Ahsay™ Ahsay Backup

Ahsay Cloud Backup Suite v8

User's Guide

Ahsay Systems Corporation Limited

11 October 2021

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

Copyright Notice

Trademarks

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

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

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

Dropbox is a registered trademark of Dropbox Inc.

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

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

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

MariaDB is a registered trademark of MariaDB Corporation AB.

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

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

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

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

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

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

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

Ubuntu is a registered trademark of Canonical Ltd.

ShadowProtect is a registered trademark of StorageCraft Technology Corporation.

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

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

Disclaimer

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

Revision History

Date	Descriptions	Type of modification
25 March 2021	Updated Ch. 1.4.2, 1.4.2.1 and 1.4.2.2; Added storage statistics calculation in Ch. 2.6; Added different run direct restore scenarios in Ch. 5.3	Modification
30 April 2021	Updated discussion on storage statistic in Ch. 2.6; Updated diagram in Ch. 5.1	Modification
18 June 2021	Added note on VM Run Direct tile in Ch. 1.4; Updated screenshot in Ch. 1.6;	New / Modification
9 August 2021	Updated windows user authentication discussion in Ch. 4.1	Modification
11 October 2021	Added how to register device in Ch. 2; Moved login instructions to Ch. 3; Added unable to login instructions in Ch. 4; Updated authentication tab in Ch. 5.3.5	New / Modification

Table of Contents

1 Overview

1.1 Introduction

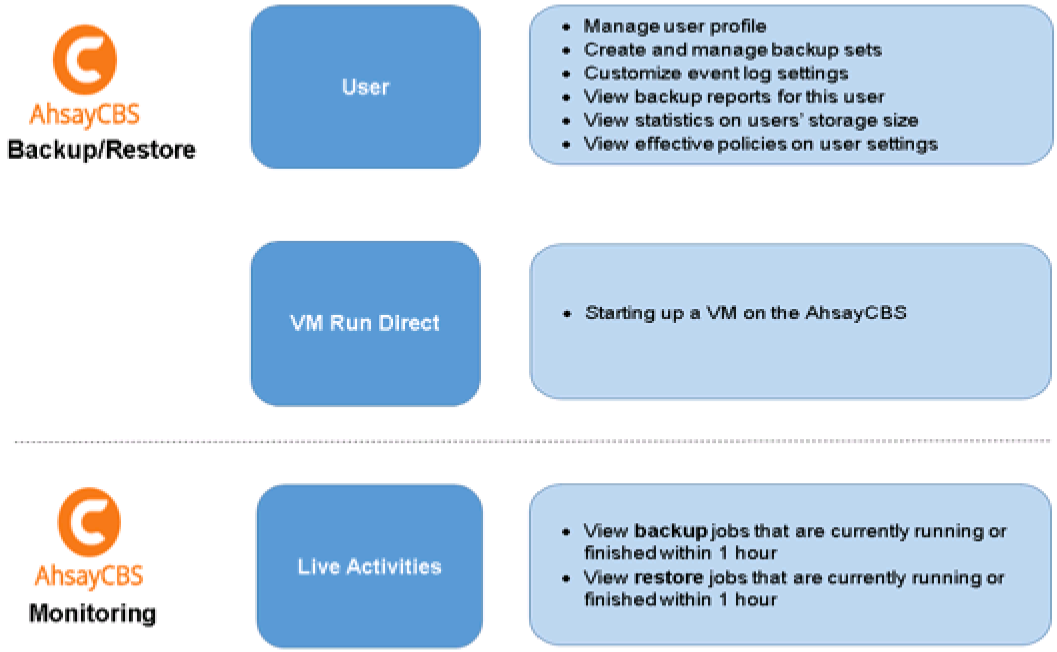
What is this software?

Ahsay Cloud Backup Suite v8 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.



- Manage user profile
- Create and manage backup sets
- Customize event log settings
- View backup reports for this user
- View statistics on users' storage size
- View effective policies on user settings

- Starting up a VM on the AhsayCBS

- View **backup** jobs that are currently running or finished within 1 hour
- View **restore** jobs that are currently running or finished within 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

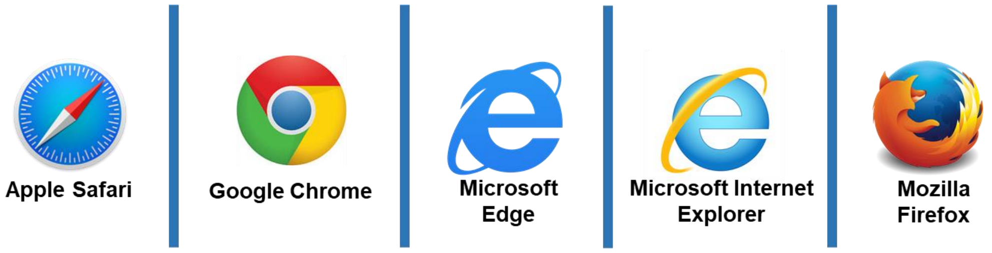
In order to use the AhsayCBS user web console, you need the following:

- **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.



- **AhsayCBS login account**

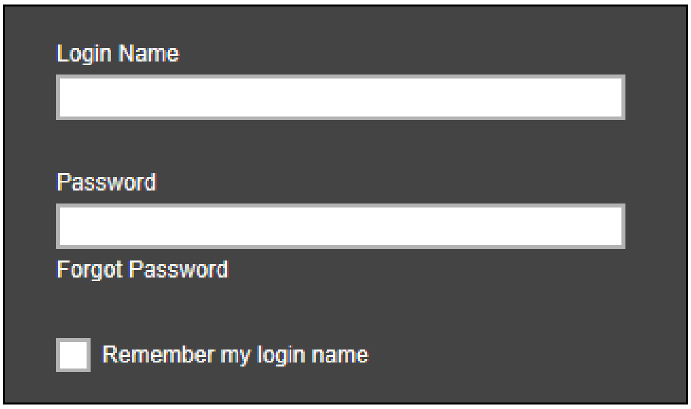
  You need an AhsayCBS login account to access the AhsayCBS server component.

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

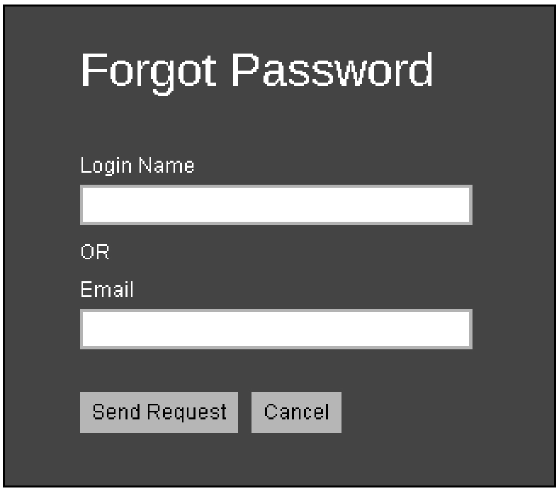
1.4 Resetting Your Password

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

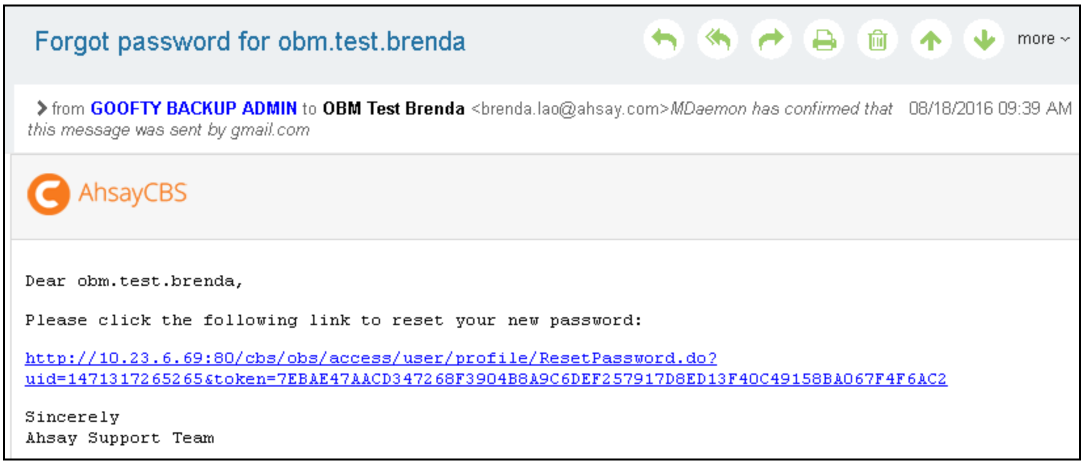
1. On the AhsayCBS Logon page, click **Forgot Password**.



2. The following screen appears. Enter either your **Login Name** or your **Email** to reset the password. Click **Send Request**. Ensure that you have included your e-mail address on the Manage Contact Information upon the creation of user profile. For further details, this will be discussed on Ch. 5.3 User Profile, Contact Tab.



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



Forgot password for obm.test.brenda

from GOOFTY BACKUP ADMIN to OBM Test Brenda <brenda.lao@ahsay.com> *MDaemon has confirmed that this message was sent by gmail.com* 08/18/2016 09:39 AM

AhsayCBS

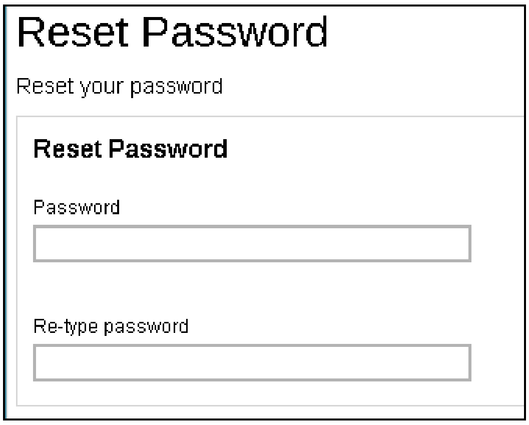
```
Dear obm.test.brenda,

Please click the following link to reset your new password:

http://10.23.6.69:80/cbs/obs/access/user/profile/ResetPassword.do?
uid=1471317265265&token=7EBAE47AACD34726 8F3904B8A9C6DEF257917D8ED13F40C49158BA067F4F6AC2

Sincerely
Ahsay Support Team
```

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

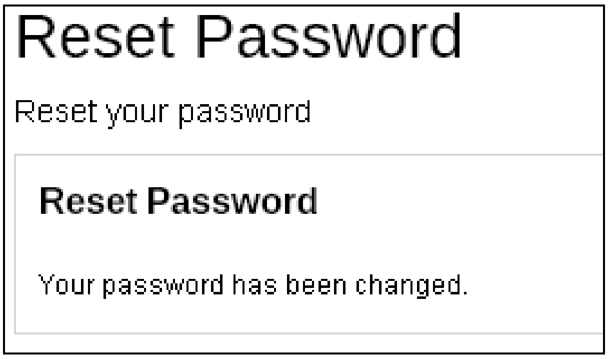


Reset Password

Reset your password

Reset Password

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



Reset Password

Reset your password

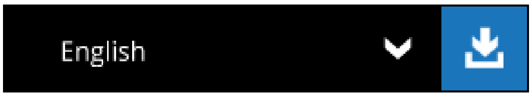
Reset Password

Your password has been changed.

1.5 Downloading Software

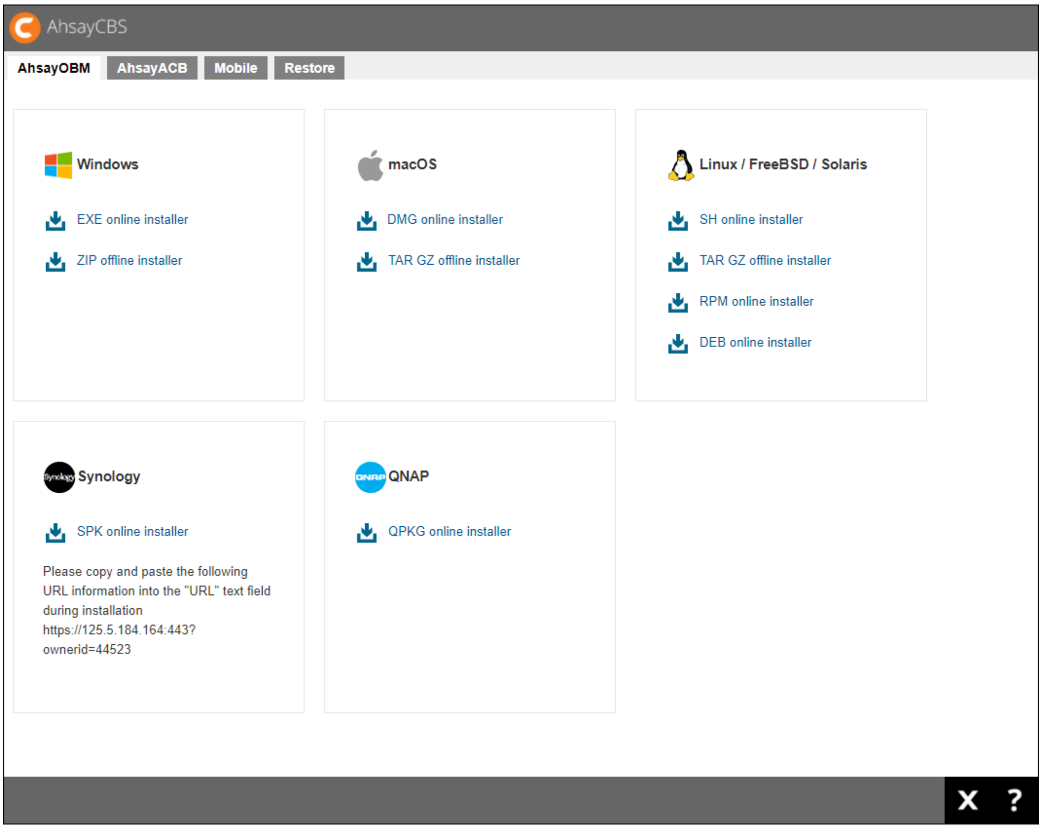
You can choose what client software you wish to download as follows:

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.



Please copy and paste the following URL information into the "URL" text field during installation https://125.5.184.164:443?ownerid=44523

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 Office 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 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, Office365, 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	➢ 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.	➢ 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	➢ 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	➢ Suitable for single or small amount of device installations. ➢ Suitable for client sites with fast and stable internet connection.	➢ 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.

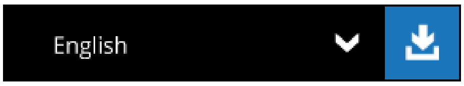
NOTE

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

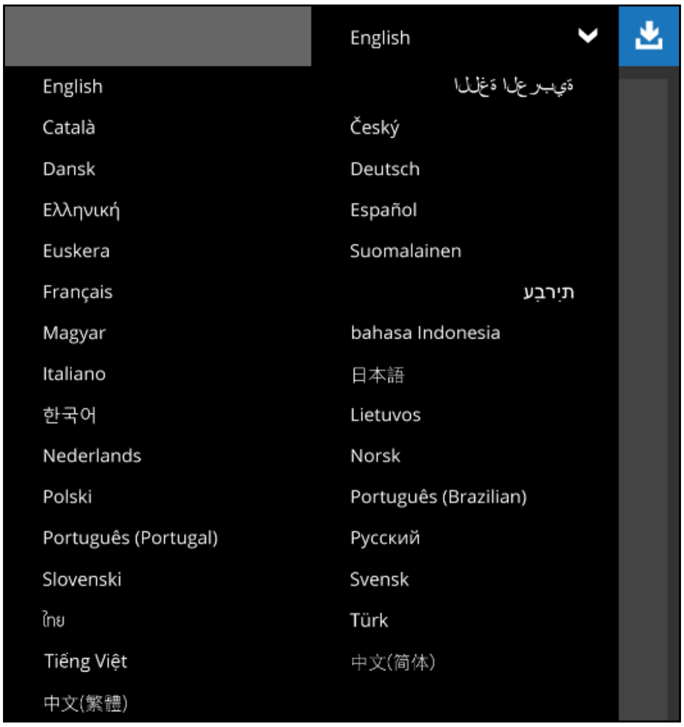
The available languages are:

- 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.



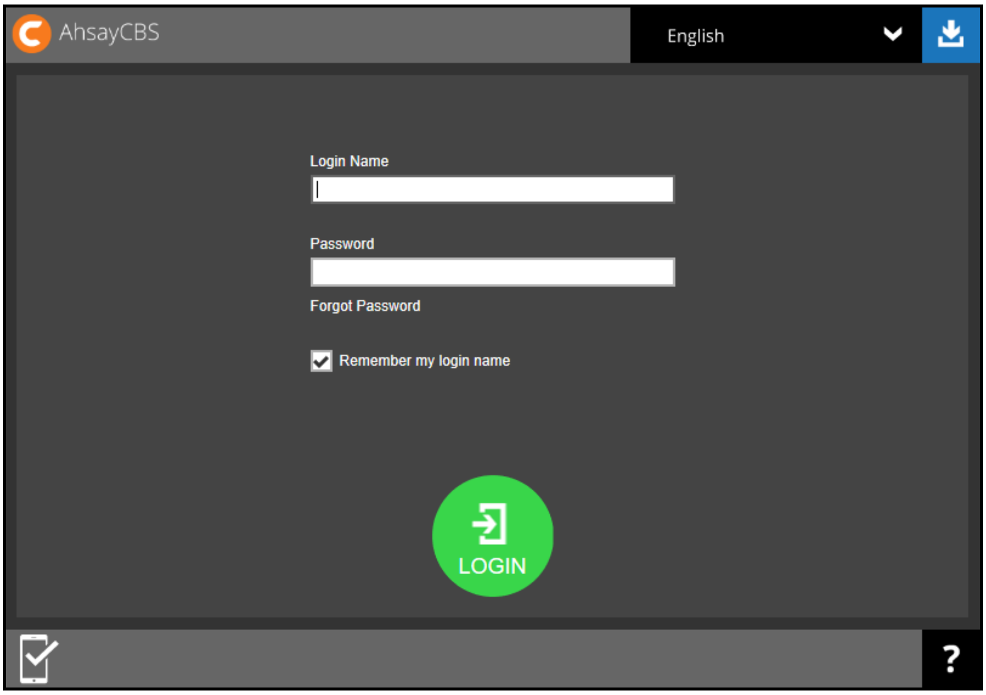
2. A list of available language is displayed for your choice.



1.7 Invoking Online Help

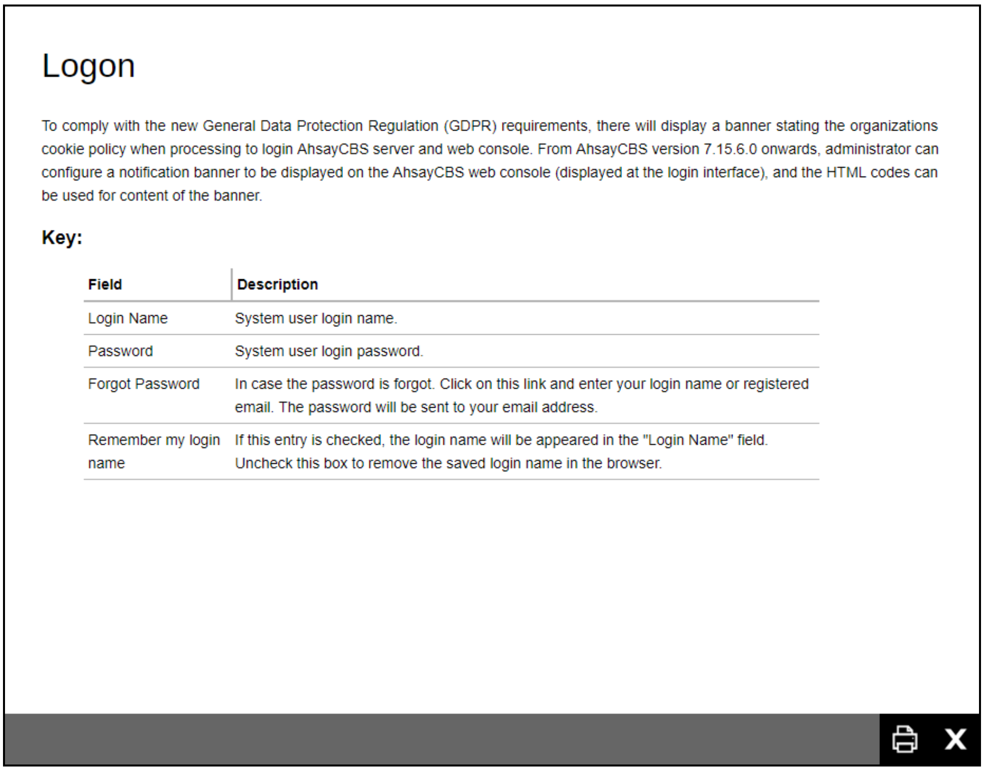
You can invoke the online help if you have problems logging in to the AhsayCBS server.

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 Register Device for 2FA in AhsayCBS

Upon logging in to AhsayCBS for the first time with two-factor authentication (2FA) enabled, you are required to register a device that will be used for 2FA to proceed with the login.

Starting with AhsayCBS v8.5.4.20 and above, there are four types of authenticator apps that can be used for 2FA, which are:

- Ahsay Mobile or branded Mobile app
- Microsoft Authenticator
- Google Authenticator
- Third party authenticators

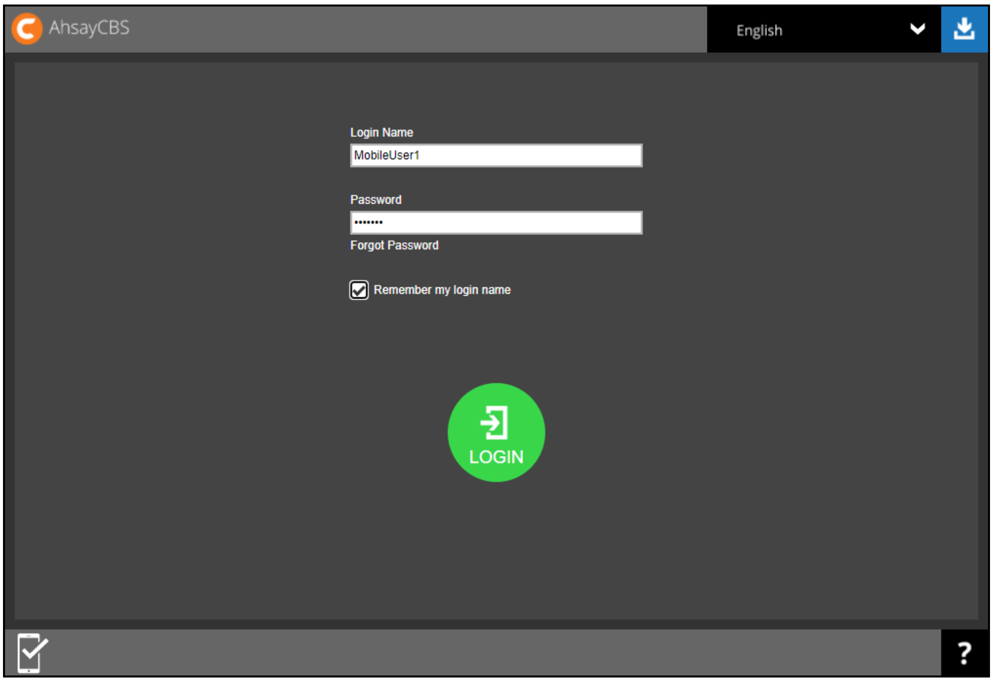
The authenticator app that will be available depends on the settings made by your backup service provider.

Instructions on how to register your device for 2FA will be discussed in detail for each authenticator app in the succeeding sub-chapters. First follow these login steps to register your device for 2FA then refer to the sub-chapter which cover the details of the registration for the authenticator app that you are using.

1. Login 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**.



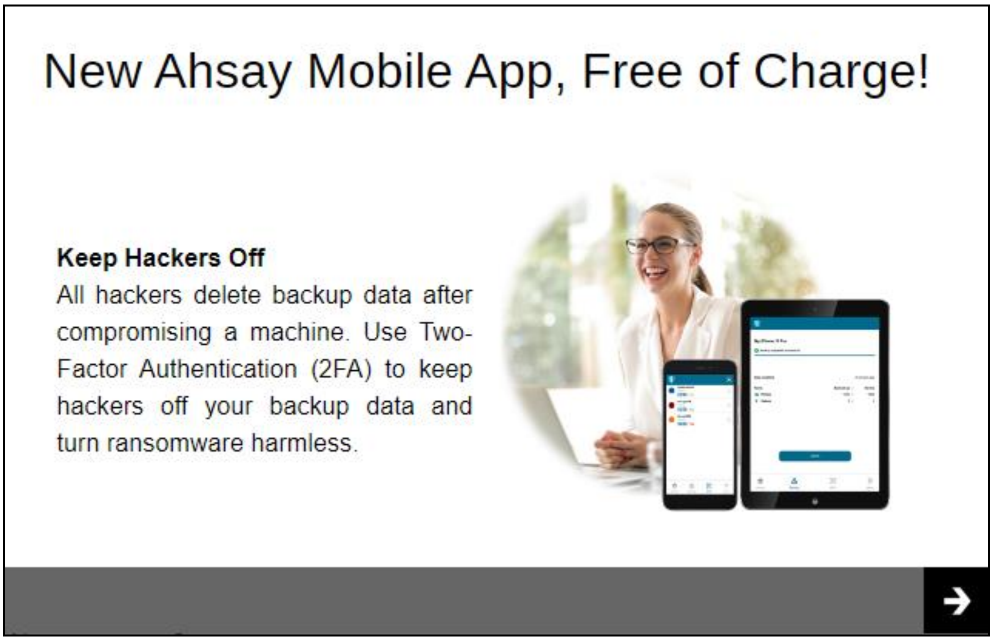
Login Name: MobileUser1

Password: •••••••

Forgot Password

☑ Remember my login name

3. To set up your two-factor authentication, click ➔ to proceed with setting up your 2FA.



New Ahsay Mobile App, Free of Charge!

Keep Hackers Off

All hackers delete backup data after compromising a machine. Use Two-Factor Authentication (2FA) to keep hackers off your backup data and turn ransomware harmless.

NOTE

This screen may not be displayed, this is dependent on the settings made by your backup service provider.

4. Follow the steps in the sub-chapter which covers the authenticator app that you are using:

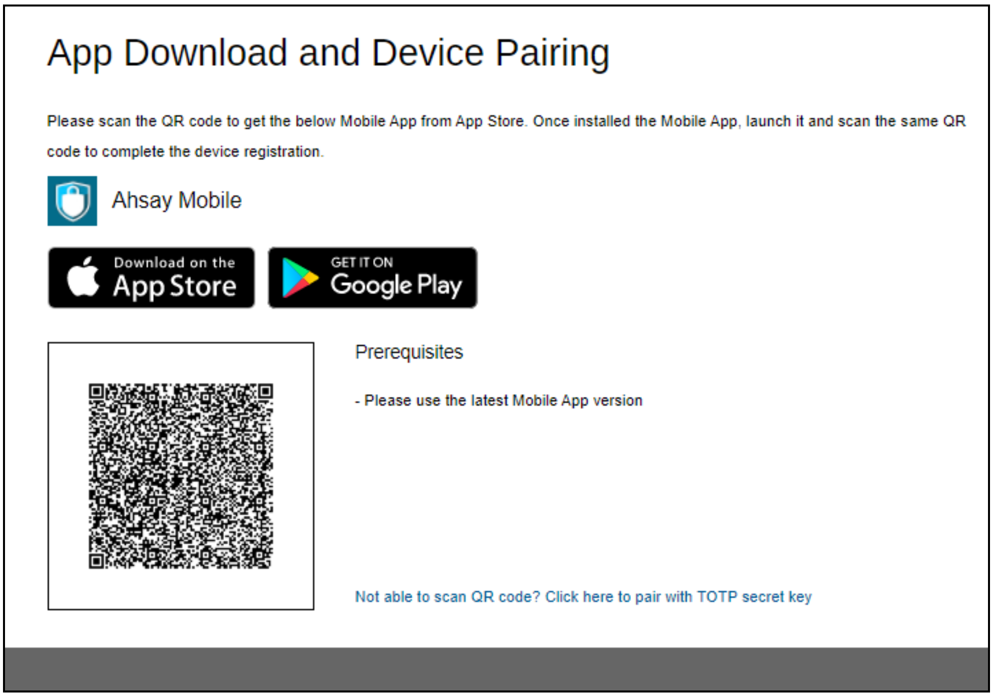
- Ahsay Mobile or branded Mobile app
- Microsoft Authenticator
- Google Authenticator
- Third party authenticators

NOTE

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

2.1 Register device for 2FA using Ahsay Mobile or branded Mobile app

1. Download and install Ahsay Mobile or branded Mobile app in your device.



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

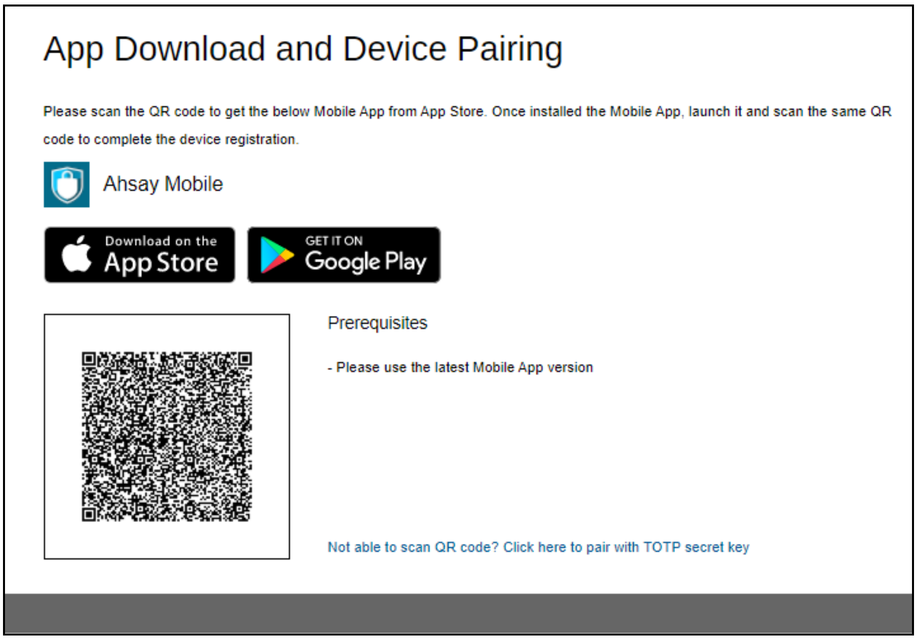
Prerequisites

- Please use the latest Mobile App version

Not able to scan QR code? Click here to pair with TOTP secret key

2. Pair your mobile device with AhsayCBS. Ahsay Mobile can be configured to support two 2FA modes which are:
   - Push Notification and TOTP (default)
   - TOTP only

- For Push Notification and TOTP, scan the QR code.



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.

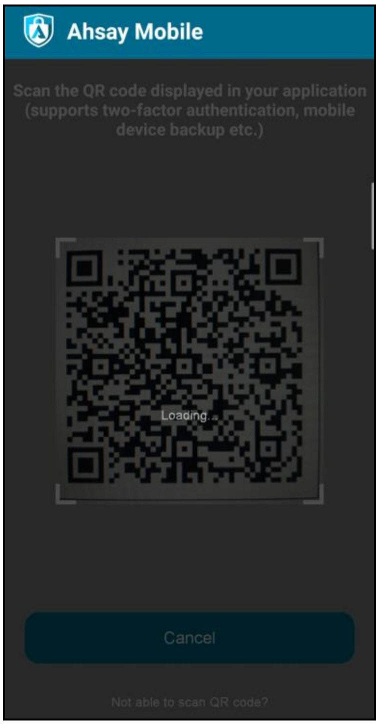
Ahsay Mobile

Prerequisites

- Please use the latest Mobile App version

Not able to scan QR code? Click here to pair with TOTP secret key

This is a sample of the Ahsay Mobile app installed on a mobile device named “Galaxy A70”.



Ahsay Mobile

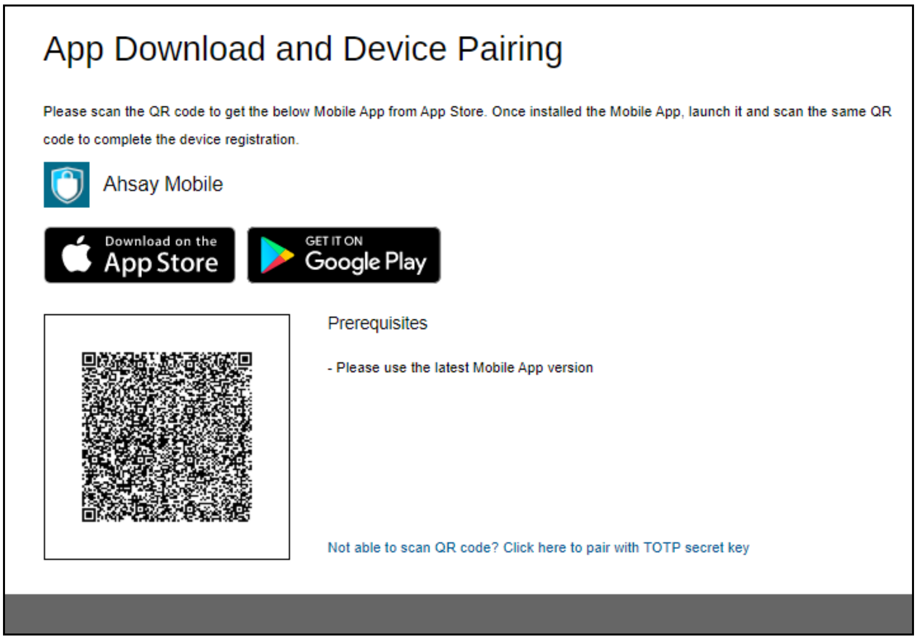
Scan the QR code displayed in your application (supports two-factor authentication, mobile device backup etc.)

Loading...

Cancel

Not able to scan QR code?

- For TOTP only, click the Not able to scan QR code? Click here to pair with TOTP secret key link.



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.

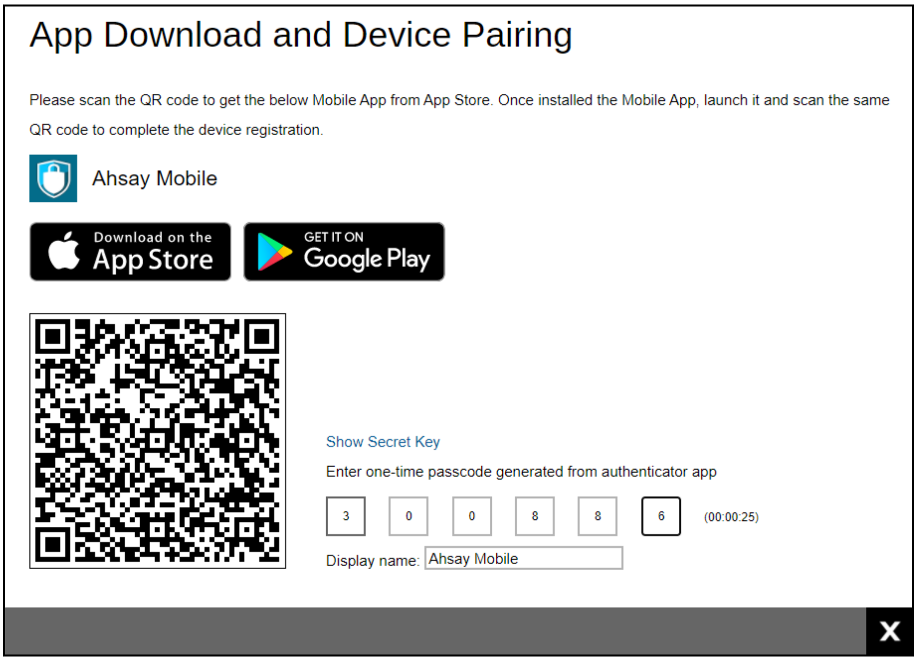
Ahsay Mobile

Prerequisites

- Please use the latest Mobile App version

Not able to scan QR code? Click here to pair with TOTP secret key

Scan the QR code. A one-time passcode will be generated in Ahsay Mobile, enter it here.



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

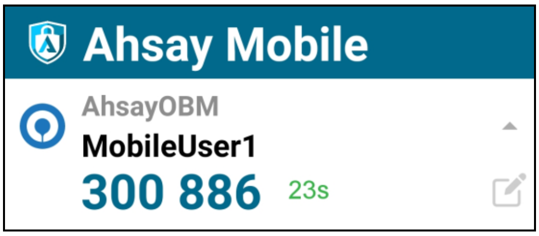
Show Secret Key

Enter one-time passcode generated from authenticator app

3 0 0 8 8 6 (00:00:25)

Display name: Ahsay Mobile

This is a sample of the one-time passcode generated in Ahsay Mobile.



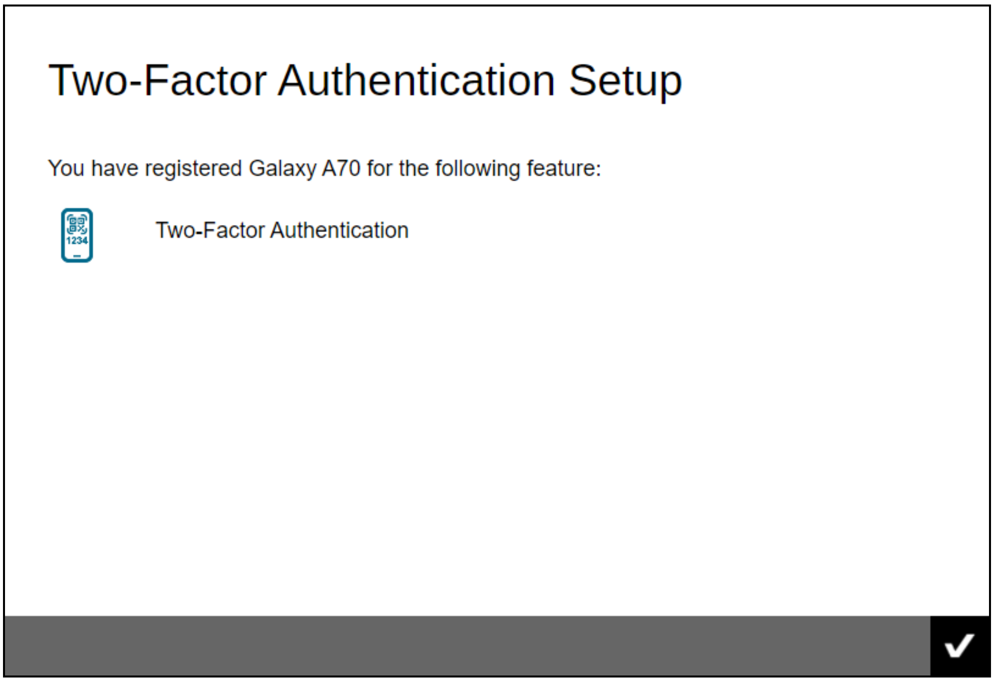
Ahsay Mobile

AhsayOBM

MobileUser1

300 886 23s

3. When pairing is completed, the screen below will be displayed. Click ✓ to finish the setup.



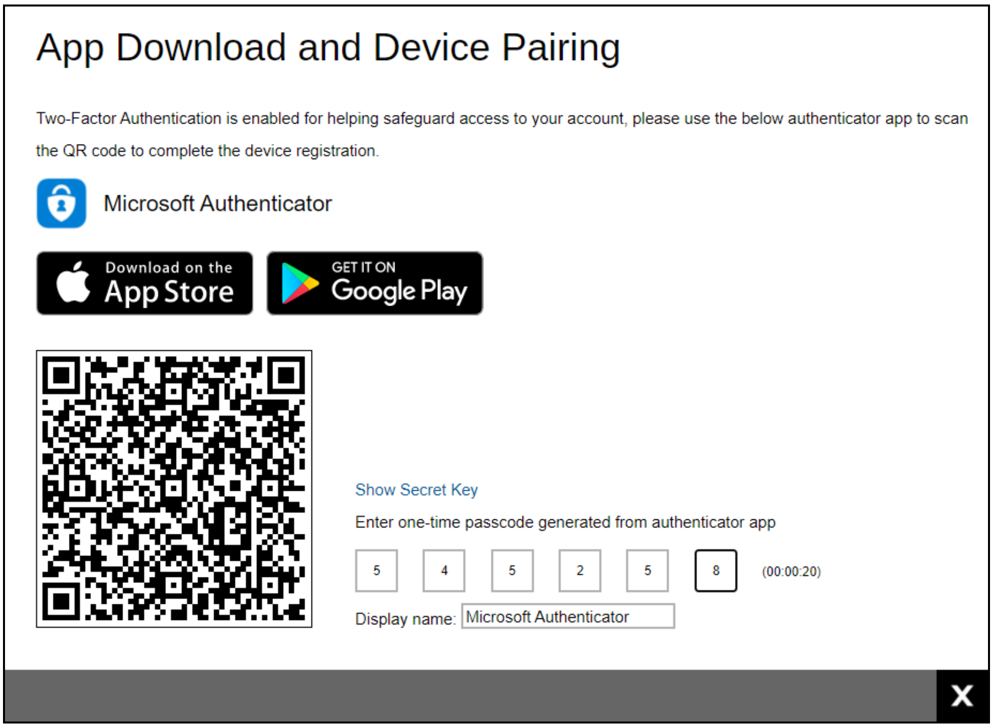
Two-Factor Authentication Setup

You have registered Galaxy A70 for the following feature:

Two-Factor Authentication

2.2 Register device for 2FA using Microsoft Authenticator

1. Download and install Microsoft Authenticator app in your device.
2. Scan the QR code and enter the one-time passcode generated in Microsoft Authenticator.



