Encryption Within TSM

Encryption Within TSM

On this page:

Data in Motion
Data at Rest

Data in Motion

Encrypting your data when your machine is sending it over the network to the TSM server:

- You must be using a TSM client that is version 8.1.2 or later (or 7.1.8 or later if you are using a v7 client)
- add **SSL yes** to your dsm.sys file (dsm.opt on Windows)
- restart the tsm service

Warning: The data is only encrypted when it is in transit to the TSM server, once there is is stored unencrypted. See below for encrypting your data while it is stored on the TSM server.

Data at Rest

By default, your data is not encrypted when it is stored within TSM. However, when you use the TSM encryption function, you can encrypt the data and ensure that your information is secure and protected, if the backup media (tapes and disks) were to fall into the wrong hands.

To protect your data – especially sensitive data such as documents containing social security numbers, payroll data, and health records – you can encrypt your data using the encryption function within TSM (Tivoli Storage Manager).

You must add two lines (and may optionally add a third) to your dsm.sys file (dsm.opt on Windows)

- Add one of **ENCRYPTKEY GENERATE** or **ENCRYPTKEY SAVE** or **ENCRYPTKEY PROMPT** If you use GENERATE, the key will be stored on the TSM server. For either of the other two options you are responsible for keeping a safe backup copy of the key. (see https://www.ibm.com/docs/en/storage-protect/8.1.21?topic=reference-encryptkey#r_opt_encryptkey for details)
- Add **INCLUDE.ENCRYPT /.../*** to encrypt all files (you may also give an alternate specification, if only some files need to be encrypted. (see https://www.ibm.com/docs/en/storage-protect/8.1.21?topic=reference-include-options#r_opt_include for details)
- The default encryption type is AES128. Add **ENCRYPTIONTYPE AES256** if you want to use AES256 encryption (see https://www.ibm.com/docs/en/storage-protect/8.1.21?topic=reference-encryptiontype#r_opt_encryptiontype for details)

If you choose the SAVE or PROMPT setting for ENCRYPTKEY, you should store the password somewhere safe, such as Lastpass (http://kb.mit.edu/confluence/display/istcontrib/LastPass+Landing+Page)

Warning: If you lose or forget the encryption key password, your data cannot be restored or retrieved, and IS&T cannot recover this password for you. If you are using the ENCRYPTKEY SAVE option, remember that the saved copy may be lost in the case of disk failure, ransomware attack, fire, or other disaster.

Warning: Setting this option will not encrypt existing backups, only newly backed up files. If you want existing files to be encrypted, they must be backed up again. Depending on the amount of data involved, this may take a long time

Consider the use of encryption carefully, especially for files that are being archived for a long period of time.

If you have questions about encryption within TSM, send email to tsm-systems@mit.edu.

Also see Policy on the Use of Information Technology.