Ahsay Backup

Ahsay Backup Software v9

Whitepaper on Data Security

Ahsay Systems Corporation Limited

6 April 2022

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.

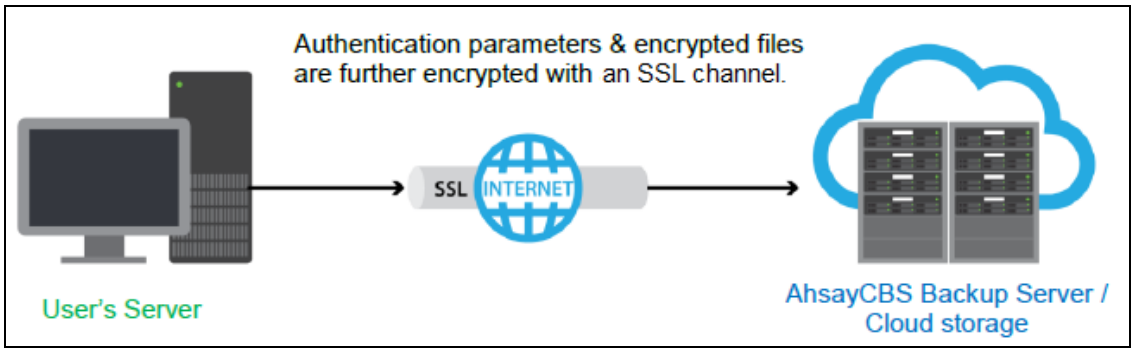
Table of Contents

1 Introduction

This document describes the security measures available in Ahsay Backup Software from a user's perspective. It serves as a reference for partners when addressing customers' queries on security.

