Ahsay Backup

Ahsay Online Backup Manager v9

Quick Start Guide for QNAP NAS

Ahsay Systems Corporation Limited

22 November 2022

www.ahsay.com

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

Copyright Notice

Trademarks

Disclaimer

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

Revision History

Date	Descriptions	Version
25 January 2022	▪ Ch. 6.6 – added Deduplication	9.1.0.0
7 March 2022	▪ Ch. 9 – updated note for Migrate Data	9.1.0.0
8 August 2022	▪ Ch.2.11 – added non-compressible file list	9.1.0.0
3 November 2022	▪ Ch. 5 – added how to register device in 2FA ▪ Ch. 6 – added how to login with 2FA using different authenticators ▪ Ch. 7 – added unable to login using 2FA ▪ Ch. 8.6 – added Recycle Bin ▪ Ch. 8.10.1 – added Rebuild index and Delete corrupted data blocks permanently ▪ Appendix C – added removal of Scheduler in Settings	9.5.0.0
22 November 2022	▪ Ch. 8.6 – fixed typo in Recycle Bin	9.5.0.0

Table of Contents

1 Overview

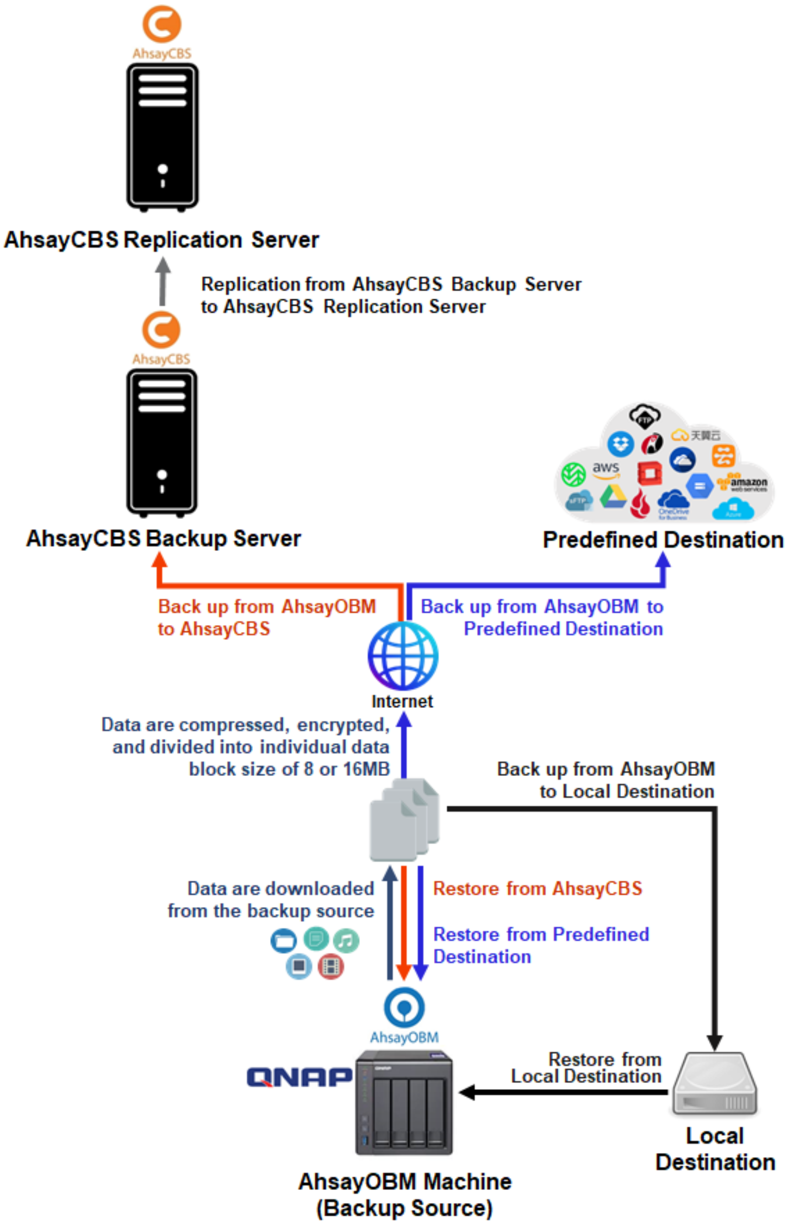
1.1 What is this software?

Ahsay brings you specialized client backup software, namely AhsayOBM, to provide a comprehensive backup solution for protecting file(s) / folder(s) on your machine, with a wide variety of backup destinations (major cloud storage service providers, FTP/SFTP, local drive, etc.) of your choice.

1.2 System Architecture

Below is the system architecture diagram illustrating the major elements involved in the backup process among the backup machine, AhsayOBM and AhsayCBS.

In this user guide, we will focus on the software installation, as well as the end-to-end backup and restore process using the AhsayOBM as a client backup software.


AhsayCBS
AhsayCBS Replication Server
Replication from AhsayCBS Backup Server to AhsayCBS Replication Server
AhsayCBS
AhsayCBS Backup Server
Predefined Destination
Back up from AhsayOBM to AhsayCBS
Back up from AhsayOBM to Predefined Destination
Internet
Data are compressed, encrypted, and divided into individual data block size of 8 or 16MB
Back up from AhsayOBM to Local Destination
Data are downloaded from the backup source
Restore from AhsaycBS
Restore from Predefined Destination
AhsayOBM
QNAP
Restore from Local Destination
Local Destination
AhsayOBM Machine (Backup Source)

2 Requirements for AhsayOBM on QNAP NAS

2.1 Hardware Requirements

Refer to the following article for the list of supported QNAP NAS modes:
FAQ: Ahsay Hardware Compatibility List (HRL) for AhsayOBM on QNAP NAS

WARNING

QNAP NAS models with less than 1GB RAM are not supported. As 1GB RAM or above is required to ensure application stability and optimal backup/restore performance. To back up data on unsupported QNAP NAS models, share the folder(s) then backup the data as network shared folder from a Windows machine.

For more details on how to create a shared folder(s), please refer to this link Creating a Shared Folder.

2.2 Software Requirements

Refer to the following article on supported QTS versions for QNAP NAS
FAQ: Ahsay Hardware Compatibility List (HRL) for AhsayOBM on QNAP NAS

2.3 AhsayOBM Installation

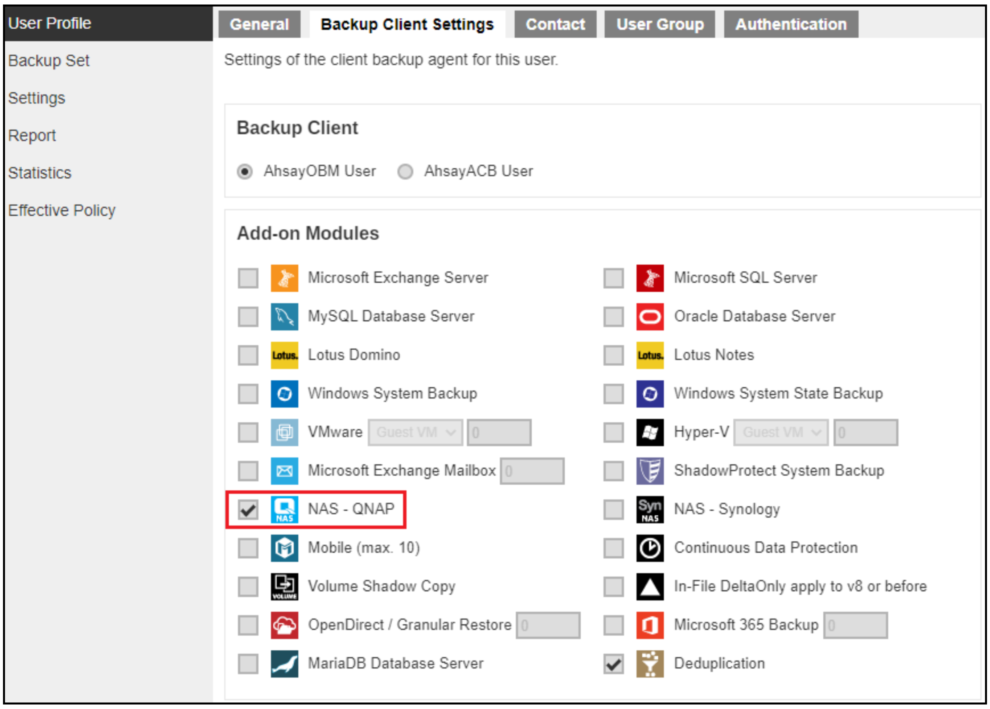
The latest version of AhsayOBM must be installed on the QNAP NAS.

2.4 NAS-QNAP Add-on Module

Make sure the NAS-QNAP add-on module in your AhsayOBM user account covers the backup of your QNAP NAS.

NOTE

The NAS-QNAP add-on module allows for the backup of unlimited number of QNAP NAS devices. However, each new AhsayOBM installation on a QNAP NAS device will require an additional AhsayOBM device license. Please contact your backup service provider for more details.



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 0
- □ Microsoft Exchange Mailbox 0
- ☑ NAS - QNAP
- □ Mobile (max. 10)
- □ Volume Shadow Copy
- □ OpenDirect / Granular Restore 0
- □ MariaDB Database Server
- □ Microsoft SQL Server
- □ Oracle Database Server
- □ Lotus Notes
- □ Windows System State Backup
- □ Hyper-V Guest VM 0
- □ ShadowProtect System Backup
- □ NAS - Synology
- □ Continuous Data Protection
- □ In-File DeltaOnly apply to v8 or before
- □ Microsoft 365 Backup 0
- ☑ Deduplication

2.5 Backup Quota Storage

Please ensure there is sufficient storage quota allocated on your AhsayOBM user account to accommodate the data from the QNAP NAS device.

Please contact your backup service provider for more details.

2.6 Java Requirement

In v9 the Oracle Java JDK files are already included and deployed as part of the AhsayOBM installation.

2.7 Memory Requirement

The default Java heap size of AhsayOBM installation on QNAP NAS is 256 MB. It is recommended that 1 GB RAM or more is installed for stability and better backup / restore performance.

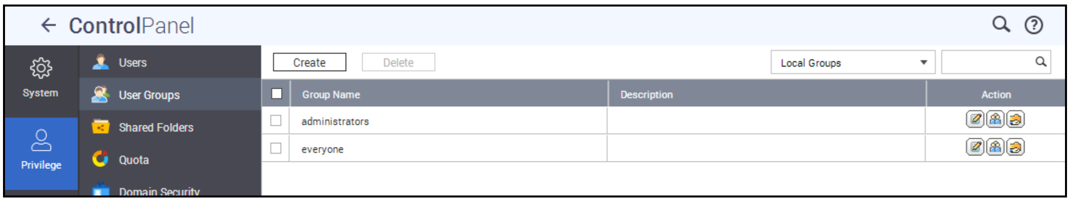
2.8 TCP Port Requirement

By default, the QNAP NAS machine uses TCP port 32168 for the WuiService.

TCP port 32168 must be free on the machine. Otherwise, the AhsayOBM client will not start and its backup and/or restore functions will not work.

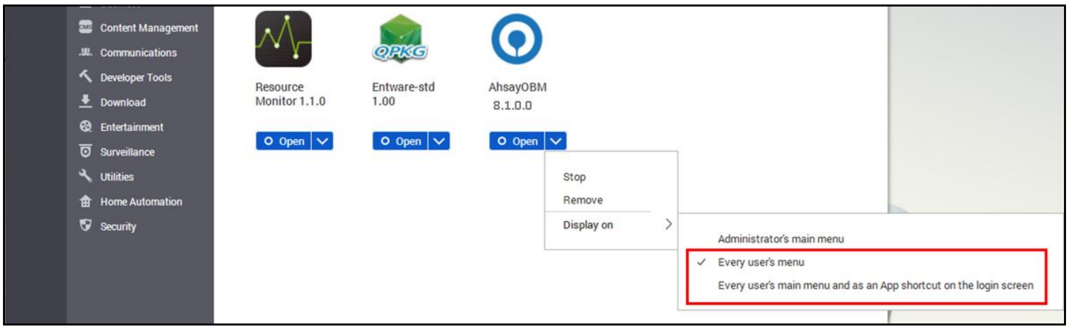
2.9 QNAP NAS User Account Permission

The QNAP NAS user account used for the AhsayOBM installation must be a member of "**administrator**" user group.

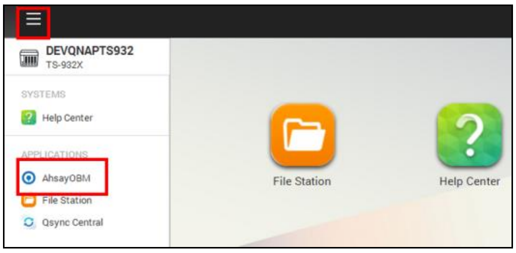


Group Name	Description	Action
administrators		
everyone		

The QNAP NAS user account belongs to "**everyone**" user group, select AhsayOBM to Display on "Every user's menu" or "Every user's main menu and as an App shortcut on the login screen" in App Center.



After login with user account belongs to "everyone" user group, you can find the App in the user's menu.



2.10 Network Bandwidth

10 Mbps or above connection speed.

2.11 Limitations

These are the unsupported features of AhsayOBM on QNAP NAS devices.

- Auto Upgrade
- Backup of Network Drives
- Decrypt Backup Data
- OpenDirect
- Restore Filter
- Space Freeing Up

The following is a list of non-compressible files:

Archive	Audio		Graphics	Video		
.7z	.aac	.ac3	.gif	.3gp	.asf	.avi
.bz2	.aifc	.amr	.jfif	.divx	.ivf	.m1v
.gz	.flac	.m4a	.jpeg	.m4v	.mkv	.mov
.rar	.mka	.mp2	.jpg	.mp2v	.mp4	.mpe
.xz	.mp3	.mpa	.png	.mpeg	.mpg	.mpv2
.zip	.ogg	.ra	.wim	.mts	.qt	.rmvb
	.rm	.snd	.wmp	.rv	.smil	.swf
	.ssm	.wma	.wmz	.vob	.webm	.wm
				.wmd	.wmv	

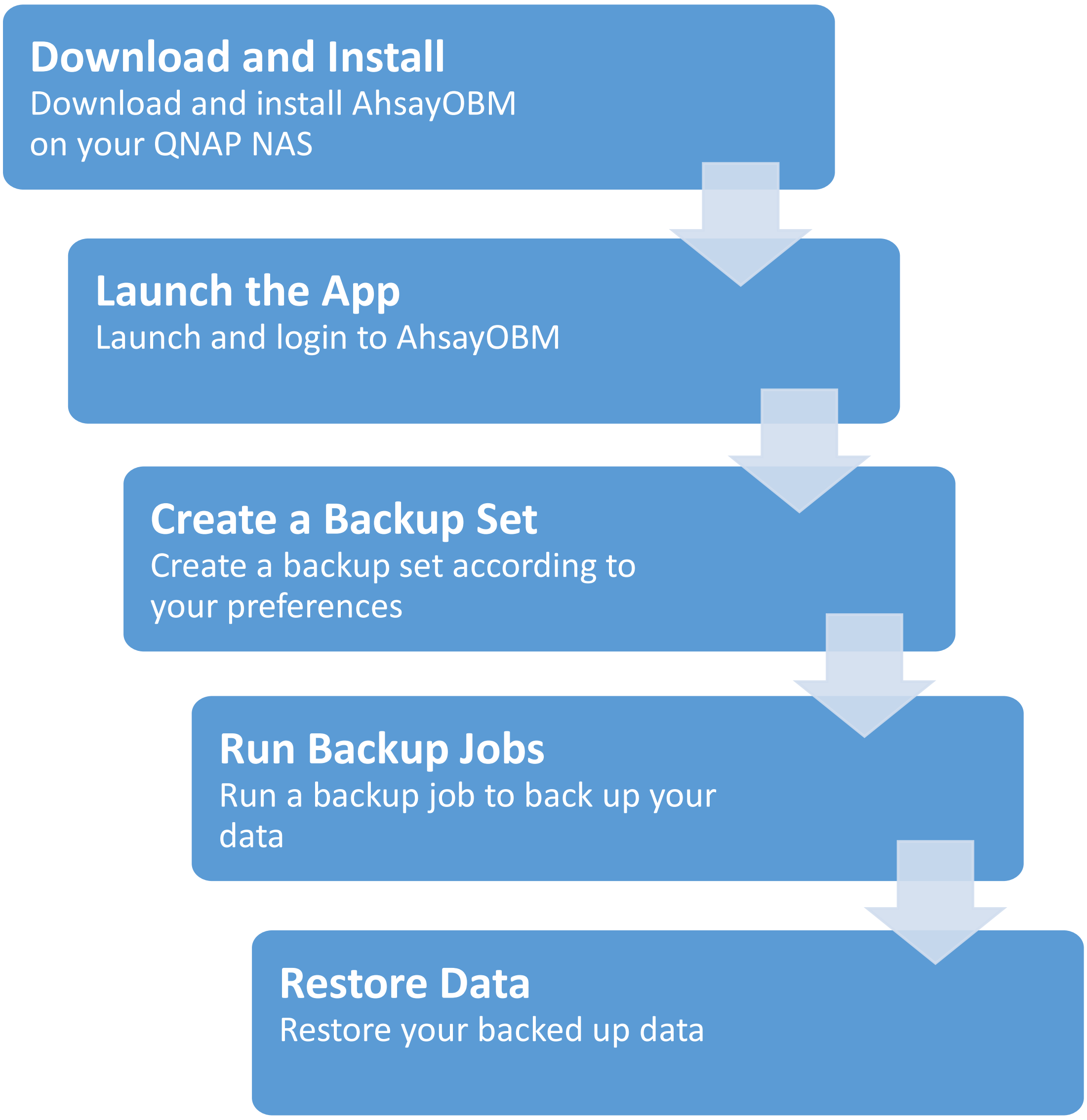
2.12 Supported Features from AhsayCBS Web Console

The following features of AhsayOBM on QNAP NAS devices but not displayed on the AhsayOBM GUI. These features can only be accessed or configured using AhsayCBS Web Console:

- Backup Source Filter
- Advanced Retention Policy Type
- Command Line Tool
- Bandwidth Control
- Follow Link
- Compression
- Usage Statistics Report

3 Get started with AhsayOBM

This quick start guide will walk you through the following 5 major parts to get you started with using AhsayOBM.



Download and Install
Download and install AhsayOBM on your QNAP NAS

Launch the App
Launch and login to AhsayOBM

Create a Backup Set
Create a backup set according to your preferences

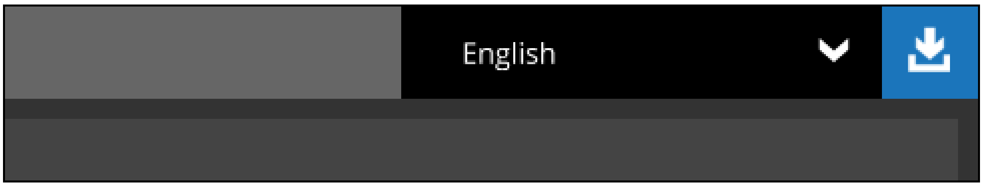
Run Backup Jobs
Run a backup job to back up your data

Restore Data
Restore your backed up data

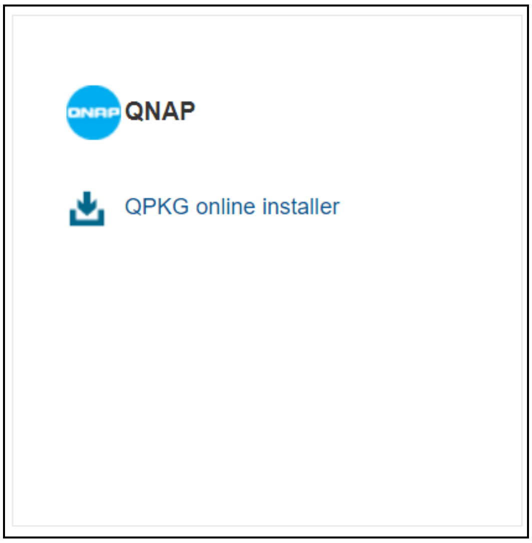
4 Download and Install AhsayOBM

4.1 Download AhsayOBM

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

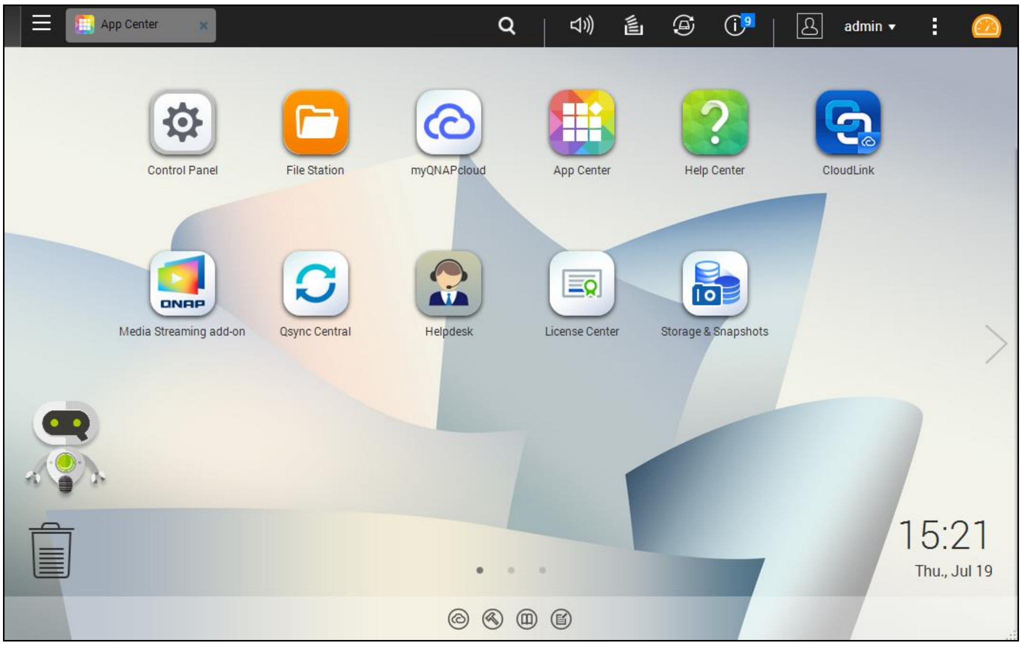


2. In the **QNAP** section under the **AhsayOBM** tab of the download page, download the AhsayOBM **QPKG online installer**.



4.2 Install AhsayOBM using QPKG online installer

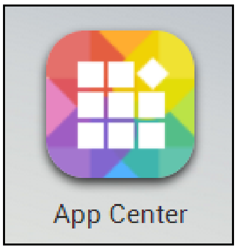
1. Login to QNAP QTS with the admin account. In a web browser, enter the QNAP NAS device IP address and use the login credentials to login.



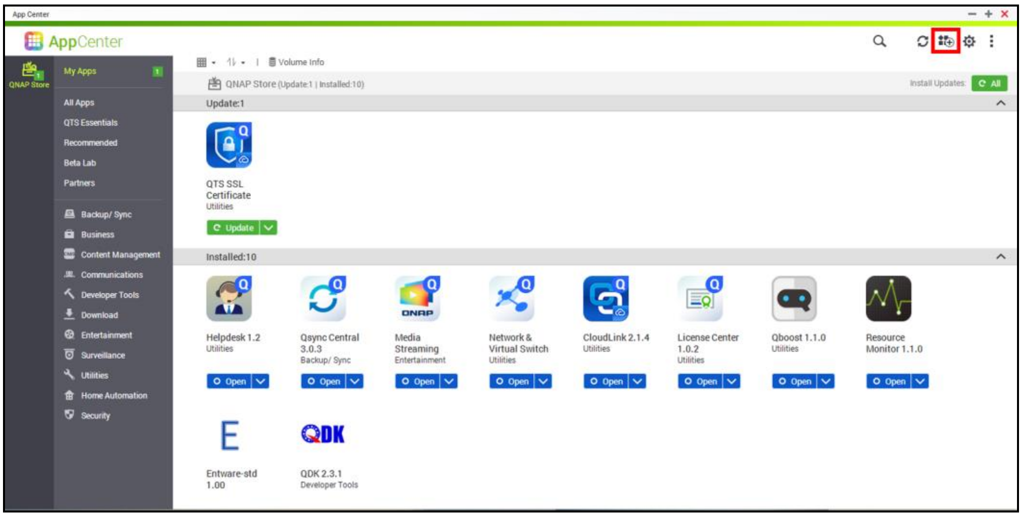
NOTE

Refer to the following user manual for information on how to login to QTS:
https://www.qnap.com/en/support/con_show.php?cid=11

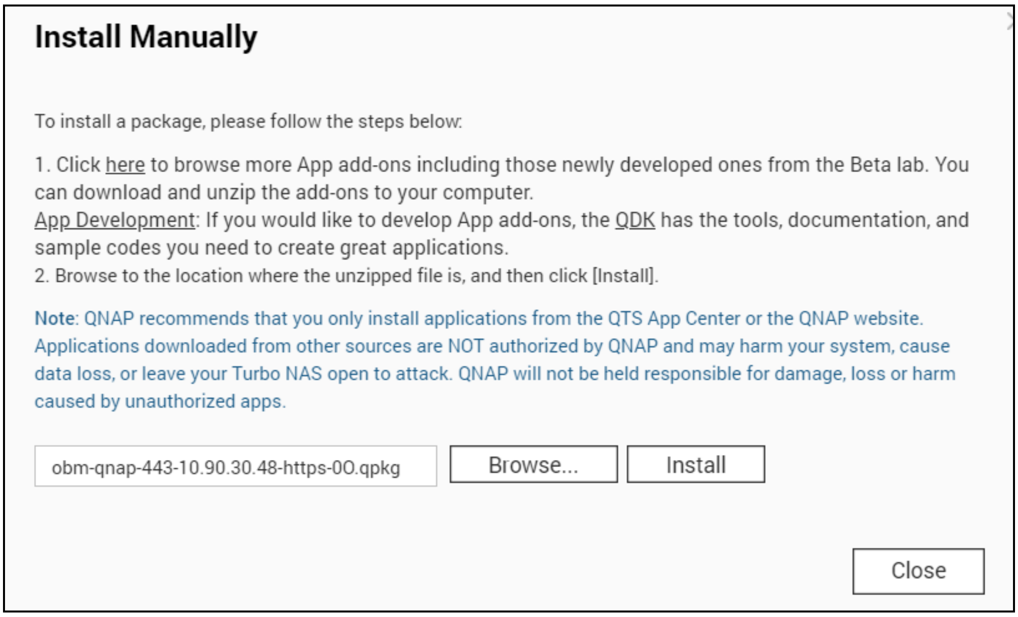
2. To install AhsayOBM on QNAP NAS, click the **App Center** icon from the desktop.



3. When the App Center window appears, select **Install Manually**.



4. When the Install Manually window appears, click **Browse** to select the AhsayOBM QPKG file which you have downloaded (e.g., obm-qnap-443-10.90.30.48-https-0O). Then, click **Install** to proceed.



Install Manually

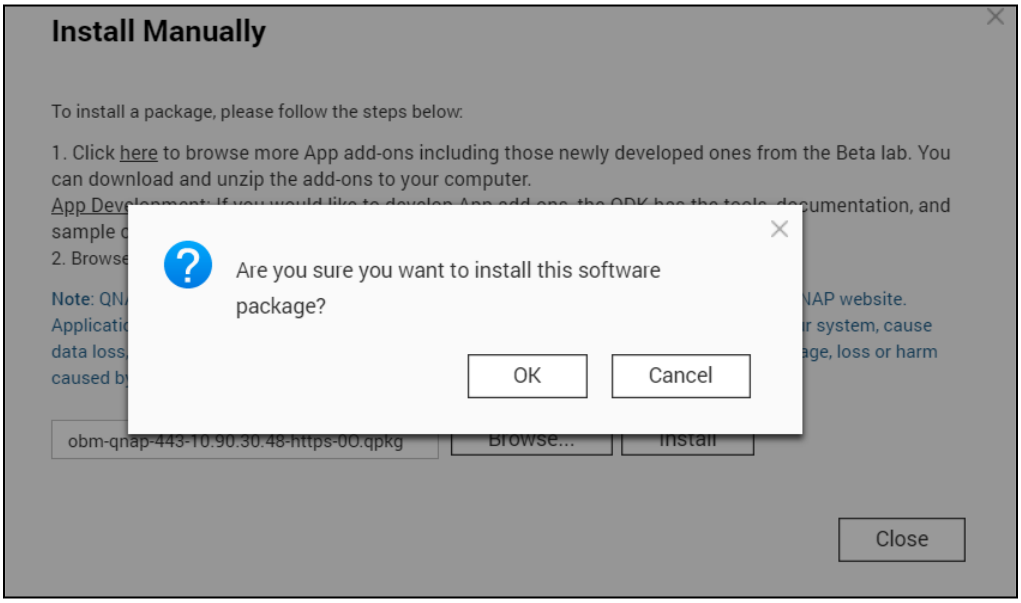
To install a package, please follow the steps below:

1. Click here to browse more App add-ons including those newly developed ones from the Beta lab. You can download and unzip the add-ons to your computer.
App Development: If you would like to develop App add-ons, the QDK has the tools, documentation, and sample codes you need to create great applications.
2. Browse to the location where the unzipped file is, and then click [Install].

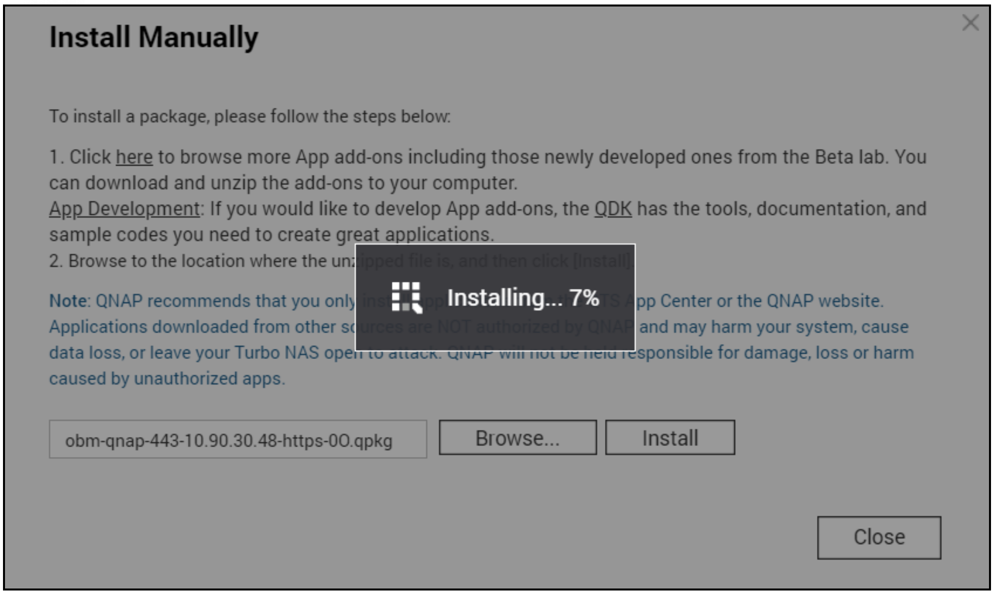
Note: QNAP recommends that you only install applications from the QTS App Center or the QNAP website. Applications downloaded from other sources are NOT authorized by QNAP and may harm your system, cause data loss, or leave your Turbo NAS open to attack. QNAP will not be held responsible for damage, loss or harm caused by unauthorized apps.

obm-qnap-443-10.90.30.48-https-0O.qpkg

5. When the following message appears, click **OK** to start the installation of AhsayOBM.



Are you sure you want to install this software package?



Install Manually

To install a package, please follow the steps below:

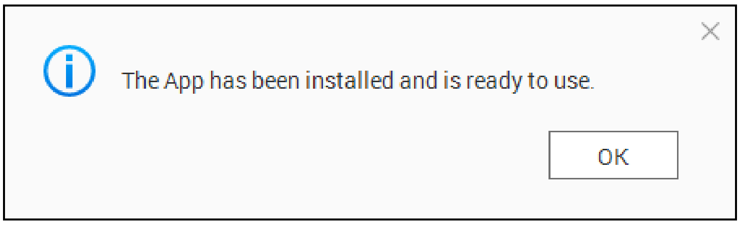
1. Click here to browse more App add-ons including those newly developed ones from the Beta lab. You can download and unzip the add-ons to your computer.
App Development: If you would like to develop App add-ons, the QDK has the tools, documentation, and sample codes you need to create great applications.
2. Browse to the location where the unzipped file is, and then click [Install].

Note: QNAP recommends that you only ins... TS App Center or the QNAP website. Applications downloaded from other sources are NOT authorized by QNAP and may harm your system, cause data loss, or leave your Turbo NAS open to attack. QNAP will not be held responsible for damage, loss or harm caused by unauthorized apps.

Installing... 7%

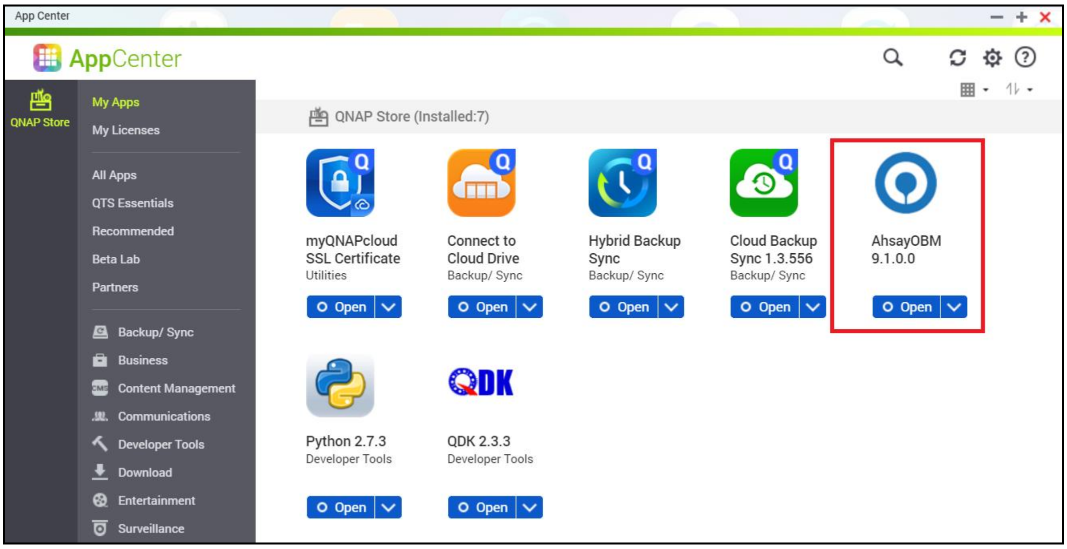
obm-qnap-443-10.90.30.48-https-00.qpkg

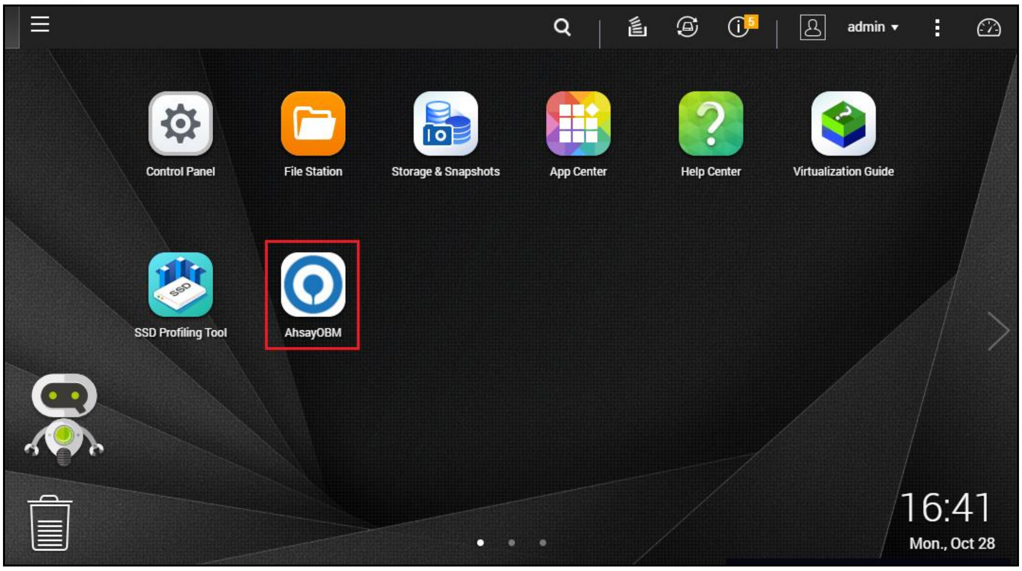
6. When the installation is completed, the following message will be displayed. Click **OK** to finish the installation.



The App has been installed and is ready to use.

7. After the installation, AhsayOBM will be listed in App Center and desktop.





4.3 AhsayOBM Scheduler Service Check

This option is used to kick automated or scheduled backup jobs. To start, login to QNAP NAS device using ssh client, i.e., putty.

To **check** if the AhsayOBM scheduler service is running, use the **ps** command.

Scheduler service is running, highlighted in red.

```
login as: admin
admin@10.3.0.122's password:
[~] # ps -ef|grep java
 3562 admin    640772 S
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/jvm/bin/java
-Xrs -Xms64m -Xmx1024m -Dsun.nio.PageAlignDirectMemory=true -
Djava.library.path= . -cp .:./cb.jar WuiService
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm /share/CACH
EDEV1_DATA/.qpkg/AhsayOBM/.obm --port=32168
11017 admin 956 S grep java
20327 admin 157000 S /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/jvm/bin/java
-Xms64m -Xmx256m -Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=.
-cp .:./cbs.jar cbs /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm
```

To manually **stop** the scheduler service,

- First get the system volume path, use the **getcfg SHARE_DEF defVolMP -f /etc/config/def_share.info** script
- Then use the **touch /%system volume path%/.qpkg/AhsayOBM/obm/ipc/Scheduler/stop** script
- Last, use the **ps** command to check if the scheduler is still running.

For example

```
[~] # getcfg SHARE_DEF defVolMP -f /etc/config/def_share.info
/share/CACHEDEV1_DATA
[~] # touch /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/ipc/Scheduler/stop
[~] # ps -ef|grep java
 3562 admin 640772 S
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/jvm/bin/java -Xrs -Xms64m -
Xmx1024m -Dsun.nio.PageAlignDirectMemory=true -Djava.library.path=
. -cp .:./cb.jar WuiService /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/.obm --port=32168
12542 admin 1000 S grep java
```

To manually **start** the scheduler service, use the

/%system volume path%/.qpkg/AhsayOBM/obm/bin/Scheduler.sh script and use the **ps** command again to check.

In our example, the scheduler service is running highlighted in red.

```
[~] # /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/bin/Scheduler.sh
[~] # ps -ef|grep java
 3562 admin 640772 S /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/jvm/bin/java
-Xrs -Xms64m -Xmx1024m -Dsun.nio.PageAlignDirectMemory=true -
Djava.library.path=. -cp .:./cb.jar WuiService
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/.obm --port=32168
17562 admin 86536 S /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm/jvm/bin/java
-Xms64m -Xmx256m -Dsun.nio.PageAlignDirectMemory=true -
Djava.library.path=. -cp .:./cbs.jar cbs
/share/CACHEDEV1_DATA/.qpkg/AhsayOBM/obm
18004 admin 944 R grep java
```

4.4 RunLevel Symlink Check

During installation, the following symlinks to the scheduler startup script **/%system volume path%/.qpkg/AhsayOBM/AhsayOBM.sh** will be created that allows the AhsayOBM Scheduler Service to automatically start each time the machine is rebooted or restarted.

To verify if the symlinks have been created correctly, use the **ls** command. You will see the symlink, highlighted in red.

```
[~] # ls -la /etc/init.d/Ahsay*
lrwxrwxrwx 1 admin administrators 48 2019-05-23 12:55 /etc/init.d/AhsayOBM
.sh -> /share/CACHEDEV1_DATA/.qpkg/AhsayOBM/AhsayOBM.sh*
[~] #
```

5 Register device for 2FA in AhsayOBM

There are two types of authenticators that can be used to register a device for 2FA in AhsayOBM:

- Ahsay Mobile Authenticator
- Third-party TOTP Authenticator (e.g. Microsoft Authenticator, Google Authenticator, Authy, Duo, LastPass Authenticator, iOS 15 Built-in Two-Factor Authenticator, etc.)

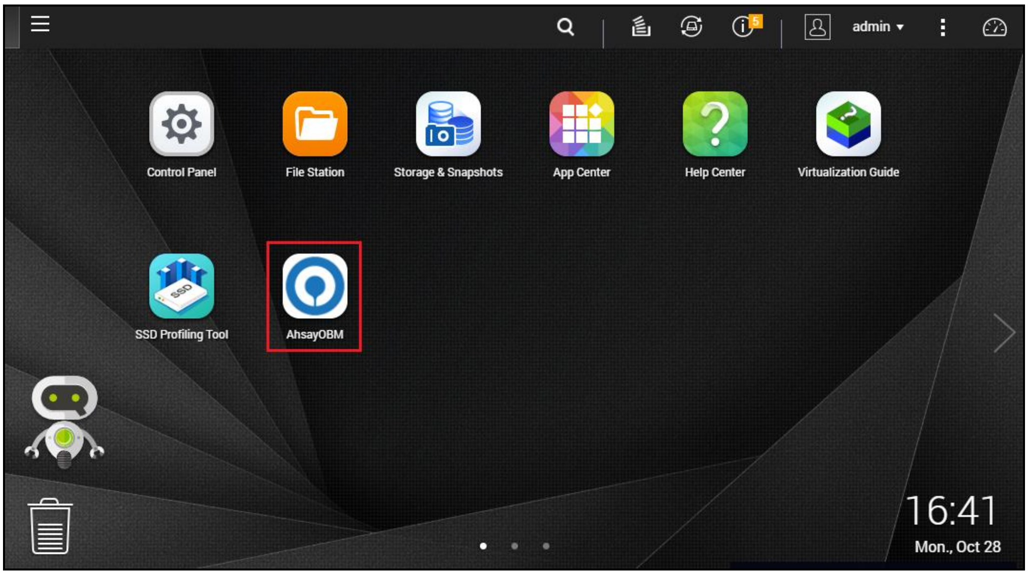
The 2FA registration steps using the different types of authenticators will be discussed in this chapter.

- Using Ahsay Mobile Authenticator
  - Supports two types of authentication:
    - Push Notification
    - TOTP
  - Can be configured to support two 2FA modes:
    - Push Notification and TOTP (default mode); or
    - TOTP only
- Using Microsoft Authenticator
- Using Google Authenticator

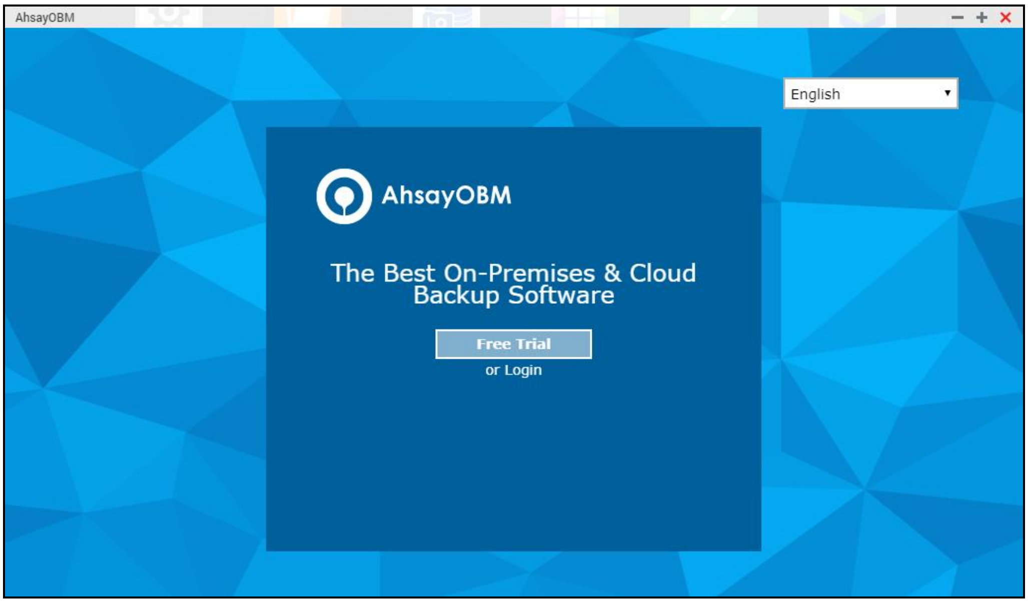
5.1 Using Ahsay Mobile Authenticator

To register a device for 2FA in AhsayOBM using Ahsay Mobile, please follow the steps below:

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

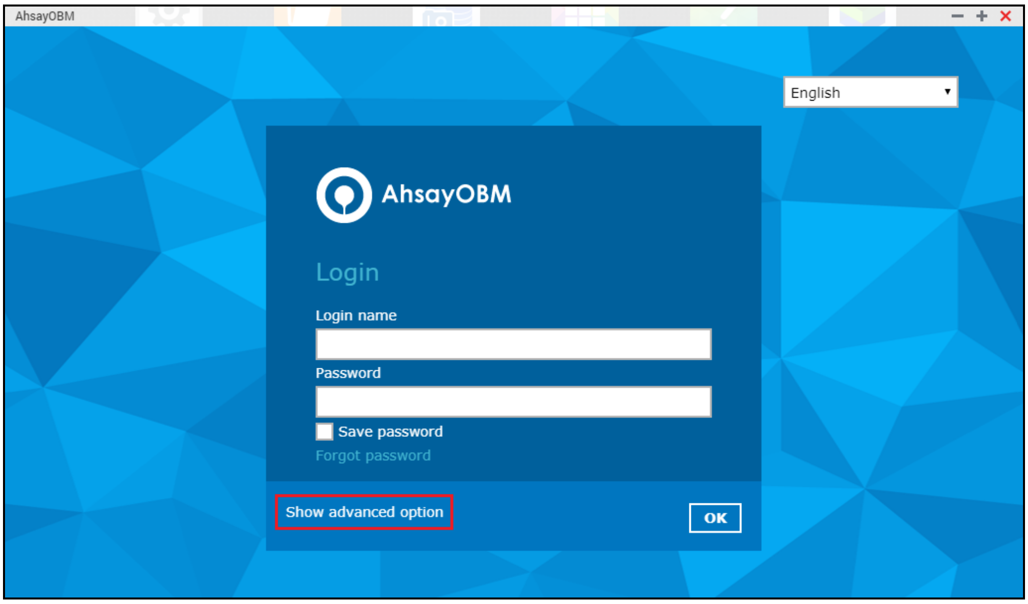


2. The Free Trial registration option may be displayed when you login for the first time. If you want to create a free trial account, proceed to Appendix D. Otherwise, click **Login** if you already have an AhsayOBM account.

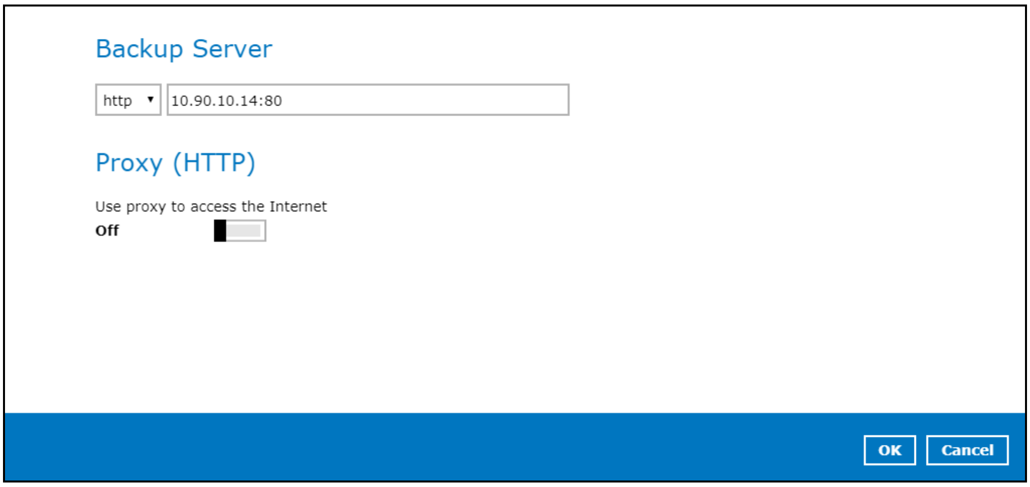


NOTE
The Free Trial Registration option will only be displayed if your backup service provider has enabled free trial registration on the backup server.

3. In case you want to enter the backup server setting provided by your backup service provider, click **Show advanced option**.



4. Click **OK** after typing in the backup server information. You can turn on the Proxy feature if needed.



Backup Server

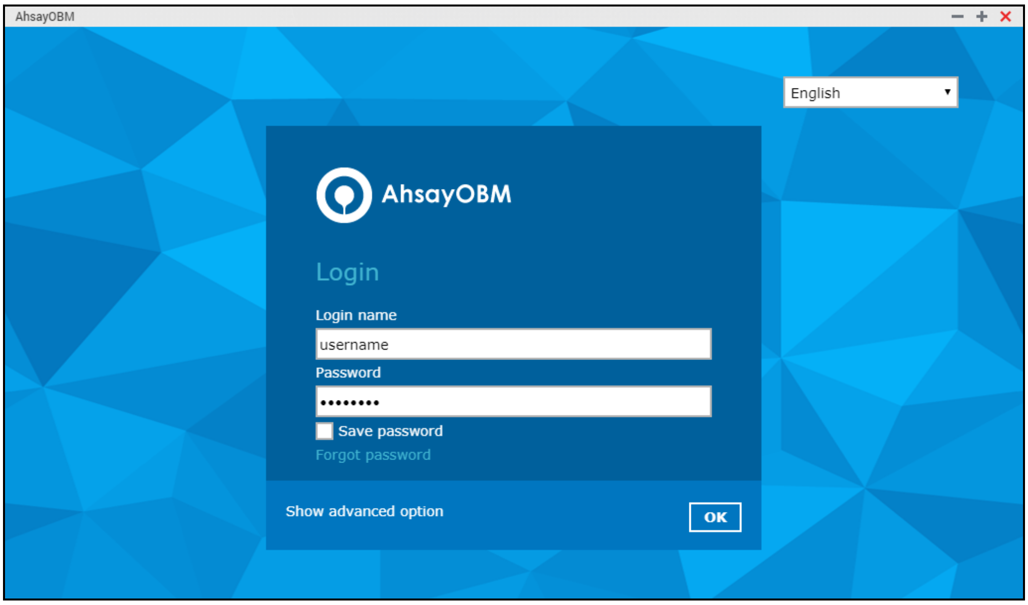
http ▾ 10.90.10.14:80

Proxy (HTTP)

Use proxy to access the Internet

Off

5. Enter the Login name and Password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



Login

Login name: username

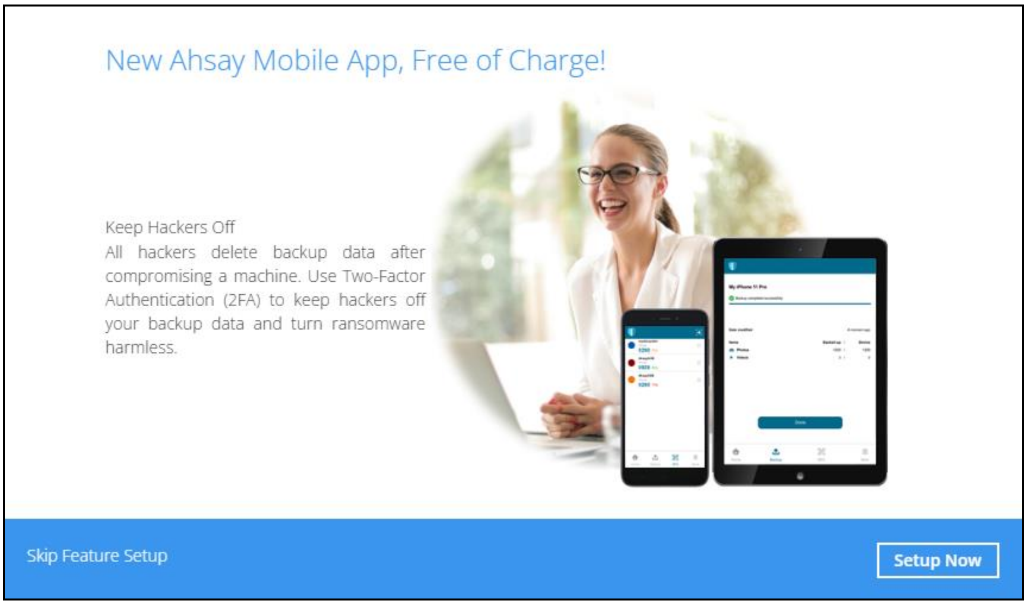
Password: ••••••••

□ Save password

NOTE

The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

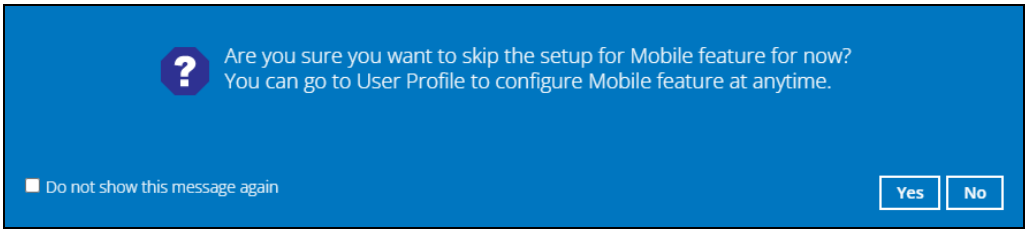
6. You will have the option to set up your 2FA. Click **Setup Now**.



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.

If you do not want to setup the 2FA feature, click the **Skip Feature Setup** link. If you click **Yes** in the pop-up message that will be displayed, it will skip to step 9. Otherwise, click **No** to continue with the setup of the 2FA feature.



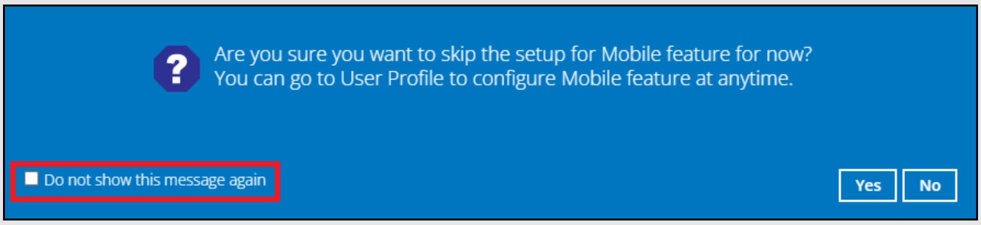
Are you sure you want to skip the setup for Mobile feature for now?
You can go to User Profile to configure Mobile feature at anytime.

NOTE

The 2FA reminder screen will be displayed every time the user logs in if:

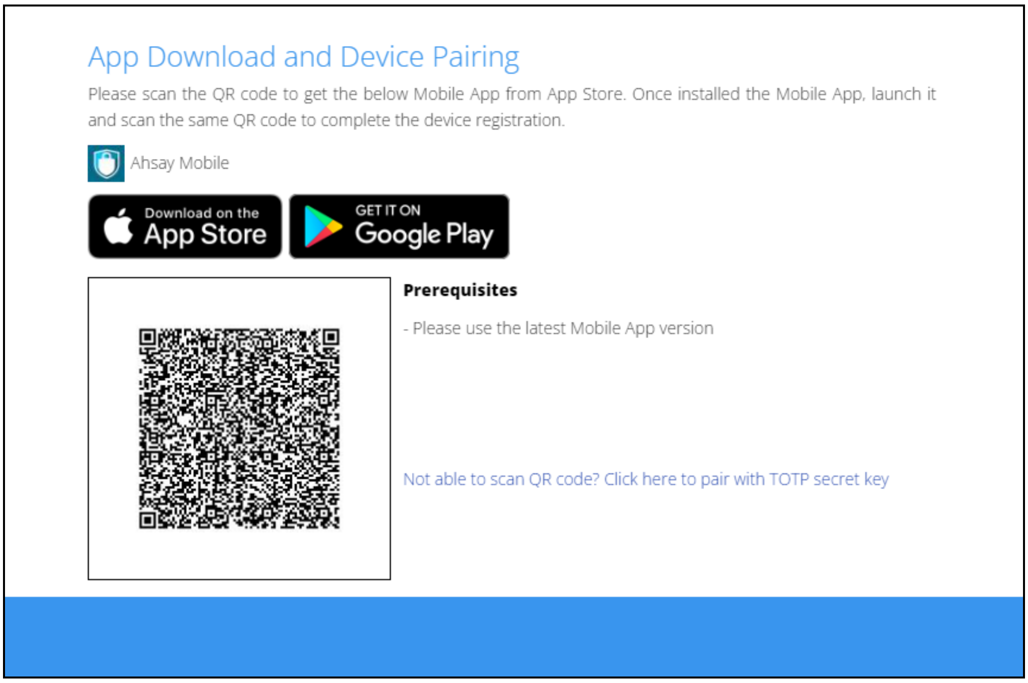
- 2FA is enabled
- the user does not have a paired device for 2FA

To stop the 2FA reminder screen from being displayed again upon login, tick the **Do not show this message again** checkbox.



Are you sure you want to skip the setup for Mobile feature for now?
You can go to User Profile to configure Mobile feature at anytime.

7. Download the Ahsay Mobile app from the App Store / Google Play Store.



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

8. Ahsay Mobile supports two types of authentication method:

   - Push Notification
   - TOTP

   Ahsay Mobile can be configured to support two 2FA modes:

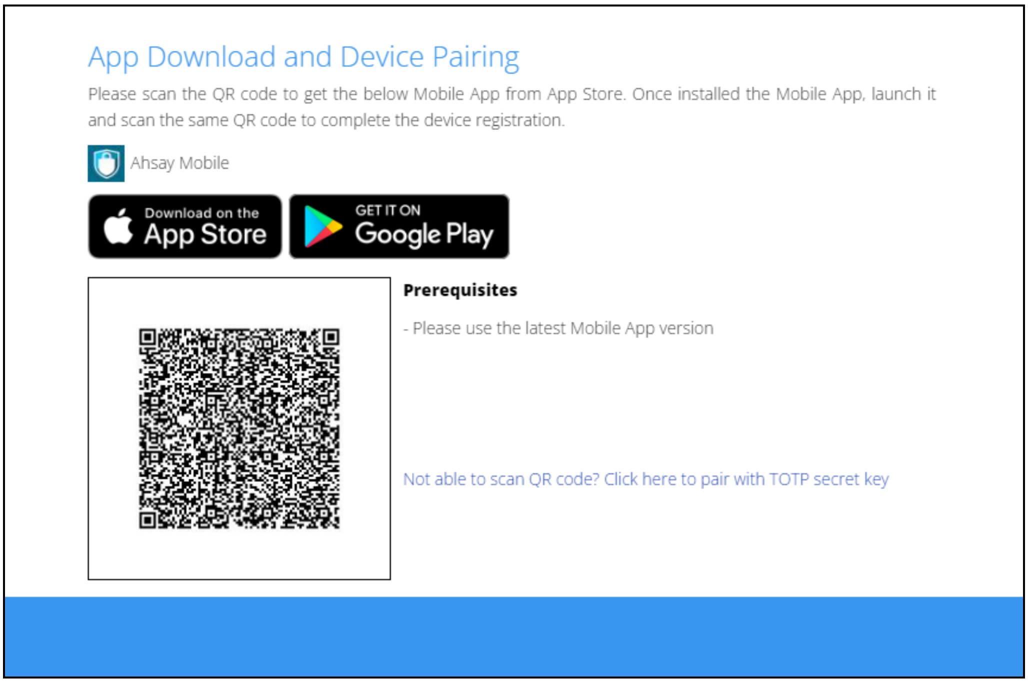
   - Push Notification and TOTP (default mode)

     or

   - TOTP only

Push Notification and TOTP (default mode)

i. To configure Push Notification and TOTP 2FA with Ahsay Mobile, simply scan the displayed QR code using the Ahsay Mobile app.



App Download and Device Pairing

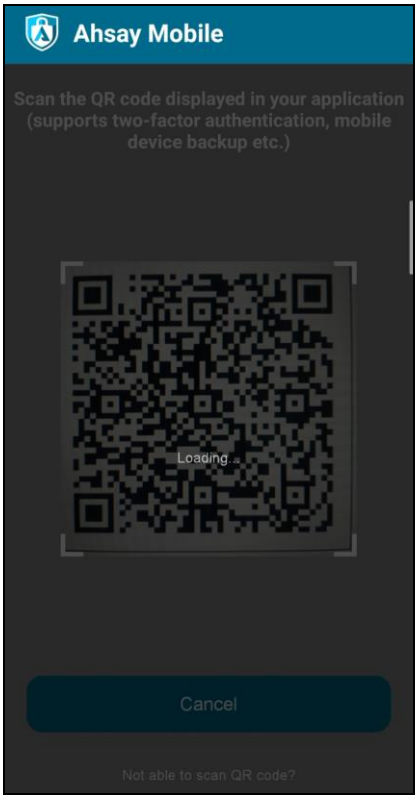
Please scan the QR code to get the below Mobile App from App Store. Once installed the Mobile App, launch it and scan the same QR code to complete the device registration.

Prerequisites

- Please use the latest Mobile App version

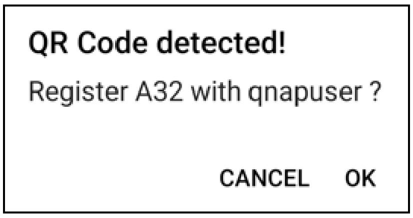
Not able to scan QR code? Click here to pair with TOTP secret key

ii. In this example, the Ahsay Mobile app is installed on a mobile device named “A32”.



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?

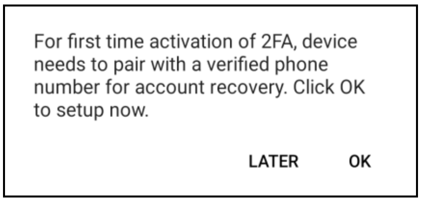
Tap **OK** to continue.



QR Code detected!

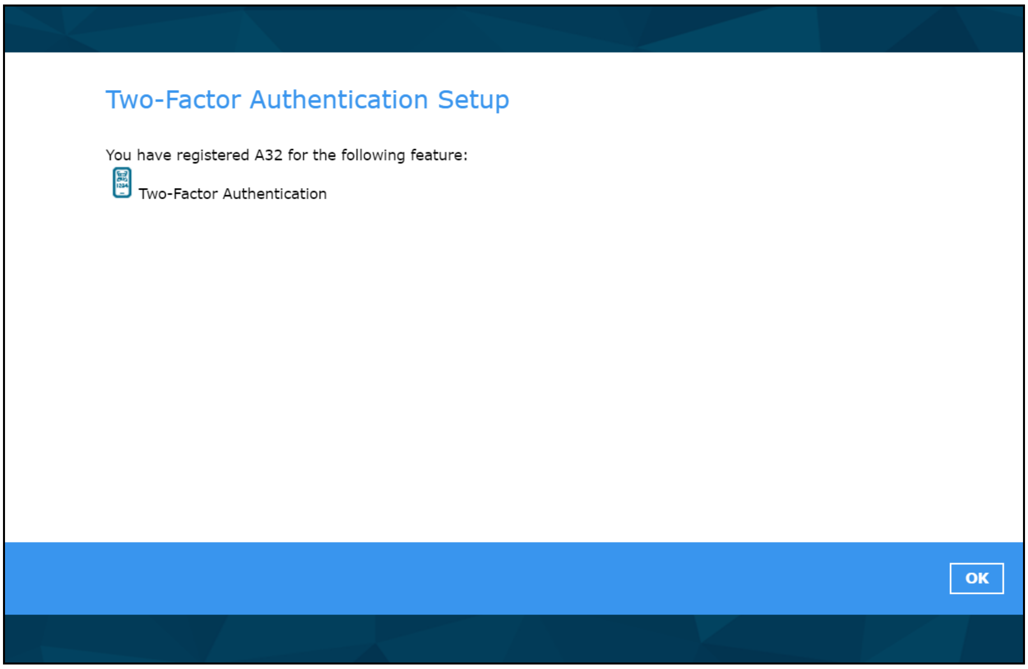
Register A32 with qnapuser ?

Once the device is successfully paired, the following message will be displayed in the Ahsay Mobile app. You can set up a recovery number here that will be used in case of “Authentication Recovery” procedure by tapping **OK**. Otherwise, tap **LATER** to set it up later on.



For first time activation of 2FA, device needs to pair with a verified phone number for account recovery. Click OK to setup now.

iii. After successful scan of the QR code, you have now registered Ahsay Mobile for Push Notification and TOTP 2FA. Click **OK** to continue.



Two-Factor Authentication Setup

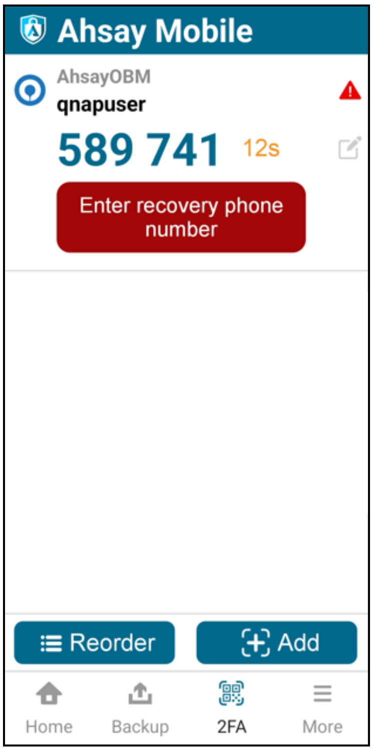
You have registered A32 for the following feature:

Two-Factor Authentication

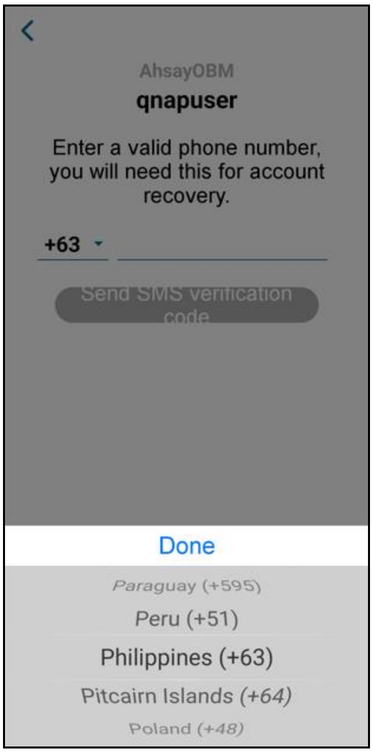
Phone number verification for account recovery

iv. In the Ahsay Mobile app, go to 2FA to enter the phone number for account recovery. Tap **Enter recovery phone number**.

NOTE
Although push notification and TOTP will still work if the recovery phone number registration is not completed, it is still strongly recommended to complete **step iv** as you will not be able to access AhsayOBM if you lose your mobile device which also means loss of access to backup data.



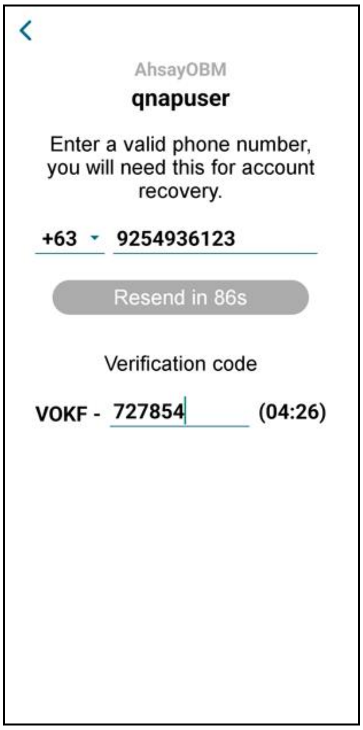
v. Select your country code and enter your phone number. Tap **Send SMS verification code**.

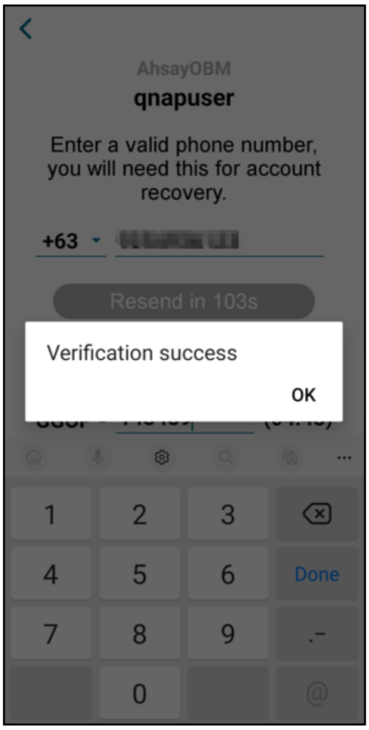

AhsayOBM

qnapuser

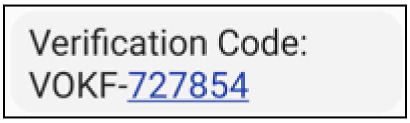
Enter a valid phone number, you will need this for account recovery.

vi. Enter the verification code sent to your mobile device.

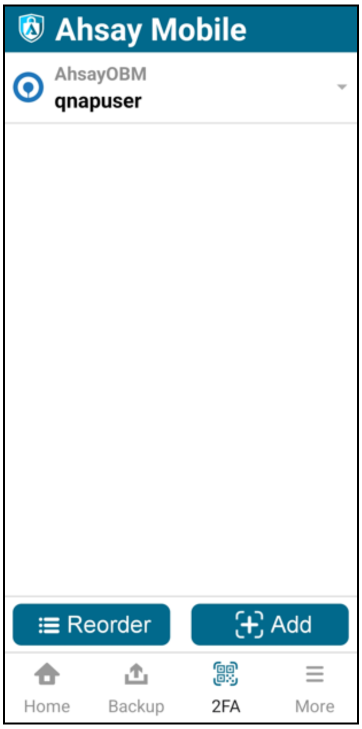

AhsayOBM
qnapuser
Enter a valid phone number, you will need this for account recovery.
+63 9254936123
Verification code
VOKF - 727854 (04:26)

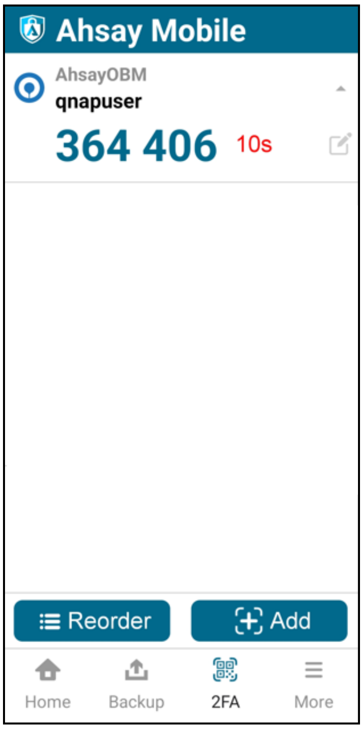

AhsayOBM
qnapuser
Enter a valid phone number, you will need this for account recovery.
+63 [redacted]
Verification success

Example of verification code:


Verification Code:
VOKF-727854

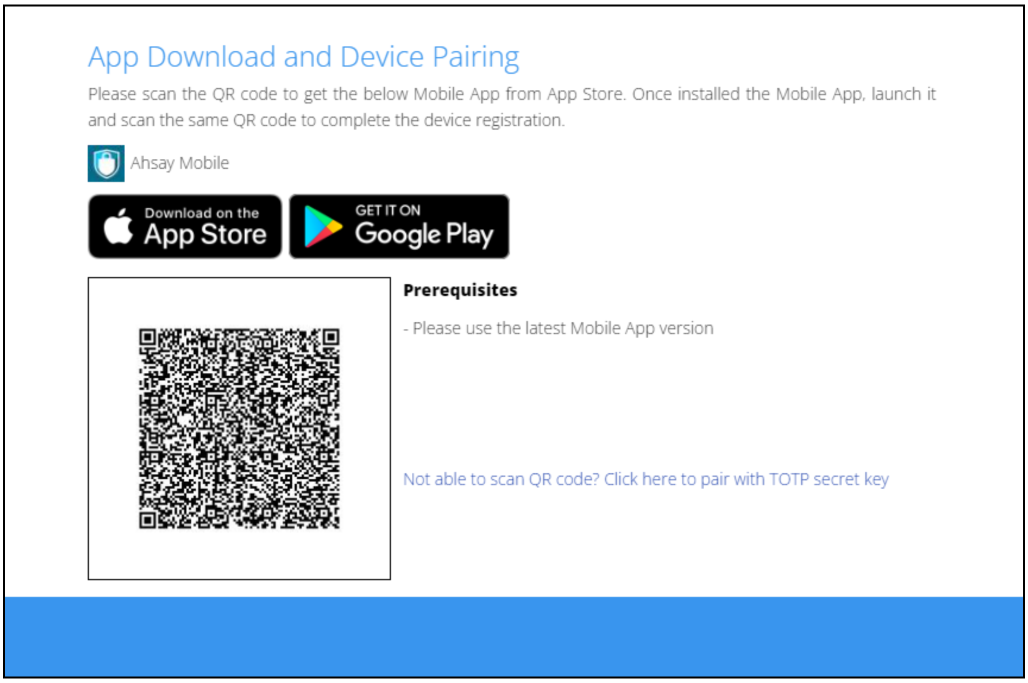
vii. Your phone number for account recovery is successfully verified.


