M-Files 2015.3
User Guide

Contents

1. Introduction to M-Files

Congratulations on your purchase of M-Files® Dynamic Content Management software!

M-Files® enterprise content management software helps you easily store, organize and access all kinds of documents and information. Our revolutionary approach organizes content based on what something is (and what it relates to) instead of where it's been stored. Eliminating the traditional folder-based method ensures that you have instant access to all of your content via search or dynamic views. It's simple, dynamic, and flexible. From managing a wide variety of content to ensuring regulatory compliance, M-Files has you covered.

Access your information anywhere: M-Files can be deployed on-premise, in the cloud, or a hybrid of both.

Thank you for choosing M-Files and welcome to a new chapter in productivity!

▶ Video: *M-Files Overview*

About this user guide

You can access this help documentation anytime M-Files is active by pressing the *F1* key on your keyboard. Opening the user guide via *F1* adds the advantage of directly accessing a topic that is related to what you are doing at the moment in M-Files.

You can also open the documentation via the M-Files icon on the Windows notification area, as well as via numerous help buttons in the M-Files user interface.

In addition, the user guide is available as a PDF version. You can download it by clicking the PDF icon in the upper right corner of the web help documentation.

This user guide contains a number of typographic and writing conventions as well as visual elements that will help you to better understand information and to perform tasks instructed in this guide. For a comprehensive list of these conventions, see *Conventions Used in This User Guide* on page 10.

Additional documentation

If you are a developer or an M-Files system administrator, you might be interested in our documentation for:

- *M-Files API*
- *M-Files Web Service*
- *M-Files UI Extensibility Framework*

For a full list of M-Files documentation, please visit *m-files.com*.

1.1. M-Files Components

Your M-Files software includes the following components:

- *M-Files Setup:* Use this to install M-Files.
- *M-Files Desktop:* The most commonly used component that displays content in various views and is tightly integrated into Windows.
- *M-Files Desktop Settings:* Use this component to connect your client computer to document vaults on M-Files Server, and to edit other local settings.
- *M-Files Server:* This component manages the centralized saving and sharing of content.
- *M-Files Admin:* A tool used by your company's information systems administrator for adjusting M-Files Server settings, managing the document vault, and modifying the vault structure.

- *Show Status:* With this component, you can monitor file transfer status. This is useful if you are using M-Files over a slow connection and need to view the transfer progress.
- *M-Files Web:* In addition to using the M-Files Desktop, you can access M-Files by using a web browser.
- *Automatic Updates:* Automatically keep your M-Files software up to date.

M-Files also includes an ActiveX/COM API as well as the M-Files Web Service API that allows programmatic access to M-Files through a REST like interface. The M-Files API and its documentation are included within the installation of the M-Files software, and the M-Files Web Service API is documented at: *www.m-files.com/mfws*.

1.2. M-Files Terminology

The following table describes daily M-Files terminology.

M-Files software	The M-Files document management software consists of the following components: *M-Files Desktop*, *M-Files Admin*, *M-Files Desktop Settings*, *Show Status* and *M-Files Server*. You can also use M-Files with a web browser or a mobile device.
File vs. document	An example of a file is a memo created using *Microsoft Word* and saved on the C:\ drive. The file becomes a document only after you have associated metadata with it. When you have implemented M-Files and start transferring existing files to M-Files, you add metadata to the files to make them documents. In addition to documents, an M-Files vault can also store other types of objects, such as customers, assignments, or project data.
Multi-file documents	A multi-file document is a special M-Files document type that can contain more than one file. The files share one set of metadata. Typical uses include linking of an electronic document with its signed and scanned counterpart, an email and all its attachments, or any such case where files need to be linked together and treated as one unit.
Temporary local file	For example, Microsoft Word creates temporary files during the work. These are so-called *temporary local files.* Some programs cannot remove these temporary files, and they remain as temporary local files in M-Files. As temporary local files have no associated metadata, they are not saved on the server. The temporary local files can be converted to documents, refer to *Convert to Document* on page 106, and removed, refer to *Clear Local Cache* on page 138.
Metadata	*Metadata* consists of information about the document's properties, such as the parties of a contract or the recipient of a letter. Metadata is used to, for example, search for and organize documents.
Document / object permissions	Each document can be assigned *permissions* to specify the access rights of a *user* or *user group.* The permissions can be either allowed or denied separately. One user can have *allowed* or *denied* permissions in two different ways: the permissions have been specified for that particular user, or the user belongs to a user group for which the permissions have been specified. If no permissions have been specified for a user, the user cannot view the document or access it in any way. If certain permissions have been allowed, the user can perform the procedures determined by these permissions.
Vault	A *vault* is a centralized storage location for documents and other objects. Its physical location is on the server running M-Files Server. Regardless of the physical location, all

	users see the document vault as a directory on their local computer's M-Files drive. This means that using a document vault is similar to using a local hard drive.
View	*Views* are locations in which the documents and other objects are listed based on the metadata they contain.
Virtual folder	The objects and documents in the views include virtual folders (property folders). Virtual folders enable sorting documents in the view into categories.
Traditional folder	You can create *traditional folders* in M-Files. These folders do not have the additional properties provided by views. Traditional folders are comparable to, for example, folders on your C:\ drive and can be used for importing files to M-Files. Traditional folders allow you to retain the original folder structure of the imported files.
Client	A *client* is the regular M-Files user's computer and the software installed on it. The regular user performs operations like creating documents and exploring the document vault.
Object type	By defining *object types*, you can create different types of objects. *Document* is one of such object types, one that every vault contains. In addition, the M-Files administrator can create other object types for the vault, such as *customer, contact*, and *project*. This way, you can use M-Files to, for example, store the company's customer and project databases.
Object	The term *object* refers to instances of various object types – that is, individual objects created using object types. For example, one contact person in the document vault is an object. Most functions are identical for documents and for other objects. This manual often represents operations as being performed on documents, but the same operations are available for, e.g., document sets and other objects. An individual document can therefore also be thought of as an object.
Document collection	*Document collections* are collections of individual documents in the document vault. Each collection member document has its own metadata. In addition, the document collection has a collective set of metadata independently of member documents (cf. multi-file document). Each document in the collection can still be accessed as an individual document but also through the document collection.
Relationships	You can also define the *relationships* between objects. Using relationships you can, for example, indicate that two documents are related. Relationships enable easy tracking of all documents related to an issue.
Template	You can use another object as a template for creating a new object. When you select a template from the list, the metadata card adjusts itself to the specifications of the template object. You can edit and add metadata. Specify an object as a template by setting its *Is template* property to *Yes*.
Workflow	The M-Files Workflow feature enables modeling object lifecycles according to real world processes. The workflow is grouped into states that correspond to the working stages of the document or other object. The M-Files administrator can easily define workflows to meet company requirements. For more information about workflows, refer to *Workflows* on page 313.

Server	M-Files Server runs on the server. Clients connect to the server and retrieve data so that the contents of the document can be viewed on the clients. The server is the physical location of the document vault.
Login account	Login accounts are server-level (or in some cases vault-level) accounts that are used for authenticating users to M-Files Server. A login account can be associated with multiple users, but only one user per vault. Compare with *users* on page 10.
User	Users are vault-level objects that store user-specific settings and user history and that have permissions to perform specific operations in a vault. A user is linked to one and only one login account. Compare with *login accounts* on page 10.

1.3. Conventions Used in This User Guide

This user guide contains a number of typographic and writing conventions as well as visual elements that will help you to better understand information and to perform tasks.

Terms and writing conventions

The following writing conventions are used in this user guide:

Writing convention	Description
<version>	Indicates that you must replace the text enclosed in angled brackets with information specific to your installation or environment. For example, in the registry path `HKEY_CURRENT_USER\Software \Motive\M-Files\<version>\Client`, you would replace *<version>* with the version number of your specific M-Files installation.
File > **Save**	The > symbol indicates that you need to select an item from a menu. For example, **Settings** > **Applications** indicates that you need to open the menu bar and select the **Applications** item from the **Settings** menu.
Before you begin	The *Before you begin* section tells you what you need to do before you can perform a given task. Complete the tasks listed in the *Before you begin* section before you move on to the task at hand.
Steps	The *Steps* section contains an ordered list of steps that need to be performed in consecutive order to complete the given task.
Optional	*Optional* indicates that a step in a task is optional and up to the users to decide whether or not they need to complete the step.
Results	The *Results* section describes the outcome of a successfully completed task. If you have completed the task correctly as instructed, you should experience the same outcome as described in the *Results* section.

For a list of terms commonly referenced in this user guide, see *M-Files Terminology* on page 8.

Visual elements

The following visual elements are used in this user guide:

Visual element	Name	Description
	Note	The *Note* icon highlights important information related to the topic at hand.
	Tip	The *Tip* icon highlights alternative procedures and additional information related to the topic being discussed.
	Video	The *Video* icon indicates that the chapter contains an instructional video related to the topic being discussed.
	Information	The *Information* icon highlights important information related to a specific step in a task. This information is always listed under the related step.
	Step example	The *Step example* icon highlights an example of how a given step should be completed. This information is always listed under the related step.
	Step result	The *Step result* icon highlights a description of the expected results for successfully completing

Typographic conventions

The following typographic conventions are used in this user guide:

Typographic convention	Description
Bold	In task steps, bolded text indicates user interface elements that the user can interact with, such as buttons and menu items. Example: Click **OK** to continue.
Italics	In task steps, italics indicates user interface elements that are not directly interactable, such as dialog names and labels and dialog section titles. Example: The **Object Type Properties** dialog is opened.
Blue text on page 10	Blue underlined text indicates hyperlinks. There are mainly three types of hyperlinks in this user guide: • Links leading to other parts in the user guide • Links leading to M-Files Knowledgebase articles • Links leading to external pages

Typographic convention	Description
Task heading	A heading with a blue background indicates a section that outlines procedural instructions. Such a section answers the question "How do I..." and it contains an ordered list of steps to be taken for completing a specific task.
Main heading	A heading with a grey background indicates a section containing information on a specific topic. In contrast to procedural instructions above, these sections answer the question "What is..." and they contain background information on a single subject.
Subtopic heading	These headings are subheadings of a larger chapter and they cover a related subtopic of the parent topic.
Section heading	These headings represent a subordinate heading for a subheading for further dividing the topic at hand into smaller sections.

2. System Overview

An M-Files system is composed of 1) a server computer (or multiple servers) running the *M-Files Server* component and containing the document vault or vaults, and of 2) *M-Files clients* used for displaying and editing the vault-stored information via the end-users' computers or mobile devices.

▶ Video: *Technical Structure*

You can access document vaults 1) by installing *M-Files Desktop* on page 48 on your desktop or laptop, 2) via any web browser (*M-Files Web* on page 15), or 3) with the *M-Files mobile apps* on page 17 for iOS, Android and Windows Phone devices.
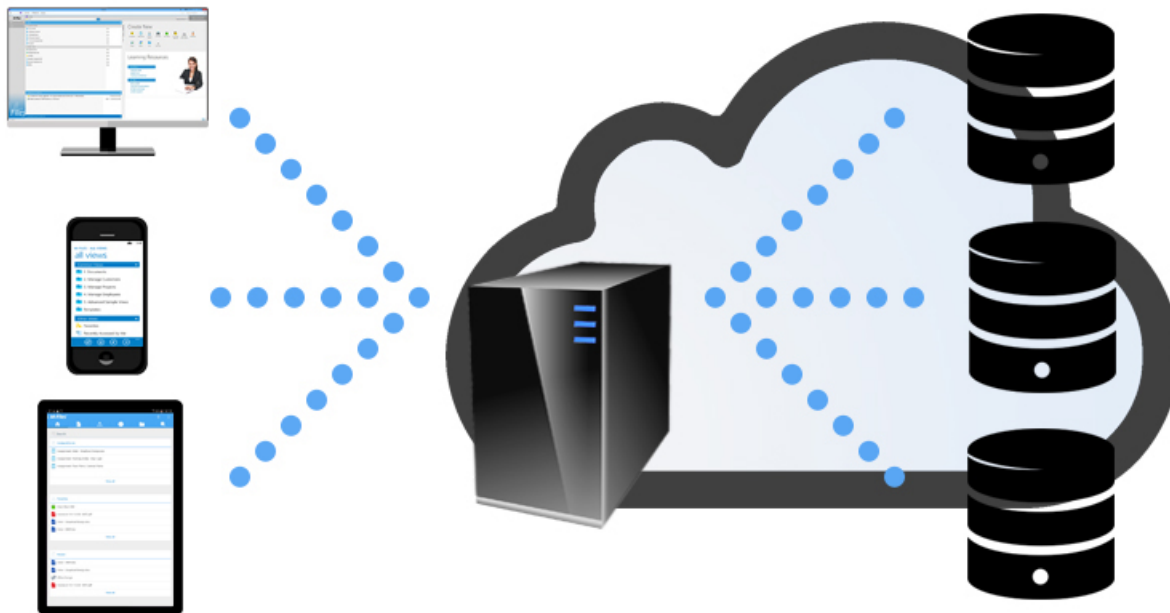
Figure 1: M-Files clients (on the left) are used for accessing M-Files Server (in the center), which manages the document vaults (on the right).

The image above offers a high-level description of the M-Files system: the clients (M-Files Desktop, M-Files Web, or any of the M-Files mobile applications) on the left are used for accessing the server computer (center of the image), which in turn manages one or more document vaults (on the right). Alternatively, M-Files Server and the document vaults may be located on a cloud-based server (see *Deployment Options for M-Files Server* on page 14).

You can edit server settings and the document vault structure with *M-Files Admin* on page 175. With *M-Files Desktop Settings* on page 34, you can add, remove and edit vault connections. For more information about using M-Files Web and the mobile applications, see the topics *M-Files Web* on page 15 and *M-Files Mobile* on page 17.

M-Files Server Deployment Options

M-Files Server can be set up on-premises, in the cloud, or as a hybrid deployment, the latter combining the advantages of on-premises and cloud-based systems. Refer to *Deployment Options for M-Files Server* on page 14 for more information.

M-Files languages

The M-Files user interface is available in multiple languages. For a list of the currently available M-Files software languages, see *Language Versions of the M-Files Software* on page 15.

2.1. Deployment Options for M-Files Server

M-Files offers several server deployment options, giving you the flexibility to leverage M-Files based on the model that best suits your organization's business needs and budget. Below is a short description of each server deployment option. Contact M-Files sales at *sales@m-files.com* if you need more information and advice on finding the best solution for your organization.

You will be able to use any of the clients (M-Files Desktop, M-Files Web, and/or M-Files Mobile) for vault connections regardless of the server deployment solution that you decide is best suited for your organization.

On-premises server

An on-premises server deployment is best suited for organizations that have already invested in existing servers and systems, or are required to use an on-premises solution deployed behind the organization's own firewall for regulatory reasons.

Using on-premises servers for M-Files document vaults does not, however, mean that they could not be securely accessed from outside (or inside) the company network. The vaults in the organization's private network can be accessed via *M-Files Web* on page 15, *M-Files mobile applications* on page 17, or M-Files Desktop (via a VPN connection or by using a *pre-shared key* on page 19) regardless of your location.

Cloud server

Document and enterprise content management via a cloud-based server deployment provides software as service (SaaS) flexibility associated with licensing and scalability (such as the ability to easily expand storage, or to modify the number of user licenses as necessary) without significant capital investment and incremental resources to support it. In addition, cloud-based solutions offer inherent remote access to company documents, and flexible monthly billing. Powered by the Windows Azure cloud platform, M-Files Cloud Vault delivers additional redundancy and automated third-party backup that offers greater protection against data loss or theft.

Please note that using a cloud-based deployment also enables you to use all the client options for connecting to your document vaults.

Cloud Vault Subscription Management Portal

The M-Files *Cloud Vault Subscription Management Portal* allows end user administrators to manage their subscriptions online.

The portal enables the following functions:

- Adding new licenses and removing existing licenses.
- Adding new user accounts and removing existing ones.
- Changing user details and license types.
- Downloading M-Files installers.

Hybrid server

With an M-Files hybrid deployment, organizations can both leverage their existing on-premises technology investments and take advantage of an award-winning document and enterprise content management solution running in the public cloud or a private cloud, as needed.

Furthermore, M-Files Cloud Vault can be seamlessly integrated with existing on-premises systems like an ERP or CRM, such as SAP or Microsoft Dynamics GP and AX. Conversely, an on-premises deployment of M-Files can be easily integrated into existing cloud-based business applications, such as Salesforce, Microsoft Dynamics Online or NetSuite.

The same client options (M-Files Desktop, M-Files Web, or any of the M-Files mobile applications) are equally available for organization's using a hybrid server deployment.

2.2. Language Versions of the M-Files Software

M-Files software is currently available in the following languages:

- Albanian
- Arabic
- Bulgarian
- Chinese (Simplified/PRC)
- Chinese (Traditional/Taiwan)
- Croatian
- Czech
- Danish
- Dutch
- English
- Estonian
- Finnish
- French
- German
- Greek
- Hebrew

- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese (Brazil)
- Romanian
- Russian
- Serbian
- Slovak
- Slovenian
- Spanish
- Swedish
- Turkish
- Vietnamese

You may change the language of the software and the document vault (metadata structure) while the software is running. Even if, for example, a Finnish version of M-Files has been installed on the computer, you can easily switch to the English version without reinstalling the software. This is a significant benefit when shared computers are used.

> **Note:** Only when 1) the software installation language, 2) the vault language, and 3) the Windows display language are the same, all the M-Files functions and the metadata structure of the document vault are displayed in the language in question. For more information, see *Languages and Translations* on page 231.

2.3. M-Files Web

You can access M-Files vaults also via the M-Files Web browser interface. M-Files Web is an ideal client for users that use the system less frequently. For optimal user experience, we recommend installing the M-Files Desktop client.

▶ Video: *M-Files Web*

Ask your system administrator for the address of M-Files Web in your organization. Or if you are looking for instructions on how to set up the M-Files Web connection in your organization, please refer to *Web and Mobile Access* on page 185.

> **Note:** M-Files Web is, by default, installed and configured to run on the same computer with M-Files Server, providing access to the vaults on this server. If you need to set M-Files Web to use M-Files

Server located on another computer, refer to the document *How to Configure M-Files Web Access on a Separate Server Computer*.

For additional security, M-Files can be configured to require a pre-shared key in addition to the user's username and password. This provides an additional level of security without requiring users to open a VPN connection for accessing M-Files. For more information, see *Accessing M-Files Vaults without VPN* on page 19. In case your organization is using federated identity management, see *Using Federated Authentication with M-Files*.

