SETTING UP M-FILES TO USE GRPC

VERSION 4.1 | LAST UPDATED 10 JULY 2025

This document explains how you can set up M-Files to use the gRPC protocol for connections between your M-Files server and the M-Files clients. gRPC is a remote procedure call (RPC) implementation created by Google and implemented on top of HTTP/2. It is required for all vault connections in M-Files Cloud and is recommended for all new on-premises server implementations as a future-proof connection protocol.

Take note of these details before you start the setup:

- gRPC is supported in M-Files September '20 Update and later.
- To use a gRPC connection for M-Files Hubshare, a server certificate must be set up on the M-Files server (see section 2.2).

The necessary setup steps are given in this table:

CLIENT	SERVER TYPE	SET UP CLIENT	SET UP SERVER	ADDITIONAL INFORMATION
M-Files Desktop	M-Files Cloud	X		
	On-premises	X	X	
M-Files Admin	M-Files Cloud	X		
	On-premises	X	X	

M-Files Mobile	M-Files Cloud			If gRPC is set to use port 443 or 7766, the connection address format is:
				`https://<server name>`
				
				If another port is set, the connection address must contain the port number:
				`https://<server name>:<port>`

	On-premises		X	
M-Files Web	M-Files Cloud			
	On-premises		X	
Classic M-Files Web	M-Files Cloud	Only supports HTTP and HTTPS		Refer to Network Communication in the M-Files user guide.
	On-premises			

Contents

1. Setting Up the Clients 2

1.1 Creating a gRPC Connection 2

2. Setting Up the M-Files Server 3

2.1 Specifying the Port for gRPC Connections 3

2.2 Setting Up Server Certificates 4

2.2.1 Creating the PEM Certificate with the Entire Trust Chain 5

2.2.2 Testing the PEM Certificate 5

2.3 Creating Self-Signed Server Certificates (Optional) 5

3. Connecting Through Proxies 5

3.1 Using a Reverse Proxy 6

3.2 Connecting to Many Servers Through a Proxy Server 6

4. Logging 6

5. Change History 7

6. Reference Documents 8

Appendix A: Fine-Tuning Settings 9

1. Setting Up the Clients

This section explains how you can set up gRPC connections from M-Files Desktop and M-Files Admin to M-Files servers that support the protocol. For setting up your on-premises servers to accept gRPC connections, see section 2.

1.1 Creating a gRPC Connection

You can select gRPC as a connection protocol in the dialogs for adding a vault connection and creating a server connection in M-Files Admin. There are two variants of the protocol: *gRPC* and *Local gRPC*. For connections to an on-premises server on the same computer, we recommend that you use *Local gRPC* because it detects the server settings automatically. For connections to remote servers, edit the settings with the information given in Table 1. Contact your system administrator for the hostname and port number.

SETTING NAME	DESCRIPTION
Name	The server hostname.
Port number	The port for gRPC connections. M-Files cloud servers in M-Files Cloud always listen to port 443. The default port for on-premises servers is 7766, but you can specify a different port when you set up the server. The firewall on the client computer must allow outbound connections to the port you use.
Protocol	The protocol to be used. Select **gRPC**.
Enforce encrypted connection	In most cases, do not disable this option. Disable it only if the server is for some reason not configured to use secured connections. However, it is best practice and usually mandatory to use encrypted connection. Important information: • With on-premises servers that have been set to use a certificate, this setting must be enabled for the connection to be operational. • Secured connections require that the client machine trusts the certificate provided by the server. • Connections to M-Files Cloud are always secured even when this setting is disabled but we recommend that you enable it anyway.

Table 1: Descriptions for gRPC connection settings.

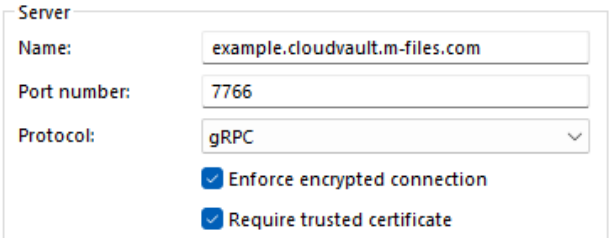


Image 1: Example connection settings in the *Add Document Vault Connection* dialog.

2. Setting Up the M-Files Server

This section tells you how to set an M-Files server to allow gRPC connections. You need to make these changes for on-premises servers only. M-Files cloud servers automatically allow gRPC connections.

