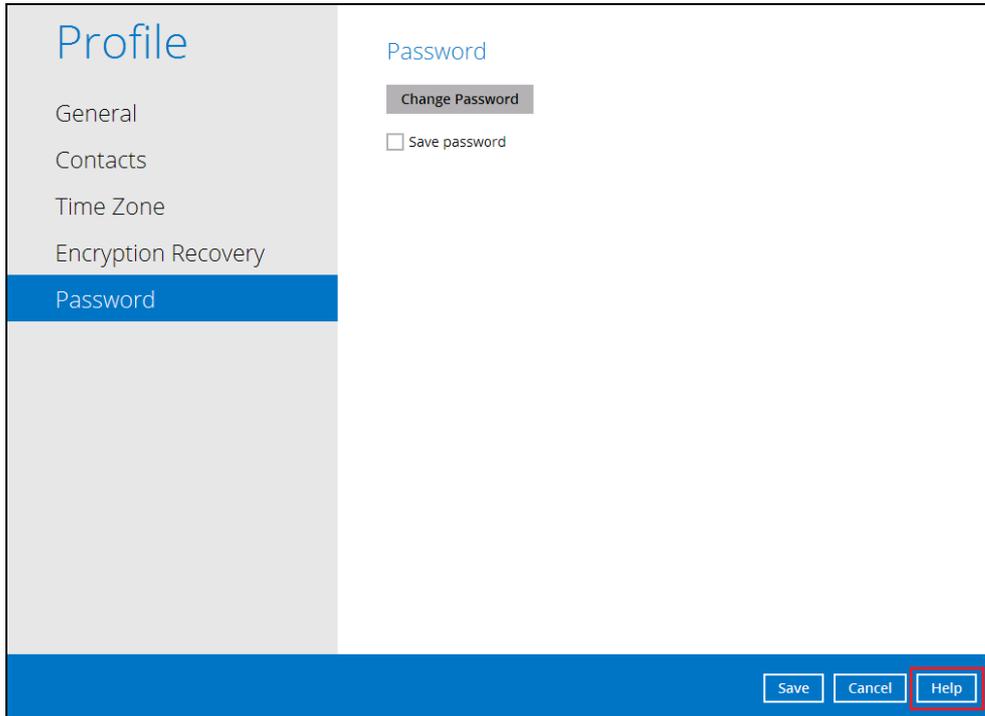


5. The status will be shown once completed.



8.10 Online Help

This allows the user to view the summary of information and instructions of each available features in OBM.

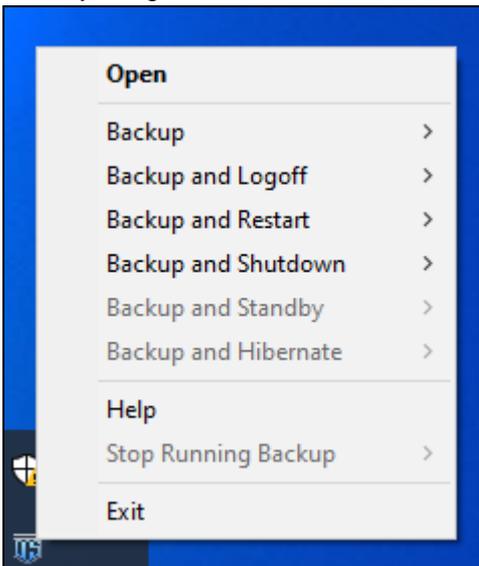


8.11 System Tray

If OBM is installed in the computer, you will see an OBM icon in the taskbar at the lower right corner of the screen.



When you right-click the OBM icon, a control menu will pop-up.

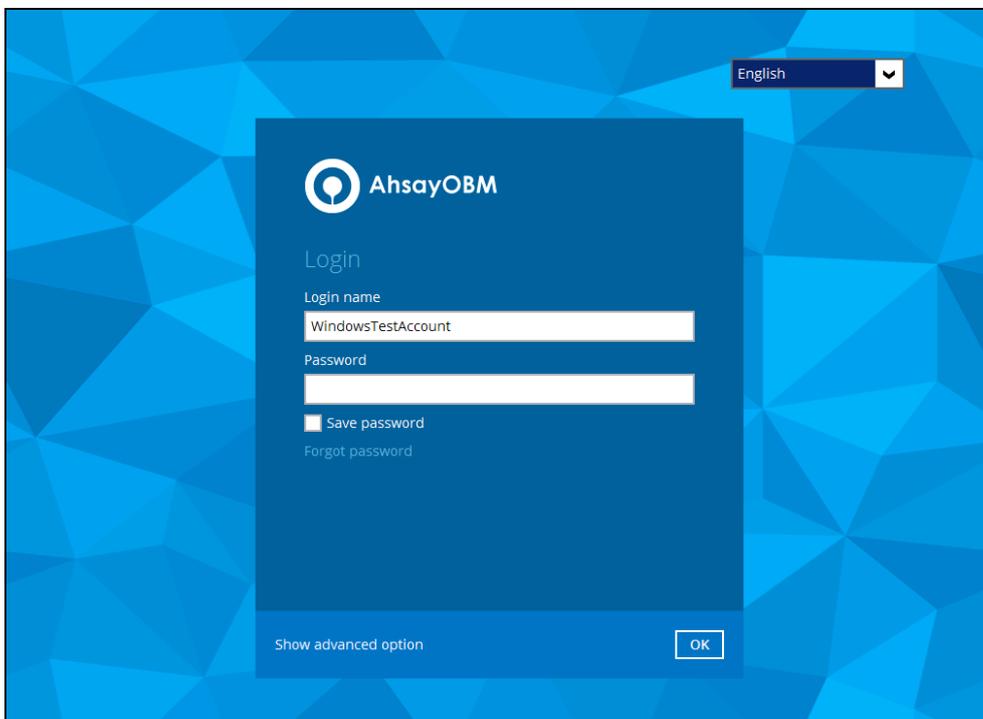
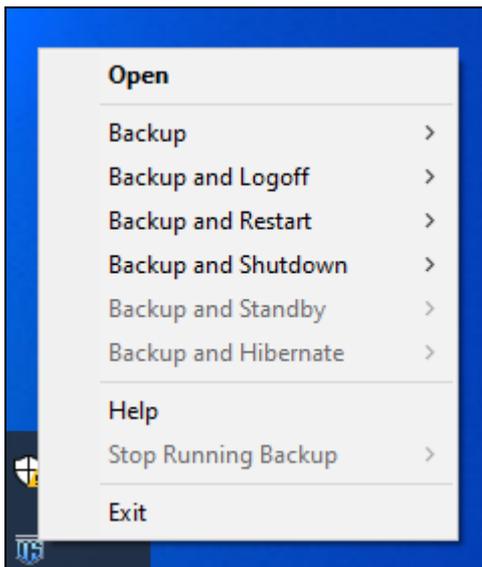


OBM system tray has ten (10) controls:

- Open
- Backup
- Backup and Logoff
- Backup and Restart
- Backup and Shutdown
- Backup and Standby
- Backup and Hibernate
- Help
- Stop Running Backup
- Exit

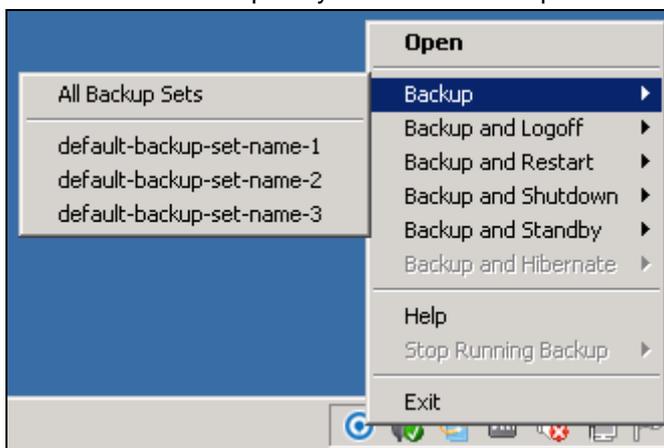
Open

Select this option to open the OBM login screen.



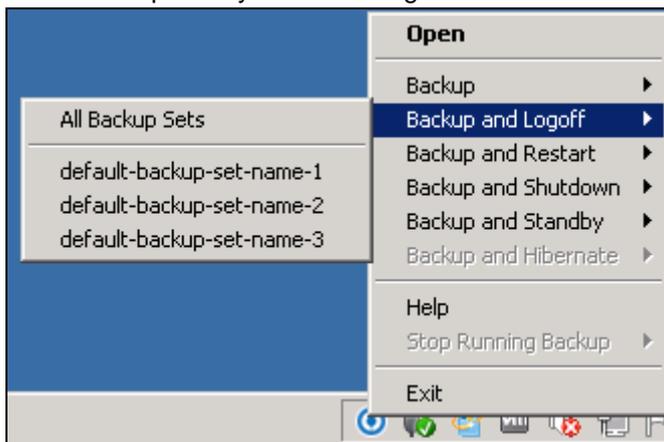
Backup

If you want to perform a backup without going to the interface, hover the mouse to this option and select the backup set you want to back up.



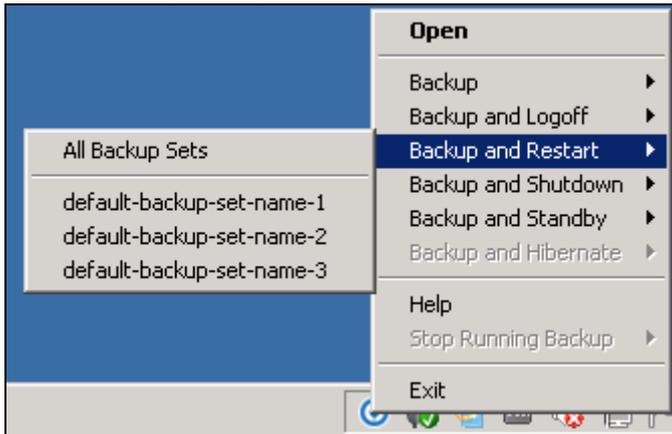
Backup and Logoff

Select this option if you want to logoff Windows after a manual backup job is done.



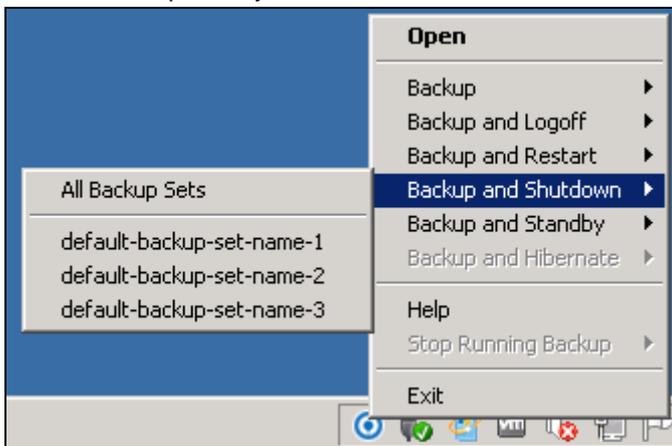
Backup and Restart

Choose this option if you want the machine to restart after a manual backup job is done.



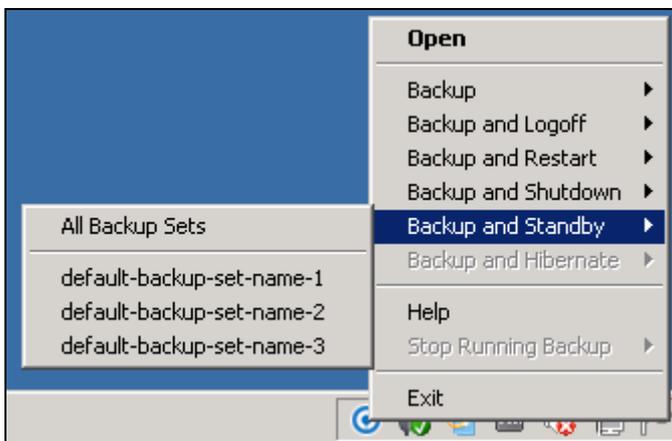
Backup and Shutdown

Choose this option if you want the machine to shut down after a manual backup job is done.



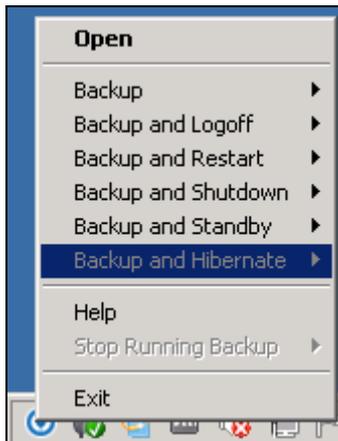
Backup and Standby

Choose this option if you want the machine to go on standby after a manual backup job is done.



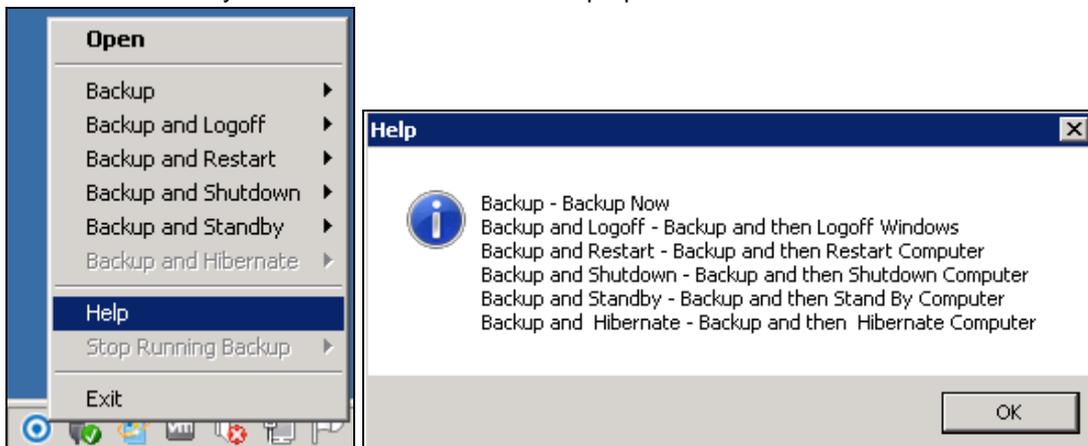
Backup and Hibernate

Choose this option if you want the machine to hibernate after a manual backup job is done. This will be disabled if hibernate mode is not available on the Windows version you are using.



