FAQ: Best practices for managing encryption key on AhsayOBM or AhsayACB?

Article ID: 5034
Reviewed: 28/08/2015

Product Version:
AhsayACB / AhsayOBM: 7.3 or above
OS: All platforms

Contents

Frequently Asked Questions:

1. What is the 'default' encryption setting of a backup set?

Answer) For backup sets created with AhsayOBM or AhsayACB version 7.3 or above, the default encryption setting of a backup set is:

- Encryption Key: A randomly generated key of 44 alpha numeric characters
- Encryption Key Length: 256 bits
- Encryption Algorithm: AES
- Encryption Method: CBC

Note that for backup account with multiple backup sets, even if the user had chosen to use 'default' setting for their backup sets, each backup set will have its own encryption key.

Important:
For users who may have used older releases of AhsayOBM or ACB, the 'default' encryption setting is no longer the password. The default setting has changed since version 7.3.

2. Can I change the encryption setting of a backup set?

Answer) The encryption setting of a backup set is generated at the backup set creation time, and cannot be changed afterward.

3. Can I restore my backup data if I have lost my encryption key?

Answer) No, if you have lost the encryption key of your backup set, it will be impossible to restore data from the corresponding backup set.

4. Where is the encryption setting of a backup set saved at?

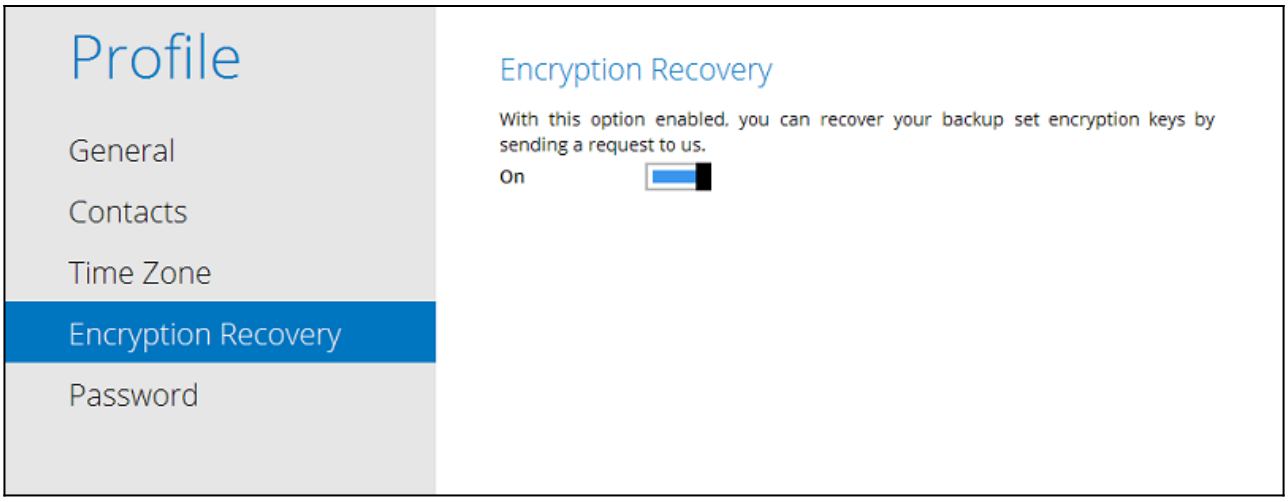
Answer) The encryption setting of a backup set is saved locally on the client computer, at:

~/.obm/config/settings.sys

You can also save the encryption setting of your backup sets on the backup server by enabling the 'Encryption Recovery' option within the client user interface:

- Login to the AhsayOBM / ACB user interface.
- Click on the User Profile (icon beside the username):

- Select **Encryption Recovery** then enable the setting:



Or from the AhsayCBS web console:

- Login to the AhsayCBS console.
- Select **User & User Group** under **User Management**.
- Select the corresponding user, then under **User Profile**, enable **Upload encryption key after running backup for recovery**:

If this option is enabled, the encryption key (in encrypted format) of the backup set would be uploaded to the backup server whenever a backup job is performed.