Logging in to M-Files Web

1. Navigate in your web browser to the M-Files Web address provided by your system administrator or an M-Files consultant.

   ✎ Let's say the name of your vault is *Sales Tracker*. In that case, the address can be, for example, *https://sales-tracker.cloudvault.m-files.com* for cloud-based deployments, or *http://sales-tracker.mydomain.com* for on-premises vaults. Within your corporate network, the connection protocol might be *HTTP* instead of *HTTPS*.

2. Input your login credentials or select **Log in with current Windows credentials**.

3. If you have access to several vaults, select the vault you want to connect to.

   ⓘ If you have access to only one vault, you will be connected automatically.

You should now be logged in and you should see the M-Files home screen.

M-Files Web User Interface

M-Files Web enables you to use all the basic M-Files functions, including electronic signatures for workflow state transitions (see *Electronic Signature* on page 329).

The user interface is also highly similar to that of M-Files Desktop. Refer to the *Using M-Files Desktop* on page 48 section for more details about the user interface components.
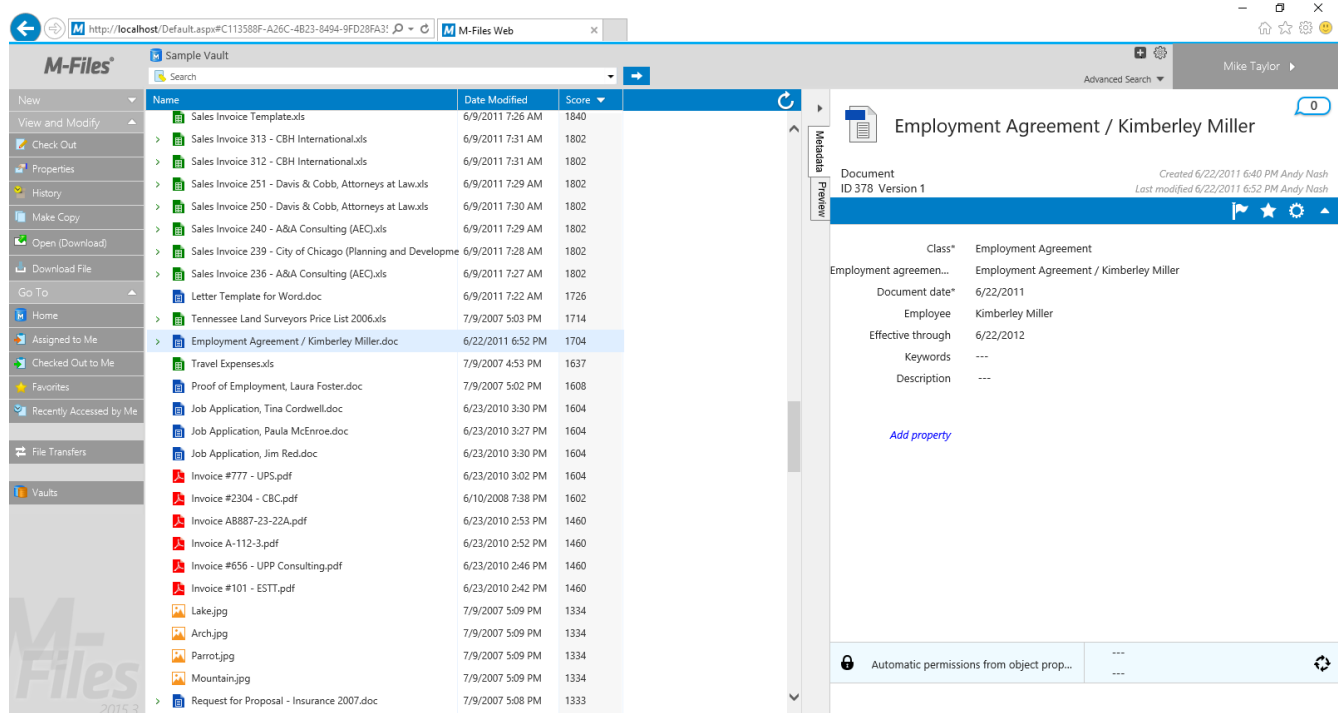
Figure 2: M-Files Web user interface.

2.4. M-Files Mobile

M-Files is also available as a mobile application for iOS, Android and Windows Phone devices. The mobile applications enable you to, for example, gain access to all vault content and mark your assignments as complete on the go, as well as to create and share new objects with your mobile device.

You can download the latest version of the mobile applications from your application store:

- *M-Files for iOS* (iPhone and iPad)
- *M-Files for Android* (phones and tablets)
- *M-Files for Windows Phone*

For a description of functional differences between the mobile applications, see the Knowledge Base article *M-Files Mobile Apps Feature Comparison*.

For additional security, M-Files can be configured to require a pre-shared key in addition to the user's username and password. This provides an additional level of security without requiring users to open a VPN connection for accessing M-Files. For more information, see *Accessing M-Files Vaults without VPN* on page 19).

▶ Video: *M-Files Mobile*
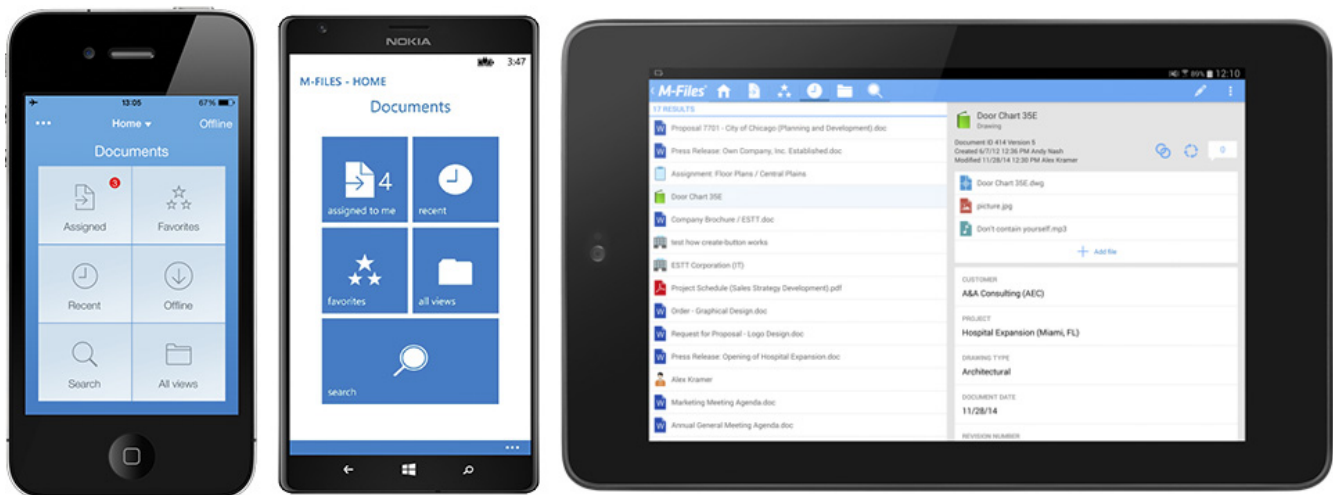
Figure 3: The M-Files mobile apps.

Application language

M-Files mobile applications use your device's language settings to determine the user interface language.

Enabling the use of mobile apps for on-premises vaults

In order for you to access your organization's on-premises vault(s) via a mobile device, M-Files Web must be enabled and configured. M-Files Web acts as the connection point for the native mobile apps by providing the M-Files Web Service REST API services. For more information about M-Files Web settings, refer to *Web and Mobile Access* on page 185.

In cloud-based deployments, you can always use mobile apps without any special configuration.

Logging in to M-Files Mobile

1. Ask your vault administrator or an M-Files consultant for the login details of the document vault.

2. On the login screen, input the server address and your username and password.

✏️ Let's say the name of your vault is *Sales Tracker*. In that case, the address can be, for example, *https://sales-tracker.cloudvault.m-files.com* for cloud-based deployments, or *http://sales-tracker.mydomain.com* for on-premises vaults. Within your corporate network, the connection protocol might be *HTTP* instead of *HTTPS*.

ℹ️ For cloud vaults hosted in the M-Files cloud, M-Files recognizes the server address even if you only enter the *sales-tracker* part. Although, to be absolutely sure that the correct protocol and address is used, it is always recommended to use the full server address.

3. Tap **Log in**.

4. If you have access to several vaults, select the vault you want to connect to.

    ℹ️ If you have access to only one vault, you will be connected automatically.

You should now be logged in and you should see the M-Files home screen.

Adding vault connections with links

Administrators can create links for facilitating the end users' vault connection process. The end user only has to open the link with their mobile device and input their username and password. After a successful connection, the vault connection information is saved to the user's device.

For more details and an example, refer to the document *M-Files URL Properties*.

2.5. Security and Authentication

This section discusses various topics related to system security and connections to M-Files Server and the M-Files vaults.

M-Files and Virus Scanning

M-Files is compatible with all commonly used virus scanning products.

It is, however, important to ensure that the virus scanners on the end users' computers do not perform scheduled scanning for the virtual M-Files drive (the M: drive by default). A scheduled scan for the M-Files drive would load all the content from the M-Files server to the user's client and unnecessarily strain both the network and the server.

Additionally, for best performance, you may wish to disable any real-time scanning for the virtual M-Files drive (the M: drive by default) and the M-Files installation folder ("C:\Program Files\M-Files" by default). Excluding these locations from real-time scans can help prevent unnecessary system load and possible conflicts between M-Files and the anti-virus software.

Excluding the M-Files drive and installation folder from virus scanning

To exclude the M-Files drive and the installation folder from virus scanning, you should add their paths to the appropriate exclusion lists or exceptions lists in the anti-virus software. For example with Symantec Endpoint Protection Manager (SEPM), this would be done via an *exceptions policy* as described in the Symantec knowledge base article *Create Centralized Exceptions Policies in Endpoint Protection Manager 12.1*. Other commonly used anti-virus software products may use terminology such as "excluded items list", "exclude objects", or "exclude from scanning".

There are typically separate exclusion lists for scheduled scanning and real-time scanning.

Excluding the M-Files Client process from virus scanning

If your anti-virus software supports excluding processes by name, it is usually a good idea to exclude the *MFClient.exe* process from any real-time scanning. By default, the path to *MFClient.exe* is "C:\Program Files

\M-Files*<version>*\Bin\x64\MFClient.exe" on 64-bit systems and "C:\Program Files\M-Files*<version>*\Bin \x86\MFClient.exe" on 32-bit systems. With SEPM, for instance, this can be done by following the instructions in the Symantec knowledge base article *How to create an application exception in the Symantec Endpoint Protection Manager*.

Excluding the *MFClient.exe* process from real-time scanning can help improve performance by preventing the virus scanner from scanning the same files twice: once when the application opens the file and another time when *MFClient.exe* performs an internal *open* operation on the same file.

Accessing M-Files Vaults without VPN

Organizations have traditionally relied on Virtual Private Network (VPN) technology to secure access to corporate resources (such as M-Files vaults) from outside the private network of the organization. M-Files versions 10.2 and later enable you to provide secure access to the M-Files system without the downsides of the traditional VPN-based approach.

The security of this approach is based on encrypting all network traffic between client devices and the server with HTTPS (SSL/TLS) and on using a pre-shared key as an additional "shared secret" in authentication to ensure that only authorized devices can attempt to connect to the system.

> **Note:** Cloud-based servers, M-Files Web, and the mobile applications use the HTTPS protocol by default, but for pre-shared keys to work on desktop clients connecting to an on-premises server, "RPC over HTTP with SSL" communication between the server and the desktop clients needs to be enabled. For more information, refer to the document *Enabling RPC over HTTPS connections to M-Files Server*.

Together, the HTTPS encryption and the use of a pre-shared key as a second factor in authentication provide similar security as VPN but without the complexity and compatibility challenges of VPN. However, it needs to be noted that the approach is not identical to VPN from the security point of view, and that each organization needs to determine if granting access to M-Files vaults without VPN is appropriate considering the organization's business needs and security requirements.

For more information about using pre-shared keys for secure M-Files access, please refer to *Securing Access to M-Files Vaults with a Pre-Shared Key*.

HTTPS Connections to M-Files Server

The communication between M-Files Server and the M-Files clients can be accomplished by using various connection protocols. Cloud-based servers (as well as the M-Files Web client and the M-Files mobile applications) only accept communication via the HTTPS protocol, whereas the default way for M-Files Desktop to communicate with an on-premises M-Files server is to use the Remote Procedure Call (RPC) protocol (TCP/IP, port 2266). Since this mode of communication does not require any additional configuration steps, it is usually the preferred way of communicating inside the organization's internal network.

In some situations, however, it is preferable to enable M-Files Desktop to communicate with M-Files Server via the HTTPS protocol instead of RPC. This is especially useful if clients are connecting from outside the company's internal network. HTTPS connections are always encrypted and are typically not blocked in hotel networks or other public networks.

For instructions on how to enable "RPC over HTTP with SSL" communication between M-Files Desktop and M-Files Server, refer to the document *Enabling RPC over HTTPS connections to M-Files Server*. With the configuration described in the document, all traffic from M-Files Desktop is encrypted and tunneled through TCP port 443.

Once the "RPC over HTTP with SSL" connections have been enabled on the server, end users will be able to use the HTTPS protocol while adding or editing a document vault connection in *M-Files Desktop Settings* on page 35.

M-Files and Federated Authentication

Traditionally, the need to verify user identity has been met by using software-specific credentials or Windows credentials. Federated authentication offers organizations the possibility to use an authentication system that is

completely external to M-Files. In many cases, having a centralized repository for all the M-Files user credentials completely *outside* the M-Files system can be very useful. Federated identity management also enables single sign-on, and provides the opportunity for the users to utilize their existing credentials.

For more information about using federated authentication with M-Files, see the article *Using Federated Authentication with M-Files*.

3. Installation and Implementation of the Software

This section guides you through the steps and requirements for an M-Files installation or *upgrade* on page 43, along with describing how to set up a vault, add users to it, and establish a vault connection.

If you already have the M-Files software installed on your computer, and have an active vault connection, you can move to *Exploring the Document Vault* on page 48.

3.1. System Requirements and Technical Details

This section lists the system requirements for the various M-Files components, as well as technical details, for instance, about using M-Files in special environments, securing information with file data encryption, and integrating 3rd party applications to M-Files.

System Requirements

This topic lists the system requirements for the various M-Files components.

Operating system requirements

M-Files Desktop:

- Microsoft Windows 10
- Microsoft Windows 8 and 8.1
- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008

M-Files Server:

- Microsoft Windows Server 2016 (recommended)
- Microsoft Windows Server 2012 R2 (recommended)
- Microsoft Windows Server 2012 (recommended)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows 10
- Microsoft Windows 8 and 8.1
- Microsoft Windows 7
- Microsoft Windows Vista

> **Note:** Both the server computer and client workstations must have *.NET Framework* 4.0 or above installed in order for all M-Files functions to work properly.

The operating system version can be either Workstation or Server.

For data security reasons, we do not recommended installing M-Files Server on a computer that is also used as a Microsoft domain controller. However, M-Files Server can technically run on a Microsoft domain controller server.

Mac and Linux users can access M-Files via *M-Files Web* on page 15.

> **Note:** M-Files Desktop/Client for M-Files 10.x and later is not compatible with Microsoft Windows XP. Microsoft Windows XP users can use M-Files Server for M-Files 10.x and later with the client version 9.0. M-Files Desktop/Client for M-Files 10.x and later also requires Internet Explorer 9 or newer.

32/64-bit support

M-Files is compatible with both 32-bit and 64-bit Microsoft Windows operating systems. The 32-bit and 64-bit systems have separate installation programs.

M-Files Server hardware requirements

The minimum requirements and recommended hardware setups for M-Files Server are listed in the tables below.

Minimum requirements	
Processor	1 processor with 2 cores (Intel Xeon or similar)
RAM	1 GB

Recommendation for up to 50,000 objects	
Processor	1 or 2 processors with 4 or more cores in each (Intel Xeon or similar)
RAM	4 GB
Storage	RAID 1 or RAID 5 disks

Recommendation for up to 1,000,000 objects	
Processor	2 or 4 processors with 4 or more cores in each (Intel Xeon or similar)
RAM	16 GB
Storage	RAID 1 or RAID 5 disks
Operating system	64-bit operating system
Database management system	MS SQL Server 2012, 2014, or 2016 Standard or Enterprise Edition

Recommendation for more than 1,000,000 objects	
Processor	4 processors with 4 or more cores in each (Intel Xeon or compatible)
RAM	32 GB
Storage	RAID 1 or RAID 5 disks
Operating system	64-bit operating system
Database management system	MS SQL Server 2012, 2014, or 2016 Standard or Enterprise Edition

M-Files Server can be installed either on a physical or a virtualized server, for instance using Hyper-V or VMWare ESXi.

> **Note:** Consult us for requirements and best practices in environments with more than 1,000,000 objects.

Supported operating systems for the M-Files mobile apps

The M-Files mobile apps support the following mobile operating systems:

App name	Required OS version
M-Files Universal App	Windows 10
M-Files Mobile for Windows Phone	Windows Phone 8.0/8.1 or later
M-Files Mobile for iOS	iOS 7.0 or later
M-FIles Mobile for Android	Android 2.3.3 or later

Recommended browsers for M-Files Web

For optimal user experience, consider using M-Files Web with Google Chrome and the M-Files Web browser plugin available in the Chrome Store.

The supported browser versions for M-Files Web are:

Web browser	Recommended version	Operating system
Google Chrome (recommended)	Latest available version	Microsoft Windows
Internet Explorer	IE11	Microsoft Windows
Mozilla Firefox	Latest available version	Microsoft Windows
Safari	Latest available version	OS X
Microsoft Edge (limited)	Latest available version	Microsoft Windows

Note: If you cannot use Google Chrome and must edit documents frequently with M-Files Web, we recommend enabling the Java applet for M-Files Web. The Java applet can be used with IE11 and with the latest versions of Mozilla Firefox and Safari. See *Enabling the Java applet for M-Files Web* on page 24 for instructions on how to enable the applet for a vault of your choice. In case you are upgrading M-Files, though, this does not need to be done as M-Files only disables the applet for any new M-Files installations.

Note: Internet Explorer 8, 9 and 10 are no longer supported by M-Files Web.

Tip: We recommend you to integrate M-Files Web with Microsoft Office 365 Online Apps. See the article *Enabling Office Online Services for M-Files Web* for more information.