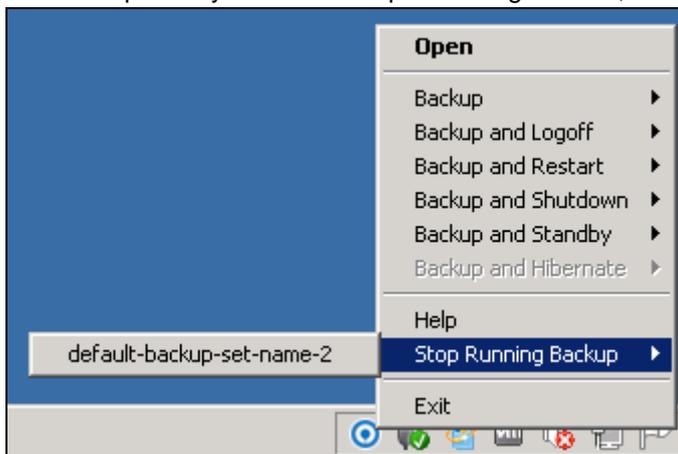
Help

This tab will show you the function of each backup option.

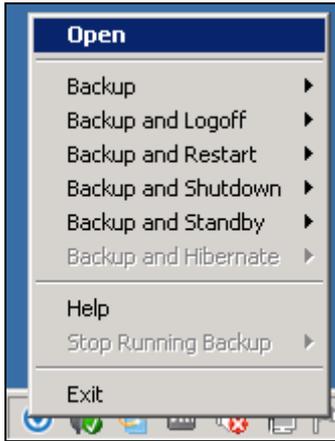


Stop Running Backup

Use this option if you wish to stop a running manual, continuous or scheduled backup.

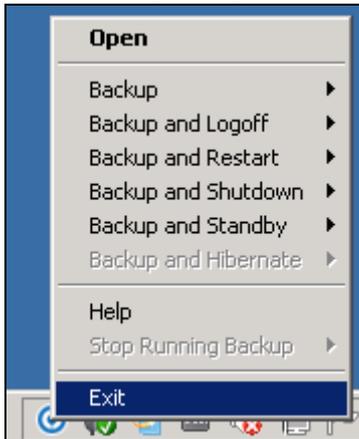


This option will be disabled if there is no backup job running.



Exit

Select this option if you want to close the application including the OBM icon at the taskbar.

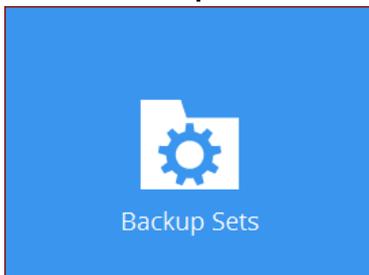


9 Create a Backup Set

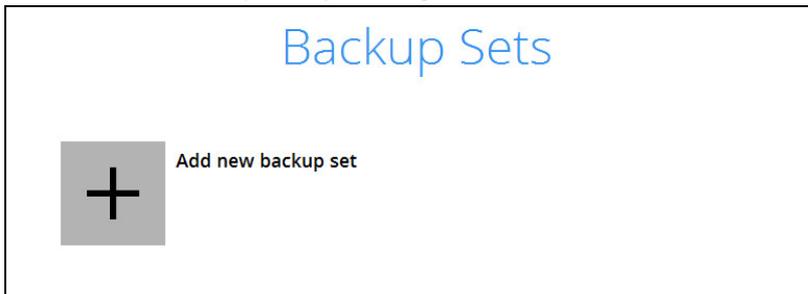
Starting with v8.3.4.0 and onwards, network drive support has been enhanced which will allow users to access different network drives not limited to Windows-based backup source. This enhancement will support:

- Network drives with different login credentials instead of limited to Windows User Authentication login or network drives without login credential.
- Network drives without the need for them to be setup first on Windows.
- Network drives as Backup Source (including filter), Backup Destination and Restore Location (Original or Alternate).

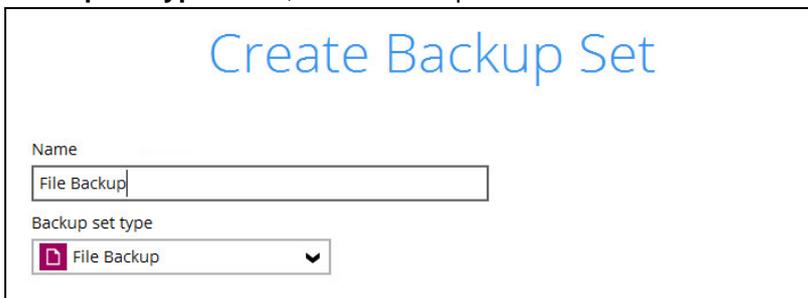
1. Click the **Backup Sets** icon on the OBM main interface.



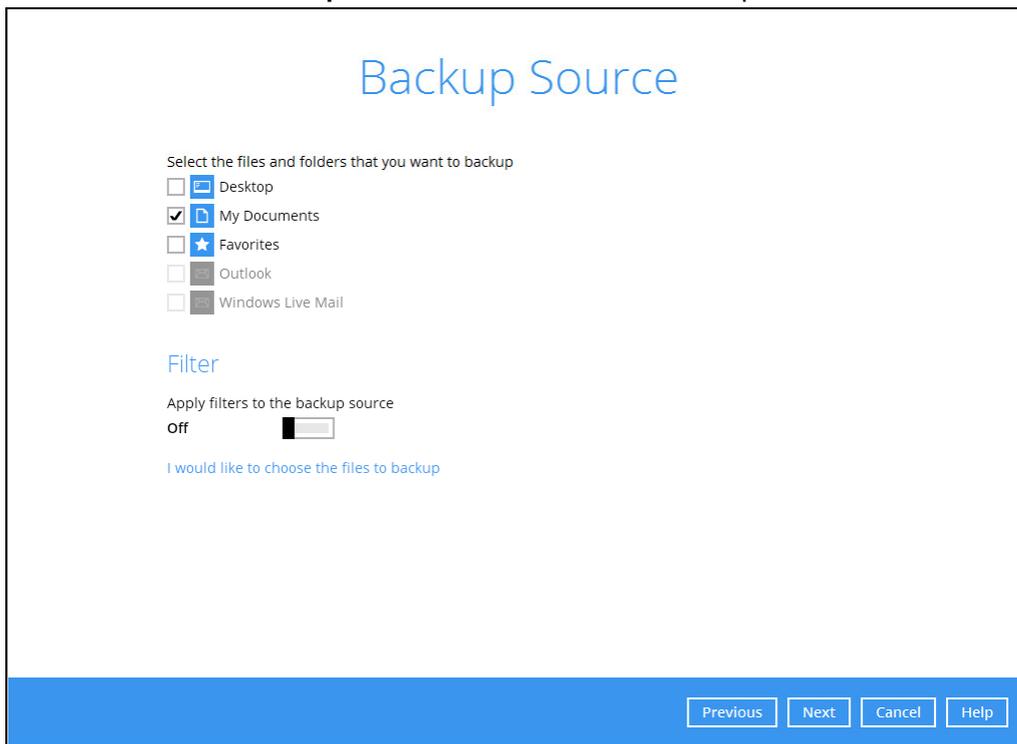
2. Create a new backup set by clicking the "+" icon next to **Add new backup set**.



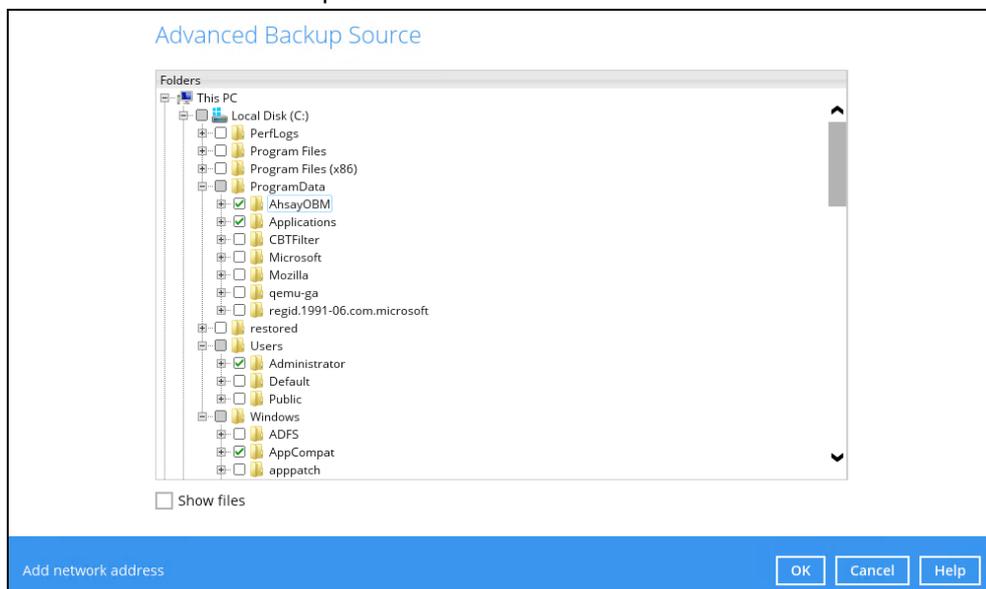
3. When the Create Backup Set window appears, name your new backup set, and select the **Backup set type**. Then, click **Next** to proceed.

A screenshot of the "Create Backup Set" window. The title "Create Backup Set" is at the top. Below it is a form with two fields: "Name" with a text input field containing "File Backup", and "Backup set type" with a dropdown menu showing "File Backup" and a downward arrow.

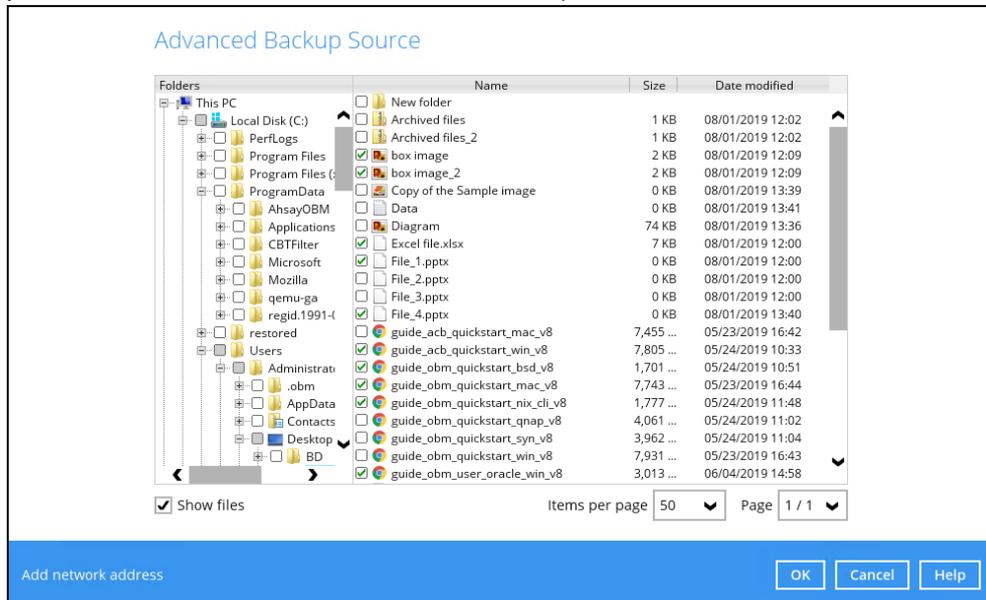
4. In the Backup Source window, select the files and folders for backup. Click **I would like to choose the files to backup** to select individual files for backup.



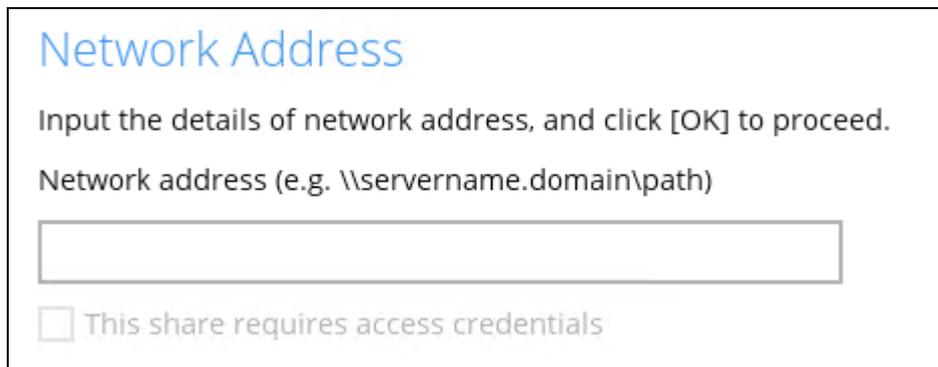
5. In the Advanced Backup Source window there are three (3) ways to select file(s) and folder(s) for back up:
- Select folder(s) to back up all files in the folder(s). Click **OK** to save the selection and close the Advanced Backup Source window.



