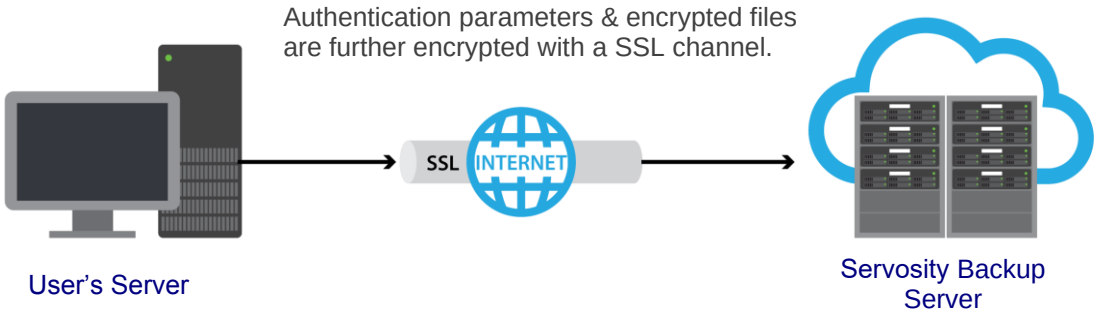
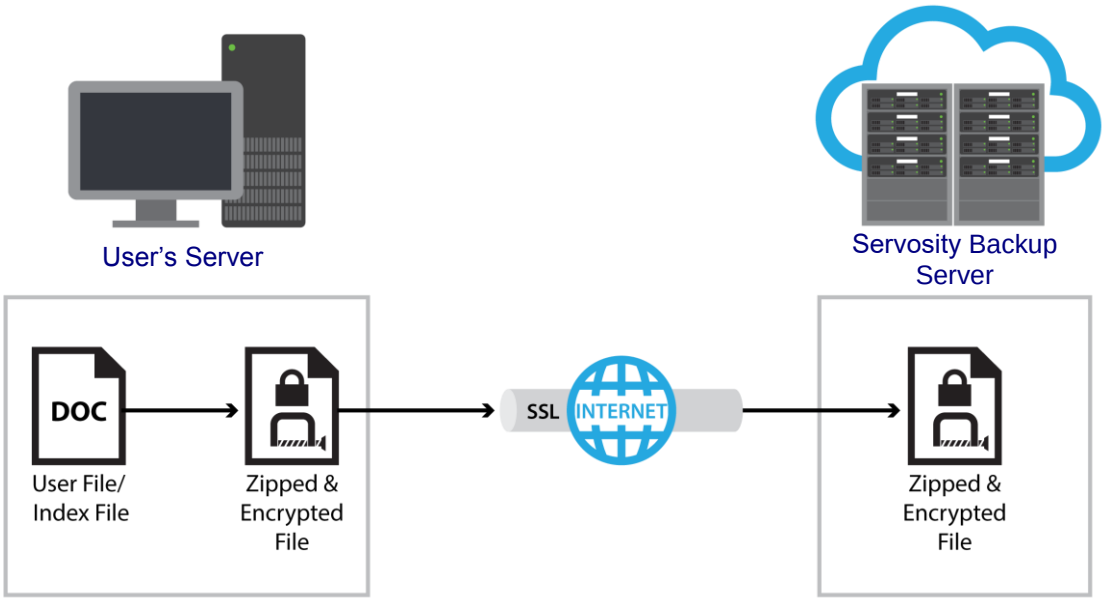
Data security of your backup