App Download and Device Pairing

Two-Factor Authentication is enabled for helping safeguard access to your account, please use the below authenticator app to scan the QR code to complete the device registration.

Microsoft Authenticator

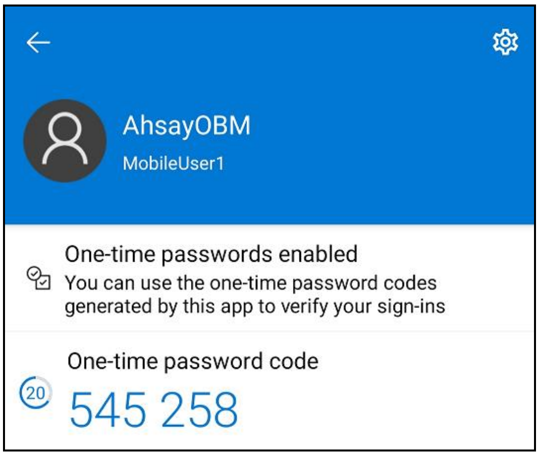
Show Secret Key

Enter one-time passcode generated from authenticator app

5 4 5 2 5 8 (00:00:20)

Display name: Microsoft Authenticator

This is a sample of the one-time passcode generated in Microsoft Authenticator.

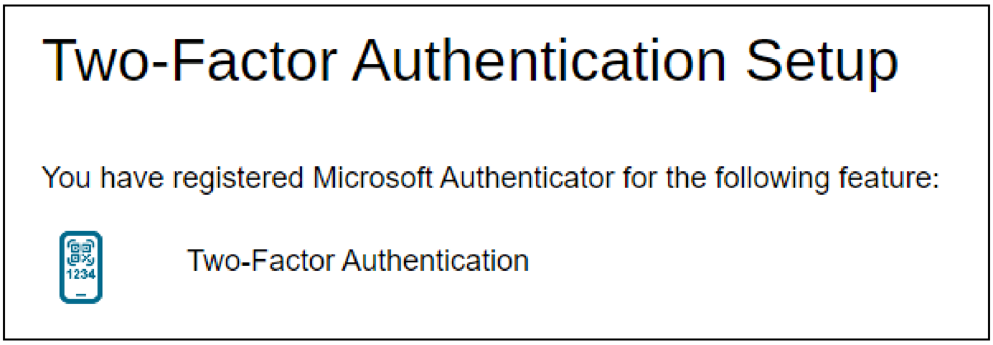


AhsayOBM
MobileUser1

One-time passwords enabled
You can use the one-time password codes generated by this app to verify your sign-ins

One-time password code
20
545 258

3. When pairing is completed, the screen below will be displayed. Click ☑ to finish the setup.



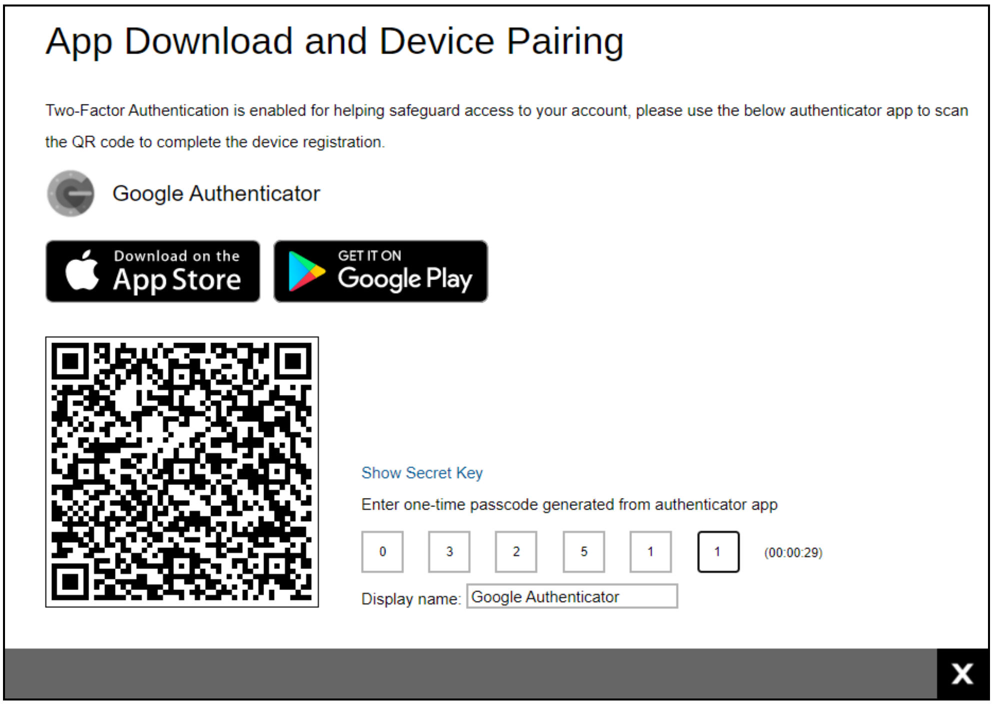
Two-Factor Authentication Setup

You have registered Microsoft Authenticator for the following feature:

Two-Factor Authentication

2.3 Register device for 2FA using Google Authenticator

1. Download and install Google Authenticator app in your device.
2. Scan the QR code and enter the one-time passcode generated in Microsoft Authenticator.



App Download and Device Pairing

Two-Factor Authentication is enabled for helping safeguard access to your account, please use the below authenticator app to scan the QR code to complete the device registration.

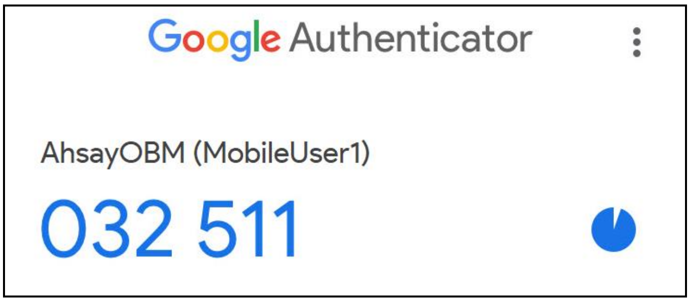
Google Authenticator

Enter one-time passcode generated from authenticator app

0 3 2 5 1 1 (00:00:29)

Display name: Google Authenticator

This is a sample of the one-time passcode generated in Google Authenticator.

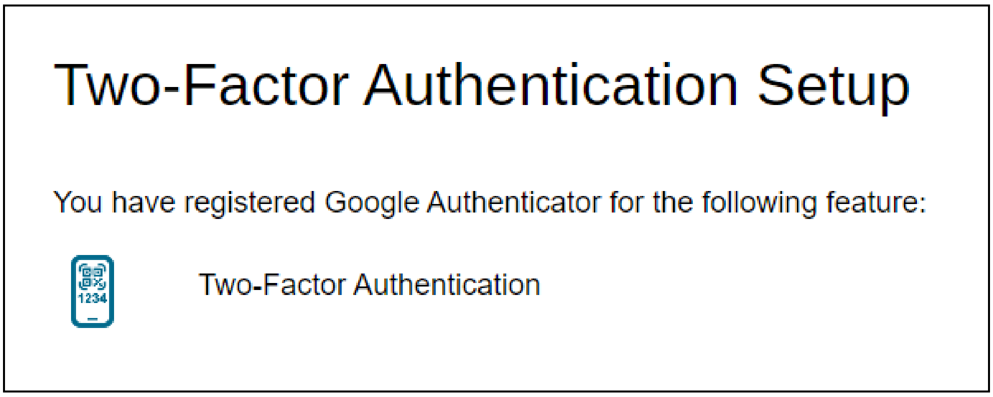


Google Authenticator

AhsayOBM (MobileUser1)

032 511

3. When pairing is completed, the screen below will be displayed. Click ☑ to finish the setup.



Two-Factor Authentication Setup

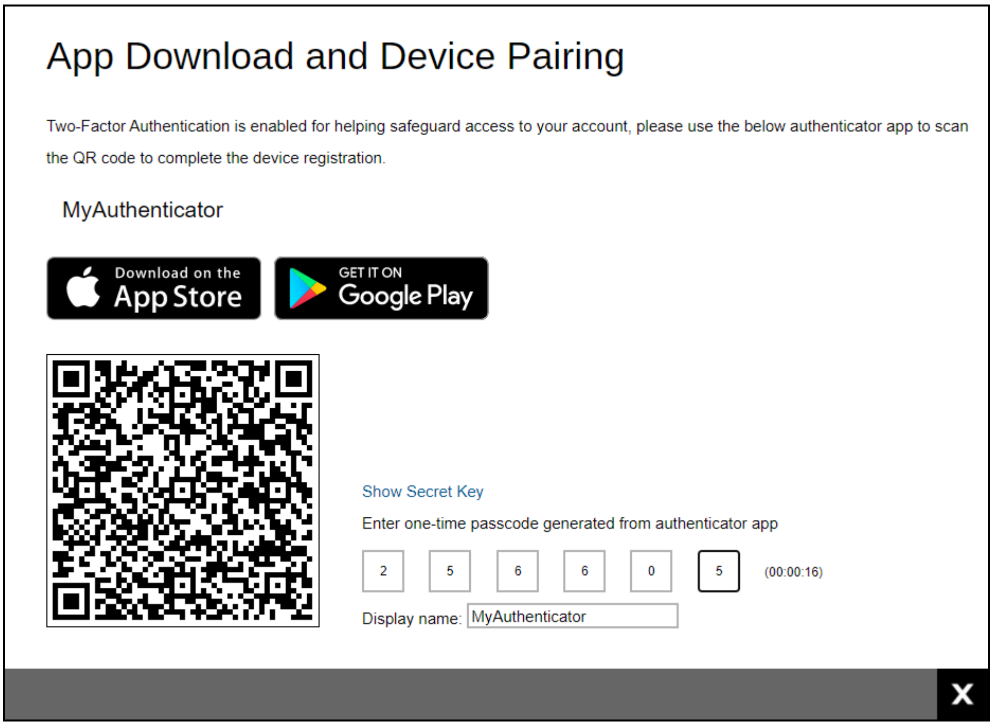
You have registered Google Authenticator for the following feature:

Two-Factor Authentication

2.4 Register device for 2FA using Third party authenticators

For **Third Party authenticators**, the Display name is dependent on the settings made by your backup service provider. For this type, you can use the authenticator app of your choice. You will know that it is a third parry authenticator if the Display name is not one of these three: Ahsay Mobile, Microsoft Authenticator and Google Authenticator. In our example the Display name is “MyAuthenticator”, which means that it is a third party authenticator and you can use any third party TOTP authenticator app that you want, e.g. LastPass, Duo, Authy, Microsoft Authenticator, Google Authenticator etc.

1. Download and install the authenticator app of your choice in your device.
2. Scan the QR code and enter the one-time passcode generated in the authenticator app.



App Download and Device Pairing

Two-Factor Authentication is enabled for helping safeguard access to your account, please use the below authenticator app to scan the QR code to complete the device registration.

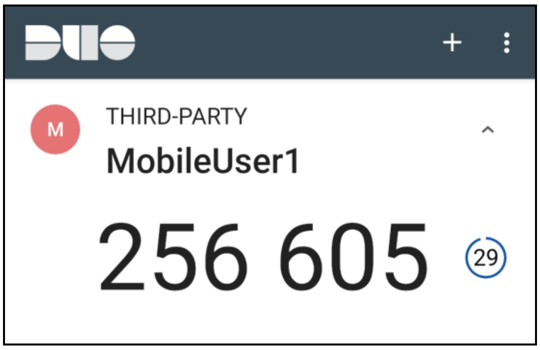
MyAuthenticator

Enter one-time passcode generated from authenticator app

2 5 6 6 0 5 (00:00:16)

Display name: MyAuthenticator

This is a sample of the one-time passcode generated in a third party authenticator, in this case Duo was used.

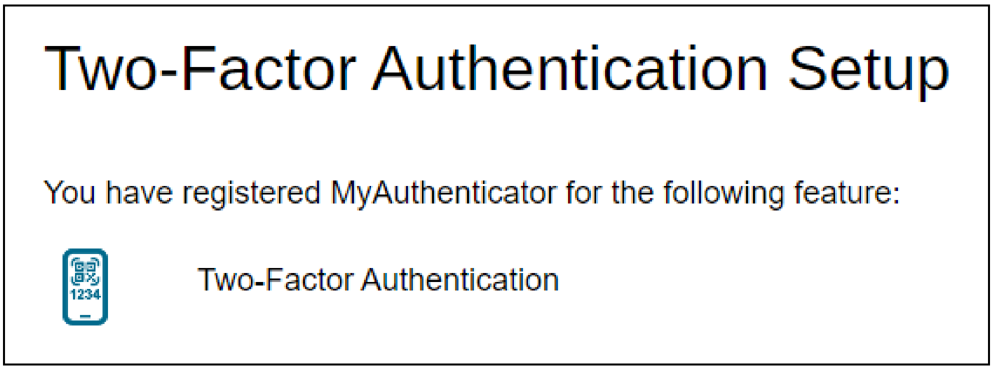


THIRD-PARTY

MobileUser1

256 605

3. When pairing is completed, the screen below will be displayed. Click ✓ to finish the setup.



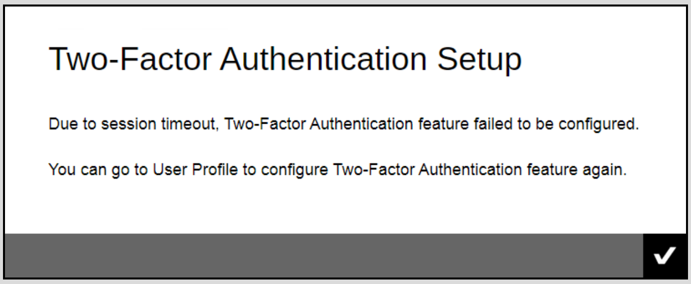
Two-Factor Authentication Setup

You have registered MyAuthenticator for the following feature:

Two-Factor Authentication

NOTE

In case device pairing takes a while, session timeout message will be displayed. Just click ✓ to register your device again, for instructions please refer to Ch. 2.5.



Two-Factor Authentication Setup

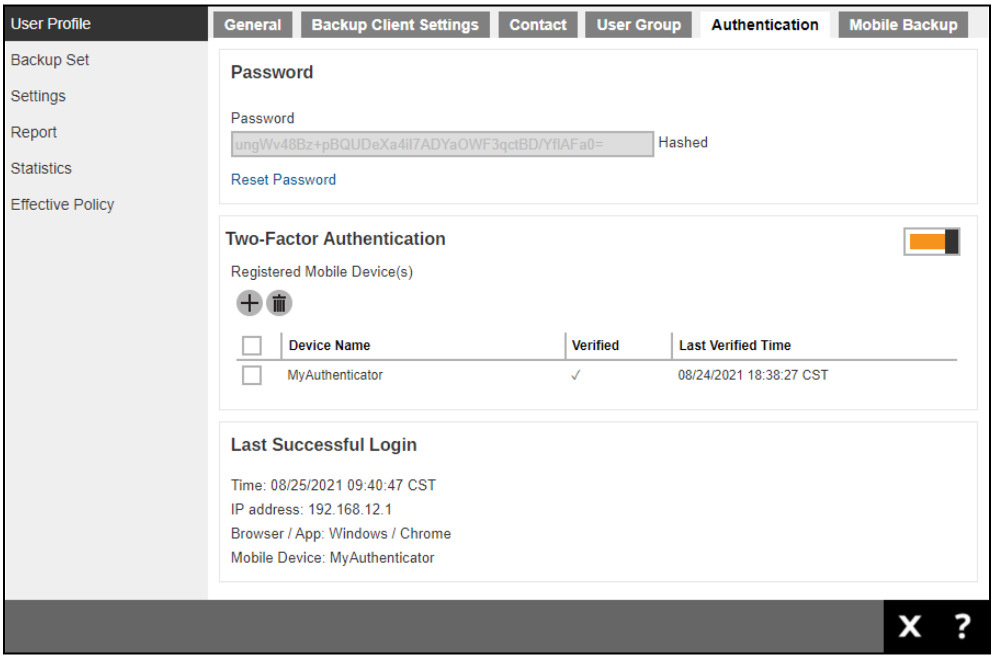
Due to session timeout, Two-Factor Authentication feature failed to be configured.

You can go to User Profile to configure Two-Factor Authentication feature again.

2.5 Register additional device/app for 2FA

If you want to register an additional device and/or app for 2FA you may do so by following the instructions below:

1. Go to **Backup/Restore** > **User** > **User Profile** > **Authentication** > **Two-Factor Authentication**.



Password

Password

ungWv48Bz+pBQUDeXa4il7ADYaOWF3qctBD/YfIAFa0= Hashed

Reset Password

Two-Factor Authentication

Registered Mobile Device(s)

□	Device Name	Verified	Last Verified Time
□	MyAuthenticator	✓	08/24/2021 18:38:27 CST

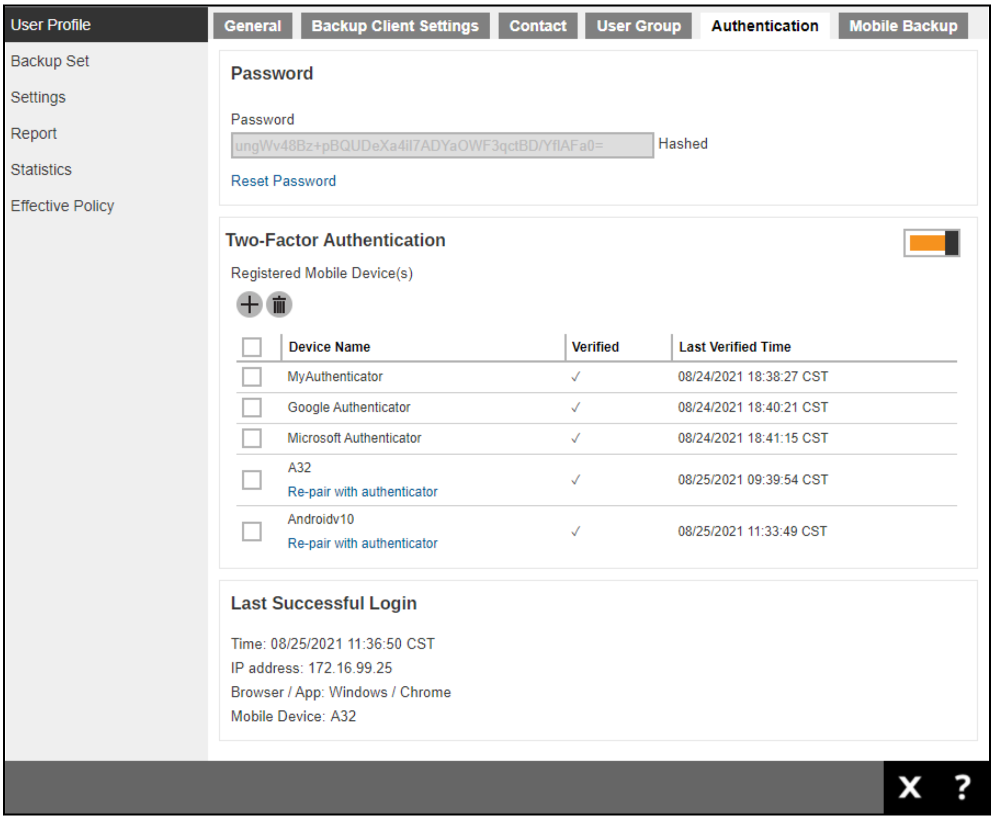
Last Successful Login

Time: 08/25/2021 09:40:47 CST
IP address: 192.168.12.1
Browser / App: Windows / Chrome
Mobile Device: MyAuthenticator

2. Click + then follow the instructions discussed in the previous chapters 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

3. After successful registration, the device and/or app will be listed under Registered Mobile Device(s).



Password

Password: ungWv48Bz+pBQUDeXa4il7ADYaOWF3qctBD/YflAFa0= Hashed

Reset Password

Two-Factor Authentication

Registered Mobile Device(s)

□	Device Name	Verified	Last Verified Time
□	MyAuthenticator	✓	08/24/2021 18:38:27 CST
□	Google Authenticator	✓	08/24/2021 18:40:21 CST
□	Microsoft Authenticator	✓	08/24/2021 18:41:15 CST
□	A32 Re-pair with authenticator	✓	08/25/2021 09:39:54 CST
□	Androidv10 Re-pair with authenticator	✓	08/25/2021 11:33:49 CST

Last Successful Login

Time: 08/25/2021 11:36:50 CST
IP address: 172.16.99.25
Browser / App: Windows / Chrome
Mobile Device: A32

NOTE

If several authenticator apps are registered for an account and one of those apps is Ahsay Mobile, by default a login request will be sent to login with 2FA. If there are two devices registered using Ahsay Mobile, then both devices will receive the login request.

3 Logging in to AhsayCBS User Web Console

Starting with AhsayCBS v8.5.0.0, you will find a new feature introduced with this latest version which is the Two-Factor Authentication. With this new feature, there are several scenarios that will be encountered for login. Login steps for the different scenarios will be discussed in this chapter.

- Login to AhsayCBS without 2FA
- Login to AhsayCBS with 2FA using authenticator app
- Login to AhsayCBS with 2FA using Twilio

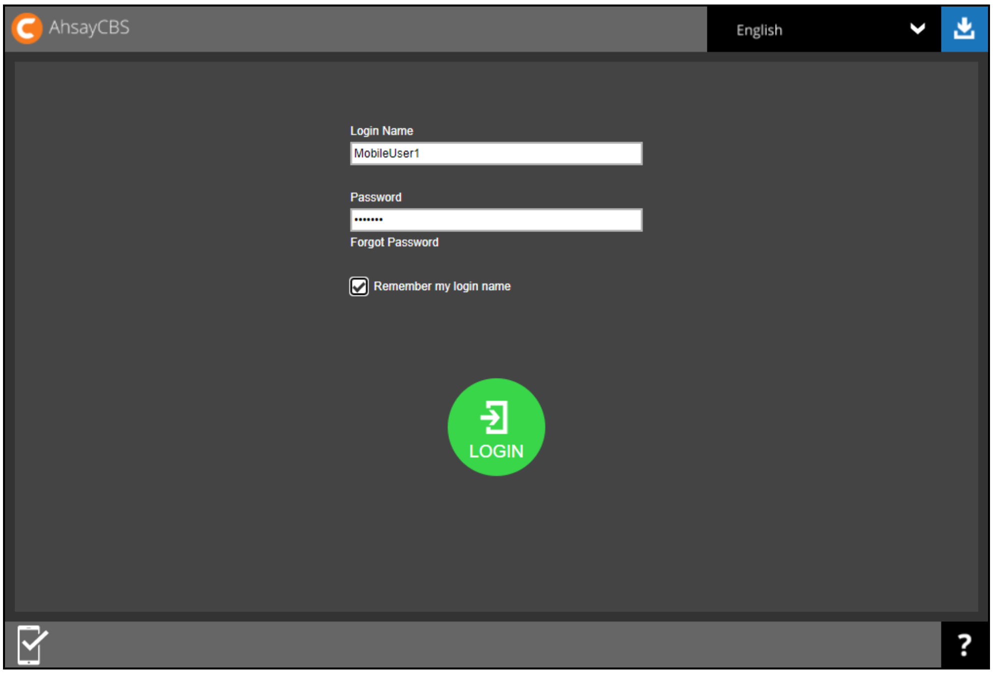
3.1 Login to AhsayCBS without 2FA

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

1. Login 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**.



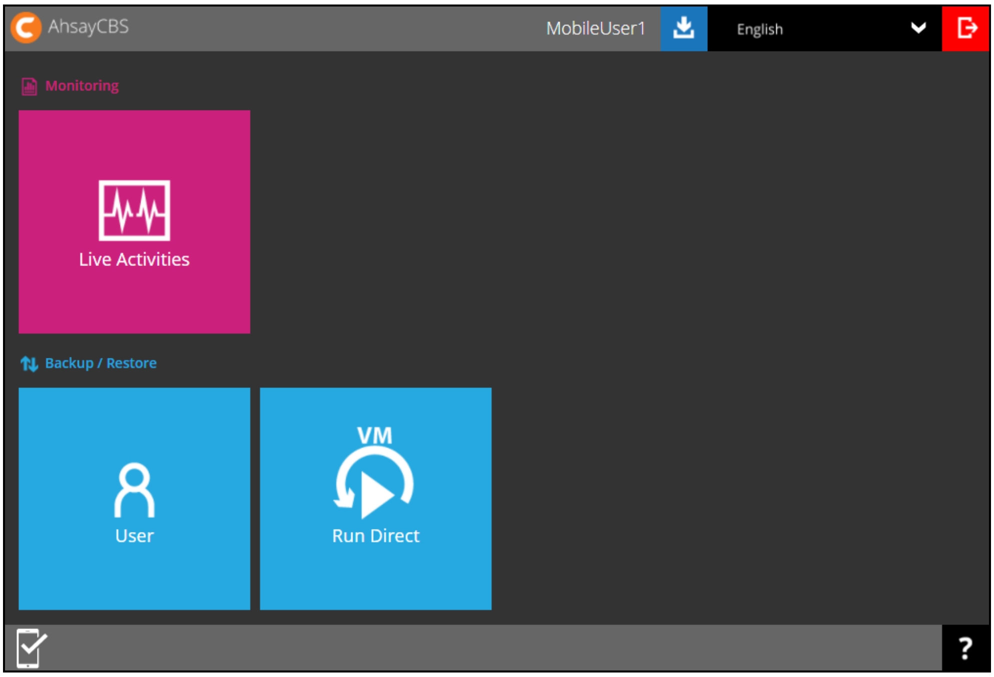
Login Name: MobileUser1

Password: •••••••

☑ Remember my login name

3. After successful login, 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.

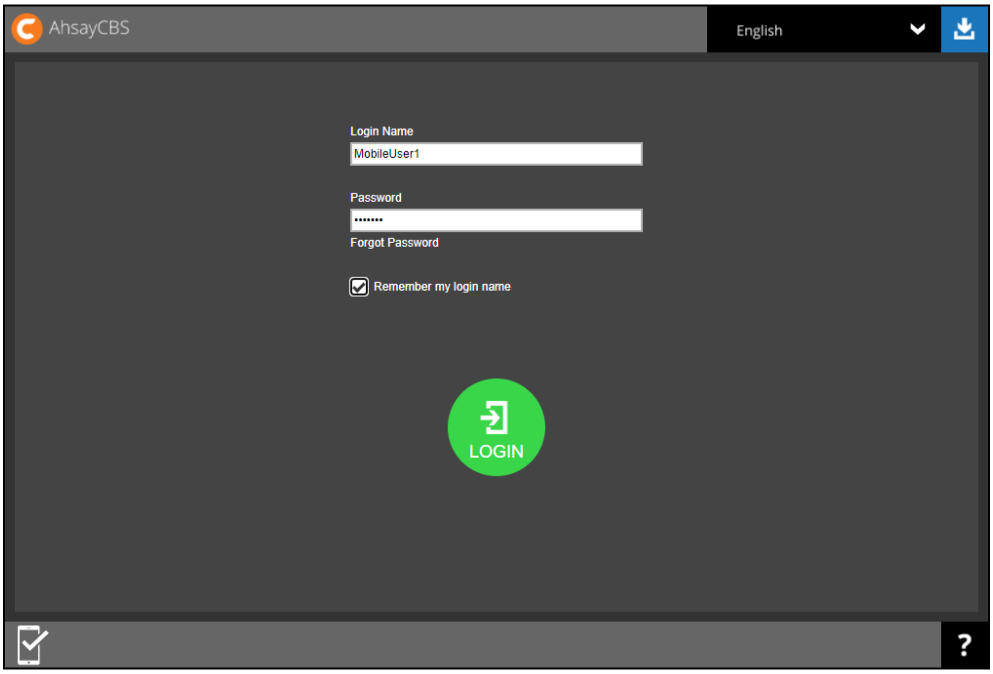
3.2 Login to AhsayCBS with 2FA using authenticator app

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

1. Login 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**.



Login Name: MobileUser1

Password: •••••••

☑ Remember my login name

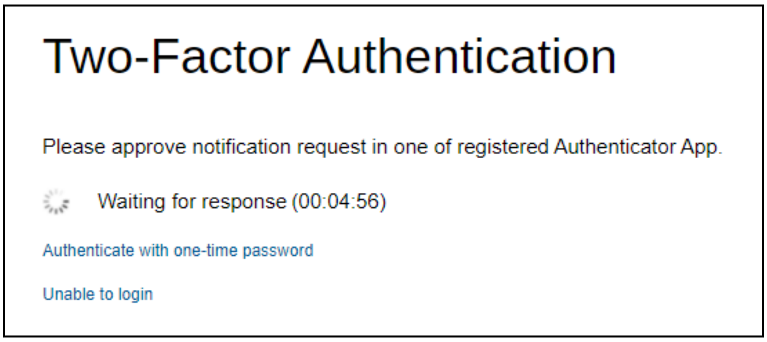
3. One of the two authentication methods will be displayed to continue with the login:

   - 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 login request on Ahsay Mobile to complete the login.



Two-Factor Authentication

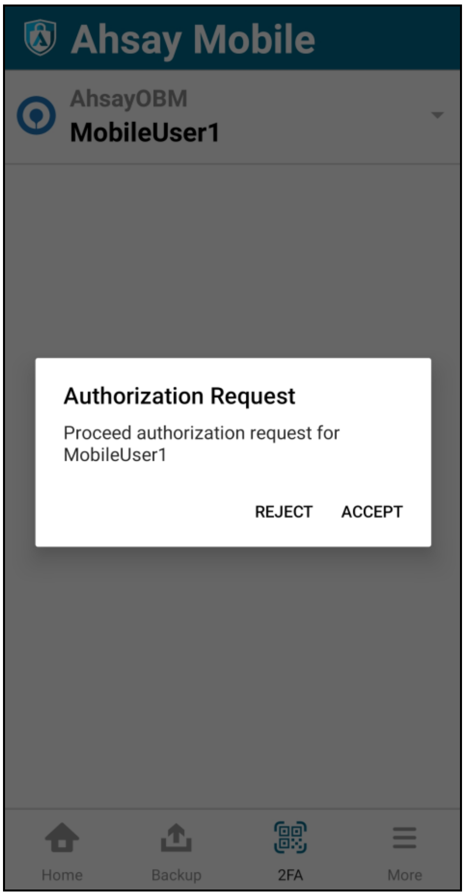
Please approve notification request in one of registered Authenticator App.

Waiting for response (00:04:56)

Authenticate with one-time password

Unable to login

Example of the login request sent to the Ahsay Mobile app.



Ahsay Mobile

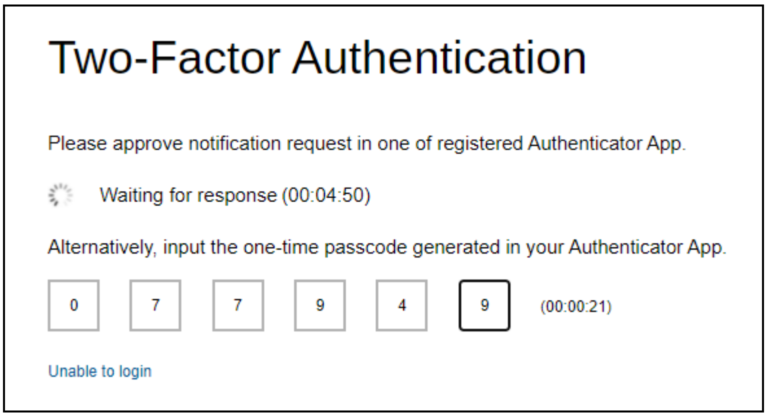
AhsayOBM
MobileUser1

Authorization Request

Proceed authorization request for MobileUser1

- 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 login.



Two-Factor Authentication

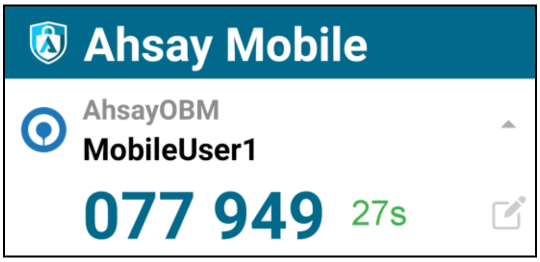
Please approve notification request in one of registered Authenticator App.

Waiting for response (00:04:50)

Alternatively, input the one-time passcode generated in your Authenticator App.

0 7 7 9 4 9 (00:00:21)

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



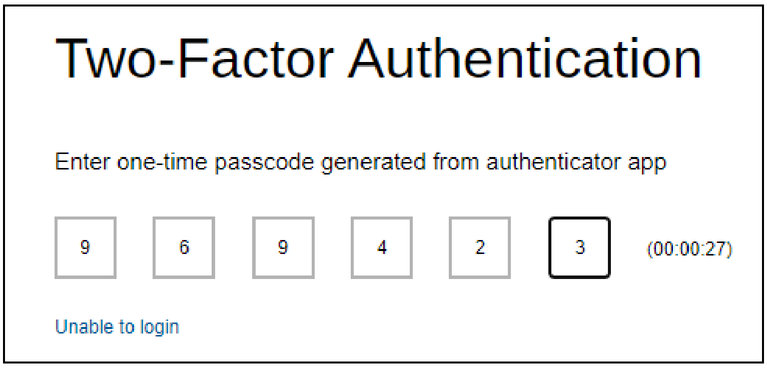
Ahsay Mobile

AhsayOBM
MobileUser1

077 949 27s

- TOTP only

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



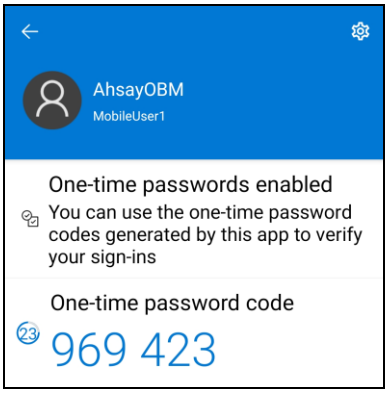
Two-Factor Authentication

Enter one-time passcode generated from authenticator app

9 6 9 4 2 3 (00:00:27)

Unable to login

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



AhsayOBM

MobileUser1

One-time passwords enabled

You can use the one-time password codes generated by this app to verify your sign-ins

One-time password code

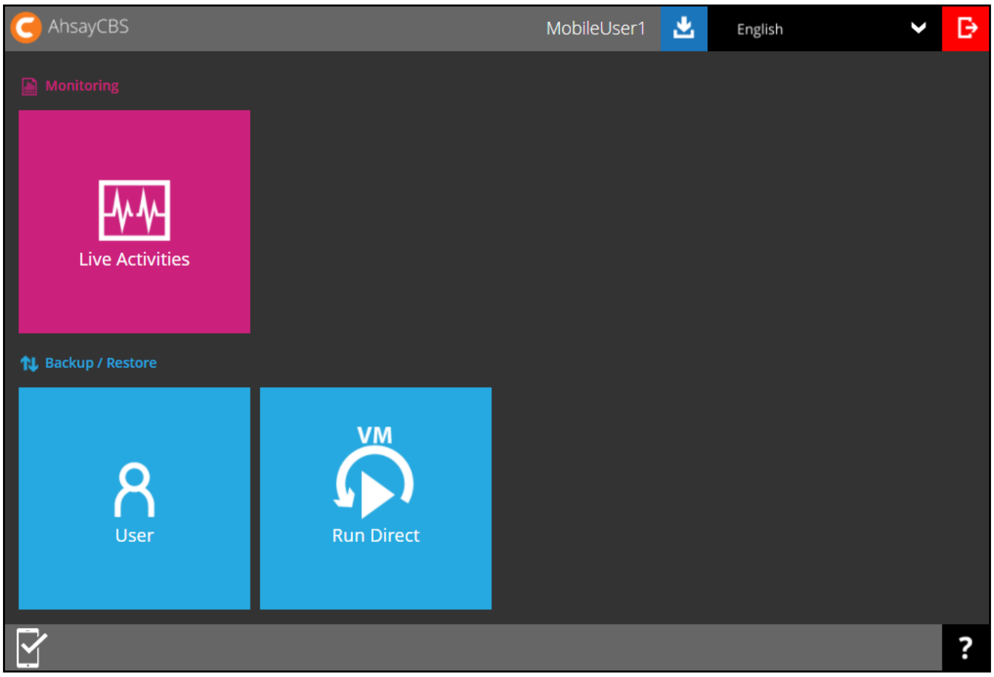
23

969 423

NOTE

Please refer to Chapter 4 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 login, the following screen will appear. For the details of the available options in the main screen, please refer to the description in Ch. 3.1.



NOTE

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

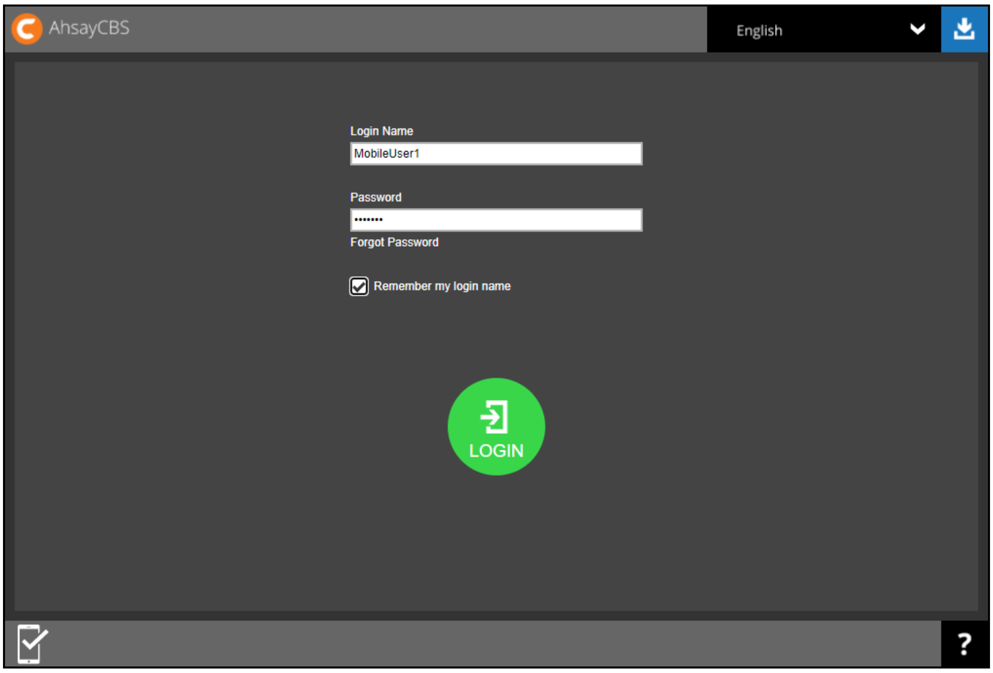
3.3 Login to AhsayCBS with 2FA using Twilio

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

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

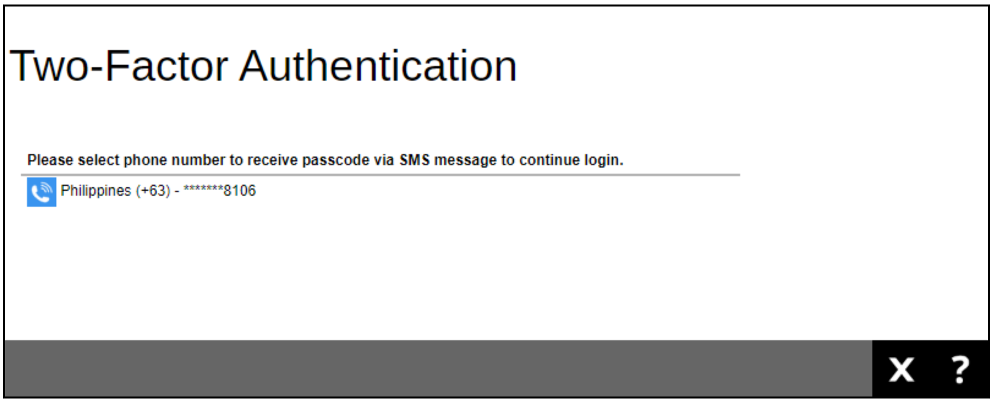
> **NOTE**
>
> Contact your backup service provider for the URL to connect to the web console if necessary.

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



Login Name
MobileUser1
Password
•••••••
Forgot Password
☑ Remember my login name

3. Select your phone number.

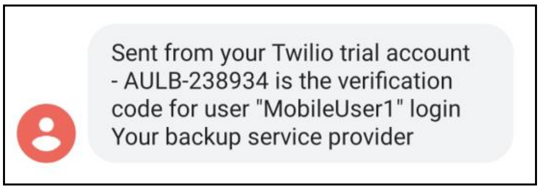


Two-Factor Authentication

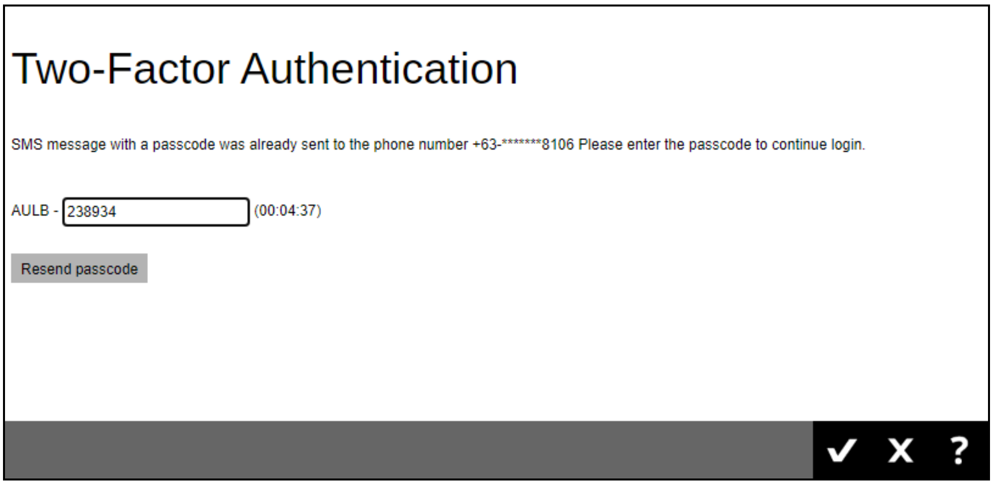
Please select phone number to receive passcode via SMS message to continue login.

