M-FILES CORPORATION

# M-FILES SYSTEM ARCHITECTURE AND TECHNICAL HANDBOOK

LAST UPDATED 9 JUNE 2025

VERSION 2.1

# Contents

# 1. Introduction

This document gives you a technical overview of M-Files and collects feature-specific documents under an easily accessible umbrella. Thus, the document has many links to instructions and guides that explain specific parts of M-Files in more detail. Some links are accessible by M-Files partners only. If necessary, you can ask your M-Files contact persons for these documents.

This document is for administrators and other technical people. For example, system specialists and resellers. The reader of this document is expected to be familiar with the concepts of Microsoft Windows and networking.

This document deals with self-managed environments. That is, environments that are outside M-Files Cloud. These environments can be on customer's on-premises servers or Windows virtual machines on a hosting provider or a cloud platform, such as Microsoft Azure, Amazon AWS, or Google Cloud. To learn more about M-Files Cloud, see section 2.

# 2. About M-Files Cloud

M-Files Cloud is a secure and scalable cloud-based deployment option for knowledge work automation. With M-Files Cloud, you can manage your documents and information without investing in local server infrastructure and maintenance.

M-Files Cloud uses industry-leading cloud services by Microsoft Azure that are designed for high availability, accessibility, reliability, and security. M-Files Cloud is recommended especially for customers with strict high-availability or security requirements. Setting up, operating, and managing this kind of environment is complex, which can lead to high costs with other deployment options.

The M-Files Cloud architecture and other cloud service details are available in M-Files Cloud - Service Description in the M-Files Support Portal. You can find M-Files cloud requirements in the M-Files user guide.

> **Note:** M-Files Cloud is different from solutions where the customer deploys M-Files Server to a virtual Windows server on a cloud platform, such as Microsoft Azure or Amazon AWS. These cloud deployments are self-managed in the same way as M-Files on-premises deployments. M-Files Cloud is an enterprise-grade infrastructure that is provided by M-Files Corporation as a SaaS service.

# 3. M-Files Server Architecture (Self-Managed Environments)

The key component in the M-Files server architecture is M-Files Server. M-Files Server can host one or more M-Files vaults that are centralized storage locations for documents and other M-Files objects.

M-Files Server operates as a Windows service. By default, the M-Files Server service uses the identity of the local system account. It is important to take this into consideration when you plan the security settings of the folders or other resources that M-Files Server accesses. The local system account must have the necessary access rights on the M-Files Server computer. To access a resource that is located on the network, you must give the access rights to the computer that hosts the M-Files Server service.

Figure 1 illustrates the main components of the M-Files system.