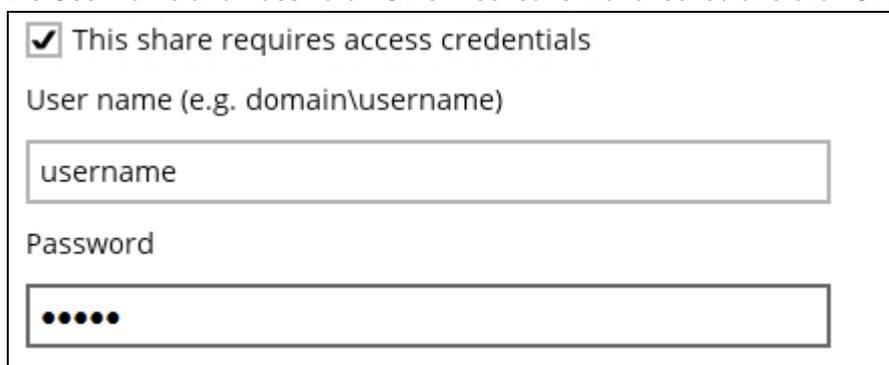
- ii. Back up only individual file(s) instead of all files in the selected folder(s). Check the **Show files** checkbox at the bottom of the screen. A list of files will appear on the right-hand side. Select the checkbox(es) next to the file(s) to back up. Then, click **OK** to save your selections and close the Advanced Backup Source window.



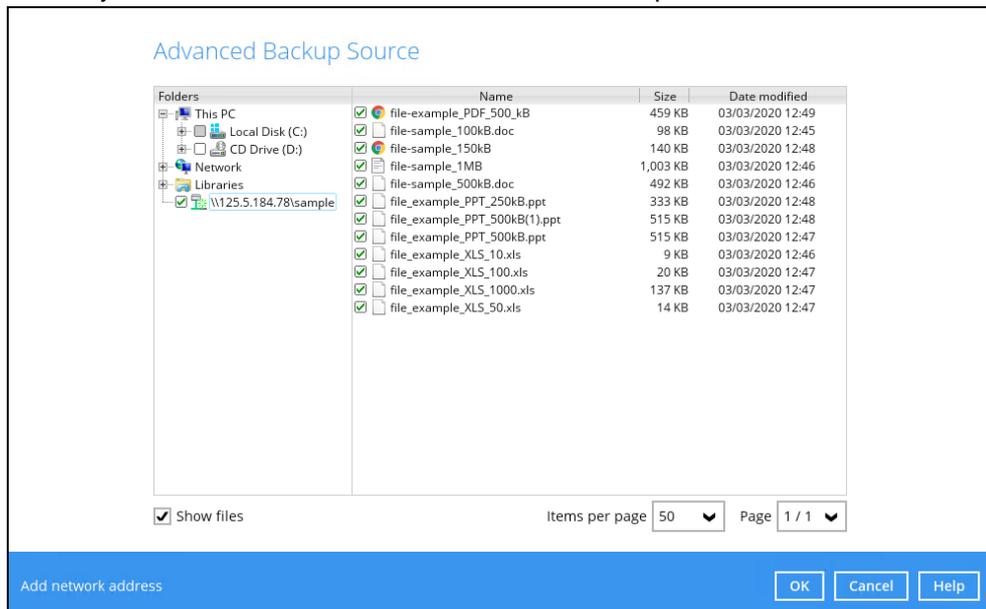
- iii. Back up file(s) and/or folder(s) located in a network drive. Click the **Add network address** link at the bottom of the screen. In the Network Address window, enter the network address.



Once a network address is entered, **This share requires access credentials** will be enabled. Check the box beside it if access credentials are required to backup and enter the User name and Password. Otherwise leave it unchecked and click **OK**.



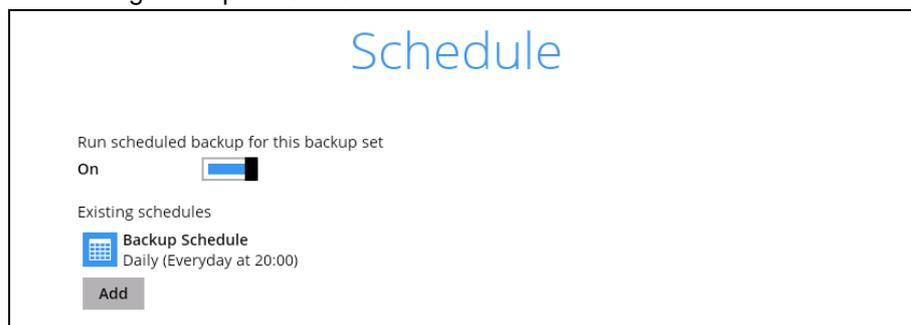
The network drive will now be added and automatically selected. There is still an option to select only specific file(s) to back up by checking the **Show files** checkbox. Click **OK** to save your selections and close the Advanced Backup Source window.



NOTE

Once a network drive is added, its network credentials may still be edited. For instructions on how to do this please refer to [Appendix F: How to Manage non-Windows based Network Drives](#).

6. In the Backup Source window, click **Next** to proceed.
7. When the **Schedule** window appears, you can configure a backup schedule to automatically run a backup job at your specified time interval. In the Schedule window, the Run scheduled backup for this backup set is **On** by default.
 - In the default backup schedule, there will be a scheduled backup that will be performed daily at 8pm. You can leave it as is or you can modify it by clicking on the existing backup schedule.



- If you want to add another schedule, click **Add**. When the New Backup Schedule window appears, specify your backup schedule. Then, click **OK** to save your changes and close the New Backup Schedule window.

New Backup Schedule

Name
Daily-1

Type
Daily

Start backup
at 13 : 00

Stop
until full backup completed

Run Retention Policy after backup

OK Cancel Help

8. In case you have added a schedule, it will be shown in the Schedule window. Click **Next** to proceed when you are done setting.
9. The **Destination** window will appear.

Destination

Backup mode
Sequential

Existing storage destinations
+ Add new storage destination / destination pool

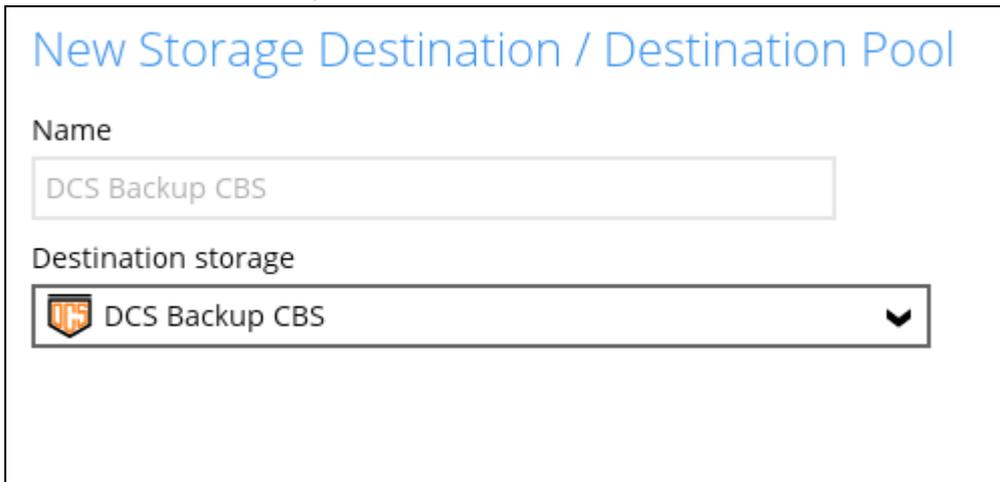
^ v

Select the appropriate option from the **Backup mode** dropdown menu.

- **Sequential** (default value) – run backup jobs to each backup destination one by one
- **Concurrent** – run backup jobs to all backup destinations at the same time

To select a backup destination for the backup data storage, click **+** next to **Add new storage destination / destination pool**.

10. In the **New Storage Destination / Destination Pool** window, select the destination storage. Then, click **OK** to confirm your selection.



New Storage Destination / Destination Pool

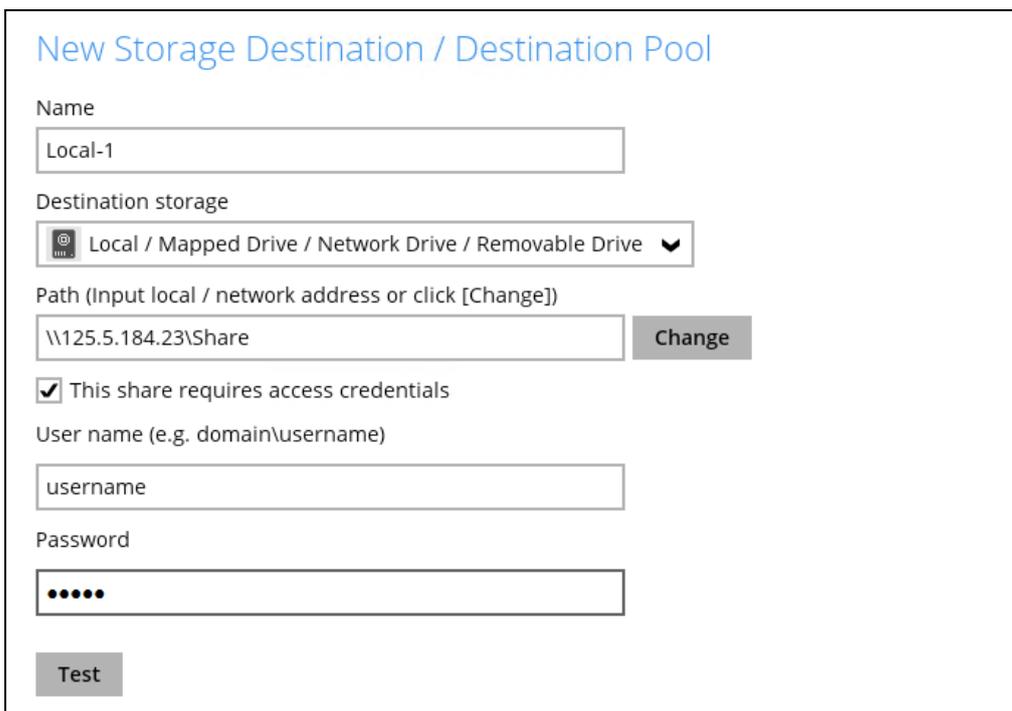
Name

DCS Backup CBS

Destination storage

DCS Backup CBS

If **Local / Mapped Drive / Network Drive / Removable Drive** is selected, you need to specify the path by clicking **Change** to select the path or you can manually enter it. Once a network address is entered, **This share requires access credentials** check box will be enabled. Check the box beside it if access credentials are required to connect to the storage destination and enter the User name and Password. Otherwise, leave it unchecked and click **Test** to check the connection. Click **OK** to add the storage destination.



New Storage Destination / Destination Pool

Name

Local-1

Destination storage

Local / Mapped Drive / Network Drive / Removable Drive

Path (Input local / network address or click [Change])

\\125.5.184.23\Share Change

This share requires access credentials

User name (e.g. domain\username)

username

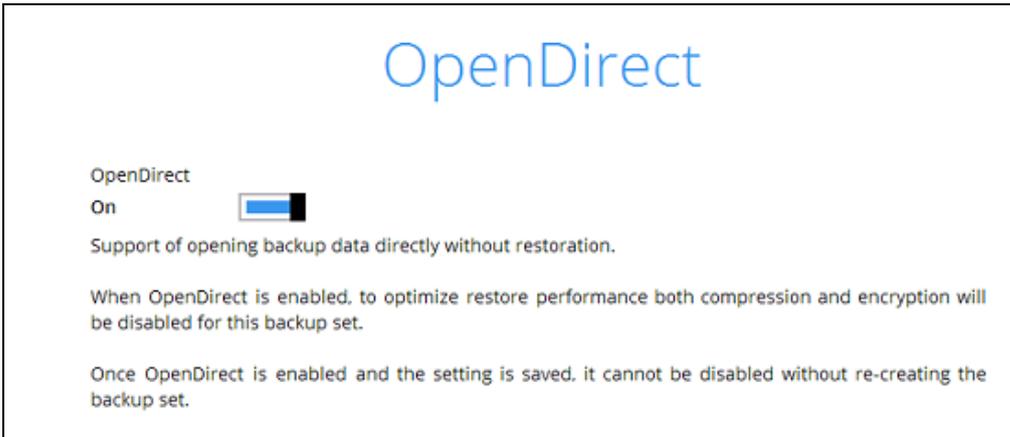
Password

.....

Test

11. In the **Destination** window, your selected storage destination will be shown. Click **Next** to proceed.

12. If you wish to enable the **OpenDirect Restore** feature, make sure you turn on the OpenDirect restore switch in this menu. Click **Next** to proceed.