Ahsay Mobile
AhsayOBM
qnapuser


Ahsay Mobile
AhsayOBM
qnapuser
364 406 10s

TOTP only

i. To configure a TOTP only 2FA with Ahsay Mobile, click the "**Not able to scan QR code? Click here to pair with TOTP secret key**" link.



App Download and Device Pairing

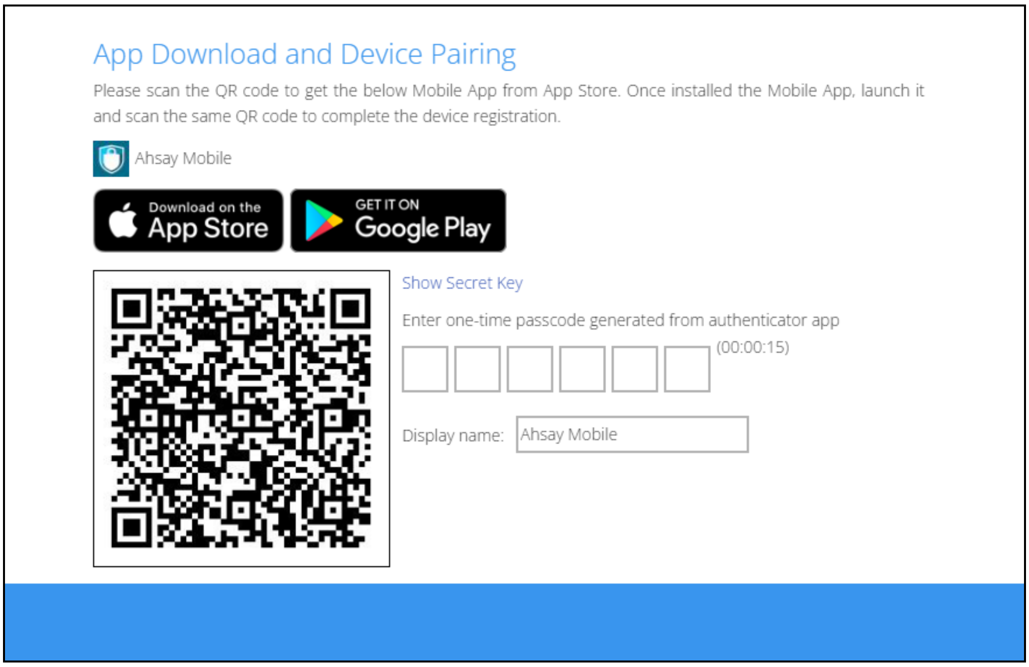
Please scan the QR code to get the below Mobile App from App Store. Once installed the Mobile App, launch it and scan the same QR code to complete the device registration.

Prerequisites

- Please use the latest Mobile App version

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

ii. The QR code for the TOTP only authenticator will be displayed.



App Download and Device Pairing

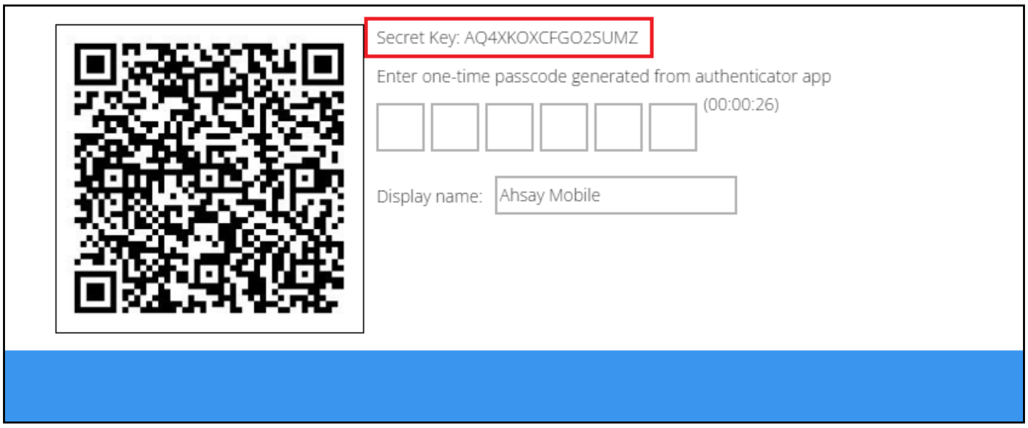
Please scan the QR code to get the below Mobile App from App Store. Once installed the Mobile App, launch it and scan the same QR code to complete the device registration.

Enter one-time passcode generated from authenticator app

(00:00:15)

Display name: Ahsay Mobile

To show the secret key, click the **Show Secret Key** link to display the 16-character alphanumeric secret key. The display name will be “Ahsay Mobile” by default.



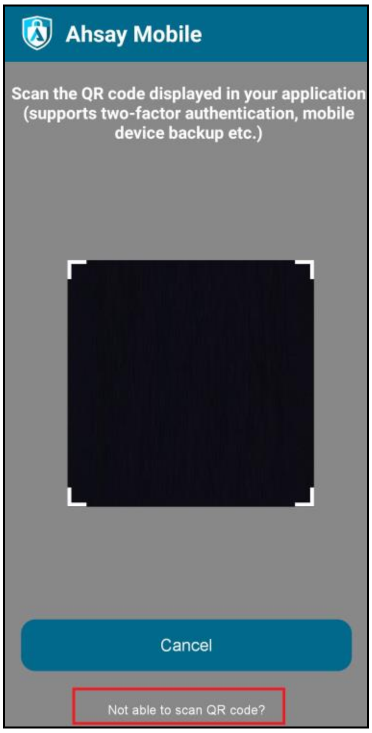
Secret Key: AQ4XKOXCFGO2SUMZ

Enter one-time passcode generated from authenticator app

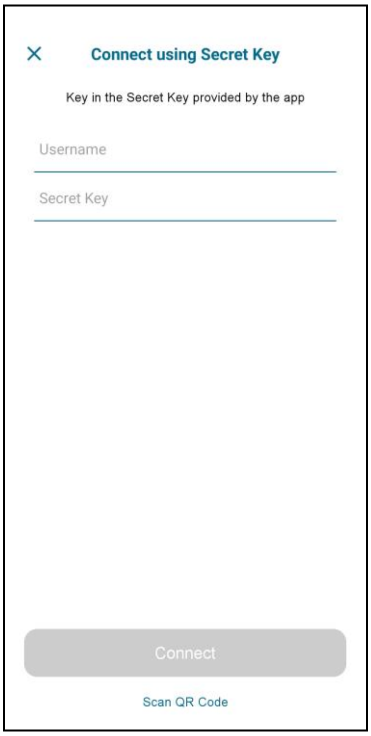
(00:00:26)

Display name: Ahsay Mobile

iii. In the Ahsay Mobile app, go to 2FA. Tap the **Not able to scan QR code?** link.

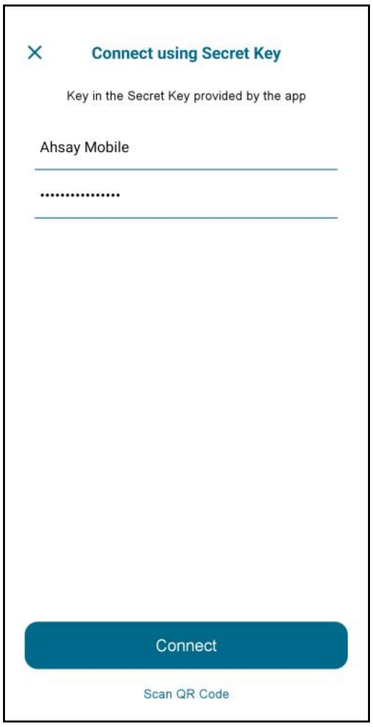


Scan the QR code displayed in your application (supports two-factor authentication, mobile device backup etc.)



Key in the Secret Key provided by the app

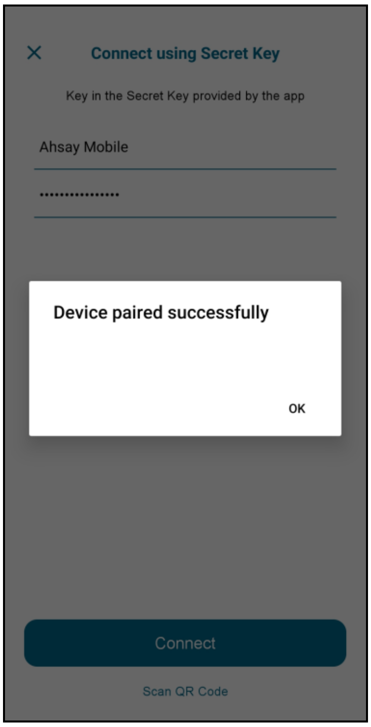
iv. Enter the Username and Secret Key shown in AhsayOBM then tap Connect. Once the device is paired successfully, tap **OK** to continue.


Connect using Secret Key

Key in the Secret Key provided by the app

Ahsay Mobile

••••••••••••••••••


Connect using Secret Key

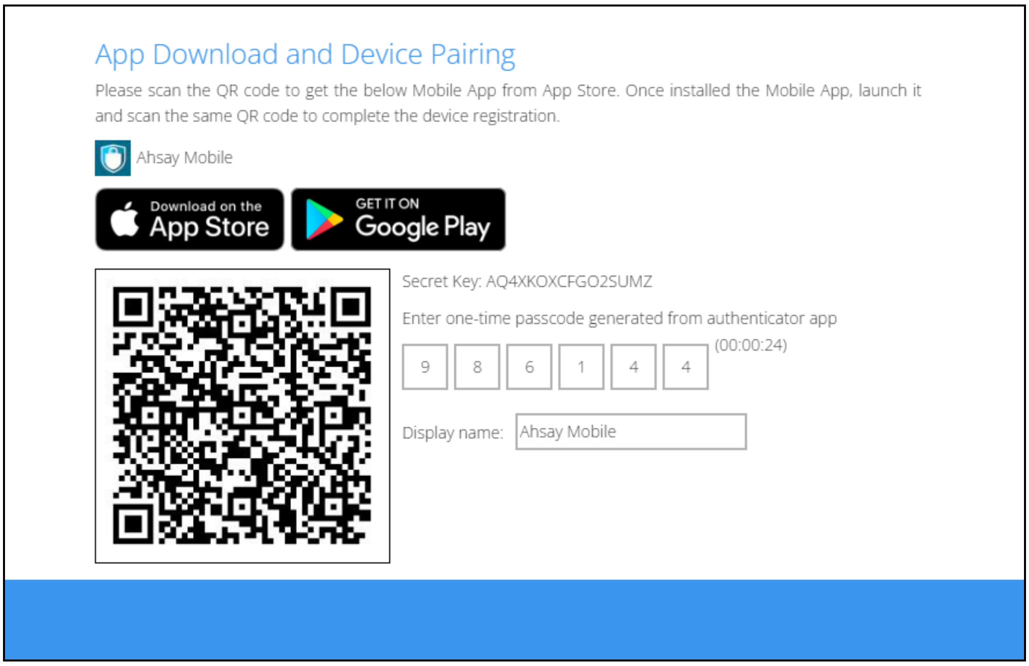
Key in the Secret Key provided by the app

Ahsay Mobile

••••••••••••••••••

Device paired successfully

v. Enter the one-time passcode from the Ahsay Mobile app.


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

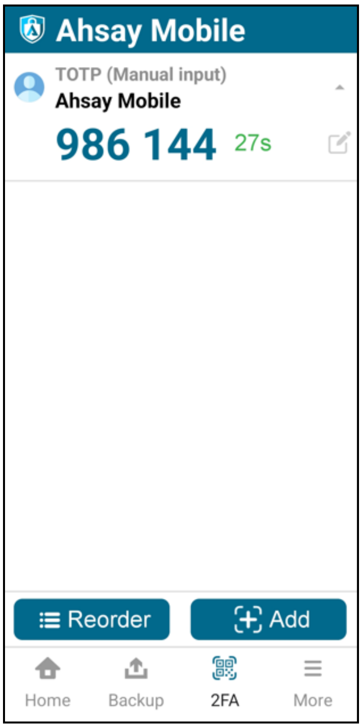
Secret Key: AQ4XKOXCFGO2SUMZ

Enter one-time passcode generated from authenticator app

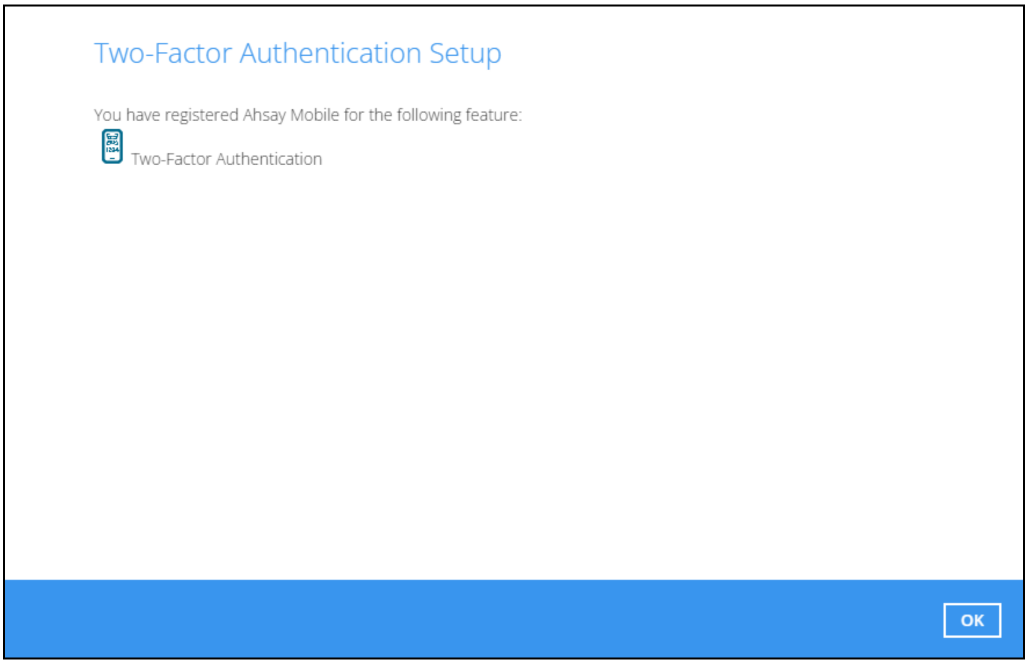
9 8 6 1 4 4 (00:00:24)

Display name: Ahsay Mobile

Example of the one-time passcode generated by Ahsay Mobile:



vi. Once the registration is successful, the following screen will be displayed. You have now registered Ahsay Mobile for TOTP only 2FA.



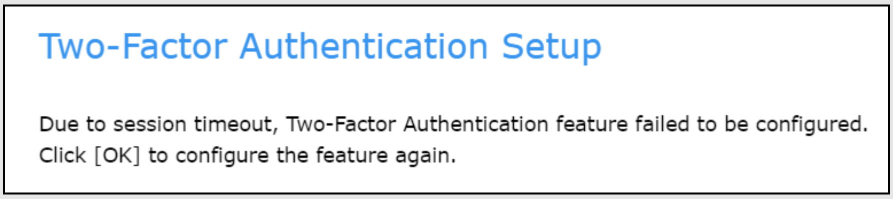
Two-Factor Authentication Setup

You have registered Ahsay Mobile for the following feature:

Two-Factor Authentication

NOTE

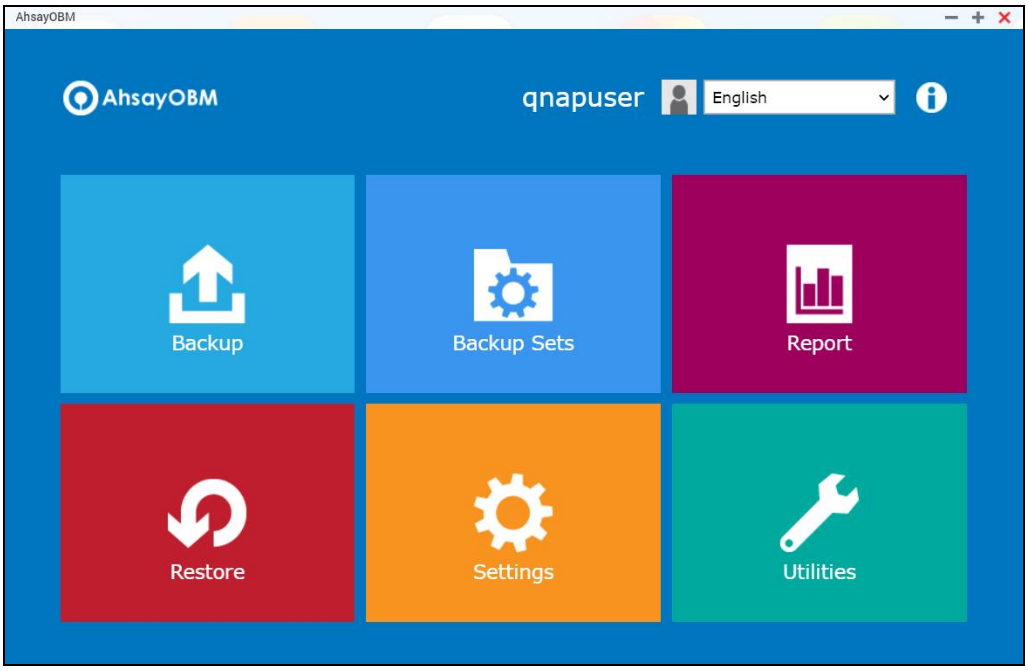
In case device pairing takes a while, session timeout message will be displayed. Just click **OK** to resume with the device pairing.



Two-Factor Authentication Setup

Due to session timeout, Two-Factor Authentication feature failed to be configured. Click [OK] to configure the feature again.

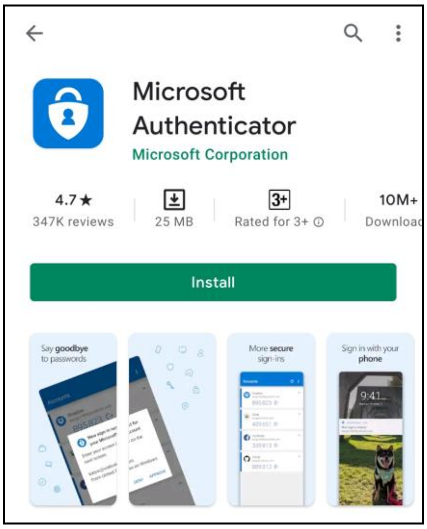
9. After successful pairing, the following screen will be displayed.



5.2 Using Microsoft Authenticator

To register a device for TOTP 2FA in AhsayOBM using Microsoft Authenticator, please follow the steps below:

1. Download and install Microsoft Authenticator from the Play Store for Android devices or the App Store for iOS devices.



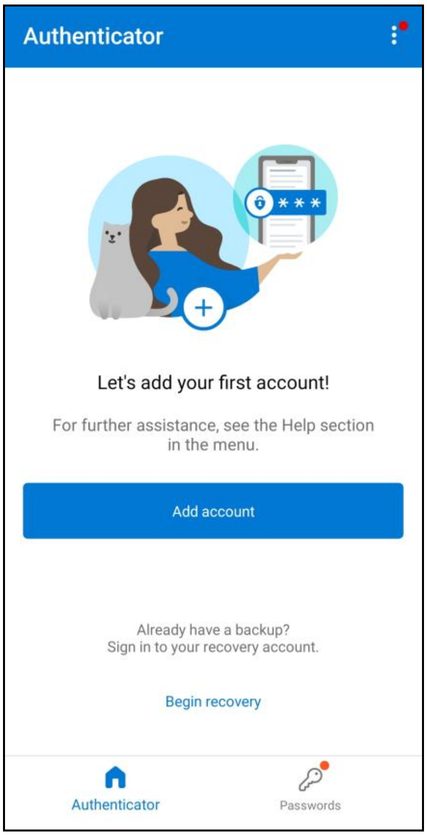
Microsoft Authenticator

Microsoft Corporation

4.7★ 347K reviews | 25 MB | Rated for 3+ | 10M+ Download

2. Launch the Microsoft Authenticator app.

3. Tap **Add account**.



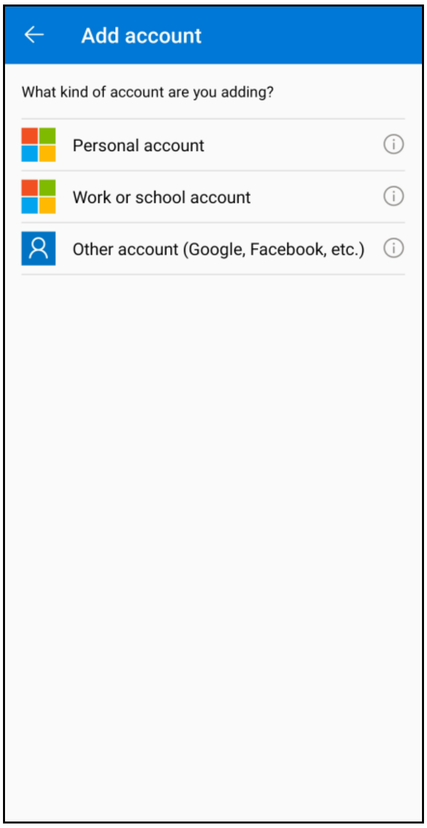
Authenticator

Let's add your first account!

For further assistance, see the Help section in the menu.

Already have a backup?
Sign in to your recovery account.

4. Select **Other account (Google, Facebook, etc.)**.

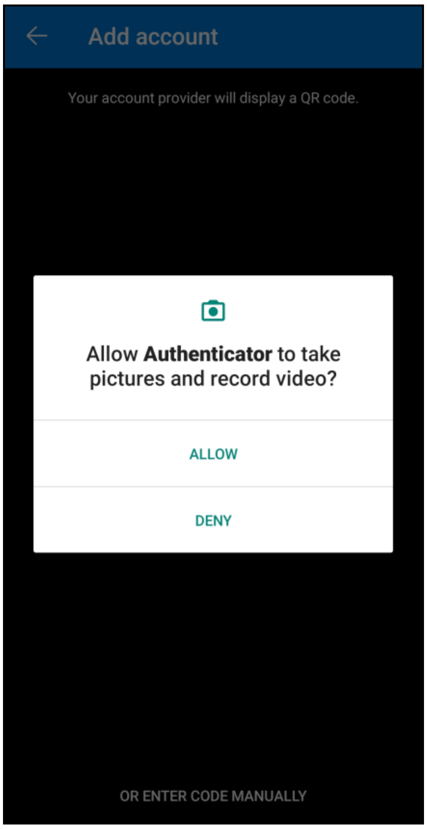


Add account

What kind of account are you adding?

- Personal account
- Work or school account
- Other account (Google, Facebook, etc.)

5. Allow permission to take pictures and record video.



Add account

Your account provider will display a QR code.

Allow **Authenticator** to take pictures and record video?

ALLOW

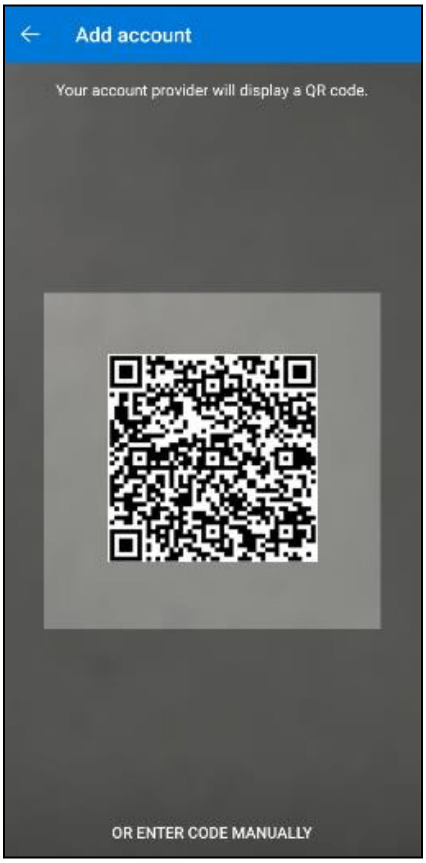
DENY

OR ENTER CODE MANUALLY

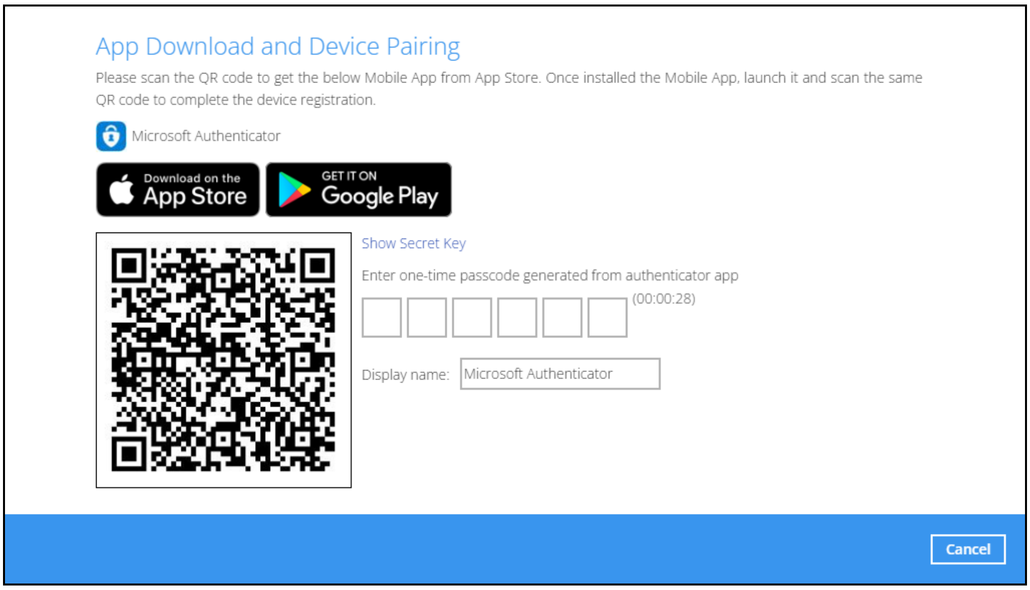
6. Set up the account by selecting from the following methods: Scan the QR code or Enter code manually.

   Method 1: Scan the QR code

   i. Scan the QR code on AhsayOBM.



Example of the displayed 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.

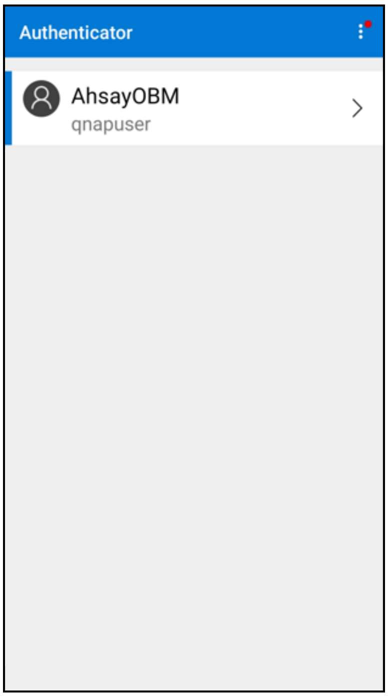
Microsoft Authenticator

Enter one-time passcode generated from authenticator app

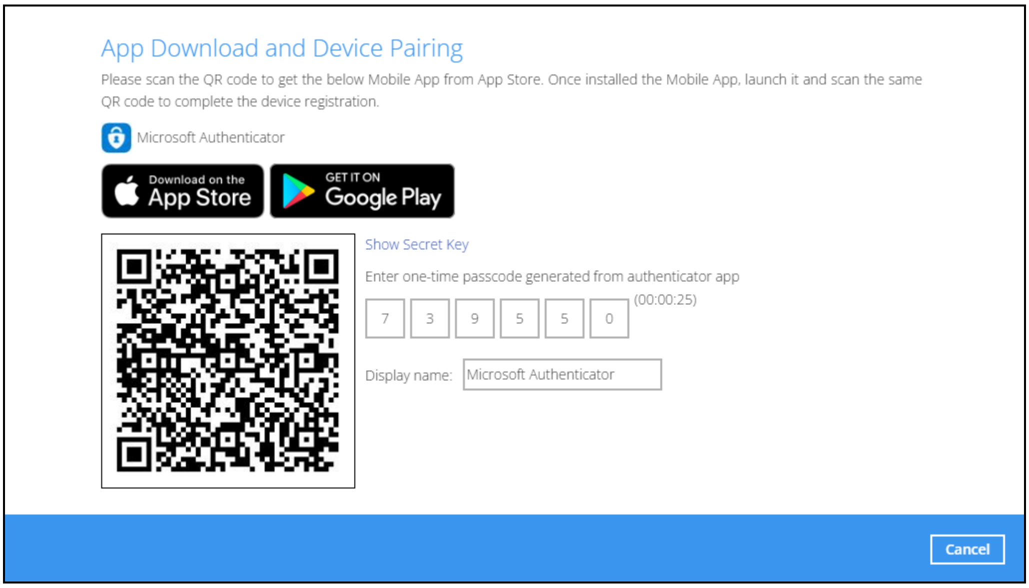
□□□□□□ (00:00:28)

Display name: Microsoft Authenticator

ii. The AhsayOBM account is successfully added to Microsoft Authenticator and the mobile device is registered in AhsayOBM.



iii. Once the account is added to Microsoft Authenticator, enter the one-time passcode generated from the authenticator app in AhsayOBM.



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.

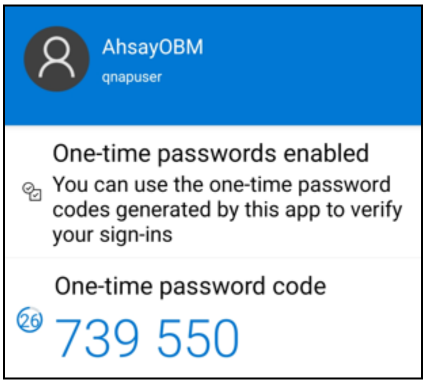
Microsoft Authenticator

Enter one-time passcode generated from authenticator app

7 3 9 5 5 0 (00:00:25)

Display name: Microsoft Authenticator

Example of the one-time passcode generated:



AhsayOBM
qnapuser

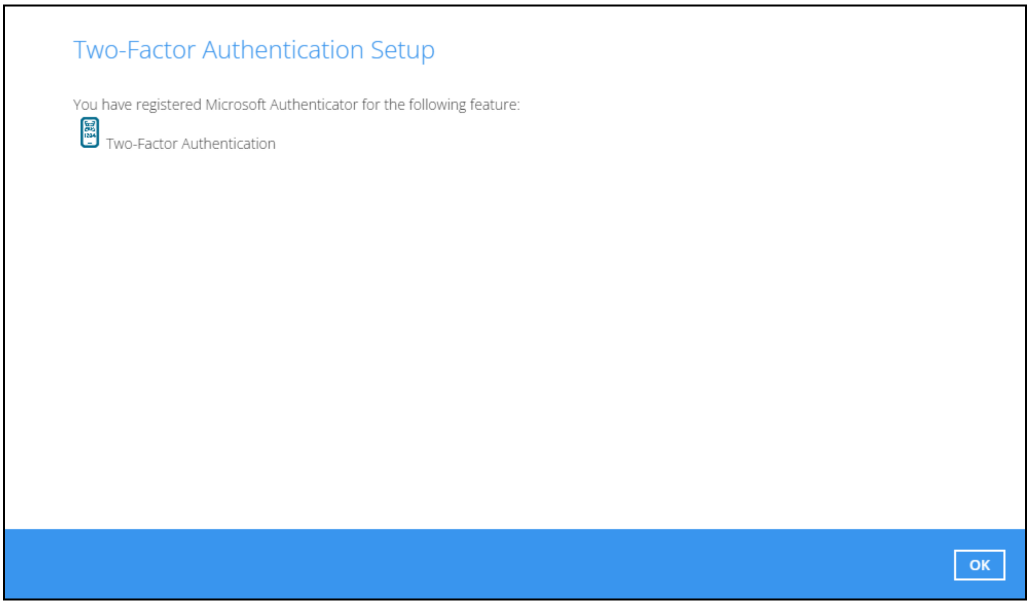
One-time passwords enabled

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

One-time password code

26 739 550

iv. The device is successfully registered for TOTP 2FA in AhsayOBM using Microsoft Authenticator. Click **OK** to continue.



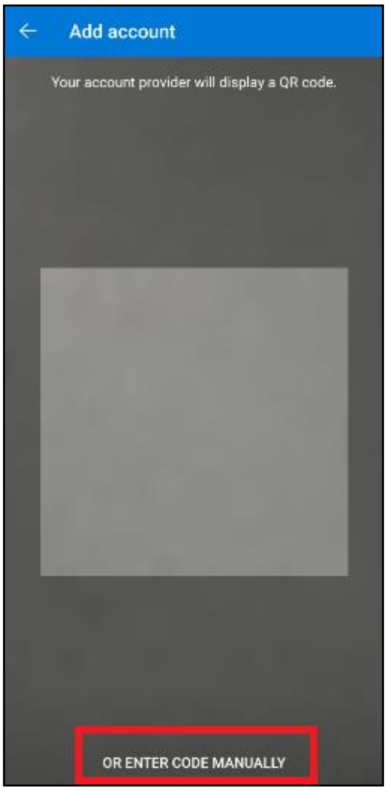
Two-Factor Authentication Setup

You have registered Microsoft Authenticator for the following feature:

Two-Factor Authentication

Method 2: Enter Code Manually

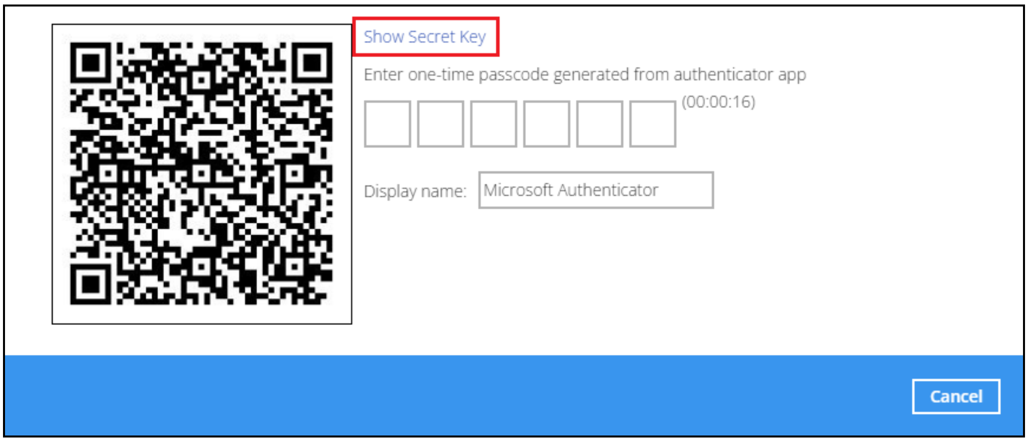
i. Tap **OR ENTER CODE MANUALLY**.

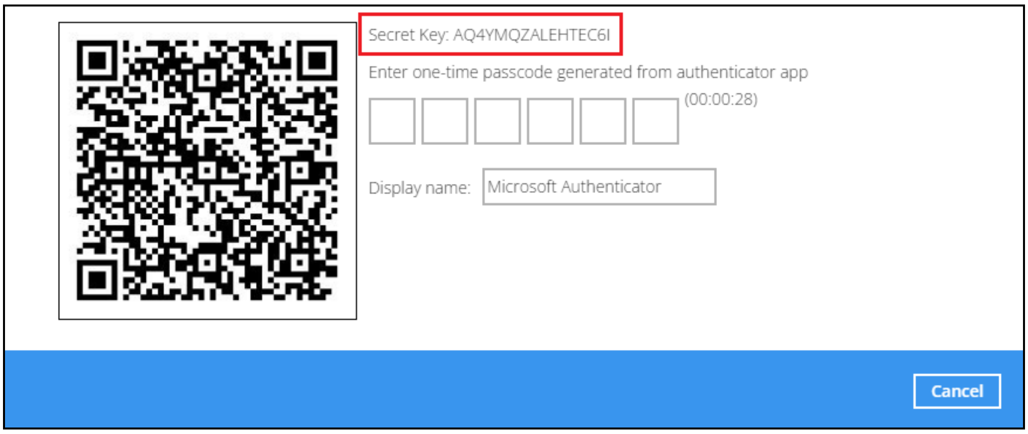


Add account

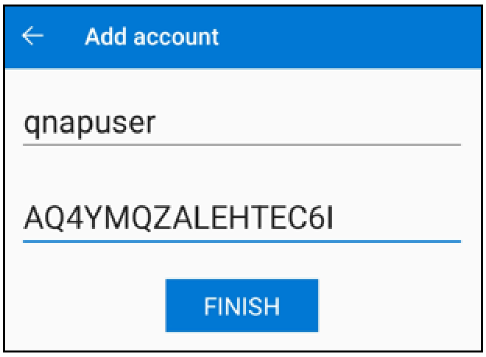
Your account provider will display a QR code.

ii. Click the **Show Secret Key** link in AhsayOBM to display the Secret Key which must be entered manually in Microsoft Authenticator.




Secret Key: AQ4YMQZALEHTEC6I

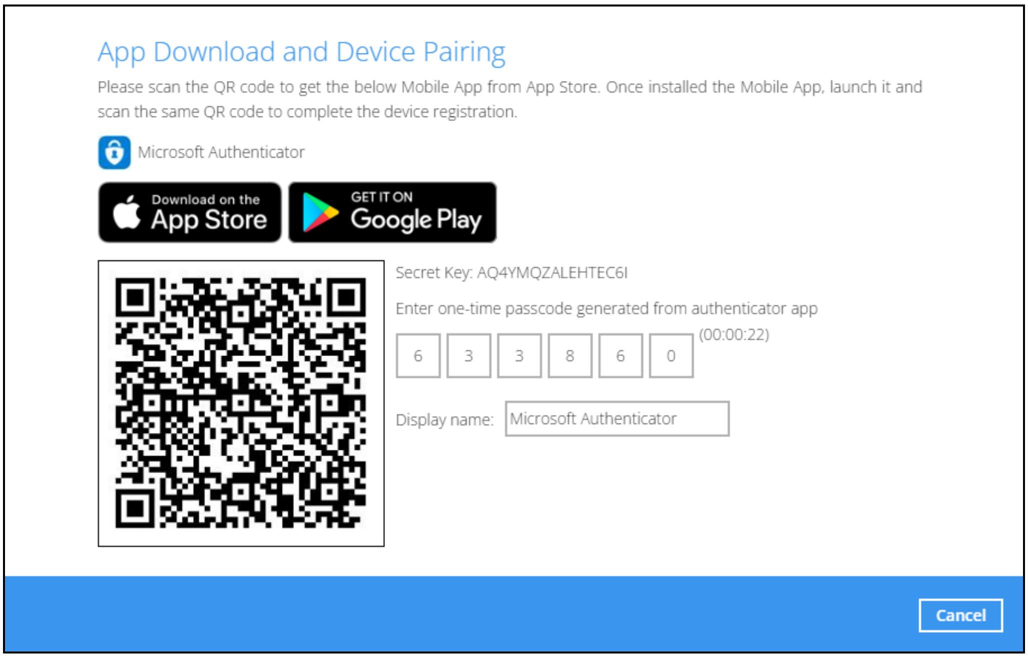
iii. On the Microsoft Authenticator app, input an account name, then enter the displayed Secret Key in AhsayOBM. Tap **FINISH** to proceed.



qnapuser

AQ4YMQZALEHTEC6I

iv. Once the account is added to Microsoft Authenticator, enter the one-time passcode generated in the authenticator app in AhsayOBM.



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.

Microsoft Authenticator

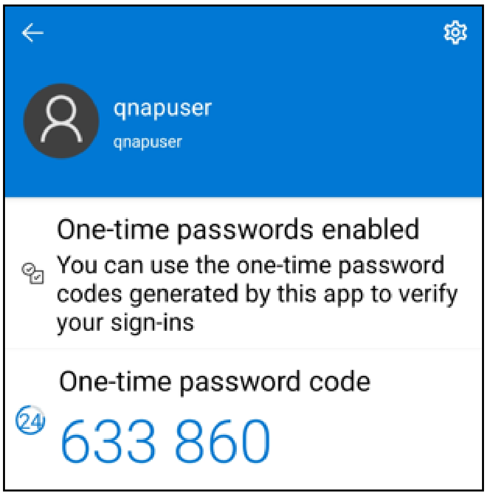
Secret Key: AQ4YMQZALEHTEC6I

Enter one-time passcode generated from authenticator app

6 3 3 8 6 0 (00:00:22)

Display name: Microsoft Authenticator

Example of the one-time passcode generated:



qnapuser

qnapuser

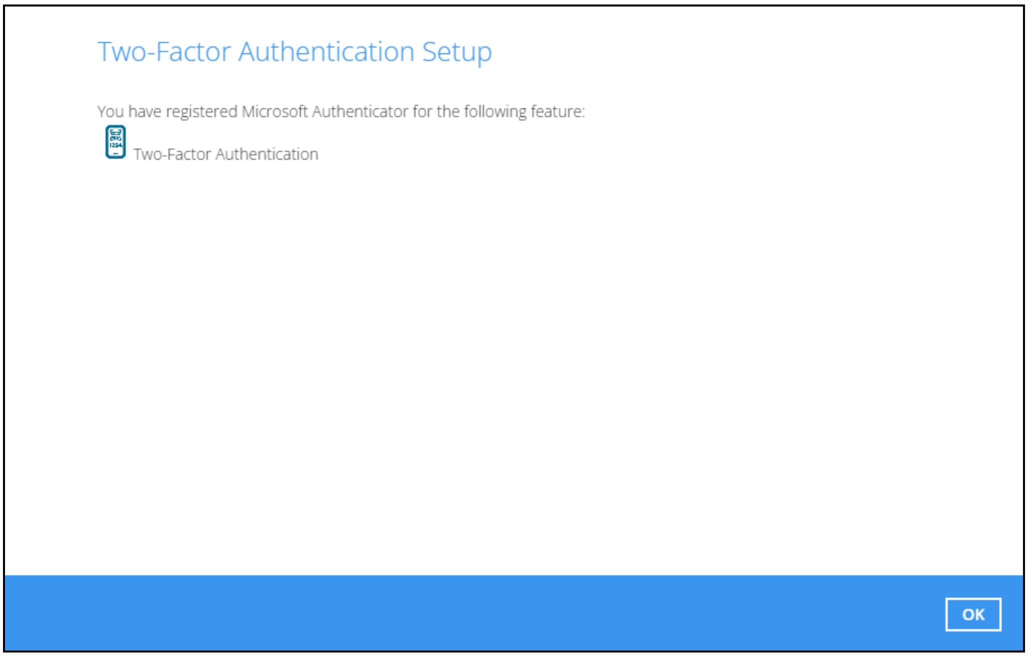
One-time passwords enabled

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

One-time password code

633 860

v. The device is successfully registered for TOTP 2FA in AhsayOBM using Microsoft Authenticator. Click **OK** to continue.

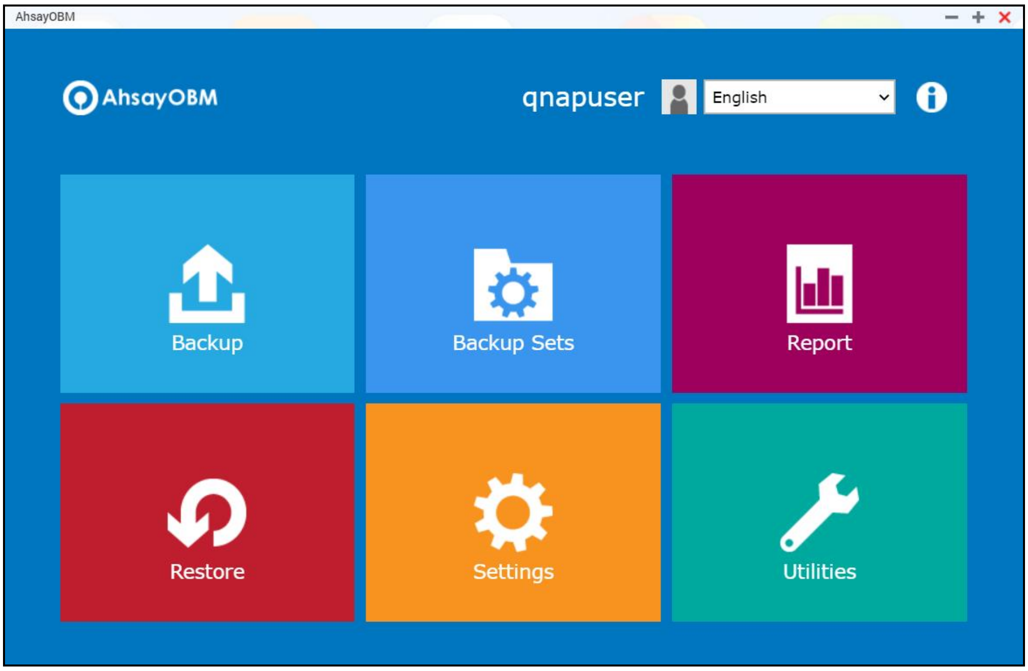


Two-Factor Authentication Setup

You have registered Microsoft Authenticator for the following feature:

Two-Factor Authentication

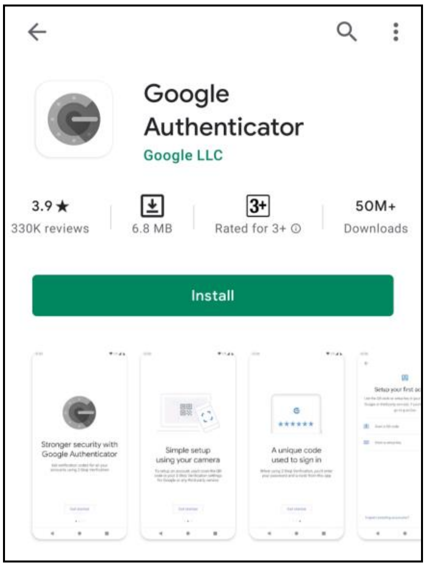
7. After successful pairing, the following screen will be displayed.



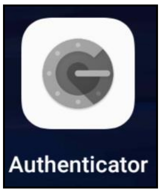
5.3 Using Google Authenticator

To register a device for TOTP 2FA in AhsayOBM using Google Authenticator, please follow the steps below:

1. Download and install Google Authenticator from the Play Store for Android devices or the App Store for iOS devices.



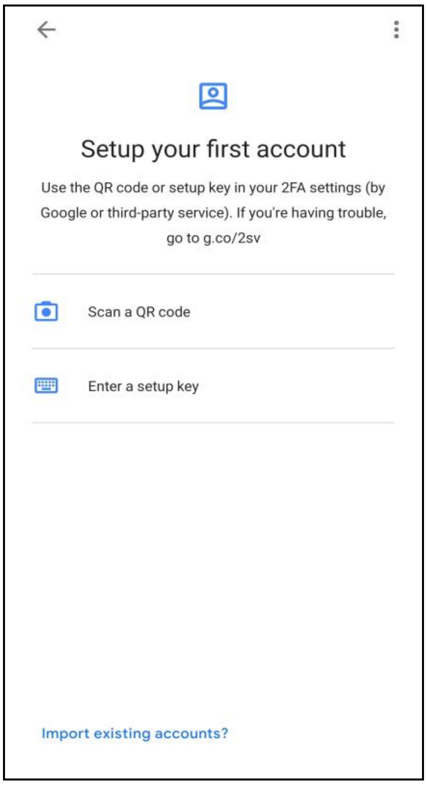
2. Launch the Google Authenticator app.



3. Set up the account by selecting from the following methods: Scan the QR code or Enter a setup key manually.

Method 1: Scan the QR code

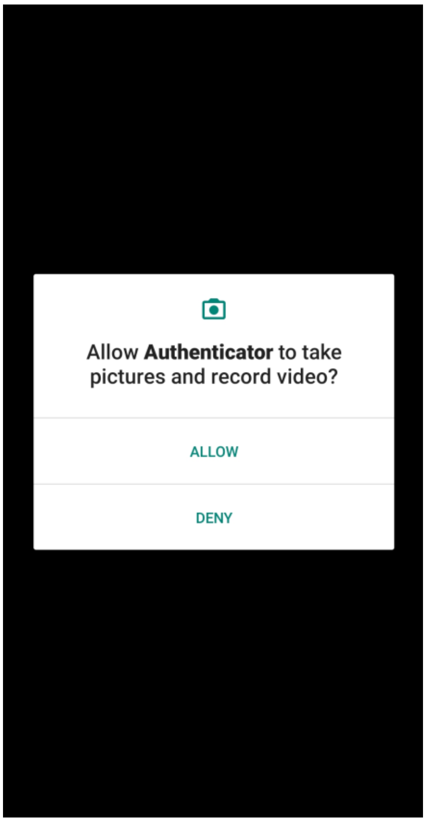
i. Tap **Scan a QR code**.



Setup your first account

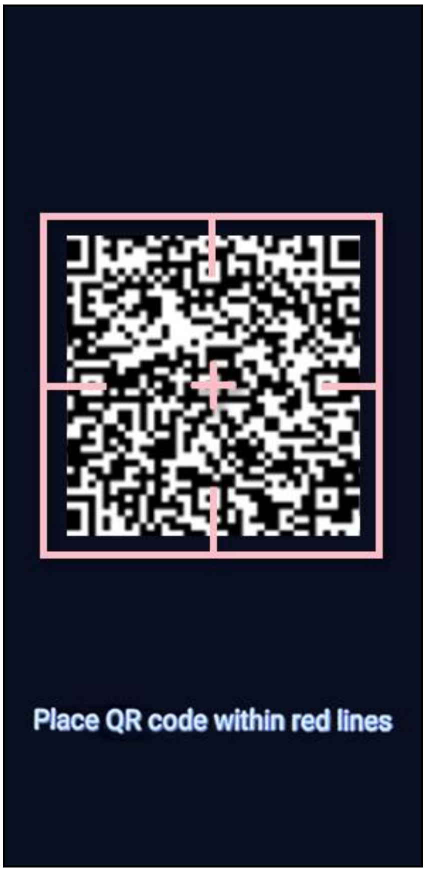
Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

ii. Allow permission to take pictures and record video.

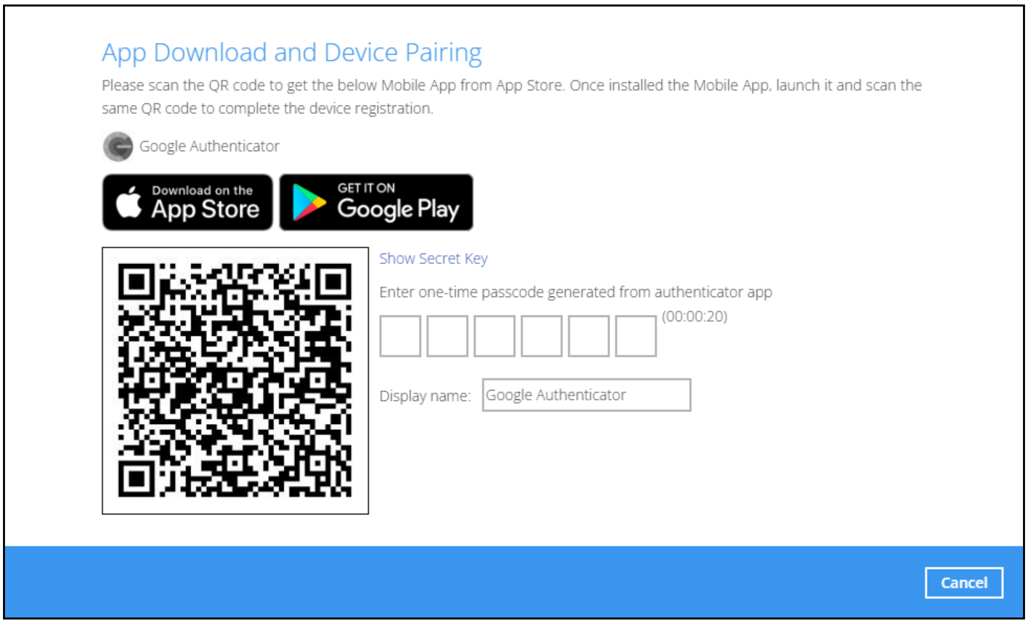


Allow **Authenticator** to take pictures and record video?

iii. Scan the QR code on AhsayOBM.



Example of the displayed 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.

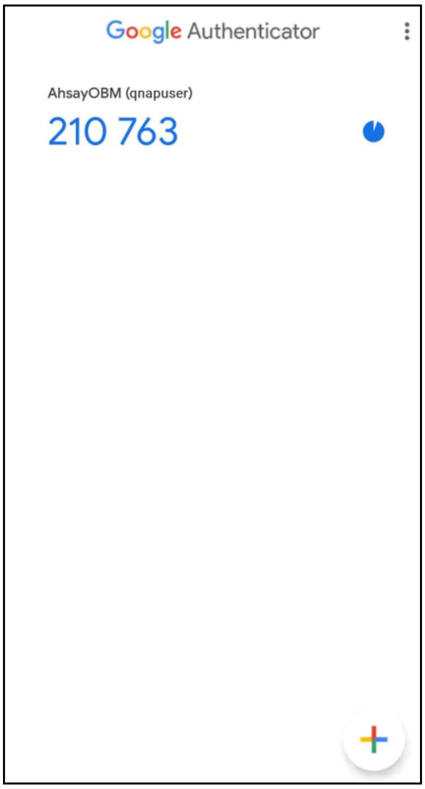
Google Authenticator

Enter one-time passcode generated from authenticator app

□□□□□□ (00:00:20)

Display name: Google Authenticator

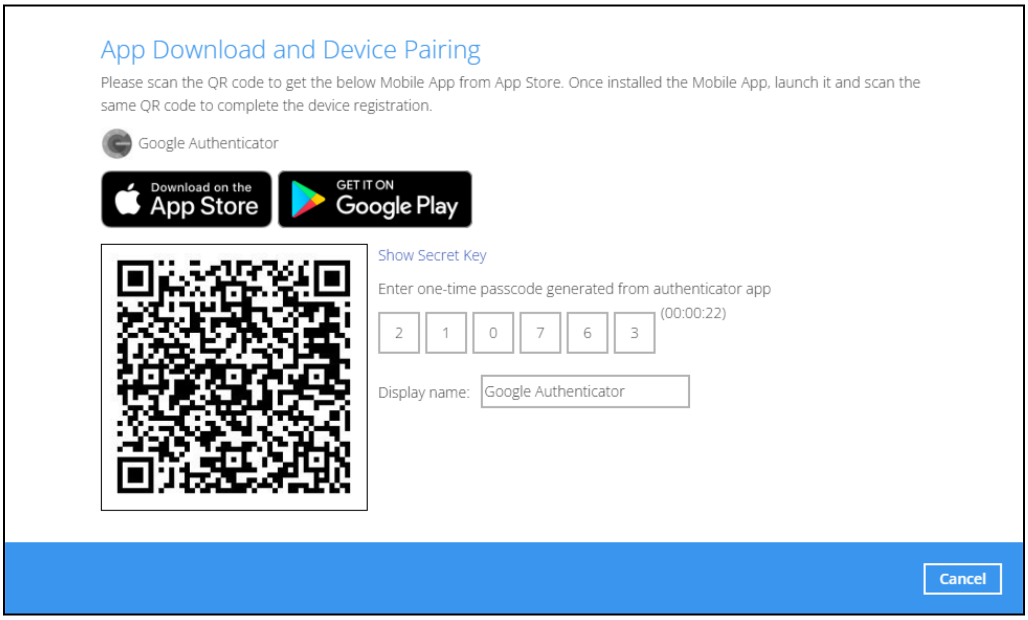
iv. The AhsayOBM account is successfully added to Google Authenticator and the mobile device is registered in AhsayOBM.



AhsayOBM (qnapuser)

210 763

v. Once the account is added to Google Authenticator, enter the one-time passcode generated from the authenticator app to AhsayOBM.



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.

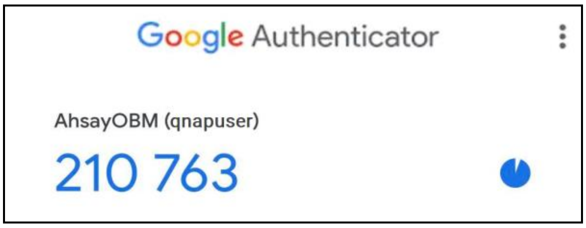
Google Authenticator

Enter one-time passcode generated from authenticator app

2 1 0 7 6 3 (00:00:22)

Display name: Google Authenticator

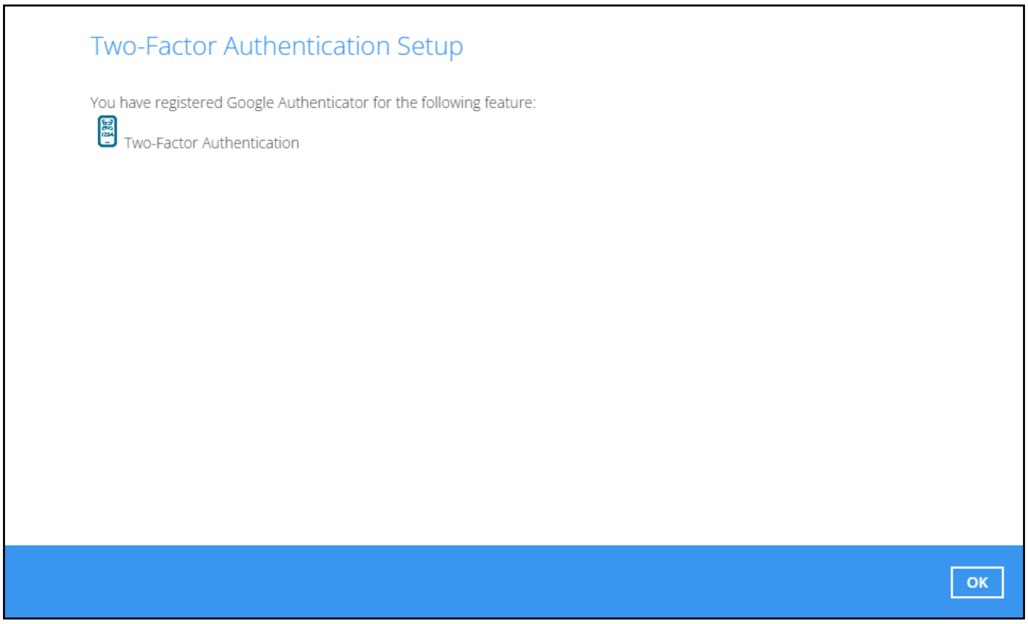
Example of the one-time passcode generated:



AhsayOBM (qnapuser)

210 763

vi. The device is successfully registered for TOTP 2FA in AhsayOBM using Google Authenticator. Click **OK** to continue.



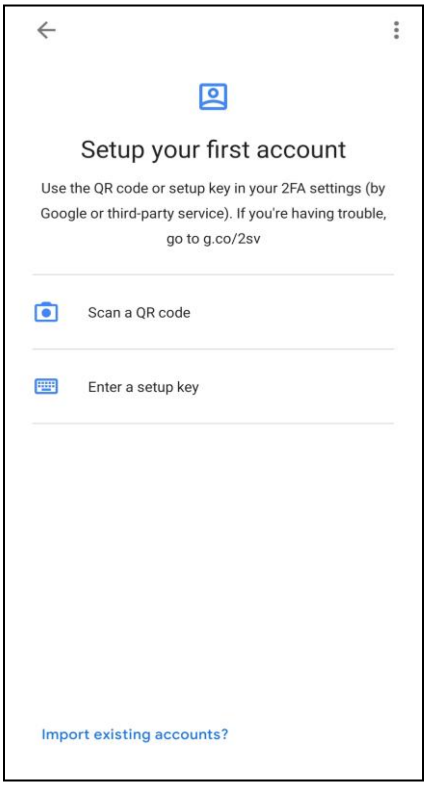
Two-Factor Authentication Setup

You have registered Google Authenticator for the following feature:

Two-Factor Authentication

Method 2: Enter a setup key manually

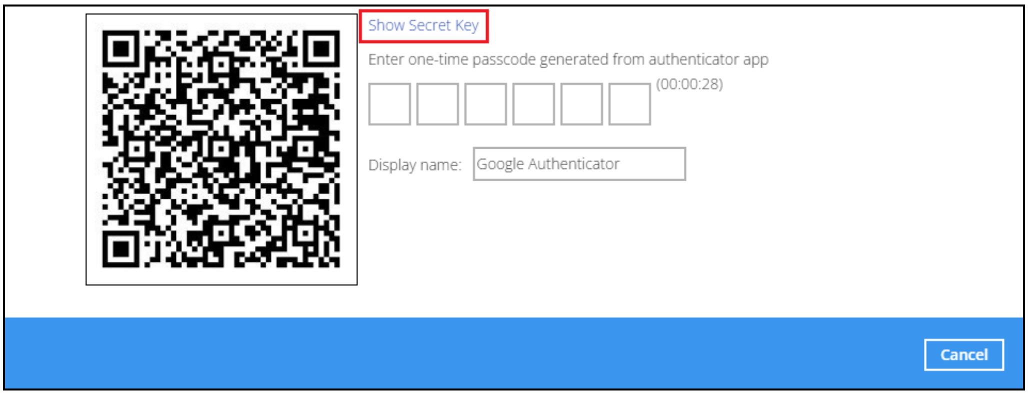
i. Tap **Enter a setup key**.



Setup your first account

Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

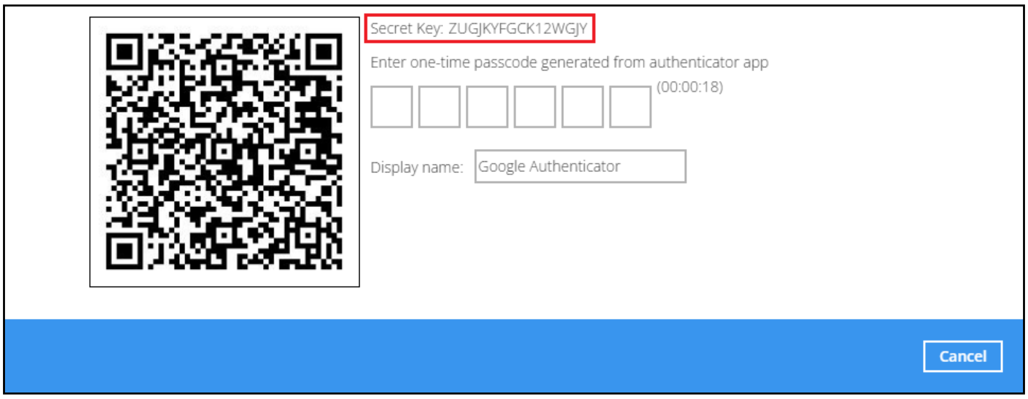
ii. Click the **Show Secret Key** link in AhsayOBM to display the Secret Key which must be entered manually in Google Authenticator.



Enter one-time passcode generated from authenticator app

(00:00:28)

Display name: Google Authenticator



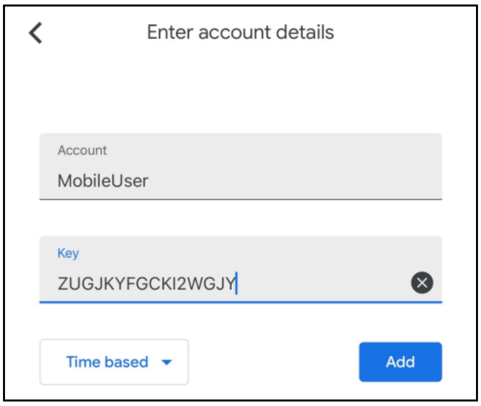
Secret Key: ZUGJKYFGCK12WGJY

Enter one-time passcode generated from authenticator app

(00:00:18)

Display name: Google Authenticator

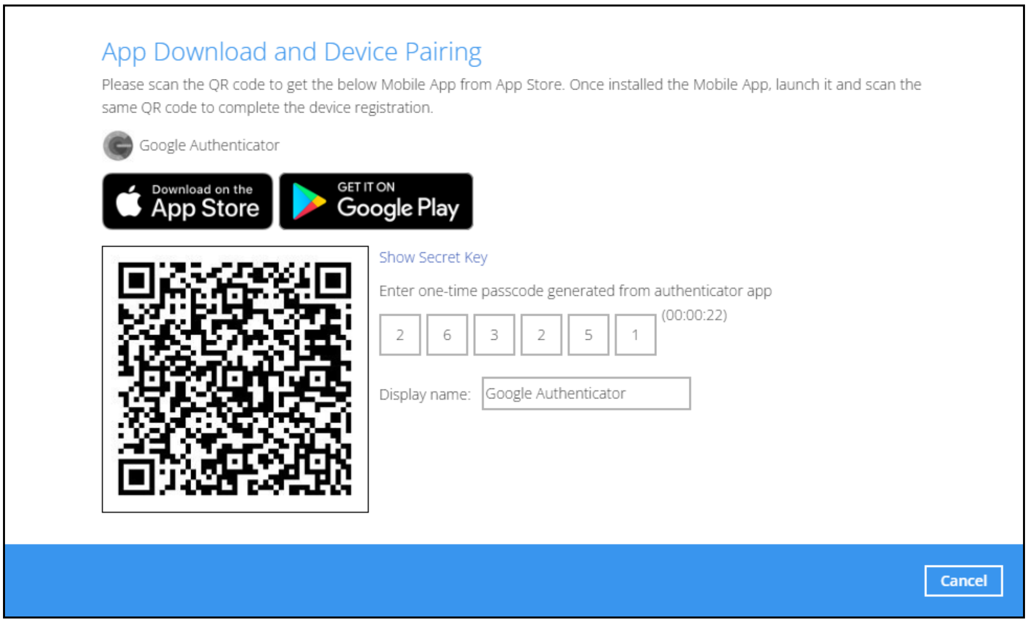
iii. On the Google Authenticator app, input an account name, then enter the displayed Secret Key in AhsayOBM. Tap **Add** to proceed.



Account: MobileUser

Key: ZUGJKYFGCKI2WGJY

iv. Once the account is added to Google Authenticator, enter the one-time passcode generated from the authenticator app to AhsayOBM.



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.

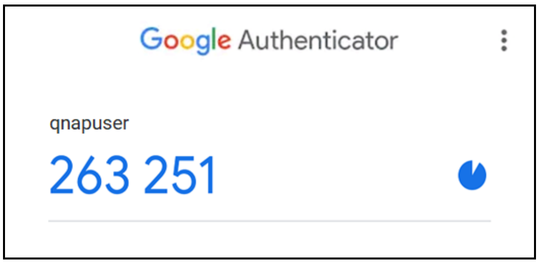
Google Authenticator

Enter one-time passcode generated from authenticator app

2 6 3 2 5 1 (00:00:22)

Display name: Google Authenticator

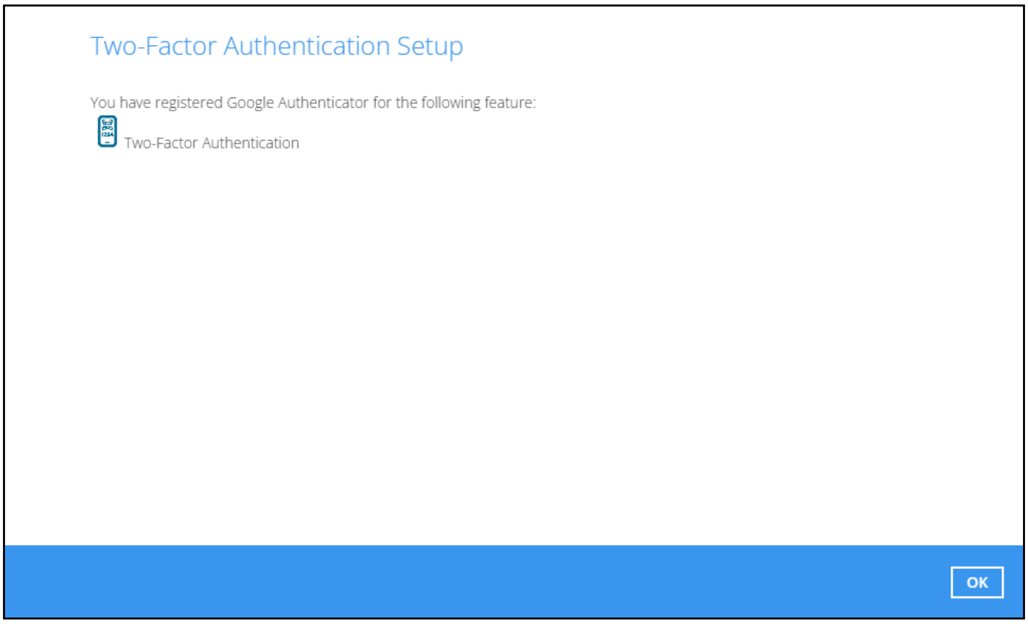
Example of the one-time passcode generated:



qnapuser

263 251

v. The device is successfully registered for TOTP 2FA in AhsayOBM using Google Authenticator. Click **OK** to continue.

