M-FILES CORPORATION

WORKING COPY - PROTECTING DATA IN TRANSIT WITH ENCRYPTION IN M-FILES

VERSION 4

24 SEPTEMBER 2014

CONTENTS

1. OVERVIEW

"Data in transit" refers to information that flows over the network. For an M-Files system, this typically means the network communication between M-Files clients and M-Files Server. Three different client types need to be considered:

- M-Files desktop client (Windows)
- Web client (M-Files Web Access)
- Mobile apps of M-Files (iOS, Android, and Windows Phone)

If all communication between the clients and M-Files Server is within the organization's private network, unencrypted network communication between the client applications and M-Files Server may be acceptable. However, even in this case the organization should consider the risks of users within the organization potentially being able to gain unauthorized access to content by means of network sniffing, for example.

If users access data from outside the organization's private network, encrypting the network communication is usually mandatory. This is typically achieved either by using the HTTPS protocol or VPN technology.

The best practice for ensuring that data in transit does not cause a security risk is to encrypt the network communication between M-Files clients and M-Files Server in all cases, regardless of if the information flows over the public Internet or in the organization's internal network.

This document describes the recommended ways for protecting data in transit between M-Files clients and M-Files Server with encryption.

2. ENCRYPTION OF DATA IN TRANSIT IN M-FILES

There are multiple options for achieving encryption of network communication between M-Files clients and M-Files Server. Some of the options are independent of M-Files, such as using VPN technology for remote users, or IPSec for encrypting network communications in the local area network. Such techniques can be used with any version of M-Files and are out of the scope of this document.

This document describes the two main options for encrypting data in transit in M-Files 10.2 and later:

- HTTPS
- RPC Encryption (requires M-Files 10.2 or later)

2.1. HTTPS

The HTTPS protocol uses TLS/SSL to encrypt the data flow between client and server. In M-Files, HTTPS can be used as the communication protocol with all client types of M-Files:

- M-Files desktop client (Windows)
- Web client (M-Files Web Access)
- Mobile apps of M-Files (iOS, Android, and Windows Phone)

For M-Files web clients and mobile apps, HTTPS is the only available encrypted communication protocol.

HTTPS can be used with the desktop client of M-Files as well, if Microsoft Internet Information Services (IIS) and RPC over HTTP Proxy are set up as described in the article "Enabling RPC over HTTPS connections to M-Files Server" (ID 48424).

Using HTTPS as the secure communications protocol for all client types of M-Files is a good option especially if users access M-Files both within the internal company network and from the public Internet. In such case, you may want to use pre-shared keys and a separate proxy server for additional security as described in the article "Securing Access to M-Files Vaults with a Pre-Shared Key" (ID 143601).

2.2. RPC ENCRYPTION

M-Files Desktop and M-Files Server communicate by using the Remote Procedure Call (RPC) protocol. By default, the RPC communication uses TCP port 2266 and is not encrypted.

Prior to M-Files 10.2, the only option to encrypt the network communication between M-Files Desktop and M-Files Server was to use HTTPS (RPC over HTTP with TLS/SSL). M-Files 10.2 adds the option to use RPC encryption to secure the communication between M-Files Desktop and M-Files Server.

RPC encryption does not require IIS or any other additional components and is often the simplest way to achieve encryption of network communication between M-Files Desktop and M-Files Server in the organization's internal network.

For connections from outside the organization's internal network, HTTPS or VPN should still be used because RPC communication to TCP port 2266 would often be blocked by firewalls.

3. CONFIGURING M-FILES TO USE RPC ENCRYPTION

To enable RPC encryption in M-Files 10.2 and later, turn on the "Enforce encrypted connection" option when specifying connection properties.

The "Enforce encrypted connection" option is available for the TCP/IP protocol only. If the protocol is HTTPS, the connection is always encrypted at the HTTPS protocol level.

Enabling the "Enforce encrypted connection" option does not affect the port that is used (TCP port 2266 by default).

For RPC encryption to work, the user as well as the computer must be able to authenticate to the server computer. In practice, this requires that the client computer belongs to the Windows domain and that the user is a domain user.

3.1. M-FILES DESKTOP

To enable RPC encryption between M-Files Desktop and M-Files Server, use M-Files Desktop Settings to turn on the "Enforce encrypted connection" option:

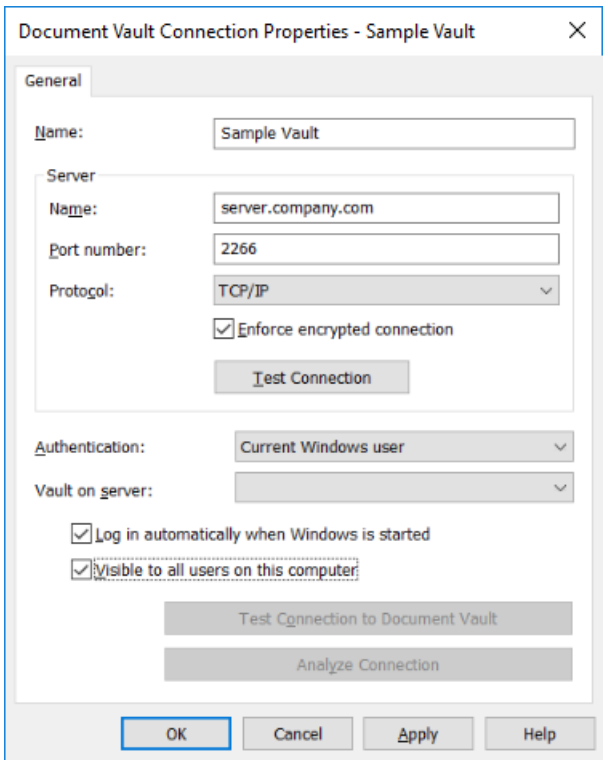

Figure 1: The "Enforce encrypted connection" option in M-Files Desktop Settings.

