



Ahsay Cloud Backup Suite v9

User's Guide

Ahsay Systems Corporation Limited

22 November 2022

Copyright Notice

© 2022 Ahsay Systems Corporation Limited. All rights reserved.

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

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

Trademarks

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

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

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

Dropbox is a registered trademark of Dropbox Inc.

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

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

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

MariaDB is a registered trademark of MariaDB Corporation AB.

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

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

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

OpenJDK is a registered trademark of Oracle America, Inc.

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.

Debian is a registered trademark of Software in the Public Interest, Inc.

Rocky is a registered trademark of Rocky Brands.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

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

Disclaimer

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

Revision History

Date	Descriptions	Version
25 January 2022	<ul style="list-style-type: none">Ch. 1.1 – updated system architecture diagram to include documents and 2FA accountsCh. 6.2 – added description for each backup set settings	9.1.0.0
6 May 2022	<ul style="list-style-type: none">Ch. 6.2.8 – additional note in Command Line Tool	9.1.0.0
15 July 2022	<ul style="list-style-type: none">Ch. 6 – added difference between AhsayOBM and AhsayACB UI	9.3.0.0
3 November 2022	<ul style="list-style-type: none">Ch. 1.4 – updated instructions on how to reset password and added noteCh. 6.2.3 – added backup schedule priorityCh. 6.2.6 – updated Deduplication block sizeCh. 6.2.12 – added Recycle Bin description	9.5.0.0
22 November 2022	<ul style="list-style-type: none">Ch. 6.2.12 – fixed typo in Recycle Bin	9.5.0.0

Table of Contents

1	Overview	1
1.1	Introduction	1
1.2	About This Document	2
1.3	Requirements for Using the AhsayCBS User Web Console	2
1.4	Resetting Your Password	3
1.5	Downloading Software	5
1.6	Changing the Language	8
1.7	Invoking Online Help.....	9
2	Logging in to AhsayCBS User Web Console	10
2.1	Log in to AhsayCBS without 2FA	10
2.2	Log in to AhsayCBS with 2FA using authenticator app	12
2.3	Log in to AhsayCBS with 2FA using Twilio	16
3	Unable to Log in to AhsayCBS with 2FA	18
3.1	Registered a recovery number in Ahsay Mobile app	18
3.2	Did not register a recovery number in Ahsay Mobile	20
3.3	Using third party authenticator app	20
4	Managing Your AhsayCBS User Account.....	21
4.1	Log in to AhsayCBS.....	21
4.2	Managing AhsayCBS Backup User.....	21
4.3	User Profile	22
4.3.1	General Tab.....	22
4.3.2	Backup Client Settings Tab	24
4.3.3	Contact Tab	30
4.3.4	User Group Tab	31
4.3.5	Authentication Tab.....	32
4.3.6	Mobile Backup Tab.....	34
4.4	Settings	35
4.5	Report.....	37
4.5.1	Backup Reports	37
4.5.2	Restore Reports.....	39
4.6	Statistics.....	42
4.7	Effective Policy.....	46
5	Monitoring Live Activities	49
5.1	Managing Live Activities	49
5.2	Backup Status.....	50
5.3	Restore Status	51

6	Managing Backup Set	53
6.1	Create Backup Set (Generic Steps)	54
6.2	Manage Backup Set.....	69
	Difference between AhsayOBM and AhsayACB Backup Set	69
6.2.1	General	71
6.2.2	Source.....	74
6.2.3	Backup Schedule.....	85
6.2.4	Continuous Backup	87
6.2.5	Destination.....	90
6.2.6	Deduplication	92
6.2.7	Retention Policy.....	94
6.2.8	Command Line Tool	102
6.2.9	Reminder	106
6.2.10	Bandwidth Control	107
6.2.11	IP Allowed for Restore.....	109
6.2.12	Others	110
6.3	Run a Backup Job.....	116
6.4	Restore a Backup (Non-Run Direct Restore).....	117
7	Run Direct Restore	118
7.1	Introduction	118
7.2	Run Direct Restore Options.....	121
7.3	Performing a Run Direct Restore on VM.....	122
7.3.1	Restore a backup from VMFS datastore to VMFS datastore.....	122
7.3.2	Restore a backup from VMFS datastore to vSAN datastore.....	129
7.3.3	Restore a backup from vSAN datastore to vSAN datastore.....	135
7.3.4	Restore a backup from vSAN datastore to VMFS datastore.....	139
8	Contacting Ahsay	144
8.1	Technical Assistance	144
8.2	Documentation.....	144
	Appendix	145
	Appendix A Set Backup Destination on AhsayOBM for Backup Sets Created on AhsayCBS User Web Console	145

1 Overview

1.1 Introduction

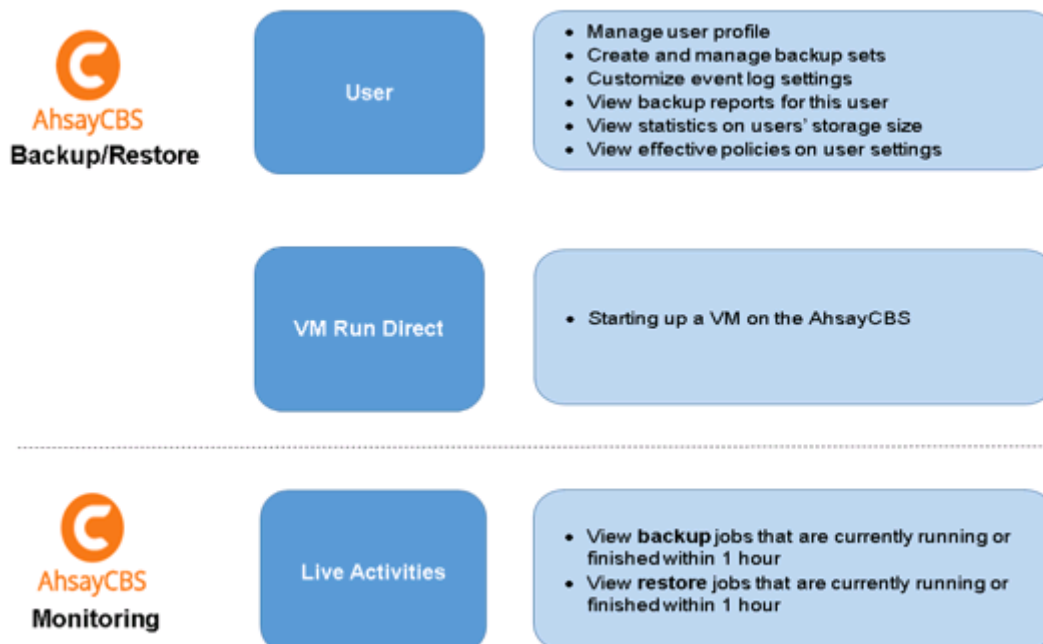
What is this software?

Ahsay Cloud Backup Suite v9 allows you to back up your data on the cloud. You can access the AhsayCBS server environment easily on a user web console. This is a user interface that allows you to login remotely to a backup server.

The **User** option in the main interface allows the AhsayCBS user to update user profile and manage other settings such as reports.

The **VM Run Direct** option allows the AhsayCBS user to restore a VM by running it directly from the backup files in the AhsayCBS. This is much faster than extracting from backup files and copying to the production storage, which can take hours to complete. This feature helps reduce disruption and downtime of your production VMs. Administrator can troubleshoot on the failed virtual machine, while users are back in production with minimal disruption.

The **Live Activities** option is a monitoring tool which allows you to view the backup jobs and restore jobs as they are running as well as to view all jobs that were run within the previous 1 hour.



1.2 About This Document

What is the purpose of this document?

This document aims at providing all necessary information for you to work with the AhsayCBS server at the user level to manage backup and restore jobs.

What should I expect from this document?

After reading through this documentation, you can expect to have sufficient knowledge to perform various tasks on the AhsayCBS server. These include modifying user profile settings, monitoring the backup and restore processes real time, and running the AhsayCBS from a virtual machine directly.

Who should read this document?

This documentation is intended for IT professionals who need to work with AhsayCBS server at the user level.

1.3 Requirements for Using the AhsayCBS User Web Console

In order to use the AhsayCBS user web console, you need the following:

- **Internet connection**

You need to have internet connection to access the AhsayCBS user web console.

- **Web browsers**

The AhsayCBS User Web Console runs with all major browsers. Please make sure that you are using the latest version and enable pop-ups on your preferred web browsers.



Apple Safari



Google Chrome



Microsoft
Edge



Microsoft Internet
Explorer



Mozilla
Firefox

- **AhsayCBS login account**

You need an AhsayCBS login account to access the AhsayCBS server component.

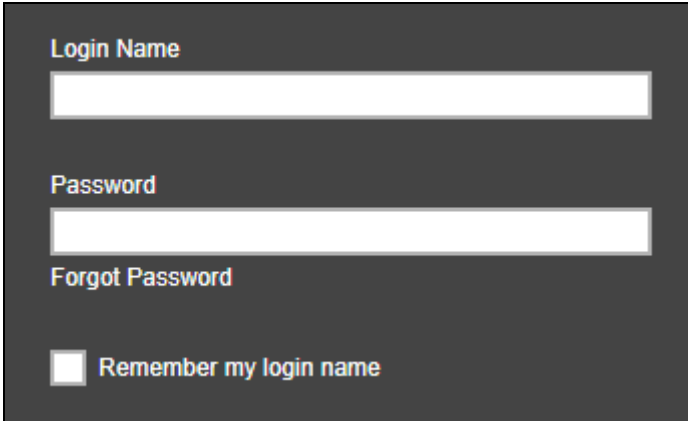
NOTE

Please contact your Ahsay backup service provider to create an AhsayCBS login account for you.

1.4 Resetting Your Password

If you have forgotten your password, you can perform the following steps to reset your password.

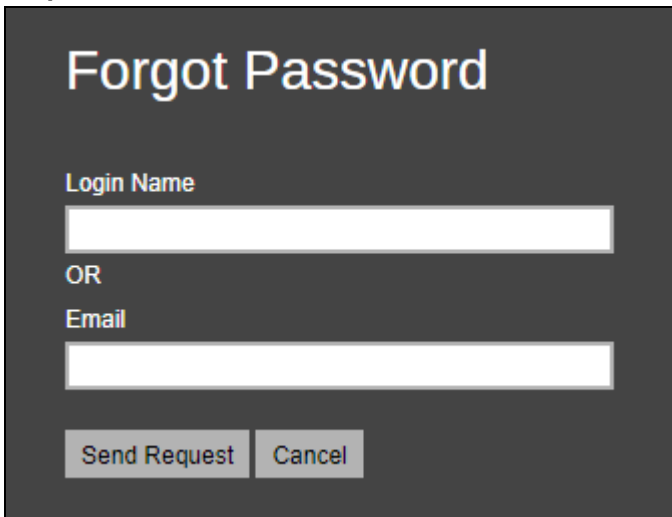
1. On the AhsayCBS Logon page, click **Forgot Password**.



The screenshot shows a dark grey login form with the following elements:

- Login Name**: A text input field.
- Password**: A text input field.
- Forgot Password**: A text link.
- Remember my login name**: A checkbox with a label.

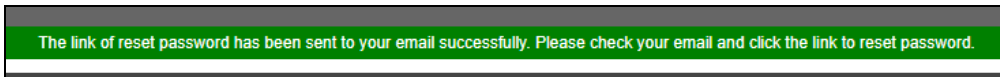
2. The following screen appears. Enter your Login Name or Email address then click **Send Request**.



The screenshot shows a dark grey screen titled **Forgot Password** with the following elements:

- Login Name**: A text input field.
- OR**: A separator text.
- Email**: A text input field.
- Send Request**: A button.
- Cancel**: A button.

The following message will be displayed.

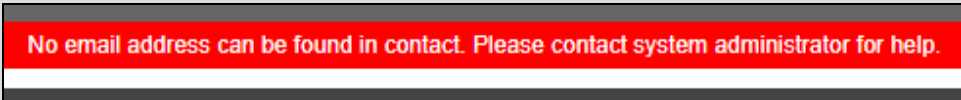


The screenshot shows a green message box with the text: **The link of reset password has been sent to your email successfully. Please check your email and click the link to reset password.**

NOTE

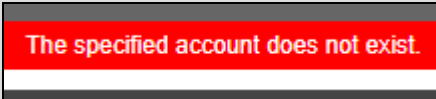
The following messages will be displayed instead if:

- the backup account has no email address saved.



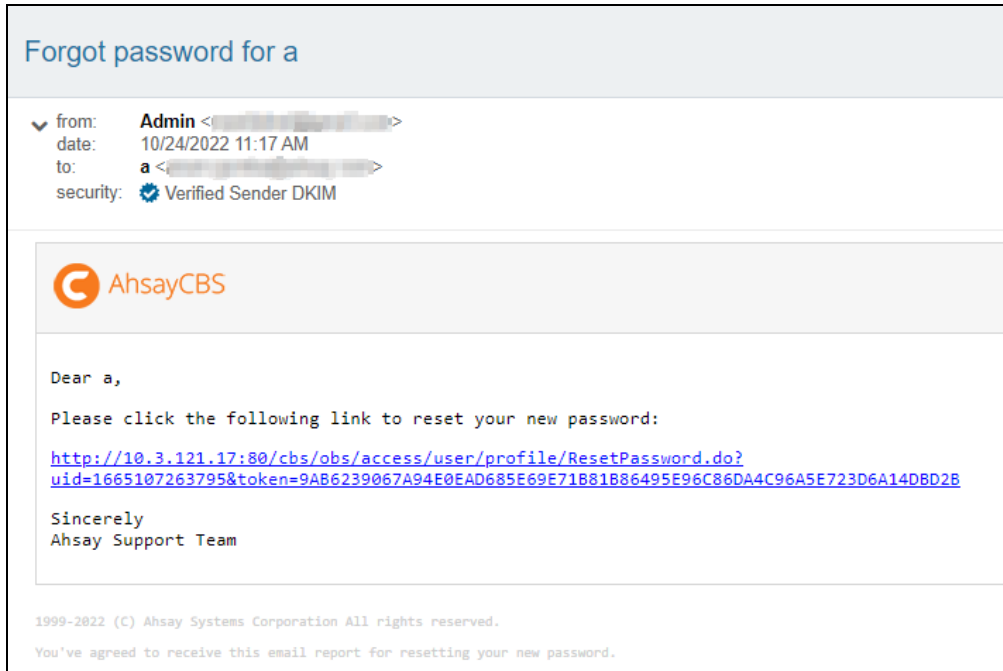
No email address can be found in contact. Please contact system administrator for help.


- the Login Name or Email entered is incorrect/not found.



The specified account does not exist.

3. You will receive an email containing a link. Click on the link to reset your password.



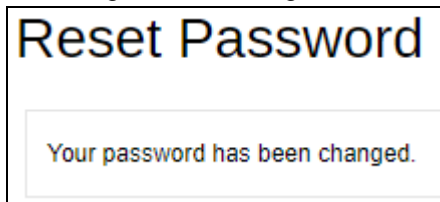
4. The Reset Password screen appears. Enter the new **Password** and then **Re-type Password**. Click  to save the modification.

Reset Password

Password

Re-type password

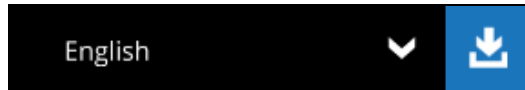
5. You will get the following screen confirming that your password has been changed.



1.5 Downloading Software

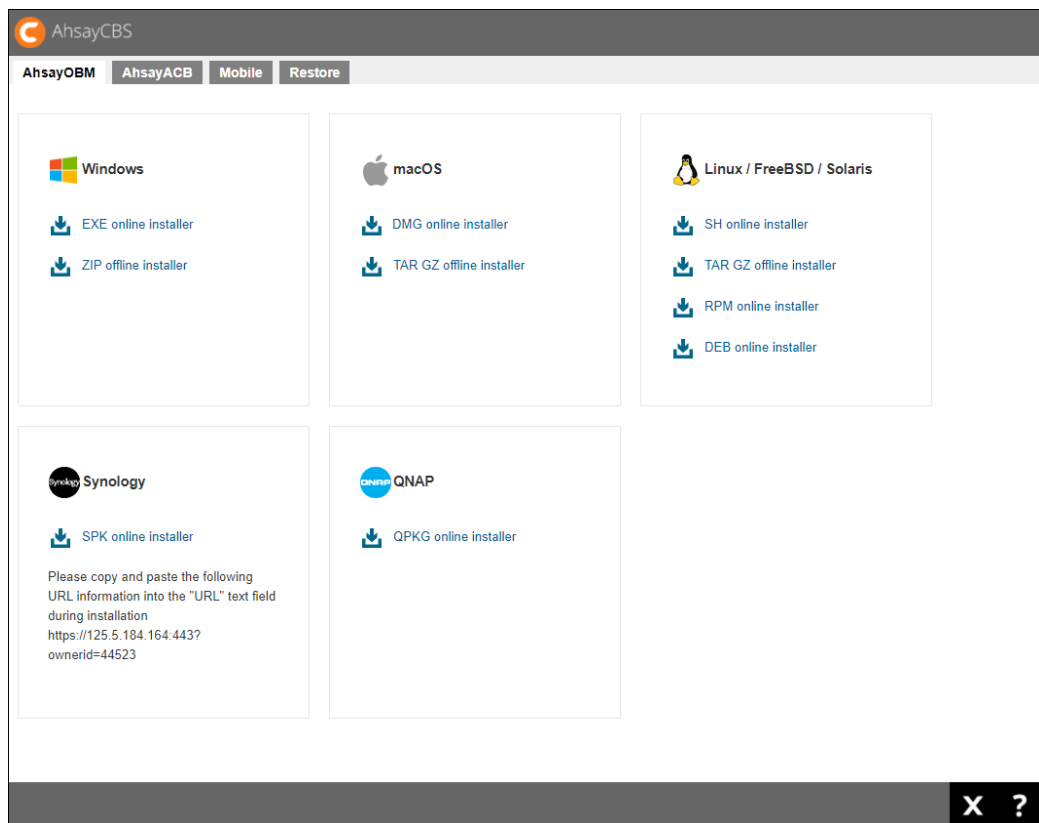
You can choose what client software you wish to download as follows:

1. On the AhsayCBS Logon page, click the downward arrow on the top right-hand corner.






2. The software download page appears. You can choose which product and which platform to download.


There are four (4) available tabs, AhsayOBM, AhsayACB, Mobile, and Restore.



NOTE

The actual options available is dependent on your backup service provider.

Client Backup Agents	Brief Description
AhsayOBM 	AhsayOBM is a versatile backup application that backup databases, applications, and virtual machines to local and offsite destinations.
AhsayACB 	AhsayACB is an advanced yet easy-to-use desktop and laptop backup software for backing up files, Cloud files, Windows System backup, IBM Lotus Notes and Microsoft 365 to local and offsite destinations.
Ahsay Mobile 	Ahsay Mobile is an easy to use 2FA Authenticator app and backup/restore solution for Android and iOS mobile devices. It can be used for login with 2FA and can also backup photos, videos, documents and 2FA accounts to local destination on the AhsayOBM and AhsayACB machine. It can be downloaded from the App Store and Google Play Store.

Client Restore Agent	Brief Description
Restore 	AhsayOBR supports the restore of multiple backup sets; file, databases, and virtual machines, such as VMware, Hyper-V, Microsoft Exchange Database Availability Group (DAG), Microsoft Exchange Database, Microsoft Exchange Mailbox, Microsoft SQL Server, Oracle Database, Lotus Domino/Notes, MySQL, MariaDB, Windows System, Windows System State, ShadowProtect, Synology NAS Devices, Microsoft 365, Cloud File with our dedicated restore modules.

AhsayCBS also supports two (2) installation modes, online and offline installation (except for Linux (rpm), Debian/Ubuntu (deb), Synology NAS and QNAP which supports online installation only). User can download and run either one of the installers.

Below is the table of comparison between online installation and offline installation.

	Online Installation	Offline Installation
Internet	<ul style="list-style-type: none"> ➤ It cannot be started without an internet connection. ➤ Clients need to have an internet connection each time an installation is run. ➤ If the client internet connection is interrupted or is not stable the installation may be unsuccessful. ➤ 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"> ➤ Once the offline installer is downloaded, the client does not require an internet connection each time an installation is run. ➤ The offline installer size is 80MB to 140MB depending on operating system as it contains all the necessary binary and component files
Backup Server Availability	The online installer requires the backup server to be online in order to run and complete the installation.	An offline installation can be performed independently of the backup server availability.
Installation Time	<ul style="list-style-type: none"> ➤ Takes more time as it needs to download the binary and component files (80MB to 140MB depending on operating system) each time the installation is run. ➤ A slow internet connection on the client machine will also result in longer installation time. 	Takes less time as all the necessary binary and component files are already available in the offline installer.
Version Control	Online installation ensures the latest version of the product is installed.	May need to update the product version after installation if an older offline installer is used.
Administrative Support	Need more time on the support for the installation as network factor might lead to unsuccessful installation.	Need less time as independent of network factor influence.
Deployments	<ul style="list-style-type: none"> ➤ Suitable for single or small amount of device installations. ➤ Suitable for client sites with fast and stable internet connection. 	<ul style="list-style-type: none"> ➤ Suitable for multiple or mass device installations. ➤ Suitable for client sites with metered internet connections.

3. Download the executable and install the product in the usual way.

1.6 Changing the Language

You can change the language of AhsayCBS anytime, whether before or after you have logon to the system.

NOTE

If the language you want is not available, please contact your backup service provider for assistance.

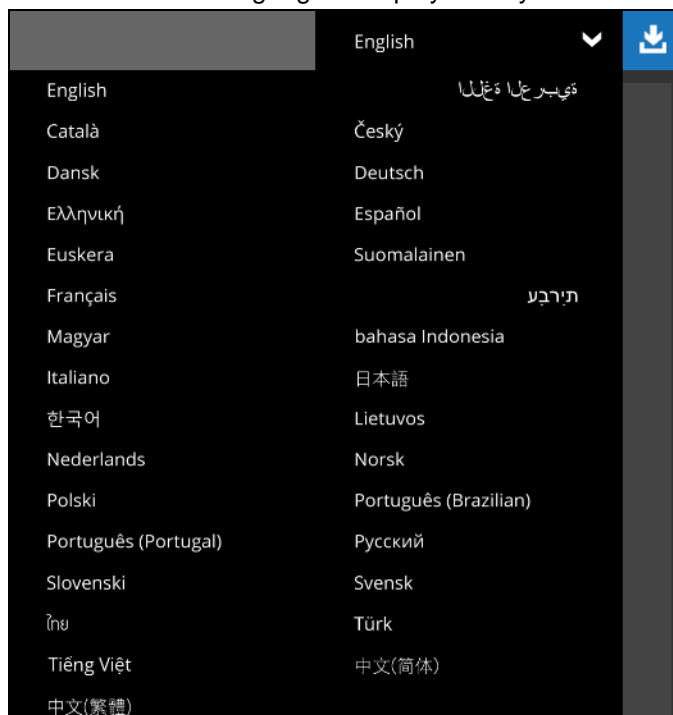
The available languages are:

- ▶ Arabic
- ▶ Basque
- ▶ Catalan
- ▶ Chinese (Simplified)
- ▶ Chinese (Traditional)
- ▶ Czech
- ▶ Danish
- ▶ Dutch
- ▶ English (default)
- ▶ Finnish
- ▶ French
- ▶ German
- ▶ Greek Modern
- ▶ Hebrew
- ▶ Hungarian
- ▶ Indonesian
- ▶ Italian
- ▶ Japanese
- ▶ Korean
- ▶ Lithuanian
- ▶ Norwegian
- ▶ Polish
- ▶ Portuguese (Brazilian)
- ▶ Portuguese (Portugal)
- ▶ Russian
- ▶ Slovenian
- ▶ Spanish
- ▶ Swedish
- ▶ Thai
- ▶ Turkish
- ▶ Vietnamese

1. On the AhsayCBS Logon page, click the downward arrow on the upper right-hand side.



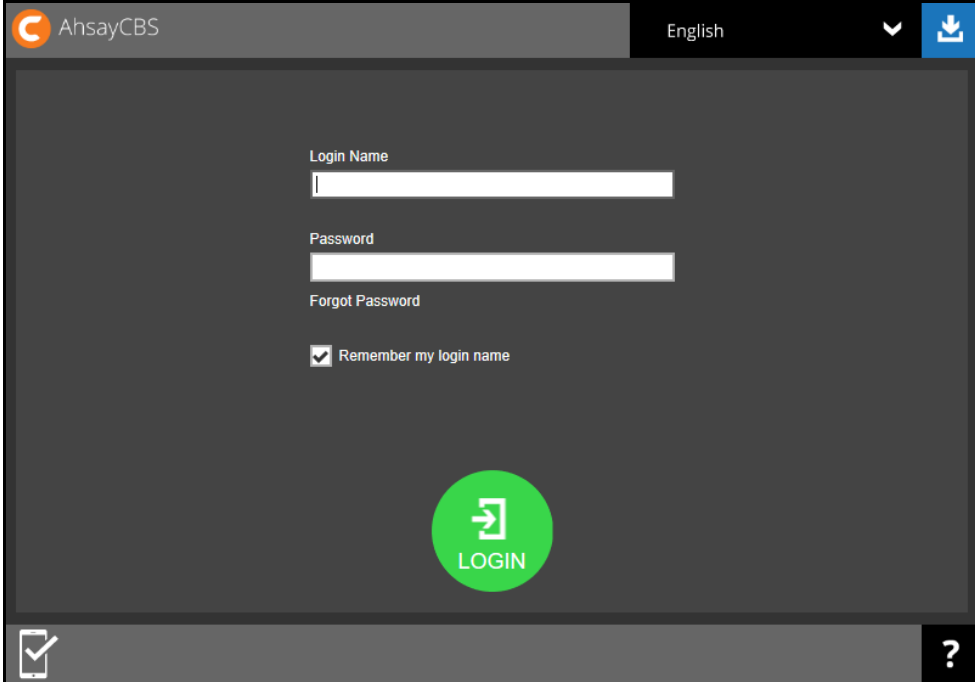
2. A list of available language is displayed for your choice.



1.7 Invoking Online Help

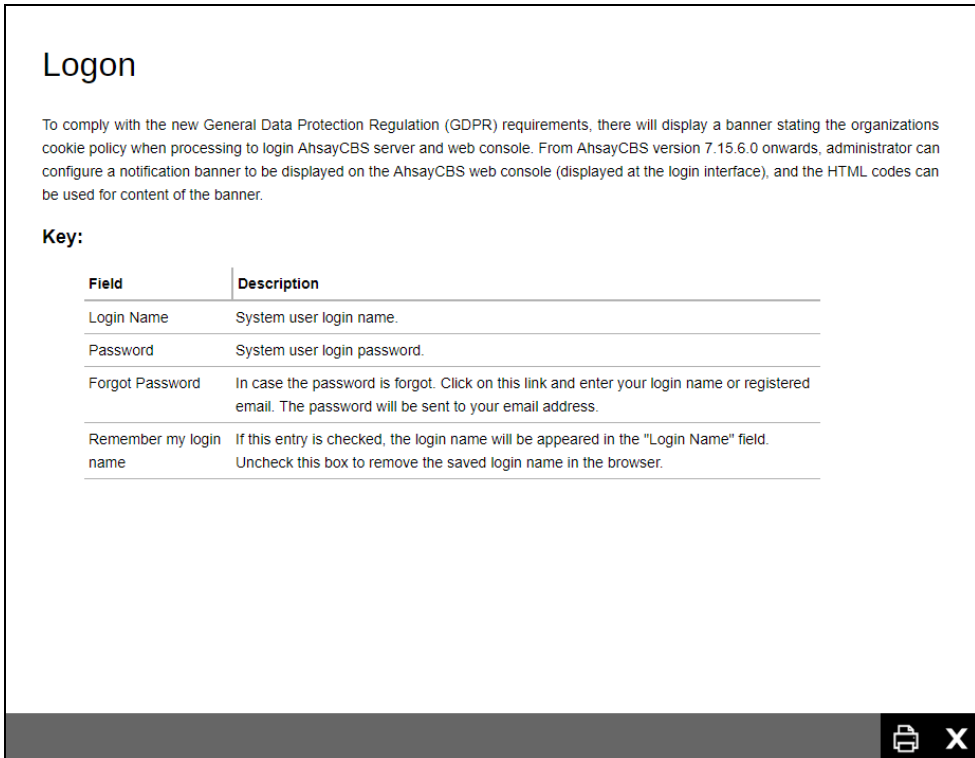
You can invoke the online help if you have problems logging in to the AhsayCBS server.

1. On the AhsayCBS Logon page, click the question mark at the bottom right corner.



2. The online help for the topic “Logon” appears.

It contains detailed description of each field on the logon screen and gives a brief description of each field.



Logon

To comply with the new General Data Protection Regulation (GDPR) requirements, there will display a banner stating the organizations cookie policy when processing to login AhsayCBS server and web console. From AhsayCBS version 7.15.6.0 onwards, administrator can configure a notification banner to be displayed on the AhsayCBS web console (displayed at the login interface), and the HTML codes can be used for content of the banner.

Key:

Field	Description
Login Name	System user login name.
Password	System user login password.
Forgot Password	In case the password is forgot. Click on this link and enter your login name or registered email. The password will be sent to your email address.
Remember my login name	If this entry is checked, the login name will be appeared in the "Login Name" field. Uncheck this box to remove the saved login name in the browser.

3. You can print the online help by clicking  at the bottom right corner. To exit, click X.

2 Logging in to AhsayCBS User Web Console

Upon logging in to AhsayCBS with two-factor authentication (2FA) enabled, you are required to register a device that will be used for 2FA to proceed with the log in. For more information on how to register a device, please refer to [Chapter 7](#) of the AhsayCBS v9 Quick Start Guide.

There are several scenarios that will be encountered for log in. Log in steps for the different scenarios will be discussed in this chapter.

- ▶ [Log in to AhsayCBS without 2FA](#)
- ▶ [Log in to AhsayCBS with 2FA using authenticator app](#)
- ▶ [Log in to AhsayCBS with 2FA using Twilio](#)

2.1 Log in to AhsayCBS without 2FA

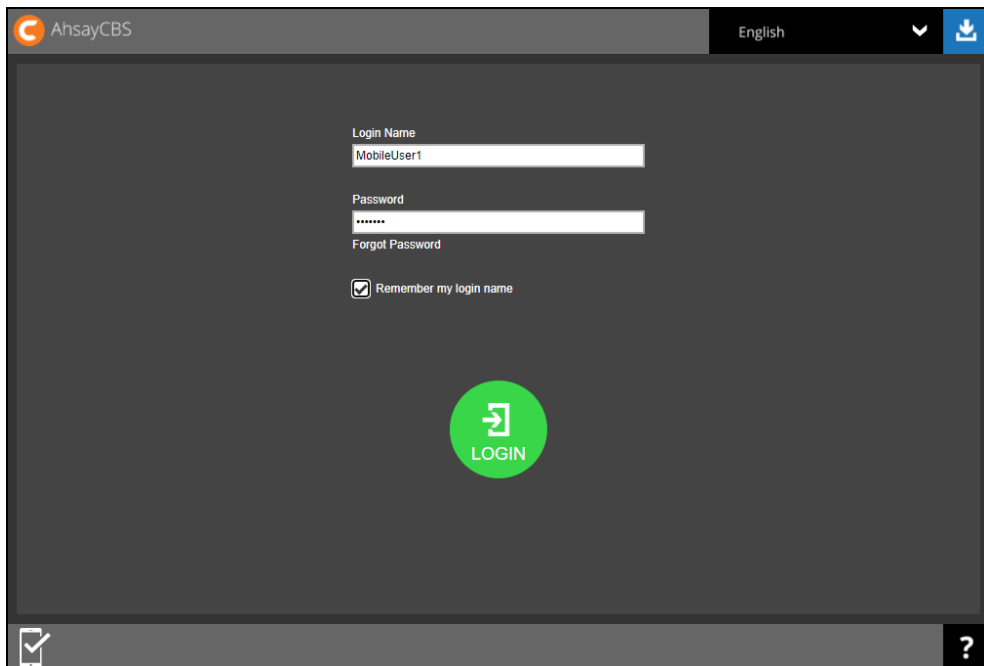
To log in to AhsayCBS without two-factor authentication, please follow the steps below:

1. Log in to the AhsayCBS User Web Console at `https://<IP_AhsayCBS_Server>:443/`

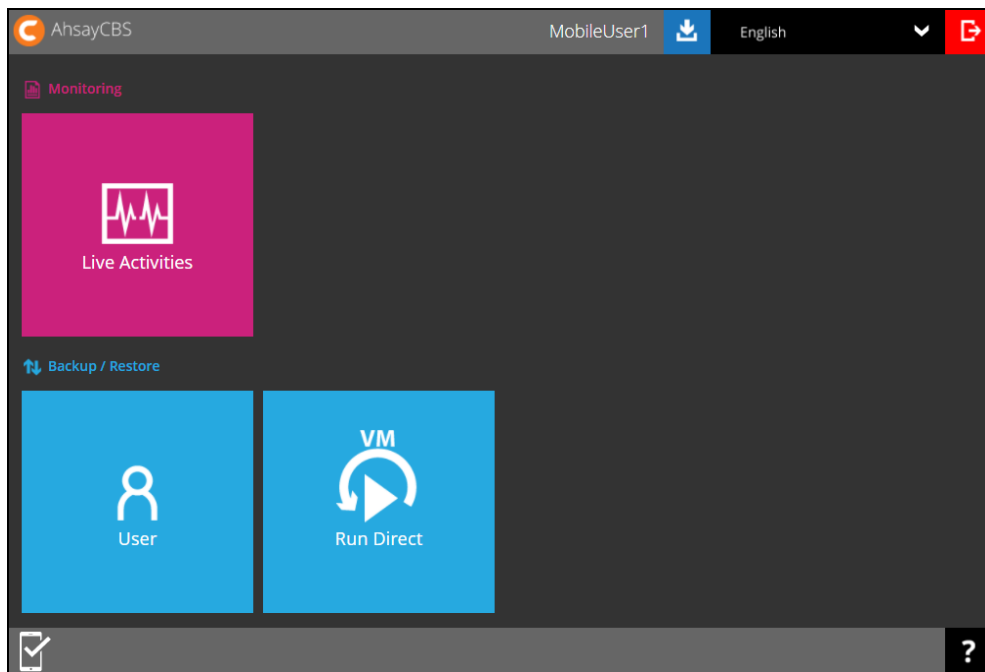
NOTE

Contact your backup service provider for the URL to connect to the web console if necessary.

2. Enter the Login Name and Password of your AhsayOBM/AhsayACB account then click **LOGIN**.



3. After successful log in, the following screen will appear with the available options:
- ◉ **Live Activities** – for monitoring of backup and restore activities
 - ◉ **User** – for backup and restore
 - ◉ **Run Direct** – for backup and restore
 - ◉ **Download** – able to download the following products: AhsayOBM, AhsayACB, Mobile, and AhsayOBR
 - ◉ **Language** – for multiple selection of languages
 - ◉ **Logout** – exit from the AhsayCBS Web Console
 - ◉ **Online Help** – able to check brief descriptions and instructions of each module



NOTE

The VM Run Direct tile may not be available. Please contact your backup service provider for more information.

2.2 Log in to AhsayCBS with 2FA using authenticator app

For subsequent log ins to AhsayCBS with two-factor authentication, please follow the steps below:

1. Log in to the AhsayCBS User Web Console at `https://<IP_AhsayCBS_Server>:443/`

NOTE

Contact your backup service provider for the URL to connect to the web console if necessary.

2. Enter the Login Name and Password of your AhsayOBM/AhsayACB account then click **LOGIN**.

3. One of the two authentication methods will be displayed to continue with the log in:

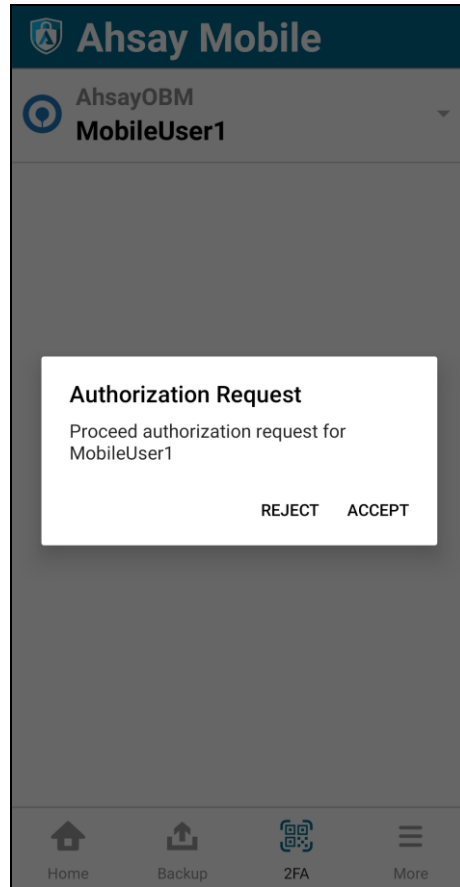
- [Push Notification and TOTP when using Ahsay Mobile app](#)
- [TOTP only](#)

-
- If **Ahsay Mobile app** was configured to use Push Notification and TOTP then there are two 2FA modes that can be used:

- ▶ Push Notification (default)

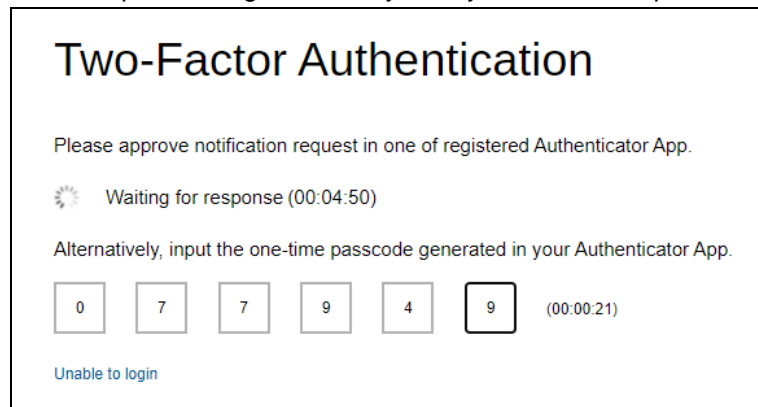
Push notification is the default 2FA mode. Accept the log in request on Ahsay Mobile to complete the log in.