M-Files Server disk space requirements

Metadata database

- Local hard disk drive
- 2–5 GB of disk space for 100,000 objects
- 20–50 GB of disk space for 1,000,000 objects

Consult M-Files Corporation for requirements and best practices in environments with more than 1,000,000 objects. Please also note that the hard disk space requirements for the metadata database highly depend on the complexity of the metadata structure as well as on the number of object versions in the database. The estimates above apply to typical document management use cases.

File data

- Local hard disk drive OR a network file server

- Sufficient disk space for storing the document files, thumbnails, viewer files, and full-text search index files

M-Files uses a binary delta algorithm to process old versions of document files. This reduces the disk space consumption of old file versions considerably.

Administrators can free disk space by archiving or destroying old versions.

Microsoft SQL Server requirements

The following Microsoft SQL Server features need to be enabled if you wish to use Microsoft SQL Server as the M-Files database engine:

Instance features

- Database Engine Services
- Reporting Services, Native Mode (if reporting is used)

Shared features

- Management Tools, Basic
- Management Tools, Complete (if reporting is used)

Enabling the Java applet for M-Files Web

The Java applet for M-Files Web is disabled by default if you are not upgrading from a previous M-Files installation.

If you cannot use Google Chrome and must edit documents frequently with M-Files Web, we recommend enabling the Java applet for M-Files Web. The Java applet can be used with IE11 and with the latest versions of Mozilla Firefox and Safari.

Follow these steps to enable the Java applet for M-Files Web in a vault of your choice:

1. Open the web browser of your choice.

2. Open the address `http(s)://<Your M-Files Web domain>/Configuration.aspx`.

3. Log in with system administrator credentials.

4. Under *Vault-specific settings*, select any of the available vaults.

5. Set the *Java applet* option to **Enable**.

6. Optional: Repeat the steps from *1* on page 24 to *5* on page 24 if you want to enable the Java applet for other vaults as well.

The Java applet is now enabled for the vault(s) of your choice.

Technical Details

Database engine and data storage

M-Files Server includes Firebird Embedded, a powerful SQL database engine. Firebird is the default database engine of M-Files. Purchasing additional database software is thus not required. When using Firebird as the database engine of M-Files, the metadata of documents and other objects will be stored in a SQL database. The data files of objects are stored in the file system.

Optionally, Microsoft SQL Server 2008, 2008 R2, 2012, 2014, or 2016 can be used as the database engine of M-Files for better performance and support for larger repositories. M-Files supports all the editions, for example, Express Edition, Standard Edition, and Enterprise Edition. When using Microsoft SQL Server as the database

engine of M-Files, the metadata of documents and other objects will be stored in a SQL database. The data files of objects can be stored either in the MS SQL database or in the file system. MS SQL Server can be installed on the M-Files Server computer, or alternatively, the M-Files Server computer can connect to an existing SQL Server farm. In the latter case, the processor and RAM requirements of the M-Files Server may be smaller than indicated above.

M-Files uses Unicode and thus supports storing and finding data in East Asian languages as well. The data saved in the file system can be encrypted with the AES-256 algorithm. For more information, refer to *Protecting File Data at Rest with Encryption in M-Files*.

Network communication

M-Files Desktop communicates with M-Files Server via TCP/IP or HTTPS protocol. M-Files Web and the M-Files Mobile apps communicate with M-Files Server via HTTP or HTTPS protocol.

It is recommended to use encrypted connections in all client-to-server communication. For more information, see *Protecting Data in Transit with Encryption in M-Files.*

Special environments

M-Files is compatible with the following special environments:

- Remote Desktop Services (Terminal Services)
- Citrix XenApp

  - M-Files is Citrix Ready for Citrix XenApp 7.6. See *M-Files and Citrix XenApp* for the configuration details.
- Linux file servers
- Novell networks

User authentication

M-Files supports multiple authentication methods (can be mixed):

Windows authentication	Users are authenticated using their Windows account names and passwords. Login accounts can be imported from Active Directory (LDAP).
Federated authentication	Users are authenticated against an external Identity Provider (IdP), such as Azure Active Directory. See *Using Federated Authentication with M-Files* for more information.
M-Files authentication	Users are authenticated with usernames and passwords specified within M-Files.

M-Files supports using pre-shared keys for an additional level of security. For more information, see *Securing Access to M-Files Vaults with a Pre-Shared Key*.

Database connections

M-Files Server can be integrated with existing databases, such as CRM and ERP databases. All databases with an OLE DB or ODBC driver are supported (includes SQL Server, Access, Oracle, and MySQL).

Integrations with 3rd party applications

Numerous 3rd party applications can be intergrated to M-Files. See *www.m-files.com/integrations* and *https://catalog.m-files.com* for examples.

Application programming interface (API)

M-Files includes an ActiveX/COM API. Supported languages include VB.NET, C#, Visual Basic, VBScript, and C++. Additionally, M-Files includes the M-Files Web Service API that allows programmatic access to M-Files through a REST-like interface.

M-Files API is included within the installation of the M-Files software. The API documentation is available as an *online version* and as a Microsoft HTML Help file, which you can download at *https://www.m-files.com/en/api*.

M-Files Web Service API is documented at *https://www.m-files.com/mfws*.

M-Files UI Extensibility Framework allows external add-ins (M-Files Applications) to be used for personalizing the behavior of M-Files Desktop. With these applications, the M-Files experience can be modified to better match specific business areas and needs. For more information, please refer to the *UI Extensibility Framework documentation*.

Backups and maintenance

M-Files automatically optimizes the vault database once a week. No other regular database maintenance is needed.

M-Files supports scheduled full and differential backups. When using Firebird as the database engine, document vaults are backed up using the M-Files Admin tool.

When using Microsoft SQL Server as the database engine, document vaults are backed up using the management tools of Microsoft SQL Server and file system level backup tools. Any backup system compatible with Microsoft SQL Server can be used.

Technical assistance

For further technical inquiries, please contact *support@m-files.com*.

3.2. Installing the Software

M-Files can be installed as a single installation or distributed and installed on several computers at once. These instructions are for executing a single M-Files installation. For advanced installation options, such as customizing the installation package to automatically configure client or server connections, disabling automatic checking for software updates or using Active Directory group policies in distributing M-Files, refer to the document *M-Files Setup: Advanced User's Guide*.

> 📄 **Tip:** While the M-Files installation is in progress, you might want to see information about *M-Files and Virus Scanning* on page 18.

- Both the server computer and client workstations must have *.NET Framework* 4.0 or above installed in order for all M-Files functions to work properly.
- You have received the M-Files setup file from your system administrator, or you have downloaded it via the *M-Files download page*.

    For a single M-Files installation, follow these steps:

1. Quit all other applications running on your computer and double-click the M-Files setup file.

    ☑ The welcome screen of the installation wizard appears.

2. Click **Next**.

3. Read and accept the end-user license agreement to be able to continue.

4. Click **Next**.

5. Select the software components to be installed.

   ℹ️ You can install M-Files for *evaluation* or perform a *normal installation*.

   If you are not an M-Files system administrator in your organization, you only need to install M-Files Desktop. In this case, M-Files Server has been installed on your organization's local area network, and your M-Files system administrator has the M-Files Server Tools (M-Files Admin) installed. After the normal installation, you can *connect to the document vault(s)* on page 35 on your M-Files server via M-Files Desktop Settings.

   The evaluation installation includes all the software components as well as a sample vault, which you can start exploring immediately after installation.

6. Continue the installation by clicking **Next**.

7. Specify the installation location and click **Next**.

8. If you do not want to change anything, click **Next** to start the installation.

9. Select whether or not you would like to see the *Guided Tour* and click **Finish** to complete the installation process.

The M-Files software has now been installed on your computer. If you have performed an evaluation installation, you can continue familiarizing yourself with the software by opening the *Guided Tour* via the Windows Programs menu.

3.3. Creating a Document Vault and a User

If you are an M-Files Desktop user, you can move to *M-Files Desktop Settings* on page 34.

This is a general description for creating a document vault and its user(s) with M-Files Admin. You can find a more detailed description in the chapter *M-Files Admin* on page 175.

📄 **Note:** If you chose the evaluation installation option when installing M-Files Server, two vaults are automatically deployed. The "Sample Vault" contains a reference metadata structure and views for some common information management processes and sample files to help you to easily evaluate the search. The "My Vault" contains the same metadata structure and views as the "Sample Vault", but does not contain the sample content. You can use the structure of "My Vault" as a foundation for your purposes instead of creating a new vault from scratch. You can also *restore* on page 201 the sample structure from the M-Files Server installation folder ("C:\Program Files\M-Files\<*version*>\Server\sample \My Vault.mfb" by default).

You can open M-Files Admin from your Windows start menu. The user interface consists of the left-side tree view for navigation, and of a content section on the right. Most of the content windows also include a task area for the most common operations.
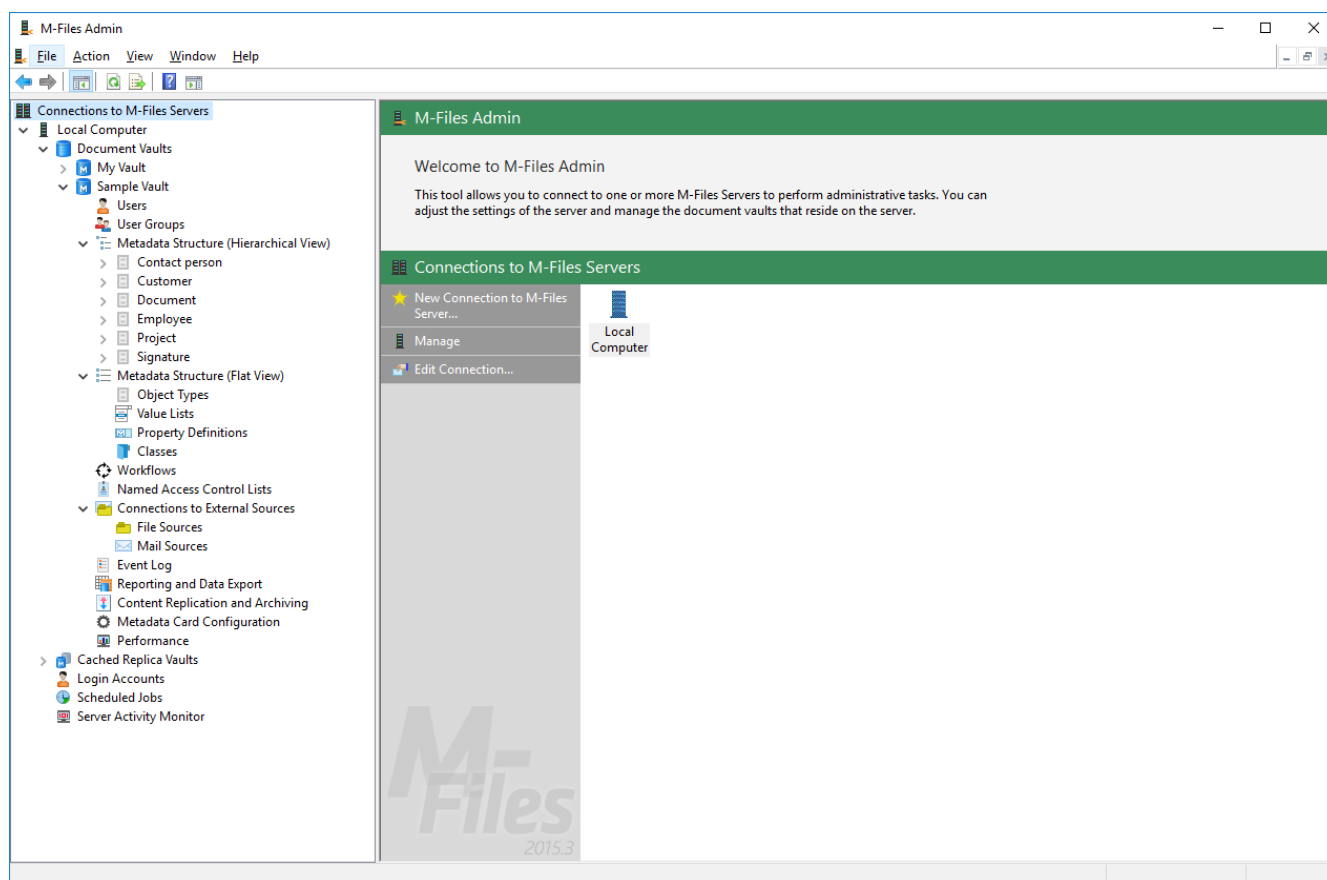
Figure 4: The main window of the M-Files Admin.

Creating a New Document Vault

▶ Video: *New Document Vault*

If you want to create a new vault in a language other than the currently selected software language, you must first change the software language and restart the M-Files Server service via Windows Task Manager before creating the vault. For instructions on changing the software language, see *Selecting the Software and Vault Language* on page 238.

Do the following steps to create a new document vault:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Select **Document Vaults** in the left-side tree view.

☑ The **Document Vaults** list is opened in the right-side pane.

4. Click **New Document Vault...** on the task area.

☑ The **Document Vault Properties** dialog for a new vault is opened.

5. In the **Name** field, enter a name for the new document vault.

6. Use the **Primary language** and **Secondary language** drop-down menus to select the primary and secondary languages for full-text search features.

   ⓘ These selections affect, for example, the way inflected or irregular forms of words or compounds are dealt with in searches. If the document vault is to contain material in several languages, it is recommended to select the language that is used most as the primary language and a less commonly used language as the secondary language.

   Selecting a language or languages improves the probability of finding the right search results. Even if a certain language was not selected as the primary or secondary language, the full-text search will nevertheless return results if words in this language were used in the search.

7. Optional: Click **Import...** to change the vault icon to facilitate finding the right vault in case you are using multiple vaults.
   a) In the **Change Icon** dialog, select an item from the list or click **Browse...** to search for a different icon.
   b) Click **OK** once you have selected the new icon.

      ⓘ You can revert back to the default icon by clicking **Use Default**.

8. Optional: Change the *advanced settings* on page 197 on the **Advanced** tab.

9. Click **OK** once you are done.

You should now have created the document vault and it should appear on the left-side tree view of M-Files Admin under **Document Vaults**.

> 📄 **Note:** When you create a document vault, M-Files automatically creates an ID for it. The ID can be changed later in the **Document Vault Properties** dialog of the vault by clicking the **Change Unique ID** button.

After you have created the vault, the users of the vault must add a connection to it via M-Files Desktop settings. For instructions, see *Adding a Document Vault Connection* on page 35.

New Login Account

The document vault has users who must first authenticate themselves from the point of view of the M-Files Server. Before creating the users, login accounts must be created for the M-Files Server. These login accounts are then added to document vaults as users. The same server login can be added to several document vaults.

▶ Video: *New Login Account*

Figure 5: The "Login Account Properties" window.

From the **New Login Account** dialog, you can assign a *name*, *authentication method*, and *password* for the login account. You can also specify the type of license acquired for the login account. If you are using M-Files for an evaluation period, you can select *No license*.

▶ Video: *Authentication Methods*

For more information about authentication and server roles, refer to *Login Accounts* on page 209. License management is described in more detail in *License Management* on page 179.

You can also import Windows login accounts to M-Files. For more information, refer to *Importing Login Accounts* on page 213.

Creating a Login Account

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Highlight **Login Accounts** in the left-side tree view.

4. Click **New Login Account...** on the task area.

    ☑ The **New Login Account** dialog is opened.

5. Enter a username.

6. Select an authentication method by clicking the appropriate radio button and enter authentication details in the fields below the selected authentication method.

7. Enter an email address and a full name in the personal information fields.

    ⓘ If you are using Windows authentication, you can click **Update Information from Domain** to retrieve personal information from the domain's directory service.

8. Select a license from the **License type** drop-down menu to set an appropriate license for the login account.

9. Optional: Check the **Login account is disabled** check box if you want to disable the login account for the time being.

10. Optional: Check the **System administrator** check box if you want to assign a system administrator role for the login account. This role entitles the user to make any changes on the server level, including *changing the server logins* and *creating and deleting document vaults*.

11. Click **OK** once you are done.

You should now have a new login account and it should appear in the **Login Accounts** list when you highlight **Login Accounts** in the left-side tree view in M-Files Admin.

Creating a User

▶ Video: *Configure User Properties*

Do the following steps to create a new user to a selected document vault:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight **Users**.

5. Click **New User...** on the task area.

    ☑ The **New User** dialog is opened.

6. Use the **Login account** drop-down menu to select a login account for the user or select **New login account...** from the same drop-down menu to create a new login account for the user.

    ⓘ For instructions on creating a new login account, see *New Login Account* on page 30.

    ☑ The **Full name** field is updated with the full name information of the selected login account.

7. Use the **Vault language** drop-down menu to select the default vault language for the user from the list of available vault languages.

    ⓘ For instructions on adding a new vault language, see *Languages and Translations* on page 231.

8. Set the properties and administrative rights for the new user in the selected vault by checking or unchecking the relevant option check boxes:

Option	Description
User account is disabled	When the account is disabled, the user cannot access the document vault. Logging in to the document vault has been disabled, but the user information is retained. The account can be easily enabled again by unchecking this option check box when necessary. For example, you may want an employee's account to be disabled during her vacation for data security reasons.
User cannot create documents or other objects	The user cannot create documents or other objects in the vault but can, for example, read them if provided with the necessary permissions.

Option	Description
User cannot create or modify traditional folders	The user cannot create traditional folders in the vault or modify existing traditional folders.
External user	Users can be grouped into external and internal users. A user can be defined as an external user by enabling the **External user** option. External users cannot see or access any documents other than those specifically marked for them. By default, they do not have permissions to view any documents. For example, you can define your customers as external users and grant them access to customer-specific documents in the document vault.
	As stated above, external users do not, by default, have permissions for accessing any documents. To share a document with an external user, access must be explicitly granted in the permissions of the document.
Full control of vault	With this option, the user is assigned all *administrative permissions* in the vault.
See and read all vault content (including deleted objects)	Regardless of the permissions specified for a document or object, a user with this permission can see and read all objects, including deleted ones.
See and undelete deleted objects	The user has the permission to restore documents and other objects marked as deleted.
Destroy objects	The user has the permission to permanently destroy objects.
Force undo checkout	A user with this permission can undo the *checkout* made by another user. For example, if a user has forgotten to check in a document that others should be able to edit, a user with this permission can check in the document. In this case, the changes made to the document during the checkout will not be saved on the server.
Change permissions for all objects	The user has the right to change the permissions for any object that they are permitted to see. You can edit the permissions for an object, for instance, remove the write permission to a document from other users.
	Note: The user with this permission has the power to obtain edit rights to documents that they would normally be able to only read.
Change metadata structure	The user has the permission to modify document vault metadata, such as add new document classes or value lists. For example, if you want to change the *Invoice* document class so that the *Project* property field must be filled in for each invoice, you can make the change if you have this permission. Even if the user does not have the permission to do this, the user can still add new metadata fields to individual objects using the metadata card.
Manage workflows	This permission enables the user to create, edit and delete workflows in M-Files Admin.
Manage user accounts	The user has the permission to manage login accounts in the selected document vault. With this permission, you can, for instance, add or remove users from the document vault.
Manage common views and notification rules	The user has the permission to manage the document vault views and notification rules. With this permission, you can create a document vault view

Option	Description

visible to all users. You can also define common notification rules. Common views and notifications are created via M-Files Desktop.

