AhsayCBS v8.5 New Features Datasheet

Ahsay Systems Corporation Limited

26 January 2021

Revision History

Date	Descriptions	Type of modification
26 January 2021	Initial draft	New

Table of Contents

The following table is an overview with brief description of the new features available in AhsayCBS, AhsayOBM, AhsayACB v8.5 (or above), and Ahsay Mobile.

Feature	Description
Two-factor Authentication (2FA)	Extra layer of security to prevent an unauthorized user from logging in to AhsayCBS/AhsayOBM/AhsayACB.
Mobile Backup	Mobile backup and restore of photos and videos using Ahsay Mobile to AhsayOBM/AhsayACB machine. If required, the local backup of the photos and videos can be backed up to a Cloud destination by using a separate File backup set on AhsayOBM/AhsayACB.

The following table shows the supported features for each product running on different types of Operating System:

Product	Operating System (OS)		Features	
			Two-Factor Authentication (2FA)	Mobile Backup
AhsayCBS			✓	✗
AhsayOBM	**Windows**		✓	✓
	macOS		✓	✓
	Linux GUI		✓	✓
	Linux CLI		✗	✗
	FreeBSD		✗	✗
	NAS Synology		✗	✗
	NAS QNAP		✗	✗
AhsayACB	**Windows**		✓	✓
	macOS		✓	✓

Two-Factor Authentication (2FA)

The new enhanced Two-Factor Authentication (2FA) in v8.5 (or above) will provide additional two-factor authentication security options to secure login to **AhsayCBS**, **AhsayOBM** and **AhsayACB** to cater for different requirements of each customer.

Key Features

- Supported for system accounts; AhsayCBS Admin, Sub-Admin, and Read-only Admin account types
- Supported for AhsayOBM and AhsayACB user paid and trial accounts
- Two-Factor Authentication (2FA) using Ahsay Mobile which supports:
  - Push notifications authentication
  - TOTP (Time-based One-Time Password)
- Two-Factor Authentication (2FA) using third-party TOTP (Time-based One-Time Password) Authenticator apps that provide time-based one-time password. A few examples are:
  - Google Authenticator
  - Microsoft Authenticator
  - LastPass Authenticator
- Supports multiple mobile devices registered for the Two-Factor Authentication (2FA) per account
- Each system or user account can support authentication using multiple mobile devices with different Authenticator apps

  For example:
  - Mobile device 1 – using Ahsay Mobile
  - Mobile device 2 – using Google Authenticator
  - Mobile device 3 – using Microsoft Authenticator etc.

Starting v8.5 (or above), the Two-Factor Authentication (2FA) feature will replace Twilio and the Twilio feature will be desupported. Twilio and Two-Factor Authentication (i.e. Ahsay Mobile Authenticator and third-party TOTP Authenticator) cannot be used at the same time. Once the Twilio setup is turned off in v8.5 (or above), this feature is automatically deleted and cannot be reverted.

Requirements

In order to log in using the Two-Factor Authentication (2FA), the following requirements must be satisfied:

For AhsayCBS/AhsayOBM/AhsayACB

- AhsayCBS v8.5 (or above) must be installed.
- AhsayOBM/AhsayACB v8.5 (or above) must be installed.
- AhsayOBM/AhsayACB v8.5 (or above) must be connected to AhsayCBS.
- AhsayCBS must be connected to the internet.
- To use the Two-Factor Authentication (2FA) with **https** protocol, a valid SSL certicate from a trusted CA must be installed on AhsayCBS. Otherwise, you will have to use **http** instead, which means all AhsayOBM and AhsayACB users with Two-Factor Authentication (2FA) enabled will need to connect to AhsayCBS using **http** as well.
- The firewall on the AhsayCBS machine must be configured to allow outbound connections to the Push Notification Server **pns.ahsay.com** via port 80 and 443. Failure to do so will prevent you from using Push Notification feature on the Ahsay Mobile for the Two-Factor Authentication (2FA).
- The Two-Factor Authentication (2FA) must be enabled on AhsayCBS system, AhsayOBM and/or AhsayACB user accounts.

For Ahsay Mobile

- A mobile device with the Ahsay Mobile and/or a TOTP Authenticator App such as Google or Microsoft Authenticator installed is available for the Two-Factor Authentication (2FA). Although only one authenticator app is needed for the 2FA, several authenticator apps may be used.

  For example: AhsayOBM/AhsayACB can register and use both Ahsay Mobile and Google Authenticator.

- **Android and iOS version Supported**

OS	Description
	For Android mobile device, the Android version must be Android 8 (or above).
	For iOS mobile device, the iOS version must be iOS 12 (or above).

- A supported mobile device with Ahsay Mobile and/or a third-party TOTP Authenticator app must be installed.
- The Ahsay Mobile or a third-party TOTP Authenticator app must be registered with AhsayCBS/AhsayOBM/AhsayACB.
- The mobile device must have a valid mobile service and able to receive SMS notifications.
- The mobile device must have a functioning camera for QR code scanning for the Two-Factor Authentication (2FA) registration.
- To use push notification for the Two-Factor Authentication (2FA) with Ahsay Mobile, the mobile device must have an internet connection.

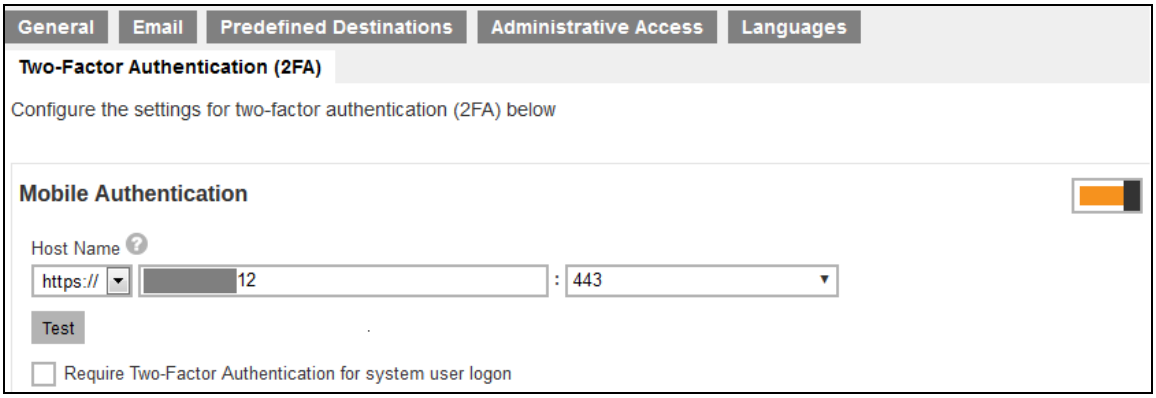
Limitations

- Not supported on API system accounts.
- For Replication, the Two-Factor Authentication (2FA) is not available for both sending and receiving.
- For Redirector, the Two-Factor Authentication (2FA) is not available for both hosting and joining.
- Not supported in AhsayOBM and/or AhsayACB pre-v8.5.
- Not supported in AhsayOBR.
- Not supported in AhsayOBM running on Linux CLI, FreeBSD, Synology and QNAP NAS.

Set up Two-Factor Authentication (2FA)

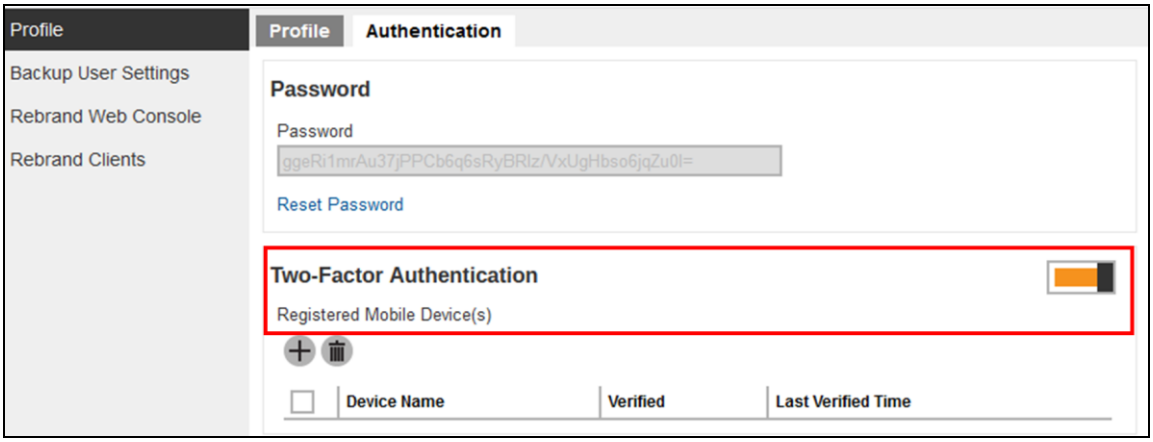
1. To enable Two-Factor Authentication (2FA) on AhsayCBS, the **Mobile Authentication** option must be enabled. Select the preferred protocol, then enter the FQDN or public IP address of the AhsayCBS server and port number. By default, this setting is disabled.

   To use the Two-Factor Authentication (2FA) with **https** protocol, a valid SSL certicate from a trusted CA must be installed on AhsayCBS. Otherwise, the Two-Factor Authentication (2FA) must be setup using **http** instead. This means all AhsayOBM and AhsayACB users with Two-Factor Authentication (2FA) enabled will need to connect to AhsayCBS using **http** as well.

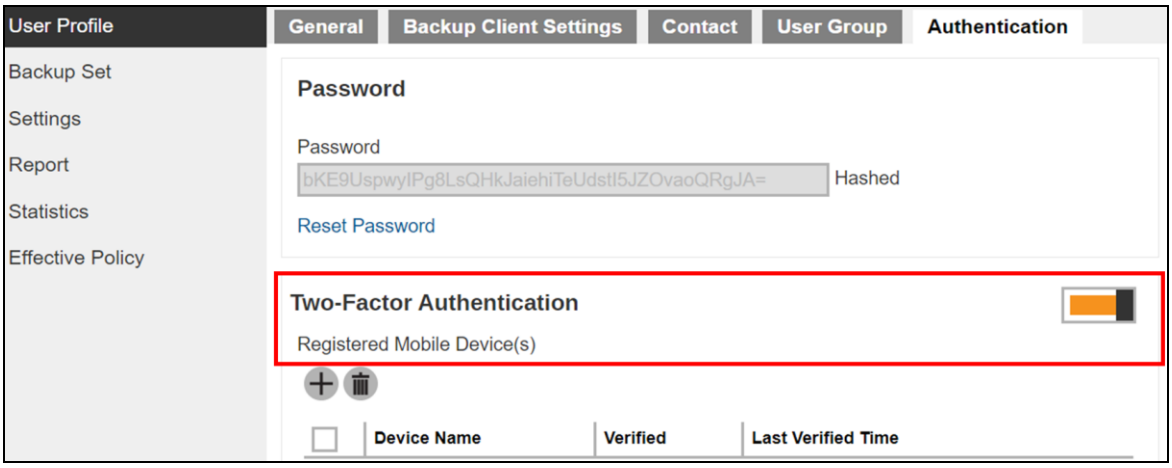


   If you want to apply the Two-Factor Authentication (2FA) for system users, then you will need to enable the "**Require Two-Factor Authentication for system user logon**" option.

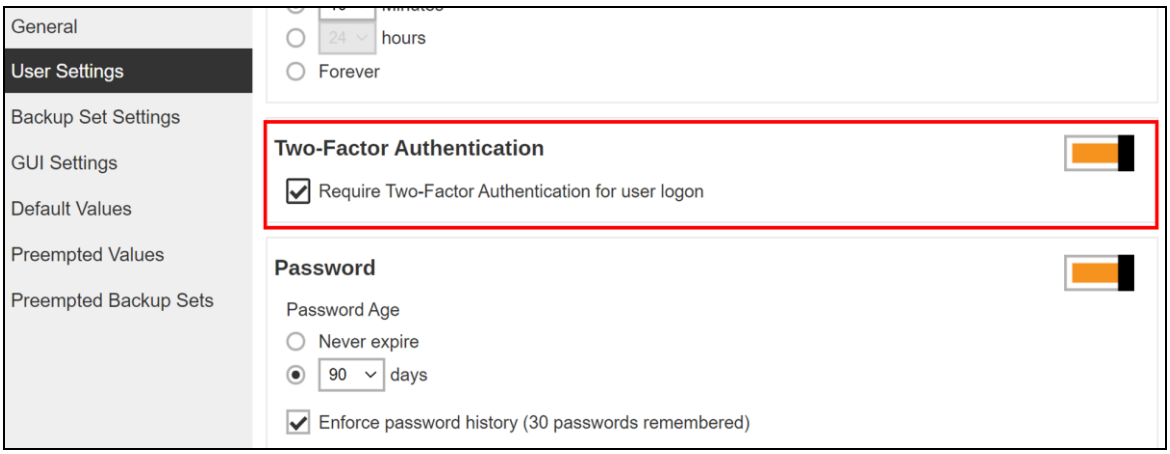
   Otherwise, you will need to enable the Two-Factor Authentication (2FA) for each system user account in **> Basic > Administrative Access > Manage System User > %username% > Profile** tab **> Authentication**.



2. To enable Two-Factor Authentication (2FA) for each AhsayOBM/AhsayACB user account, this can be done on the **> Backup User > %username% > User Profile > Authentication** tab under the Two-Factor Authentication option. The Two-Factor Authentication option will only be visible if **Mobile Authentication** option is enabled on AhsayCBS server.



Alternatively, to make the Two-Factor Authentication (2FA) mandatory for all AhsayOBM/AhsayACB user accounts on AhsayCBS, this can be done via the **Users, Groups & Policies > Policy Group > Default Settings > User Settings** page. By default, this setting is disabled.

