M-FILES CORPORATION

PROTECTING FILE DATA AT REST WITH ENCRYPTION IN M-FILES

VERSION 1.2

NOVEMBER 10, 2016

CONTENTS

1. OVERVIEW

"Data at Rest" refers to inactive data which is stored physically in any digital form. For an M-Files system, this typically means the files and database data related to M-Files vaults.

The database file and file data on the M-Files Server computer should not be made directly accessible via network shares or such. Only the M-Files Server process should be able to access this data. Users should only access the data via M-Files clients and APIs.

To enhance the data security of the M-Files system, administrators can encrypt the data on the M-Files Server computer. This document discusses the encryption of file data at rest. The scope of this document is limited to file data encryption at rest. Encryption options for protecting database data at rest is explained in the Encryption of M-Files Vault Database with Transparent Data Encryption (TDE) document and the encryption options for data in transit are explained in the Protecting Data in Transit with Encryption in M-Files document.

This documentation applies to M-Files 2015 and later.

2. ENCRYPTION OF FILE DATA AT REST ON M-FILES SERVER

Administrators can enable file data encryption at rest via the *Advanced* tab of the *Document Vault Properties* window in M-Files Server Administrator:

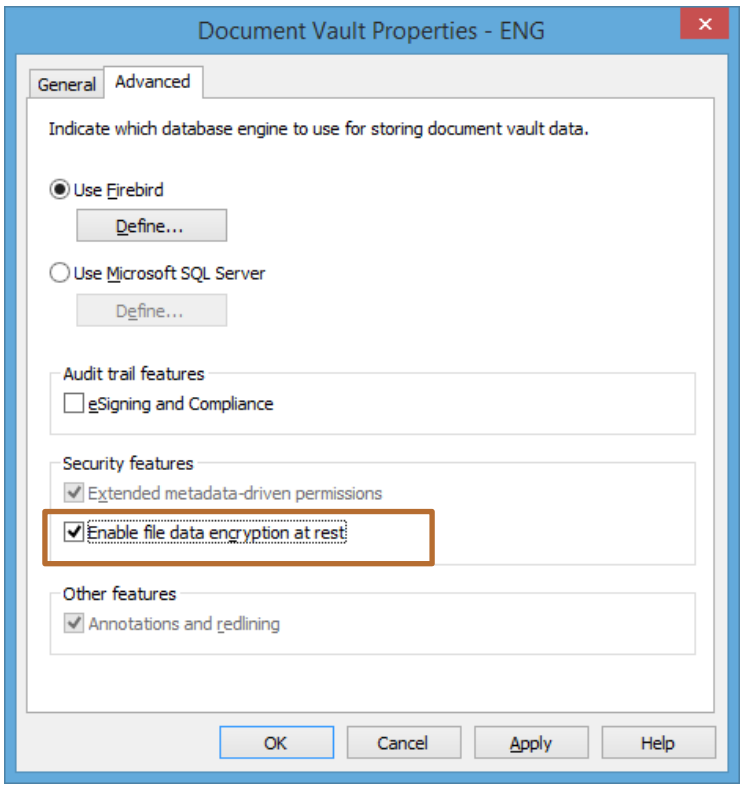

Image 1: Enable file data encryption at rest

After enabling this feature, all new file versions are encrypted with the AES-256 algorithm. The encryption algorithm is compliant with the FIPS 140-2 standard.

2.1. ENCRYPTING EXISTING FILES

If you enable the file data encryption at rest feature in a vault that already contains files, be aware that only the file versions that are uploaded to the server after you have enabled the feature are encrypted. If you want to encrypt also all existing files in the vault, run the *Update Encryption Status of Existing Files* feature in M-Files Admin.