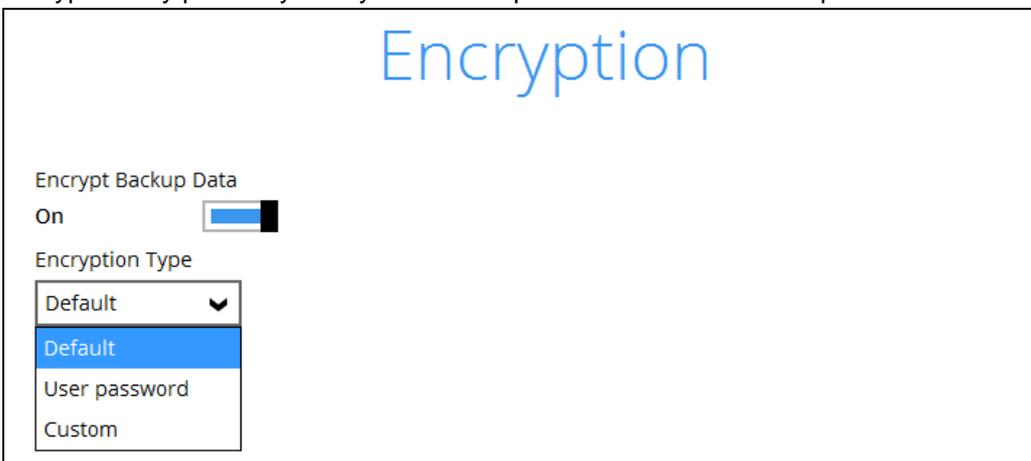


NOTES

1. Once the OpenDirect Restore feature is enabled and the backup set is saved, it is **NOT** possible to disable it afterwards, and vice versa. A new backup set will have to be created again if you wish to do so.
2. It is possible to enable both OpenDirect restore and Run Direct restore at the same time. However, OBM restore job will only allow either OpenDirect or Run Direct to run, but not to run concurrently.
3. OpenDirect restore requires an additional OpenDirect restore module license to work. Contact your backup service provider for further details.
4. OpenDirect restore might not be available, this depends on your backup service provider settings. Contact your backup service provider for more information.

13. **IMPORTANT:** If you have enabled the OpenDirect Restore, backup data will not be compressed and encrypted to optimize restore performance, therefore you can skip to step 16.

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 OBM at the time when this backup set is created. Please be reminded that if you change the OBM 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.

Encryption

Encrypt Backup Data
On

Encryption Type
Custom ▼

Algorithm
AES ▼

Encryption key

Re-enter encryption key

Method
 ECB CBC

Key length
 128-bit 256-bit

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

14. 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.

Encryption

Encrypt Backup Data
On

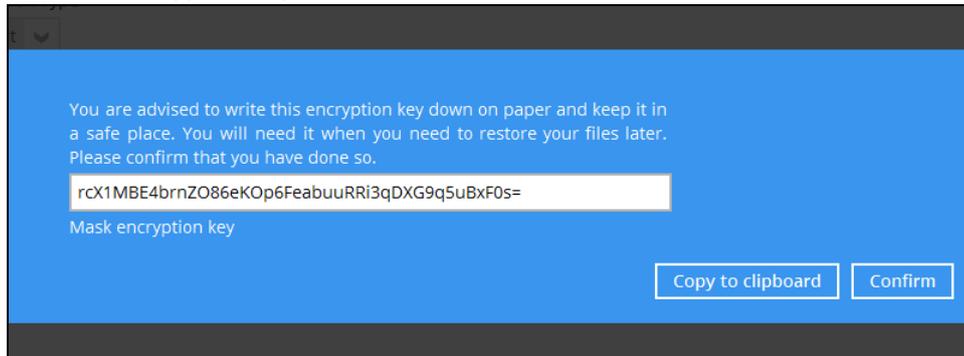
Encryption Type
Default ▼

You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

[Unmask encryption key](#)

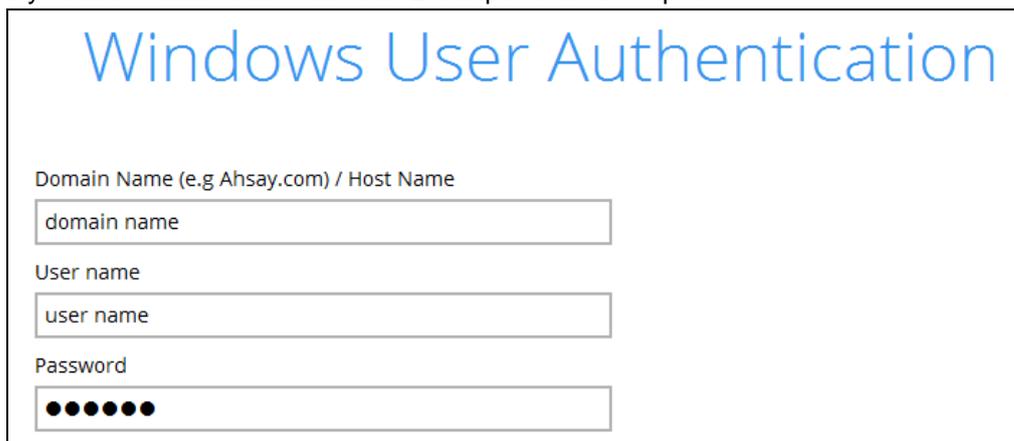
The pop-up window has the following three options to choose from:

- **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.

15. The following screen prompts you to enter the Windows login credentials for user authentication if you have enabled the Schedule Backup feature in step 8.

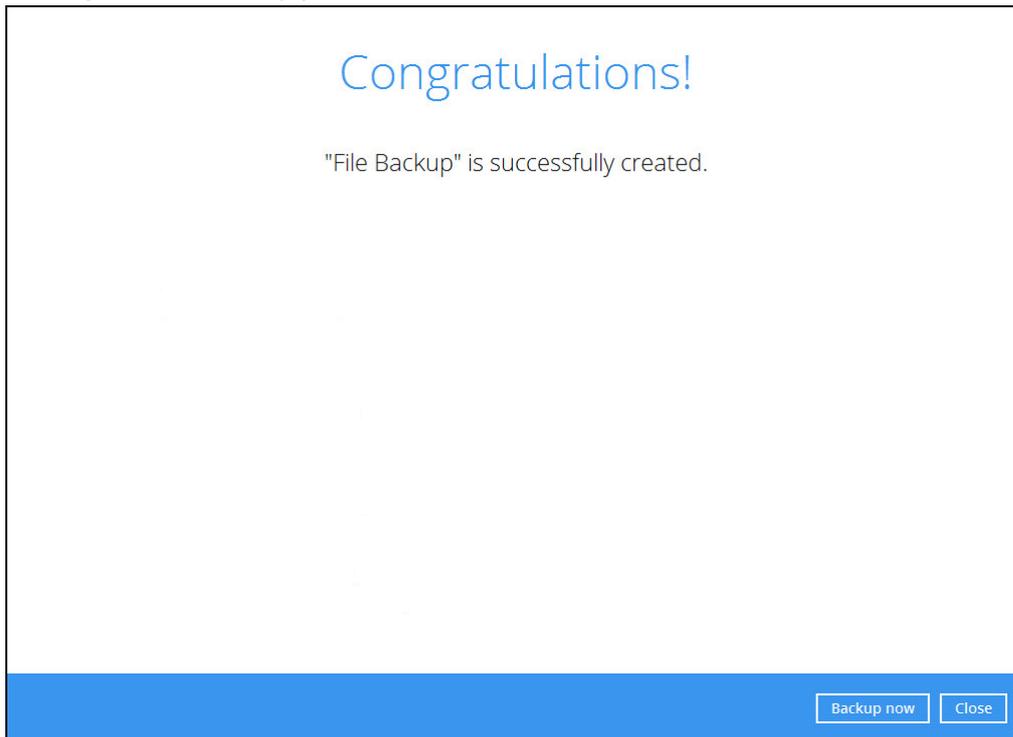


NOTE

If you have selected to back up individual folder(s) / file(s) on your local computer's drive in step 5, the Windows User Authentication request will be bypassed and therefore the screen shown above will not display even though the Schedule Backup feature has been turned on.

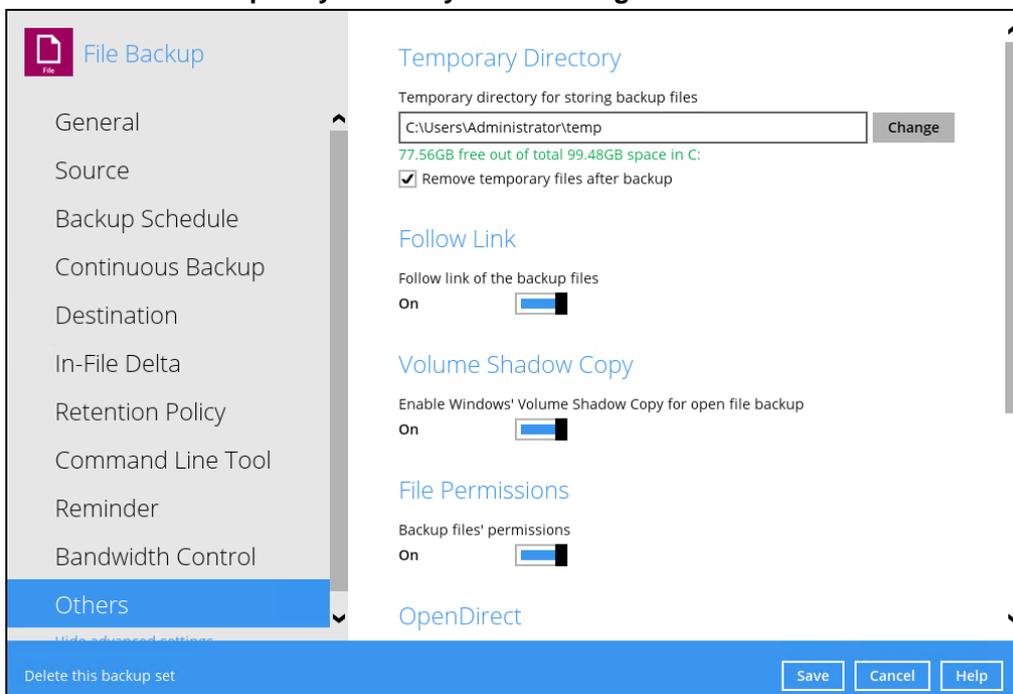
It is recommended to enter the information of user with Administrator privilege to support backup of network drives.

16. Upon successful creation of the backup set, the following screen will appear. You can click **Backup now** to back up your data or click **Close** to exit.



17. Based on [Best Practices and Recommendations](#), it is highly recommended to change the **Temporary Directory**. Select another location with sufficient free disk space other than Drive C.

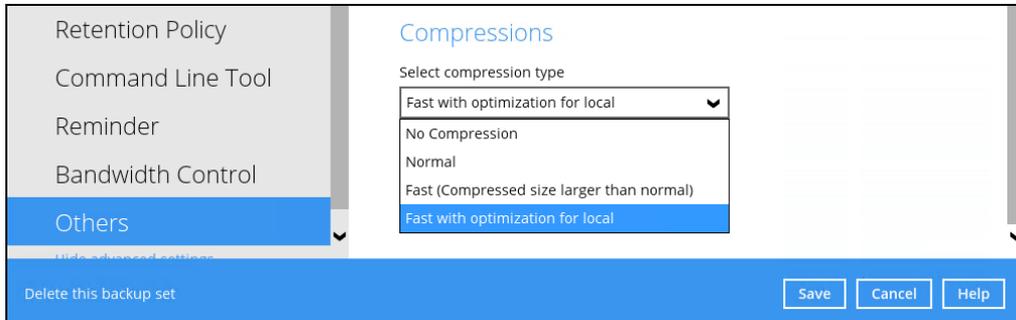
Go to **Others > Temporary Directory**. Click **Change** to browse for another location.



18. Optional: Select your preferred **Compression** type. By default, the compression is Fast with optimization for local.

Go to **Others > Compressions**. Select from the following:

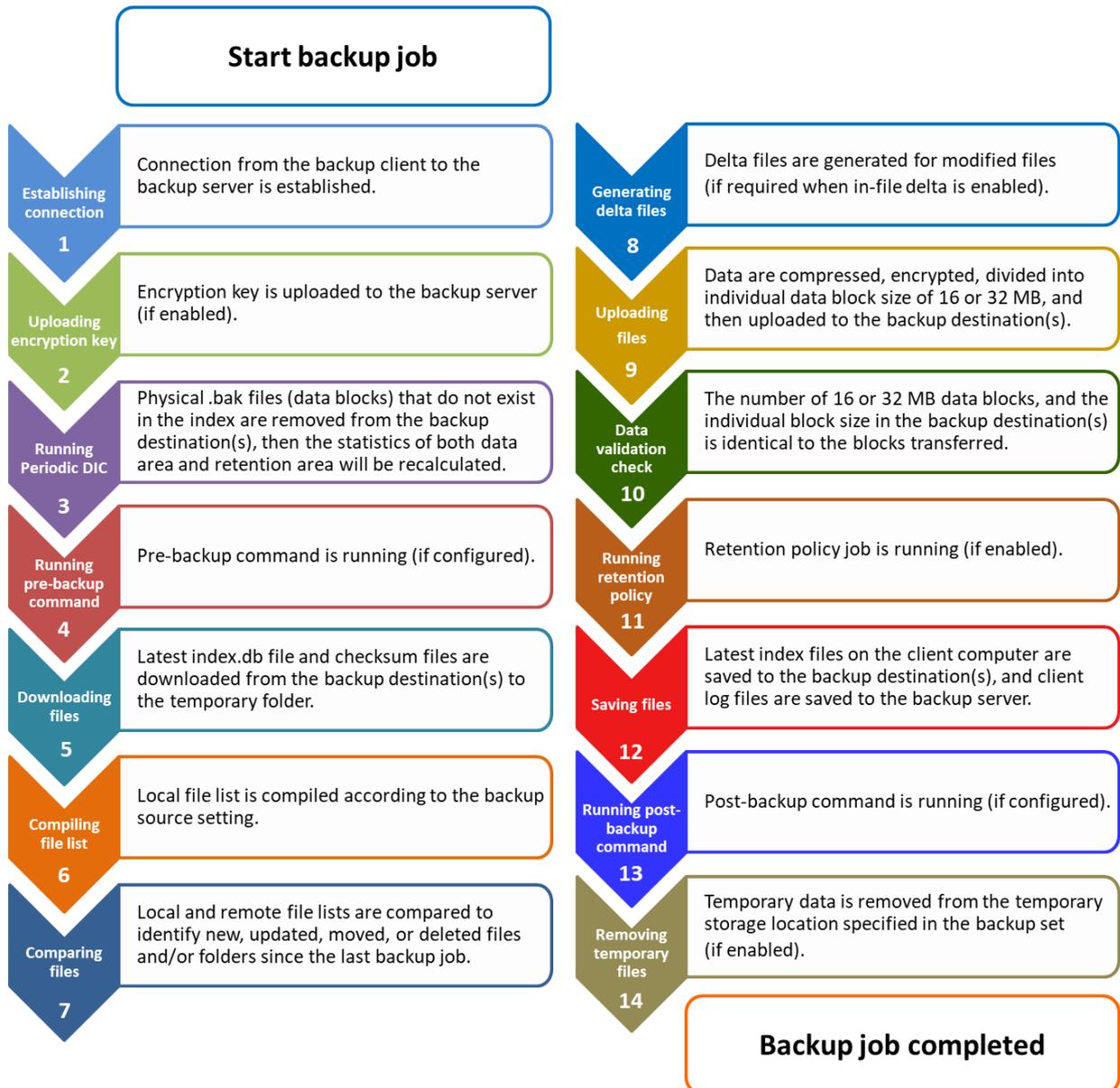
- No Compression
- Normal
- Fast (Compressed size larger than normal)
- Fast with optimization for local



10 Overview on the Backup Process

The following steps are performed during a backup job. For an overview of the detailed process for Steps 3, 5, 10, and 12, please refer to the following chapters.