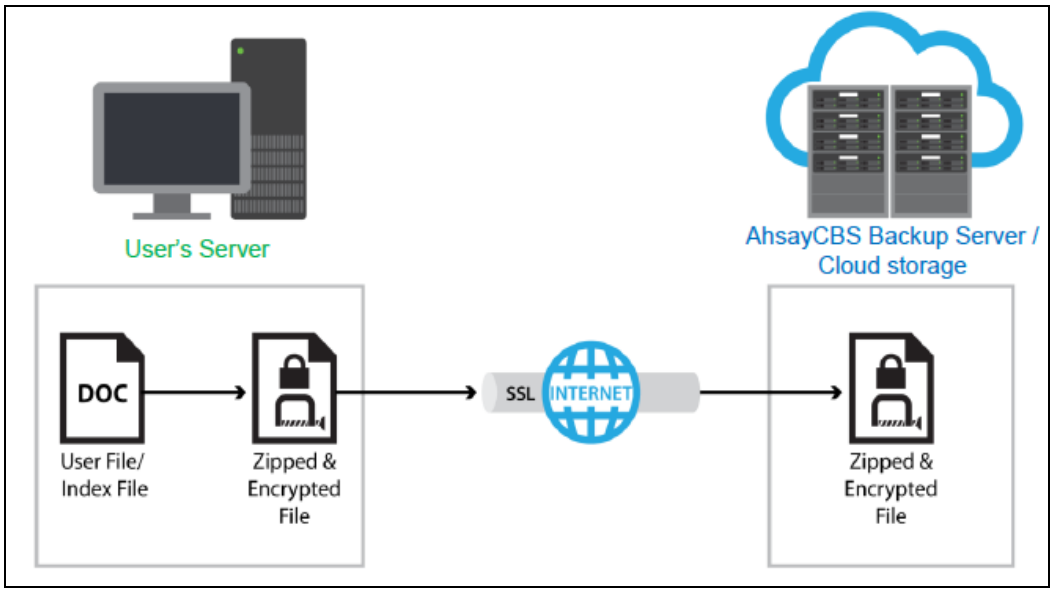
2 Data Security of your Backup Data

2.1 Secure 256-bit SSL Communication



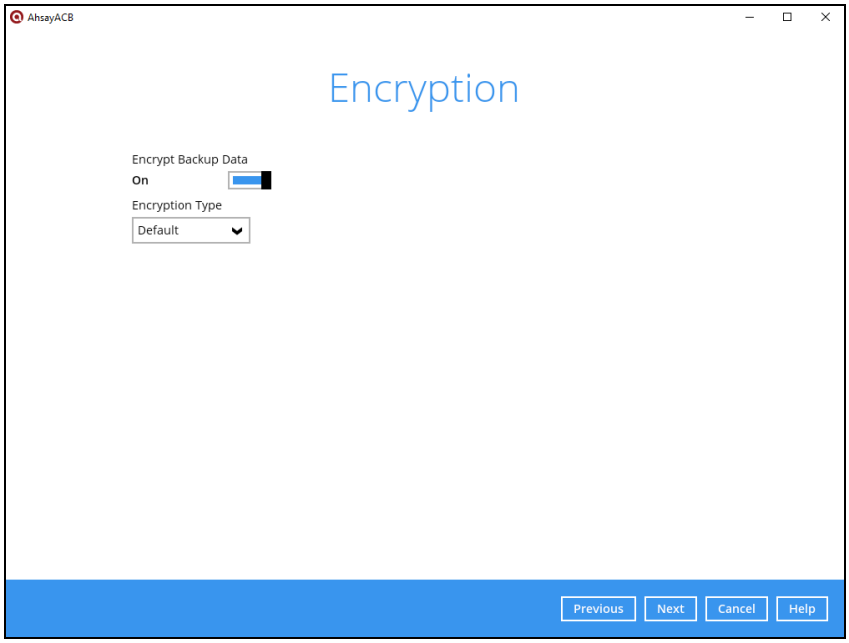
When enabled with HTTPS and the AhsayCBS installed with a trusted SSL certificate, all communications between AhsayCBS backup server/cloud storage and your computer are transported in a 256-bitSSL (Secure Socket Layer) channel. Although all your backup files travel through a public network (Internet), eavesdroppers have no knowledge of what has been exchanged.

2.2 Backup Data are securely encrypted



By default, the Encryption feature is enabled on your AhsayOBM / AhsayACB client backup software. Data encryption is done on your machine before your backup data are uploaded to AhsayCBS backup server or cloud storage.

When "Default" encryption type is selected, a randomly generated 44 alpha numeric characters will be used as the encryption key, and data will be encrypted with 256-bit AES algorithm and CBC method. This encryption method cannot be hacked even by supercomputer and thus is totally secure. To all people but you, your files stored on AhsayCBS backup server are no more than some garbage files with random content.

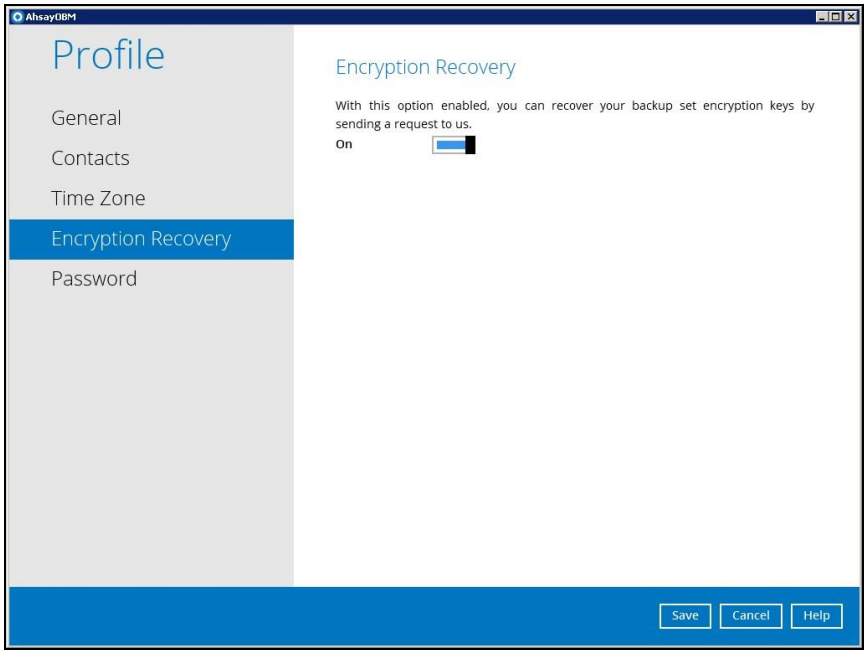


Other choices for Encryption Type are: *Custom* and *Password*.

Note: Selecting '*User Password*' type, will use your password from the day this Backup Set is created.

2.3 Your Encryption Key is well protected

You can decide whether to upload your encryption key to AhsayCBS backup server, through the Encryption Recovery feature in your AhsayOBM / AhsayACB software.



The benefit of having the Encryption Recovery feature disabled is that the encryption key used to encrypt your files will reside only on your computer and is known only to you. Thus, even the AhsayCBS System Administrator will not be able to decrypt and view the content of your files stored on the backup server or cloud storage without your permission.

However, this unfortunately means if the encryption key is lost, you will never be able to recover your backup files.