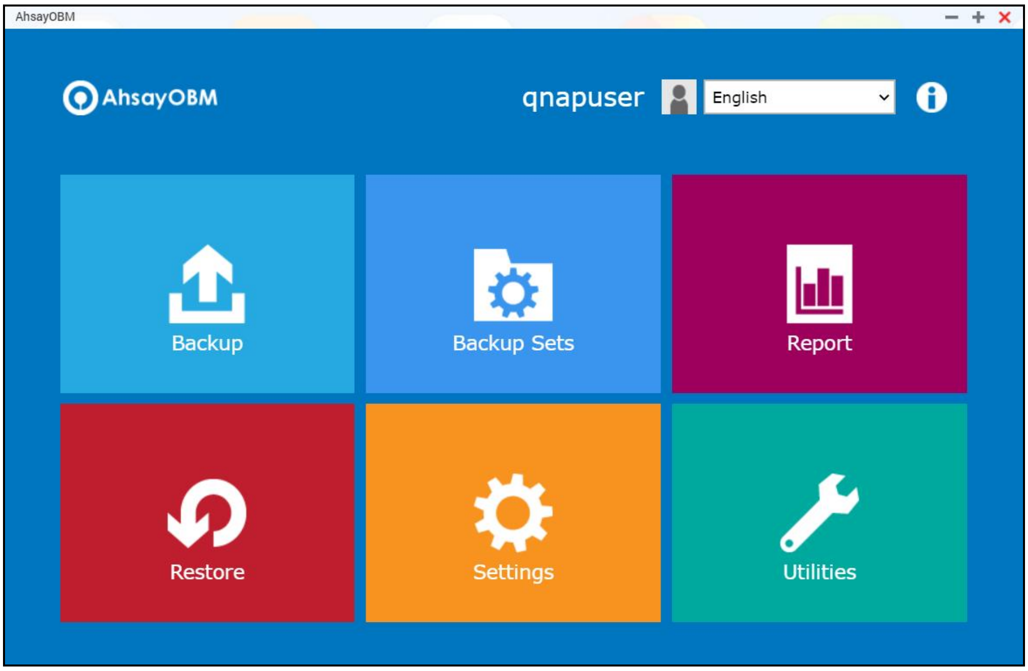


Two-Factor Authentication Setup

You have registered Google Authenticator for the following feature:

Two-Factor Authentication

4. After successful pairing, the following screen will be displayed.



6 Logging in to AhsayOBM

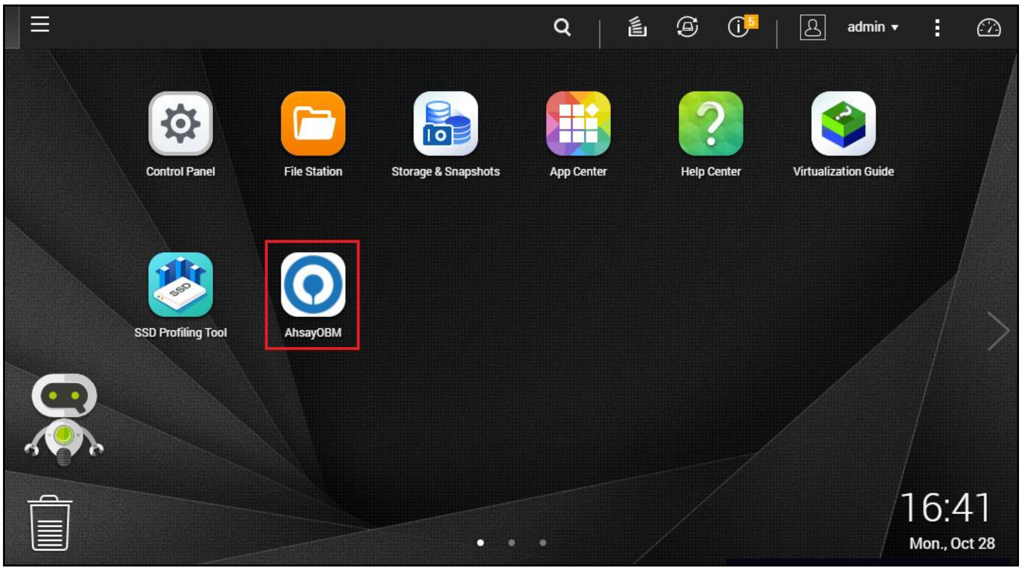
Login steps without 2FA and with 2FA using the different types of authenticators will be discussed in this chapter.

- Login to AhsayOBM without 2FA
- Login to AhsayOBM with 2FA using Ahsay Mobile
- Login to AhsayOBM with 2FA using third-party TOTP authenticator
- Login to AhsayOBM with 2FA using Twilio

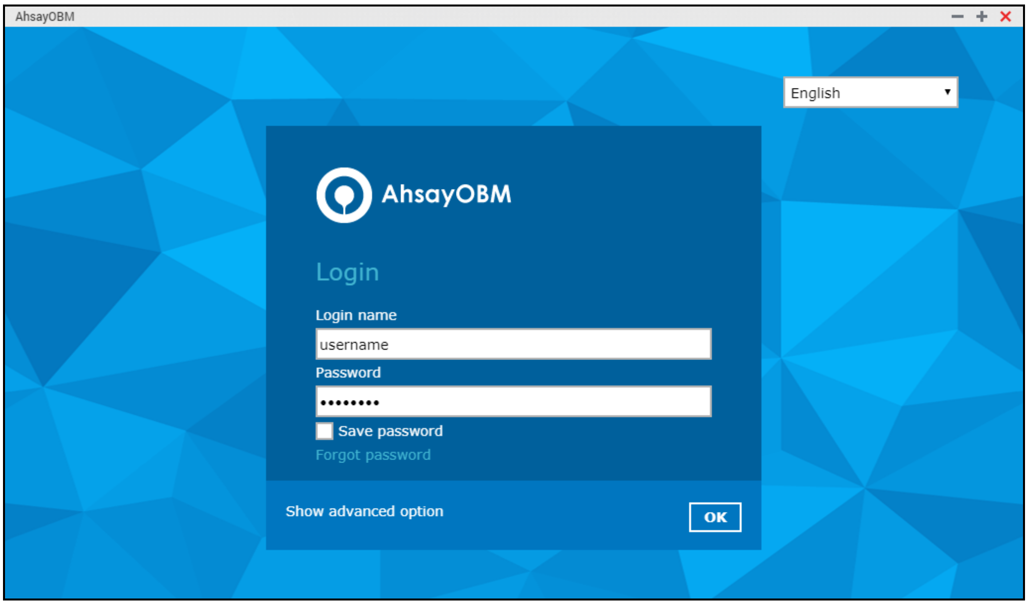
6.1 Login to AhsayOBM without 2FA

When logging in to AhsayOBM without Two-Factor Authentication, follow the steps below:

1. Click the AhsayOBM icon on the desktop to launch the application.



2. Enter the Login name and Password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



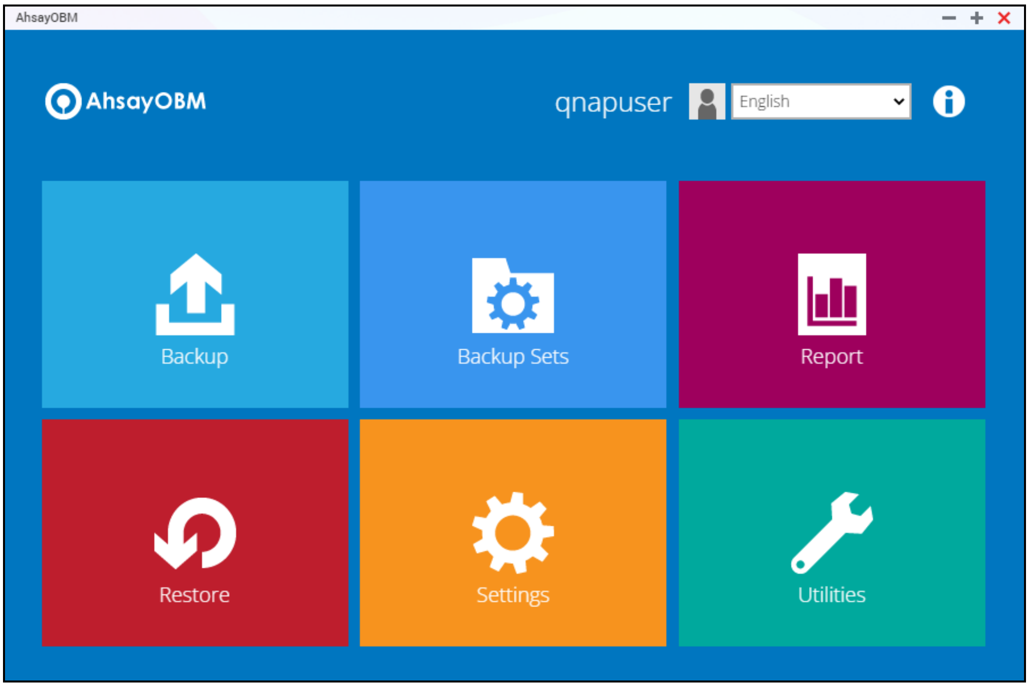
Login name: username

Password: ••••••••

NOTE

The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

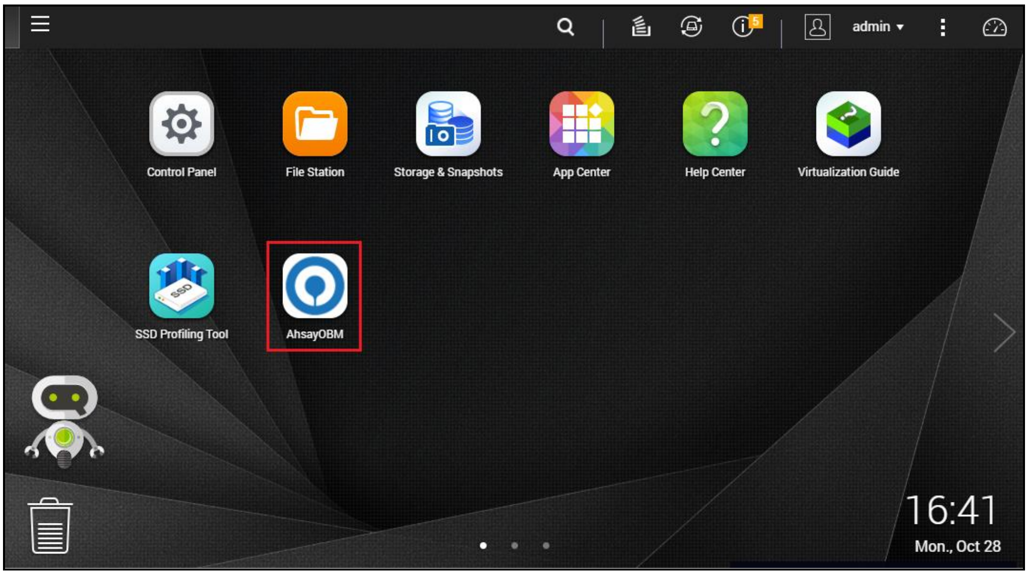
3. After successful login, the following screen will be displayed.



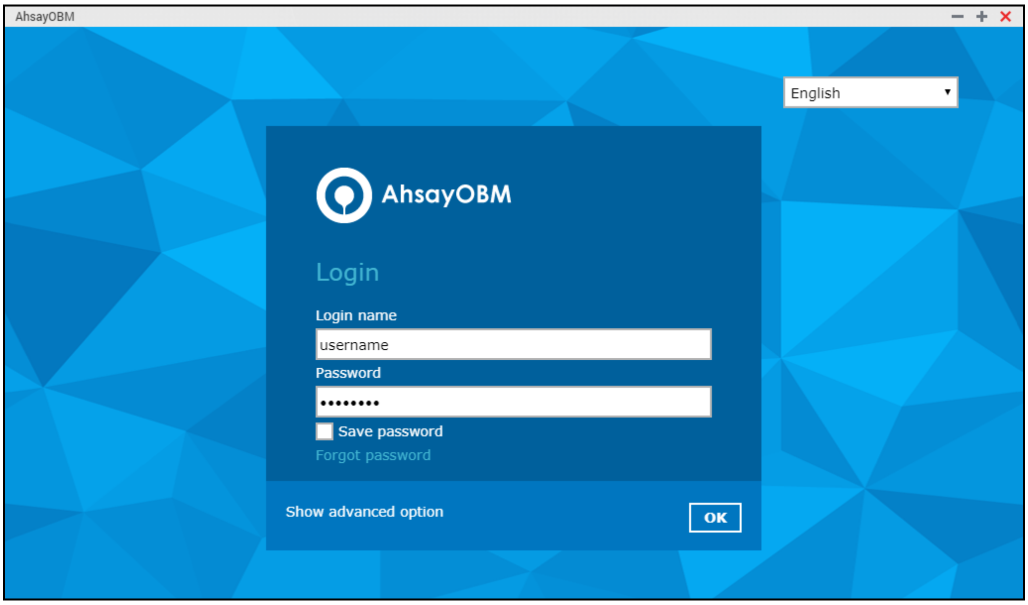
6.2 Login to AhsayOBM with 2FA using Ahsay Mobile

When logging in to AhsayOBM with Two-Factor Authentication using Ahsay Mobile, please follow the steps below:

1. Click the AhsayOBM icon on the desktop to launch the application.



2. Enter the Login name and Password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



NOTE

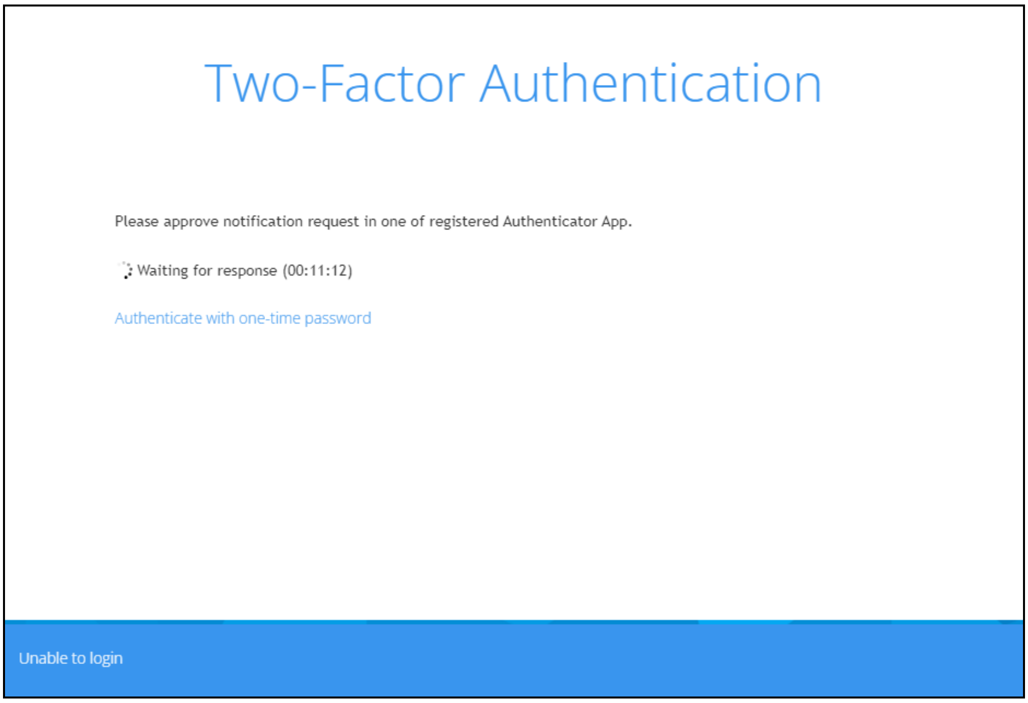
The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

Please refer to Appendix A: Troubleshooting Login in the Ahsay Mobile User Guide for Android and iOS if you are experiencing problems logging to AhsayOBM with Two-Factor Authentication using Ahsay Mobile.

3. Select the authentication method to continue with the login.

- **Push Notification and TOTP (default mode)**

  Example of the 2FA alert screen on AhsayOBM after login with correct username and password:



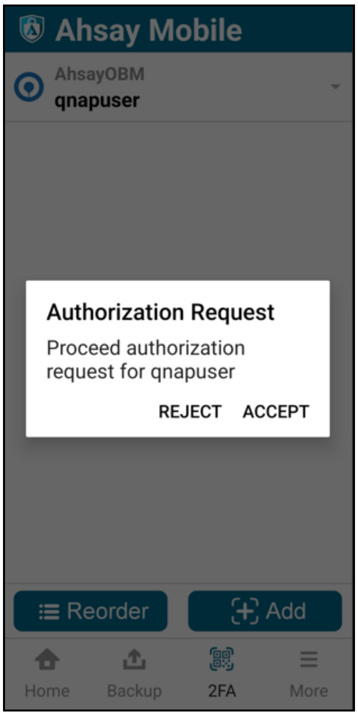
Two-Factor Authentication

Please approve notification request in one of registered Authenticator App.

Waiting for response (00:11:12)

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

Example of the login request sent to Ahsay Mobile:

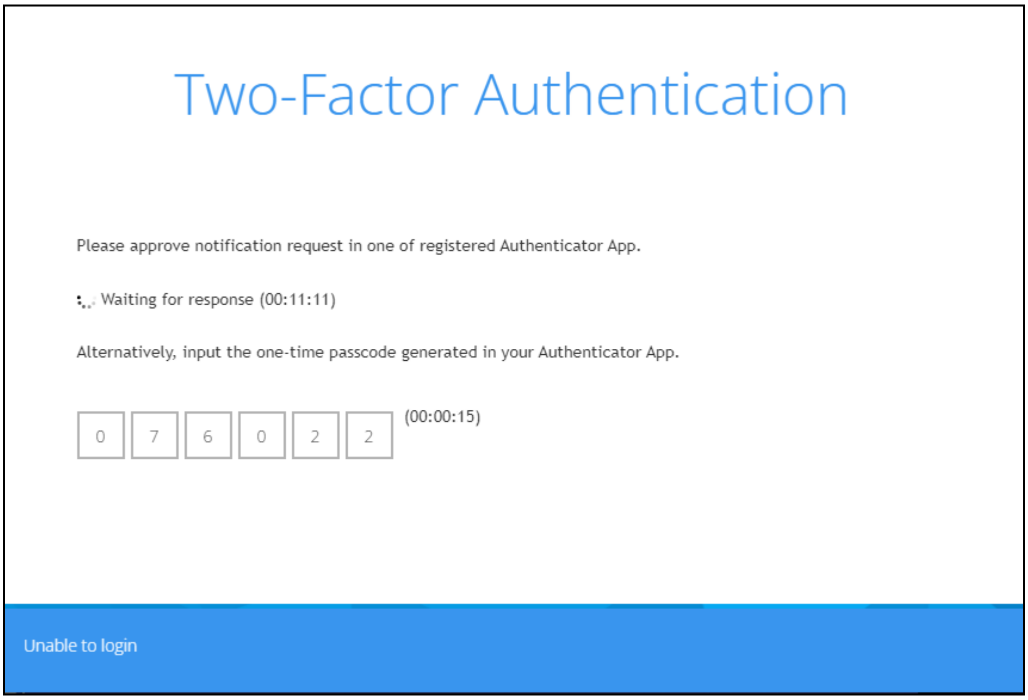


Authorization Request

Proceed authorization request for qnapuser

REJECT ACCEPT

However, if push notification is not working or you prefer to use one-time password instead, click the “**Authenticate with one-time password**” link, then input the one-time password generated from Ahsay Mobile to complete the login.



Two-Factor Authentication

Please approve notification request in one of registered Authenticator App.

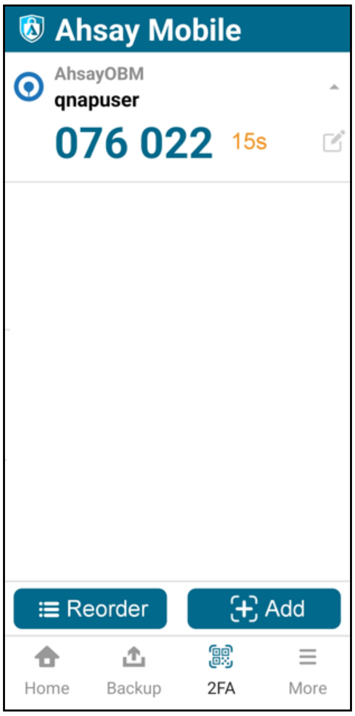
Waiting for response (00:11:11)

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

0 7 6 0 2 2 (00:00:15)

Unable to login

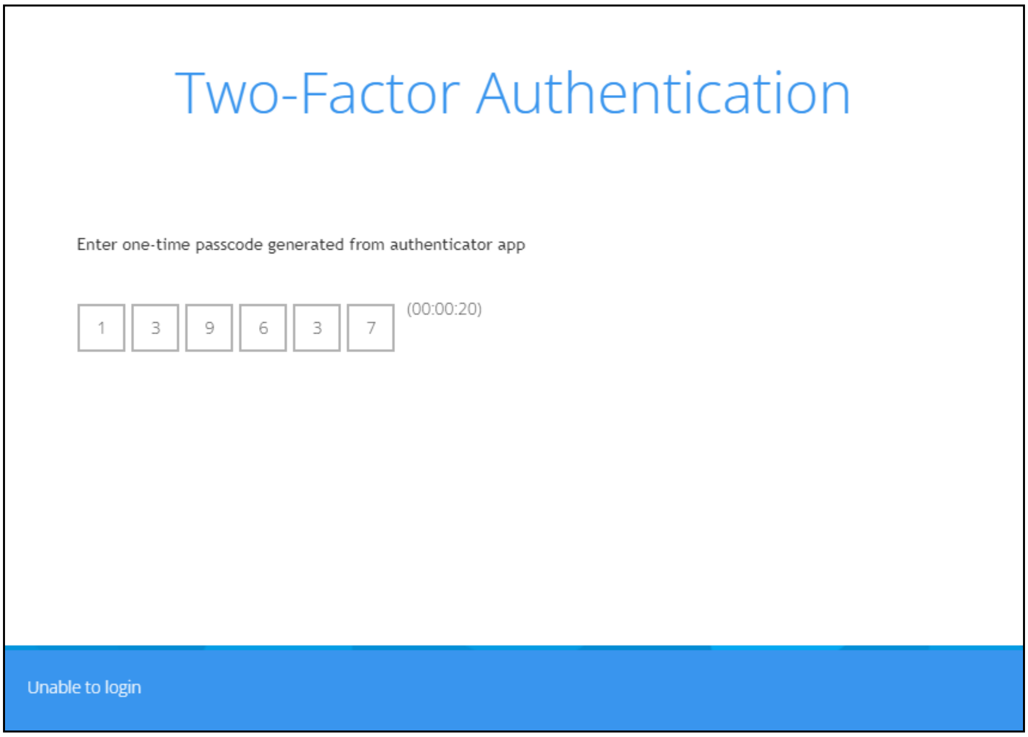
Example of the one-time password generated by Ahsay Mobile:



- **TOTP only**

Input the one-time password generated by Ahsay Mobile to complete the login.

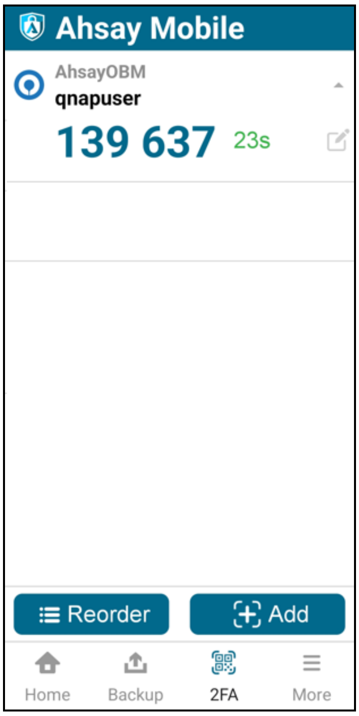
Example of the 2FA alert screen on AhsayOBM after login with correct username and password.


Two-Factor Authentication

Enter one-time passcode generated from authenticator app

1 3 9 6 3 7 (00:00:20)

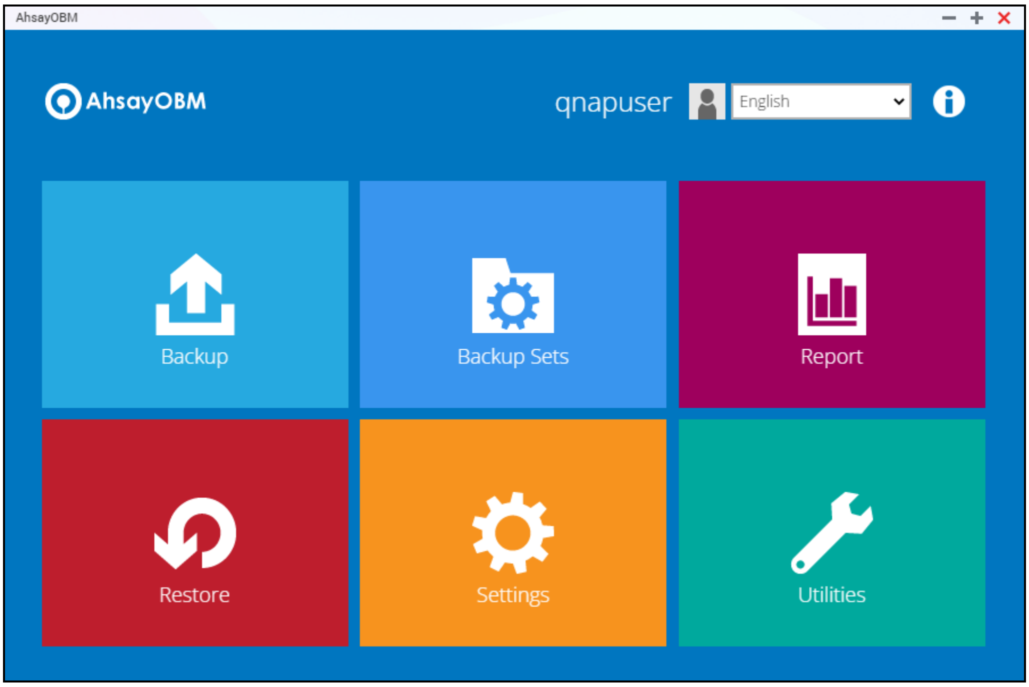
Example of the one-time password generated by Ahsay Mobile:



NOTE

If you are unable to login using any of the authentication method, refer to Chapter 7 Unable to login to AhsayOBM with 2FA.

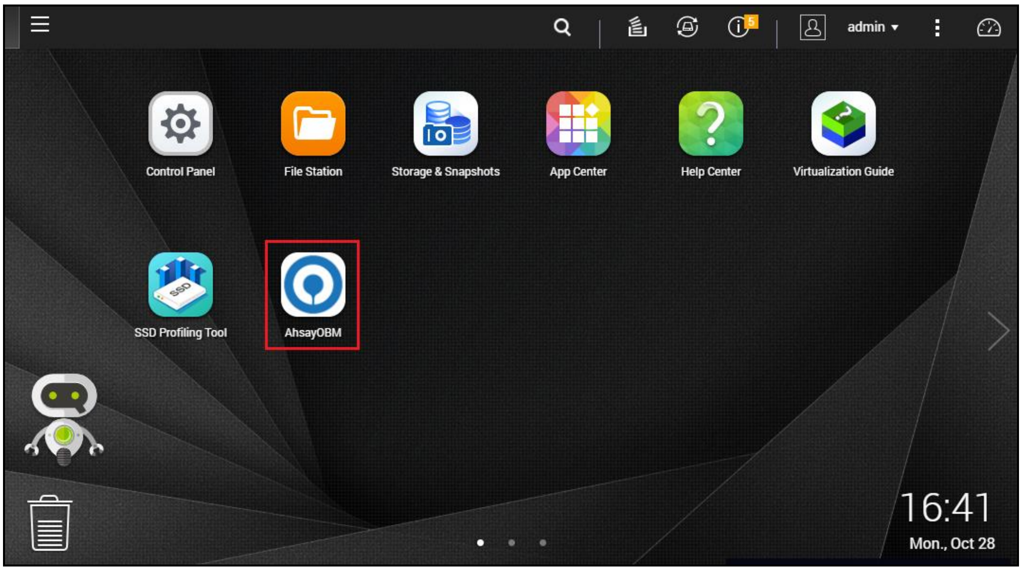
4. After successful login, the following screen will be displayed.



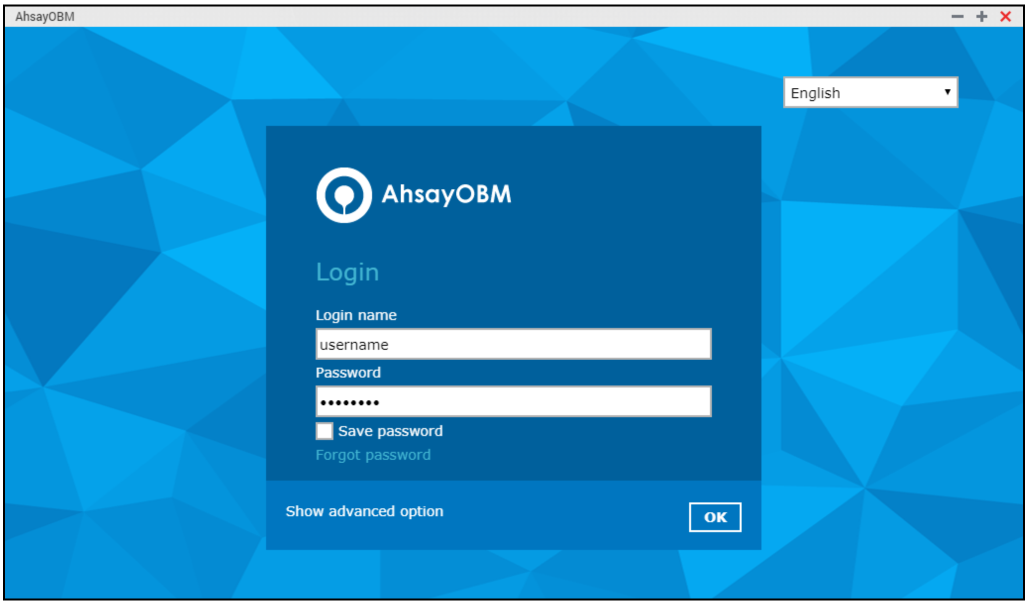
6.3 Login to AhsayOBM with 2FA using third-party TOTP authenticator

When logging in to AhsayOBM with Two-Factor Authentication using third-party TOTP authenticator, please follow the steps below:

1. Click the AhsayOBM icon on the desktop to launch the application.



2. Enter the Login name and Password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



Login name: username

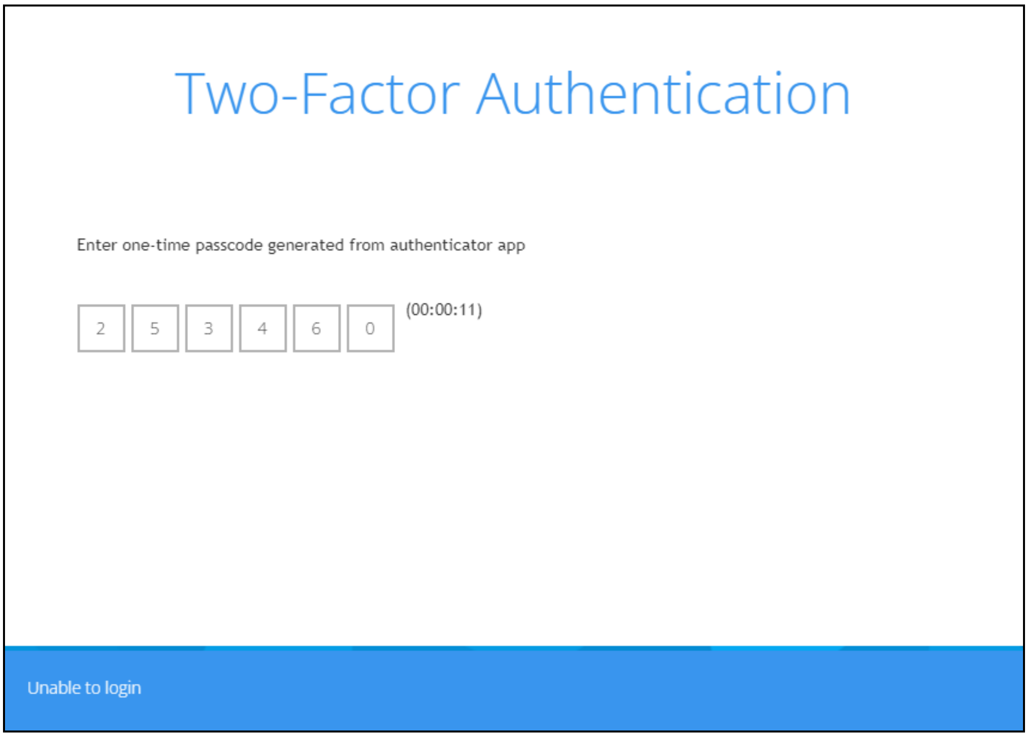
Password: ••••••••

□ Save password

NOTE

The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

3. Enter the one-time passcode generated from the third-party TOTP authenticator.

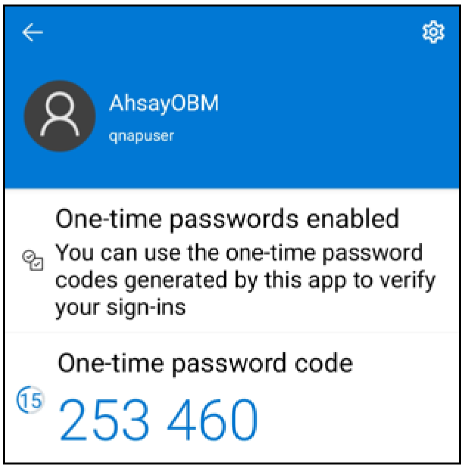


Two-Factor Authentication

Enter one-time passcode generated from authenticator app

2 5 3 4 6 0 (00:00:11)

Example of the one-time passcode generated.



AhsayOBM

qnapuser

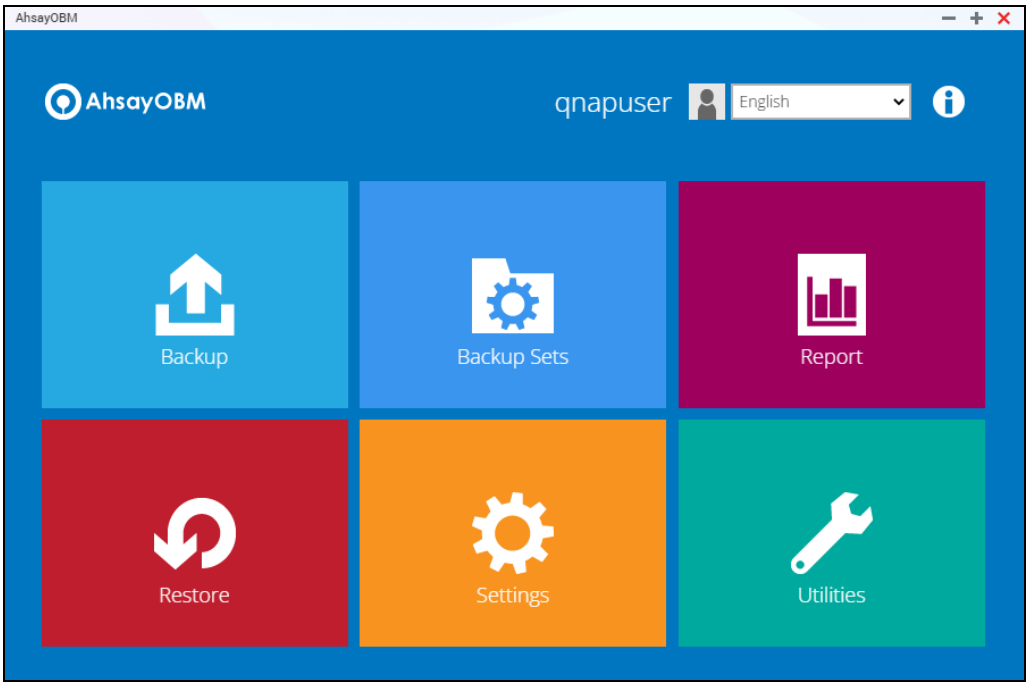
One-time passwords enabled

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

One-time password code

253 460

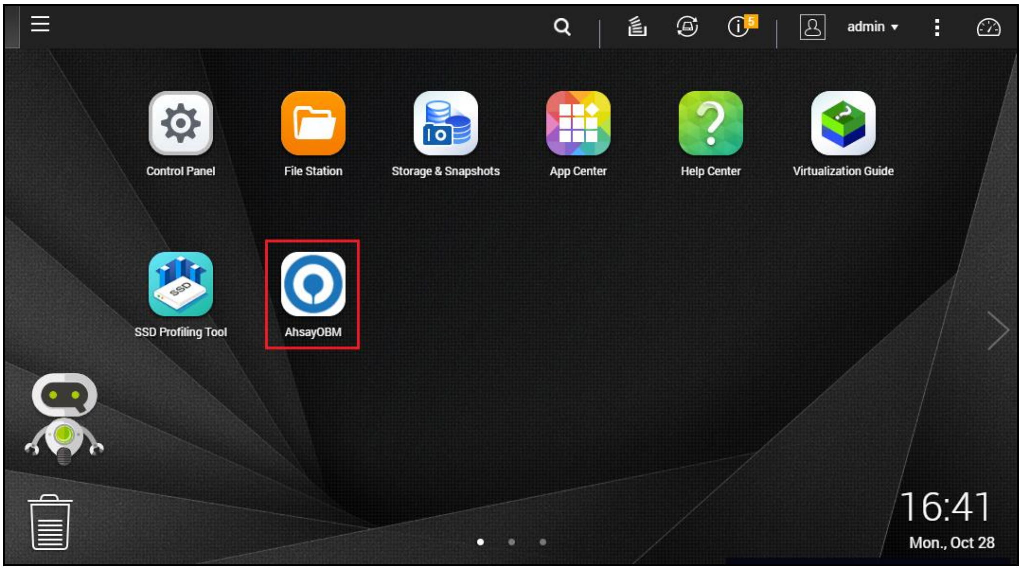
4. After successful login, the following screen will be displayed.



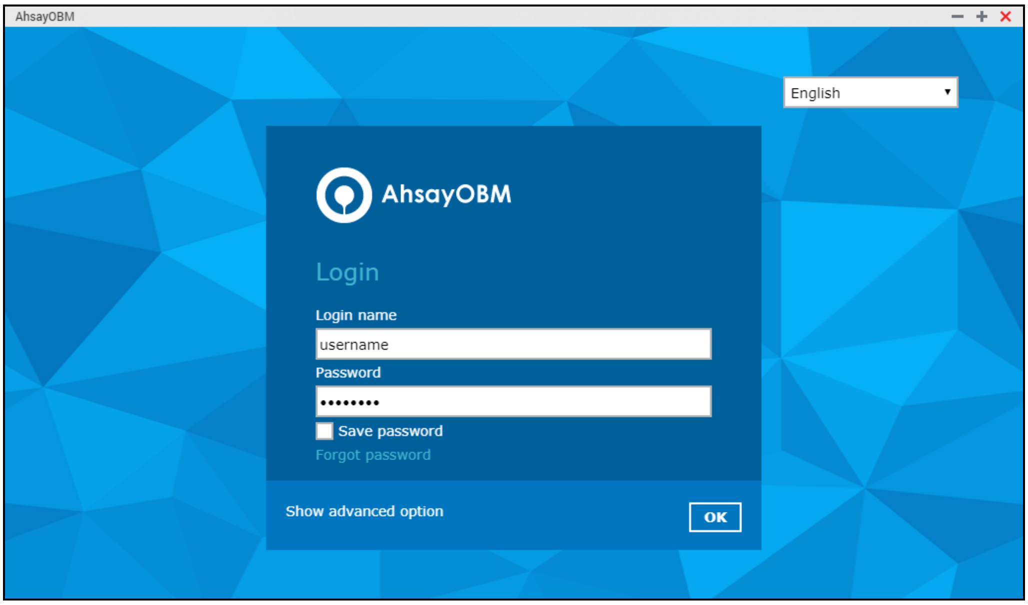
6.4 Login to AhsayOBM with 2FA using Twilio

When logging in to AhsayOBM for user accounts using Twilio, please follow the steps below:

1. Click the AhsayOBM icon on the desktop to launch the application.



2. Enter the Login name and Password of your AhsayOBM account provided by your backup service provider. Then, click **OK** to login.



Login name: username

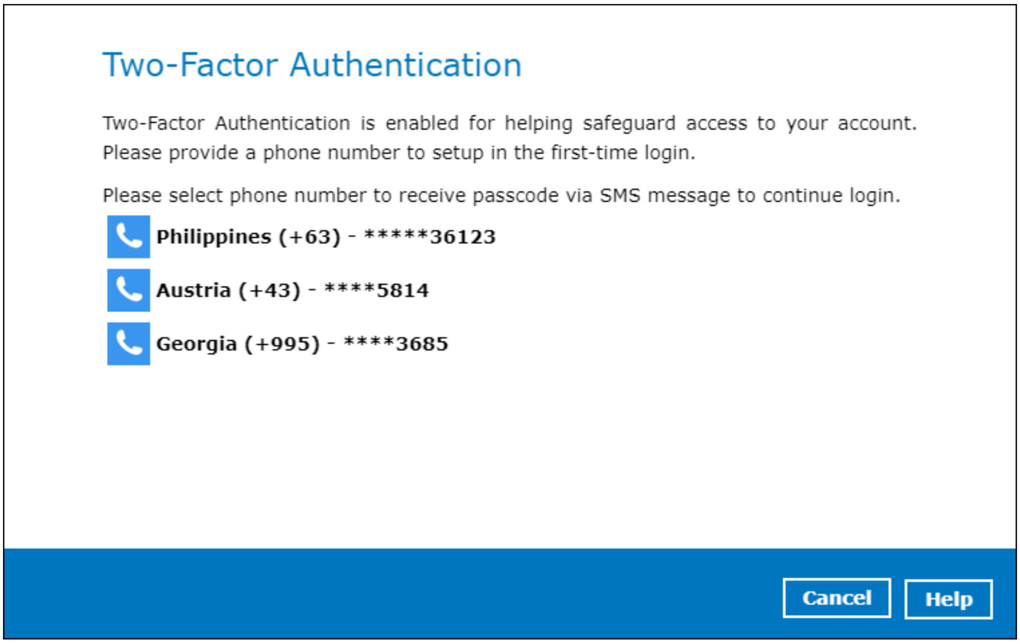
Password: ••••••••

□ Save password

NOTE

The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

3. Select your phone number to receive the passcode.



Two-Factor Authentication

Two-Factor Authentication is enabled for helping safeguard access to your account. Please provide a phone number to setup in the first-time login.

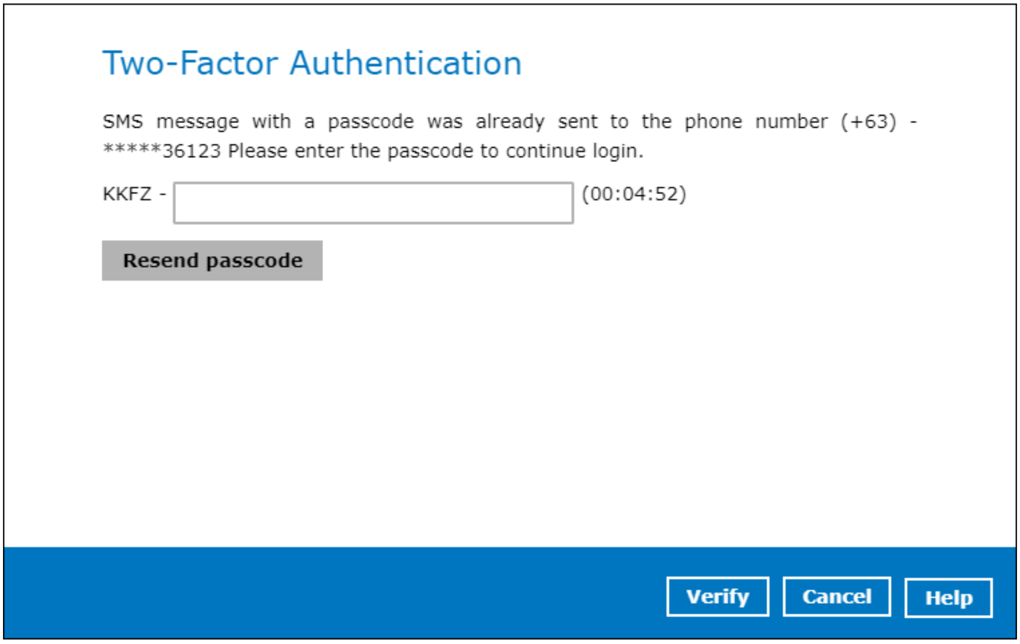
Please select phone number to receive passcode via SMS message to continue login.

☎ **Philippines (+63) - *****36123**

☎ **Austria (+43) - ****5814**

☎ **Georgia (+995) - ****3685**

4. Enter the passcode and click **Verify** to login.

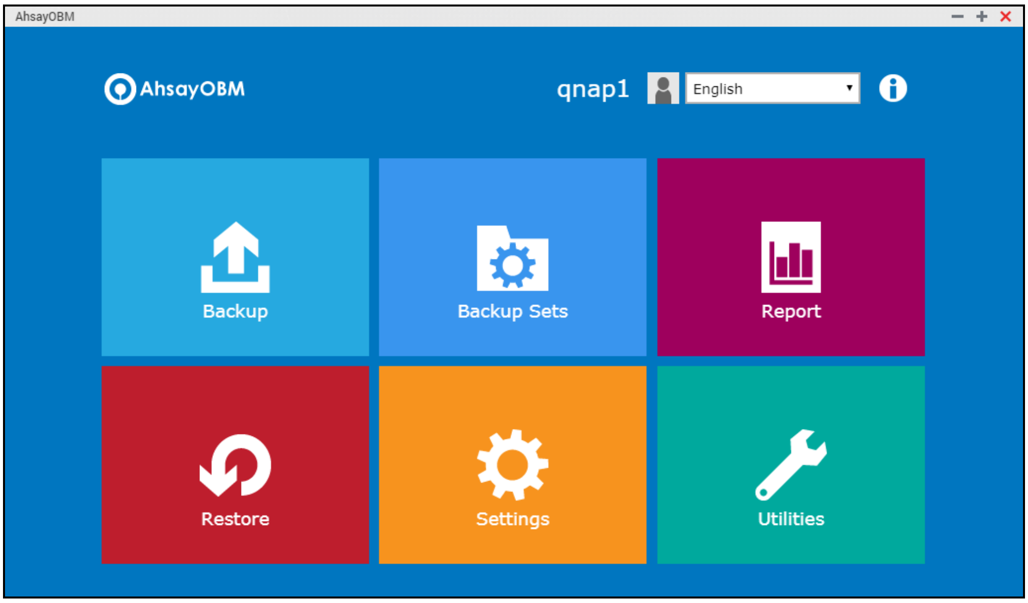


Two-Factor Authentication

SMS message with a passcode was already sent to the phone number (+63) - *****36123 Please enter the passcode to continue login.

KKFZ - (00:04:52)

5. After successful login, the following screen will be displayed.

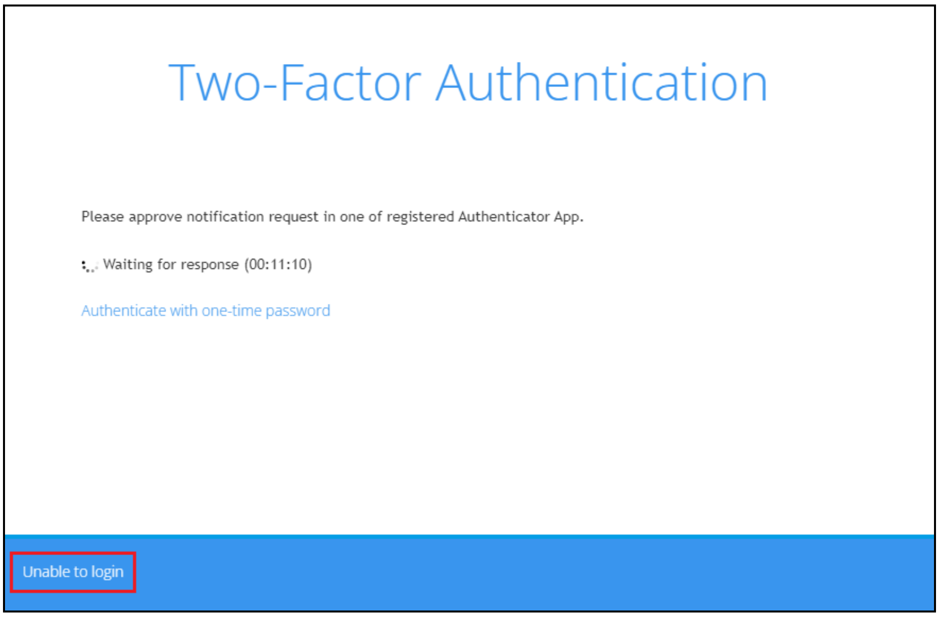


7 Unable to login to AhsayOBM with 2FA

AhsayOBM supports Unable to login feature for users who were not able to accept the notification request from the Ahsay Mobile app and/or cannot obtain the TOTP code from Ahsay Mobile on the subsequent login to AhsayOBM.

Here are the three scenarios after clicking the **Unable to login** link:

- No recovery number was registered on Ahsay Mobile for the 2FA account
- "Authentication Recovery" procedure
- Unable to perform the "Authentication Recovery" procedure



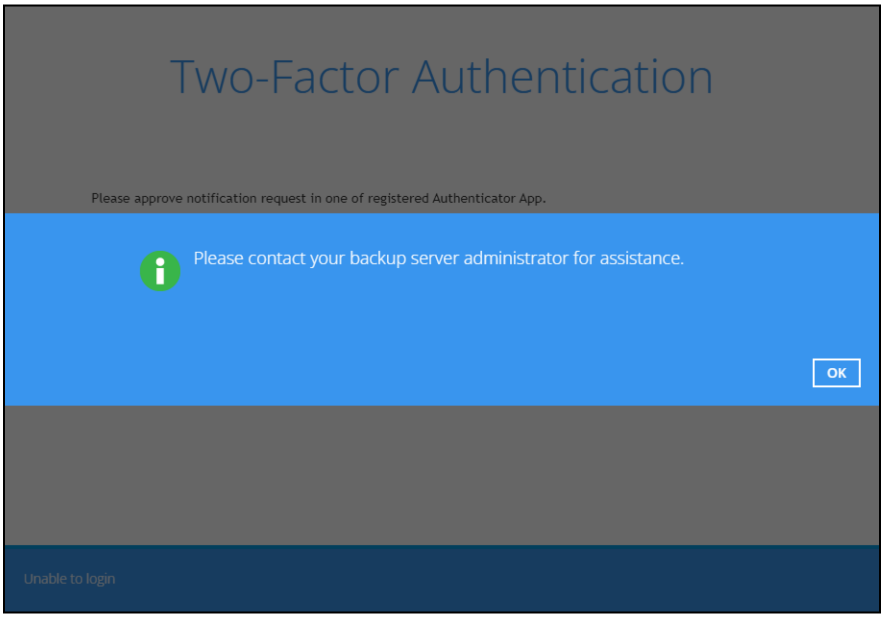
Two-Factor Authentication

Please approve notification request in one of registered Authenticator App.

Waiting for response (00:11:10)

No recovery number was registered on Ahsay Mobile for the 2FA account

If no recovery number was registered on Ahsay Mobile for the 2FA account, then the following message will be displayed "Please contact your backup server administrator for assistance" in gaining access to your AhsayOBM account.



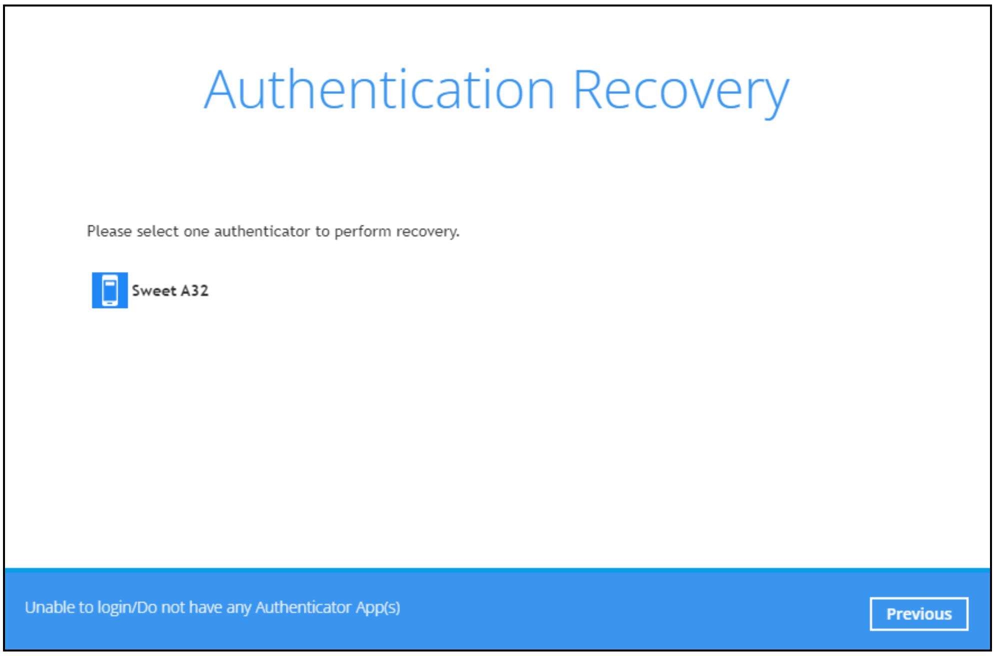
Two-Factor Authentication

Please approve notification request in one of registered Authenticator App.

Please contact your backup server administrator for assistance.

"Authentication Recovery" procedure

If a recovery number was registered on Ahsay Mobile for the 2FA account, then select the registered mobile device to perform the following "Authentication Recovery" procedure.



Authentication Recovery

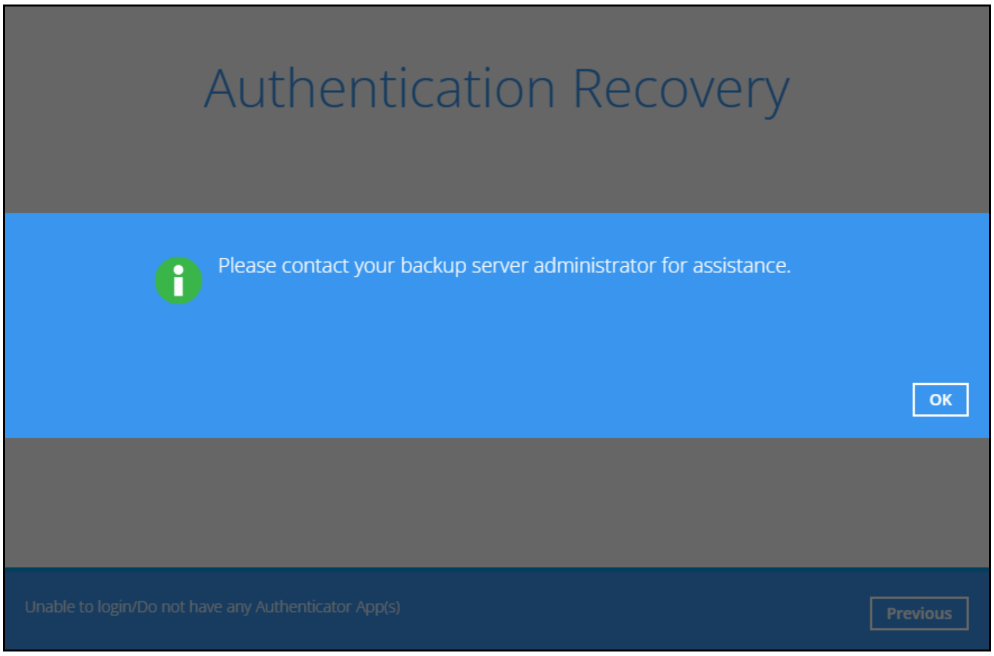
Please select one authenticator to perform recovery.

NOTE

For the detailed steps in performing Authentication Recovery, please refer to Appendix A: Troubleshooting Login in the Ahsay Mobile User Guide for Android and iOS.

Unable to perform the "Authentication Recovery" procedure

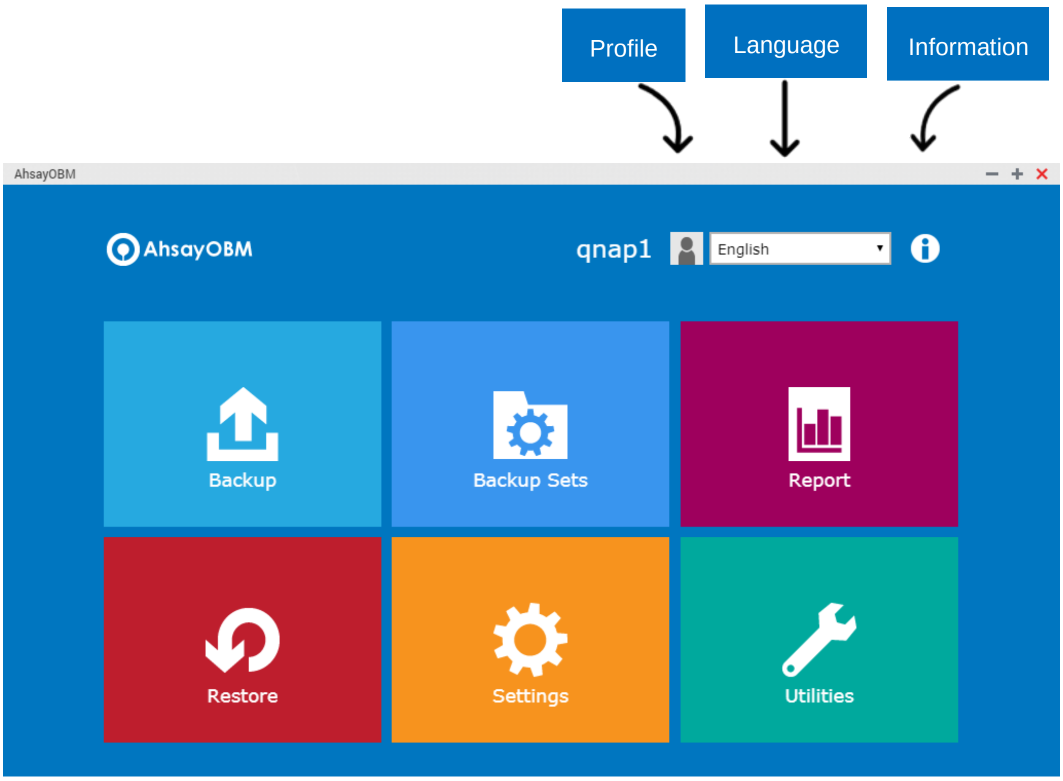
If you are not able to perform the "Authentication Recovery" procedure, click the Unable to login/Do not have any Authenticator App(s) link, then the following message will be displayed "Please contact your backup server administrator for assistance" in gaining access to your AhsayOBM account.



Authentication Recovery

Please contact your backup server administrator for assistance.

8 AhsayOBM Overview



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

- **Profile**
- **Language**
- **Information**
- **Backup**
- **Backup Sets**
- **Report**
- **Restore**
- **Settings**
- **Utilities**

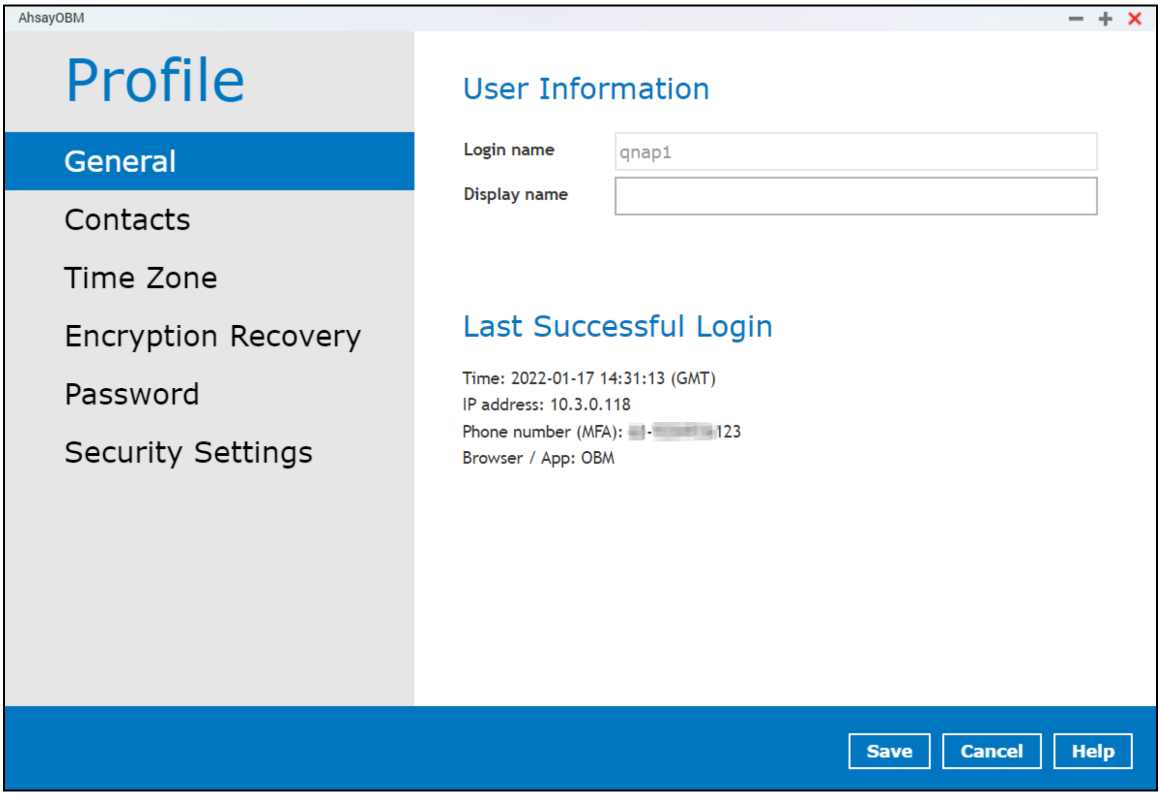
8.1 Profile

The **profile** icon shows the profile settings that can be modified by the user.

Profile has six (6) features:

- General
- Contacts
- Time Zone
- Encryption Recovery
- Password
- Security Settings

The **General** tab displays the user information.



User Information

Login name: qnap1

Display name:

Last Successful Login

Time: 2022-01-17 14:31:13 (GMT)

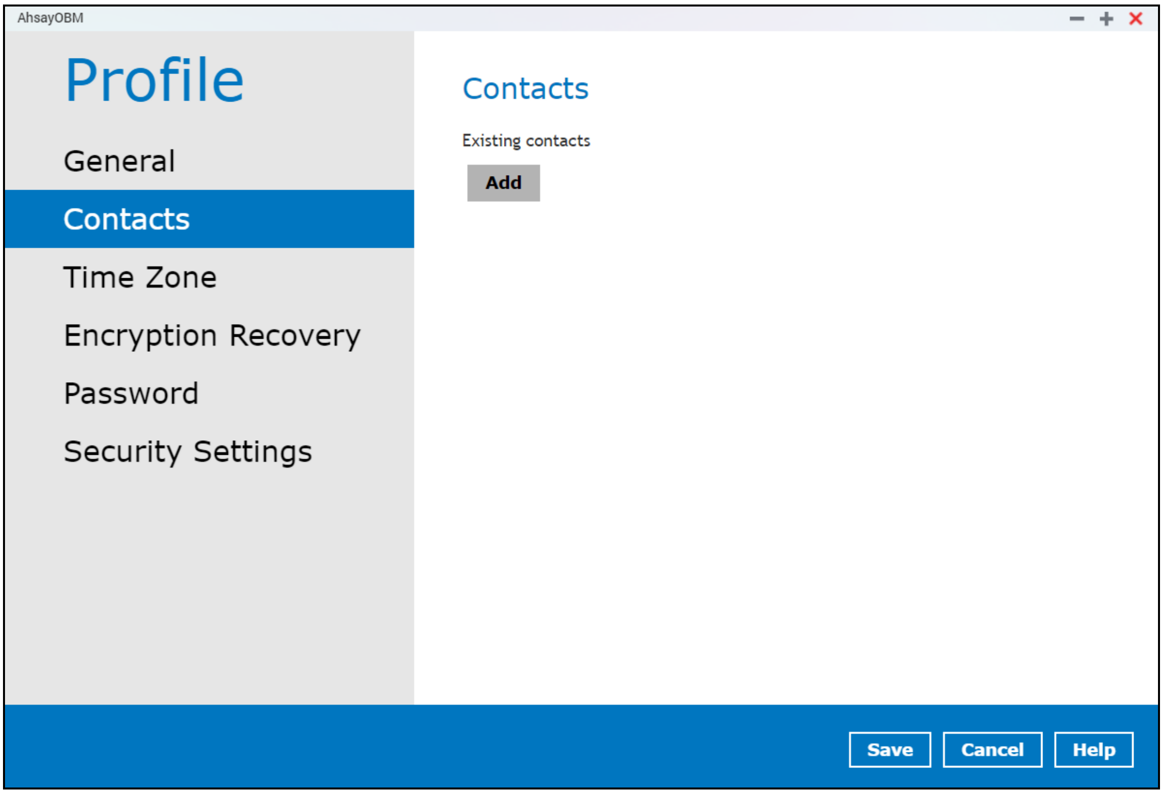
IP address: 10.3.0.118

Phone number (MFA): [redacted]-[redacted]123

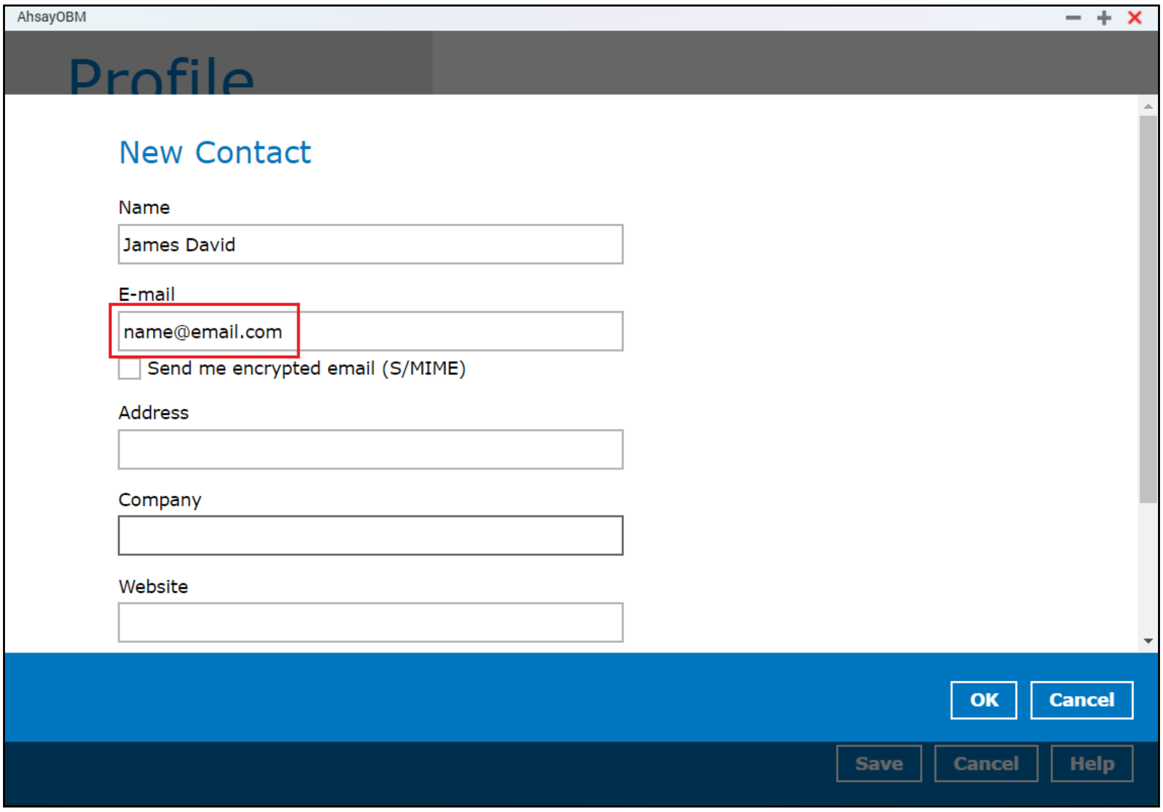
Browser / App: OBM

- The **Login name** is the name of your backup account.
- The **Display name** is the display name of your backup account as you log on to the AhsayCBS management console.
- The **Time** is the date and time the user last logged in.
- The **IP address** used to login.
- The **Phone number (MFA)** is where the sms authentication will be sent when 2FA is enabled.
- The **Browser / App** used to login to AhsayCBS User Web Console or AhsayOBM.

You can add or modify the email address of the **contact person** here. Having this filled in will help us to know where to send the **backup** and **daily reports**, and the **recovered backup set encryption key** in case it was forgotten or lost.



E-mail cannot be left blank.



Name: James David

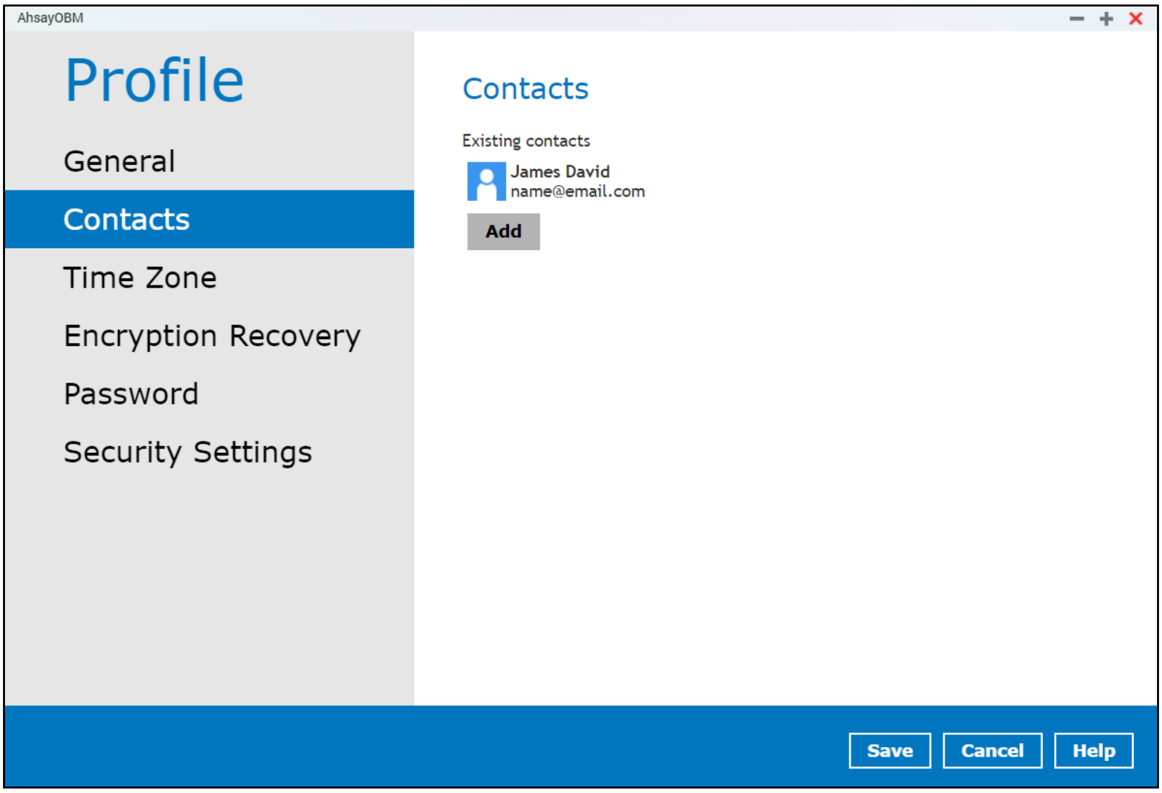
E-mail: name@email.com

□ Send me encrypted email (S/MIME)

Address:

Company:

Website:


AhsayOBM

Profile

General

Contacts

Time Zone

Encryption Recovery

Password

Security Settings

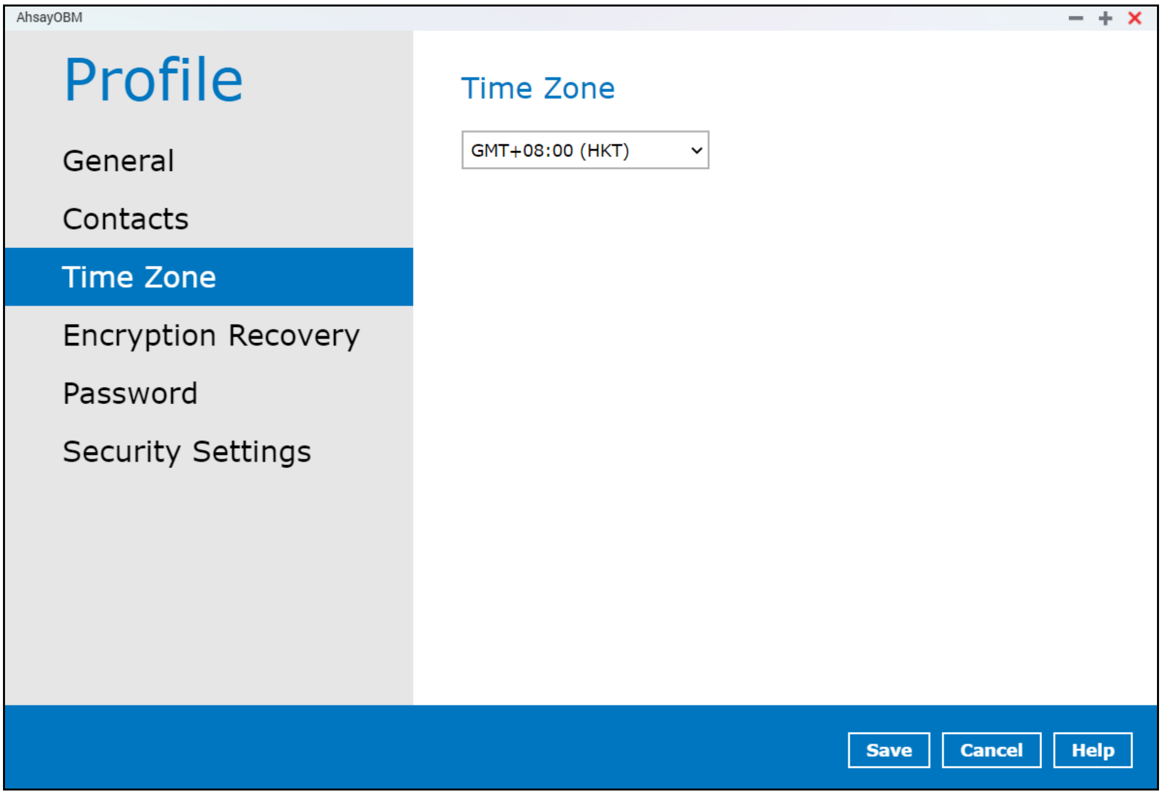
Contacts

Existing contacts

James David
name@email.com

NOTE
You can add multiple contacts here.