> 📋 **Note:** For more information on common views, see *"View" Menu* on page 79. For more information on common notification rules, see *Notification Settings (M-Files Desktop)* on page 127.

9. Optional: On the **Permissions** tab, specify the users or user groups who may see this user.

   a) On the **Users and user groups** list, highlight the user or the user group for which you wish to set the permissions for seeing this user.

   > ℹ️ If the desired user or user group is not on the list, click **Add...** to add the user or user group to the **Users and user groups** list.

   b) Check either the **Allow** or **Deny** checkbox to modify the permissions of the selected user.

10. Click **OK** once you are done.

A new user is created and it is listed in the **Users** list. The new user can now access the selected document vault with the permissions that you have defined.

> 📋 **Note:** You can also import domain users to M-Files. For instructions, see *Importing Users* on page 255.

3.4. M-Files Desktop Settings

Start M-Files Desktop Settings in order to set up the document vault that you want to access. Organizations normally use only one document vault, but there can be more than one in some cases.

> 📋 **Note:** Before you start setting up your client, consult your organization's M-Files system administrator to ensure that M-Files Server and the document vault have been installed on your local area network.
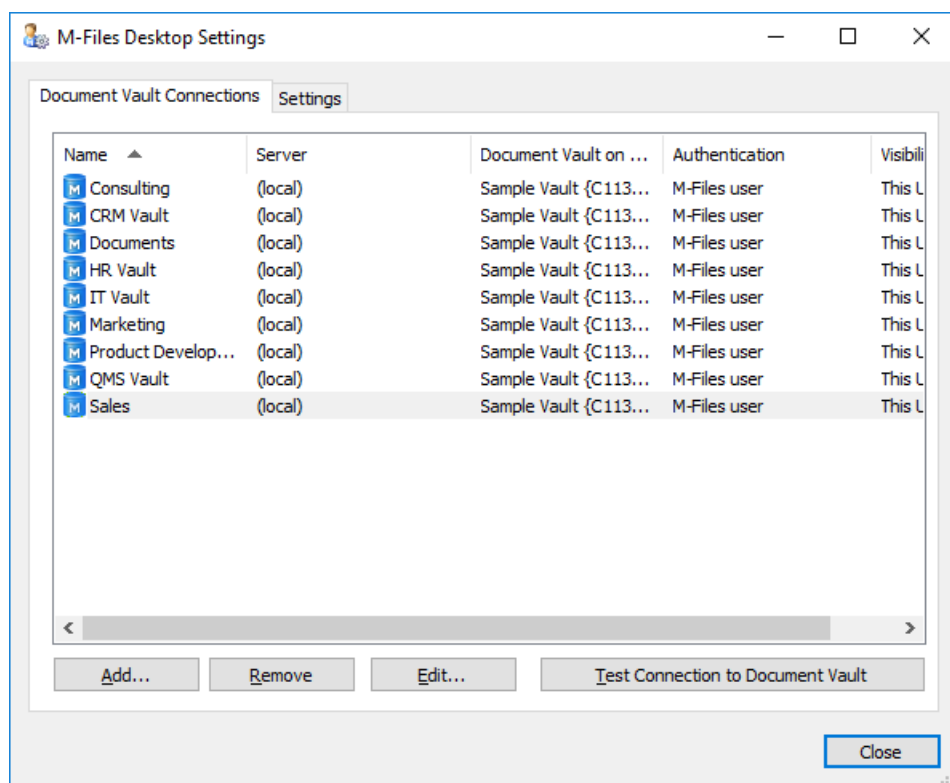
Figure 6: The M-Files Desktop Settings main window.

In M-Files Desktop Settings, the *Document Vault Connections* tab is displayed by default. Here you can add, remove, edit, and test your vault connections. The *Settings* tab lets you modify certain user- and computer-specific behavior, such as disabling the automatic check-in prompt or changing the M-Files drive letter.

▶ Video: *Desktop Settings*

Adding a Document Vault Connection

You can start adding a new document vault connection by clicking **Add...** in the M-Files Desktop Settings main window.

▶ Video: *New Vault Connections*
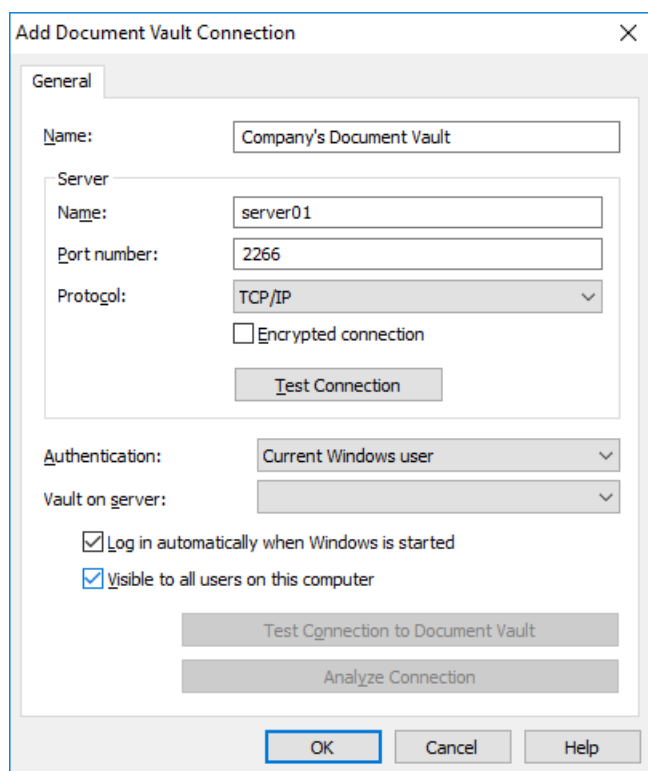
Figure 7: The Add Document Vault Connection dialog.

In order to establish the connection, you first need to specify a few properties.

Name

Begin by assigning a name to the document vault connection. The name can be anything, but it is a good idea to make it descriptive. The name will be displayed on the M:\ drive as a directory containing the contents of the document vault.

Server / Name

Enter the network name or IP address of the server on which M-Files Server has been installed and that contains the document vault.

Server / Port number

The server was specified in the previous field, and in this field you specify the port to connect to on the server. Enter the server port number to connect to. M-Files uses port 2266 by default for TCP/IP protocol.

Server / Protocol

Define the protocol to be used for the network connection. The available protocols are *TCP/IP*, *SPX*, *Local Procedure Call (LPC)* and *HTTPS*. *TCP/IP* is usually used for connecting to a document vault located on a different computer.

Encrypted connection

Enable this option to secure the communication between M-Files Desktop and M-Files Server. RPC encryption does not require Internet Information Services 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.

The option is available for the TCP/IP protocol only. If the protocol is HTTPS, the connection is always encrypted at the HTTPS protocol level. For connections from outside the organization's internal network, HTTPS or VPN should still be used, as RPC communication to the default TCP port, 2266, is often blocked by firewalls.

> 📝 **Note:** 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.

For more information on encrypted connections and for instructions on how to configure the server to require encrypted connections, refer to *Protecting Data in Transit with Encryption in M-Files*.

It is also possible to use *pre-shared keys* on page 19 in combination with HTTPS for securing a VPN-less access from outside the organization's private network.

Server / Test Connection

You can use this button to check that the server connection works correctly.

Authentication

Specify the method the document vault is to use for authenticating the user. The authentication options are *Current Windows user*, *Specific Windows user*, and *M-Files user*.

The user is always authenticated on M-Files Server when logging in to the document vault, for example. M-Files Server is capable of checking the login accounts and passwords of all M-Files users. This is the M-Files authentication method. When Windows authentication is used, M-Files Server has the passwords checked by the domain server.

With Windows authentication, users log in to the database with same information that they use to log in to the local computer or the organization domain. If the organization uses a domain, using the domain logins and passwords is the quickest and easiest authentication method. This means that new passwords and logins are not needed, which makes this a rather user-friendly method.

Differences between the various authentication methods

Current Windows user	When you have logged in to the local computer, you can use the same information to log in to M-Files Server. This is the *Current Windows user* authentication method.
Specific Windows user	A *Specific Windows user* will always be prompted for the login, domain, and password, i.e., the user does not necessarily log in to M-Files Server with the same information that was used to log in to the local computer.
M-Files user	The M-Files authentication method allows the user to log in to M-Files only. If the organization does not have a Windows domain or the user is not to have access to it, it is a good idea to use *M-Files authentication* for the document vault.

Vault on server

When there are several document vaults on the server, you can use this field to specify the document vault to connect to.

Log in automatically when Windows is started

You can choose to establish the connection to the document vault whenever Windows is started. This is a useful option if you are going to use the document vault daily. For more information, refer to *Login Accounts* on page 209.

Visible to all users on this computer

In Windows, there can be several users who each have their own user-specific settings. It is possible to provide user-specific access to M-Files document vaults. If you want the document vault to be visible to all users on this computer that have been defined in the operating system, check this box.

Test Connection to Document Vault

After specifying the contents of the above fields, you can check whether you can successfully connect to the document vault. If the connection works, the server has responded to the connection test.

User-specific Settings

To get here, click the **User-specific Settings** button on the *Settings* tab of M-Files Desktop Settings.
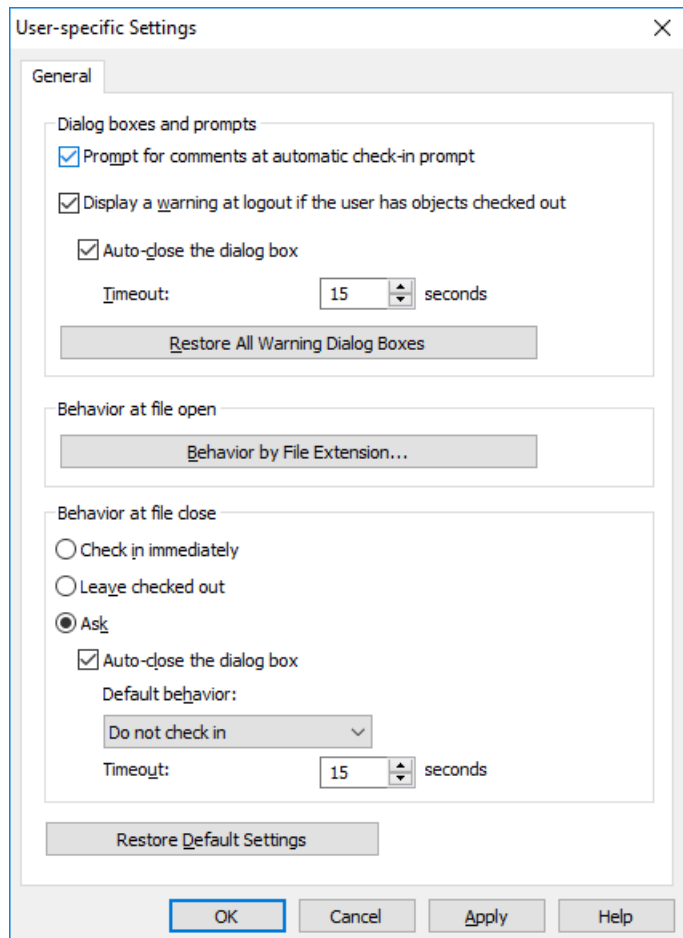
Figure 8: The user-specific settings are specific to Windows users per workstation.

Dialog boxes and prompts

You can define comments to be asked of the user upon each check-in. If the *Check in immediately* option has been selected for file closure, comments are not requested.

By default, a warning is always displayed when the user logs out if the user has objects checked out. Dialog boxes are also closed after a default timeout.

Behavior at file open

You can define for each file extension type whether the specific file format is always opened in *Check Out* or *Open as read-only* state. You can also specify for each extension type that, upon opening each file, the software asks the state in which the file is to be opened.

Behavior at file close

You can define which actions are performed on the file upon closing it. The definition applies to all file formats. By default, the user will be asked what they wish to do to the file upon closing it. If the user does not change the default procedure (*Do not check in),* the dialog will be automatically closed after a chosen time and the document will remain checked out.

Computer-specific Drive and Cache Settings

To get here, click the **Computer-specific Settings** button on the *Settings* tab of M-Files Desktop Settings.
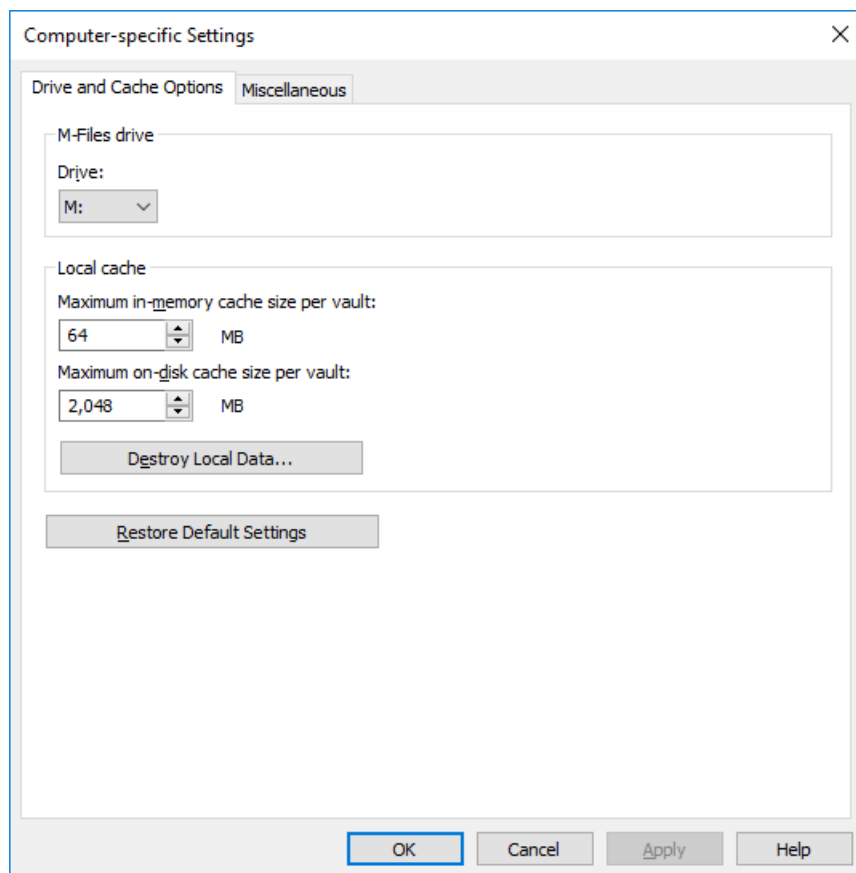
Figure 9: Drive and Cache options of M-Files Desktop.

Drive

Select the drive letter for the M-Files drive. The default drive is M:\.

Local cache

When using M-Files, the documents are retrieved from the server to the computer's local hard drive. The local cache makes M-Files significantly faster to use over slow connections.

Maximum in-memory cache size per vault

Here you can specify the amount of the computer's main memory that the document cache is allowed to take up.

Maximum on-disk cache size per vault

Here you can specify the amount of the computer's disk space that the document cache is allowed to take up.

Destroy Local Data

M-Files saves information about the documents locally in the computer's cache. The data remains on the server, but the cache makes M-Files faster to use. Local files take up space on the computer's hard drive and for this reason, it may sometimes be necessary to destroy local data. This function can be used to destroy local cache information about the documents by user and by document vault.
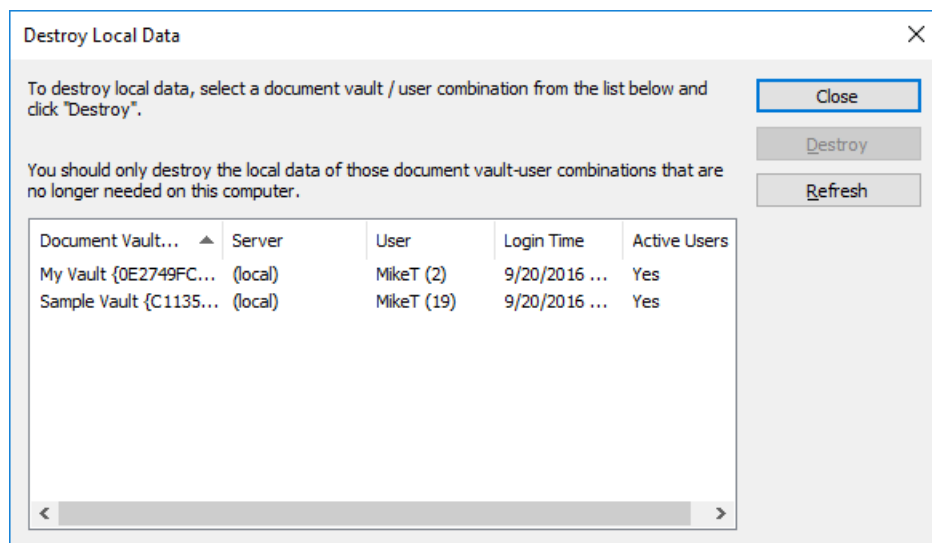
Figure 10: The local vault/user combinations are listed in the Destroy Local Data window.