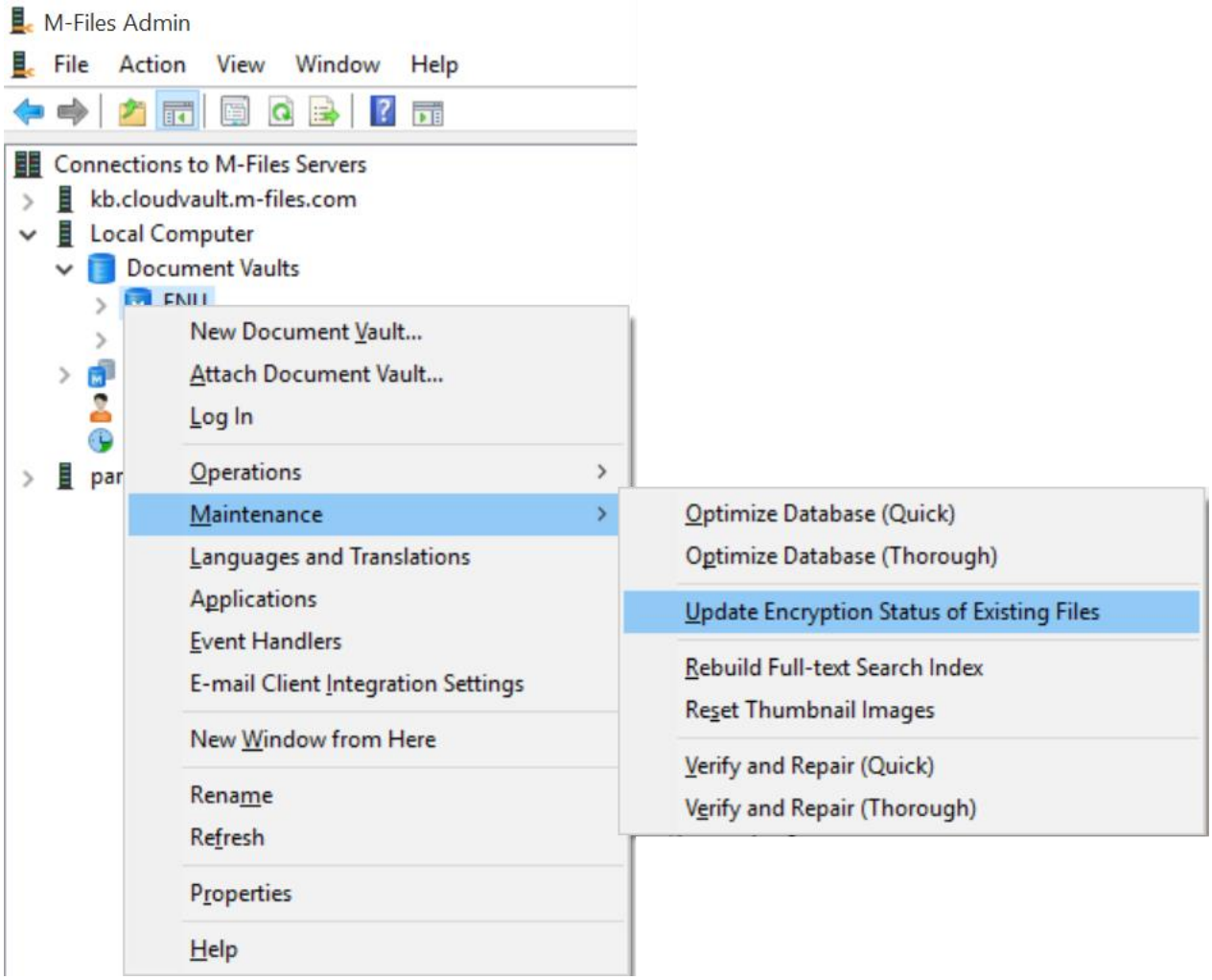

Image 2: Enable file data encryption at rest

2.2. CHANGING THE ENCRYPTION KEYS

The encryption keys are automatically generated and never stored anywhere in a plain text format. Administrators can change the encryption key by disabling and re-enabling the file data encryption feature. The new encryption key is used to encrypt the file versions that are uploaded to M-Files Server after changing the key. If you want to encrypt all the existing files using the new encryption key, you must run the *Update Encryption Status of Existing Files* feature in M-Files Admin (see above)

3. MORE DETAILS

The encryption process is totally transparent to users: the user saves a file to M-Files, and M-Files Server encrypts the file and saves it to the file storage.

To allow M-Files Server to index files and to ensure that the encryption of file data does not significantly affect the system performance, the files requested by the client are decrypted in M-Files Server and transferred to the client in a decrypted format. Hence, it is important that the network connections between M-Files clients and M-Files Server are encrypted. Refer to Protecting Data in Transit with Encryption in M-Files document for instructions.

3.1. THE LOCATION OF THE ENCRYPTED FILES

M-Files Server stores the encrypted files either in Azure Blob Storage, in a file-system folder, or in the vault database. This chapter explains the location of the encrypted files in different configurations.

3.1.1 M-FILES CLOUD VAULT

M-Files Cloud Vault Servers store the encrypted files in Azure BLOB Storage.