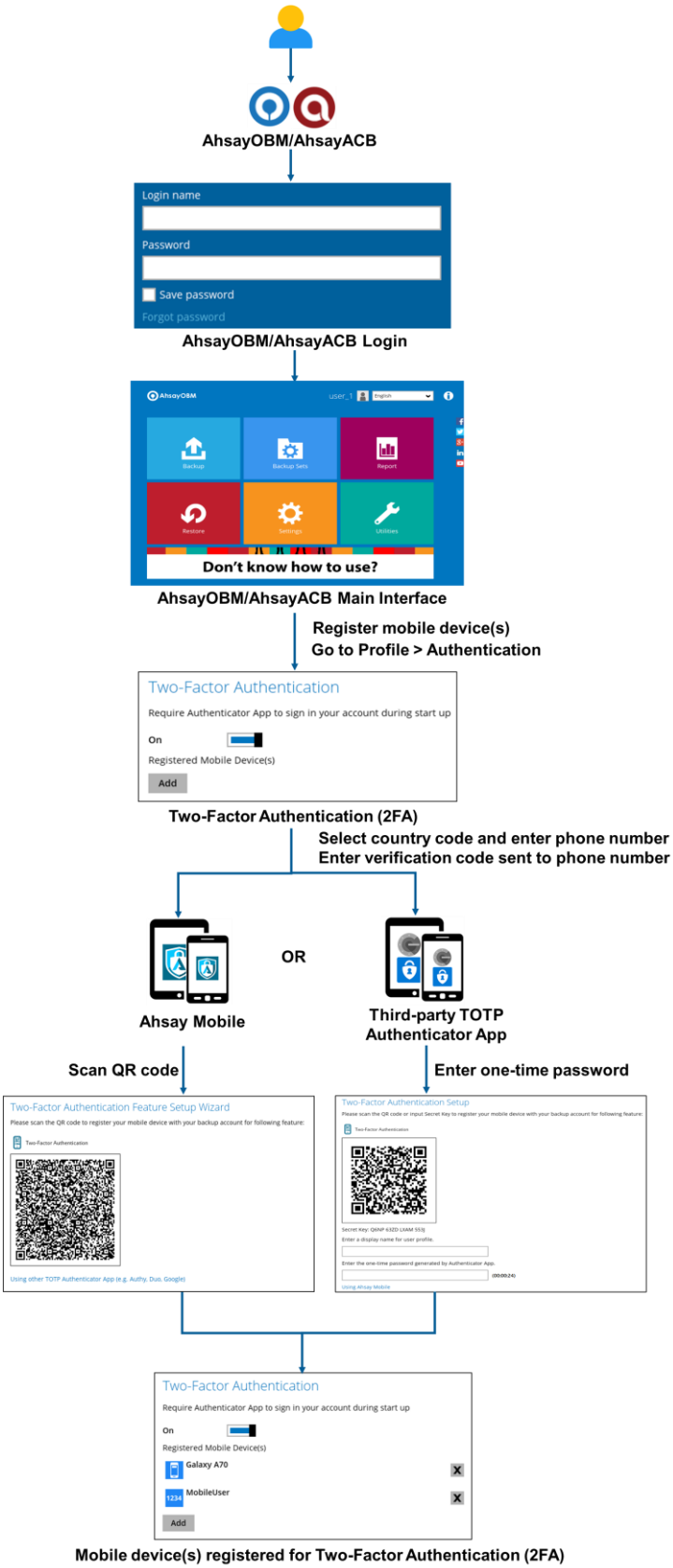


Two-Factor Authentication (2FA) Registration

The following diagram illustrates the registration of mobile device(s) for the Two-Factor Authentication (2FA) on AhsayCBS, AhsayOBM, and AhsayACB.

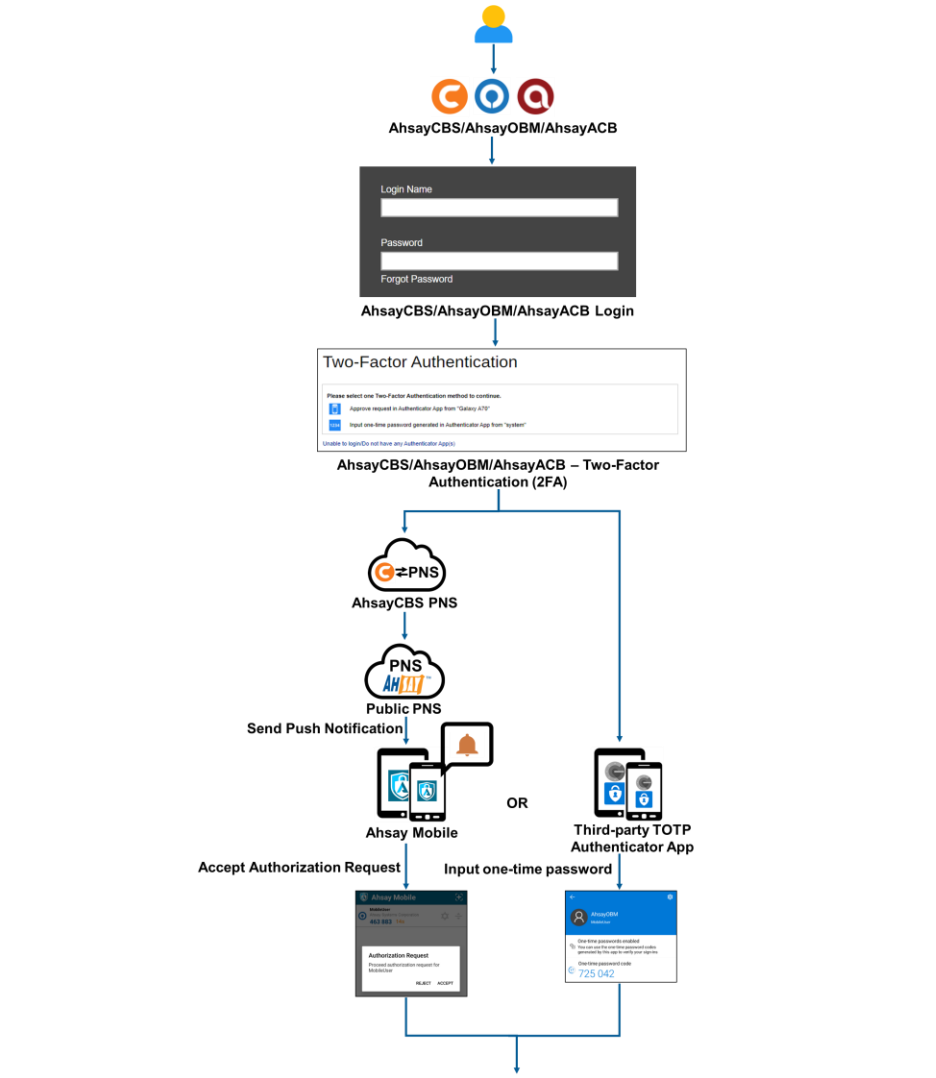
AhsayCBS

AhsayOBM/AhsayACB



How it works?

The following diagram illustrates the login process to AhsayCBS/AhsayOBM/AhsayACB v8.5 (or above) with the Two-Factor Authentication (2FA) enabled for the account.



1. When starting up AhsayCBS/AhsayOBM/AhsayACB, you will first enter the Login Name and Password.
2. The selection of the Two-Factor Authentication (2FA) such as **Ahsay Mobile** or **TOTP Authenticator** will be displayed.
3. If the Ahsay Mobile Authenticator is selected:
   a Push Notification will be sent to the Ahsay Mobile to either accept or reject the authorization request to log in to AhsayCBS/AhsayOBM/AhsayACB.

   If the TOTP Authenticator is selected:
   a one-time password will be generated in the TOTP Authenticator app which must be entered to AhsayCBS/AhsayOBM/AhsayACB to log in.
4. If the Ahsay Mobile Authenticator is selected:
   After accepting the authorization request, the AhsayCBS/AhsayOBM/AhsayACB landing page will be displayed.

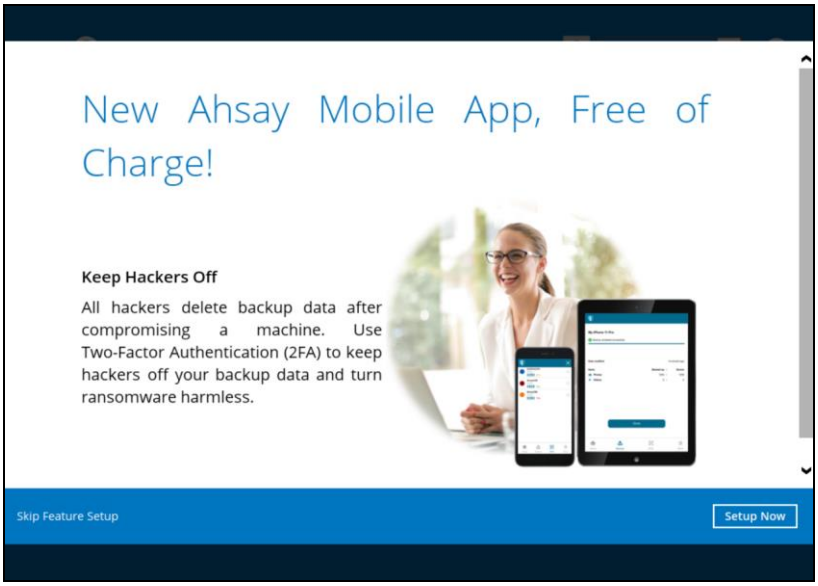
   If the TOTP Authenticator is selected:
   After entering the generated one-time password to AhsayCBS/AhsayOBM/AhsayACB, the AhsayCBS/AhsayOBM/AhsayACB landing page will be displayed.

Initial login to AhsayOBM/AhsayACB v8.5 (or above) after new installation

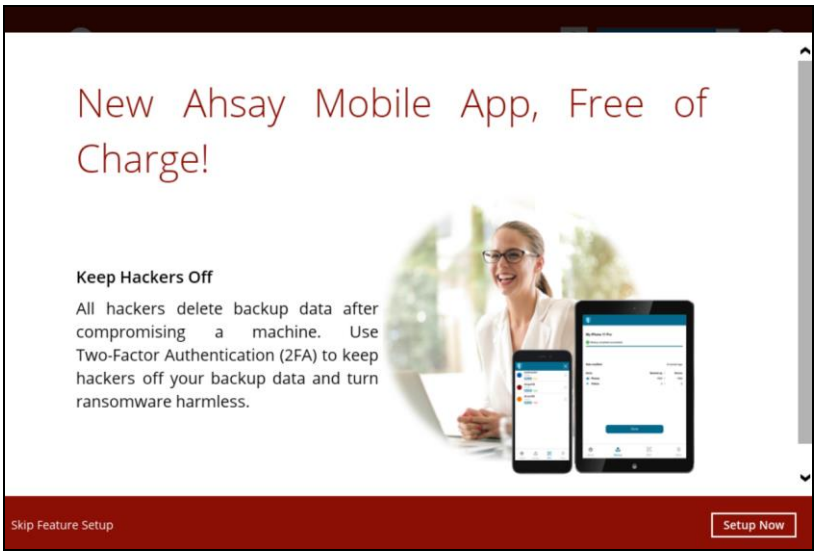
Without Ahsay Mobile Add-on Module

On the initial login to AhsayOBM/AhsayACB v8.5 (or above) without the Ahsay Mobile Add-on Module enabled for the AhsayOBM/AhsayACB user account, the following screen will be displayed. This is where you can choose to set up the Two-Factor Authentication (2FA) by clicking **Setup Now** or set it up later on by selecting **Skip Feature Setup**.

AhsayOBM



AhsayACB

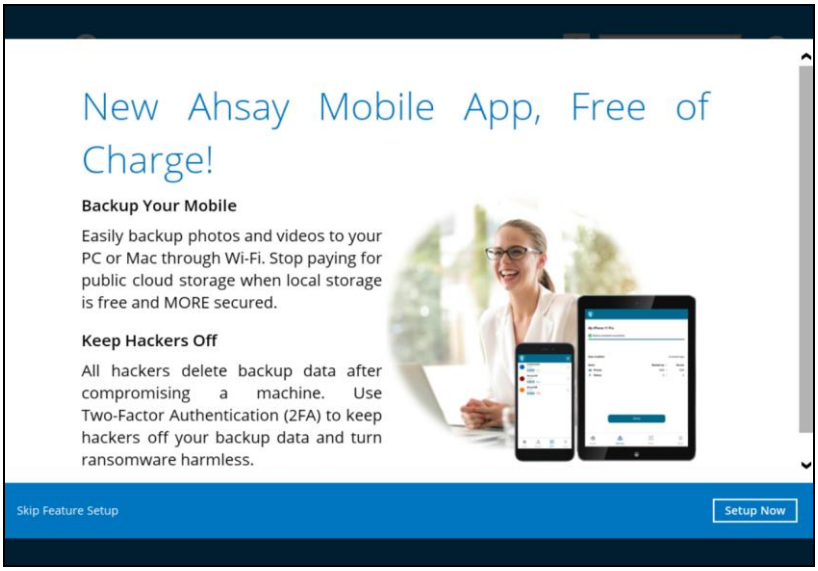


The images and texts will only be customized by branding the AhsayOBM/AhsayACB.

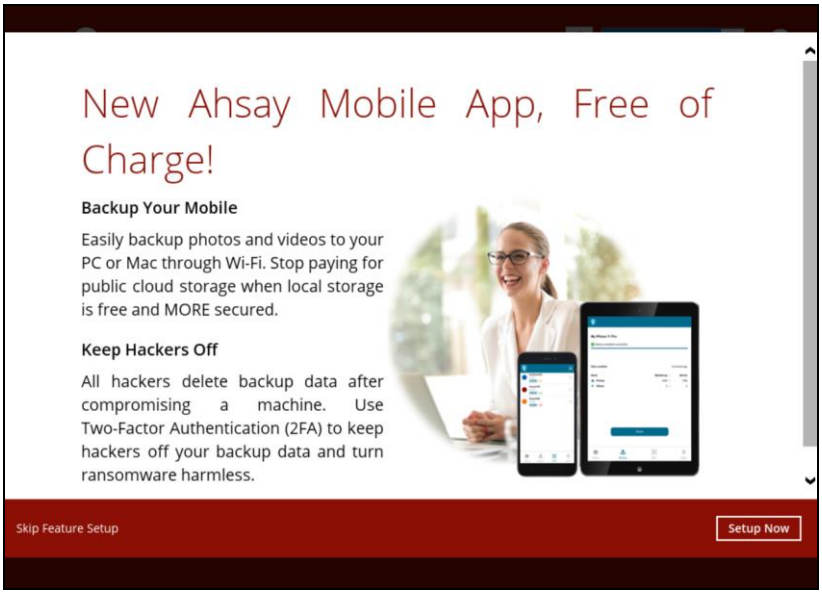
With Ahsay Mobile Add-on Module

On the initial login to AhsayOBM/AhsayACB v8.5 (or above) with the Ahsay Mobile Add-on Module enabled for the AhsayOBM/AhsayACB user account, the following screen will be displayed. This is where you can choose to set up the Two-Factor Authentication (2FA) and Mobile backup by clicking **Setup Now** or set it up later on by selecting **Skip Feature Setup**.

AhsayOBM



AhsayACB



The images and texts will only be customized by branding the AhsayOBM/AhsayACB.