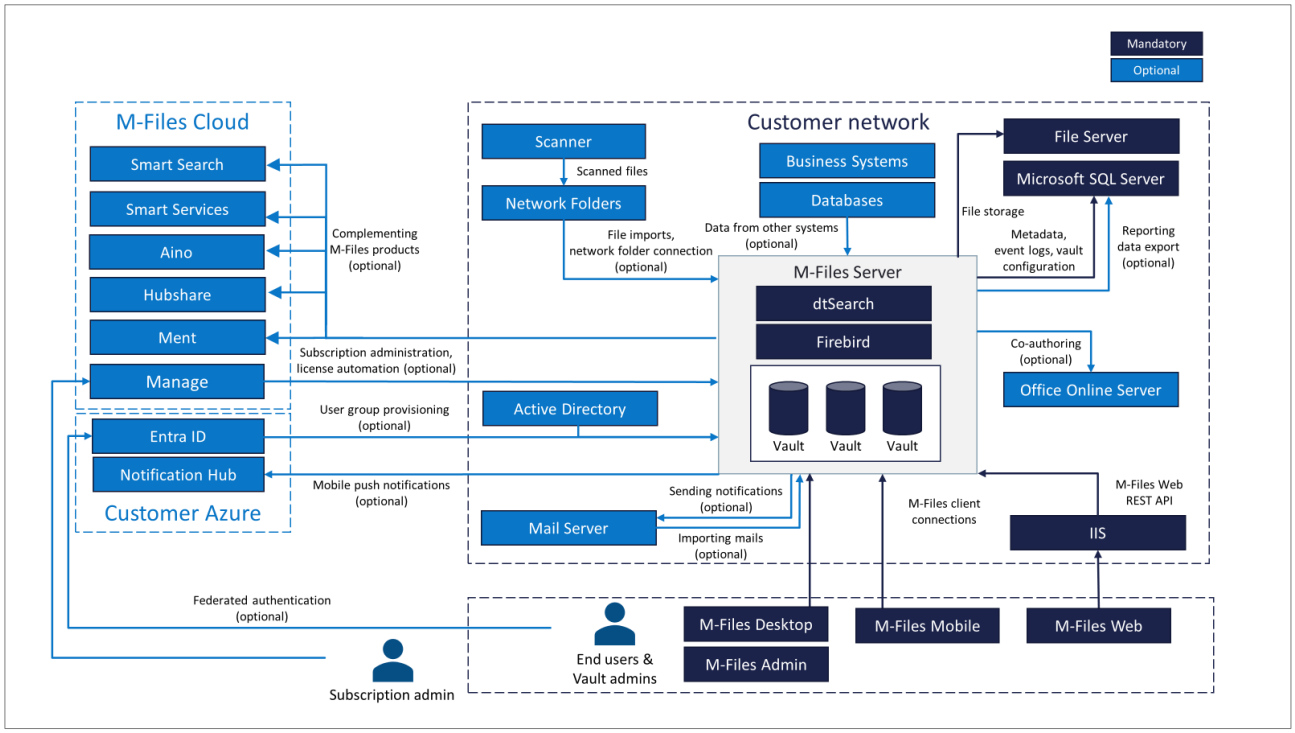


**Figure 1:** M-Files system architecture (self-managed environments).

## 3.1 System Requirements

Refer to System Requirements and Technical Details in the M-Files user guide for hardware and software requirements and guidelines.

## 3.2 Database

M-Files can use Firebird or Microsoft SQL Server as a database engine. You can select the database engine for each vault separately.

### 3.2.1 Firebird

M-Files Server uses Firebird as the default database engine. If the vault contains several hundreds of thousands of objects, it is recommended to use Microsoft SQL Server instead.

The Firebird database engine is installed during M-Files Server setup. If M-Files Server is uninstalled, the database engine will also be removed from the system.

Since the database engine is closely integrated with M-Files Server, it does not interfere with other applications. Other applications cannot see or use this instance of the database. However, they can install their own instances of the Firebird database engine. Thus, there can be several Firebird database engines on the same computer at the same time.

### 3.2.2 Microsoft SQL Server

Instead of Firebird, you can use Microsoft SQL Server as the database engine. It is recommended that SQL Server is used if the vault contains several hundreds of thousands of objects. With large vaults, SQL Server provides better efficiency than Firebird. However, with SQL Server, the administrator must be familiar with SQL Server management.

There are two ways to configure a vault to use SQL Server:

- All vault data except object files are stored into a single SQL database in SQL Server. Object files are stored on a file server. This is the **recommended setup**.
- All vault data is stored into a single SQL database in SQL Server.

The Microsoft SQL database engine can run on the same server as the M-Files Server, or it can be installed on another server. The M-Files Server software uses the OLE DB protocol to communicate with the SQL database engine.

The uninstallation of M-Files Server software does not have an effect on the database engine and vice versa.

## 3.3 File Server

M-Files Server can store the vault data files on local hard drives or on a separate file server. In Microsoft Azure environments, it is also possible to store files in Blob Storage, which has some benefits over file server.

Vault file data can also be stored in the Microsoft SQL Server database, but, for performance reasons, this is not recommended in production vaults. However, secondary vault data, such as search indices and logs, are always stored on a local disk, file server, or network share.

## 3.4 Search Engines

M-Files Server uses **dtSearch** as the default search engine. Instead of dtSearch, vaults can be set to use the cloud-based Smart Search search engine. It is recommended to switch from dtSearch to Smart Search when the number of objects in the vault exceeds 1 million. **M-Files Smart Search** uses memory-based search technology that gives an instant search experience and supports larger repositories than dtSearch. With Smart Search, the search engine and the search index always operate in the Microsoft Azure cloud.