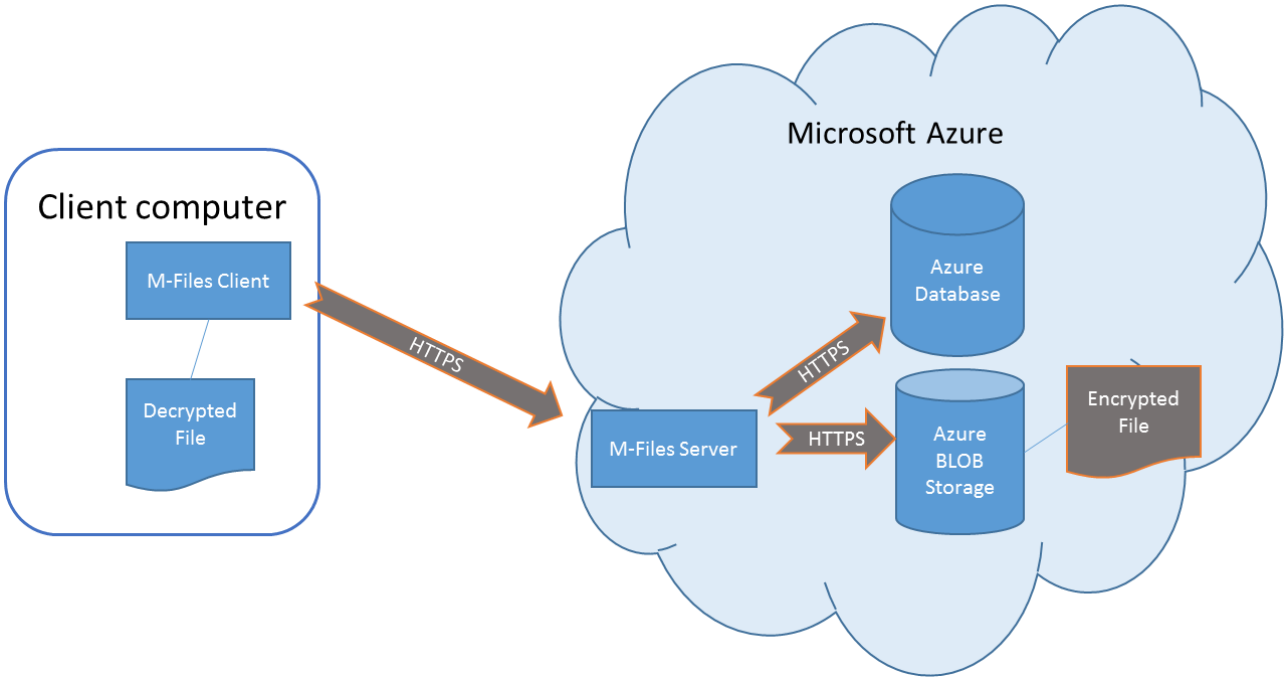

Image 3: File data encryption on M-Files Cloud Vault Server

3.1.2 M-FILES ON-PREMISES

The object files are stored in a file-system folder when using Firebird as the database engine. When using Microsoft SQL Server as the database engine, you can choose to store files in a file-system folder (image 3), or in the vault database (image 4):