Succeeding logins to AhsayOBM/AhsayACB v8.5 (or above) with Two-Factor Authentication (2FA) enabled

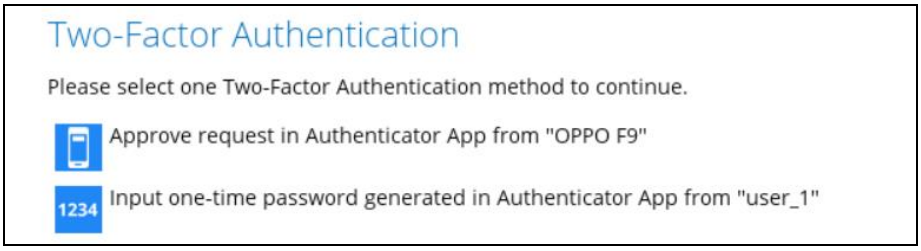
After the Two-Factor Authentication (2FA) has been setup, the following screen will be displayed on the succeeding logins to AhsayOBM/AhsayACB v8.5 (or above). This is where you can select which type of authentication method will be used to log in:

- **Ahsay Mobile Authenticator**
- **TOTP (Time-based One-Time Password) Authenticator**

On the examples below, "OPPO F9" is the name of the mobile device where the Ahsay Mobile app is installed on. Select this to use Ahsay Mobile Authenticator to log in.

"user_1" and "user2" are the account name(s) on the TOTP authenticator app. Select this to use the installed third-party TOTP authenticator app to log in.

AhsayOBM



AhsayACB

For a complete instructions on the Two-Factor Authentication (2FA) and Mobile backup setup, please refer to the following guides:

Ahsay Mobile App v8 User Guide for Android and iOS

AhsayOBM

AhsayOBM v8 Quick Start Guide for Windows

AhsayOBM v8 Quick Start Guide for macOS

AhsayACB

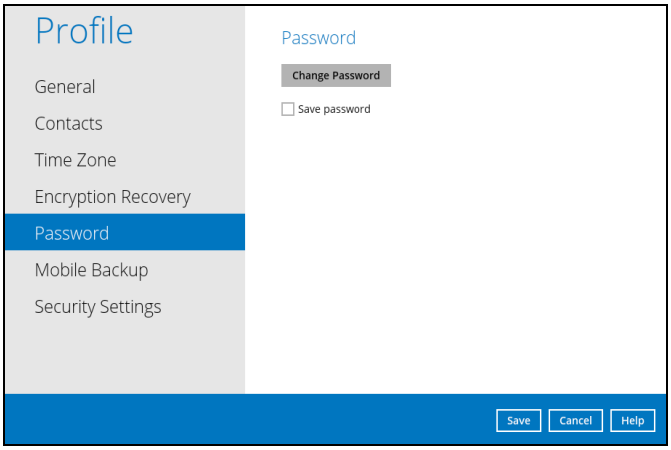
AhsayACB v8 Quick Start Guide for Windows

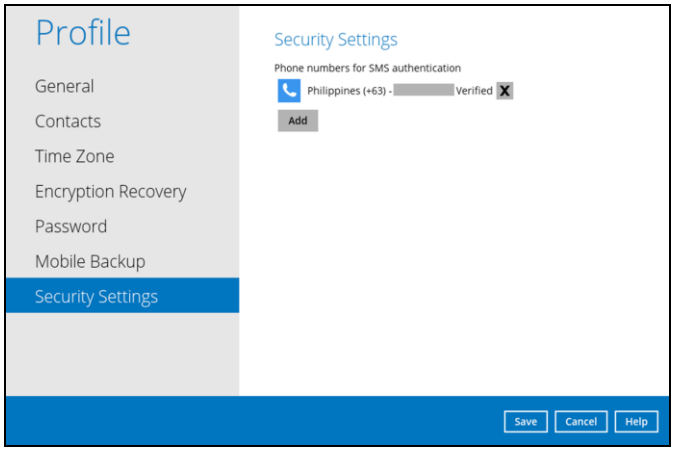
AhsayACB v8 Quick Start Guide for macOS

AhsayOBM/AhsayACB v8.5 (or above) Profile Page Legacy Layout

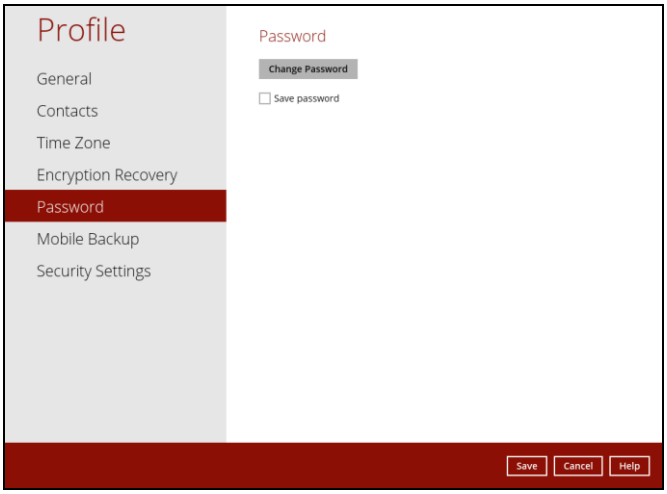
For AhsayOBM/AhsayACB user account(s) with Twilio enabled, the AhsayOBM/AhsayACB **Profile** page will display the **Password** and **Security Settings** tabs for backward compatibility.

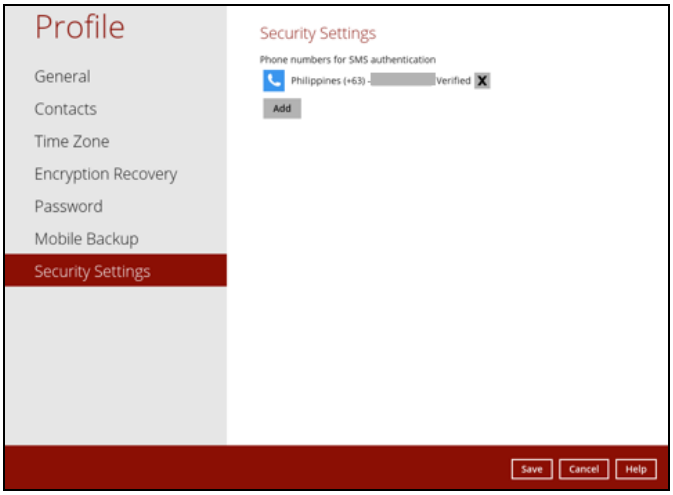
AhsayOBM





AhsayACB

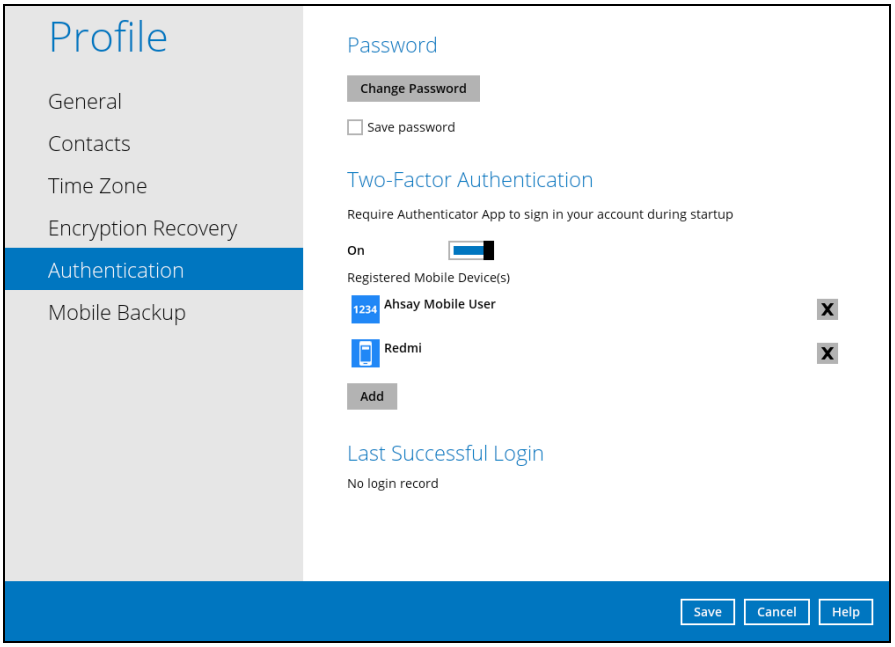




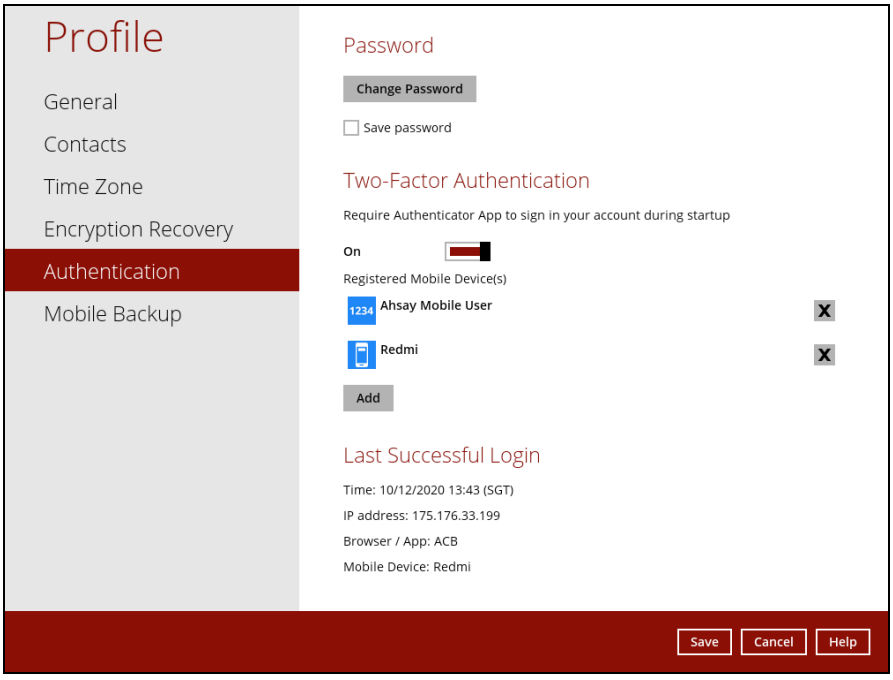
AhsayOBM/AhsayACB v8.5 (or above) Profile Page New Layout

If the Twilio is not used, then on the AhsayOBM/AhsayACB **Profile** page, the following screen will be displayed. The **Password** is included into the **Authentication** tab along with Two-Factor Authentication settings, which displays and manages the registered mobile device(s) for the two-factor authentication once setup.

AhsayOBM



AhsayACB



Mobile Backup

Mobile devices such as smartphones and tablets have become one of the primary tools in managing electronic files. With its diverse functionalities, it can already be used as almost a portable computer which help people work with their important files with ease by the palm of their hand.

To provide customers with improved mobile backup solution, **Ahsay Mobile** is introduced in v8.5 (or above) which replaces the existing **AhsayMOB** that was supported in pre-v8.5. Users with existing AhsayMOB installed will still be able to use the AhsayMOB app but is no longer available for new users to download the app from Google Play Store or App Store. New users should use the Ahsay Mobile.

Licensing

The new Ahsay Mobile licenses will be listed under **Mobile** Add-on Modules which are free of charge, and each license key is assigned an unlimited quota.

The **Mobile** Add-on Modules are required by an AhsayOBM/AhsayACB user if they are using the Ahsay Mobile app for Android and iOS backups. If the Ahsay Mobile app is only used for the Two-Factor Authentication (2FA) purposes, then the Mobile license modules are not required.

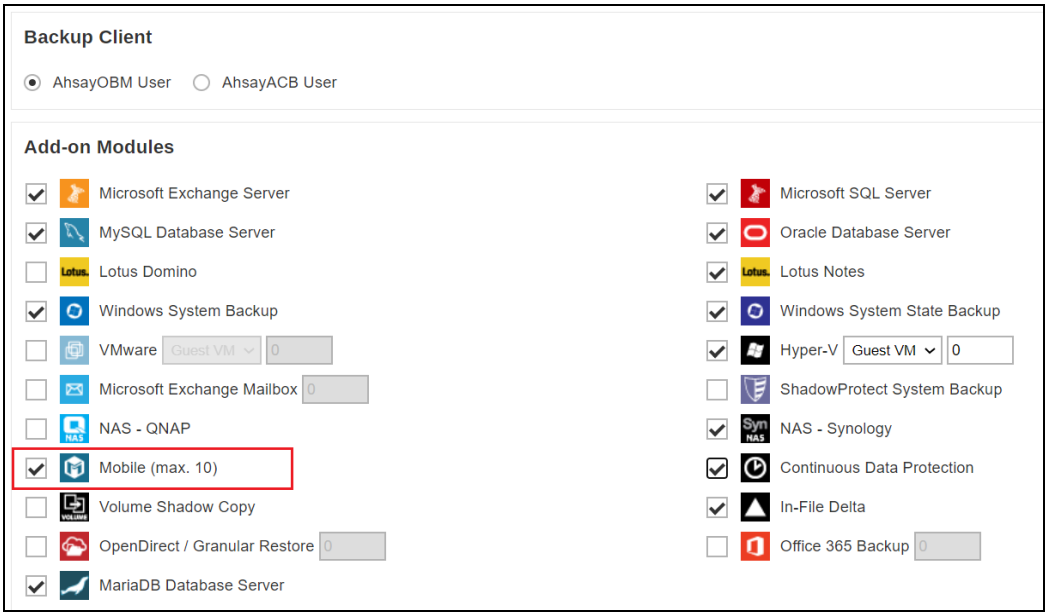
Client Add-on Modules	Quota	Used	Available
Microsoft Exchange Mailbox (Per Mailbox)	2000	1520	480
Hyper-V / VMware (Per Guest VM)	4000	260	3740
Hyper-V / VMware (Per Socket)	4000	0	4000
NAS - Synology / NAS - QNAP	2010	11	1999
Mobile	Unlimited	0	Unlimited
Office 365	4000	111	3889
OpenDirect / Granular Restore	2000	0	2000

If the license key already contains AhsayMOB licenses before upgrade to v8.5 (or above), then these licenses are listed as **Mobile (Legacy)** after v8.5 (or above) to distinguish them from Ahsay Mobile licenses.