This is the **time zone** of the machine where AhsayOBM is installed. To ensure that the backup will run accurately at your specified time, setup the correct time.


AhsayOBM

Profile

General

Contacts

Time Zone

Encryption Recovery

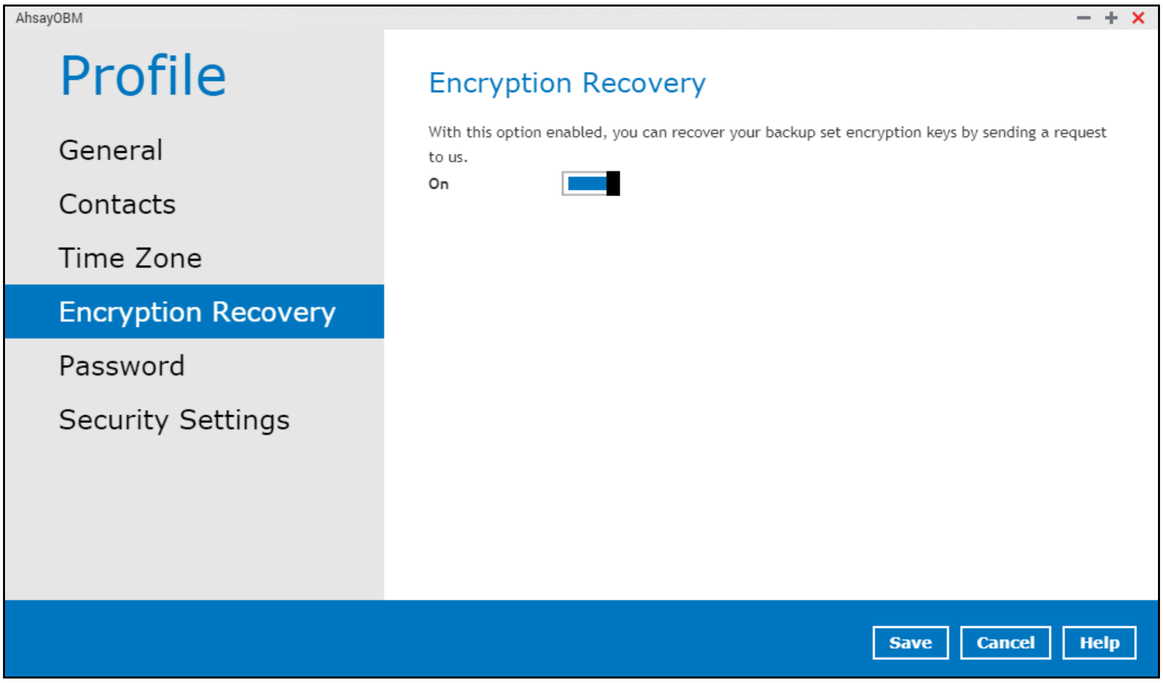
Password

Security Settings

Time Zone

GMT+08:00 (HKT)

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



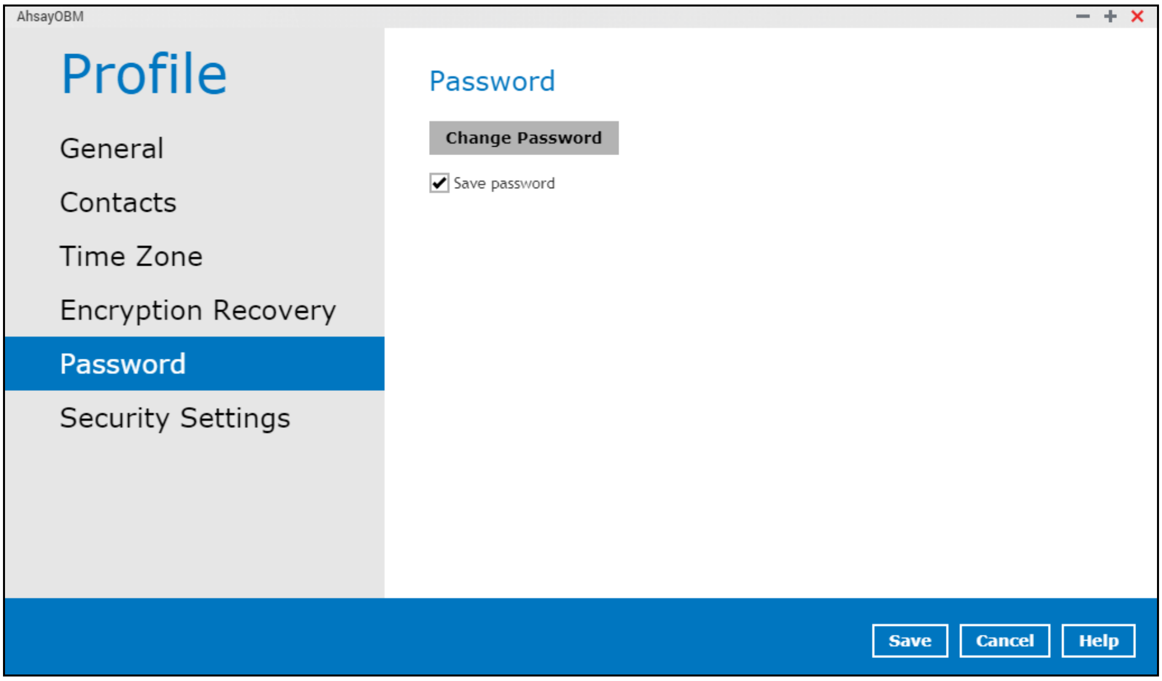
Encryption Recovery

With this option enabled, you can recover your backup set encryption keys by sending a request to us.

On

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

Login password can be modified anytime. You can also check the **Save password** box to bypass the password entry when opening the AhsayOBM interface.

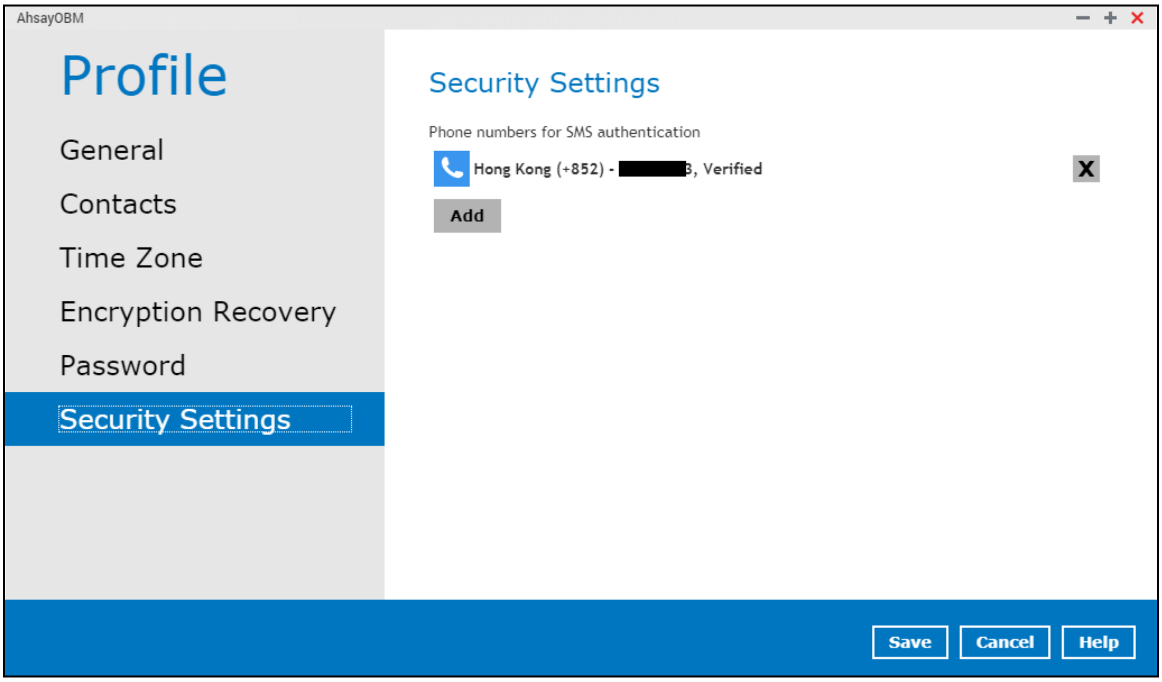


Password

☑ Save password

NOTE
The Save password option may not be available. This depends on the settings of your backup service provider. Please contact your backup service provider for more information.

Security Settings will only be visible if two-factor authentication is enabled. Phone numbers that will be used for sending sms authentication will be listed here and will show the status if it is verified or not. You can also add phone numbers here that can be used for sending the sms authentication.

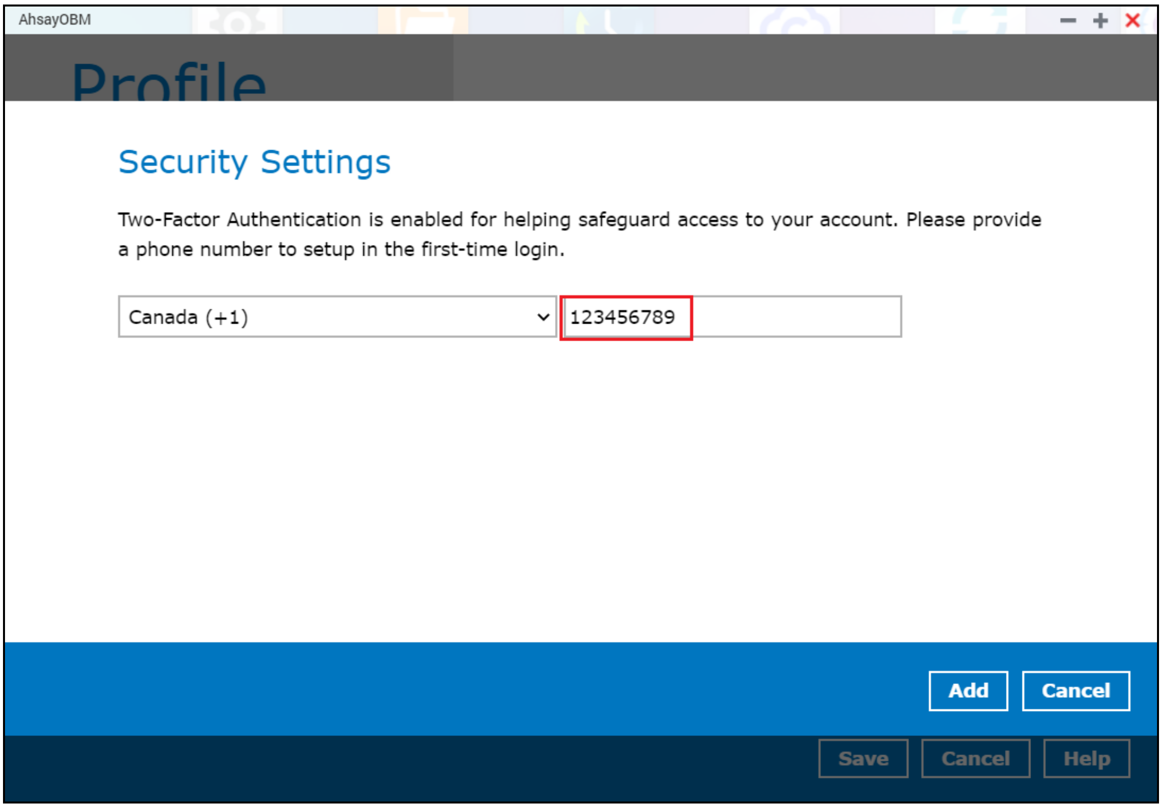


Security Settings

Phone numbers for SMS authentication

☎ Hong Kong (+852) - [redacted], Verified ☒

Select the country click **Add**.



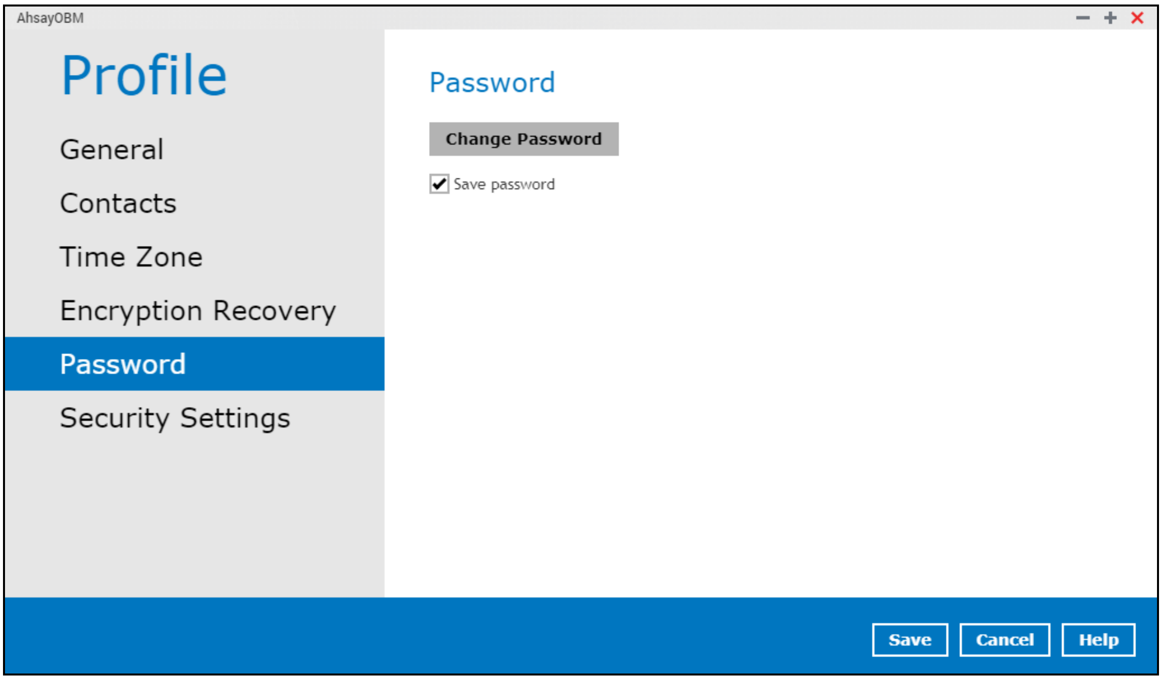
Security Settings

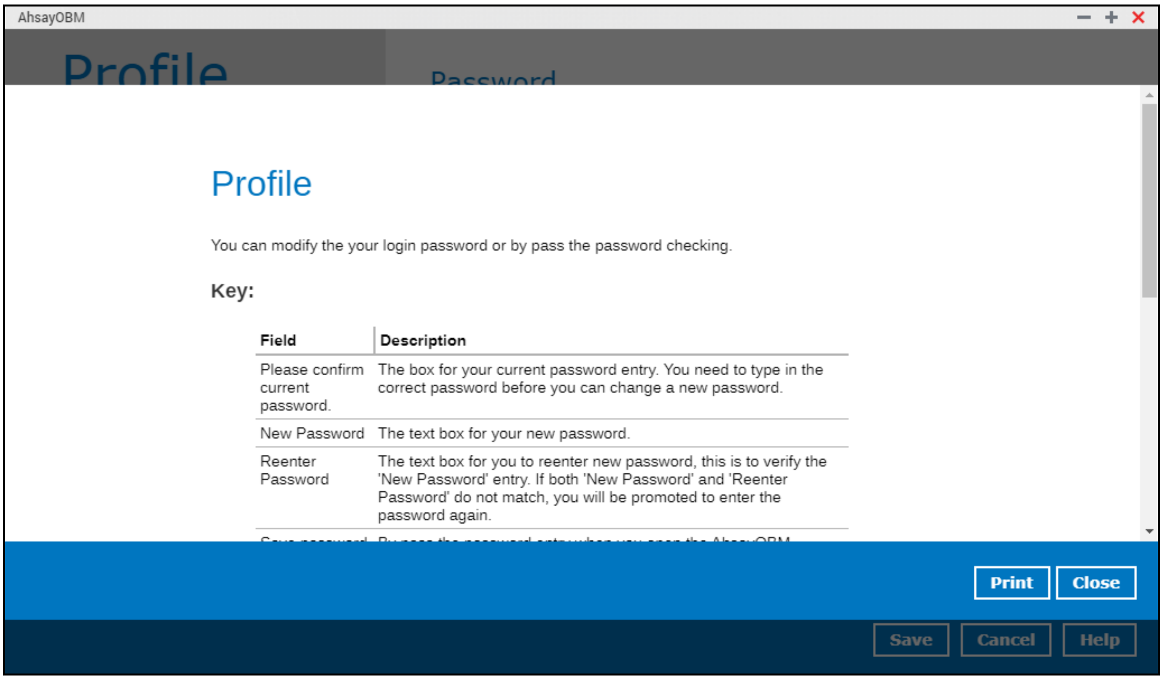
Two-Factor Authentication is enabled for helping safeguard access to your account. Please provide a phone number to setup in the first-time login.

Canada (+1) | 123456789

8.2 Online Help

Clicking on the H**elp** tab will show you the information and instructions you may need.





Profile

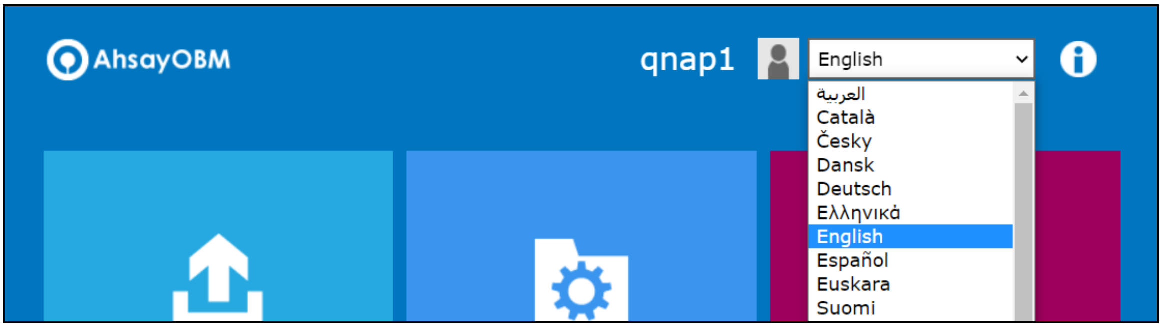
You can modify the your login password or by pass the password checking.

Key:

Field	Description
Please confirm current password.	The box for your current password entry. You need to type in the correct password before you can change a new password.
New Password	The text box for your new password.
Reenter Password	The text box for you to reenter new password, this is to verify the 'New Password' entry. If both 'New Password' and 'Reenter Password' do not match, you will be promoted to enter the password again.
Save password	By pass the password entry when you open the AhsayOBM

8.3 Language

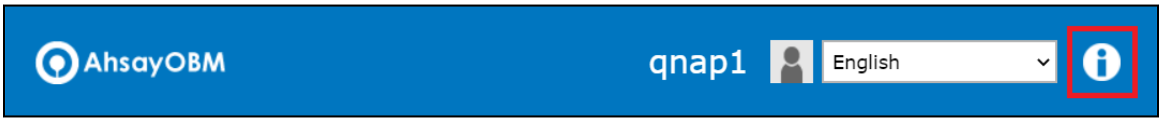
This option is used to change the language of the user interface. The list of available languages depends on the backup service provider.

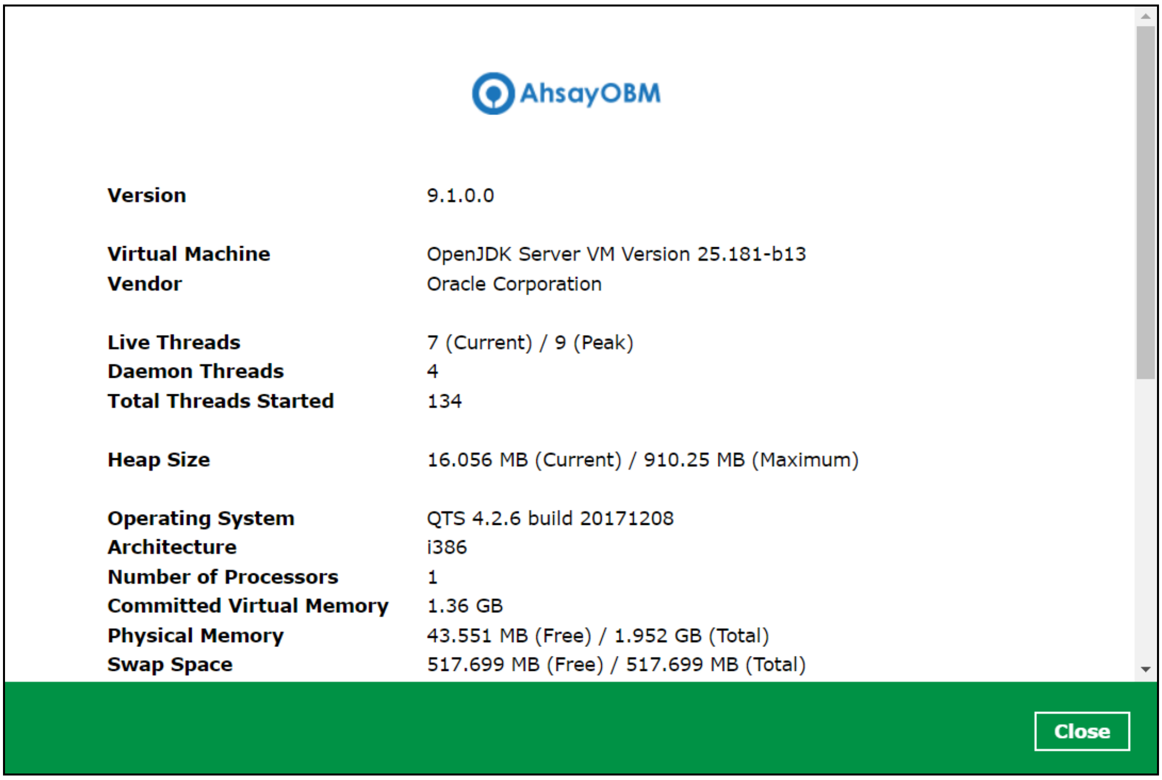


Once the language is set, it will reflect on the AhsayOBM interface right away.

8.4 Information

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

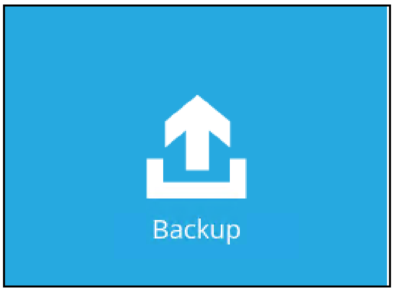




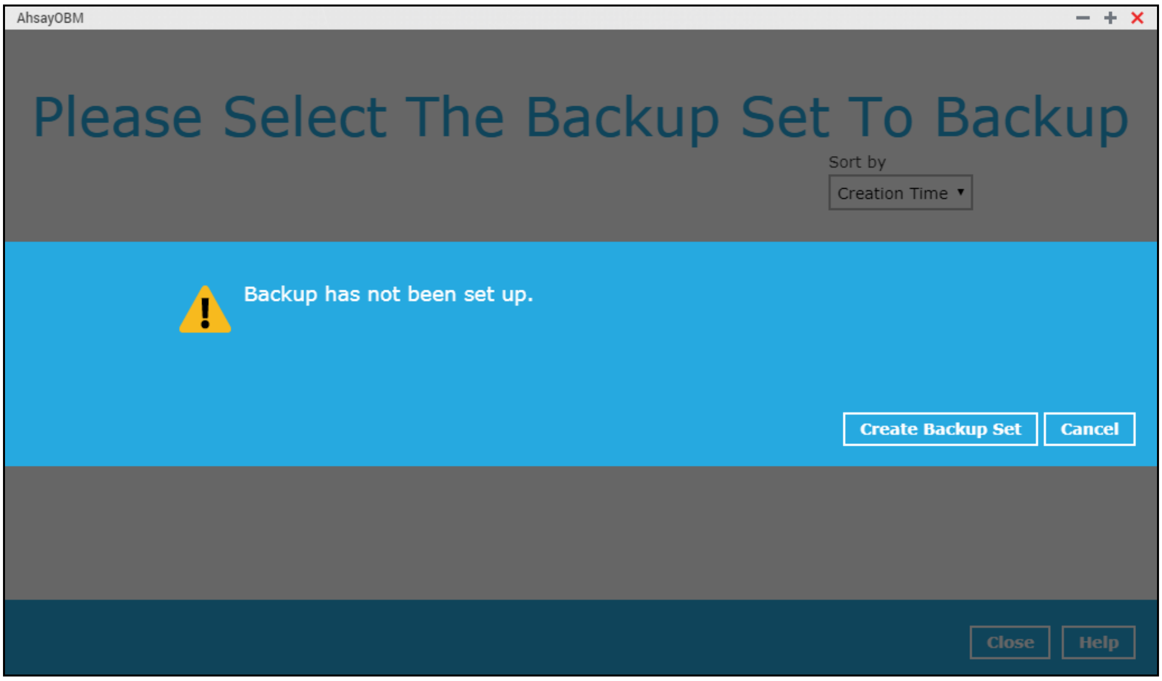
Version	9.1.0.0
Virtual Machine	OpenJDK Server VM Version 25.181-b13
Vendor	Oracle Corporation
Live Threads	7 (Current) / 9 (Peak)
Daemon Threads	4
Total Threads Started	134
Heap Size	16.056 MB (Current) / 910.25 MB (Maximum)
Operating System	QTS 4.2.6 build 20171208
Architecture	i386
Number of Processors	1
Committed Virtual Memory	1.36 GB
Physical Memory	43.551 MB (Free) / 1.952 GB (Total)
Swap Space	517.699 MB (Free) / 517.699 MB (Total)

8.5 Backup

This feature is used to run your backup set(s).



When using AhsayOBM for the first time, you will be asked to create a new backup set first.

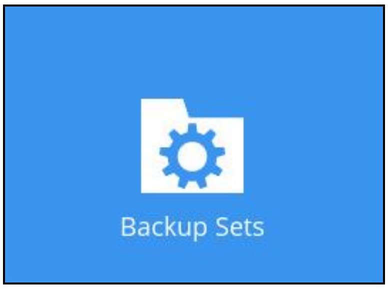


Backup has not been set up.

For instructions on how to start a backup, refer to Chapter 11 Run Backup Jobs.

8.6 Backup Sets

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



To create or modify a backup set, follow the instructions on Chapter 7 Creating a File Backup Set.

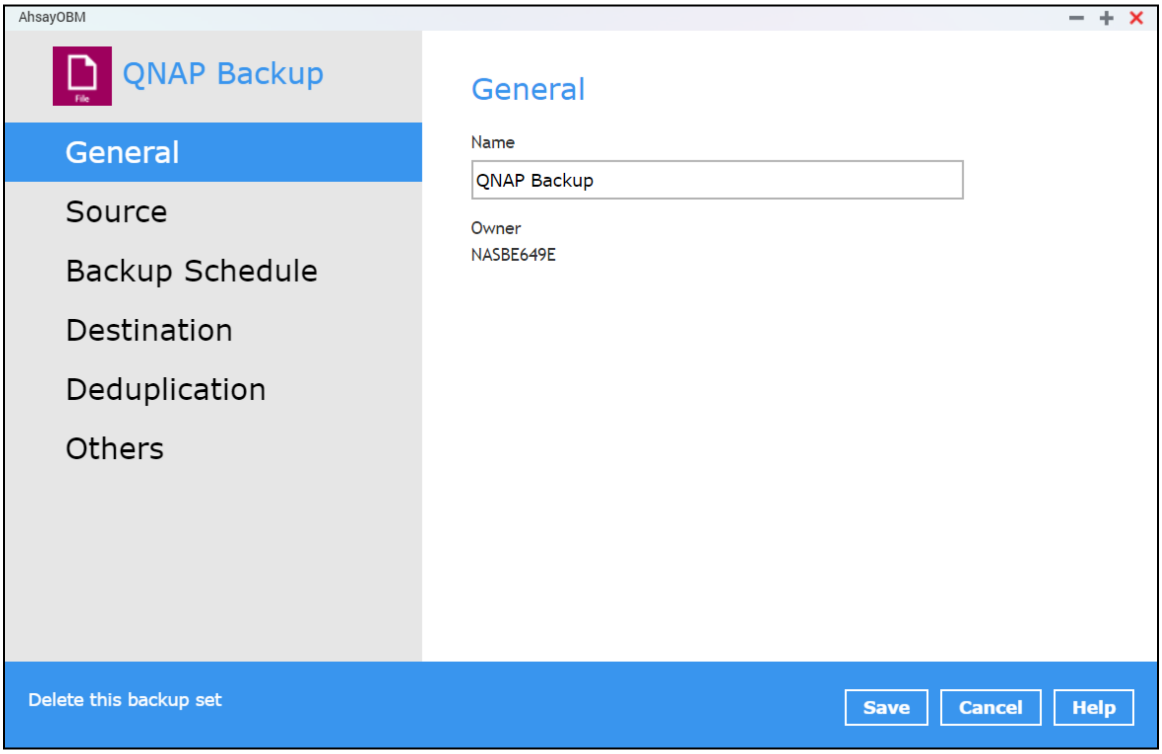
Backup Set Settings

Below is the list of configurable items under the Backup Sets:

- General
- Source
- Backup Schedule
- Destination
- Deduplication
- Others

General

This allows the user to modify the name of the backup set and displays the Owner which is the name of the machine where the backup set was created on.



General

Name: QNAP Backup

Owner: NASBE649E

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

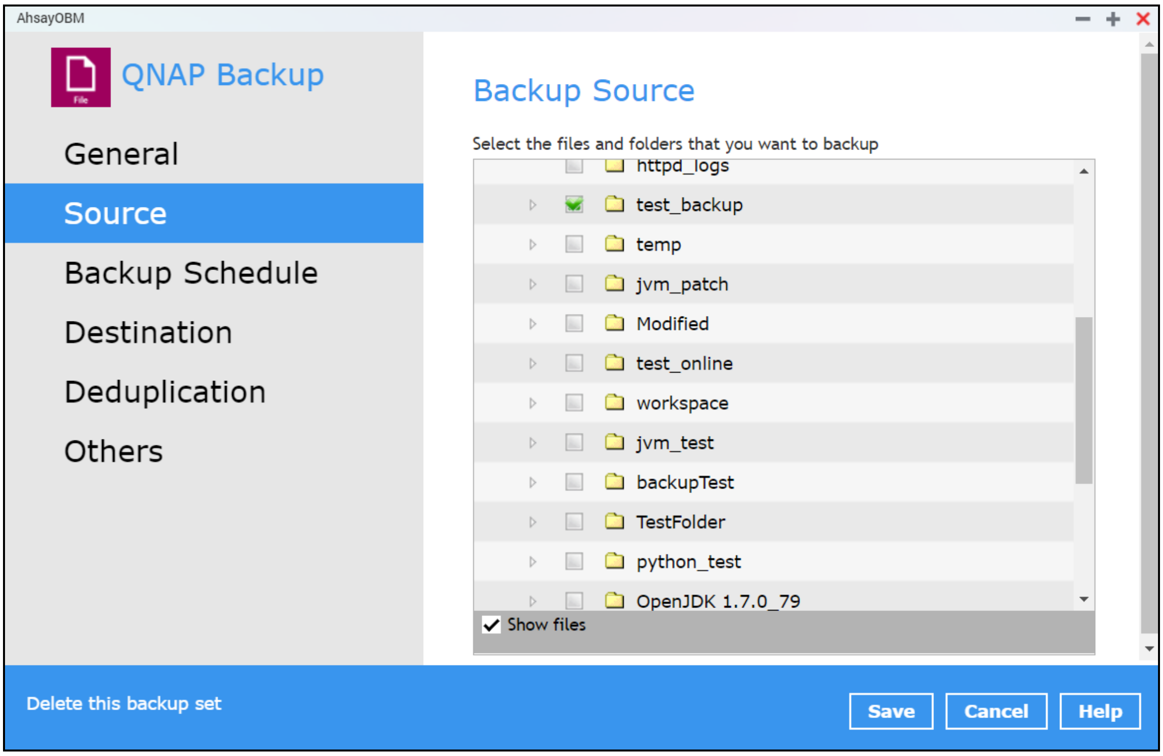
1. Select **General**.

2. Enter the new backup set name on the Name field.

3. Click the **Save** button to save the new backup set name.

Source

This allows the user to select from the available files and/or folders to back up from NAS device.



Backup Source

Select the files and folders that you want to backup

- □ httpd_logs
- ☑ test_backup
- □ temp
- □ jvm_patch
- □ Modified
- □ test_online
- □ workspace
- □ jvm_test
- □ backupTest
- □ TestFolder
- □ python_test
- □ OpenJDK 1.7.0_79

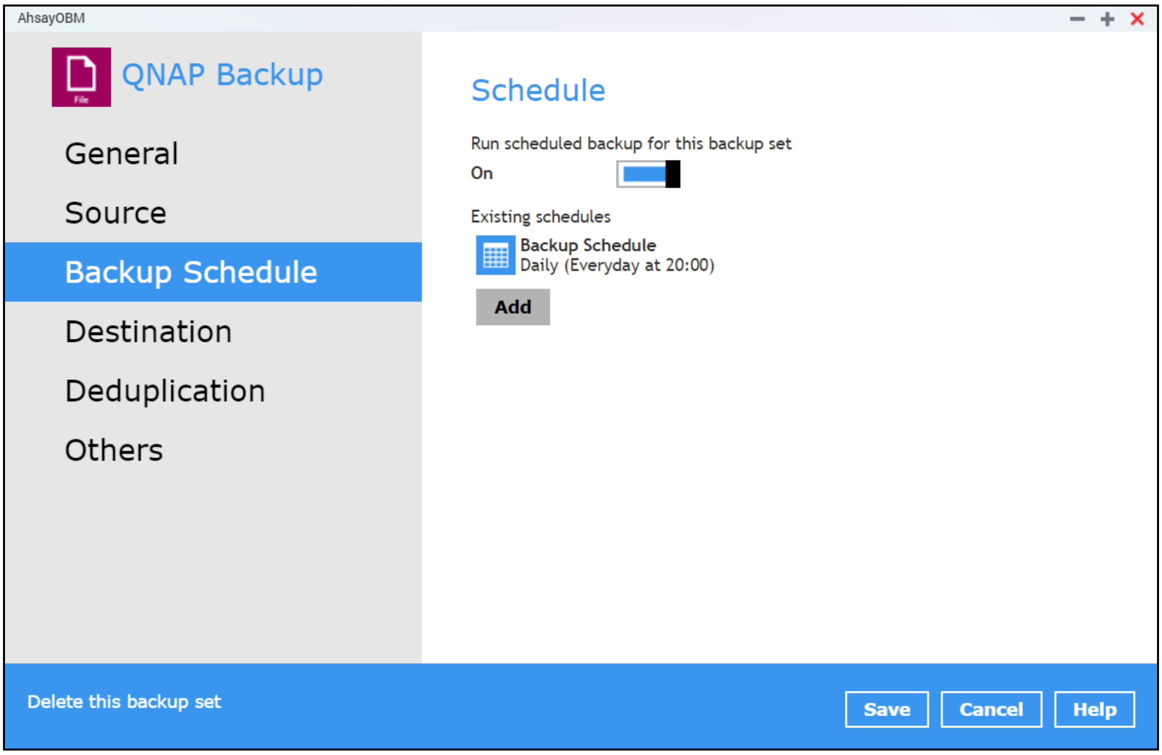
☑ Show files

To add backup source, follow the instructions below:

1. Select **Source**.
2. On the right side of the screen, select files and/or folders you want to backup.
3. Tick the “Show files” checkbox to show the files under a specific folder.
4. Click the **Save** button to save the settings made.

Backup Schedule

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



Schedule

Run scheduled backup for this backup set

On

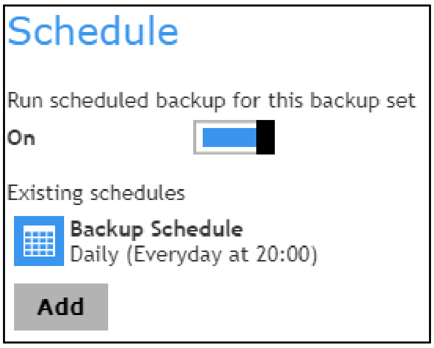
Existing schedules

Backup Schedule
Daily (Everyday at 20:00)

Add

To configure a backup schedule, follow the steps below:

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



Schedule

Run scheduled backup for this backup set

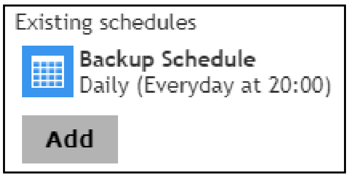
On

Existing schedules

Backup Schedule
Daily (Everyday at 20:00)

Add

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

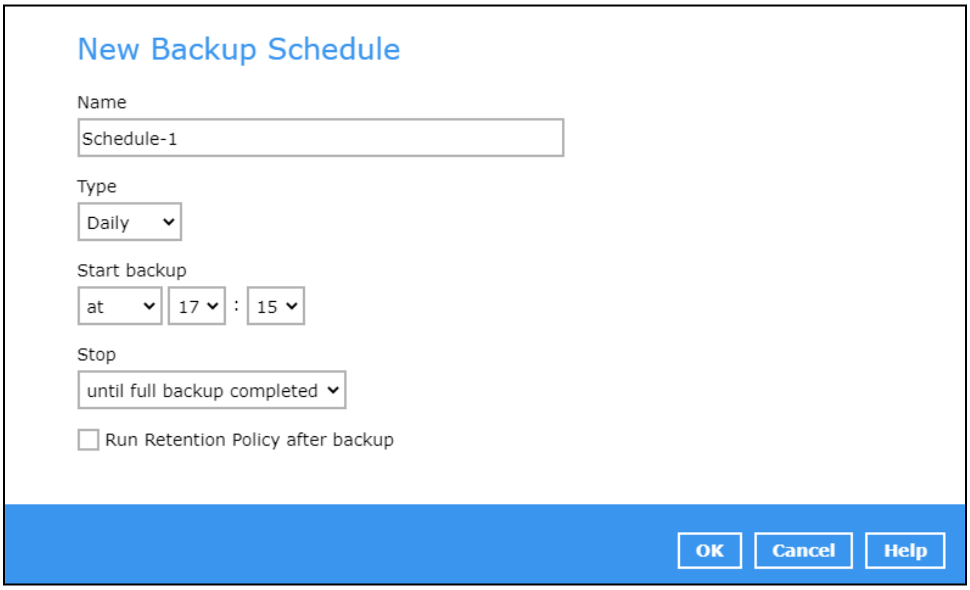


Existing schedules

Backup Schedule
Daily (Everyday at 20:00)

Add

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



New Backup Schedule

Name: Schedule-1

Type: Daily

Start backup: at 17 : 15

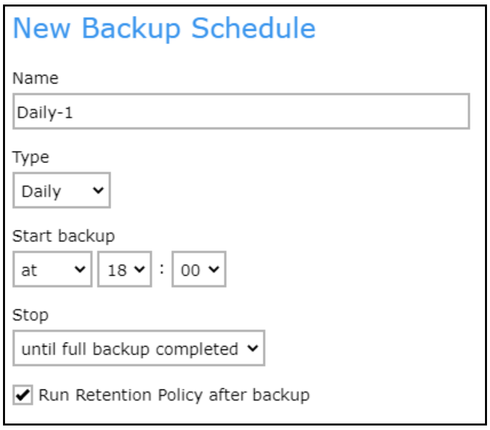
Stop: until full backup completed

□ Run Retention Policy after backup

- **Name** – the name of the backup schedule.

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

  - **Daily** – the time of the day when the backup job will run.



New Backup Schedule

Name: Daily-1

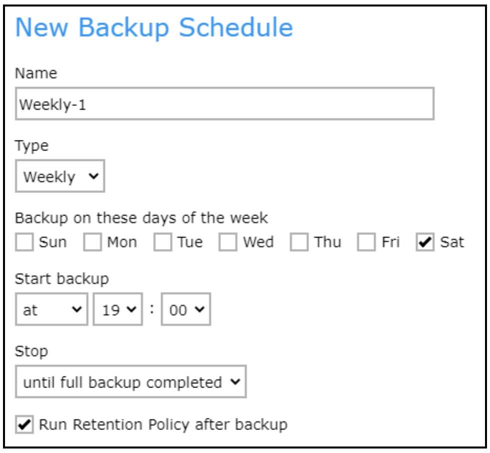
Type: Daily

Start backup: at 18 : 00

Stop: until full backup completed

☑ Run Retention Policy after backup

  - **Weekly** – the day of the week and the time of the day when the backup job will run.



New Backup Schedule

Name: Weekly-1

Type: Weekly

Backup on these days of the week

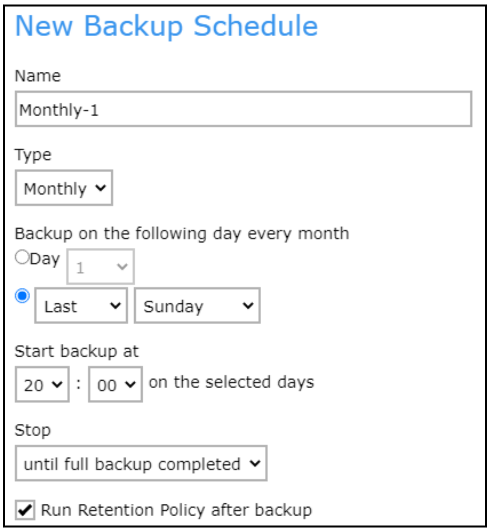
□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat

Start backup: at 19 : 00

Stop: until full backup completed

☑ Run Retention Policy after backup

- **Monthly** – the day of the month and the time of the day when the backup job will run.



New Backup Schedule

Name
Monthly-1

Type
Monthly

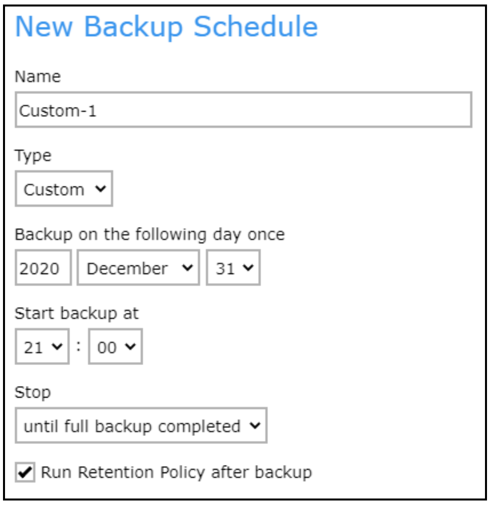
Backup on the following day every month
○ Day 1
● Last Sunday

Start backup at
20 : 00 on the selected days

Stop
until full backup completed

☑ Run Retention Policy after backup

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



New Backup Schedule

Name
Custom-1

Type
Custom

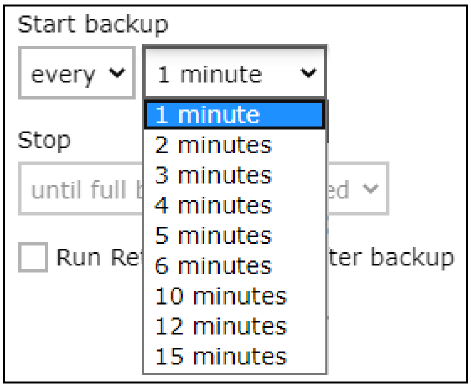
Backup on the following day once
2020 December 31

Start backup at
21 : 00

Stop
until full backup completed

☑ Run Retention Policy after backup

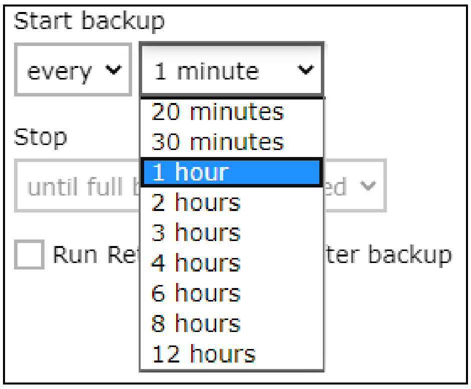
- **Start backup** – the start time of the backup job.
  - **at** – this option will start a backup job at a specific time.
  - **every** – this option will start a backup job in intervals of minutes or hours.



Start backup
every 1 minute

Stop
until full b...ed

□ Run Re...ter backup

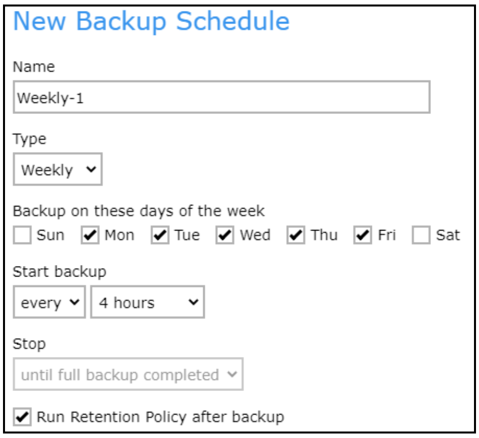


Start backup
every 1 minute

Stop
until full ...ed

□ Run Re...ter backup

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



New Backup Schedule

Name: Weekly-1

Type: Weekly

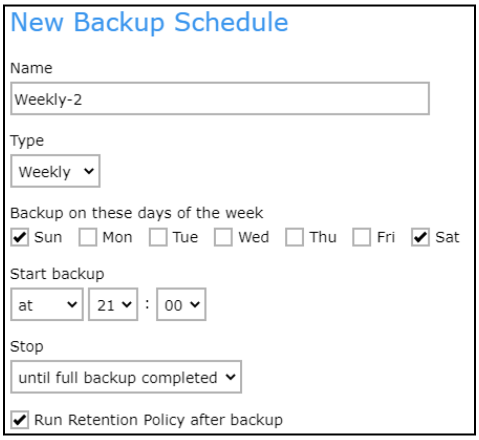
Backup on these days of the week: ☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat

Start backup: every 4 hours

Stop: until full backup completed

☑ Run Retention Policy after backup

Figure 1.1



New Backup Schedule

Name: Weekly-2

Type: Weekly

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

Start backup: at 21 : 00

Stop: until full backup completed

☑ Run Retention Policy after backup

Figure 1.2

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

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

- **Stop** – the stop **time** of the backup job. This only applies to schedules with start backup "at" and is not supported for periodic backup schedule (start backup "every")

  - **until full backup completed** – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.

  - **after (defined no. of hrs.)** – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

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

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

    The partially backed up data will have to be removed by running the data integrity check.

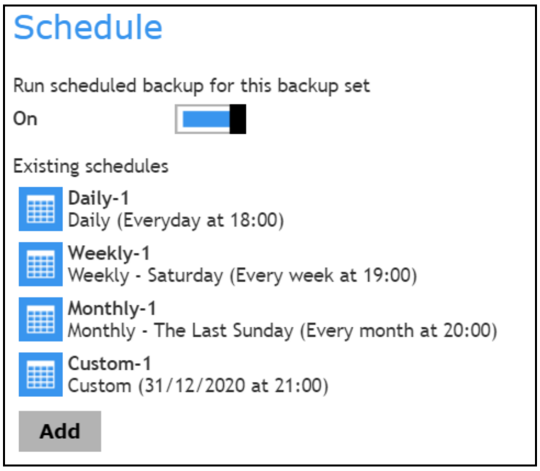
    As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.

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

4. Click the **OK** button to save the configured backup schedule settings.

5. Click the **Save** button to save settings.

6. Multiple backup schedules can be created.



Schedule

Run scheduled backup for this backup set

On

Existing schedules

Daily-1
Daily (Everyday at 18:00)

Weekly-1
Weekly - Saturday (Every week at 19:00)

Monthly-1
Monthly - The Last Sunday (Every month at 20:00)

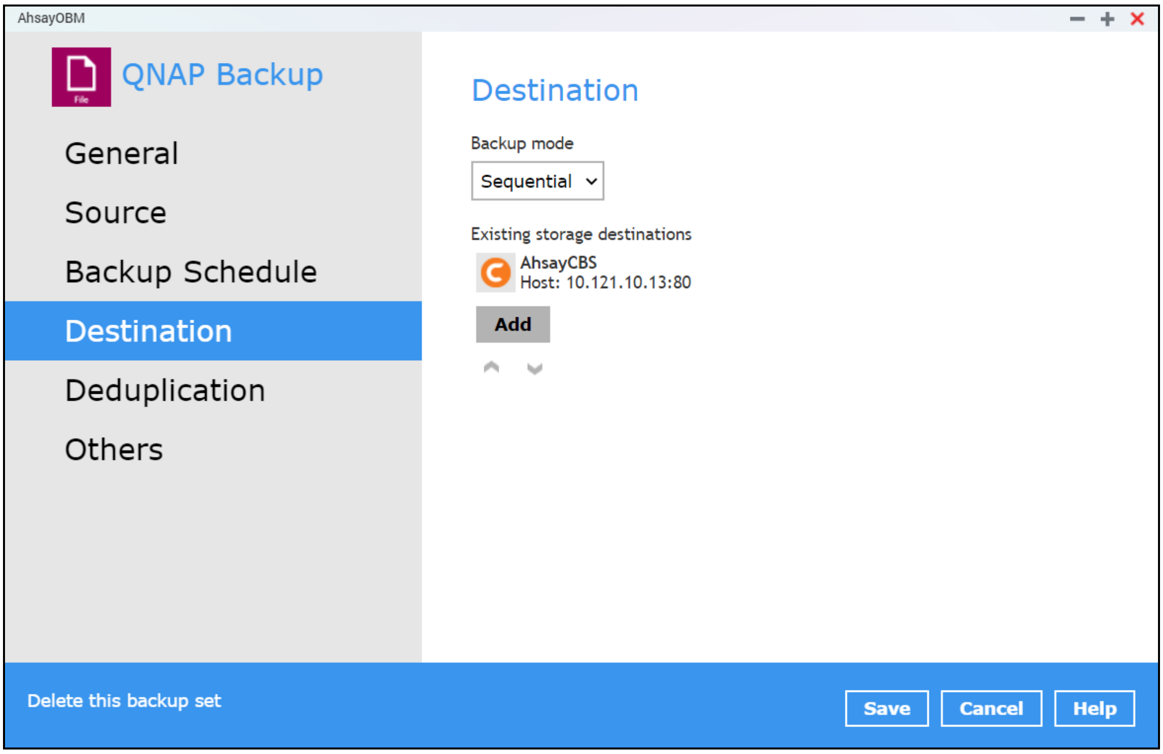
Custom-1
Custom (31/12/2020 at 21:00)

NOTE

For more details on the scenario for Backup Schedule under Backup Set Settings, refer to Appendix C: Scheduler Scenarios.

Destination

This allows the user to view the current backup mode and existing storage destination(s). It also allows the user to add more storage destinations.



Destination

Backup mode
Sequential

Existing storage destinations
AhsayCBS
Host: 10.121.10.13:80

To add a destination, follow the instructions below:

1. Select **Destination**.

2. Click the **Add** button.

3. Complete the following fields:
   a. Name
   b. Destination Storage

4. Click the **OK** button to add the new schedule.

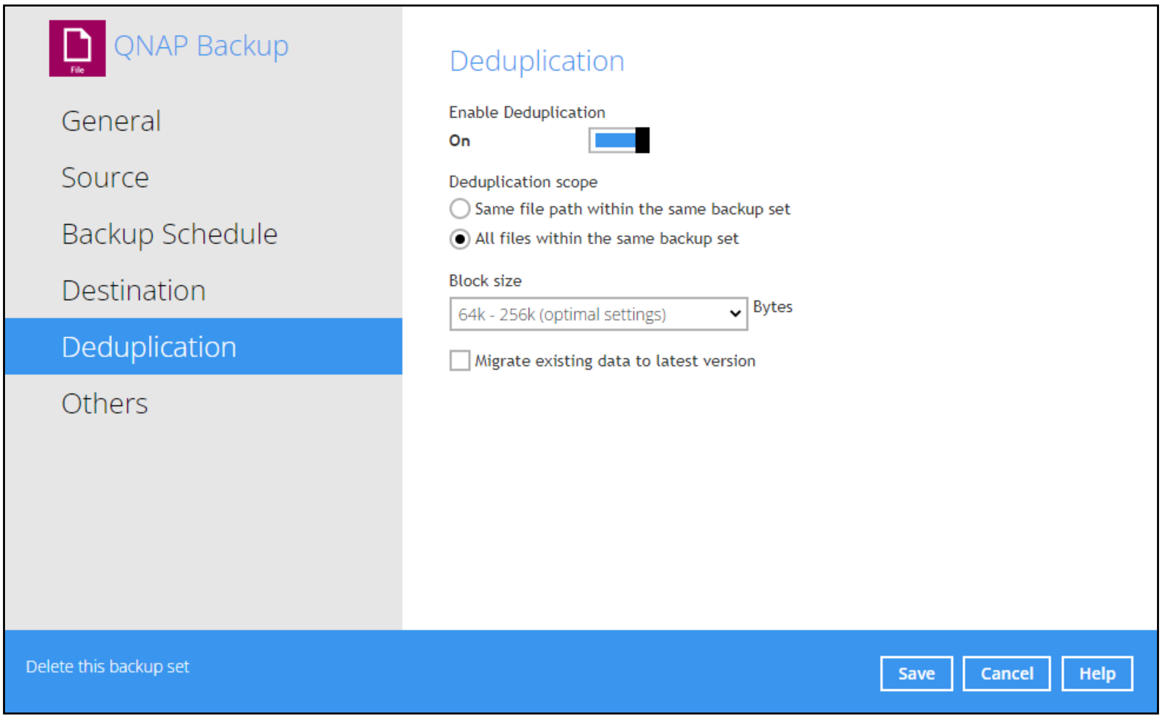
5. Click the **Save** button to save the changes made.

Deduplication

Starting with AhsayOBM v9.0.0.0 or above, the In-File Delta feature (i.e., Incremental, Differential and Full) will be replaced with Deduplication. This feature is **On (enabled)** by default.

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

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



Deduplication

Enable Deduplication
On

Deduplication scope
○ Same file path within the same backup set
● All files within the same backup set

Block size
64k - 256k (optimal settings) Bytes

□ Migrate existing data to latest version

There are two types of deduplication scope:

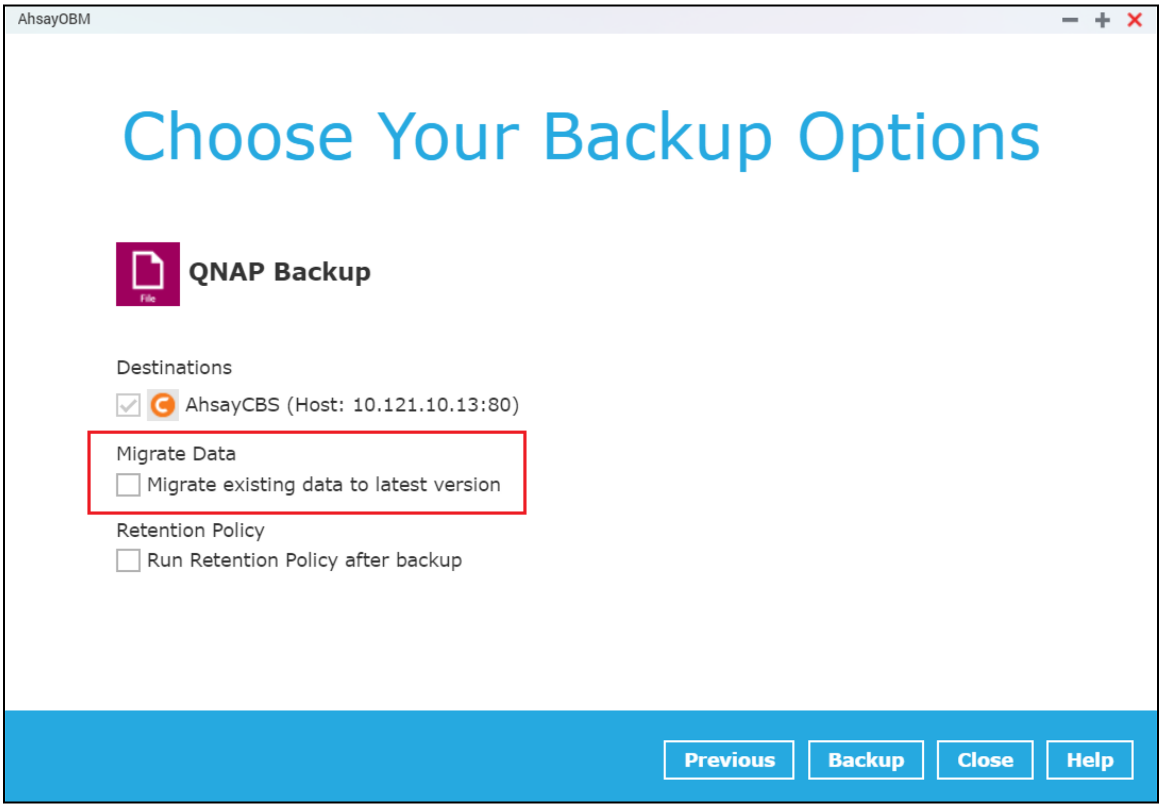
- Same file path within the same backup set – deduplication will be applied to the contents within a file during the current backup job.
- All files within the same backup set – deduplication will be applied across the different files in the backup set.

NOTE

For more details about the **Deduplication** feature, refer to the AhsayCBS v9 New Features Supplemental document.

When the Deduplication feature is enabled for the backup set, a **Migrate Data** option will be available in the advanced backup options which can be configured before starting a backup job.

Below is an example of a backup set with Deduplication setting enabled.

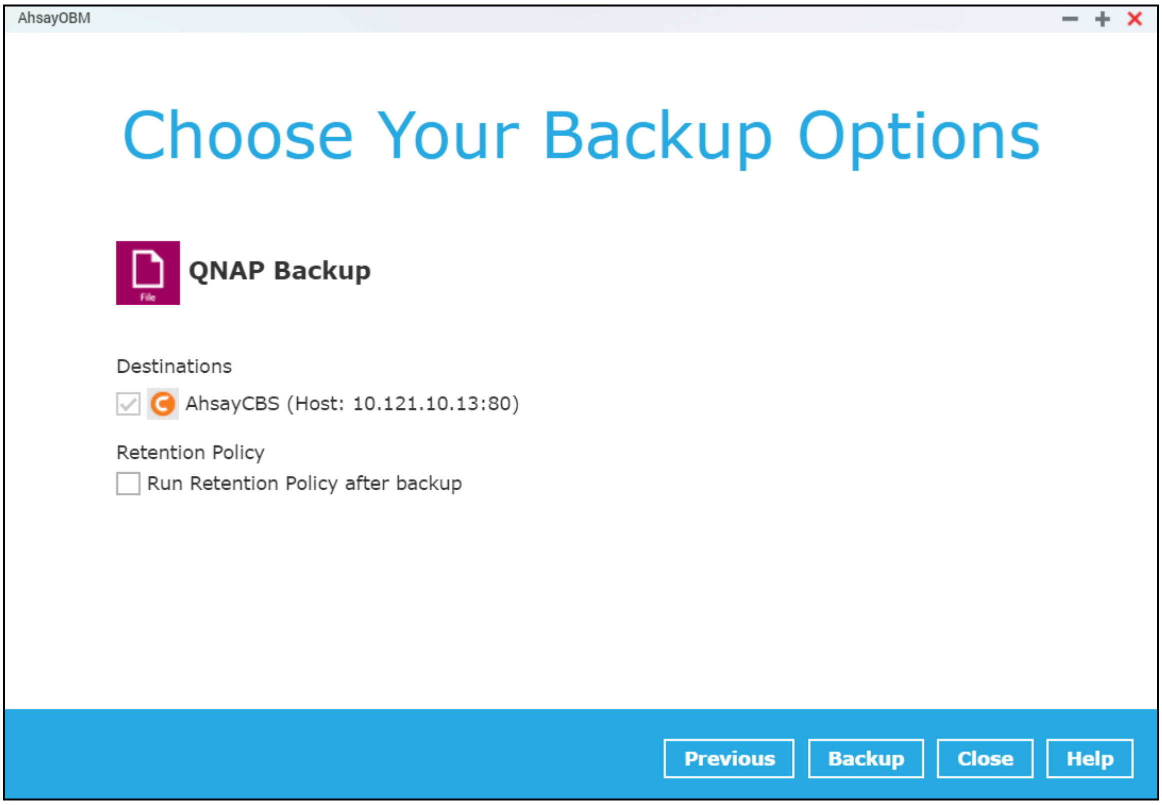

AhsayOBM
Choose Your Backup Options
QNAP Backup
Destinations
☑ AhsayCBS (Host: 10.121.10.13:80)
Migrate Data
□ Migrate existing data to latest version
Retention Policy
□ Run Retention Policy after backup
Previous
Backup
Close
Help

Migrate Data

When this option is enabled, the existing data will be migrated to the latest version during a backup job. This option is disabled by default.

NOTE
In case the Deduplication setting is **Off (disabled)** for the backup set, the Migrate Data option will not be displayed.

Below is an example of a backup set with Deduplication setting **Off (disabled)**.



Destinations

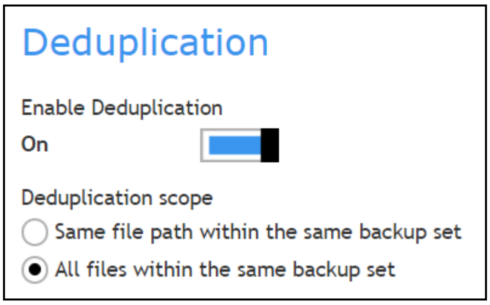
☑ AhsayCBS (Host: 10.121.10.13:80)

Retention Policy

□ Run Retention Policy after backup

To configure the Deduplication settings, follow the steps below:

1. Select a type of Deduplication scope.



Enable Deduplication

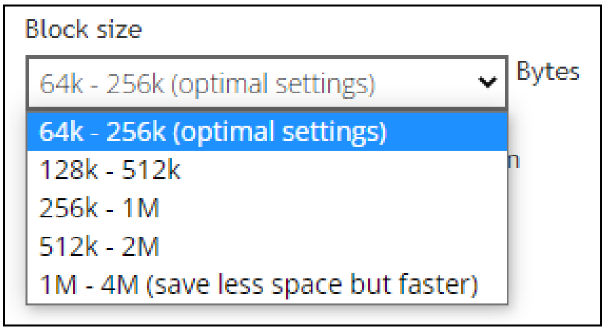
On

Deduplication scope

○ Same file path within the same backup set

● All files within the same backup set

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

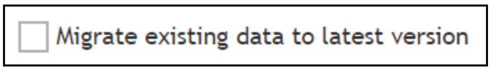


Block size

64k - 256k (optimal settings) Bytes

64k - 256k (optimal settings)
128k - 512k
256k - 1M
512k - 2M
1M - 4M (save less space but faster)

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



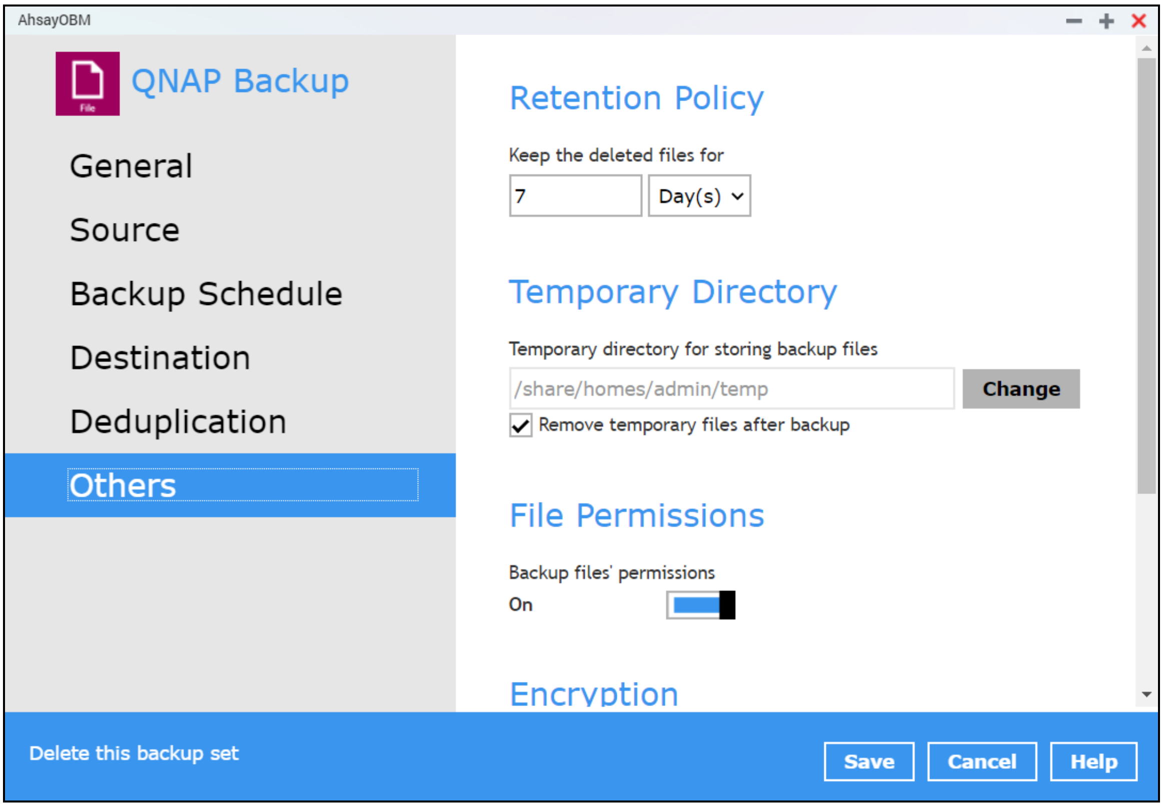
□ Migrate existing data to latest version

4. Click the **Save** button to store the modified Deduplication settings.

Others

These are the list of other backup set settings that can be configured.

- Retention Policy
- Temporary Directory
- File Permissions
- Encryption
- Recycle Bin



Retention Policy

Keep the deleted files for

7 Day(s)

Temporary Directory

Temporary directory for storing backup files

/share/homes/admin/temp Change

☑ Remove temporary files after backup

File Permissions

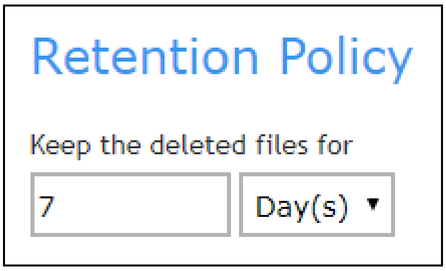
Backup files' permissions

On

Encryption

Retention Policy

This allows the user to retain the deleted files based on the selected retention type policy.



Retention Policy

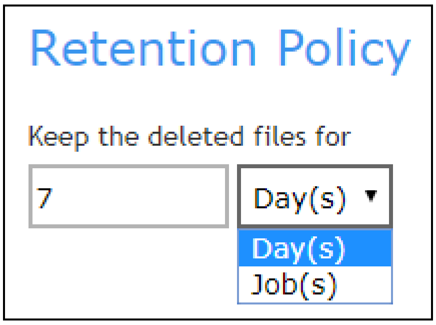
Keep the deleted files for

7 Day(s) ▼

To modify the retention policy, follow the instructions below:

1. Select **Others**.

2. On the right side of the screen, select from the two (2) options: Day(s) or Job(s).



Retention Policy

Keep the deleted files for

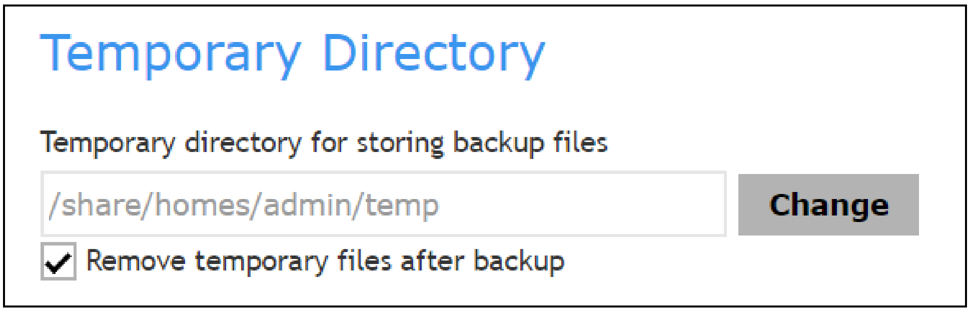
7 Day(s) ▼

3. Input a valid number for the Day(s) or Job(s).

4. Click the **Save** button to save the settings made.

Temporary Directory

This allows the user to configure the temporary directory of spooled files, remote file list, and other temporary backup files.



Temporary Directory

Temporary directory for storing backup files

/share/homes/admin/temp

☑ Remove temporary files after backup

To configure the temporary directory, follow the instructions below:

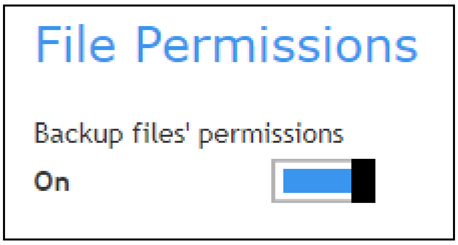
1. Click the **Change** button to select a directory path for storing the temporary data.

2. You also have an option to check or uncheck the “Remove temporary files after backup”.

3. Click the **Save** button to save the settings.

File Permissions

This allows the user to enable or disable the backup file permission which backups the operating system file permission of the data selected as backup source.



File Permissions

Backup files' permissions

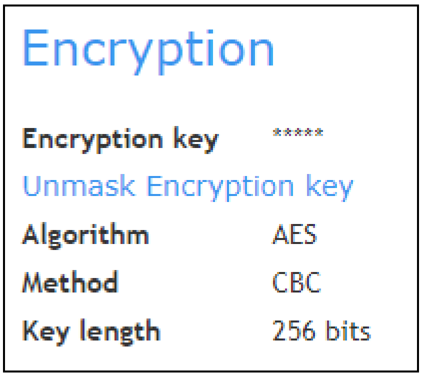
On

1. Slide the lever to the right to turn on the File Permissions option. Otherwise, slide to the left to turn it off.

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

Encryption

This allows the user to view the current encryption settings. For more details about the encryption, check Chapter 9 Creating a File Backup Set.



