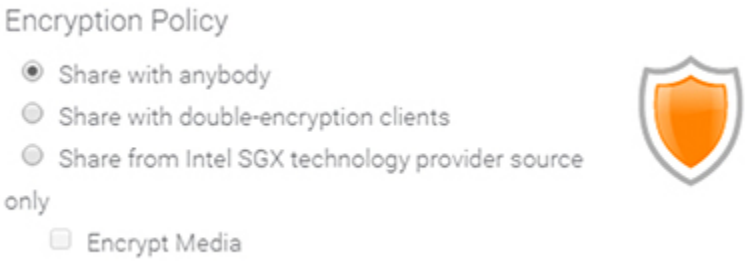
Encryption Options

Note: Your IT department may control the type of encryption access is supported in your company. You may need to contact your IT department in order to be able to set or connect to encrypted content repositories. If you have permission, you may see the following encryption options when you add a repository.

Note: FileFlex Enterprise uses encryption to protect all communications including the streaming of digital media. It is possible to enforce higher levels of encryption to provide additional protection against snooping, intercept, and malware, however using a higher level of encryption may prohibit some users from accessing your shared content depending on their device type and client application.



Encryption Options

Share with anybody - Normal Encryption - This is the default encryption setting as it is the most flexible. Anyone can receive a document shared with this setting on any FileFlex Enterprise client. This setting also allows for the streaming of digital media such as music, movies, and videos.

Share with double-encryption clients - Double Encryption - This adds a second layer of encryption of the data stream from sender to receiver with keys generated outside of system memory in the PKI server. This brings extra protection against snooping and intercept. The drawback however is that files shared with double-encryption cannot be accessed from the FileFlex Enterprise web client. The recipient must be using a downloaded FileFlex Enterprise desktop, iOS, or Android native client. Typically, the web client is used when sharing with recipients outside of your company. When sharing with this option, outside recipients will be forced to download and install the FileFlex Enterprise desktop or mobile apps in order to access this content. If the option is grayed out it is not supported by the device and is unavailable.

Share from Intel SGX technology provider source only - Intel SGX Protection - In addition to double encryption, this option also provides protection even if the sender or receiver's systems are compromised with malware as the encryption keys are generated within a protected enclave inside of the Intel CPU. The drawback however is that the recipient must be using a Windows PC that has a 7th generation Intel Core CPU or later. When sharing with this option, recipients using smartphones, tablets or Apple computers will not be able to access the file. If the option is grayed out it is unavailable as the device does not have or support Intel SGX technology.

Encrypt Media - If either the Double Encryption or Intel SGX Protection is enabled, then the higher level of encryption selected is disabled by default for media such as music, movies, and videos. This will allow for the streaming of digital media. That streaming is still protected with some level of encryption. If the Encrypt Media radio button is selected, then the higher level of encryption selected is applied to digital media as well, but that means that the digital media cannot be streamed. Digital media must be downloaded the local device before it can be accessed. In this case, also the sharer must enable the files to be downloadable when they set their options for each share.