3.2. M-FILES ADMIN

To enable RPC encryption between M-Files Admin and M-Files Server, turn on the "Enforce encrypted connection" option when specifying connection properties in M-Files Admin:

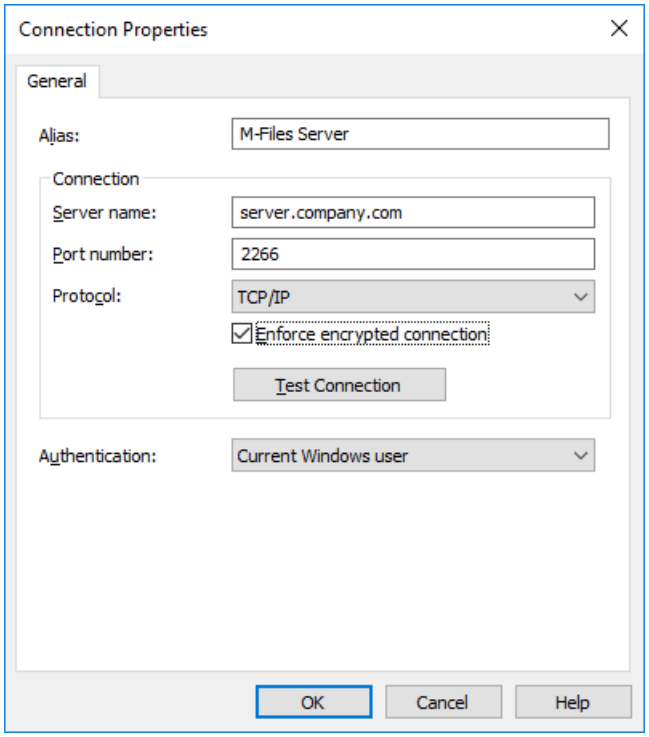

Figure 2: The "Enforce encrypted connection" option in M-Files Admin.

3.3. M-FILES API

To enable RPC encryption between an application that uses M-Files API and M-Files Server, specify True in the EncryptedConnection parameter when connecting to M-Files Server. The following methods of the MFilesServerApplication object support the EncryptedConnection parameter:

- ConnectEx
- ConnectAdministrativeEx

Applications that use the client interface of M-Files API rely on the connection settings of M-Files Desktop and automatically use an encrypted connection if specified in the vault connection properties in M-Files Desktop Settings.

3.4. M-FILES SERVER

In M-Files 10.2 and later, M-Files Server supports RPC encryption by default and no configuration steps are necessary to enable encrypted connections.

However, M-Files Server still accepts unencrypted connections by default. If you want to ensure that clients can only connect to M-Files Server with encryption enabled, you can configure M-Files Server to require RPC encryption by specifying the following registry setting:

Key name: HKEY_LOCAL_MACHINE\Software\Motive\M-Files\<version>\Server\MFServer
Value name: RequireRPCSecurity
Value type: REG_DWORD
Value data: 1 (default = 0)

After changing the above registry setting, the M-Files Server service needs to be restarted for the setting to take effect.

When the RequireRPCSecurity option is set to non-zero on the server, connections from clients will fail with the "Access denied" message if an encrypted connection cannot be established on the client side. Note that even if the "Enforce encrypted connection" option has been disabled in the Document Vault Connection Properties dialog, M-Files still attempts to establish an encrypted connection and only if establishing an encrypted connection is unsuccessful, will an unencrypted connection be used.

By default, M-Files Server will still allow connections via the RPC over HTTP protocol without RPC-level security if RPC over HTTP has been enabled on the server by specifying a non-zero value for the EnableRPCOverHTTP registry setting. This is typically desirable because those connections already have encryption at the HTTPS level and do not use RPC-level encryption by default. If you want M-Files Server to require RPC-level encryption for RPC over HTTP connections as well, you can set the registry setting RequireRPCSecurityAlsoWithRPCOverHTTP to a non-zero value.

After changing any of the above registry settings, the M-Files Server service needs to be restarted for the settings to take effect.

3.5. REPLICA SERVER

M-Files Server may act as a replica server for one or more cached replica vaults. In such a case, the M-Files Server service on the replica server establishes a connection to the M-Files Server service on the master server. The connection is configured in M-Files Admin under Cached Replica Vaults.

The configuration user interface for cached replica vaults in M-Files Admin does not support the "Enforce encrypted connection" option for TCP/IP connections. Thus, the connection between the cached replica server and the master M-Files server will not use RPC encryption by default.

In order to encrypt the connection between the cached replica server and the master M-Files server, you can configure the cached replica server to use RPC encryption in its connections to master M-Files servers by specifying the following registry setting:

Key name: HKEY_LOCAL_MACHINE\Software\Motive\M-Files\<version>\Server\MFServer
Value name: UseRPCEncryptionWithRemoteServers
Value type: REG_DWORD
Value data: 1 (default = 0)

After changing the above registry setting, the M-Files Server service needs to be restarted for the setting to take effect.

Another possibility for achieving an encrypted connection between a cached replica server and a master M-Files server is to use the HTTPS protocol. This requires that RPC over HTTP has been enabled on the master M-Files server as described in the article "Enabling RPC over HTTPS connections to M-Files Server" (ID 48424).