Example of the log in request sent to the Ahsay Mobile app.

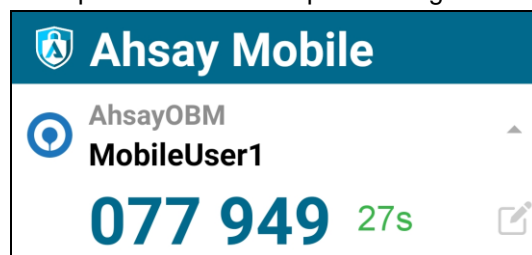


► TOTP

However, if push notification is not working or you prefer to use one-time passcode, click the [Authenticate with one-time password](#) link, then input the one-time passcode generated by Ahsay Mobile to complete the log in.

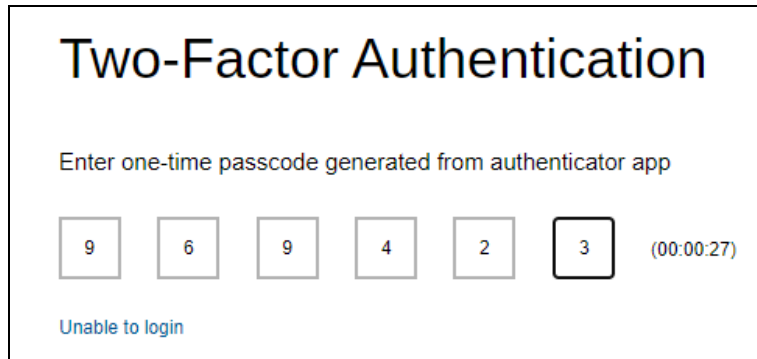


Example of the one-time passcode generated in Ahsay Mobile.

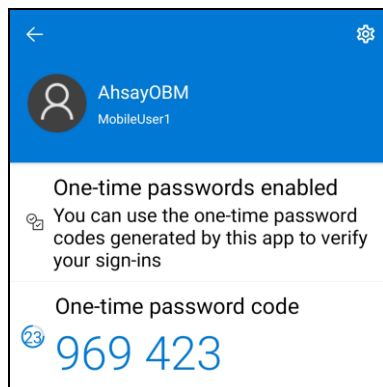


• TOTP only

Enter the one-time passcode generated by the authenticator app to complete the log in.



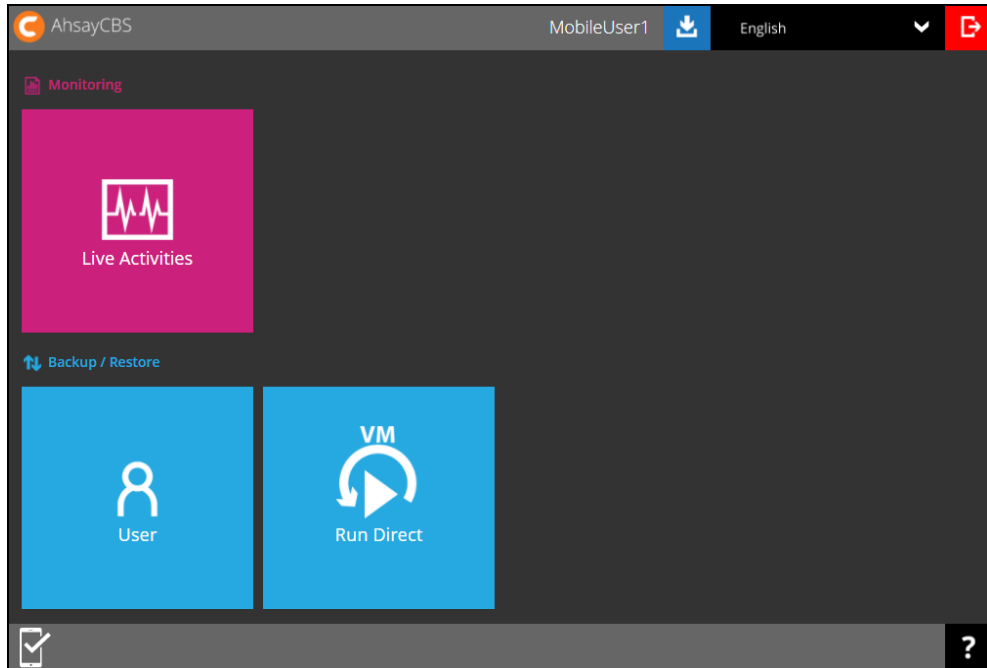
Example of the one-time passcode generated in the third party authenticator app Microsoft Authenticator.



NOTE

Please refer to [Chapter 3](#) or the [Ahsay Mobile App User Guide for Android and iOS – Appendix A: Troubleshooting Login](#) if you are experiencing problems logging in to AhsayCBS User Web Console with Two-Factor Authentication using Ahsay Mobile app or other third party authenticator app.

4. After successful log in, the following screen will appear. For the details of the available options in the main screen, please refer to the description in [Ch. 2.1](#).



NOTE

The VM Run Direct tile may not be available. Please contact your backup service provider for more information.

2.3 Log in to AhsayCBS with 2FA using Twilio

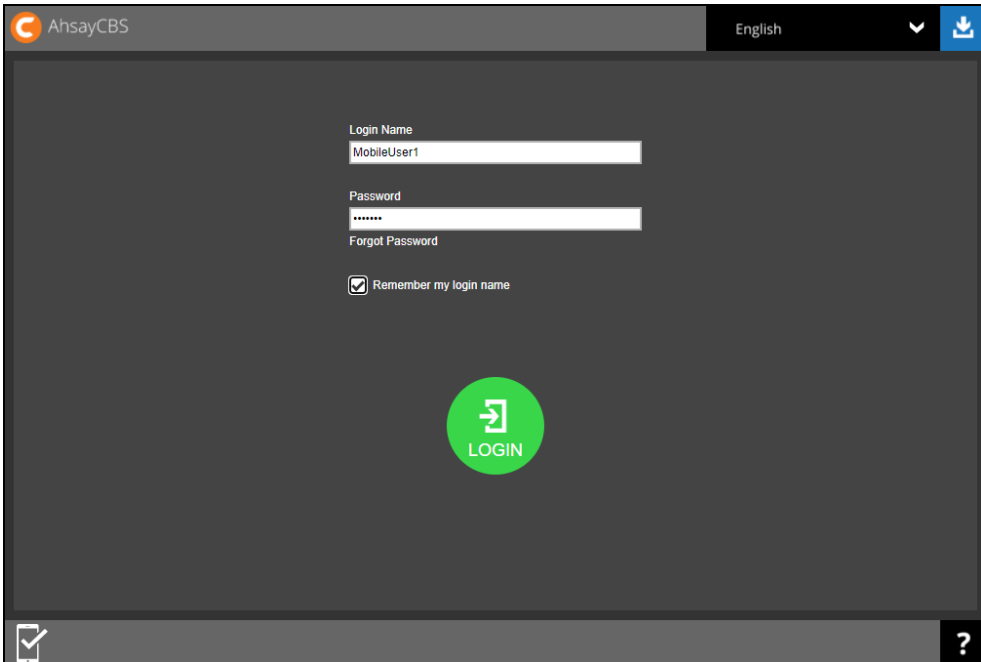
For AhsayOBM/AhsayACB user accounts using Twilio, please follow the steps below:

1. Log in to the AhsayCBS User Web Console at https://<IP_AhsayCBS_Server>:443/

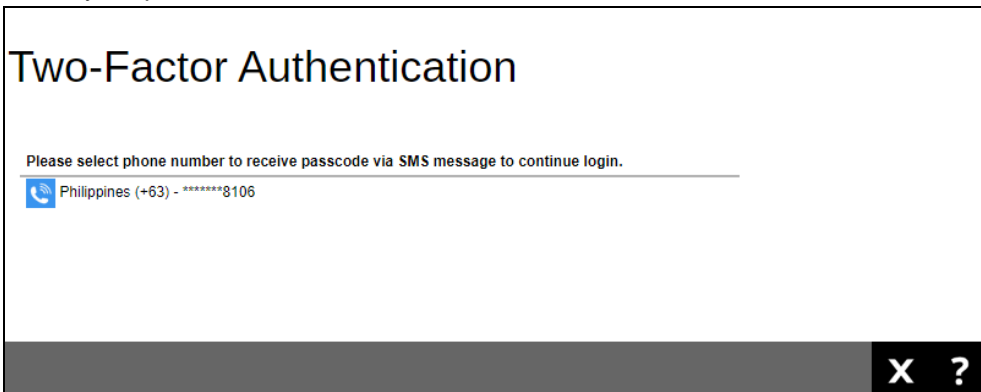
NOTE


Contact your backup service provider for the URL to connect to the web console if necessary.

2. Enter the Login Name and Password of your AhsayOBM/AhsayACB account then click **LOGIN**.



3. Select your phone number.






4. Enter the passcode and click  to log in.

Sent from your Twilio trial account
- AULB-238934 is the verification
code for user "MobileUser1" login
Your backup service provider

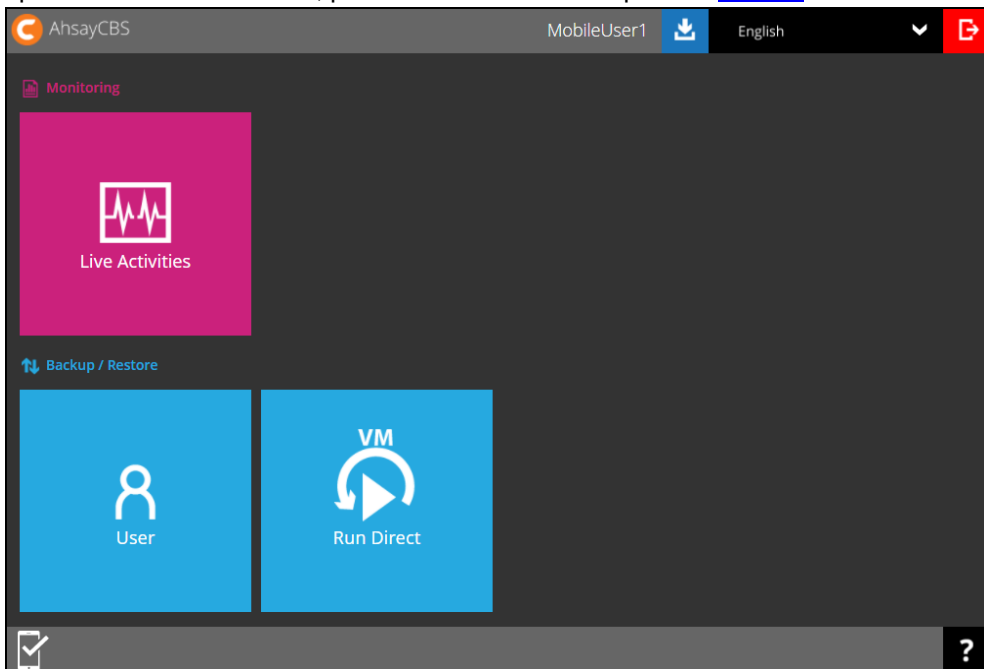
Two-Factor Authentication

SMS message with a passcode was already sent to the phone number +63-*****8106 Please enter the passcode to continue login.

AULB - (00:04:37)

5. After successful log in, the following screen will appear. For the details of the available options in the main screen, please refer to the description in [Ch. 2.1](#).



NOTE

The VM Run Direct tile may not be available. Please contact your backup service provider for more information.

3 Unable to Log in to AhsayCBS with 2FA

In case you have trouble logging in please refer to the three scenarios for instructions:

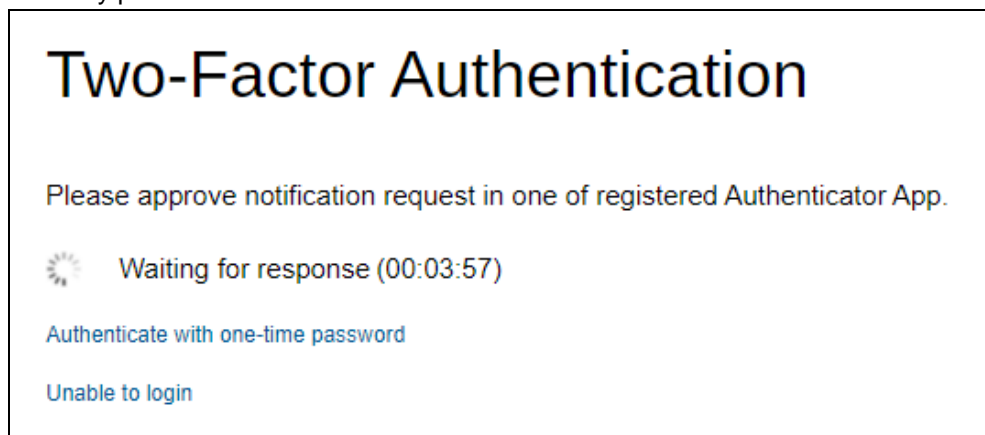
- [Registered a recovery number in Ahsay Mobile app](#)
- [Did not register a recovery number in Ahsay Mobile app](#)
- [Using third party authenticator app](#)

3.1 Registered a recovery number in Ahsay Mobile app

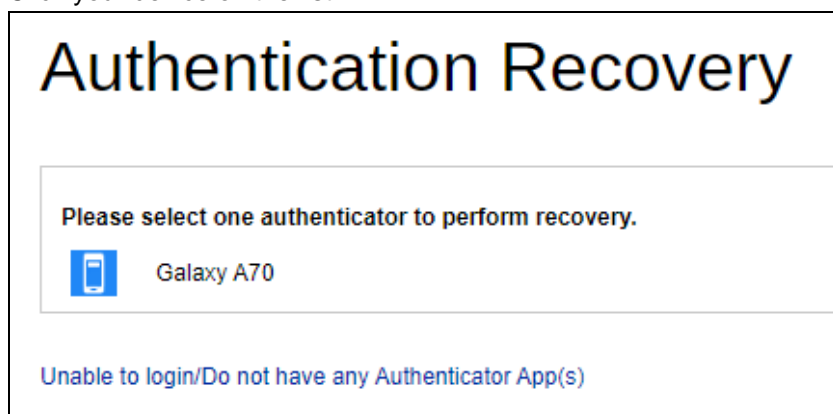
If you have registered a recovery number in your Ahsay Mobile app, then there are two scenarios for this situation:

- [Still have the device but unable to login](#)
- [Lost the device](#)

-
- If you still have the device but unable to log in, you can perform the authentication recovery procedure. Click the [Unable to login](#) link.



Click your device on the list.



Enter the recovery number that you registered and click

Send SMS Verification code

Authentication Recovery


Please enter the first few digits of "Galaxy A70"(*) for recovery. It will be discarded after the recovery process is completed.

Please fill in the recovery phone number

Argentina (+54) 123456789 75

*This phone number will be used for account security and recovery only. Please be reminded that standard SMS charge will be applied.

Send SMS Verification code

Enter the verification code sent to your device and click  to proceed.

Authentication Recovery

You have selected Galaxy A70 and it will be discarded after recovery is completed.

Verification code


YYVQ - 115643 (00:04:44)



Resend SMS Verification code

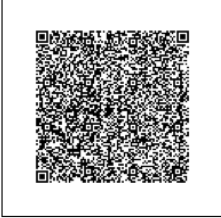
Register your device to be able to log in using 2FA again.

App Download and Device Pairing

Please scan the QR code to get the below Mobile App from App Store. Once installed the Mobile App, launch it and scan the same QR code to complete the device registration.

 Ahsay Mobile




Prerequisites

- Please use the latest Mobile App version

[Not able to scan QR code? Click here to pair with TOTP secret key](#)

- ⦿ If you have lost the device, the authentication recovery procedure will not work until your new device is installed with a replacement SIM card. Since you will need to enter the verification code that will be sent to the recovery number that you registered in Ahsay Mobile. So please contact your backup service provider instead.

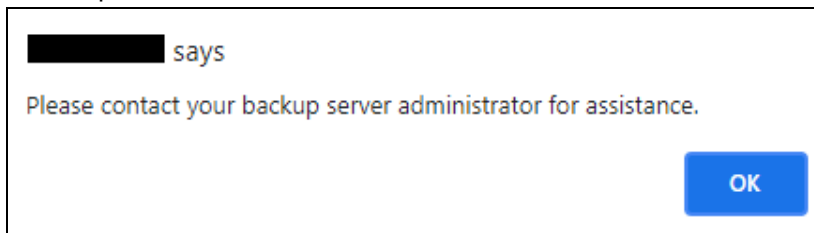
 says

Please contact your backup server administrator for assistance.

OK

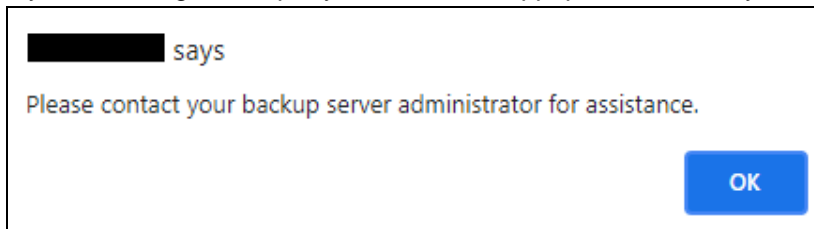
3.2 Did not register a recovery number in Ahsay Mobile

If you have not registered a recovery number in Ahsay Mobile, please contact your backup service provider.



3.3 Using third party authenticator app

If you are using a third party authenticator app, please contact your backup service provider.



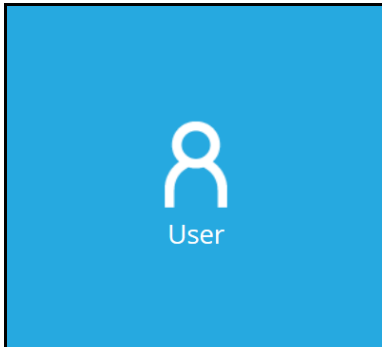
4 Managing Your AhsayCBS User Account

4.1 Log in to AhsayCBS

Log in to the AhsayCBS user web console according to the instruction provided in section [Logging in to AhsayCBS User Web Console](#).

4.2 Managing AhsayCBS Backup User

To manage your AhsayCBS backup user account, simply click the **User** icon from your AhsayCBS environment.



You can perform the following operations on your own user account:

- Manage your user profile settings, e.g. New Password, Language, Timezone, Contact Information.
- Customize event log settings, which is supported on AhsayOBM/ AhsayACB clients installed on Windows platform only.
- View backup or restore reports for different time periods.
- View usage statistics by selecting destination, backup set, and period.
- View details of policies and settings on users, backup sets, GUIs, default values, preempted values, preempted backup sets, and mobile. The settings and the availability of this feature is dependent on your backup service provider.
- Register mobile device for two-factor authentication.
- View mobile device registered for mobile backup.

4.3 User Profile

User Profile page contains your user backup account settings information, subscribed modules backup quota, subscription type, contact information, user group information, two-factor authentication settings and registered mobile device for mobile backup.

Among all the above information, you can modify user backup account settings information, contact information and registered mobile device for two-factor authentication. However, for the subscribed modules backup quota, subscription type, and user group information, as the setting was done when the user account was created, the settings cannot be modified by the user. While the registered mobile device for mobile backup and its backup destination can only be viewed here.

There are six (6) tabs under **User Profile**, each of which is described below:

4.3.1 General Tab

The following shows the General tab under the User Profile settings page.

The screenshot displays the 'User Profile' settings page, specifically the 'General' tab. The page is divided into a left sidebar and a main content area. The sidebar contains navigation links: Backup Set, Settings, Report, Statistics, and Effective Policy. The main content area is titled 'General information of this user.' and contains several sections:

- Basic**: ID (1607015428255), Login Name (WindowsTest_1), and Alias (empty field).
- Home Directory**: C:\Program Files\AhsayCBS\user\WindowsTest_1
- Subscription Type**: Radio buttons for Trial User and Paid User (selected).
- Suspend At**: Date field (04-12-2020) with format (dd-mm-yyyy).
- Status**: Radio buttons for Enable (selected), Suspended, and Locked.
- Upload Encryption Key**: Checkmark for 'Upload encryption key after running backup for recovery'.
- Language**: Dropdown menu set to English.
- Timezone**: Dropdown menu set to GMT+08:00 (CST).
- Notes**: A large empty text area for notes.

There are several groups of settings under the **General** tab, and they are described below.

Section	Description
Basic	<p>There are three (3) elements in the Basic section, which are the following:</p> <ul style="list-style-type: none"> • ID of the backup user, this is system generated and cannot be changed. • Login Name of the backup user, defined by the service provider which cannot be changed. • Alias is another name for the backup user which can be modified.
Home Directory	<p>This is the path where your backup data is stored on AhsayCBS backup destination.</p> <p>This was set when your account was created and cannot be modified by the user.</p>
Subscription Type	<p>There are two (2) subscription types: Trial User and Paid User. Trial users are subject to automatic removal after the trial period. Paid users do not have such restrictions.</p> <p>This was set when your account was created and cannot be modified by the user. If you need to change it, please contact your backup service provider.</p>
Suspend At	<p>This shows the date when a trial user account is scheduled to be suspended.</p> <p>This was set when your account was created and cannot be modified by the user. If you need to update it, please contact your backup service provider.</p>
Status	<p>There are three (3) user account statuses: Enable, Suspended, and Locked. The Locked status refers to account lockout rules. For example, when the user has three (3) consecutive unsuccessful log in attempts, the user account will be locked.</p> <p>This was set when your account was created and cannot be modified by the user. If you need to change it, please contact your backup service provider.</p>
Upload Encryption Key	<p>To enable or disable this feature please contact your backup service provider for support. The encryption key file will be uploaded to the backup server when a backup run.</p> <p>If you forget the encryption key, please contact your backup service provider for support.</p>
Language	Select your preferred language for all email reports.
Timezone	Select the time zone of the backup user.
Notes	A field for the AhsayCBS user to add notes.

NOTE

The **Mobile Backup** tab will only be visible if Mobile Add-on Module is enabled.

4.3.2 Backup Client Settings Tab

This shows the **Backup Client Settings** tab under the **User Profile** settings page.

User Profile
General
Backup Client Settings
Contact
User Group
Authentication
Mobile Backup

Backup Set

Settings

Report

Statistics

Effective Policy

Settings of the client backup agent for this user.

Backup Client

AhsayOBM User AhsayACB User

Add-on Modules

<input checked="" type="checkbox"/> Microsoft Exchange Server	<input checked="" type="checkbox"/> Microsoft SQL Server
<input checked="" type="checkbox"/> MySQL Database Server	<input checked="" type="checkbox"/> Oracle Database Server
<input type="checkbox"/> Lotus Domino	<input type="checkbox"/> Lotus Notes
<input checked="" type="checkbox"/> Windows System Backup	<input checked="" type="checkbox"/> Windows System State Backup
<input checked="" type="checkbox"/> VMware <input type="text" value="Guest VM"/> <input type="text" value="10"/>	<input checked="" type="checkbox"/> Hyper-V <input type="text" value="Guest VM"/> <input type="text" value="10"/>
<input checked="" type="checkbox"/> Microsoft Exchange Mailbox <input type="text" value="10"/>	<input type="checkbox"/> ShadowProtect System Backup
<input checked="" type="checkbox"/> NAS - QNAP	<input checked="" type="checkbox"/> NAS - Synology
<input checked="" type="checkbox"/> Mobile (max. 10)	<input checked="" type="checkbox"/> Continuous Data Protection
<input checked="" type="checkbox"/> Volume Shadow Copy	<input checked="" type="checkbox"/> In-File DeltaOnly apply to v8 or before
<input checked="" type="checkbox"/> OpenDirect / Granular Restore <input type="text" value="10"/>	<input checked="" type="checkbox"/> Office 365 Backup <input type="text" value="10"/>
<input checked="" type="checkbox"/> MariaDB Database Server	<input checked="" type="checkbox"/> Deduplication

Quota

Unlimited storage space for the destination not shown in the following table

<input type="checkbox"/>	Destination	Quota	
<input type="checkbox"/>	AhsayCBS	<input type="text" value="10.0"/>	<input type="text" value="Gbytes"/>

(If preempted mode is enabled in policy settings, the quota settings are disabled)

Client host limit

Maximum number of host [Used: 1]

Run Direct

Maximum number of VM [Used: 0]

There are several groups of settings under the **Backup Client Settings** tab, and they are described below.

Section	Description
Backup Client	<p>There are two (2) types of backup user accounts: AhsayOBM and AhsayACB.</p> <p>This was set when your account was created and cannot be modified by the user. If you need to change it, please contact your backup service provider.</p>
Add-on Modules	<p>The backup client comes with add-on modules.</p> <p>These add-on modules were set when the user account was created and cannot be modified by the user. If you need to change the add-on modules, please contact your backup service provider.</p>
Quota	<p>List all the predefined and standard destinations associated with the user account and the backup quota of predefined destination for the user account can be set.</p> <p>The quota of standard destination was set when your account was created and cannot be modified by the user. If you need to change it, please contact your backup service provider.</p>
Client Host Limit	<p>This is for your backup service provider to set the maximum number of host machine for your backup user account.</p> <p>This field cannot be changed by the user. If you need to update this field, please contact your backup service provider.</p>
Run Direct	<p>This allows the user to select the maximum number of VMs to be restored by running them directly from the backup files on the AhsayCBS.</p> <p>This field cannot be changed by the user. If you need to update this field, please contact your backup service provider.</p>

Add-on Modules

The following table shows all the add-on modules available under the **Backup Client Settings** tab. The backup of these add-on modules is supported by the AhsayOBM client. For some of the add-on modules, their backup are also supported by the AhsayACB client.

NOTE	
<ul style="list-style-type: none"> The File and Cloud File Backup types are available by default for both AhsayACB and AhsayOBM. As a result, they do not need to be added and are not included in the Add-on Modules section of the Backup Client Settings tab. 	
<ul style="list-style-type: none"> There is no limit to number of Cloud file backup sets per AhsayOBM and AhsayACB account. 	

The following table shows the name of the add-on modules, what it is used for, whether it is available in AhsayOBM client or AhsayACB client, and reference materials you can refer to for more information.

Add-on Module	Reference	AhsayOBM	AhsayACB
Microsoft Exchange Server	Backup and restore of Microsoft Exchange Server. Refer to the following link for how to use Microsoft Exchange Database Server with AhsayOBM client: Ahsay Online Backup Manager v9 Microsoft Exchange Database Backup and Restore Guide	✓	X
Microsoft SQL Server	Backup and restore of Microsoft SQL Server. Refer to the following link for how to use Microsoft SQL Server with AhsayOBM client: Ahsay Online Backup Manager v9 Microsoft SQL Server Backup and Restore Guide	✓	X
MySQL Database Server	Backup and restore of MySQL Database Server. Refer to the following link for how to use MySQL Database for the Windows platform with AhsayOBM client: Ahsay Online Backup Manager v9 MySQL Database Backup and Restore for Windows Refer to the following link for how to use MySQL Database for the Linux platform with AhsayOBM client: Ahsay Online Backup Manager v9 MySQL Database Backup and Restore for Linux (CLI)	✓	X
Oracle Database Server	Backup and restore of Oracle Database Server. Refer to the following link for how to use Oracle Database for the Windows platform with AhsayOBM client: Ahsay Online Backup Manager v9 Oracle Database Backup and Restore for Windows Refer to the following link for how to use Oracle Database for the Linux platform with AhsayOBM client: Ahsay Online Backup Manager v9 Oracle	✓	X

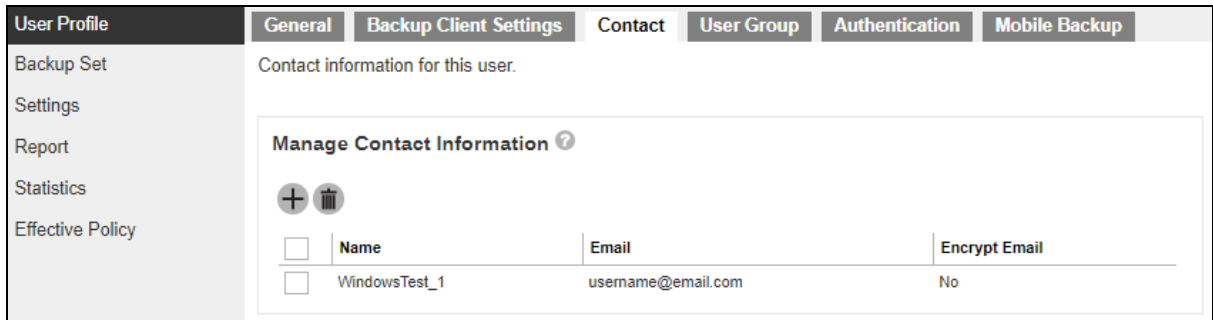
	Database Backup and Restore for Linux (CLI) Ahsay Online Backup Manager v9 Oracle Database Backup and Restore for Linux (GUI)		
Lotus Domino	Backup and restore of Lotus Domino.	✓	X
Lotus Notes	Backup and restore of Lotus Notes.	✓	✓
Windows System Backup	Backup and restore of Windows System Backup. Refer to the following link for how to use Windows System Backup with AhsayOBM and AhsayACB clients: Ahsay Online Backup Manager v9 Microsoft System Backup and Restore Guide	✓	✓
Windows System State Backup	Backup and restore of Windows System State Backup. Refer to the following link for how to use Windows System State Backup with AhsayOBM client: Ahsay Online Backup Manager v9 Microsoft System State Backup and Restore Guide	✓	X
VMware	Backup and restore of VMware guest virtual machines. Refer to the following link for how to use VMware VCenter/ESXi with AhsayOBM client: Ahsay Online Backup Manager v9 VMware vCenter/ESXi Backup and Restore Guide	✓	X
Hyper-V	Backup and restore of Hyper-V guest virtual machines. Refer to the following link for how to use Microsoft Hyper-V with AhsayOBM client: Ahsay Online Backup Manager v9 Microsoft Hyper-V Backup and Restore Guide	✓	X
Microsoft Exchange Mailbox	Backup and restore of Microsoft Exchange Mailbox. Refer to the following link for how to use Microsoft Exchange 2007/2010/2013 (MAPI) Mailbox with AhsayOBM client: Ahsay Online Backup Manager v9 Microsoft Exchange 2007/2010/2013 (MAPI) Mail-Level Backup & Restore Guide Refer to the following link for how to use Microsoft Exchange 2013/2016/2019 (EWS) Mailbox with AhsayOBM client: Ahsay Online Backup Manager v9 Microsoft Exchange 2013/2016/2019 (EWS) Mail Level Backup & Restore Guide	✓	X
Shadow Protect System Backup	Backup and restore of Shadow Protect System image (requires Shadow Protect).	✓	X

	<p>Refer to the following link for how to use the ShadowProtect System Backup with AhsayOBM client:</p> <p>Ahsay Online Backup Manager v7 StorageCraft ShadowProtect System Backup & Restore Guide</p>		
NAS - QNAP	<p>Backup and restore of file on QNAP NAS devices.</p> <p>Refer to the following link for how to use the QNAP NAS with AhsayOBM client:</p> <p>Ahsay Online Backup Manager v9 Quick Start Guide for QNAP NAS</p> <p>Refer to the following link for a list of QNAP hardware compatible with AhsayOBM:</p> <p>FAQ: Ahsay Hardware Compatibility List (HRL) for AhsayOBM on QNAP NAS</p>	✓	X
NAS - Synology	<p>Backup and restore of file on Synology NAS devices.</p> <p>Refer to the following link for how to use the Synology NAS with AhsayOBM client:</p> <p>Ahsay Online Backup Manager v9 Quick Start Guide for Synology NAS</p> <p>Refer to the following link for a list of Synology hardware compatible with AhsayOBM:</p> <p>FAQ: Ahsay Hardware Compatibility List (HRL) for AhsayOBM on Synology NAS</p>	✓	X
Mobile	<p>Backup and restore of Mobile data (iOS and Android).</p> <p>Refer to the following links for instructions on using the Ahsay Mobile for Android and iOS platforms.</p> <p>Ahsay Mobile Getting Started Guide for Mobile Backup</p> <p>Ahsay Mobile Getting Started Guide for 2FA</p> <p>Ahsay Mobile User Guide for Android and iOS</p>	✓	✓
Continuous Data Protection	<p>A backup will be made whenever there is a change (between 1 min to 12-hour intervals). Applies to File backup sets on Windows platform.</p>	✓	✓
Volume Shadow Copy	<p>Volume Shadow Copy to support open file backups on Windows platform.</p>	✓	✓
In-File Delta	<p>When enabled only the changes since the last backup job is backed up. Only available for versions prior to v9.</p>	✓	✓
OpenDirect / Granular Restore	<p>For OpenDirect and Granular Restore.</p> <p>Refer to the following link for instructions on using OpenDirect / Granular Restore.</p> <p>AhsayACB v9 Quick Start Guide for Windows</p>	✓	X

	Ahsay Online Backup Manager v9 Quick Start Guide for Windows Ahsay Online Backup Manager v9 Microsoft Hyper-V Backup and Restore Guide Ahsay Online Backup Manager v9 VMware vCenter/ESXi Backup and Restore Guide		
Microsoft 365 Backup	<p>Backup and restore of mailboxes and files of Microsoft 365 including the One Drive, Personal Site, Public Folders, and Site Collections.</p> <p>Refer to the following link for instructions on using Microsoft 365.</p> <p>Ahsay Online Backup Manager v9 User Guide for Microsoft 365 Backup & Restore for Windows</p> <p>Ahsay Online Backup Manager v9 User Guide for Microsoft 365 Backup & Restore for Mac</p> <p>AhsayACB v9 User Guide for Microsoft 365 for Windows</p> <p>AhsayACB v9 User Guide for Microsoft 365 for Mac</p> <p>AhsayCBS v9 User Guide - Microsoft 365 Run on Server (Agentless) Backup and Restore Guide</p>	✓	✓
MariaDB Database Server	<p>Backup and restore of MariaDB Database Server.</p> <p>Refer to the following link for how to use MariaDB Database for the Windows platform with AhsayOBM client:</p> <p>Ahsay Online Backup Manager v9 MariaDB Database Backup and Restore for Windows</p> <p>Refer to the following link for how to use MariaDB Database for the Linux platform with AhsayOBM client:</p> <p>Ahsay Online Backup Manager v9 MariaDB Database Backup and Restore for Linux (CLI)</p>	✓	X
Deduplication	<p>Replaces the In-File Delta module. This is a standard add-on module, not a premium (pay) add-on module. When enabled, will deduplicate the data under the same backup set.</p>	✓	✓



4.3.3 Contact Tab


You can add your contact information here to receive backup or restore reports. You can also delete your contact information here. The following shows the **Contact** tab under the **User Profile** settings page.



The screenshot shows the 'Contact' tab selected in the 'User Profile' settings. The left sidebar contains 'Backup Set', 'Settings', 'Report', 'Statistics', and 'Effective Policy'. The main content area is titled 'Contact information for this user.' and features a 'Manage Contact Information' section with a plus icon and a trash icon. Below this is a table with columns for Name, Email, and Encrypt Email. The table contains one entry: 'WindowsTest_1', 'username@email.com', and 'No'.



<input type="checkbox"/>	Name	Email	Encrypt Email
<input type="checkbox"/>	WindowsTest_1	username@email.com	No

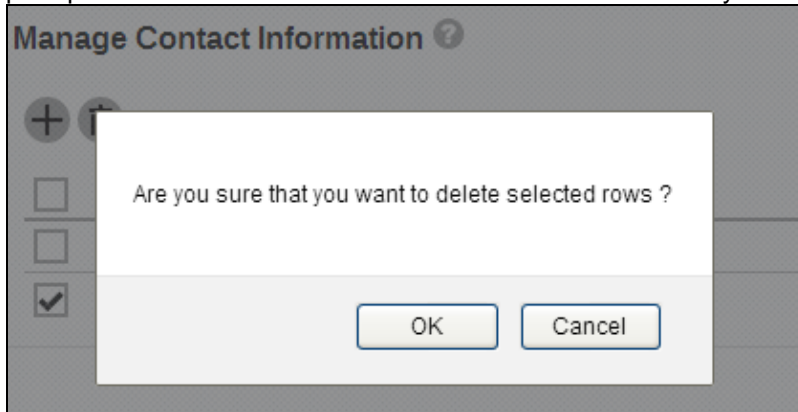
- To add your contact information, click  in the middle of the screen. Enter your **Name**, **Email**, **Address**, **Company**, **Website**, **Phone1**, **Phone2**, then click  at the bottom right corner of the screen. A new contact is added.