The encryption key would be saved within the user home of the corresponding account:

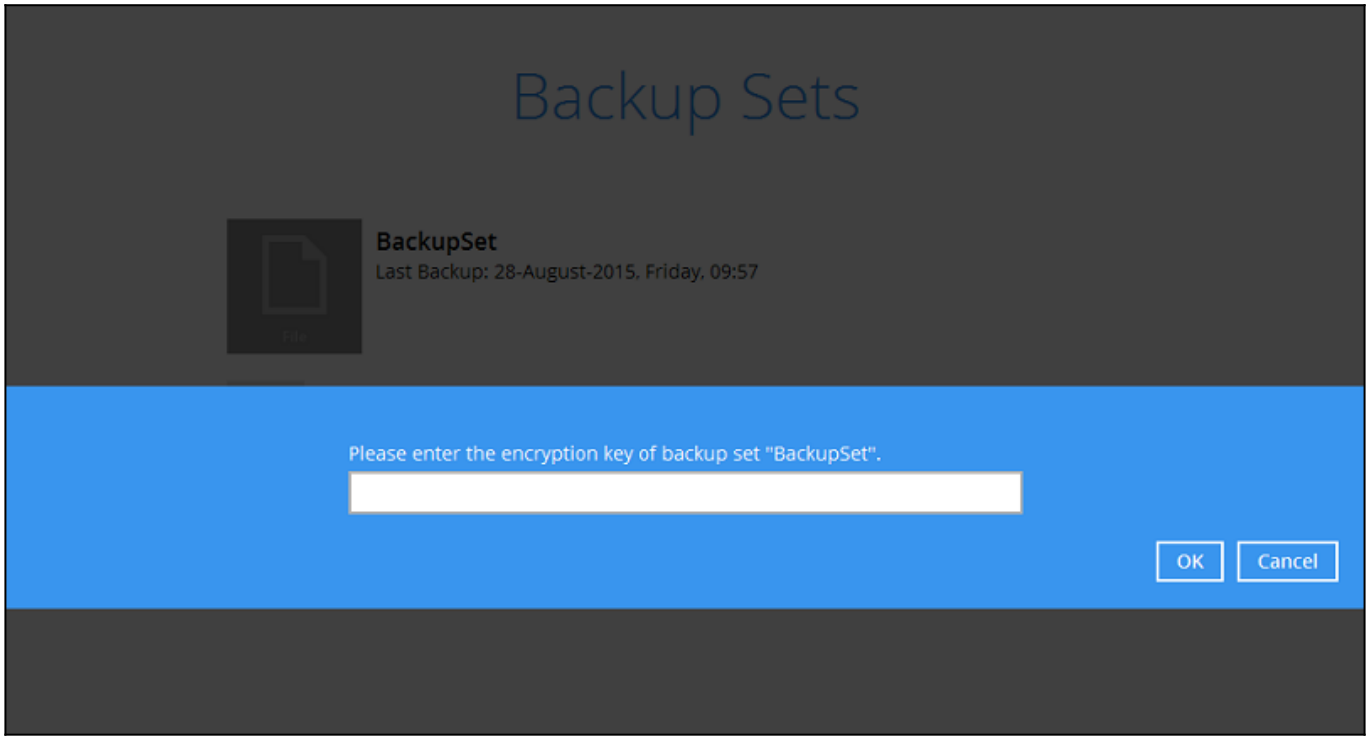
%UserHome%\%username%\%backupset_id%\settings\EncryptionKeys-%YYYY-MM-DD%.json.rgz

Contact email address of the user account will also be saved within this file.

Important:
Note that this file cannot be decrypted by the AhsayCBS administrator.

You must engage Ahsay's Professional Encryption Recovery Service to decrypt this file for retrieving the encryption key of a backup set. The encryption key will be sent directly to the end user's contact email address.

5. I am prompted to enter the encryption key of my backup sets, why is that?



Answer) The client application will prompt for the encryption key of all existing backup sets when the user, if it cannot detect the present of the settings.sys file (within the operating system profile (e.g. ~/.obm/config/settings.sys).

For example:

- Login to the client application on multiple computers with the same backup account.

  You have login to AhsayOBM with backup account 'username' on Computer A, then when you login to AhsayOBM with the same account on Computer B, when you access the Backup Sets tile, you will be prompted to enter the encryption key for all existing backup sets.

- Login to the client application with multiple backup accounts.

  You have login to AhsayOBM with backup account 'username' on Computer A, then when you login to AhsayOBM with backup account 'username2' on Computer A, you will be prompted to enter the encryption key for all existing backup sets.