Philippines (+63) - *******8106

4. Enter the passcode and click ☑ to login.



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

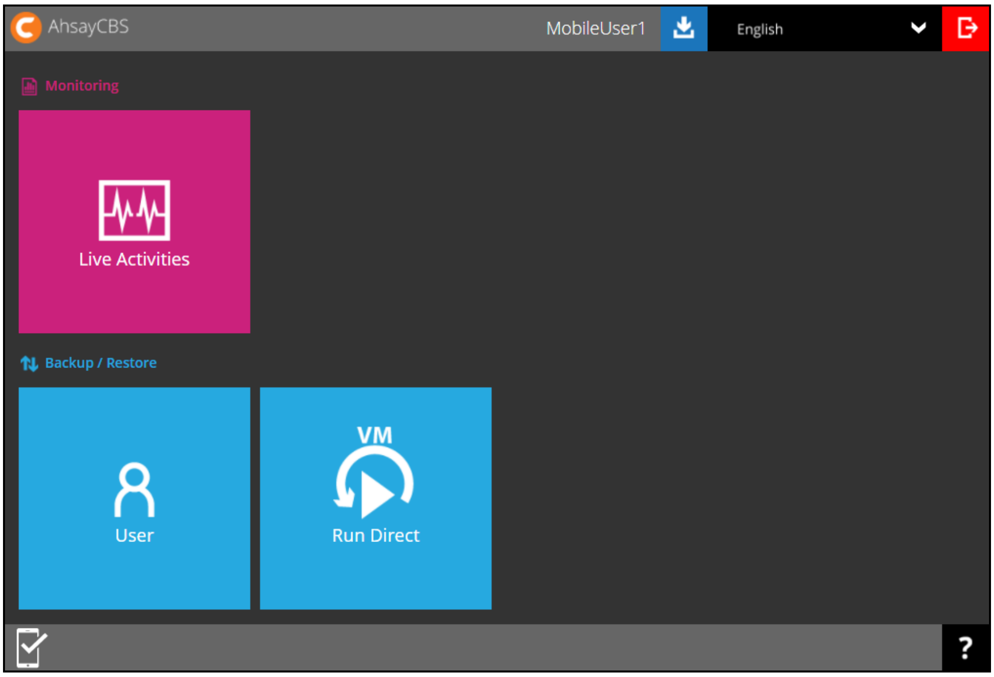


Two-Factor Authentication

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

AULB - 238934 (00:04:37)

5. After successful login, the following screen will appear. For the details of the available options in the main screen, please refer to the description in Ch. 3.1.



NOTE

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

4 Unable to Login to AhsayCBS with 2FA

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

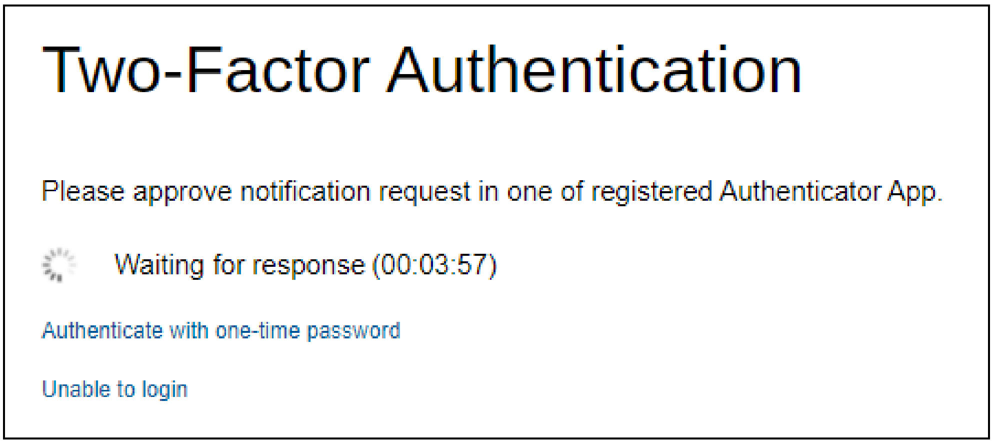
- Registered a recovery number in Ahsay Mobile app
- Did not register a recovery number in Ahsay Mobile app
- Using third party authenticator app

4.1 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 login, you can perform the authentication recovery procedure. Click the Unable to login link.

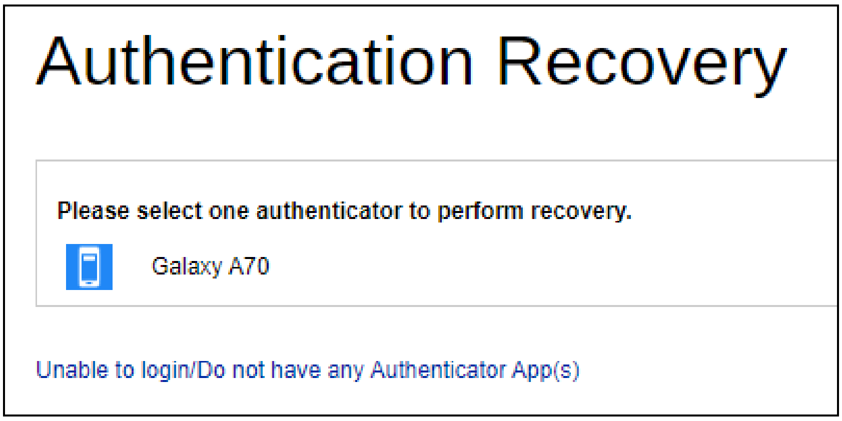


Two-Factor Authentication

Please approve notification request in one of registered Authenticator App.

Waiting for response (00:03:57)

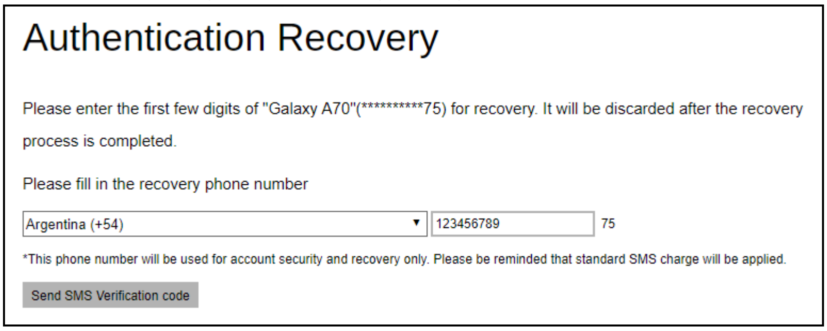
Click your device on the list.



Authentication Recovery

Please select one authenticator to perform recovery.

Enter the recovery number that you registered and click Send SMS Verification code.



Authentication Recovery

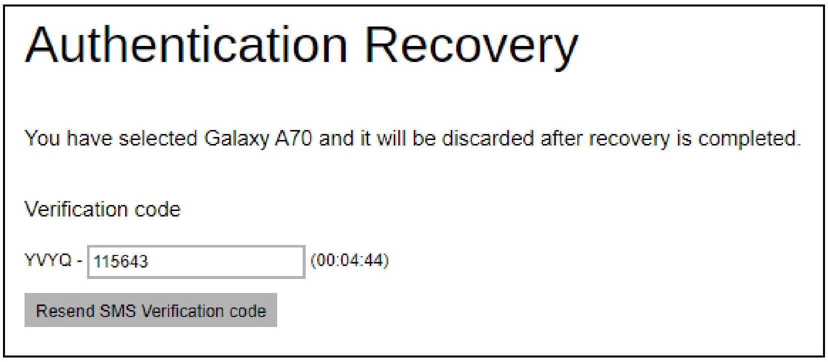
Please enter the first few digits of "Galaxy A70"(**********75) for recovery. It will be discarded after the recovery process is completed.

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.

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



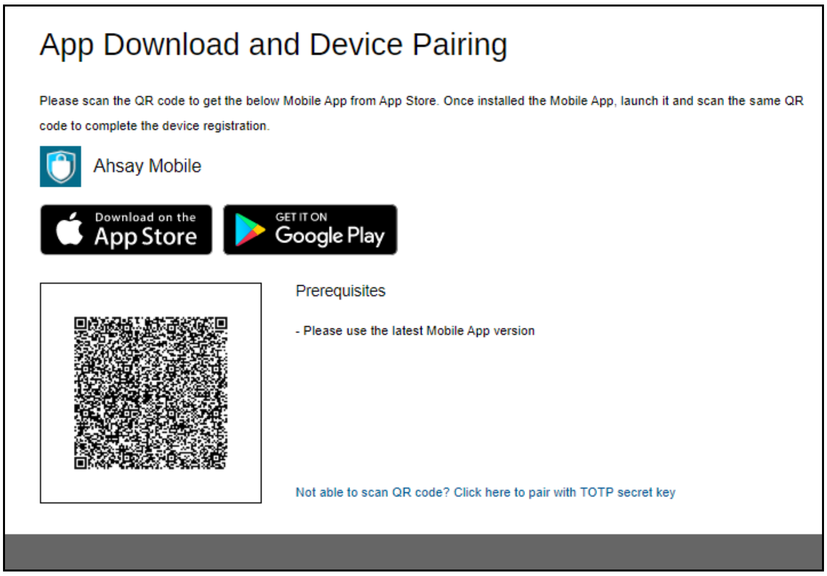
Authentication Recovery

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

Verification code

YVYQ - 115643 (00:04:44)

Register your device to be able to login 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.

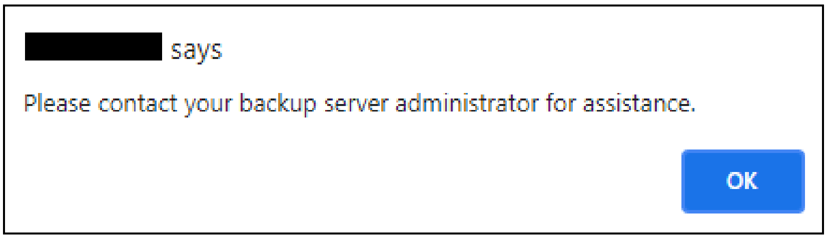
Ahsay Mobile

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.

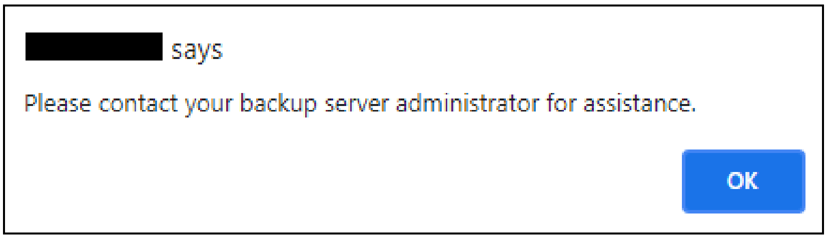


[redacted] says

Please contact your backup server administrator for assistance.

4.2 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.

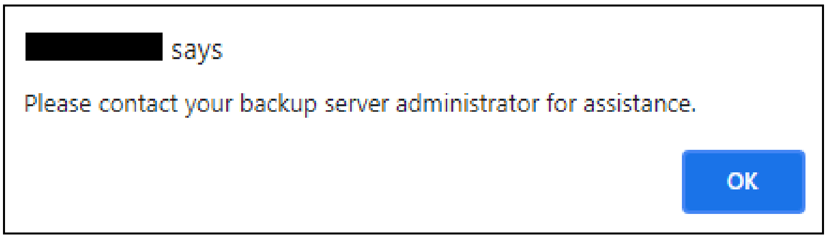


[redacted] says

Please contact your backup server administrator for assistance.

4.3 Using third party authenticator app

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



[redacted] says

Please contact your backup server administrator for assistance.

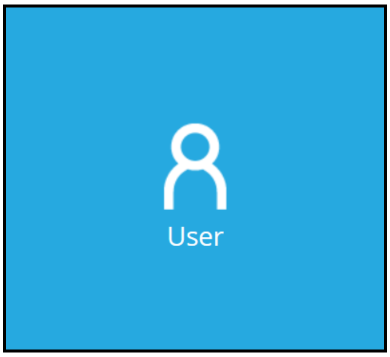
5 Managing Your AhsayCBS User Account

5.1 Login to AhsayCBS

Login to the AhsayCBS user web console according to the instruction provided in section Logging in to AhsayCBS User Web Console.

5.2 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.

5.3 User Profile

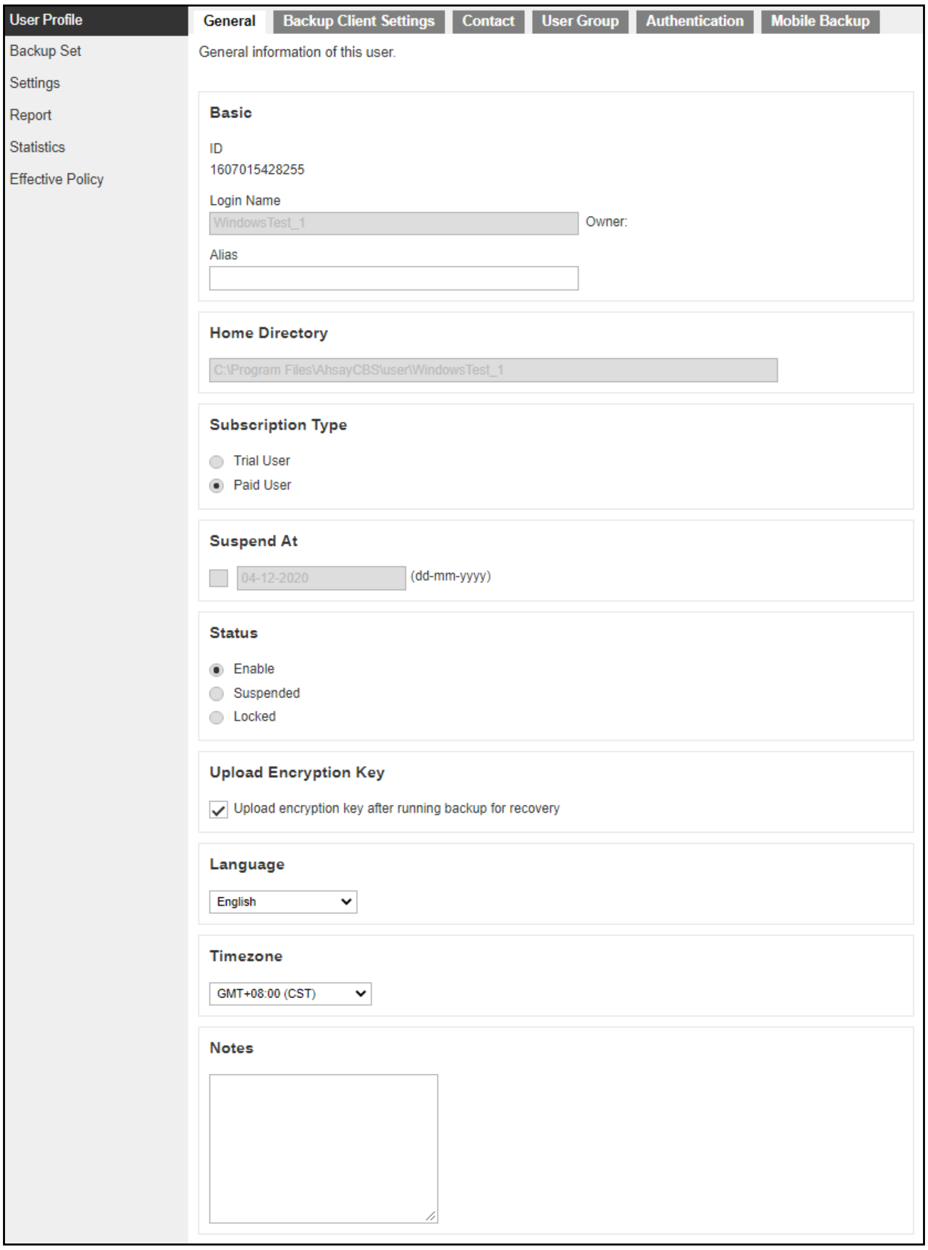
User Profile tab contains your user backup account settings information, subscribed modules backup quota, subscription type, contact information, user group information, two-factor authentication settings and registered mobile device for mobile backup.

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:

5.3.1 General Tab

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



General information of this user.

Basic

ID
1607015428255

Login Name: WindowsTest_1 Owner:

Alias:

Home Directory

C:\Program Files\AhsayCBS\user\WindowsTest_1

Subscription Type

○ Trial User
● Paid User

Suspend At

□ 04-12-2020 (dd-mm-yyyy)

Status

● Enable
○ Suspended
○ Locked

Upload Encryption Key

☑ Upload encryption key after running backup for recovery

Language

English

Timezone

GMT+08:00 (CST)

Notes

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

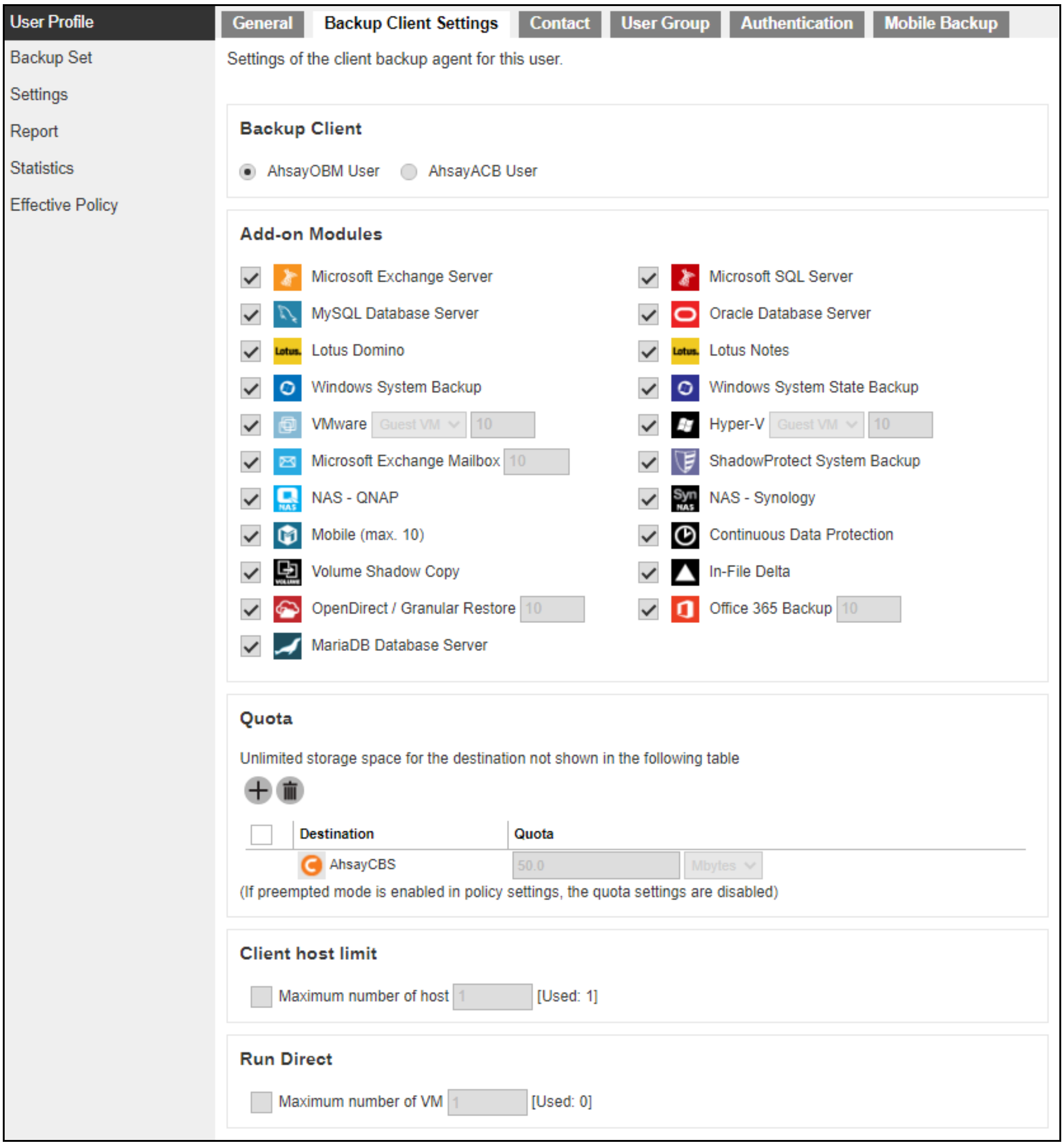
Section	Description
Basic	There are three (3) elements in the Basic section, which are the following: - **ID** of the backup user, this is system generated and cannot be changed. - **Login Name** of the backup user, defined by the service provider which cannot be changed. - **Alias** is another name for the backup user which can be modified.
Home Directory	This is the path where your backup data is stored on AhsayCBS backup destination. This was set when your account was created and cannot be modified by the user.
Subscription Type	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. 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.
Suspend At	This shows the date when a trial user account is scheduled to be suspended. 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.
Status	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 login attempts, the user account will be locked. 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.
Upload Encryption Key	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. If you forget the encryption key, please contact your backup service provider for support.
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.

5.3.2 Backup Client Settings Tab

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



Settings of the client backup agent for this user.

Backup Client

● AhsayOBM User ○ AhsayACB User

Add-on Modules

- ☑ Microsoft Exchange Server
- ☑ MySQL Database Server
- ☑ Lotus Domino
- ☑ Windows System Backup
- ☑ VMware Guest VM 10
- ☑ Microsoft Exchange Mailbox 10
- ☑ NAS - QNAP
- ☑ Mobile (max. 10)
- ☑ Volume Shadow Copy
- ☑ OpenDirect / Granular Restore 10
- ☑ MariaDB Database Server
- ☑ Microsoft SQL Server
- ☑ Oracle Database Server
- ☑ Lotus Notes
- ☑ Windows System State Backup
- ☑ Hyper-V Guest VM 10
- ☑ ShadowProtect System Backup
- ☑ NAS - Synology
- ☑ Continuous Data Protection
- ☑ In-File Delta
- ☑ Office 365 Backup 10

Quota

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

□	Destination	Quota
	AhsayCBS	50.0 Mbytes

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

Client host limit

□ Maximum number of host 1 [Used: 1]

Run Direct

□ Maximum number of VM 1 [Used: 0]

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

Section	Description
Backup Client	There are two (2) types of backup user accounts: **AhsayOBM** and **AhsayACB**. 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.
Add-on Modules	The backup client comes with add-on modules. 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.
Quota	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. 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.
Client Host Limit	This is for your backup service provider to set the maximum number of host machine for your backup user account. This field cannot be changed by the user. If you need to update this field, please contact your backup service provider.
Run Direct	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. This field cannot be changed by the user. If you need to update this field, please contact your backup service provider.

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

- 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.
- 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 v8 Microsoft Exchange Database Backup and Restore Guide	✓	✗
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 v8 Microsoft SQL Server Backup and Restore Guide	✓	✗
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 v8 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 v8 MySQL Database Backup and Restore for Linux (CLI)	✓	✗
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 v8 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 v8 Oracle	✓	✗

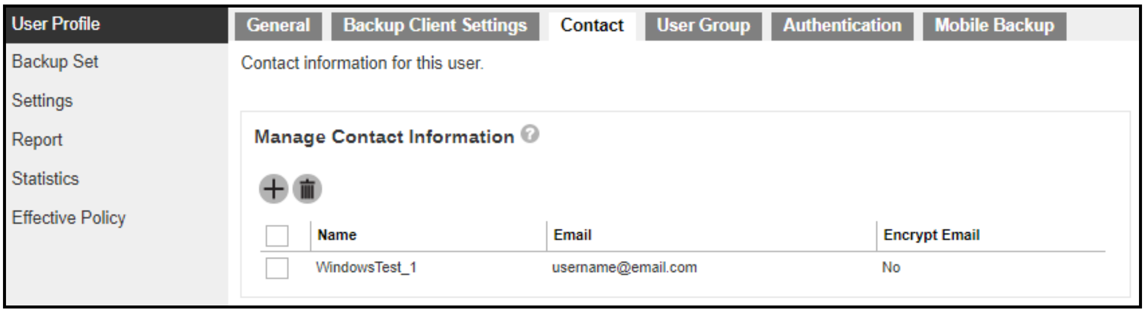
	Database Backup and Restore for Linux (CLI) Ahsay Online Backup Manager v8 Oracle Database Backup and Restore for Linux (GUI)		
Lotus Domino	Backup and restore of Lotus Domino.	✓	✗
Lotus Notes	Backup and restore of Lotus Notes.	✓	✓
Windows System Backup	Backup and restore of Windows System Backup. Refer to the following link for how to use Windows System Backup with AhsayOBM and AhsayACB clients: Ahsay Online Backup Manager v8 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 v8 Microsoft System State Backup and Restore Guide	✓	✗
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 v8 VMware vCenter/ESXi Backup and Restore Guide	✓	✗
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 v8 Microsoft Hyper-V Backup and Restore Guide	✓	✗
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 v8 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 v8 Microsoft Exchange 2013/2016/2019 (EWS) Mail Level Backup & Restore Guide	✓	✗
Shadow Protect System Backup	Backup and restore of Shadow Protect System image (requires Shadow Protect).	✓	✗

	Refer to the following link for how to use the ShadowProtect System Backup with AhsayOBM client: Ahsay Online Backup Manager v7 StorageCraft ShadowProtect System Backup & Restore Guide		
NAS - QNAP	Backup and restore of file on QNAP NAS devices. Refer to the following link for how to use the QNAP NAS with AhsayOBM client: Ahsay Online Backup Manager v8 Quick Start Guide for QNAP NAS Refer to the following link for a list of QNAP hardware compatible with AhsayOBM: FAQ: Ahsay Hardware Compatibility List (HRL) for AhsayOBM on QNAP NAS (8018)	✓	✗
NAS - Synology	Backup and restore of file on Synology NAS devices. Refer to the following link for how to use the Synology NAS with AhsayOBM client: Ahsay Online Backup Manager v8 Quick Start Guide for Synology NAS Refer to the following link for a list of Synology hardware compatible with AhsayOBM: FAQ: Ahsay Hardware Compatibility List (HRL) for AhsayOBM on Synology NAS (8017)	✓	✗
Mobile	Backup and restore of Mobile data (iOS and Android). Refer to the following links for instructions on using the Ahsay Mobile for Android and iOS platforms. Ahsay Mobile Getting Started Guide for Mobile Backup Ahsay Mobile Getting Started Guide for 2FA Ahsay Mobile User Guide for Android and iOS	✓	✓
Continuous Data Protection	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.	✓	✓
Volume Shadow Copy	Volume Shadow Copy to support open file backups on Windows platform.	✓	✓
In-File Delta	When enabled only the changes since the last backup job is backed up.	✓	✓
OpenDirect / Granular Restore	For OpenDirect and Granular Restore. Refer to the following link for instructions on using OpenDirect / Granular Restore. AhsayACB v8 Quick Start Guide for Windows Ahsay Online Backup Manager v8 Quick Start	✓	✗

	Guide for Windows Ahsay Online Backup Manager v8 Microsoft Hyper-V Backup and Restore Guide Ahsay Online Backup Manager v8 VMware vCenter/ESXi Backup and Restore Guide		
Office 365 Backup	Backup and restore of mailboxes and files of Office 365 including the One Drive, Personal Site, Public Folders, and Site Collections. Refer to the following link for instructions on using Office 365. Ahsay Online Backup Manager v8 User Guide for Office365 Backup & Restore for Windows Ahsay Online Backup Manager User Guide for Office365 Backup & Restore for Mac AhsayACB v8 User Guide for Office 365 for Windows AhsayACB v8 User Guide for Office 365 for Mac AhsayCBS v8 User Guide - Office365 Run on Server (Agentless) Backup and Restore Guide	✓	✓
MariaDB Database Server	Backup and restore of MariaDB Database Server. Refer to the following link for how to use MariaDB Database for the Windows platform with AhsayOBM client: Ahsay Online Backup Manager v8 MariaDB Database Backup and Restore for Windows Refer to the following link for how to use MariaDB Database for the Linux platform with AhsayOBM client: Ahsay Online Backup Manager v8 MariaDB Database Backup and Restore for Linux (CLI)	✓	✗

5.3.3 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.

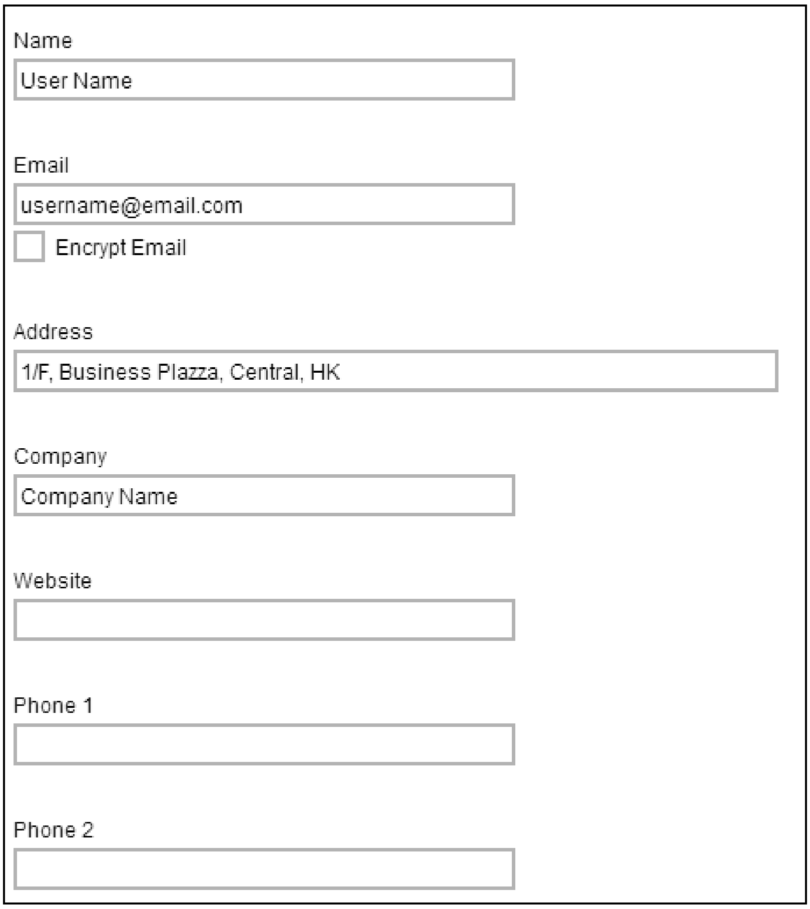


Contact information for this user.

Manage Contact Information

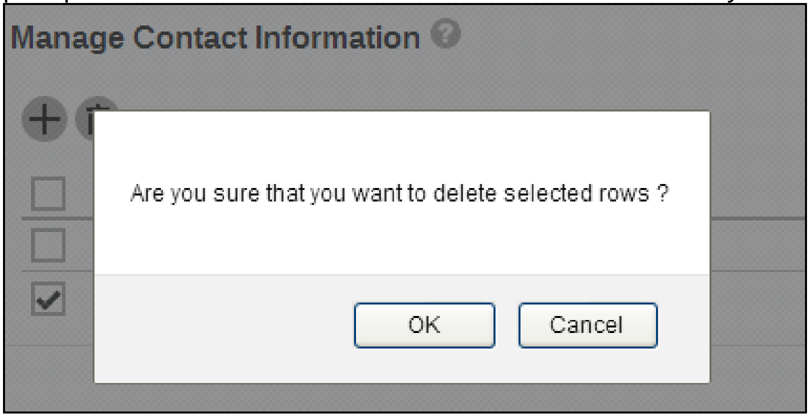
□	Name	Email	Encrypt Email
□	WindowsTest_1	username@email.com	No

- 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.



Name	User Name
Email	username@email.com
□ Encrypt Email	
Address	1/F, Business Plazza, Central, HK
Company	Company Name
Website	
Phone 1	
Phone 2	

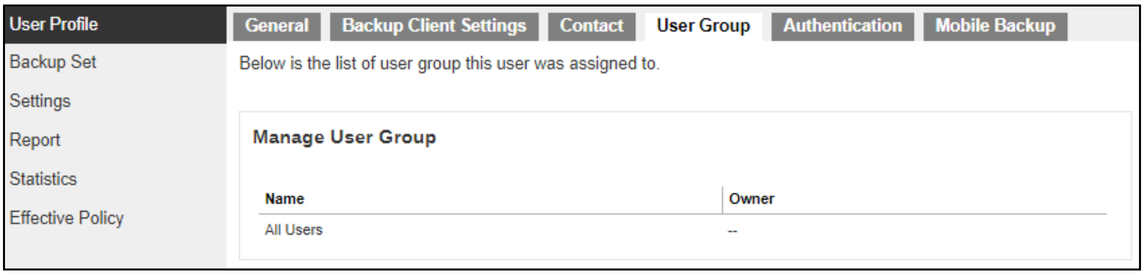
- To delete a contact information, check the box next to the contact information you want to delete, then click 🗑 in the middle of the screen. Click OK to delete the contact when prompted. The selected contact is deleted. Click 💾 to save your changes.



Are you sure that you want to delete selected rows ?

5.3.4 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.



Below is the list of user group this user was assigned to.

Manage User Group

Name	Owner
All Users	--

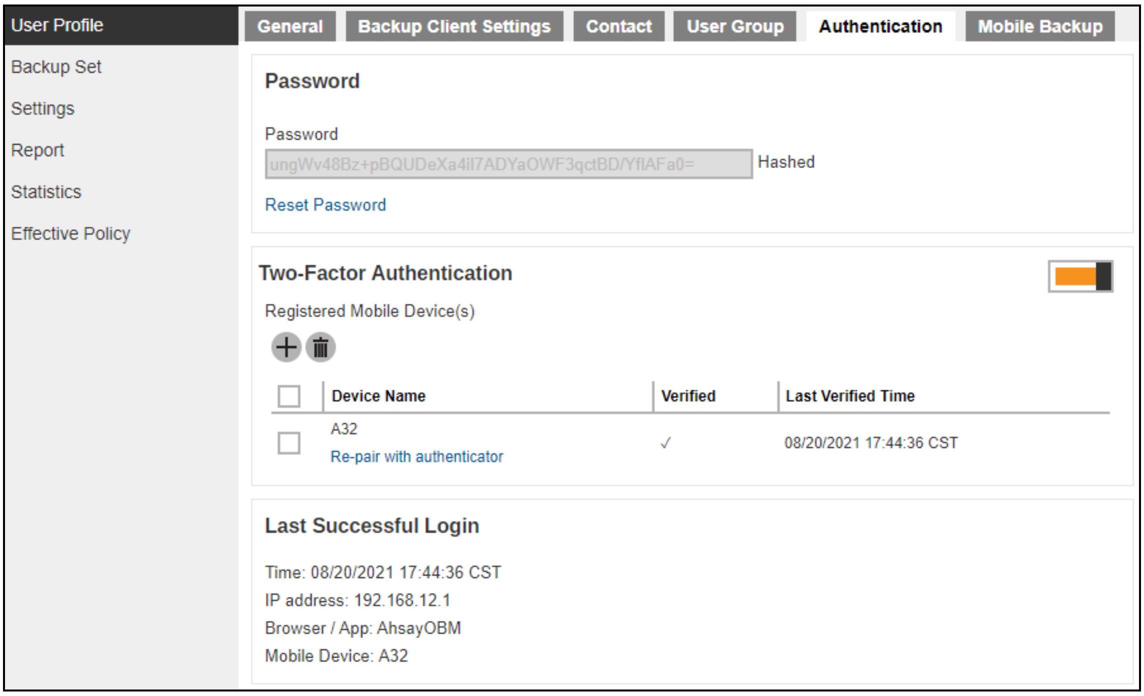
NOTE

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

5.3.5 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.



Password

Password

ungWv48Bz+pBQUDeXa4il7ADYaOWF3qctBD/YfIAFa0= Hashed

Reset Password

Two-Factor Authentication

Registered Mobile Device(s)

□	Device Name	Verified	Last Verified Time
□	A32 Re-pair with authenticator	✓	08/20/2021 17:44:36 CST

Last Successful Login

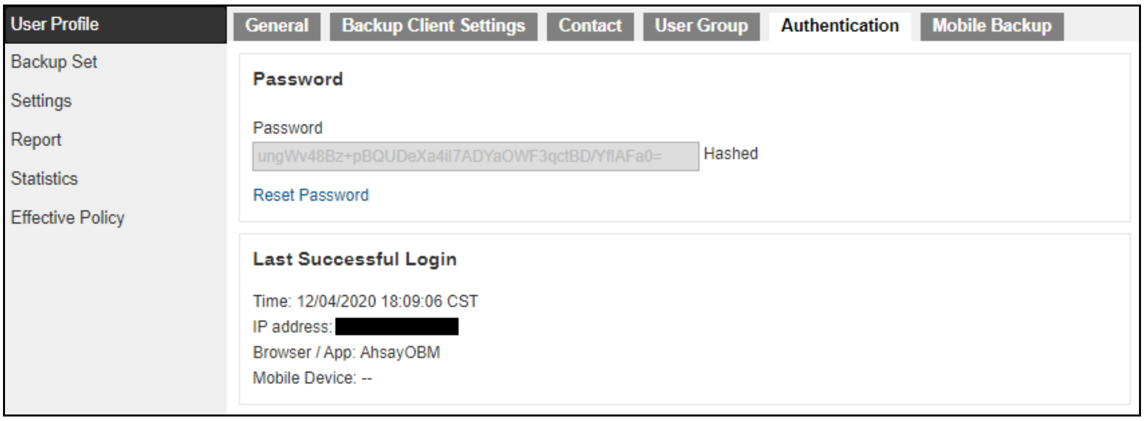
Time: 08/20/2021 17:44:36 CST

IP address: 192.168.12.1

Browser / App: AhsayOBM

Mobile Device: A32

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



Password

Password

ungWv48Bz+pBQUDeXa4il7ADYaOWF3qctBD/YfIAFa0= Hashed

Reset Password

Last Successful Login

Time: 12/04/2020 18:09:06 CST

IP address: [redacted]

Browser / App: AhsayOBM

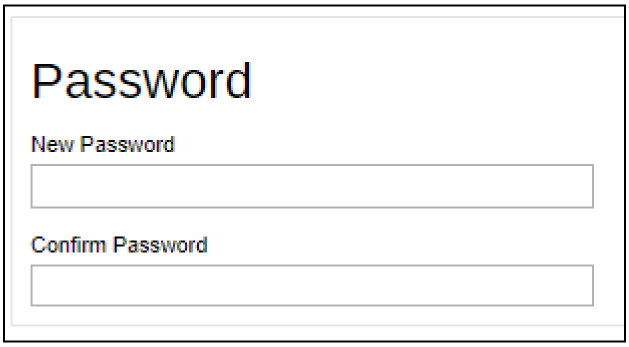
Mobile Device: --

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

Section	Description
Password	There are two (2) elements in the Password section, which are the following: • **Password** in hashed format defined by the service provider which cannot be changed. • **Reset Password** allows the backup user to change the password.
Two-Factor Authentication	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.

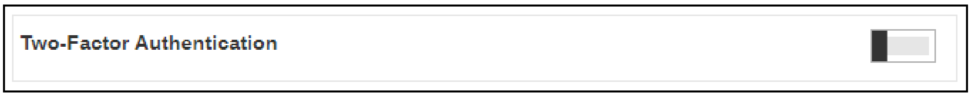
	This will only be visible if two-factor authentication is enabled for the user account. The **Re-pair with authenticator** will only be available if Ahsay Mobile is used as the authenticator app. If the registered device used for 2FA was damaged, lost or missing; the backup content of the device can 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. Please contact your backup service provider for details.
Last Successful Login	There are four (4) elements in the Last Successful Login section, which are the following: - **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.