In environments where communication with external cloud services is not allowed, large vaults can be set to use **Micro Focus IDOL** instead. However, it is recommended to use IDOL only if Smart Search cannot be used. This is because IDOL makes the environment more complex and harder to maintain.

When the vault uses M-Files Smart Search or IDOL as the search engine, it is possible to enable faceted search in the vault. Faceted search gives a user-friendly way to refine searches in M-Files.

## 3.5 M-Files Clients

M-Files has three clients: M-Files Desktop, Web, and Mobile. Additionally, there is the M-Files Admin client that is used to configure and manage M-Files servers and vaults. To connect to M-Files server with M-Files Desktop, refer to Adding a Vault Connection in the M-Files user guide. To enable M-Files Web and Mobile connections, refer to Setting Up Web and Mobile Access to M-Files.

M-Files Server can accept both encrypted and unencrypted calls. If M-Files clients connect to the server within the company network or with VPN, it is recommended to use unencrypted connections. If clients connect to the server from a public network, use encrypted connections instead.

M-Files Server supports client communication with several protocols. gRPC is recommended for all new implementations as a future-proof connection protocol. M-Files Web and Mobile use gRPC automatically if it is enabled on the M-Files server. Unencrypted gRPC traffic is transferred over HTTP/2. If the traffic is encrypted, it is encapsulated to HTTPS, which must be allowed in the firewall rules.

For comprehensive configuration instructions, refer to Setting Up M-Files to Use gRPC and Protecting Data in Transit with Encryption in M-Files in M-Files Support Portal. If your organization's security policy does not allow direct gRPC connections to the M-Files server from outside the organization's network, refer to Using Reverse Proxy with M-Files.

## 3.6 Internet Information Services (IIS)

Internet Information Services (IIS) is used to set up M-Files Web, Mobile, and REST API. It is an optional component in the M-Files server implementation. The IIS components can be enabled on the M-Files application server or on a separate server machine in the domain or on the DMZ.

## 3.7 Office Online Server

M-Files supports co-authoring for Microsoft Office files. To enable co-authoring with Office for the web, the environment must have Office Online Server deployed. For more information, refer to Enabling Web Co-Authoring in the M-Files user guide.

Desktop co-authoring with Office desktop applications is only available on M-Files Cloud.

## 3.8 Complementing Products and Features

### 3.8.1 M-Files Hubshare

M-Files Hubshare is a portal in which you can share documents and work collaboratively. You can use it for internal and external collaboration with your employees and customers. For more information, refer to M-Files Hubshare user guide and admin guide.

### 3.8.2 M-Files Ment

With M-Files Ment, you can automate document creation in M-Files with easy-to-use document creation wizards.

### 3.8.3 M-Files Aino

M-Files Aino is an AI assistant. You can ask Aino about the contents of a vault or specific documents. M-Files Aino is separate from the search engines in section 3.4. For more information about M-Files Aino, refer to Using M-Files Aino in the M-Files user guide.

### 3.8.4 M-Files Intelligence Services

M-Files intelligence services include add-ons that you can use, for example, to automate the filling of metadata for new objects, or to extract relevant information from the contents of the vault and connected external repositories. For more information, refer to Intelligence Services in the M-Files user guide.

# 4. Identity Management

## 4.1 User Provisioning

You can create users manually in M-Files or import users from an identity provider.

You can import user groups by domain and by organizational unit from a local Active Directory. It is also possible to set up user synchronization from Microsoft Entra ID or Okta.

## 4.2 Authentication

M-Files supports three authentication mechanisms:

- Federated authentication with an identity provider that is compatible with OpenID Connect or OAuth 2.0.
  - Microsoft Entra ID is recommended.
- Windows authentication
- M-Files authentication

Federated authentication provides additional security options, such as multi-factor authentication (MFA) and password policies. It is recommended to use federated or Windows authentication because the security options of M-Files authentication are limited.

### 4.2.1 Anonymous authentication

Vaults that are used to publish information can be set to use anonymous authentication. When enabled, this lets you set the M-Files Web and M-Files Mobile users to have read-only access to the publishing vault without username and password. For more information, refer to Anonymous authentication in the M-Files user guide.