Other Computer-specific Settings

To get here, click the **Computer-specific Settings** button on the *Settings* tab of M-Files Desktop Settings and select the *Miscellaneous* tab.
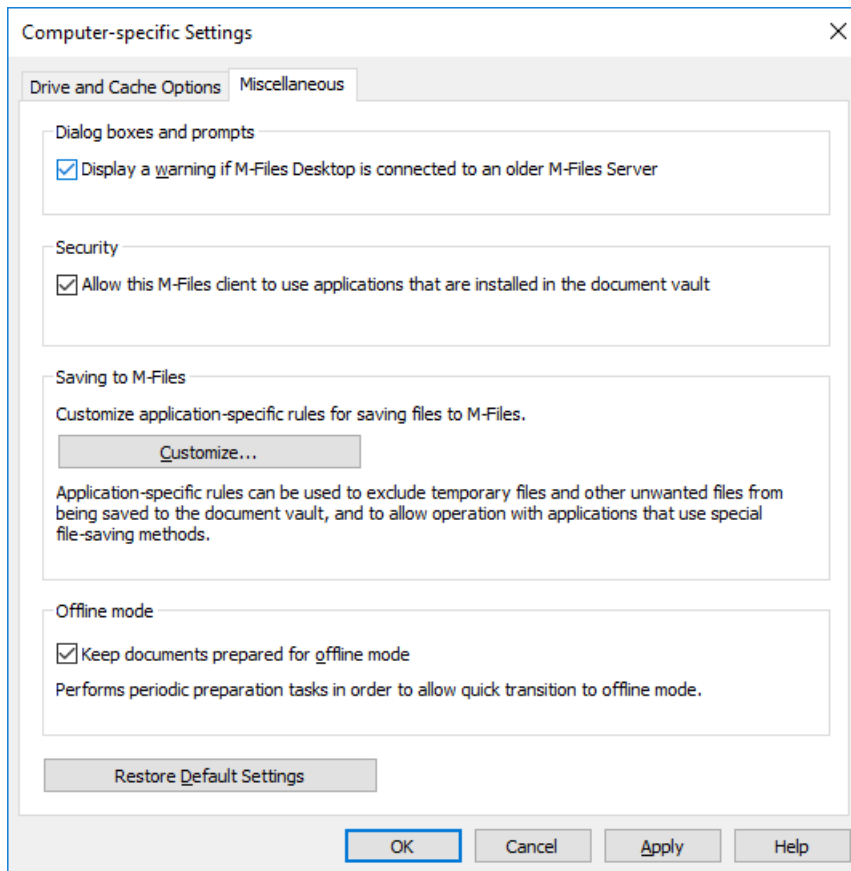
Figure 11: The Miscellaneous tab contains different computer-specific settings.

Dialog boxes and prompts, Security

The default settings are:

- *Display a warning if M-Files Desktop is connected to an older M-Files server.*
- *Allow this M-Files client to use applications that are installed in the document vault.*

Saving to M-Files

You can customize application-specific rules for saving files to M-Files. Application-specific rules can be used to, for example, exclude temporary files and other unwanted files from being saved to the document vault. Rules can also be used to allow operation with applications that use special file saving methods. The rules guarantee that, for instance, a metadata card of new files is displayed if automatic identification is not functioning.
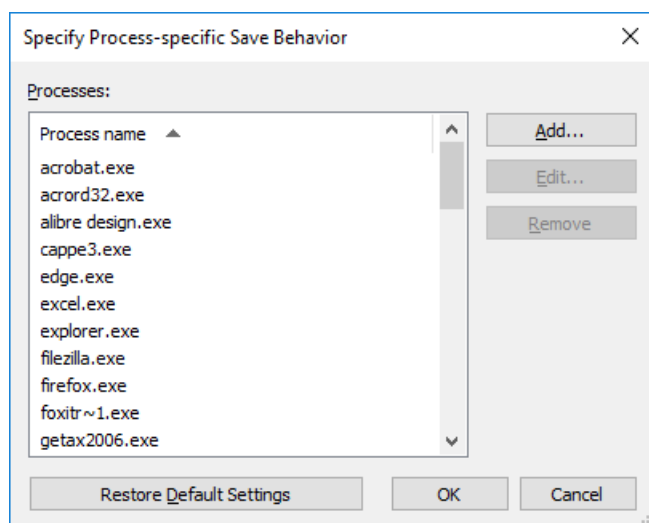
Figure 12: Add and edit process-specific saving behavior.

Add a new behavior by selecting **Customize...** > **Add...**

Saving to M-Files: General

General settings can be used to disable the default setting *Detect file save operations from standard file dialog boxes*.

You can also define process-specific file formats that are always accepted or never accepted for saving in M-Files. Use of an asterisk (*) defines that the process-specific setting is valid for all file formats.
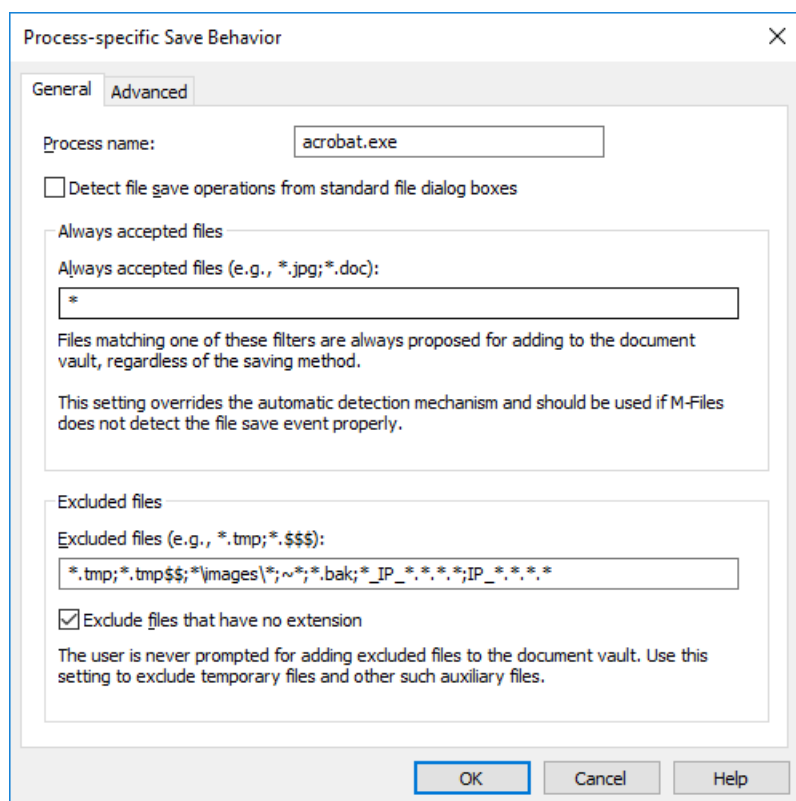
Figure 13: General process-specific settings.

Saving to M-Files: Advanced

In the advanced settings, you can disable the default setting *Detect file closing and apply user-specific check-in behavior.*

You can also define process-specific file formats that will be immediately checked-in when the new file with the extension in question has been saved and the metadata card has been completed.
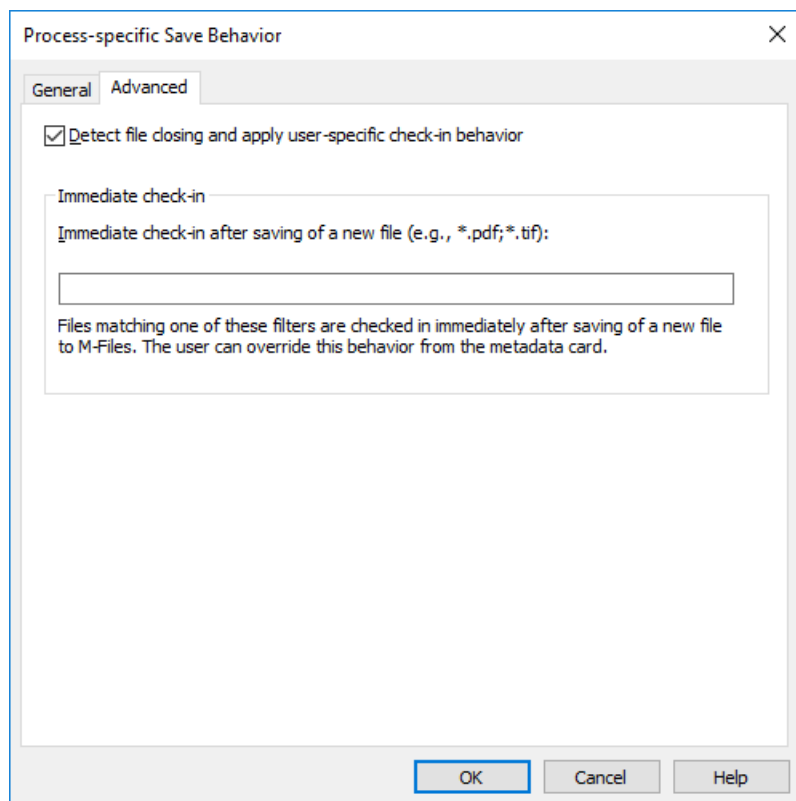
Figure 14: Advanced process-specific settings.

Offline mode

By default, the documents are kept ready for the offline state. If the workstation is never used offline, the documents need not be ready for the offline state. The selection can also be removed if the offline state is seldom used or seems to cause additional load for the machine.

Export Vault Connections and Settings

Document vault connections and settings can be exported to a Windows registry file.

By sharing and enabling the exported registry file on other computers, you will be able to use common M-Files configuration data on several computers.

The export options can be found on the *Settings* tab of the *M-Files Desktop Settings* component.

3.5. Installing M-Files Upgrades

The M-Files installer automatically detects the previous versions of the software and can migrate the settings from the old to the new version. Hence, do not uninstall any previous versions of M-Files before upgrading.

Perform the following tasks to upgrade M-Files with a higher version:

1. Execute the M-Files installer for the new version.
2. Select the "Simple upgrade" option.

With the "Simple upgrade" option selected, the setup automatically installs the same components that were installed in the earlier M-Files version. The setup installs the new version and transfers the M-Files settings along with all local data from the earlier version to the new version. Finally, the setup uninstalls the earlier version.

📄 **Note:** If you are upgrading to M-Files 2015.3 and both of the following are true:

- You have a document vault that contains documents either in the Chinese, Japanese, or Korean language.
- The selected primary or secondary language for the full-text search features of the vault is some other than Chinese, Japanese, or Korean. For more information, see *Creating a New Document Vault* on page 28.

In such a case, you should rebuild the full-text search index of the vault after the upgrade is complete so that the documents in the aforementioned languages are still retrievable by searching their contents. For instructions, see *Vault Maintenance* on page 230.

📄 **Note:** Speed and performance improvements in M-Files 2015.2 and newer can cause some empty virtual folders to appear in views in which empty folders are set to be hidden. Because of this, we recommend reading the document *Security Aspects to Consider When Upgrading to M-Files 2015.2* before upgrading your system.

📄 **Note:** In case you are upgrading from a version that is older than M-Files 2015, please note that the new installation includes significant improvements to the vault database structure. This means that – especially with large document vaults – the upgrade process might take substantially longer than usual. It is also recommended to ensure that the server computer has at least twice the amount of free space required by the metadata database file (*.fdb* file for Firebird and *.mdf* file for MS SQL Server databases). The database structure is upgraded automatically by the M-Files installer.

📄 **Note:** Property group and dynamic property configuration for M-Files 10.2 and M-Files 2015 has been replaced with more versatile configuration options in M-Files 2015.1 and later. See the document *Configuring the Metadata Card (M-Files 2015.3)* for more details.

Installation preconditions

- All M-Files Servers in a replication setup must have the same four-digit build number (for instance 11.2.**4320**.32 and 11.2.**4320**.33).
- M-Files Admin and M-Files Server must have the same four-digit build number (for instance 11.2.**4320**.32 and 11.2.**4320**.33).

📄 **Note:** M-Files Desktop is not compatible with Windows XP from the M-Files version 10.0 onwards. See *Upgrade Instructions for Organizations Using Windows XP* on page 46 for more information.

You can use the following table to verify M-Files Server–Client/Desktop compatibility:

	M-Files Client 9.0	M-Files Client 10.x	M-Files Desktop 2015, 2015.1, 2015.2, and 2015.3
M-Files Server 9.0	Compatible	Compatible	Not compatible
M-Files Server 10.x	Compatible	Compatible	Compatible
M-Files Server 2015, 2015.1, 2015.2, and 2015.3	Compatible	Compatible	Compatible

📄 **Note:** To verify compatibility with M-Files API and replication, see *M-Files version compatibility regarding API and Replication*.

Installation order

You can choose to either first upgrade the client computers and then the server computer, or first the server computer and then the client computers. If you do not upgrade to the immediately subsequent M-Files version, make sure that the new version is compatible with the old version to avoid unplanned interruptions (see the compatibility chart above).

> 📄 **Note:** Some of the new properties of the higher M-Files version may not be available until both the M-Files Client/Desktop and M-Files Server have been upgraded to the new version.

Preparing for the server upgrade

Before installing the upgrade on M-Files Server, make sure that your server fulfills the hardware and software requirements of the new version (see *System Requirements and Technical Details* on page 21).

The administrator should also ensure that recent backups of the document vaults are available. The backups may be useful should an unexpected fault situation occur during the server upgrade.

In the event of a fault situation, contact M-Files customer support immediately. Do not attempt to rectify the fault, as solving the fault situation is usually much easier if no additional actions have been performed.

Service Releases

Service releases are smaller M-Files software upgrades that share the same main version number (for example "11.0" for M-Files 2015), followed by the four-digit version ID for the service release. For instance, versions 11.0.**4300**.47 and 11.0.**4300**.58 are service releases for M-Files 2015 (11.0.4300.27). Usually, the service releases do not contain any new properties, but rather are released if faults requiring repair are detected in the software, or if compatibility with higher versions of other software requires changes to M-Files.

Service release versions are fully compatible between each other and can be installed in whichever order. In other words, whether the service release is installed first on the workstations and then on the server, or vice versa, makes no difference.

Automatic Updates

Automatic Updates is a program that keeps your M-Files software up to date. If a newer version of M-Files covered by your M-Files subscription becomes available, it is downloaded to your computer and you are notified about it. New M-Files versions normally become available as automatic updates about a month after a new version has been officially released.

> 📄 **Note:** See *Installation preconditions* on page 44 for ensuring version compatibility.

Disabling the updates

You can open the automatic updates control panel via your Windows start menu or the M-Files icon in your Windows notification area. If you wish to disable automatic updates, you can do so by unselecting the *Check for updates automatically* checkbox on the *Settings* tab. Administrators can disable automatic updating altogether by using a modified installation package. For more information, refer to *M-Files Setup: Advanced User's Guide*.

Checking for updates manually

You can check for updates manually by clicking the **Check now** button on the *Installation* tab.

Upgrading the M-Files OCR Module for Versions M-Files 2015 and Later

M-Files Server versions for M-Files 2015 and later do not support the OCR module of the M-Files versions prior to M-Files 2015, so you might need to upgrade this module after upgrading the server software. See *Instructions for enabling the M-Files OCR Module* for detailed instructions.

Centralized Deployment via Group Policy

You can use the Windows Group Policy feature to automatically distribute M-Files to client computers. Alternatively, you may use any other centralized deployment mechanism that you are familiar with. You can also customize the behavior of the M-Files setup program. For further information on these options, refer to *M-Files Setup: Advanced User's Guide*.

Upgrade Instructions for Organizations Using Windows XP

M-Files Desktop is not compatible with Windows XP computers from the M-Files version 10.0 onwards. Organizations with both Windows XP and newer Windows client computers (Vista/7/8/8.1) are suggested to leave the 9.0 Client version on XP computers and upgrade Windows Vista/7/8/8.1 clients to the newest version.

The only compatibility issue in the mixed environment with M-Files 9.0 and newer clients is that inserted properties added with the newer client versions to MS Office and AutoCAD files cannot be resolved on M-Files Client 9.0. This compatibility issue may cause issues with metadata structure replication as well.

When using the *Insert Property* feature with M-Files Client 10.x, M-Files Desktop 2015, and newer client versions, the reference to the property value is made by using the property GUID. In M-Files 9.0, the references are made by using the property ID.

To resolve the issue on these mixed environments, the newer client versions can be enforced to make references to property definitions using the property ID. This configuration can be done by adding the following registry settings on each client computer with M-Files 10.x or later installed:

Force the compatibility setting to all vaults (MS Office)	
Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Client\MFOfficeAddin`
Name	`UseIDBasedPropertyReferences`
Type	DWORD
Value	1 (default = 0)

Force the compatibility setting to all vaults (AutoCAD)	
Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Client \MFAutoCADAddin`
Name	`UseIDBasedPropertyReferences`
Type	DWORD
Value	1 (default = 0)

Force the compatibility setting to a specific vault (MS Office)	
Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Client\MFOfficeAddin \Vaults\<vault GUID>`
Name	`UseIDBasedPropertyReferences`
Type	DWORD
Value	1 (default = 0)

Force the compatibility setting to a specific vault (AutoCAD)	
Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Client \MFAutoCADAddin\Vaults\<vault GUID>`

Force the compatibility setting to a specific vault (AutoCAD)	
Name	`UseIDBasedPropertyReferences`
Type	DWORD
Value	1 (default = 0)

📄 **Note:** Vault-specific settings have precedence over the client-specific settings.

Installation sequence

1. Deploy the registry settings described above on all the Windows Vista/7/8 client computers.
2. Upgrade M-Files Client/Desktop on Windows Vista/7/8 workstations to the newest version.
3. Upgrade M-Files Server to its newest version.

4. Exploring the Document Vault

At this stage, the following steps should have been completed:

• *M-Files Server* has been installed in your organization.
• Your organization's M-Files system administrator has created a *document vault* on page 28, *login accounts* on page 30 and *users* on page 31.
• The document vault has been set up on your computer with *M-Files Desktop Settings* on page 35.

You should now be able to start using your M-Files vault by clicking the icon on your desktop, by using the Windows Start menu, or via the virtual M-Files drive (as seen below). *Explore M-Files* can also be opened via the M-Files icon in the Windows notification area.