Encryption

Encryption key	*****
Unmask Encryption key	
Algorithm	AES
Method	CBC
Key length	256 bits

Recycle Bin

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

This is how the Recycle Bin will treat deleted data:

- Data in the Recycle Bin will consume Quota.

- It does not move the data in another location within the storage, instead the index tracks the xxxxxx.bak files and the remaining time in the Recycle Bin.

- If the index is reverted to a previous timestamp, the settings of the Recycle Bin in the reverted index will be followed.

- Recoverability of data is not affected when the Recycle Bin is alternately enabled or disabled.

  - When enabled, it will only check if the data inside the Recycle Bin is still within the set number of days. Once it is beyond the set number of days it will only be deleted when the following operations are run: Backup, Space Freeing Up, Data Integrity Check and Delete Backup Data.

  - When disabled, if there are already deleted files it will not automatically delete the data inside the Recycle Bin. It will remain in the Recycle Bin even if it is beyond the set number of days. It will only be deleted when the following operations are run: Backup, Space Freeing Up, Data Integrity Check and Delete Backup Data.

- Once the Recycle Bin is disabled, deleted files will be removed immediately and will not be moved in the Recycle Bin.

- The setting applies to all destinations for the backup set.

- Viewing Recycle Bin contents is not available.

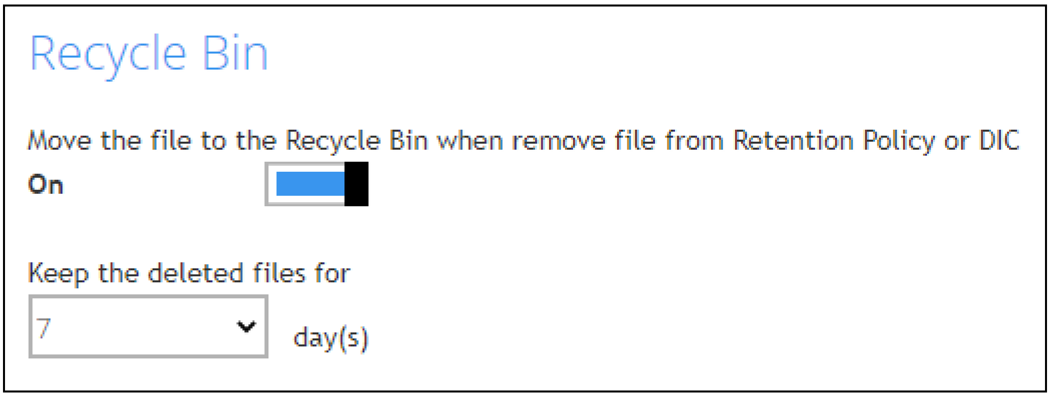
- Recycle Bin cleanup is done at the start of the backup job process.

- Recovering from Recycle Bin requires reverting the index. For instructions on how to revert the index please refer to this article: FAQ: How to un-delete backup data moved to Retention, or revert indexes to a healthy state from an earlier successful backup.

WARNING

When reverting index, new data will be lost.

This is enabled by default set with 7 days.



Recycle Bin

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

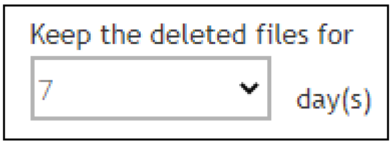
On

Keep the deleted files for

7 day(s)

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

1. Go to Backup Sets, then select a backup set.
2. Click the **Others** tab in the backup set settings.
3. Under Recycle Bin, select the number of days or you can enter it manually.

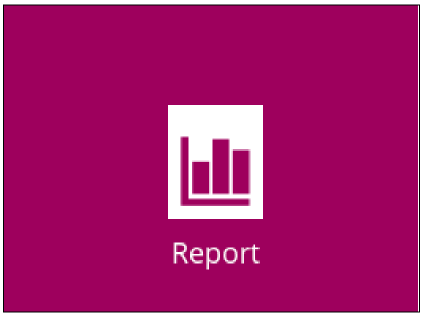


Keep the deleted files for

7 day(s)

8.7 Report

This feature allows user to run and view **backup** and **restore reports**.



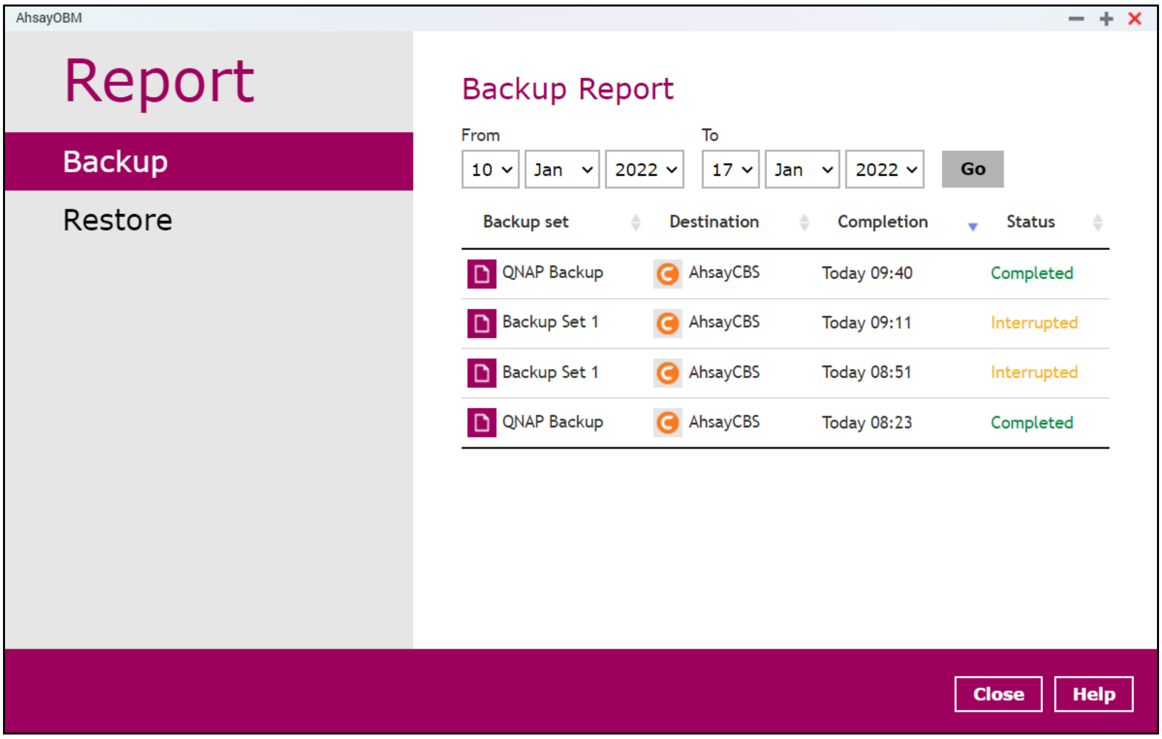
There are two (2) functions that are available for this feature:

- **Backup**
- **Restore**

8.7.1 Backup

This feature is used for viewing backup report(s). There are four (4) filters that can be applied on this feature, namely:

- Date Range
- Backup set
- Destination
- Status

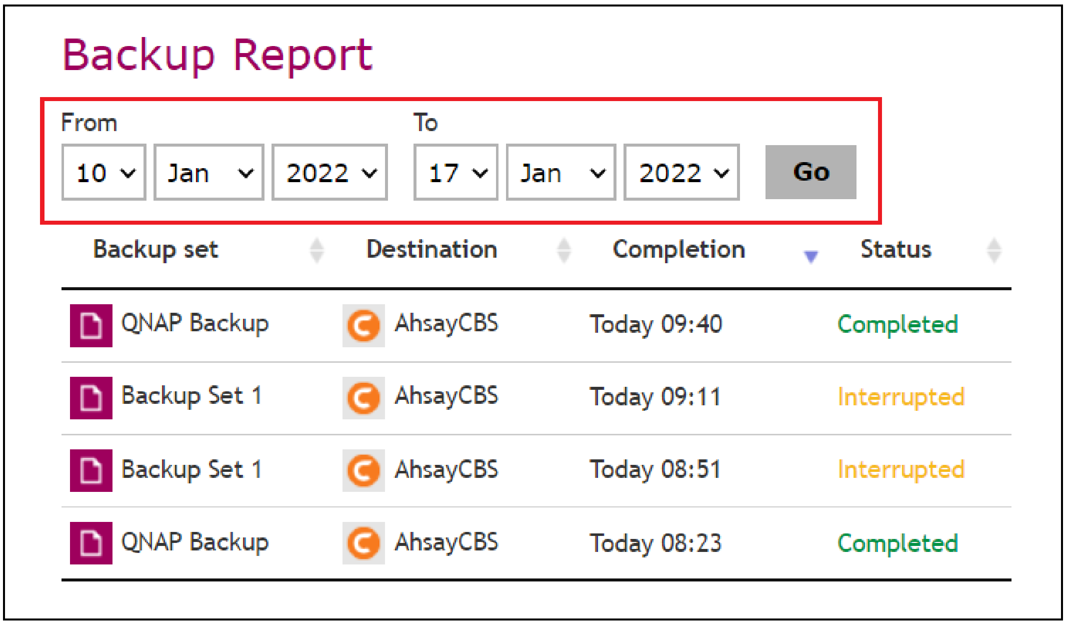


Backup Report

From 10 Jan 2022 To 17 Jan 2022 Go

Backup set	Destination	Completion	Status
QNAP Backup	AhsayCBS	Today 09:40	Completed
Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted
QNAP Backup	AhsayCBS	Today 08:23	Completed

By setting the **Date Range**, you will see the list of all backup report(s) within that period.

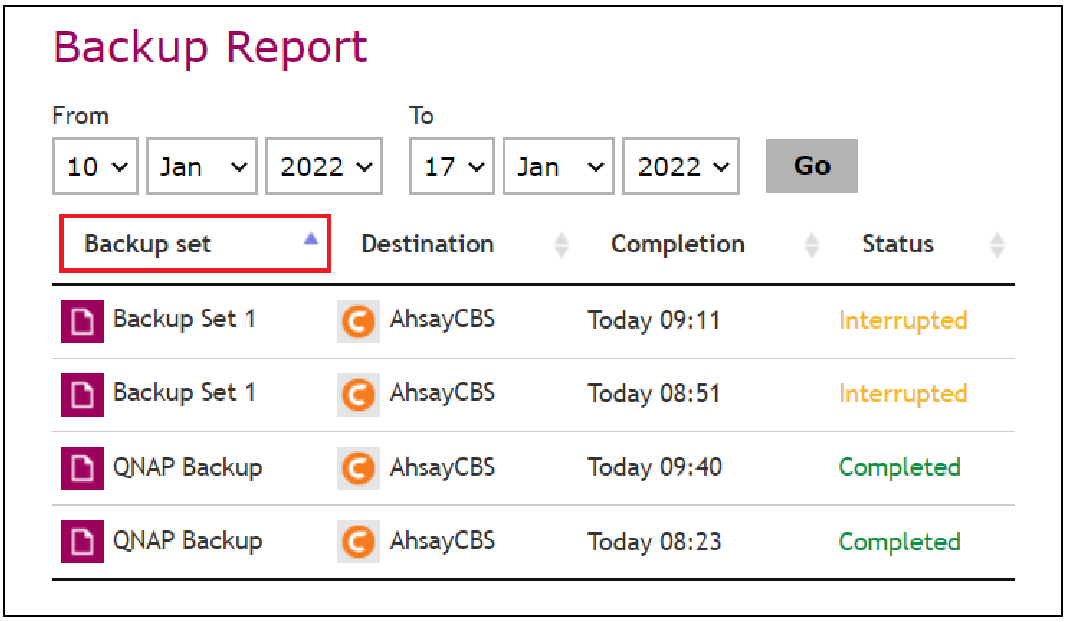


Backup Report

From: 10 Jan 2022 To: 17 Jan 2022 Go

Backup set	Destination	Completion	Status
QNAP Backup	AhsayCBS	Today 09:40	Completed
Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted
QNAP Backup	AhsayCBS	Today 08:23	Completed

Backup report(s) can be sorted alphabetically by using the **Backup up set** filter.

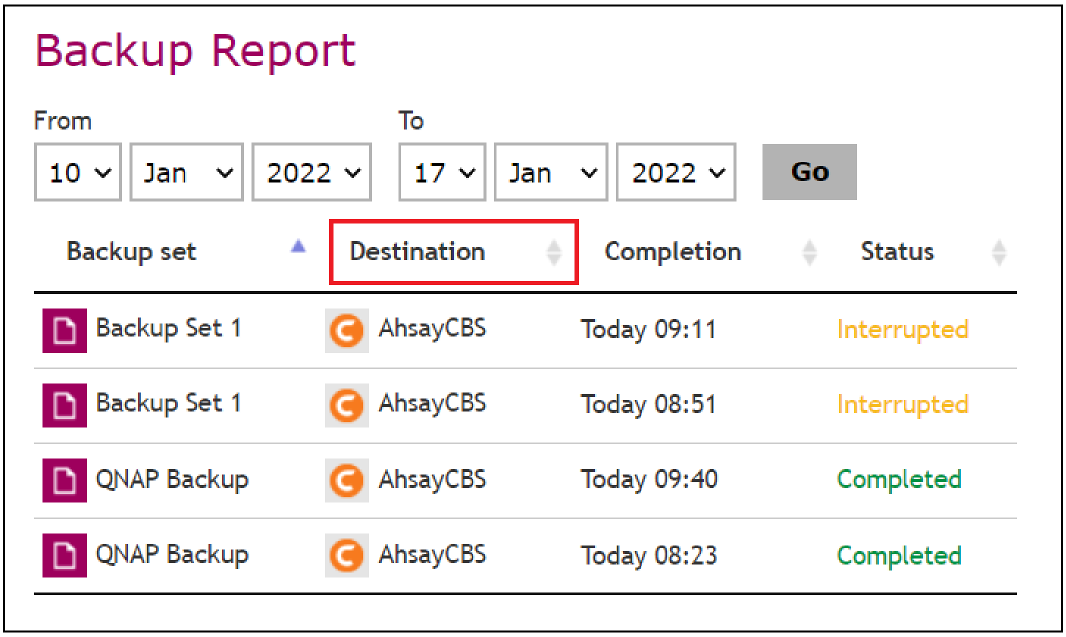


Backup Report

From: 10 Jan 2022 To: 17 Jan 2022 Go

Backup set	Destination	Completion	Status
Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted
QNAP Backup	AhsayCBS	Today 09:40	Completed
QNAP Backup	AhsayCBS	Today 08:23	Completed

You can view all the backup report(s) in your storage location by sorting the **Destination** filter.

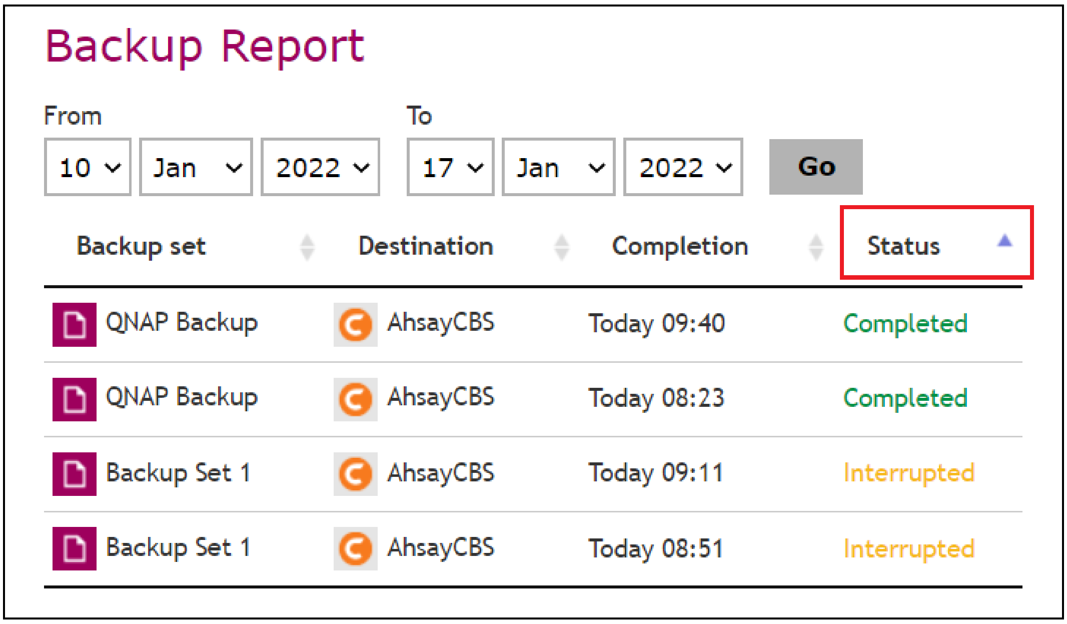


Backup Report

From 10 Jan 2022 To 17 Jan 2022 Go

Backup set	Destination	Completion	Status
Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted
QNAP Backup	AhsayCBS	Today 09:40	Completed
QNAP Backup	AhsayCBS	Today 08:23	Completed

You can sort backup reports with the same status by using the **Status** filter.

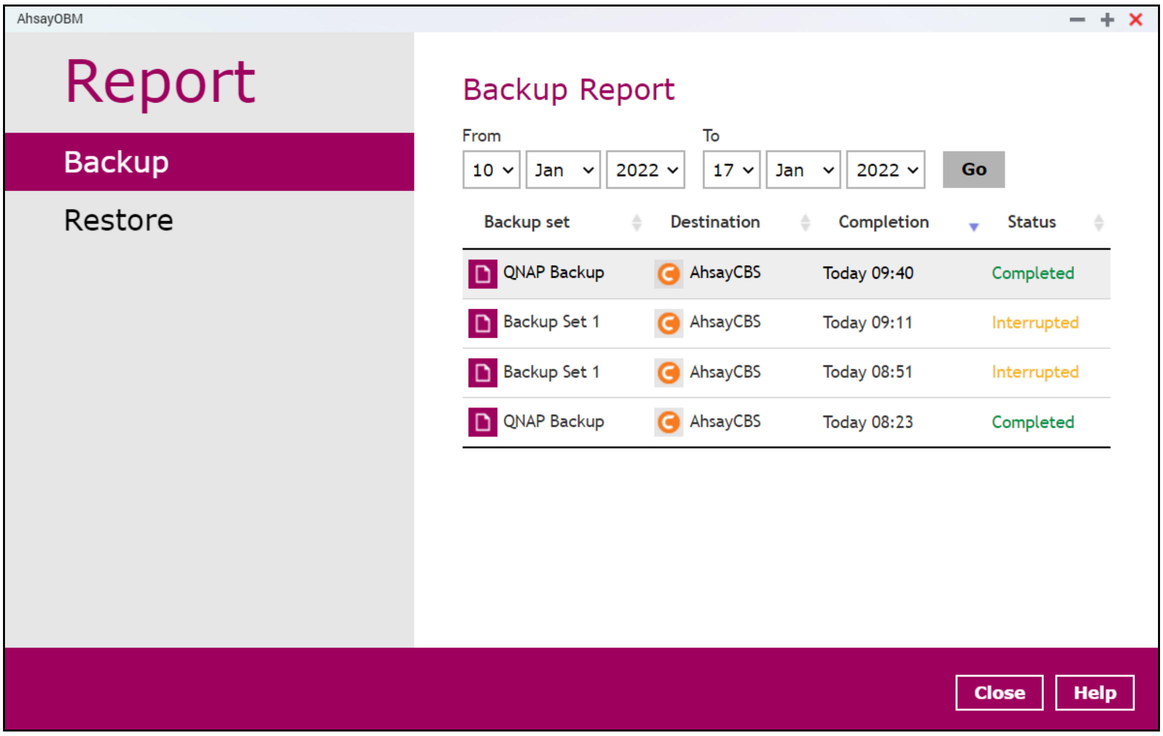


Backup Report

From 10 Jan 2022 To 17 Jan 2022 Go

Backup set	Destination	Completion	Status
QNAP Backup	AhsayCBS	Today 09:40	Completed
QNAP Backup	AhsayCBS	Today 08:23	Completed
Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted

To view a backup report in detail, choose a specific backup set.

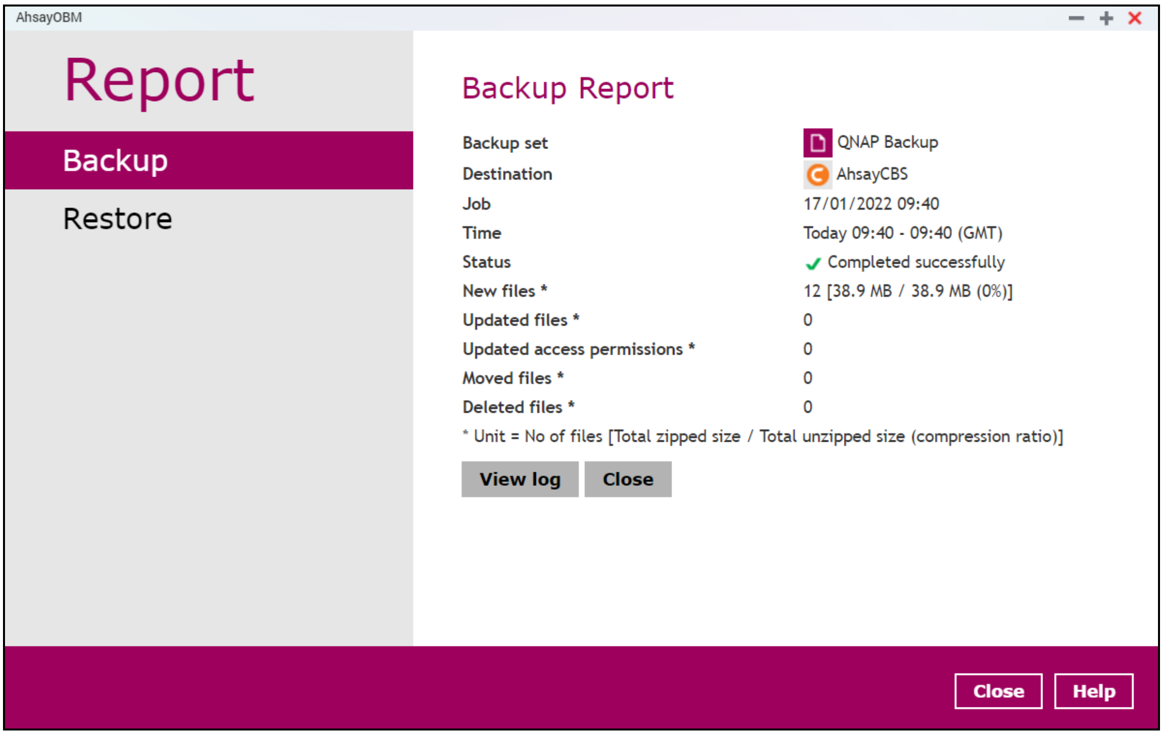


Backup Report

From 10 Jan 2022 To 17 Jan 2022 Go

Backup set	Destination	Completion	Status
QNAP Backup	AhsayCBS	Today 09:40	Completed
Backup Set 1	AhsayCBS	Today 09:11	Interrupted
Backup Set 1	AhsayCBS	Today 08:51	Interrupted
QNAP Backup	AhsayCBS	Today 08:23	Completed

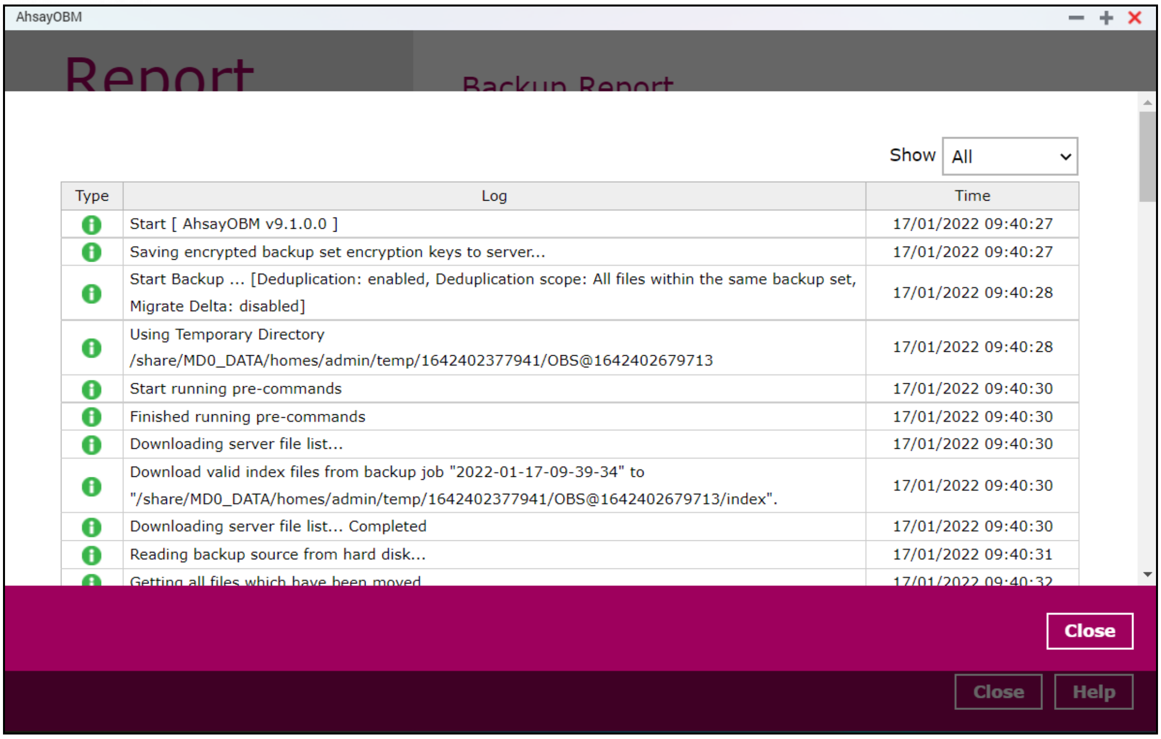
Click **View log** to show the event log during a backup.



Backup Report

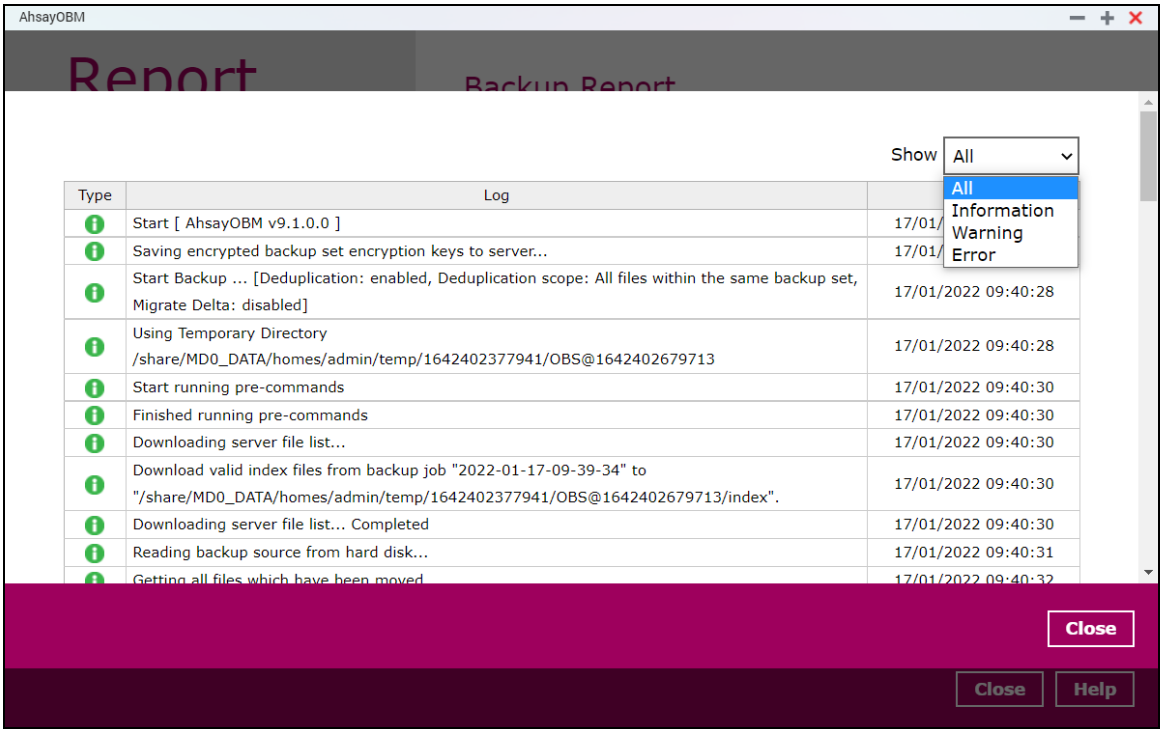
Backup set	QNAP Backup
Destination	AhsayCBS
Job	17/01/2022 09:40
Time	Today 09:40 - 09:40 (GMT)
Status	✓ Completed successfully
New files *	12 [38.9 MB / 38.9 MB (0%)]
Updated files *	0
Updated access permissions *	0
Moved files *	0
Deleted files *	0

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



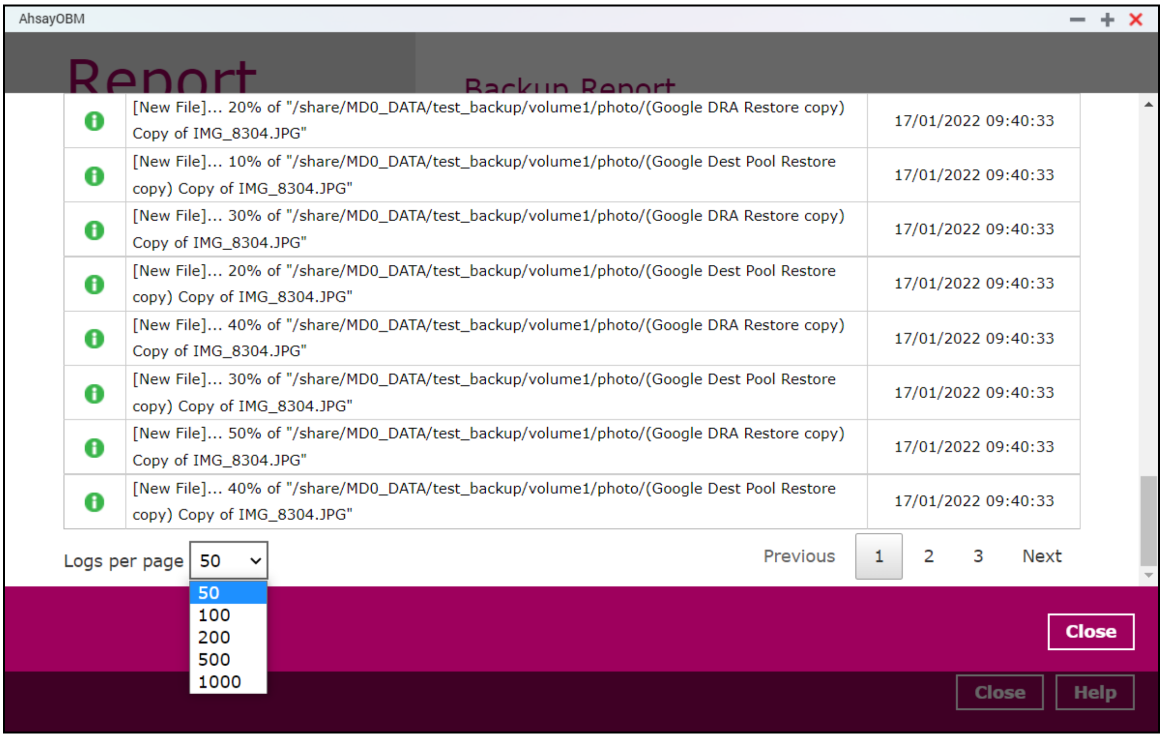
Type	Log	Time
ⓘ	Start [AhsayOBM v9.1.0.0]	17/01/2022 09:40:27
ⓘ	Saving encrypted backup set encryption keys to server...	17/01/2022 09:40:27
ⓘ	Start Backup ... [Deduplication: enabled, Deduplication scope: All files within the same backup set, Migrate Delta: disabled]	17/01/2022 09:40:28
ⓘ	Using Temporary Directory /share/MD0_DATA/homes/admin/temp/1642402377941/OBS@1642402679713	17/01/2022 09:40:28
ⓘ	Start running pre-commands	17/01/2022 09:40:30
ⓘ	Finished running pre-commands	17/01/2022 09:40:30
ⓘ	Downloading server file list...	17/01/2022 09:40:30
ⓘ	Download valid index files from backup job "2022-01-17-09-39-34" to "/share/MD0_DATA/homes/admin/temp/1642402377941/OBS@1642402679713/index".	17/01/2022 09:40:30
ⓘ	Downloading server file list... Completed	17/01/2022 09:40:30
ⓘ	Reading backup source from hard disk...	17/01/2022 09:40:31
ⓘ	Getting all files which have been moved	17/01/2022 09:40:32

You can apply filter on the status of the event by clicking the drop-down list.



Type	Log	
ⓘ	Start [AhsayOBM v9.1.0.0]	17/01/
ⓘ	Saving encrypted backup set encryption keys to server...	17/01/
ⓘ	Start Backup ... [Deduplication: enabled, Deduplication scope: All files within the same backup set, Migrate Delta: disabled]	17/01/2022 09:40:28
ⓘ	Using Temporary Directory /share/MD0_DATA/homes/admin/temp/1642402377941/OBS@1642402679713	17/01/2022 09:40:28
ⓘ	Start running pre-commands	17/01/2022 09:40:30
ⓘ	Finished running pre-commands	17/01/2022 09:40:30
ⓘ	Downloading server file list...	17/01/2022 09:40:30
ⓘ	Download valid index files from backup job "2022-01-17-09-39-34" to "/share/MD0_DATA/homes/admin/temp/1642402377941/OBS@1642402679713/index".	17/01/2022 09:40:30
ⓘ	Downloading server file list... Completed	17/01/2022 09:40:30
ⓘ	Reading backup source from hard disk...	17/01/2022 09:40:31
ⓘ	Getting all files which have been moved	17/01/2022 09:40:32

You can choose to view the number of logs per page by clicking the drop-down list.

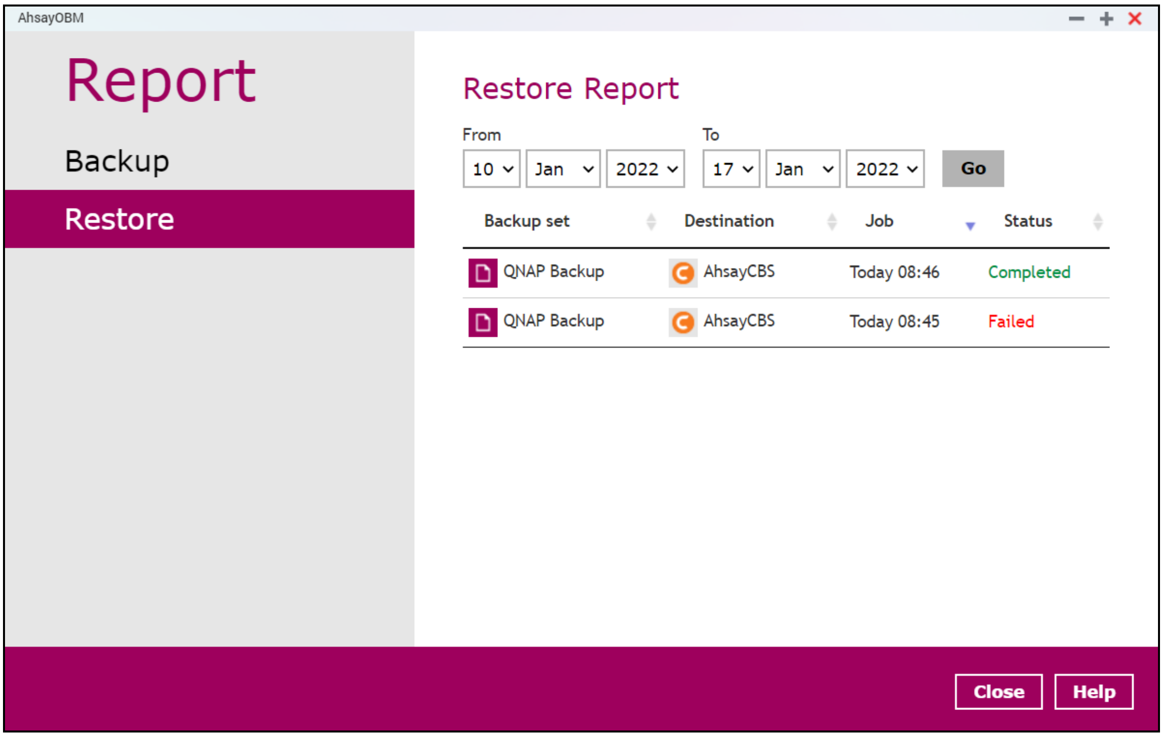


ⓘ	[New File]... 20% of "/share/MD0_DATA/test_backup/volume1/photo/(Google DRA Restore copy) Copy of IMG_8304.JPG"	17/01/2022 09:40:33
ⓘ	[New File]... 10% of "/share/MD0_DATA/test_backup/volume1/photo/(Google Dest Pool Restore copy) Copy of IMG_8304.JPG"	17/01/2022 09:40:33
ⓘ	[New File]... 30% of "/share/MD0_DATA/test_backup/volume1/photo/(Google DRA Restore copy) Copy of IMG_8304.JPG"	17/01/2022 09:40:33
ⓘ	[New File]... 20% of "/share/MD0_DATA/test_backup/volume1/photo/(Google Dest Pool Restore copy) Copy of IMG_8304.JPG"	17/01/2022 09:40:33
ⓘ	[New File]... 40% of "/share/MD0_DATA/test_backup/volume1/photo/(Google DRA Restore copy) Copy of IMG_8304.JPG"	17/01/2022 09:40:33
ⓘ	[New File]... 30% of "/share/MD0_DATA/test_backup/volume1/photo/(Google Dest Pool Restore copy) Copy of IMG_8304.JPG"	17/01/2022 09:40:33
ⓘ	[New File]... 50% of "/share/MD0_DATA/test_backup/volume1/photo/(Google DRA Restore copy) Copy of IMG_8304.JPG"	17/01/2022 09:40:33
ⓘ	[New File]... 40% of "/share/MD0_DATA/test_backup/volume1/photo/(Google Dest Pool Restore copy) Copy of IMG_8304.JPG"	17/01/2022 09:40:33

Logs per page: 50

8.7.2 Restore

This feature is used for viewing restore report(s). You can also apply filter on **Date Range**, **Backup set**, **Destination** and **Status** here.

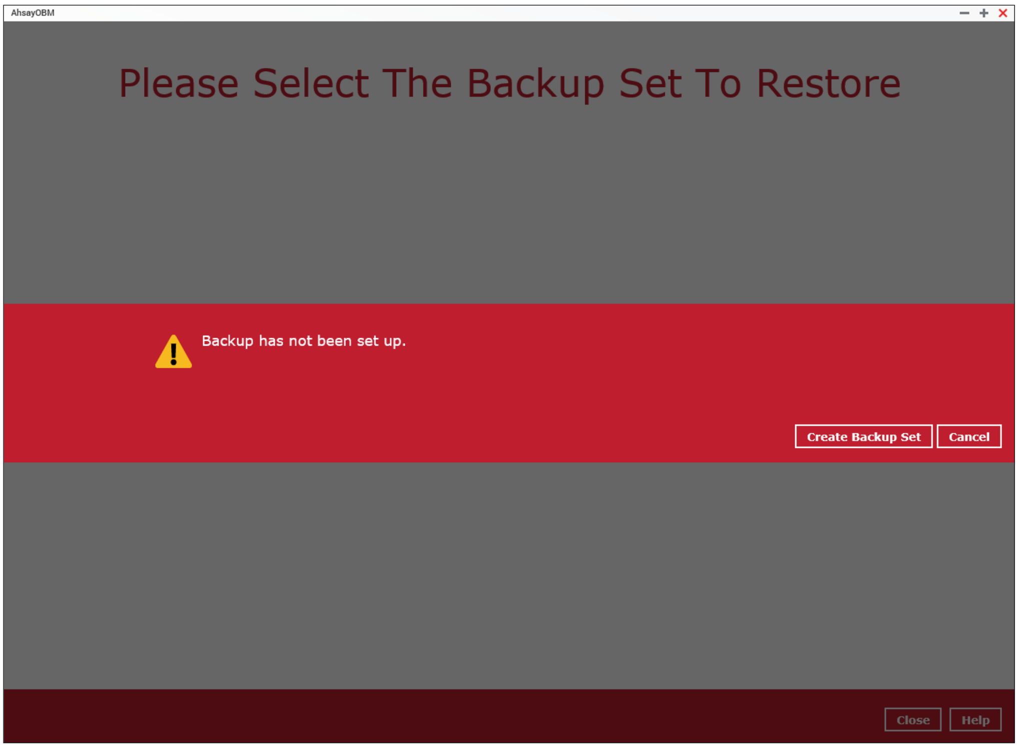


Backup set	Destination	Job	Status
QNAP Backup	AhsayCBS	Today 08:46	Completed
QNAP Backup	AhsayCBS	Today 08:45	Failed

8.8 Restore

This feature is used to copy the backed-up file(s) from the backup set and restoring it to its original location or new location.

If using AhsayOBM for the first time, you will be asked to create a backup set first. A restore cannot be performed unless you already run a backup.

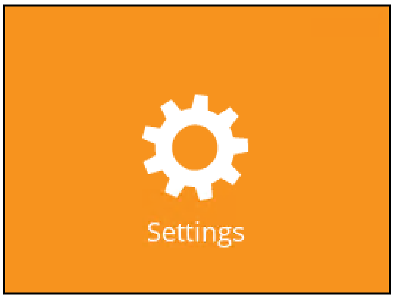


Backup has not been set up.

For instructions on how to perform a restore, refer to Chapter 12 Restore Data.

8.9 Settings

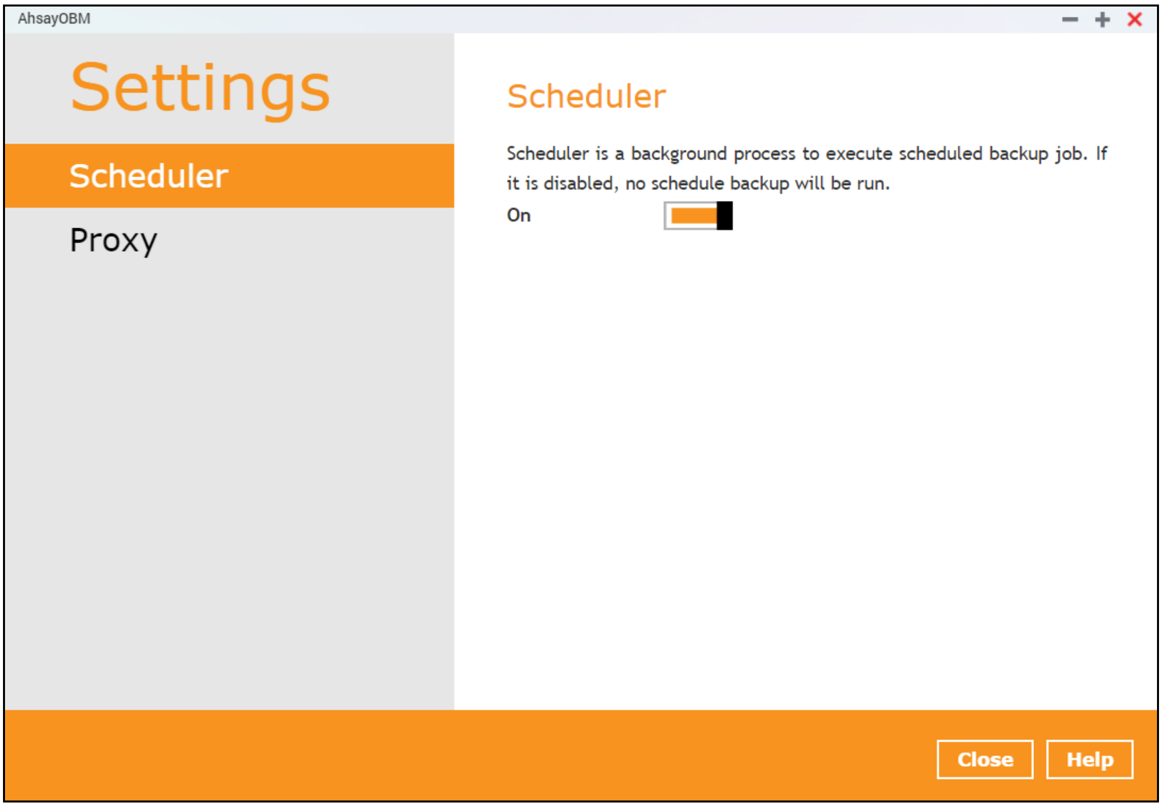
This feature allows user to enable the **Scheduler** and **Proxy Settings**.



8.9.1 Scheduler

The Scheduler setting was for AhsayOBM pre-v9.3.2.0 and has been removed.

When this feature is on, the user can execute a **scheduled backup** job. Otherwise, no scheduled backup will run.



Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

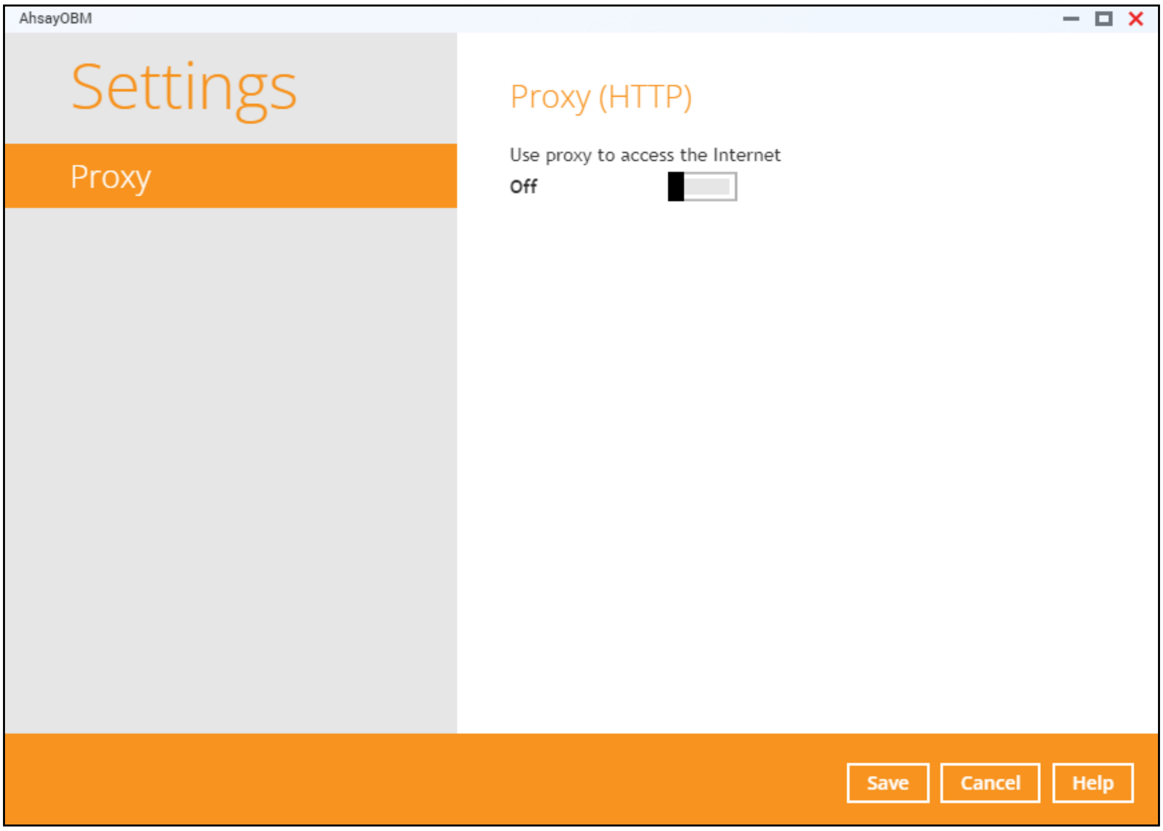
On

NOTE

For more details on the scenario for the Scheduler under Settings, refer to Appendix C: Scheduler Scenarios.

8.9.2 Proxy

This feature is used to allow AhsayOBM to gain access to the internet.



Proxy (HTTP)

Use proxy to access the Internet

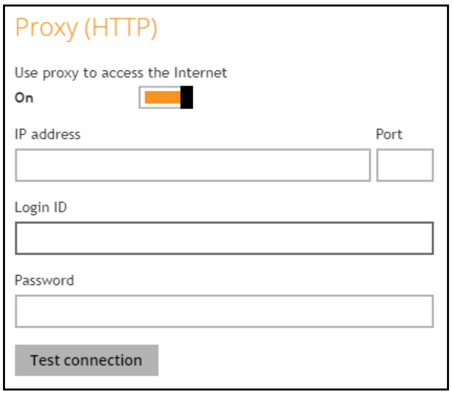
Off

To enable the Proxy settings, follow the instructions below:

1. Slide the lever to the right to turn on this feature.

2. Complete the following fields:

   - IP address
   - Port
   - Login ID
   - Password



Proxy (HTTP)

Use proxy to access the Internet

On

IP address

Port

Login ID

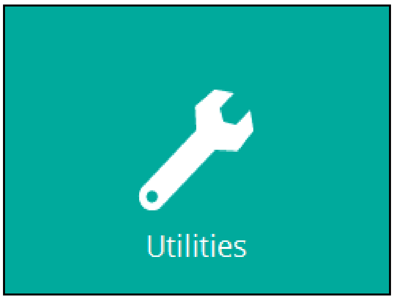
Password

3. Click the **Test connection** button to validate the connection.

4. Click the **Save** button to apply the settings.

8.10 Utilities

This allows the user to perform quality check on the backed up data and delete backed up data.



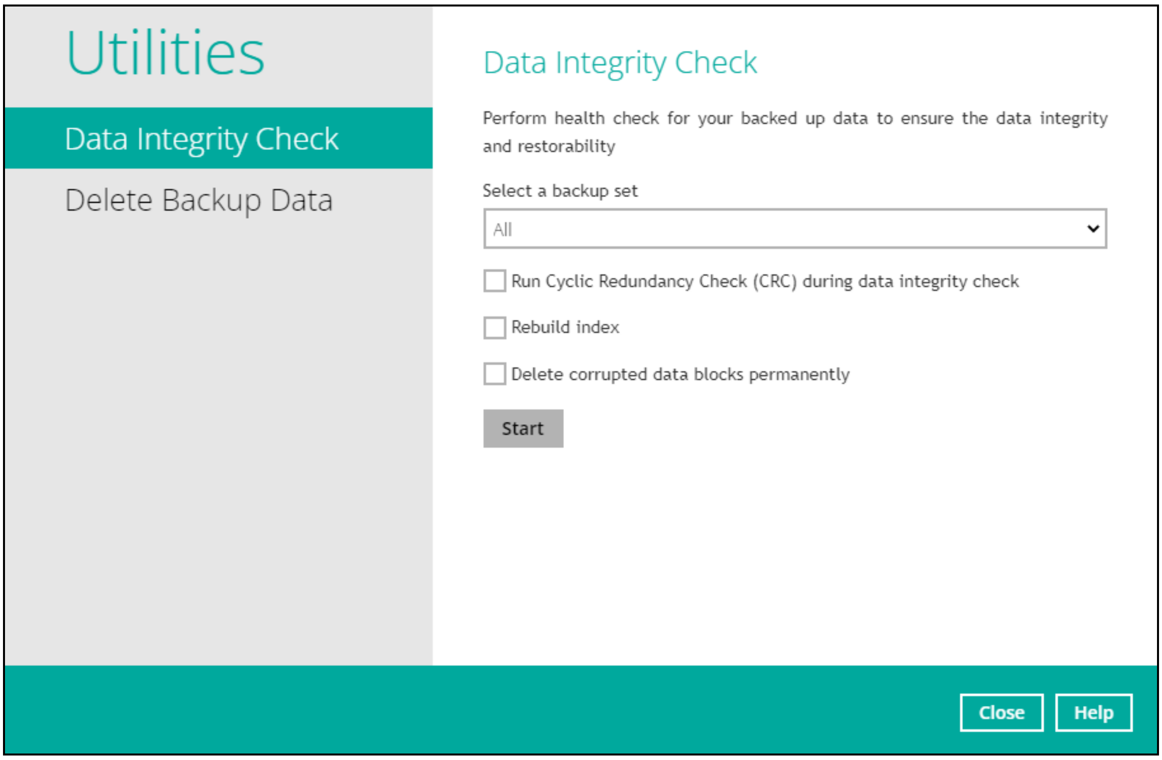
There are two (2) options available for this feature:

- Data Integrity Check
- Delete Backup Data

8.10.1 Data Integrity Check

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

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



Data Integrity Check

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

Select a backup set

All

□ Run Cyclic Redundancy Check (CRC) during data integrity check

□ Rebuild index

□ Delete corrupted data blocks permanently

NOTES

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

Run Cyclic Redundancy Check (CRC)

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

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

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

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

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

NOTE

For user(s) with metered internet connection, additional data charges may be incurred if the Cyclic Redundancy Check (CRC) is enabled. As the Cyclic Redundancy Check data involves downloading the data from the backup destination(s) to the client machine in order to perform this check.

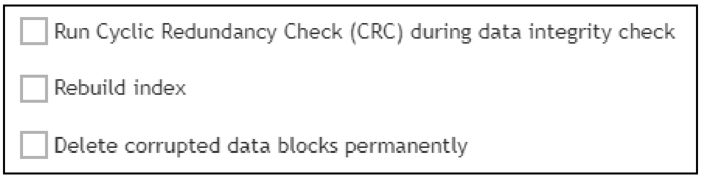
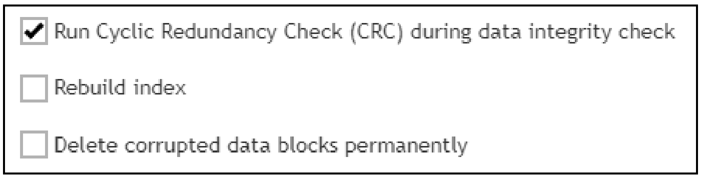
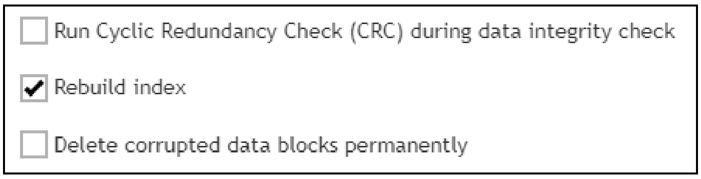
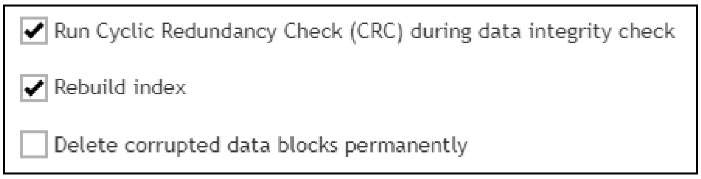
Rebuild index

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

Delete corrupted data blocks permanently

When this option is enabled, it overrides the Recycle Bin setting of the backup set. The DIC will delete corrupted data blocks permanently instead of moving it to the Recycle Bin.

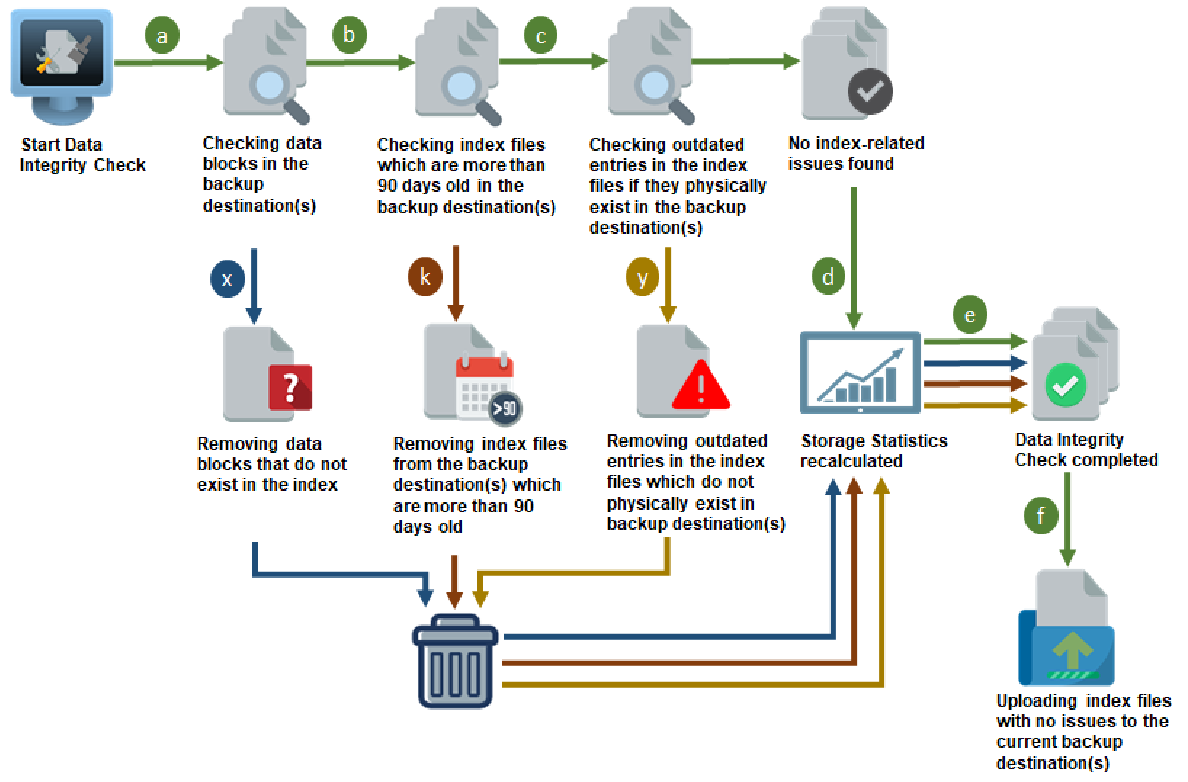
There are four (4) options in performing the DIC:

Settings	Function
Option 1  □ Run Cyclic Redundancy Check (CRC) during data integrity check □ Rebuild index □ Delete corrupted data blocks permanently	For checking of index and data.
Option 2  ☑ Run Cyclic Redundancy Check (CRC) during data integrity check □ Rebuild index □ Delete corrupted data blocks permanently	For checking of index and integrity of files against the checksum file generated at the time of the backup job.
Option 3  □ Run Cyclic Redundancy Check (CRC) during data integrity check ☑ Rebuild index □ Delete corrupted data blocks permanently	For checking and rebuilding of index.
Option 4  ☑ Run Cyclic Redundancy Check (CRC) during data integrity check ☑ Rebuild index □ Delete corrupted data blocks permanently	For checking of index, integrity of files against the checksum file generated at the time of the backup job and rebuilding of index.

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

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

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


a
b
c
Start Data Integrity Check
Checking data blocks in the backup destination(s)
Checking index files which are more than 90 days old in the backup destination(s)
Checking outdated entries in the index files if they physically exist in the backup destination(s)
No index-related issues found
x
k
y
d
e
Removing data blocks that do not exist in the index
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Storage Statistics recalculated
Data Integrity Check completed
f
Uploading index files with no issues to the current backup destination(s)

a Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.

➔ If **YES**, proceed to b

➔ If **NO**, proceed to x

b Check the index files in the backup destination(s) to determine if they were more than 90 days old.

➔ If **YES**, proceed to k

➔ If **NO**, proceed to c

c Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).

➔ If **YES**, proceed to d

➔ If **NO**, proceed to y

d Storage Statistics for Data area and Retention area usage will be recalculated.

e Data integrity check is completed.

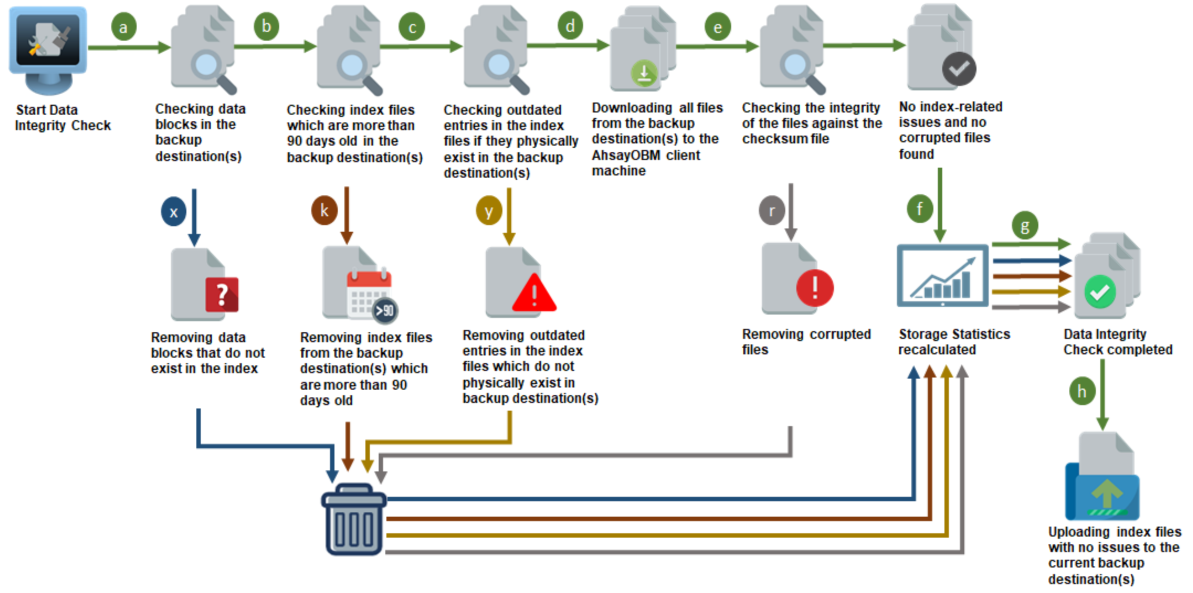
f Index files with no issues will be uploaded to the current backup destination(s).

x Data blocks (.bak files) that do not exist in the index and partially uploaded orphan files will be automatically removed from the backup destination(s).

k Index files which are more than 90 days old will be removed from the backup destination(s).

y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.

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



a
b
c
d
e
Start Data Integrity Check
Checking data blocks in the backup destination(s)
Checking index files which are more than 90 days old in the backup destination(s)
Checking outdated entries in the index files if they physically exist in the backup destination(s)
Downloading all files from the backup destination(s) to the AhsayOBM client machine
Checking the integrity of the files against the checksum file
No index-related issues and no corrupted files found
x
k
y
r
f
g
>90
Removing data blocks that do not exist in the index
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Removing corrupted files
Storage Statistics recalculated
Data Integrity Check completed
h
Uploading index files with no issues to the current backup destination(s)

a Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.

➔ If **YES**, proceed to b

➔ If **NO**, proceed to x

b Check the index files in the backup destination(s) to determine if they were more than 90 days old.

➔ If **YES**, proceed to k

➔ If **NO**, proceed to c

c Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).

➔ If **YES**, proceed to d

➔ If **NO**, proceed to y

d For **Run on Client (agent-based)** backup sets, files in the backup set are downloaded from the backup destination(s) to the AhsayOBM client machine.

For **Run on Server (agentless)** backup sets, proceed to e

e Check the integrity of files in the backup destination(s) against the checksum file generated at the time of the backup job.

➔ If any discrepancy is **FOUND**, proceed to r

➔ If **NO** discrepancy is found, proceed to f

f Storage Statistics for Data area and Retention area usage will be recalculated.

g Data integrity check is completed.

h Index files with no issues will be uploaded to the current backup destination(s).

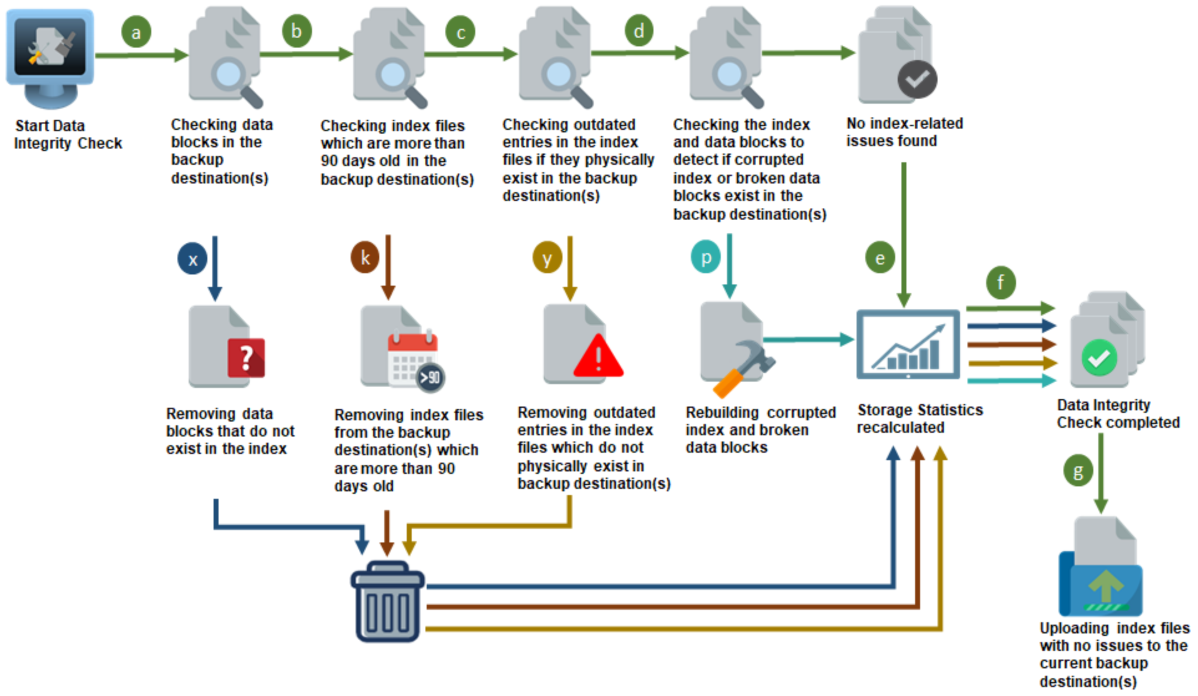
x Data blocks (.bak files) that do not exist in the index and partially uploaded orphan files will be automatically removed from the backup destination(s).

k Index files which are more than 90 days old will be removed from the backup destination(s).

y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.

r Corrupted files will be automatically removed from the backup destination(s).

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



a
b
c
d
Start Data Integrity Check
Checking data blocks in the backup destination(s)
Checking index files which are more than 90 days old in the backup destination(s)
Checking outdated entries in the index files if they physically exist in the backup destination(s)
Checking the index and data blocks to detect if corrupted index or broken data blocks exist in the backup destination(s)
No index-related issues found
x
k
y
p
e
f
>90
Removing data blocks that do not exist in the index
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Rebuilding corrupted index and broken data blocks
Storage Statistics recalculated
Data Integrity Check completed
g
Uploading index files with no issues to the current backup destination(s)

a Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.

➔ If **YES**, proceed to b

➔ If **NO**, proceed to x

b Check the index files in the backup destination(s) to determine if they were more than 90 days old.

➔ If **YES**, proceed to k

➔ If **NO**, proceed to c

c Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).

➔ If **YES**, proceed to d

➔ If **NO**, proceed to y

d Check the index and data blocks in the backup destination(s) to identify corrupted index and broken data blocks.

➔ If corrupted index and broken data blocks are **FOUND**, proceed to p

➔ If **NO** corrupted index and broken data blocks are **FOUND**, proceed to e

e Storage Statistics for Data area and Retention area usage will be recalculated.

f Data integrity check is completed.

g Index files with no issues will be uploaded to the current backup destination(s).

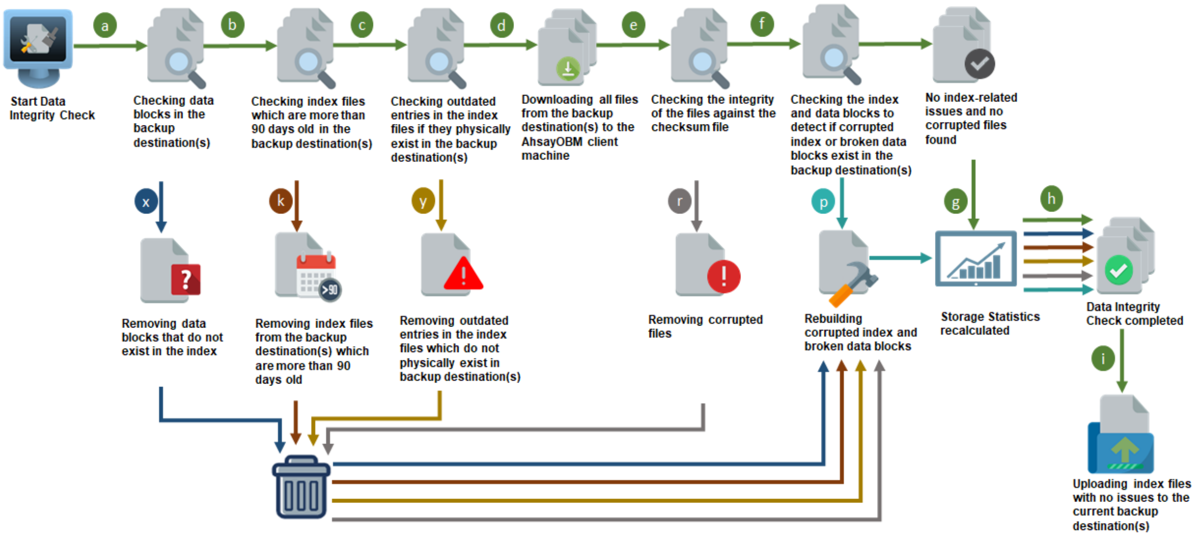
x Data blocks (.bak files) that do not exist in the index and partially uploaded orphan files will be automatically removed from the backup destination(s).

k Index files which are more than 90 days old will be removed from the backup destination(s).

y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.

p Corrupted index and broken data blocks (.bak files) identified will be rebuilt.

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


Start Data Integrity Check
a
Checking data blocks in the backup destination(s)
b
Checking index files which are more than 90 days old in the backup destination(s)
c
Checking outdated entries in the index files if they physically exist in the backup destination(s)
d
Downloading all files from the backup destination(s) to the AhsayOBM client machine
e
Checking the integrity of the files against the checksum file
f
Checking the index and data blocks to detect if corrupted index or broken data blocks exist in the backup destination(s)
No index-related issues and no corrupted files found
x
Removing data blocks that do not exist in the index
k
Removing index files from the backup destination(s) which are more than 90 days old
y
Removing outdated entries in the index files which do not physically exist in backup destination(s)
r
Removing corrupted files
p
Rebuilding corrupted index and broken data blocks
g
Storage Statistics recalculated
h
Data Integrity Check completed
i
Uploading index files with no issues to the current backup destination(s)

a Check the data blocks (.bak files) located in the backup destination(s) if they exist in the index.
→ If **YES**, proceed to b
→ If **NO**, proceed to x

b Check the index files in the backup destination(s) to determine if they were more than 90 days old.
→ If **YES**, proceed to k
→ If **NO**, proceed to c

c Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).
→ If **YES**, proceed to d
→ If **NO**, proceed to y

d For **Run on Client (agent-based)** backup sets, files in the backup set are downloaded from the backup destination(s) to the AhsayOBM client machine.
For **Run on Server (agentless)** backup sets, proceed to e

e Check the integrity of files in the backup destination(s) against the checksum file generated at the time of the backup job.
→ If any discrepancy is **FOUND**, proceed to r
→ If **NO** discrepancy is found, proceed to f

f Check the index and data blocks in the backup destination(s) to identify corrupted index and broken data blocks.
→ If corrupted index and broken data blocks are **FOUND**, proceed to p
→ If **NO** corrupted index and broken data blocks are found, proceed to g

g Storage Statistics for Data area and Retention area usage will be recalculated.

h Data integrity check is completed.

i Index files with no issues will be uploaded to the current backup destination(s).

x Data blocks (.bak files) that do not exist in the index and partially uploaded orphan files will be automatically removed from the backup destination(s).

k Index files which are more than 90 days old will be removed from the backup destination(s).

y Outdated entries in the index files for files and/or folders which do not physically exist in the backup destination(s) will be removed.