- [Periodic Data Integrity Check \(PDIC\) Process \(Step 3\)](#)
- Backup Set Index Handling Process
 - [Start Backup Job \(Step 5\)](#)
 - [Completed Backup Job \(Step 12\)](#)
- [Data Validation Check Process \(Step 10\)](#)



10.1 Periodic Data Integrity Check (PDIC) Process

For OBM v8.3.6.0 (or above), the PDIC will run on the first backup job that falls on the corresponding day of the week from **Monday to Friday**.

To minimize the impact of the potential load of large number of PDIC jobs running at the same time on the DCS CBS server, the schedule of a PDIC job for each backup set is automatically determined by the result of the following formula:

| |
|---|
| <i>PDIC schedule = %BackupSetID% modulo 5</i> or <i>%BackupSetID% mod 5</i> |
|---|

The calculated **result** will map to the corresponding day of the week (i.e., from Monday to Friday).

| | |
|----------|------------------|
| 0 | Monday |
| 1 | Tuesday |
| 2 | Wednesday |
| 3 | Thursday |
| 4 | Friday |

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

Calculation: $1594627447932 \text{ mod } 5 = 2$

| | |
|----------|------------------|
| 2 | Wednesday |
|----------|------------------|

In this example:

- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTES

Although according to the PDIC formula for determining the schedule is ***%BackupSetID% mod 5***, this schedule only applies if the previous PDIC job was actually run more than 7 days prior.

Under certain conditions, the PDIC may not run strictly according to this formula. For example:

1. If OBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.
2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it detects that the previous PDIC job was run more than 7 days ago.
3. Every time a data integrity check (DIC) is run, the latest PDIC run date is reset, the next PDIC job will run after 7 days.
4. The PDIC job will not run if there are no files in both the data and retention areas. For example: a newly created backup set with no backup job history or a backup set where all the data has been deleted using the [Delete Backup Data](#) feature.
5. The PDIC job will not run on a backup set that contains any data which still in v6 format. It will only run if all v6 data format on a backup set has undergone data migration to v8 block format.

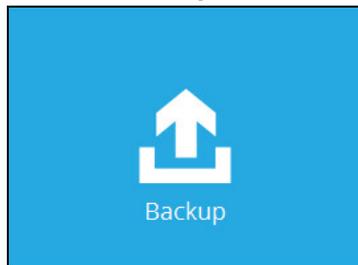
11 Run Backup Jobs

11.1 Login to OBM

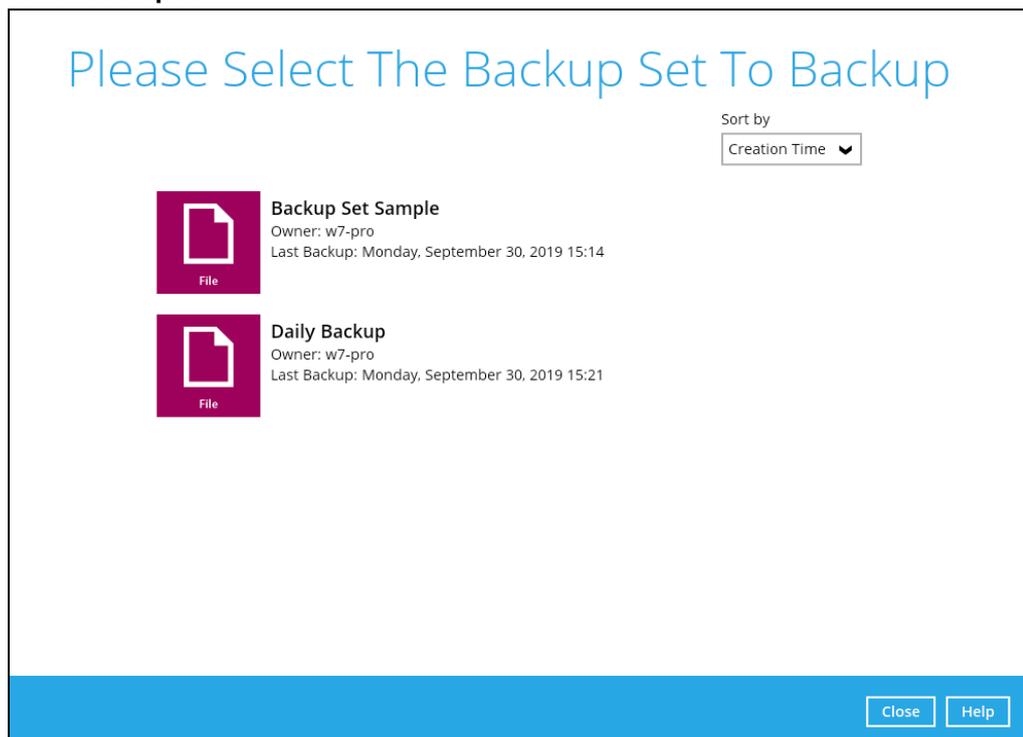
Login to the OBM application according to the instructions in [Chapter 7 Start OBM](#).

11.2 Start a Manual Backup

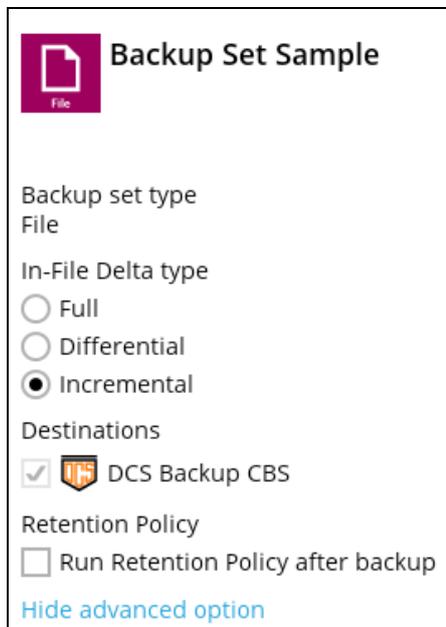
1. Click the **Backup** icon on the main interface of OBM.



2. Select the backup set which you would like to start a backup for. In case you want to modify the In-File Delta type, Destinations and Retention Policy settings, click **Show advanced option**.

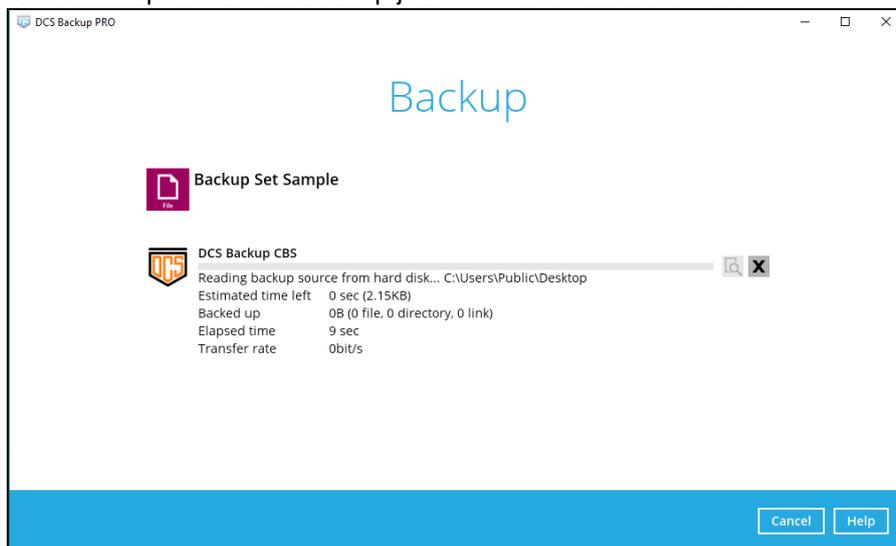


- When advanced options are shown, it is recommended that you tick the checkbox next to **Run Retention Policy after backup** in the Retention Policy section at the bottom. This will help you save hard disk quota in the long run. In the In-File Delta type section, the following three options are available:

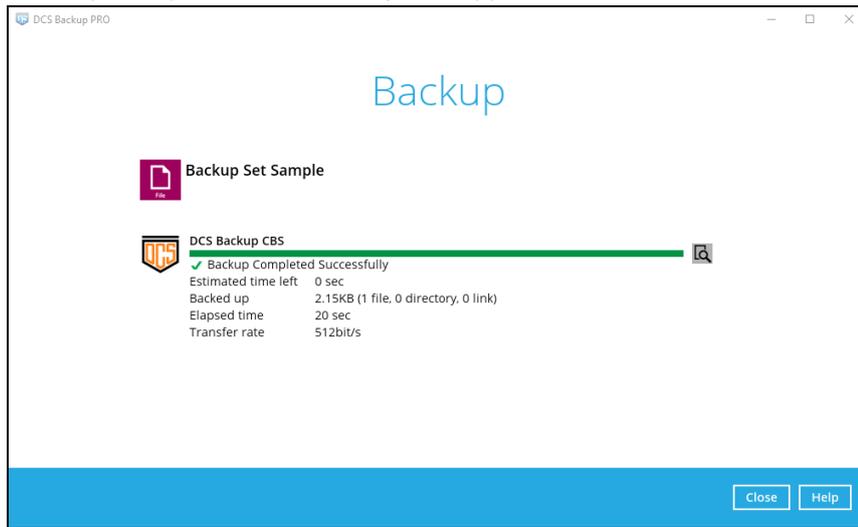


- Full** – A full backup captures all the data that you want to protect. When you run a backup job for the first time, OBM will run a full backup regardless of the in-file delta setting.
- Differential** – A differential backup captures only the changes made as compared with the last uploaded full file only (i.e. changes since the last full backup, not since the last differential backup).
- Incremental** – An incremental backup captures only the changes made as compared with the last uploaded full or delta file (i.e. changes since the last incremental backup).

- Click Backup to start the backup job. The status will be shown.



- When the backup is completed, the progress bar will be green in color and the message “Backup Completed Successfully” will appear.



- You can click the  **View** icon on the right-hand side to check the log. A window will pop up to show the log. Click **Close** to exit the pop-up window.

Backup set
Destination

Log
Show

| Type | Log | Time |
|---|---|---------------------|
|  | The In-File Delta Backup feature is not enabled on this account. Please be aware that files are being backed up in their ent... | 09/30/2019 15:34:22 |
|  | Start [AhsayOBM v8.3.0.0] | 09/30/2019 15:34:22 |
|  | Saving encrypted backup set encryption keys to server... | 09/30/2019 15:34:22 |
|  | Start Backup ... [In-File Delta: Full] | 09/30/2019 15:34:23 |
|  | Using Temporary Directory C:\Users\Administrator\temp\1569828013271\OBS@1569828075210 | 09/30/2019 15:34:23 |
|  | Start running pre-commands | 09/30/2019 15:34:24 |
|  | Finished running pre-commands | 09/30/2019 15:34:24 |
|  | Downloading server file list... | 09/30/2019 15:34:24 |
|  | Downloading server file list... Completed | 09/30/2019 15:34:24 |
|  | Contact your service provider to enable [Volume Shadow Copy] support | 09/30/2019 15:34:25 |
|  | Reading backup source from hard disk... | 09/30/2019 15:34:25 |
|  | Reading backup source from hard disk... Completed | 09/30/2019 15:34:26 |
|  | [New Directory]... C:\ | 09/30/2019 15:34:26 |
|  | [New Directory]... C:\Users | 09/30/2019 15:34:26 |
|  | [New Directory]... C:\Users\Administrator | 09/30/2019 15:34:26 |
|  | [New Directory]... C:\Users\Administrator\Documents | 09/30/2019 15:34:26 |
|  | [New Directory]... C:\Users\Administrator\Documents\Test Files | 09/30/2019 15:34:26 |
|  | [New File]... 100% of "C:\Users\Administrator\Documents\Test Files\Copy of the Sample image.bmp" | 09/30/2019 15:34:26 |
|  | [New File]... 100% of "C:\Users\Administrator\Documents\Test Files\Data.txt" | 09/30/2019 15:34:26 |
|  | [New File]... 21% of "C:\Users\Administrator\Documents\Test Files\Diagram.png" | 09/30/2019 15:34:27 |
|  | [New File]... 32% of "C:\Users\Administrator\Documents\Test Files\Diagram.png" | 09/30/2019 15:34:27 |

Logs per page
Page

12 Restore Data

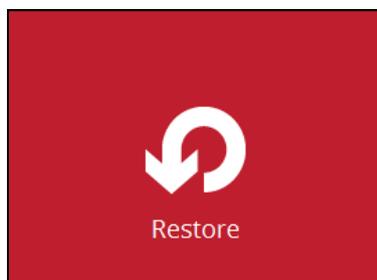
12.1 Restore Method

There are two restore methods available, the traditional restore and OpenDirect restore. OpenDirect restore applies only to File backup sets with OpenDirect feature enabled.