> 📄 **Note:** The virtual M-Files drive does not, in fact, take up any space from your actual hard drive. Windows requires drives to report their capacity and the amount of free space available in Windows Explorer. The default reported size of the M-Files drive is 1 terabyte, and the amount of reported free space is 90 percent.
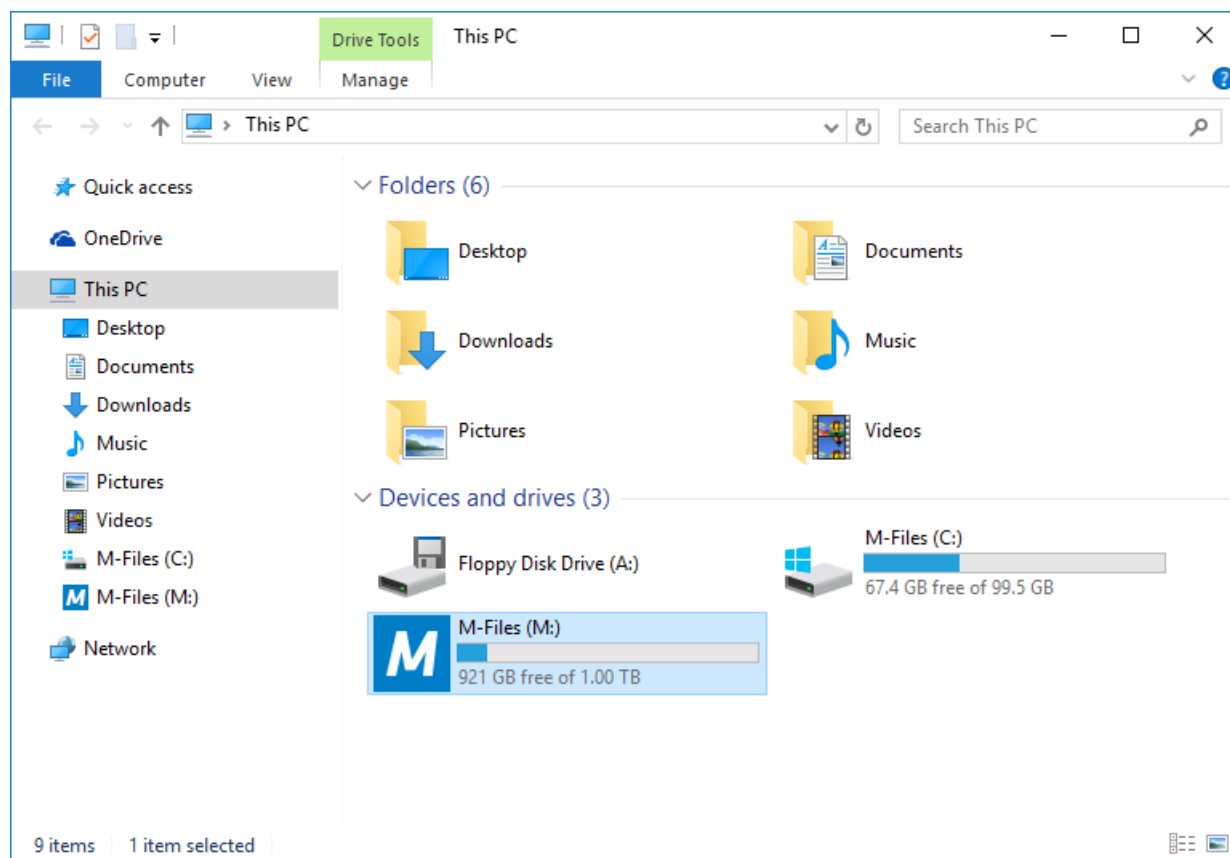
Figure 15: The virtual M-Files drive in File Explorer.

4.1. Using M-Files Desktop

For instructions on installing M-Files Desktop, refer to *Installing the Software* on page 26.

Once M-Files Desktop has been installed and your vault connections are set up via *M-Files Desktop Settings* on page 34, you should be able to see all the vault connections on your M-Files drive (for instance via the File Explorer).

Logging in

You can log in by double-clicking the vault. If you want to log in to the document vault as a different user than the default one, select the *Log In As* function from the document vault context menu. Unless you have already logged in during Windows login, the system prompts for your credentials upon opening the vault.

> 📝 **Note:** M-Files can be configured to use single sign-on (SSO) with various solutions for federated authentication. Using SSO promotes productivity by reducing password fatigue and time spent on re-entering login credentials. For more information, refer to *Using Federated Authentication with M-Files*.

The M-Files Desktop user interface

The M-Files Desktop user interface is composed of four main components: the task area, listing area, right pane and search bar.

▶ Video: *M Files User Interface*
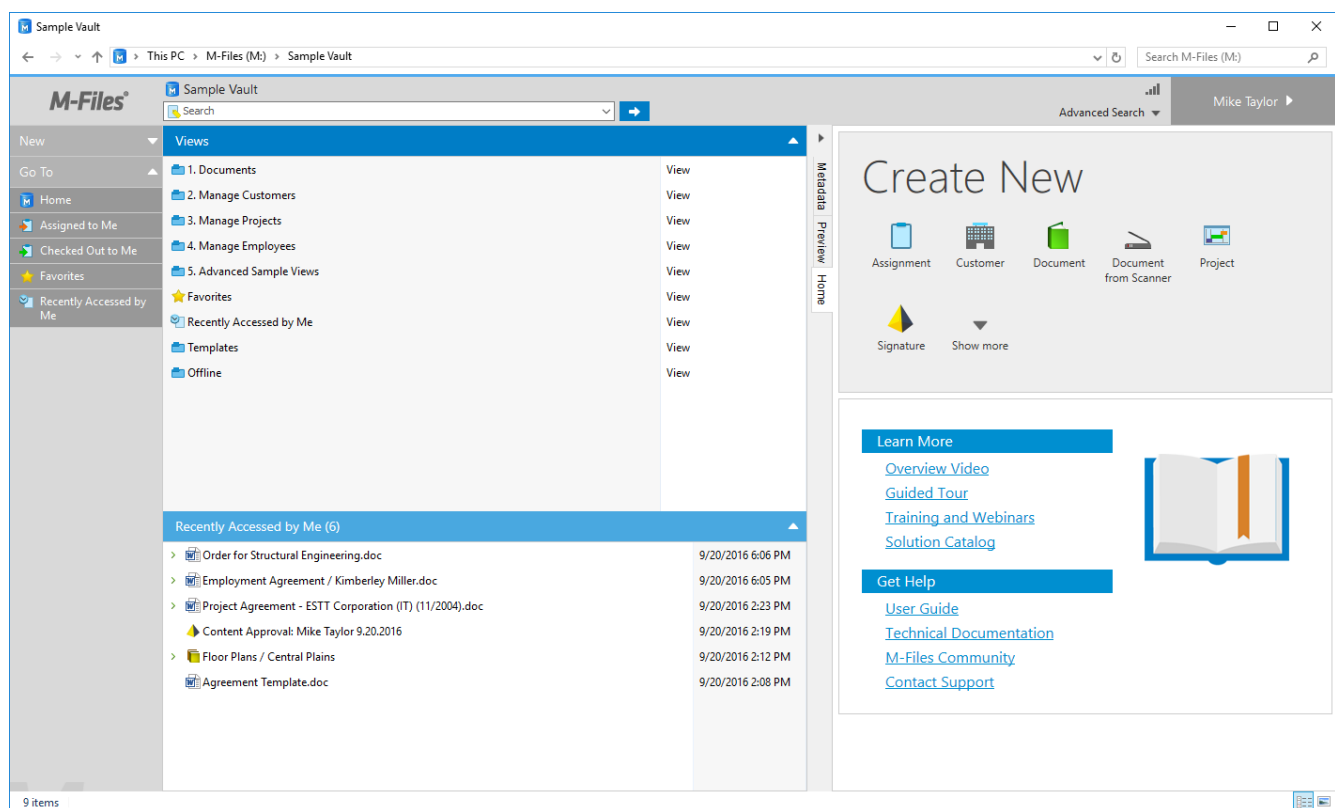
Figure 16: The M-Files home view.

Task area

The task area is located on the left side of the window. By default, it contains options for creating new objects (*New*) as well as a *Go To* section for quickly navigating to useful views, such as the *Favorites* and *Recently Accessed by Me*.

Listing area

The listing area in the center normally contains views and objects. The area functions very similarly to the one in File Explorer. In *M-Files Desktop*, however, users can expand/collapse objects to view and hide, for instance, the content of an M-Files multi-file document.

If the listing exceeds the number of objects to be displayed in a single listing, the option **Show more results** is shown in the grouping title. By clicking this option, you can enter the *paginated view* on page 53.

> 📝 **Tip:** You can quickly browse objects in the listing with your keyboard. Just select your preferred tab for the right pane (for instance the *Preview* tab), and start browsing with the up and down arrow keys.

> 📝 **Note:** Some of the item names in the listing view may be displayed in gray text. This means that the full item path is too long for Windows (more than 259 characters) and that parts of it should be renamed to make the content function properly.

Right pane

When no object has been selected in the home view, the right side of the window displays quick access to creating new objects along with the *Learning Resources* section. When an object is selected, the right side of the window displays the metadata and preview panes (see *Metadata Card* on page 53) by default, but can also contain customized content and be modified according to individual needs.

Search

The search functions are located on top of the user interface. For more information on the functionality of the search bar, see *Search Functions* on page 139.

Right above the search word field, there is a breadcrumb indicator displaying the vault and the view that you are currently in. The breadcrumb can be, for instance, *Sample Vault > Document > By Customer > A&A Consulting*.

The top right corner of the interface displays the name of the user logged into the vault. Clicking this area opens a menu for logging out of the vault, using M-Files in offline mode, as well as for opening settings for notifications, languages, your M-Files password and substitute users.

Figure 17: An overall view of the M-Files user interface with the metadata positioned at the bottom and the preview on the right side.

The M-Files Desktop user interface can be customized according to various user requirements. For example, users can change the position of the metadata card on the user interface.

Connection Status

The connection status icon (📶) in the upper right conrner to the left of the username displays the status of your connection to the document vault by measuring the round-trip time to the server that hosts the vault. The icon has five different statuses:

- 📶 The round-trip time to the server is less than 50 milliseconds.

- 📶 The round-trip time to the server is from 50 to 149 milliseconds.

- 📶 The round-trip time to the server is from 150 to 299 milliseconds.

- 📶 The round-trip time to the server is 300 milliseconds or more.

- 📶 You have no connection to the server.

To display additional information about your connection, click the connection status icon (📶) to display the **Connection Status** dialog:
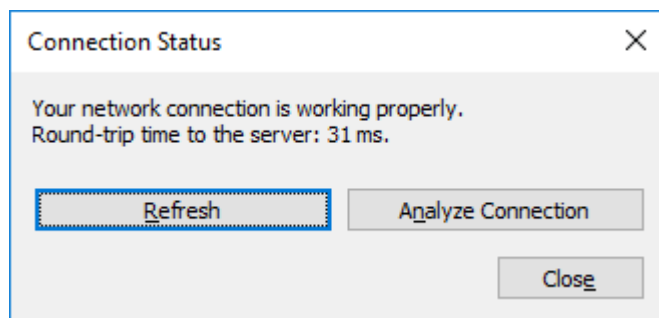
One of the following messages is displayed in the dialog:

- Your network connection is working properly.
- Your network connection is slow.
- No connection to the server or the server is unavailable.

If your connection is slow or you have no connection to the server, contact your M-Files system administrator. You can click **Refresh** to refresh the information regarding your connection status. Clicking **Analyze Connection** shows you additional details about your connection status.

Task Area

The left side of the user interface (task area) contains a number of context-sensitive shortcuts:

Under the *New* title, you can find quick links for creating new objects by object type.

Under the *View and Modify* title, you can select object-specific operations, such as *Check in/out* or *Make Copy*, to be performed. You can add new shortcuts to the list by right-clicking an empty space on the task area and selecting a shortcut from the *Commands* list.

The *Go To* title lists a number of pre-defined links to the most commonly used views, such as *Favorites* and *Checked Out to Me*.

In addition, you can add new shortcuts under the *Go To* section yourself. To add a shortcut to the selected view or virtual folder, right-click on it and select *Add Shortcut to Task Area*. To add an object to the list, select the object, open the menu bar with the *Alt* key on your keyboard, and select **Operations** > **Add Shortcut to Task Area**.

You can rename, delete, and organize shortcuts on the task area using the right mouse button.

You can also define *common task area settings*, although this requires you to at least *Manage common views and notification rules*. At the same time, you can also delete *users' custom task area settings* to immediately activate the common settings. Alternatively, the common settings can be activated by restoring the common default settings. The user can also restore the *M-Files software default settings*.

You can open and close the quick links below each title by clicking the arrowheads in the title.

Favorites

In addition to *My Views* and task area shortcuts, you can add documents and other objects to favorites. Favorites are user-specific.

You can add objects to favorites and remove them via the *Operations* menu, the context menu, or via the object's metadata card.

> **Note:** You cannot delete favorites with the *Delete* function.

You can conveniently access your favorites via the quick link in the task area.

Shortcuts for changing the workflow state

You can change the workflow state directly via the quick links in the task area. The various workflow states are available for selection under the *Move into State* title. You can move the object to the desired state simply by clicking the state. If you wish, you can add a comment about the state change at this point.

> **Note:** The *Move into State* title and the various workflow states are displayed in the task area only if the object has an associated workflow for whose state changes the user has the required permissions.

You can also change the state by clicking the workflow name or state control in the metadata card.

Listing Area

Grouping views on the main level

The main-level views have been grouped into *My Views*, *Common Views* and *Other Views*. In addition, traditional folders are in a separate group. This makes it easier for the user to distinguish among these different views and navigate to *My Views*. Also, the regular user often does not have the permission for editing common views, so grouping common views separately clarifies the distinction between common views and the user's own views.

It is also possible to display predefined views, such as *Favorites*, *Assigned to Me* or *Recently Accessed by Me*, at the bottom of the listing view.

Related objects listed below the main object

Objects related to a particular object can easily be browsed directly from the view or from the search result by means of the expand/collapse arrow buttons. M-Files shows all related objects below the main object. This allows you to easily browse, for example, documents and contact persons related to the project, directly from the listing view.

Grouping titles

Related objects are automatically grouped by object type or by property definition. This allows you to find the desired document or other object quickly and easily. For example, if you are looking for contact persons related to the project, you can find them easily under the grouping title *Contact persons.*

Sorting by columns

You can change the sort order the objects in the listing area by clicking a specific column heading in the listing area. The objects can be sorted, for example, alphabetically, in the order of relevance or by date. Clicking the column heading once more changes the sort order from ascending to descending, or vice versa. By holding down the *CTRL* key and clicking another column heading, you can select secondary, tertiary and further sortings orders. You can add more columns to the listing area by right-clicking on the column heading area and selecting **Choose Columns...** from the context menu.

▶ Video: *Column Settings*

Listing pagination

If the listing exceeds the total number of objects allowed to be displayed in a single listing, the option **Show more results** is shown in the grouping title. By clicking this option, you can enter the paginated view.

The paginated listing displays the range and total number of objects matching your search criteria or view filter, as well as the commands **Previous** and **Next**.

You can change the number results shown per page via the *Display Mode* options:

1. Open either the context-menu for an empty area in the listing view, or the menu bar by pressing *Alt* on your keyboard.
2. Select **Display Mode** from the list (or **View** > **Display Mode** via the menu bar).
3. Select **Objects per Group**.
4. Select any of the options in the list.

Metadata Card

By default, the metadata card and the preview pane are positioned on the right side of the user interface. The size of the right pane can be adjusted according to different user needs and preferences.

Figure 18: Metadata card on the right side of the user interface.

The metadata card comprises the following elements (from top to bottom):

- Title area
- Option ribbon
- Property listing
- Permission/workflow controls

The title area displays the name, type, ID and the M-Files version of the object, as well as information on the creation and modification dates.

The option ribbon enables various object and metadata card related actions. These actions are presented in more detail further below.

The property listing area displays all the object's properties, property groups, as well the option for adding new properties. See *Properties* on page 81 for instructions on adding and editing properties.

> 📝 **Note:** M-Files can be configured to use dynamic properties as well as property groupings. Dynamic properties enable administrators to define "trigger" properties that, when set, automatically generate additional properties to the metadata card. Property groupings can be used to group properties together on the metadata card in order to better organize the metadata cards of objects that contain a large number of properties. See *Metadata Card Configuration* on page 398 for more information.

The ribbon below the properties area enables you to modify the permission settings of the object, as well as to assign and change workflows and workflow states. For further information, see *Permissions* on page 84 and *Workflow* on page 116.

Metadata card option ribbon

There are four icons in the ribbon below the title of the object, a flag, a star, a cogwheel and an arrowhead.

With the flag icon, you can mark the object as *followed* or *unfollowed*. When the object is marked as *followed*, you get an email notification when the object is modified.

Clicking the star icon toggles the inclusion of the object in your *Favorites* view.

The cogwheel icon opens a list of options, including the options for changing the metadata card location and detaching the metadata card into a new window (*Pop Out the Metadata Card*).

By clicking the arrowhead, you can toggle the compact view of the metadata card on or off.

Figure 19: The options ribbon on the metadata card.

"Follow this object" functionality

When the functionality *Follow this object* or *Follow this document* is active, M-Files sends you an email message when the object or document is modified.

These changes are:

- The metadata or the file content of the followed object is modified.
- The followed object is deleted or destroyed.
- The metadata or file content of an object or a document related to the followed object is changed. For instance, a document related to a project is modified.
- A document or an object related to the followed object is created, deleted or destroyed.

  📝 **Note:** The person who modified the object will not receive a notification.

Positioning the metadata card

In some cases, such as when working with views that show multiple columns in the listings, or when working with a smaller screen, it makes more sense to show the metadata card in the bottom pane. You can change the position of the metadata card to the bottom pane by opening the context menu in the *listing view* on page 52 and selecting **Display Mode** > **Show Metadata in Bottom Pane**. Alternatively, you can do this by clicking the

Settings icon (the cogwheel) on the metadata card and selecting *Toggle Metadata Card Location*, or by opening the context menu of the *Metadata* tab. You can also hide the right pane altogether by clicking the arrowhead above the topmost tab.

Comments view

The comments view can be accessed by selecting the *Comments* icon on the metadata card. This view presents all the comments related to the object in chronological order, as well as the option to add new comments.

> 📄 **Note:** Comments retain their permission settings. This means that they are visible only to the users defined in the permission settings that were in use when the comment was added.

Selecting the *Properties* icon from the comments view brings you back to the properties view.

Preview

You can activate the preview by opening the *Preview* tab of the right pane. If the pane is not enabled, you can display it by opening the context menu in the listing view and selecting **Display Mode** > **Show Right Pane**.

You can also use the metadata card in a separate window by using the *Pop Out* control located in the **Settings** menu (the cogwheel icon) of the metadata card. This functionality allows you to view and edit several metadata cards in parallel and also to view the document metadata and the preview window side-by-side.