2.1 Specifying the Port for gRPC Connections

The gRPC port is configured with a registry setting on the server machine. Changes made to the registry require you to restart the *M-Files Server* service with Windows Task Manager.

Key	`HKEY_LOCAL_MACHINE\Software\Motive\M-Files\<version>\Server\MFServer`

Value name	`gRPCEndpoint`
Value type	`REG_DWORD`
Description	The port at which the server listens for gRPC connections. Make sure that the server firewall allows inbound connections to the specified port.
Default value	7766

2.2 Setting Up Server Certificates

To secure the endpoint, M-Files Server requires a certificate that can be used to authenticate the server for the clients and to encrypt the connection. A certificate is not necessary for unsecured endpoints.

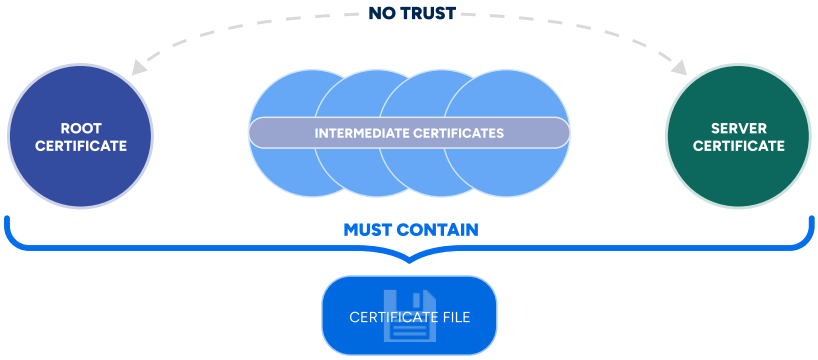
For instructions on how to set up or update a server certificate, see Managing Server Certificates in the M-Files user guide. For information about digital certificates, refer to information given by certificate authorities. For example, Verisign, IdenTrust, or DigiCert.

Please read this important information before you start:

- Use unsecured endpoints and connections **only** in environments otherwise secured against attackers. For example, with a corporate VPN.
- Only install a certificate to the M-Files application server with M-Files Admin if you prefer an encrypted, direct connection to the M-Files server.
    - **If you use a third-party proxy**, for example Traefik, **the certificate must only be installed to the proxy application**, which then terminates the encrypted connection. See section Connecting Through Proxies for more information.
- If you have issues with the certificate, you can use third-party services to analyze it.
    - For example, https://decoder.link/result. This can help you to detect problems, for example, with the certificate's chain of trust.

These features are required for the certificate:

- The certificate and private key files must be in PEM format (Base64 encoding).
    - Both EC and RSA certificates are supported.
        - EC private keys must be in the PKCS#8 PEM format (`-----BEGIN PRIVATE KEY----`).
        - RSA certificates are also supported in the PKCS#1 format (`-----BEGIN RSA PRIVATE KEY----`).
- The hostname of the server must either match the Common Name (CN) of the certificate or be included among its Subject Alternative Names (SAN).
- The certificate must be trusted by a trusted root certificate on the client computers.
    - M-Files Desktop requires the root certificate to be installed under the local machine certificate store.
    - M-Files Admin requires the root certificate to be installed under the current user certificate store.
    - If the server certificate is not trusted directly by the root certificate, the certificate file must contain all the certificates of the trust chain: The server certificate, all intermediate certificates, and the root certificate. See section 2.2.1 for instructions.



Important: Complete the initial configuration with M-Files Admin on the computer that runs the M-Files Server service. Remote connections to M-Files Server are not secured against interception or eavesdropping before you have set up the certificate.

2.2.1 Creating the PEM Certificate with the Entire Trust Chain

In the PEM format, the certificate contents can be written into the file one after another. The content must be in this order:

1. Your certificate (for example, cert.crt)
2. Intermediate certificates (for example, cert-ca.crt)
3. Root certificate

Example PEM file content:

```
-----BEGIN CERTIFICATE-----
<Your primary certificate content>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate content>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root certificate content>
-----END CERTIFICATE-----
```

2.2.2 Testing the PEM Certificate

To make sure that the certificate chain is correct, use OpenSSL to test it. Replace the parts marked with orange with details that apply to your own environment.

```
openssl s_client -connect yourserver:443 -CAfile path/to/filename.pem
```

```
openssl s_client -connect yourserver:7766 -CAfile path/to/filename.pem
```

2.3 Creating Self-Signed Server Certificates (Optional)

You can create your own certificate, for example, with OpenSSL (https://www.openssl.org).

