Ahsay Backup

Ahsay Backup Software | v7

Whitepaper on Data Security

Ahsay Systems Corporation Limited

27 June 2016

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

Ahsay Backup Software | Backup Software

Whitepaper on Data Security

Copyright Notice

Trademarks

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

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

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

Dropbox is registered trademark of Dropbox Inc.

Google Cloud Storage and Google Drive are registered trademarks of Google Inc.

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

Microsoft, Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, One Drive and One Drive for Business are registered trademarks of Microsoft Corporation.

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

Oracle, Oracle 10g, Oracle 11g and MySQL are registered trademarks of Oracle Corporation.

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

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

ShadowProtect is registered trademark of StorageCraft Technology Corporation.

Vmware, ESX, ESXi, Vcenter are registered trademarks of Vmware, Inc.

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

Disclaimer

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

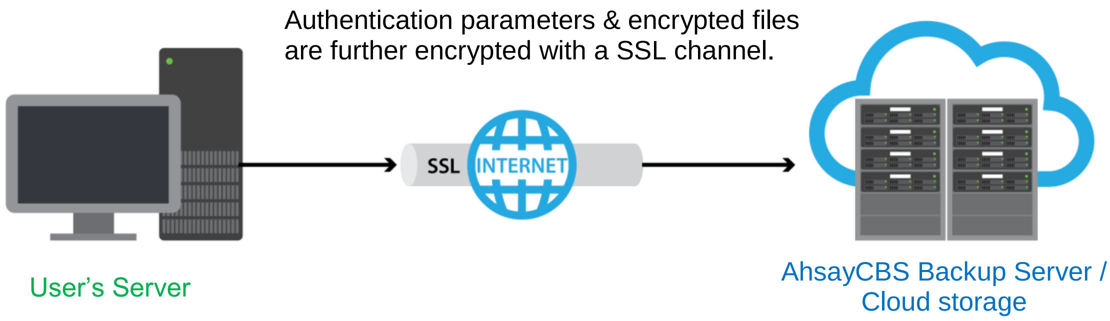
Table of Contents

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.

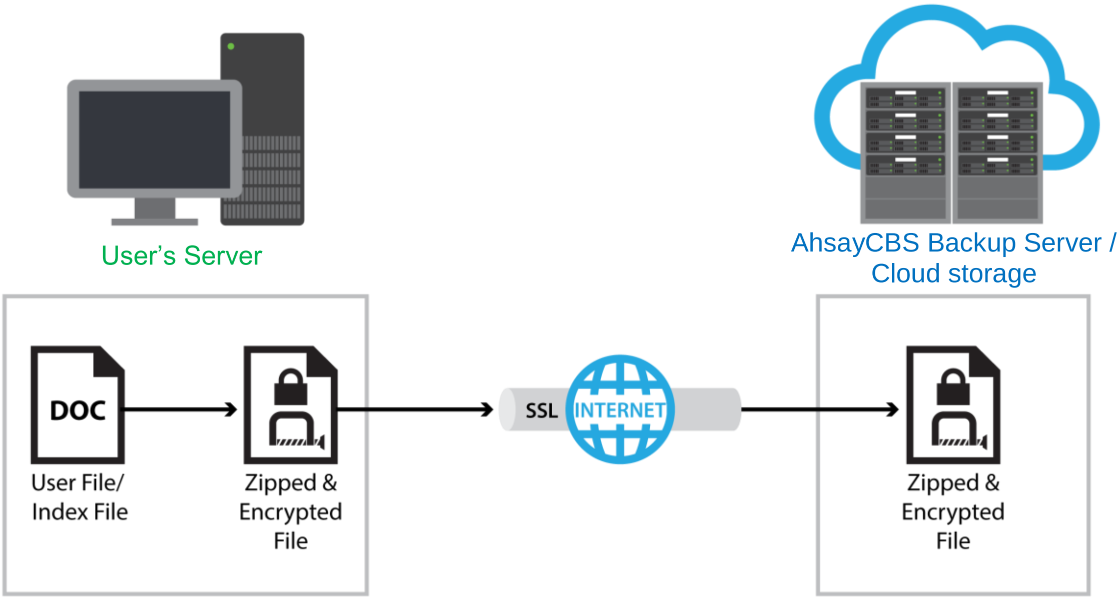
2 Data security of your backup data

2.1 Secure 256-bit SSL communication


Authentication parameters & encrypted files are further encrypted with a SSL channel.
SSL
INTERNET
User's Server
AhsayCBS Backup Server / Cloud storage

