



SECURSTORE
...because recovery matters

SECURITY

Confidentiality of Backup data

Data is transmitted and stored using highest security methods available eliminating the risk of the data getting into the wrong hands. The SecurStore backup service uses many defence mechanisms such as strong authentication, data encryption, password protection and client and system side logging. It is designed to keep backed up data confidential, while retaining the ability for legitimate users to perform data recovery when needed.

In order to achieve this, the DS-Client uses various protections, which will be described in the following sections.

SecurStore DS-Client and DS-System authentication

The DS-Client/DS-System authentication protocol is designed to ensure that no-one can impersonate a DS-Client account, connect to the DS-System and gain access to confidential data. In order to do this, the DS-System uses a DS-Client authentication mechanism:

- A DS-Client is accepted if and only if it is configured using correct DS-Client and account numbers. These values are unique and are generated when a DS-Client account is created.
- A DS-Client is accepted if and only if it has valid encryption keys (these keys are set and locked at the first DS-Client activity)
- A DS-Client is accepted if and only if it has a valid hardware hash (the hash is set and locked during the first DS-Client activity and can be reset by the Service Provider only). This means that even when knowing the DS-Client number, account number and encryption keys, a DS-Client cannot be impersonated by a computer with different hardware.
- A DS-Client is accepted if and only if the IP address of the DS-Client is inside the configured range, range which is set at the DS-Client creation time. The DS-System will reject DS-Client accounts that connect using invalid IP addresses, even if they have valid connection credentials.

Data encryption

All backup data transmitted between the DS-Client and DSSystem is encrypted using strong encryption (AES 128, AES 192 or AES 256). This means that even by gaining access to the data stream, the data will be in processed (delta, common file elimination), compressed (zlib or lzop) and encrypted (strong encryption) format. All encryption/decryption is done at the DS-Client side only. This avoids the following potential attacks:

- Monitoring data transmitted between the DS-Client and DSSystem would intercept only encrypted blocks. Access to confidential file content is not possible.
- Even with full access to the DS-System storage, attackers would not be able to read the contents of the files. The data is always stored encrypted and the DS-System does not store the DS-Client encryption keys (it uses a one-way hash to validate encryption keys).

Stored password encryption

The DS-Client stores access passwords to the source machines in encrypted format (AES 128) in its database. The DS-Client encryption keys are stored in encrypted format (AES 128) in the registry. This has the following effect:

- In case the DS-Client machine is compromised (a hacker gains full access to this machine), the passwords that the DS-Client uses to access the remote machines are not compromised.
- In case the DS-Client machine is compromised (a hacker gains full access to this machine), the DS-Client encryption keys are not compromised.

UK Office HQ

20 Garrick Street, London WC2E 9BT

Tel: +44 (0)20 7331 4304 email: info@securstore.com

www.securstore.com