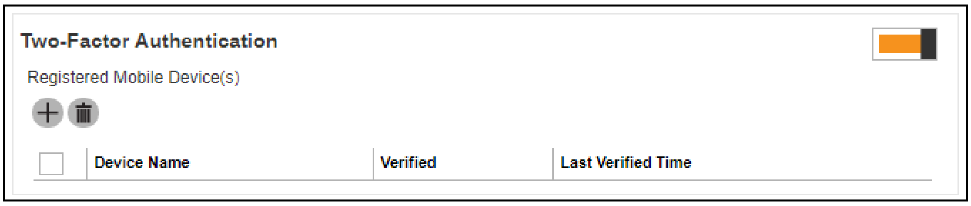


- To add a mobile device for two-factor authentication, follow the instructions below:

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



2. Click the ⊕ button.



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:

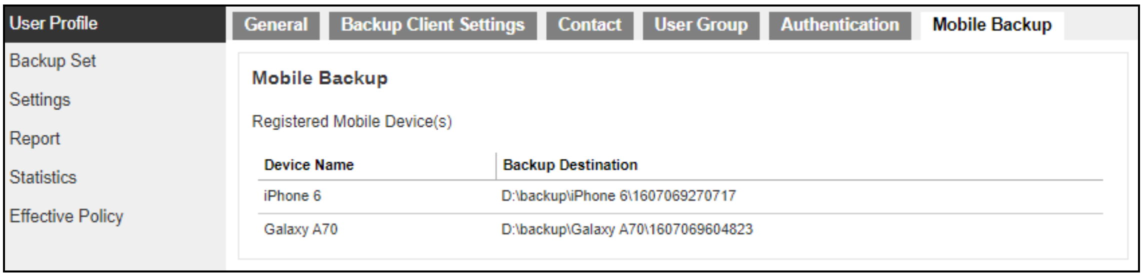
   - Ahsay Mobile or branded Mobile app
   - Microsoft Authenticator
   - Google Authenticator
   - Third party authenticators

5.3.6 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



Mobile Backup

Registered Mobile Device(s)

Device Name	Backup Destination
iPhone 6	D:\backup\iPhone 6\1607069270717
Galaxy A70	D:\backup\Galaxy A70\1607069604823

5.4 Settings

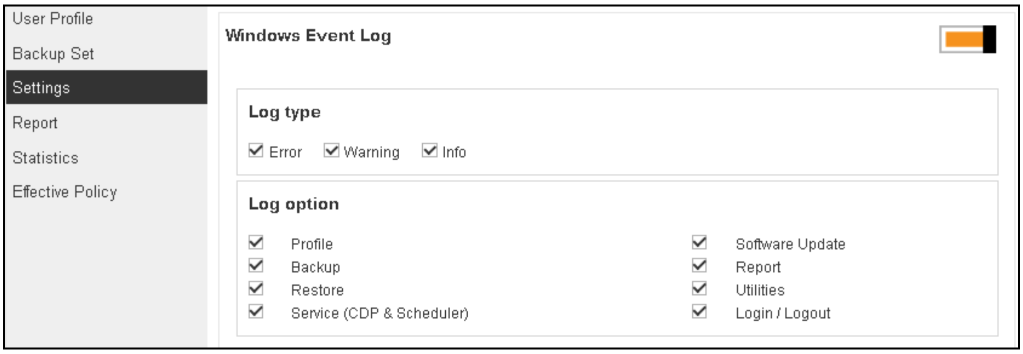
The **Settings** page allows the user to log the optional events, besides AhsayOBM/ AhsayACB logs, to the Windows event log.

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.



Windows Event Log

Log type

☑ Error ☑ Warning ☑ Info

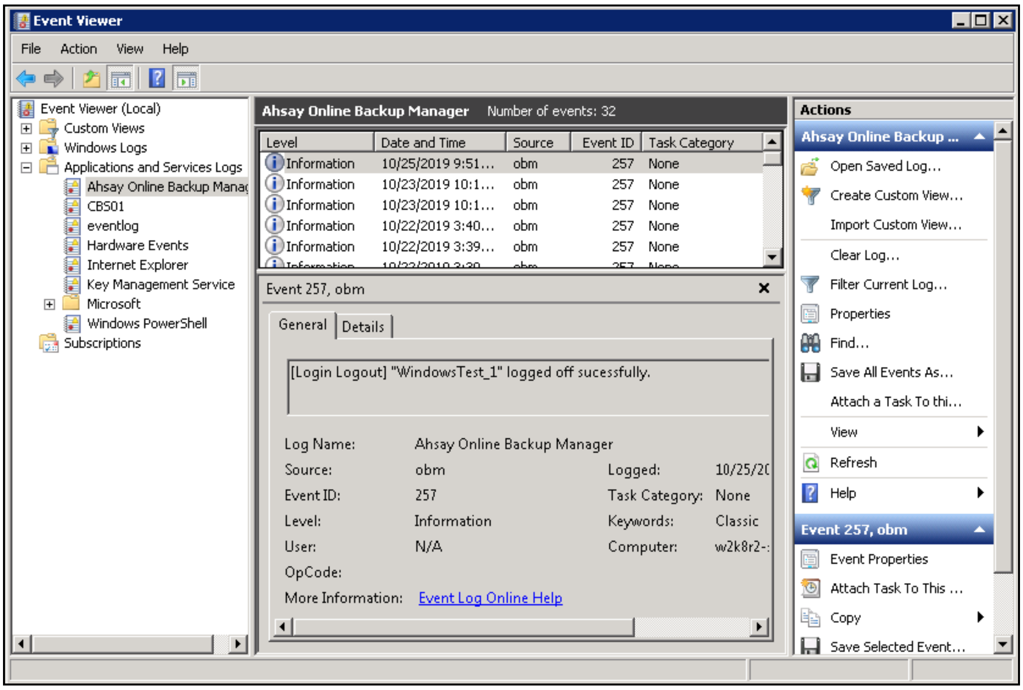
Log option

☑ Profile
☑ Backup
☑ Restore
☑ Service (CDP & Scheduler)
☑ Software Update
☑ Report
☑ Utilities
☑ 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:



Ahsay Online Backup Manager   Number of events: 32

Level	Date and Time	Source	Event ID	Task Category
Information	10/25/2019 9:51...	obm	257	None
Information	10/23/2019 10:1...	obm	257	None
Information	10/23/2019 10:1...	obm	257	None
Information	10/22/2019 3:40...	obm	257	None
Information	10/22/2019 3:39...	obm	257	None
Information	10/22/2019 3:39...	obm	257	None

Event 257, obm

General | Details

[Login Logout] "WindowsTest_1" logged off sucessfully.

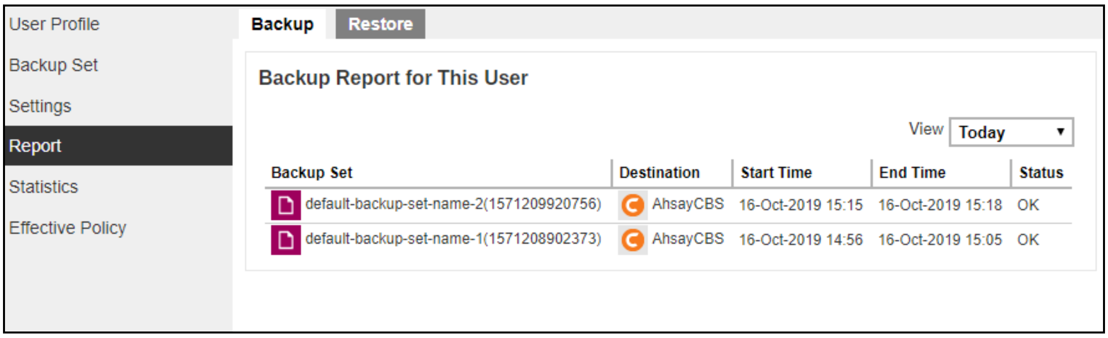
Log Name: Ahsay Online Backup Manager
Source: obm   Logged: 10/25/2C
Event ID: 257   Task Category: None
Level: Information   Keywords: Classic
User: N/A   Computer: w2k8r2-:
OpCode:
More Information: Event Log Online Help

5.5 Report

The **Report** tab 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.

5.5.1 Backup Reports

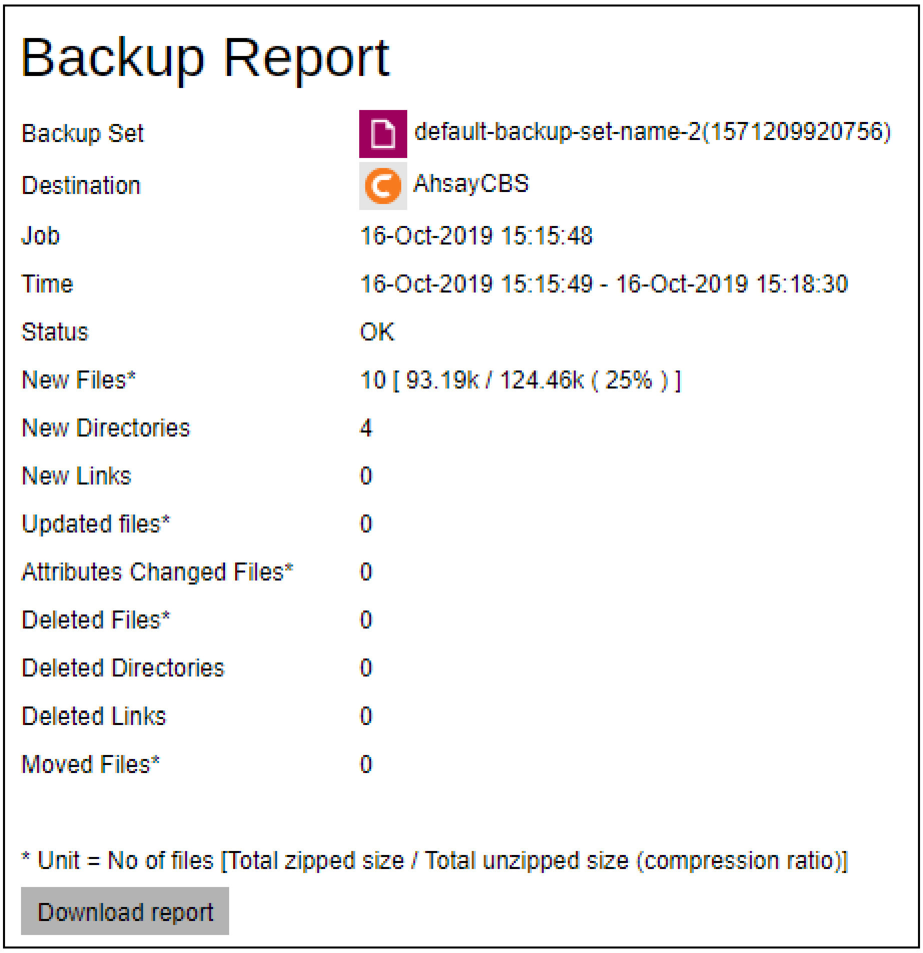
1. A list of backup reports for this AhsayCBS user can be found on the **Backup** tab. Click on the desired report to get more details on the report.



Backup Report for This User

Backup Set	Destination	Start Time	End Time	Status
default-backup-set-name-2(1571209920756)	AhsayCBS	16-Oct-2019 15:15	16-Oct-2019 15:18	OK
default-backup-set-name-1(1571208902373)	AhsayCBS	16-Oct-2019 14:56	16-Oct-2019 15:05	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.

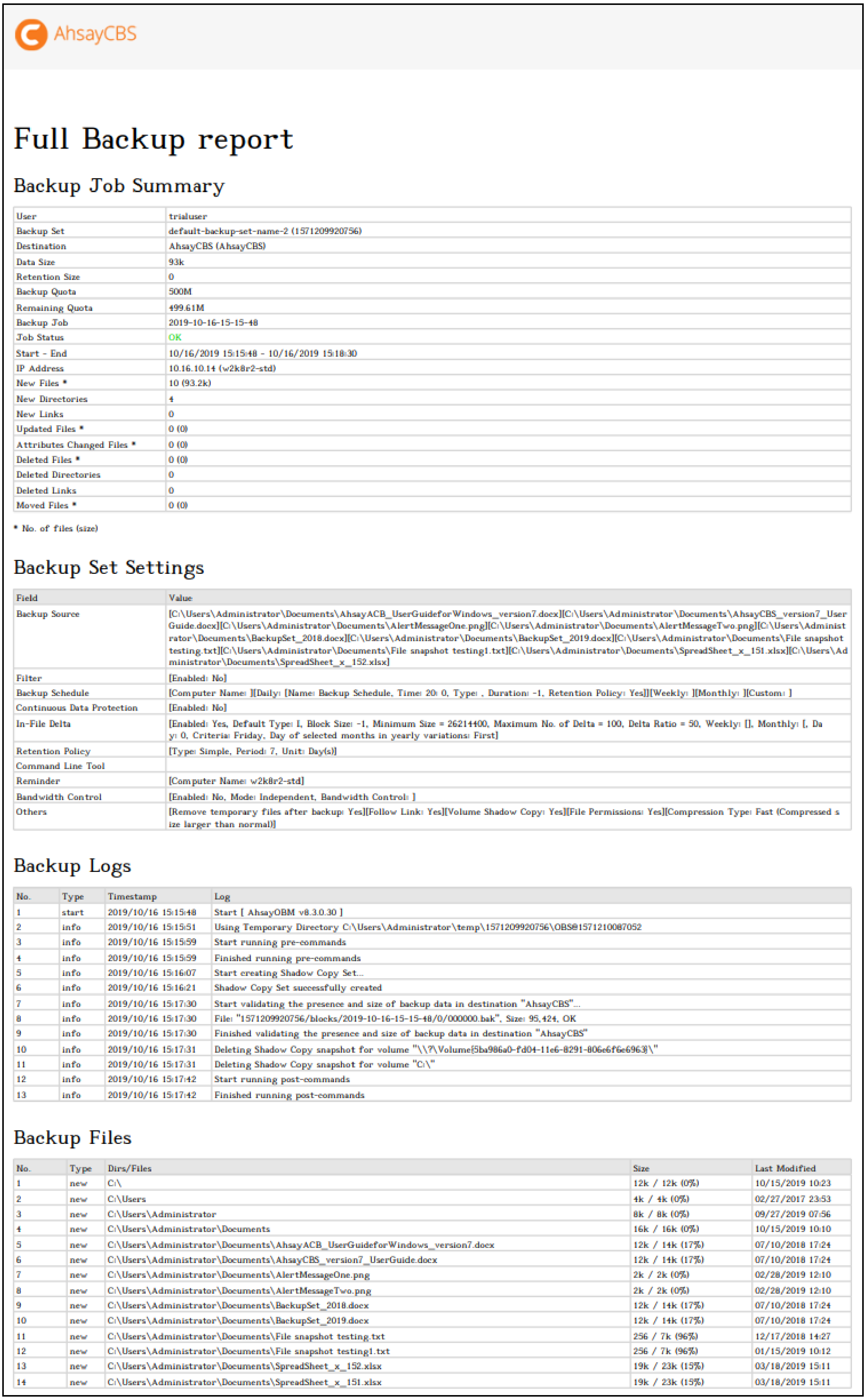


Backup Report

Backup Set	default-backup-set-name-2(1571209920756)
Destination	AhsayCBS
Job	16-Oct-2019 15:15:48
Time	16-Oct-2019 15:15:49 - 16-Oct-2019 15:18:30
Status	OK
New Files*	10 [93.19k / 124.46k (25%)]
New Directories	4
New Links	0
Updated files*	0
Attributes Changed Files*	0
Deleted Files*	0
Deleted Directories	0
Deleted Links	0
Moved Files*	0

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

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



AhsayCBS

Full Backup report

Backup Job Summary

User	trialuser
Backup Set	default-backup-set-name-2 (1571209920756)
Destination	AhsayCBS (AhsayCBS)
Data Size	93k
Retention Size	0
Backup Quota	500M
Remaining Quota	499.61M
Backup Job	2019-10-16-15-15-48
Job Status	OK
Start - End	10/16/2019 15:15:48 - 10/16/2019 15:18:30
IP Address	10.16.10.14 (w2k8r2-std)
New Files *	10 (93.2k)
New Directories	4
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)

* No. of files (size)

Backup Set Settings

Field	Value
Backup Source	[C:\Users\Administrator\Documents\AhsayACB_UserGuideforWindows_version7.docx][C:\Users\Administrator\Documents\AhsayCBS_version7_UserGuide.docx][C:\Users\Administrator\Documents\AlertMessageOne.png][C:\Users\Administrator\Documents\AlertMessageTwo.png][C:\Users\Administrator\Documents\BackupSet_2018.docx][C:\Users\Administrator\Documents\BackupSet_2019.docx][C:\Users\Administrator\Documents\File snapshot testing.txt][C:\Users\Administrator\Documents\File snapshot testing1.txt][C:\Users\Administrator\Documents\SpreadSheet_x_151.xlsx][C:\Users\Administrator\Documents\SpreadSheet_x_152.xlsx]
Filter	[Enabled: No]
Backup Schedule	[Computer Name:][Daily: [Name: Backup Schedule, Time: 20: 0, Type: , Duration: -1, Retention Policy: Yes]][Weekly:][Monthly:][Custom:]
Continuous Data Protection	[Enabled: No]
In-File Delta	[Enabled: Yes, Default Type: I, Block Size: -1, Minimum Size = 26214400, Maximum No. of Delta = 100, Delta Ratio = 50, Weekly: [], Monthly: [, Day: 0, Criteria: Friday, Day of selected months in yearly variations: First]
Retention Policy	[Type: Simple, Period: 7, Unit: Day(s)]
Command Line Tool	
Reminder	[Computer Name: w2k8r2-std]
Bandwidth Control	[Enabled: No, Mode: Independent, Bandwidth Control:]
Others	[Remove temporary files after backup: Yes][Follow Link: Yes][Volume Shadow Copy: Yes][File Permissions: Yes][Compression Type: Fast (Compressed size larger than normal)]

Backup Logs

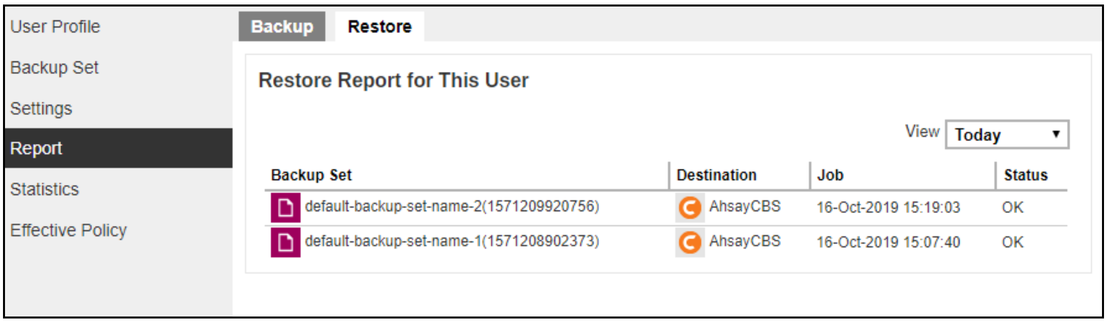
No.	Type	Timestamp	Log
1	start	2019/10/16 15:15:48	Start [AhsayOBM v8.3.0.30]
2	info	2019/10/16 15:15:51	Using Temporary Directory C:\Users\Administrator\temp\1571209920756\OBS@1571210087052
3	info	2019/10/16 15:15:59	Start running pre-commands
4	info	2019/10/16 15:15:59	Finished running pre-commands
5	info	2019/10/16 15:16:07	Start creating Shadow Copy Set...
6	info	2019/10/16 15:16:21	Shadow Copy Set successfully created
7	info	2019/10/16 15:17:30	Start validating the presence and size of backup data in destination "AhsayCBS"...
8	info	2019/10/16 15:17:30	File: "1571209920756/blocks/2019-10-16-15-15-48/0/000000.bak", Size: 95,424, OK
9	info	2019/10/16 15:17:30	Finished validating the presence and size of backup data in destination "AhsayCBS"
10	info	2019/10/16 15:17:31	Deleting Shadow Copy snapshot for volume "\\?\Volume{5ba986a0-fd04-11e6-8291-806e6f6e6963}\"
11	info	2019/10/16 15:17:31	Deleting Shadow Copy snapshot for volume "C:\"
12	info	2019/10/16 15:17:42	Start running post-commands
13	info	2019/10/16 15:17:42	Finished running post-commands

Backup Files

No.	Type	Dirs/Files	Size	Last Modified
1	new	C:\	12k / 12k (0%)	10/15/2019 10:23
2	new	C:\Users	4k / 4k (0%)	02/27/2017 23:53
3	new	C:\Users\Administrator	8k / 8k (0%)	09/27/2019 07:56
4	new	C:\Users\Administrator\Documents	16k / 16k (0%)	10/15/2019 10:10
5	new	C:\Users\Administrator\Documents\AhsayACB_UserGuideforWindows_version7.docx	12k / 14k (17%)	07/10/2018 17:24
6	new	C:\Users\Administrator\Documents\AhsayCBS_version7_UserGuide.docx	12k / 14k (17%)	07/10/2018 17:24
7	new	C:\Users\Administrator\Documents\AlertMessageOne.png	2k / 2k (0%)	02/28/2019 12:10
8	new	C:\Users\Administrator\Documents\AlertMessageTwo.png	2k / 2k (0%)	02/28/2019 12:10
9	new	C:\Users\Administrator\Documents\BackupSet_2018.docx	12k / 14k (17%)	07/10/2018 17:24
10	new	C:\Users\Administrator\Documents\BackupSet_2019.docx	12k / 14k (17%)	07/10/2018 17:24
11	new	C:\Users\Administrator\Documents\File snapshot testing.txt	256 / 7k (96%)	12/17/2018 14:27
12	new	C:\Users\Administrator\Documents\File snapshot testing1.txt	256 / 7k (96%)	01/15/2019 10:12
13	new	C:\Users\Administrator\Documents\SpreadSheet_x_152.xlsx	19k / 23k (15%)	03/18/2019 15:11
14	new	C:\Users\Administrator\Documents\SpreadSheet_x_151.xlsx	19k / 23k (15%)	03/18/2019 15:11

5.5.2 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.

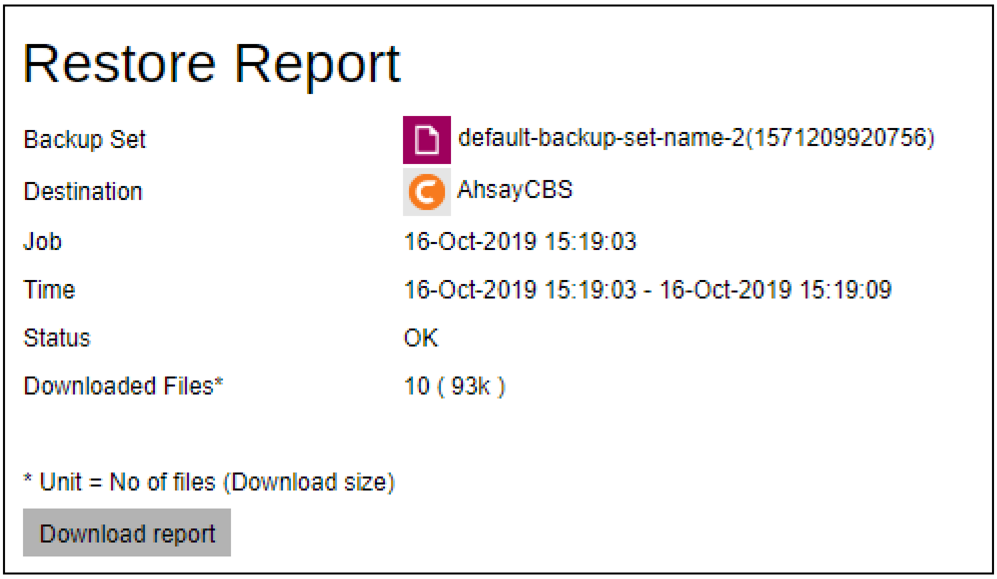


Restore Report for This User

View Today

Backup Set	Destination	Job	Status
default-backup-set-name-2(1571209920756)	AhsayCBS	16-Oct-2019 15:19:03	OK
default-backup-set-name-1(1571208902373)	AhsayCBS	16-Oct-2019 15:07:40	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.



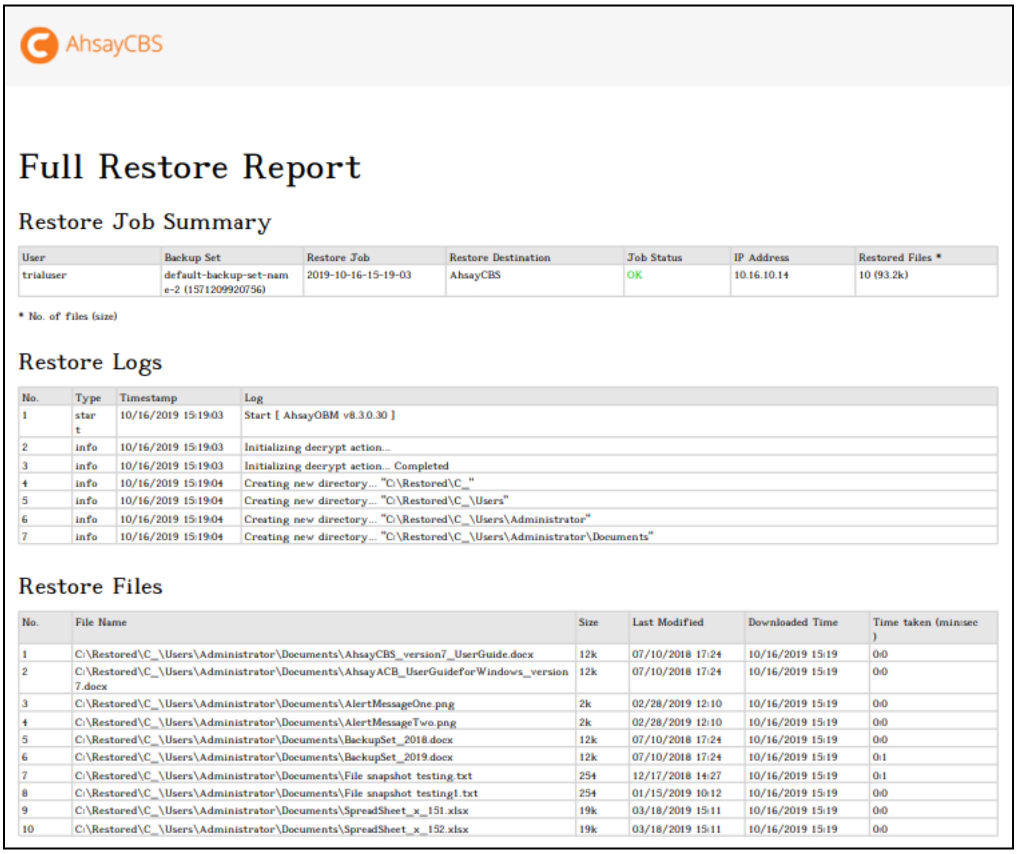
Restore Report

Backup Set	default-backup-set-name-2(1571209920756)
Destination	AhsayCBS
Job	16-Oct-2019 15:19:03
Time	16-Oct-2019 15:19:03 - 16-Oct-2019 15:19:09
Status	OK
Downloaded Files*	10 (93k)

* Unit = No of files (Download size)

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

i. Normal Restore



AhsayCBS

Full Restore Report

Restore Job Summary

User	Backup Set	Restore Job	Restore Destination	Job Status	IP Address	Restored Files *
trialuser	default-backup-set-name-2 (1571209920756)	2019-10-16-15-19-03	AhsayCBS	OK	10.16.10.14	10 (93.2k)

* No. of files (size)

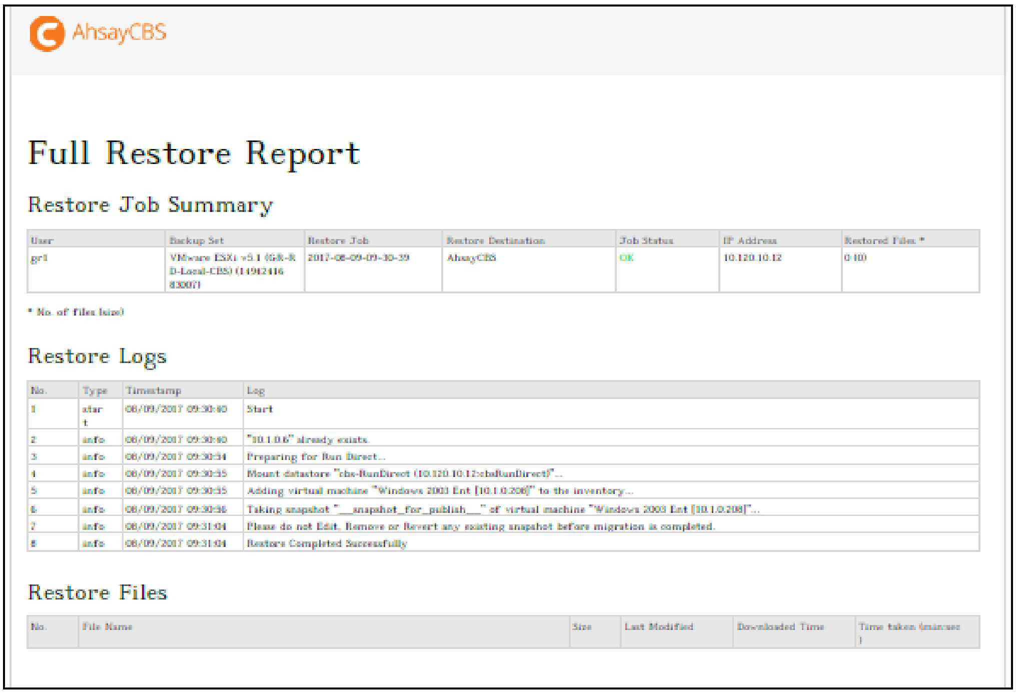
Restore Logs

No.	Type	Timestamp	Log
1	start	10/16/2019 15:19:03	Start [AhsayOBM v8.3.0.30]
2	info	10/16/2019 15:19:03	Initializing decrypt action...
3	info	10/16/2019 15:19:03	Initializing decrypt action... Completed
4	info	10/16/2019 15:19:04	Creating new directory... "C:\Restored\C_"
5	info	10/16/2019 15:19:04	Creating new directory... "C:\Restored\C_\Users"
6	info	10/16/2019 15:19:04	Creating new directory... "C:\Restored\C_\Users\Administrator"
7	info	10/16/2019 15:19:04	Creating new directory... "C:\Restored\C_\Users\Administrator\Documents"

Restore Files

No.	File Name	Size	Last Modified	Downloaded Time	Time taken (min:sec)
1	C:\Restored\C_\Users\Administrator\Documents\AhsayCBS_version7_UserGuide.docx	12k	07/10/2018 17:24	10/16/2019 15:19	0:0
2	C:\Restored\C_\Users\Administrator\Documents\AhsayACB_UserGuideforWindows_version7.docx	12k	07/10/2018 17:24	10/16/2019 15:19	0:0
3	C:\Restored\C_\Users\Administrator\Documents\AlertMessageOne.png	2k	02/28/2019 12:10	10/16/2019 15:19	0:0
4	C:\Restored\C_\Users\Administrator\Documents\AlertMessageTwo.png	2k	02/28/2019 12:10	10/16/2019 15:19	0:0
5	C:\Restored\C_\Users\Administrator\Documents\BackupSet_2018.docx	12k	07/10/2018 17:24	10/16/2019 15:19	0:0
6	C:\Restored\C_\Users\Administrator\Documents\BackupSet_2019.docx	12k	07/10/2018 17:24	10/16/2019 15:19	0:1
7	C:\Restored\C_\Users\Administrator\Documents\File snapshot testing.txt	254	12/17/2018 14:27	10/16/2019 15:19	0:1
8	C:\Restored\C_\Users\Administrator\Documents\File snapshot testing1.txt	254	01/15/2019 10:12	10/16/2019 15:19	0:0
9	C:\Restored\C_\Users\Administrator\Documents\SpreadSheet_x_151.xlsx	19k	03/18/2019 15:11	10/16/2019 15:19	0:0
10	C:\Restored\C_\Users\Administrator\Documents\SpreadSheet_x_152.xlsx	19k	03/18/2019 15:11	10/16/2019 15:19	0:0

ii. Run Direct Restore without Auto Migration.



AhsayCBS

Full Restore Report

Restore Job Summary

User	Backup Set	Restore Job	Restore Destination	Job Status	IP Address	Restored Files *
gr1	VMware ESXi v5.1 (GR-RD-Local-CBS) (1491241683007)	2017-08-09-09-30-39	AhsayCBS	OK	10.120.10.12	0 (0)

* No. of files (size)

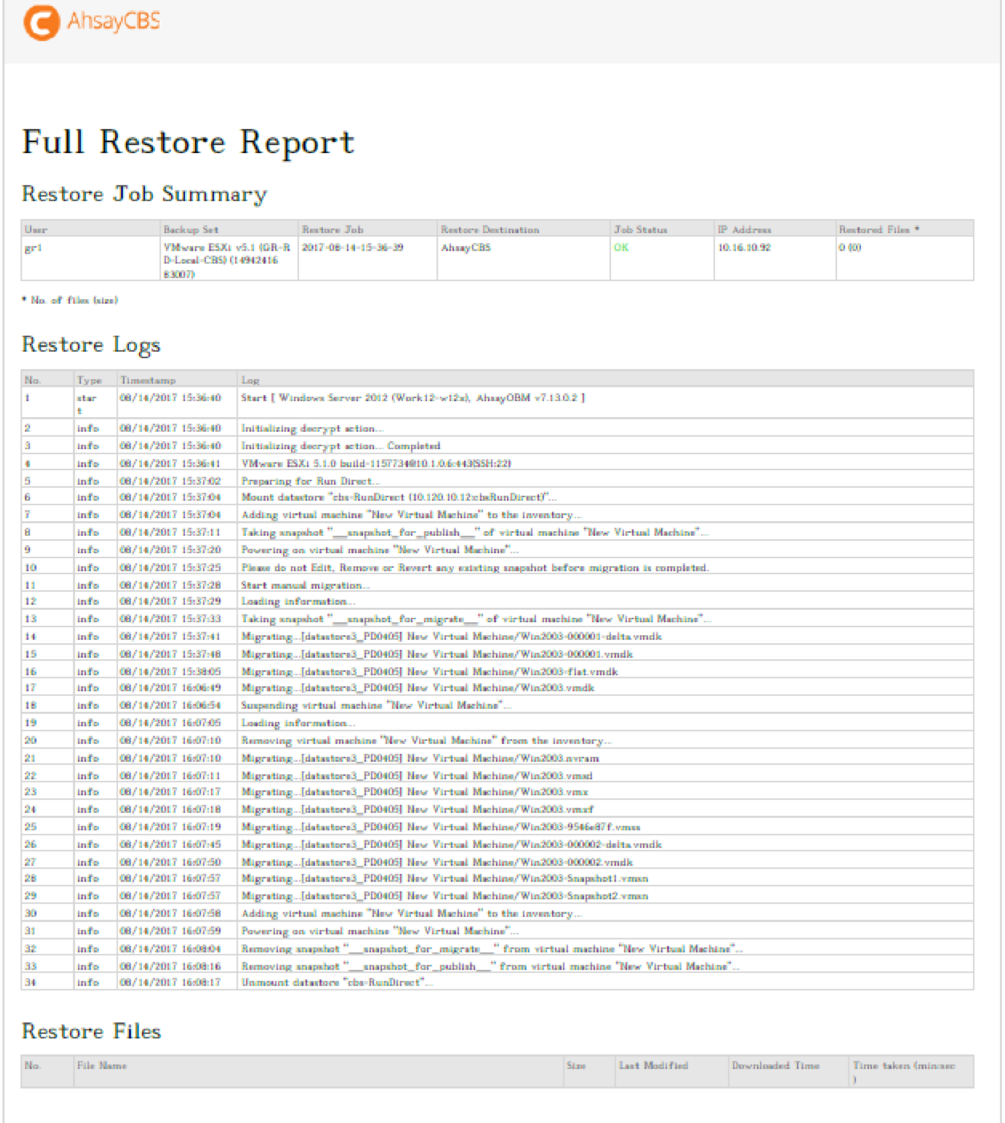
Restore Logs

No.	Type	Timestamp	Log
1	start	08/09/2017 09:30:40	Start
2	info	08/09/2017 09:30:40	"10.1.0.6" already exists.
3	info	08/09/2017 09:30:54	Preparing for Run Direct...
4	info	08/09/2017 09:30:55	Mount datastore "cbs-RunDirect (10.120.10.12:/cbsRunDirect)"...
5	info	08/09/2017 09:30:55	Adding virtual machine "Windows 2003 Ent [10.1.0.208]" to the inventory...
6	info	08/09/2017 09:30:56	Taking snapshot "__snapshot_for_publish__" of virtual machine "Windows 2003 Ent [10.1.0.208]"...
7	info	08/09/2017 09:31:04	Please do not Edit, Remove or Revert any existing snapshot before migration is completed.
8	info	08/09/2017 09:31:04	Restore Completed Successfully

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 *
gr1	VMware ESXi v5.1 (GR-RD-Local-CBS) (1494241683007)	2017-08-14-15-36-39	AhsayCBS	OK	10.16.10.92	0 (0)

* No. of files (size)

Restore Logs

No.	Type	Timestamp	Log
1	start	08/14/2017 15:36:40	Start [Windows Server 2012 (Work12-w12s), AhsayOBM v7.13.0.2]
2	info	08/14/2017 15:36:40	Initializing decrypt action...
3	info	08/14/2017 15:36:40	Initializing decrypt action... Completed
4	info	08/14/2017 15:36:41	VMware ESXi 5.1.0 build-1157734@10.1.0.6:443(SSH:22)
5	info	08/14/2017 15:37:02	Preparing for Run Direct...
6	info	08/14/2017 15:37:04	Mount datastore "cbs-RunDirect (10.120.10.12:cbsRunDirect)"...
7	info	08/14/2017 15:37:04	Adding virtual machine "New Virtual Machine" to the inventory...
8	info	08/14/2017 15:37:11	Taking snapshot "__snapshot_for_publish__" of virtual machine "New Virtual Machine"...
9	info	08/14/2017 15:37:20	Powering on virtual machine "New Virtual Machine"...
10	info	08/14/2017 15:37:25	Please do not Edit, Remove or Revert any existing snapshot before migration is completed.
11	info	08/14/2017 15:37:28	Start manual migration...
12	info	08/14/2017 15:37:29	Loading information...
13	info	08/14/2017 15:37:33	Taking snapshot "__snapshot_for_migrate__" of virtual machine "New Virtual Machine"...
14	info	08/14/2017 15:37:41	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003-000001-delta.vmdk
15	info	08/14/2017 15:37:48	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003-000001.vmdk
16	info	08/14/2017 15:38:05	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003-flat.vmdk
17	info	08/14/2017 16:06:49	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003.vmdk
18	info	08/14/2017 16:06:54	Suspending virtual machine "New Virtual Machine"...
19	info	08/14/2017 16:07:05	Loading information...
20	info	08/14/2017 16:07:10	Removing virtual machine "New Virtual Machine" from the inventory...
21	info	08/14/2017 16:07:10	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003.nvram
22	info	08/14/2017 16:07:11	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003.vmsd
23	info	08/14/2017 16:07:17	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003.vmx
24	info	08/14/2017 16:07:18	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003.vmxf
25	info	08/14/2017 16:07:19	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003-9546e87f.vmss
26	info	08/14/2017 16:07:45	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003-000002-delta.vmdk
27	info	08/14/2017 16:07:50	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003-000002.vmdk
28	info	08/14/2017 16:07:57	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003-Snapshot1.vmsn
29	info	08/14/2017 16:07:57	Migrating...[datastore3_PD0405] New Virtual Machine/Win2003-Snapshot2.vmsn
30	info	08/14/2017 16:07:58	Adding virtual machine "New Virtual Machine" to the inventory...
31	info	08/14/2017 16:07:59	Powering on virtual machine "New Virtual Machine"...
32	info	08/14/2017 16:08:04	Removing snapshot "__snapshot_for_migrate__" from virtual machine "New Virtual Machine"...
33	info	08/14/2017 16:08:16	Removing snapshot "__snapshot_for_publish__" from virtual machine "New Virtual Machine"...
34	info	08/14/2017 16:08:17	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 Office 365 and Cloud File backups.

5.6 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.