3. Connecting Through Proxies

You can route connections from M-Files Desktop to M-Files Server through a proxy as well. We have tested a proxy connection with Traefik, but it can work with other tools as well. Before you set up the proxy, make sure that these prerequisites are:

- gRPC requires all connections to use HTTP/2, regardless of encryption.
  - Any proxy that supports HTTP/2 through Application-Layer Protocol Negotiation (ALPN) for TLS normally works with secured connections.
  - For unsecured connections, the proxy must support HTTP/2 without relying on the HTTP/1.1 upgrade.
- For secured connections, check the certificate requirements for both the client and the server.

    - The proxy must provide the full certificate chain, including intermediates, for the client. Conversely, it must trust the certificate chain provided by the server. It is also possible to secure only one part of the connection and leave the other unsecured.
- gRPC uses trailing metadata in the calls, and the servers expect a `TE: trailers` header in the messages. The proxies must not drop this header.

3.1 Using a Reverse Proxy

For instructions on how to set up a reverse proxy, refer to Using Reverse Proxy with M-Files.

3.2 Connecting to Many Servers Through a Proxy Server

Read these instructions if your environment matches this description:

- Two or more subdomains registered in public DNS and all subdomains point to the same public IP address.
- The subdomains are also registered in the internal DNS. All the subdomains point to the same proxy server to give users the same experience whether they are on the road or in the office.
- The router is configured to forward incoming traffic on port 443 to the proxy server.
- Two or more servers behind the firewall each run an instance of M-Files Server. All the servers are set to accept gRPC and M-Files Web traffic.

Do these steps:

- In IIS Manager, make sure that the web site has your SSL certificate and bindings to each of the subdomains with HTTPS in port 443.
- In the URL Rewrite module, for each subdomain, add a rule that specifies to which server traffic for that subdomain should be forwarded. In each rule, add a condition that states that HTTP_HOST must match subdomain.domain.com configured for that server.

  For example:

```
<rule name="ReverseProxyInboundRule1" enabled="true" stopProcessing="true">
  <match url="(.*)" />
  <conditions logicalGrouping="MatchAll" trackAllCaptures="false">
    <add input="{HTTP_HOST}" pattern="subdomain-a.domain.com" />
  </conditions>
  <action type="Rewrite" url="">server-a.domain.com:7767/{R:1}" logRewrittenUrl="false" />
  <serverVariables>
    <set name="HTTP_X_FORWARDED_HOST" value="{HTTP_HOST}" />
    <set name="HTTP_X_FORWARDED_PROTO" value="{MapProtocol:{HTTPS}}" />
  </serverVariables>
</rule>
```

4. Logging

For performance reasons gRPC logging is normally disabled when M-Files logging is in use. You can enable the `grpc` logging scope with the registry setting given here. When you make changes to this scope, you must restart the M-Files application for which the configuration was changed, usually the `MFServer` or `MFClient` service.

In most cases, the `Logging` key exists under the application key, but you must create the `grpc` key yourself.

M-Files Server:

Key	HKEY_LOCAL_MACHINE\Software\Motive\M-Files\<version>\Server\MFServer\Logging\grpc

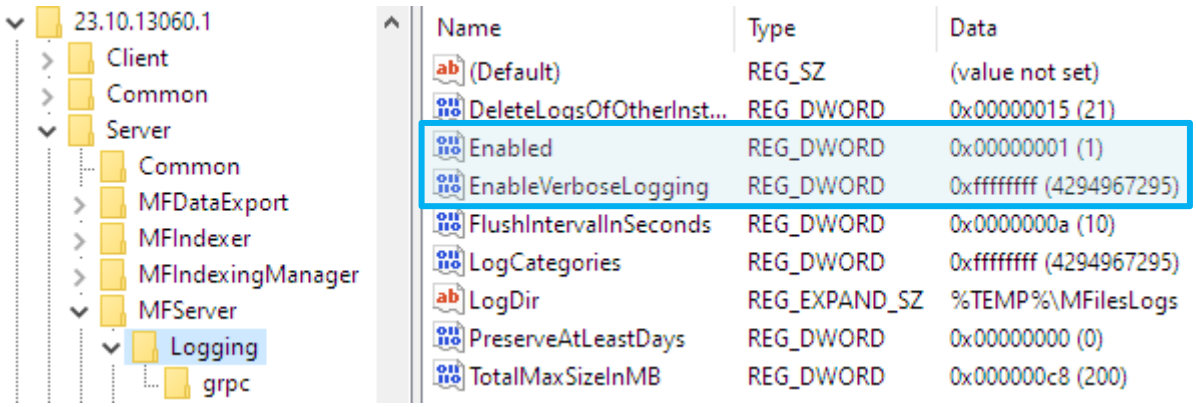
M-Files Desktop:

Key	HKEY_LOCAL_MACHINE\Software\Motive\M-Files\<version>\Client\MFClient\Logging\grpc

Value name	LogCategories	
Value type	REG_DWORD	
Description	The categories to log. Use the value `0xffffffff` to enable logging. You must restart the service for the changes to take effect. You can disable logging without a restart, but this leaves parts of gRPC logging in use.	
Default value	`0`	gRPC logging is not in use.

Make note that **for the gRPC logging to be used, you must set the `Enabled` value of the parent `Logging` key to `1`**. Normally, only ERROR level logs are recorded. To have gRPC record INFO level messages, set `EnableVerboseLogging` to have the value `11` or greater. To make gRPC record DEBUG level errors, set `EnableVerboseLogging` to have the value `101` or greater. After these value changes, it is not necessary to restart the M-Files applications.

For example:



The logs are normally recorded to `C:\Windows\Temp\MFilesLogs`.

> **Important**: When logging is no longer required, remember to set the `Enabled` and `EnableVerboseLogging` values back to `0`.

5. Change History

The table below describes the essential changes by document version.

VERSION	DATE	ESSENTIAL CHANGES
1.0	2019/01/09	Initial published version.
1.1	2019/02/06	Key and value name changes to registry settings.
1.2	2019/04/09	Changes to the registry setting descriptions.

1.3	2019/05/06	The default values of the `gRPCEndpoint` and `gRPCLocalEndpoint` settings were updated.
1.4	2019/08/06	The default values of the `gRPCMaxMessageLength` and `gRPCMaxLocalMessageLength` settings were updated.
1.5	2019/09/02	General updates.
1.6	2020/06/02	Added registry settings for logging (section 4).
2.0	2020/09/08	Updated configuration to match release configuration.
2.1	2020/10/15	Introduction updated.
2.2	2020/12/11	Clarified gRPC logging setup.
2.3	2021/10/27	Introduction updated.
2.4	2021/12/30	Reviewed the entire document and moved it to the new template. Updated section 2.2.
2.5	2022/06/16	Updated the introduction.
2.6	2023/01/19	Updated advanced options for message length limits.
2.7	2023/02/06	Updated the table in section 1.1.
2.8	2023/05/11	Updated the introduction.
2.9	2023/07/27	Updates to the introduction. Tip added to section 2.2.
3.0	2023/08/09	Clarified the importance of encrypted connection in section 1.
3.1	2023/08/18	Added an infographic to section 2.2.
3.2	2023/09/22	Updated the logging section.
3.3	2024/04/29	Updated sections about setting up server certificates and connecting through proxies.
3.4	2024/06/03	Added instructions on how to connect to many servers through a proxy.
3.5	2024/06/12	M-Files Cloud terminology updated.
3.6	2024/09/05	Updated the wording about the M-Files Hubshare requirement in the introduction.
3.7	2024/11/12	Added information about "Require server authentication" setting in table 1. Updated image 1.
3.8	2024/11/21	Updated information about "Require server authentication" setting in table 1.
3.9	2025/03/28	Clarified logging registry keys in section 4. Updated the default gRPC port in section 1.1.
4.0	2025/05/09	Updated image 1.
4.1	2025/07/10	Reverted default port for on-premises servers to 7766.

6. Reference Documents

You might want to see the following content for further information:

- Adding a Vault Connection (M-Files user guide)
- Adding a New Server Connection (M-Files user guide)
- Managing Server Certificates (M-Files user guide)

Appendix A: Fine-Tuning Settings

This section contains information on more advanced options that you do not have to use unless you have a specific reason to do so. The connection settings under the `Common` key apply to all M-Files software components installed on the computer. You need to restart the M-Files applications and services after you have added or modified the settings.

Server Settings

You can use these settings to affect the behavior of the server.