# 5. Logging

## 5.1 Vault Event Log

Vault events, such as logins and document operations, are recorded to the vault event log that is accessible with M-Files Admin. By default, M-Files keeps 10,000 latest events in the vault event log. If the full audit trail is necessary in your organization, Advanced Event Log features can be enabled in the vault. With advanced logging, all the events are kept without restrictions.

The log messages are stored in the vault database. They can be archived manually or automatically.

For a list of recorded event types, refer to Event Types.

## 5.2 Windows Event Log

Usually, M-Files reports error messages and notifications to users in the client user interface. If it is not possible to show an error message to the user (for example, in case no one has logged on to the M-Files server computer), an error is written to the Windows event log of M-Files server or client computers.

M-Files administrators must check the Windows event log on a regular basis for issues. It can be necessary to make changes to the system to resolve the issues. The best practice is to configure event logs to notify administrators by email whenever a new error is written to the log.

## 5.3 Troubleshooting and Debugging

Different M-Files features, components, and add-ons have additional logging capabilities for troubleshooting and debugging. These log messages can be recorded in the Windows event log, written to log files in the file system, or shown on dashboards in M-Files Admin.

Refer to the product documentation and support articles for each component in the M-Files Support Portal for more information on possible additional logging.

# 6. Management and Maintenance

## 6.1 M-Files Manage

M-Files Manage is a web application for centralized user and license management of your M-Files subscription. With M-Files Manage, you can see information about your subscription, users, vaults, object and storage usage, and more. For more information, refer to M-Files Manage user guide.

M-Files Manage is designed for M-Files Cloud environments but it can also be used in on-premises environments. To start using M-Files Manage in an on-premises environment, refer to Joining Servers to M-Files Manage in M-Files Support Portal.

## 6.2 M-Files Automatic Updates

M-Files can automatically update its software. When automatic updates are enabled, the computers that have M-Files installed monitor M-Files Automatic Update Server hosted by M-Files Corporation for updates. New versions of M-Files become available for download through this service. It is possible to specify that client computers download the new version automatically and ask the user to install it. In this case, the user must have rights to install new software on their computer.

Many organizations prefer to install software updates centrally. In this case, it is a good practice to disable automatic updates.

TCP ports 443 and 80 are used to check and download new M-Files versions. These ports must be allowed as destination ports in the firewall rules.

## 6.3 Maintenance Operations

Refer to Vault Maintenance in the M-Files user guide for guidance on recommended maintenance operations.

## 6.4 Backups

Refer to M-Files Backup Policy in M-Files Support Portal for guidance on backups and related best practices.

# 7. Extending M-Files Capabilities

You can install vault applications or user interface extensions to vaults to extend the M-Files capabilities and integrate M-Files into other systems. M-Files Catalog contains applications developed by M-Files and M-Files Solution Partners. Additionally, anyone with relevant programming skills can create their own applications to extend the functionality of M-Files to better match their organization's business area and needs. For more information, refer to M-Files Developer Portal.

## 7.1 Application Programming Interfaces

M-Files has two Application Programming Interfaces (APIs) that you can use to create custom functionality or connect other systems into M-Files:

- M-Files COM/.NET API
- M-Files Web Service (REST API)

## 7.2 Vault Application Framework

With M-Files Vault Application Framework, you can create custom complex business logic or automation to extend the built-in configuration options. For more information, refer to Vault Application Framework.

## 7.3 UI Extensibility Framework

M-Files UI Extensibility Framework is an interface for building custom UI applications to change the behavior of the M-Files Desktop user interface. For example, you can create your own tabs besides the built-in Metadata and Preview tabs. For more information, refer to M-Files UI Extensibility Framework.

# 8. Integrations to Other Systems

One of the advantages of M-Files is that it can be integrated seamlessly with other systems. M-Files supports, for example, these integration methods:

- OLE DB or ODBC connections
- M-Files COM/.NET API
- M-Files Web Service (REST API)
- M-Files UI Extensibility Framework.
- M-Files Links

- Intelligent Metadata Layer

Refer to M-Files Integration Handbook for more information about the integration options and considerations.