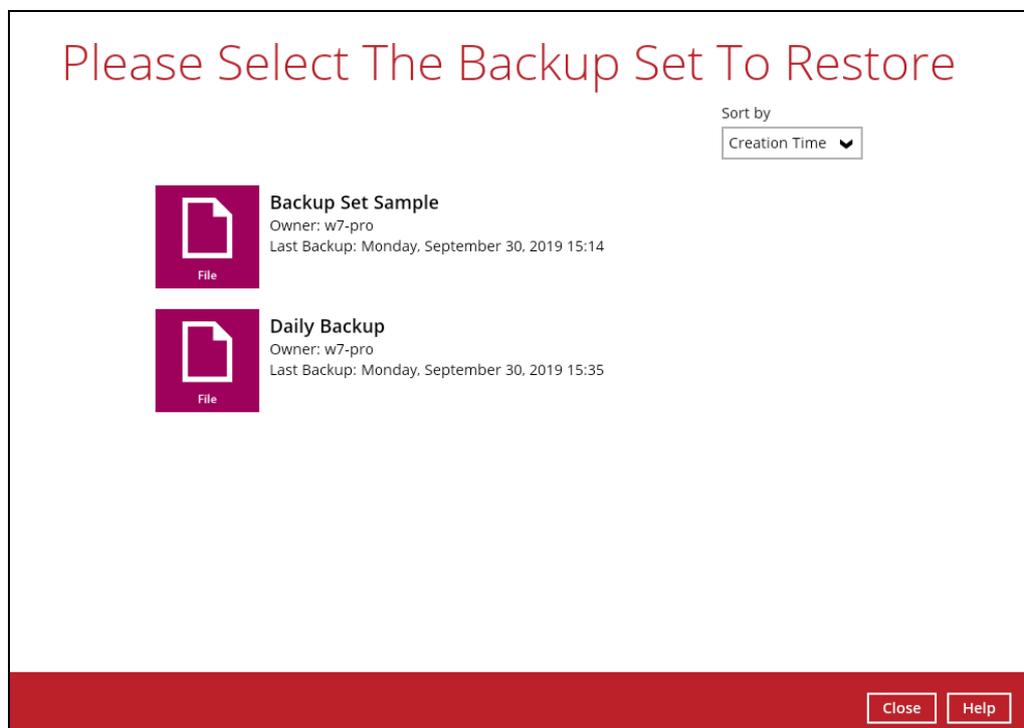
For more details on the differences of the two restore methods, refer to [Benefits of using OpenDirect Restore](#).

12.1.1 Traditional Restore

1. Log in to the OBM application according to the instructions in section [Login to OBM](#).
2. Click the **Restore** icon on the OBM main interface.



3. All the available backup sets for restore will be listed. Select the backup set that you would like to restore data from.



4. Select where you would like to restore your data from.



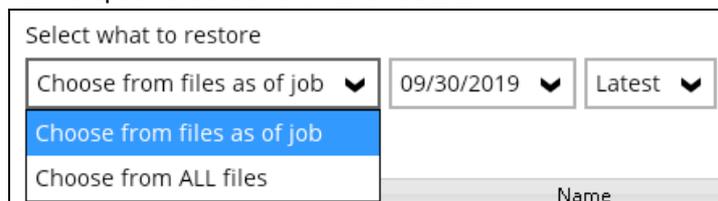
5. Select **Normal restore**.



6. 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** dropdown 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.

The following is an example showing all the available backup versions of the file **Test files.rtf**. 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.

| | Name | Size | Date modified |
|-------------------------------------|------------------|------|------------------|
| <input checked="" type="checkbox"/> | Test files.rtf | 1 KB | 09/30/2019 15:57 |
| <input checked="" type="checkbox"/> | Test files.rtf | 1 KB | 09/30/2019 15:55 |
| <input checked="" type="checkbox"/> | Test files.rtf | 1 KB | 08/01/2019 13:40 |
| <input checked="" type="checkbox"/> | Test files_2.rtf | 1 KB | 09/30/2019 15:57 |
| <input checked="" type="checkbox"/> | Test files_2.rtf | 1 KB | 09/30/2019 15:55 |
| <input checked="" type="checkbox"/> | Test files_2.rtf | 1 KB | 08/01/2019 13:40 |
| <input checked="" type="checkbox"/> | Text files.txt | 2 KB | 09/30/2019 15:57 |
| <input checked="" type="checkbox"/> | Text files.txt | 1 KB | 09/30/2019 15:55 |
| <input checked="" type="checkbox"/> | Text files.txt | 0 KB | 08/01/2019 12:02 |

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.

| Name | Date modified | Type | Size |
|----------------------------------|-------------------|-------------------|------|
| Test files | 9/30/2019 3:57 PM | Rich Text Docu... | 1 KB |
| Test files_2 | 9/30/2019 3:57 PM | Rich Text Docu... | 1 KB |
| Test files_2_2019-09-30-15-43-06 | 8/1/2019 1:40 PM | Rich Text Docu... | 1 KB |
| Test files_2_2019-09-30-15-56-12 | 9/30/2019 3:55 PM | Rich Text Docu... | 1 KB |
| Test files_2019-09-30-15-43-06 | 8/1/2019 1:40 PM | Rich Text Docu... | 1 KB |
| Test files_2019-09-30-15-56-12 | 9/30/2019 3:56 PM | Rich Text Docu... | 1 KB |
| Text files | 9/30/2019 3:57 PM | Text Document | 2 KB |
| Text files_2019-09-30-15-43-06 | 8/1/2019 12:02 PM | Text Document | 0 KB |
| Text files_2019-09-30-15-56-12 | 9/30/2019 3:55 PM | Text Document | 1 KB |

- Click the **Show files** checkbox to select individual files for restoration. Click **Next** to proceed when you are done with the selections.
- 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 OBM under the same directory path as on the machine storing the backup source. For example, if the backup source files are stored under **Users/[User's Name]/Downloads** folder, the data will be restored to **Users/[User's Name]/Downloads** as well on the computer running OBM.

Choose Where The Files To Be Restored

Restore files to

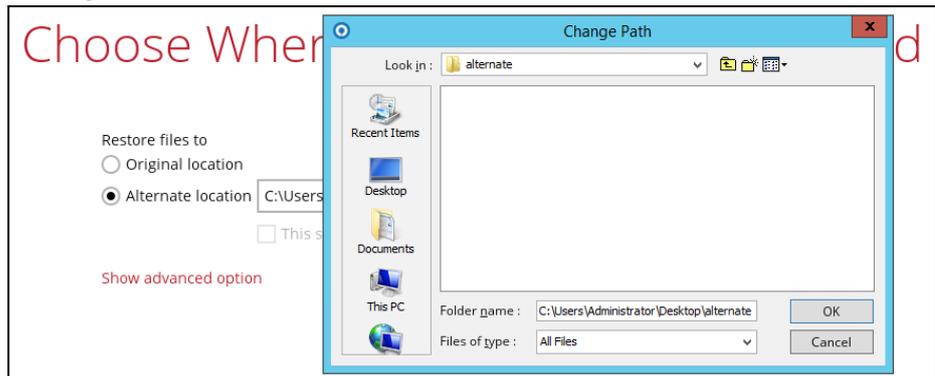
Original location
 Alternate location

This share requires access credentials

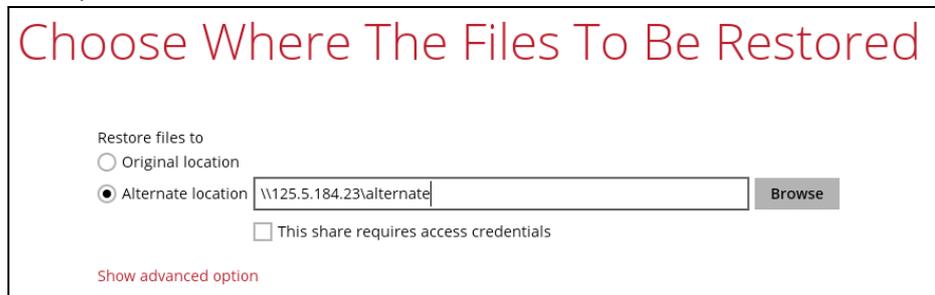
[Show advanced option](#)

- Alternate location** – You can choose to restore the data to a location of your choice on the computer where OBM is running or to a network drive.

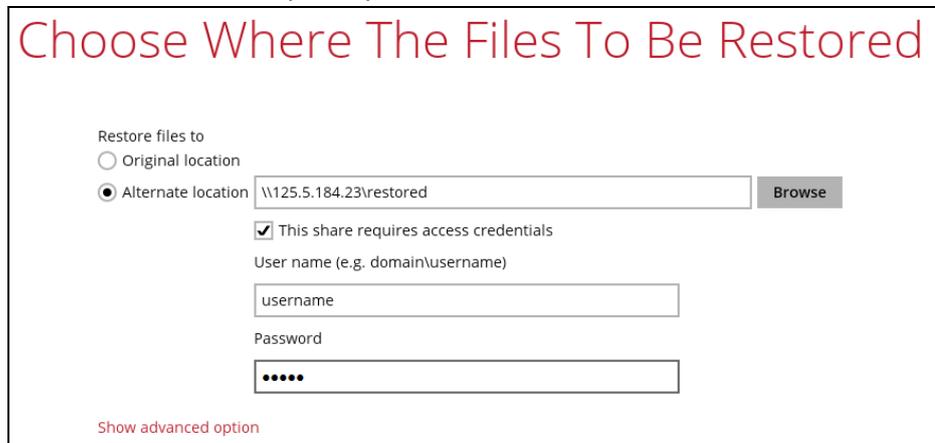
- i. To restore to a location of your choice on the computer where OBM is running, click Browse. Select the location and click **OK**.



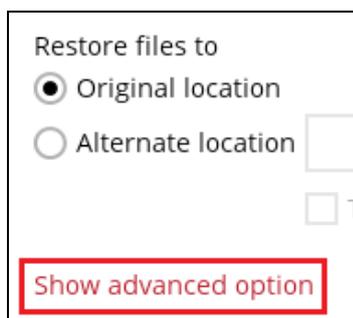
- ii. To restore to a network drive, enter the network address where you want the backup files to be restored.



Check the box beside **This share requires access credentials** if the network drive was set up with password. Enter the User name and Password.



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



- Restore file permissions
 - Delete extra files
 - Follow Link
 - Resolve Link
 - Verify checksum of in-file delta files during restore
- Hide advanced option

⦿ **Restore file permissions**

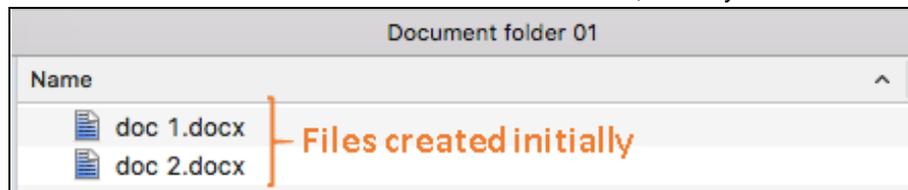
Restore file permissions are disabled by default. When you perform a file restore on shared files or folders using a shared computer, it is recommended that you enable Restore file permissions by ticking the checkbox so that the files restored will not be fully accessible to everyone using the shared computer.

⦿ **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.

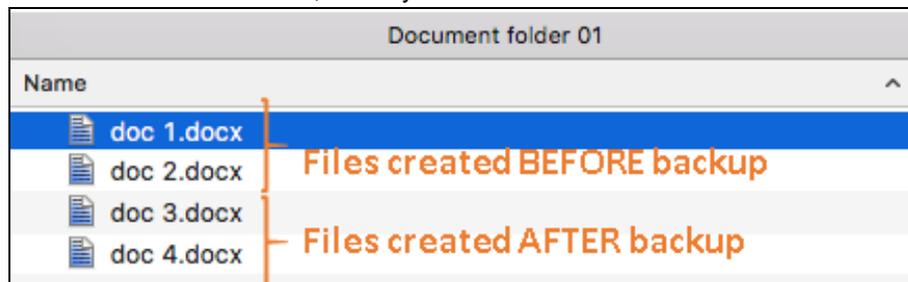
Example:

- 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**.

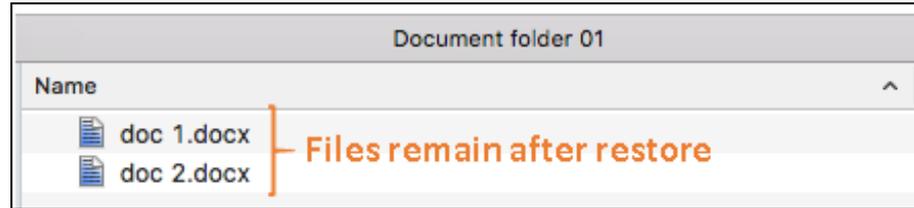
- iii) Two new files are created, namely doc 3 & doc 4.