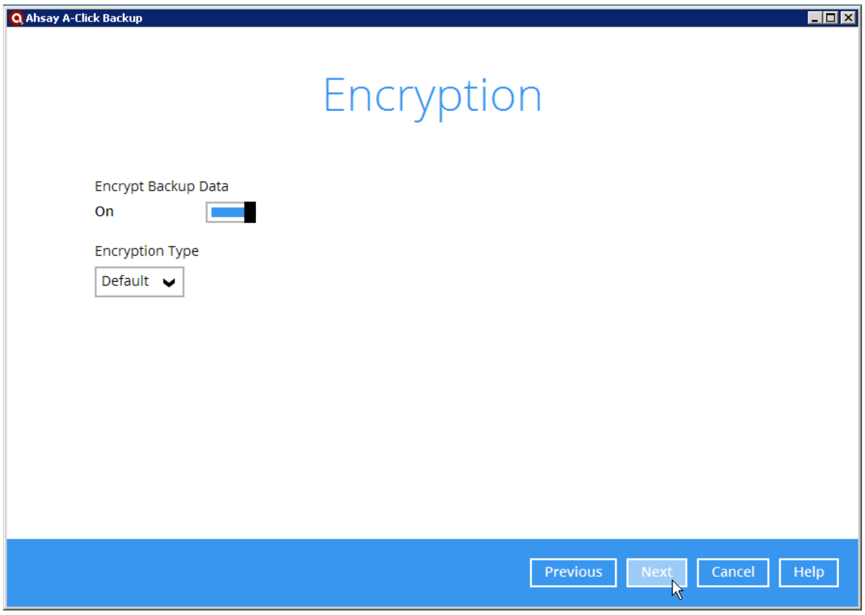
All communications between AhsayCBS backup server / cloud storage and your computer are transported in a 256-bit SSL (Secure Socket Layer) channel. Although all your backup files travel through a public network (Internet), eavesdroppers have no knowledge of what has been exchanged.

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.



Ahsay A-Click Backup

Encryption

Encrypt Backup Data

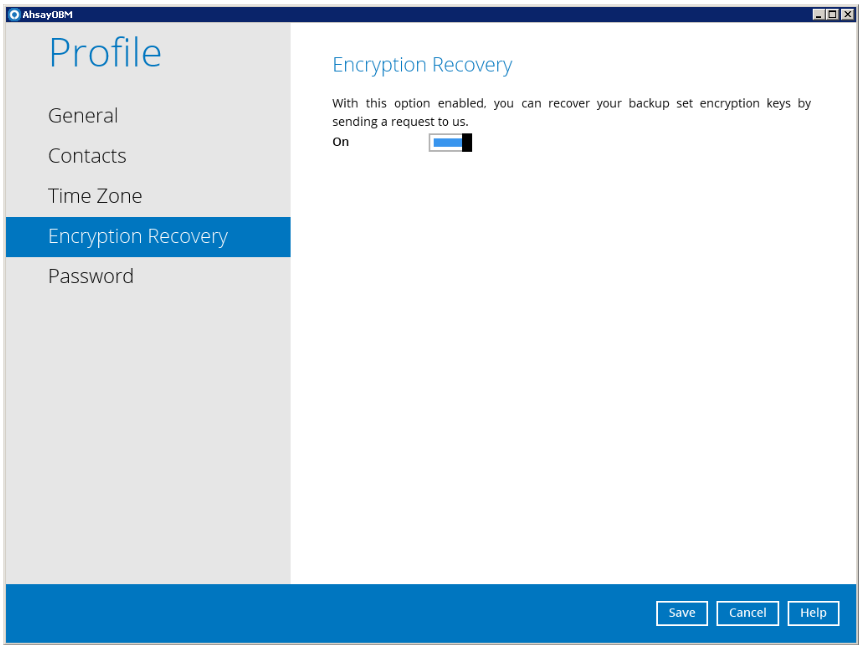
On

Encryption Type

Default

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.



AhsayOBM

Profile

Encryption Recovery

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

On

The benefit of having the Encryption Recovery feature disabled is that the encrypting key used to encrypt your files will be resided 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 encrypting key is lost, you will never be able to recover your backup files.