On the other hand, even if the Encryption Recovery is enabled, no security will be compromised, as your encryption key will be uploaded to AhsayCBS, in unreadable encrypted format instead of readable plain text format. That means your encryption key will first be encrypted on your computer before it is uploaded to AhsayCBS. In case you lost your encryption key, you can send a request to AhsayCBS System Administrator, and the Administrator will then send your encrypted encryption key to our software vendor (Ahsay). Ahsay will decrypt your encrypted encryption key file, and directly send the decrypted key to your registered email address. Since your encryption key uploaded to AhsayCBS is in encrypted format, administrator won't be able to decrypt and know your encryption key. Besides, the decrypted key will be directly sent to your email address registered in your AhsayOBM/ AhsayACB client backup software, the administrator won't be able to get the decrypted encryption key. For the software vendor, they only have the encryption key but do not have the access to your backup data. Therefore, the whole mechanism is secure.

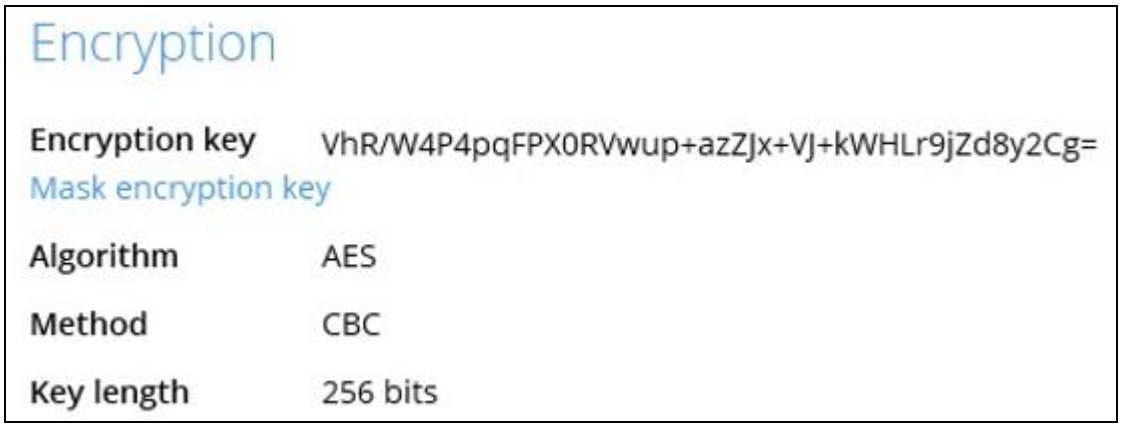
If you resort to using Encryption Recovery service, it would be good practice to create a new Backup Set afterwards, with a new encryption key, and run new jobs; then phase out and eventually delete the Backup Set which had its key recovered.

2.4 NSA-approved encryption algorithm is used

Currently, the algorithm used by the Default encryption type for encrypting your files is Advanced Encryption Standard (AES), with 256-bit block ciphers. It is adapted from a larger collection originally published as Rijndael. AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) of USA for protecting top secret information. It is commonly recognized as one of the most secure encryption algorithms in today's standard. You may refer to this Wiki article for the details of AES algorithm: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

2.5 Require 3 x 10^{51} years to crack the 256-bit encryption

When you use Default encryption type in your AhsayOBM / AhsayACB software to encrypt your backup data, your encryption key will have 256-bit key size which has 2256 or around 1.16 x 1077 possible combination. According to this Wiki article (https://en.wikipedia.org/wiki/Brute-force_attack), even if 50 supercomputers are used to crack your key by brute-force attack, they still need 3 x 1051 years to crack it. It's thus super safe. Below is a sample encryption key for your reference:



2.6 Cloud Storage

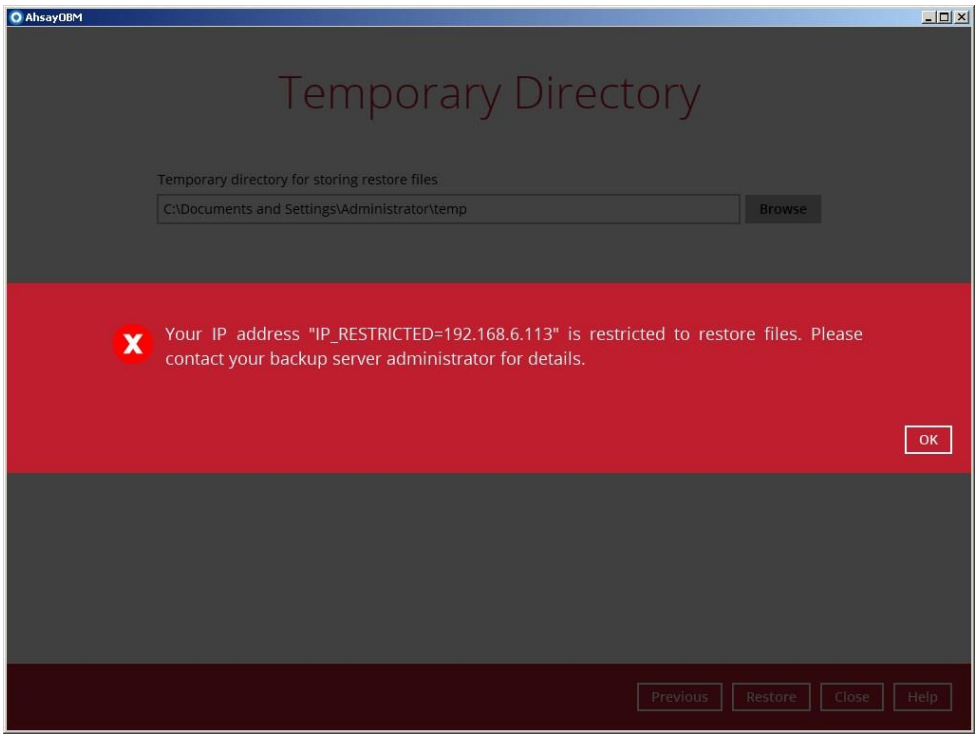
Amongst the Destinations visible to you, if your AhsayCBS Administrator allows, you can back up your source data to one of the supported cloud destinations. You'll need to input your cloud destination's access key or credential to link your Backup Set with your cloud destination. Certain cloud destinations allow you to select whether to connect with or without SSL/TLS; this will vary as some destinations have it enabled by default while others allow granular selection.

Below example input for adding S3-Compatible Storage:

2.7 Restrict access to data by IP addresses

In case you want to further tighten the security, you can also send your list of "IP Allowed for Restore" to us (the AhsayCBS Administrator), so that we can help you restrict the access to your backup files from the set of IP addresses you defined.

If someone tries to access and restore your data from an IP address that is not on your defined list, their access will be denied. This additional security ensures your backup data will not be accessible to all location, even the username and password of AhsayOBM / AhsayACB software are known.



2.8 TLS and Cipher

For backward compatibility with our legacy clients (AhsayOBM, AhsayACB, AhsayOBS), out of the box the product supports TLS 1.0, 1.1, and 1.2.

If you do not require legacy support, then with some simple edits to the AhsayCBS configuration, the AhsayCBS Administrator can enable only TLS1.2 and strong cipher.

2.9 Mobile Authentication

Mobile Authentication feature is introduced to provide Two-Factor Authentication (2FA) during log in for added security.

During log in, aside from providing the normal Ahsay password, an additional step will need to be completed to finish the log in steps.

AhsayCBS v9 supports two options of Mobile Authentication:

Ahsay Mobile app - Accept the notification request sent to the Ahsay Mobile app or use a time-based one-time password (TOTP) code.

Third-Party Authenticator app - Provide the time-based one-time password code generated by a third-party authenticator app. Examples of these apps are Google Authenticator, Microsoft Authenticator, LastPass Authenticator etc.

Your AhsayCBS System Administrator may enable this for all or select users for improved security.

Note: Twilio, formerly supported by AhsayCBS v8, is no longer supported for new setup.

2.10 Policy

As a user, your view may be limited or removed if the AhsayCBS System Administrators created custom Policies and User Groups which help to manage some security parameters that are featured in our product.

Such as,

- Require Two-Factor Authentication for users.
- Set Password complexity and age requirements.
- Block access due to too many failed attempts.
- Disable user ability to Save Password on the client application.
- Disable user access to Deleting Backup Sets.
- Destinations visibility.

Your administrator should provide you with how your user account is policed.

2.11 Ransomware

Your backup data stored on AhsayCBS or other destinations, if enabled with encryption help to protect your data from hackers accessing your data. However, as with any binary file stored on a file system, they can be susceptible to wrapped by ransomware. Think of a zip file being zipped again.

You should consult with your AhsayCBS Administrator if they further protect your data at rest, by such feature as AhsayCBS Replication.

AhsayCBS Replication can replicate data stored on the AhsayCBS Backup Server, to a secondary AhsayCBS server acting as a repository. AhsayCBS to CBS Replication provides additional benefit as Replication Retention setting, a feature to provide additional days of recovery (snapshot) from the Replication Receiver server.

3 Contact Ahsay

If you have any question or suggestion about this document, please contact your local AhsayCBS Administrator, or Ahsay Customer Service Team at: http://www.ahsay.com/support.