The form contains the following fields:

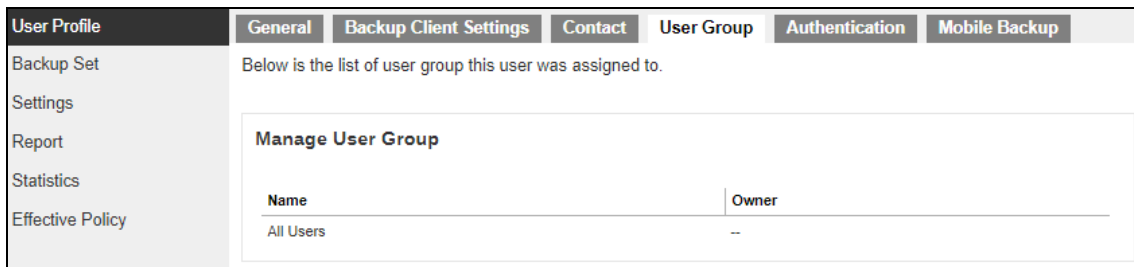
- Name:
- Email:
 Encrypt Email
- Address:
- Company:
- Website:
- Phone 1:
- Phone 2:

- To delete a contact information, check the box next to the contact information you want to delete, then click  in the middle of the screen. Click OK to delete the contact when prompted. The selected contact is deleted. Click  to save your changes.




4.3.4 User Group Tab

The following shows the **User Group** tab under the **User Profile** settings page. It shows the user group your user account belongs to. This is set when your account was created and cannot be modified.



NOTE

Please remember to click  after modification to save the changes. Otherwise the modification will be lost after quitting the setting page.

4.3.5 Authentication Tab

The Authentication tab allows the User to add additional layer of security to their backup user accounts. This tab allows resetting of password and enables the Two-Factor Authentication (2FA). Please contact your service provider for more details on this feature.

This view applies when two-factor authentication is enabled for the user account.

The screenshot shows the 'Authentication' tab selected in the user profile settings. The left sidebar contains 'User Profile', 'Backup Set', 'Settings', 'Report', 'Statistics', and 'Effective Policy'. The main content area is divided into three sections:

- Password:** A text field containing a hashed password 'ungWv48Bz+pBQUDeXa4iI7ADYaOWF3qctBD/YfiAFa0=' with a 'Hashed' label and a 'Reset Password' link below it.
- Two-Factor Authentication:** A toggle switch is turned on. Below it, there is a 'Registered Mobile Device(s)' section with a '+' icon to add a device and a trash icon to remove one. A table lists the registered devices:

<input type="checkbox"/>	Device Name	Verified	Last Verified Time
<input type="checkbox"/>	A32	✓	08/20/2021 17:44:36 CST
<input type="checkbox"/>	Re-pair with authenticator		
- Last Successful Login:** Displays login details: Time: 08/20/2021 17:44:36 CST, IP address: [redacted], Browser / App: AhsayOBM, and Mobile Device: A32.

If two-factor authentication is not enabled, this will be displayed instead.


The screenshot shows the 'Authentication' tab selected in the user profile settings. The left sidebar is the same as in the previous screenshot. The main content area is divided into two sections:

- Password:** A text field containing a hashed password 'ungWv48Bz+pBQUDeXa4iI7ADYaOWF3qctBD/YfiAFa0=' with a 'Hashed' label and a 'Reset Password' link below it.
- Last Successful Login:** Displays login details: Time: 10/25/2021 09:48:43 SGT, IP address: [redacted], Browser / App: AhsayOBM, and Mobile Device: --.

There are several groups of settings under the **Authentication** tab, and they are described below:

Section	Description
Password	<p>There are two (2) elements in the Password section, which are the following:</p> <ul style="list-style-type: none"> • Password in hashed format defined by the service provider which cannot be changed. • Reset Password allows the backup user to change the password.

<p>Two-Factor Authentication</p>	<p>Allows the user to add mobile device(s) that will be used for two-factor authentication. It displays the device name, whether it has been verified or not and the last verified time and date.</p> <p>This will only be visible if two-factor authentication is enabled for the user account.</p> <p>The Re-pair with authenticator will only be available if Ahsay Mobile is used as the authenticator app. If the registered device used for 2FA was damaged, lost or missing; the backup content of the device can be migrated to the new device by using AhsayOBM/AhsayACB. For instructions on how to do this please refer to the Ahsay Mobile User Guide for Android and iOS. Once the migration is finished, the new device must be re-paired with the Ahsay Mobile app to enable sign-in using push notification and disable the one in the original device.</p> <p>Please contact your backup service provider for details.</p>
<p>Last Successful Login</p>	<p>There are four (4) elements in the Last Successful Login section, which are the following:</p> <ul style="list-style-type: none"> • Time, this is the date and time the backup user last logged in, this changes every time the user logs in. • IP address used to log in, which cannot be changed. • Browser / App used to log in. If browser, the operating system, and browser used will be displayed. If app, either AhsayOBM or AhsayACB will be displayed. • Mobile Device, the name of the mobile device used to log in.

- To reset the password, click [Reset Password](#). Enter the new password twice and click  to save.

Password

New Password

Confirm Password

- To add a mobile device for two-factor authentication, follow the instructions below:



1. Enable Two-Factor Authentication by sliding the switch to the right.

Two-Factor Authentication

2. Click the  button.

Two-Factor Authentication

Registered Mobile Device(s)

<input type="checkbox"/>	Device Name	Verified	Last Verified Time

3. The following screen that will be displayed will depend on the settings made by your backup service provider. Follow the instructions discussed in Chapter 2 on how to register your device depending on the authenticator app that you will be using:

- ◉ [Ahsay Mobile or branded Mobile app](#)
- ◉ [Microsoft Authenticator](#)
- ◉ [Google Authenticator](#)
- ◉ [Third party authenticators](#)

4.3.6 Mobile Backup Tab

The Mobile Backup tab allows the User to view the mobile device(s) that has been registered for mobile backup and the corresponding backup destination. To add a mobile device use AhsayOBM or AhsayACB.

For more information on how to do this please refer to the following guides:

[AhsayOBM Quick Start Guide](#), [AhsayACB Quick Start Guide](#), [Ahsay Mobile Getting Started Guide for Mobile Backup](#) and [Ahsay Mobile User Guide](#)

User Profile	General	Backup Client Settings	Contact	User Group	Authentication	Mobile Backup						
Backup Set	Mobile Backup Registered Mobile Device(s) <table border="1"><thead><tr><th>Device Name</th><th>Backup Destination</th></tr></thead><tbody><tr><td>iPhone 6</td><td>D:\backup\iPhone 6\1607069270717</td></tr><tr><td>Galaxy A70</td><td>D:\backup\Galaxy A70\1607069604823</td></tr></tbody></table>						Device Name	Backup Destination	iPhone 6	D:\backup\iPhone 6\1607069270717	Galaxy A70	D:\backup\Galaxy A70\1607069604823
Device Name							Backup Destination					
iPhone 6							D:\backup\iPhone 6\1607069270717					
Galaxy A70							D:\backup\Galaxy A70\1607069604823					
Settings												
Report												
Statistics												
Effective Policy												

4.4 Settings

The **Settings** page allows the user to log the optional events, besides AhsayOBM/ AhsayACB logs, to the Windows event log.

NOTE

This feature is supported on AhsayOBM/AhsayACB clients installed on Windows platform only.

Windows event log

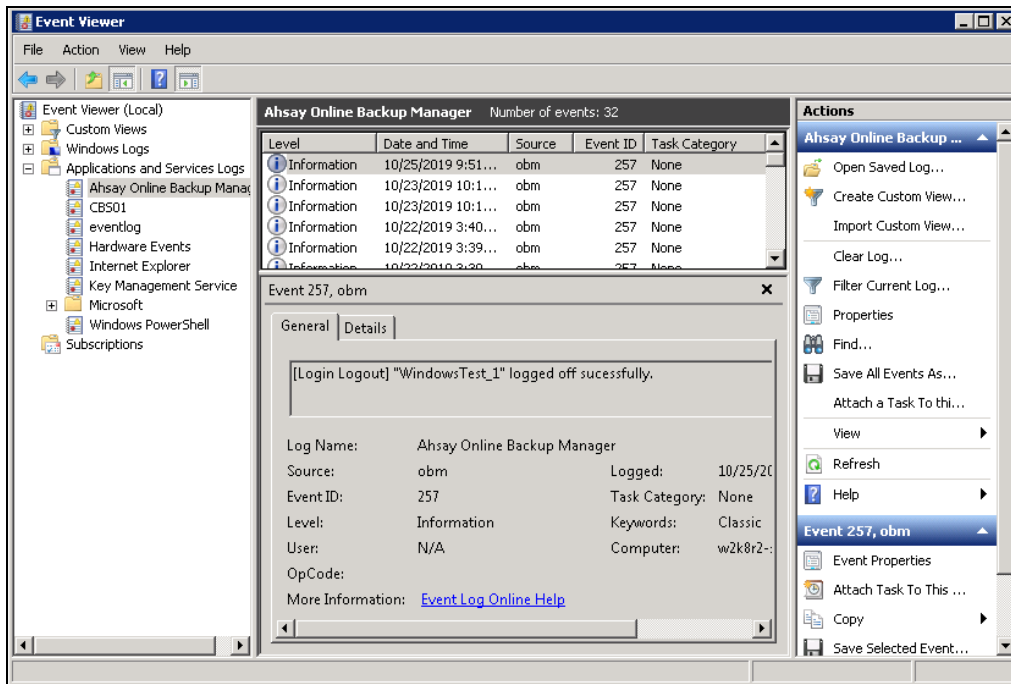
The following shows the options on the **Settings** page.

The screenshot shows the 'Windows Event Log' configuration page. On the left, a sidebar lists navigation items: User Profile, Backup Set, Settings (selected), Report, Statistics, and Effective Policy. The main area is titled 'Windows Event Log' and features a 'Log type' section with three checked options: Error, Warning, and Info. Below that is a 'Log option' section with eight checked options: Profile, Backup, Restore, Service (CDP & Scheduler), Software Update, Report, Utilities, and Login / Logout.

There are two groups of settings under the **Settings** tab, and they are described below.

Setting	Description
Log Type	There are three (3) log types available: Error , Warning , and Info . You can select any combinations of the 3 log types, and the messages will be logged in the Windows event log.
Log Option	Select the log option by which the particular action will be captured in the Windows event log. Currently there are eight (8) different log options that can be selected: Profile , Backup , Restore , Service (CDP & Scheduler) , Software Update , Report , Utilities , and Login/Logout .

The events are logged in the Windows event log and can be viewed from the Windows Event Viewer:



4.5 Report

The **Report** page allows you to check the **Backup** and **Restore** report of both backup and restore jobs proceeded in agent-based (AhsayOBM/ AhsayACB/ AhsayOBR) and agentless (AhsayCBS User Web Console) type.

4.5.1 Backup Reports

1. A list of backup reports for this AhsayCBS user can be found on the **Backup** tab. Click on the desired report to get more details on the report.

Backup Set	Destination	Start Time	End Time	Status
backupset-2(1641869270986)	AhsayCBS	11-Jan-2022 10:53 CST	11-Jan-2022 10:54 CST	OK
backupset-1(1641867252796)	AhsayCBS	11-Jan-2022 10:42 CST	11-Jan-2022 10:42 CST	OK

2. Click the **Download report** button at the bottom to download the complete report in PDF format. The backup report will be available around 15 to 20 minutes after a backup job has finished.

Backup Report

Backup Set backupset-2(1641869270986)

Destination AhsayCBS

Job 11-Jan-2022 10:53:56

Time 11-Jan-2022 10:53:57 CST - 11-Jan-2022 10:54:04 CST

Status OK

New Files* 33 [315.02K / 487.51K (35%)]

New Directories 2

New Links 0

Updated files* 0

Attributes Changed Files* 0

Deleted Files* 0

Deleted Directories 0

Deleted Links 0


Moved Files* 0

Dedupe Saving 351.75K / 487.51K [72.2%]

* Unit = No of files [Total zipped size / Total unzipped size (compression ratio)]

[Download report](#)

- A full version of the backup report appears. You can view the detailed backup set settings on this report.



Full Backup report

Backup Job Summary

User	user5
Backup Set	backupset-2 (164180927096)
Destination	AhsayCBS (AhsayCBS)
Data Size	77K
Retention Size	0
Backup Quota	5G
Remaining Quota	5G
Backup Job	2022-01-11-10-53-56
Job Status	OK
Start - End	01/11/2022 10:53:57 CST - 01/11/2022 10:54:04 CST
IP Address	10.31.21.17 6/2c1682-std-maq(2k-12)
New Files *	33 (315K)
New Directories	2
New Links	0
Updated Files *	0 (0)
Attributes Changed Files *	0 (0)
Deleted Files *	0 (0)
Deleted Directories	0
Deleted Links	0
Moved Files *	0 (0)
Dedupe Saving	351K / 487K [72.2%]

* No. of files (size)

Backup Set Settings

Field	Value
Backup Source	[D:\filter\sample]
Filter	[Enabled: No]
Backup Schedule	[Computer Name:] [Daily:] [Weekly:] [Monthly:] [Custom:]
Continuous Data Protection	[Enabled: No]
Deduplication	[Enabled: Yes] Migrate existing data to latest version: No
Retention Policy	[Type: Simple, Period: 7, Unit: Day(s)]
Command Line Tool	
Reminder	[Computer Name:]
Bandwidth Control	[Enabled: No, Mode: Independent, Bandwidth Control:]
Others	[Remove temporary files after backup: Yes] [Follow Link: Yes] [Volume Shadow Copy: No] [File Permissions: Yes] [Compression Type: Fast with optimization for local]

Backup Logs

No.	Type	Timestamp	Log
1	start	2022/01/11 10:53:57	Start [AhsayCBS v6.0.3.12]
2	info	2022/01/11 10:53:57	Saving encrypted backup set encryption keys to server...
3	info	2022/01/11 10:53:59	Using Temporary Directory C:\Users\Administrator\ohm\temp\164180927096\O258164180329470
4	info	2022/01/11 10:54:00	Start running pre-commands
5	info	2022/01/11 10:54:00	Finished running pre-commands
6	info	2022/01/11 10:54:02	Download valid index files from backup job "aid" to "C:\Users\Administrator\ohm\temp\164180927096\O258164180329470\index".
7	info	2022/01/11 10:54:02	Deduplication: Infile File="D:\filter\sample\AhsayCBS_UserGuideforWindows_version7.docx", duplicated file="D:\filter\sample\AhsayCBS_version7_UserGuide.docx (2022-01-11-10-53-56)", size="14,902"
8	info	2022/01/11 10:54:02	Deduplication: Infile File="D:\filter\sample\AhsayCloudFileBackupSolution_v7.pptx", duplicated file="D:\filter\sample\AhsayCloudFileBackupSolution_v10.pptx (2022-01-11-10-53-56)", size="38,994"
9	info	2022/01/11 10:54:02	Deduplication: Infile File="D:\filter\sample\AhsayCloudFileBackupSolution_v8.pptx", duplicated file="D:\filter\sample\AhsayCloudFileBackupSolution_v10.pptx (2022-01-11-10-53-56)", size="38,994"
10	info	2022/01/11 10:54:02	Deduplication: Infile File="D:\filter\sample\AhsayCloudFileBackupSolution_v9.pptx", duplicated file="D:\filter\sample\AhsayCloudFileBackupSolution_v10.pptx (2022-01-11-10-53-56)", size="38,994"
11	info	2022/01/11 10:54:02	Deduplication: Infile File="D:\filter\sample\AhsayOBM_version7_QuickStartGuide.docx", duplicated file="D:\filter\sample\AhsayCBS_version7_UserGuide.docx (2022-01-11-10-53-56)", size="14,902"
12	info	2022/01/11 10:54:02	Deduplication: Infile File="D:\filter\sample\AlertMessageOne.png", duplicated file="D:\filter\sample\AlertMessageFive.png (2022-01-11-10-53-56)", size="2,593"
13	info	2022/01/11 10:54:02	Deduplication: Infile File="D:\filter\sample\AlertMessageFour.png", duplicated file="D:\filter\sample\AlertMessageTwo.png (2022-01-11-10-53-56)", size="2,593"
14	info	2022/01/11 10:54:02	Deduplication: Infile File="D:\filter\sample\BackupSet_2015.docx", duplicated file="D:\filter\sample\AhsayCBS_version7_UserGuide.docx (2022-01-11-10-53-56)", size="14,902"

4.5.2 Restore Reports

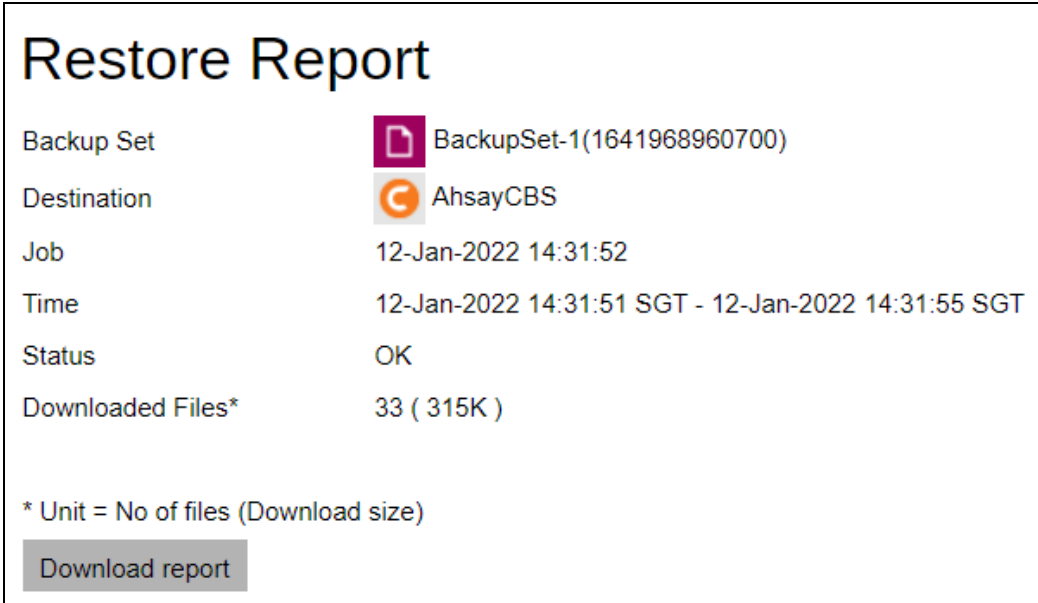
1. A list of restore reports for this AhsayCBS user can be found on the **Restore** tab. Click on the desired report to get more details on the report.





The screenshot shows the AhsayCBS interface with the 'Restore' tab selected. A sidebar on the left contains navigation options: User Profile, Backup Set, Settings, Report (highlighted), Statistics, and Effective Policy. The main content area is titled 'Restore Report for This User' and includes a 'View' dropdown menu set to 'Today'. Below this is a table with the following data:

Backup Set	Destination	Job	Status
 BackupSet-1(1641968960700)	 AhsayCBS	12-Jan-2022 14:31:52 SGT	OK

2. Click the **Download report** button at the bottom to download the complete report in PDF format. The restore report will be available around 15 to 20 minutes after a restore job has finished.



The screenshot shows the 'Restore Report' details page. It features a large heading 'Restore Report' and a list of key-value pairs for the report details. At the bottom, there is a 'Download report' button.


Backup Set	 BackupSet-1(1641968960700)
Destination	 AhsayCBS
Job	12-Jan-2022 14:31:52
Time	12-Jan-2022 14:31:51 SGT - 12-Jan-2022 14:31:55 SGT
Status	OK
Downloaded Files*	33 (315K)

* Unit = No of files (Download size)

[Download report](#)

3. A full version of the restore report appears. You can view the detailed backup set settings on this report.

- i. Normal Restore



Full Restore Report

Restore Job Summary

User	Backup Set	Restore Job	Restore Destination	Job Status	IP Address	Restored Files *
Win0365	BackupSet-1 (1641968960700)	2022-01-12-14-31-52	AhsayCBS	OK	172.16.99.207	0 (315K)

* No. of files (size)


Restore Logs

No.	Type	Timestamp	Log
1	start	01/12/2022 14:31:52	Start [AhsayOBM v9.0.3.12]
2	info	01/12/2022 14:31:54	Creating new directory... "C:\restored\C_"
3	info	01/12/2022 14:31:54	Creating new directory... "C:\restored\C_Users"
4	info	01/12/2022 14:31:54	Creating new directory... "C:\restored\C_Users\user"
5	info	01/12/2022 14:31:54	Creating new directory... "C:\restored\C_Users\user\Documents"
6	info	01/12/2022 14:31:54	Creating new directory... "C:\restored\C_Users\user\Documents\backup sample files"
7	info	01/12/2022 14:31:54	Creating new directory... "C:\restored\C_Users\user\Documents\backup sample files\filtersamples"

Restore Files

No.	File Name	Size	Last Modified	Downloaded Time	Time taken (min:sec)

- ii. Run Direct Restore without Auto Migration.



Full Restore Report

Restore Job Summary

User	Backup Set	Restore Job	Restore Destination	Job Status	IP Address	Restored Files *
user5	BackupSet-3 (1642562181224)	2022-01-19-11-27-04	AhsayCBS	OK	10.3.121.17	0 (0)

* No. of files (size)


Restore Logs

No.	Type	Timestamp	Log
1	start	01/19/2022 11:27:04	Start [AhsayOBM v9.1.0.0]
2	info	01/19/2022 11:27:06	VMware ESXi 6.0.0 build-5050593810.121.8.29-443SSH22
3	info	01/19/2022 11:27:26	New Virtual Machine UUID will be generate to "New Virtual Machine".
4	info	01/19/2022 11:27:48	Preparing for Run Direct...
5	info	01/19/2022 11:27:49	Mount datastore "cbs-RunDirect (10.3.121.17:cbsRunDirect)"...
6	info	01/19/2022 11:27:50	Adding virtual machine "New Virtual Machine" to the inventory...
7	info	01/19/2022 11:27:59	Taking snapshot "_snapshot_for_publish_" of virtual machine "New Virtual Machine"...
8	info	01/19/2022 11:28:06	Please do not Edit, Remove or Revert any existing snapshot before migration is completed.

Restore Files

No.	File Name	Size	Last Modified	Downloaded Time	Time taken (min:sec)

iii. Run Direct with Auto Migration


AhsayCBS

Full Restore Report

Restore Job Summary

User	Backup Set	Restore Job	Restore Destination	Job Status	IP Address	Restored Files *
user5	BackupSet-3 (164256218 1224)	2022-01-19-11-35-23	AhsayCBS	OK	10.3.121.17	0 (0)

* No. of files (size)

Restore Logs

No.	Type	Timestamp	Log
1	start	01/19/2022 11:35:23	Start [AhsayOBM v9.1.0.0]
2	info	01/19/2022 11:35:24	VMware ESXi 6.0.0 build-5050993810.121.8.29-443SSH22)
3	info	01/19/2022 11:37:39	New Virtual Machine UUID will be generate to "New Virtual Machine"
4	info	01/19/2022 11:38:01	Preparing for Run Direct...
5	info	01/19/2022 11:38:02	Mount datastore "cbs-RunDirect (10.3.121.17:cbsRunDirect)"...
6	info	01/19/2022 11:38:02	Adding virtual machine "New Virtual Machine" to the inventory...
7	info	01/19/2022 11:38:12	Taking snapshot "__snapshot_for_publish_" of virtual machine "New Virtual Machine"...
8	info	01/19/2022 11:38:18	Please do not Edit, Remove or Revert any existing snapshot before migration is completed.
9	info	01/19/2022 11:38:31	Start manual migration...
10	info	01/19/2022 11:38:32	Loading information...
11	info	01/19/2022 11:38:37	Taking snapshot "__snapshot_for_migrate_" of virtual machine "New Virtual Machine"...
12	info	01/19/2022 11:38:45	Migrating [vexi02_datastore1] New Virtual Machine/Centos-000001-delta.vmdk
13	info	01/19/2022 11:38:46	Migrating [vexi02_datastore1] New Virtual Machine/Centos-000001.vmdk
14	info	01/19/2022 11:38:47	Migrating [vexi02_datastore1] New Virtual Machine/Centos-Flat.vmdk
15	info	01/19/2022 11:43:44	Migrating [vexi02_datastore1] New Virtual Machine/Centos.vmdk
16	info	01/19/2022 11:43:45	Loading information...
17	info	01/19/2022 11:43:48	Removing virtual machine "New Virtual Machine" from the inventory...
18	info	01/19/2022 11:43:48	Migrating [vexi02_datastore1] New Virtual Machine/Centos.nvram
19	info	01/19/2022 11:43:53	Migrating [vexi02_datastore1] New Virtual Machine/Centos.vmsd
20	info	01/19/2022 11:43:54	Migrating [vexi02_datastore1] New Virtual Machine/Centos.vmx
21	info	01/19/2022 11:43:55	Migrating [vexi02_datastore1] New Virtual Machine/Centos-000002-delta.vmdk
22	info	01/19/2022 11:43:55	Migrating [vexi02_datastore1] New Virtual Machine/Centos-000002.vmdk
23	info	01/19/2022 11:43:57	Migrating [vexi02_datastore1] New Virtual Machine/Centos-Snapshot1.vmsn
24	info	01/19/2022 11:43:57	Migrating [vexi02_datastore1] New Virtual Machine/Centos-Snapshot2.vmsn
25	info	01/19/2022 11:43:58	Adding virtual machine "New Virtual Machine" to the inventory...
26	info	01/19/2022 11:44:07	Removing snapshot "__snapshot_for_migrate_" from virtual machine "New Virtual Machine"...
27	info	01/19/2022 11:44:11	Removing snapshot "__snapshot_for_publish_" from virtual machine "New Virtual Machine"...
28	info	01/19/2022 11:44:12	Unmount datastore "cbs-RunDirect"...

Restore Files

No.	File Name	Size	Last Modified	Downloaded Time	Time taken (min:sec)

NOTE

OpenDirect restore of file backup sets or granular restore of files from VMware and Hyper-V backup sets performed using Windows File Explorer will not generate any restore reports on AhsayCBS. Restore reports are only available when the restore is performed directly through AhsayOBM /AhsayACB/ AhsayOBR or on agentless Microsoft 365 and Cloud File backups.

4.6 Statistics

You can generate a graph of storage statistics for the user by modifying a few factors such as the backup destination, backup set and the period of the backup.

The statistics shows the storage capacity of different backup sets on different dates. Only restorable files in the data and retention area for each backup set are included in the calculation of storage statistics.

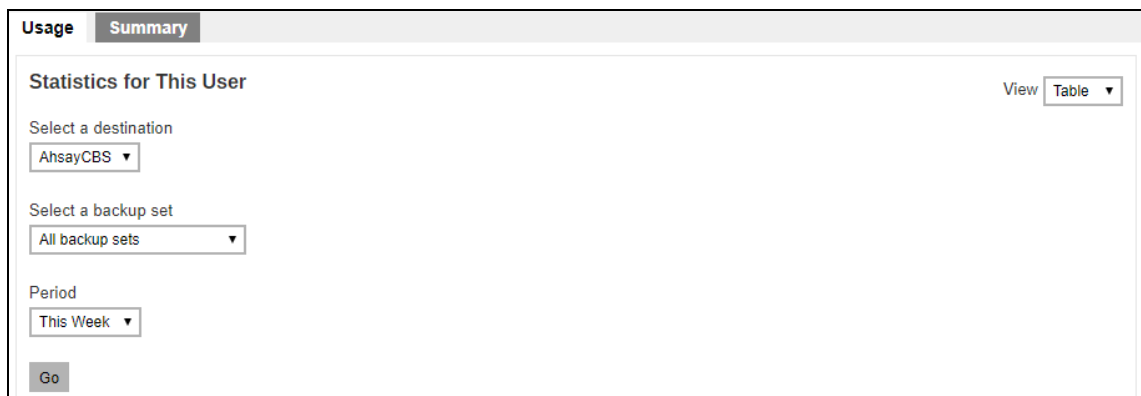
Storage statistics of a backup set are updated every time the following functions are run:

- Backup job
- Data Integrity Check (DIC)
- Periodic Data Integrity Check (PDIC)
- Space Freeing Up
- Delete Backup Data

Usage

The following options are configurable for generating statistics in your desirable view.

- **Select a destination** – select the backup destination of your choice
- **Select a backup set** – you can choose a specific backup set or all backup sets
- **Period** – select the period of time during which backups were performed
- **View** – you can choose a view, graph or table



The screenshot shows a web interface titled "Usage Summary". It features a section "Statistics for This User" with a "View" dropdown menu set to "Table". Below this, there are three dropdown menus: "Select a destination" (set to "AhsayCBS"), "Select a backup set" (set to "All backup sets"), and "Period" (set to "This Week"). A "Go" button is located at the bottom left of the form.

Graph view

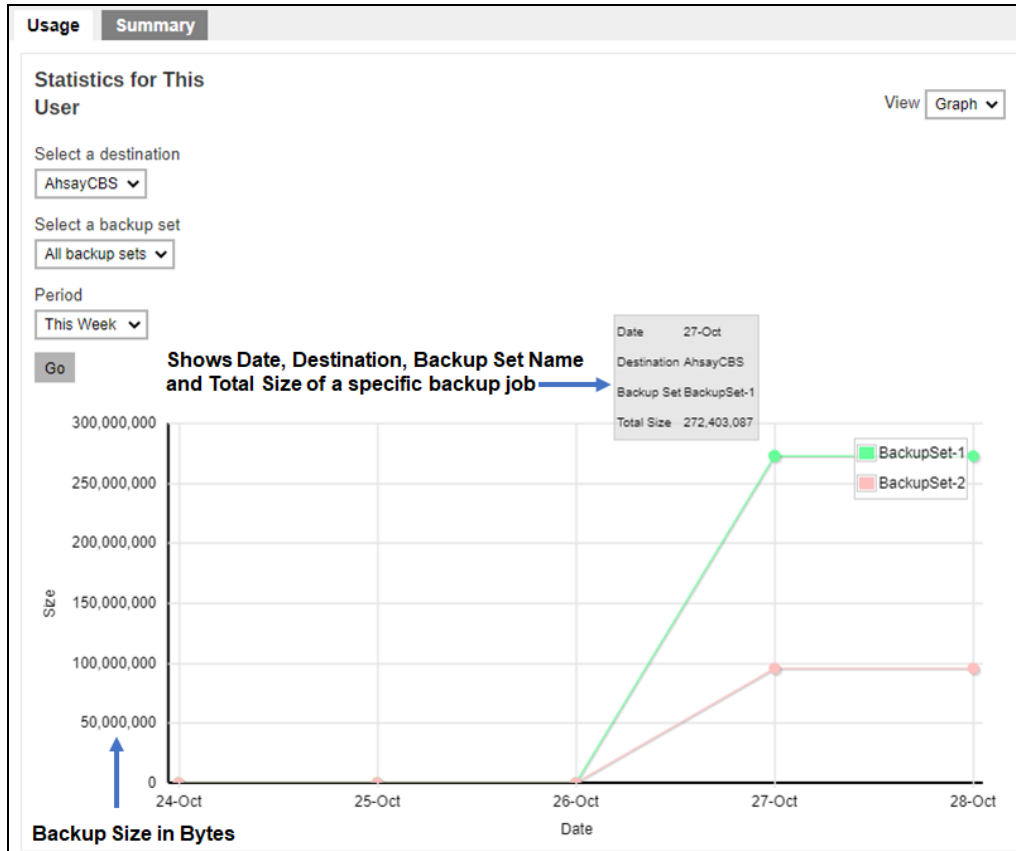


Table view

Usage **Summary**

Statistics for This User View **Table** ▼

Select a destination
AhsayCBS ▼

Select a backup set
All backup sets ▼

Period
This Week ▼

Go

Date	Backup Set	Total Size
2021-10-26	Total	0
	BackupSet-1(1635325749908)	0
	BackupSet-2(1635325859312)	0
2021-10-27	Total	350.72M
	BackupSet-1(1635325749908)	259.78M
	BackupSet-2(1635325859312)	90.94M
2021-10-28	Total	350.72M
	BackupSet-1(1635325749908)	259.78M
	BackupSet-2(1635325859312)	90.94M

Summary

Usage		Summary					
Summary for This User							
* Unit (Storage): Compressed Size / Uncompressed Size [Ratio] [Total No. of Files]							
** Unit (Data Transfer): Compressed Size [Total No. of Files]							
*** Unit (Deduplication): Uncompressed Dedupe Size / Uncompressed Original Size [Deduplication Ratio]							
(^) Backup Set completely migrated from v6							
Backup Set	Destination	Data Area*	Recycle Bin	Total Upload**	Total Restore**	Dedupe Saving***	
Backup Set 1	AhsayCBS	78.64 K / 204.02 K [62%] [34]	24.40 K [2]	78.64 K [34]	59.77 K [5]	323.31 K / 527.33 K [61.3%]	
Backup Set 2	Local-1	87.36 K / 143.75 K [40%] [33]	0 [0]	87.36 K [33]	0 [0]	0	
Backup Set 3	AhsayCBS	0 / 0 [0%] [0]	0 [0]	0 [0]	0 [0]	0	

There are 5 columns showing the following information of each backup set.

Data Area

Data Area*
78.64 K / 204.02 K [62%] [34]
87.36 K / 143.75 K [40%] [33]
0 / 0 [0%] [0]

Format:

[Compressed Size] / [Uncompressed Size] [Compression Ratio in %] [Number of files]

Example: 78.64 K / 204.02 K [62%] [34]

The Data Area also include files that are in the Retention Area. The data interpreted as the backup set has 34 files in the data area; the files compressed, and uncompressed sizes are 78.64 K and 204.02 K respectively; the compression ratio is 62%.

Recycle Bin

Recycle Bin
24.40 K [2]
0 [0]
0 [0]

Format:

[Compressed Size] [Total number of files]

Example: 24.40 K [2]

The data interpreted as the backup set has 2 files in the Recycle Bin with a compress size of 24.40 K.

Total Upload

Total Upload**
78.64 K [34]
87.36 K [33]
0 [0]

Format:

[Compressed Size] [Total number of files]

Example: 78.64 K [34]

There is a total of 34 files with a size of 78.64 K uploaded for this backup set.

The Total Upload is a lifetime counter, computed by adding up all the New Files, New Directories, New Links, Uploaded Files, Attributed Changed Files, Deleted Files, Deleted Directories, Deleted Links and Moved Files.

Total Restore

Total Restore**
59.77 K [5]
0 [0]
0 [0]

Format:

[Compressed Size] [Total number of files]

Example: 59.77 K [5]

There is a total of 5 files with a size of 59.77 K restored from this backup set.

The Total Restore is a lifetime counter, computed by adding up all the New Files, New Directories, New Links, Uploaded Files, Attributed Changed Files, Deleted Files, Deleted Directories, Deleted Links and Moved Files.

Dedupe Saving

Dedupe Saving***
323.31 K / 527.33 K [61.3%]
0
0

Format:

[Dedupe Size] / [Original Size] [Deduplication Ratio in %]

Example: 323.31 K / 527.33 K [61.3%]

The files dedupe size and original size are 59.96M and 1.02G respectively; the dedupe saving is only 5.7%.

4.7 Effective Policy

NOTE

Effective Policy page may be hidden depending on the configuration your backup service provider made.

There are six (6) tabs containing different groups of policy, and they are described below.

User Settings Tab

You can see the effective policy on user settings for this user on the User Settings tab.

User Profile	User Settings	Backup Set Settings	GUI Settings	Default Values	Preempted Values	Preempted Backup Sets
Backup Set	User Settings Related Policies					
Settings	Detail	Value	User Group	Policy		
Report	Quota > Quota limits calculation method	Compressed Size	All Users	Default settings		
Statistics	User Quota > Enable	Yes, User Quota Settings: Enabled = true, Mode = Default	All Users	Default settings		
Effective Policy	User Quota > Value	Destination Quota Settings: DestinationKey=OBS, Enable=true, Quota=52428800, DestinationName=AhsayCBS	All Users	Default settings		
	Invalid login attempt limit (password only) > Maximum number of invalid login attempts allowed within specified period	3 times within 5 mins	All Users	Default settings		
	Invalid login attempt limit (password only) > Blocking period for IP address and user that exceed the maximum allowed invalid login attempts	10 Minutes	All Users	Default settings		
	Email Reports > Backup Report	Yes	All Users	Default settings		
	Email Reports > Restore Report	Yes	All Users	Default settings		

Backup Set Settings Tab

You can see the effective policy on backup set settings for this user on the Backup Set Settings tab.

User Profile	User Settings	Backup Set Settings	GUI Settings	Default Values	Preempted Values	Preempted Backup Sets
Backup Set	Backup Set Settings Related Policies					
Settings	Detail	Value	User Group	Policy		
Report	Destinations Visible to Users > Predefined Destination	Wasabi-1 (Wasabi)	All Users	Default settings		
Statistics	Destinations Visible to Users > Standard Destination	Local / Mapped Drive / Network Drive / Removable Drive, Enable=Yes	All Users	Default settings		
Effective Policy	Destinations Visible to Users > Standard Destination	AhsayCBS, Enable=Yes	All Users	Default settings		
	Destinations Visible to Users > Standard Destination	Google Cloud Storage, Enable=No	All Users	Default settings		
	Destinations Visible to Users > Standard Destination	Amazon S3, Enable=No	All Users	Default settings		
	Destinations Visible to Users > Standard Destination	SFTP, Enable=No	All Users	Default settings		
	Destinations Visible to Users > Standard Destination	FTP, Enable=No	All Users	Default settings		
	Destinations Visible to Users > Standard Destination	CTYun, Enable=No	All Users	Default settings		

GUI Settings Tab

You can see the effective policy on AhsayOBM or AhsayACB GUI settings for this user on the GUI Settings tab.

