Southwest Cyberport Online Backup Service

Data Security White Paper

Introduction

Southwest Cyberport uses the Ahsay Online backup software both as the backup server and for the customer's client program. The connection path from the customer's machine to our servers is always encrypted using 128-bit SSL communication.

Secure 128-bit SSL communication path

Backup data can be encrypted

In addition, the customer has the option of encrypting the data itself. This is the default when using the SWCP provided Ahsay client software and we recommend this option for all sensitive data.
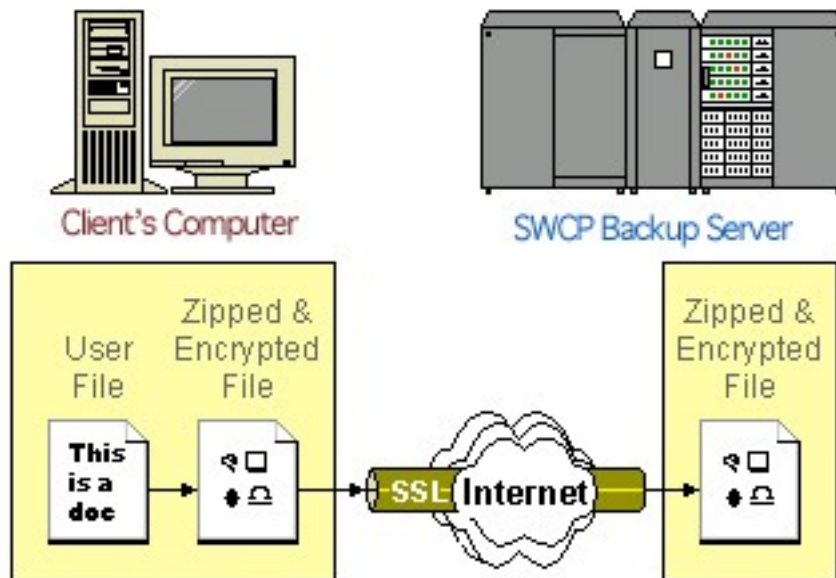
The Encryption key is well protected

The encrypting key used to encrypt your files resides only on your computer and is known only to you. It is never transmitted anywhere across the network. Thus, even the system administrators will not be able to decrypt and view the content of your files stored on the backup server without your permission. This unfortunately means if the encrypting key is lost, you will never be able to recover your backup files.

We recommend storing a copy of your encryption key off-site in a secure location, such as a bank safety-deposit boxes, a fireproof safe, with a trusted friend or relative, or held in escrow by your attorney or accountant.

Technical Details

The encrypting keys for the different backup sets are stored the config.sys file, which is encoded by a proprietary algorithm:

(Windows) C:\Documents and Settings\administrator\.obm\config\config.sys

(Linux/Mac OS X) ~/.obm/config/config.sys

If the client software cannot locate the config.sys (due to accidental deletion or data corruption), it will prompt the user to re-enter the encrypting key for the backup set and then store it in the local config.sys.

Note: To log onto the backup server for restoring files or just checking to make sure your files are correctly being backed up you will be given a password. This password is used as the default encryption key. Changing your login password DOES NOT change your encryption key. Be sure to capture the encryption key you're using. We can help you with a new login password, but **we cannot recover your encryption key.**

State of the Art Encryption Algorithm is Used

Currently, the algorithm that Ahsay uses to encrypt your files is 128-bit Twofish. It is a block cipher designed by Counterpane Labs. It was also one of the five Advanced Encryption Standard (AES) finalists chosen by National Institute of Standard and Technology (NIST). It is subjected to frequent public reviews and no known attack against this algorithm has been reported.

Ahsay is committed to providing state of the art encryption.

Access to your data can be restricted by IP address

You can also restrict access to your backup files by a set of IP addresses you define. If someone tries to access your data from an IP address not on your defined list, their access will be denied. This additional security ensures backup files are not open to all locations, even if your username and password are compromised.