# How to recover (decrypt) old v4/v5 encrypted VFSs

Es explained in our developers blog, starting from Syncplify Server! version 6 we had to change the way encrypted VFSs operate, because the old way (v4/v5) can no longer be considered 100% safe. This was not a lighthearted decision, but it had to be taken.

So what now? What does this entail for customers who were using these encrypted VFSs in old v4/v5, and now wish to upgrade to the latest v6 to take advantage of all the new features and its improved speed and stability?

Fear not. We have developed a little tool (mentioned in the blog article above) which can greatly help you with the transition.

Before we begin, it's important to understand one important detail: encrypted VFSs cannot be imported from a v4/v5 backup into your new v6, and as a result all user profiles using such encrypted VFSs also cannot be imported. So after upgrading to v6 your old encrypted VFSs (and the user profiles that used them) will be missing.

Here's what to do to recover access to the data stored in those old v4/v5 encrypted VFSs:

1. Download the DiskAES256Decrypt.zip archive from our website, and extract it into a directory of your choice on the machine/VM where the encrypted VFSs content is stored
2. Run it, and decrypt the content of each old v4/v5 encrypted VFS into fresh new empty folders (one per folder)
3. In your new Syncplify Server! v6, create a new encrypted VFS for each one of the old ones, all of these new VFSs **must** point to empty folders/directories
4. In your new Syncplify Server! v6, manually create the user profiles to use the newly created encrypted VFSs
5. Use an actual SFTP client software to log into those user profiles and re-upload the contents from the decrypted (in clear) directories: Syncplify Server! v6 will then automatically re-encrypt all of those files as they are being uploaded via the SFTP client

This is a one-time operation, once done you'll be good to go for the entire life of your Syncplify Server! v6 (and all future versions for the foreseeable future).

---