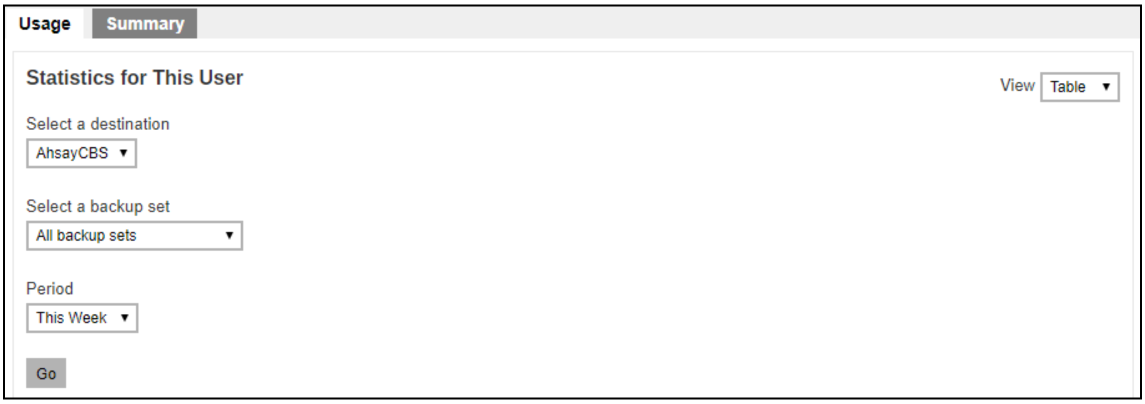
Storage statistics of a backup set are updated every time the following functions are run:

- 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



Statistics for This User

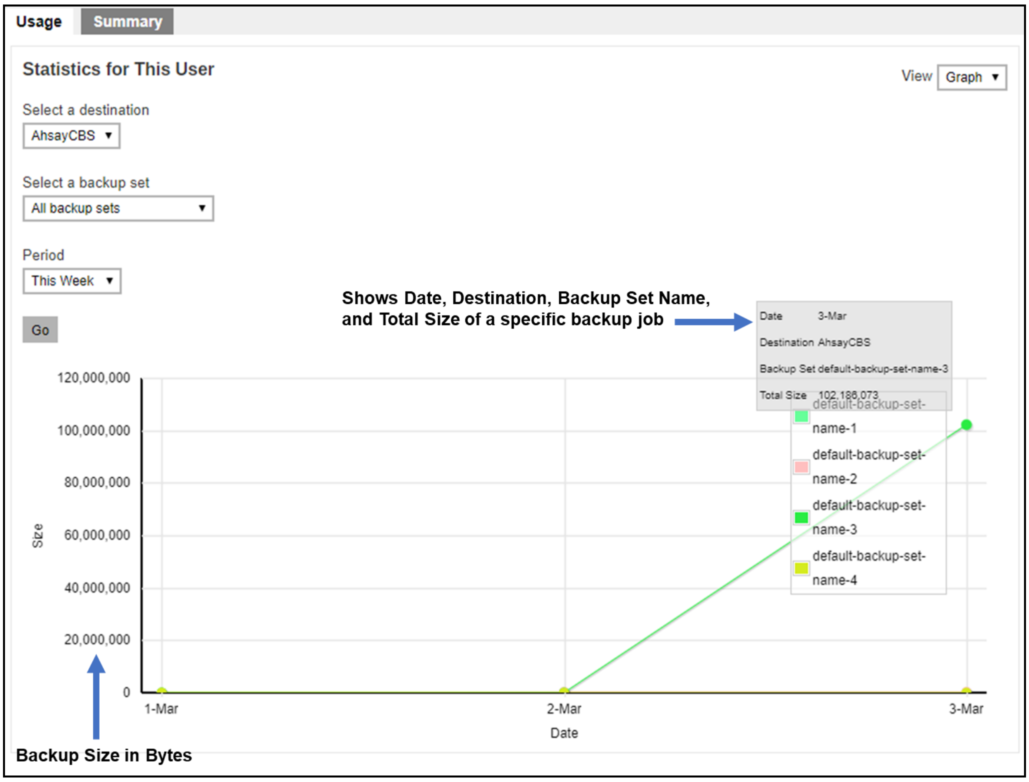
View: Table ▾

Select a destination: AhsayCBS ▾

Select a backup set: All backup sets ▾

Period: This Week ▾

Graph view



Statistics for This User

View: Graph

Select a destination: AhsayCBS

Select a backup set: All backup sets

Period: This Week

Shows Date, Destination, Backup Set Name, and Total Size of a specific backup job

Date 3-Mar

Destination AhsayCBS

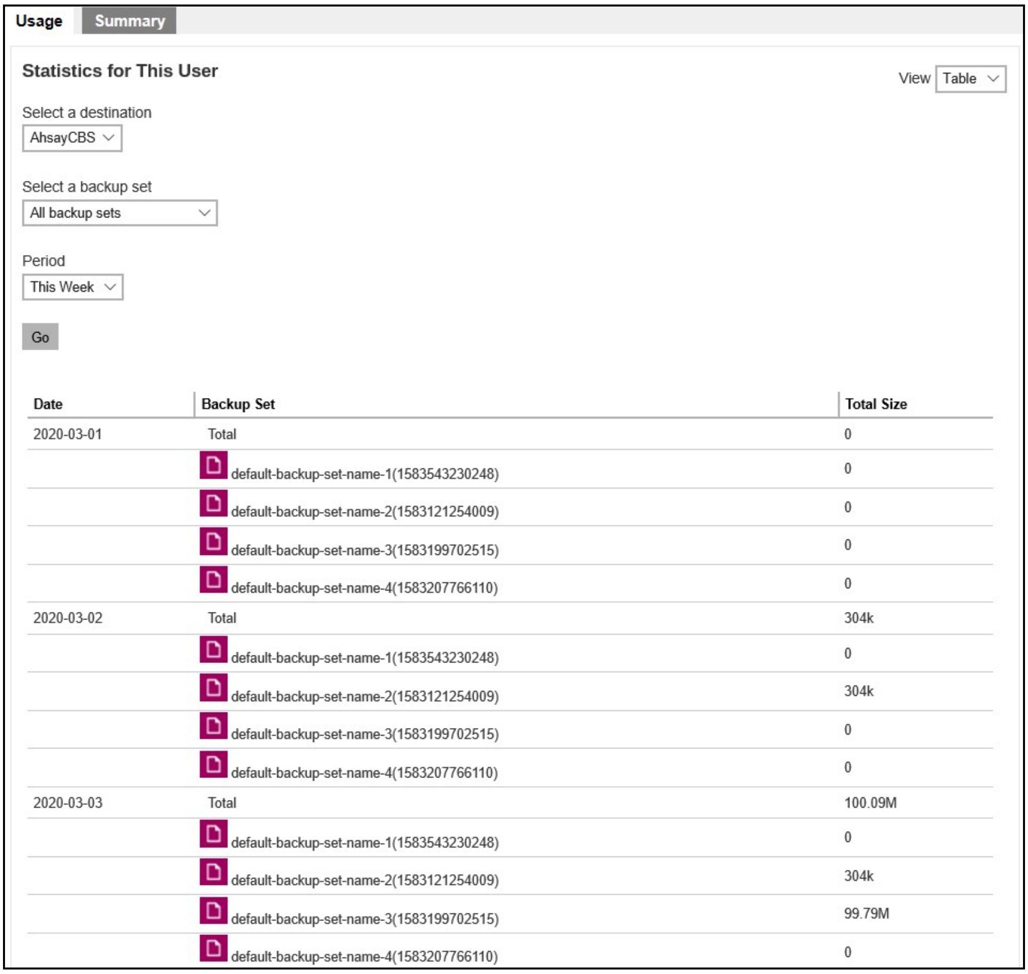
Backup Set default-backup-set-name-3

Total Size 102,186,073

120,000,000
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
0
Size
1-Mar
2-Mar
3-Mar
Date
default-backup-set-name-1
default-backup-set-name-2
default-backup-set-name-3
default-backup-set-name-4

Backup Size in Bytes

Table view



Statistics for This User

View: Table

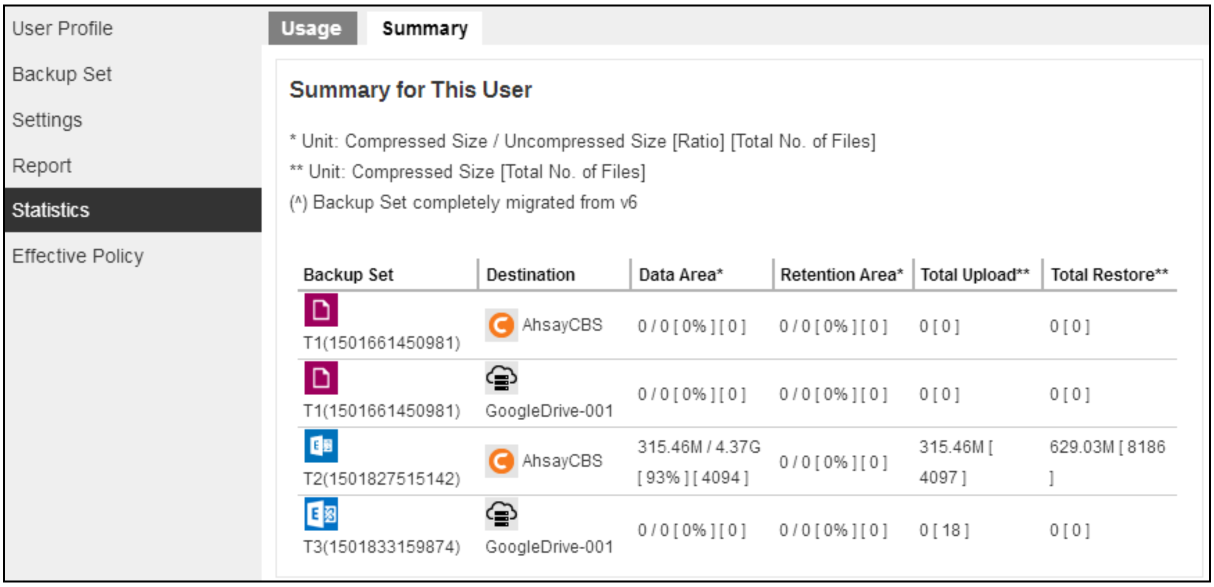
Select a destination: AhsayCBS

Select a backup set: All backup sets

Period: This Week

Date	Backup Set	Total Size
2020-03-01	Total	0
	default-backup-set-name-1(1583543230248)	0
	default-backup-set-name-2(1583121254009)	0
	default-backup-set-name-3(1583199702515)	0
	default-backup-set-name-4(1583207766110)	0
2020-03-02	Total	304k
	default-backup-set-name-1(1583543230248)	0
	default-backup-set-name-2(1583121254009)	304k
	default-backup-set-name-3(1583199702515)	0
	default-backup-set-name-4(1583207766110)	0
2020-03-03	Total	100.09M
	default-backup-set-name-1(1583543230248)	0
	default-backup-set-name-2(1583121254009)	304k
	default-backup-set-name-3(1583199702515)	99.79M
	default-backup-set-name-4(1583207766110)	0

Summary



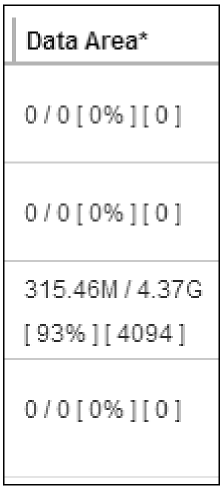
Summary for This User

* Unit: Compressed Size / Uncompressed Size [Ratio] [Total No. of Files]
** Unit: Compressed Size [Total No. of Files]
(^) Backup Set completely migrated from v6

Backup Set	Destination	Data Area*	Retention Area*	Total Upload**	Total Restore**
T1(1501661450981)	AhsayCBS	0 / 0 [0%] [0]	0 / 0 [0%] [0]	0 [0]	0 [0]
T1(1501661450981)	GoogleDrive-001	0 / 0 [0%] [0]	0 / 0 [0%] [0]	0 [0]	0 [0]
T2(1501827515142)	AhsayCBS	315.46M / 4.37G [93%] [4094]	0 / 0 [0%] [0]	315.46M [4097]	629.03M [8186]
T3(1501833159874)	GoogleDrive-001	0 / 0 [0%] [0]	0 / 0 [0%] [0]	0 [18]	0 [0]

There are 4 columns showing the following information of each backup set.

Data Area



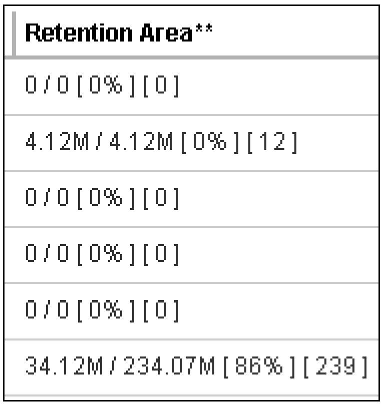
Data Area*
0 / 0 [0%] [0]
0 / 0 [0%] [0]
315.46M / 4.37G [93%] [4094]
0 / 0 [0%] [0]

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

Example: 315.46M / 4.37G [93%] [4094]

The data interpreted as the backup set has 4094 files in the data area; the files compressed, and uncompressed sizes are 315.64M and 4.37G respectively; the compression ratio is 93%.

Retention Area



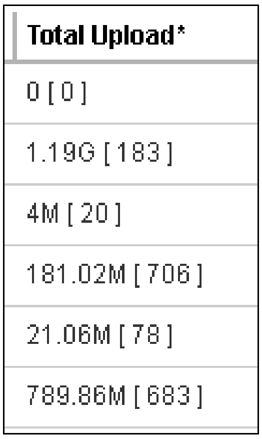
Retention Area**
0 / 0 [0%] [0]
4.12M / 4.12M [0%] [12]
0 / 0 [0%] [0]
0 / 0 [0%] [0]
0 / 0 [0%] [0]
34.12M / 234.07M [86%] [239]

Format:
[Compressed Size] / [Uncompressed Size] [Compression Ratio in %] [Total number of files]

Example: 34.12M / 234.07M [86%] [239]

The data interpreted as the backup set has 239 files in the retention area; the files compressed, and uncompressed sizes are 34.12M and 234.07M respectively; the compression ratio is 86%.

Total Upload



Total Upload*
0 [0]
1.19G [183]
4M [20]
181.02M [706]
21.06M [78]
789.86M [683]

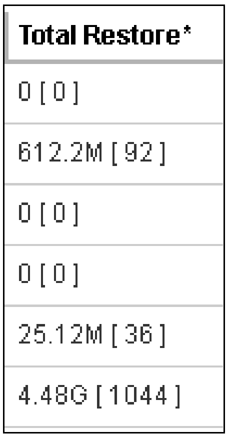
Format:
[Compressed Size] [Total number of files]

Example: 4M [20]

There is a total of 20 files sized of 4M uploaded for this backup set.

The Total Upload is 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*
0 [0]
612.2M [92]
0 [0]
0 [0]
25.12M [36]
4.48G [1044]

Format:
[Compressed Size] [Total number of files]

Example: 612.2M [92]

There is a total of 92 files sized of 612.2M restored from this backup set.

5.7 Effective Policy

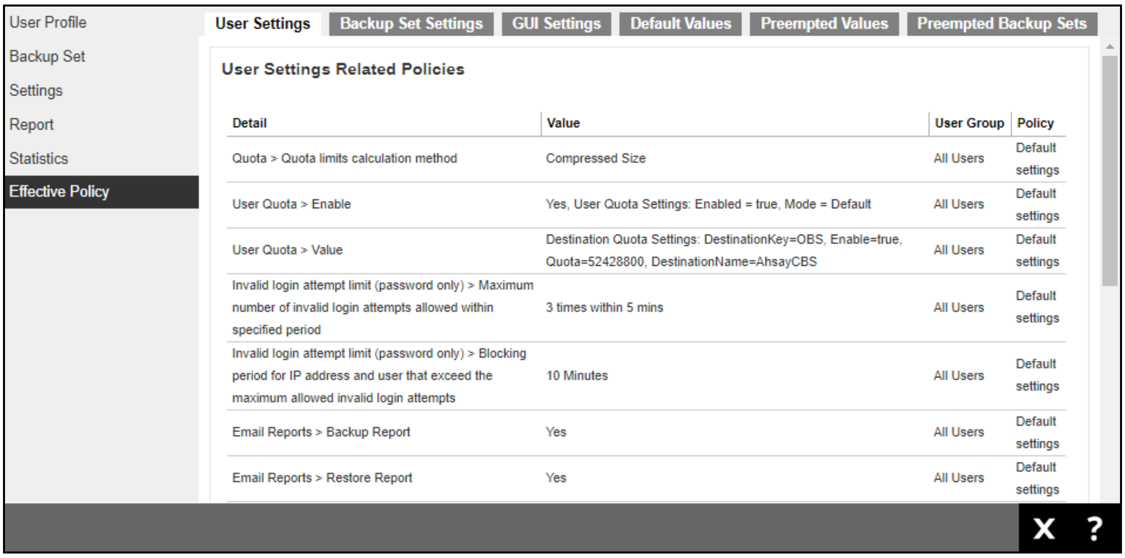
NOTE

Effective Policy tab 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.

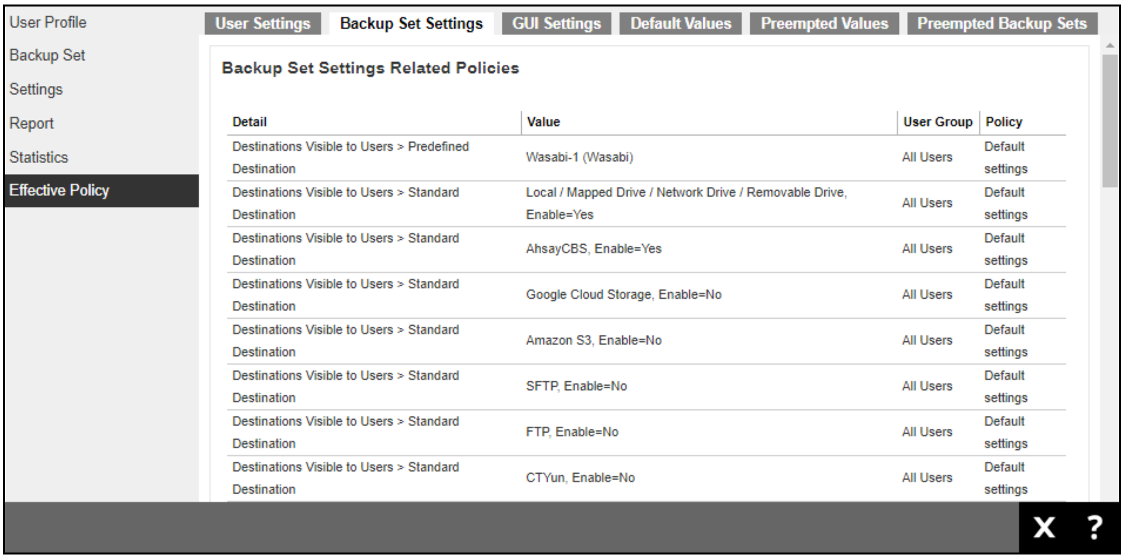


User Settings Related Policies

Detail	Value	User Group	Policy
Quota > Quota limits calculation method	Compressed Size	All Users	Default settings
User Quota > Enable	Yes, User Quota Settings: Enabled = true, Mode = Default	All Users	Default settings
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.

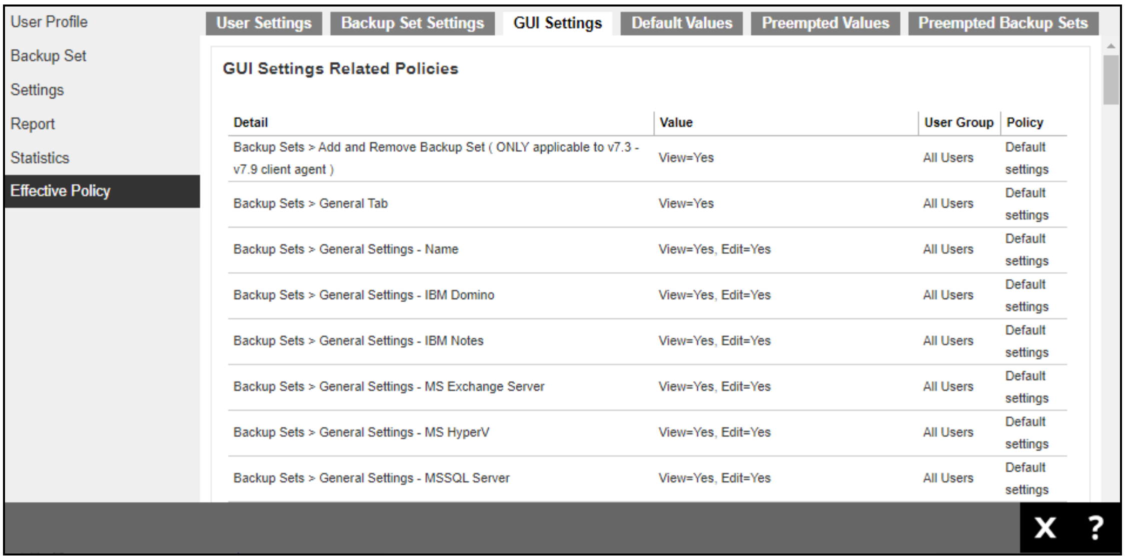


Backup Set Settings Related Policies

Detail	Value	User Group	Policy
Destinations Visible to Users > Predefined Destination	Wasabi-1 (Wasabi)	All Users	Default settings
Destinations Visible to Users > Standard Destination	Local / Mapped Drive / Network Drive / Removable Drive, Enable=Yes	All Users	Default settings
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.

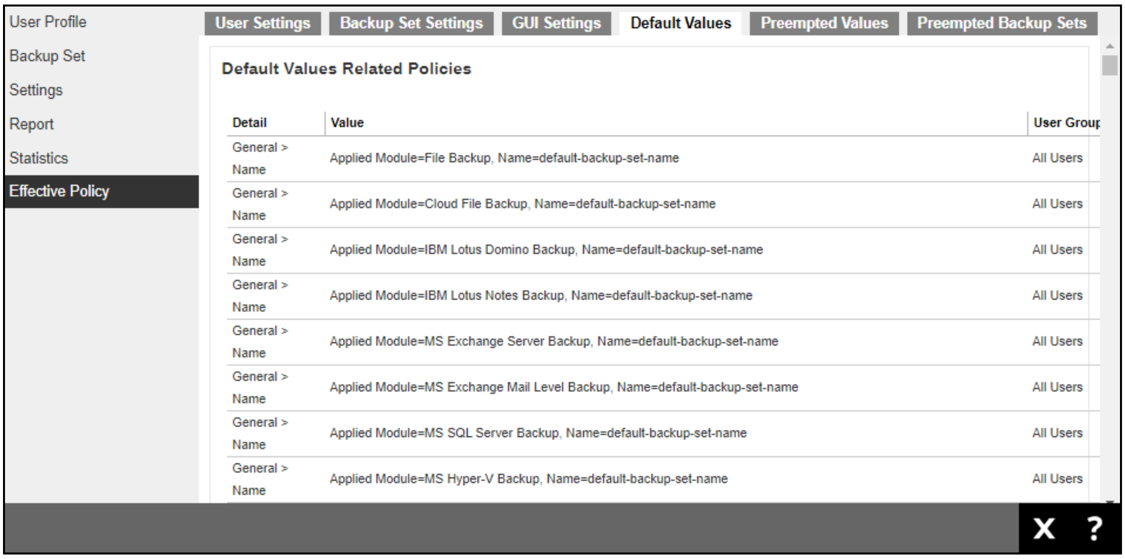


GUI Settings Related Policies

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

Default Values Tab

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

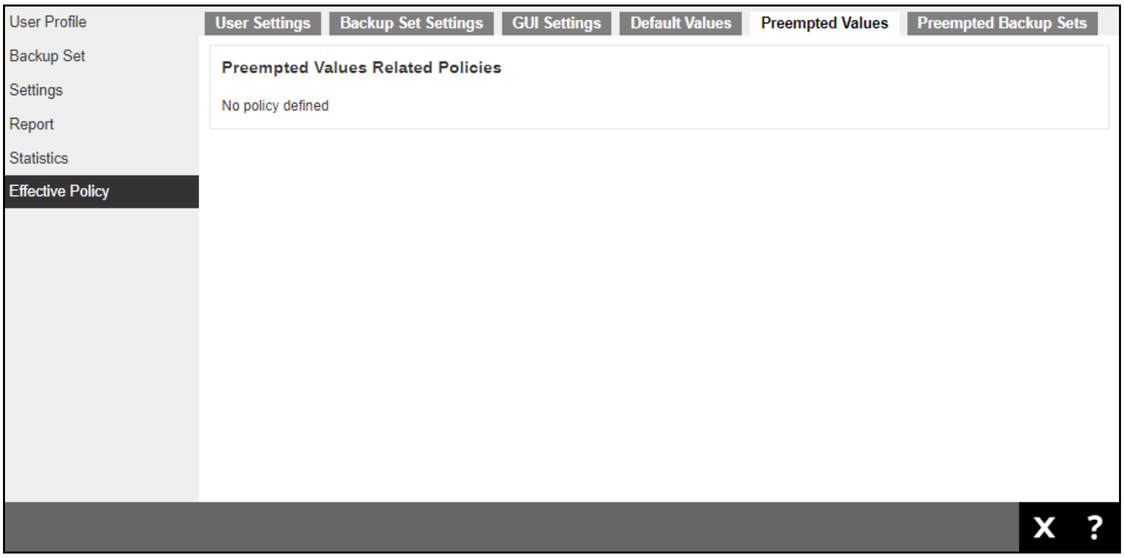


Default Values Related Policies

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

Preempted Values Tab

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

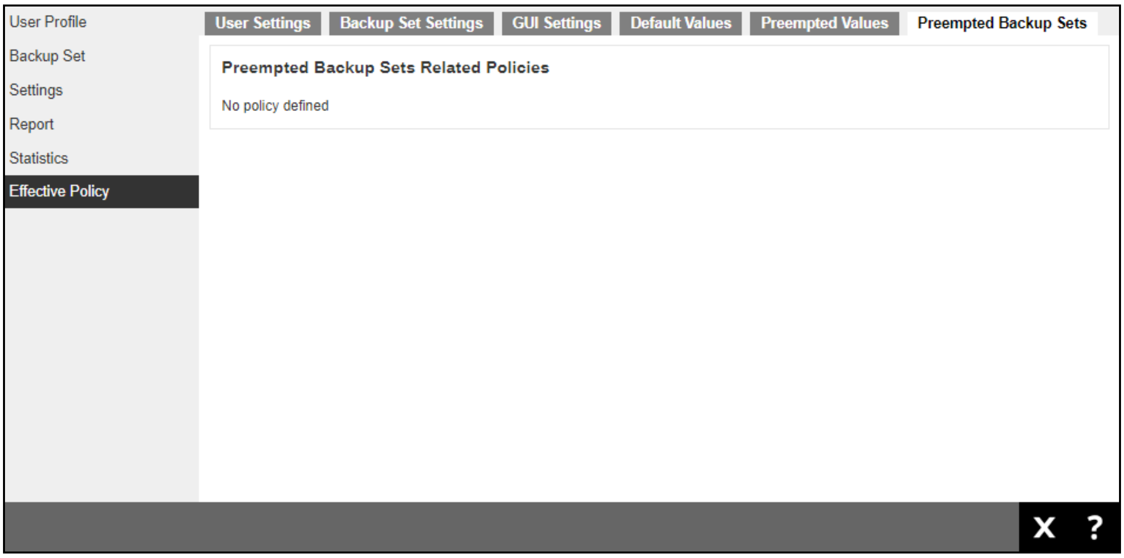


Preempted Values Related Policies

No policy defined

Preempted Backup Sets Tab

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



Preempted Backup Sets Related Policies

No policy defined

6 Monitoring Live Activities

6.1 Managing Live Activities

1. Login 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

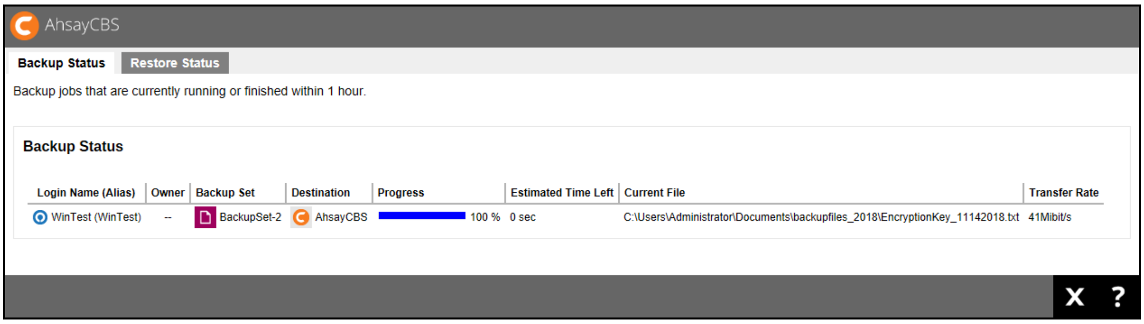
If there are any backup and restore jobs which are unexpectedly terminated or crashed the job status should automatically clear after 72 hours.

6.2 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
Office 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



Backup jobs that are currently running or finished within 1 hour.

Backup Status

Login Name (Alias)	Owner	Backup Set	Destination	Progress	Estimated Time Left	Current File	Transfer Rate
WinTest (WinTest)	--	BackupSet-2	AhsayCBS	100 %	0 sec	C:\Users\Administrator\Documents\backupfiles_2018\EncryptionKey_11142018.txt	41Mibit/s

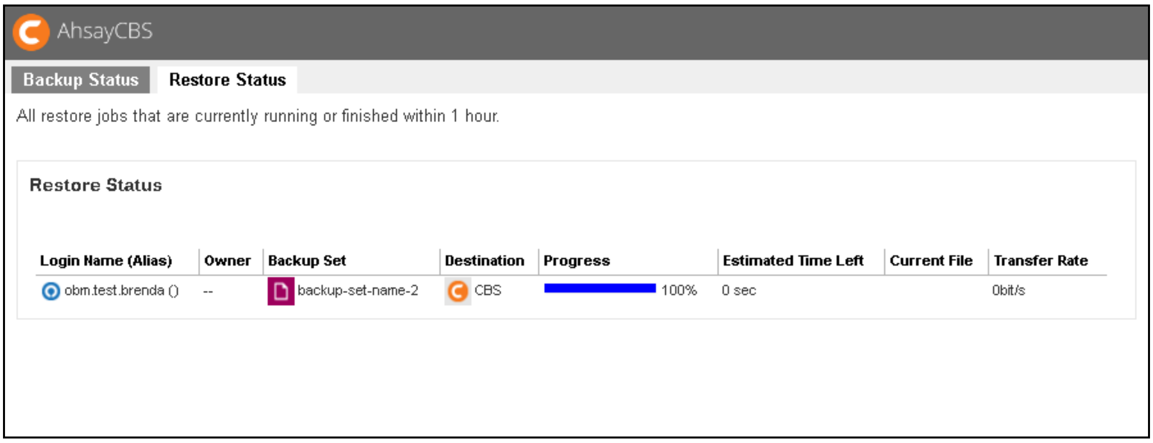
6.3 Restore Status

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	✗	✗	✗	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	✗	NA	✗	NA
MS SQL Server Backup		✓	NA	✓	NA
MySQL Backup		✓	NA	✓	NA
Office 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	✗	NA	✗	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.



All restore jobs that are currently running or finished within 1 hour.

Restore Status

Login Name (Alias)	Owner	Backup Set	Destination	Progress	Estimated Time Left	Current File	Transfer Rate
obm.test.brenda ()	--	backup-set-name-2	CBS	100%	0 sec		0bit/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.

7 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 Office 365 and Cloud File.

Agent-based

Cloud File

- AhsayACB v8 User Guide – Cloud File Backup & Restore for Windows
- AhsayACB v8 User Guide – Cloud File Backup & Restore for Mac
- AhsayOBM v8 User Guide – Cloud File Backup & Restore for Windows
- AhsayOBM v8 User Guide – Cloud File Backup & Restore for Mac

Office 365

- AhsayACB v8 User Guide - Office365 Backup & Restore for Windows
- AhsayACB v8 User Guide - Office365 Backup & Restore for Mac
- AhsayOBM v8 User Guide - Office365 Backup & Restore for Windows
- AhsayOBM v8 User Guide - Office365 Backup & Restore for Mac

Agentless

Cloud File – Cloud File Run on Server (Agentless) Backup and Restore Guide

Office 365 – Office 365 Run on Server (Agentless) Backup and Restore Guide

The links above will redirect you to the user guides of Office 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).

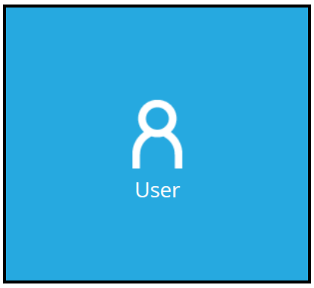
7.1 Create Backup Set (Generic Steps)

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.

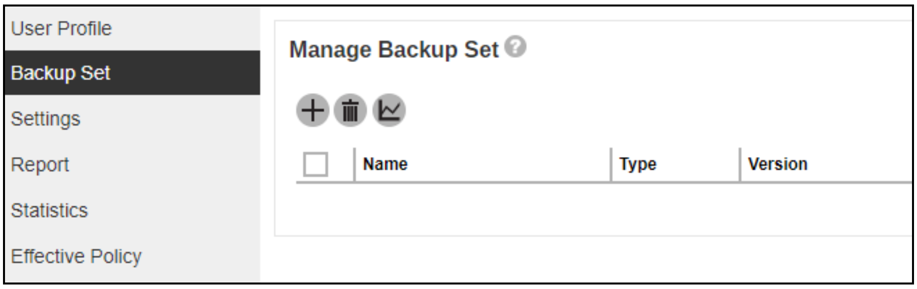
To add a new backup set, do the following:

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

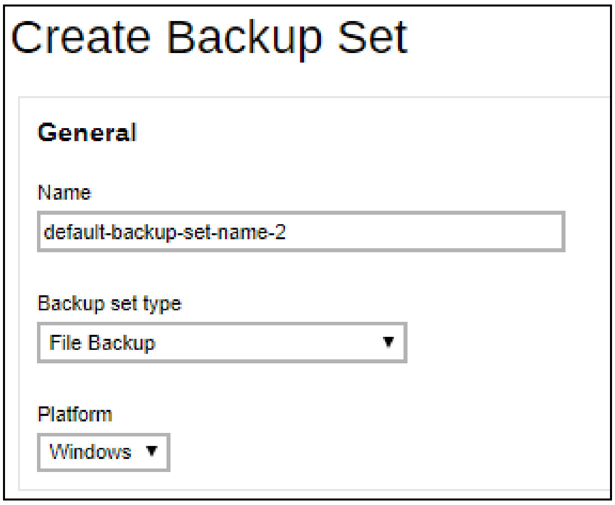
Also select the operating system used for the backup client from the **Platform** dropdown box. The choices for the platform are:

- Windows
- Mac
- Linux

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

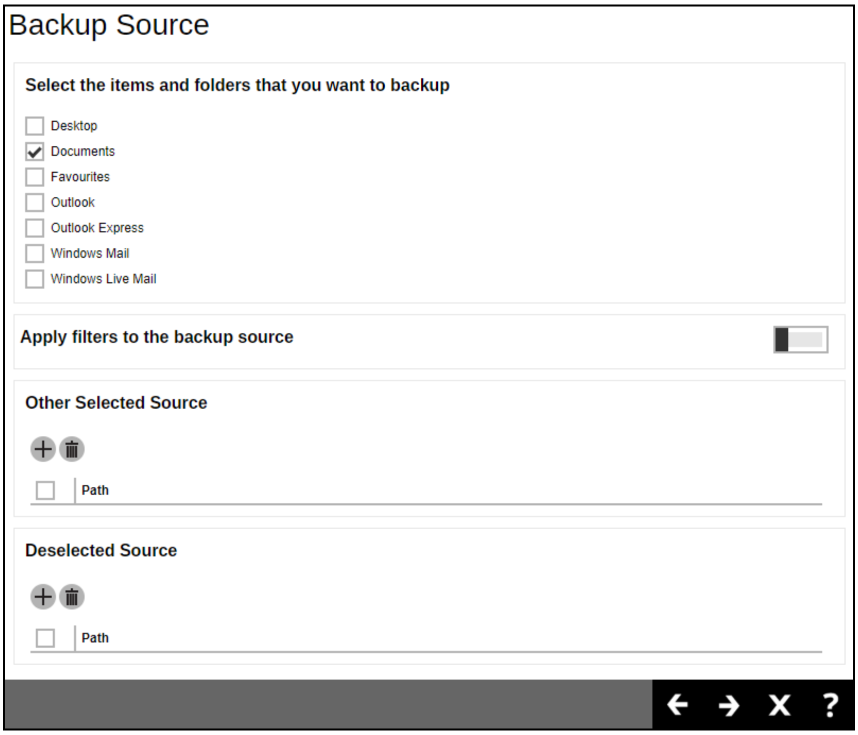
General

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

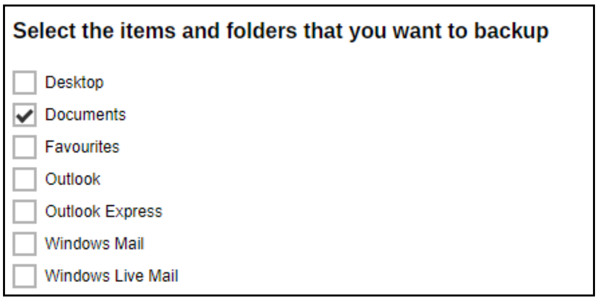
□ Path

Deselected Source

□ Path

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).

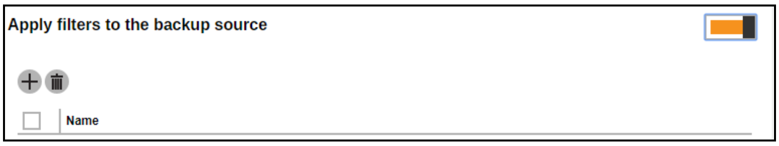


Select the items and folders that you want to backup

□ 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.

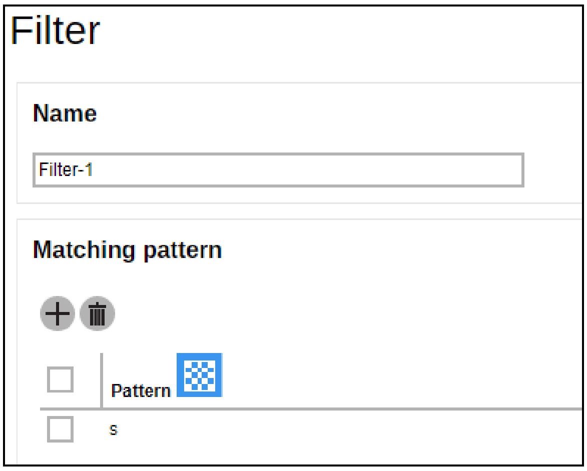
Turn on **Apply filters to the backup source** and click ⊕ to create a filter.



Apply filters to the backup source

□ Name

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



Filter

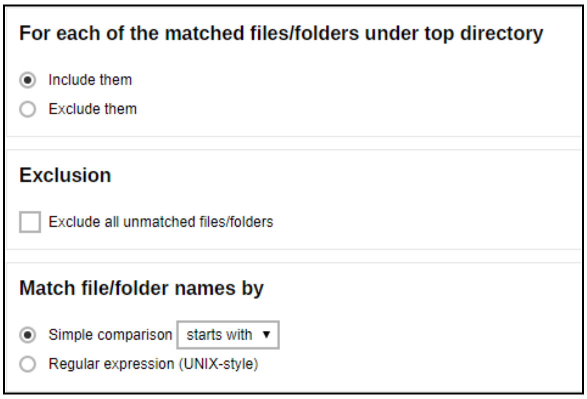
Name

Filter-1

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

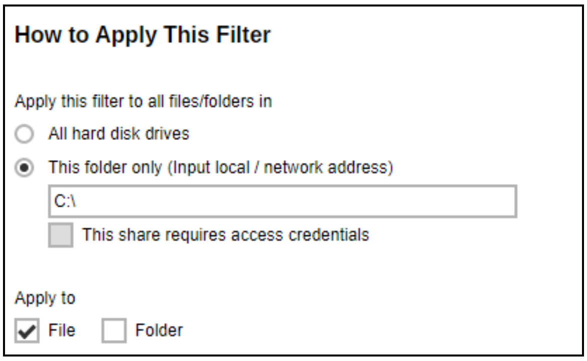
Exclusion

□ Exclude all unmatched files/folders

Match file/folder names by

● Simple comparison starts with ▾
○ 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)

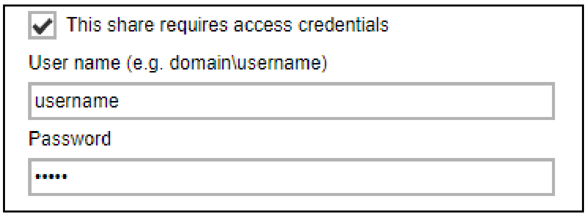
C:\

□ 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)

username

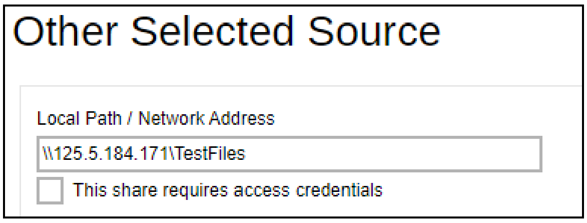
Password

•••••

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**.



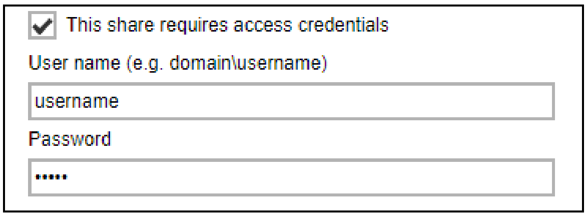
Other Selected Source

Local Path / Network Address

\\125.5.184.171\TestFiles

□ 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

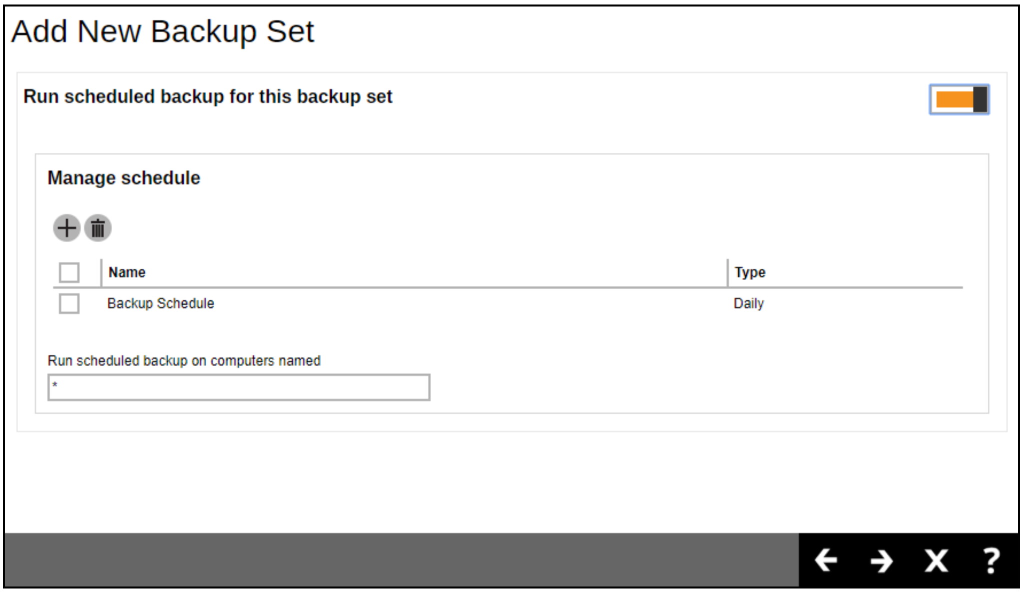
•••••

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.