Client Add-on Modules	Quota	Used	Available
Microsoft Exchange Mailbox (Per Mailbox)	2000	1520	480
Hyper-V / VMware (Per Guest VM)	4000	260	3740
Hyper-V / VMware (Per Socket)	4000	0	4000
NAS - Synology / NAS - QNAP	2010	11	1999
Mobile (Legacy)	2000	0	2000
Mobile	Unlimited	0	Unlimited
Office 365	4000	111	3889
OpenDirect / Granular Restore	2000	0	2000

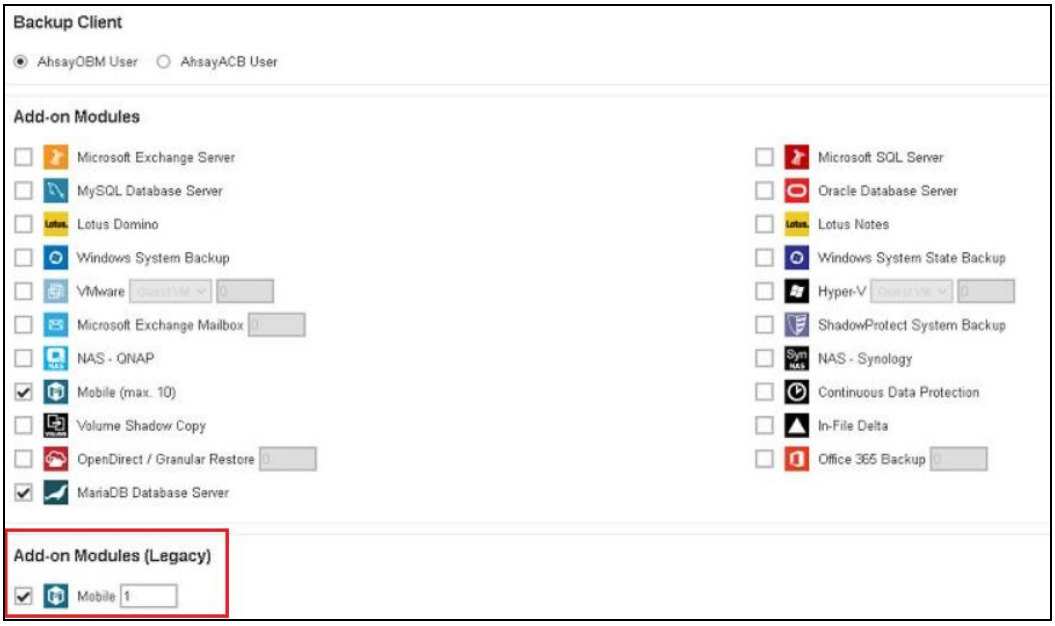
Key Features

- Mobile license Add-on Module is free of charge
- Each AhsayCBS license key supports unlimited mobile license quota
- Mobile licenses are calculated on a per mobile device basis
- An AhsayOBM/AhsayACB user account requires Mobile Add-on Module to be enabled to support mobile device backup
- Each AhsayOBM/AhsayACB user account is currently limited to 10 Mobile CALs



NOTE: The Mobile Add-on Module is only for mobile backup and it does not apply the use of Ahsay Mobile as a Two-Factor Authentication (2FA) tool.

For AhsayOBM/AhsayACB user accounts with existing AhsayMOB licenses before upgrade to v8.5 (or above), the AhsayMOB Add-on Module (Legacy) will be displayed.



- Able to back up and restore photos and videos from Ahsay Mobile to AhsayOBM/AhsayACB machine and/or Cloud destination
- Supported mobile backup source are photos and videos
- Supports Multiple Restore options such as,
  - Restore photos and videos to **Original location** on your registered mobile device - Android and iOS
  - Restore photos and videos to **Alternate mobile device**. It could be on the same or opposite operating system:

    Same mobile operating system – Android to Android / iOS to iOS

    Cross mobile operating system – Android to iOS / iOS to Android

Requirements

In order to back up and/or restore using Ahsay Mobile, the following requirements must be satisfied:

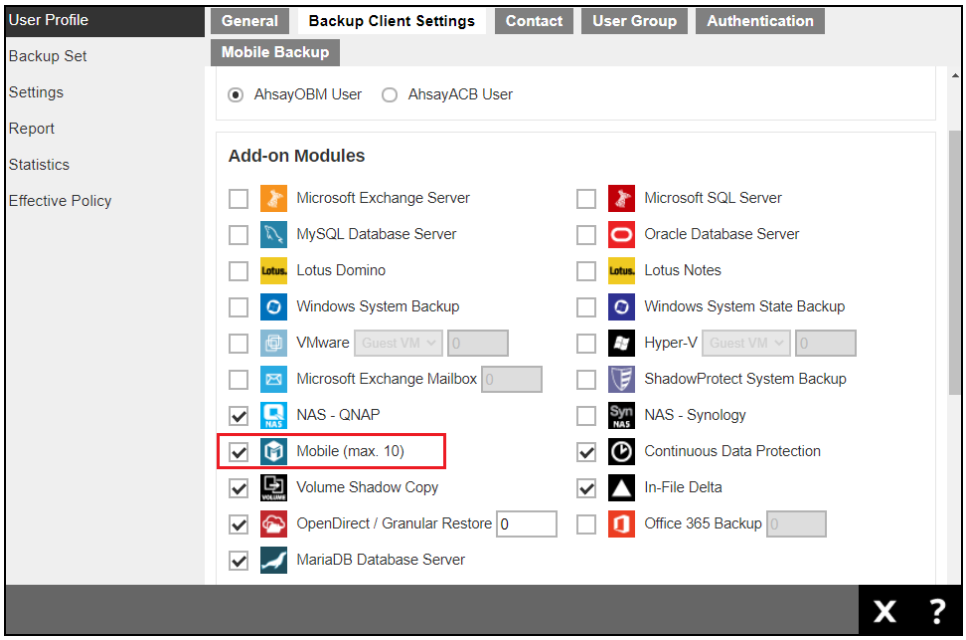
Android and iOS version Supported

OS	Description
android	For Android mobile device, the Android version must be Android 8 (or above).
iOS	For iOS mobile device, the iOS version must be iOS 12 (or above).

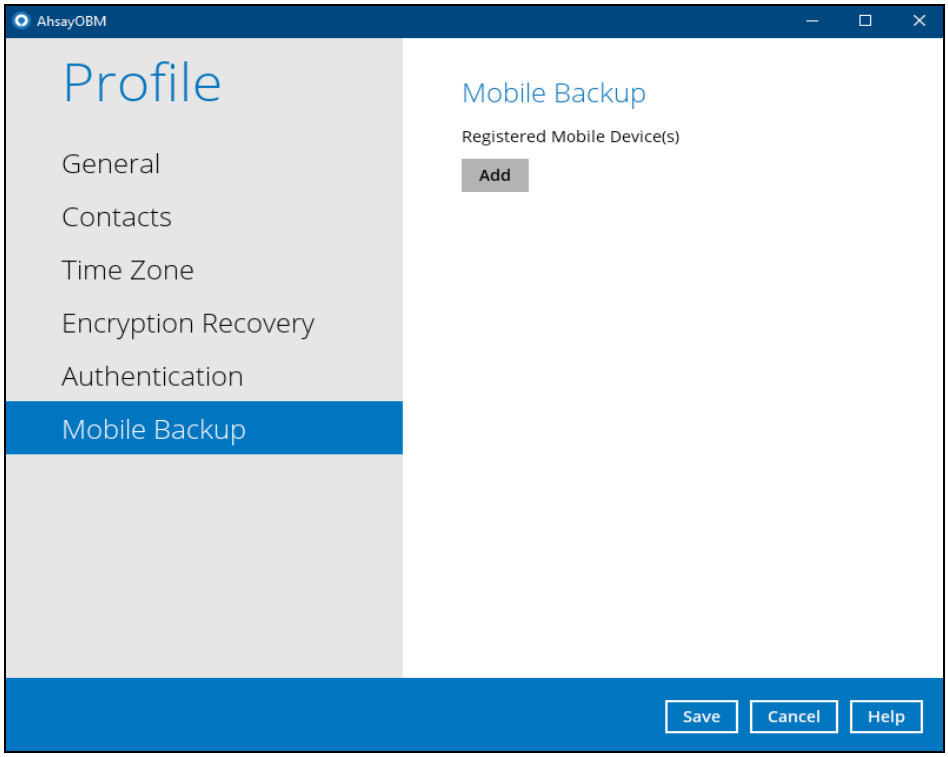
Mobile Add-on Module

AhsayOBM/AhsayACB requires the **Mobile** Add-on Module enabled to support mobile backups. The **Mobile Backup** tab will be only shown on AhsayOBM/AhsayACB if the Mobile Add-on Module is enabled on the AhsayOBM/AhsayACB user account.

Example: An AhsayOBM user account with **Mobile** add-on module enabled.

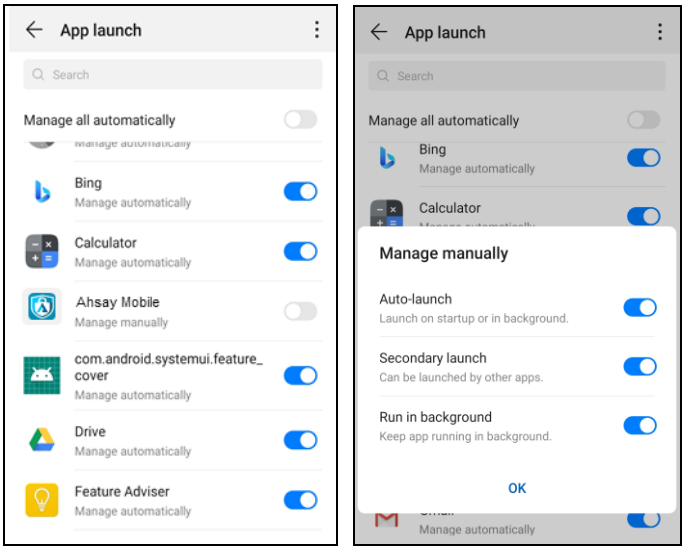
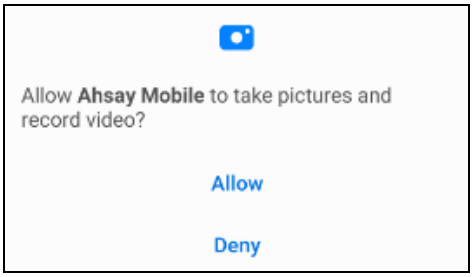
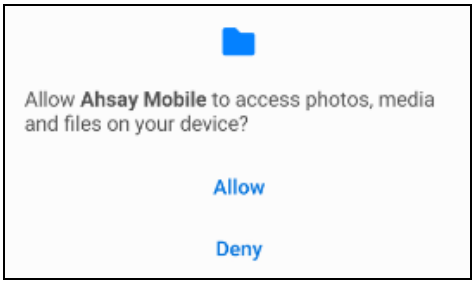


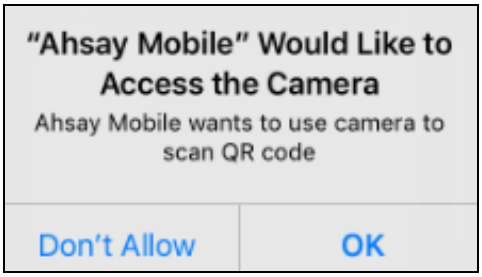
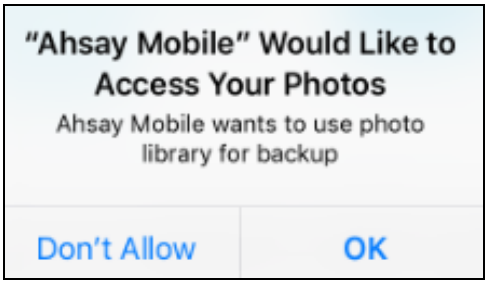
On the AhsayOBM, the **Mobile Backup** feature is only available if the **Mobile** add-on module is enabled on the AhsayOBM user account.



Permission Requirements

In order for the Ahsay Mobile to access the contents on your Android/iOS mobile device, ensure to **Allow** these requests when prompted to grant access permission on the first launch of Ahsay Mobile.

Mobile device	Permission		
ANDROID	Auto-Launch and Run in Background		
	Camera		
	Read / Write External Storage		

iOS	Camera		
	Face ID		
	Photo Library		

Network Settings

Ensure that the Ahsay Mobile is connected to the same local Wi-Fi network as the AhsayOBM/AhsayACB machine. Otherwise, this will prevent Ahsay Mobile from performing mobile backup and/or restore.

The following port ranges will be used by the Mobile Backup Server (MBS) for the request of Ahsay Mobile.

- **AhsayOBM - TCP Port:** 54000 to 54099 **UDP Port:** 54200 to 54299 **Protocol:** HTTP
- **AhsayACB - TCP Port:** 55000 to 55099 **UDP Port:** 55200 to 55299 **Protocol:** HTTP

The default HTTP and UDP Ports are the following:

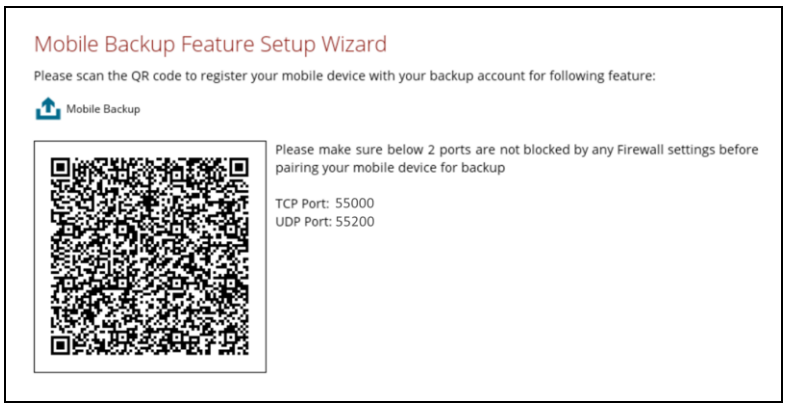
- **AhsayOBM - TCP Port:** 54000 **UDP Port:** 54200
- **AhsayACB - TCP Port:** 55000 **UDP Port:** 55200

If the default port is already in use by other applications or services, then the MBS will automatically acquire another port. For example on AhsayOBM machine, the default TCP port is 54000. If this port is in use, then the MBS will automatically acquire another port from the port range until an available port is found (e.g. **TCP port:** 54001, 54002, 54003 – 54099).

The actual **TCP** and **UDP Ports** can be seen on AhsayOBM/AhsayACB when pairing a mobile device for mobile backup.

