Encryption Within TSM

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

How to Encrypt your data as stored on the TSM server

Encrypt and Back Up

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).

By default, your data is not encrypted when it is backed up over the network. However, when you use the TSM encryption function, you can encrypt the data and ensure that your information is secure and protected.

Warning: The encryption process takes place on the backup server and not on the client. See above for encrypting your data when it is in transit to the TSM server.

Encryption Key

When you turn on encryption within TSM, you are asked to enter an encryption key password. This encryption key password is used to encrypt your data before it is sent over the network and stored on the TSM backup server.

Consider the management of the encryption key password carefully. Without the encryption key password, you will not be able to restore data that was backed up and encrypted with this key.

Warning: If you lose or forget the encryption key password, your data cannot be restored or retrieved.

Keep a copy of this encryption key password some place other than on the computer that is being backed up. One option is to copy the key to removable media, e.g., a CD-R, or onto another computer. Whatever method you choose for storing this key, there should be a copy stored offsite for Disaster Recovery purposes.

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

The TSM client software supports encryption of data that is sent to the server during a backup or archive operation. TSM versions 5.3 and above use AES 128-bit encryption while earlier versions that supported encryption used DES 56-bit.

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

Also see Policy on the Use of Information Technology.