Add New Backup Set

Run scheduled backup for this backup set

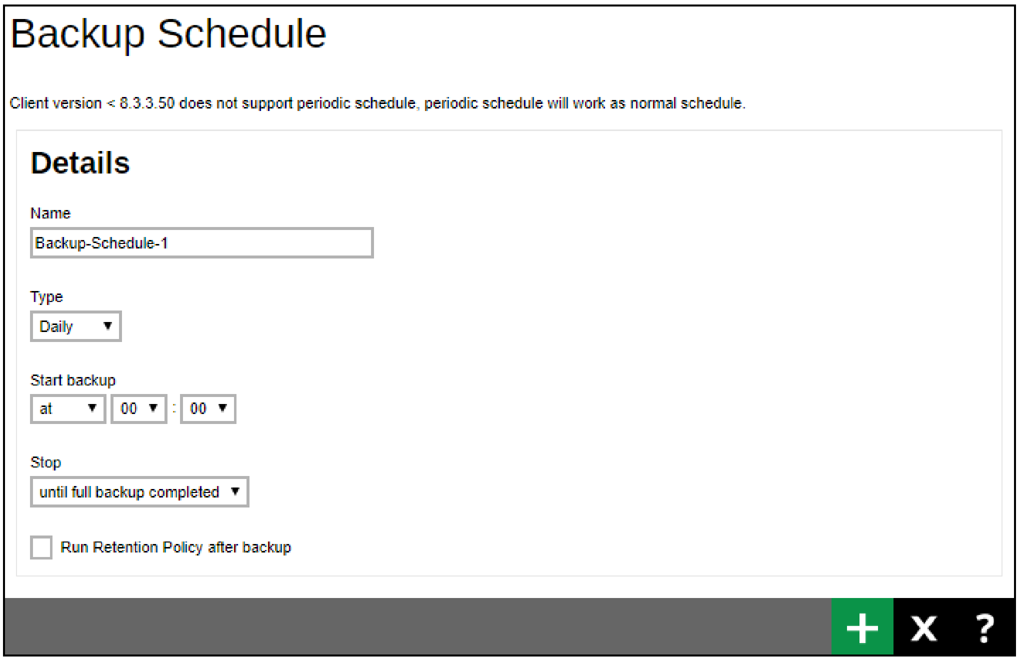
Manage schedule

□	Name	Type
□	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 < 8.3.3.50 does not support periodic schedule, periodic schedule will work as normal schedule.

Details

Name

Backup-Schedule-1

Type

Daily ▼

Start backup

at ▼ 00 ▼ : 00 ▼

Stop

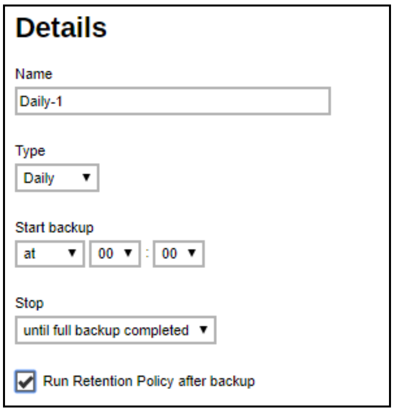
until full backup completed ▼

□ 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

Daily-1

Type

Daily ▼

Start backup

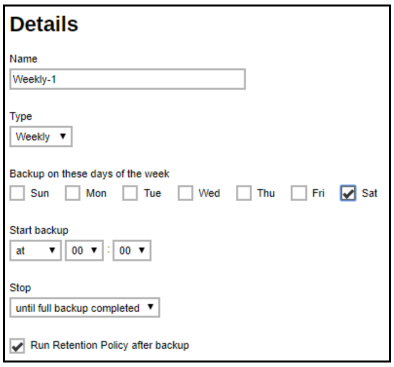
at ▼ 00 ▼ : 00 ▼

Stop

until full backup completed ▼

☑ 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

Weekly-1

Type

Weekly ▼

Backup on these days of the week

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat

Start backup

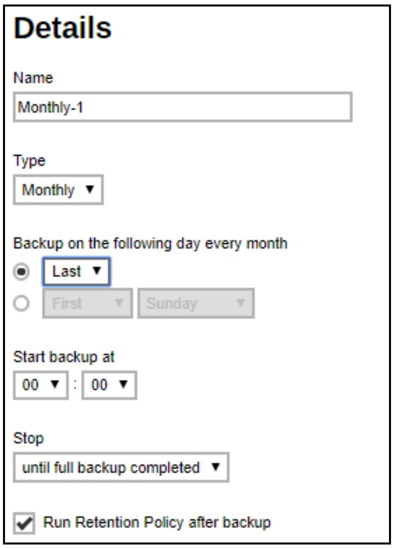
at ▼ 00 ▼ : 00 ▼

Stop

until full backup completed ▼

☑ 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

Monthly-1

Type

Monthly ▼

Backup on the following day every month

● Last ▼

○ First ▼ Sunday ▼

Start backup at

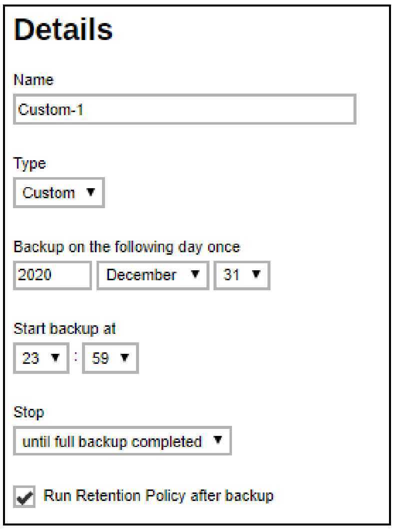
00 ▼ : 00 ▼

Stop

until full backup completed ▼

☑ Run Retention Policy after backup

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



Details

Name

Custom-1

Type

Custom ▼

Backup on the following day once

2020 December ▼ 31 ▼

Start backup at

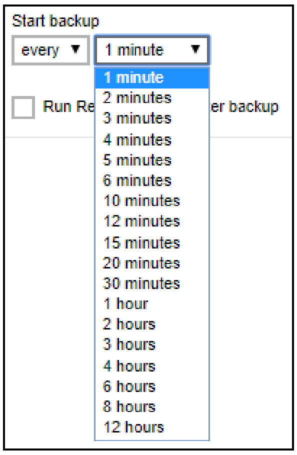
23 ▼ : 59 ▼

Stop

until full backup completed ▼

☑ Run Retention Policy after backup

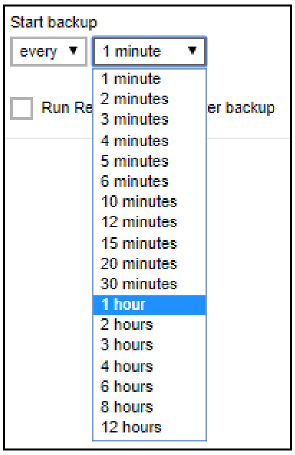
- **Start backup** – the start time of the backup job.
  - **at** – this option will start a backup job at a specific time.
  - **every** – this option will start a backup job in intervals of minutes or hours.



Start backup

every ▼ 1 minute ▼

□ Run Re er backup

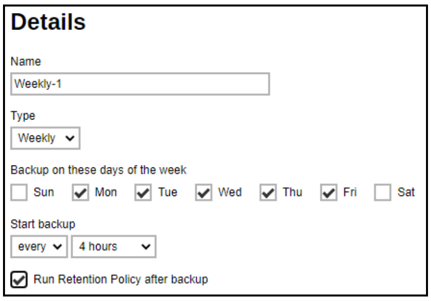


Start backup

every ▼ 1 minute ▼

□ Run Re er backup

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



Details

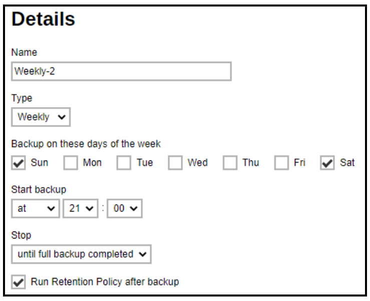
Name
Weekly-1

Type
Weekly

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

Start backup
every 4 hours

☑ Run Retention Policy after backup



Details

Name
Weekly-2

Type
Weekly

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

Start backup
at 21 : 00

Stop
until full backup completed

☑ Run Retention Policy after backup

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

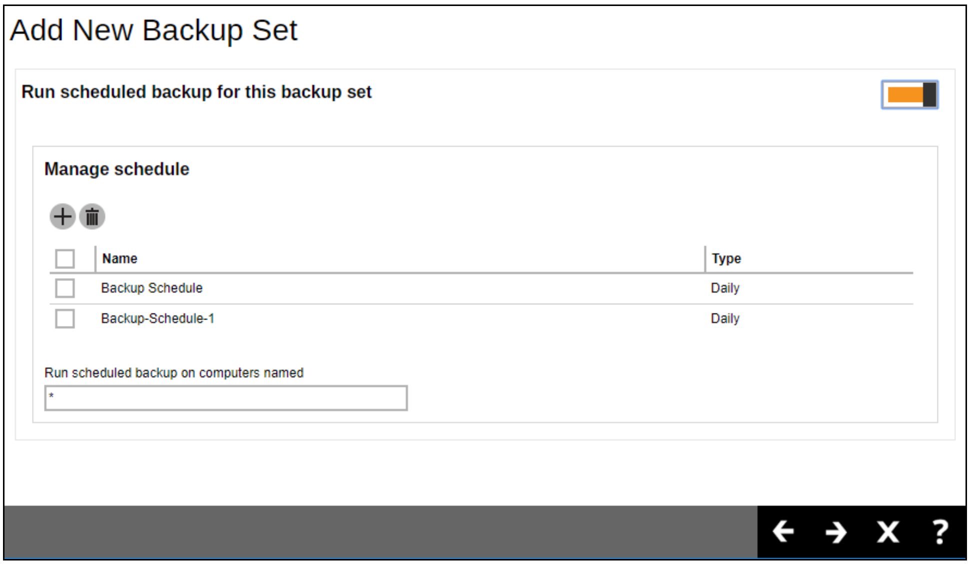
    As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time

- **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.



Add New Backup Set

Run scheduled backup for this backup set

Manage schedule

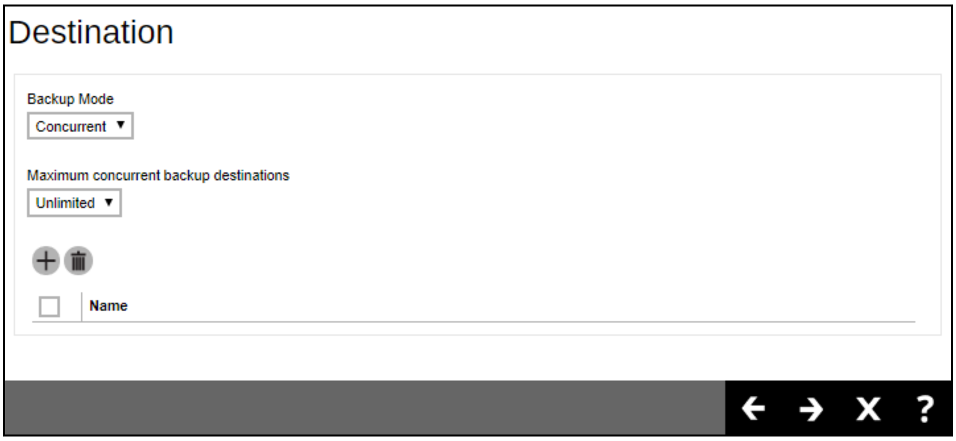
□	Name	Type
□	Backup Schedule	Daily
□	Backup-Schedule-1	Daily

Run scheduled backup on computers named

*

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.

- Add a Standard Destination or Predefined Destination set by your backup service provider by clicking the ⊕ in the left side of the screen.



Destination

Backup Mode

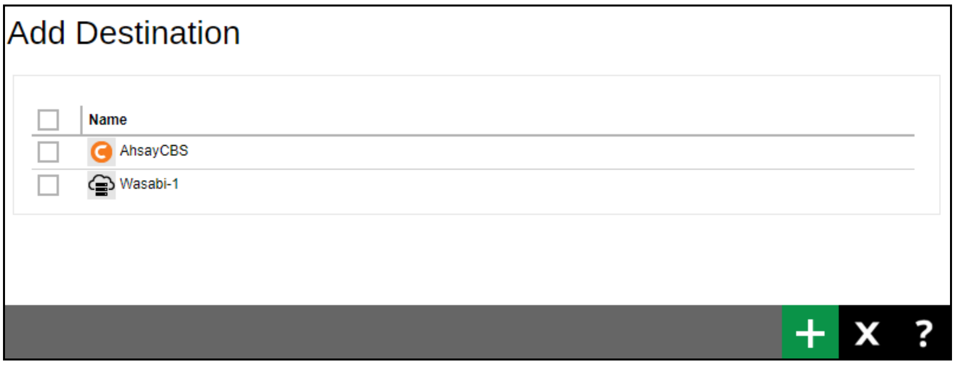
Concurrent ▼

Maximum concurrent backup destinations

Unlimited ▼

□ Name

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



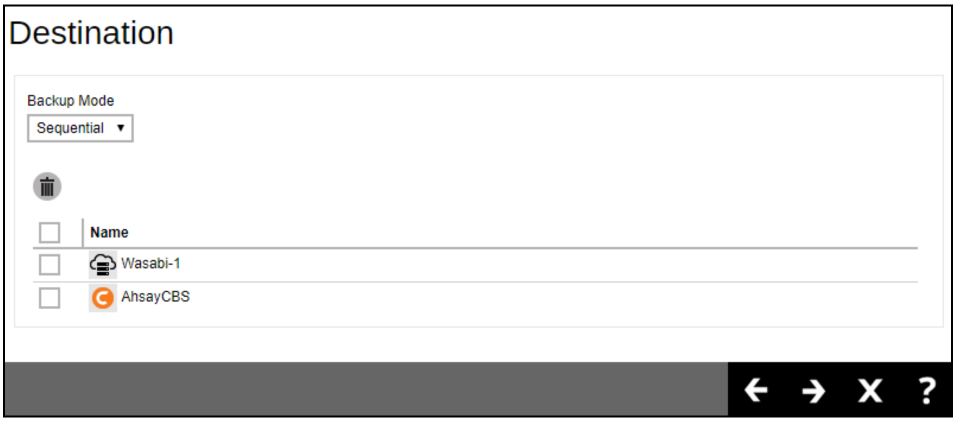
Add Destination

□	Name
□	AhsayCBS
□	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.

- The Standard and Predefined Destinations have been successfully added.



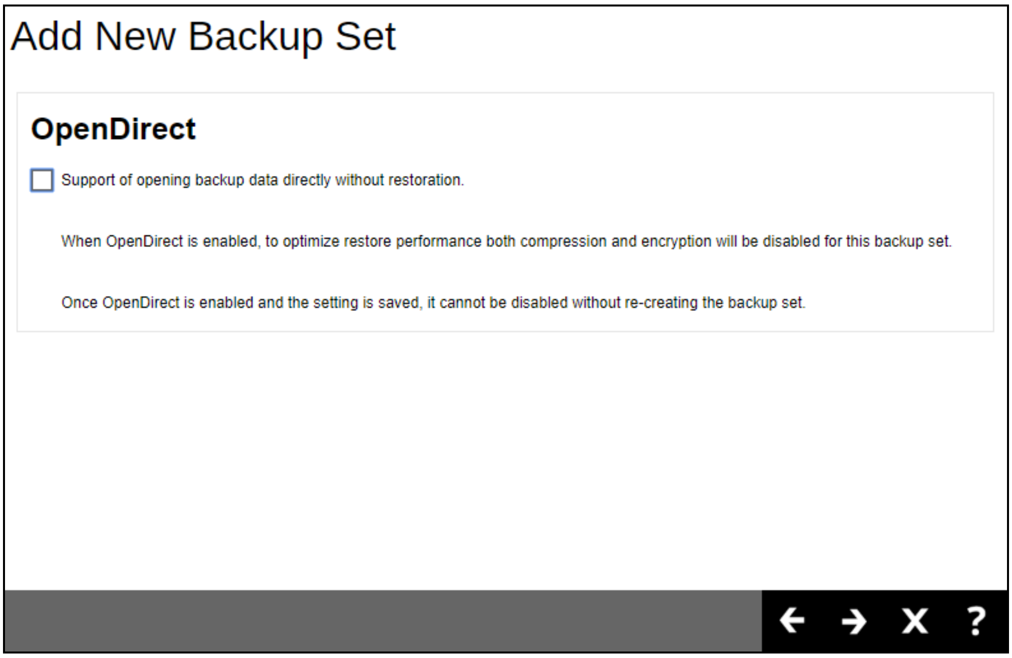
Destination

Backup Mode: Sequential

□	Name
□	Wasabi-1
□	AhsayCBS

- 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.

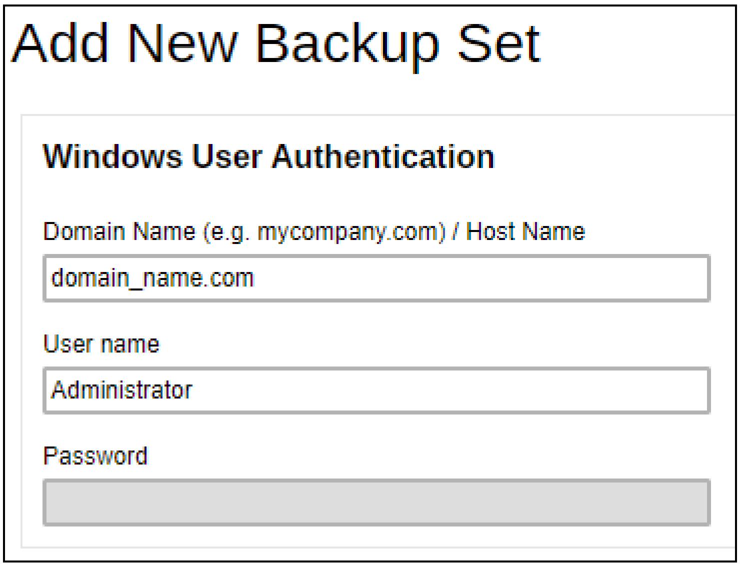
Once OpenDirect is enabled and the setting is saved, it cannot be disabled without re-creating the backup set.

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 login 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

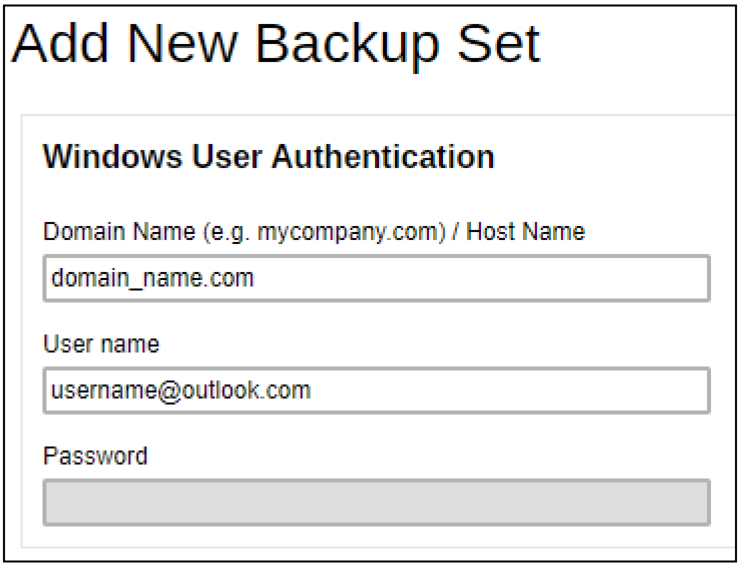
Domain Name (e.g. mycompany.com) / Host Name: domain_name.com

User name: Administrator

Password:

or

Example using a Microsoft account.



Add New Backup Set

Windows User Authentication

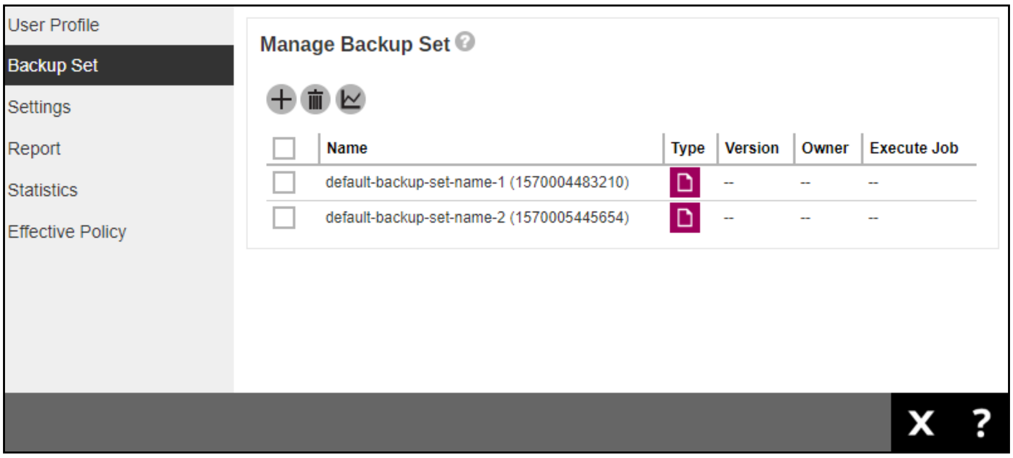
Domain Name (e.g. mycompany.com) / Host Name: domain_name.com

User name: username@outlook.com

Password:

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

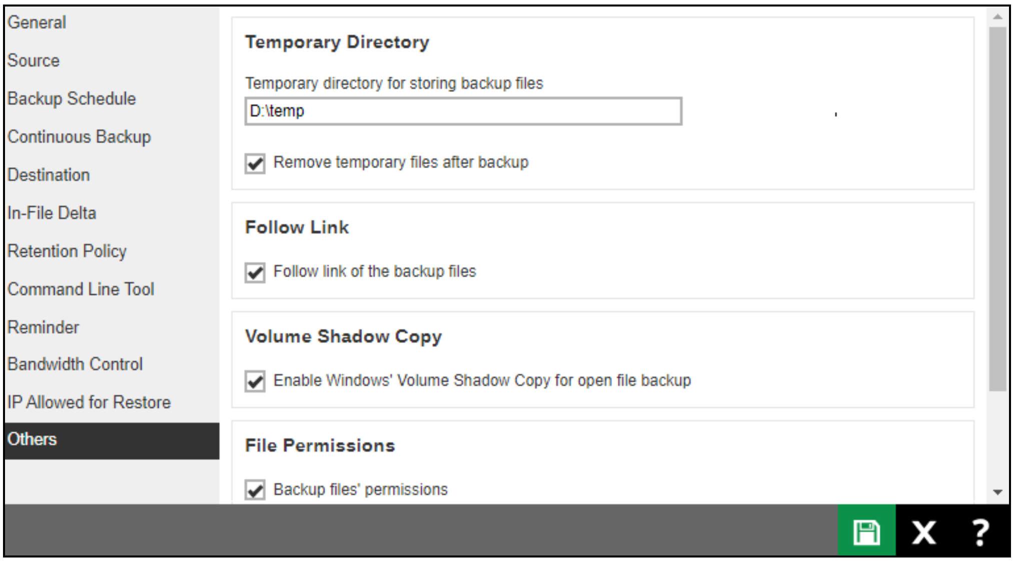
10. A new backup set called **default-backup-set-name-2** is created and can be seen in the backup set list.



Manage Backup Set

□	Name	Type	Version	Owner	Execute Job
□	default-backup-set-name-1 (1570004483210)		--	--	--
□	default-backup-set-name-2 (1570005445654)		--	--	--

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



Temporary Directory

Temporary directory for storing backup files: D:\temp

☑ Remove temporary files after backup

Follow Link

☑ Follow link of the backup files

Volume Shadow Copy

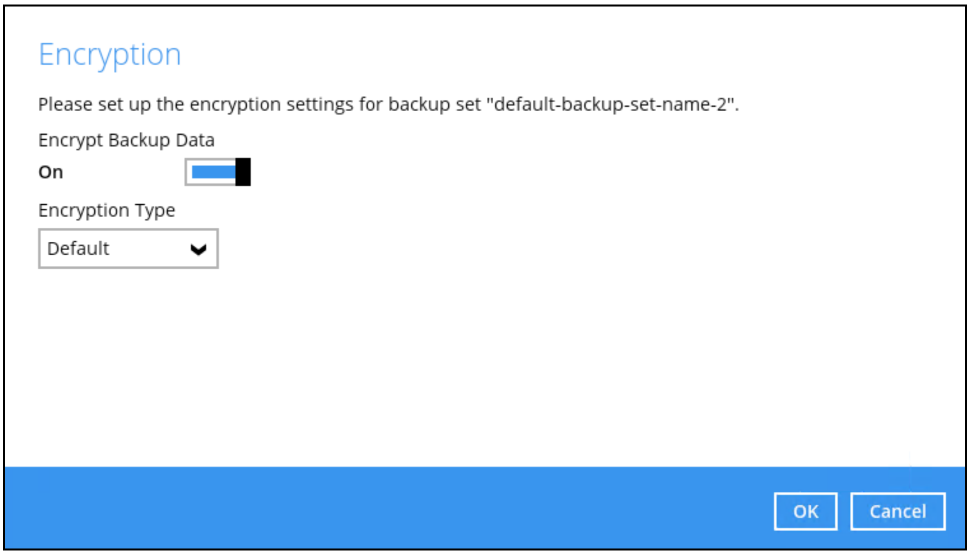
☑ Enable Windows' Volume Shadow Copy for open file backup

File Permissions

☑ Backup files' permissions

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**.



Encryption

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

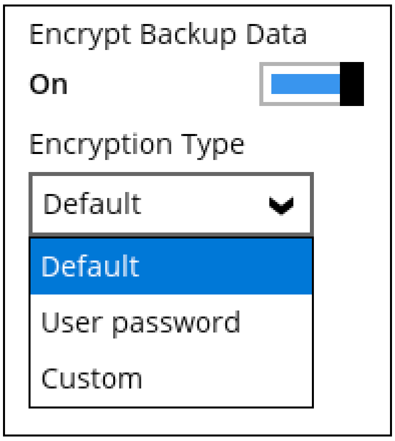
Encrypt Backup Data

On

Encryption Type

Default

- 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.



Encrypt Backup Data

On

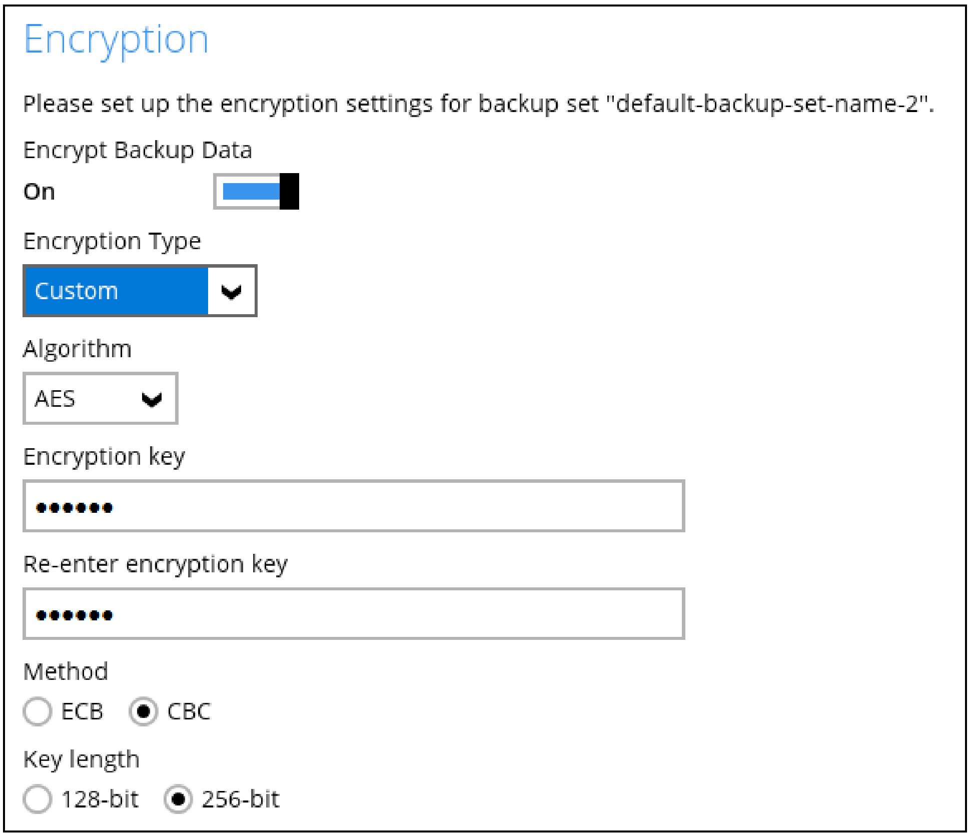
Encryption Type

Default

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

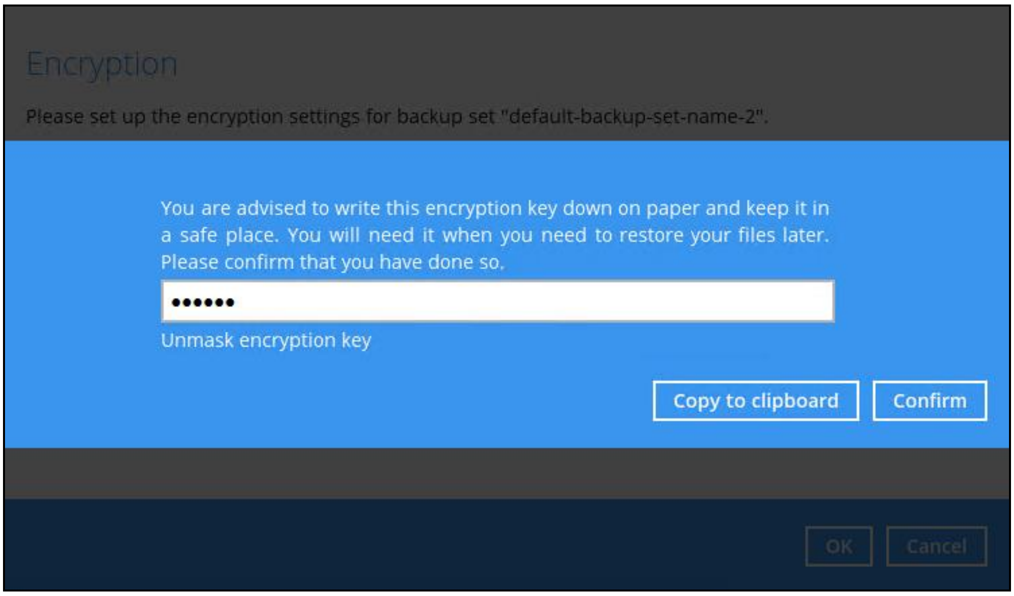
○ ECB ● CBC

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".

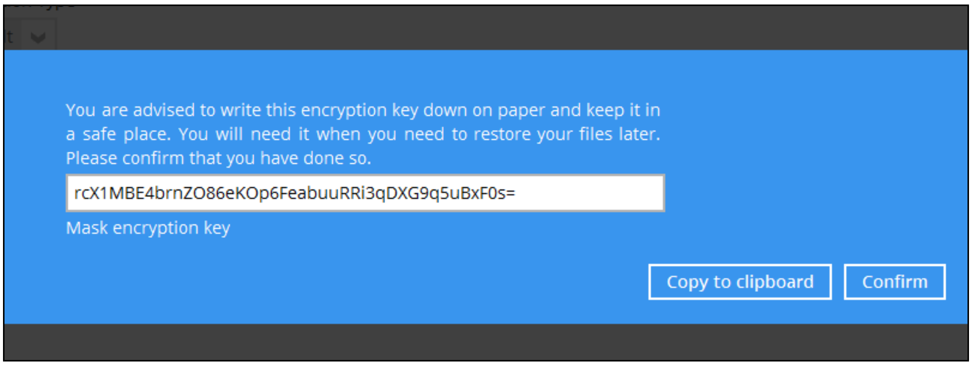
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

••••••

Unmask encryption key

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

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

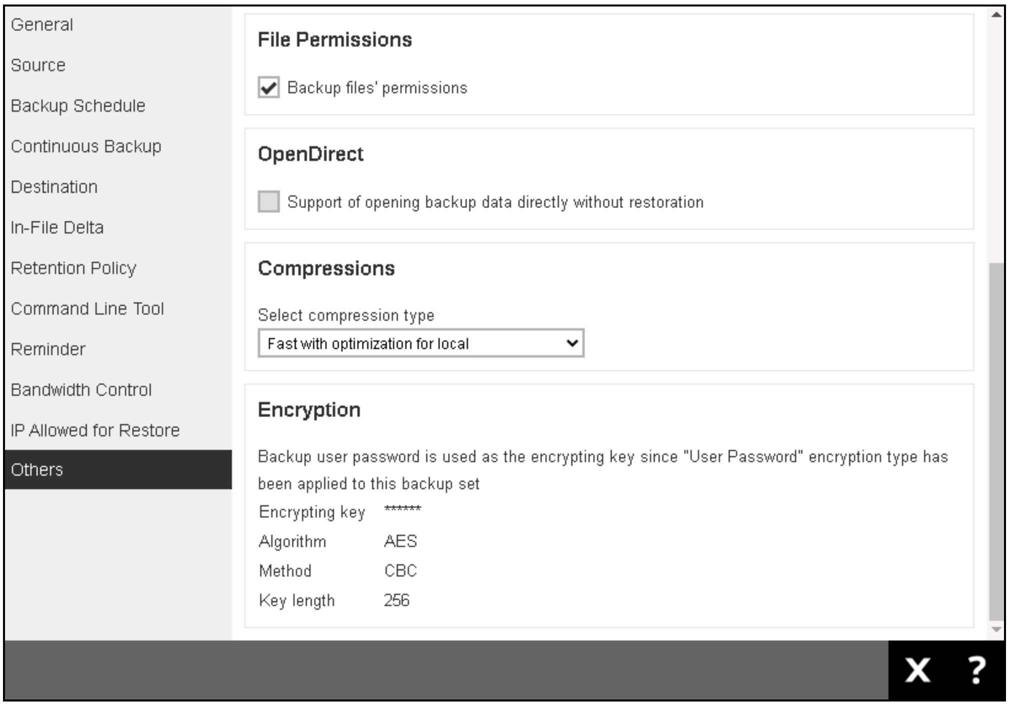


You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

rcX1MBE4brnZO86eKOp6FeabuuRRi3qDXG9q5uBxF0s=

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

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



File Permissions

☑ Backup files' permissions

OpenDirect

□ Support of opening backup data directly without restoration

Compressions

Select compression type: Fast with optimization for local

Encryption

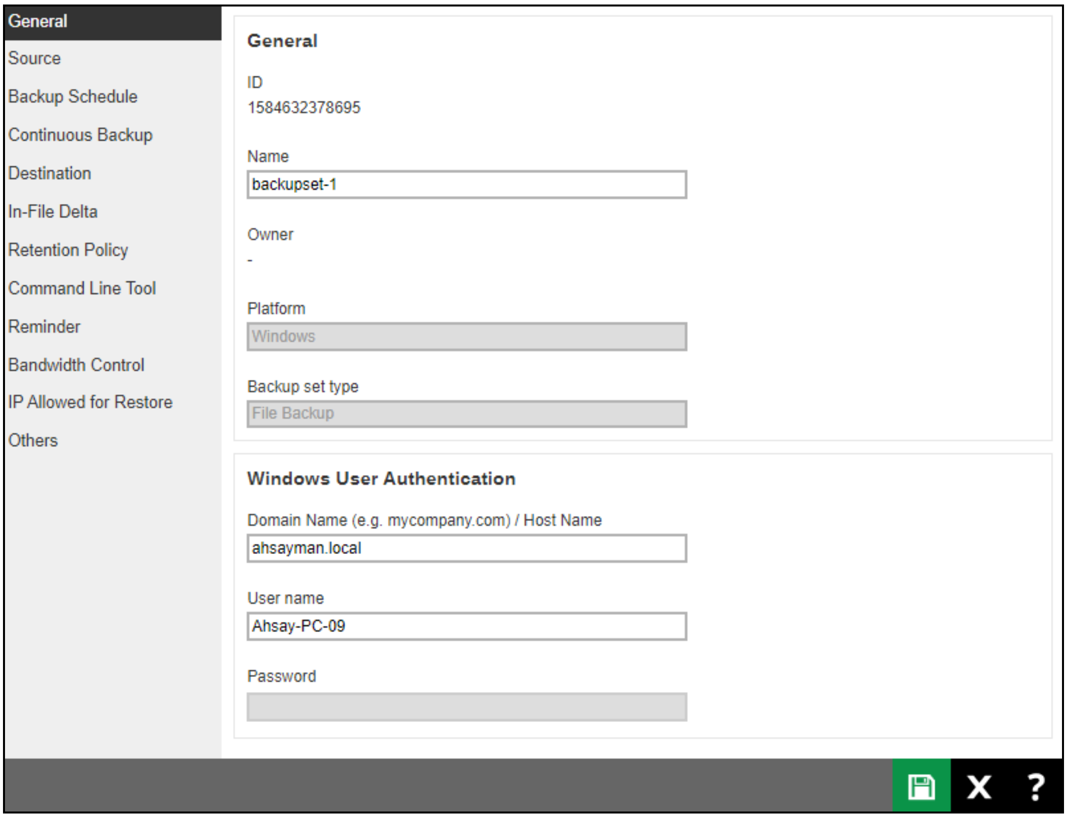
Backup user password is used as the encrypting key since "User Password" encryption type has been applied to this backup set

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

7.2 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
- Continuous Backup
- Retention Policy
- Bandwidth Control
- Source
- Destination
- Command Line Tool
- IP Allowed for Restore
- Backup Schedule
- In-File Delta
- Reminder
- Others



General

ID
1584632378695

Name
backupset-1

Owner
-

Platform
Windows

Backup set type
File Backup

Windows User Authentication

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

User name
Ahsay-PC-09

Password

7.3 Run a Backup Job

Run an Agent-based Backup using AhsayOBM / AhsayACB

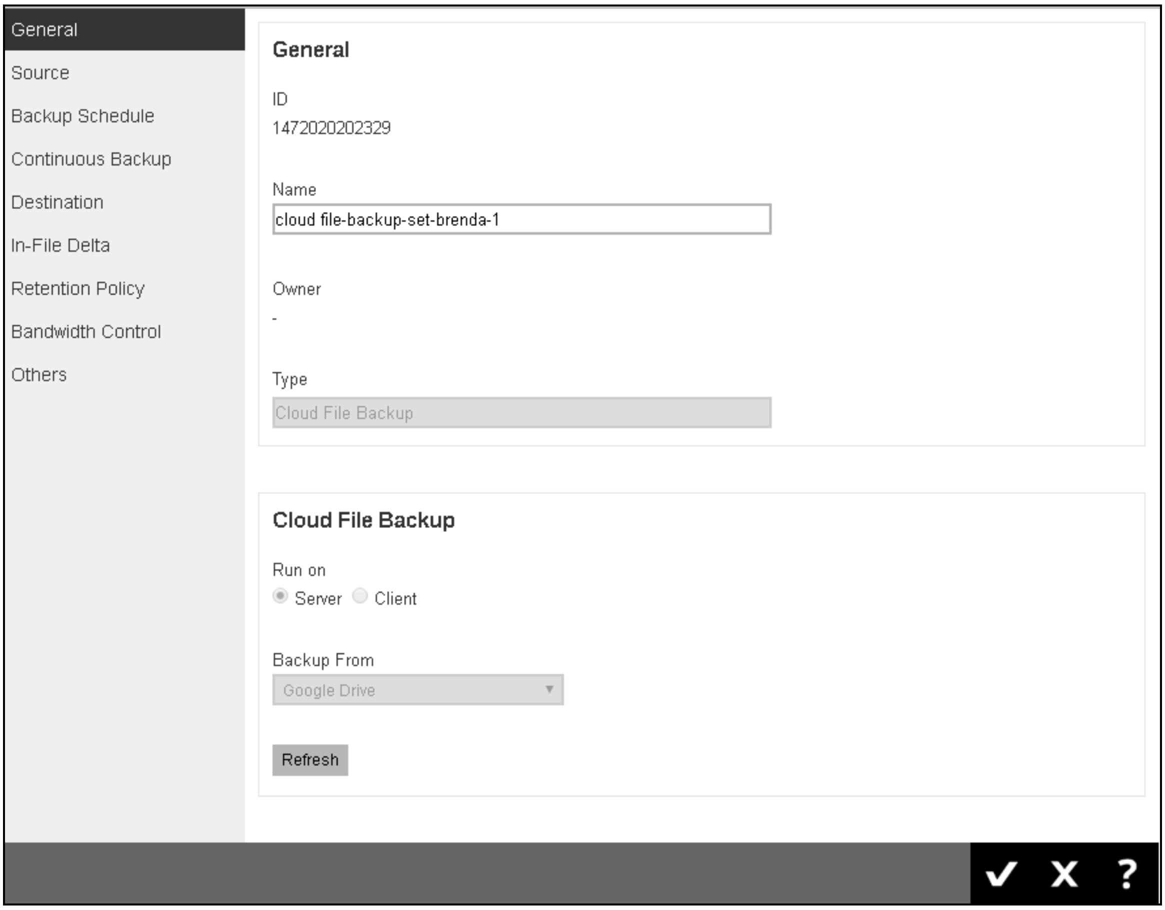
Except for Cloud File Backup and Office 365 Backup which you can run an agentless backup in AhsayCBS, all other backup modules require you to perform backup and restore using your client backup agent (AhsayOBM or AhsayACB).

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 Office 365 Backup only)

There are two types of backup set, **Cloud File Backup** and **Office 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.