AhsayOBM

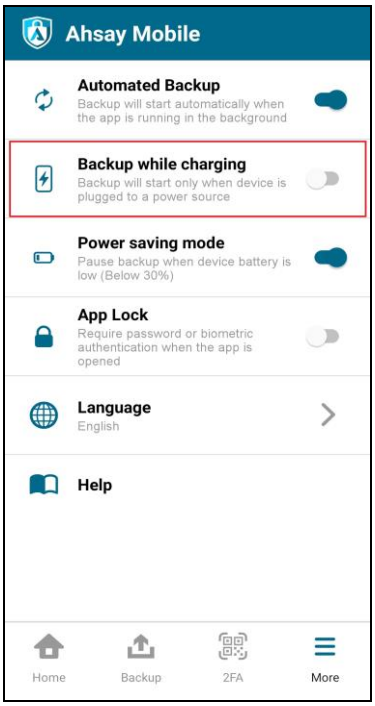
AhsayACB



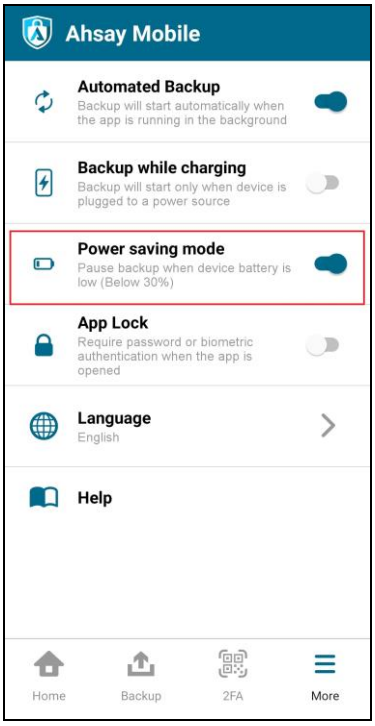
Ensure that AhsayOBM/AhsayACB and Ahsay Mobile are connected to the same Wi-Fi or have the same connection. Otherwise, the mobile backup and/or restore will not work.

Battery Requirements

- If the Backup while charging feature is enabled, the mobile device should be connected to a power source to resume backup. This feature is disabled by default.



- The Power saving mode feature is enabled by default. When enabled, a backup and/or restore is unable to be performed if the battery level is less than 30%.

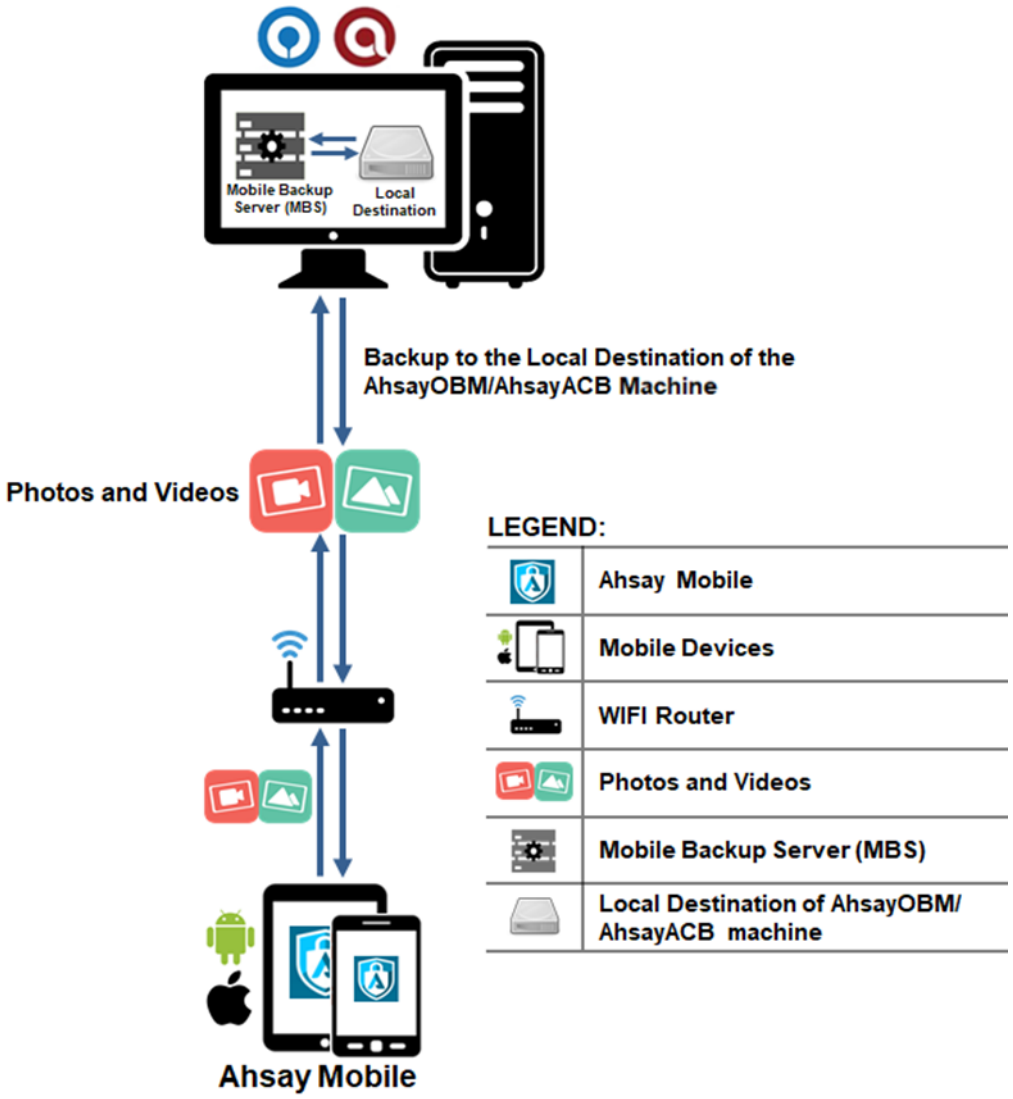


Limitations

- Mobile backup is not supported on AhsayCBS and AhsayOBM running on Linux CLI, FreeBSD, Synology and QNAP NAS.
- The maximum number of mobile devices that can be paired with AhsayOBM/AhsayACB user account for mobile backup is 10.
- Photos and videos are the only supported backup source for both Android and/or iOS mobile devices.
- Most common file types of photo and video can be supported, including but not limited to files with file extensions: .jpg, .png, .bmp, .gif, .mp4, .mkv, .mov, .avi, .flv etc.
- Backup of photos and videos are only supported if they can be opened by the device's built-in photo and/or video application.
- Backup and/or restore can only be performed if the mobile device is connected to the same local Wi-Fi network as the AhsayOBM/AhsayACB machine.
- Backup and/or restore can be performed if the battery level is NOT lower than 30%, unless the Power saving mode feature is disabled.
- For iOS device:
  - Backup of photos and videos synchronized from iTunes are not supported due to iOS limitations
  - EXIF (Exchangeable Image File Format) meta data of photo and video files are not retained after a restore, except the last modified data and time.
- Due to limitations on Android and iOS mobile devices, the timestamp of photo and video files are not retained after a restore.
- The current release does not support backup/restore of multiple snapshots. Only the latest backup snapshot is available to be restored.
- The current release does not support folder-by-folder or item-by-item restore. Only the complete set of backed-up photos and/or videos are available to be restored.

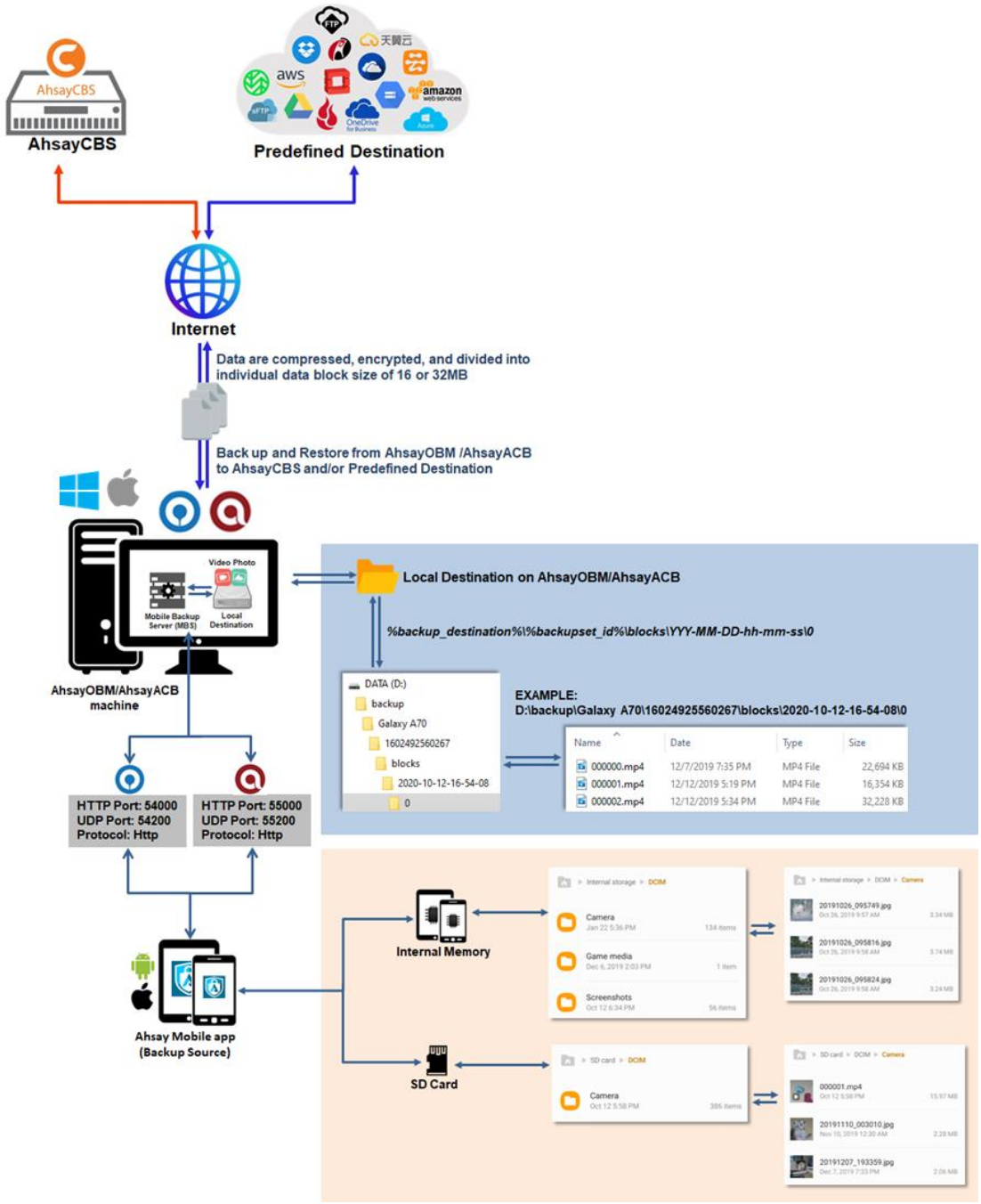
System Architecture

The Ahsay Mobile is connected to the local network of the AhsayOBM/AhsayACB machine via a Wi-Fi router to back up and restore photos and videos that are stored primarily on the local destination of the AhsayOBM/AhsayACB machine.



Photos and videos are either from the mobile device's internal memory or SD Card. These are selected as backup source using the Ahsay Mobile and will be backed up to the local destination of the AhsayOBM/AhsayACB machine which can be a hard drive, flash drive, and/or network drive in their ORIGINAL format unencrypted.

The Mobile Backup Server (MBS) is an integral part of the AhsayOBM/AhsayACB machine that manages the backup and restore of the Ahsay Mobile.

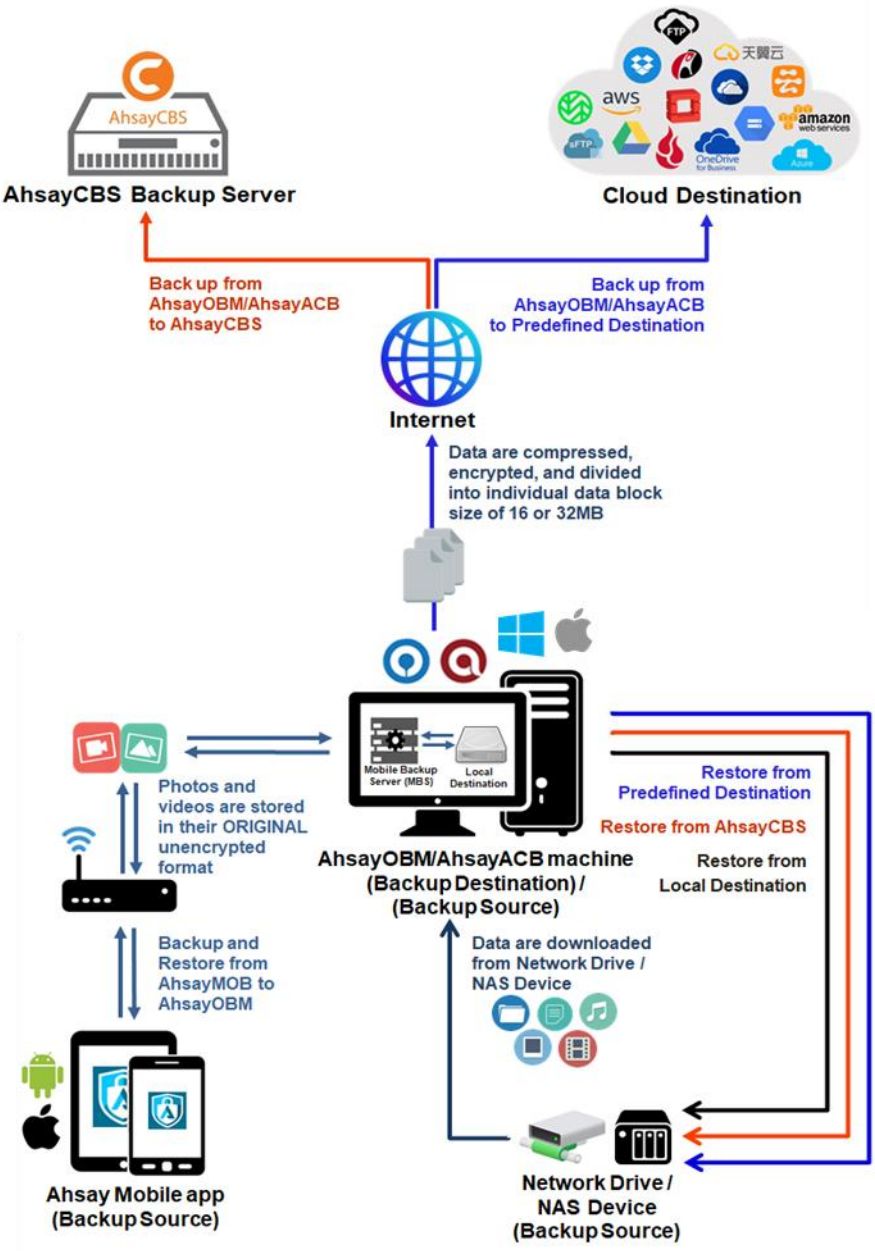


If storage of photos and videos to AhsayCBS and Predefined Destination is required, then this can be done using AhsayOBM/AhsayACB to perform a secondary backup and restore of the photos and videos on the local destination to AhsayCBS and Predefined Destination.