User Profile	User Settings	Backup Set Settings	GUI Settings	Default Values	Preempted Values	Preempted Backup Sets																																				
Backup Set	GUI Settings Related Policies <table border="1"> <thead> <tr> <th>Detail</th> <th>Value</th> <th>User Group</th> <th>Policy</th> </tr> </thead> <tbody> <tr> <td>Backup Sets > Add and Remove Backup Set (ONLY applicable to v7.3 - v7.9 client agent)</td> <td>View=Yes</td> <td>All Users</td> <td>Default settings</td> </tr> <tr> <td>Backup Sets > General Tab</td> <td>View=Yes</td> <td>All Users</td> <td>Default settings</td> </tr> <tr> <td>Backup Sets > General Settings - Name</td> <td>View=Yes, Edit=Yes</td> <td>All Users</td> <td>Default settings</td> </tr> <tr> <td>Backup Sets > General Settings - IBM Domino</td> <td>View=Yes, Edit=Yes</td> <td>All Users</td> <td>Default settings</td> </tr> <tr> <td>Backup Sets > General Settings - IBM Notes</td> <td>View=Yes, Edit=Yes</td> <td>All Users</td> <td>Default settings</td> </tr> <tr> <td>Backup Sets > General Settings - MS Exchange Server</td> <td>View=Yes, Edit=Yes</td> <td>All Users</td> <td>Default settings</td> </tr> <tr> <td>Backup Sets > General Settings - MS HyperV</td> <td>View=Yes, Edit=Yes</td> <td>All Users</td> <td>Default settings</td> </tr> <tr> <td>Backup Sets > General Settings - MSSQL Server</td> <td>View=Yes, Edit=Yes</td> <td>All Users</td> <td>Default settings</td> </tr> </tbody> </table>						Detail	Value	User Group	Policy	Backup Sets > Add and Remove Backup Set (ONLY applicable to v7.3 - v7.9 client agent)	View=Yes	All Users	Default settings	Backup Sets > General Tab	View=Yes	All Users	Default settings	Backup Sets > General Settings - Name	View=Yes, Edit=Yes	All Users	Default settings	Backup Sets > General Settings - IBM Domino	View=Yes, Edit=Yes	All Users	Default settings	Backup Sets > General Settings - IBM Notes	View=Yes, Edit=Yes	All Users	Default settings	Backup Sets > General Settings - MS Exchange Server	View=Yes, Edit=Yes	All Users	Default settings	Backup Sets > General Settings - MS HyperV	View=Yes, Edit=Yes	All Users	Default settings	Backup Sets > General Settings - MSSQL Server	View=Yes, Edit=Yes	All Users	Default settings
Detail							Value	User Group	Policy																																	
Backup Sets > Add and Remove Backup Set (ONLY applicable to v7.3 - v7.9 client agent)							View=Yes	All Users	Default settings																																	
Backup Sets > General Tab							View=Yes	All Users	Default settings																																	
Backup Sets > General Settings - Name							View=Yes, Edit=Yes	All Users	Default settings																																	
Backup Sets > General Settings - IBM Domino							View=Yes, Edit=Yes	All Users	Default settings																																	
Backup Sets > General Settings - IBM Notes							View=Yes, Edit=Yes	All Users	Default settings																																	
Backup Sets > General Settings - MS Exchange Server							View=Yes, Edit=Yes	All Users	Default settings																																	
Backup Sets > General Settings - MS HyperV							View=Yes, Edit=Yes	All Users	Default settings																																	
Backup Sets > General Settings - MSSQL Server							View=Yes, Edit=Yes	All Users	Default settings																																	
Settings																																										
Report																																										
Statistics																																										
Effective Policy																																										

Default Values Tab

You can see the effective policy on default values for this user on the Default Values tab.

User Profile	User Settings	Backup Set Settings	GUI Settings	Default Values	Preempted Values	Preempted Backup Sets																											
Backup Set	Default Values Related Policies <table border="1"> <thead> <tr> <th>Detail</th> <th>Value</th> <th>User Group</th> </tr> </thead> <tbody> <tr> <td>General > Name</td> <td>Applied Module=File Backup, Name=default-backup-set-name</td> <td>All Users</td> </tr> <tr> <td>General > Name</td> <td>Applied Module=Cloud File Backup, Name=default-backup-set-name</td> <td>All Users</td> </tr> <tr> <td>General > Name</td> <td>Applied Module=IBM Lotus Domino Backup, Name=default-backup-set-name</td> <td>All Users</td> </tr> <tr> <td>General > Name</td> <td>Applied Module=IBM Lotus Notes Backup, Name=default-backup-set-name</td> <td>All Users</td> </tr> <tr> <td>General > Name</td> <td>Applied Module=MS Exchange Server Backup, Name=default-backup-set-name</td> <td>All Users</td> </tr> <tr> <td>General > Name</td> <td>Applied Module=MS Exchange Mail Level Backup, Name=default-backup-set-name</td> <td>All Users</td> </tr> <tr> <td>General > Name</td> <td>Applied Module=MS SQL Server Backup, Name=default-backup-set-name</td> <td>All Users</td> </tr> <tr> <td>General > Name</td> <td>Applied Module=MS Hyper-V Backup, Name=default-backup-set-name</td> <td>All Users</td> </tr> </tbody> </table>						Detail	Value	User Group	General > Name	Applied Module=File Backup, Name=default-backup-set-name	All Users	General > Name	Applied Module=Cloud File Backup, Name=default-backup-set-name	All Users	General > Name	Applied Module=IBM Lotus Domino Backup, Name=default-backup-set-name	All Users	General > Name	Applied Module=IBM Lotus Notes Backup, Name=default-backup-set-name	All Users	General > Name	Applied Module=MS Exchange Server Backup, Name=default-backup-set-name	All Users	General > Name	Applied Module=MS Exchange Mail Level Backup, Name=default-backup-set-name	All Users	General > Name	Applied Module=MS SQL Server Backup, Name=default-backup-set-name	All Users	General > Name	Applied Module=MS Hyper-V Backup, Name=default-backup-set-name	All Users
Detail							Value	User Group																									
General > Name							Applied Module=File Backup, Name=default-backup-set-name	All Users																									
General > Name							Applied Module=Cloud File Backup, Name=default-backup-set-name	All Users																									
General > Name							Applied Module=IBM Lotus Domino Backup, Name=default-backup-set-name	All Users																									
General > Name							Applied Module=IBM Lotus Notes Backup, Name=default-backup-set-name	All Users																									
General > Name							Applied Module=MS Exchange Server Backup, Name=default-backup-set-name	All Users																									
General > Name							Applied Module=MS Exchange Mail Level Backup, Name=default-backup-set-name	All Users																									
General > Name							Applied Module=MS SQL Server Backup, Name=default-backup-set-name	All Users																									
General > Name							Applied Module=MS Hyper-V Backup, Name=default-backup-set-name	All Users																									
Settings																																	
Report																																	
Statistics																																	
Effective Policy																																	

Preempted Values Tab

You can see the effective policy on preempted values for this user on the Preempted Values tab.

The screenshot shows a web interface with a left sidebar containing menu items: User Profile, Backup Set, Settings, Report, Statistics, and Effective Policy (which is highlighted). The main content area has a top navigation bar with tabs: User Settings, Backup Set Settings, GUI Settings, Default Values, Preempted Values (selected), and Preempted Backup Sets. Below the tabs is a box titled "Preempted Values Related Policies" containing the text "No policy defined". A dark footer bar at the bottom right contains an "X" and a "?" icon.

Preempted Backup Sets Tab

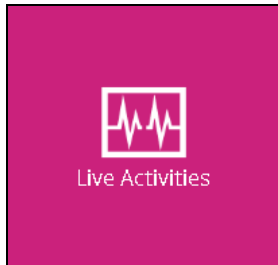
You can see the effective policy on preempted backup sets for this user on the Preempted Backup Sets tab.

The screenshot shows a web interface similar to the one above. The left sidebar is the same. The main content area has a top navigation bar with tabs: User Settings, Backup Set Settings, GUI Settings, Default Values, Preempted Values, and Preempted Backup Sets (selected). Below the tabs is a box titled "Preempted Backup Sets Related Policies" containing the text "No policy defined". A dark footer bar at the bottom right contains an "X" and a "?" icon.

5 Monitoring Live Activities

5.1 Managing Live Activities

1. Log in to AhsayCBS user web console according to the instruction provided in section [Logging on to AhsayCBS User Web Console](#).
2. To manage your backup and restore live activities, simply click the Live Activities icon from your AhsayCBS environment.



You can perform the following operations on your own user account:

- View the status of an agent based and agentless backup job that is currently running. Once a backup job is completed, the entry will be immediately removed from the Live Activities.
- View the status of an agent based and agentless restore job that is currently running. Once a restore job is completed, the entry will be immediately removed from the Live Activities.

NOTE

If there are any backup and restore jobs which are unexpectedly terminated or crashed the job status should automatically clear after 72 hours.

5.2 Backup Status

The **Backup Status** tab allows you to monitor the live activities of backup jobs running in both agent-based (AhsayOBM/ AhsayACB) and agentless (AhsayCBS User Web Console) type.

Available Restore Jobs Can Be Monitored by Live Activities			
Backup Type	AhsayOBM	AhsayACB	Ahsay Mobile
File Backup	✓	✓	NA
Cloud File Backup	✓	✓	NA
IBM Lotus Domino Backup	✓	NA	NA
IBM Lotus Notes Backup	✓	✓	NA
MS Exchange Server Backup	✓	NA	NA
MS Exchange Mail Level Backup	✓	NA	NA
MS SQL Server Backup	✓	NA	NA
MS Windows System Backup	✓	✓	NA
MS Windows System State Backup	✓	NA	NA
MS Hyper-V Backup	✓	NA	NA
MySQL Backup	✓	NA	NA
Microsoft 365 Backup	✓	✓	NA
Oracle Database Server	✓	NA	NA
ShadowProtect System Backup	✓	NA	NA
VMware Backup	✓	NA	NA
Synology NAS Backup	✓	NA	NA
QNAP NAS Backup	✓	NA	NA
MariaDB Backup	✓	NA	NA

The following shows the backup status of a live backup activity

The screenshot displays the AhsayCBS Backup Status interface. It features a header with the AhsayCBS logo and two tabs: 'Backup Status' (selected) and 'Restore Status'. Below the tabs, there is a sub-header 'Backup Status' and a filter section with dropdown menus for 'Client Type', 'User', 'Registration Date', and 'User Group'. The main content is a table with columns: 'Login Name (Alias)', 'Owner', 'Backup Set', 'Destination', 'Progress', 'Estimated Time Left', 'Current File', and 'Transfer Rate'. The table shows one backup job for 'user1 ()' with a progress bar at 100% and an estimated time left of 0 seconds. The current file path is 'C:\Users\user1\Documents\installers' and the transfer rate is 0bit/s.

Login Name (Alias)	Owner	Backup Set	Destination	Progress	Estimated Time Left	Current File	Transfer Rate
user1 ()	--	BackupSet-2	AhsayCBS	100 %	0 sec	C:\Users\user1\Documents\installers	0bit/s

5.3 Restore Status

The **Restore Status** tab allows you to monitor the live activities of restore jobs running in both agent-based (AhsayOBM/ AhsayACB/ AhsayOBR) and agentless (AhsayCBS User Web Console) type.

Restore Type		Ahsay OBM	Ahsay ACB	Ahsay OBR	Ahsay Mobile
File	Normal Restore	✓	✓	✓	NA
	OpenDirect Restore	X	X	X	NA
Cloud File Backup		✓	✓	✓	NA
IBM Lotus Domino Backup		✓	NA	✓	NA
IBM Lotus Notes Backup		✓	✓	✓	NA
MS Exchange Server Backup		✓	NA	✓	NA
MS Exchange Mail Level Backup		✓	NA	✓	NA
MS SQL Server Backup		✓	NA	✓	NA
MS Windows System Backup		✓	✓	✓	NA
MS Windows System State Backup		✓	NA	✓	NA
MS Hyper-V	Normal Restore	✓	NA	✓	NA
	Run Direct Restore	✓	NA	✓	NA
	Granular Restore with AhsayOBM File Explorer	✓	NA	✓	NA
	Granular Restore with Windows File Explorer	X	NA	X	NA
MS SQL Server Backup		✓	NA	✓	NA
MySQL Backup		✓	NA	✓	NA
Microsoft 365 Backup		✓	✓	✓	NA
Oracle Database Server		✓	NA	✓	NA
ShadowProtect System Backup		✓	NA	✓	NA
VMware	Normal Restore	✓	NA	✓	NA

	Run Direct Restore	✓	NA	✓	NA
	Granular Restore with AhsayOBM File Explorer	✓	NA	✓	NA
	Granular Restore with Windows File Explorer	X	NA	X	NA
	Synology NAS Backup	✓	NA	NA	NA
	QNAP NAS Backup	✓	NA	NA	NA
	MariaDB Backup	✓	NA	✓	NA

The following shows the restore status of a live restore activity.

AhsayCBS

Backup Status Restore Status

All restore jobs that are currently running.

Restore Status

Login Name (Alias)	Owner	Backup Set	Destination	Progress	Estimated Time Left	Current File	Transfer Rate
user1 ()	--	BackupSet-2	AhsayCBS	100 %	0 sec		63Kibit/s

NOTE

OpenDirect restore of file backup sets or granular restore from VMware and Hyper-V backup sets performed using Windows File Explorer will not show up on the [Restore Status] tab in Live Activities. This only applies to the restore performed directly through AhsayOBM/AhsayACB/AhsayOBR or AhsayCBS User Web Console.

6 Managing Backup Set

Since all the steps in [creating a backup set](#), [running a backup job](#), and [restoring a backup](#) are generic, follow these links for detailed instructions for Microsoft 365 and Cloud File.

Agent-based

Cloud File

- [AhsayACB v9 User Guide – Cloud File Backup & Restore for Windows](#)
- [AhsayACB v9 User Guide – Cloud File Backup & Restore for Mac](#)
- [AhsayOBM v9 User Guide – Cloud File Backup & Restore for Windows](#)
- [AhsayOBM v9 User Guide – Cloud File Backup & Restore for Mac](#)

Microsoft 365

- [AhsayACB v9 User Guide - Microsoft 365 Backup & Restore for Windows](#)
- [AhsayACB v9 User Guide - Microsoft 365 Backup & Restore for Mac](#)
- [AhsayOBM v9 User Guide - Microsoft 365 Backup & Restore for Windows](#)
- [AhsayOBM v9 User Guide - Microsoft 365 Backup & Restore for Mac](#)

Agentless

Cloud File – [Cloud File Run on Server \(Agentless\) Backup and Restore Guide](#)

Microsoft 365 – [Microsoft 365 Run on Server \(Agentless\) Backup and Restore Guide](#)

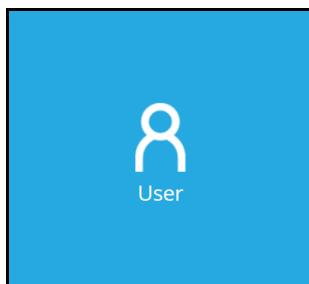
The links above will redirect you to the user guides of Microsoft 365 and Cloud File and from there it will discuss the two (2) options of [creating a backup set](#), [running a backup job](#), and [restoring a backup](#) which are through AhsayCBS User Web Console (Agentless) and AhsayACB/AhsayOBM (Agent-based).

6.1 Create Backup Set (Generic Steps)

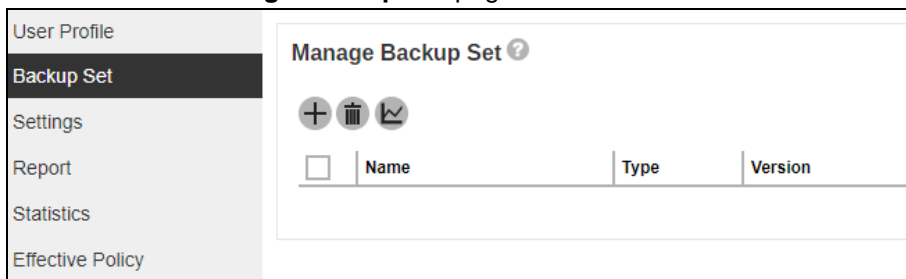
You can use your AhsayCBS user account to create backup sets and complete the remaining part of the process on the backup client for setting up the encryption type and/or encryption key. In some cases, you may need to create backup sets first before you install a backup client on the client machine.

To add a new backup set, do the following:

1. Log in to the AhsayCBS user web console according to the instruction provided in section [Logging in to AhsayCBS User Web Console](#).
2. Click **User** icon from AhsayCBS environment.



3. Click **+** on the **Manage Backup Set** page.



4. Enter the **Name** of the new backup set and select the backup set type from the **Backup set type** dropdown box. The choices for backup set types are:


- File Backup
- IBM Lotus Domino Backup
- IBM Lotus Notes Backup
- MS Exchange Server Backup
- MS Exchange Mail Level Backup
- MS SQL Server Backup
- MS Hyper-V Backup
- MS Windows System Backup
- MySQL Backup
- MariaDB Backup
- Oracle Database Server Backup
- ShadowProtect System Backup
- MS Windows System State Backup
- VMware Backup
- Cloud File Backup
- Microsoft 365 Backup

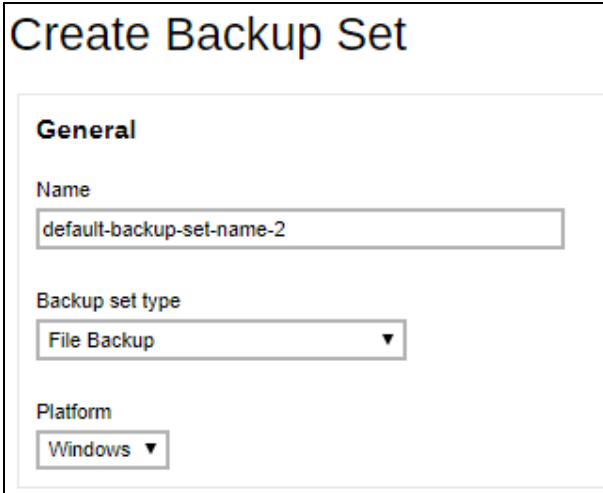
Also select the operating system used for the backup client from the **Platform** dropdown box. The choices for the platform are:

- Windows
- Linux
- Mac

The Linux platform option also applies to backup sets running under FreeBSD, QNAP and Synology.

Once the backup set creation process is completed on the backup client, the value for the platform will be updated accordingly. For QNAP the platform value is QTS, for Synology the platform value is DSM and for FreeBSD the platform value is FreeBSD.

In our example, the new File backup set running on Windows is called default-backup-set-name-2. Click  at the bottom right corner of the screen to continue.



Create Backup Set

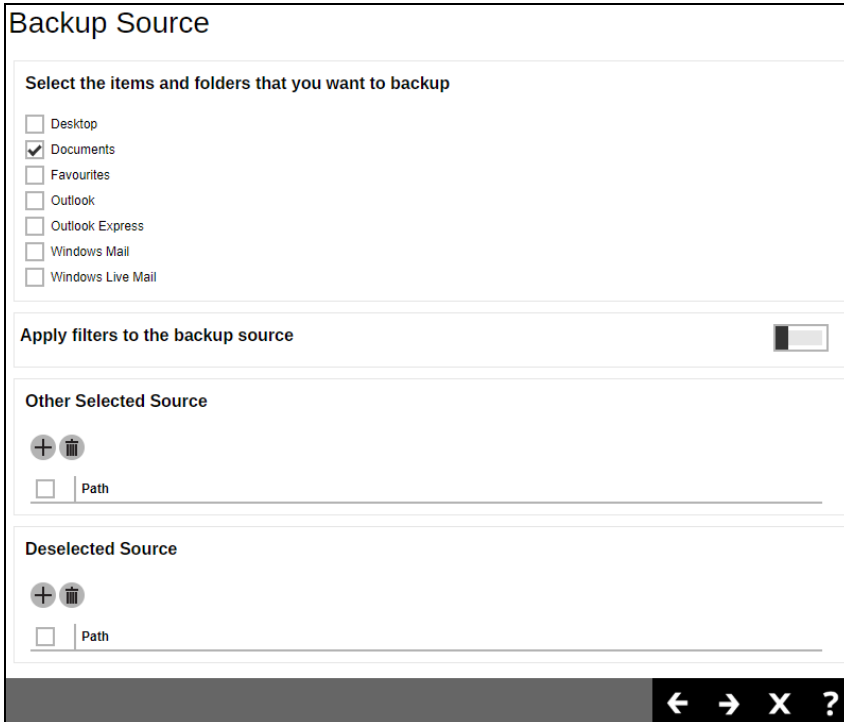
General

Name
default-backup-set-name-2

Backup set type
File Backup

Platform
Windows

5. Specify the backup source for the new backup set. The content of the Backup Source page differs depending on the backup set type you have chosen. Below is an example of creating a file backup set on Windows.



Backup Source

Select the items and folders that you want to backup

- Desktop
- Documents
- Favourites
- Outlook
- Outlook Express
- Windows Mail
- Windows Live Mail

Apply filters to the backup source

Other Selected Source

Path

Deselected Source

Path

Navigation icons: < > X ?

There are three (3) ways to select file(s) and/or folder(s) for back up:

- i. Select folder(s) to back up all files in the folder(s).

Select the items and folders that you want to backup

Desktop

Documents

Favourites

Outlook

Outlook Express

Windows Mail

Windows Live Mail

- ii. Use the filter to specify file(s) and/or folder(s) that will be included in the back up.

Turn on **Apply filters to the backup source** and click **+** to create a filter.

Apply filters to the backup source

+

Name

Enter the **Name** of the filter. Click **+** to specify the **Matching pattern**.

Filter

Name

Matching pattern

+

Pattern

s

Select from the options below. In this example, all files that starts with the letter “s” will be included in the backup job.

For each of the matched files/folders under top directory

Include them

Exclude them

Exclusion

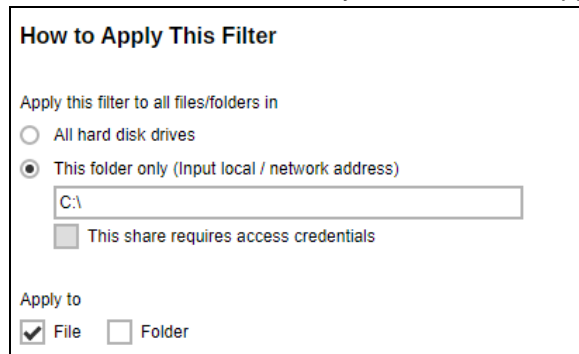
Exclude all unmatched files/folders

Match file/folder names by

Simple comparison **▼**

Regular expression (UNIX-style)

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, enter the local / network address that you would like to apply the filter to.



How to Apply This Filter

Apply this filter to all files/folders in


All hard disk drives

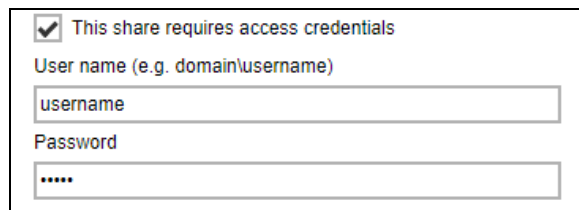
This folder only (Input local / network address)

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. Click  to add the filter.



This share requires access credentials

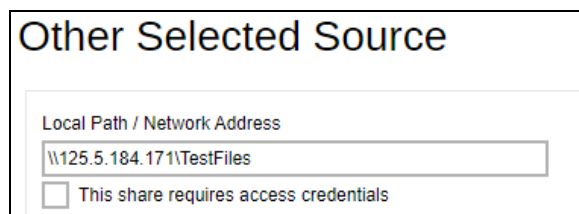
User name (e.g. domain\username)

Password

iii. Specify the source folder or network drive where the file(s) and folder(s) for back up are located. 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).

Click  under **Other Selected Source**. Enter the **Local Path / Network Address**.



Other Selected Source


Local Path / Network Address


This share requires access credentials


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  to add the selected source. You may add multiple source folder and/or network drive by doing the steps above until all the source folders and/or network drives are added.

You may also specify a source which would be excluded from the backup job by clicking the  under **Deselected Source** instead. Steps are the same as with Other Selected Source.



Click  at the bottom right corner of the screen to continue.

6. By default, the **Run scheduled backup for this backup set** option is enabled. There is already a backup schedule created which is scheduled to run daily at 8pm. This may be edited, or you may opt to create a new backup schedule by clicking  in the middle of the screen.

Schedule





Run scheduled backup for this backup set 

Manage schedule

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	Backup Schedule	Daily

Run scheduled backup on computers named

Enter the information of the new backup schedule you want to add.

Backup Schedule

Client version < 8.3.3.20 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name

Type

Start backup
 :

Stop

Run Retention Policy after backup

- **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.

Details

Name

Type

Start backup
 :

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.

Details

Name

Type

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

Start backup
 :

Stop

Run Retention Policy after backup

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

Details

Name

Type

Backup on the following day every month
 Last
 First

Start backup at
 :

Stop

Run Retention Policy after backup

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

Details

Name

Type

Backup on the following day once

Start backup at
 :

Stop

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

Run Retention Policy after backup

- 1 minute
- 2 minutes
- 3 minutes
- 4 minutes
- 5 minutes
- 6 minutes
- 10 minutes
- 12 minutes
- 15 minutes
- 20 minutes
- 30 minutes
- 1 hour
- 2 hours
- 3 hours
- 4 hours
- 6 hours
- 8 hours
- 12 hours

Start backup

Run Retention Policy after backup

- 1 minute
- 2 minutes
- 3 minutes
- 4 minutes
- 5 minutes
- 6 minutes
- 10 minutes
- 12 minutes
- 15 minutes
- 20 minutes
- 30 minutes
- 1 hour
- 2 hours
- 3 hours
- 4 hours
- 6 hours
- 8 hours
- 12 hours

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

Details	Details
Name Weekly-1	Name Weekly-2
Type Weekly	Type Weekly
Backup on these days of the week <input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat	Backup on these days of the week <input checked="" type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat
Start backup every 4 hours	Start backup at 21:00
<input checked="" type="checkbox"/> Run Retention Policy after backup	Stop until full backup completed <input checked="" type="checkbox"/> Run Retention Policy after backup

Periodic backup schedule runs every 4 hours Monday to Friday during business hours while the normal backup schedule runs at 21:00 or 9:00 PM on Saturday and Sunday during 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.

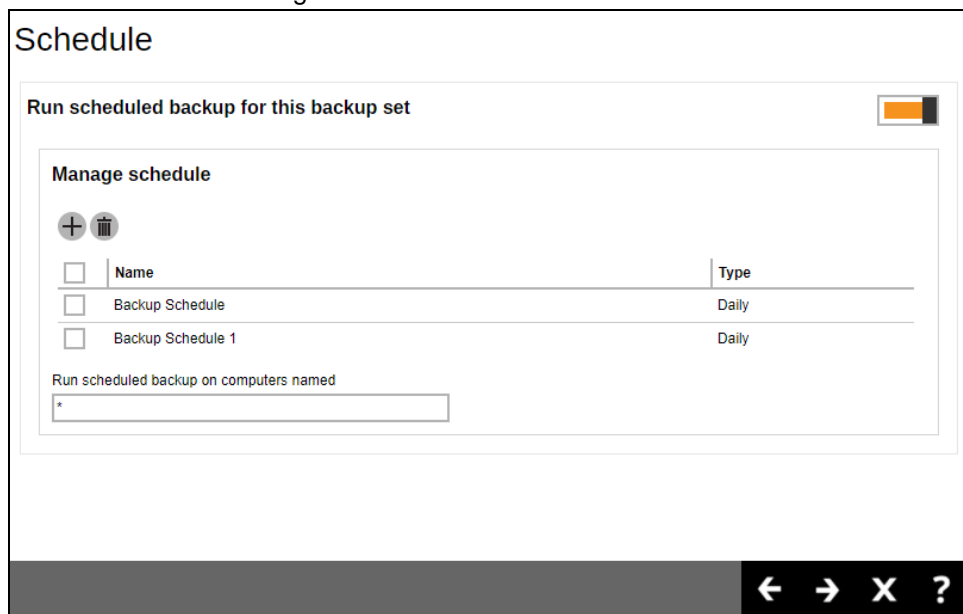
As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time

- ⦿ **Run Retention Policy after backup** – if enabled, the AhsayOBM 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.


Click  at the bottom right corner of the screen to continue.

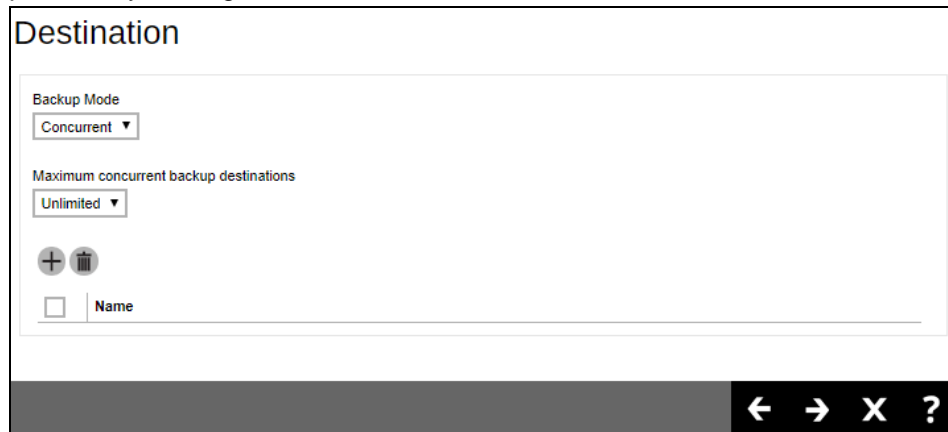
The new backup schedule, **Backup Schedule 1** in our example, can be seen under the **Manage schedule** list.

Click  at the bottom right corner of the screen to continue.



<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	Backup Schedule	Daily
<input type="checkbox"/>	Backup Schedule 1	Daily

7. Add a new backup destination for this backup set. By default, **Sequential** is selected. From the Backup Mode dropdown box, select either **Sequential** or **Concurrent**. In our example, we selected **Concurrent** as the backup set has more than one backup destination.
 - i. Add a Standard Destination or Predefined Destination set by your backup service provider by clicking the  in the left side of the screen.



<input type="checkbox"/>	Name
<input type="checkbox"/>	

- ii. Select your desired destination, it could be one or both displayed destinations. Tick the checkbox and click the plus sign to proceed.



<input type="checkbox"/>	Name
<input type="checkbox"/>	AhsayCBS
<input type="checkbox"/>	Wasabi-1

NOTE

You can choose the Standard Destination which is the AhsayCBS. However, if there are other backup destinations which are already configured by your backup service provider, you can still add them as one of your destinations.

- iii. The Standard and Predefined Destinations have been successfully added.

Destination

Backup Mode
Sequential ▾

<input type="checkbox"/>	Name
<input type="checkbox"/>	Wasabi-1
<input type="checkbox"/>	AhsayCBS

← → X ?

Click at the bottom right corner of the screen to continue.

- 8. Click the checkbox if you want to restore using OpenDirect.

Add New Backup Set

OpenDirect

Support of opening backup data directly without restoration.

When OpenDirect is enabled, to optimize restore performance both compression and encryption will be disabled for this backup set.

Once OpenDirect is enabled and the setting is saved, it cannot be disabled without re-creating the backup set.

← → X ?

9. Enter the Windows User Authentication information. This is needed for backup sets with backup schedule enabled and/or network shared drive selected as a temporary folder, backup source or backup destination. Enter the domain name and user name for AhsayOBM to access the network location.

For the user name, the local account or a Microsoft account may be used. The Microsoft account is supported for AhsayOBM installed on Microsoft Windows version 8, 8.1 and 10.

Some users prefer to use a pin to log in to Windows, this cannot be used for the Windows User Authentication. The pin can only be used for logging in to Windows and is not applicable for the Windows User Authentication. The password of the account must be provided instead of the pin to access files and/or folders in the network location.

Example using a local account.

Add New Backup Set

Windows User Authentication

Domain Name (e.g. mycompany.com) / Host Name

User name

Password

or

Example using a Microsoft account.


Add New Backup Set

Windows User Authentication

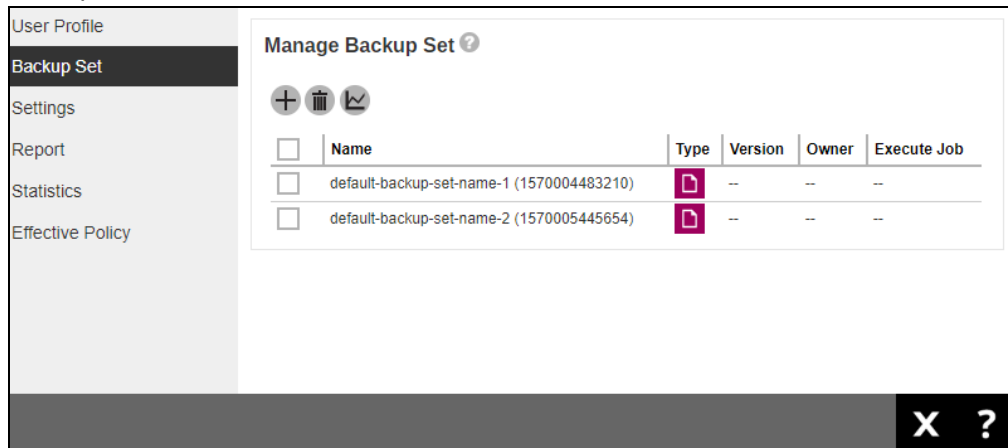
Domain Name (e.g. mycompany.com) / Host Name

User name

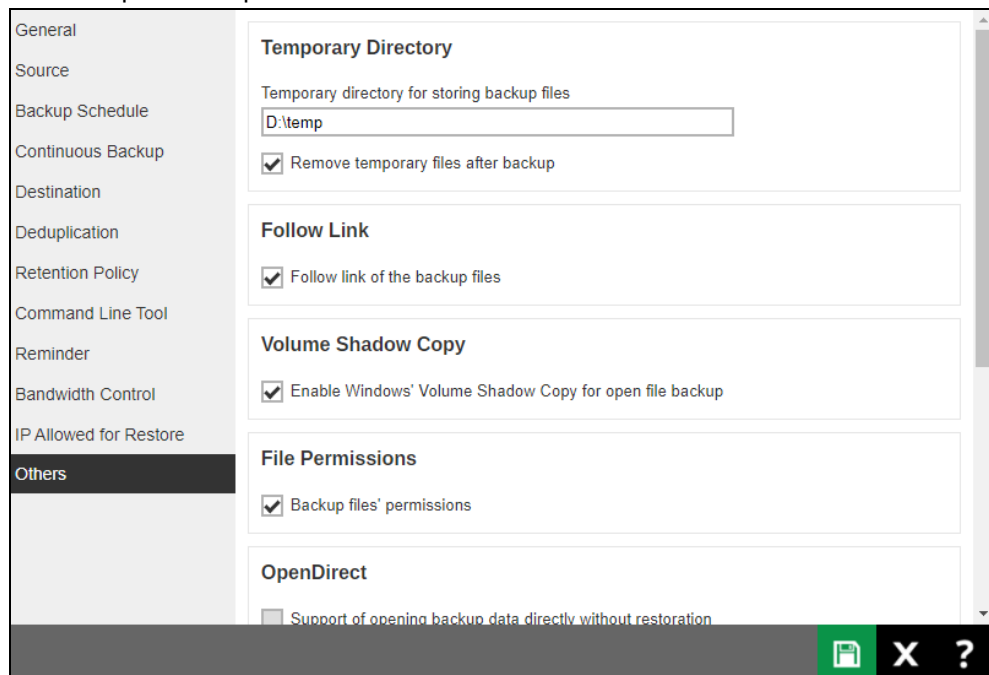
Password


Click  at the bottom right corner of the screen to continue.