General

ID
1472020202329

Name
cloud file-backup-set-brenda-1

Owner
-

Type
Cloud File Backup

Cloud File Backup

Run on
● Server ○ Client

Backup From
Google Drive

Backup Destination for Run-on-Server Backup Set

For **Office 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.

7.4 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 Office 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 **Office 365 Backup**, provided that the backup set was created to **Run on Server**.

8 Run Direct Restore

8.1 Introduction

What is Run Direct?

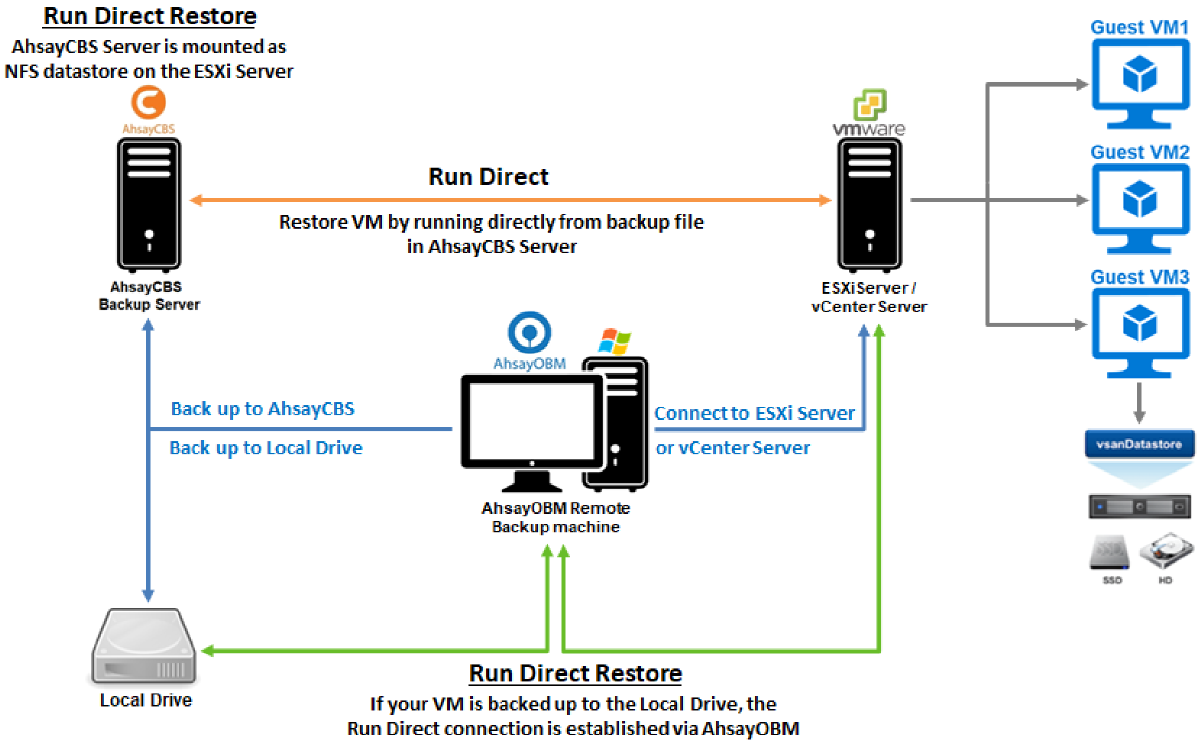
Run Direct is a feature that is supported by AhsayCBS v8.1, which helps reduce disruption and downtime of your production VMs.

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.

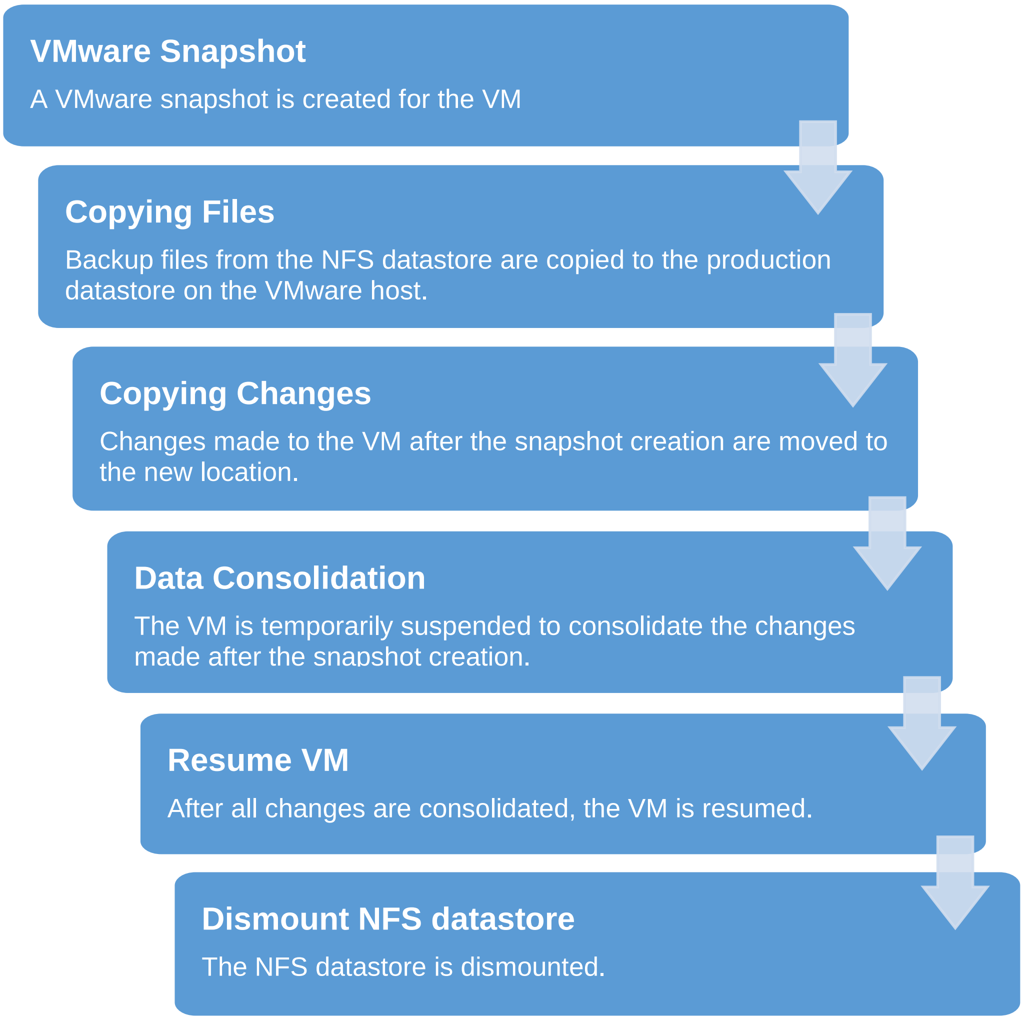
The backup destination can either be the AhsayCBS server or a local drive that can connect with AhsayOBM. Initiating a Run Direct from the AhsayCBS (also known as agentless restore) will trigger a connection directly with the VMware host (ESXi server and direction shown in orange indicator below), while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


Run Direct Restore
AhsayCBS Server is mounted as NFS datastore on the ESXi Server
AhsayCBS
AhsayCBS Backup Server
Run Direct
Restore VM by running directly from backup file in AhsayCBS Server
vmware
ESXi Server / vCenter Server
Guest VM1
Guest VM2
Guest VM3
vsanDatastore
SSD
HD
AhsayOBM
Back up to AhsayCBS
Back up to Local Drive
Connect to ESXi Server or vCenter Server
AhsayOBM Remote Backup machine
Local Drive
Run Direct Restore
If your VM is backed up to the Local Drive, the Run Direct connection is established via AhsayOBM

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:



VMware Snapshot

A VMware snapshot is created for the VM

Copying Files

Backup files from the NFS datastore are copied to the production datastore on the VMware host.

Copying Changes

Changes made to the VM after the snapshot creation are moved to the new location.

Data Consolidation

The VM is temporarily suspended to consolidate the changes made after the snapshot creation.

Resume VM

After all changes are consolidated, the VM is resumed.

Dismount NFS datastore

The NFS datastore is dismounted.

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).

8.2 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.

8.3 Performing a Run Direct Restore on VM

AhsayCBS v8.5.0.118 or above now supports backup and restore of VMware VMs stored on vSAN datastore. With this development, there are now several scenarios for restoring VMs using Run Direct.

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

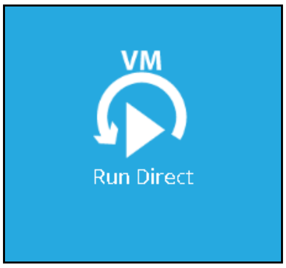
- Restore backup from VMFS datastore to VMFS datastore
- Restore backup from VMFS datastore to vSAN datastore
- Restore backup from vSAN datastore to vSAN datastore
- Restore backup from vSAN datastore to VMFS datastore

8.3.1 Restore a backup from VMFS datastore to VMFS datastore

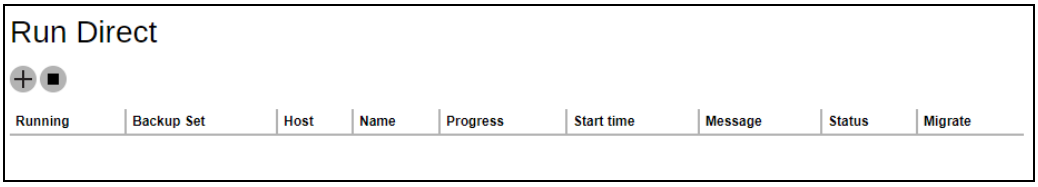
1. Login to AhsayCBS user web console according to the instruction provided in section Logging on to AhsayCBS User Web Console.

> **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 v8 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.



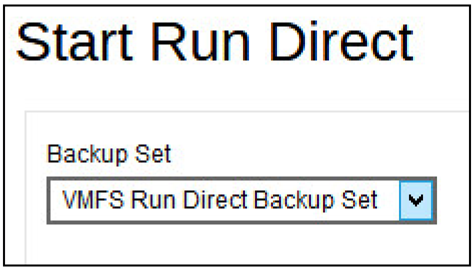
Run Direct

⊕ ■

Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate

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.

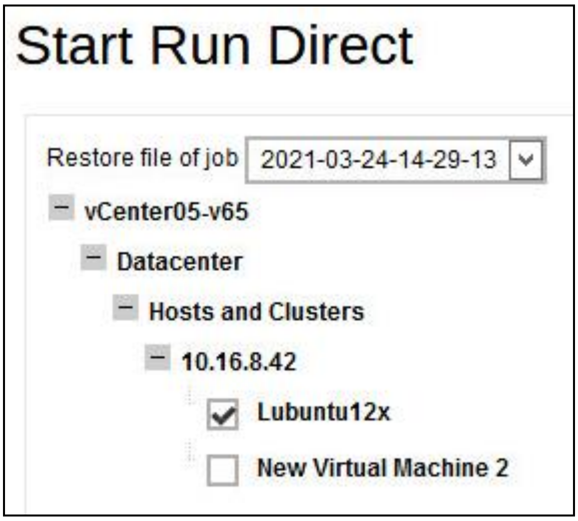


Start Run Direct

Backup Set

VMFS Run Direct Backup Set

5. 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**.



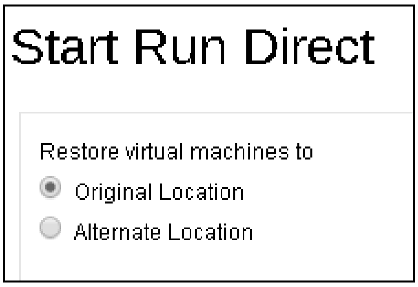
Start Run Direct

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

6. 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.



Start Run Direct

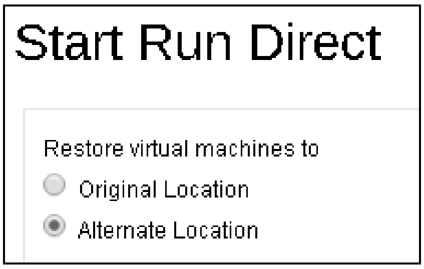
Restore virtual machines to

● Original Location

○ Alternate Location

   - 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.



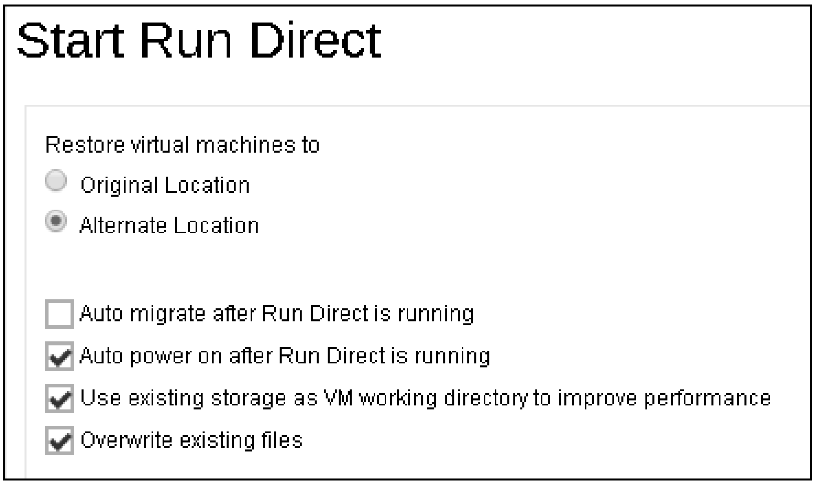
Start Run Direct

Restore virtual machines to

○ Original Location

● Alternate Location

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.

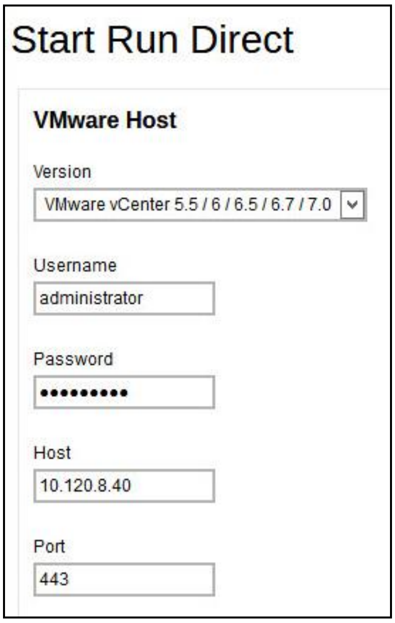
- **Overwrite existing files** (Alternate Location only)

  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

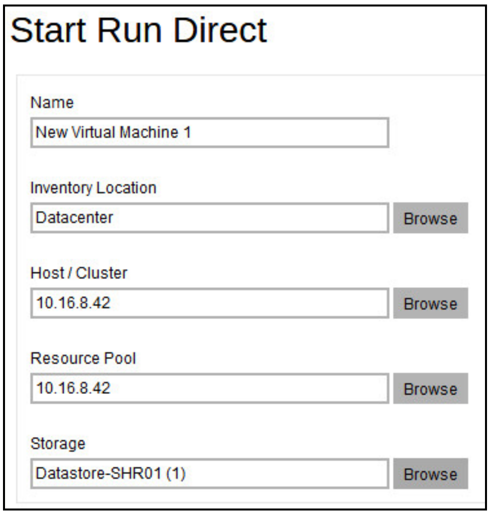
Username: administrator

Password: ●●●●●●●●●●

Host: 10.120.8.40

Port: 443

8. 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

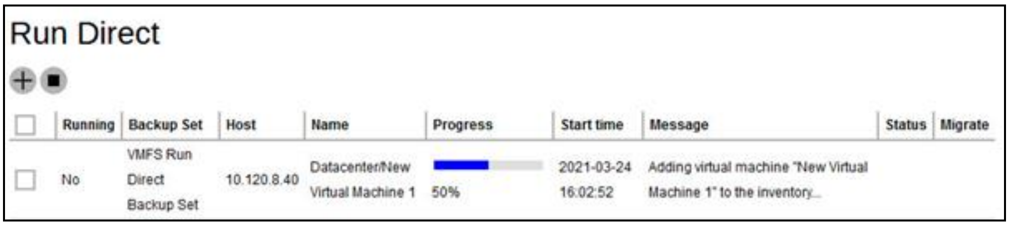
Host / Cluster: 10.16.8.42

Resource Pool: 10.16.8.42

Storage: Datastore-SHR01 (1)

Click ▶ to start the restore.

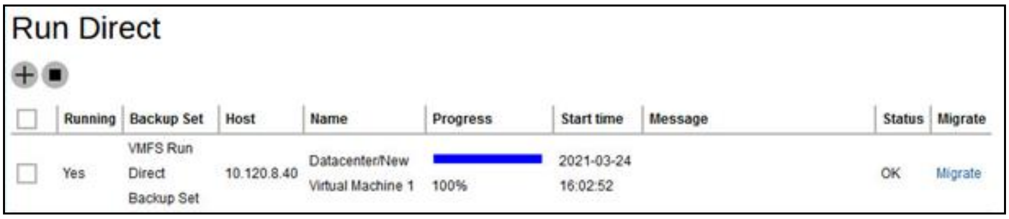
9. The **Run Direct** page appears, showing the status message of the Run Direct restore job.



Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	No	VMFS Run Direct Backup Set	10.120.8.40	Datacenter/New Virtual Machine 1	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%.

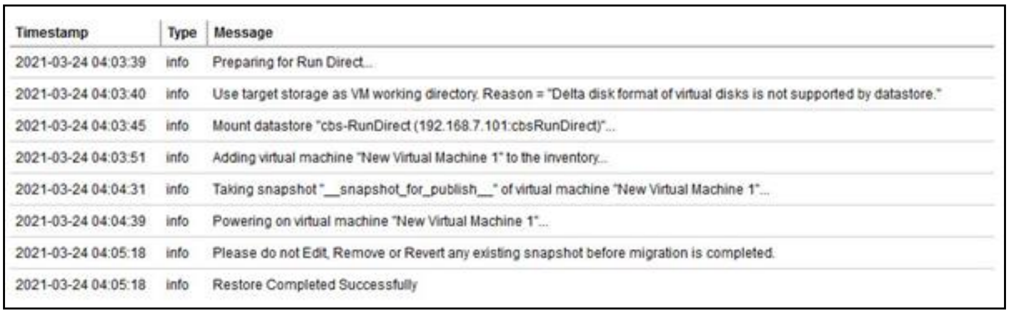


Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	Yes	VMFS Run 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

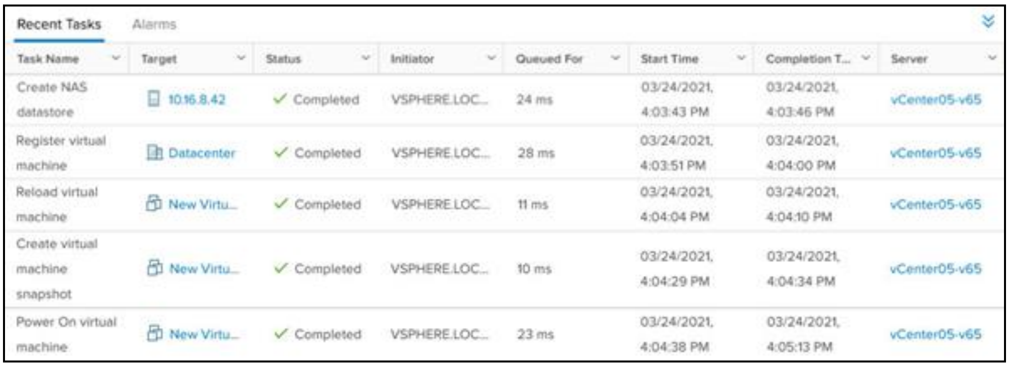
Click on the item on the Run Direct page.



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

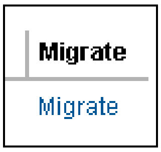
Restore log messages on the VMware vSphere Client

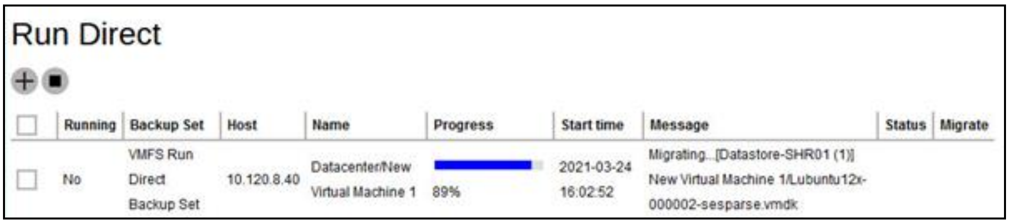
Open your VMware vSphere Client and you will see the following messages from the Recent Tasks section.



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

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.

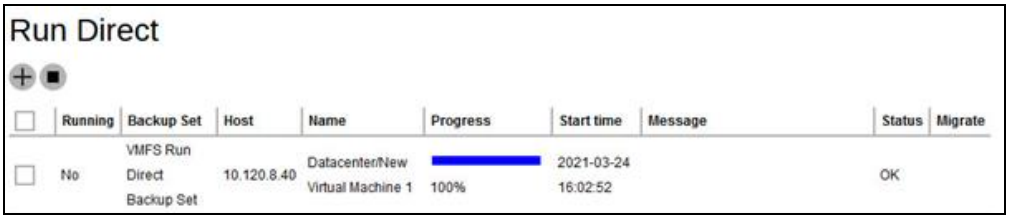




Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	No	VMFS Run 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.

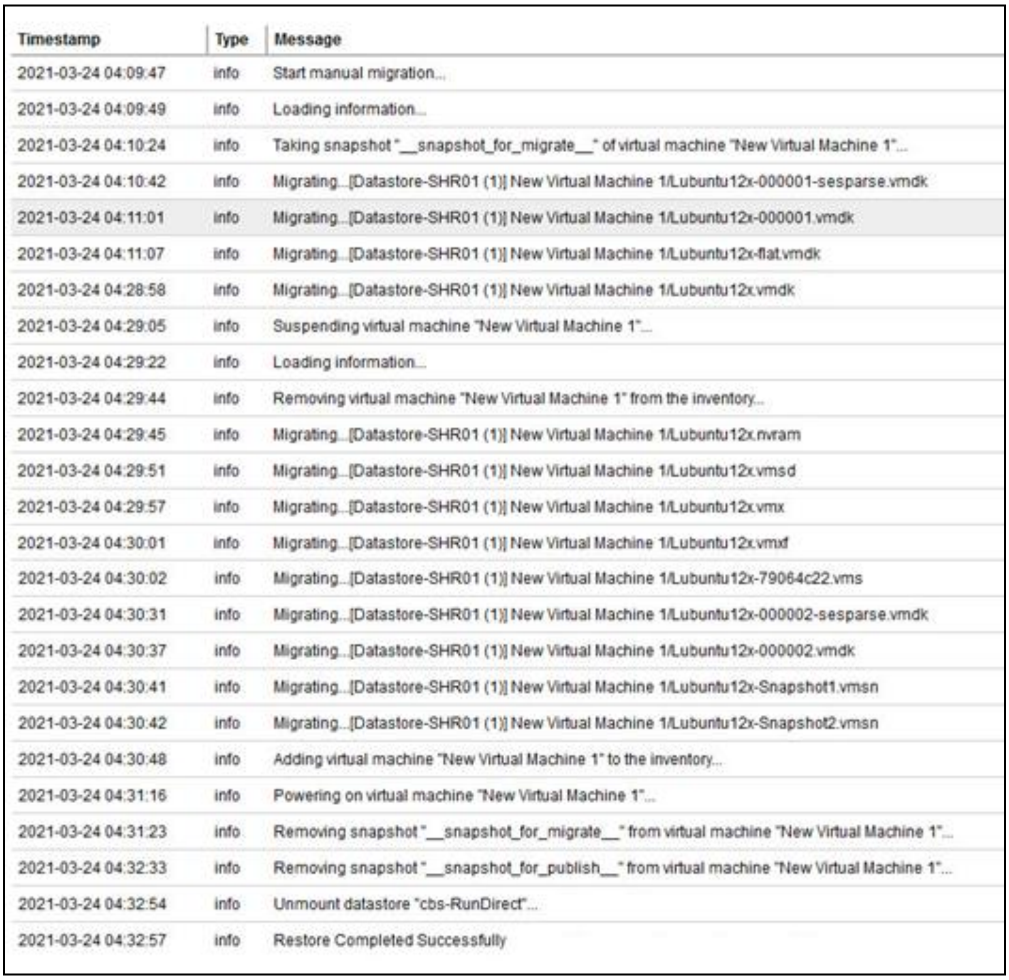


Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	No	VMFS Run Direct Backup Set	10.120.8.40	Datacenter/New Virtual Machine 1	100%	2021-03-24 16:02:52		OK	

Restore log messages on AhsayCBS

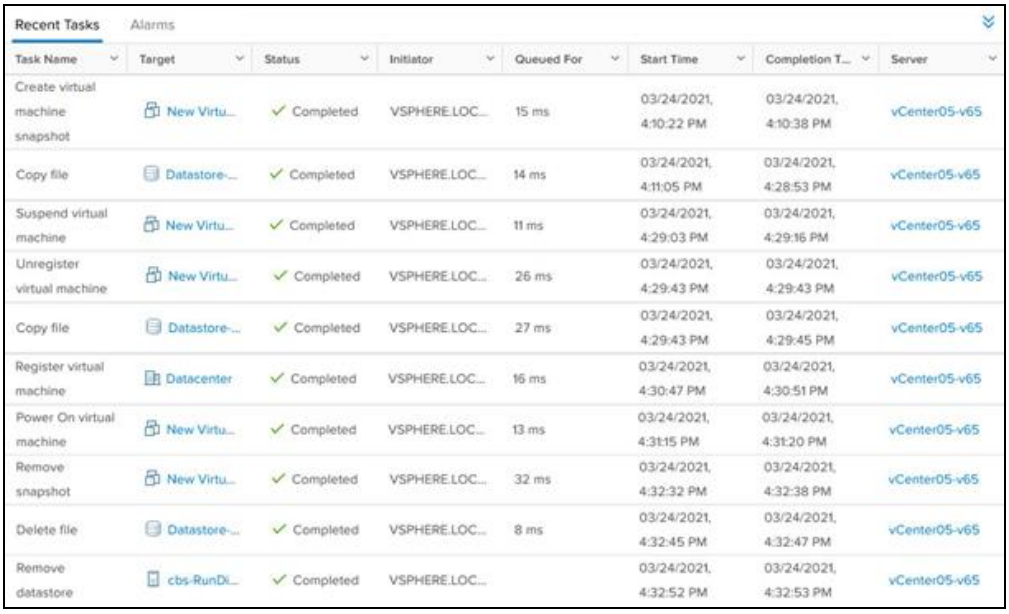
Click on the restore item on the Run Direct page to see the restore log messages.



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.vmxf
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.



Recent Tasks Alarms

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	Datacenter	✓ 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

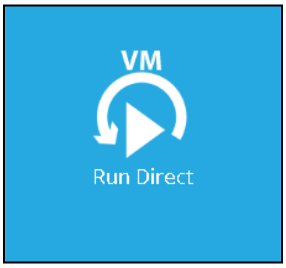
11. Click X to exit when finished.

8.3.2 Restore a backup from VMFS datastore to vSAN datastore

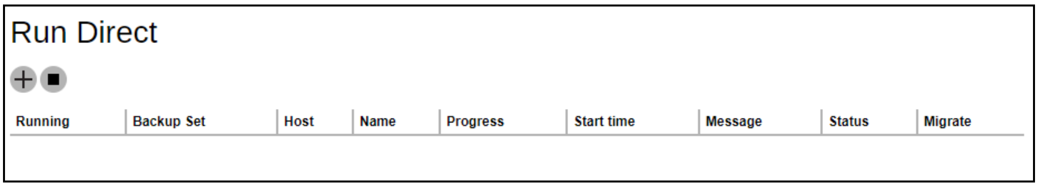
1. Login to AhsayCBS user web console according to the instruction provided in section Logging on to AhsayCBS User Web Console.

> **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 v8 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.

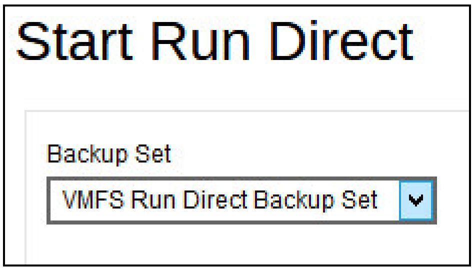


Run Direct

⊕ ■

Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate

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.



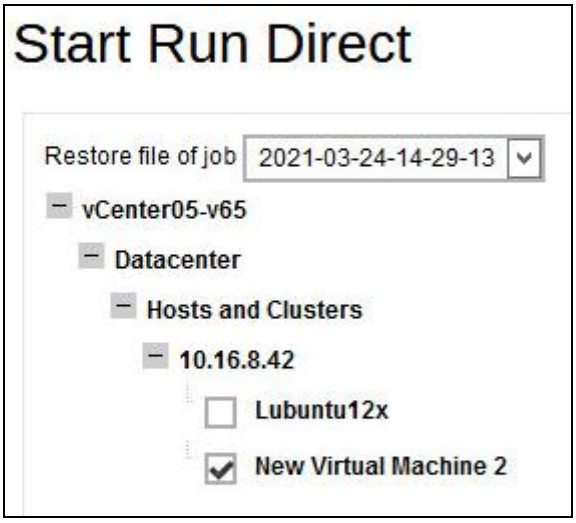
Start Run Direct

Backup Set

VMFS Run Direct Backup Set

5. 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

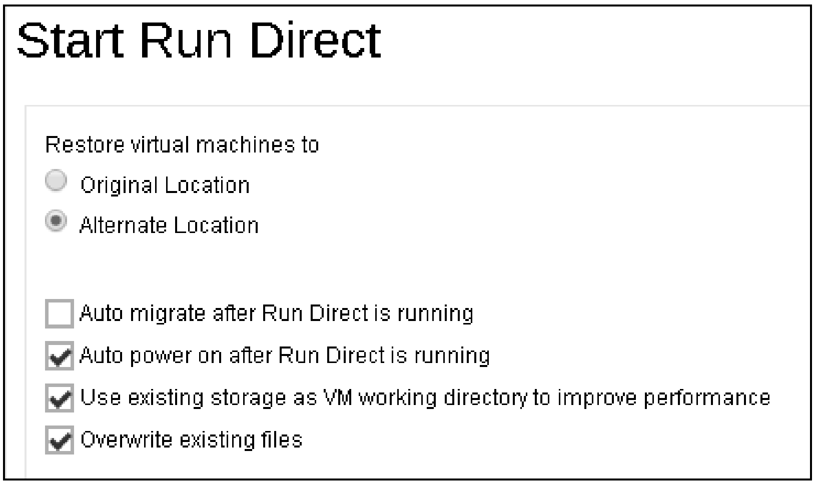
Restore file of job 2021-03-24-14-29-13

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

6. 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**

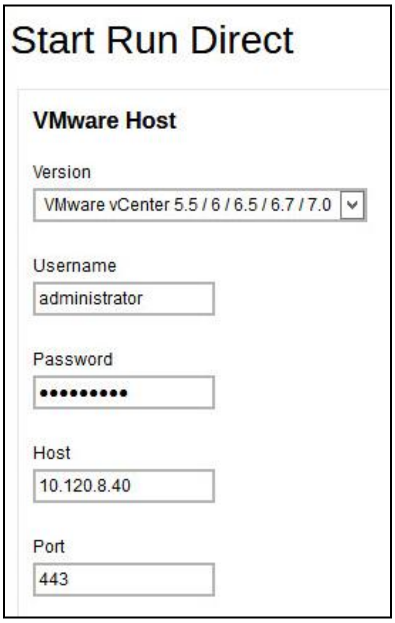
  Select this option to enhance performance of the restored VM.

- **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.



Start Run Direct

VMware Host

Version

VMware vCenter 5.5 / 6 / 6.5 / 6.7 / 7.0

Username

administrator

Password

•••••••••

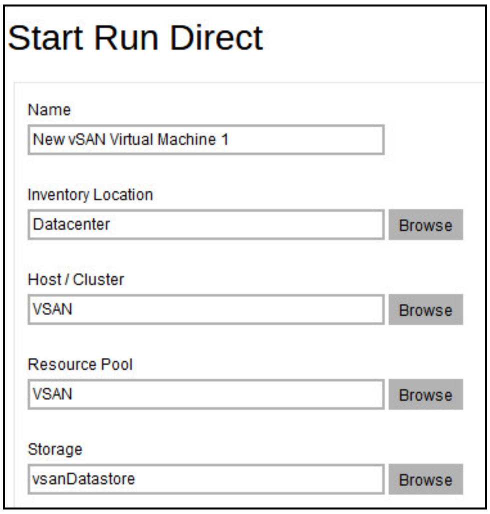
Host

10.120.8.40

Port

443

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



Start Run Direct

Name

New vSAN Virtual Machine 1

Inventory Location

Datacenter

Host / Cluster

VSAN

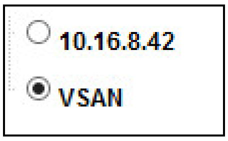
Resource Pool

VSAN

Storage

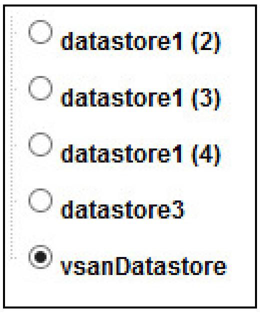
vsanDatastore

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



○ 10.16.8.42

● VSAN



○ datastore1 (2)

○ datastore1 (3)

○ datastore1 (4)

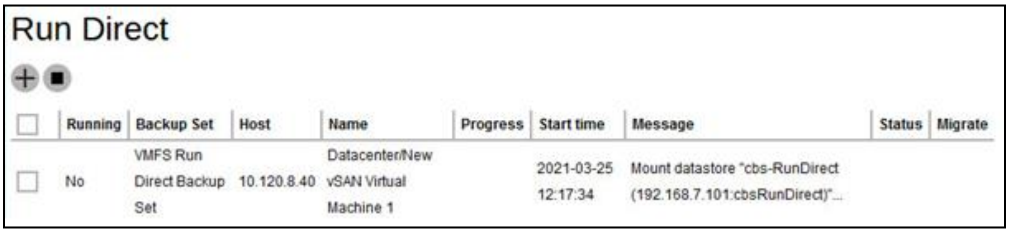
○ datastore3

● 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.

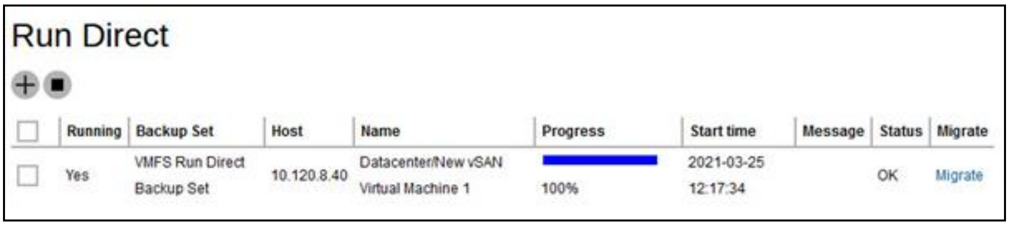
9. The **Run Direct** page appears, showing the status message of the Run Direct restore job.



Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	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%.

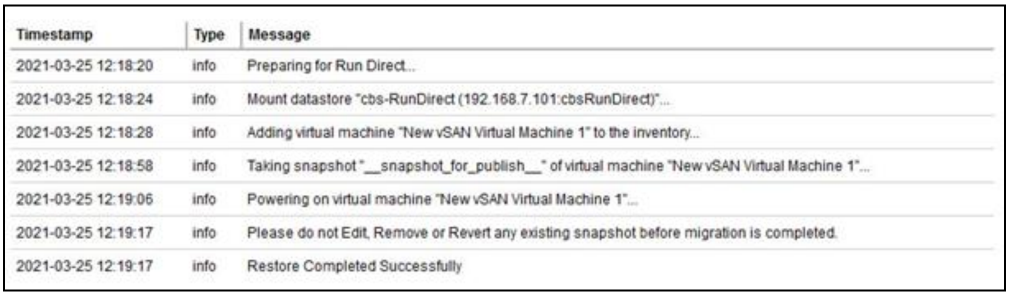


Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	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

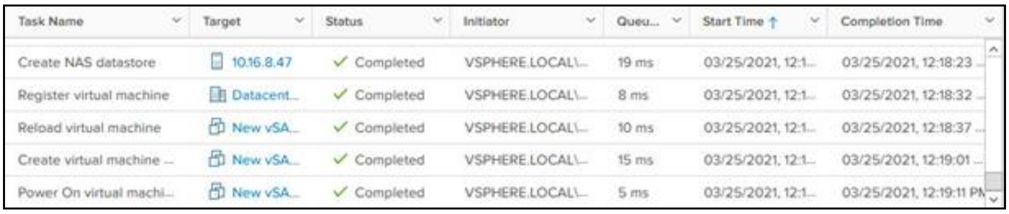
Click on the item on the Run Direct page.



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

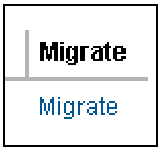
Restore log messages on the VMware vSphere Client

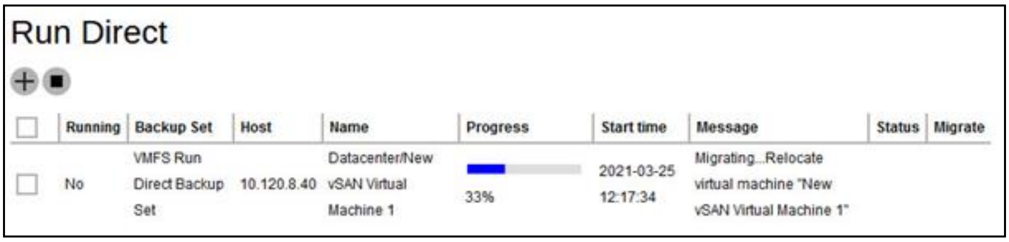
Open your VMware vSphere Client and you will see the following messages from the Recent Tasks section.



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.

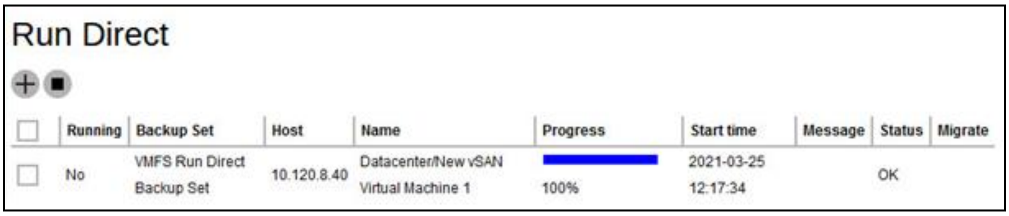




Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	No	VMFS Run Direct Backup Set	10.120.8.40	Datacenter/New vSAN Virtual Machine 1	33%	2021-03-25 12:17:34	Migrating...Relocate virtual machine "New vSAN Virtual Machine 1"		

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

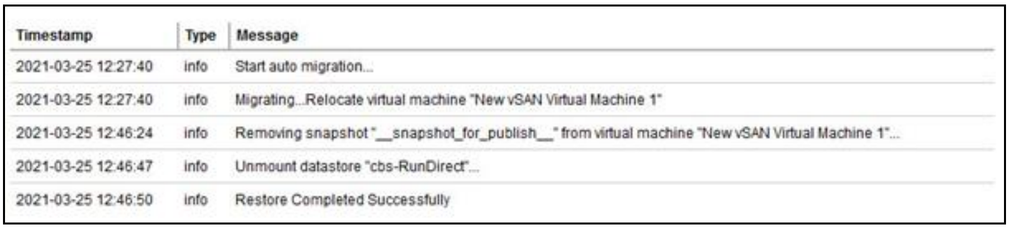


Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	No	VMFS Run Direct Backup Set	10.120.8.40	Datacenter/New vSAN Virtual Machine 1	100%	2021-03-25 12:17:34		OK	

Restore log messages on AhsayCBS

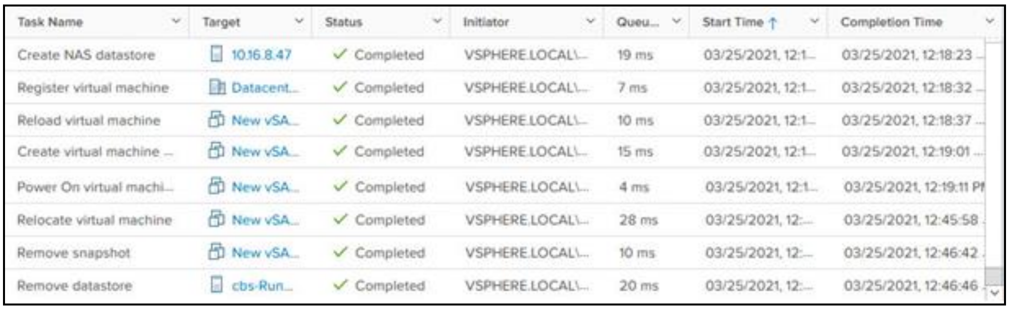
Click on the restore item on the Run Direct page to see the restore log messages.



Timestamp	Type	Message
2021-03-25 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 PI
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.

8.3.3 Restore a backup from vSAN datastore to vSAN datastore

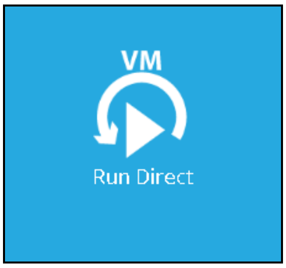
1. Login to AhsayCBS user web console according to the instruction provided in section Logging on to AhsayCBS User Web Console.