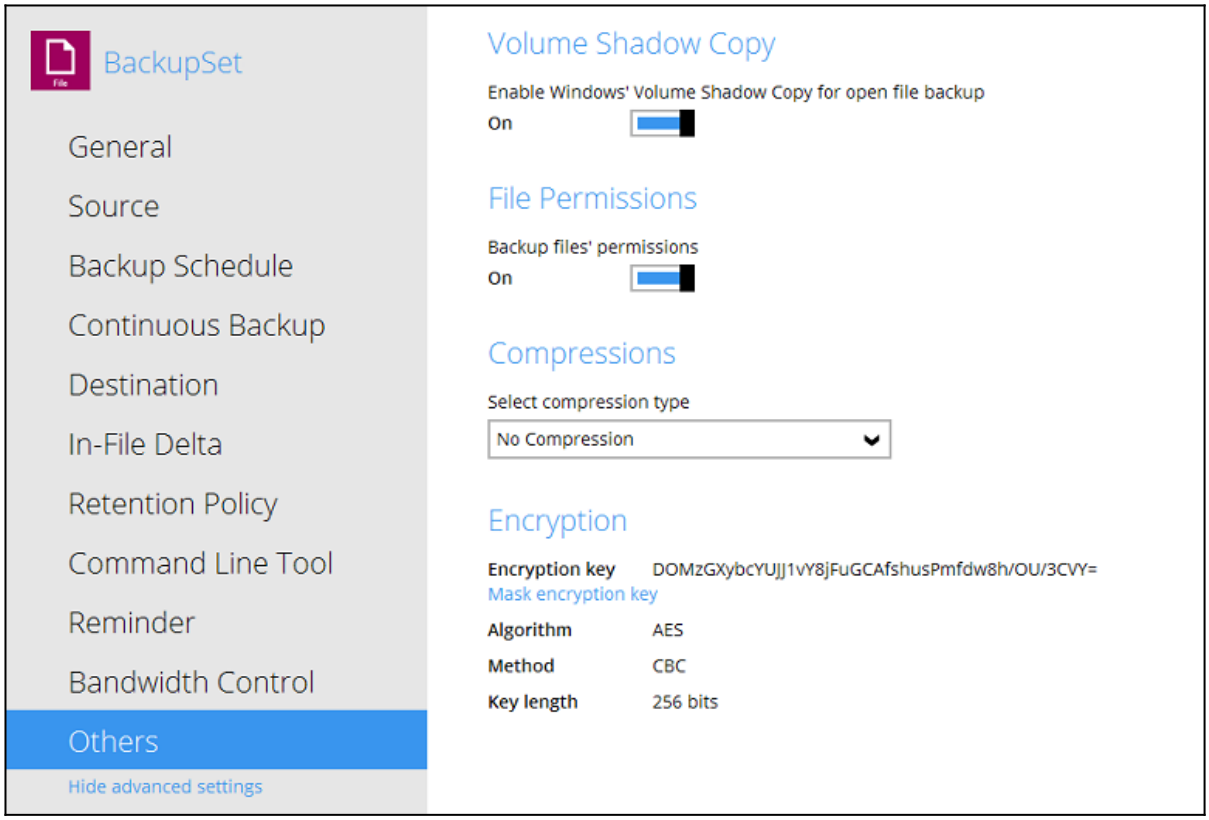
- The client application was completely uninstalled (including the user profile at ~/.obm/config/settings.sys).

The user must enter the correct encryption key at this point to manage or continue with the backup or restore operation (of that backup set) on this computer.

Best practices for managing your encryption key:

We would like to stress that it is **very very very important** to keep a record of your encrypting key at multiple locations.

1. Write down the encryption keys of all of your backup sets.
    - Login to the AhsayOBM / ACB user interface.
    - Click on the **Backup Sets** tile.
    - Select the corresponding backup set, then **Show advanced settings**.
    - Click on **Others**, select **Unmask encryption key** at the bottom of the menu.



    - Copy the encryption key at multiple locations.

2. Make copies of the backup account profiles on the client computer:

   ~/config/settings.sys

3. Enable the **Encryption Recovery** setting for your account.

   As a last step to protect yourself from losing the encryption key of your backup sets, enable the 'Encryption Recovery' setting of your backup account, to save the key to the backup server.

   Refer to Question 4 - Where is the encryption setting of a backup set saved at? for instruction.

Keywords

encryption, encrypt, decrypt, decryption, restore, restoration, recovery