In order to back up and restore photos and videos from Ahsay Mobile to AhsayOBM/AhsayACB and Predefined Destination, this will be a two-step process.

1st: Back up photos and videos from Ahsay Mobile to AhsayOBM/AhsayACB.

2nd: Create a file backup set by means of AhsayOBM/AhsayACB using the local destination as the backup source, then back up this backup set to AhsayCBS and Predefined Destination.



Ahsay Mobile app branding for v8.5

NOTE: While the Ahsay Mobile app fully supports branding, however during the initial rollout phases of version 8.5.x, the branding of Ahsay Mobile app can only be done by Ahsay. If partners are interested in branding the Ahsay mobile app, they must engage Ahsay professional services.

Ahsay Mobile Branding Service

To engage our professional services for Ahsay Mobile branding, please contact our sales team to obtain a service quotation by email at sales-kb@ahsay.com or call our International Sales Hotline +852 3580 8091.

Ahsay Mobile Customization supports the following primary files to be modified:

- **File customization**
  - Application images – images used for icons and other graphics within the various application screens
  - Application icons – icons shown on the Home screen for both iOS and Android mobile devices wherein each OS type will have different specifications for customization
  - Splash screen (for iOS mobile device) – the first screen displayed when launching the application
  - Adverts – Ads that can be customized by the user's preference and by language
- **Colors**
  - Colors dictionary are defined in the colors.json file. This is a major component in the Ahsay Mobile Customization.
- **Localization**
  - Ahsay Mobile can support four (4) languages which are customizable by the user for translation (i.e. Base (English), Chinese – China, Chinese – Hong Kong SAR and Chinese – Taiwan)

For more information on the specifications needed for Ahsay Mobile branding, please refer to the following document:

Ahsay Mobile Image Specifications

Requirements

The following materials must be submitted by the partner to Ahsay for branding of their Ahsay mobile application:

- Image files and icons with your branding:
  - Application images
  - Application icons
  - Splash screen (iOS)
  - Colors dictionary
  - Localization
  - Adverts
- Organization Information
  - Organization ID and Organization Name for your Apple Business Account
  - Mobile application description
  - Keywords to be used for searching of the mobile application
  - Support URL

For further details, please refer to **Chapter 10.8 Ahsay Mobile Branding** of the following guide:

AhsayCBS v8 Administrator's Guide

Mobile Backup Server (MBS)

Starting with AhsayCBS v8.5 (or above), the **Mobile Backup Server (MBS)** will be utilized to handle mobile backup and restore of Ahsay Mobile. It is an integral part of AhsayOBM and AhsayACB located in the "mbs" folder which can be found inside the AhsayOBM/AhsayACB folder.

Once a mobile device installed with Ahsay Mobile is successfully registered for mobile backup with AhsayOBM/AhsayACB, the MBS will be automatically activated. Afterwards, it will automatically start whenever the AhsayOBM/AhsayACB services are restarted or when the AhsayOBM/AhsayACB machine is rebooted or powered on. The MBS will be deactivated when all mobile devices are deregistered from the mobile backup settings and the AhsayOBM/AhsayACB services are restarted.

Internal Components of MBS

- **running.txt file**
- **cbssvc.ini file**
- **logs**

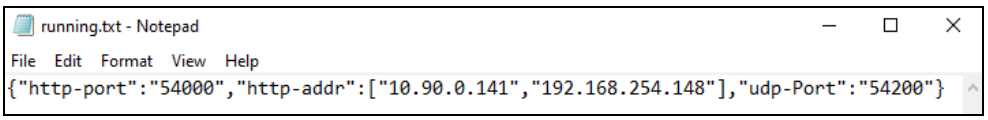
running.txt

Once the mobile device is paired with AhsayOBM/AhsayACB for the mobile backup, a "running.txt" file will be created inside the following folder.

	Location
AhsayOBM	
Windows	*C:\ProgramData\AhsayOBM\mbs\running.txt*
macOS	*/Application/AhsayOBM.app/mbs/running.txt*
AhsayACB	
Windows	*C:\ProgramData\AhsayACB\mbs\running.txt*
macOS	*/Application/AhsayACB.app/mbs/running.txt*

The "running.txt" file contains the **HTTP Port**, **IP address**, and **UDP Port** which are in actual use of the MBS.

Example of "running.txt" file on AhsayOBM running on Windows



The following port ranges will be used by the Mobile Backup Server (MBS) for the request of Ahsay Mobile.

- **AhsayOBM - TCP Port:** 54000 to 54099 **UDP Port:** 54200 to 54299 **Protocol:** HTTP
- **AhsayACB - TCP Port:** 55000 to 55099 **UDP Port:** 55200 to 55299 **Protocol:** HTTP

The default TCP and UDP Ports are the following:

- **AhsayOBM - TCP Port:** 54000 **UDP Port:** 54200
- **AhsayACB - TCP Port:** 55000 **UDP Port:** 55200

If the default port is already in use by other applications or services, then the MBS will automatically acquire another port. For example on AhsayOBM machine, the default TCP port is 54000. If this port is in use, then the MBS will automatically acquire another port from the port range until an available port is found (e.g. **TCP port:** 54001, 54002, 54003 – 54099).

The actual **TCP** and **UDP Ports** can be seen on AhsayOBM/AhsayACB when pairing a mobile device for mobile backup.

AhsayOBM

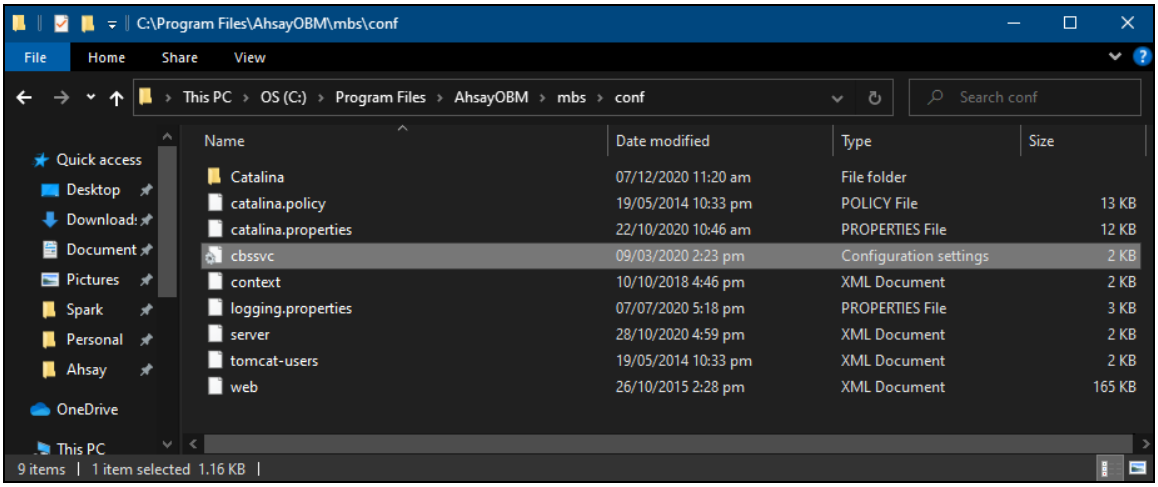
AhsayACB

cbssvc.ini

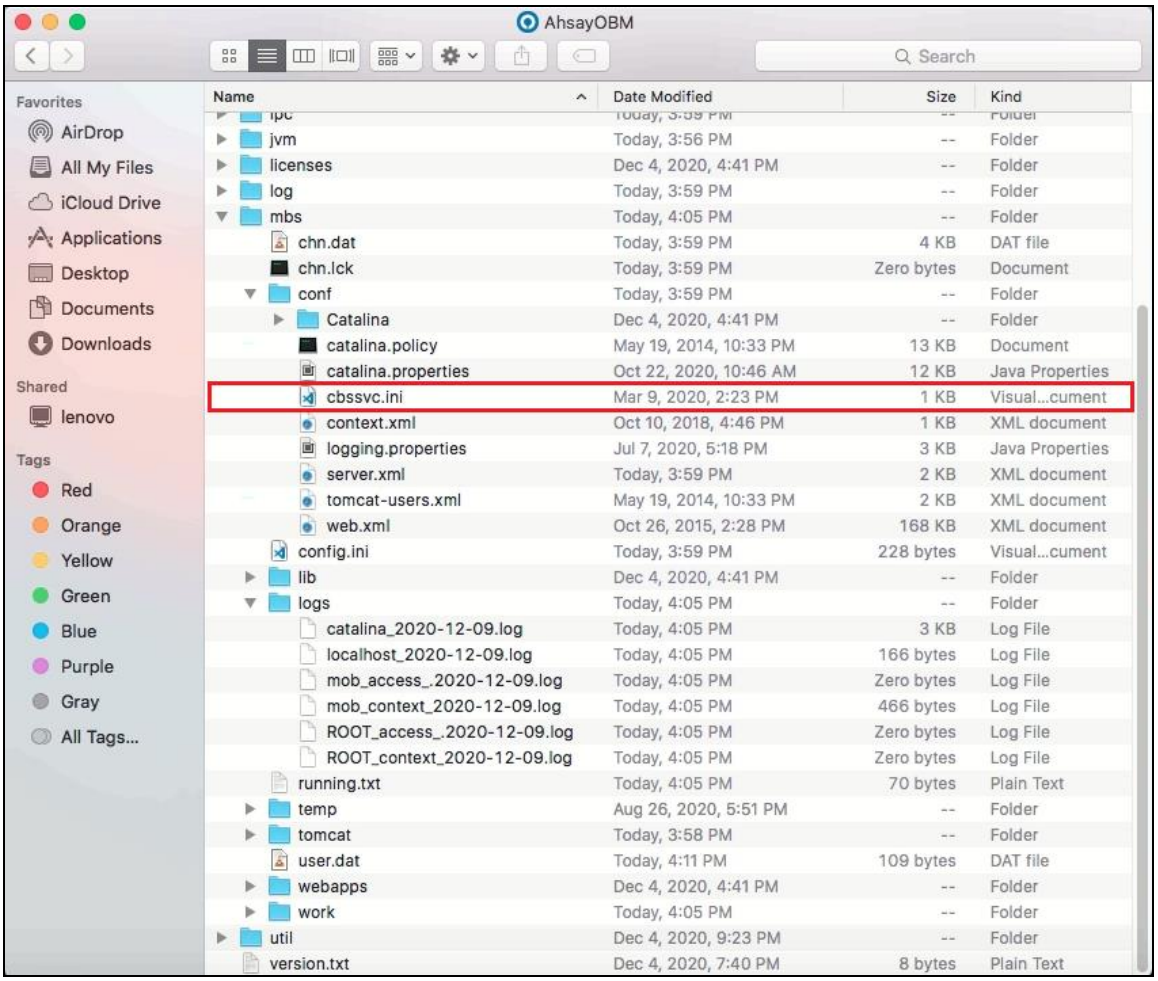
The "cbssvc.ini" is a configuration file of MBS which contains the memory settings. The important setting you need to be aware of is the **Java Heap Size.** The "cbssvc.ini" file is located in the following folder.

	Location
AhsayOBM	
Windows	*C:\Program Files\AhsayOBM\mbs\conf\cbssvc.ini*
macOS	*/Application/AhsayOBM.app/mbs/conf/cbssvc.ini*
AhsayACB	
Windows	*C:\Program Files\AhsayACB\mbs\conf\cbssvc.ini*
macOS	*/Application/AhsayOBM.app/mbs/conf/cbssvc.ini*

Example for AhsayOBM running on Windows



Example for AhsayOBM running on macOS



To check for the Java Heap Size settings, open the "cbssvc.ini" file using a text editor, then look for the values of Java Heap Size which are **`Xms512m`** and **`Xmx2048m`**.

```
-Xrs
-Xms512m
-Xmx2048m
-Xss384k
-XX:MetaspaceSize=96m
#-XX:MaxMetaspaceSize=160m
-XX:MaxMetaspaceSize=256m
-XX:MaxDirectMemorySize=512m
-XX:NewRatio=3
#-XX:SurvivorRatio=30
-XX:SurvivorRatio=32
-XX:MinHeapFreeRatio=20
-XX:MaxHeapFreeRatio=80
-verbose:gc
-XX:+PrintGCDetails
-XX:+PrintGCDateStamps
-XX:+UseConcMarkSweepGC
```

```
-XX:+UseCMSInitiatingOccupancyOnly
-XX:CMSInitiatingOccupancyFraction=85
-XX:+ScavengeBeforeFullGC
-XX:+CMSScavengeBeforeRemark
-Dsun.net.inetaddr.ttl=3600
-Dnetworkaddress.cache.ttl=3600
-Dsun.net.inetaddr.negative.ttl=300
-Dnetworkaddress.cache.negative.ttl=300
-Dsun.nio.PageAlignDirectMemory=true
-Djava.net.preferIPv4Stack=true
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Djava.util.logging.config.file=conf/logging.properties
-Dtc.work.path=work
-Dtc.log.path=logs
-Djavax.servlet.context.tempdir=work
-Djdk.nio.maxCachedBufferSize=262144
-Dfile.encoding=UTF-8
-Dsun.jnu.encoding=UTF-8
#-Dcom.sun.management.jmxremote
#-Dcom.sun.management.jmxremote.port=10010
#-Dcom.sun.management.jmxremote.rmi.port=10011
#-Dcom.sun.management.jmxremote.ssl=false
#-Dcom.sun.management.jmxremote.authenticate=false
```

-Xms512m

In the “cbssvc.ini” file, this specifies that the minimum Java heap size setting is 512MB.