NOTE

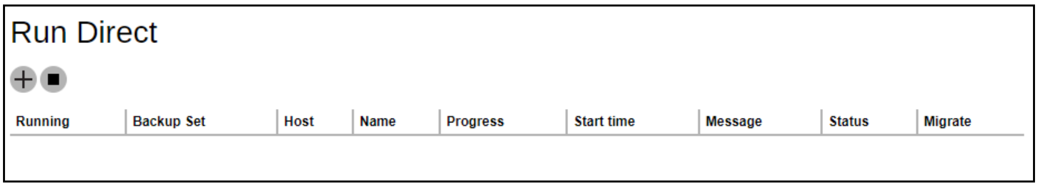
Before you can start Run Direct, you must have a VMware backup set created in the AhsayOBM client. Please refer to the Ahsay Online Backup Manager v8 VMware vCenter/ESXi Backup & Restore Guide for information on how to create the backup set.

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.



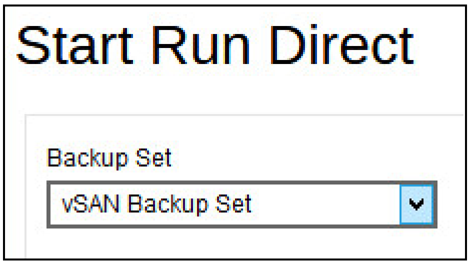
3. Click ⊕ from the **Run Direct** page to start a new Run Direct session.


Run Direct

⊕ ■

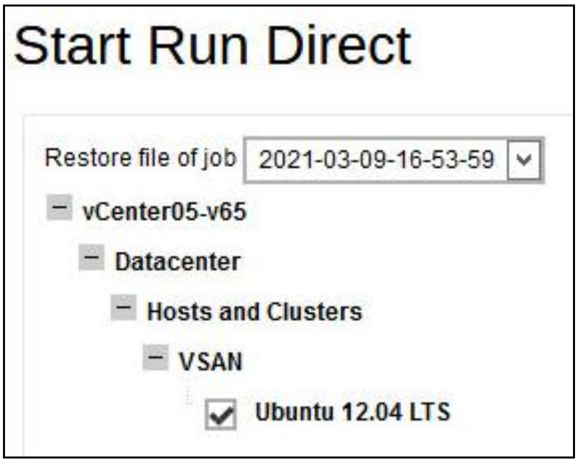
Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate

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.


Start Run Direct

Backup Set: vSAN Backup Set

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.



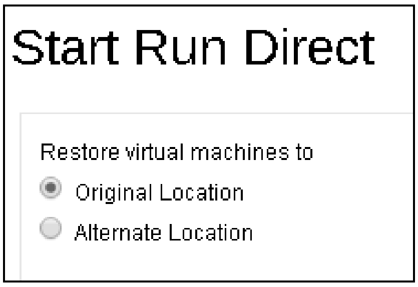
Start Run Direct

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**.



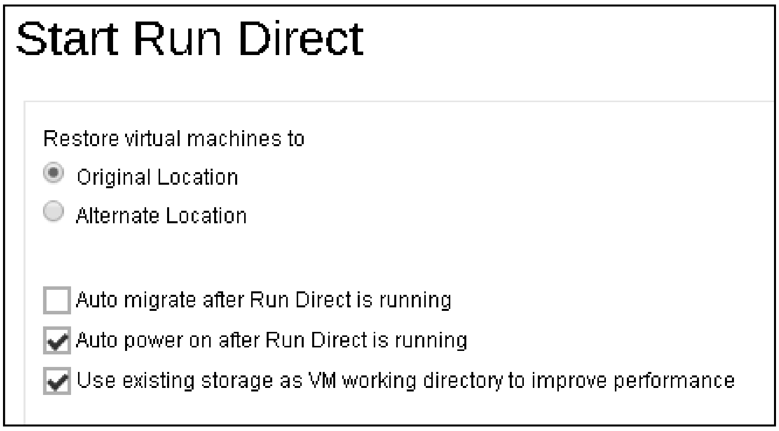
Start Run Direct

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**

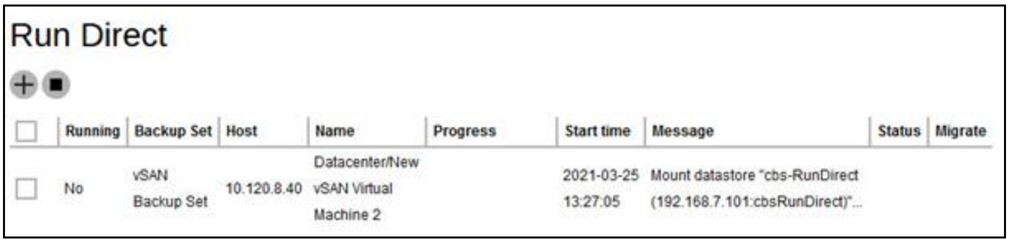
  Select this option to power up the virtual machine automatically, after Run Direct is running for the VM.

◉ **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.

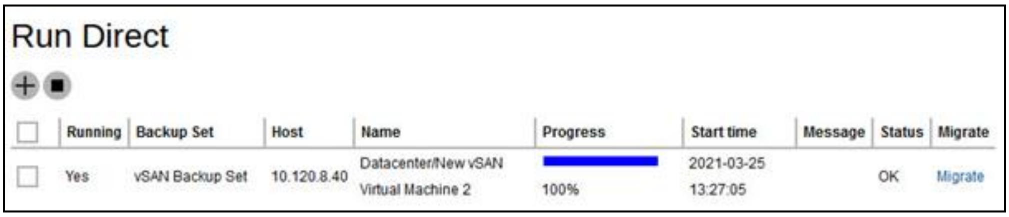
8. The **Run Direct** page appears, showing the status message of the Run Direct restore job.



Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	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%.

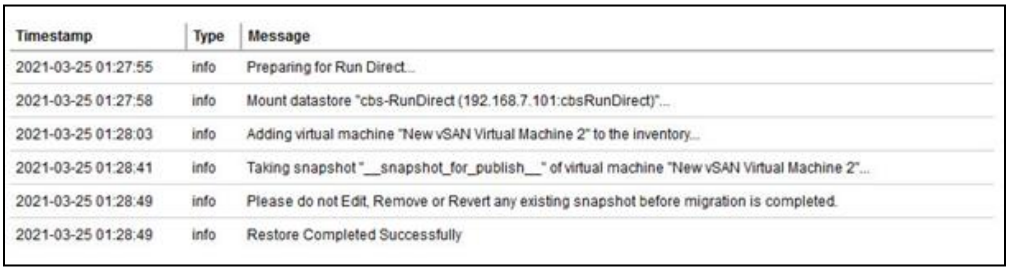


Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	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

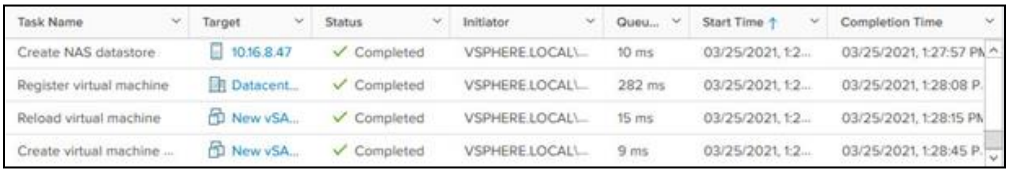
Click on the item on the Run Direct page.



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

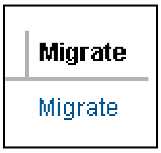
Restore log messages on the VMware vSphere Client

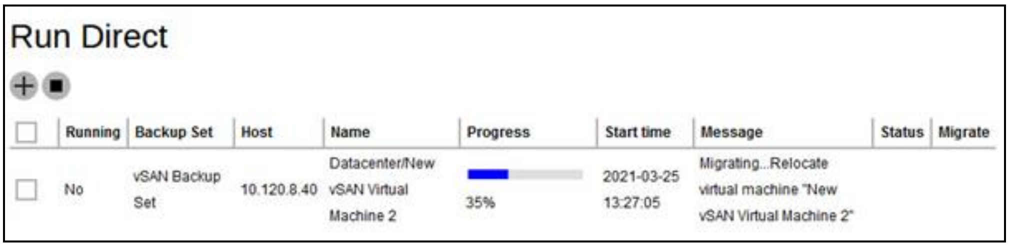
Open your VMware vSphere Client and you will see the following messages from the Recent Tasks section.



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...

9. 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.

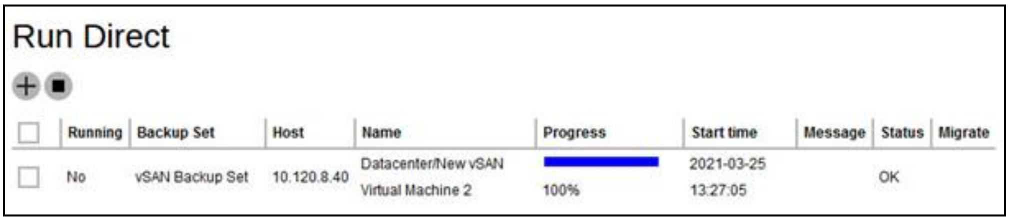




Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	No	vSAN Backup Set	10.120.8.40	Datacenter/New vSAN Virtual Machine 2	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.

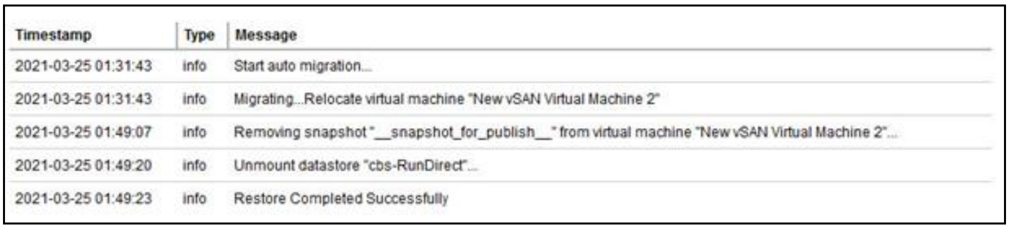


Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	No	vSAN Backup Set	10.120.8.40	Datacenter/New vSAN Virtual Machine 2	100%	2021-03-25 13:27:05		OK	

Restore log messages on AhsayCBS

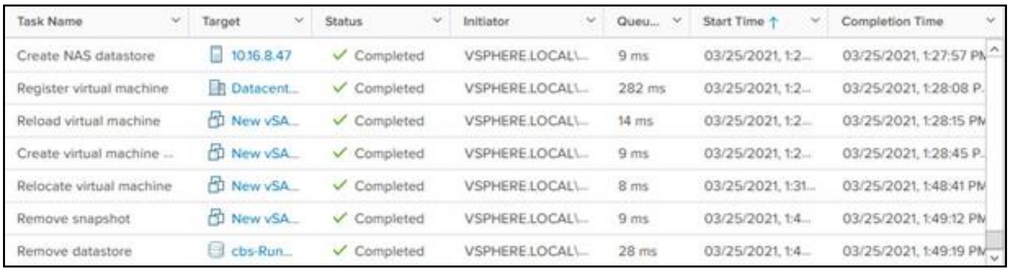
Click on the restore item on the Run Direct page to see the restore log messages.



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.

8.3.4 Restore a backup from vSAN datastore to VMFS datastore

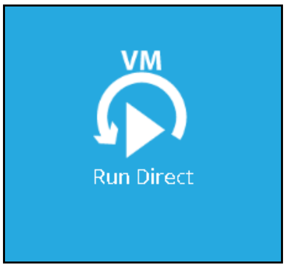
1. Login to AhsayCBS user web console according to the instruction provided in section Logging on to AhsayCBS User Web Console.

NOTE

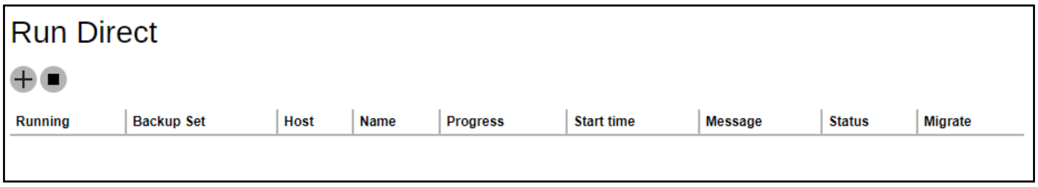
Before you can start Run Direct, you must have a VMware backup set created in the AhsayOBM client. Please refer to the Ahsay Online Backup Manager v8 VMware vCenter/ESXi Backup & Restore Guide for information on how to create the backup set.

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.

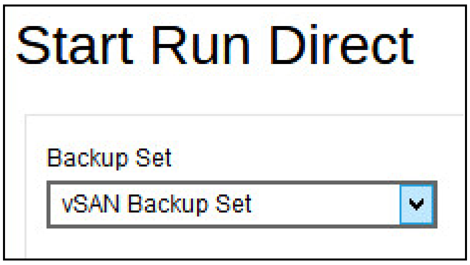


Run Direct

⊕ ■

Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate

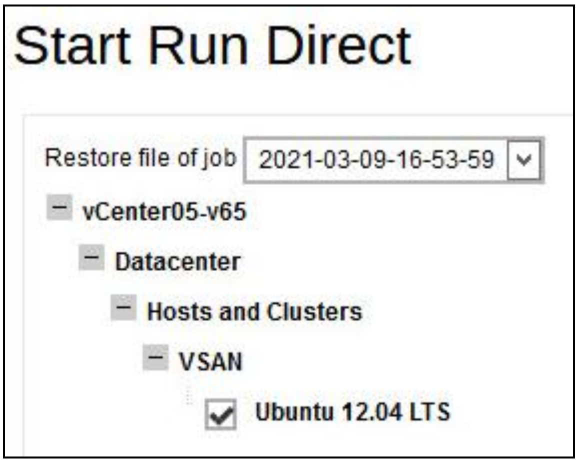
4. Select the **Backup Set** from the dropdown box of VMware backup set you have created. In our example, the backup set is called **vSAN Backup Set**. Click ➔ to continue.



Start Run Direct

Backup Set: vSAN Backup Set

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

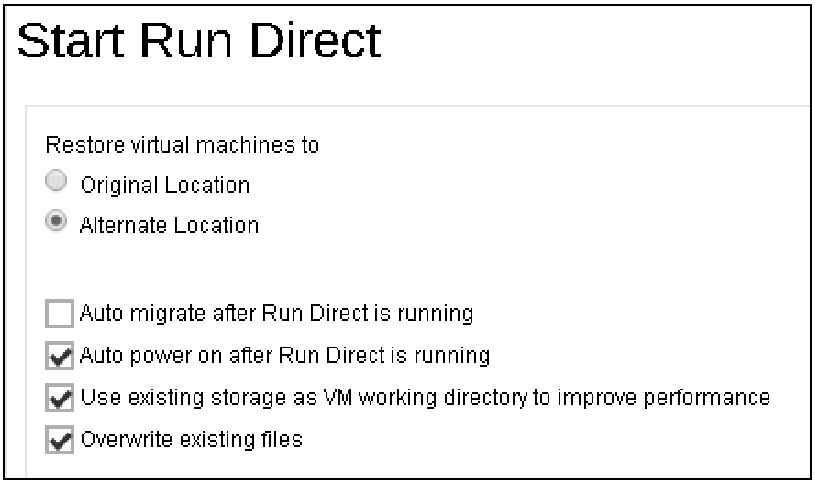
- vCenter05-v65
  - Datacenter
    - Hosts and Clusters
      - VSAN
        - ☑ Ubuntu 12.04 LTS

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

Select **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**

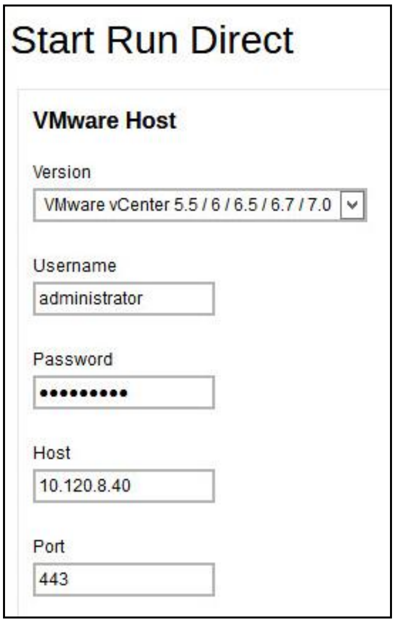
  Select this option to enhance performance of the restored VM.

- **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.



Start Run Direct

VMware Host

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

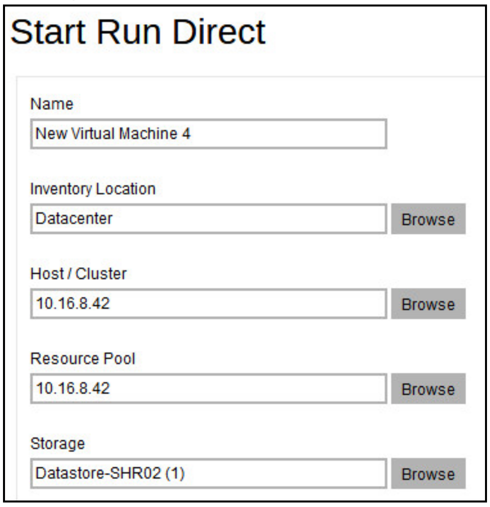
Username: administrator

Password: ●●●●●●●●●

Host: 10.120.8.40

Port: 443

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



Start Run Direct

Name: New Virtual Machine 4

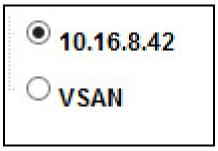
Inventory Location: Datacenter

Host / Cluster: 10.16.8.42

Resource Pool: 10.16.8.42

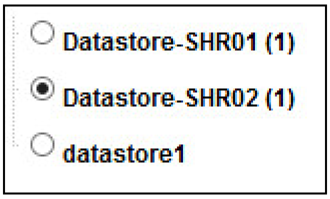
Storage: Datastore-SHR02 (1)

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



● 10.16.8.42

○ VSAN



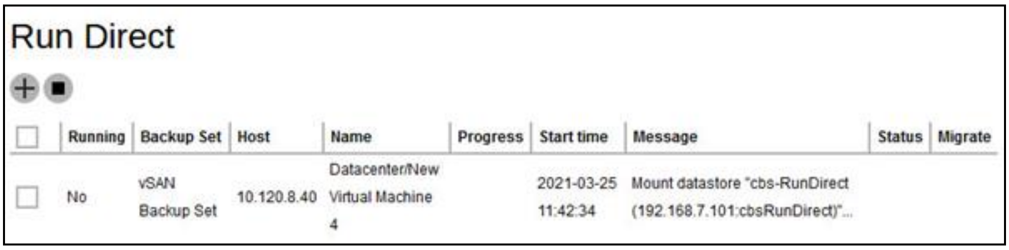
○ Datastore-SHR01 (1)

● Datastore-SHR02 (1)

○ datastore1

Click ▶ to start the restore.

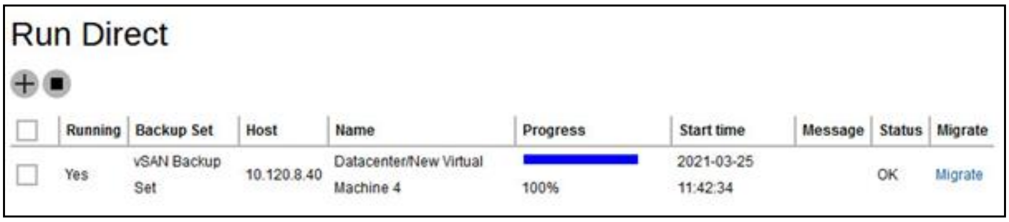
9. The **Run Direct** page appears, showing the status message of the Run Direct restore job.



Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	No	vSAN Backup Set	10.120.8.40	Datacenter/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%.

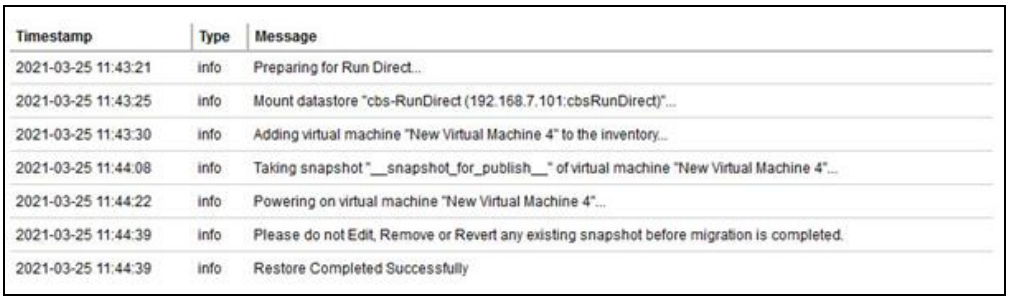


Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	Yes	vSAN Backup Set	10.120.8.40	Datacenter/New Virtual Machine 4	100%	2021-03-25 11:42:34		OK	Migrate

Restore log messages on AhsayCBS

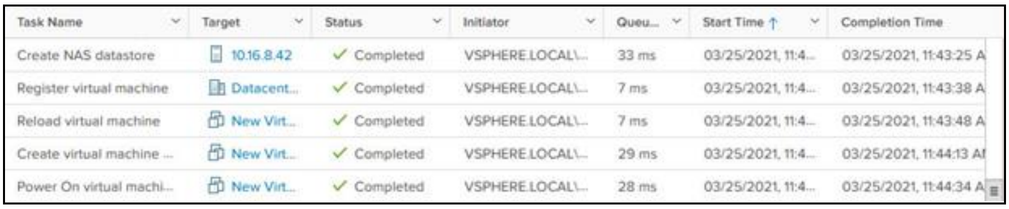
Click on the item on the Run Direct page.



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

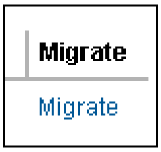
Restore log messages on the VMware vSphere Client

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

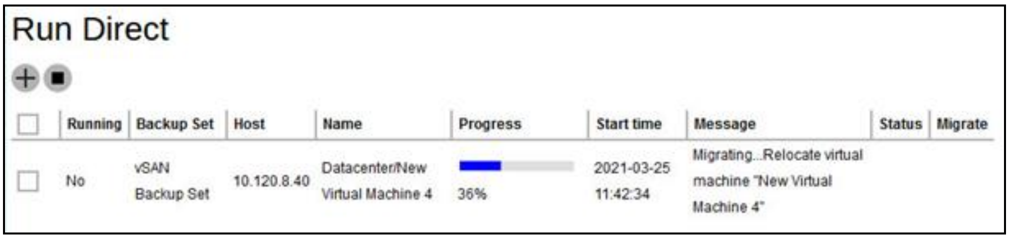


Task Name	Target	Status	Initiator	Queu...	Start Time ↑	Completion Time
Create NAS datastore	10.16.8.42	✓ Completed	VSPHERE.LOCAL\...	33 ms	03/25/2021, 11:4...	03/25/2021, 11:43:25 A
Register virtual machine	Datacent...	✓ Completed	VSPHERE.LOCAL\...	7 ms	03/25/2021, 11:4...	03/25/2021, 11:43:38 A
Reload 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 AI
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.



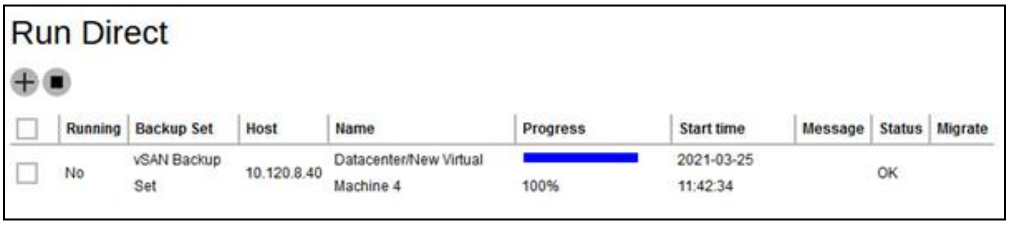
Migrate
Migrate



Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	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.

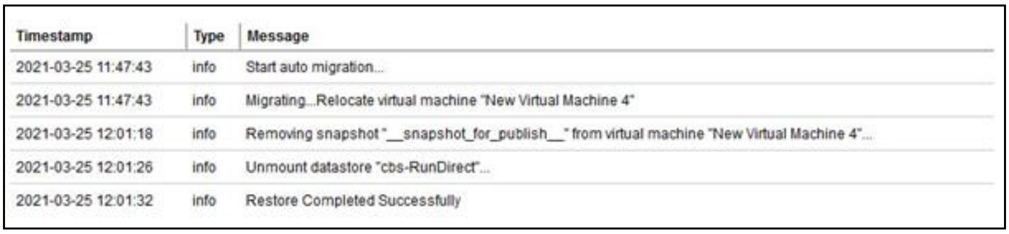


Run Direct

□	Running	Backup Set	Host	Name	Progress	Start time	Message	Status	Migrate
□	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

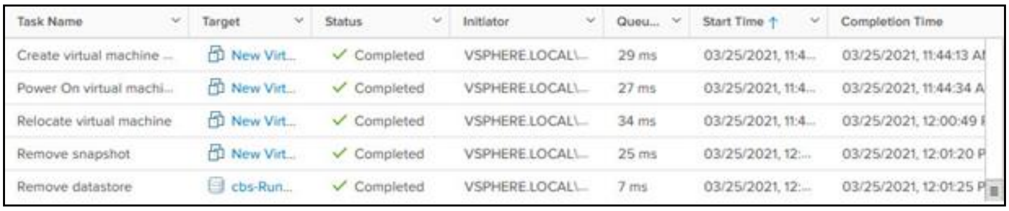
Click on the restore item on the Run Direct page to see the restore log messages.



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 AI
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 I
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.

9 Contacting Ahsay

9.1 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/

9.2 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

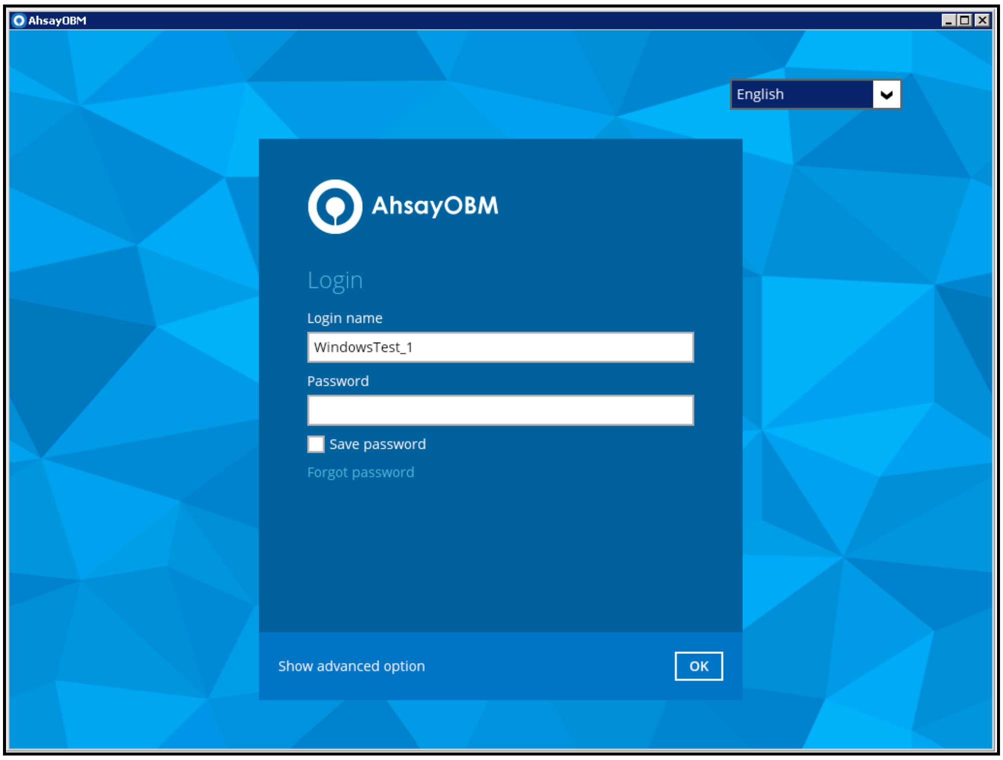
You need to read the instructions below only if you:

- Have created a backup set on AhsayCBS User Web Console; **AND**
- Selected the backup set to Run on Client (if you are running Office 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-

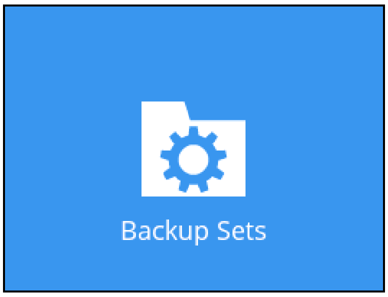
  Have selected a Predefined Destination in the backup creation process on AhsayCBS User Web Console but wish to add additional backup destination other than the predefined destination.

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

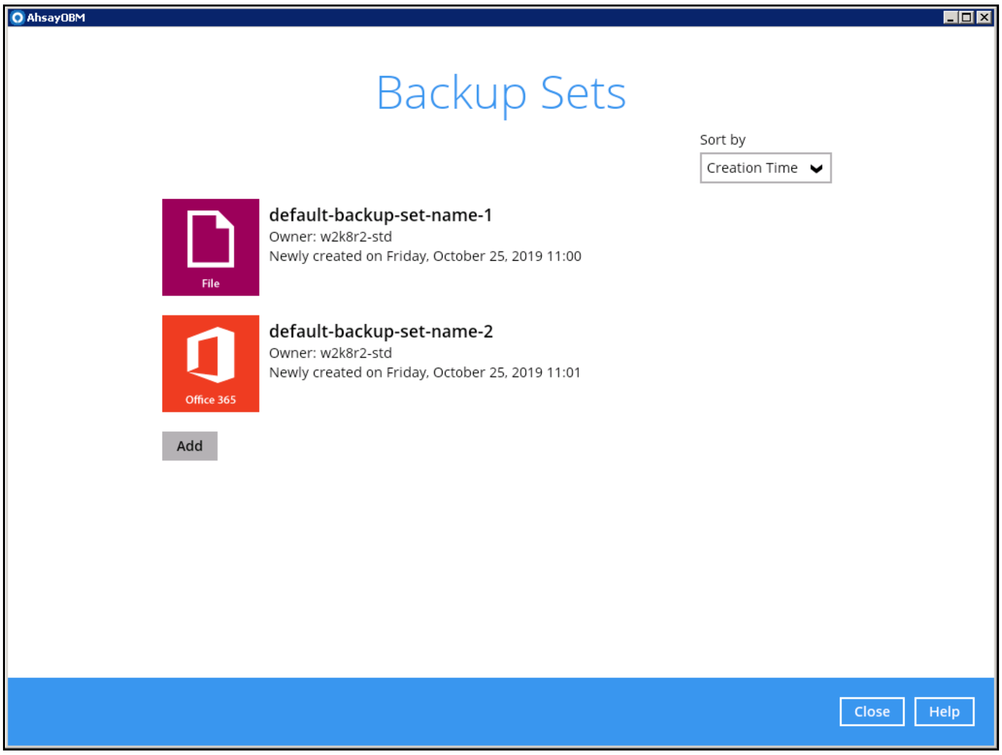


WindowsTest_1

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**.



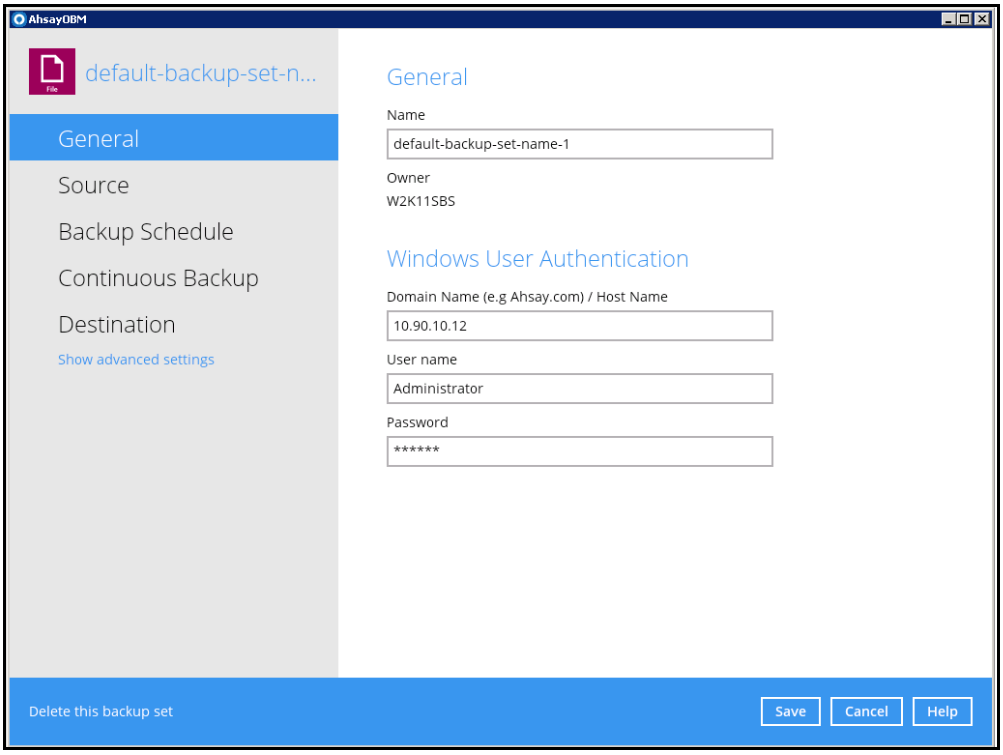
Backup Sets

Sort by
Creation Time

default-backup-set-name-1
Owner: w2k8r2-std
Newly created on Friday, October 25, 2019 11:00

default-backup-set-name-2
Owner: w2k8r2-std
Newly created on Friday, October 25, 2019 11:01

4. The General page of the backup set opens.



General

Name
default-backup-set-name-1

Owner
W2K11SBS

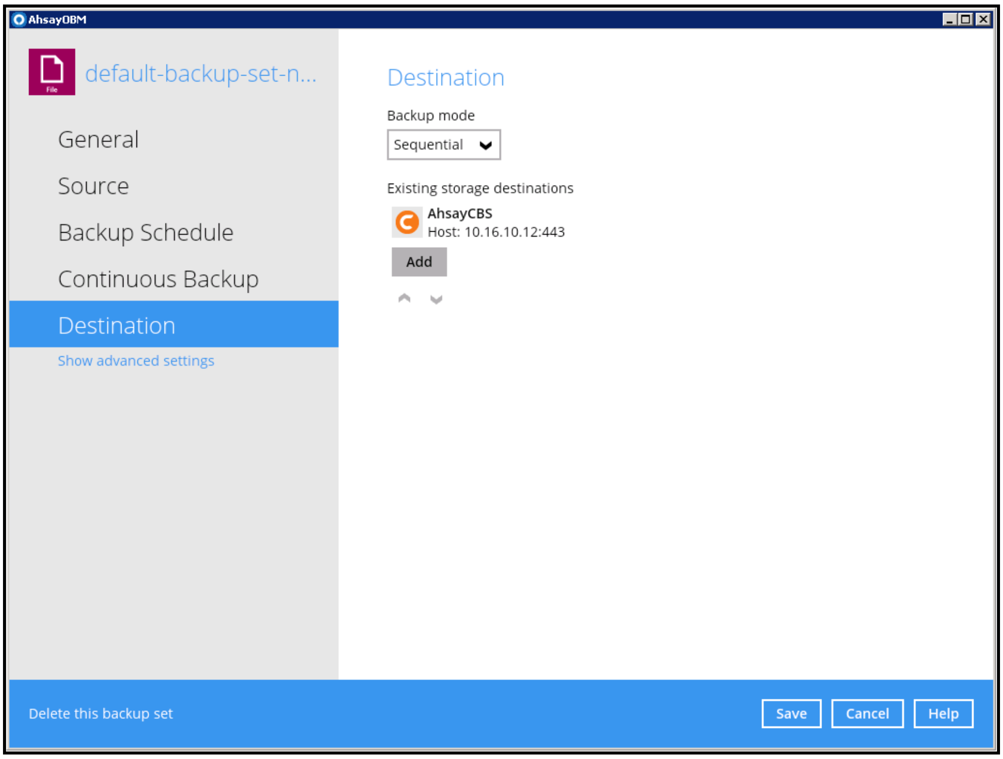
Windows User Authentication

Domain Name (e.g Ahsay.com) / Host Name
10.90.10.12

User name
Administrator

Password
******

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



Destination

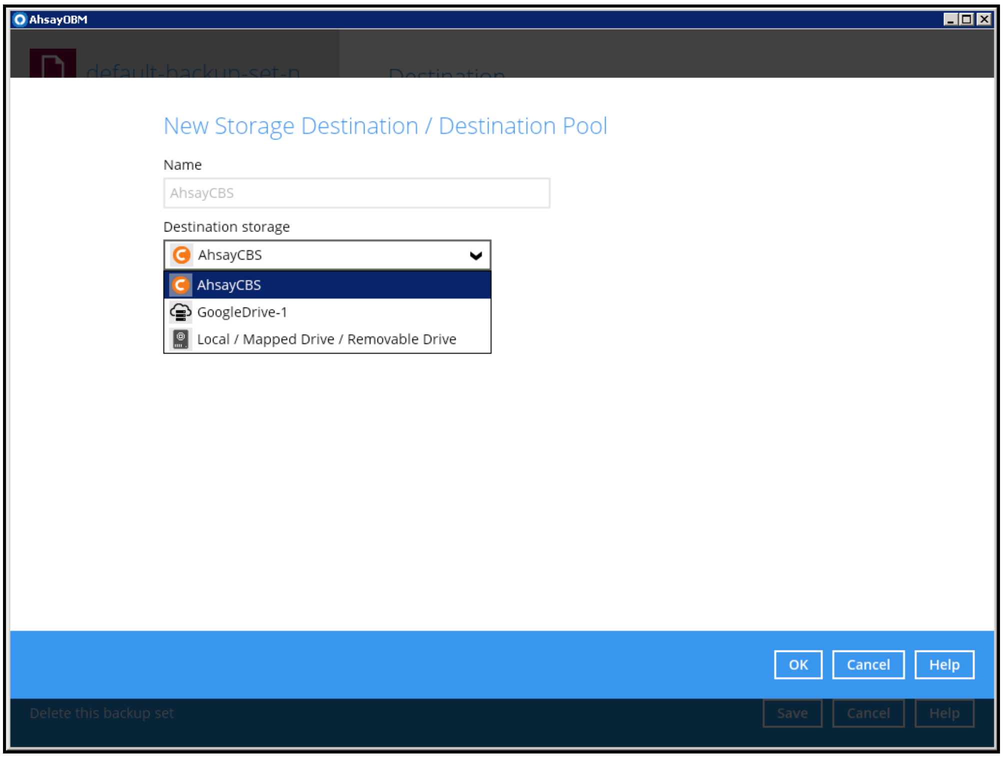
Backup mode

Sequential

Existing storage destinations

AhsayCBS
Host: 10.16.10.12:443

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**.



New Storage Destination / Destination Pool

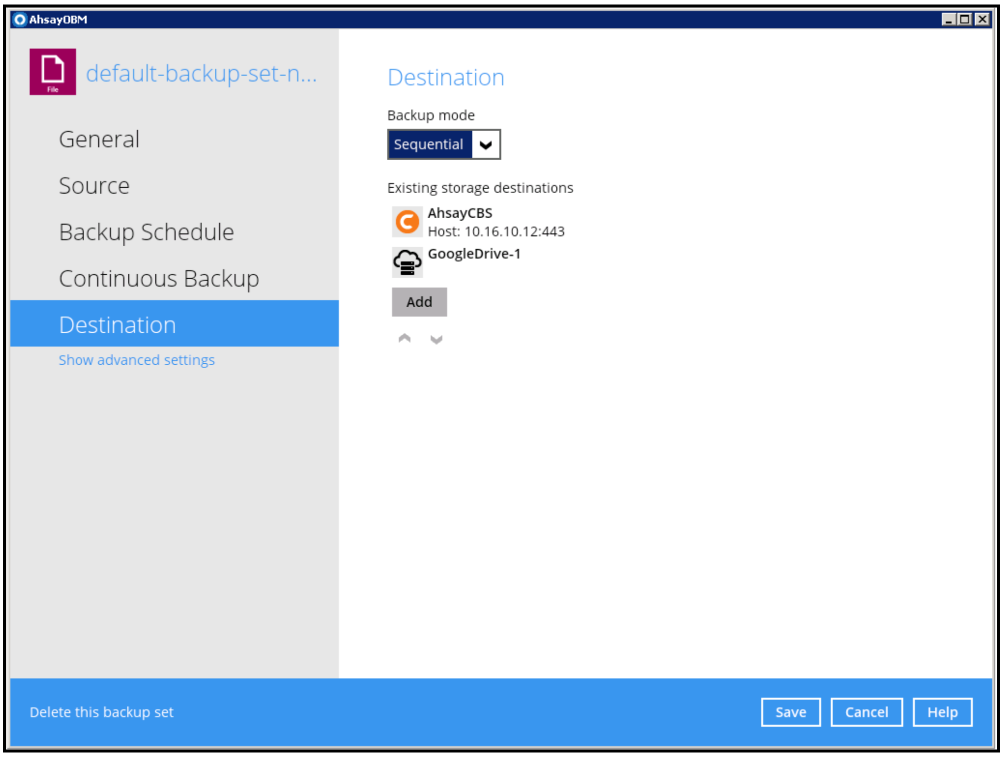
Name

AhsayCBS

Destination storage

AhsayCBS

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



Destination

Backup mode: Sequential

Existing storage destinations

AhsayCBS
Host: 10.16.10.12:443

GoogleDrive-1

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