Secure 256-bit SSL communication

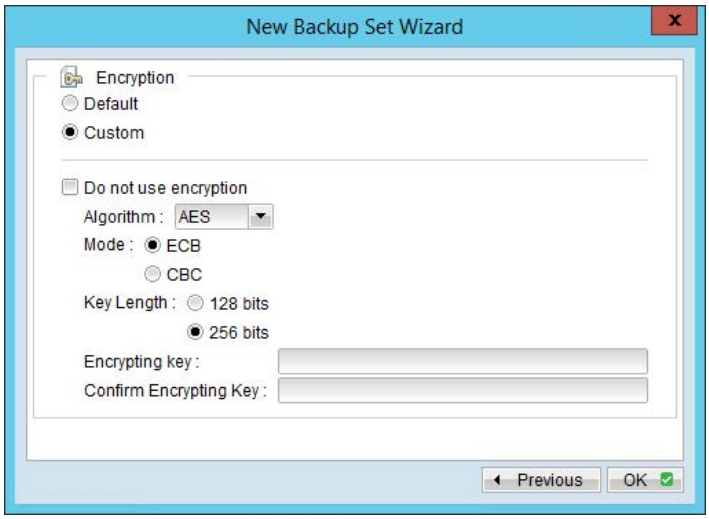


All communications between Servosity's backup servers and your servers are transported in a 256-bit SSL (Secure Socket Layer) channel. Although all your backup files travel through a public network (Internet), eavesdroppers are unable to read the data in flight.

Backup data is securely encrypted



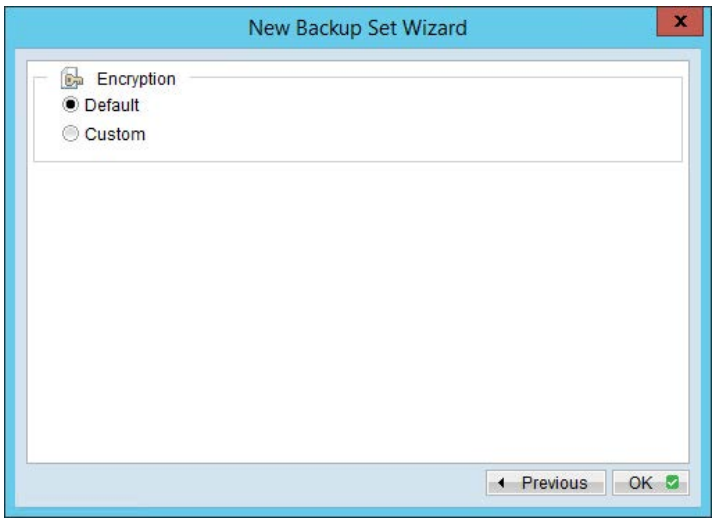
By default, the Encryption feature is enabled on your Servosity Professional / Servosity Standard client software. Data encryption happens on your local machine before your backup data is uploaded to Servosity's backup servers or local destination. Data being restored is also encrypted and goes through the unencrypting process on the local machine running the agent software.



Servosity provides three encryption options:

AES, Twofish or DESede, with AES providing the highest level of protection and DESede being the lowest. Different levels of encryption allow you to protect your backup sets at varying levels, as there is a tradeoff between backup/restore performance and data security. When encrypting data using an AES algorithm the backup speed may be affected verses DESede algorithm. Therefore, you may want to use AES for sensitive data such as client information, commercial secrets, and financial records. While for less sensitive data, you may consider using a lower encryption option such as Twofish or DESede.

In addition, two encryption methods are available: ECB (Electronic Cook Book) and CBC (Cypher Block Chaining), where CBC is the stronger method. Servosity also provides support for 128 bit and 256 bit key lengths.



When "Default" encryption type is selected, Servosity will use the agent password that you set when creating the backup account in our web portal. The default encryption algorithm that is used provides the highest level of protection in the industry (AES with a 256 bit key length and CBC mode). This is the only publicly available encryption algorithm approved by the US government for securing top secret information.

Encryption Key

The encryption key is used by Servosity to encrypt and protect your backup sets and data from unauthorized access, it is a password for your data. Once an encryption key is confirmed for a backup set, it cannot be removed or changed later. If the encryption key on a backup sets needs to be removed or changed then:

- A new backup set will need to be created with the new encryption key.
- The data will have to be backed up again from scratch.