Once the metadata card has been detached from its default position, it can be operated as any normal window in the user interface.
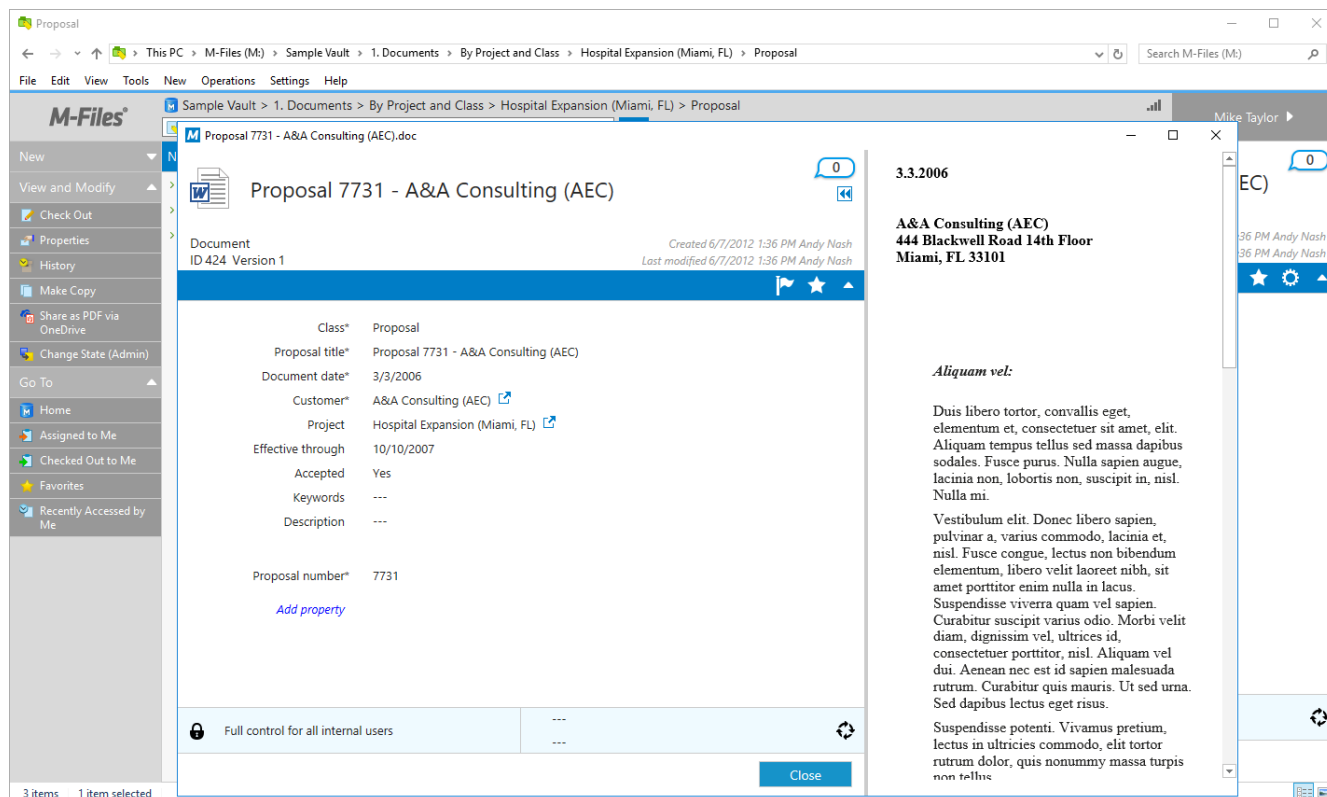
Figure 20: Metadata card in detached mode with document preview.

In the preview mode, you can easily browse and copy document content. You can preview for instance Word, Excel, PowerPoint, PDF, and AutoCAD files. The preview is possible if the software supporting the relevant file format has been installed on your computer. For example, preview for Microsoft Office files requires Microsoft Office 2007 or higher, and preview of PDF files requires Adobe Reader 8 or higher.

> 📄 **Tip:** When you are transferring files to M-Files, the preview function makes it easier to fill in the metadata.

Contents of the following types of files can be viewed in the **Preview** tab:

- Email files (eml, emlx, msg)
- HTML and web archive files (htm, html, mht, mhtml)
- Image files (tif, tiff, jpg, jpeg, bmp, gif, png)
- Microsoft Excel files (xlsx, xlsm, xltx, xltm, xlsb, xls, xlt)
- Microsoft PowerPoint files (pptx, pptm, ppsx, ppsm, potx, potm, ppt, pps, pot)
- Microsoft Word files (docx, docm, dotx, dotm, doc, dot)
- OpenDocument files (odt, ott, ods, odp)
- PDF files
- RTF files
- Text files (txt)
- Visio Drawings (vsd, vdx, vss, vsx, vst, vtx, vdw)

Efficient Use of the Metadata Card

The metadata card can be fully operated with your mouse (except for typing in values, of course), but there are also several ways for you to optimize the process of filling in the metadata by using your keyboard. The aim of this chapter is to make you even more proficient in using the metadata card, which is essentially one of the key components of the M-Files user interface.

First, you can use the Tab ⇆ key to move from one property field to the next. You can also go back to the previous field by pressing ⇧ Shift + Tab ⇆.

You can add and remove fields via the toolbar shown above the active field by using your mouse, but it might be faster to use the keyboard shortcuts: use Ctrl + I to add a new field, Ctrl + D to delete the selected field, or Ctrl + N to add a new value to the value list.

As a recap, here are the shortcuts in a table:

Keyboard Shortcut	Description
Tab ⇆	Move to the next property field.
⇧ Shift + Tab ⇆	Move to the previous property field.
Ctrl + I	Insert a new value field for a property.
Ctrl + D	Delete the selected property field.
Ctrl + N	Add a new value to the value list and set it as the property value.
↑ / ↓	Move between available property value options.

4.2. M-Files Shortcuts

These keyboard shortcuts can be used when the listing area is active:

Quick Search	Ctrl + F	See *Quick Search* on page 141.
New Document	Ctrl + N	See *New Document* on page 80.

These shortcuts are available when an object has been selected on the listing area:

Check Out	Ctrl + O	See *Check Out* on page 107.

Check In	Ctrl + I	See *Check In* on page 110.
Check in with comments	Ctrl + ⇧ Shift + I	See *Check In* on page 110.
Relationships	Ctrl + L	See *Relationships* on page 113.
Collection members	Ctrl + ⇧ Shift + L	See *Collection Members* on page 115.
Comments	Ctrl + M	See *Comments* on page 116.
Subobjects	Ctrl + J	See *Subobjects* on page 115.
History	Ctrl + H	See *History* on page 111.

For the available shortcuts while editing the metadata card, see *Efficient Use of the Metadata Card* on page 57.

4.3. Creating a Document

You can create documents just like before, and *save them directly to the M-Files drive* on page 61.

You can also create a document using the **New Document** function in the M-Files task menu (or by pressing Ctrl + N in the M-Files user interface). The new document creation wizard helps you select the right template and class for the new document. Templates can also be searched by typing a search term. The search will display all templates and file formats that match to the search criteria, and highlight the results.

▶ Video: *Creating Documents*
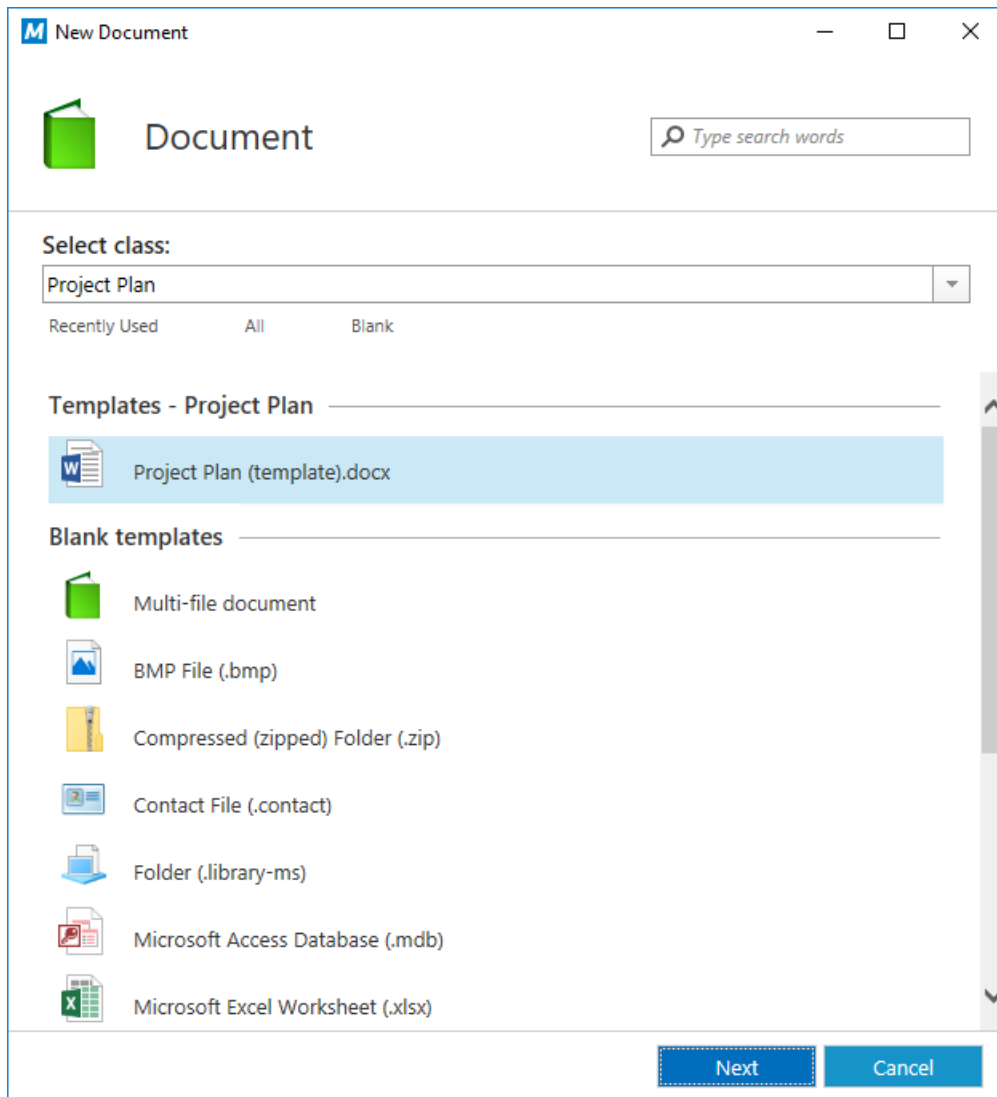
Figure 21: The new document creation wizard.

Selecting *All* displays all templates and file formats that are defined for the vault in question. The *Recently Used* option shows all the templates you have recently accessed. Recently used templates are also shown by default when you open the template selection wizard. The *Blank* option shows all the file formats that can be selected for a new document.

These predefined options are followed by a list of classes that can also be used for the template selection. Selecting a class displays the templates that are available for that class.

After you have selected a template or a blank document, a metadata card for the new document opens and you can start editing the properties. Properties marked with an asterisk (*) are mandatory.

> 📄 **Tip:** You can use keyboard shortcuts while editing the metadata. See *Efficient Use of the Metadata Card* on page 57.

Figure 22: The metadata card of a new document.

Selecting **Create** saves the document and adds the object to the vault. Selecting *Open for editing* makes sure that the document is checked out to you for editing until you manually check it in, and opens the new file in a suitable application for editing. If you have selected *Check in immediately*, the document will be available for others right away. Selecting **Cancel** discards all the changes and closes the dialog.

When you create a document in some other application, you fill in the metadata card only when you save the document in the document vault on the M-Files drive.

> 📄 **Tip:** When filling in the metadata card, you can specify the *permissions* on page 84 for the document in the *Permissions* field. This way, you can specify who can view, open, or edit the document.

Example: A New M-Files Document

1. Open M-Files Desktop and navigate to a vault.

   ℹ By default, your active M-Files vault connections are located in Windows Explorer under the M-drive.

2. Select **New** > **Document** via the task area on the left side of the user interface.

   ☑ The **New Document** wizard should be opened.

3. Either:

    a. Enter a search term to the search field and select a template based on the search results.

       or

    b. Select a class from the **Select class** drop-down menu and then a template belonging to the selected class.

       or

    c. Select a template via the **Recently Used**, **All**, or **Blank** quick lists.

4. Click **Next**.

    ☑ A **New Document** dialog should be opened.

5. Enter a name for the document.

6. At minimum, enter values to the mandatory metadata fields (marked with an asterisk).

    ⓘ You may want to add additional metadata fields by clicking the **Add property** command below the last metadata property on the list.

7. Define permissions for your document.

    ⓘ For more infomation on setting document permissions, see *Permissions* on page 84.

8. Select a workfow and a workflow state for the document.

    ⓘ For more information about workflows, see *Workflows* on page 313.

9. Either:

    a. Select **Open for editing** if you want to modify the content before making the document public.

       or

    b. Select **Check in immediately** if you are planning on adding the content later on, or having someone else add it.

10. Select **Create**.

Your newly created document has been added to the vault. If you chose **Check in immediately** in the ninth step, the document is also visible to others, according to your permission settings.

4.4. Saving in M-Files

When using M-Files, you no longer save documents in a single folder but on the M-Files drive, which can be found on your computer like a hard drive. You do not need to specify any other location than the document vault, as M-Files locates the document in the correct views on the basis of the metadata you define in the metadata card.

▶ Video: *Saving Documents*

You can save the documents directly to M-Files from the applications that you use. The new save location is the document vault.
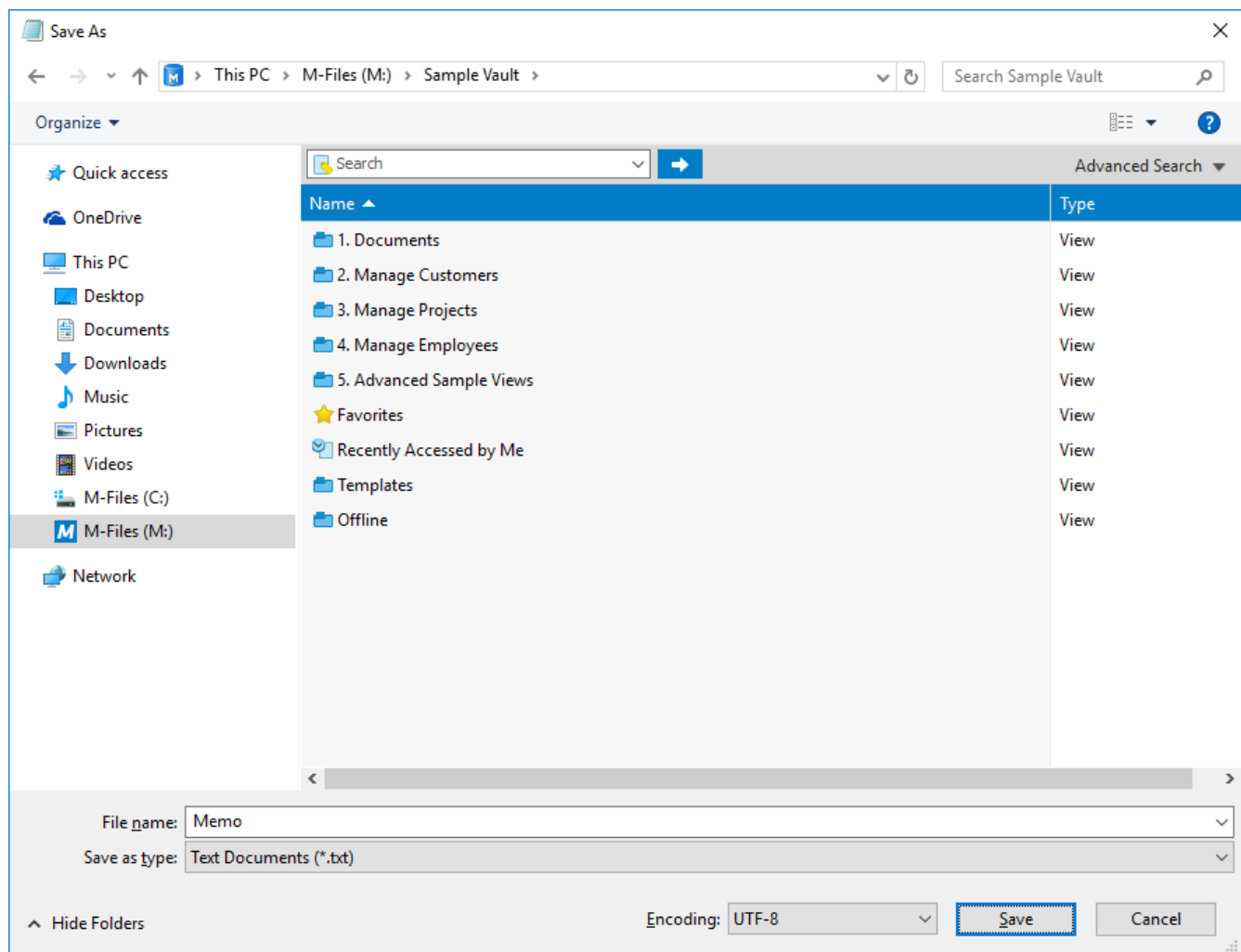
Figure 23: Saving a document to a document vault.

📄 **Tip:** On the left side of the save dialog, there is a quick link to M-Files.

Below are some examples of how you can save your work directly from an application to M-Files. The first example applies to virtually every desktop application. The second example applies to Office products (Office 2007 and newer).

Example: Saving a PowerPoint Presentation to M-Files

1. Open PowerPoint and create a new presentation or open an existing one.

2. Once your presentation is ready, select **File** > **Save As** > **Computer** > **Browse**.

   ✅ The **Save As** dialog is opened.

3. On the left pane of the **Save As** dialog...

   a. Click the **Computer** location and and on the right pane, double-click **M-Files**.

   or

   b. Click the arrow next to **Computer** to expand the location and click **M-Files**.

4. Double-click the vault where you want to save your presentation.

5. Enter a file name for your presentation in the **File name** field.

6. Click **Save**.

   ☑ The **New Document** dialog is opened.

7. Select an appropriate class for your presentation from the **Class** drop-down menu.

8. Optional: Enter other optional property values.

   ⓘ Click **Add property** to add additional properties.

9. Click **Create**.

Your presentation is saved to M-Files.

Example: Saving a PowerPoint Presentation to M-Files by Using the M-Files Tab

1. Open PowerPoint and create a new presentation or open an existing one.

2. Once your presentation is ready, select the **M-Files** tab on the PowerPoint ribbon.

3. Click **Save to M-Files**.

4. In the drop-down menu that opens, click the vault where you want to save your presentation.

   ☑ The **New Document** dialog is opened.

5. Select an appropriate class for your presentation from the **Class** drop-down menu.

6. Optional: Enter other optional property values.

   ⓘ Click **Add property** to add additional properties.

7. Click **Create**.

Your presentation is saved to M-Files.

4.5. Checking In a Document

Even when you have saved and closed a document, it will remain *checked out* to you until you *check it in*. Select the document you have created and check the document in by selecting the *Check In* function from the task area. This enables others to edit the document.

📄 **Tip:** You can simultaneously check in all documents that you have checked out from the *Checked Out to Me* view. The shortcut for checking in a document is Ctrl + I.