-Xmx2048m

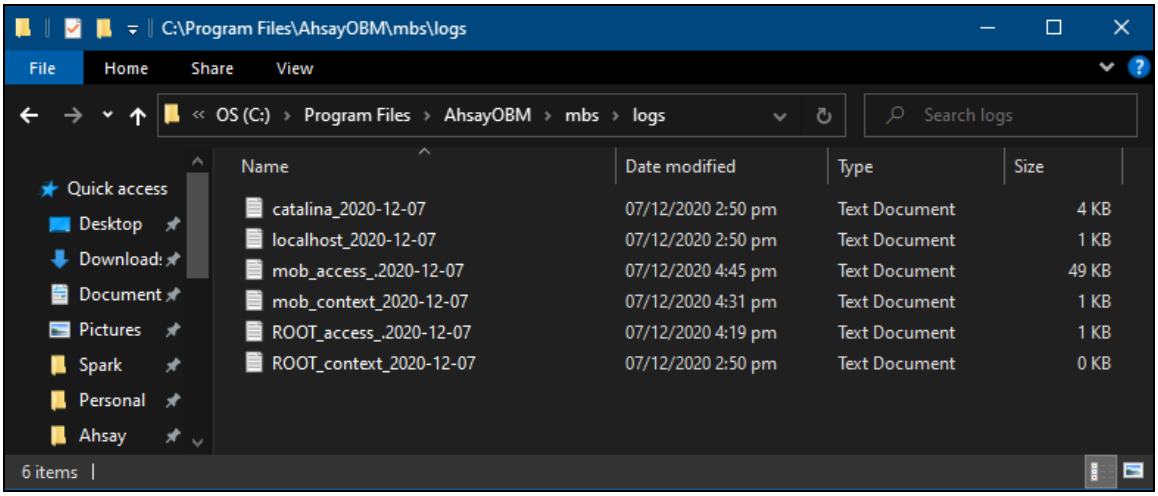
In the “cbssvc.ini” file, this specifies that the maximum Java heap size setting is 2048MB.

MBS logs

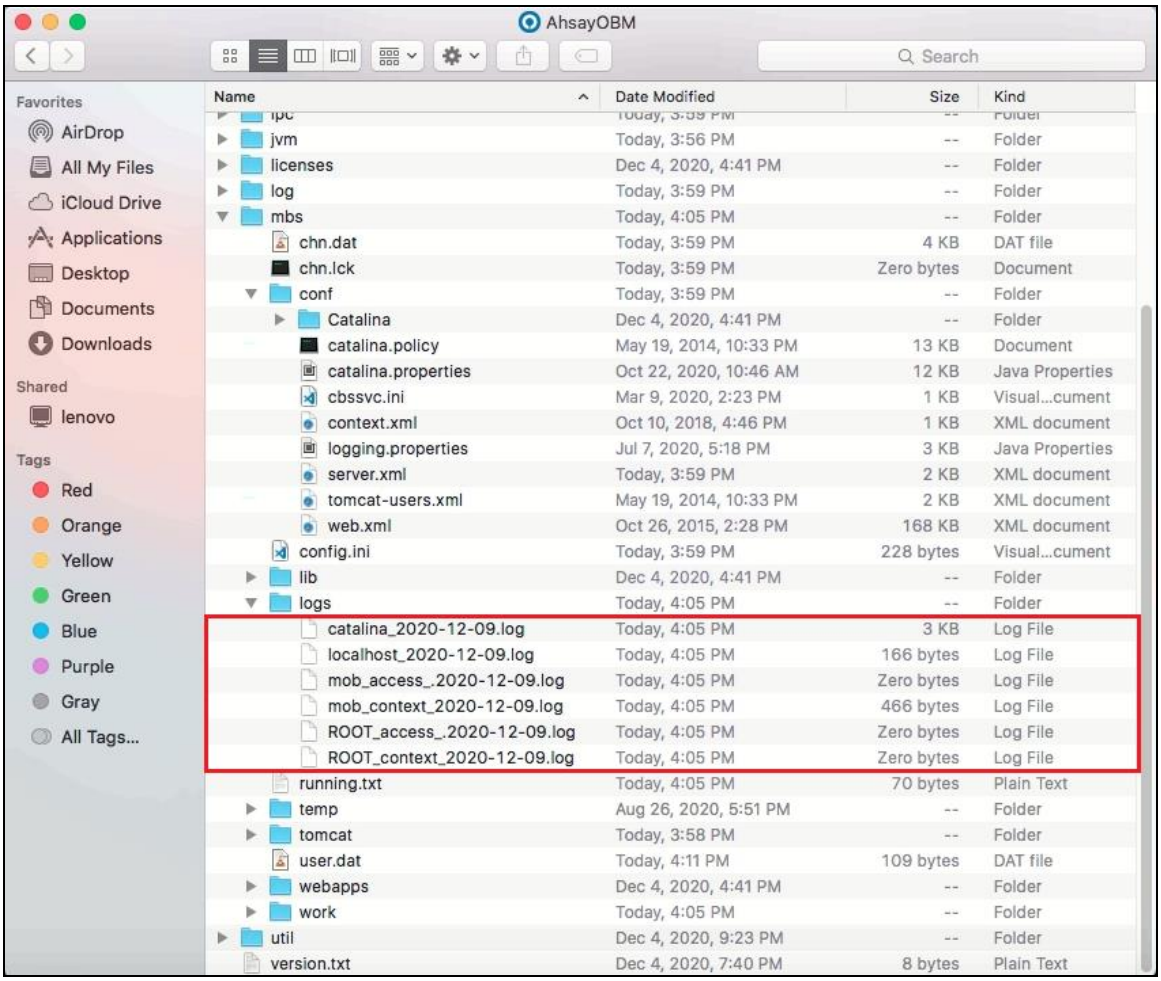
This folder contains the logs which can be used to check for any issues that may occur on the Mobile Backup Server (MBS).

	Location
AhsayOBM	
Windows	*C:\Program Files\AhsayOBM\mbs\logs*
macOS	*/Application/AhsayOBM.app/mbs/logs*
AhsayACB	
Windows	*C:\Program Files\AhsayACB\mbs\logs*
macOS	*/Application/AhsayACB.app/mbs/logs*

Example for AhsayOBM running on Windows



Example for AhsayOBM running on macOS



The MBS logs consist of the following:

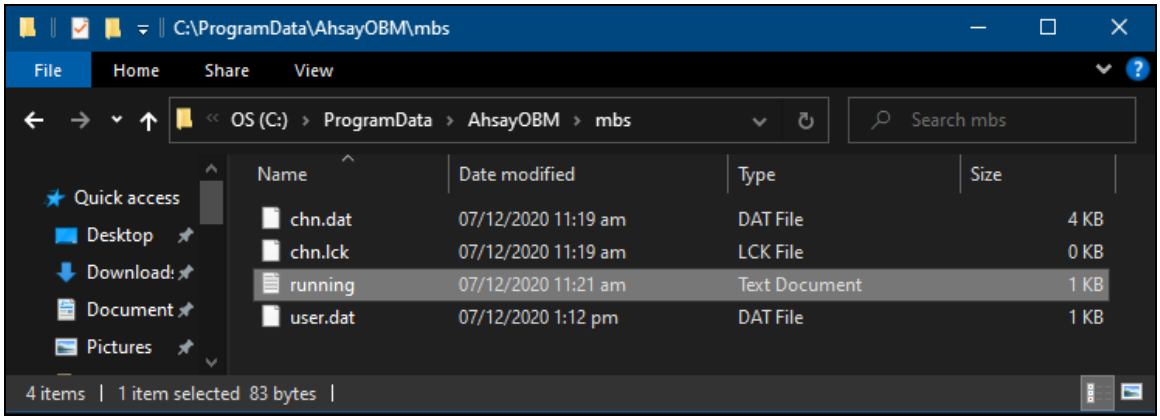
- catalina_YYYY-MM-DD.log
- localhost_YYYY-MM-DD.log
- mob_access_.YYYY-MM-DD.log
- mob_context_YYYY-MM-DD.log
- ROOT_access_.YYYY-MM-DD.log
- ROOT_context_YYYY-MM-DD.log

Troubleshooting MBS and Ahsay Mobile Connection Issues

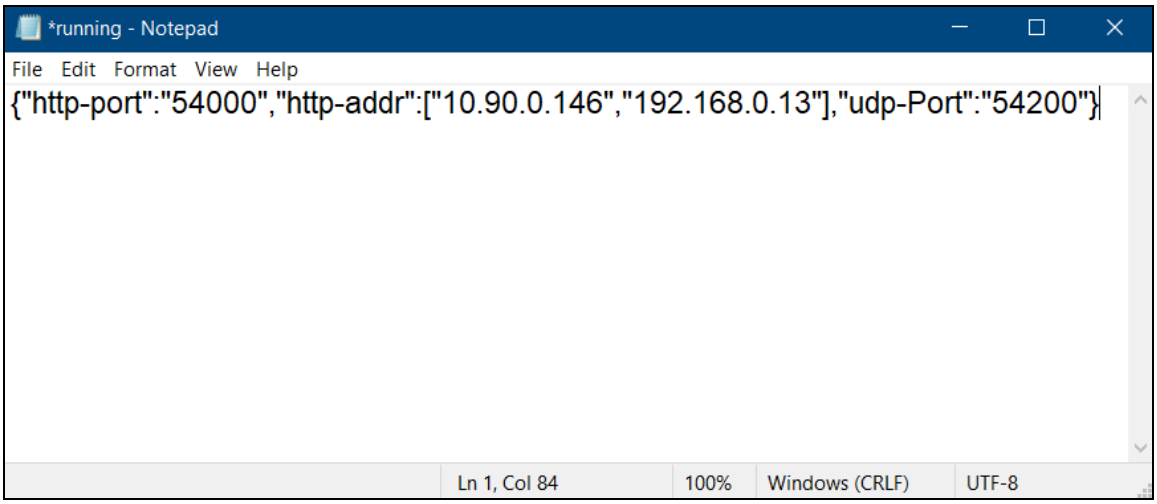
Usually once a mobile device installed with Ahsay Mobile is successfully registered for mobile backup with AhsayOBM/AhsayACB, the MBS will be automatically activated. However, if there are any issues connecting the mobile device to AhsayOBM/AhsayACB occur, then you can use the following steps to troubleshoot the problem.

Example for AhsayOBM running on Windows

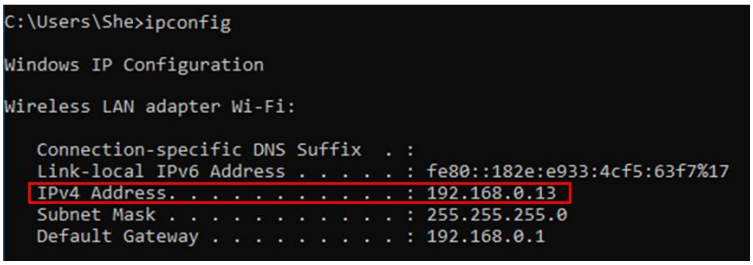
1. Go to *C:\ProgramData\AhsayOBM\mbs* then search for the "running.txt" file.



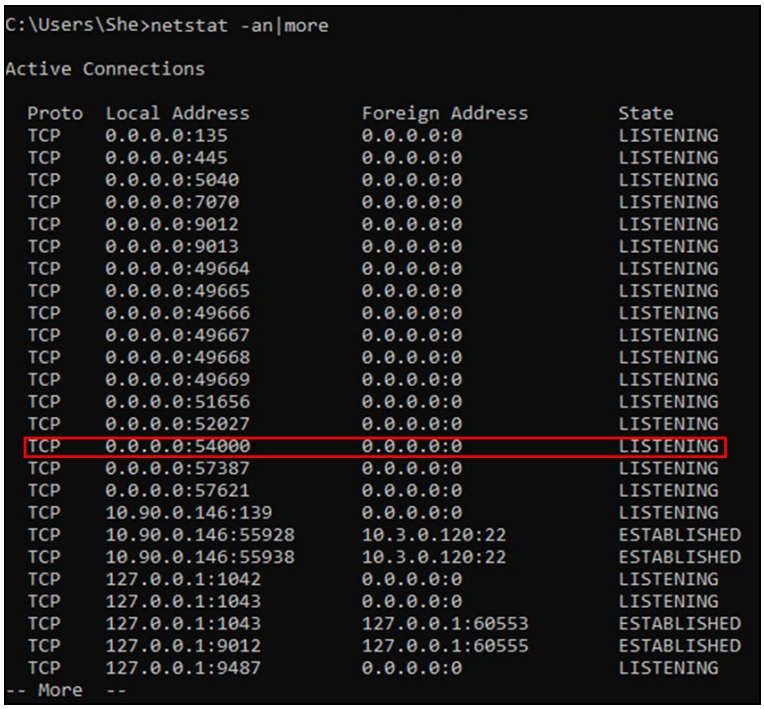
2. Open the "running.txt" file using a text editor (e.g. Notepad). The "running.txt" file contains the **HTTP Port**, **IP address**, and **UDP Port** which are in actual use of the MBS.



3. Using command prompt (cmd), verify if the IP address captured in the "running.txt" file is the correct IP address on the machine where AhsayOBM/AhsayACB is installed. To check the IP address, use the command **ipconfig**.



4. Also check for the actual TCP Port used by the MBS by running the command **netstat -an|more**.



5. Make sure that your firewall setting allows network traffic through the following TCP and UDP ports to ensure that the communication between your machine and mobile device is successful.

   AhsayOBM - TCP Port: 54000 to 54099 **UDP Port:** 54200 to 54299

   AhsayACB - TCP Port: 55000 to 55099 **UDP Port:** 55200 to 55299

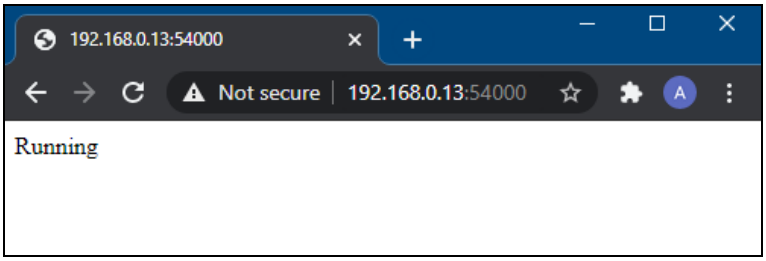
   Otherwise, mobile backup and restore will not work.

6. To perform an MBS status check, open a web browser on the AhsayOBM/AhsayACB machine and enter the IP address followed by the TCP port.

   Example:

   If the TCP Port used is 54000, enter “http://192.168.0.13:54000”. When the “Running” status is displayed, this means that the MBS is running.

   In the AhsayOBM machine

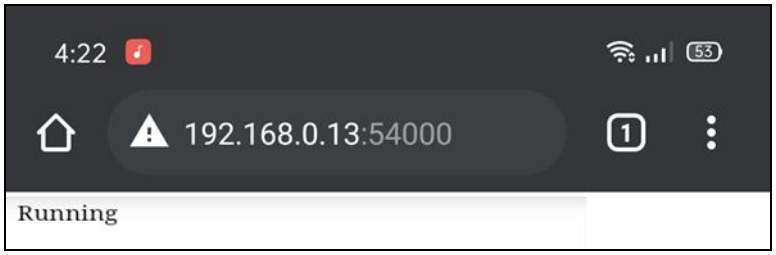


7. To run a connection test between the mobile device and AhsayOBM/AhsayACB machine, open a web browser on the mobile device and enter the IP address followed by the TCP port.

   Example:

   If the TCP Port used is 54000, enter “http://192.168.0.13:54000”. When the “Running” status is displayed, this means that the MBS is running.