- 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 destination has not been backed up and what impact it would cause if those data is deleted.

Prior to the data restore and synchronization, a warning message shows as the one shown below. Only clicking **Yes** will the “extra file” be deleted. You can click **Apply to all** 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 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, as well as the directories and files that the symbolic link links to will also be restored in the alternate location you have

chosen. That means the symbolic link 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.

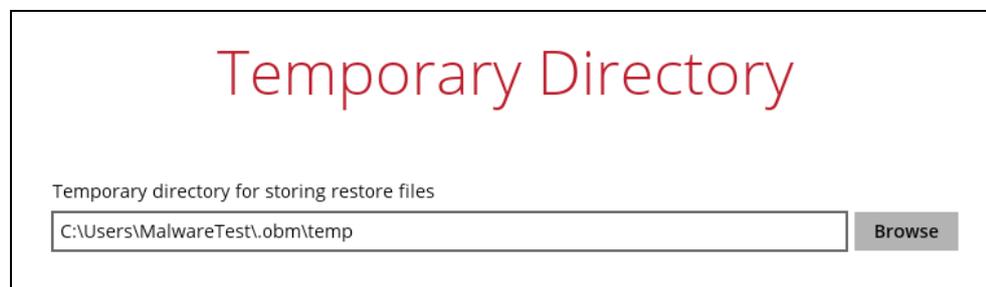
| Resolve Link | Behavior |
|-----------------|--|
| Enabled | Symbolic link is restored to the alternate location specified, with its target directories and files also restored to the same location in their relative path. Target of the link is updated to the new relative path. In other word, the link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

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

Verify checksum of in-file delta files during restore is disabled by default. When you perform restore for non-RunDirect backup set, you can enable the feature by ticking the checkbox so that the checksum of in-file delta files will be verified. As the feature will make the restore process time longer, it is recommended to enable the feature only if you want to verify if the merged file were correct.

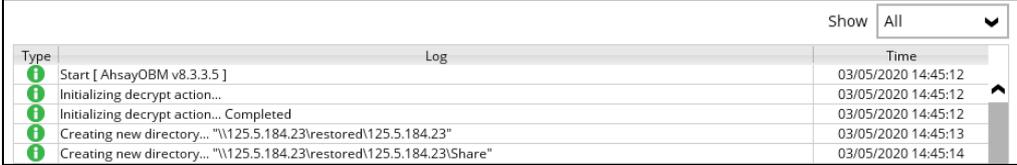
10. Click **Next** to proceed when you are done with the settings.
11. Select the temporary directory for storing temporary files, such as delta files, when they are being merged.

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



12. Click **Restore** to start the restore. The status will be shown.
13. When the restore is completed, the message "Restore Completed Successfully" will appear.

You can click the  **View** icon on the right-hand side to check the log. A window will pop up to show the log. Click **Close** to exit the pop-up window.



The screenshot shows a log window with a table of events. The window has a title bar and a 'Show' dropdown menu set to 'All'. The table has three columns: 'Type', 'Log', and 'Time'. The events listed are:

| Type | Log | Time |
|---|--|---------------------|
|  | Start [AhsayOBM v8.3.3.5] | 03/05/2020 14:45:12 |
|  | Initializing decrypt action... | 03/05/2020 14:45:12 |
|  | Initializing decrypt action... Completed | 03/05/2020 14:45:12 |
|  | Creating new directory... "\\125.5.184.23\restored\125.5.184.23" | 03/05/2020 14:45:13 |
|  | Creating new directory... "\\125.5.184.23\restored\125.5.184.23\Share" | 03/05/2020 14:45:14 |

14. In the Restore window, click **Cancel** to close the Restore window.
15. To exit OBM, click the “**x**” on the top right corner. A message will appear to ask for your confirmation. Click **Yes** to close the application. If you wish to run OBM again, you will then have to launch it again.

12.1.2 OpenDirect Restore

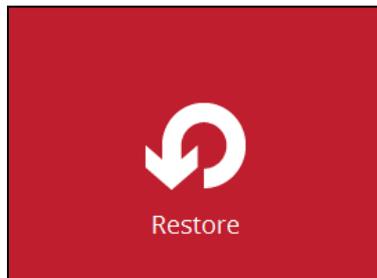
This restore method applies to backup sets created with OpenDirect restore enabled only.

IMPORTANT

Before you proceed with the OpenDirect Restore, make sure 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-us/download/details.aspx?id=48145>
- Update for Universal C Runtime in Windows
<https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows>
- Microsoft Security Advisory 3033929 (for Windows 7 and Windows Server 2008 R2)
<https://technet.microsoft.com/en-us/library/security/3033929.aspx>

1. Log in to the OBM application according to the instructions in section [Login to OBM](#).
2. Click the **Restore** icon on the OBM main interface.



3. All the available backup sets for restore will be listed. Select the backup set that you would like to restore data from.

Please Select The Backup Set To Restore

Sort by

Creation Time ▼



Backup Set Sample

Owner: w7-pro

Last Backup: Monday, September 30, 2019 15:14



Daily Backup

Owner: w7-pro

Last Backup: Monday, September 30, 2019 15:57



OpenDirect Backup

Owner: w7-pro

Last Backup: Wednesday, October 02, 2019 11:06

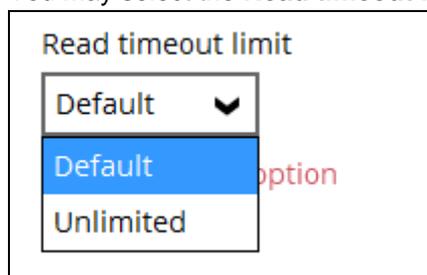
4. Select where you would like to restore your data from.



5. Select **Open backup data directly without restoration (OpenDirect)**.



You may select the **Read timeout limit** by clicking Show advanced option.



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

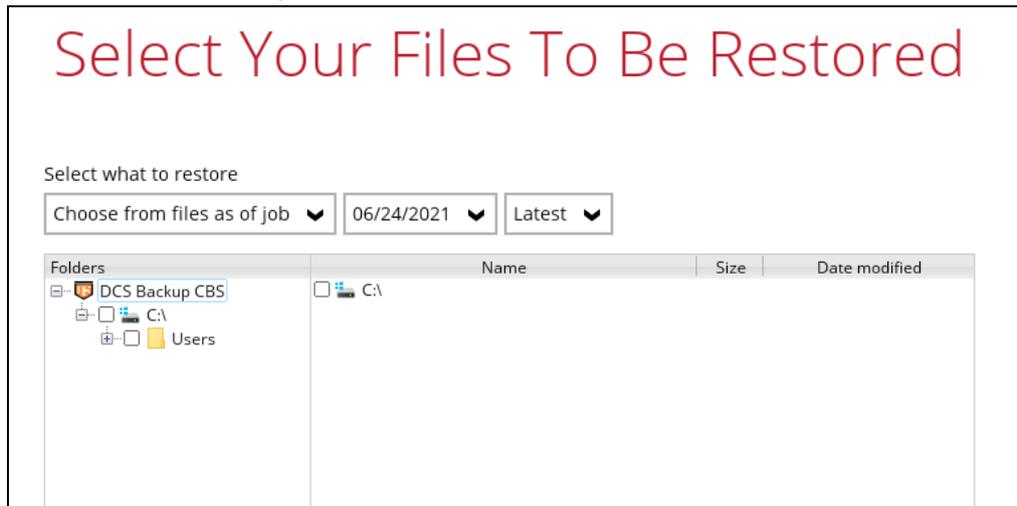
- **Default** – This setting should be suitable for compressed or image file located on a local, removable, or network drive. The time out value is 15 seconds.
- **Unlimited** – the connection will not be time out when this is selected. This selection is recommended under the following usage:
 - Backup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

NOTE

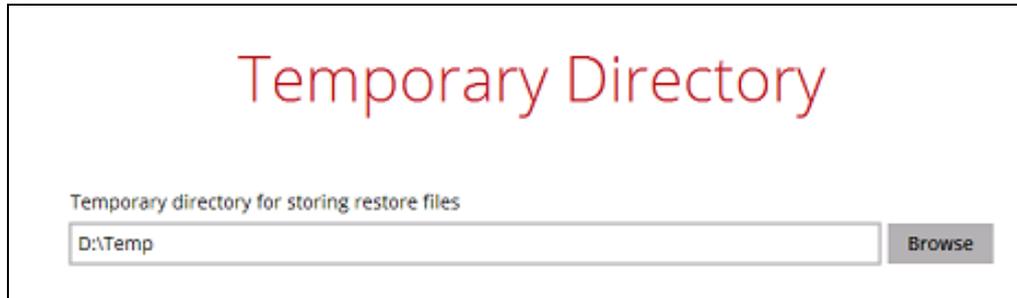
If in doubt or unsure about the compressed or image file size or network stability, it is recommended to use **Unlimited**.

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

6. 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.



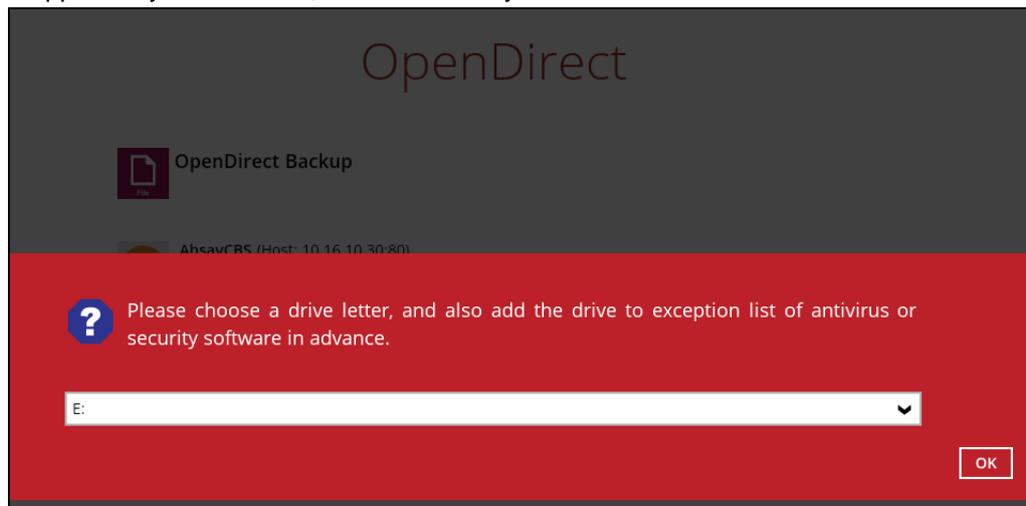
7. Select a temporary directory for storing restore files, then click Restore to start the OpenDirect restore.



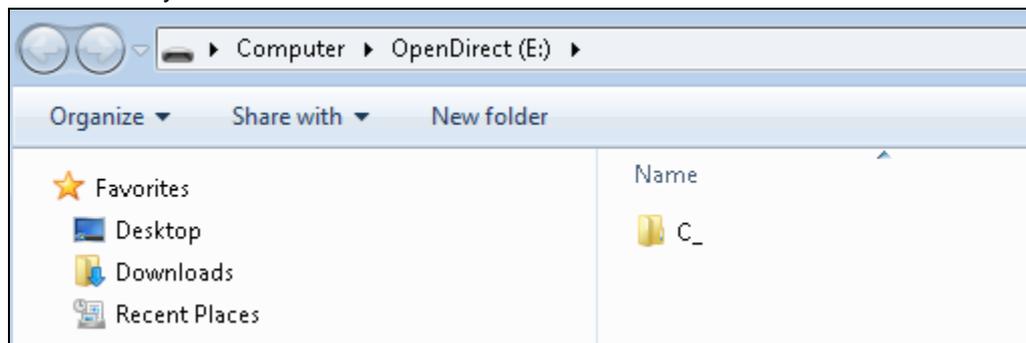
8. Click **Restore** to start the restore. The status will be shown.
9. The following screen shows when you perform OpenDirect restore for this backup set on this machine for the first time only. Make sure you click **Yes** to confirm mounting the file(s) on this machine. Clicking **No** will exit the restore process.



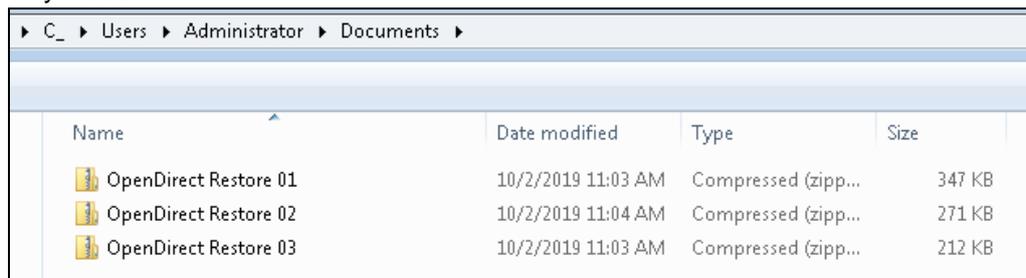
10. You will be prompted to select drive letter where you wish the mounted files to be mapped on your machine, click **OK** when you have finished selection.