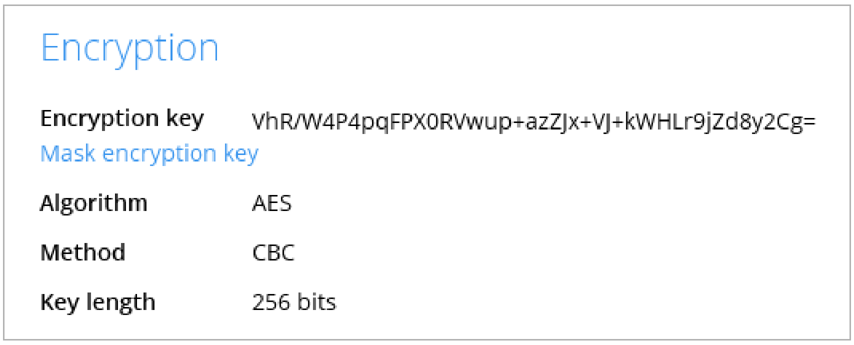
On the other hand, even if the Encryption Recovery is enabled, no security will be compromised, as your encryption key will be uploaded to AhsayCBS, in unreadable encrypted format instead of readable plain text format. That means your encryption key will first be encrypted on your computer before it is uploaded to AhsayCBS. In case you lost your encryption key, you can send a request to AhsayCBS system administrator, and the administration 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 totally secure.

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 2^{256} or around 1.16 x 10^{77} 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 10^{51} years to crack it. It’s thus super safe. Below is a sample encryption key for your reference:



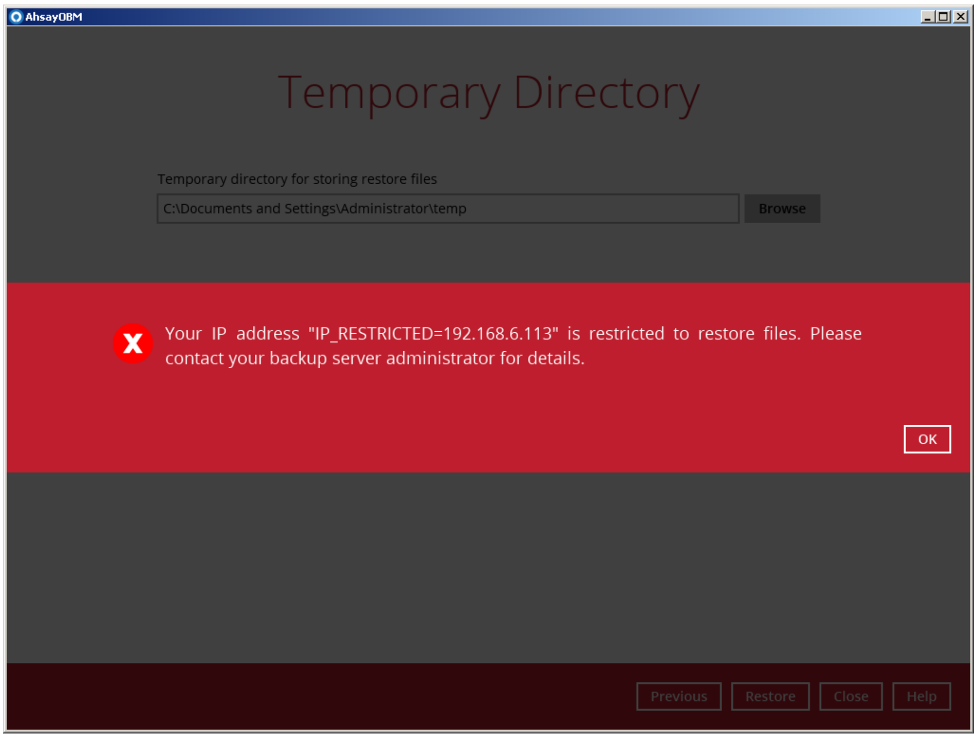
Encryption

Encryption key	VhR/W4P4pqFPX0RVwup+azZJx+VJ+kWHLr9jZd8y2Cg=
Algorithm	AES
Method	CBC
Key length	256 bits

2.6 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, 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.



C:\Documents and Settings\Administrator\temp

Your IP address "IP_RESTRICTED=192.168.6.113" is restricted to restore files. Please contact your backup server administrator for details.

3 Further Information

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