Key	`HKEY_LOCAL_MACHINE\Software\Motive\M-Files\<version>\Server\MFServer`

Value name	`gRPCLocalEndpoint`	
Value type	REG_DWORD	
Description	The port at which the server listens for local gRPC connections. If the port specified here is reserved, the server automatically identifies a free port and updates this value to be used by the local clients. Local clients should not assume the port to remain constant, instead clients attempting to use the local endpoint should read the current port through this registry value. If you modify this value, restart the *MFServer* service via Windows Task Manager.	
Default value	`7769`	The default port for local gRPC connections.

Value name	`gRPCMinPingIntervalMilliseconds`	
Value type	REG_DWORD	
Description	The smallest acceptable interval for keepalive pings from a single connection in milliseconds for incoming connections. More frequent pings cause the server to drop the connection.	
Default value	`5000`	5 seconds (half of the default client ping interval).

Value name	`gRPCMaxMetadataSize`	
Value type	REG_DWORD	
Description	The maximum metadata size in bytes for incoming connections. Larger metadata may be truncated or cause an error. The client and server should have the same metadata size limit.	
Default value	`524288`	512 kilobytes.

Value name	`gRPCMaxMessageLength`	
Value type	REG_DWORD	
Description	The maximum length of the request message in bytes for incoming connections. Messages longer than this cause an error during server calls.	
Default value	`50331648`	48 megabytes.

Value name	gRPCMaxResponseLength	
Value type	REG_DWORD	
Description	The maximum response length in bytes for incoming connections. Responses longer than this cause an error during server calls.	
Default value	2147483647	Maximum length allowed by gRPC.

Value name	gRPCMaxLocalMessageLength	
Value type	REG_DWORD	
Description	The maximum length of a request message in bytes for incoming local connections. Messages longer than this cause an error during server calls.	
Default value	2147483647	Maximum length allowed by gRPC.

Value name	gRPCMaxLocalResponseLength	
Value type	REG_DWORD	
Description	The maximum response length in bytes for incoming local connections. Responses longer than this cause an error during server calls.	
Default value	2147483647	Maximum length allowed by gRPC.

Common Settings

You can use these settings to affect the behavior of all M-Files software components installed on the computer.

Key	HKEY_LOCAL_MACHINE\Software\Motive\M-Files\<version>\Common\Grpc

Value name	ConnectTimeoutMilliseconds	
Value type	REG_DWORD	
Description	The timeout for establishing a connection to the server in milliseconds for outgoing connections. Lower values may detect faulty connections faster but may also fail to connect over a slow network. Calls via a successfully established connection have no timeout.	
Default value	5000	5 seconds.

Value name	KeepaliveIntervalMilliseconds	
Value type	REG_DWORD	
Description	The interval for keepalive pings sent during active server calls in milliseconds for outgoing connections. Lower values may detect lost connections more swiftly but use more bandwidth. Overly frequent pings may cause the server to drop the connection (see gRPCMinPingIntervalMilliseconds).	
Default value	10000	10 seconds (double the default smallest acceptable ping interval for the server).

Value name	KeepaliveTimeoutMilliseconds	
Value type	REG_DWORD	
Description	The timeout for keepalive pings for outgoing connections. Lower values may detect lost connections more swiftly but may lose a connection over a slow network.	
Default value	5000	5 seconds.

Value name	MaxMetadataSize	
Value type	REG_DWORD	
Description	The maximum metadata size in bytes for outgoing connections. Larger metadata may be truncated or lost. The client and server should have the same metadata size limit.	
Default value	524288	512 kilobytes.

Value name	MaxMessageLength	
Value type	REG_DWORD	
Description	The maximum length of a request message in bytes for outgoing connections. Messages longer than this cause an error during server calls.	
Default value	50331648	48 megabytes.

Value name	MaxResponseLength	
Value type	REG_DWORD	
Description	The maximum response length in bytes for outgoing connections. Responses longer than this cause an error during server calls.	
Default value	2147483647	Maximum length allowed by gRPC.

Value name	MaxLocalMessageLength	
Value type	REG_DWORD	
Description	The maximum length of a request message in bytes for outgoing local connections. Messages longer than this cause an error during server calls.	
Default value	2147483647	Maximum length allowed by gRPC.

Value name	MaxLocalResponseLength	
Value type	REG_DWORD	
Description	The maximum response length in bytes for outgoing local connections. Responses longer than this cause an error during server calls.	
Default value	2147483647	Maximum length allowed by gRPC.