10. A new backup set called **default-backup-set-name-2** is created and can be seen in the backup set list.

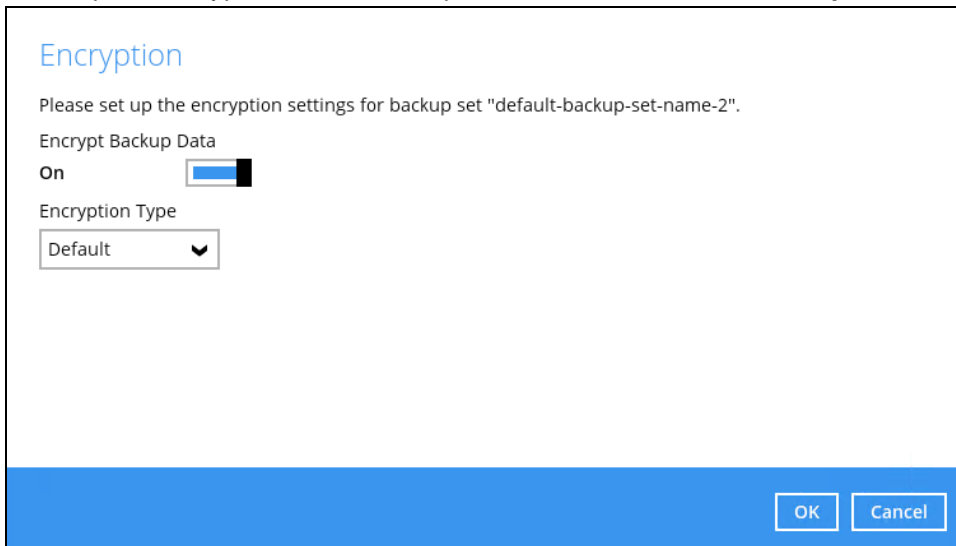


11. Click on the backup set and select **Others**, enter the path of the **Temporary Directory**. For example D:\temp

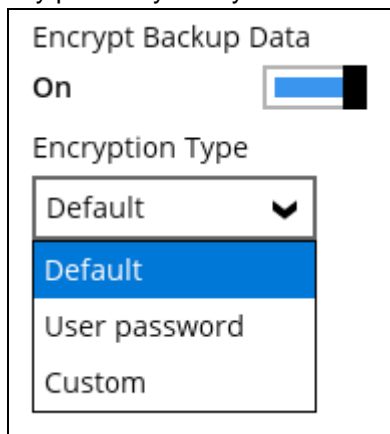


Click  at the bottom right corner of the screen to save.

12. Go to your backup client, in this case we are using AhsayOBM, to complete the setup of the backup set by configuring the encryption settings. Once logged in, you will be asked to set up the encryption for the backup set, in this case **default-backup-set-name-2**.



- By default, the **Encrypt Backup Data** option is enabled. The **Encryption Type** selected is **Default** which provides the most secure protection with an encryption key preset by the system.



Select from one of the 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 AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM 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

Please set up the encryption settings for backup set "default-backup-set-name-2".

Encrypt Backup Data
On

Encryption Type
Custom

Algorithm
AES

Encryption key
.....

Re-enter encryption key
.....

Method
 ECB CBC

Key length
 128-bit 256-bit

NOTE

For best practice on managing your encryption key, refer to the following Wiki article.
http://wiki.ahsay.com/doku.php?id=public:8015_faq:best_practices_for_managing_encryption_key.

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

Encryption

Please set up the encryption settings for backup set "default-backup-set-name-2".

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.

.....

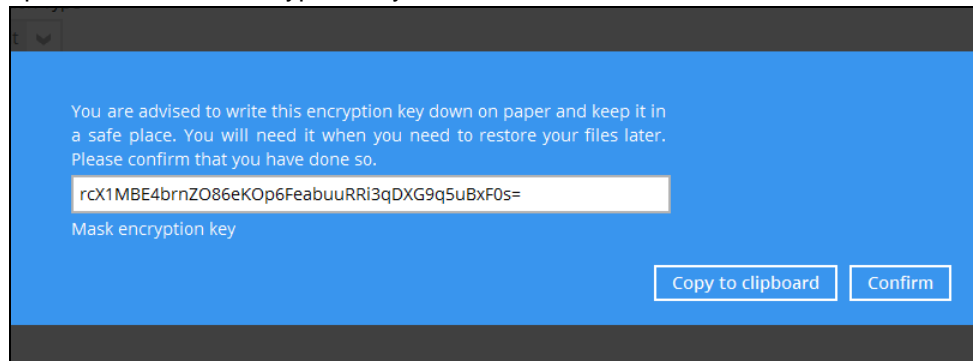
Unmask encryption key

Copy to clipboard Confirm

OK Cancel

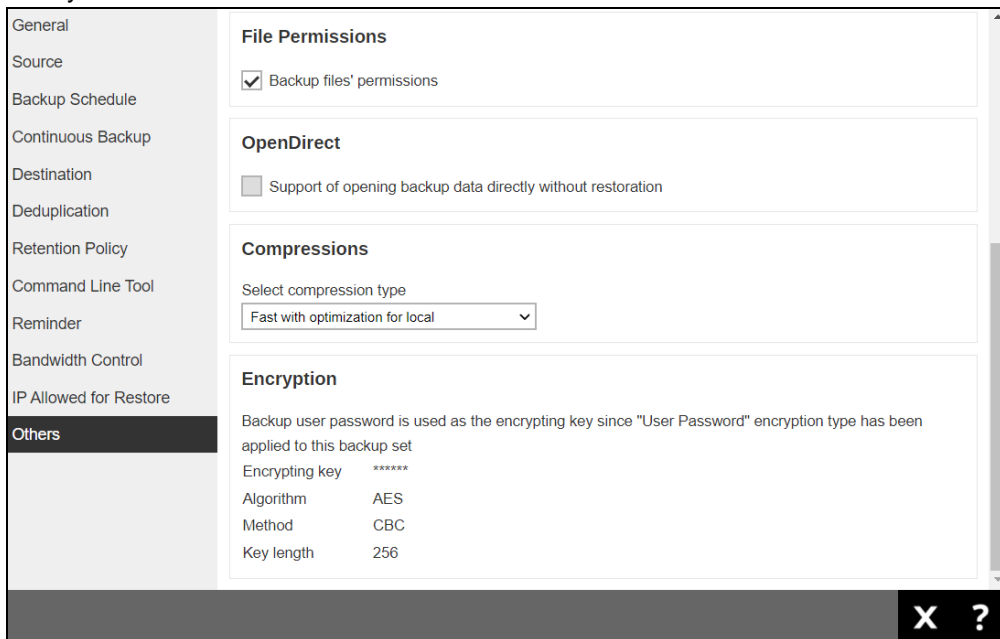
The pop-up window has the following three options to choose from:

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



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

This completes the setup of the backup set and can be seen under **Encryption** in AhsayCBS user web console.



6.2 Manage Backup Set

Click the backup set name you want to manage from the **Backup Set** tab. It is sub divided into the following tabs:

- [General](#)
- [Source](#)
- [Backup Schedule](#)
- [Continuous Backup](#)
- [Destination](#)
- [Deduplication](#)
- [Retention Policy](#)
- [Command Line Tool](#)
- [Reminder](#)
- [Bandwidth Control](#)
- [IP Allowed for Restore](#)
- [Others](#)

The screenshot displays the configuration page for a backup set. The left sidebar lists various tabs: General, Source, Backup Schedule, Continuous Backup, Destination, Deduplication, Retention Policy, Command Line Tool, Reminder, Bandwidth Control, IP Allowed for Restore, and Others. The 'General' tab is active, showing the following details:

- General**
 - ID: 1635325749908
 - Name: BackupSet-1
 - Owner: AM017L
 - Backup set type: File Backup
- Windows User Authentication**
 - Domain Name (e.g. mycompany.com) / Host Name: example.com
 - User name: username
 - Password: [Redacted]

Difference between AhsayOBM and AhsayACB Backup Set

Starting with AhsayCBS v9, the available tabs that can be accessed from an AhsayOBM and AhsayACB Backup Sets are different. This is to align the actual settings displayed in AhsayACB with AhsayCBS.

	AhsayOBM	AhsayACB
General	✓	✓
Source	✓	✓
Backup Schedule	✓	✓
Continuous Backup	✓	Found in Others
Destination	✓	✓
Deduplication	✓	✗
Retention Policy	✓	Found in Others

Command Line Tool	✓	✗
Reminder	✓	✓
Bandwidth Control	✓	✗
IP Allowed for Restore	✓	✓
Others	✓	✓

Here is a screenshot of AhsayOBM and AhsayACB to show the difference:

AhsayOBM

General	General
Source	ID 1659944625448
Backup Schedule	Name <input type="text" value="BackupSet-1"/>
Continuous Backup	Owner w2k16R2-std-mssql2k12
Destination	Platform <input type="text" value="Windows Server 2012 R2"/>
Deduplication	Backup set type <input type="text" value="File Backup"/>
Retention Policy	Windows User Authentication
Command Line Tool	
Reminder	
Bandwidth Control	
IP Allowed for Restore	
Others	

AhsayACB

General	General
Source	ID 1661500801043
Backup Schedule	Name <input type="text" value="BackupSet-1"/>
Destination	Owner -
Reminder	Platform <input type="text" value="Windows"/>
IP Allowed for Restore	Backup set type <input type="text" value="File Backup"/>
Others	

NOTE

Screenshots of Backup Sets that will be shown throughout the guide will be based on AhsayOBM.

6.2.1 General

The General page allows you to modify the backup set name and manage the Windows User Authentication information.

Backup Set Name

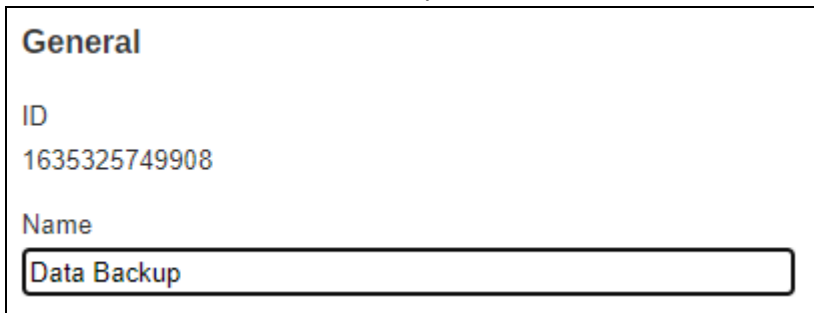
To modify the backup set name, follow the steps below:

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



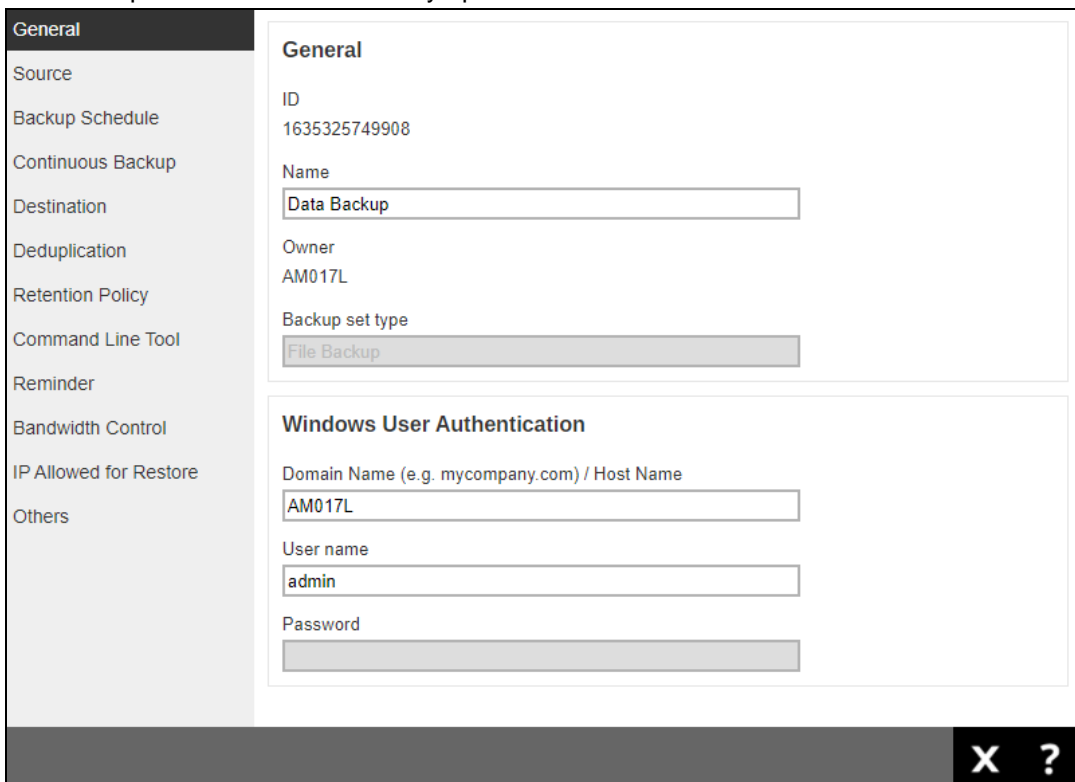
The screenshot shows a 'General' configuration window. The 'ID' field contains the value '1635325749908'. The 'Name' field contains the value 'BackupSet-1'.

2. In this example, we are going to change the backup set name to "Data Backup". Click the **Save** button to store the new backup set name.



The screenshot shows the same 'General' configuration window, but the 'Name' field now contains the value 'Data Backup'.

3. The backup set name is successfully updated.



The screenshot shows the full backup configuration interface. On the left is a sidebar with a 'General' tab selected. The main content area shows the 'General' configuration page with the following fields:

- General**
- ID: 1635325749908
- Name: Data Backup
- Owner: AM017L
- Backup set type: File Backup

Below the 'General' section is the 'Windows User Authentication' section with the following fields:

- Domain Name (e.g. mycompany.com) / Host Name: AM017L
- User name: admin
- Password: (empty)

At the bottom right of the interface, there are 'X' and '?' icons.

NOTE

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

Windows User Authentication

The Windows User Authentication information is needed for backup set with backup schedule and network shared drive selected as backup source.

- 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 AhsayOBM/AhsayACB 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).
- For the user name, the local account or a Microsoft account may be used. The Microsoft account is supported for AhsayOBM/AhsayACB installed on Microsoft Windows version 8, 8.1 and 10.

Some users prefer to use a pin to log in to Windows, this cannot be used for the Windows User Authentication. The pin can only be used for logging in to Windows and is not applicable for the Windows User Authentication. The password of the account must be provided instead of the pin to access files and/or folders in the network location

Example using a local account.

Windows User Authentication
Domain Name (e.g. mycompany.com) / Host Name
<input type="text" value="example.com"/>
User name
<input type="text" value="username"/>
Password
<input type="password"/>

or

Example using a Microsoft account.

Windows User Authentication
Domain Name (e.g. mycompany.com) / Host Name
<input type="text" value="example.com"/>
User name
<input type="text" value="username@outlook.com"/>
Password
<input type="password"/>

To modify the Windows User Authentication information, follow the steps below:

1. In the Domain Name and User name fields, enter a new name.

Windows User Authentication

Domain Name (e.g. mycompany.com) / Host Name

User name

2. In this example, we are going to change the domain name to “example.com” and user name to “Administrator”. Click the **Save** button to store the new domain and user names.

Windows User Authentication

Domain Name (e.g. mycompany.com) / Host Name

User name

3. The domain and user names are successfully updated.

General

Source

Backup Schedule

Continuous Backup

Destination

Deduplication

Retention Policy

Command Line Tool

Reminder

Bandwidth Control

IP Allowed for Restore

Others

General

ID
1635325749908

Name

Owner
AM017L

Backup set type

Windows User Authentication

Domain Name (e.g. mycompany.com) / Host Name

User name

Password

X ?

6.2.2 Source

The Source page allows you to select files and/or folders to back up.

The screenshot shows the 'Source' configuration page. On the left is a sidebar with the following menu items: General, Source (highlighted), Backup Schedule, Continuous Backup, Destination, Deduplication, Retention Policy, Command Line Tool, Reminder, Bandwidth Control, IP Allowed for Restore, and Others. The main content area is titled 'Select the items and folders that you want to backup' and contains a list of checkboxes: Desktop, Documents, Favourites, Outlook, Outlook Express, Windows Mail, and Windows Live Mail. A red box surrounds this list, with an arrow pointing to the text 'Quick Selection'. Below this is a section titled 'Apply filters to the backup source' with a 'Filter' toggle switch and a red arrow pointing to the text 'Filter'. The next section is 'Other Selected Source', which includes a table with columns for a checkbox and 'Path'. It contains three entries: 'C:\Users\user\Documents\backup sample files\Archive', 'C:\Users\user\Documents\backup sample files\Documents', and 'C:\Users\user\Documents\backup sample files\Excel'. A red box surrounds this table, with an arrow pointing to the text 'Other Source'. Below that is the 'Deselected Source' section, which is currently empty. At the bottom right of the window are 'X' and '?' icons.

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

Quick Selection – this allows you to back up files and/or folders in the selected backup source entirely.

Filter – this allows you to select or exclude files and/or folders from the backup job.

Other Source – this allows you to select files and/or folders individually to back up.

Option 1: Quick Selection

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

Select the items and folders that you want to backup

- Desktop
- Documents
- Favourites
- Outlook
- Outlook Express
- Windows Mail
- Windows Live Mail

If any of the following backup source is selected and the [Backup Schedule](#) is enabled, the Windows User Authentication credentials must be entered in AhsayOBM/AhsayACB to enable the backup job to run.

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

Backup Source	Description
Desktop	If Desktop is selected, all files and/or folders in the following location will be backed up: %UserProfile%\Desktop
Documents	If Documents is selected, all files and/or folders located in the following location will be backed up: %UserProfile%\Documents If the Follow Link is enabled, all files and/or folders located in the following locations will also be backed up: %UserProfile%\Music %UserProfile%\Pictures %UserProfile%\Videos NOTE: The Follow link is enabled by default.

Favourites	If Favourites 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>
Outlook Express	If Outlook Express is selected, all files and/or folders located in the following location will be backed up: <i>%UserProfile%\Local Settings\AppData\Identities\ %UniqueAlphanumericString%\Microsoft\Outlook Express</i>
Windows Mail	If Windows Mail is selected, all files and/or folders located in the following location will be backed up: <i>%UserProfile%\AppData\Local\Microsoft\Windows Mail</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 folders to backup using the Quick Selection option, follow the steps below:

1. Select a backup source.

Select the items and folders that you want to backup

Desktop

Documents


Favourites

Outlook

Outlook Express

Windows Mail

Windows Live Mail

2. Click  to save 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	<p>Apply this filter to all files/folders in</p> <p><input checked="" type="radio"/> All hard disk drives</p>
Specific folder	<p><input checked="" type="radio"/> This folder only (Input local / network address)</p> <p><input type="text" value="C:\"/></p> <p><input type="checkbox"/> This share requires access credentials</p>


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

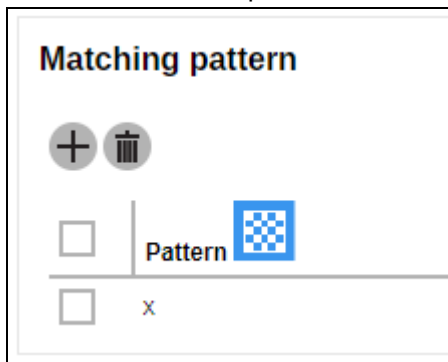
1. Slide the lever to the right to turn on the filter setting.





2. Click  to create a filter.
3. Enter a name for the backup filter.




4. Click  to add the pattern to be used. You can add multiple patterns here.



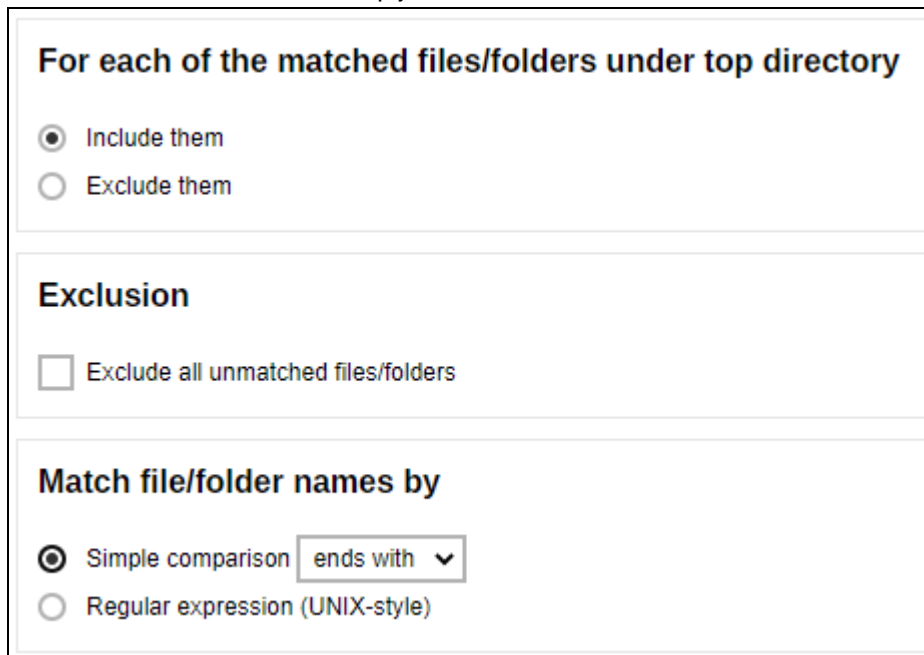
Matching pattern

| Pattern 

x

5. Select from the options below. In this example, all files and/or folders that end with the letter “x” will be included in the backup job.



For each of the matched files/folders under top directory

Include them

Exclude them

Exclusion

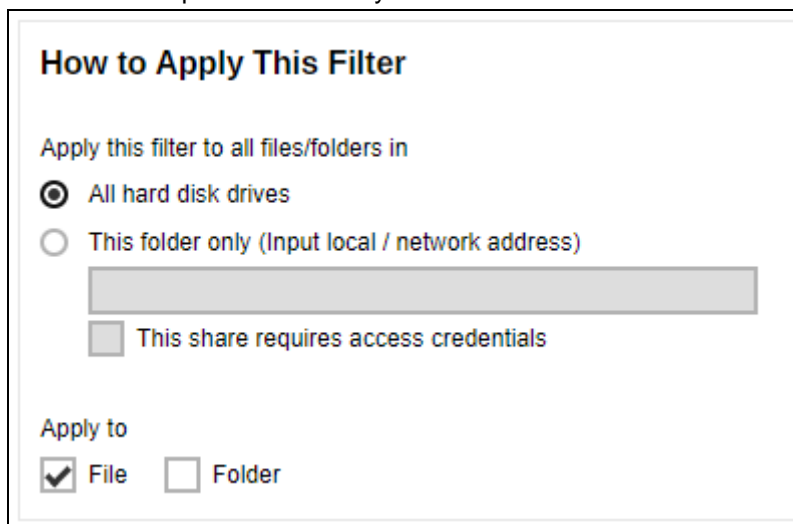
Exclude all unmatched files/folders

Match file/folder names by

Simple comparison

Regular expression (UNIX-style)

6. 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.



How to Apply This Filter

Apply this filter to all files/folders in

All hard disk drives

This folder only (Input local / network address)

This share requires access credentials

Apply to

File Folder

If 'This folder only' is selected, enter the local path or network address that you would like to apply the filter to.

This folder only (Input local / network address)

This share requires access credentials


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

7. Click  to add the created filter, then click  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  button.

Apply filters to the backup source

<input type="checkbox"/>	Name
<input type="checkbox"/>	Filter-1
<input type="checkbox"/>	Filter-2


NOTE

For a broader discussion regarding backup source file filtering, please refer to the [Ahsay Online Backup Manager v9 Backup Source File Filter Guide](#).

Option 3: Other Source

The Other 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. You can either select a source that will be included in the backup or select a source that will be excluded from the backup.

To select files and/or folders for back up using Other Source, follow the steps below:

1. Click  to select a source to be included in the backup.

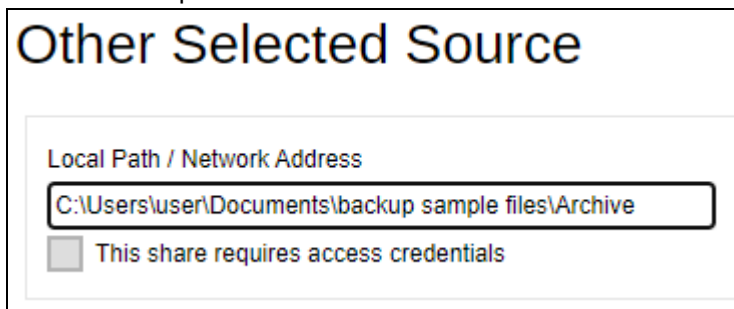


Other Selected Source

Path

2. Enter the local path or network address of the file and/or folder.

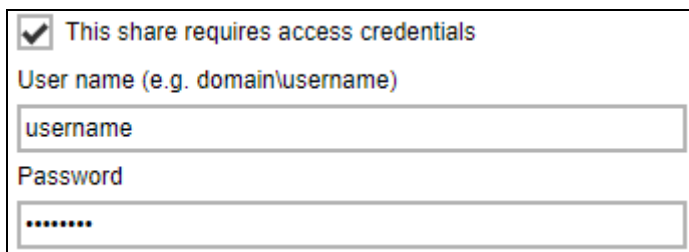


Other Selected Source

Local Path / Network Address

This share requires access credentials



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.




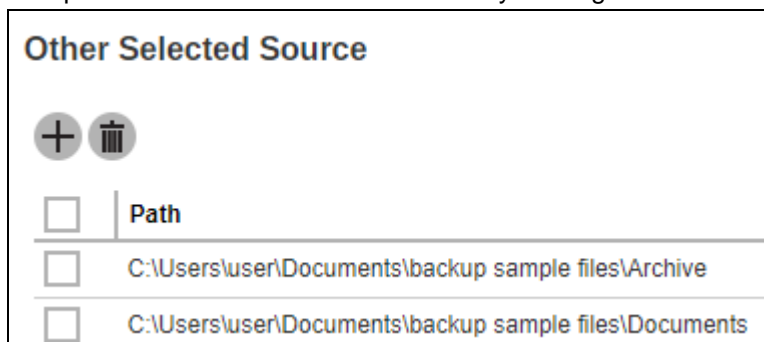
This share requires access credentials

User name (e.g. domain\username)



Password

3. Click  to add the selected source and click  to save the settings.

Multiple selected sources can be added by clicking the  button.



Other Selected Source


 

Path

C:\Users\user\Documents\backup sample files\Archive

C:\Users\user\Documents\backup sample files\Documents

To exclude files and/or folders from back up using Other Source, follow the steps below:

1. Click  to select a source to be included in the backup.

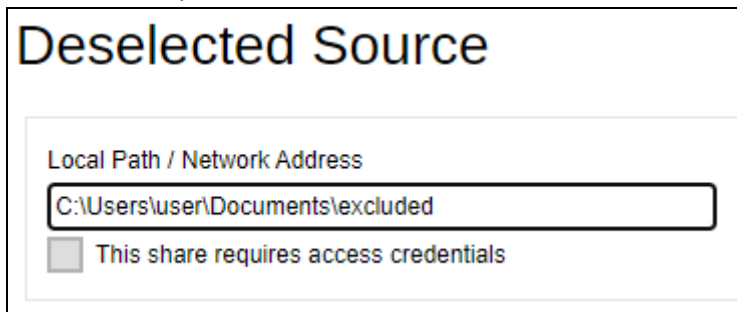


Deselected Source

Path

2. Enter the local path or network address of the file and/or folder.



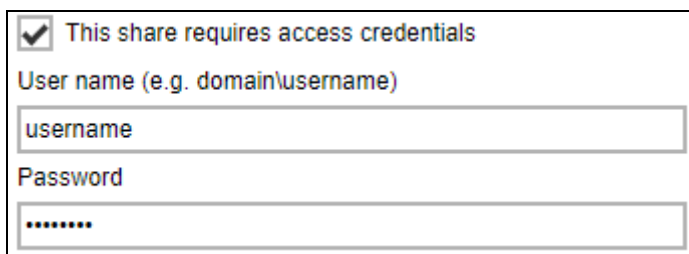
Deselected Source

Local Path / Network Address

C:\Users\user\Documents\excluded

This share requires access credentials

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)

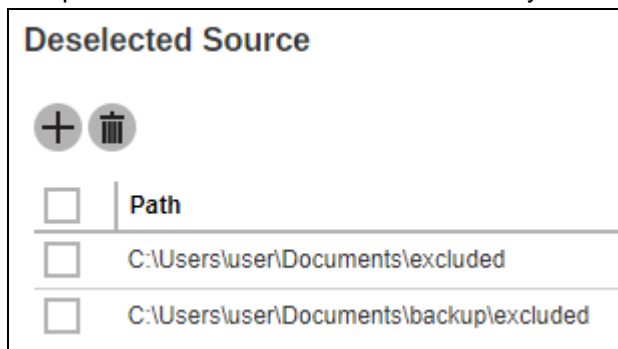
username

Password



.....

3. Click  to add the deselected source and click  to save the settings.

Multiple deselected sources can be added by clicking the  button.



Deselected Source

Path

C:\Users\user\Documents\excluded

C:\Users\user\Documents\backup\excluded

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 Selection + Filter)

You can use the quick selection 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.

Select the items and folders that you want to backup

- Desktop
- Documents
- Favourites
- Outlook
- Outlook Express
- Windows Mail
- Windows Live Mail




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

Apply filters to the backup source


Filter




Name



Matching pattern
 
 Pattern 
 x

For each of the matched files/folders under top directory
 Include them
 Exclude them

Exclusion
 Exclude all unmatched files/folders

Match file/folder names by
 Simple comparison 
 Regular expression (UNIX-style)

3. Click  to add the created filter then click  to save the settings.


Scenario 2 (Quick Selection + Other Source)

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

1. Choose a backup source.

Select the items and folders that you want to backup

- Desktop
- Documents
- Favourites
- Outlook
- Outlook Express
- Windows Mail
- Windows Live Mail

2. Click  to select a source to be included in the backup.

Other Selected Source



 

Path

Other Selected Source

Local Path / Network Address

This share requires access credentials



3. Click  to add the selected source then click  to save the settings.

Scenario 3 (Filter + Other Source)

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


1. Create a filter.

Apply filters to the backup source

Name

Filter-1

2. Click  to select a source to be included in the backup.

Other Selected Source



 

Path

Other Selected Source

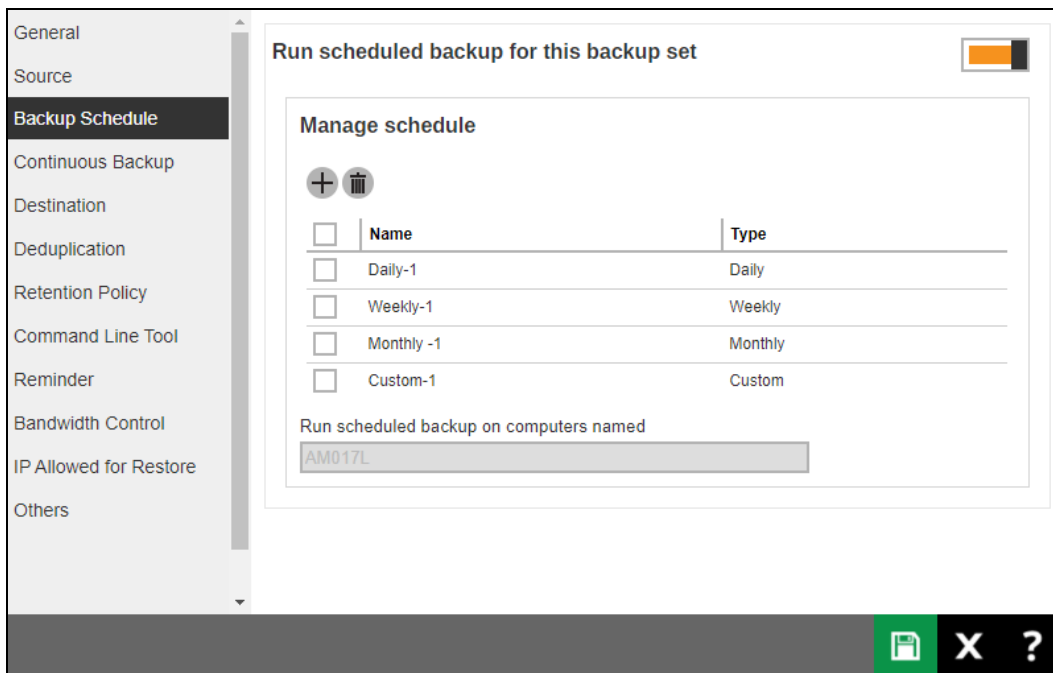
Local Path / Network Address

This share requires access credentials


3. Click  to add the selected source then click  to save the settings

6.2.3 Backup Schedule

The Backup Schedule page allows you to modify the backup schedule for the backup job to run automatically.






To configure a backup schedule follow the steps below:

1. Select an existing backup schedule to modify or click  to create a new one.
2. In the Backup Schedule window, configure the following settings: Name, Type, Start backup, Stop and Run Retention Policy after backup. For more details, please refer to the discussion regarding backup schedule setting in [Chapter 6.1](#).



The screenshot shows a "Backup Schedule" configuration window. At the top, it says "Client version < 8.3.3.20 does not support periodic schedule, periodic schedule will work as normal schedule." Below this is a "Details" section with the following fields:

- Name: A text input field.
- Type: A dropdown menu currently set to "Daily".
- Start backup: A time selection field with "at" in the first dropdown, "00" in the second, and "00" in the third.
- Stop: A dropdown menu currently set to "until full backup completed".
- Run Retention Policy after backup: A checkbox that is currently unchecked.

3. Click  or  to save the configured backup schedule settings.
4. Click  to save the backup schedule.

Multiple backup schedules can be created.

Manage schedule

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	Daily-1	Daily
<input type="checkbox"/>	Weekly-1	Weekly
<input type="checkbox"/>	Monthly -1	Monthly
<input type="checkbox"/>	Custom-1	Custom

NOTE

For backup sets with multiple backup schedules configured **at the same time**, this will be the order of priority to determine which schedule will be run:

1. Backup type: Full > Differential

While for Schedules that have selectable Backup Type:

- IBM Lotus Domino: Database > Log
- MS Exchange Server: Database > Log File
- MS SQL Server: Full > Differential > Incremental (VSS Backup Mode)
Full > Differential > Transaction Log (ODBC Backup Mode)
- MS Hyper-V: Full > Incremental
- Oracle Database: Database > Log
- ShadowProtect: Complete > Differential > Incremental
- VMWare: Full > Incremental

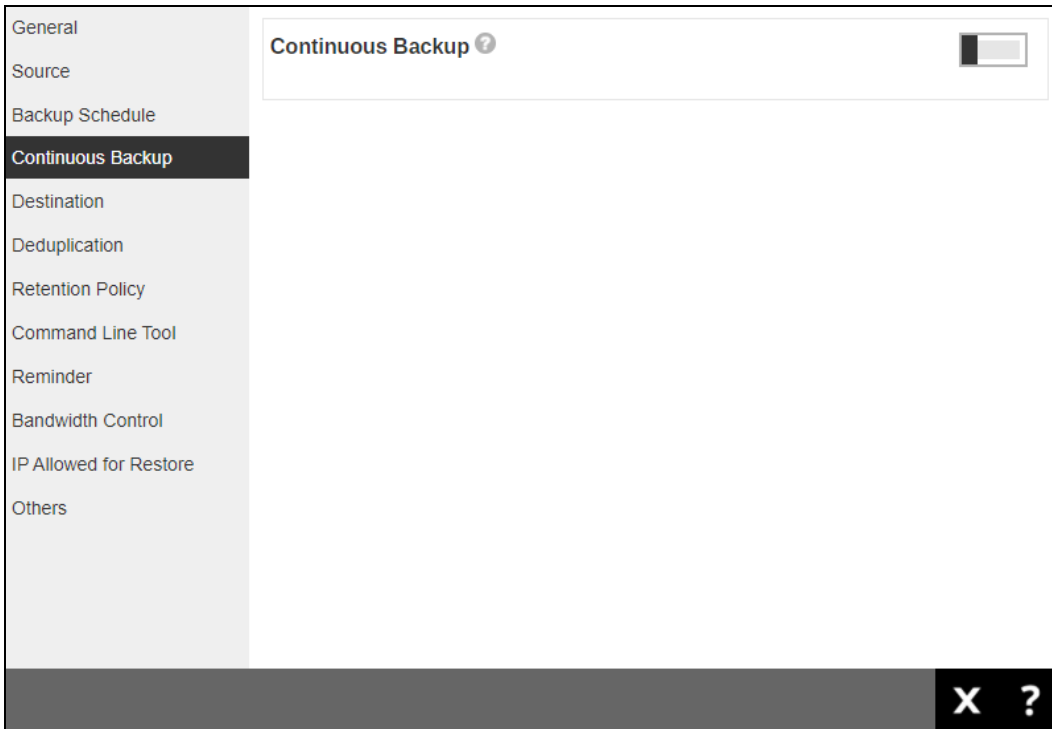
2. Stop: after X hours > after Y hours > until full backup completed (where X < Y)
3. Run Retention Policy after backup: enabled > disabled
4. Schedule type: Daily > Weekly > Monthly > Custom
5. Creation order

Examples:

- a. If there are 2 backup schedules with Full backup type and with Stop after 2 hours and 4 hours respectively. The backup schedule with Stop after 2 hours will be run.
- b. If there are 2 backup schedules with any Run Retention Policy enabled, it will have priority and execute that Schedule in this instance and ignore Schedule Type prioritization.
- c. For backup sets with backup schedules Daily and Weekly, the Daily backup schedule will be run.

6.2.4 Continuous Backup

The Continuous Backup page allows you to backup selective data whenever a change is made. This is disabled by default.

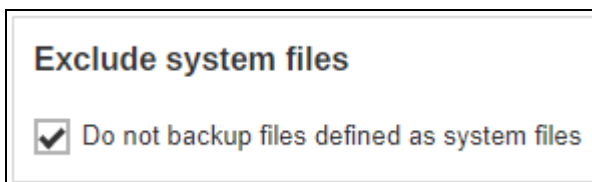


To enable continuous backup, follow the steps below:

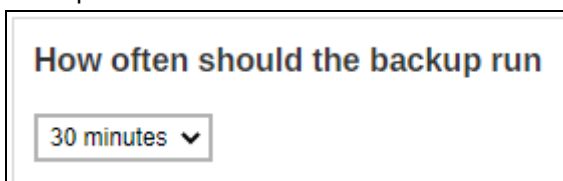
1. Slide the lever to the right to turn on the continuous backup setting.