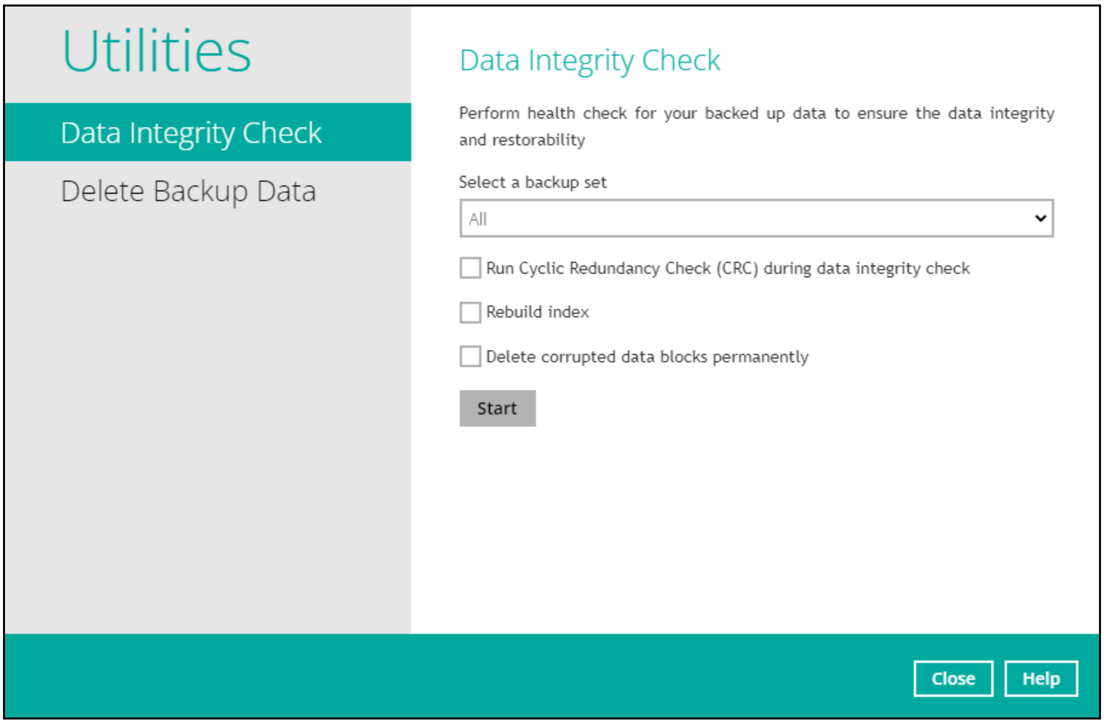
r Corrupted files will be automatically removed from the backup destination(s).

p Corrupted index and broken data blocks (.bak files) identified will be rebuilt.

Perform a Data Integrity Check

To perform a DIC, follow the instructions below:

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



Data Integrity Check

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

Select a backup set

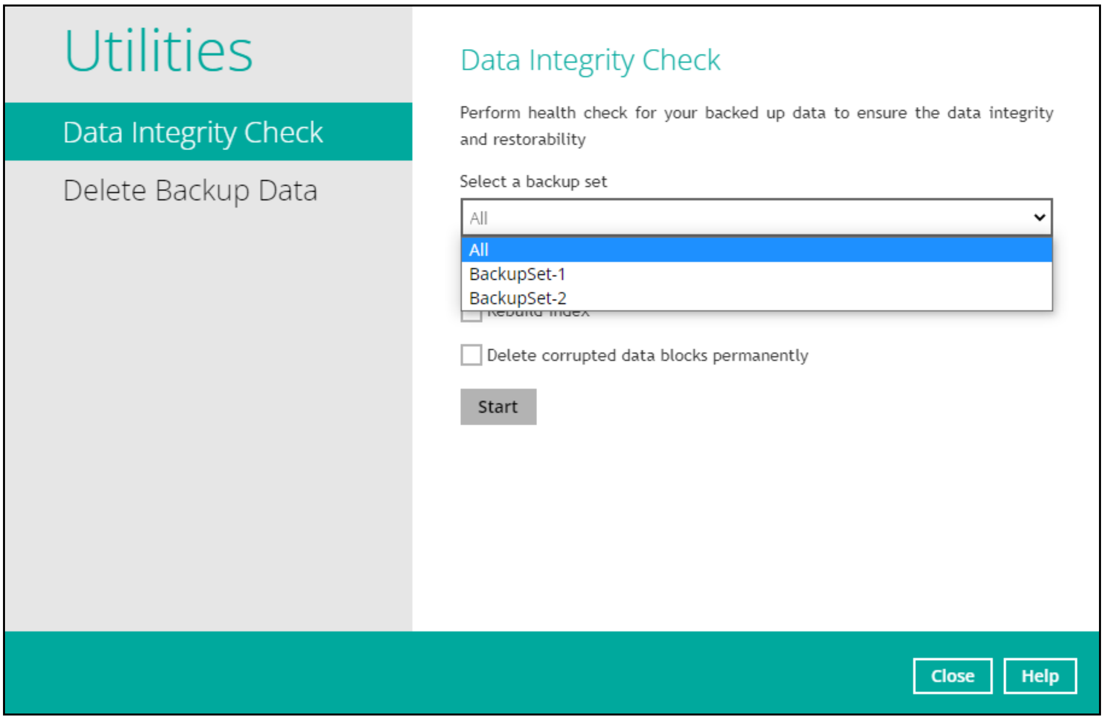
All

□ Run Cyclic Redundancy Check (CRC) during data integrity check

□ Rebuild index

□ Delete corrupted data blocks permanently

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



Data Integrity Check

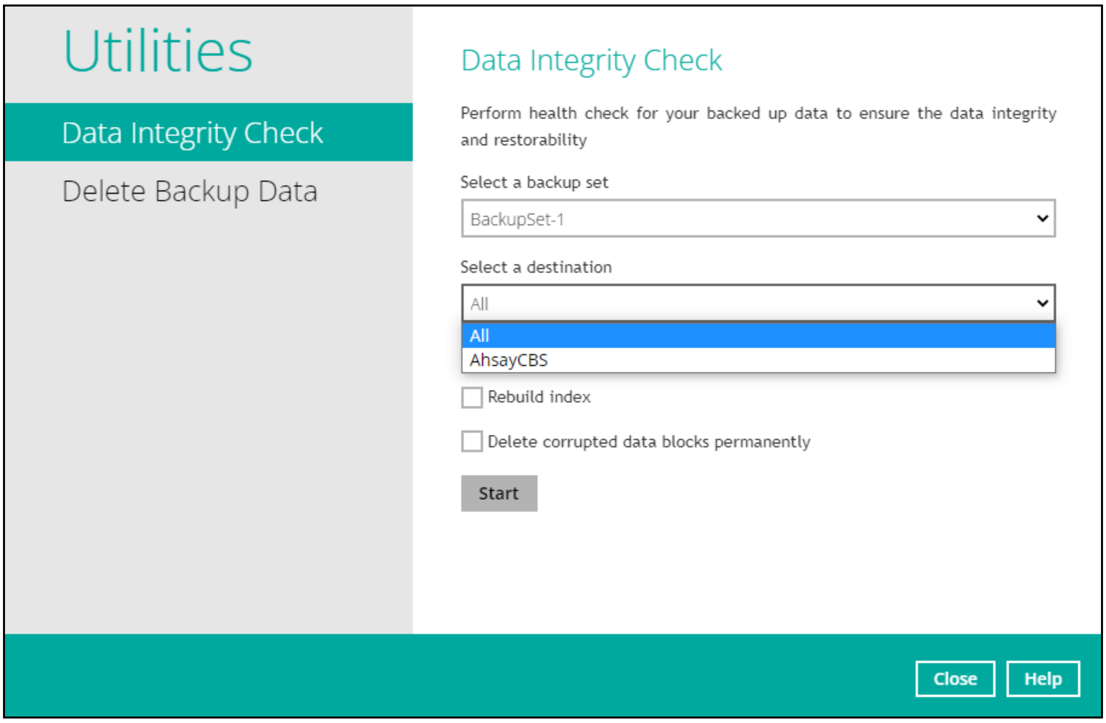
Perform health check for your backed up data to ensure the data integrity and restorability

Select a backup set

All

□ Delete corrupted data blocks permanently

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



Data Integrity Check

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

Select a backup set: BackupSet-1

Select a destination: All

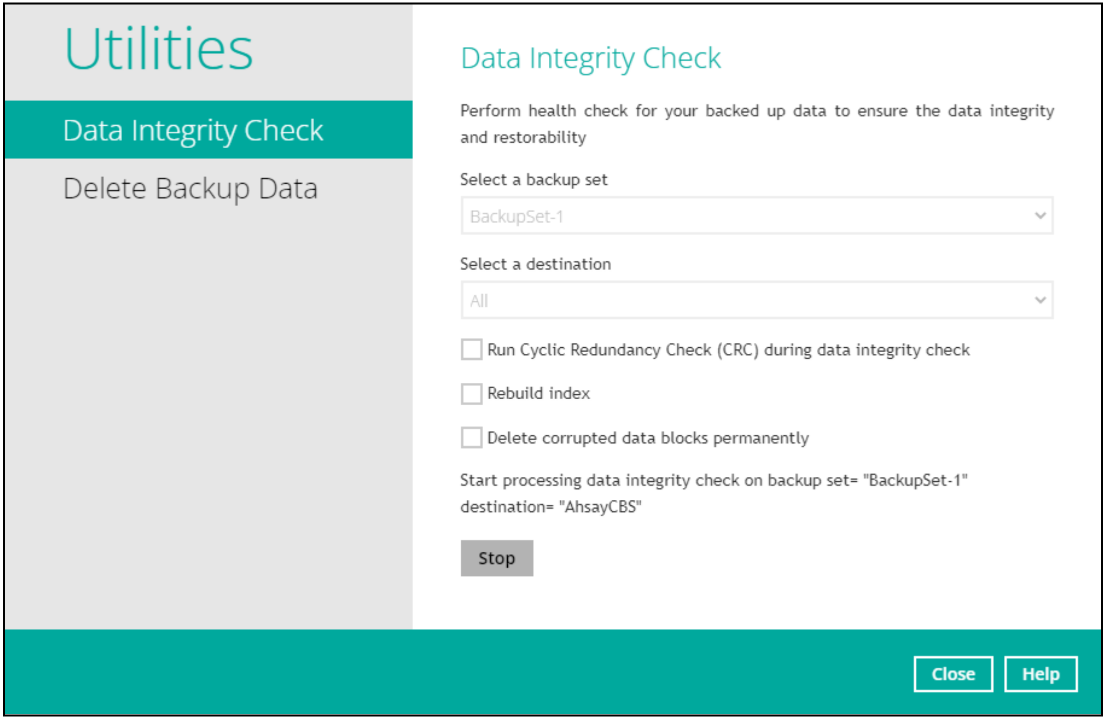
All
AhsayCBS

□ Rebuild index

□ Delete corrupted data blocks permanently

4. Click the **Start** button to begin the DIC.

5. DIC will start running on the selected backup set(s) and backup destination(s).



Data Integrity Check

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

Select a backup set: BackupSet-1

Select a destination: All

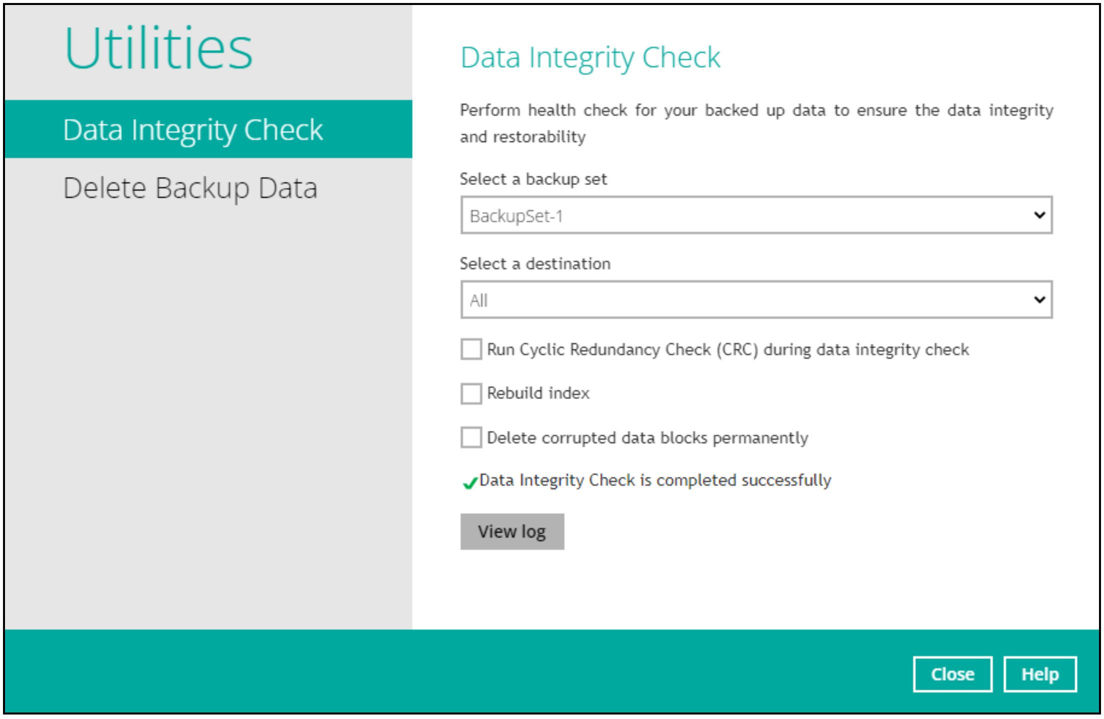
□ Run Cyclic Redundancy Check (CRC) during data integrity check

□ Rebuild index

□ Delete corrupted data blocks permanently

Start processing data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS"

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



Data Integrity Check

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

Select a backup set: BackupSet-1

Select a destination: All

□ Run Cyclic Redundancy Check (CRC) during data integrity check

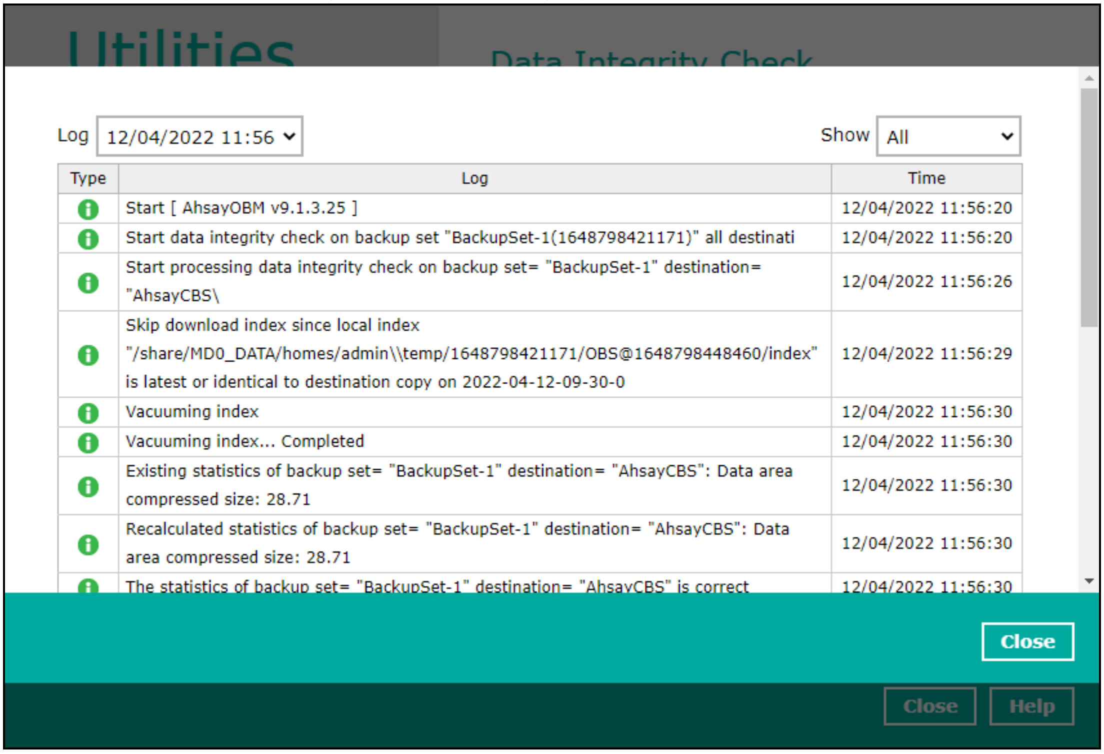
□ Rebuild index

□ Delete corrupted data blocks permanently

✓Data Integrity Check is completed successfully

View log

7. The detailed log of the DIC process will be displayed.

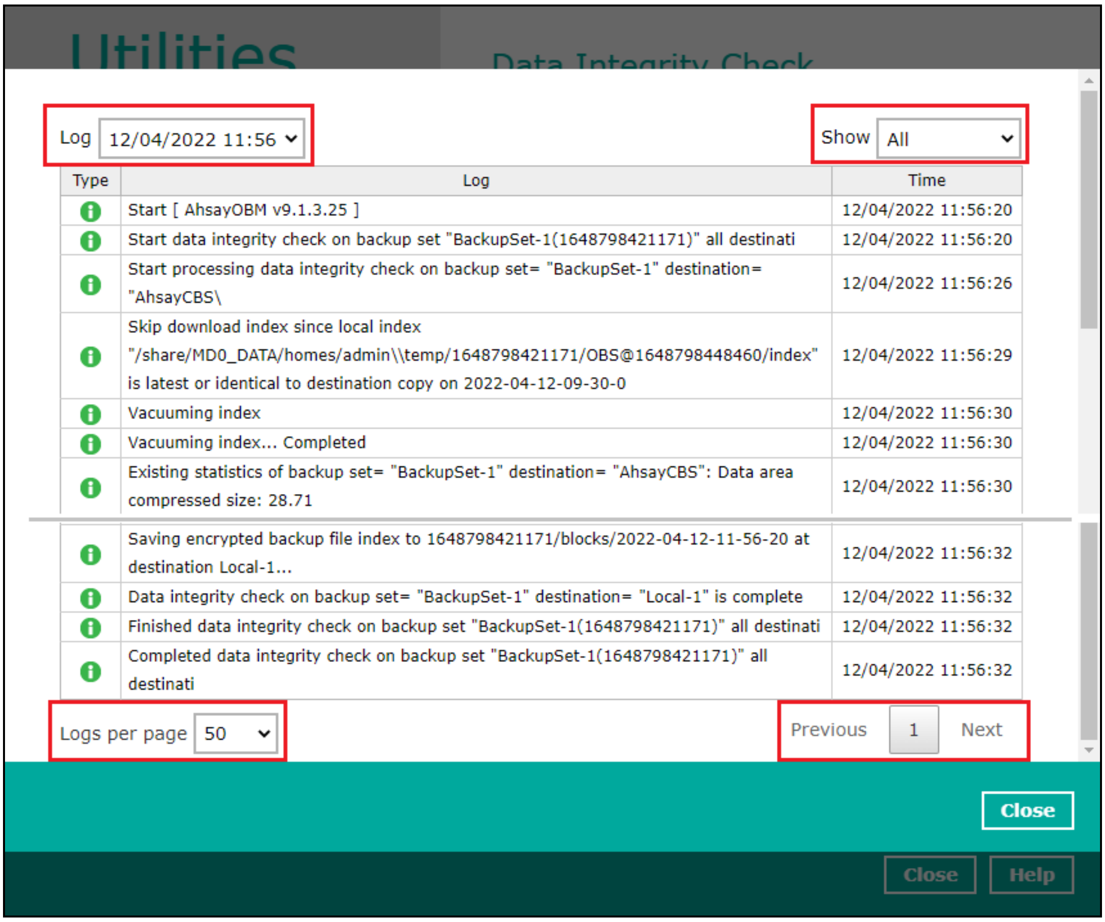


Log 12/04/2022 11:56 Show All

Type	Log	Time
ⓘ	Start [AhsayOBM v9.1.3.25]	12/04/2022 11:56:20
ⓘ	Start data integrity check on backup set "BackupSet-1(1648798421171)" all destinati	12/04/2022 11:56:20
ⓘ	Start processing data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS\	12/04/2022 11:56:26
ⓘ	Skip download index since local index "/share/MD0_DATA/homes/admin\\temp/1648798421171/OBS@1648798448460/index" is latest or identical to destination copy on 2022-04-12-09-30-0	12/04/2022 11:56:29
ⓘ	Vacuuming index	12/04/2022 11:56:30
ⓘ	Vacuuming index... Completed	12/04/2022 11:56:30
ⓘ	Existing statistics of backup set= "BackupSet-1" destination= "AhsayCBS": Data area compressed size: 28.71	12/04/2022 11:56:30
ⓘ	Recalculated statistics of backup set= "BackupSet-1" destination= "AhsayCBS": Data area compressed size: 28.71	12/04/2022 11:56:30
ⓘ	The statistics of backup set= "BackupSet-1" destination= "AhsayCBS" is correct	12/04/2022 11:56:30

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

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

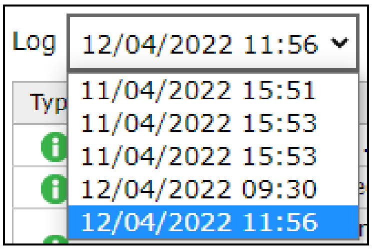
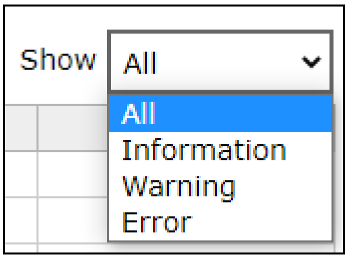
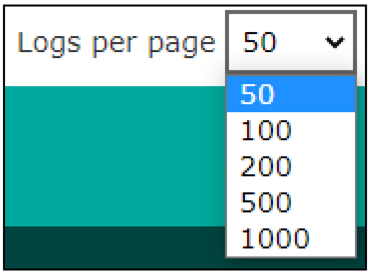
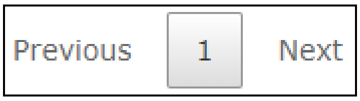


Log 12/04/2022 11:56

Show All

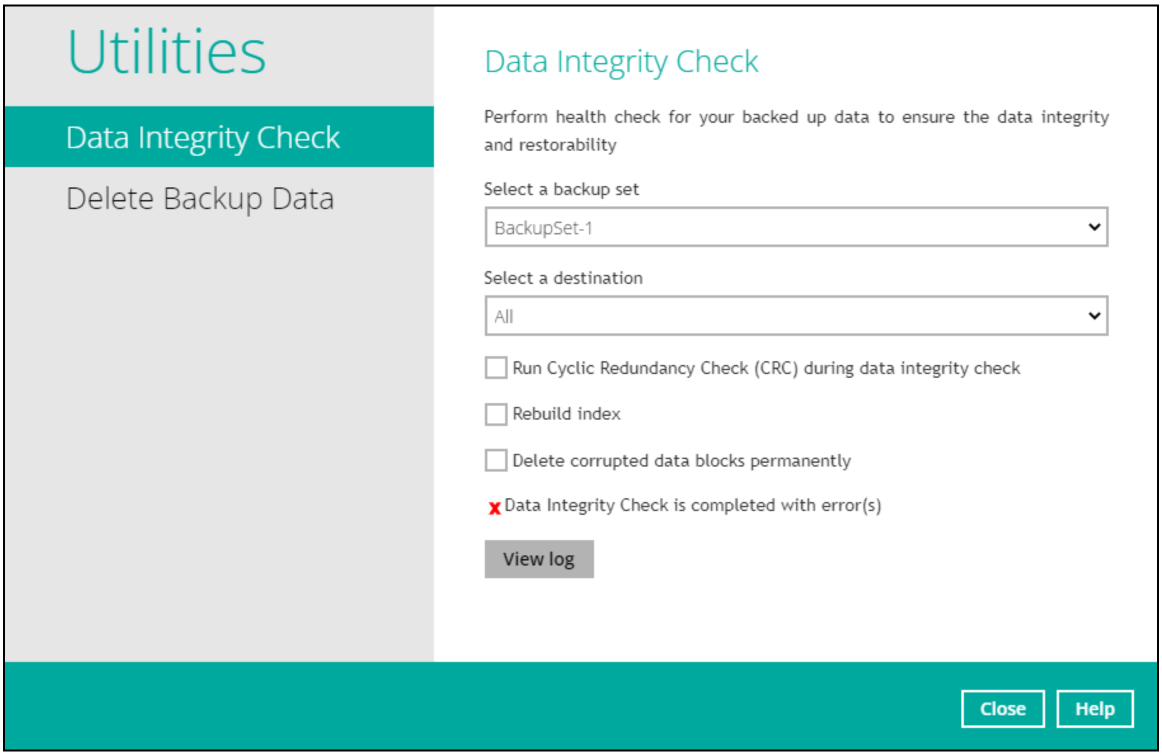
Type	Log	Time
ℹ	Start [AhsayOBM v9.1.3.25]	12/04/2022 11:56:20
ℹ	Start data integrity check on backup set "BackupSet-1(1648798421171)" all destinati	12/04/2022 11:56:20
ℹ	Start processing data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS\	12/04/2022 11:56:26
ℹ	Skip download index since local index "/share/MD0_DATA/homes/admin\\temp/1648798421171/OBS@1648798448460/index" is latest or identical to destination copy on 2022-04-12-09-30-0	12/04/2022 11:56:29
ℹ	Vacuuming index	12/04/2022 11:56:30
ℹ	Vacuuming index... Completed	12/04/2022 11:56:30
ℹ	Existing statistics of backup set= "BackupSet-1" destination= "AhsayCBS": Data area compressed size: 28.71	12/04/2022 11:56:30
ℹ	Saving encrypted backup file index to 1648798421171/blocks/2022-04-12-11-56-20 at destination Local-1...	12/04/2022 11:56:32
ℹ	Data integrity check on backup set= "BackupSet-1" destination= "Local-1" is complete	12/04/2022 11:56:32
ℹ	Finished data integrity check on backup set "BackupSet-1(1648798421171)" all destinati	12/04/2022 11:56:32
ℹ	Completed data integrity check on backup set "BackupSet-1(1648798421171)" all destinati	12/04/2022 11:56:32

Logs per page 50

Control	Screenshot	Description
Log filter	 Log 12/04/2022 11:56 Typ 11/04/2022 15:51 11/04/2022 15:53 11/04/2022 15:53 12/04/2022 09:30 12/04/2022 11:56	This option can be used to display logs of the previous DIC jobs.
Show filter		This option can be used to sort the DIC log by its status (i.e., All, Information, Warning, and Error). With this filter, it will be easier to sort the DIC logs by its status especially for longer DIC logs.
Logs per page		This option allows user to control the displayed number of logs per page.
Page		This option allows user to navigate the logs to the next page(s).

Data Integrity Check Completed with Errors

The following screenshot is an example of a DIC completed with error(s).



Data Integrity Check

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

Select a backup set: BackupSet-1

Select a destination: All

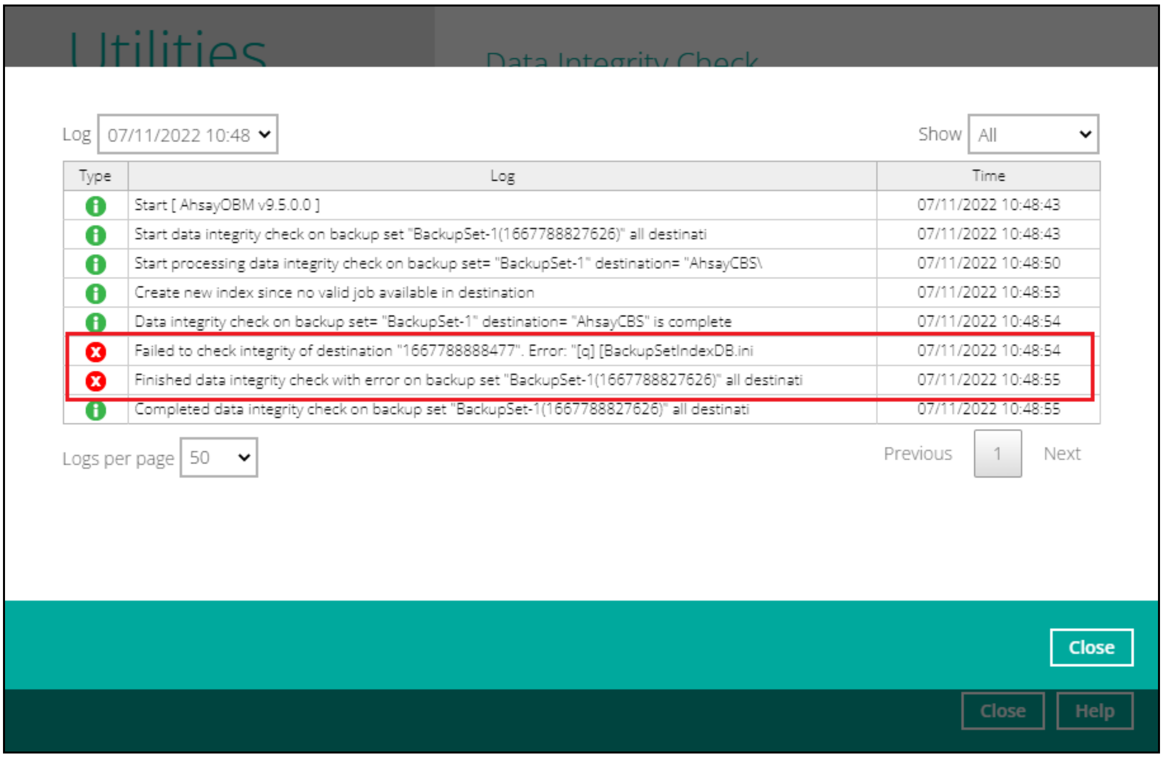
□ Run Cyclic Redundancy Check (CRC) during data integrity check

□ Rebuild index

□ Delete corrupted data blocks permanently

✗ Data Integrity Check is completed with error(s)

Clicking the **View log** button will display the details of the DIC job error(s).



Log 07/11/2022 10:48

Show All

Type	Log	Time
ℹ	Start [AhsayOBM v9.5.0.0]	07/11/2022 10:48:43
ℹ	Start data integrity check on backup set "BackupSet-1(1667788827626)" all destinati	07/11/2022 10:48:43
ℹ	Start processing data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS\	07/11/2022 10:48:50
ℹ	Create new index since no valid job available in destination	07/11/2022 10:48:53
ℹ	Data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS" is complete	07/11/2022 10:48:54
✖	Failed to check integrity of destination "1667788888477". Error: "[q] [BackupSetIndexDB.ini	07/11/2022 10:48:54
✖	Finished data integrity check with error on backup set "BackupSet-1(1667788827626)" all destinati	07/11/2022 10:48:55
ℹ	Completed data integrity check on backup set "BackupSet-1(1667788827626)" all destinati	07/11/2022 10:48:55

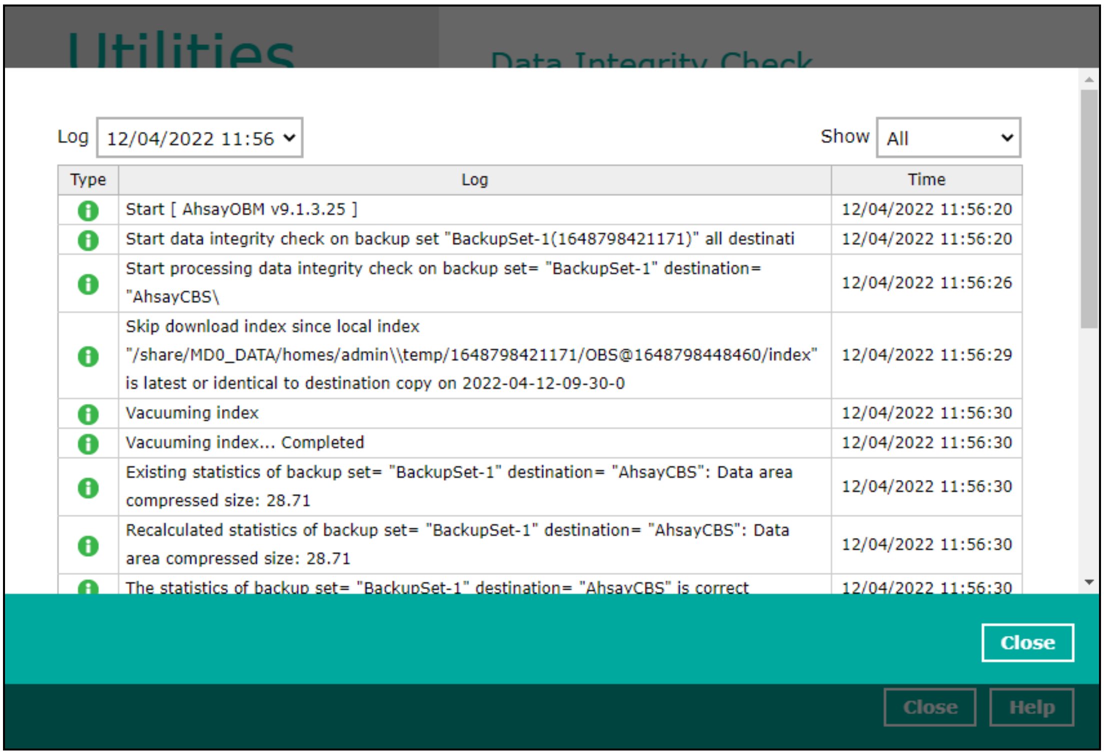
Logs per page 50

Data Integrity Check Result

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

- Data Integrity Check is completed successfully with no data corruption/issues detected;
- Corrupted data (e.g. index files, checksum files and/or broken data blocks) has been detected and deleted

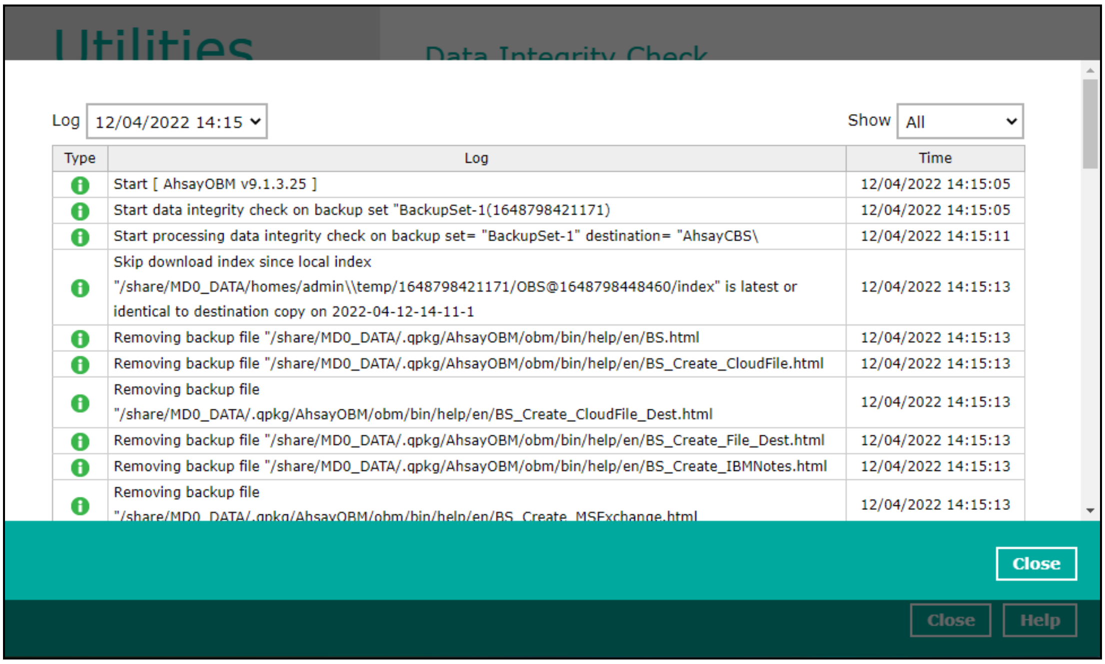
The screenshot below shows an example of a DIC log with NO data corruption/issues detected.



Log 12/04/2022 11:56 Show All

Type	Log	Time
ⓘ	Start [AhsayOBM v9.1.3.25]	12/04/2022 11:56:20
ⓘ	Start data integrity check on backup set "BackupSet-1(1648798421171)" all destinati	12/04/2022 11:56:20
ⓘ	Start processing data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS\	12/04/2022 11:56:26
ⓘ	Skip download index since local index "/share/MD0_DATA/homes/admin\\temp/1648798421171/OBS@1648798448460/index" is latest or identical to destination copy on 2022-04-12-09-30-0	12/04/2022 11:56:29
ⓘ	Vacuuming index	12/04/2022 11:56:30
ⓘ	Vacuuming index... Completed	12/04/2022 11:56:30
ⓘ	Existing statistics of backup set= "BackupSet-1" destination= "AhsayCBS": Data area compressed size: 28.71	12/04/2022 11:56:30
ⓘ	Recalculated statistics of backup set= "BackupSet-1" destination= "AhsayCBS": Data area compressed size: 28.71	12/04/2022 11:56:30
ⓘ	The statistics of backup set= "BackupSet-1" destination= "AhsayCBS" is correct	12/04/2022 11:56:30

The screenshot below shows an example of a data integrity check log when corrupted data has been detected. If any corrupted data is found, these corrupted files are automatically removed from the backup destination(s).



Log 12/04/2022 14:15 Show All

Type	Log	Time
ⓘ	Start [AhsayOBM v9.1.3.25]	12/04/2022 14:15:05
ⓘ	Start data integrity check on backup set "BackupSet-1(1648798421171)	12/04/2022 14:15:05
ⓘ	Start processing data integrity check on backup set= "BackupSet-1" destination= "AhsayCBS\	12/04/2022 14:15:11
ⓘ	Skip download index since local index "/share/MD0_DATA/homes/admin\\temp/1648798421171/OBS@1648798448460/index" is latest or identical to destination copy on 2022-04-12-14-11-1	12/04/2022 14:15:13
ⓘ	Removing backup file "/share/MD0_DATA/.qpkg/AhsayOBM/obm/bin/help/en/BS.html	12/04/2022 14:15:13
ⓘ	Removing backup file "/share/MD0_DATA/.qpkg/AhsayOBM/obm/bin/help/en/BS_Create_CloudFile.html	12/04/2022 14:15:13
ⓘ	Removing backup file "/share/MD0_DATA/.qpkg/AhsayOBM/obm/bin/help/en/BS_Create_CloudFile_Dest.html	12/04/2022 14:15:13
ⓘ	Removing backup file "/share/MD0_DATA/.qpkg/AhsayOBM/obm/bin/help/en/BS_Create_File_Dest.html	12/04/2022 14:15:13
ⓘ	Removing backup file "/share/MD0_DATA/.qpkg/AhsayOBM/obm/bin/help/en/BS_Create_IBMNotes.html	12/04/2022 14:15:13
ⓘ	Removing backup file "/share/MD0_DATA/.qpkg/AhsayOBM/obm/bin/help/en/BS_Create_MSExchange.html	12/04/2022 14:15:13

Test Mode confirmation

The (TEST MODE) confirmation screen is not supported on QNAP NAS.

When running a data integrity check on other platforms such as Windows, Mac, or Linux (GUI), a (TEST MODE) confirmation screen will prompt if either of the **criteria** below matches the backup data during the data integrity check process:

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

However, on QNAP NAS, during the data integrity check job, corrective actions will be taken automatically if the DIC has detected the following:

- Index-related issues
- Broken data blocks
- Discrepancy against checksum file (when the Cyclic Redundancy Check is enabled)

This means that the DIC will automatically remove any corrupted file(s) from the backup destination(s), and will update storage statistics without requiring user confirmation.

Aside from viewing the DIC logs directly on the AhsayOBM client, they can be viewed on the file system of the AhsayOBM client machine. For AhsayOBM on QNAP NAS, the DIC logs are located in the following directory:

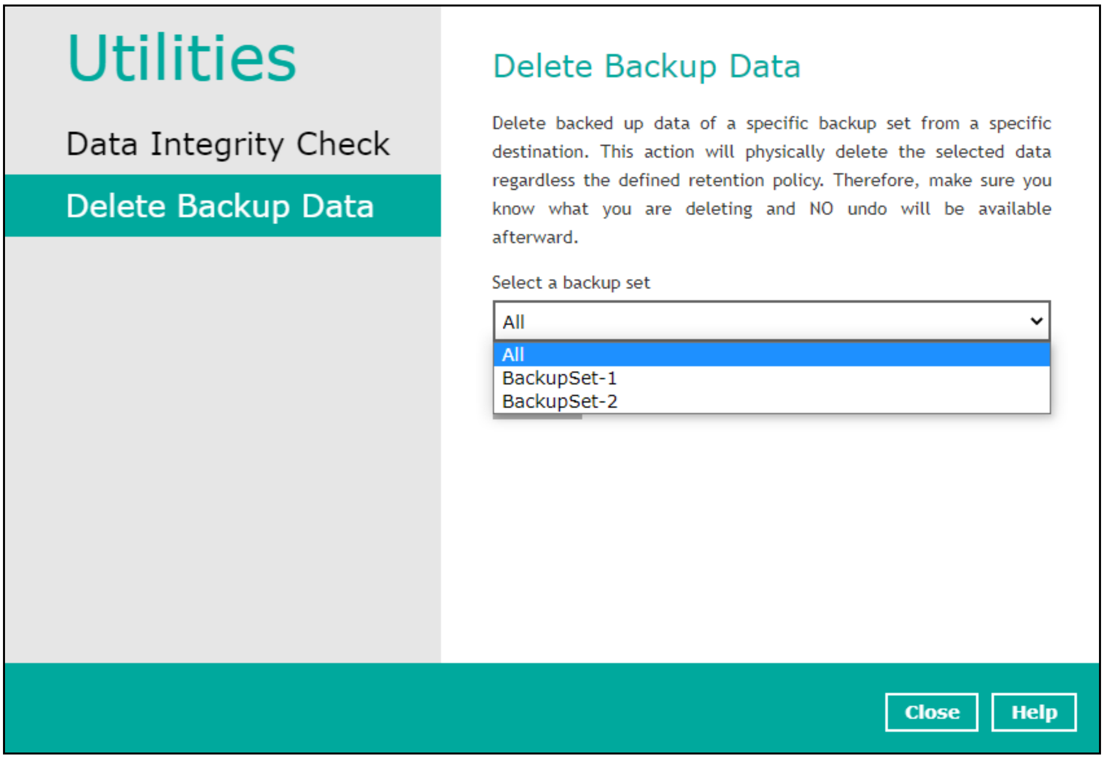
${system_volume_path}/homes/admin/.obm/system/IntegrityCheck

8.10.2 Delete Backup Data

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

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

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



Delete Backup Data

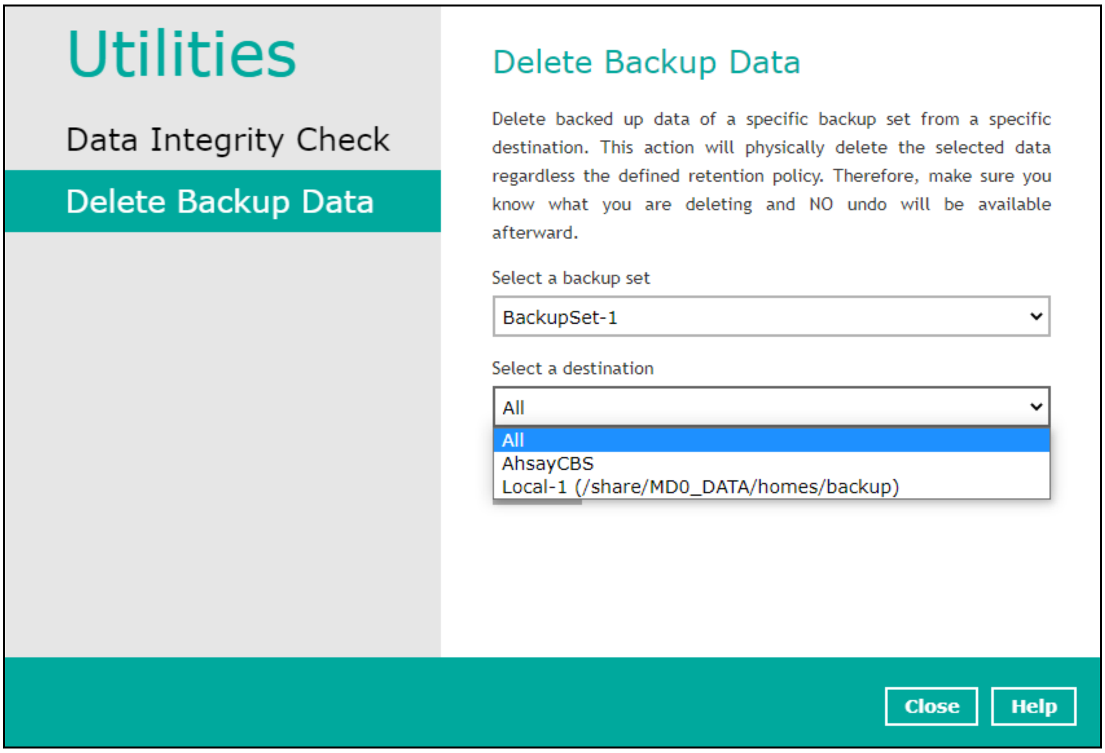
Delete backed up data of a specific backup set from a specific destination. This action will physically delete the selected data regardless the defined retention policy. Therefore, make sure you know what you are deleting and NO undo will be available afterward.

Select a backup set: All

NOTE

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

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



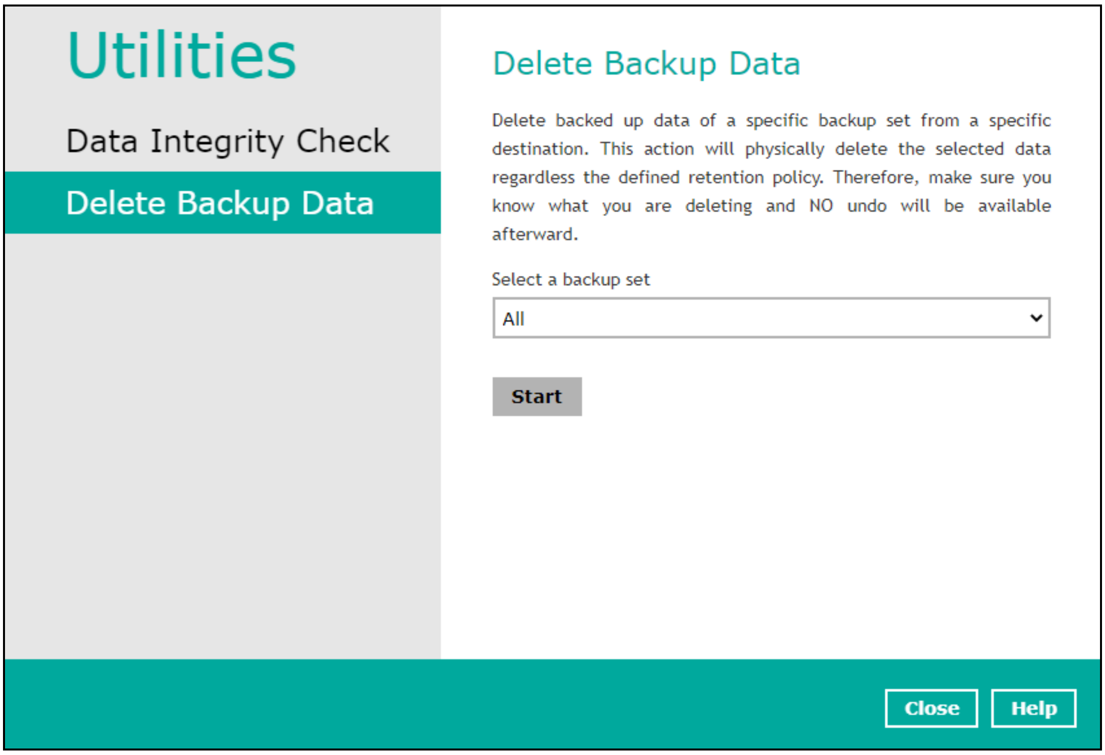
Delete Backup Data

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

Select a backup set: BackupSet-1

Select a destination: All

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

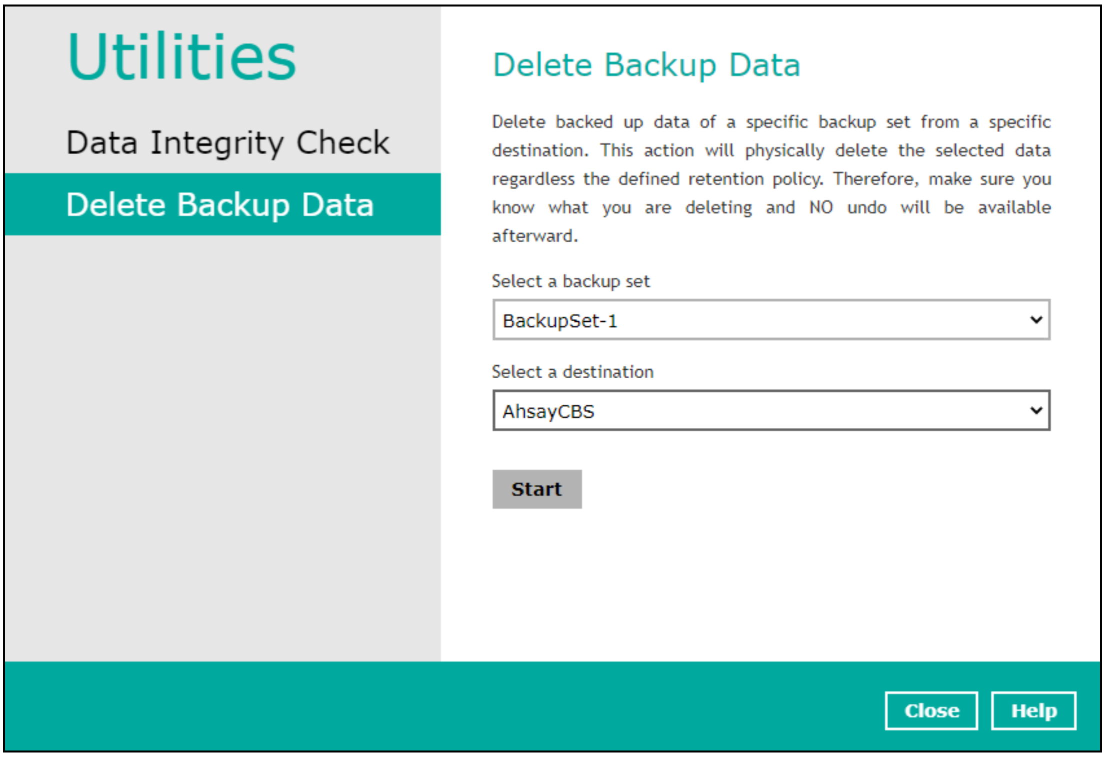


Delete Backup Data

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

Select a backup set: All

2. Click the **Start** button, then click **Yes** to proceed. This process will delete backed up data on the selected backup set(s) and destination(s).

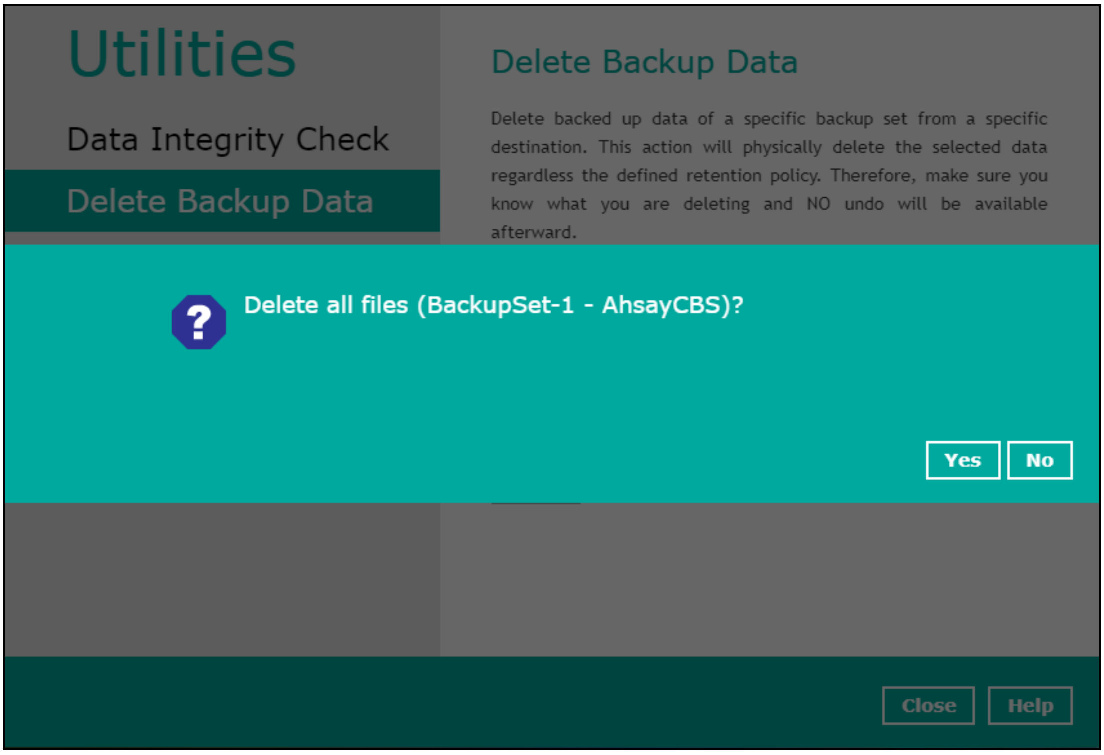


Delete Backup Data

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

Select a backup set: BackupSet-1

Select a destination: AhsayCBS

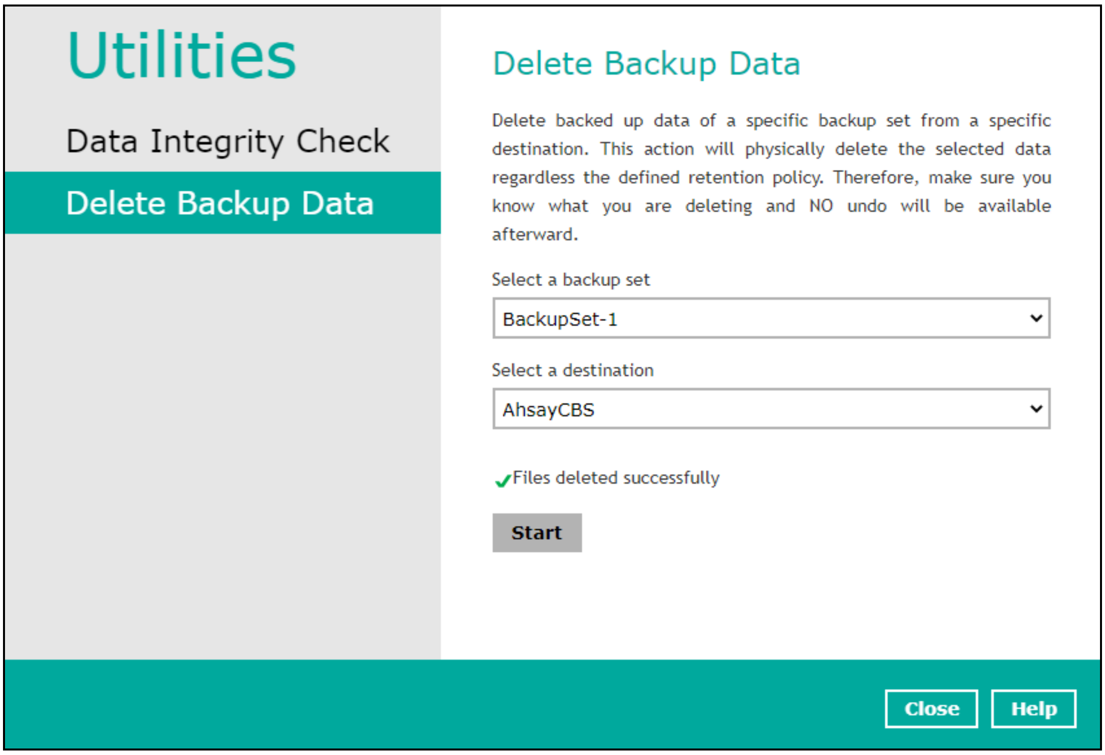


Delete Backup Data

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

Delete all files (BackupSet-1 - AhsayCBS)?

3. Files are successfully deleted.



Delete Backup Data

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

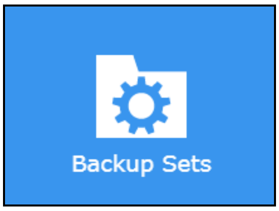
Select a backup set: BackupSet-1

Select a destination: AhsayCBS

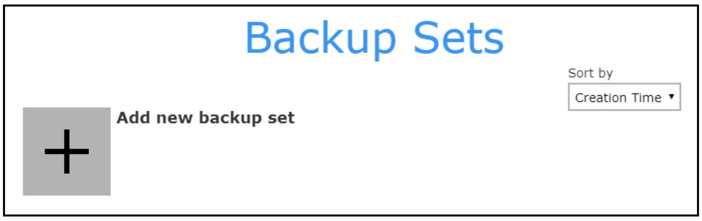
✓Files deleted successfully

9 Create a Backup Set

1. Click the **Backup Sets** icon on the main interface of AhsayOBM.

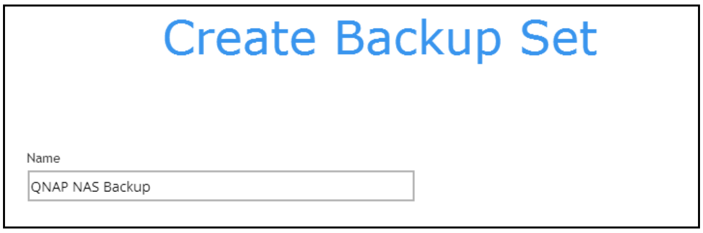


2. Create a backup set by clicking “**+ Add new backup set**”.



Sort by
Creation Time

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



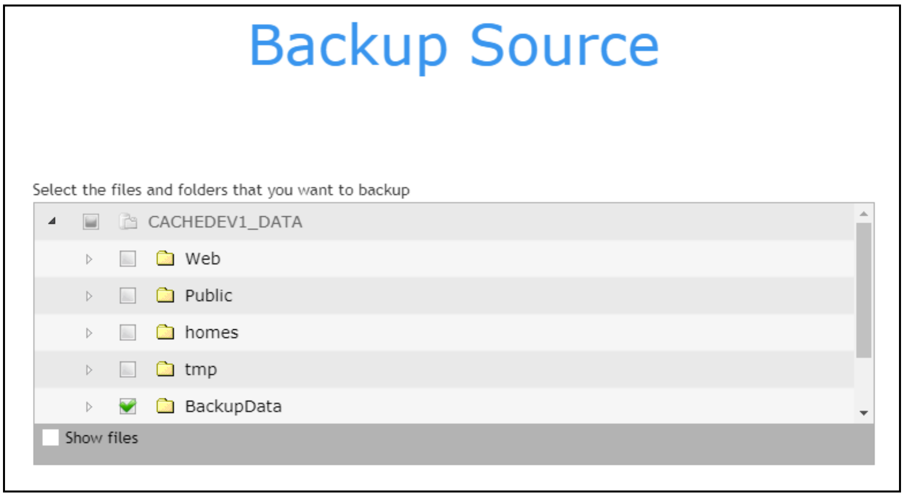
Name
QNAP NAS Backup

4. In the Backup Source window, select the files and folders that you would like to back up.

NOTE

AhsayOBM supports backup of files and/or folders from an external USB drive attached to the QNAP NAS machine where the AhsayOBM is installed.

Backup Source on the QNAP NAS

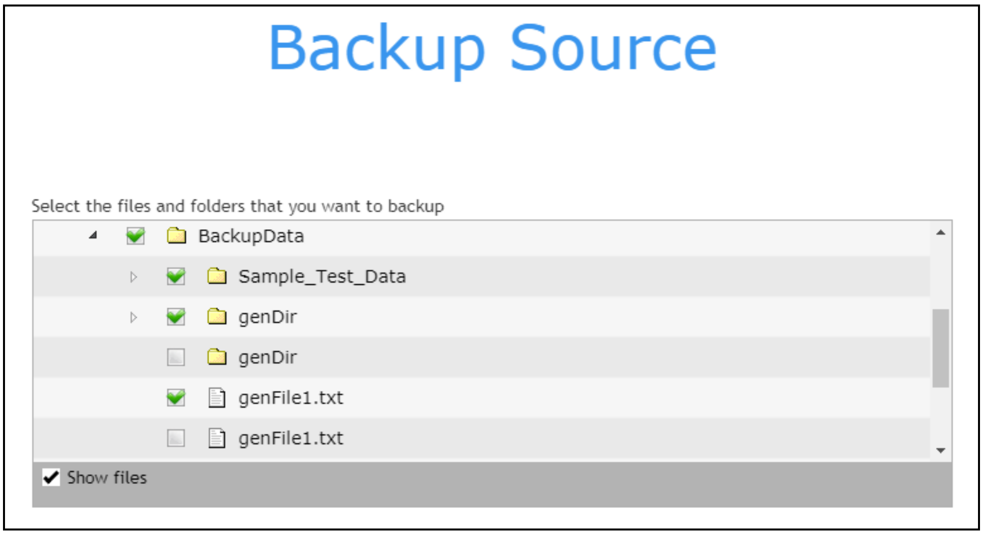


Select the files and folders that you want to backup

- CACHEDEV1_DATA
  - □ Web
  - □ Public
  - □ homes
  - □ tmp
  - ☑ BackupData

□ Show files

You may click the **Show files** checkbox if you want to select individual file(s) for backup.



Backup Source

Select the files and folders that you want to backup

- ☑ BackupData
  - ☑ Sample_Test_Data
  - ☑ genDir
  - □ genDir
  - ☑ genFile1.txt
  - □ genFile1.txt

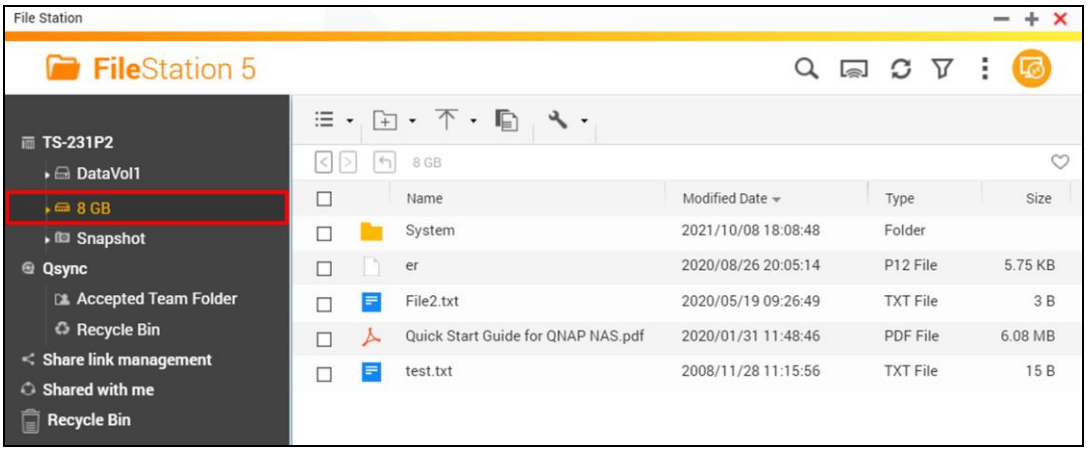
☑ Show files

Backup Source on the External USB Drive

To select a backup source from an external USB drive, follow the instructions below:

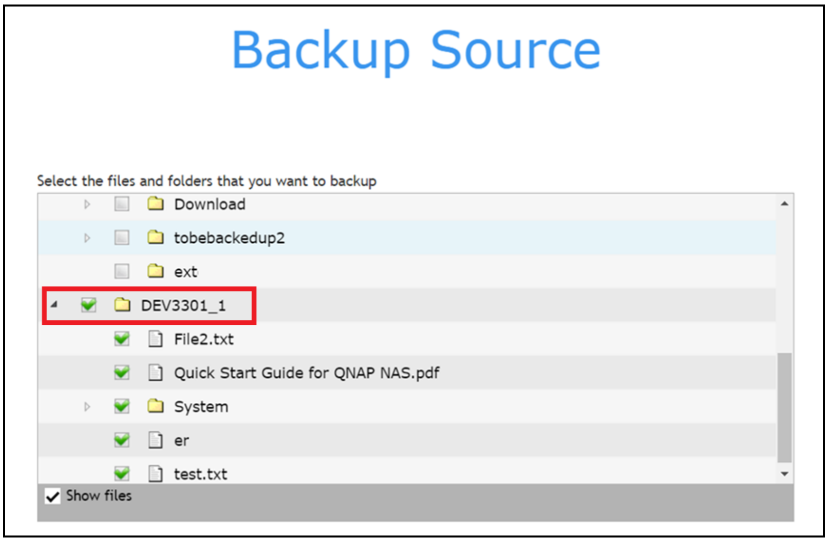
i. Ensure that your AhsayOBM is updated to v9.1.0.0 (or above).

ii. Attach your external USB drive, then verify if the attached external USB drive is visible on the File Station.



□	Name	Modified Date	Type	Size
□	System	2021/10/08 18:08:48	Folder	
□	er	2020/08/26 20:05:14	P12 File	5.75 KB
□	File2.txt	2020/05/19 09:26:49	TXT File	3 B
□	Quick Start Guide for QNAP NAS.pdf	2020/01/31 11:48:46	PDF File	6.08 MB
□	test.txt	2008/11/28 11:15:56	TXT File	15 B

iii. Select the files and/or folders from the external USB drive that you would like to back up.



Backup Source

Select the files and folders that you want to backup

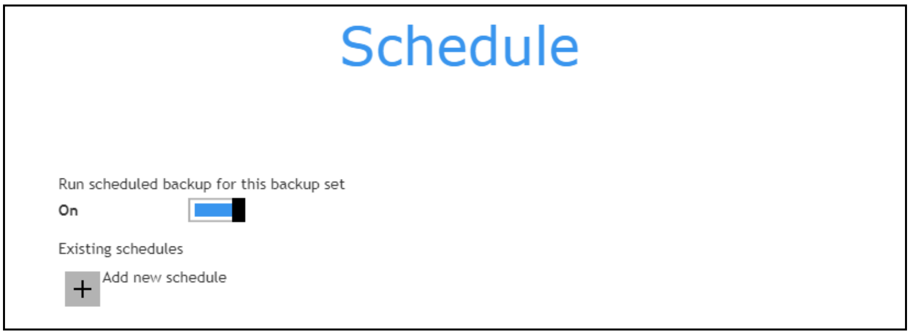
- □ Download
- □ tobebackedup2
- □ ext
- ☑ DEV3301_1
  - ☑ File2.txt
  - ☑ Quick Start Guide for QNAP NAS.pdf
  - ☑ System
  - ☑ er
  - ☑ test.txt

☑ Show files

After selecting the backup source, click **Next** to proceed.

5. When the Schedule window appears, you can configure a backup schedule to automatically run a backup job at your specified time interval. In the Schedule window, the Run scheduled backup for this backup set is **On** by default.

- You can leave it as is or you can turn it **Off** if you do not want to add a schedule again.

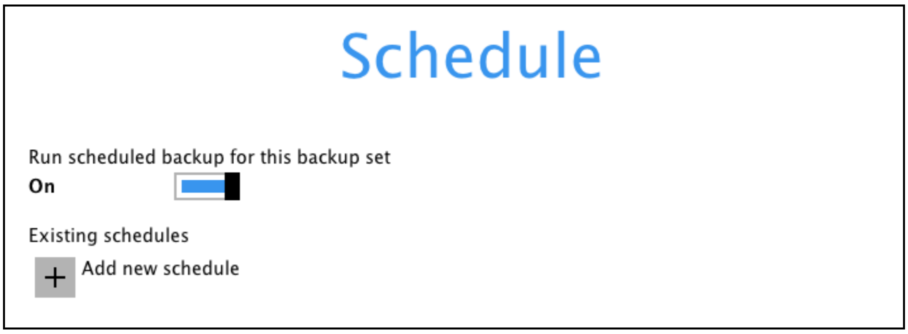


Schedule

Run scheduled backup for this backup set
On

Existing schedules

- If you want to add a schedule now, click "+" next to Add New schedule.

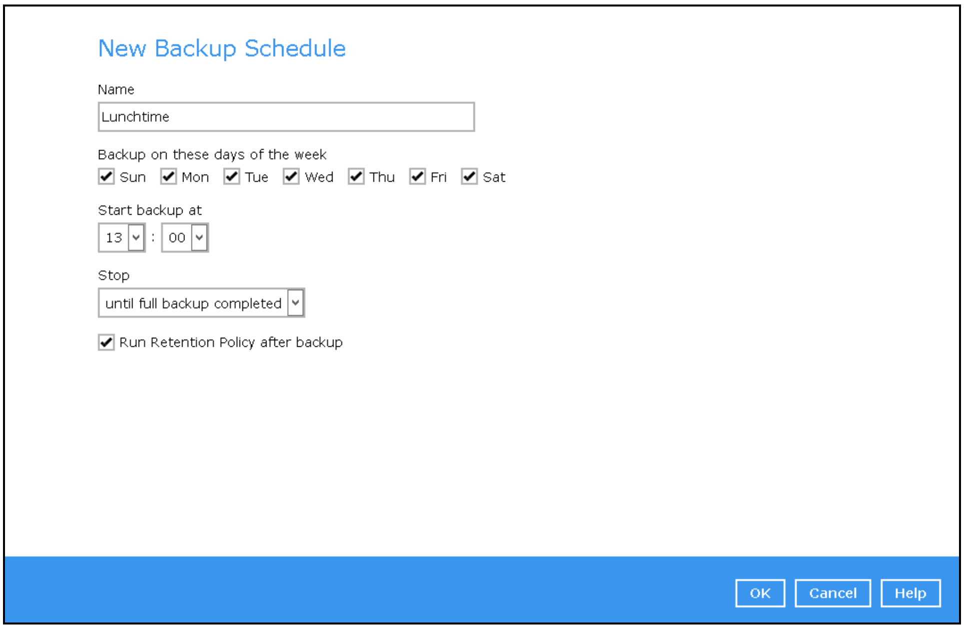


Schedule

Run scheduled backup for this backup set
On

Existing schedules

When the **New Backup Schedule** window appears, specify your backup schedule. Then, click **OK** to save your changes and close the New Backup Schedule window.



New Backup Schedule

Name: Lunchtime

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

Start backup at
13 : 00

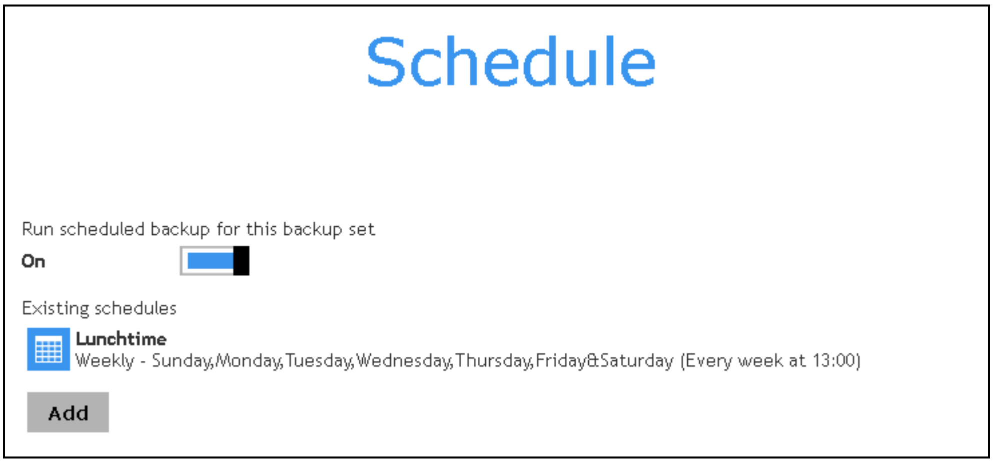
Stop
until full backup completed

☑ Run Retention Policy after backup

NOTE

For details about the options from the dropdown menus, please refer to Configure Backup Schedule for Automated Backup.