   In the mobile device



Support Oracle 19c Database

AhsayOBM v8.5 (or above) offers support for Oracle 19c database backups in standalone installation.

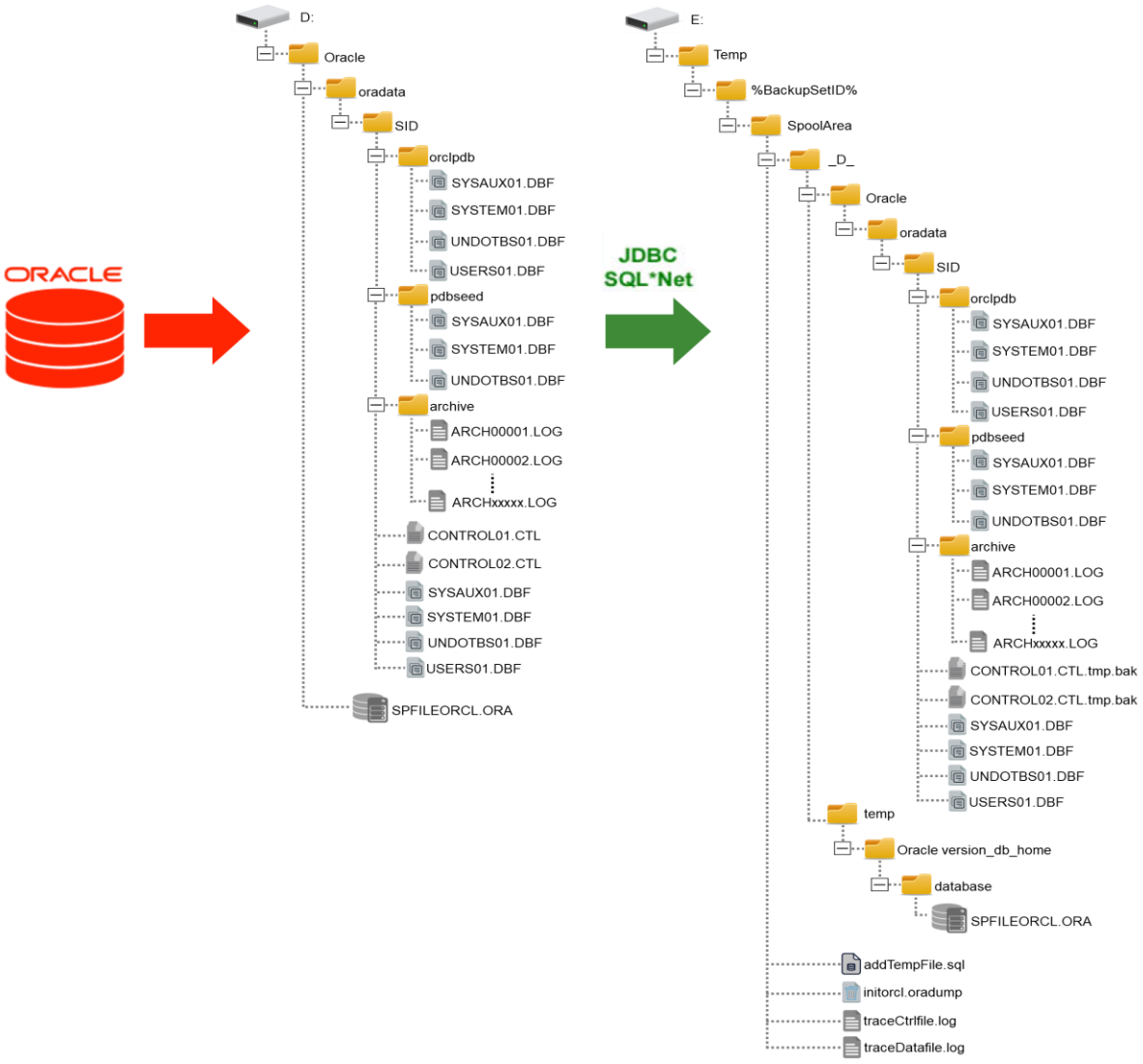
NOTE: Oracle advanced installations such as Clusterware or RAC (Real Application Clusters), ASM (Automatic Storage Management) and Data Guard etc. are not supported.

Oracle 19c database backup is supported on the following versions of Windows Server and Linux:

- **Windows Server 2019**
- **Windows Server 2012 R2**
- **Windows Server 2016**
- **Red Hat Enterprise Linux 7 and 8 (or above)**

AhsayOBM v8.5 (or above) uses a spooling method to make a consistent snapshot of the database(s) for Oracle database backup.

Below is the overview of the spooling method of Oracle database during backup for Windows:



The **temporary directory folder** will be used by AhsayOBM for each Oracle database backup as the storage of the following:

- The spooled Oracle database(s) and archived log files
- Any incremental or differential delta files generated

Therefore, it is strongly advised that the temporary directory folder is **located on a local drive with enough free disk space** to store the spooled databases and archived log files.

The temporary directory folder should not be on the location of the Oracle Home drive.

The calculation of disk space required on the drive where the temporary directory folder is located is as follows:

(Total Database Size * Delta Ratio) * number of backup destinations = **Minimum Free Space Required**

For example:

If the default Delta ratio is 50% for in-file delta, and if the total Oracle database size is 1TB and there is only one backup destination, the minimum free space needed on the drive where the temporary directory folder is located = 1.5TB:

1TB = Total Oracle database size
500GB = Total maximum size of incremental or differential delta files generated

For more details, please refer to the following guides:

AhsayOBM v8 User Guide - Oracle Backup and Restore Guide for Windows
AhsayOBM v8 User Guide - Oracle Database Backup and Restore for Linux (GUI)
AhsayOBM v8 User Guide - Oracle Database Backup and Restore for Linux (CLI)

Support MariaDB Database version 10

AhsayOBM v8.5 (or above) offers support for MariaDB database versions **10**, **10.1**, **10.2**, **10.3**, **10.4**, and **10.5**.

NOTE: AhsayOBM must be installed on MariaDB database server.

The backup of MariaDB is supported on the following versions of Windows, Windows Server and Linux:

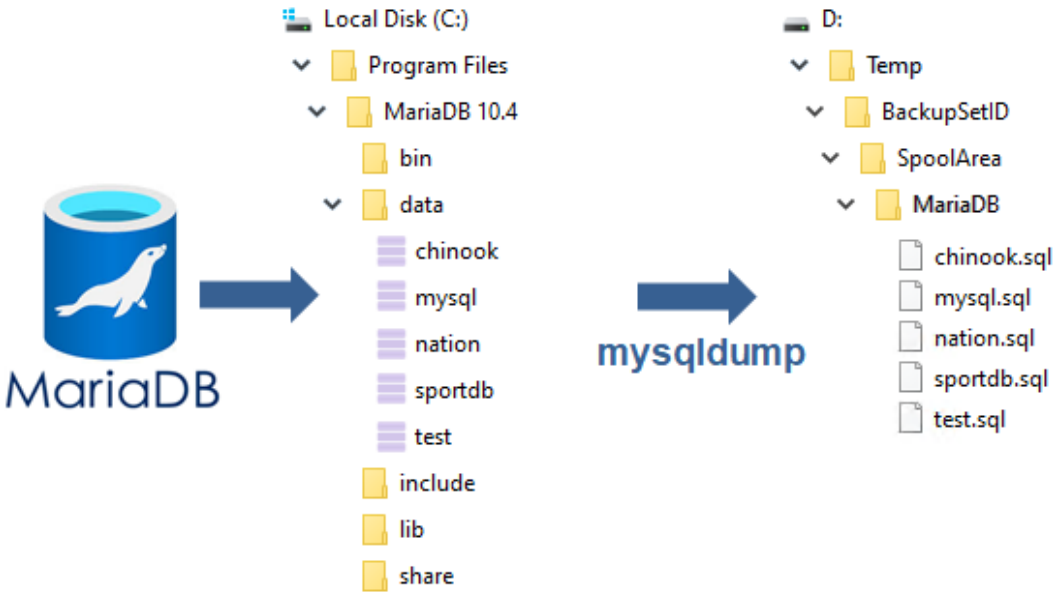
- **Windows Server 2019**
- **Windows Server 2016**
- **Windows Server 2012 R2**
- **Windows Server 2008 R2 and 2008**
- **Windows 10, 8 and 7**
- **Red Hat Enterprise Linux 7 and 8**
- **CentOS 7 and 8**

AhsayOBM v8.5 (or above) uses a spooling method to make a consistent snapshot of the database(s) for MariaDB database backup. The database files (.sql) will be spooled to the temporary directory folder using the **mysqldump** utility.

The *mysqldump* utility is installed on the MariaDB database server.

Example: The default location of the *mysqldump* utility for MariaDB v10.4 is: *C:\Program Files\MariaDB 10.4\bin*

Below is the overview of the spooling method of MariaDB database during backup for Windows:



The **temporary directory folder** will be used by AhsayOBM for each MariaDB database backup as the storage of the following:

- Database files (.sql)
- Any incremental or differential delta files generated

Therefore, it is strongly advised that the temporary directory folder is **located on a local drive with enough free disk space** to store the spooled database files.

The calculation of disk space required on the drive where the temporary directory folder is located is as follows:

(Total Database Size * Delta Ratio) * number of backup destinations = **Minimum Free Space Required**

For example:

If the default Delta ratio is 50% for in-file delta, and if the total MariaDB database size is 100GB and there is only one backup destination, the minimum free space needed on the drive where the temporary directory folder is located = 150GB:

100GB = Total MariaDB database size

50GB = Total maximum size of incremental or differential delta files generated

For more details, please refer to the following guides:

AhsayOBM v8 User Guide - MariaDB Database Backup and Restore for Windows
AhsayOBM v8 User Guide - MariaDB Database Backup and Restore for Linux (CLI)

Backup Report Selection

On the previous versions i.e. AhsayOBS v6, AhsayCBS v7 and pre-AhsayCBS v8.5, there were only two options available for email notifications for backup reports: **no reports** or **all reports**. When email notifications for backup reports is enabled, this can cause mailboxes of the AhsayCBS administrators or Managed Service Providers (MSP) to be overloaded with email notifications, especially when they manage hundreds or thousands of backups per day.

While for end users, they may not want to be bothered with daily backup email notifications when their backups are running smoothly. They only want to be notified if there are problems with the backup job, so they could take corrective action(s).

On the AhsayCBS v8.5 (or above), the email notification for backup reports settings have been enhanced to allow a selection of specific types of email notifications which the AhsayCBS administrators, Managed Service Providers (MSP), or their client would like to receive.

However, the default email notification settings for backup reports is still **All reports** on:

- New installations of AhsayCBS v8.5 (or above)
- All versions of AhsayOBS v6, AhsayCBS v7, and pre-AhsayCBS v8.5 which are upgraded to AhsayCBS v8.5 (or above)

The enhanced email notification settings for backup report consists of three (3) options:

- **No reports**
  No email notifications and backup reports will be sent to the contact email address of the backup user account.
- **All reports**
  All email notifications and backup reports will be sent to the contact email address of the backup user account. This is the default backup report option on the new AhsayCBS v8.5 (or above) after installation when upgraded from v6, v7, and pre-v8.5.
- **Specific reports**
  This option enables the AhsayCBS administrators or Managed Service Providers (MSP) to only select specific backup report(s) that they would like to receive email notification for.

The backup report settings will only affect the email notifications. If the user would like to see the details for the backup reports that are not selected on the **specific reports** option, they can either log in to the AhsayCBS web console or AhsayOBM/AhsayACB client machine to check the details for these backup reports.

The following table shows the description of each backup report type.

Backup Report	Description	
Backup Errors	Backup jobs that encounters any type of error(s) during backup process.	
Backup quota exceeded	**Storage Quota Exceeded** When the current storage usage has exceeded the storage quota defined on the backup destination(s) for the AhsayOBM/AhsayACB user account.	**License Module Quota Exceeded** When the current license quota usage has exceeded the allocated quota on the following Add-on Modules for the AhsayOBM/AhsayACB user account. AhsayOBM: • VMware • Hyper-V • MS Exchange Mailbox • Office 365 • OpenDirect / Granular Restore AhsayACB: • Office 365 • OpenDirect / Granular Restore
Backup warnings	**Warnings** When the backup job encounters any type of warning(s) during the backup process.	**User interrupted** When the user stops or terminated the backup job before it is completed.
Backup successful	**OK** When the backup job is completed successfully which involves the following actions: • new files and/or folders • updated files • updated file permissions • moved files and/or folders • deleted files and/or folders	**OK (no files backed up)** When the backup job is completed successfully but without backed up files or changes in the backup source.

For further details on the email notification settings for **specific report(s)**, refer to the following examples.

Scenario 1

RESULT: Only email notifications for the following backup reports will be sent to the contact email address, and no email notifications will be sent for successful backups:

- Backup Errors
- Backup quota exceeded (Storage and License Module Quota Exceeded)
- Backup warnings (Warnings and User interrupted)

Scenario 2

RESULT: Email notifications for all backup reports except for user interrupted backups will be sent to the contact email address, as the backup user(s) is already aware of the backup job status which is "Backup Interrupted by User", since they have stopped the backup job themselves.

VMware ESXi/vCenter VDDK API Changes

Due to issues encountered on some VMware ESXi/vCenter setups with the latest VMware VDDK 7 API implemented from AhsayOBM v8.3.4.0 onwards on VDDK mode backup set, these have been found to cause problems on AhsayOBM related to both backup and restore.

For more details, refer to the following link:

https://communities.vmware.com/t5/Virtual-Disk-Development-Kit/VixDiskLib-Open-fails-in-VDDK-7-0-using-a-vmPath-in-the-vmxSpec/m-p/1846640

Starting from v8.5, Ahsay has decided to **temporarily revert to VDDK 6 API** until the VDDK 7 API bug is addressed by VMware. Until further notice, **VDDK 6 API** will be used for:

- all new installations of AhsayOBM v8.5 (or above); and
- AhsayOBM upgrades from v6, v7, or pre-v8.5 to AhsayOBM v8.5 (or above)

Affected existing AhsayOBM versions with VDDK 7 API:

- AhsayOBM v8.3.4.0 to v8.3.6.x

Affected VMware versions:

- VMware ESXi/vCenter v6, v6.5, v6.7, and v7 backup sets running in **VDDK backup mode**.

Action required to fix this problem:

- Partners with clients with VMware VDDK mode backup sets on the affected AhsayOBM versions are strongly advised to immediately upgrade to AhsayOBM v8.5 (or above).

  Once AhsayOBM is upgraded to v8.5 (or above), the existing VMware ESXi/vCenter backup jobs will resume running without any further configuration or intervention.