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



3. Click the drop-down button to select how often the continuous backup job will run. The backup time interval can be set from 1 minute to 12 hours.




4. This option 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

Unlimited ▼ 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).

5. This allows the user to create an exclude filter to exclude files and/or folders from the backup job. Click  to create an exclude filter.

Exclude Filter

Existing Exclude Filters

| Name


If an exclude filter is created, click  to save the created exclude filter.

Exclude Filter

Name

Match file/folder names by
 Simple comparison
 Regular expression (UNIX-style)

Matching pattern

| Pattern 

A

Apply this filter to all files/folders in
 All selected sources
 This folder only (Input local / network address)

 This share requires access credentials

Apply to
 File Folder

6. Enter the name of the computer where the continuous backup will run.

Run CDP on computers named

7. Click  to save the configured continuous backup settings.

6.2.5 Destination

The Destination page allows you to select a backup mode and add storage destination.

There are two(2) types of backup mode:

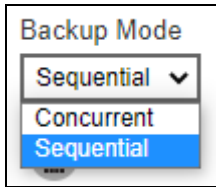
- ➊ **Sequential** - this is the configured backup mode by default. This backup mode will run a backup job to each backup destination one by one.
- ➋ **Concurrent** - this backup mode will run a backup job to all backup destinations simultaneously.

Comparison between Sequential and Concurrent Backup mode

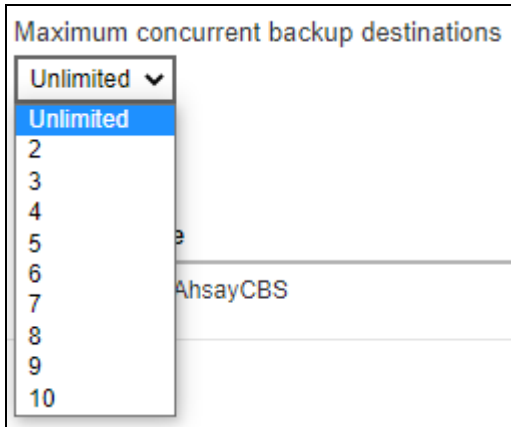
Backup mode	Pros	Cons
Sequential	<ul style="list-style-type: none"> ➤ Takes less resources in the local machine (e.g., memory, CPU, bandwidth, etc.) to complete a backup job. 	<ul style="list-style-type: none"> ➤ Backup job is slower than in concurrent mode since the backup job will upload the backup 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 configured. 	<ul style="list-style-type: none"> ➤ Requires more resources in the local machine (e.g. memory, CPU, bandwidth, etc.) to complete a backup job.


To modify the backup mode, follow the steps below:

1. Click the drop-down button to select a backup mode.




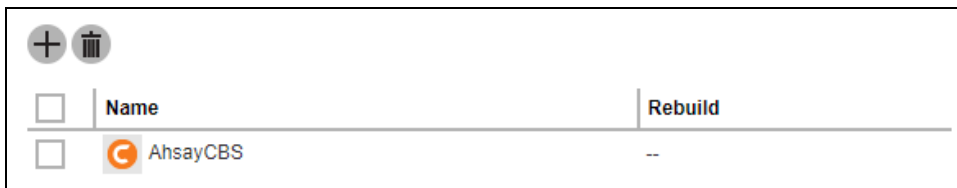
If "Concurrent" is selected, click the drop-down button to select the number of maximum concurrent backup destination.



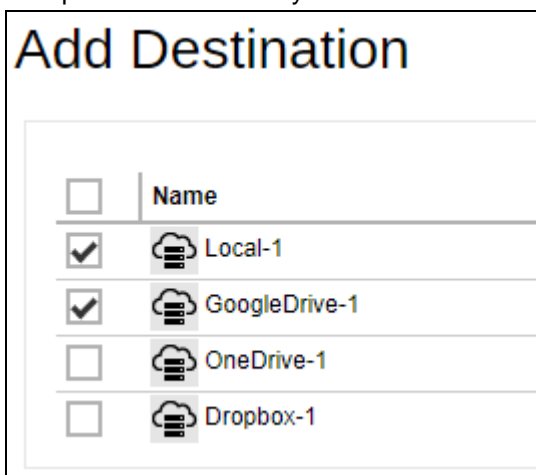
2. Click  to save the backup mode.


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

1. Click  to add a destination.



2. Select the backup destination by ticking the box beside the destination that you want to add. Multiple destinations may be added.



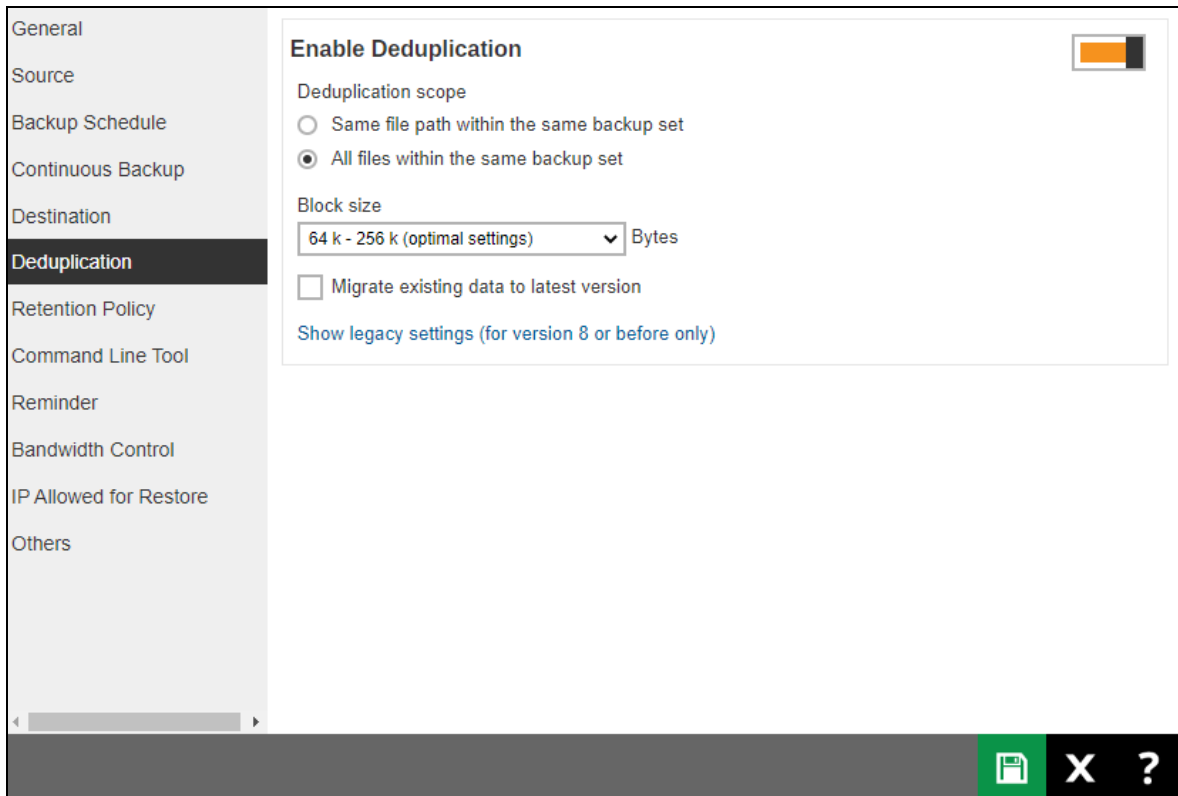
3. Click  to save the added storage destination.

6.2.6 Deduplication

Starting with AhsayCBS v9.0.0.0 or above, the In-File Delta feature will be replaced with Deduplication. The Deduplication page allows you to configure the deduplication settings which is enabled by default.

When this feature is **On (enabled)** for the backup set, a checksum verification of each backup file which was split into several blocks of varying size will be performed to compare its content and identify which block is duplicated, thus will perform deduplication of data.

When this feature is **Off (disabled)** for the backup set, a checksum verification of each backup file will not be performed, thus the duplicated data will NOT be removed or deduplicated during a backup job.



There are two(2) types of Deduplication scope:

- **Same file path within the same backup set** - this will deduplicate data under the same path during a backup job.
- **All files within the same backup set** - this is the selected deduplication scope by default. This will deduplicate data under the same backup set during a backup job.

NOTE

For more details about the Deduplication feature, please refer to the [AhsayCBS v9 New Features](#).

To configure the deduplication settings, follow the steps below:

1. Select the Deduplication scope.

Deduplication scope

Same file path within the same backup set

All files within the same backup set

2. Click the drop-down button to select the block size that will be used for the deduplicated data. This option is configured to use “64 k – 256 k (optimal settings)” by default.

The optimal setting is good for frequently changed source data, as this is the smallest block deduplication will use to compare and determine if the data is new and should be uploaded or discarded as duplicate. The larger the deduplication block size, the less efficient it would be but faster as there are less blocks of data to create. Frequent changes to this setting is not advisable since all data may need to be reuploaded because the previous block size and new block size are now different.

Block size

64 k - 256 k (optimal settings) ▾ Bytes

64 k - 256 k (optimal settings)

128 k - 512 k


256 k - 1 M

512 k - 2 M

1 M - 4 M (save less space but faster)

3. Optional: Tick the checkbox if you want the existing data to be migrated to the latest version during a backup job.

Migrate existing data to latest version

4. Click  to save the deduplication settings.

6.2.7 Retention Policy

The Retention Policy page allows you to configure the retention policy settings. By default it uses the “Simple” setting which keeps the deleted files for 7 days in the retention area.

Files and/or folders will be moved from the data area to the Retention Area if they were deleted, updated or have permission/attributes updated during a backup job. So the Retention Area is used as a temporary destination to store these files and/or folders. Files and/or folders in the Retention Area can still be restored.

While Retention Policy is used to control how long these files and/or folders remain in the Retention Area before they are removed which can be set in number of days, weeks, months or backup jobs. Retained data within all backup destinations (e.g. AhsayCBS, local drive, SFTP/FTP and cloud storage) are cleared by the Retention Policy job.

General

Source

Backup Schedule

Continuous Backup

Destination

Deduplication

Retention Policy

Command Line Tool

Reminder

Bandwidth Control

IP Allowed for Restore

Others

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 Day(s)

X ?

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) types of Retention Policy:

- 1. **Simple** - this 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.
- 2. **Advanced** - this 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. Select "Simple" from the option.

Simple
 Advanced

2. Click the drop-down button to select the number of day(s) or job(s) the deleted files will be retained.

Keep the deleted files for

▼

▼ Day(s)

1

2

3

4

5

6

7

8

9

10


14

21

28

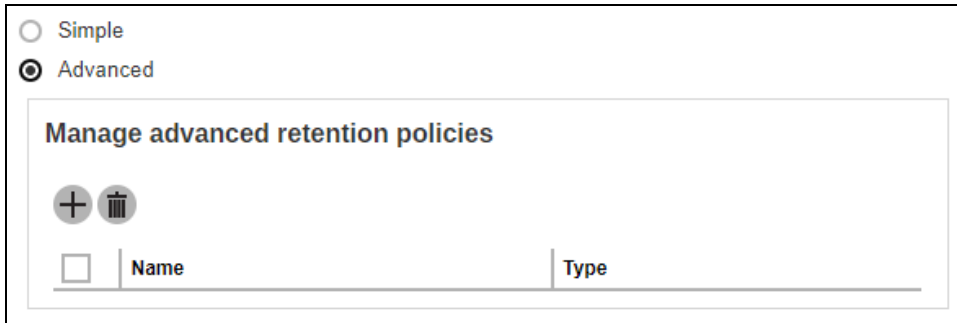
100

365


3. Click  to save the retention policy setting.

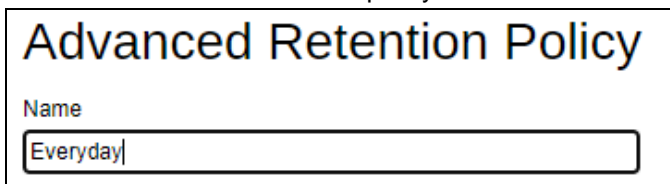
To configure an **Advanced Retention Policy**, follow the steps below:

1. Select "Advanced" from the option.



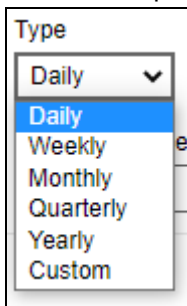
The screenshot shows a configuration window with two radio buttons: 'Simple' and 'Advanced'. The 'Advanced' radio button is selected. Below the radio buttons is a section titled 'Manage advanced retention policies' containing a plus icon, a trash icon, and a table with columns for 'Name' and 'Type'.

2. Click  to add a retention policy.
3. Enter a name for the retention policy.



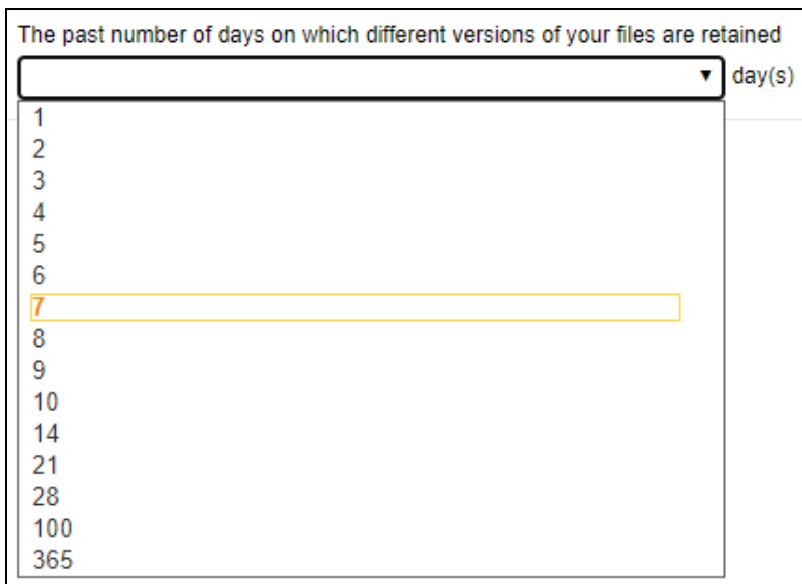
The screenshot shows a dialog box titled 'Advanced Retention Policy'. It has a 'Name' label and a text input field containing the text 'Everyday'.

4. Click the drop-down button to select a retention type.



The screenshot shows a drop-down menu with the title 'Type'. The current selection is 'Daily'. The menu is open, showing the following options: 'Daily', 'Weekly', 'Monthly', 'Quarterly', 'Yearly', and 'Custom'.

5. Click the drop-down button to select the number of days the deleted files will be kept in the retention area.



The screenshot shows a configuration window with the title 'The past number of days on which different versions of your files are retained'. It features a drop-down menu with a 'day(s)' label. The menu is open, showing a list of numbers: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 21, 28, 100, and 365. The number '7' is highlighted with a yellow background.

6. Click  to add the retention policy then click  to save the settings.

For further details about how to configure an advanced Retention Policy for each type (i.e., 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
<input type="text" value="Daily-1"/>
Type
<input type="text" value="Daily"/>
The past number of days on which different versions of your files are retained
<input type="text" value="7"/> day(s)

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

Name
<input type="text" value="Weekly-1"/>
Type
<input type="text" value="Weekly"/>
The days within a week on which different versions of your files are retained
<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat
The number of weeks to repeat the above selection
<input type="text" value="4"/> week(s)

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

Name
<input type="text" value="Monthly-1"/>
Type
<input type="text" value="Monthly"/>
The days within a month on which different versions of your files are retained
<input checked="" type="radio"/> Day <input type="text" value="1"/>
<input type="radio"/> <input type="text" value="First"/> <input type="text" value="Sunday"/>
The number of months to repeat the above selection
<input type="text" value="3"/> month(s)

- **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 quarter(s)

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

Name
Yearly-1

Type
Yearly

The day within a year on which different versions of your files are retained

January

Day 1

First Sunday

Sunday of Week 1

The number of years to repeat the above selection
7 year(s)

Multiple advanced Retention Policy can be created.

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

Simple
 Advanced

Manage advanced retention policies

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	Daily-1	Daily
<input type="checkbox"/>	Weekly-1	Weekly
<input type="checkbox"/>	Monthly-1	Monthly
<input type="checkbox"/>	Quarterly-1	Quarterly
<input type="checkbox"/>	Yearly-1	Yearly

There are two (2) ways to run the Retention Policy:

- ▶ [Backup Scheduler](#)
- ▶ [Manual Backup](#)

Option 1: Backup Scheduler (Recommended)

To run a Retention Policy job after a scheduled backup job, follow the steps below:

1. Go to the Backup Schedule page.

Run scheduled backup for this backup set

Manage schedule

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	Daily-1	Daily

Run scheduled backup on computers named

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

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

Backup Schedule

Client version < 8.3.3.20 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name

Type

Start backup
 :

Stop

Run Retention Policy after backup

- Click  then  to save the settings.

Option 2: Manual Backup

To run a Retention Policy job after a manual backup for Run on Server backup sets, follow the steps below:

- Go to the Backup Set page.

User Profile

Backup Set

Settings

Report

Statistics

Effective Policy

Manage Backup Set ?

+
-
↺

	Name	Type	Version	Owner	Execute Job
<input type="checkbox"/>	Data Backup (1635325749908)		--	AM017L	--
<input type="checkbox"/>	BackupSet-2 (1635325859312)		--	AM017L	--
<input type="checkbox"/>	BackupSet-3 (1635912967854)		Microsoft Exchange Server 2013	--	--
<input type="checkbox"/>	RoS Cloud File Backup Set (1638528064566)		--	--	Backup ▼ Run

- Select "Backup" then click **Run**.
- In the Backup window, select 'Run Retention Policy after backup' to run a Retention Policy job after the manual backup job.


Backup

Migrate Data

Migrate existing data to latest version

Retention Policy

Run Retention Policy after backup

4. Click  to start the manual backup job.

NOTE

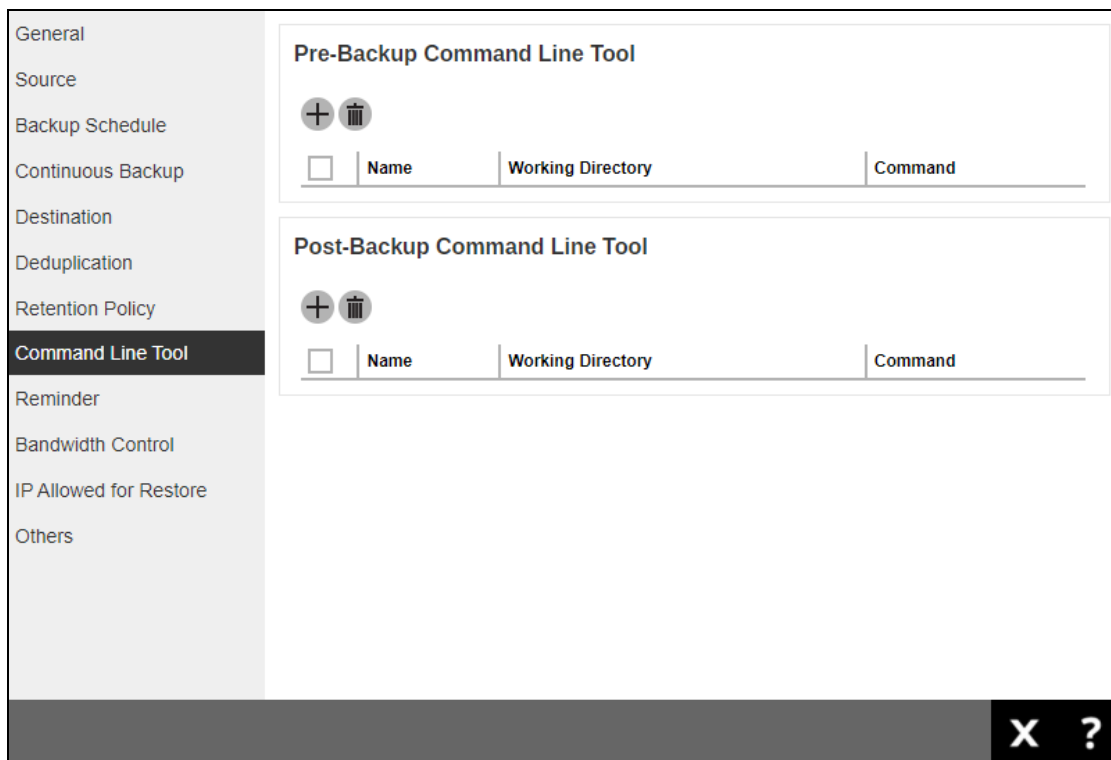
For instructions on how to run a Retention Policy job after a manual backup on Run on Client backup set please refer to [Chapter 10.5](#) of the AhsayOBM Quick Start Guide for Windows.

6.2.8 Command Line Tool

The Command Line Tool page allows you 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.

Here are some examples:

- Connecting to a network drive and disconnecting a network drive
- Stopping a third-party database (not officially supported by Ahsay) to perform a cold backup
- Restarting a third-party database after a backup



The screenshot shows the 'Command Line Tool' configuration page. On the left is a sidebar with the following menu items: General, Source, Backup Schedule, Continuous Backup, Destination, Deduplication, Retention Policy, **Command Line Tool**, Reminder, Bandwidth Control, IP Allowed for Restore, and Others. The main content area is titled 'Pre-Backup Command Line Tool' and 'Post-Backup Command Line Tool'. Each section contains a '+' icon, a trash icon, and a checkbox. Below these are three input fields: 'Name', 'Working Directory', and 'Command'. The bottom right corner of the window has a close button (X) and a help button (?).

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).

Command or Batch File Compatibility

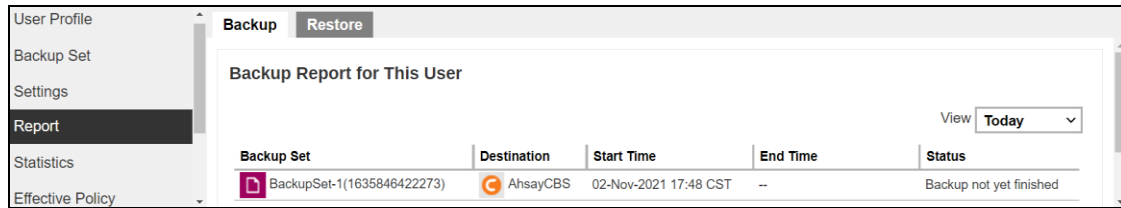
Make sure that each command (pre-backup and post-backup) are tested thoroughly before including them to the backup job.

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 Report page.



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 AhsayOBM sends the backup job status to AhsayCBS.

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.

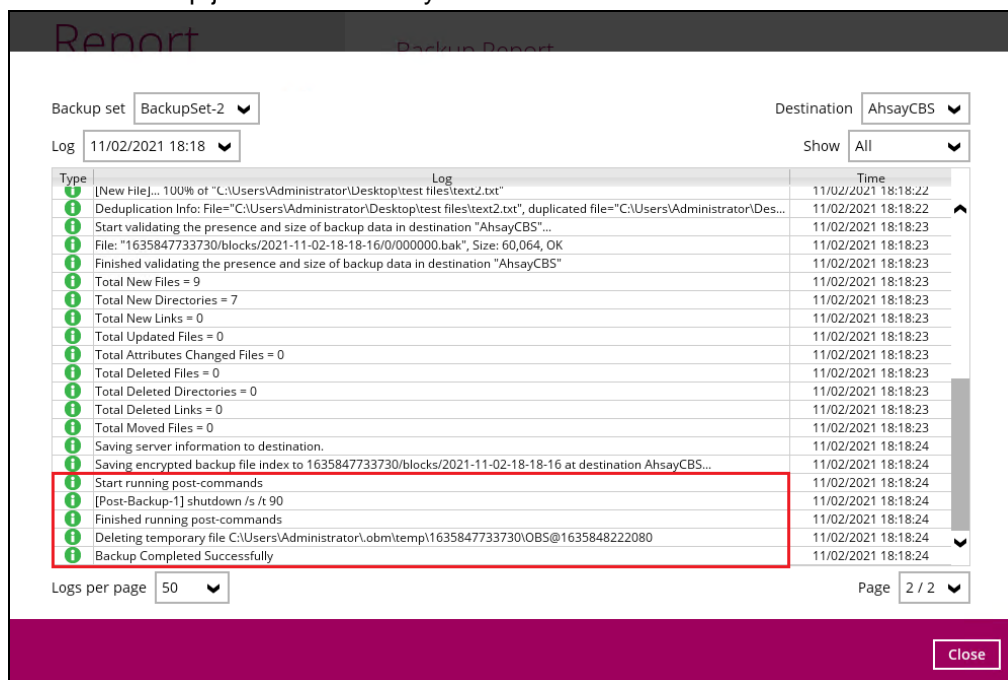
Post-Backup Command Line Tool

Name:

Working Directory:


Command:

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





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  to create a pre-backup command.

Pre-Backup Command Line Tool

<input type="checkbox"/>	Name	Working Directory	Command
<input type="checkbox"/>			

2. Enter the name.



Name

3. Enter the working directory. This is the location in the local machine where the pre-backup command will run or it can also be the location of the command or created batch file.

Working Directory


4. Enter the 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.

Command



5. Click  to create the pre-backup command then click  to save the settings.

Post-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  to create a post-backup command.

Post-Backup Command Line Tool

<input type="checkbox"/>	Name	Working Directory	Command
--------------------------	------	-------------------	---------

2. Enter the name.


Name

3. Enter the working directory. This is the location in the local machine where the post-backup command will run or it can also be the location of the command or created batch file.

Working Directory

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

Command

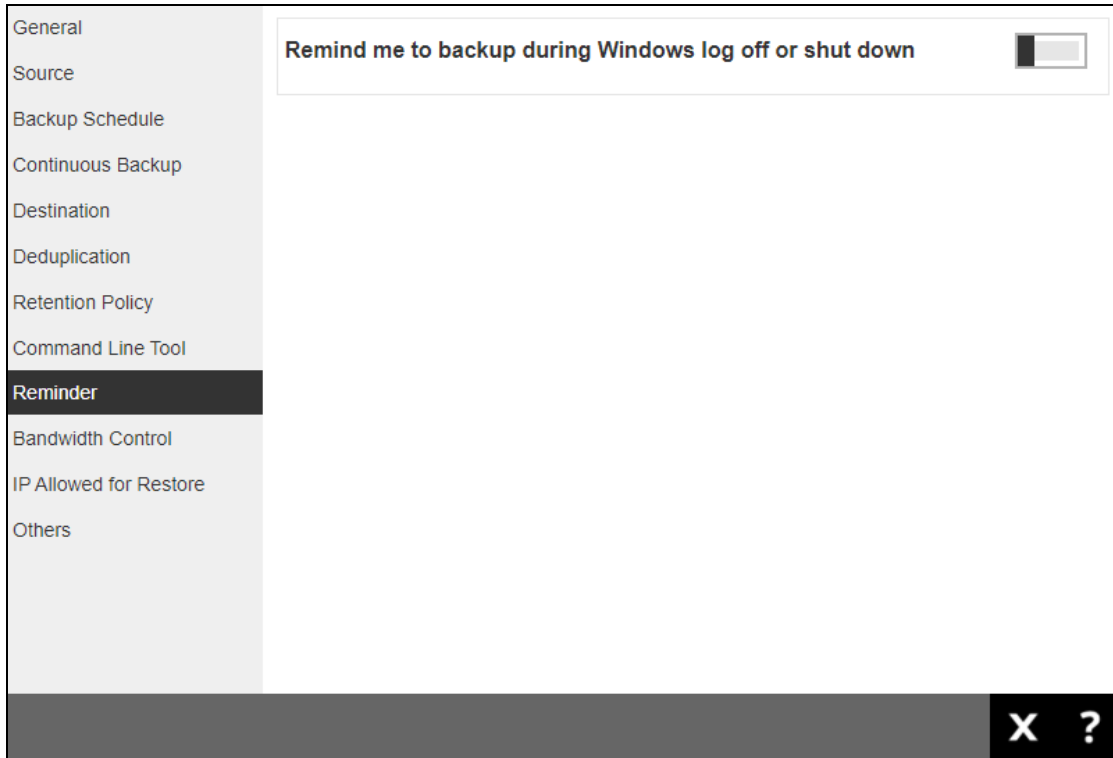
5. Click  to create the post-backup command then click  to save the settings.

NOTE

- You can check if the Pre-backup and Post-backup commands were run successfully from the backup report log once a backup job was completed.
- Multiple Pre-backup and Post-backup commands can be created in the Command Line Tool.
- Errors from Pre-backup and Post-backup commands will only be flagged as a warning and will not cause an error. The warning may be viewed in the logs.
- To trigger a job warning, Pre-backup and Post-backup commands must output a message to stderr. It is not possible to cause a job "Error" message to be logged.

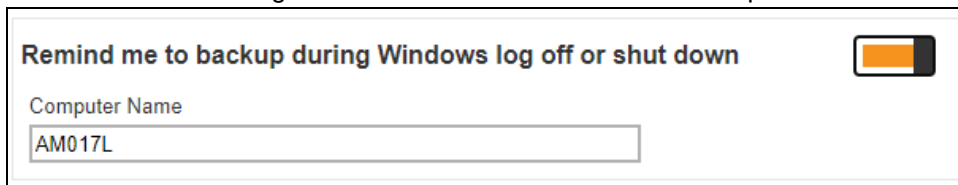
6.2.9 Reminder


The Reminder page allows you to set a reminder to run a backup during Windows log off, restart or shut down. A backup confirmation dialog box will appear once this is enabled. This is disabled by default.



To enable the Reminder setting, follow the steps below:

1. Slide the lever to the right to turn on the reminder for the backup set.



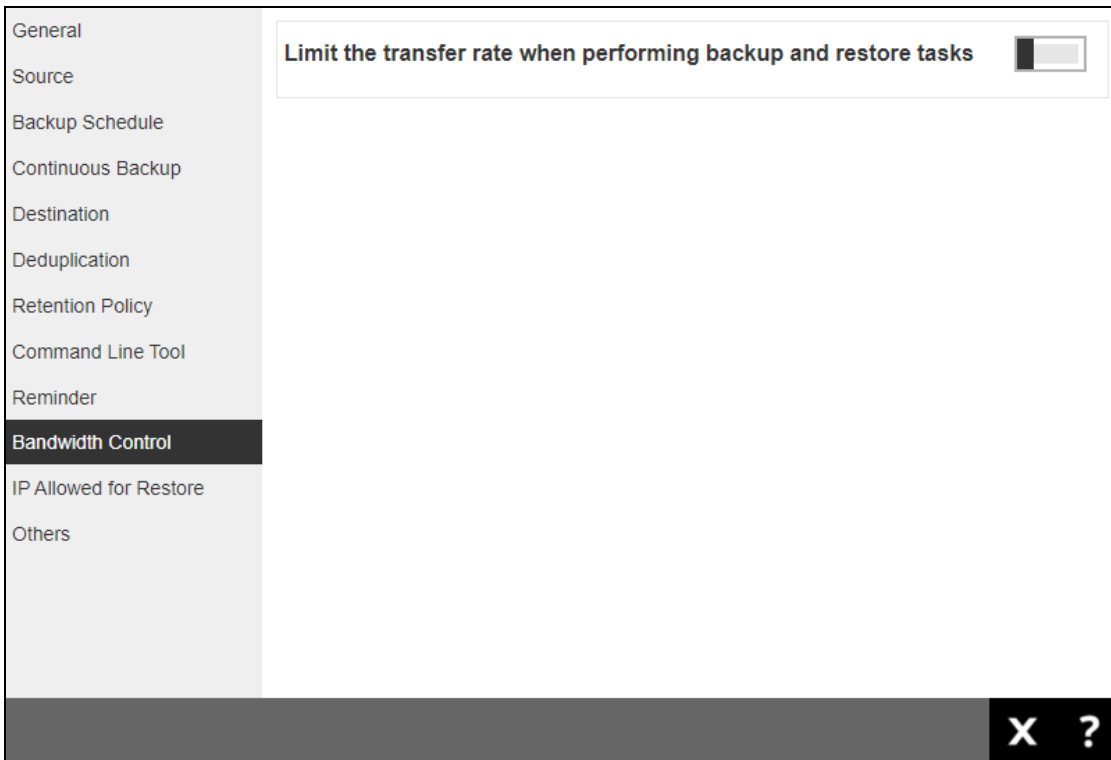
2. Enter the computer name where the backup set will be run.
3. Click  to save the settings.

NOTES

- This feature is not supported on Windows 10, Windows Server 2016, and Windows Server 2019.
- The dialog box will only appear if there is a backup set with enabled Reminder setting.
- The dialog box will only be displayed for four (4) seconds.
- 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.

6.2.10 Bandwidth Control

The Bandwidth Control page allows you to limit the amount of bandwidth used by backup traffic during specified times. This is disabled by default.



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

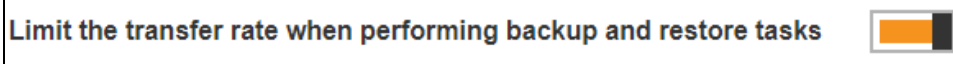
- **Independent** – each backup and restore has its assigned bandwidth.
- **Share** – all backup and restore operations share the same assigned bandwidth.

NOTE

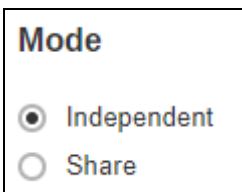
Share mode does not support performing a backup job on multiple destinations concurrently.


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

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





2. Select the mode.



3. Click  to create a bandwidth control.

Existing bandwidth controls

<input type="checkbox"/>	Name	Type	Maximum transfer rate
--------------------------	------	------	-----------------------

4. Enter the name.

Name

5. Select the type, this is the enforced bandwidth control period.

Type

Always

Only within this period

If "Only within this period" is selected, specify the period when bandwidth control will be enforced.

From

Sunday 04 : 00

To

Sunday 18 : 00



6. Enter the Maximum transfer rate, select if in Kbit/s, Mbit/s or Gbit/s.

Maximum transfer rate

100 Kbit/s

Mbit/s

Gbit/s


7. Click  to create the bandwidth control then click  to save the setting.

6.2.11 IP Allowed for Restore

The IP Allowed for Restore page allows you to define the IP ranges that will be allowed to perform a restore of the backup set.

	From	To
<input type="checkbox"/>		0.0.0.0
<input type="checkbox"/>		255.255.255.255



To add the IP range that will be allowed to restore the backup set, follow the steps below:

1. Click  to create the IP range.

	From	To
<input type="checkbox"/>		255.255.255.255

2. Enter the starting and ending IP address.

From	To
<input type="text" value="125.5.10.1"/>	<input type="text" value="125.5.10.10"/>

3. Click  to create the IP range then click  to save the settings.

6.2.12 Others

The Others page allows you to configure the following:

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

The screenshot shows the 'Others' configuration page with the following settings:

- Temporary Directory:** Temporary directory for storing backup files: C:\Users\admin\obm\temp. Remove temporary files after backup.
- Follow Link:** Follow link of the backup files.
- Volume Shadow Copy:** Enable Windows' Volume Shadow Copy for open file backup.
- File Permissions:** Backup files' permissions.
- OpenDirect:** Support of opening backup data directly without restoration.
- Compressions:** Select compression type: Fast with optimization for local.
- Encryption:** Backup user password is used as the encrypting key since "User Password" encryption type has been applied to this backup set. Encrypting key: *****. Algorithm: AES. Method: CBC. Key length: 256. [Recover Encryption Key](#)
- Recycle Bin:** Move the file to the Recycle Bin when remove file from Retention Policy or DIC. Keep the deleted files for: 7 day(s).

Temporary Directory

Temporary Directory is used for both backup and restore operations.

Temporary Directory

Temporary directory for storing backup files

 Remove temporary files after backup

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 job. The index files are synchronized to each individual backup destination at the end of each backup job

For a **restore job**, it is used to temporarily store temporary restore files.

NOTE

For best practice, the temporary directory should be located on a local drive for optimal backup and restore performance.

It should NOT be located on:

- 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.

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. Enter the new temporary directory.

Temporary directory for storing backup files

2. Optional: Tick the 'Remove temporary files after backup' checkbox.

Remove temporary files after backup

3. Click  to save the settings.

Follow Link

The Follow Link determines if the NTFS junction or symbolic link will be kept during a backup job. This is ticked by default.

Follow Link

Follow link of the backup files

NOTE

This is only applicable for File Backup Sets.

Volume Shadow Copy

Volume Shadow Copy uses 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 AhsayOBM/AhsayACB can continue to back up files even if they are opened and/or have been updated by the user.

Volume Shadow Copy

Enable Windows' Volume Shadow Copy for open file backup

NOTES

- This is only applicable for File Backup Sets on Windows platform only.
- 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 AhsayOBM 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.
- Volume Shadow Copy does not support open file backups on network drives.

File Permissions

File Permissions determines whether to back up the operating system file permission of the data selected as backup source. This is ticked by default.

File Permissions

Backup files' permissions

NOTE

This is only applicable for File Backup Sets.