6. In case you have added a schedule, it will be shown in the Schedule window. Click **Next** to proceed when you are done with the settings.



Schedule

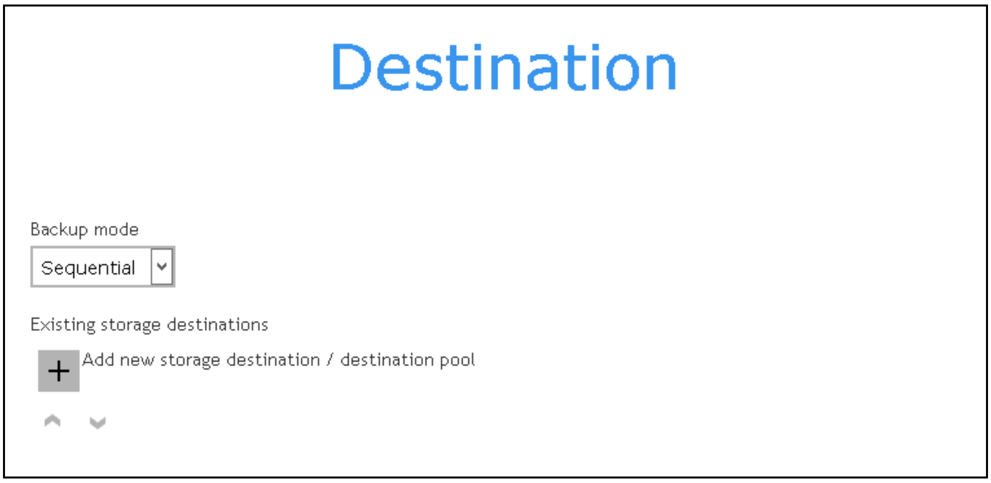
Run scheduled backup for this backup set

On

Existing schedules

Lunchtime
Weekly - Sunday,Monday,Tuesday,Wednesday,Thursday,Friday&Saturday (Every week at 13:00)

7. The Destination window will appear.



Destination

Backup mode

Sequential

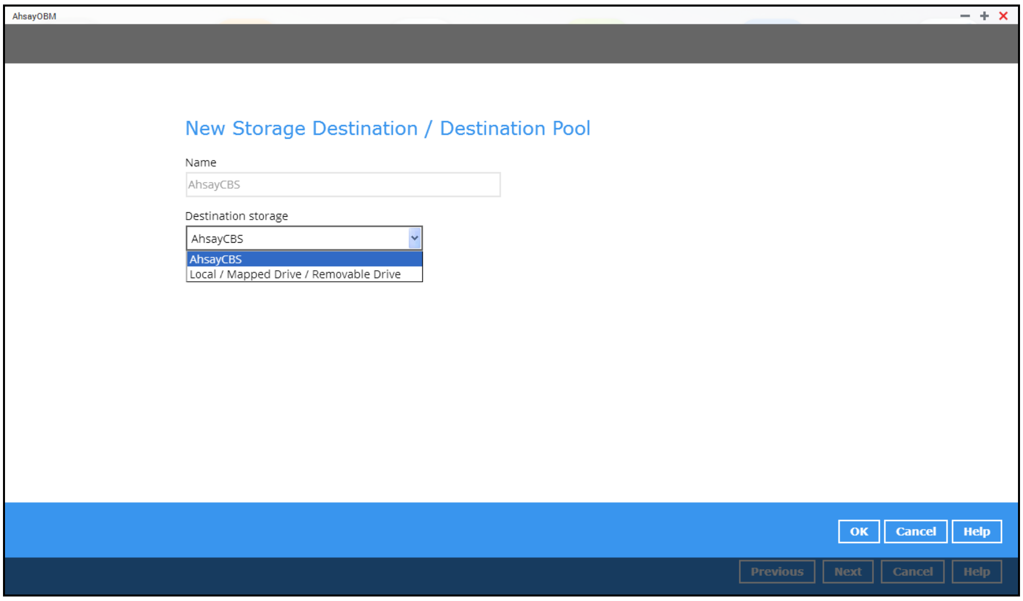
Existing storage destinations

Select the appropriate option from the **Backup mode** drop down menu.

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

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

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



AhsayOBM

New Storage Destination / Destination Pool

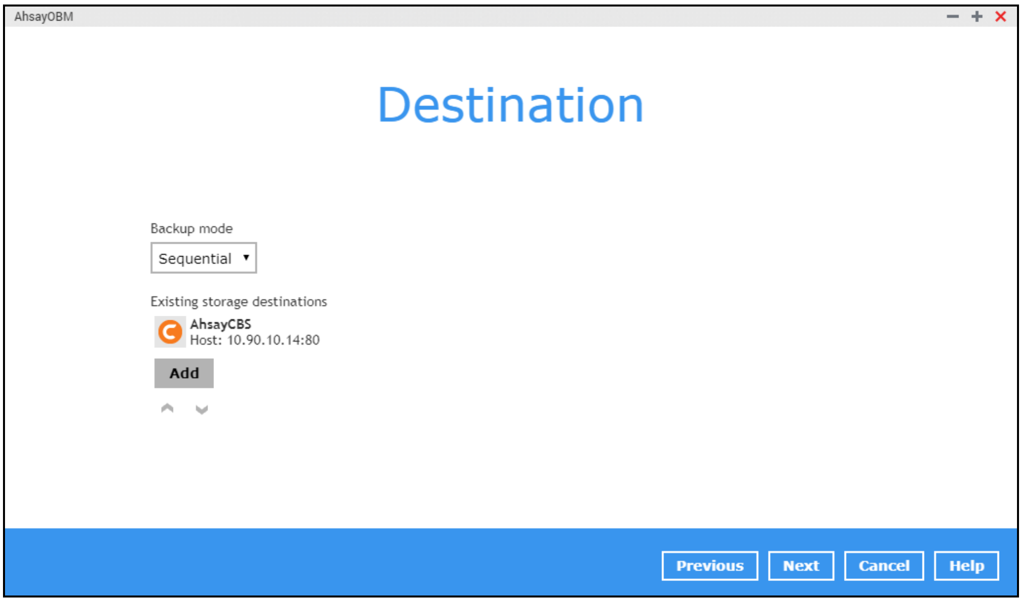
Name: AhsayCBS

Destination storage: AhsayCBS

NOTE

For more details on configuration of cloud storage as backup destination, refer to Appendix A in this guide.

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



AhsayOBM

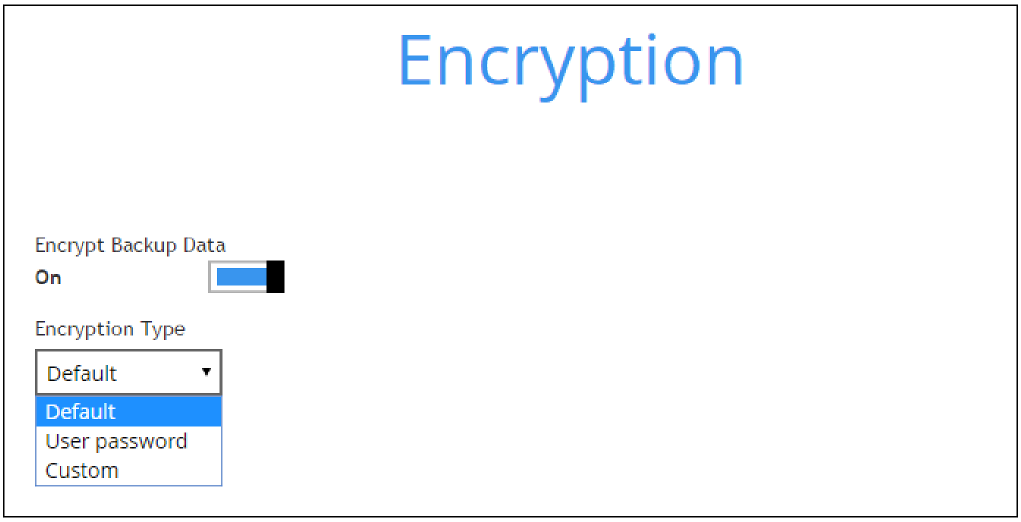
Destination

Backup mode: Sequential

Existing storage destinations

AhsayCBS
Host: 10.90.10.14:80

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



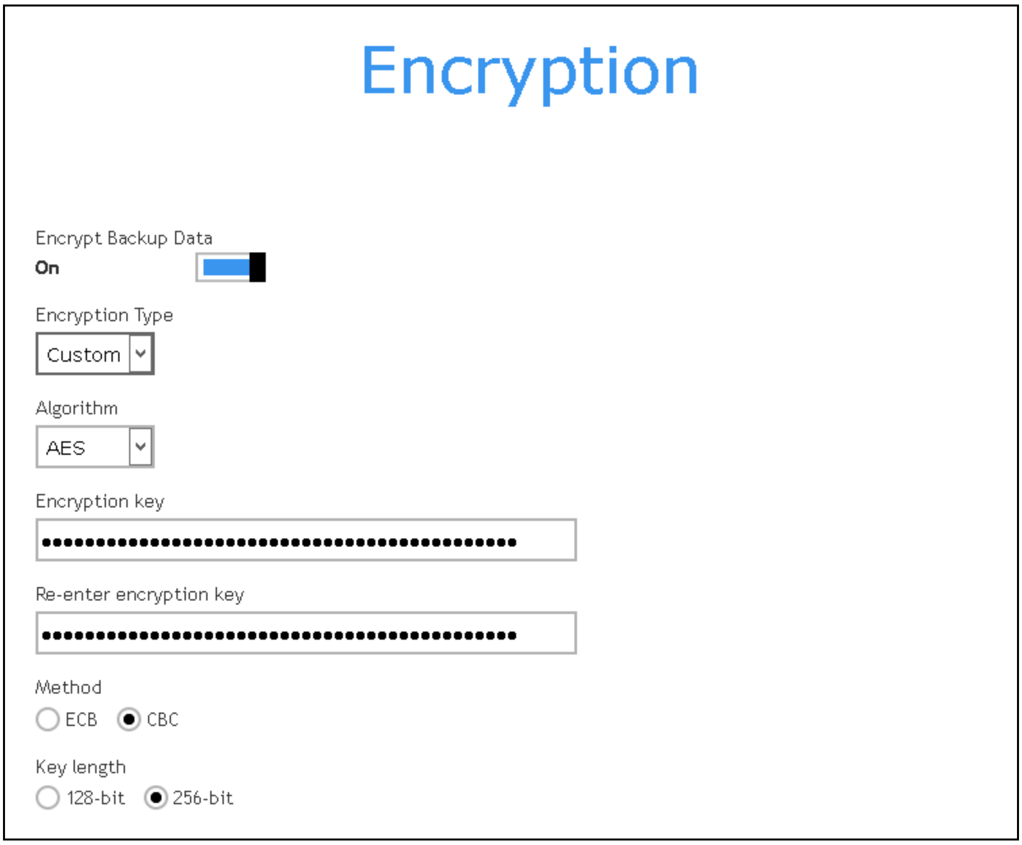
Encryption

Encrypt Backup Data
On

Encryption Type
Default

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

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system.
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup 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

Encrypt Backup Data
On

Encryption Type
Custom

Algorithm
AES

Encryption key
●●

Re-enter encryption key
●●

Method
○ ECB ● CBC

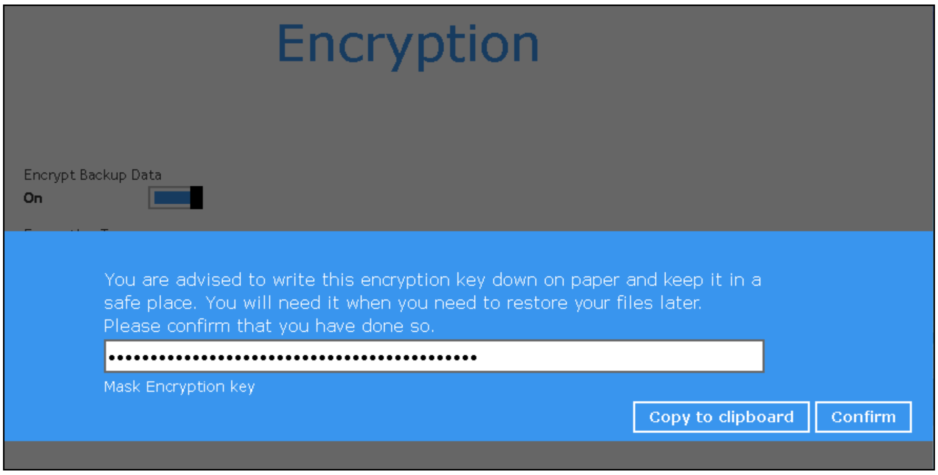
Key length
○ 128-bit ● 256-bit

NOTE

For best practice on managing your encryption key, refer to the following Wiki article. [FAQ: Best practices for managing encryption key on AhsayOBM or AhsayACB?]

Click **Save** when you are done with the settings.

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

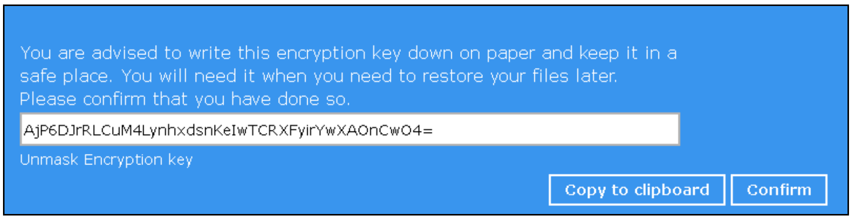


You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

•••

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.



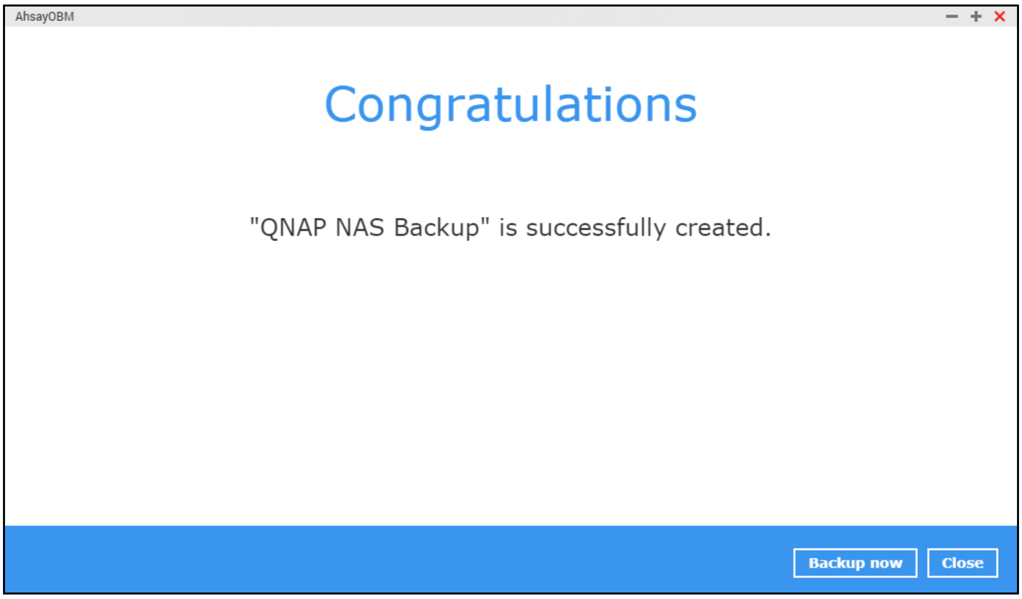
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

AjP6DJrRLCuM4LynhxdsnKeIwTCRXFyirYwXAOnCwO4=

- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.

- **Confirm** – Click to exit this pop-up window and proceed to the next step.

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



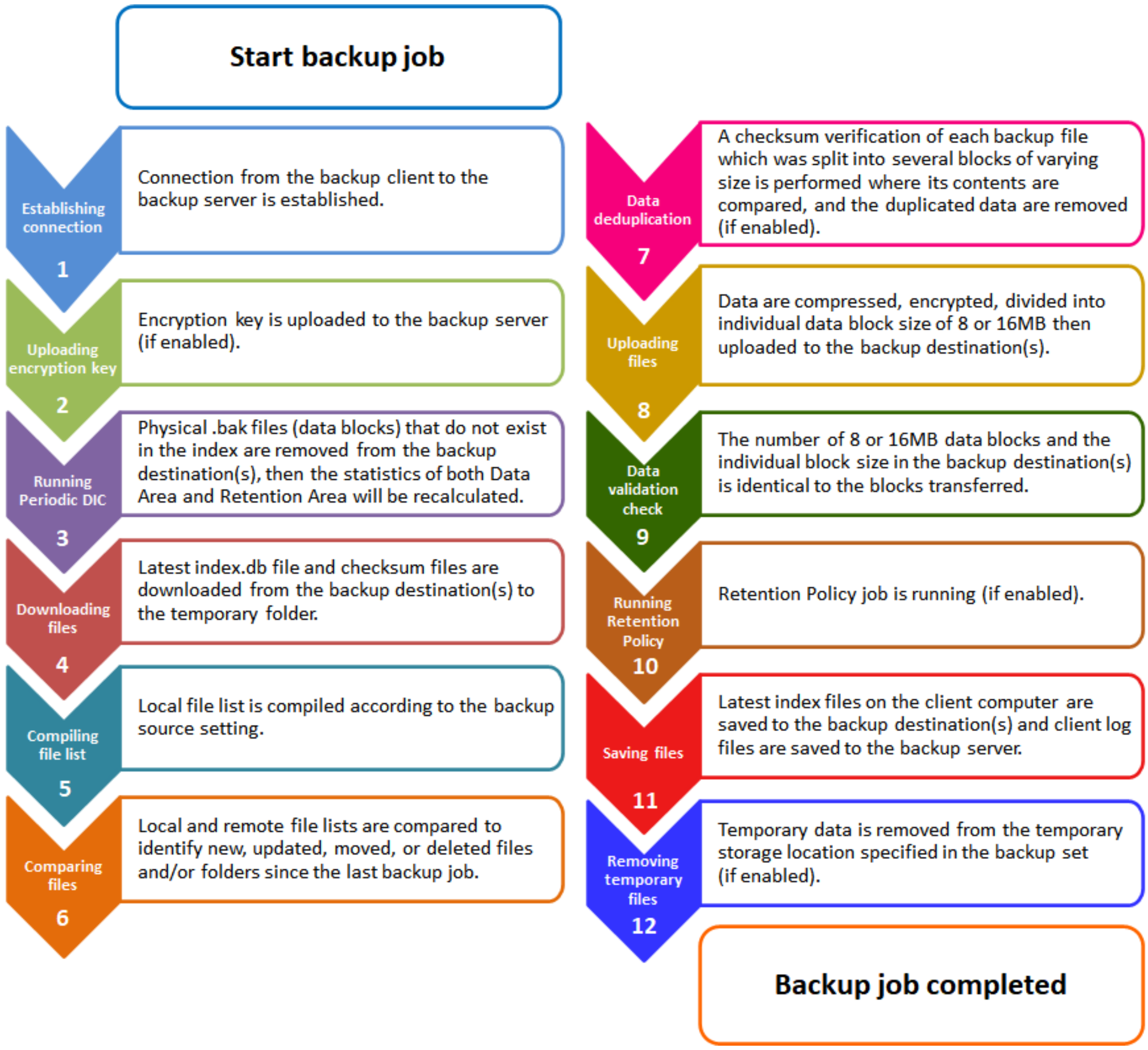
Congratulations

"QNAP NAS Backup" is successfully created.

10 Overview on the Backup Process

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

- Periodic Data Integrity Check (PDIC) Process **(Step 3)**
- Backup Set Index Handling Process
  - **Start Backup Job (Step 4)**
  - **Completed Backup Job (Step 11)**
- **Data Validation Check Process (Step 9)**



Start backup job

Establishing connection 1: Connection from the backup client to the backup server is established.

Uploading encryption key 2: Encryption key is uploaded to the backup server (if enabled).

Running Periodic DIC 3: Physical .bak files (data blocks) that do not exist in the index are removed from the backup destination(s), then the statistics of both Data Area and Retention Area will be recalculated.

Downloading files 4: Latest index.db file and checksum files are downloaded from the backup destination(s) to the temporary folder.

Compiling file list 5: Local file list is compiled according to the backup source setting.

Comparing files 6: Local and remote file lists are compared to identify new, updated, moved, or deleted files and/or folders since the last backup job.

Data deduplication 7: A checksum verification of each backup file which was split into several blocks of varying size is performed where its contents are compared, and the duplicated data are removed (if enabled).

Uploading files 8: Data are compressed, encrypted, divided into individual data block size of 8 or 16MB then uploaded to the backup destination(s).

Data validation check 9: The number of 8 or 16MB data blocks and the individual block size in the backup destination(s) is identical to the blocks transferred.

Running Retention Policy 10: Retention Policy job is running (if enabled).

Saving files 11: Latest index files on the client computer are saved to the backup destination(s) and client log files are saved to the backup server.

Removing temporary files 12: Temporary data is removed from the temporary storage location specified in the backup set (if enabled).

Backup job completed

10.1 Periodic Data Integrity Check (PDIC) Process

The PDIC will run on the first backup job that falls on the corresponding day of the week from **Monday to Friday**.

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

PDIC schedule** = **%BackupSetID% modulo 5
or
%BackupSetID% mod 5

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

0	**Monday**
1	**Tuesday**
2	**Wednesday**
3	**Thursday**
4	**Friday**

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

*Calculation: 1594627447932 mod 5 = **2***

2	**Wednesday**

In this example:

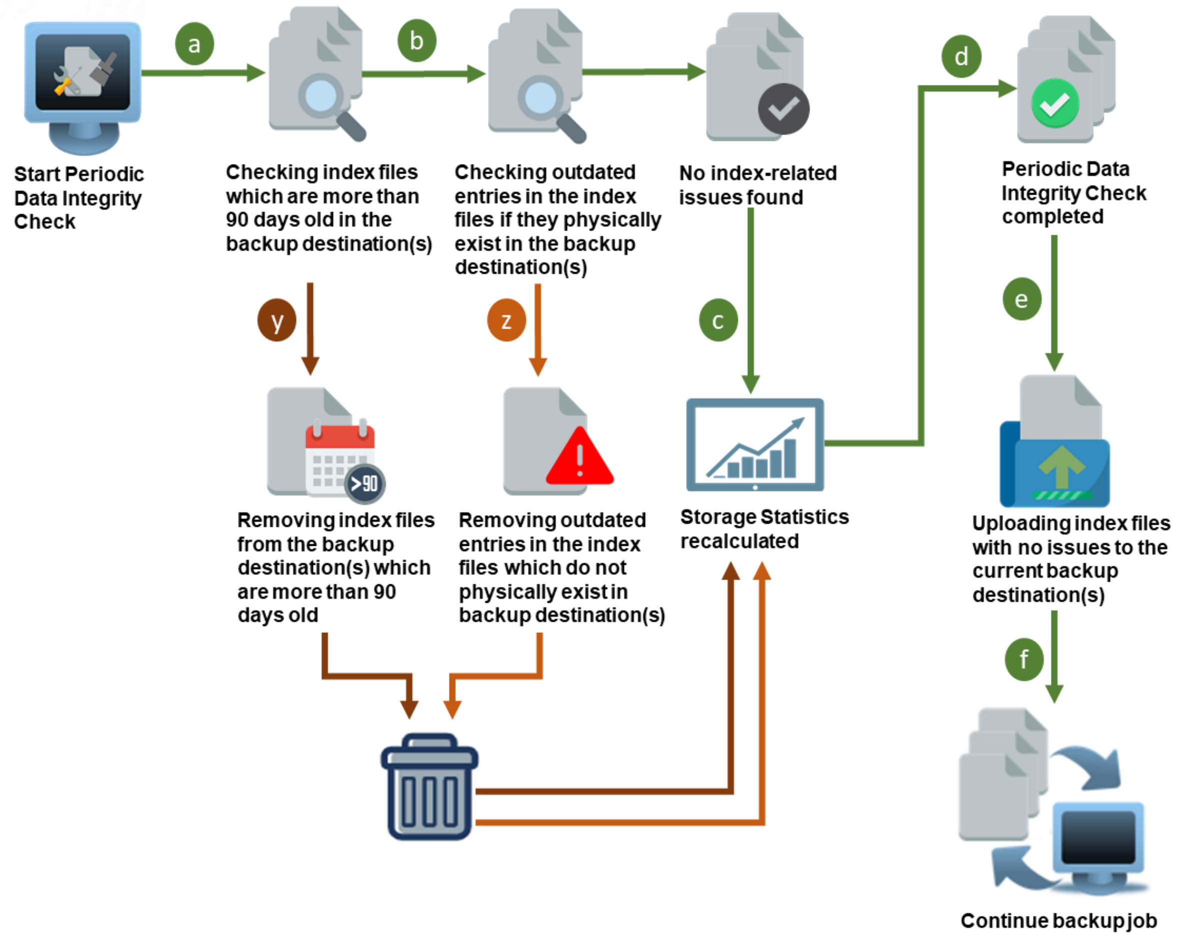
- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

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

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

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


a
b
d
Start Periodic Data Integrity Check
Checking index files which are more than 90 days old in the backup destination(s)
Checking outdated entries in the index files if they physically exist in the backup destination(s)
No index-related issues found
Periodic Data Integrity Check completed
y
z
c
e
>90
Removing index files from the backup destination(s) which are more than 90 days old
Removing outdated entries in the index files which do not physically exist in backup destination(s)
Storage Statistics recalculated
Uploading index files with no issues to the current backup destination(s)
f
Continue backup job

a Check the index files in the backup destination(s) to determine if they were more than 90 days old.

➔ If **YES**, proceed to y

➔ If **NO**, proceed to b

b Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).

➔ If **YES**, proceed to c

➔ If **NO**, proceed to z

c Storage Statistics for Data area and Retention area usage will be recalculated.

d Periodic Data Integrity check is completed.

e Index files with no issues will be uploaded to the current backup destination(s).

f The backup job process will continue.

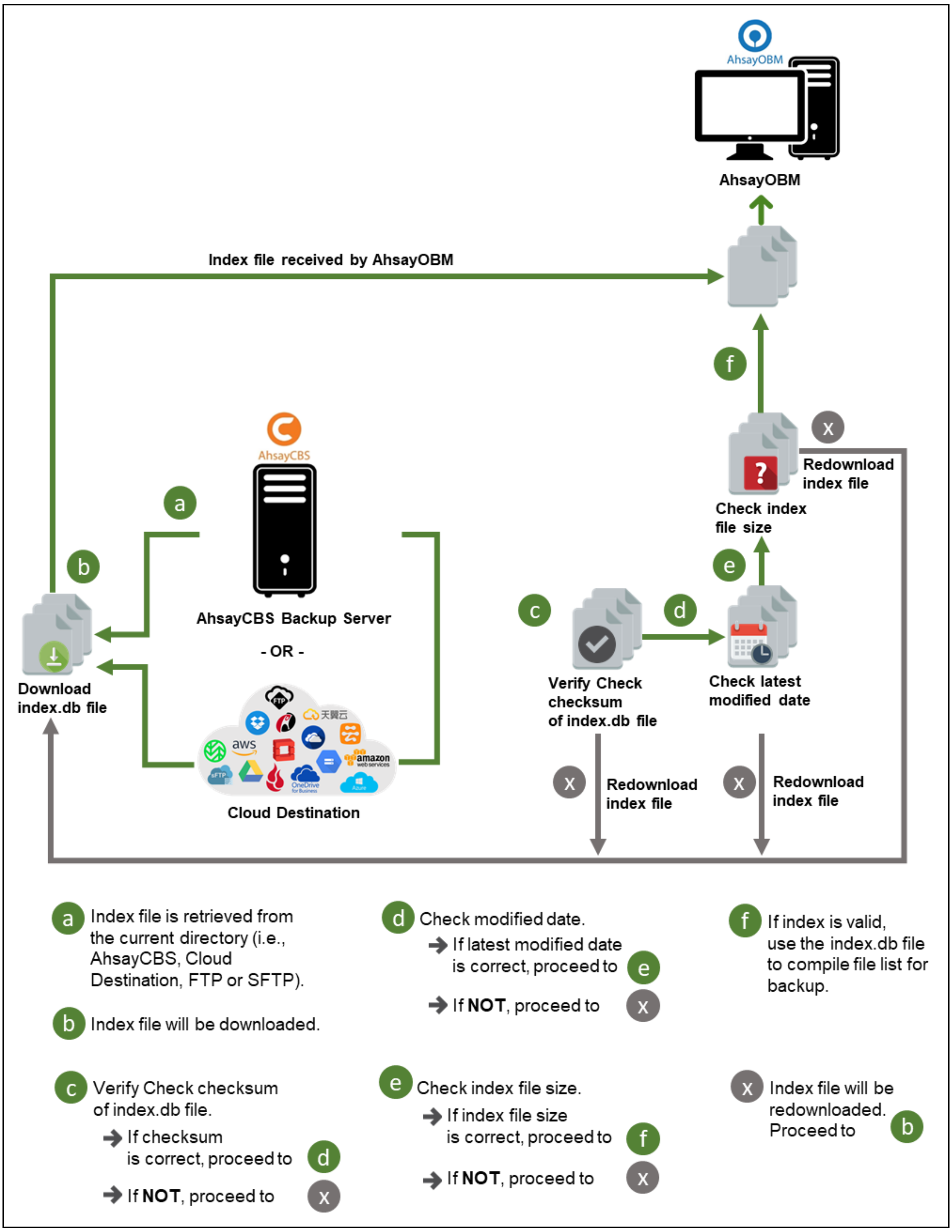
y Index files which are more than 90 days old will be removed from the backup destination(s).

z Outdated entries in the index files for files and/or folders which do not physically exist in backup destination(s) will be removed.

10.2 Backup Set Index Handling Process

To minimize the possibility of index related issues affecting backups, each time index files are downloaded from and uploaded to backup destination(s); the file size, last modified date, and checksum is verified to ensure index file integrity.

10.2.1 Start Backup Job



a Index file is retrieved from the current directory (i.e., AhsayCBS, Cloud Destination, FTP or SFTP).

b Index file will be downloaded.

c Verify Check checksum of index.db file.
➔ If checksum is correct, proceed to d
➔ If **NOT**, proceed to x

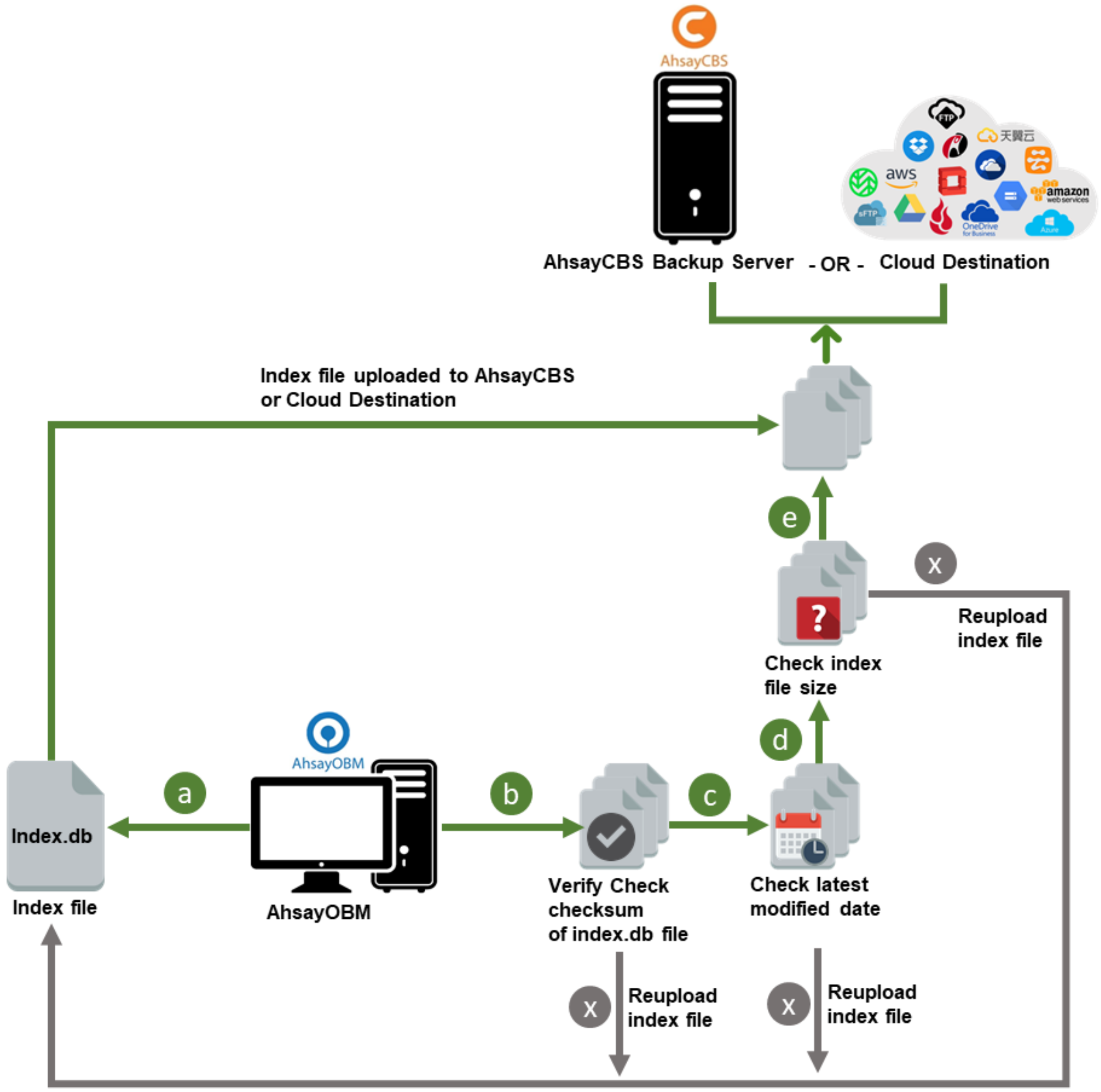
d Check modified date.
➔ If latest modified date is correct, proceed to e
➔ If **NOT**, proceed to x

e Check index file size.
➔ If index file size is correct, proceed to f
➔ If **NOT**, proceed to x

f If index is valid, use the index.db file to compile file list for backup.

x Index file will be redownloaded. Proceed to b

10.2.2 Completed Backup Job



a Index file from AhsayOBM is uploaded to AhsayCBS, Cloud Destination, FTP or SFTP.

b Verify Check checksum of index.db file.

- ➔ If checksum is correct, proceed to c
- ➔ If **NOT**, proceed to x

c Check modified date.

- ➔ If latest modified date is correct, proceed to d
- ➔ If **NOT**, proceed to x

d Check index file size.

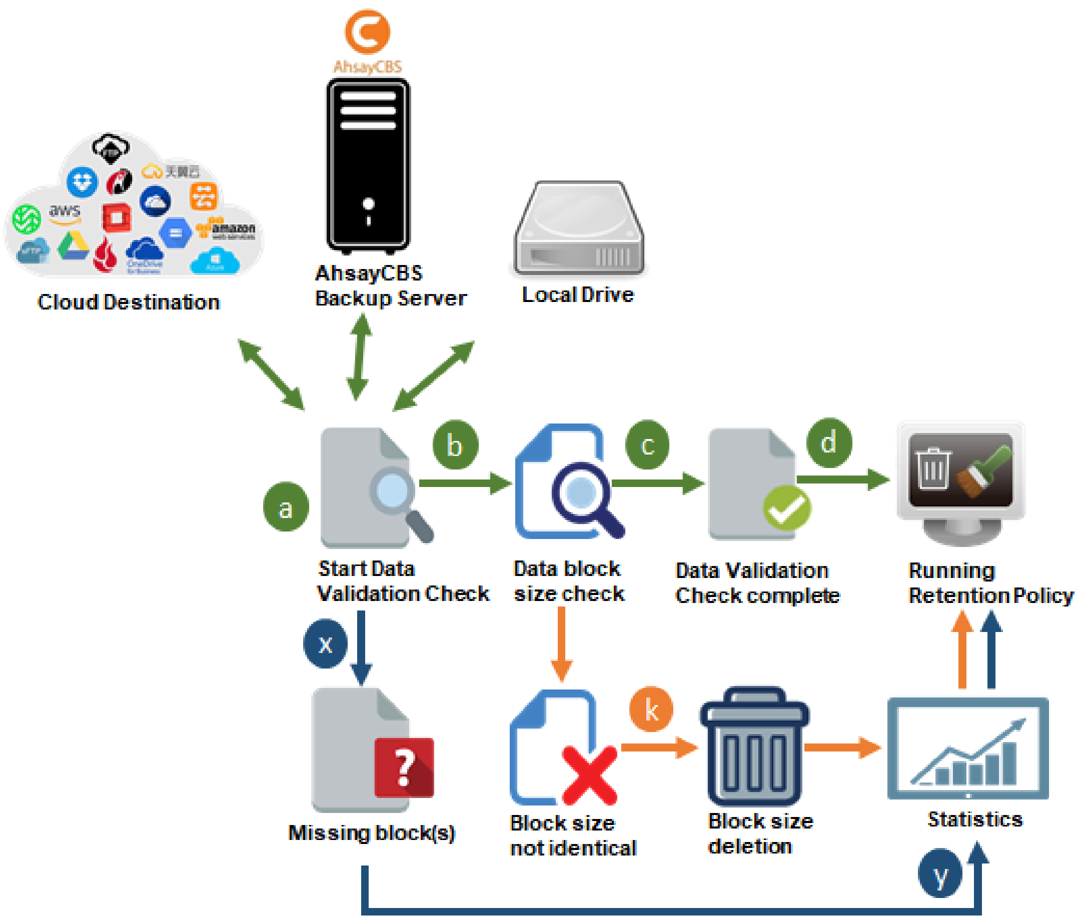
- ➔ If index file size is correct, proceed to e
- ➔ If **NOT**, proceed to x

e Index file is uploaded correctly to AhsayCBS or Cloud Destination.

x Index file will be reuploaded. Proceed to a

10.3 Data Validation Check Process

As an additional measure to ensure that all files transferred to the backup destination(s) are received and saved correctly, both the number of 8 or 16 MB data block files and the size of each block file are checked again after the files are transferred.



a Check the number of 8 or 16MB data blocks in the backup destination(s) is identical to the number of blocks transferred.

➔ If YES, proceed to b

➔ If NO, proceed to x

b Check the individual sizes of each data block in the backup destination(s) is identical to the sizes of each block transferred.

➔ If YES, proceed to c

➔ If NO, proceed to k

c Data validation check is complete.

d Retention Policy will run (if enabled).

x Files in the missing block(s) will be removed from the index.db file.

y Statistics will be updated according to the files removed.

Proceed to d

k Block size that are not identical will be removed from the backup destination(s).

Proceed to y then

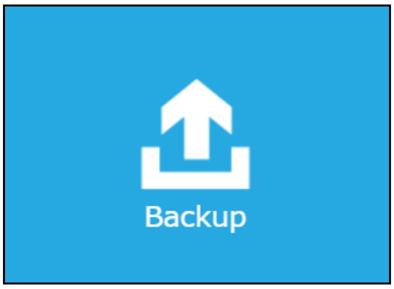
Proceed to d

11 Run Backup Jobs

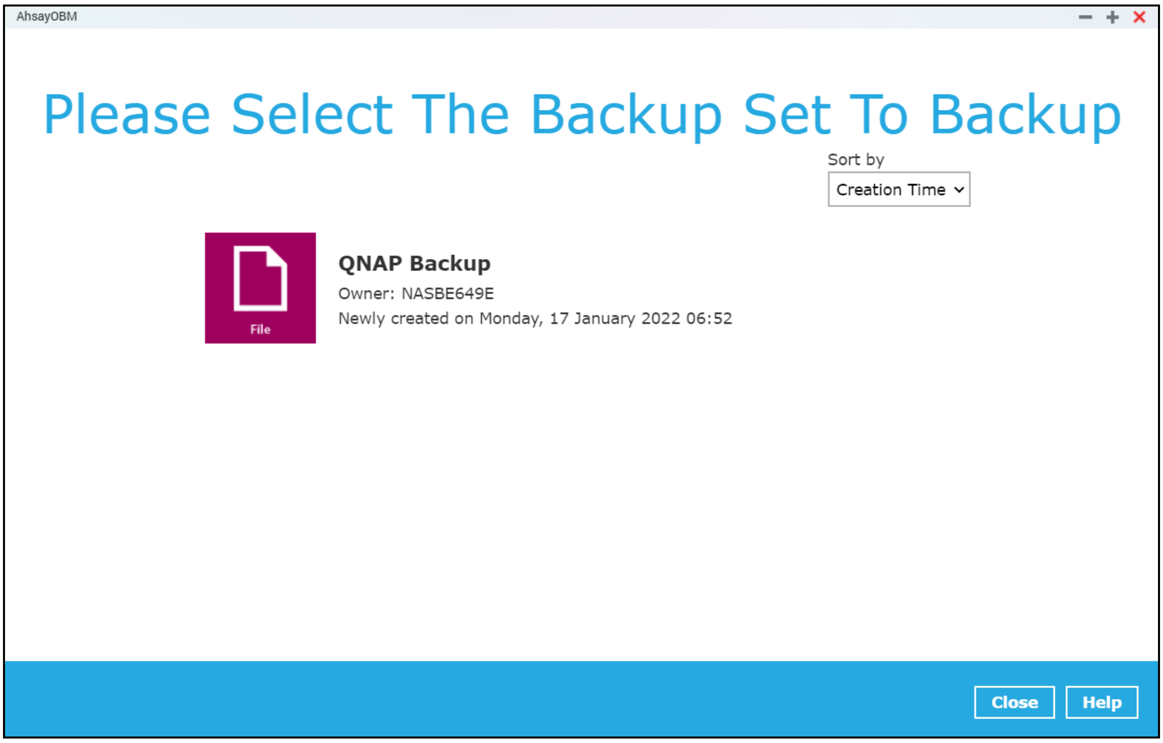
Start a Manual Backup

1. Login to the AhsayOBM application with the instructions provided in Chapter 5 Start AhsayOBM.

2. Click **Backup** on the main interface of AhsayOBM.



3. Select the backup set that you would like to start a backup job with.

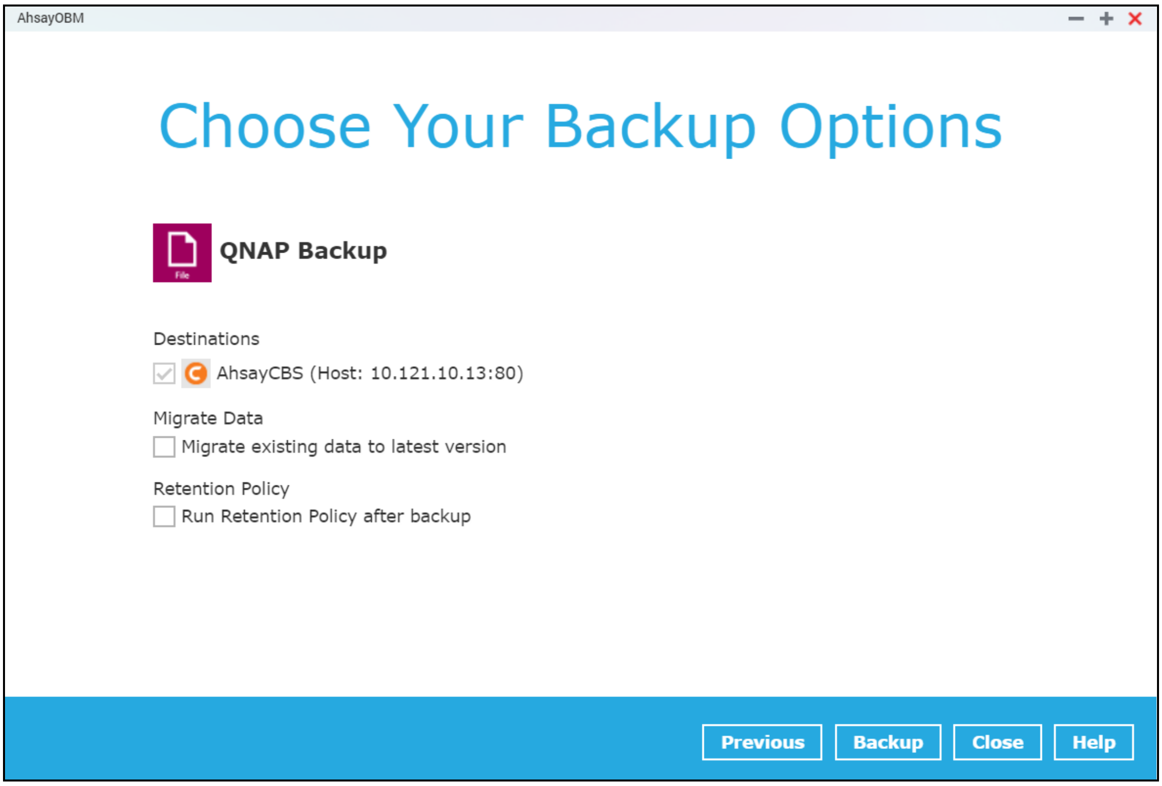


Please Select The Backup Set To Backup

Sort by: Creation Time

QNAP Backup
Owner: NASBE649E
Newly created on Monday, 17 January 2022 06:52

4. When the following options are shown, it is recommended that you tick the checkbox next to **Run Retention Policy after backup** in the Retention Policy section at the bottom. This will help you save hard disk quota in the long run.



Destinations

☑ AhsayCBS (Host: 10.121.10.13:80)

Migrate Data

□ Migrate existing data to latest version

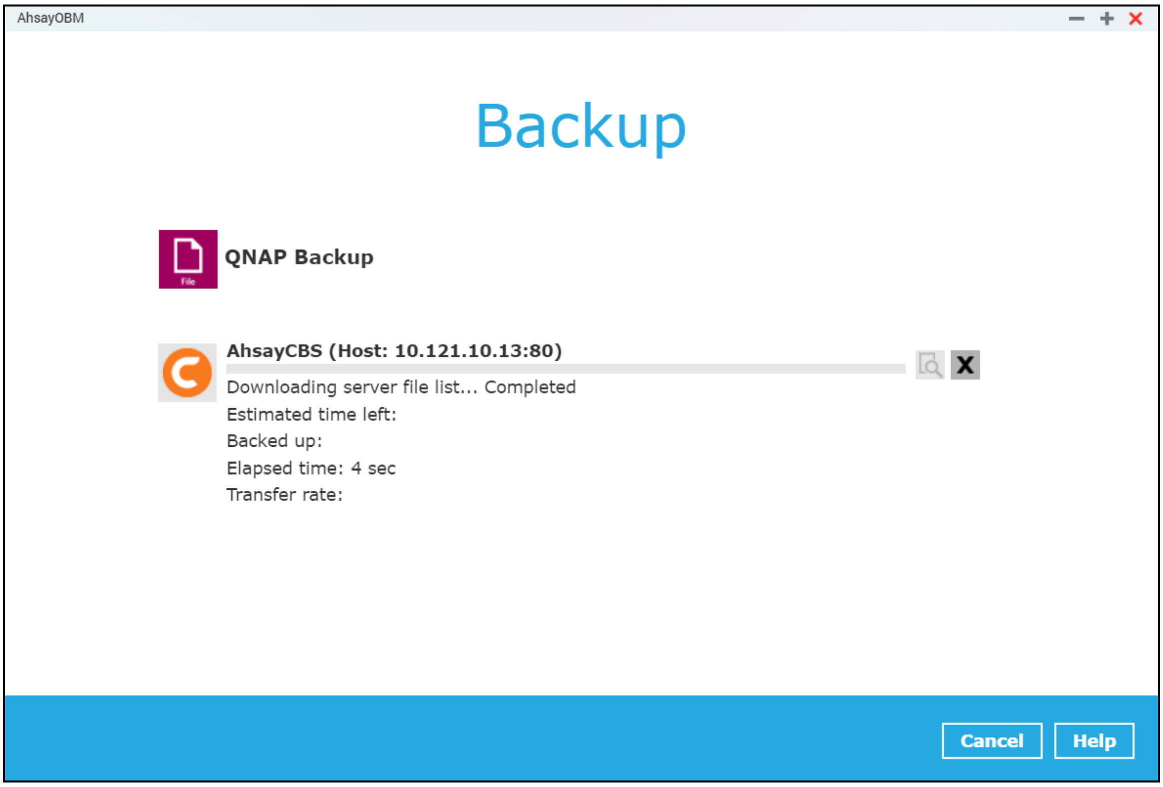
Retention Policy

□ Run Retention Policy after backup

NOTE

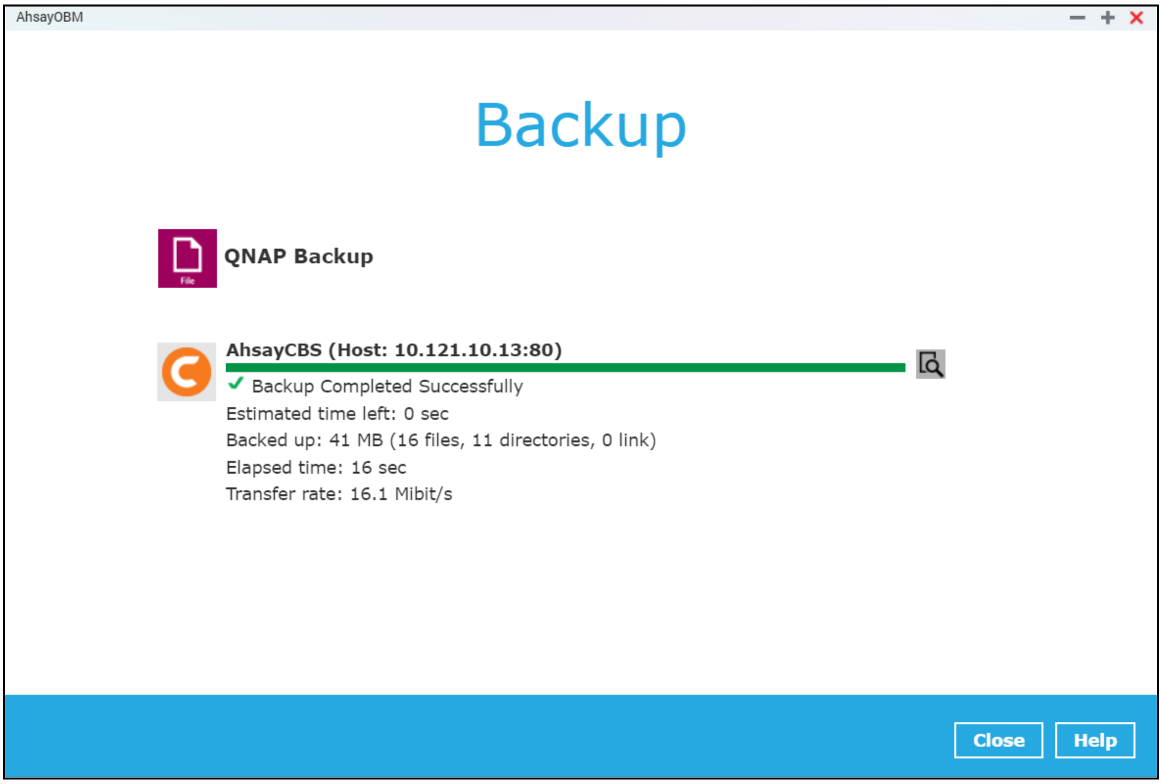
The **Migrate Data** option will only be displayed if Deduplication is enabled for the backup set. When the Migrate Data option is enabled, the existing data will be migrated to the latest version during a backup job. Backup job(s) for backup sets with Migrate Data enabled may take longer to finish. For more information about this feature, refer to AhsayCBS v9 New Features Supplemental document.

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



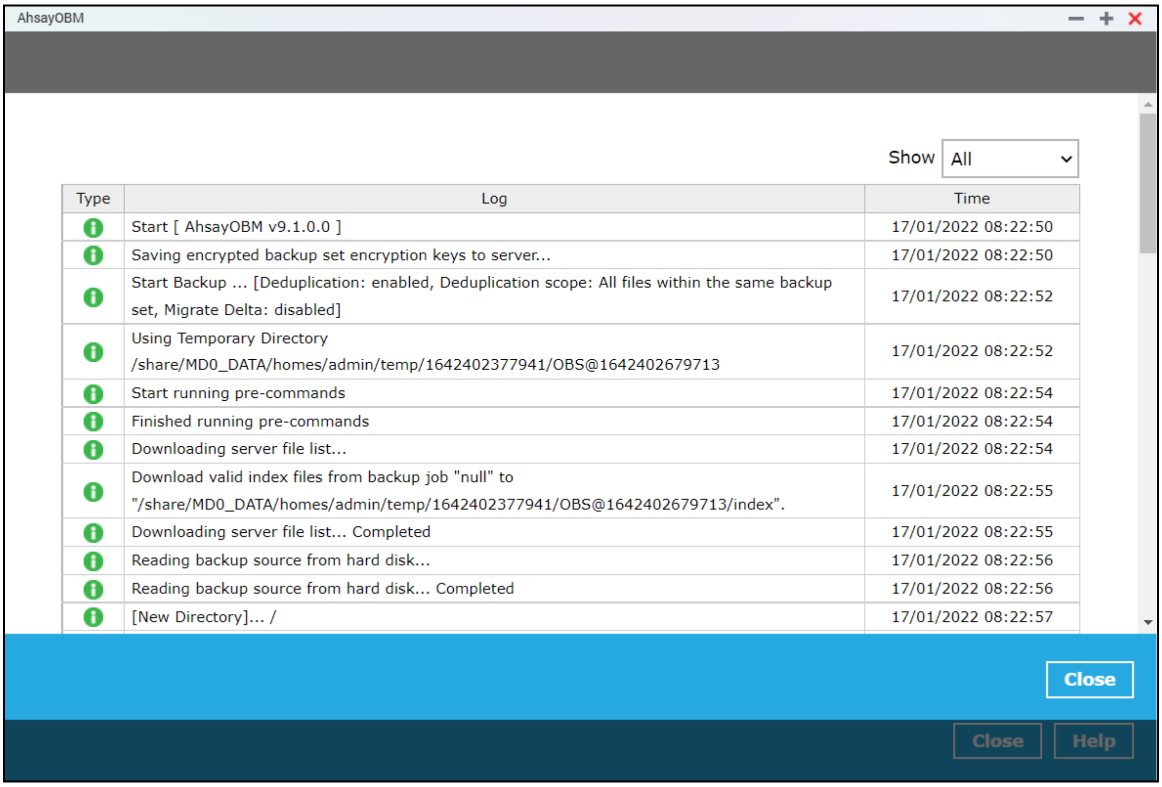
AhsayCBS (Host: 10.121.10.13:80)
Downloading server file list... Completed
Estimated time left:
Backed up:
Elapsed time: 4 sec
Transfer rate:

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



AhsayCBS (Host: 10.121.10.13:80)
✓ Backup Completed Successfully
Estimated time left: 0 sec
Backed up: 41 MB (16 files, 11 directories, 0 link)
Elapsed time: 16 sec
Transfer rate: 16.1 Mibit/s

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



Type	Log	Time
●	Start [AhsayOBM v9.1.0.0]	17/01/2022 08:22:50
●	Saving encrypted backup set encryption keys to server...	17/01/2022 08:22:50
●	Start Backup ... [Deduplication: enabled, Deduplication scope: All files within the same backup set, Migrate Delta: disabled]	17/01/2022 08:22:52
●	Using Temporary Directory /share/MD0_DATA/homes/admin/temp/1642402377941/OBS@1642402679713	17/01/2022 08:22:52
●	Start running pre-commands	17/01/2022 08:22:54
●	Finished running pre-commands	17/01/2022 08:22:54
●	Downloading server file list...	17/01/2022 08:22:54
●	Download valid index files from backup job "null" to "/share/MD0_DATA/homes/admin/temp/1642402377941/OBS@1642402679713/index".	17/01/2022 08:22:55
●	Downloading server file list... Completed	17/01/2022 08:22:55
●	Reading backup source from hard disk...	17/01/2022 08:22:56
●	Reading backup source from hard disk... Completed	17/01/2022 08:22:56
●	[New Directory]... /	17/01/2022 08:22:57

12 Restore Data

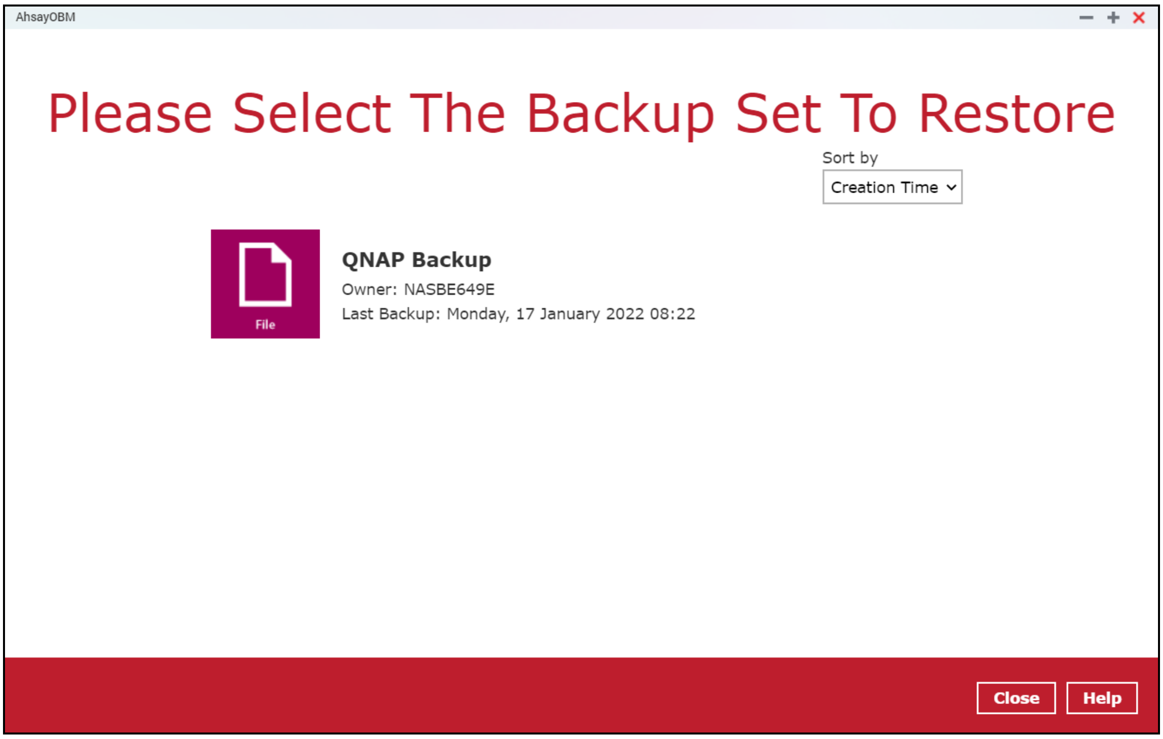
12.1 Login to AhsayOBM

Login to the AhsayOBM application with the instructions provided in Login to AhsayOBM.

12.2 Restore Data

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

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

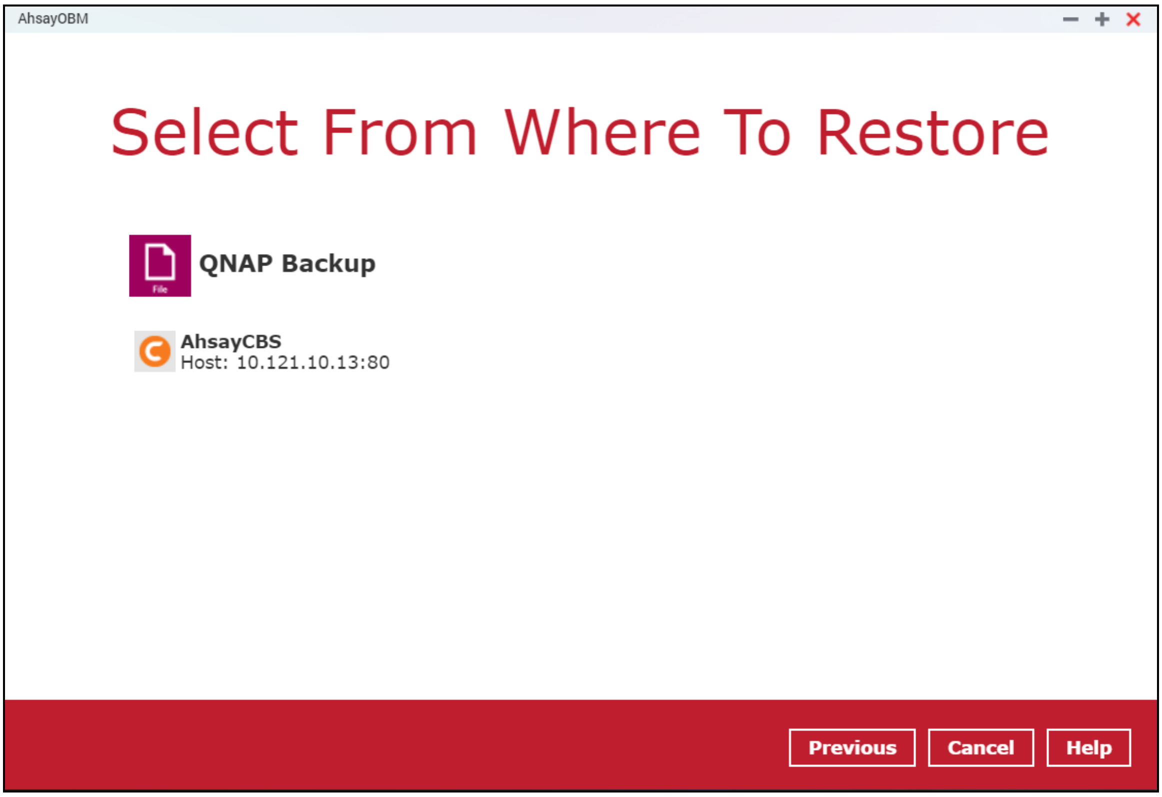

AhsayOBM

Please Select The Backup Set To Restore

Sort by: Creation Time

QNAP Backup
Owner: NASBE649E
Last Backup: Monday, 17 January 2022 08:22

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



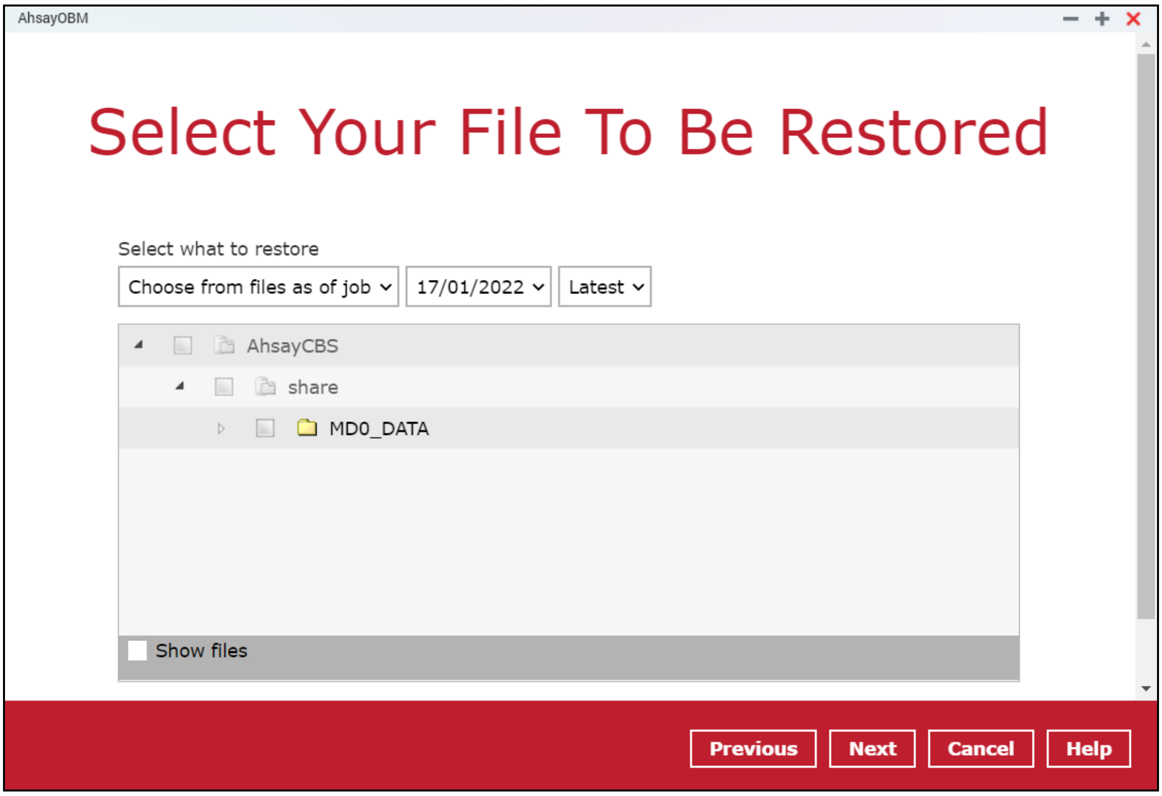
AhsayOBM

Select From Where To Restore

QNAP Backup

AhsayCBS
Host: 10.121.10.13:80

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



AhsayOBM

Select Your File To Be Restored

Select what to restore

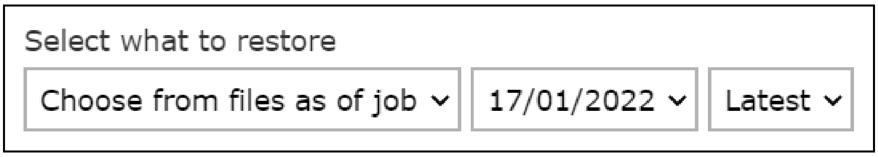
Choose from files as of job | 17/01/2022 | Latest

- AhsayCBS
  - share
    - MD0_DATA

□ Show files

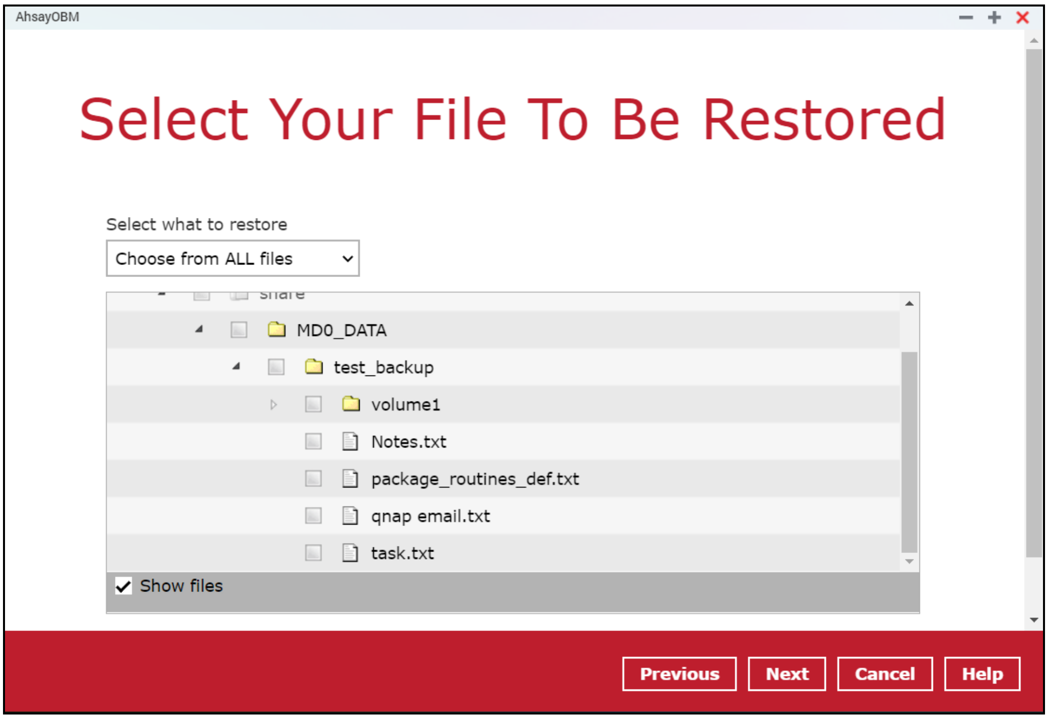
There are two options from the **Select what to restore** drop-down menu:

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



Select what to restore

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



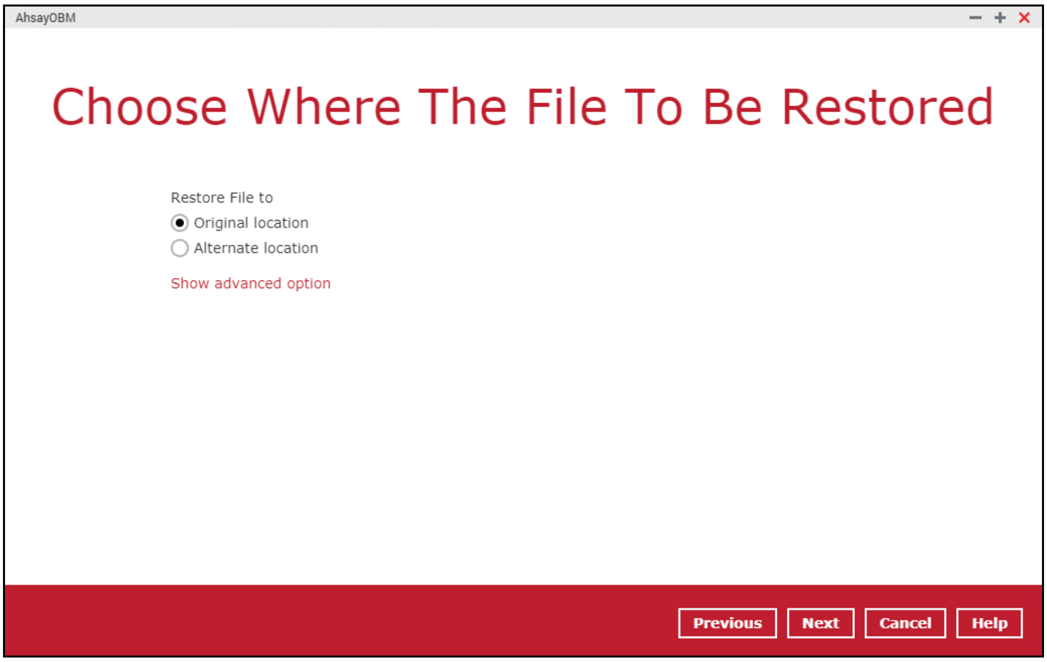
Select Your File To Be Restored

Select what to restore: Choose from ALL files

Click the **Show files** checkbox to select individual files for restoration. Click **Next** to proceed when you are done with the selections.

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

- **Original location** – the backed up data will be restored to the computer running the AhsayOBM under the same directory path as on the machine storing the backup source. For example, if the backup source files are stored under **Users/[User's Name]/Downloads** folder, the data will be restored to **Users/[User's Name]/Downloads** as well on the computer running the AhsayOBM.