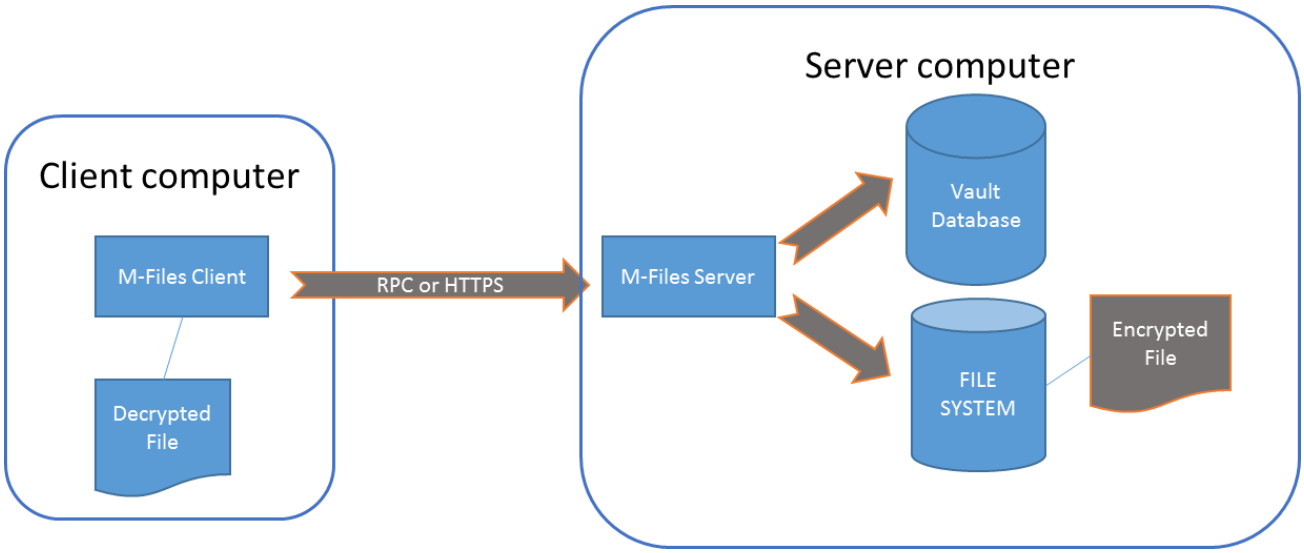

Image 4: File data encryption on M-Files on-premises Server, option 1

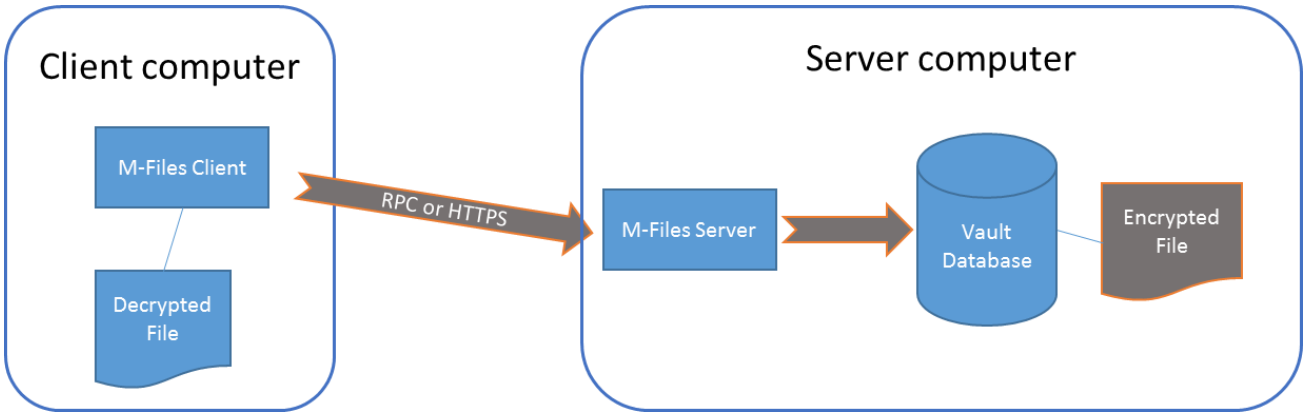

Image 5: File data encryption on M-Files on-premises Server, option 1

3.2. PROTECTING FILE DATA AT REST ON M-FILES CLIENTS

With the *Data at Rest* encryption, all file data of the vault is encrypted on M-Files Server. However, as different M-Files client software may cache data in unencrypted format, it is important to secure these devices as well. For (Windows) PC clients, it is recommended to encrypt the hard drives of the devices using Windows BitLocker or a similar tool. The encryption of the hard drive provides comprehensive protection for all files on the client device, not just for cached files from M-Files vault. Additionally, using strong passwords and a firewall for increased security on the client devices is recommended.

Use of mobile device management (MDM) tools for M-Files mobile clients, such as smartphones and tablets is recommended. These tools are capable of containing the M-Files app and also support wiping the stolen devices remotely.

3.3. PERFORMANCE IMPACT

Enabling the file data encryption at rest feature does not have noticeable impact on system performance. The files are encrypted and decrypted on the fly using a symmetric algorithm and this process is not CPU intensive. Enabling this feature can increase the file storage size by up to 0.4%.

4. VERSION HISTORY

Version	Date	Version comments
1.0	2015-02-16	The initial published version.
1.1	2016-02-22	Reference to the Encryption of M-Files Vault Database with Transparent Data Encryption (TDE) document added
1.2	2016-11-10	Chapter 3.3 added