OpenDirect

OpenDirect is used to have 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](#) of the AhsayOBM Quick Start Guide for Windows.

OpenDirect

Support of opening backup data directly without restoration

WARNING

- 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 AhsayOBM/AhsayACB 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.
- 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.
- Once OpenDirect is enabled and the setting is saved, it cannot be disabled without re-creating the backup set.

Compression

Compression allow you to compress all the files before it is backed up to the backup destination(s). For newly created backup set(s), "Fast with optimization for local" is selected by default.

Compressions

Select compression type

Fast with optimization for local ▼

There are four (4) compression types:

- **No Compression** - file will not be compressed before backup.
- **Normal** - compression is comparable to gzip Normal compression ratio.
- **Fast (Compressed size larger than normal)** - compression will be faster but with less compression and lower CPU usage compared to Normal.
- **Fast with optimization for local** - uses Snappy compression library when backing up to local destination only, otherwise setting will default to gzip if backing up to other destinations. Has the lowest CPU usage, very high speed and reasonable compression but compressed file size may be larger than Fast.

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

Encryption allows you to view the current encryption settings. The encryption settings can only be configured during the creation of backup set.

Encryption

Backup user password is used as the encrypting key since "User Password" encryption type has been applied to this backup set

Encrypting key	*****
Algorithm	AES
Method	CBC
Key length	256

NOTE

For more details about encryption settings, please refer to step number 12 in [Chapter 6.1 Create Backup Set](#).

Recycle Bin

This feature is for protection of the BAK (block) files stored in the Backup Set's destination, allows the user to set the number of days BAK files that were deleted due to Retention Policy or Data Integrity Check, will be held under Recycle Bin as added protection. Here are the features of the Recycle Bin:

- Data in the Recycle Bin will consume Quota.
- It does not move the data in another location within the storage, instead the index tracks the xxxxxx.bak files and the remaining time in the Recycle Bin.
- If the index is reverted to a previous timestamp, the settings of the Recycle Bin in the reverted index will be followed.
- Recoverability of data is not affected when the Recycle Bin is alternately enabled or disabled.
 - When enabled, it will only check if the data inside the Recycle Bin is still within the set number of days. Once it is beyond the set number of days it will only be deleted when the following operations are run: Backup, Space Freeing Up, Data Integrity Check and Delete Backup Data.
 - When disabled, if there are already deleted files it will not automatically delete the data inside the Recycle Bin. It will remain in the Recycle Bin even if it is beyond the set number of days. It will only be deleted when the following operations are run: Backup, Space Freeing Up, Data Integrity Check and Delete Backup Data.
- Once the Recycle Bin is disabled, deleted files will be removed immediately and will not be moved in the Recycle Bin.
- The setting applies to all destinations for the backup set.
- Viewing Recycle Bin contents is not available.

- Recycle Bin cleanup is done at the start of the backup job process.
- Recovering from Recycle Bin requires reverting the index. For instructions on how to revert the index please refer to this article: [FAQ: How to un-delete backup data moved to Retention, or revert indexes to a healthy state from an earlier successful backup.](#)

WARNING

When reverting index, new data will be lost.

This is enabled by default and set to 7 days.

Recycle Bin

Move the file to the Recycle Bin when remove file from Retention Policy or DIC

Keep the deleted files for day(s)

To set the number of days, follow the steps below:


1. Enable the Recycle Bin by sliding the switch to the right.

Recycle Bin

Move the file to the Recycle Bin when remove file from Retention Policy or DIC

2. Select the number of days the deleted files will remain in the Recycle Bin. There is a dropdown box available for selection but the number of days can also be entered manually.

Keep the deleted files for day(s)

3. Click  to save the settings.

6.3 Run a Backup Job

Run an Agent-based Backup using AhsayOBM / AhsayACB

Except for Cloud File Backup and Microsoft 365 Backup which you can run an agentless backup in AhsayCBS, all other backup modules require you to perform backup and restore using your client backup agent (AhsayOBM or AhsayACB).

For details on creating backup job using AhsayOBM or AhsayACB, refer to the backup module's User Guide which can be downloaded on the [User's Guide download page](#).

Run an Agentless Backup using AhsayCBS User Web Console (for Cloud File and Microsoft 365 Backup only)

There are two types of backup set, **Cloud File Backup** and **Microsoft 365 Backup**, which can run agentless backup using AhsayCBS user web console. These two (2) types of backup set can be created either on the AhsayCBS server, or the AhsayOBM or AhsayACB client and they can be both client-driven and server-driven.

When you create a new backup set with the **Type** being **Cloud File Backup**, you have a choice of whether to run the backup on the **Server** or on the **Client**. Please make sure that you choose **Server** if you want to run the backup from the AhsayCBS server directly.

The screenshot displays the configuration interface for a backup set. On the left is a sidebar with menu items: General, Source, Backup Schedule, Destination, Deduplication, Retention Policy, Bandwidth Control, and Others. The main area is titled 'General' and contains the following fields:

- ID:** 1641869444557
- Name:** Server Run Cloud File Backup
- Owner:** -
- Backup set type:** Cloud File Backup
- Run on:** Radio buttons for Server (selected) and Client.

Below this is a section for 'Cloud File Backup' with a 'Backup From' dropdown menu set to 'Google Drive' and a 'Refresh' button.

Backup Destination for Run-on-Server Backup Set

For **Microsoft 365 Backup** and **Cloud File Backup** sets created in **Run-on-Server** backup type, the available backup destinations are AhsayCBS and Predefined Destinations, only one of these destinations can be selected. For more information on the Predefined Destinations, please contact your backup service provider.

6.4 Restore a Backup (Non-Run Direct Restore)

As opposed to [Run Direct Restore](#) where you can instantly restore a VM by running it directly from the backup files in the backup destination. Non-Run Direct restore is the traditional type of restore where you can restore the backed-up data to the original location, or an alternate location based on your choice.

Restore using AhsayOBM / AhsayACB (Agent-based restore)

Except for Cloud File Backup and Microsoft 365 which you can run an agentless restore in AhsayCBS (refer to the steps below), all other backup modules require you to perform restore using your client backup agent (AhsayOBM or AhsayACB).

Restore using AhsayCBS User Web Console (Agentless restore)

There are two (2) types of backup sets that can be restored through the AhsayCBS User Web Console, **Cloud File Backup** and **Microsoft 365 Backup**, provided that the backup set was created to **Run on Server**.

7 Run Direct Restore

7.1 Introduction

What is Run Direct?

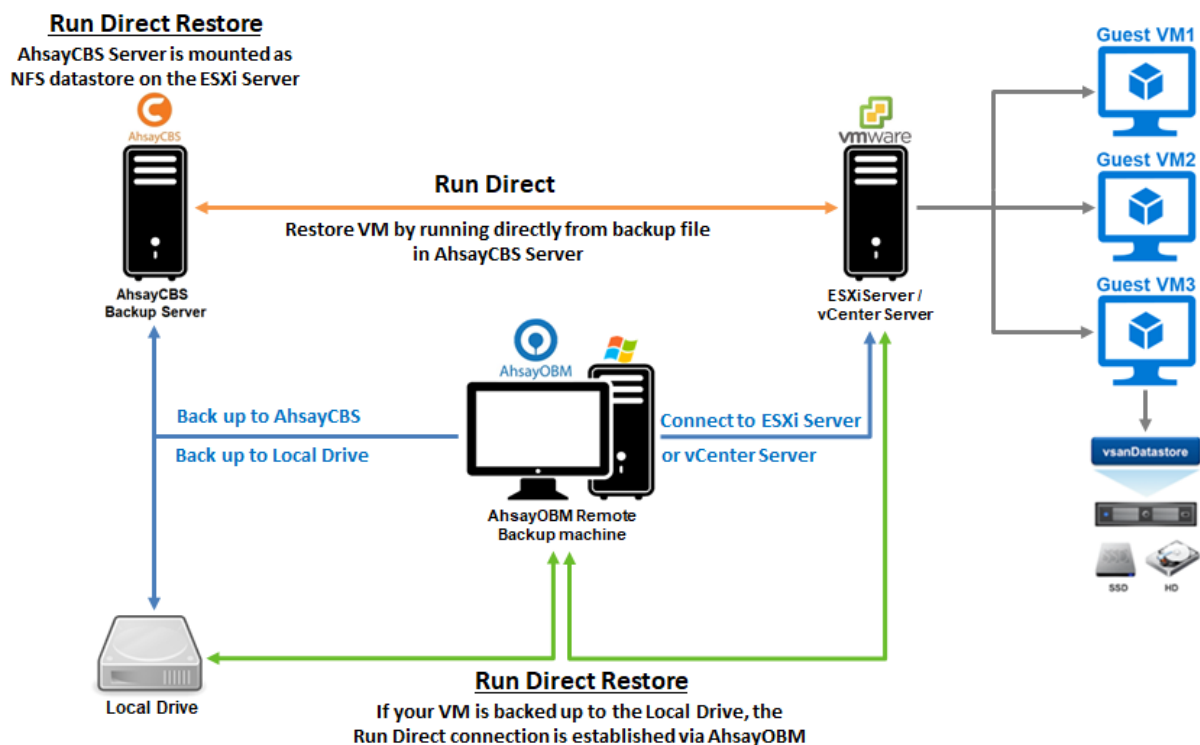
Run Direct is a feature that helps reduce disruption and downtime of your production VMs.

Unlike normal VM restore procedure where a VM is extracted from backup files and copied to the production storage, which can take hours to complete. Restore with Run Direct can instantly power up a VM by running it directly from the backup files in the backup destination so that the VM can be put into production.

How does Run Direct work?

When a Run Direct restore is performed, the backup destination is mounted as an NFS datastore from the VMware host, where the VM is run directly from the backup files.

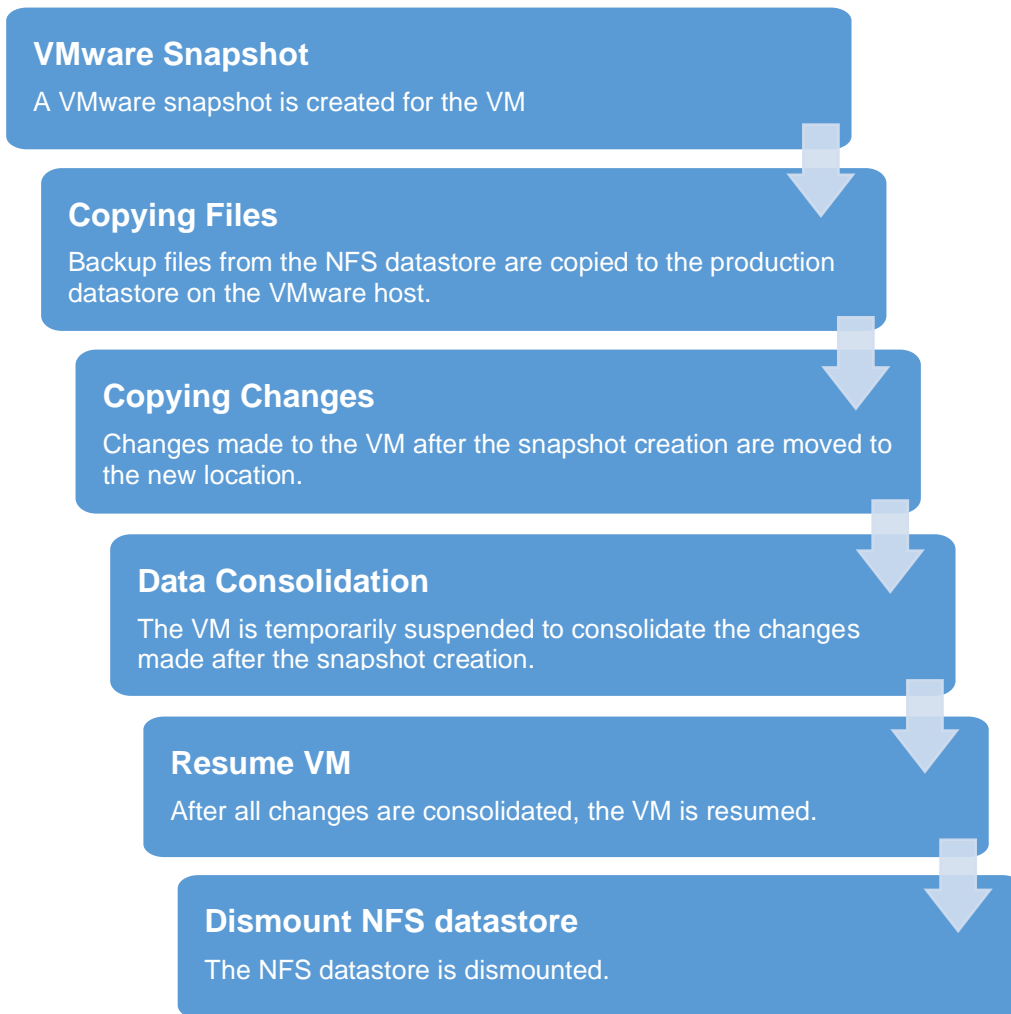
The backup destination can either be the AhsayCBS server or a local drive that can connect with AhsayOBM. Initiating a Run Direct from the AhsayCBS (also known as agentless restore) will trigger a connection directly with the VMware host (ESXi server and direction shown in orange indicator below), while initiating the same action on the AhsayOBM requires the connection to route through the AhsayOBM (shown in green indication below).



The restored virtual machine, at this stage (e.g. before the restore is finalized) is in a read-only state to preserve its integrity. All changes made to the virtual disks (e.g. operation within the guest virtual machine) are stored separately in transaction logs stored on the NFS datastore or the original datastore, depending on the setting selected. These changes are discarded when Run Direct is stopped, where the restored VM will be removed and all changes will be discarded, or the changes will be consolidated with the original virtual machine data when the restore is finalized.

Finalizing a VM Recovery (Migrating VM to permanent location)

To finalize recovery of a VM, you will still need to migrate it to a permanent location on the VMware host. The following steps are taken when you finalize a Run Direct restore:



NOTE

For vCenter VM backup set, provided that the vMotion feature of the vCenter set is working properly, the VM will not be suspended during the data consolidation.

Non-Run Direct Restore

Run Direct restore gives you the convenience of quickly restoring the VM by running it directly from the backup files in the backup destination, however, if you wish to restore the VM permanently to a location of your choice first before accessing the backup files, you should perform a Non-Run Direct restore instead. Refer to [Restoring a Backup \(Non-Run Direct Restore\)](#) for instructions.

Run Direct Requirements & Best Practices

To utilize the Run Direct feature, ensure that the following requirements are met:

• Backup Destination Requirement

When a Run Direct restore is performed, the backup destination containing the guest VM files is mounted on the VMware host as NFS datastore.

Ensure that the following requirements are met by the backup destination of the VMware VM backup set:

- **Destination Type** of the backup destination must be set to a **Single storage destination**.
- Destination must be accessible to the VMWare host.
- Destination must have sufficient disk space available for the Run Direct restore. There should be 1.5 x total provisioned size of all VMs selected for backup.
- For Run Direct restore of 1 VM with provisioned size of 100GB, there should be 150GB (e.g. 1.5 x 100GB) of free space available in the Destination.

• No compression and Encryption

Data backed up to a Run Direct enabled destination is not compressed or encrypted to optimize restore performance as Run Direct will make the VM restored by running the data directly from the backup files in the backup destination.

• Restore to Alternate Location

- When performing a Run Direct restore to **Alternate Location**, only one VM can be selected per restore session.
- Consider creating separate VMware VM backup set for each VM that you intend to perform Run Direct restore (e.g. VMs that you may restore to alternate location).

7.2 Run Direct Restore Options

Run Direct restore gives you the convenience and flexibility of quickly restoring the VM by running it directly from the backup files in the backup destination, however, you may still wish to migrate the VM permanently afterward. There are 3 Run Direct Restore options you can choose from as explained below.

- Option 1: Perform Run Direct Only

This option allows you to power up the VM instantly by running it directly from the backup files, but it won't be migrated to any permanent location on VMware host. Leave the **Auto migrate after Run Direct is running** checkbox unchecked in step 6 under [Performing a Run Direct Restore on VM](#) below if you wish to go for this option.

- Option 2: Perform Run Direct + Auto Migration

This option allows you to power up the VM instantly by running it directly from the backup files. While you can now access the Run Direct restored VM, it will also be migrated automatically to a permanent location on the original VMware host, another datastore of the original VMware host or another VMware host. Make sure the **Auto migrate after Run Direct is running** checkbox is checked in step 6 under [Performing a Run Direct Restore on VM](#) below if you wish to go for this option.

- Option 3: Perform Run Direct + Manual Migration

This option allows you to power up the VM instantly by running it directly from the backup files. While you can now access the Run Direct restored VM, you will have to manually migrate the VM to a permanent location on the original VMware host, another datastore of the original VMware host or another VMware host. Leave the **Auto migrate after Run Direct is running** checkbox unchecked in step 6 under [Performing a Run Direct Restore on VM](#) below if you wish to go for this option. When the Run Direct restore is completed, you can initiate a Manual Migration any time. Refer to step 8 below for relevant instructions.

NOTE

If perform Run Direct only without migration, any changes made to the VM during the Run Direct power up process will be lost when the VM is powered down.

If perform Run Direct with auto or manual migration, any changes made to the VM during the Run Direct power up process will be consolidated with the original virtual machine data once the migration has been completed successfully.

7.3 Performing a Run Direct Restore on VM

AhsayCBS supports backup and restore of VMware VMs stored on vSAN datastore. With this, there are now several scenarios for restoring VMs using Run Direct.

The restoration steps for the four scenarios will be discussed below:

- ▶ [Restore backup from VMFS datastore to VMFS datastore](#)
- ▶ [Restore backup from VMFS datastore to vSAN datastore](#)
- ▶ [Restore backup from vSAN datastore to vSAN datastore](#)
- ▶ [Restore backup from vSAN datastore to VMFS datastore](#)

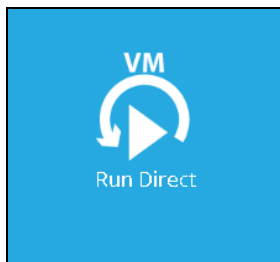
7.3.1 Restore a backup from VMFS datastore to VMFS datastore

1. Log in to AhsayCBS user web console according to the instruction provided in section [Logging on to AhsayCBS User Web Console](#).

NOTE

Before you can start Run Direct, you must have a VMware backup set created in the AhsayOBM client. Please refer to the [Ahsay Online Backup Manager v9 VMware vCenter/ESXi Backup & Restore Guide](#) for information on how to create the backup set. In addition, you must also run a successful backup on the VMware backup set before you can perform restore from Run Direct.

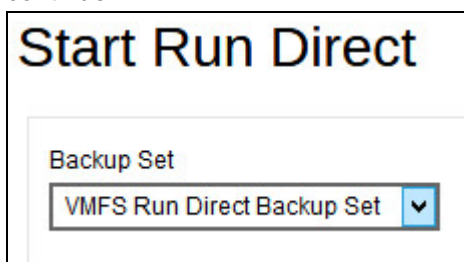
2. Click the **VM Run Direct** icon from your AhsayCBS environment.



3. Click **+** from the **Run Direct** page to start a new Run Direct session.



4. Select the **Backup Set** from the dropdown box of VMware backup set you have created. In our example, the backup set is called **VMFS Run Direct Backup Set**. Click **➔** to continue.



- Select the backup job to restore from the **Restore file of job** dropdown box. In our example, there are two virtual machines. Check the box next to the one on which we will perform a restore, **Lubuntu12x**.



- Select the location to restore your virtual machine. They are found under **Restore virtual machine to** on the **Start Run Direct** page.

- Select **Original Location** to restore the VM to its original EXSi host and datastore.



- Select **Alternate Location** to restore the VM to a different VMware host and a different datastore. Alternatively, you can also restore to the same VMware host but to a different datastore.

NOTE

If you select Alternate Location, you will see an additional option Overwrite existing files.



Configure the following options according to your restore requirements.

Start Run Direct

Restore virtual machines to

Original Location

Alternate Location

Auto migrate after Run Direct is running

Auto power on after Run Direct is running

Use existing storage as VM working directory to improve performance

Overwrite existing files

• **Auto migrate after Run Direct is running**

Select this option if you want to auto migrate the virtual machine to a permanent location on the original VMware host, another VMware host, or same VMware host but another datastore, depending on whether you have chosen **Original Location** or **Alternate Location** to restore your VM.

• **Auto power on after Run Direct is running**


Select this option to power up the virtual machine automatically, after Run Direct is running for the VM.

• **Use existing storage as VM working directory to improve performance**

Select this option to enhance performance of the restored VM.

• **Overwrite existing files** (Alternate Location only)

Select this option to overwrite existing files when restoring to a different VMware host or a different datastore.

Click  to proceed when you are done with the settings.

7. This step only applies if you selected **Alternate Location**, you need to enter the VMware host and access information of where you would like the VM to be restored to. Otherwise skip to Step 9.

For restoration to another VMware ESXi host, select **VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7** as **Version**, then enter the **Username**, **Password**, **Host**, and **Port** of the new host.

Start Run Direct

VMware Host

Version
 VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7.0

Username
 administrator

Password
 ●●●●●●●●

Host
 10.120.8.40

Port
 443

- Specify the **Name**, **Inventory Location**, **Host/Cluster**, **Resource Pool**, and **Storage** for the alternate location.

Start Run Direct

Name
 New Virtual Machine 1

Inventory Location
 Datacenter

Host / Cluster
 10.16.8.42

Resource Pool
 10.16.8.42

Storage
 Datastore-SHR01 (1)

Click  to start the restore.

- The **Run Direct** page appears, showing the status message of the Run Direct restore job.

Run Direct

<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	No	VMFS Run Direct Backup Set	10.120.8.40	Datacenter/New Virtual Machine 1	<div style="width: 50%; background-color: blue;"></div> 50%	2021-03-24 16:02:52	Adding virtual machine "New Virtual Machine 1" to the inventory...		

If your Run Direct is successful, you get a message similar to the following, with Status showing OK and Progress showing 100%.

Run Direct									
<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	Yes	Direct Backup Set	10.120.8.40	Datacenter/New Virtual Machine 1	100%	2021-03-24 16:02:52		OK	Migrate

Restore log messages on AhsayCBS

Click on the item on the Run Direct page.

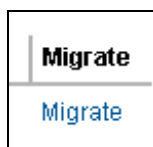
Timestamp	Type	Message
2021-03-24 04:03:39	info	Preparing for Run Direct...
2021-03-24 04:03:40	info	Use target storage as VM working directory. Reason = "Delta disk format of virtual disks is not supported by datastore."
2021-03-24 04:03:45	info	Mount datastore "cbs-RunDirect (192.168.7.101:cbsRunDirect)"...
2021-03-24 04:03:51	info	Adding virtual machine "New Virtual Machine 1" to the inventory...
2021-03-24 04:04:31	info	Taking snapshot "__snapshot_for_publish__" of virtual machine "New Virtual Machine 1"...
2021-03-24 04:04:39	info	Powering on virtual machine "New Virtual Machine 1"...
2021-03-24 04:05:18	info	Please do not Edit, Remove or Revert any existing snapshot before migration is completed.
2021-03-24 04:05:18	info	Restore Completed Successfully

Restore log messages on the VMware vSphere Client

Open your VMware vSphere Client and you will see the following messages from the Recent Tasks section.

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion T...	Server
Create NAS datastore	10.16.8.42	Completed	VSPHERE.LOC...	24 ms	03/24/2021, 4:03:43 PM	03/24/2021, 4:03:46 PM	vCenter05-v65
Register virtual machine	Datacenter	Completed	VSPHERE.LOC...	28 ms	03/24/2021, 4:03:51 PM	03/24/2021, 4:04:00 PM	vCenter05-v65
Reload virtual machine	New Virtu...	Completed	VSPHERE.LOC...	11 ms	03/24/2021, 4:04:04 PM	03/24/2021, 4:04:10 PM	vCenter05-v65
Create virtual machine snapshot	New Virtu...	Completed	VSPHERE.LOC...	10 ms	03/24/2021, 4:04:29 PM	03/24/2021, 4:04:34 PM	vCenter05-v65
Power On virtual machine	New Virtu...	Completed	VSPHERE.LOC...	23 ms	03/24/2021, 4:04:38 PM	03/24/2021, 4:05:13 PM	vCenter05-v65

- If you did not enable the **Auto Migrate after Run Direct is running** option in step 6, but still wish to migrate VM to a permanent location of your choice, click on the **Migrate** button as shown.



Run Direct									
<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	No	Direct Backup Set	10.120.8.40	Datacenter/New Virtual Machine 1	89%	2021-03-24 16:02:52	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x-000002-sesparse.vmdk		

If your migration is successful, you get a message similar to the following.

Run Direct									
<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	No	VMFS Run Direct Backup Set	10.120.8.40	DatacenterNew Virtual Machine 1	<div style="width: 100%; height: 10px; background-color: blue;"></div> 100%	2021-03-24 16:02:52		OK	

Restore log messages on AhsayCBS

Click on the restore item on the Run Direct page to see the restore log messages.

Timestamp	Type	Message
2021-03-24 04:09:47	info	Start manual migration...
2021-03-24 04:09:49	info	Loading information...
2021-03-24 04:10:24	info	Taking snapshot "__snapshot_for_migrate__" of virtual machine "New Virtual Machine 1"...
2021-03-24 04:10:42	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x-000001-sesparse.vmdk
2021-03-24 04:11:01	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x-000001.vmdk
2021-03-24 04:11:07	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x-flat.vmdk
2021-03-24 04:28:58	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x.vmdk
2021-03-24 04:29:05	info	Suspending virtual machine "New Virtual Machine 1"...
2021-03-24 04:29:22	info	Loading information...
2021-03-24 04:29:44	info	Removing virtual machine "New Virtual Machine 1" from the inventory...
2021-03-24 04:29:45	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x.nvram
2021-03-24 04:29:51	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x.vmsd
2021-03-24 04:29:57	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x.vmx
2021-03-24 04:30:01	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x.vmf
2021-03-24 04:30:02	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x-79064c22.vms
2021-03-24 04:30:31	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x-000002-sesparse.vmdk
2021-03-24 04:30:37	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x-000002.vmdk
2021-03-24 04:30:41	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x-Snapshot1.vmsn
2021-03-24 04:30:42	info	Migrating...[Datastore-SHR01 (1)] New Virtual Machine 1/Lubuntu12x-Snapshot2.vmsn
2021-03-24 04:30:48	info	Adding virtual machine "New Virtual Machine 1" to the inventory...
2021-03-24 04:31:16	info	Powering on virtual machine "New Virtual Machine 1"...
2021-03-24 04:31:23	info	Removing snapshot "__snapshot_for_migrate__" from virtual machine "New Virtual Machine 1"...
2021-03-24 04:32:33	info	Removing snapshot "__snapshot_for_publish__" from virtual machine "New Virtual Machine 1"...
2021-03-24 04:32:54	info	Unmount datastore "cbs-RunDirect"...
2021-03-24 04:32:57	info	Restore Completed Successfully

Restore log messages on the VMware vSphere Client

Open your VMware vSphere Client and you will see the following messages from the Recent Tasks section.

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion T...	Server
Create virtual machine snapshot	New Virtu...	Completed	VSPHERE.LOC...	15 ms	03/24/2021, 4:10:22 PM	03/24/2021, 4:10:38 PM	vCenter05-v65
Copy file	Datastore...	Completed	VSPHERE.LOC...	14 ms	03/24/2021, 4:11:05 PM	03/24/2021, 4:28:53 PM	vCenter05-v65
Suspend virtual machine	New Virtu...	Completed	VSPHERE.LOC...	11 ms	03/24/2021, 4:29:03 PM	03/24/2021, 4:29:16 PM	vCenter05-v65
Unregister virtual machine	New Virtu...	Completed	VSPHERE.LOC...	26 ms	03/24/2021, 4:29:43 PM	03/24/2021, 4:29:43 PM	vCenter05-v65
Copy file	Datastore...	Completed	VSPHERE.LOC...	27 ms	03/24/2021, 4:29:43 PM	03/24/2021, 4:29:45 PM	vCenter05-v65
Register virtual machine	Datscenter	Completed	VSPHERE.LOC...	16 ms	03/24/2021, 4:30:47 PM	03/24/2021, 4:30:51 PM	vCenter05-v65
Power On virtual machine	New Virtu...	Completed	VSPHERE.LOC...	13 ms	03/24/2021, 4:31:15 PM	03/24/2021, 4:31:20 PM	vCenter05-v65
Remove snapshot	New Virtu...	Completed	VSPHERE.LOC...	32 ms	03/24/2021, 4:32:32 PM	03/24/2021, 4:32:38 PM	vCenter05-v65
Delete file	Datastore...	Completed	VSPHERE.LOC...	8 ms	03/24/2021, 4:32:45 PM	03/24/2021, 4:32:47 PM	vCenter05-v65
Remove datastore	cbs-RunDi...	Completed	VSPHERE.LOC...		03/24/2021, 4:32:52 PM	03/24/2021, 4:32:53 PM	vCenter05-v65

11. Click X to exit when finished.

7.3.2 Restore a backup from VMFS datastore to vSAN datastore

1. Log in to AhsayCBS user web console according to the instruction provided in section [Logging on to AhsayCBS User Web Console](#).

NOTE

Before you can start Run Direct, you must have a VMware backup set created in the AhsayOBM client. Please refer to the [Ahsay Online Backup Manager v9 VMware vCenter/ESXi Backup & Restore Guide](#) for information on how to create the backup set. In addition, you must also run a successful backup on the VMware backup set before you can perform restore from Run Direct.

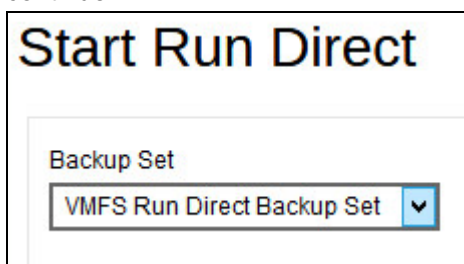
2. Click the **VM Run Direct** icon from your AhsayCBS environment.



3. Click **+** from the **Run Direct** page to start a new Run Direct session.



4. Select the **Backup Set** from the dropdown box of VMware backup set you have created. In our example, the backup set is called **VMFS Run Direct Backup Set**. Click **➔** to continue.



- Select the backup job to restore from the **Restore file of job** dropdown box. In our example, there are two virtual machines. Check the box next to the one on which we will perform a restore, **New Virtual Machine 2**.



Start Run Direct

Restore file of job: 2021-03-24-14-29-13

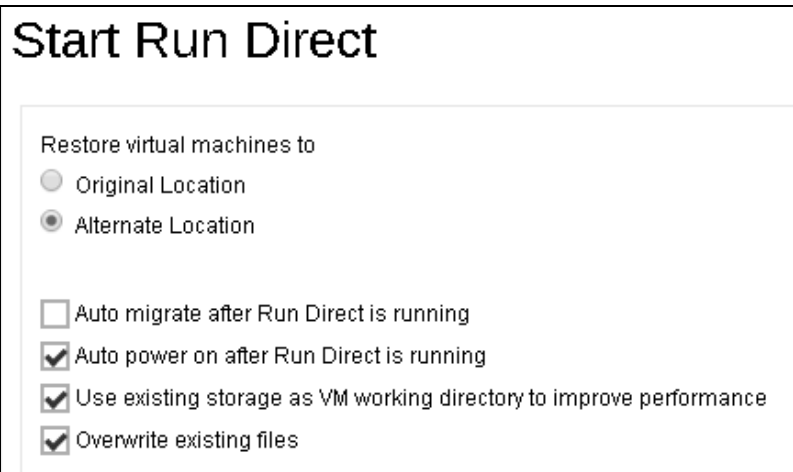
- vCenter05-v65
 - Datacenter
 - Hosts and Clusters
 - 10.16.8.42
 - Lubuntu12x
 - New Virtual Machine 2

- Select the location to restore your virtual machine. They are found under **Restore virtual machine to** on the **Start Run Direct** page.

Select **Alternate Location** to restore the VM to a different VMware host and a different datastore. Alternatively, you can also restore to the same VMware host but to a different datastore.

NOTE

If you select Alternate Location, you will see an additional option Overwrite existing files.



Start Run Direct

Restore virtual machines to

Original Location

Alternate Location

Auto migrate after Run Direct is running

Auto power on after Run Direct is running

Use existing storage as VM working directory to improve performance

Overwrite existing files

Configure the following options according to your restore requirements:

Auto migrate after Run Direct is running

Select this option if you want to auto migrate the virtual machine to a permanent location on the original VMware host, another VMware host, or same VMware host but another datastore, depending on whether you have chosen **Original Location** or **Alternate Location** to restore your VM

⦿ **Auto power on after Run Direct is running**


Select this option to power up the virtual machine automatically, after Run Direct is running for the VM.

⦿ **Use existing storage as VM working directory to improve performance**

Select this option to enhance performance of the restored VM.

⦿ **Overwrite existing files** (Alternate Location only)

Select this option to overwrite existing files when restoring to a different VMware host or a different datastore.

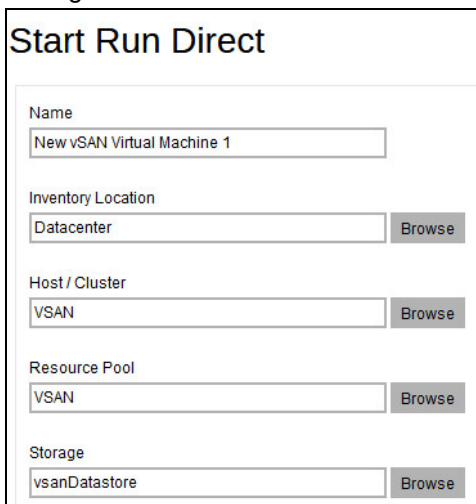
Click  to proceed when you are done with the settings.

7. Enter the VMware host and access information of where you would like the VM to be restored to. Select **VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7** as **Version**, then enter the **Username**, **Password**, **Host**, and **Port** of the new host.



The screenshot shows a dialog box titled "Start Run Direct". Under the "VMware Host" section, there are several input fields: "Version" is a dropdown menu set to "VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7.0"; "Username" is a text box containing "administrator"; "Password" is a text box with masked characters; "Host" is a text box containing "10.120.8.40"; and "Port" is a text box containing "443".

8. Enter a new **Name** for the VM, then **Browse** to modify the **Host/Cluster** and **Storage** settings to select the datastore.



The screenshot shows the same "Start Run Direct" dialog box. The "Name" field is now filled with "New vSAN Virtual Machine 1". Below it, there are four sections, each with a text box and a "Browse" button: "Inventory Location" (Datacenter), "Host / Cluster" (VSAN), "Resource Pool" (VSAN), and "Storage" (vsanDatastore).

Select the **Host / Cluster** and **Storage**.

10.16.8.42
 VSAN

datastore1 (2)
 datastore1 (3)
 datastore1 (4)
 datastore3
 vsanDatastore

NOTE

It is important to select the vSAN Host/Cluster as well as the vSAN datastore for the storage.

Click  to start the restore.

- The **Run Direct** page appears, showing the status message of the Run Direct restore job.

Run Direct										
<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate	
<input type="checkbox"/>	No	VMFS Run Direct Backup Set	10.120.8.40	Datacenter/New vSAN Virtual Machine 1		2021-03-25 12:17:34	Mount datastore "cbs-RunDirect" (192.168.7.101:cbsRunDirect)...			

If your Run Direct is successful, you get a message similar to the following, with Status showing OK and Progress showing 100%.

Run Direct										
<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate	
<input type="checkbox"/>	Yes	VMFS Run Direct Backup Set	10.120.8.40	Datacenter/New vSAN Virtual Machine 1	100%	2021-03-25 12:17:34		OK	Migrate	

Restore log messages on AhsayCBS

Click on the item on the Run Direct page.

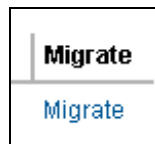
Timestamp	Type	Message
2021-03-25 12:18:20	info	Preparing for Run Direct...
2021-03-25 12:18:24	info	Mount datastore "cbs-RunDirect (192.168.7.101:cbsRunDirect)"...
2021-03-25 12:18:28	info	Adding virtual machine "New vSAN Virtual Machine 1" to the inventory...
2021-03-25 12:18:58	info	Taking snapshot "__snapshot_for_publish__" of virtual machine "New vSAN Virtual Machine 1"...
2021-03-25 12:19:06	info	Powering on virtual machine "New vSAN Virtual Machine 1"...
2021-03-25 12:19:17	info	Please do not Edit, Remove or Revert any existing snapshot before migration is completed.
2021-03-25 12:19:17	info	Restore Completed Successfully

Restore log messages on the VMware vSphere Client

Open your VMware vSphere Client and you will see the following messages from the Recent Tasks section.

Task Name	Target	Status	Initiator	Queu...	Start Time ↑	Completion Time
Create NAS datastore	10.16.8.47	✓ Completed	VSPHERE.LOCAL...	19 ms	03/25/2021, 12:1...	03/25/2021, 12:18:23
Register virtual machine	Datacent...	✓ Completed	VSPHERE.LOCAL...	8 ms	03/25/2021, 12:1...	03/25/2021, 12:18:32
Reload virtual machine	New vSA...	✓ Completed	VSPHERE.LOCAL...	10 ms	03/25/2021, 12:1...	03/25/2021, 12:18:37
Create virtual machine ...	New vSA...	✓ Completed	VSPHERE.LOCAL...	15 ms	03/25/2021, 12:1...	03/25/2021, 12:19:01
Power On virtual machi...	New vSA...	✓ Completed	VSPHERE.LOCAL...	5 ms	03/25/2021, 12:1...	03/25/2021, 12:19:11 PM

10. If you did not enable the **Auto Migrate after Run Direct is running** option in step 6, but still wish to migrate VM to a permanent location of your choice, click on the **Migrate** button as shown.