Choose Where The File To Be Restored

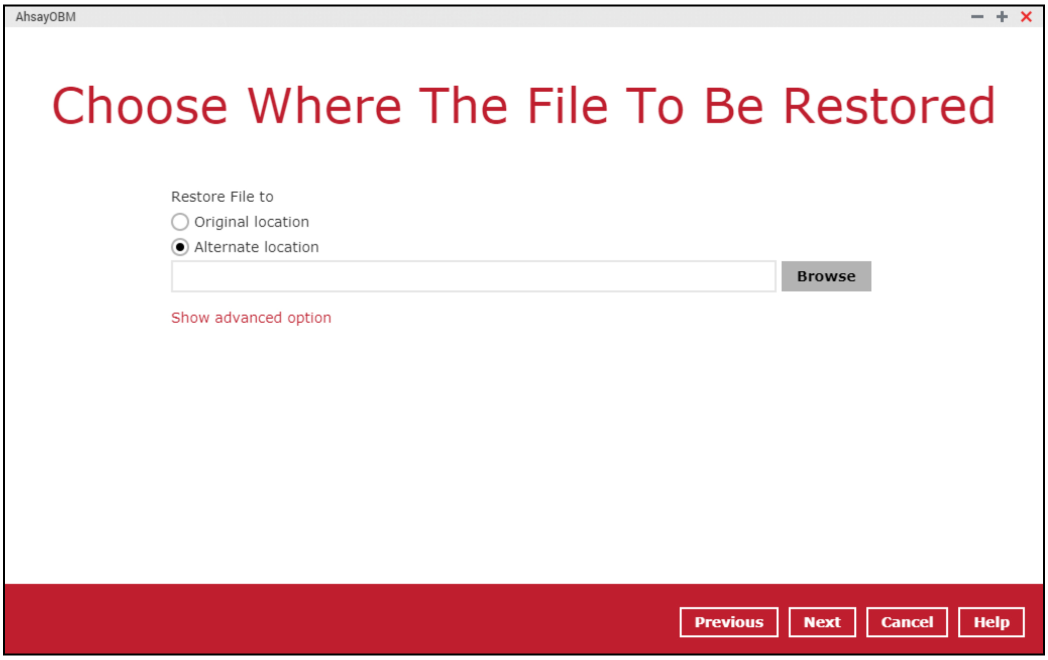
Restore File to

● Original location

○ Alternate location

Show advanced option

- **Alternate location** – you can choose to restore the data to a location of your choice on the computer where AhsayOBM is running.



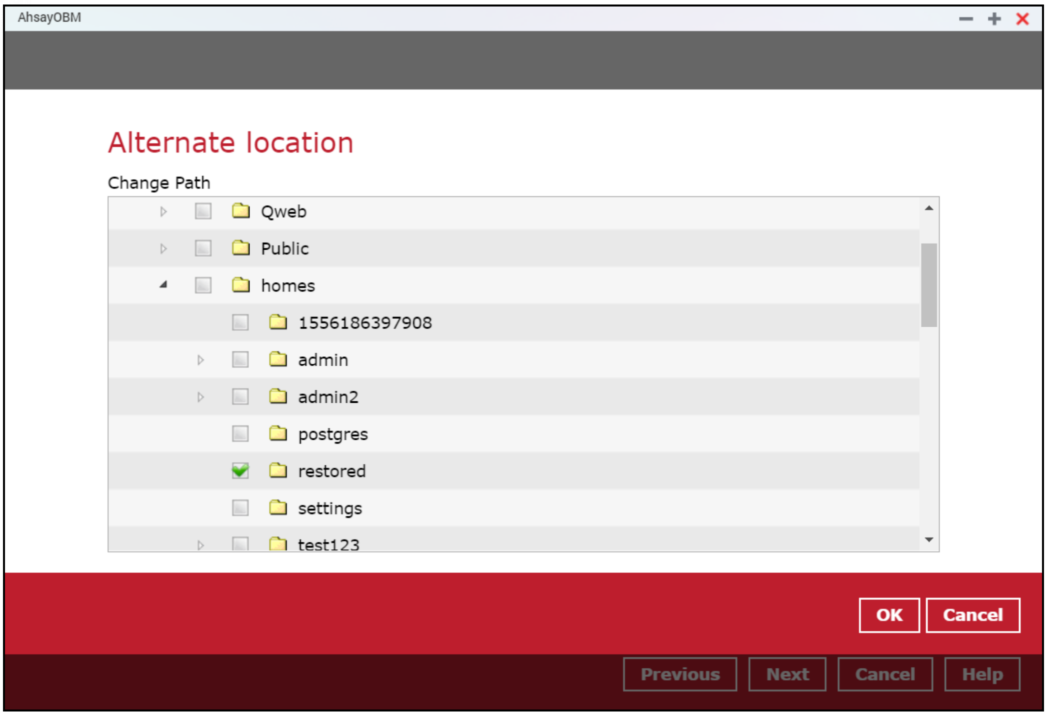
Choose Where The File To Be Restored

Restore File to

○ Original location

● Alternate location

Show advanced option

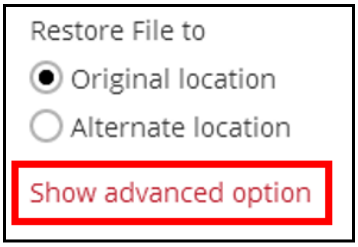


Alternate location

Change Path

- Qweb
- Public
- homes
  - 1556186397908
  - admin
  - admin2
  - postgres
  - ☑ restored
  - settings
  - test123

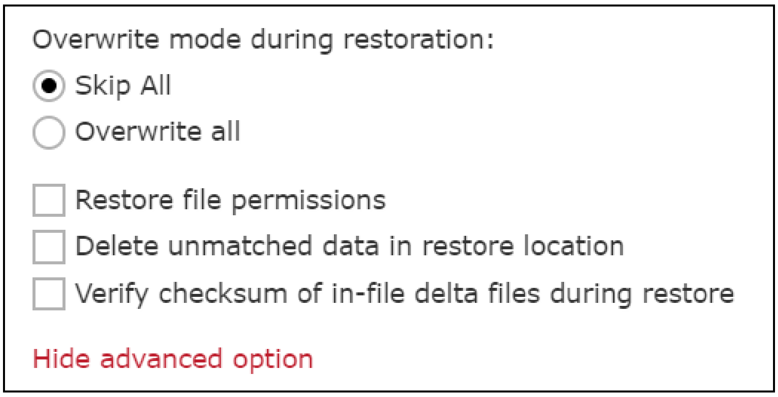
6. Click **Show advanced option** to configure other restore settings:


Restore File to

● Original location

○ Alternate location

Show advanced option


Overwrite mode during restoration:

● Skip All

○ Overwrite all

□ Restore file permissions

□ Delete unmatched data in restore location

□ Verify checksum of in-file delta files during restore

Hide advanced option

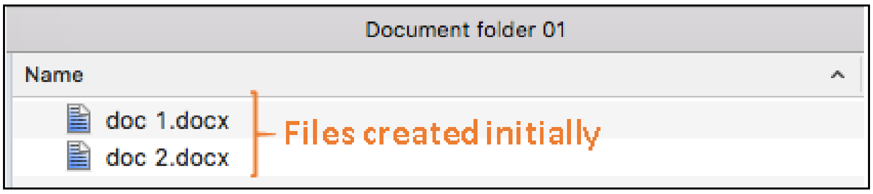
- **Overwrite mode during restoration**
  When there are file name conflicts during restoration, you can choose to skip them all or overwrite all existing files in the restore destination.

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

- **Delete unmatched data in restore location**
  Synchronize the selected restore source with the restore destination. By enabling this option, the restore process will attempt to synchronize the selected restore source with the restore destination, making sure the data in the restore destination is exactly the same as the restore source. Any data created after backup will be treated as “unmatched data” and will be deleted from the restore source if this feature is enabled.

  Example:

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



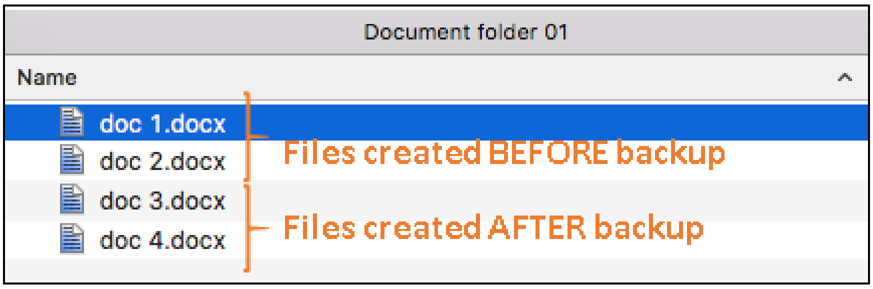
Document folder 01

Name

doc 1.docx
doc 2.docx

Files created initially

  - A backup is performed for folder Document folder 01.
  - Two new files are created, namely doc 3 & doc 4.



Document folder 01

Name

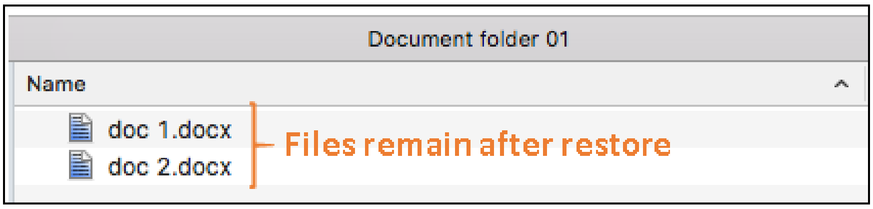
doc 1.docx
doc 2.docx

Files created BEFORE backup

doc 3.docx
doc 4.docx

Files created AFTER backup

  - A restore is performed for the Document folder 01, with Delete unmatched data in restore location option enabled.
  - Since doc 3 & doc 4 have never been backed up, therefore they will be deleted from Document folder 01, leaving only the two files that have been backed up.



Document folder 01

Name

doc 1.docx
doc 2.docx

Files remain after restore

WARNING

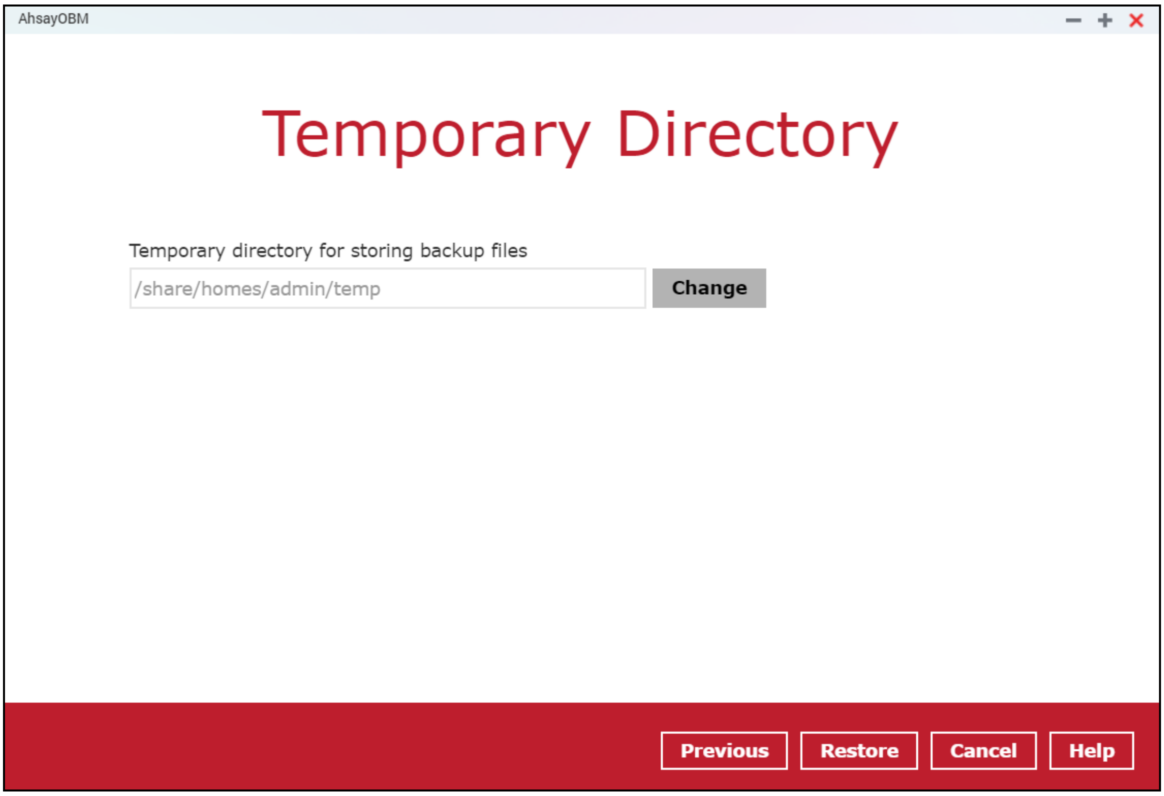
Please exercise extra caution when enabling this feature. Consider what data in the restore source has not been backed up and what impact it would cause if those data were deleted.

Prior to the data restore and synchronization, a warning message will be displayed. Only clicking **Yes** will the “unmatched data” be deleted. You can click **Apply to all** to confirm deleting all the “unmatched data” at one time.

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

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

7. Select the temporary directory for storing temporary files, such as delta files when they are being merged.

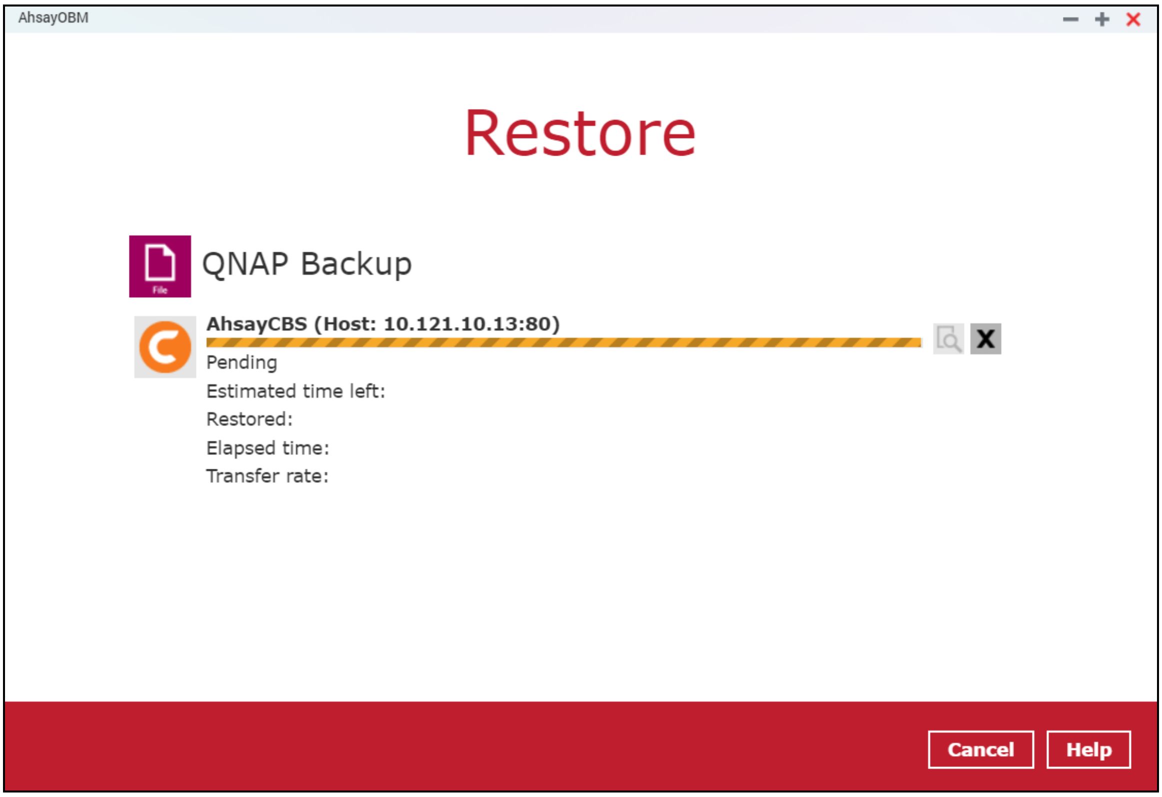


Temporary Directory

Temporary directory for storing backup files

/share/homes/admin/temp

8. Click **Restore** to start the restore. The status will be shown.



Restore

QNAP Backup

AhsayCBS (Host: 10.121.10.13:80)

Pending

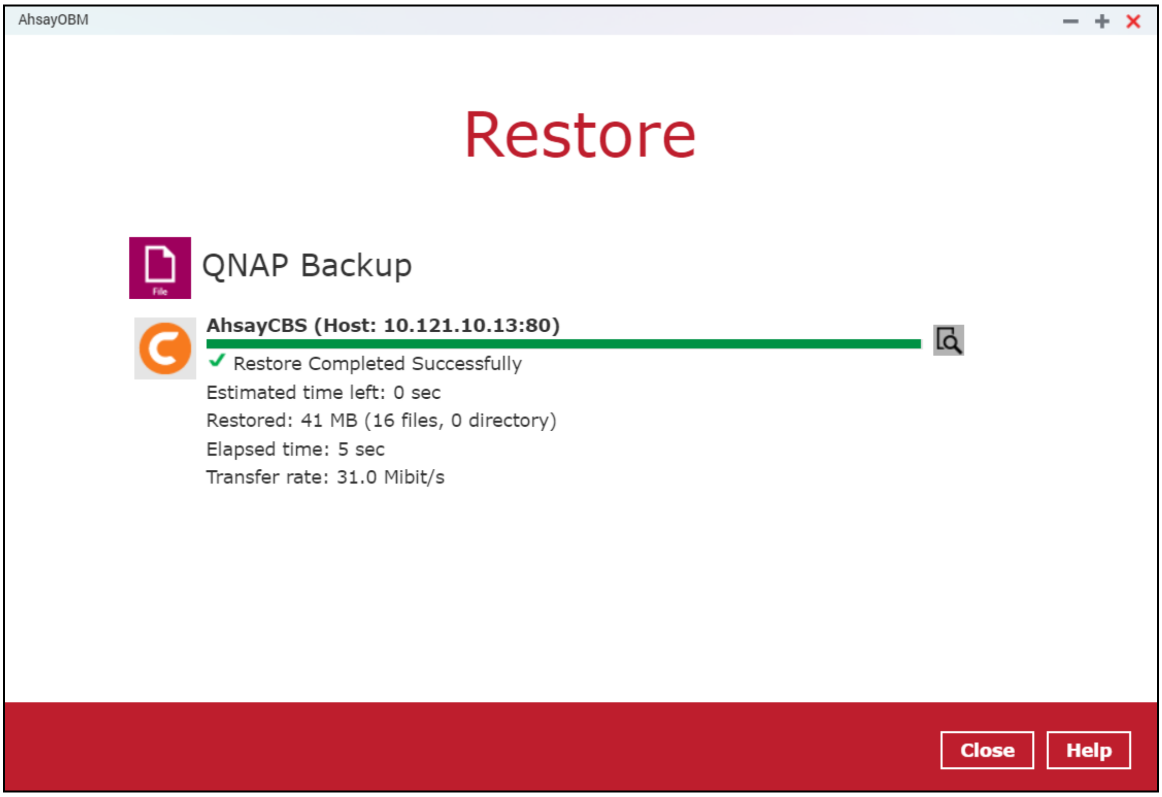
Estimated time left:

Restored:

Elapsed time:

Transfer rate:

9. When the restore is completed, the progress bar will be green in color and the message **Restore Completed Successfully** will appear.



AhsayCBS (Host: 10.121.10.13:80)

✓ Restore Completed Successfully

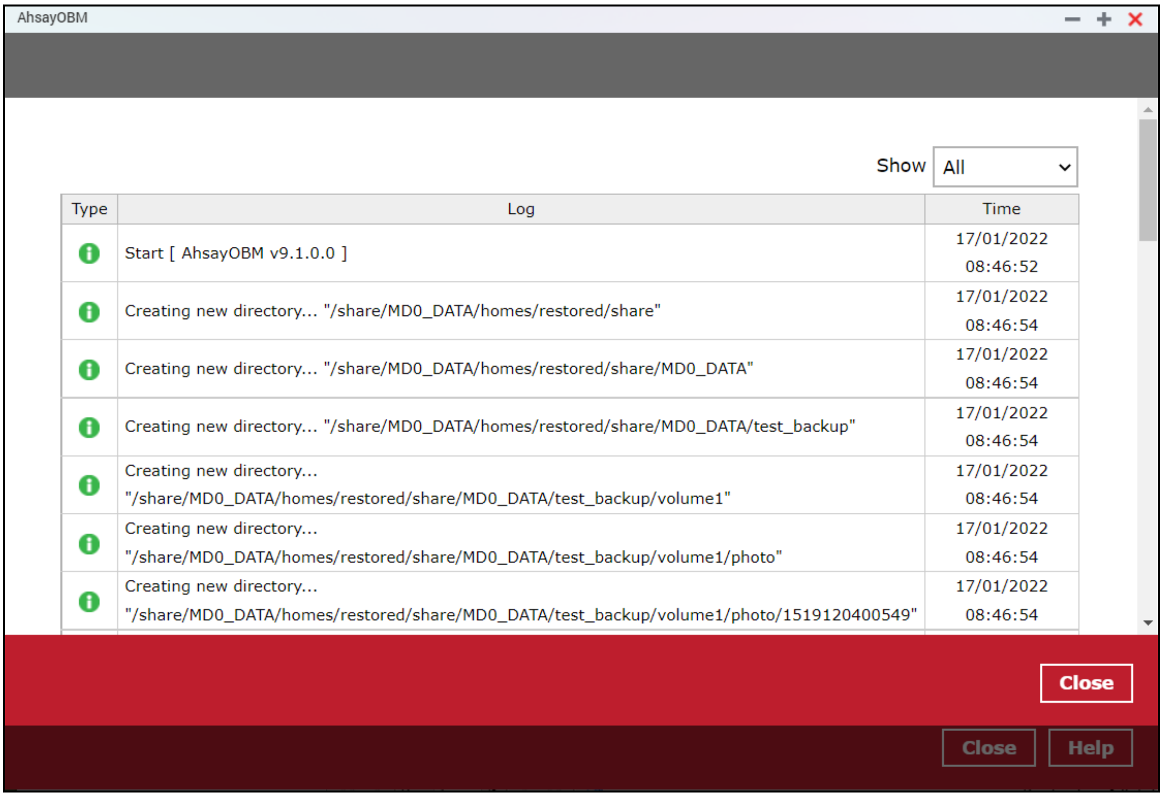
Estimated time left: 0 sec

Restored: 41 MB (16 files, 0 directory)

Elapsed time: 5 sec

Transfer rate: 31.0 Mibit/s

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



Type	Log	Time
ⓘ	Start [AhsayOBM v9.1.0.0]	17/01/2022 08:46:52
ⓘ	Creating new directory... "/share/MD0_DATA/homes/restored/share"	17/01/2022 08:46:54
ⓘ	Creating new directory... "/share/MD0_DATA/homes/restored/share/MD0_DATA"	17/01/2022 08:46:54
ⓘ	Creating new directory... "/share/MD0_DATA/homes/restored/share/MD0_DATA/test_backup"	17/01/2022 08:46:54
ⓘ	Creating new directory... "/share/MD0_DATA/homes/restored/share/MD0_DATA/test_backup/volume1"	17/01/2022 08:46:54
ⓘ	Creating new directory... "/share/MD0_DATA/homes/restored/share/MD0_DATA/test_backup/volume1/photo"	17/01/2022 08:46:54
ⓘ	Creating new directory... "/share/MD0_DATA/homes/restored/share/MD0_DATA/test_backup/volume1/photo/1519120400549"	17/01/2022 08:46:54

10. In the Restore window, click **Close** to close the Restore window.

13 Contact Ahsay

13.1 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/

13.2 Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/downloads/ahsay-downloads_documentation_guides.jsp

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

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

Appendix

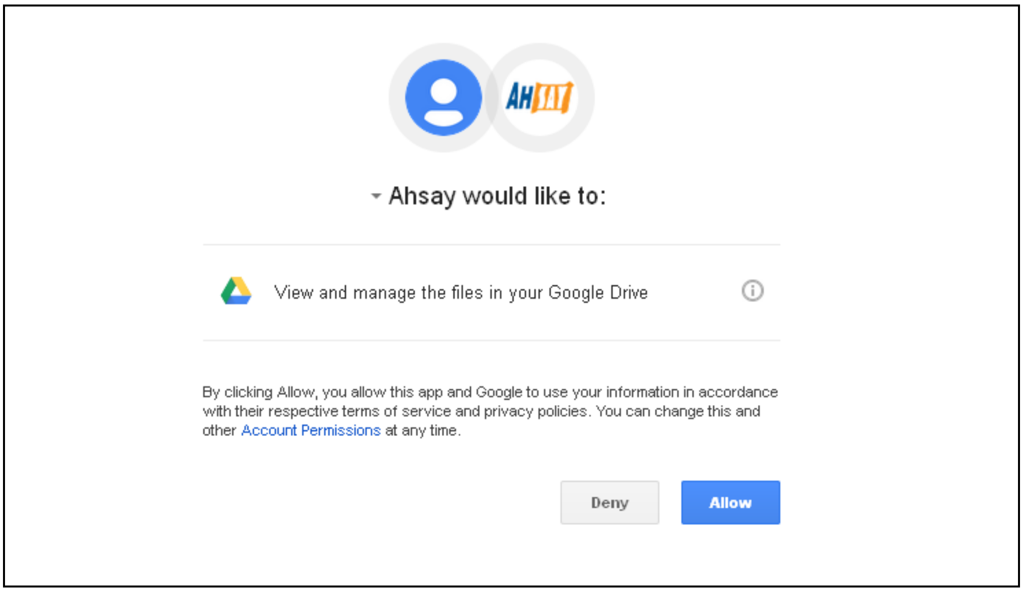
Appendix A: Cloud Storage as Backup Destination

For most cloud storage providers (e.g. Dropbox, Google Drive, etc.), you need to enable access of AhsayOBM on your cloud destination. Click **OK** / **Test**, you will be prompted to login to the corresponding cloud service.

IMPORTANT

The authentication request will be opened in a new tab / window on the browser, ensure that the pop-up tab / window is not blocked.

1. Click **Allow** to permit AhsayOBM to access the cloud storage.

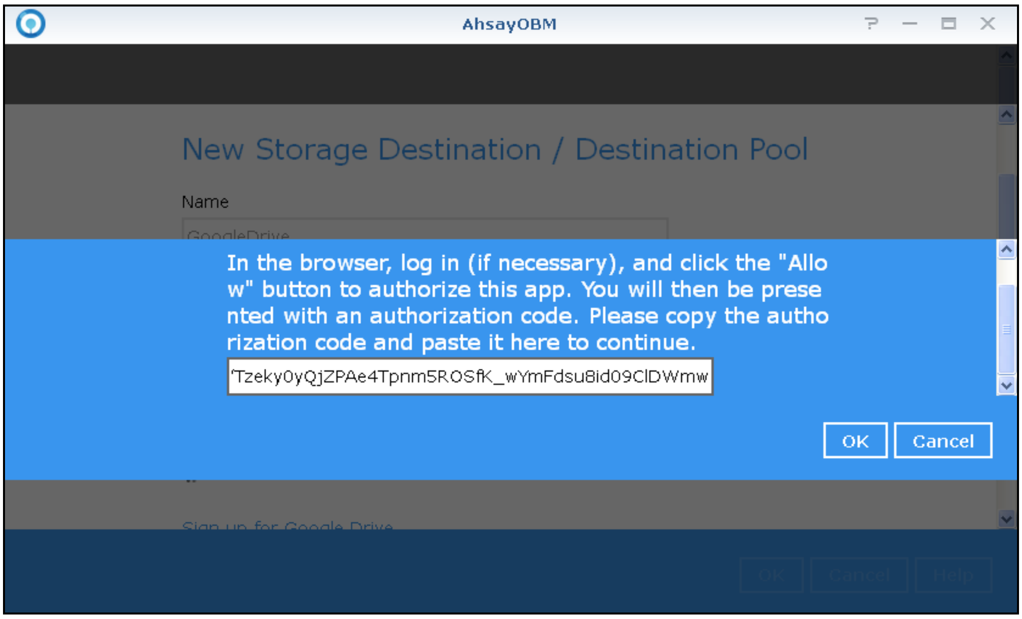


Ahsay would like to:

View and manage the files in your Google Drive

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

2. Enter the authentication code returned in AhsayOBM to complete the destination setup.



Name

GoogleDrive

In the browser, log in (if necessary), and click the "Allo w" button to authorize this app. You will then be prese nted with an authorization code. Please copy the autho rization code and paste it here to continue.

'Tzeky0yQjZPAe4Tpnm5ROSfK_wYmFdsu8id09ClDWmw

NOTE

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

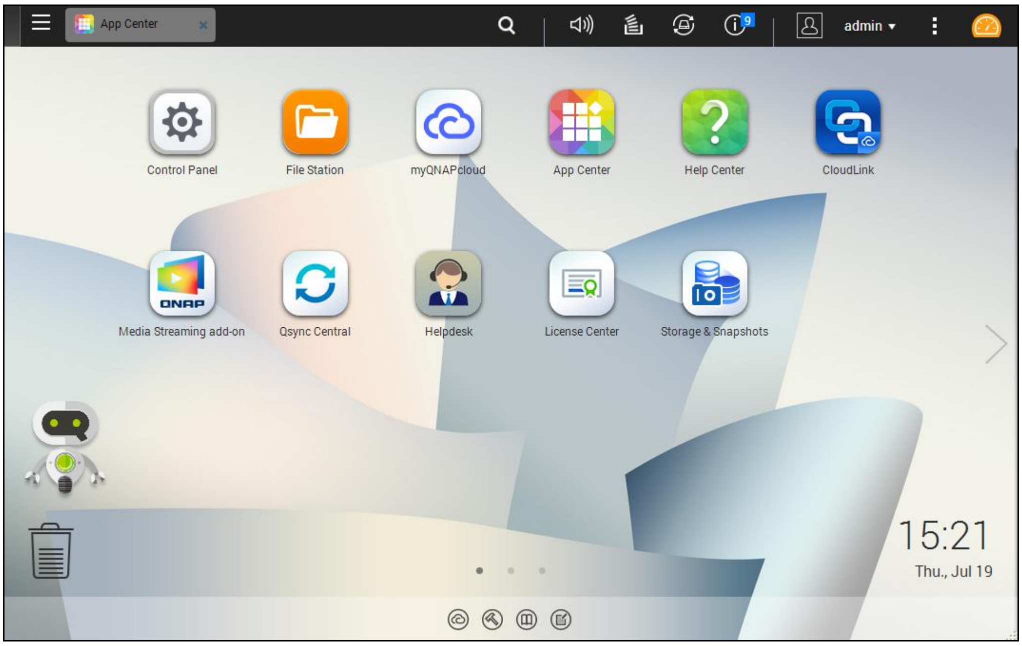
Multiple backup destinations can be configured for a single backup set. In fact it is recommended for you to set up at least 2 backup destinations for your backup set.

For more details on backup destination, for example which cloud service providers are supported, destination type, or limitation, you can refer to the following article:
FAQ: Frequently Asked Questions on Backup Destination

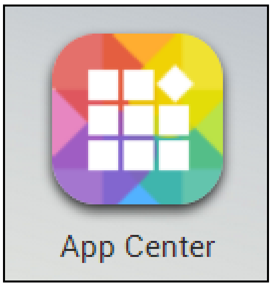
Appendix B: Uninstall AhsayOBM

Refer to the following steps to uninstall AhsayOBM.

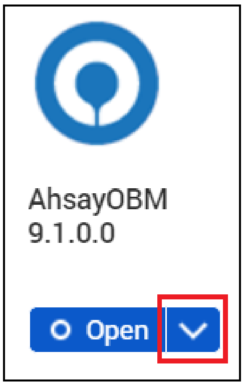
1. Login to QNAP QTS with the admin account. In a web browser, enter the QNAP NAS device IP address and use the login credentials to login.



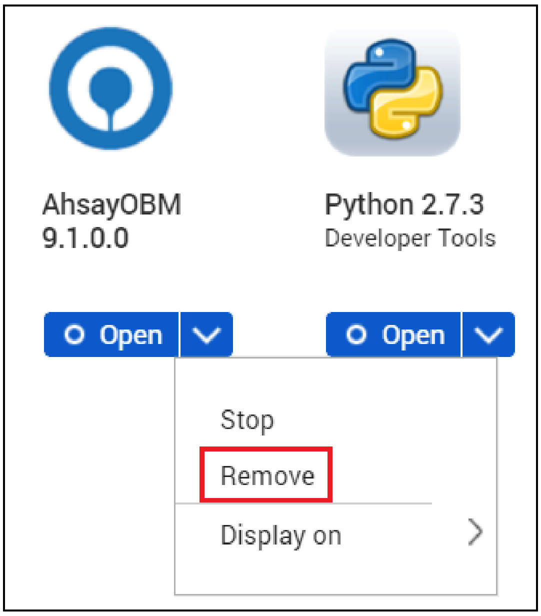
2. Click the App Center icon on the desktop.



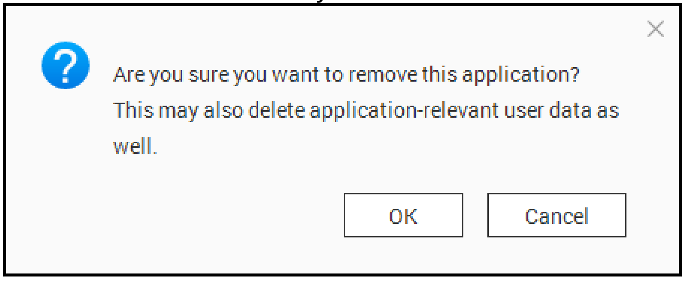
3. When the App Center window appears, click the arrow icon of AhsayOBM.



4. Select **Remove** to uninstall the AhsayOBM.



5. Click **OK** to uninstall AhsayOBM.

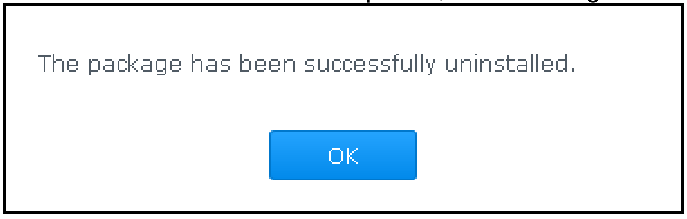


Are you sure you want to remove this application? This may also delete application-relevant user data as well.

NOTE

If you select **OK**, AhsayOBM program files, user settings and AhayOBM-relevant user data will be removed from the NAS drive.

6. When the uninstallation is completed, the following message will appear.



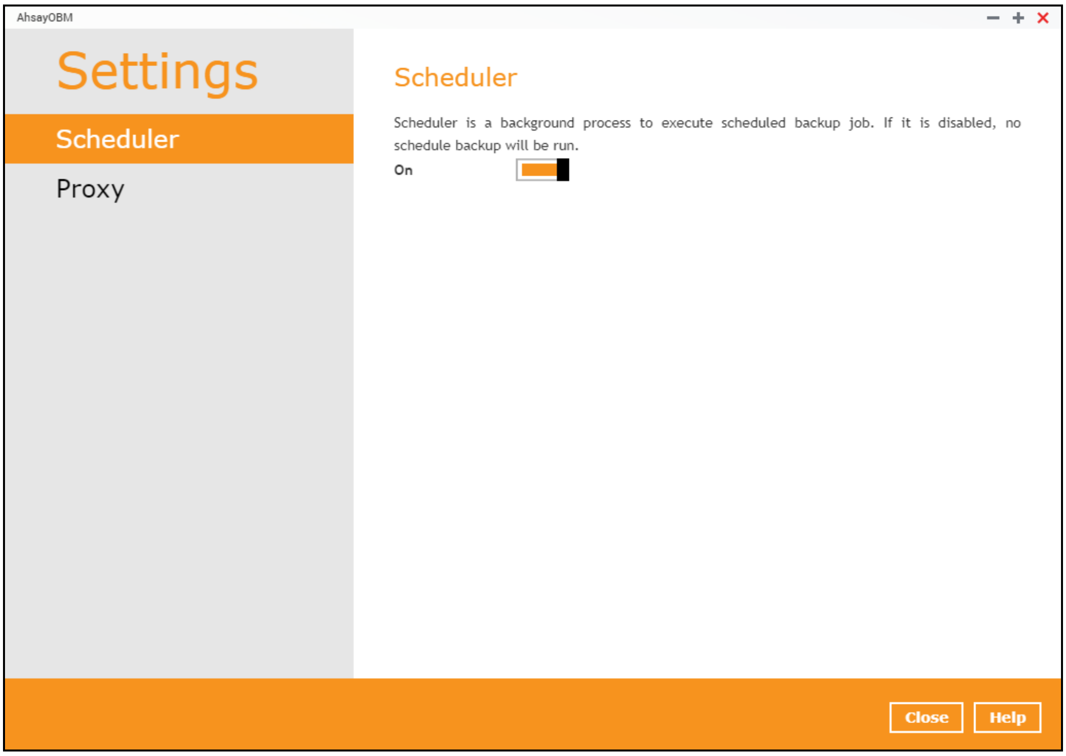
The package has been successfully uninstalled.

Appendix C: Scheduler Scenarios (pre-v9.3.2.0)

Starting with v9.3.2.0, Scheduler under Settings has been removed since the scheduler will be running together with AhsayOBM service once AhsayOBM is started in the App Center.

Applicable for pre-v9.3.2.0 AhsayOBM, NAS QNAP has two (2) levels of Scheduler settings for scheduled backup jobs.

Level 1: Scheduler under Settings

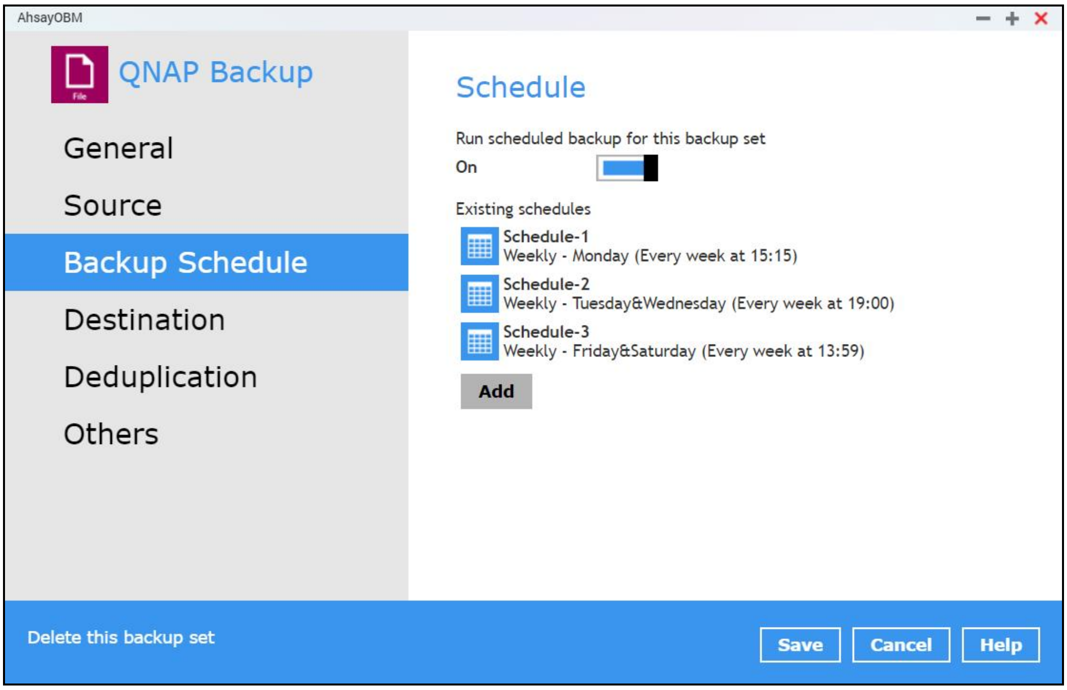


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

On

Level 2: Scheduler under Backup Set Settings



Schedule

Run scheduled backup for this backup set

On

Existing schedules

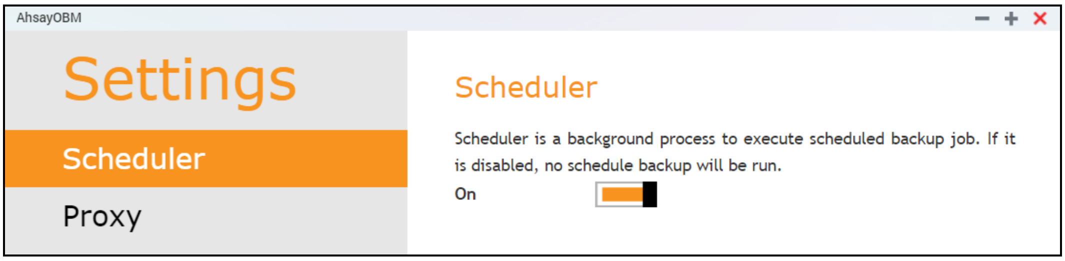
Schedule-1
Weekly - Monday (Every week at 15:15)

Schedule-2
Weekly - Tuesday&Wednesday (Every week at 19:00)

Schedule-3
Weekly - Friday&Saturday (Every week at 13:59)

Scenario no. 1: Scheduler under Settings is ON, and Scheduler under Backup Set Settings is OFF

Scheduler under Settings

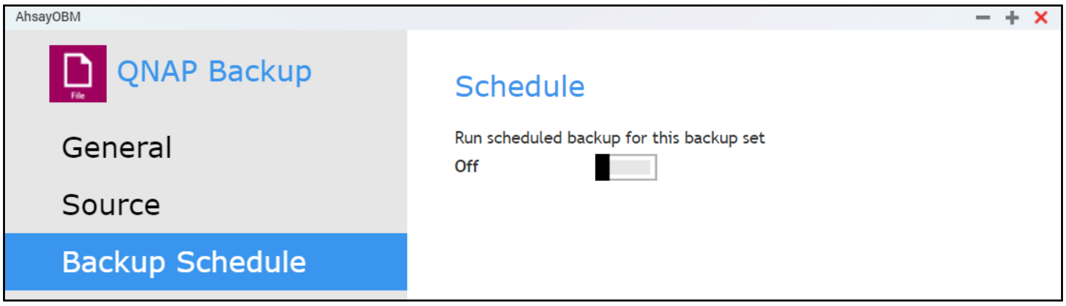


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

On

Scheduler under Backup Set Settings



Schedule

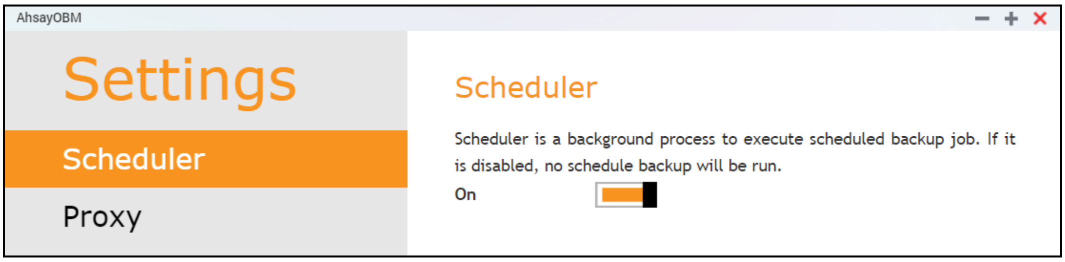
Run scheduled backup for this backup set

Off

Result: There is no scheduled backup job that will be run for the backup set.

Scenario no. 2: Scheduler under Settings is ON, and Scheduler under Backup Settings is ON

Scheduler under Settings

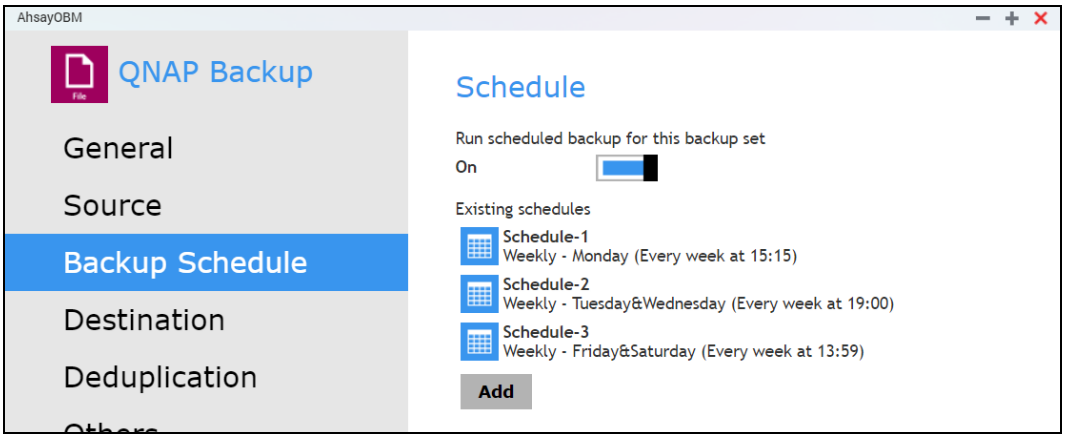


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

On

Scheduler under Backup Set Settings



Schedule

Run scheduled backup for this backup set

On

Existing schedules

Schedule-1
Weekly - Monday (Every week at 15:15)

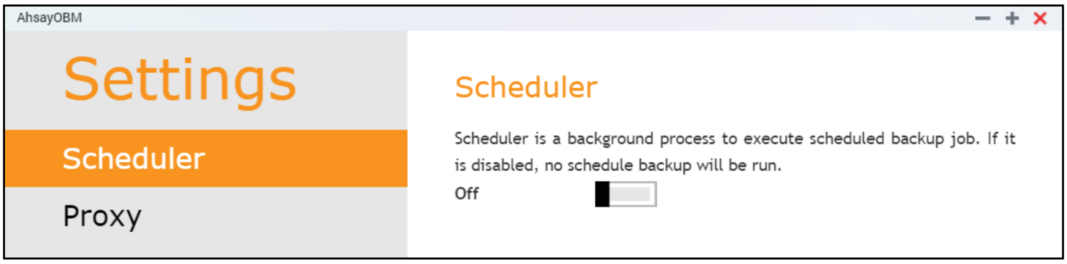
Schedule-2
Weekly - Tuesday&Wednesday (Every week at 19:00)

Schedule-3
Weekly - Friday&Saturday (Every week at 13:59)

Result: Scheduled backup jobs which are Schedule-1, Schedule-2, and Schedule-3 for the backup set will run.

Scenario no. 3: Scheduler under Settings is OFF, and Scheduler under Backup Set Settings is OFF

Scheduler under Settings

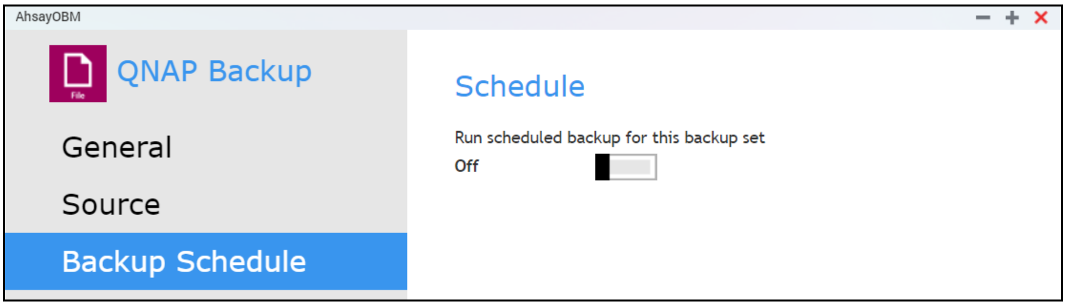


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

Off

Scheduler under Backup Set Settings



Schedule

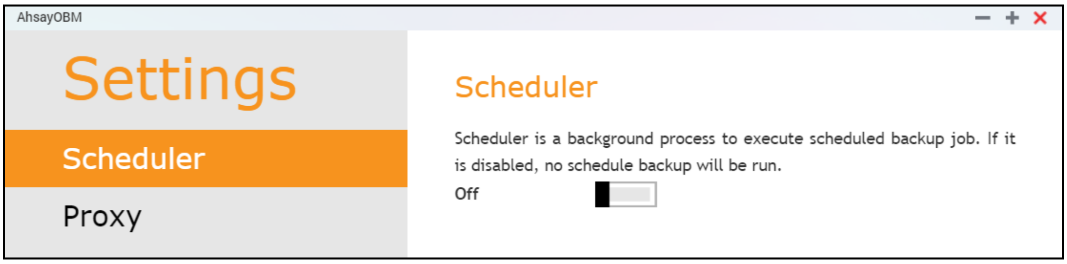
Run scheduled backup for this backup set

Off

Result: No scheduled backup job will be run for the backup set.

Scenario no. 4: Scheduler under Settings is OFF, and Scheduler under Backup Set Settings is ON

Scheduler under Settings

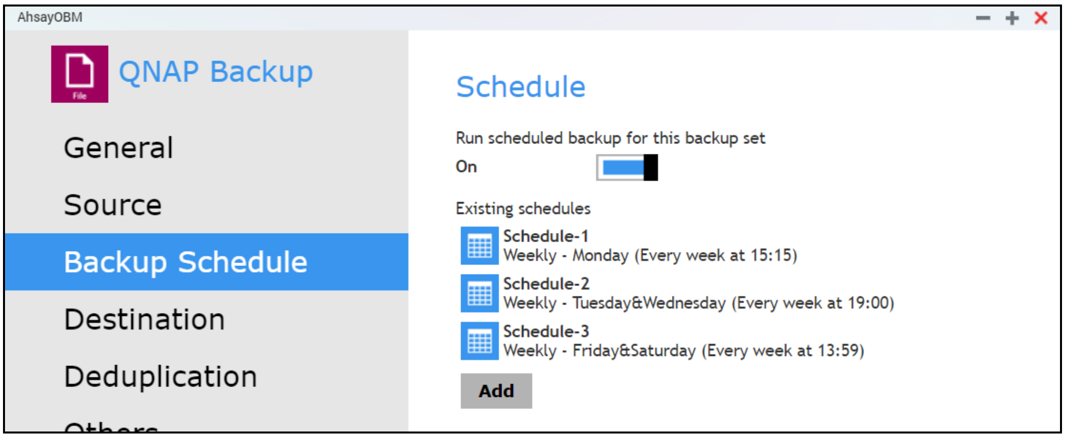


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

Off

Scheduler under Backup Set Settings



Schedule

Run scheduled backup for this backup set

On

Existing schedules

Schedule-1
Weekly - Monday (Every week at 15:15)

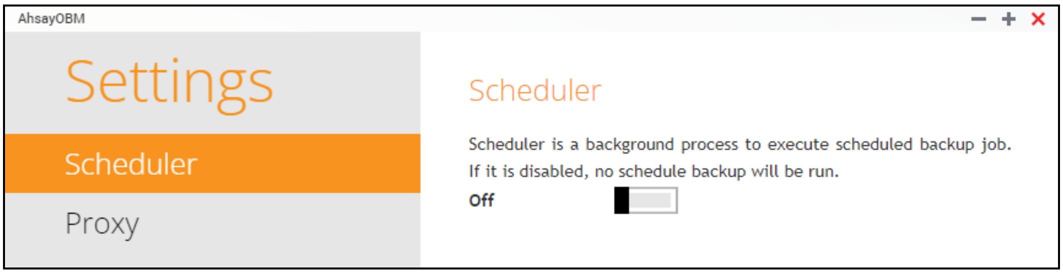
Schedule-2
Weekly - Tuesday&Wednesday (Every week at 19:00)

Schedule-3
Weekly - Friday&Saturday (Every week at 13:59)

Result: No scheduled backup job will be run for the backup set.

Scenario no. 5: Scheduler under Settings is OFF and turning ON Scheduler under Backup Set Settings

Scheduler under Settings

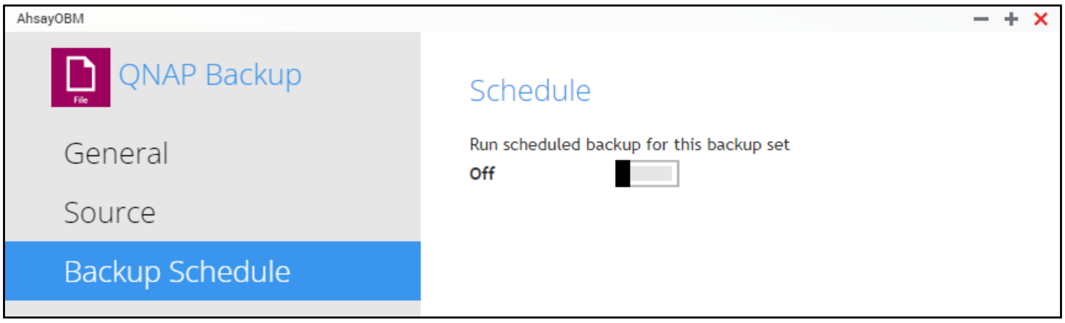


Scheduler

Scheduler is a background process to execute scheduled backup job. If it is disabled, no schedule backup will be run.

Off

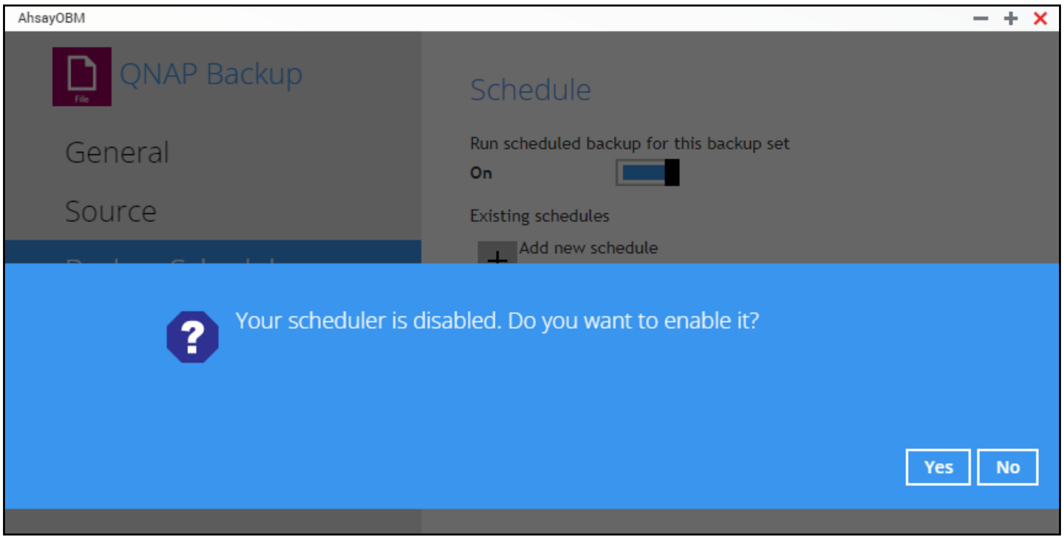
Scheduler under Backup Set Settings



Schedule

Run scheduled backup for this backup set

Off



Run scheduled backup for this backup set

On

Your scheduler is disabled. Do you want to enable it?

Result: There is an alert message that will be displayed confirming to set the Scheduler under Settings from OFF to ON.

If Yes is selected then the Scheduler under Settings will be turned ON. If No is selected, then the Scheduler under Settings will remain turned OFF.

Appendix D: Create Free Trial Account in AhsayOBM

Users can create a free trial account when they login to AhsayOBM for the first time. Please ensure that the following requirements are met before creating your trial account:

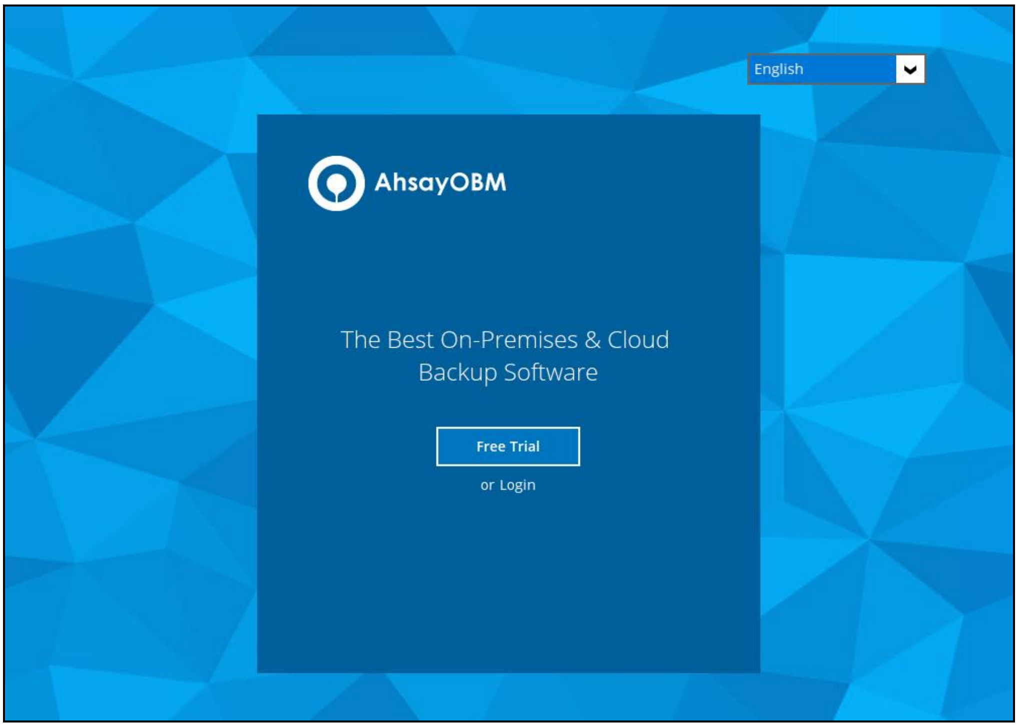
- A valid email address which will be used for receiving notices. A welcome message will also be sent upon creation of the account which specifies the User Setting and Quota set for backup in AhsayCBS.

While here are the limitations of a trial account:

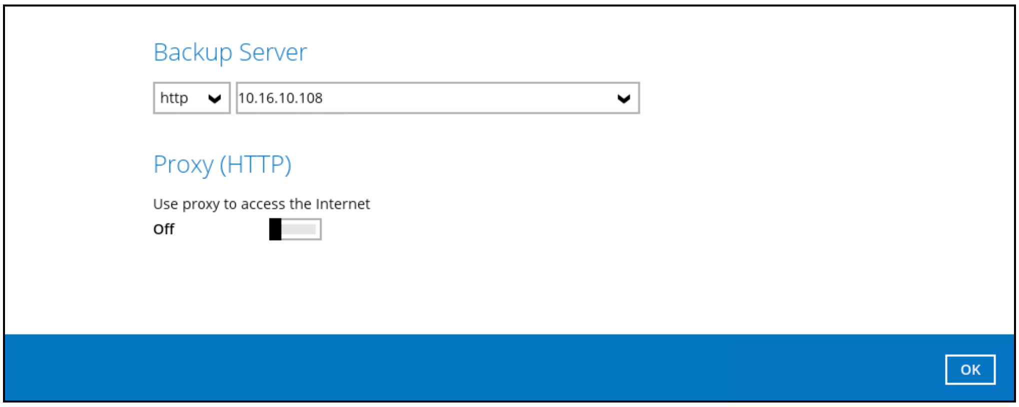
- The Free Trial button will only be displayed once when the user login for the first time. If you cannot create a free trial account kindly contact your backup service provider.
- Only alphanumeric characters and selected special characters, A to Z, 0 to 9, @, - and _, are allowed to be used for the Login name. While there may be some limitations on password complexity and age which is determined by the backup service provider. Please contact your service provider for further details.
- The add-on modules available and quota size are determined by your service provider.
- The trial account period is determined by your service provider. Please contact your service provider for details.

Follow the steps below to create a Free Trial backup account in AhsayOBM.

1. Click on **Free Trial**.



2. Configure your Backup Server settings.



Backup Server

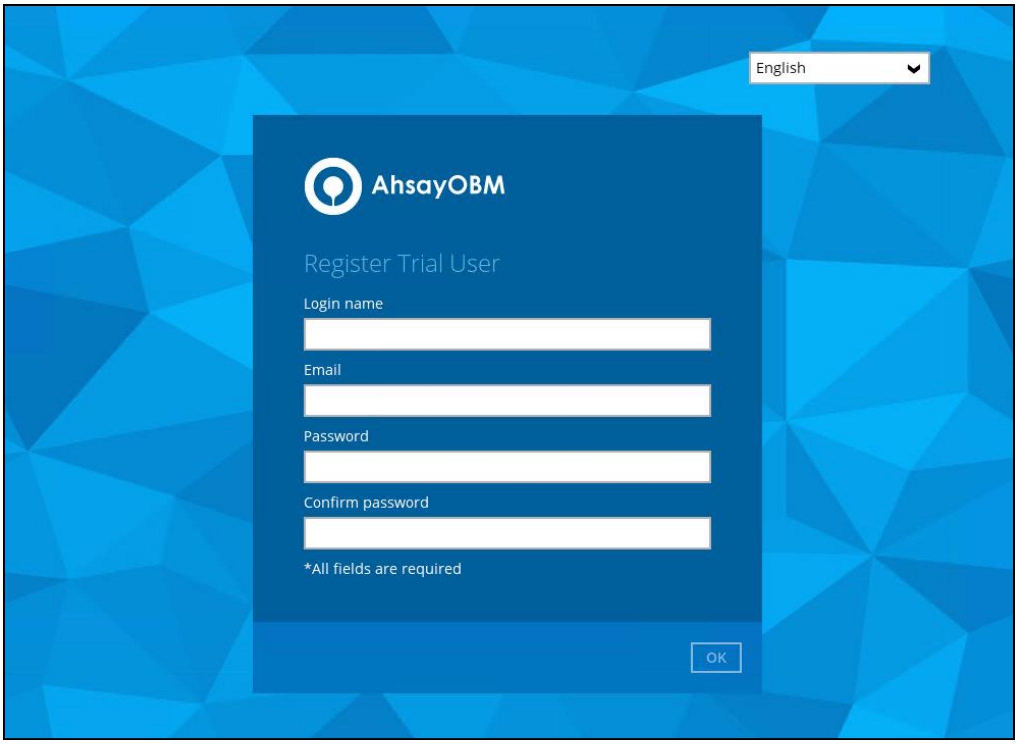
http | 10.16.10.108

Proxy (HTTP)

Use proxy to access the Internet

Off

3. Enter the Login name that you want. Also provide your email address and password. Confirm your password and click **OK** to create your trial account.



Register Trial User

Login name

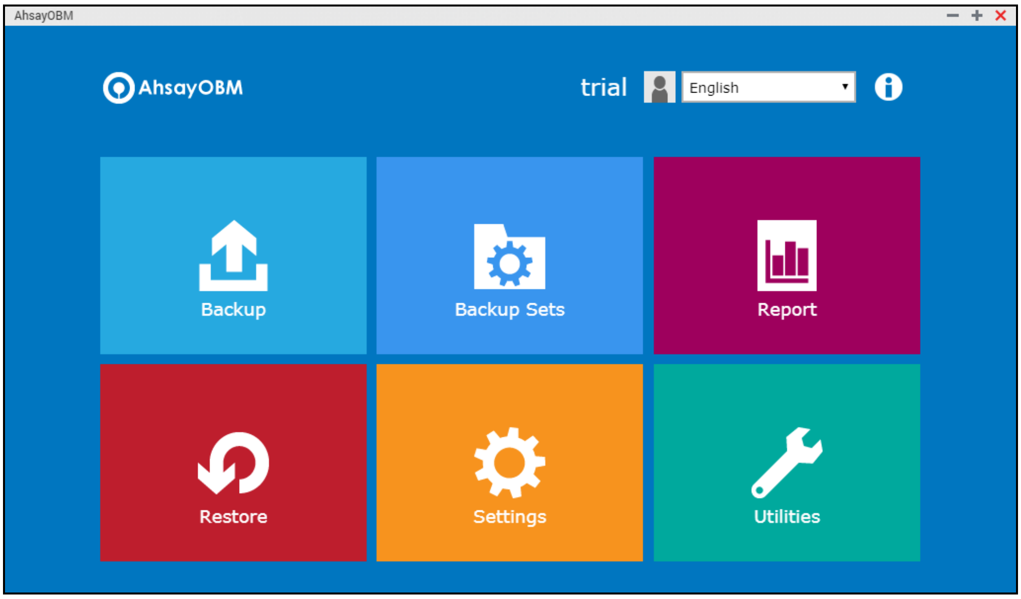
Email

Password

Confirm password

*All fields are required

4. Once the trial account is created, this screen will be displayed.



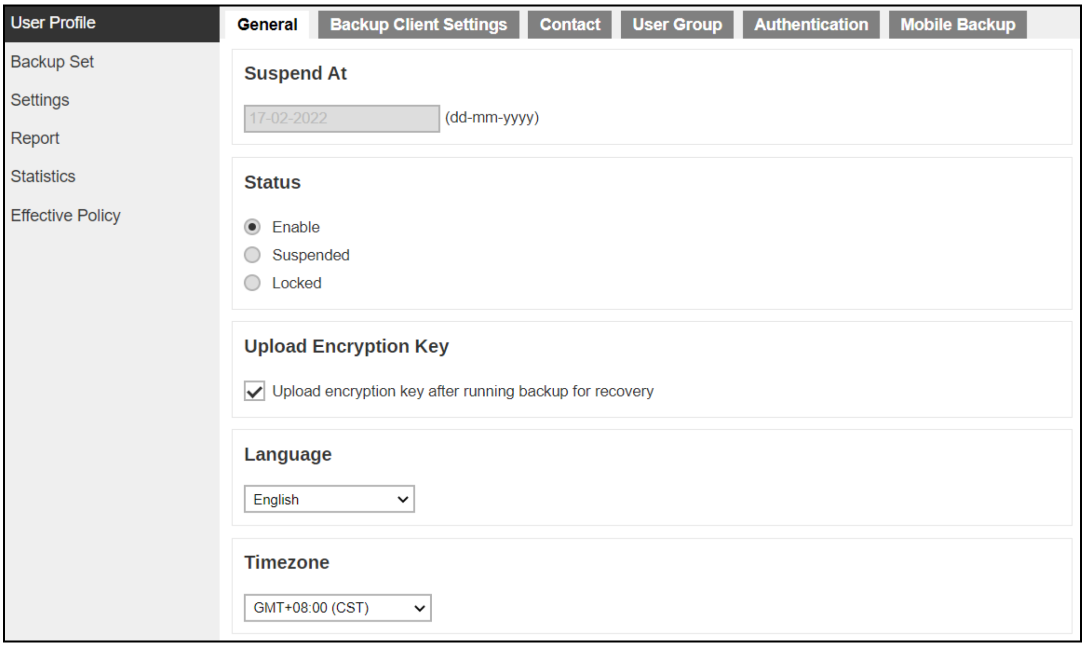
5. After your trial account has been created, you need to check several things:

➢ The expiry date of the trial account, which determines when it will be suspended.

➢ The Language which will be used for sending reports.

➢ And the Timezone, this is to ensure that your backup schedule will run at the correct time.

You can check this by logging in to AhsayCBS, go to **Backup / Restore > User > User Profile > General**. For more information please refer to the AhsayCBS User's Guide.



Suspend At

17-02-2022 (dd-mm-yyyy)

Status

● Enable
○ Suspended
○ Locked

Upload Encryption Key

☑ Upload encryption key after running backup for recovery

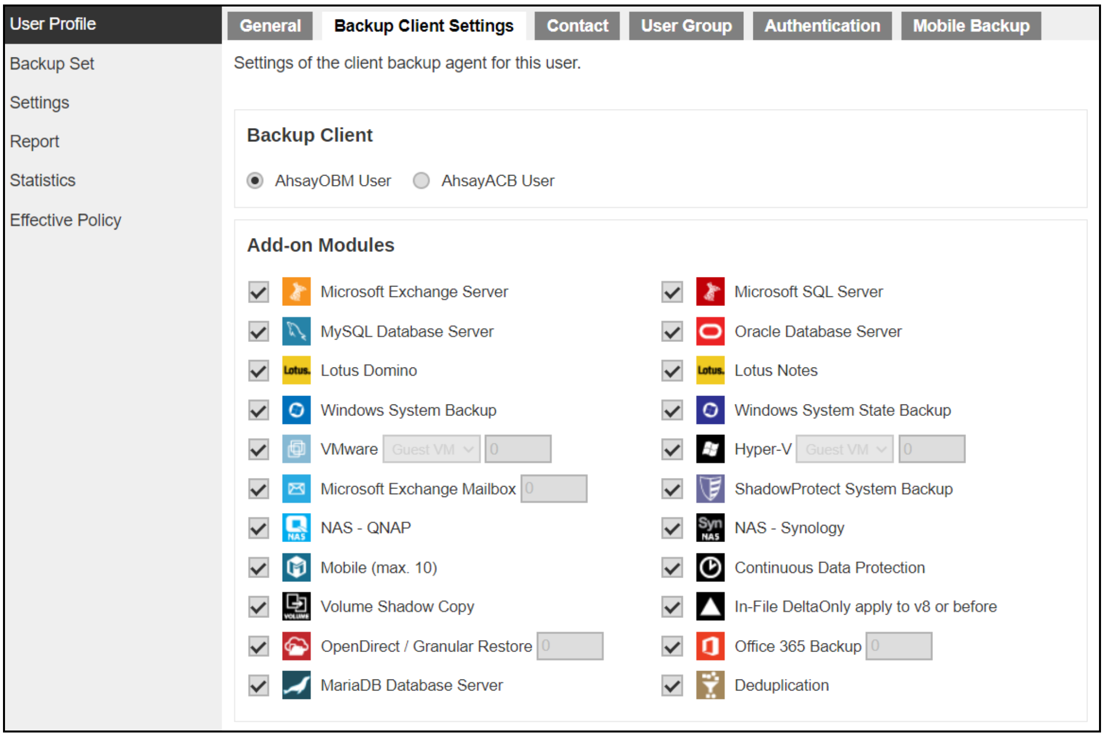
Language

English

Timezone

GMT+08:00 (CST)

6. You also need to check the available add-on modules and quota by going to the **Backup Client Settings** tab.



Settings of the client backup agent for this user.

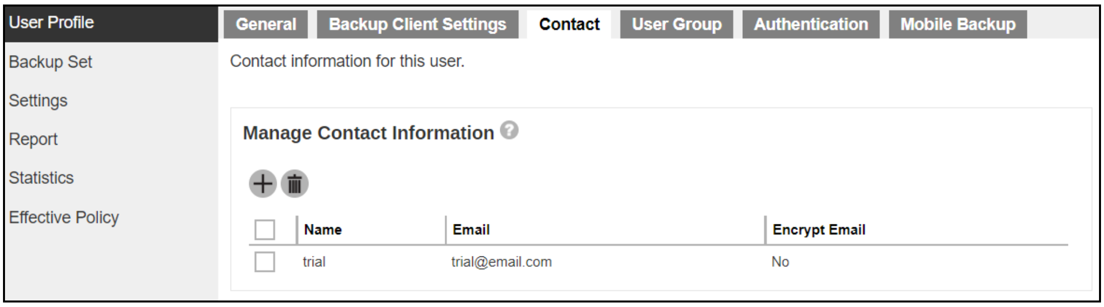
Backup Client

● AhsayOBM User ○ AhsayACB User

Add-on Modules

- ☑ Microsoft Exchange Server
- ☑ MySQL Database Server
- ☑ Lotus Domino
- ☑ Windows System Backup
- ☑ VMware Guest VM 0
- ☑ Microsoft Exchange Mailbox 0
- ☑ NAS - QNAP
- ☑ Mobile (max. 10)
- ☑ Volume Shadow Copy
- ☑ OpenDirect / Granular Restore 0
- ☑ MariaDB Database Server
- ☑ Microsoft SQL Server
- ☑ Oracle Database Server
- ☑ Lotus Notes
- ☑ Windows System State Backup
- ☑ Hyper-V Guest VM 0
- ☑ ShadowProtect System Backup
- ☑ NAS - Synology
- ☑ Continuous Data Protection
- ☑ In-File DeltaOnly apply to v8 or before
- ☑ Office 365 Backup 0
- ☑ Deduplication

7. Lastly, you need to verify if your contact details are correct by going to the **Contact** tab. If you want to add more contact information, you can add it here.



Contact information for this user.

Manage Contact Information

□	Name	Email	Encrypt Email
□	trial	trial@email.com	No