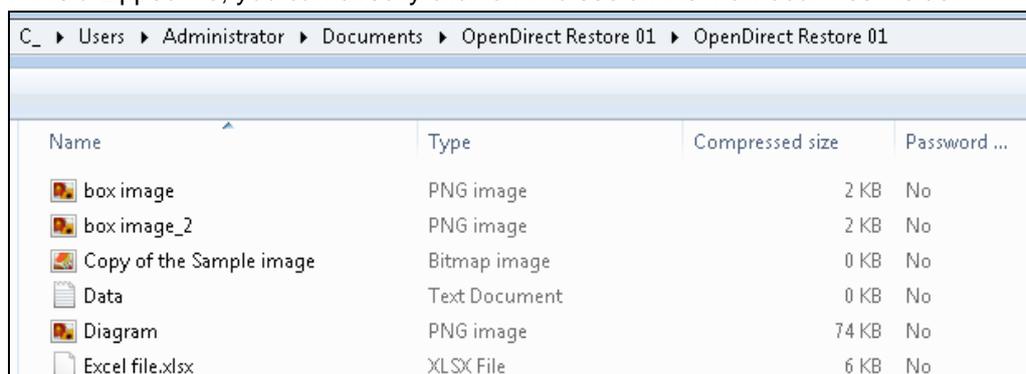
11. The selected drive letter will be mapped and prompted in the Windows Files Explorer with the files you wish to restore shown.



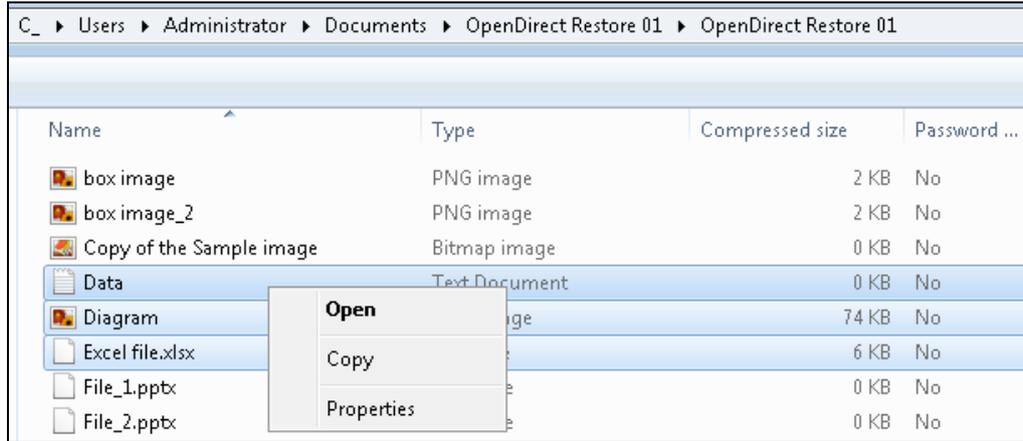
12. You can now click on the files to view them directly from here, which will be in read-only mode.



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.



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



14. When you have finished restoring the necessary files, you can go back to OBM and click **Cancel** to exit the OpenDirect Restore.



IMPORTANT

- 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 OBM. In other words, each OpenDirect restore session on OBM can only mount and unmount once.
- OpenDirect restore** of file backup sets:
 - Will not show up on the **Restore Status** tab in **Live Activities** of the backup service provider DCS CBS. **Restore Status** tab in **Live Activities** only applies to the restore performed directly through OBM.
 - Will not generate restore reports or report email on backup service provider

DCS CBS.

- Will not generate restore log on OBM.

12.2 Restore Filter

This search feature allows you to search directories, files, and folders.

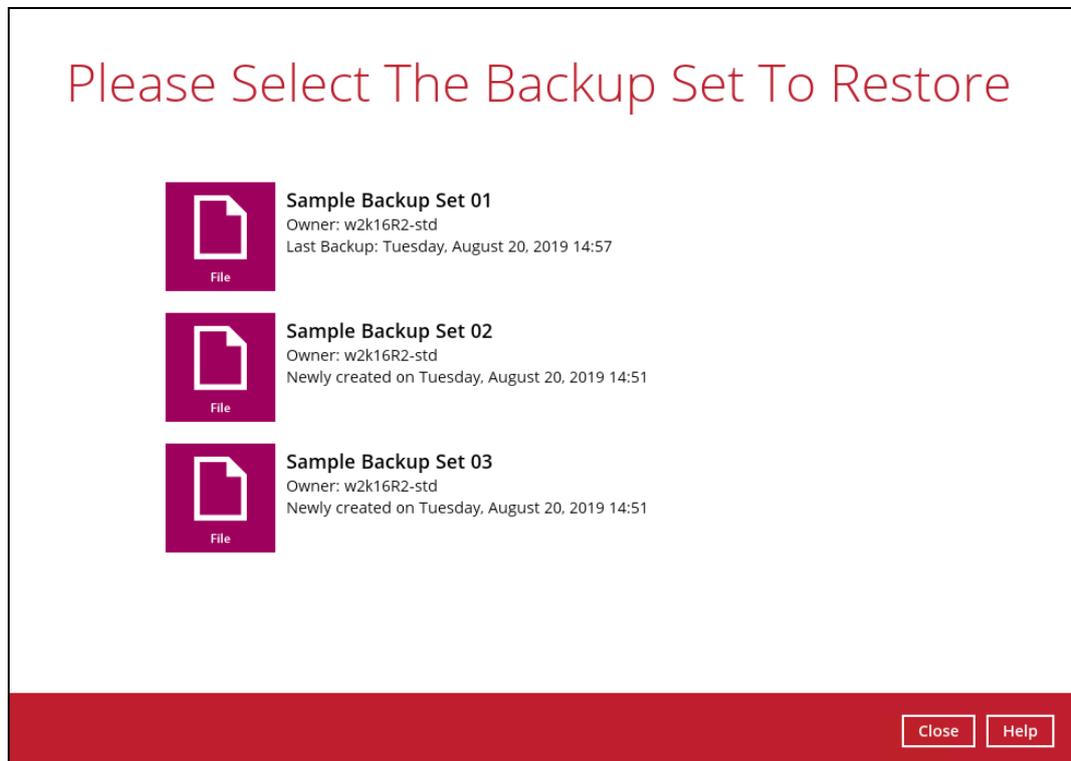
To make it more flexible, the search feature offers filtering. You can add additional pattern upon searching. Pattern includes the following criteria:

- ▶ **Contains**
These are Directories, Files, and Folders with the name **containing** the specific letter or word.
- ▶ **Exact**
These are Directories, Files, and Folders with the **exact** or **accurate** name.
- ▶ **Start With**
These are Directories, Files, and Folders with the name **starting** with a specific letter or word.
- ▶ **Ends With**
These are Directories, Files, and Folders with the name **ending** with a specific letter or word.

It also has the **Match Case** function, which serves as an additional accuracy when searching for any specific directories, files, folders, and mails.

For more detailed examples using the restore filter on OBM, refer to [Appendix B: Example Scenarios for Restore Filter](#).

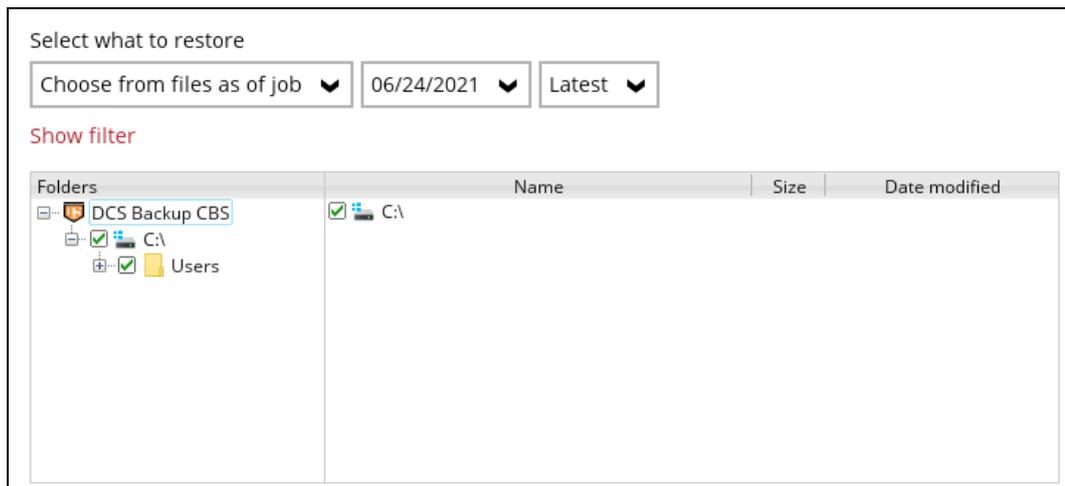
- 1 Log in to OBM according to the instructions in [Login to OBM](#).
- 2 Click the [Restore] icon on the main interface of OBM.
- 3 Select the backup set that you would like to restore.



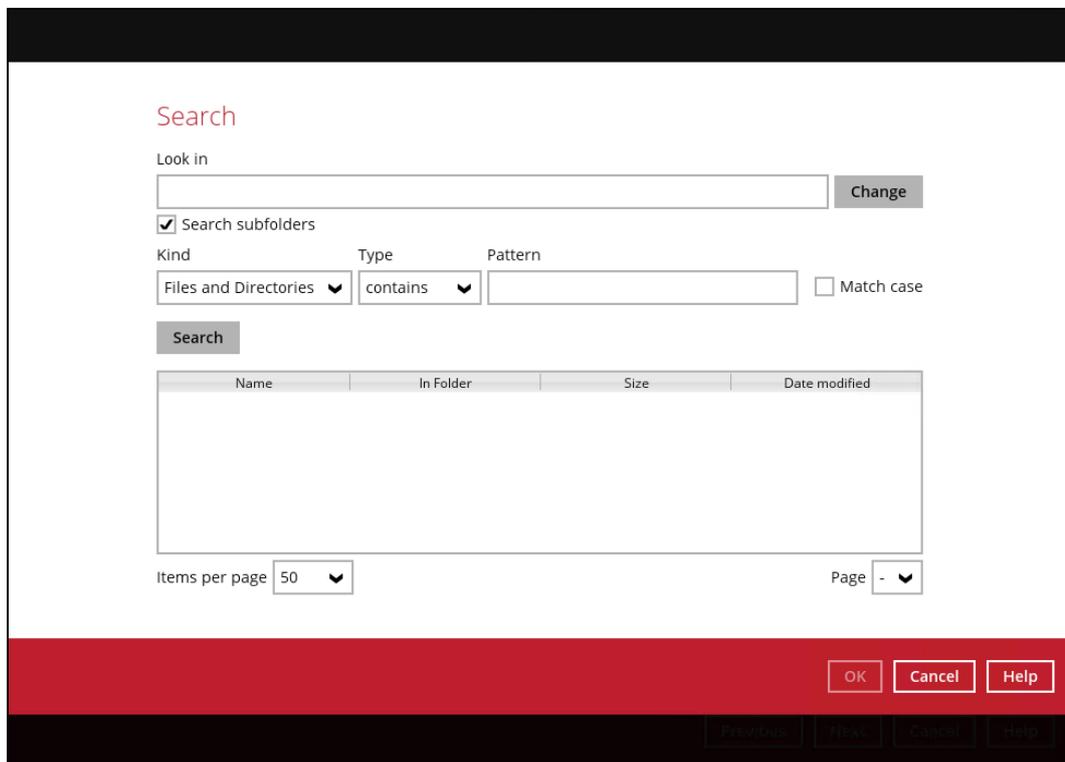
- 4 Select the backup destination that you would like to restore backed up items to.



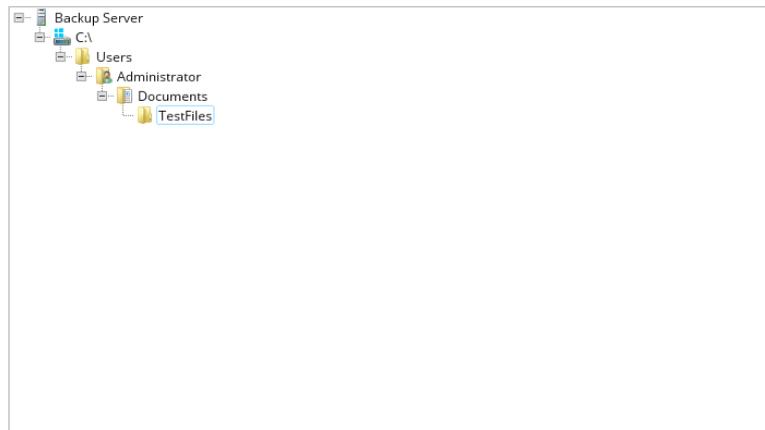
- 5 Click the [Search] located on the lower left side of the screen.



- 6 Click the [Change] button to change the path of the restore items from other location.



Change Path



OK Cancel

Search

Look in
C:\Users\Administrator\Documents\TestFiles Change

Search subfolders

Kind Type Pattern Match case
Files and Directories contains

Search

| Name | In Folder | Size | Date modified |
|------|-----------|------|---------------|
|------|-----------|------|---------------|

Items per page 50 Page -

OK Cancel Help

Previous Next Cancel Help

7 Tick the [Search subfolders] to include available subfolders upon searching.

 Search subfolders Search subfolders

8 Select from the following Kind of files you want to search.

- Files and Directories
- Files only
- Directories

9 Select from the following Type of filtering you want to search.

- Contains
- Exact
- Starts With
- Ends With

10 Enter a pattern you want and tick the [Match case] box if you want to accurately search for a specific file.

Pattern

 Match case

Pattern

 Match case

11 Click the [Search] button and the result will be displayed.

12 Check all the items or check a specific item that you want and click the [OK] button to proceed and you will return to the restore main screen.

13 Contact DCS

13.1 Technical Assistance

To contact DCS support representatives for technical assistance, email us at support@dcsbackup.com .