Run Direct									
Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate	
<input type="checkbox"/>	VMFS Run		Datacenter/New	<div style="width: 33%;"></div>	2021-03-25	Migrating...Relocate			
<input type="checkbox"/>	Direct Backup Set	10.120.8.40	vSAN Virtual Machine 1	33%	12:17:34	virtual machine "New vSAN Virtual Machine 1"			

If your migration is successful, you get a message similar to the following.

Run Direct									
Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate	
<input type="checkbox"/>	VMFS Run Direct Backup Set	10.120.8.40	Datacenter/New vSAN Virtual Machine 1	<div style="width: 100%;"></div>	2021-03-25		OK		

Restore log messages on AhsayCBS

Click on the restore item on the Run Direct page to see the restore log messages.

Timestamp	Type	Message
2021-03-25 12:27:40	info	Start auto migration...
2021-03-25 12:27:40	info	Migrating...Relocate virtual machine "New vSAN Virtual Machine 1"
2021-03-25 12:46:24	info	Removing snapshot "__snapshot_for_publish__" from virtual machine "New vSAN Virtual Machine 1"...
2021-03-25 12:46:47	info	Unmount datastore "cbs-RunDirect"...
2021-03-25 12:46:50	info	Restore Completed Successfully

Restore log messages on the VMware vSphere Client

Open your VMware vSphere Client and you will see the following messages from the Recent Tasks section.

Task Name	Target	Status	Initiator	Queu...	Start Time ↑	Completion Time
Create NAS datastore	10.16.8.47	✓ Completed	VSPHERE.LOCAL\...	19 ms	03/25/2021, 12:1...	03/25/2021, 12:18:23
Register virtual machine	Datacent...	✓ Completed	VSPHERE.LOCAL\...	7 ms	03/25/2021, 12:1...	03/25/2021, 12:18:32
Reload virtual machine	New vSA...	✓ Completed	VSPHERE.LOCAL\...	10 ms	03/25/2021, 12:1...	03/25/2021, 12:18:37
Create virtual machine ...	New vSA...	✓ Completed	VSPHERE.LOCAL\...	15 ms	03/25/2021, 12:1...	03/25/2021, 12:19:01
Power On virtual machi...	New vSA...	✓ Completed	VSPHERE.LOCAL\...	4 ms	03/25/2021, 12:1...	03/25/2021, 12:19:11 PM
Relocate virtual machine	New vSA...	✓ Completed	VSPHERE.LOCAL\...	28 ms	03/25/2021, 12:...	03/25/2021, 12:45:58
Remove snapshot	New vSA...	✓ Completed	VSPHERE.LOCAL\...	10 ms	03/25/2021, 12:...	03/25/2021, 12:46:42
Remove datastore	cbs-Run...	✓ Completed	VSPHERE.LOCAL\...	20 ms	03/25/2021, 12:...	03/25/2021, 12:46:46

11. Click X to exit when finished.

7.3.3 Restore a backup from vSAN datastore to vSAN datastore

1. Log in to AhsayCBS user web console according to the instruction provided in section [Logging on to AhsayCBS User Web Console](#).

NOTE

Before you can start Run Direct, you must have a VMware backup set created in the AhsayOBM client. Please refer to the [Ahsay Online Backup Manager v9 VMware vCenter/ESXi Backup & Restore Guide](#) for information on how to create the backup set. In addition, you must also run a successful backup on the VMware backup set before you can perform restore from Run Direct.

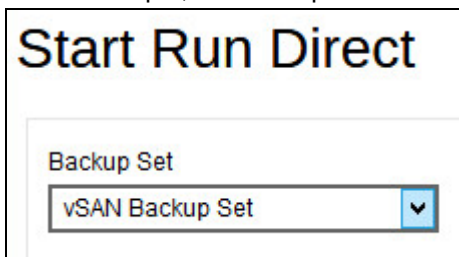
2. Click the **VM Run Direct** icon from your AhsayCBS environment.



3. Click **+** from the **Run Direct** page to start a new Run Direct session.



4. Select the **Backup Set** from the dropdown box of VMware backup set you have created. In our example, the backup set is called **vSAN Backup Set**. Click **➔** to continue.



5. Select the backup job to restore from the **Restore file of job** dropdown box. In our example, the virtual machine is named **Ubuntu 12.04 LTS**. Check the box next to it.



Start Run Direct

Restore file of job 2021-03-09-16-53-59

- vCenter05-v65
 - Datacenter
 - Hosts and Clusters
 - VSAN
 - Ubuntu 12.04 LTS

6. Select the location to restore your virtual machine. They are found under **Restore virtual machine to** on the **Start Run Direct** page.

Select to restore the VM to its **Original Location**.

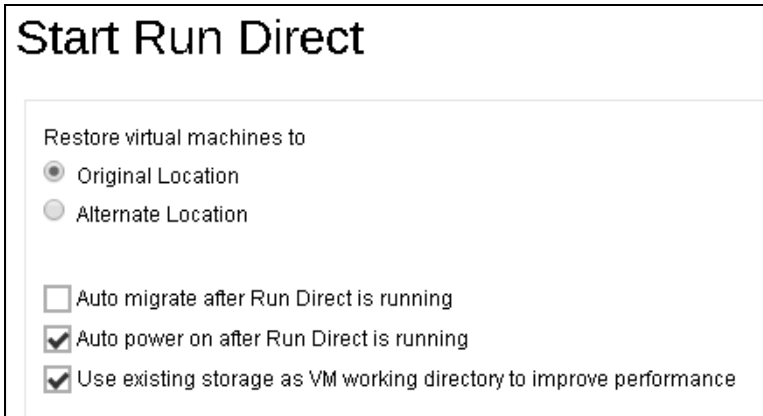


Start Run Direct

Restore virtual machines to

- Original Location
- Alternate Location

7. Configure the following options according to your restore requirements.



Start Run Direct

Restore virtual machines to

- Original Location
- Alternate Location

- Auto migrate after Run Direct is running
- Auto power on after Run Direct is running
- Use existing storage as VM working directory to improve performance

Auto migrate after Run Direct is running

Select this option if you want to auto migrate the virtual machine to a permanent location on the original VMware host, another VMware host, or same VMware host but another datastore, depending on whether you have chosen **Original Location** or **Alternate Location** to restore your VM.

Auto power on after Run Direct is running

Select this option to power up the virtual machine automatically, after Run Direct is running for the VM.

⦿ **Use existing storage as VM working directory to improve performance**

Select this option to enhance performance of the restored VM.

Click  to start the restore.

- The **Run Direct** page appears, showing the status message of the Run Direct restore job.

Run Direct									
<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	No	vSAN Backup Set	10.120.8.40	Datacenter/New vSAN Virtual Machine 2		2021-03-25 13:27:05	Mount datastore "cbs-RunDirect (192.168.7.101:cbsRunDirect)"...		

If your Run Direct is successful, you get a message similar to the following, with Status showing OK and Progress showing 100%.

Run Direct									
<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	Yes	vSAN Backup Set	10.120.8.40	Datacenter/New vSAN Virtual Machine 2	100%	2021-03-25 13:27:05		OK	Migrate

Restore log messages on AhsayCBS

Click on the item on the Run Direct page.

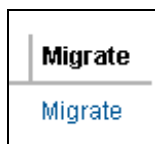
Timestamp	Type	Message
2021-03-25 01:27:55	info	Preparing for Run Direct...
2021-03-25 01:27:58	info	Mount datastore "cbs-RunDirect (192.168.7.101:cbsRunDirect)"...
2021-03-25 01:28:03	info	Adding virtual machine "New vSAN Virtual Machine 2" to the inventory...
2021-03-25 01:28:41	info	Taking snapshot "__snapshot_for_publish__" of virtual machine "New vSAN Virtual Machine 2"...
2021-03-25 01:28:49	info	Please do not Edit, Remove or Revert any existing snapshot before migration is completed.
2021-03-25 01:28:49	info	Restore Completed Successfully

Restore log messages on the VMware vSphere Client

Open your VMware vSphere Client and you will see the following messages from the Recent Tasks section.

Task Name	Target	Status	Initiator	Queu...	Start Time ↑	Completion Time
Create NAS datastore	10.16.8.47	✓ Completed	VSPHERE.LOCAL...	10 ms	03/25/2021, 1:2...	03/25/2021, 1:27:57 PM ^
Register virtual machine	Datacent...	✓ Completed	VSPHERE.LOCAL...	282 ms	03/25/2021, 1:2...	03/25/2021, 1:28:08 P
Reload virtual machine	New vSA...	✓ Completed	VSPHERE.LOCAL...	15 ms	03/25/2021, 1:2...	03/25/2021, 1:28:15 PM
Create virtual machine ...	New vSA...	✓ Completed	VSPHERE.LOCAL...	9 ms	03/25/2021, 1:2...	03/25/2021, 1:28:45 P

- If you did not enable the **Auto Migrate after Run Direct is running** option in step 6, but still wish to migrate VM to a permanent location of your choice, click on the **Migrate** button as shown.



Run Direct

<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	No	vSAN Backup Set	10.120.8.40	Datcenter/New vSAN Virtual Machine 2	<div style="width: 35%;"></div> 35%	2021-03-25 13:27:05	Migrating...Relocate virtual machine "New vSAN Virtual Machine 2"		

If your migration is successful, you get a message similar to the following.

Run Direct

<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	No	vSAN Backup Set	10.120.8.40	Datcenter/New vSAN Virtual Machine 2	<div style="width: 100%;"></div> 100%	2021-03-25 13:27:05		OK	

Restore log messages on AhsayCBS

Click on the restore item on the Run Direct page to see the restore log messages.

Timestamp	Type	Message
2021-03-25 01:31:43	info	Start auto migration...
2021-03-25 01:31:43	info	Migrating...Relocate virtual machine "New vSAN Virtual Machine 2"
2021-03-25 01:49:07	info	Removing snapshot "__snapshot_for_publish_" from virtual machine "New vSAN Virtual Machine 2"...
2021-03-25 01:49:20	info	Unmount datastore "cbs-RunDirect"...
2021-03-25 01:49:23	info	Restore Completed Successfully

Restore log messages on the VMware vSphere Client

Open your VMware vSphere Client and you will see the following messages from the Recent Tasks section.

Task Name	Target	Status	Initiator	Queu...	Start Time ↑	Completion Time
Create NAS datastore	10.16.8.47	Completed	VSPHERE.LOCAL\...	9 ms	03/25/2021, 1:2...	03/25/2021, 1:27:57 PM
Register virtual machine	Datacent...	Completed	VSPHERE.LOCAL\...	282 ms	03/25/2021, 1:2...	03/25/2021, 1:28:08 P...
Reload virtual machine	New vSA...	Completed	VSPHERE.LOCAL\...	14 ms	03/25/2021, 1:2...	03/25/2021, 1:28:15 PM
Create virtual machine ...	New vSA...	Completed	VSPHERE.LOCAL\...	9 ms	03/25/2021, 1:2...	03/25/2021, 1:28:45 P...
Relocate virtual machine	New vSA...	Completed	VSPHERE.LOCAL\...	8 ms	03/25/2021, 1:31...	03/25/2021, 1:48:41 PM
Remove snapshot	New vSA...	Completed	VSPHERE.LOCAL\...	9 ms	03/25/2021, 1:4...	03/25/2021, 1:49:12 PM
Remove datastore	cbs-Run...	Completed	VSPHERE.LOCAL\...	28 ms	03/25/2021, 1:4...	03/25/2021, 1:49:19 PM

10. Click **X** to exit when finished.

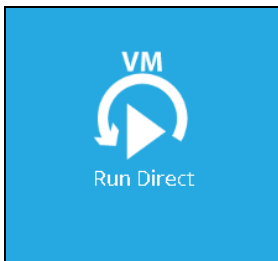
7.3.4 Restore a backup from vSAN datastore to VMFS datastore

1. Log in to AhsayCBS user web console according to the instruction provided in section [Logging on to AhsayCBS User Web Console](#).

NOTE

Before you can start Run Direct, you must have a VMware backup set created in the AhsayOBM client. Please refer to the [Ahsay Online Backup Manager v9 VMware vCenter/ESXi Backup & Restore Guide](#) for information on how to create the backup set. In addition, you must also run a successful backup on the VMware backup set before you can perform restore from Run Direct.

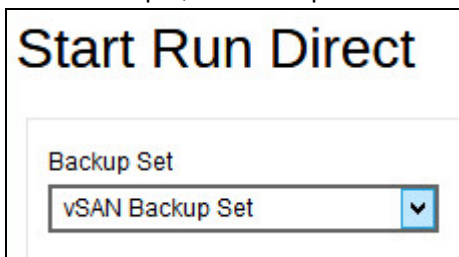
2. Click the **VM Run Direct** icon from your AhsayCBS environment.



3. Click **+** from the **Run Direct** page to start a new Run Direct session.



4. Select the **Backup Set** from the dropdown box of VMware backup set you have created. In our example, the backup set is called **vSAN Backup Set**. Click **➔** to continue.



- Select the backup job to restore from the **Restore file of job** dropdown box. In our example, the virtual machine is named **Ubuntu 12.04 LTS**. Check the box next to it.

Start Run Direct

Restore file of job: 2021-03-09-16-53-59

- vCenter05-v65
 - Datacenter
 - Hosts and Clusters
 - VSAN
 - Ubuntu 12.04 LTS

- Select the location to restore your virtual machine. They are found under **Restore virtual machine to** on the **Start Run Direct** page.

Select **Alternate Location** to restore the VM to a different VMware host and a different datastore. Alternatively, you can also restore to the same VMware host but to a different datastore.

NOTE

If you select Alternate Location, you will see an additional option Overwrite existing files.

Start Run Direct

Restore virtual machines to

Original Location

Alternate Location

Auto migrate after Run Direct is running

Auto power on after Run Direct is running

Use existing storage as VM working directory to improve performance

Overwrite existing files

Configure the following options according to your restore requirements:


- Auto migrate after Run Direct is running**
 Select this option if you want to auto migrate the virtual machine to a permanent location on the original VMware host, another VMware host, or same VMware host but another datastore, depending on whether you have chosen **Original Location** or **Alternate Location** to restore your VM
- Auto power on after Run Direct is running**
 Select this option to power up the virtual machine automatically, after Run Direct is running for the VM.

- ◉ **Use existing storage as VM working directory to improve performance**

Select this option to enhance performance of the restored VM.

- ◉ **Overwrite existing files** (Alternate Location only)

Select this option to overwrite existing files when restoring to a different VMware host or a different datastore.

Click  to proceed when you are done with the settings.

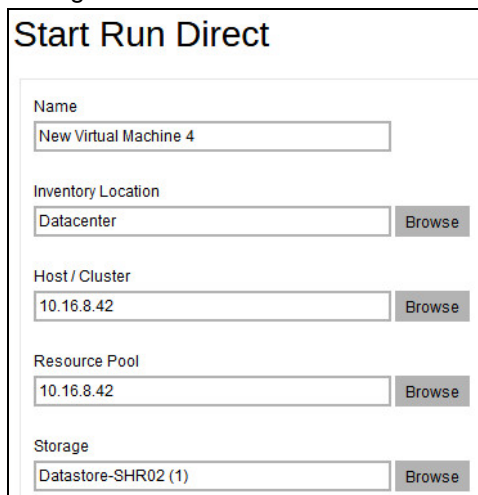
7. Enter the VMware host and access information of where you would like the VM to be restored to. Select **VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7** as **Version**, then enter the **Username**, **Password**, **Host**, and **Port** of the new host.



The screenshot shows a dialog box titled "Start Run Direct" with a section for "VMware Host". It contains the following fields:

- Version:** A dropdown menu with the selected value "VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7.0".
- Username:** A text input field containing "administrator".
- Password:** A text input field with masked characters (dots).
- Host:** A text input field containing "10.120.8.40".
- Port:** A text input field containing "443".

8. Enter a new **Name** for the VM, then **Browse** to modify the **Host/Cluster** and **Storage** settings to select the datastore.



The screenshot shows a dialog box titled "Start Run Direct" with the following fields and buttons:

- Name:** A text input field containing "New Virtual Machine 4".
- Inventory Location:** A text input field containing "Datacenter" and a "Browse" button.
- Host / Cluster:** A text input field containing "10.16.8.42" and a "Browse" button.
- Resource Pool:** A text input field containing "10.16.8.42" and a "Browse" button.
- Storage:** A text input field containing "Datastore-SHR02 (1)" and a "Browse" button.

Select the **Host / Cluster** and **Storage**.



The screenshot shows a radio button selection interface with two options:

- 10.16.8.42**
- VSAN**

Datastore-SHR01 (1)
 Datastore-SHR02 (1)
 datastore1

Click  to start the restore.

- The **Run Direct** page appears, showing the status message of the Run Direct restore job.

Run Direct									
<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	No	vSAN Backup Set	10.120.8.40	Datcenter/New Virtual Machine 4		2021-03-25 11:42:34	Mount datastore "cbs-RunDirect (192.168.7.101:cbsRunDirect)"...		

If your Run Direct is successful, you get a message similar to the following, with Status showing OK and Progress showing 100%.

Run Direct									
<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	Yes	vSAN Backup Set	10.120.8.40	Datcenter/New Virtual Machine 4	100%	2021-03-25 11:42:34		OK	Migrate

Restore log messages on AhsayCBS

Click on the item on the Run Direct page.

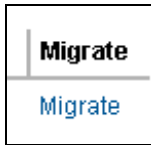
Timestamp	Type	Message
2021-03-25 11:43:21	info	Preparing for Run Direct...
2021-03-25 11:43:25	info	Mount datastore "cbs-RunDirect (192.168.7.101:cbsRunDirect)"...
2021-03-25 11:43:30	info	Adding virtual machine "New Virtual Machine 4" to the inventory...
2021-03-25 11:44:08	info	Taking snapshot "__snapshot_for_publish__" of virtual machine "New Virtual Machine 4"...
2021-03-25 11:44:22	info	Powering on virtual machine "New Virtual Machine 4"...
2021-03-25 11:44:39	info	Please do not Edit, Remove or Revert any existing snapshot before migration is completed.
2021-03-25 11:44:39	info	Restore Completed Successfully

Restore log messages on the VMware vSphere Client

Open your VMware vSphere Client and you will see the following messages from the Recent Tasks section.

Task Name	Target	Status	Initiator	Queu...	Start Time ↑	Completion Time
Create NAS datastore	10.16.8.42	Completed	VSPHERE.LOCAL...	33 ms	03/25/2021, 11:4...	03/25/2021, 11:43:25 A
Register virtual machine	Datacent...	Completed	VSPHERE.LOCAL...	7 ms	03/25/2021, 11:4...	03/25/2021, 11:43:38 A
Reload virtual machine	New Virt...	Completed	VSPHERE.LOCAL...	7 ms	03/25/2021, 11:4...	03/25/2021, 11:43:48 A
Create virtual machine ...	New Virt...	Completed	VSPHERE.LOCAL...	29 ms	03/25/2021, 11:4...	03/25/2021, 11:44:13 A
Power On virtual machi...	New Virt...	Completed	VSPHERE.LOCAL...	28 ms	03/25/2021, 11:4...	03/25/2021, 11:44:34 A

10. If you did not enable the **Auto Migrate after Run Direct is running** option in step 6, but still wish to migrate VM to a permanent location of your choice, click on the **Migrate** button as shown.



Run Direct									
<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	No	vSAN Backup Set	10.120.8.40	Datacenter/New Virtual Machine 4	36%	2021-03-25 11:42:34	Migrating...Relocate virtual machine "New Virtual Machine 4"		

If your migration is successful, you get a message similar to the following.

Run Direct									
<input type="checkbox"/>	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
<input type="checkbox"/>	No	vSAN Backup Set	10.120.8.40	Datacenter/New Virtual Machine 4	100%	2021-03-25 11:42:34		OK	

Restore log messages on AhsayCBS

Click on the restore item on the Run Direct page to see the restore log messages.

Timestamp	Type	Message
2021-03-25 11:47:43	info	Start auto migration...
2021-03-25 11:47:43	info	Migrating...Relocate virtual machine "New Virtual Machine 4"
2021-03-25 12:01:18	info	Removing snapshot "__snapshot_for_publish_" from virtual machine "New Virtual Machine 4"...
2021-03-25 12:01:26	info	Unmount datastore "cbs-RunDirect"...
2021-03-25 12:01:32	info	Restore Completed Successfully

Restore log messages on the VMware vSphere Client

Open your VMware vSphere Client and you will see the following messages from the Recent Tasks section.

Task Name	Target	Status	Initiator	Queu...	Start Time ↑	Completion Time
Create virtual machine ...	New Virt...	✓ Completed	VSPHERE.LOCAL...	29 ms	03/25/2021, 11:4...	03/25/2021, 11:44:13 A
Power On virtual machi...	New Virt...	✓ Completed	VSPHERE.LOCAL...	27 ms	03/25/2021, 11:4...	03/25/2021, 11:44:34 A
Relocate virtual machine	New Virt...	✓ Completed	VSPHERE.LOCAL...	34 ms	03/25/2021, 11:4...	03/25/2021, 12:00:49 f
Remove snapshot	New Virt...	✓ Completed	VSPHERE.LOCAL...	25 ms	03/25/2021, 12:...	03/25/2021, 12:01:20 P
Remove datastore	cbs-Run...	✓ Completed	VSPHERE.LOCAL...	7 ms	03/25/2021, 12:...	03/25/2021, 12:01:25 P

11. Click **X** to exit when finished.

8 Contacting Ahsay

8.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the Partner Portal:

<https://www.ahsay.com/partners/>

Also use the Ahsay Wikipedia for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:

<https://wiki.ahsay.com/>

8.2 Documentation

Documentations for all Ahsay products are available at:

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

You can send us suggestions for improvements or report on issues in the documentation, by contacting us at:

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

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

Appendix

Appendix A Set Backup Destination on AhsayOBM for Backup Sets Created on AhsayCBS User Web Console

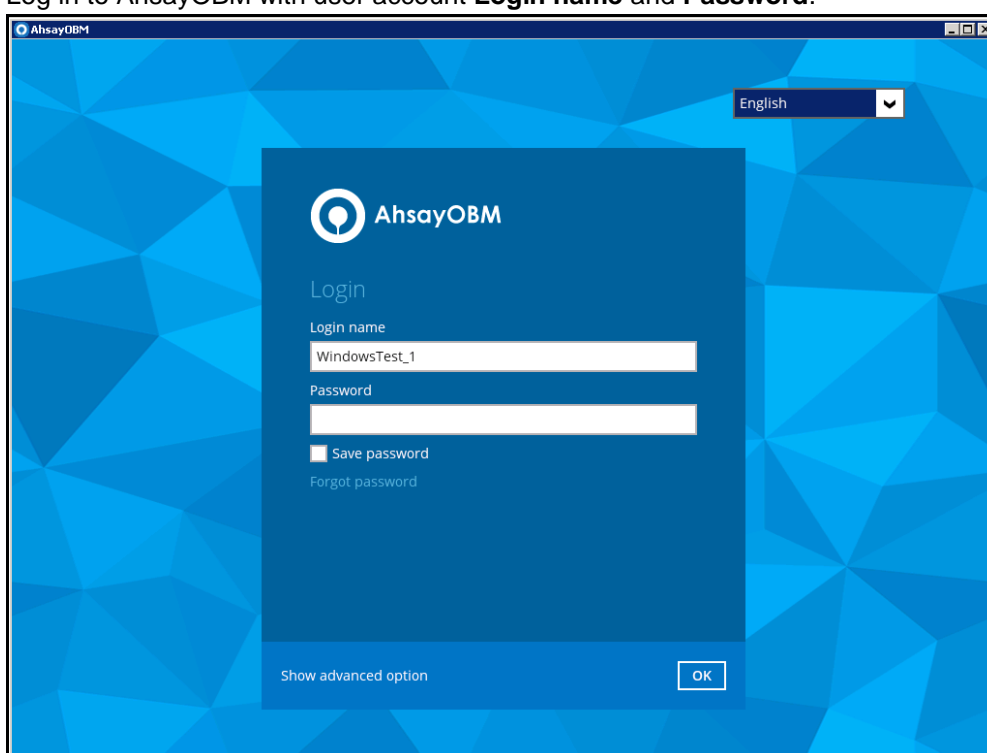
You need to read the instructions below only if you:

- Have created a backup set on AhsayCBS User Web Console; **AND**
- Selected the backup set to Run on Client (if you are running Microsoft 365 Backup and Cloud File Backup Set); **AND**
- Have not selected any Predefined Destination in the backup creation process on the AhsayCBS User Web Console

-OR-

Have selected a Predefined Destination in the backup creation process on AhsayCBS User Web Console but wish to add additional backup destination other than the predefined destination.

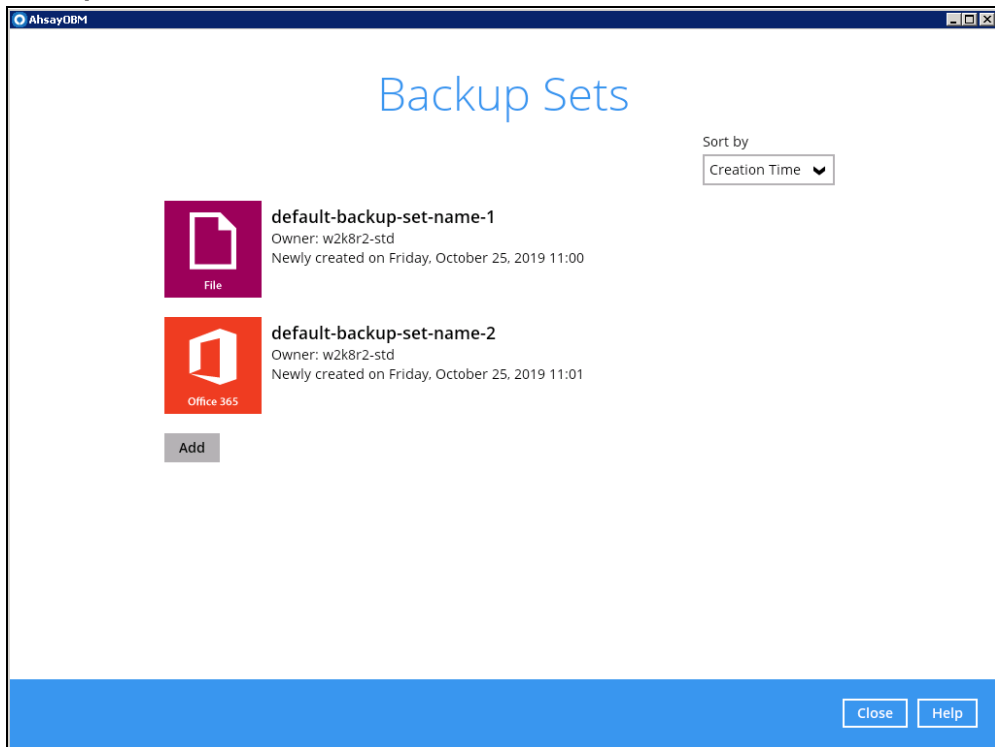
1. Log in to AhsayOBM with user account **Login name** and **Password**.



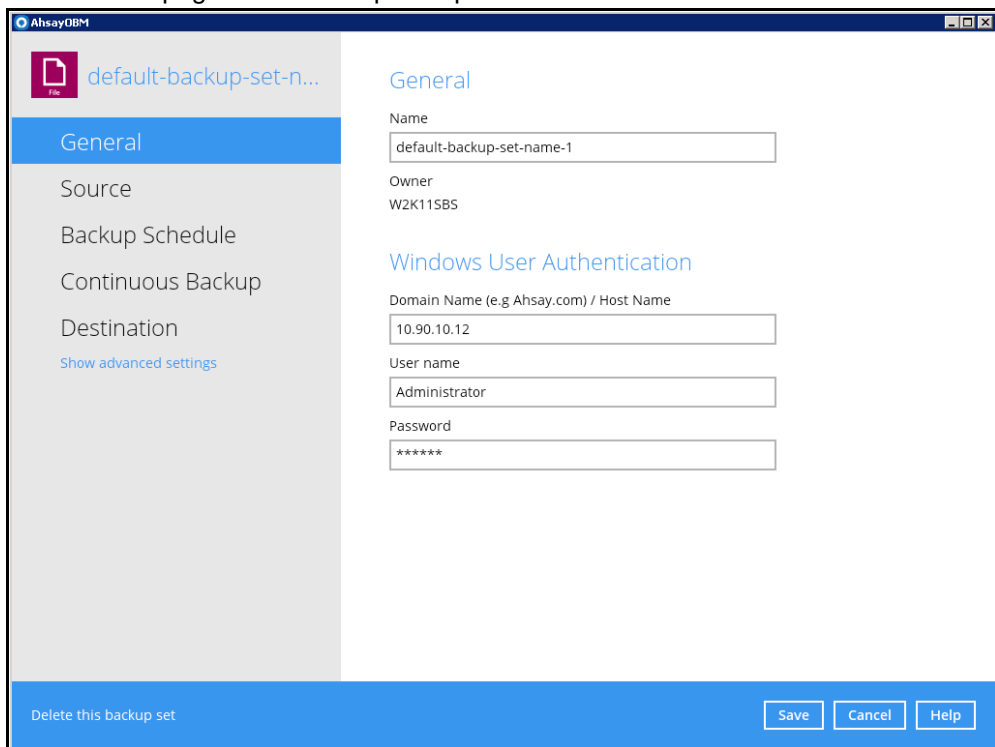
2. Click the **Backup Sets** button to open the backup sets.



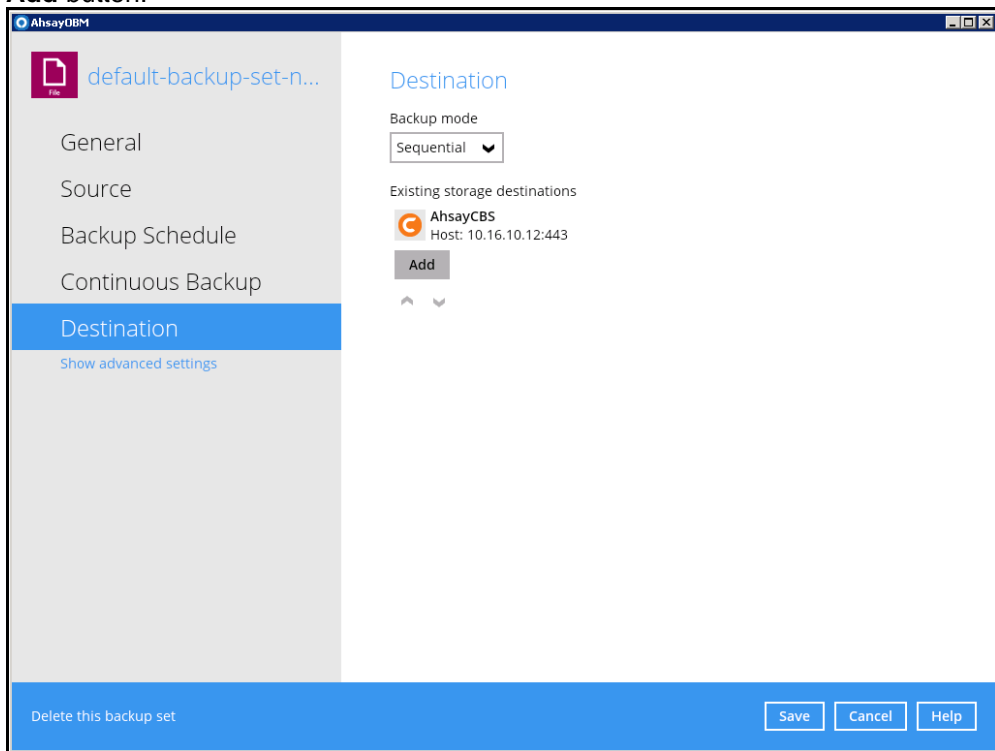
3. Select the backup set you want. In our example, the backup set is called **default-backup-set-name-1**.



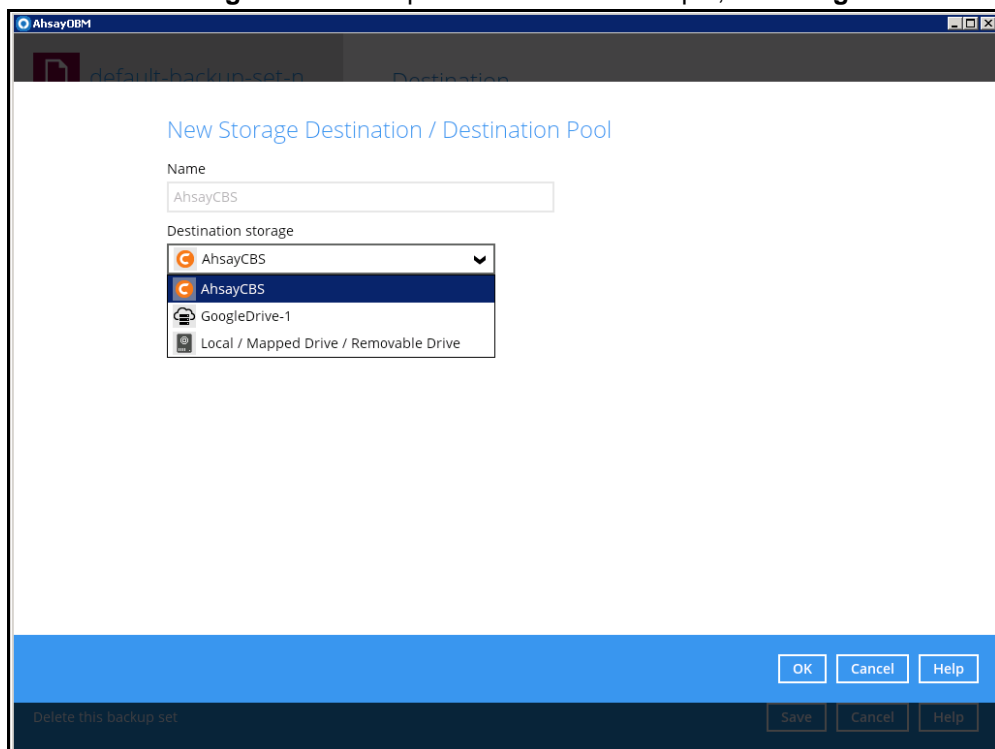
4. The General page of the backup set opens.



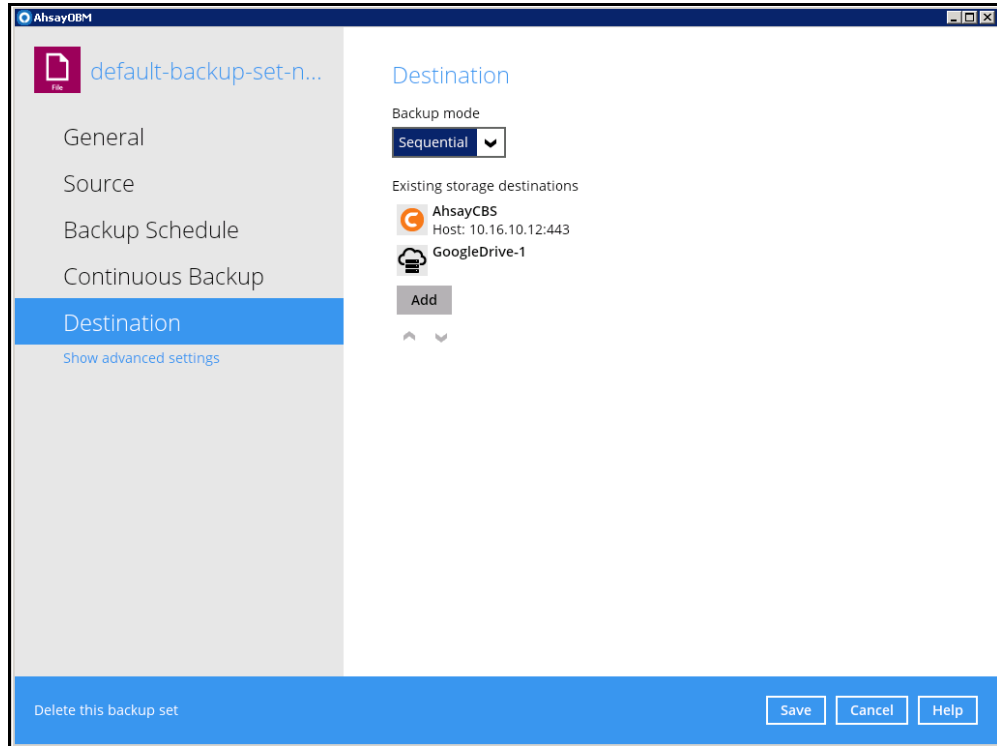
5. Go to the **Destination** page. You can add extra storage destinations here. Click the **Add** button.



6. Add a new destination on the New Storage Destination / Destination Pool. Select the **Destination storage** from the dropdown list. In our example, it is **GoogleDrive-1**.



7. The new storage destination, **GoogleDrive-1**, can be seen on the Destination page.



8. Click on **Save** to save the modification.