## 8.1 External Databases

M-Files lets you connect vaults to external databases. The only requirement is that the external database can be accessed with OLE DB, ODBC, or Web Service interfaces. M-Files can both read data from and write data to external databases.

A common way to use database integration is to bring the most important business objects (for example, customers or vendors) to M-Files. After that, you can tag vault contents to them.

Connectors for reading customer data from the most popular CRM systems, such as Salesforce CRM and Microsoft Dynamics 365 CRM, are also available.

## 8.2 Existing Files and Folders

M-Files can import files from network folders with external file sources or provide access to the files in their current location with Network Folder Connector. In addition to Network Folder, M-Files Catalog has connectors to access files in popular systems, such as SharePoint Online. After the files have been imported to M-Files or a connector is set up, the original external location can be isolated from the users. Additionally, some connectors can automatically migrate content into M-Files based on predefined rules.

Access to external repositories with the M-Files user interface can help users get started with M-Files. This way, they can use M-Files to access the existing files in the familiar structure with existing access controls applied and, at the same time, benefit from the additional functionality that M-Files provides.

The organization benefits from importing or providing access to existing files in M-Files in many ways. For example, version history starts operating immediately and M-Files' excellent search capabilities are available.

## 8.3 Mail Servers

M-Files can use mail servers in two different ways:

- Sending notifications from M-Files Server to users (SMTP)
- Importing emails from server (POP3/IMAP4)

With notifications, users get emails about vault events. For example, when a new document is created or an existing one edited. M-Files sends email messages to the users who have subscribed to them. The email messages are delivered with the standard SMTP protocol.

M-Files can be set up to monitor selected email boxes. To do this, the IMAP or POP protocol is used. M-Files creates a new document from each new message that arrives to the monitored email box. This means that the email is saved as a document to the vault, and the metadata of the document contains email-specific information.

### 8.4 Scanners

M-Files helps organizations to digitalize and index paper documentation. M-Files is compatible with any desktop and network scanner.

When network scanners are configured to produce a scanned image file to a network folder, M-Files can be set to periodically monitor this folder and import the files as new documents to the vault. M-Files OCR can convert the scanned images to searchable PDFs, which makes the contents of the scanned documents searchable.

If your scanner devices support metadata, M-Files can use the metadata XML files to add their contents as properties to the document.

## 9. Reporting and Data Export

Vault metadata can be exported to an external SQL database. You can schedule the export jobs to run at a certain frequency. It is possible to use the exported data for reporting purposes by analytics tools, such as Microsoft Power BI, or for some integration scenarios to let another system read M-Files data. For more information, refer to Reporting and Data Export.

Vault users can export search results and contents of a view from M-Files Desktop to a CSV file. This, or just cleverly built M-Files views, might serve simple reporting purposes.

## 10. Replication

With the M-Files replication feature, it is possible to synchronize metadata structure or objects between M-Files vaults. You can set up replication between two self-managed vaults (either on the same or different servers), between a self-managed vault and a cloud vault, and between two cloud vaults. Metadata structure replication lets you set up a deployment pipeline from development vault to test or QA vault to production vault.

For more information, refer to Content Replication and Archiving.

## 11. Security and High Availability

Refer to Best Practices for Data Security and High Availability in M-Files for guidance on how to set up a secure, high-availability environment.

M-Files Cloud, which has high security and availability, is the best option for customers who have strict requirements in this area. See section 2.

# 12. Change History

The table describes the changes by document version.

| VERSION | ESSENTIAL CHANGES |
|---|---|
| 1.0 | Initial version. |
| 1.1 | Links updated in section 8. |
| 1.2 | SAML mentions removed. |
| 2.0 | Major rewrite, the whole document updated. |
| 2.1 | Removed a dead link from section 2. Added a link to the integration handbook and made other small improvements. |

# 13. Referenced Materials

Refer to these materials for additional information:

- Best Practices for Data Security and High Availability in M-Files
- Maintenance Guidelines for M-Files Administrators
- M-Files Catalog
- M-Files Customer Support Portal
- M-Files Developer Portal
- M-Files Hubshare User Guide
- M-Files Manage User Guide
- M-Files User Guide
- System Requirements and Technical Details
- Using Reverse Proxy with M-Files
- M-Files Integration Handbook