4.6. Deleting a Document

If you want to delete a document, right-click the document and select **Delete** from the context menu. The document is not lost permanently, but it becomes *deleted* and can still be found by performing a detailed search (see *Deleted* under *Status* on page 148).

Please note, however, that you can see deleted documents only if you have the appropriate permissions. If you have the system administrator permissions, *full control of vault* or the right to *see and read all objects (including deleted ones)*, you can use a view that shows all the deleted documents. Refer to *New View* on page 90 and *Undelete* on page 119.

📝 **Tip:** If you want to remove a document permanently, right-click a deleted document and select **Destroy**. Alternatively, when you are deleting a document, you can activate the *Destroy permanently* checkbox.

4.7. Creating and Completing Assignments

Assignments transfer information and responsibility for task execution to the correct person. The assignment function can be used, for instance, to request a colleague to look over a proposal before it is sent to the customer.

Assignments can be included in a workflow, or they can be independent. For more information on automatic assignments included in workflows, refer to *Workflows* on page 313.

To submit a new assignment, create a new *Assignment* object. Because assignments are objects, you can define the same assignment for several objects. Or, inversely, add several different objects to the same assignment. For example, you can assign several drafts to a colleague for inspection with a single assignment.

Because the assignments are separate objects they have their own version history and permissions. For this reason, the document and assignment included in it can have separate permissions. Thus, only a user who has reading rights to the document can mark the assignment completed. The user does not have to have rights to edit the document. Users with a read-only license to M-Files can also mark the assignment completed.

▶ Video: *Assignments*

You have three ways to create an assignment:

* Create an assignment and add objects to it either by dragging and dropping or by using the *Add File* function from the context menu.
* Highlight one or more documents and select *Assignment* from the *New* menu.
* Create an assignment without adding an object to it and define the entire task in the description field of the assignment.

Figure 24: The metadata card for a new assignment.

Assignment description

Add a free-form description of the task. The assignment notice by email displays the description to the person to whom the task was assigned.

Assigned to

Select the persons you wish to assign the task to. You can add more users by clicking the plus button (+) on the toolbar. Whenever an assignment is a separate object, all persons to whom the task was assigned must mark the assignment as complete before it is switched to the "complete" state.

Deadline

If desired, you can select a deadline for the assignment. The user gets an automatic reminder if he has not marked the assignment as completed when the deadline is approaching. The reminder will be sent using a common notification rule which can be deleted by the administrator.

The deadline can also be useful for creating views. The administrator or user can create a view to display objects whose deadline is approaching. For more information about views, refer to *New View* on page 90.

Monitored by

You can use the *Monitored by* field to define the users you wish to notify every time a task is marked as complete. The person submitting the assignment is automatically defined as a task monitor as soon as the object is saved for the first time. Once the property has been automatically or manually added to the metadata card, you can change or add more monitors by clicking the plus button (+) on the toolbar.

Mark as complete icon

You can mark the assignment complete by clicking the icon next to the *Assigned to* field.

Creating a New Assignment for an Existing Document

1. In M-Files, locate the document for which you want to create a new assignment.

2. Right-click the document and select **New** > **Assignment...** from the context menu.

3. In the **Name or title** field, enter a descriptive title for the assignment.

4. In the **Assignment description** field, enter a detailed description of the assignment to ensure that the assignee is properly informed about the details of the assignment.

5. From the **Assigned to** drop-down menu, select the person to whom this assignment is assigned to.

6. Optional: In the **Deadline** field, select a deadline date by which the assignment must be completed.

7. Optional: Via the workflow controls at the bottom of the **New Assignment** dialog, select a workflow for the assignment.

8. Click **Create** to create the assignment.

The new assignment appears in the **Assigned to Me** view of the assignee and they are informed by e-mail about the new assignment.

Creating a New Assignment for a New Document

1. In M-Files, select **New** > **Assignment** in the task area.

2. In the **Name or title** field, enter a descriptive title for the assignment.

3. In the **Assignment description** field, enter a detailed description of the assignment to ensure that the assignee is properly informed about the details of the assignment.

4. From the **Assigned to** drop-down menu, select the person to whom this assignment is assigned to.

5. Optional: In the **Deadline** field, select a deadline date by which the assignment must be completed.

6. Optional: Via the workflow controls at the bottom of the **New Assignment** dialog, select a workflow for the assignment.

7. Click **Create** to create the assignment.

8. Once the new assignment has been created, right-click the assignment in the listing area and select **Add File** and choose a suitable file format for the new file.

9. Rename the new file accordingly.

10. Optional: Double-click the newly added file to edit it.

The new assignment appears in the **Assigned to Me** view of the assignee and they are informed by e-mail about the new assignment.

Completing an Assignment

Once you have been given an assignment, you have to complete the tasks associated with the assignment and mark the assignment complete to indicate that you, the task assignee, have completed the assignment given to you.

1. In M-Files, locate and highlight the assignment that has been assigned to you.

    ℹ️ You can find all the assignments assigned to you in the **Assigned to Me** view.

2. Complete all the tasks required in the assignment.

3. Mark the assignment complete by doing one of the following:

    a. On the metadata card, click the ✓ (Mark complete) icon next to your name in the **Assigned to** field.

    or

    b. In the task area, select **View and Modify** > **Mark Complete**.

    or

    c. Right-click the assignment and select **Workflow** > **Mark Complete**.

4. Optional: Depending on the workflow settings of the assignment, you may still need to add an electronic signature to authorize the assignment completion.

The assignment is completed and it is removed from the **Assigned to Me** view.

Completing an Approval Assignment

Once you have been given an approval assignment, you have to complete the tasks associated with the assignment and mark the assignment either approved or rejected to indicate that you, the task assignee, either approve or reject the target of the assignment. You could mark an assignment rejected, for instance, if you consider the target document to be unpublishable.

1. In M-Files, locate and highlight the assignment that has been assigned to you.

    ℹ️ You can find all the assignments assigned to you in the **Assigned to Me** view.

2. Complete all the tasks required in the assignment.

3. Mark the assignment either approved or rejected by doing one of the following:

    a. On the metadata card, click either the ✓ or **X** icon next to your name in the **Assigned to** field.

    or

    b. In the task area, select **View and Modify** > **Mark Approved/Rejected**.

    or

    c. Right-click the assignment and select **Workflow** > **Mark Approved/Rejected**.

4. Optional: Depending on the workflow settings of the assignment, you may still need to add an electronic signature to authorize the operation.

The assignment is completed and it is removed from the **Assigned to Me** view. The user defined in the *Monitored by* property gets a notification e-mail of the approval or rejection.

4.8. Creating Other Objects

Besides documents, you can also create other objects like customers and projects. You can thus use M-Files to manage, for instance, your customer database by adding and editing customer objects in the document vault. Similar to documents, objects such as customers and projects have a metadata card, but they can exist without any files. They are also deleted and edited the same way as documents.

▶ Video: *Creating New Objects*

When you start creating a new object, the first thing you will see is the metadata card.

Figure 25: The metadata card for a new customer.

After you have entered the values for the mandatory fields (marked with an asterisk), the object can be saved by selecting **Create**. Selecting **Cancel** deletes the newly created object.

The *Check in immediately* option is selected by default to ensure that the new object is saved to the repository immediately after selecting **Create**. You can leave the object checked out to you if you plan to add additional metadata to it before saving the information to the vault.

Object types are defined using the M-Files Admin tool. For more information, refer to *Object Types* on page 259.

Example: Creating a New Customer

You must have a connection to a vault containing the customer object type.

1. Either:

   a. Right-click on an empty space in the listing area and select **New** > **Customer...**

      or

   b. Click **New** on the left-side task area, and then click **Customer**.

      or

   c. Press Alt to open the menu bar and select **New** > **Customer...**

   ☑ The **New Customer** dialog is opened.

2. In the **Customer name** field, enter the customer's name.

3. Optional: Enter other customer details in the available fields.

   ⓘ Click **Add property** to add additional customer properties.

4. Click **Create** once you are done.

A new customer object is added to M-Files.

4.9. Transferring Existing Files to M-Files

Transferring files to M-Files is very easy. Files can be transferred by dragging and dropping or by copying files or folders to the M-Files document vault.

If you transfer one file only, M-Files asks you to fill in a metadata card for the file, which makes the file a document. It is very important to understand the difference between a file and a document. An M-Files document consists of zero or more *document files* and *metadata*.

For instance, when transferring a folder with subfolders or several individual files at a time, M-Files is able to preserve the old folder structure. If you wish the folder structure to be preserved, the contents transferred are organized into *traditional folders* created in the document vault by M-Files. You can fill in the document property data while transferring or later on. For more information, refer to *Import Files and Folders* on page 104.

You can also use existing files directly from their original locations. This way, the additional properties provided by M-Files (such as version management) are available for these files, while they can still be used externally to M-Files. You can add metadata to the documents later on as necessary. For more information, refer to *External File Sources* on page 343.

Different databases can also be used and imported into M-Files. For example, the data in the customer database can be added to the M-Files metadata structure. This way the information does not have to be copied from one location to another. For more information, refer to *Object Types* on page 259 and *Value Lists* on page 269.

When you add metadata to documents imported to M-Files, these documents are displayed both in traditional folders and in M-Files dynamic views.

   📝 **Tip:** If you are transferring several individual files with the same metadata, such as the same customer, remember to ensure that the metadata you specify the first time will be used by default for the next files. You can do this when filling in the metadata card by checking the *Use these values as defaults for the next document* box (see the image below).
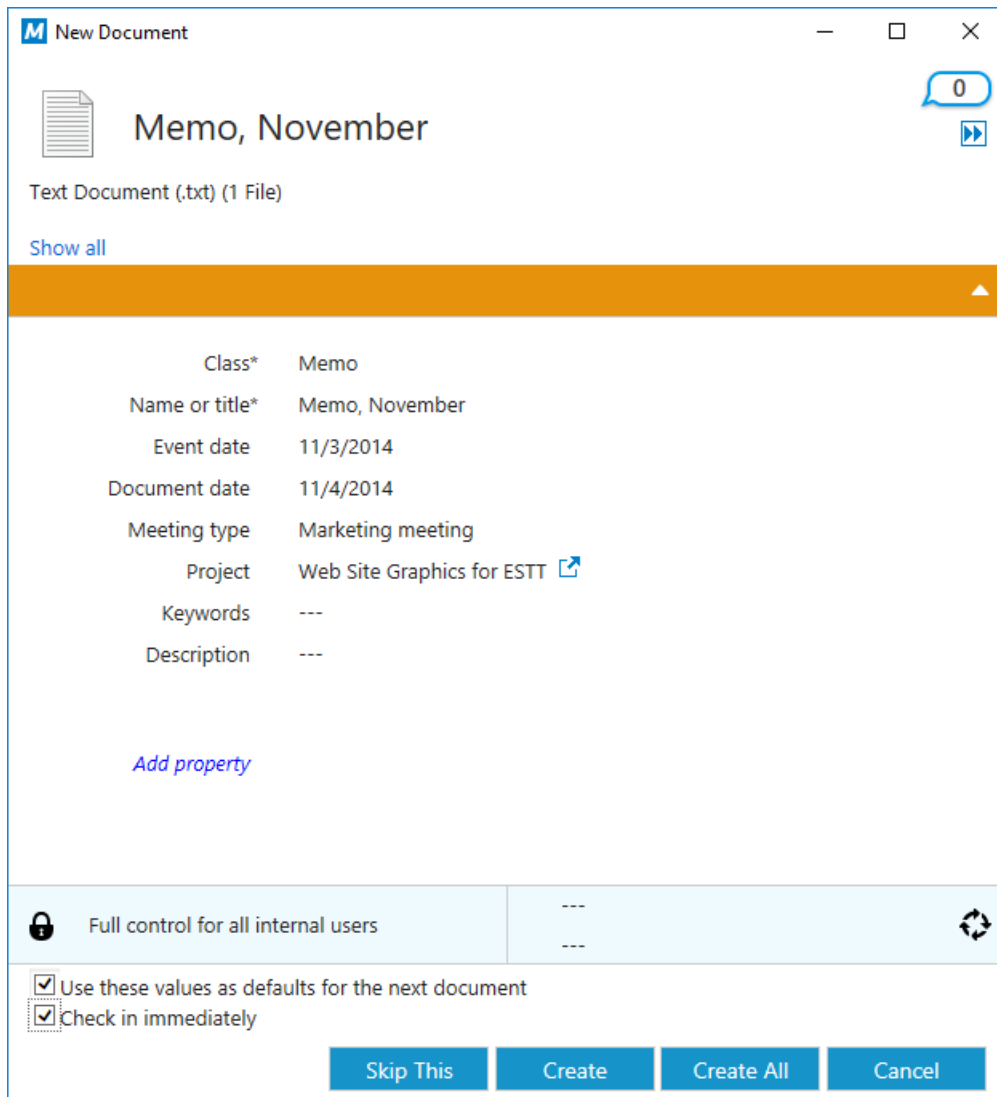
Figure 26: New Document window for a multi-file transfer.

> 📄 **Tip:** With the **Skip This** button, you can choose not to transfer a certain file. This is useful if you are transferring a large number of files and notice that you do not want to transfer one of the files after all.

Transferring Files to M-Files by Dragging and Dropping

1. Locate a file you need to transfer in File Explorer.

2. Select the file and drag and drop it to M-Files, onto an empty space in the listing area.

   ✅ The **New Document** dialog is opened.

3. Select an appropriate class for the file from the **Class** drop-down menu.

4. Enter other optional property values.

   ℹ️ Click **Add property** to add additional properties.

5. Click **Create**.

Transferring Files to M-Files by Copying and Pasting

1. Locate a file you need to transfer in File Explorer.

2. Right-click the file and select **Copy**.

3. Switch over to the M-Files window, right-click on an empty space in the listing area and select **Paste**.

   ☑ The **New Document** dialog is opened.

4. Select an appropriate class for the file from the **Class** drop-down menu.

5. Enter other optional property values.

   ⓘ Click **Add property** to add additional properties.

6. Click **Create**.

Transferring Folders to M-Files by Using the Import Files and Folders Dialog

1. In M-Files, press **ALT** to open the menu bar.

2. Select **New** > **Import Files and Folders...**

3. Click **...** to select the folder you want to import.

4. Select:

   a. **Do not preserve old folder structure** to discard the folder structure of the folder you are importing.

      or

   b. **Preserve old folder structure** to preserve the folder structure of the folder you are importing. You need to select a folder in M-Files for the content to be imported. You can create a new folder by clicking **New Folder**.

5. Optional: Uncheck the **Prompt for metadata** check box if you do not want to add metadata for the content you are importing.

6. Click **OK**.

   If you checked the **Prompt for metadata** check box, do the steps from 7 to 9 for every file you are importing.

7. In the **New Document** dialog, select an appropriate class for the file from the **Class** drop-down menu.

8. Enter other optional property values.

   ⓘ Click **Add property** to add additional properties.

9. Click **Create**.

The folder is imported to M-Files. If you chose the **Preserve old folder structure** option, the imported folder appears as a new traditional folder in M-Files.

4.10. Annotations and Redlining

You can add various comments and stamps, as well as draw arrows, boxes and other shapes to your documents. The feature supports most common file types, including Microsoft Word, Excel, PowerPoint and Visio documents, email files, RTF files, HTML and web archive files as well as OpenDocument files and PDF documents.

> **Note:** The annotations are not added to the documents themselves, but rather as detachable layers that can also be hidden if need be.

Activating the feature

The feature needs to be enabled via M-Files Admin. The options is vault-specific.

To enable the feature:

1. Open M-Files Admin.
2. Open the context menu of your document vault and select **Properties**.
3. Open the *Advanced* tab.
4. Enable the checkbox for *Annotations and redlining*.
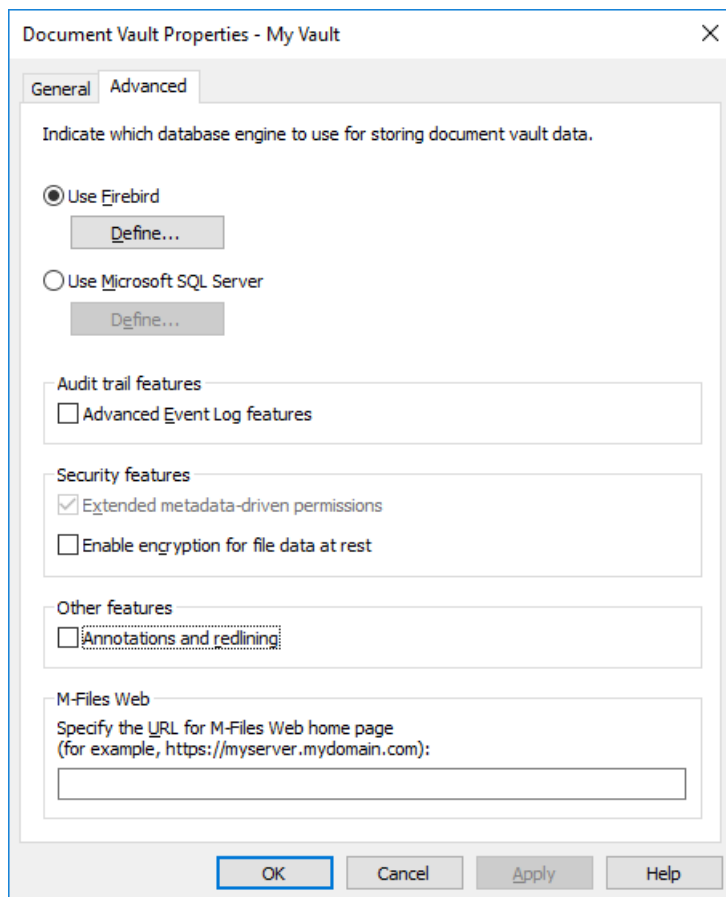
5. Select **Yes** in the confirmation dialog.
6. Select **OK** and close M-Files Admin.

The feature should be activated as soon as you have restarted M-Files Desktop.

▶ Video: *Activating Annotations*

Annotation objects

Your annotations are saved as separate *Annotation* objects under the main document. M-Files automatically creates these objects every time your start creating new annotations. Annotation objects contain an XFDF file (XML Forms Data Format) that basically tells M-Files the type, form, and location of your annotations.

Creating and editing annotations

Please see the topic *Using Annotations* on page 73 for instructions on adding and editing annotations.

Supported file formats

This feature supports the following file formats:

- Email files (eml, emlx, msg)
- HTML and web archive files (htm, html, mht, mhtml)
- Image files (tif, tiff, jpg, jpeg, bmp, gif, png)
- Microsoft Excel files (xlsx, xlsm, xltx, xltm, xlsb, xls, xlt)
- Microsoft PowerPoint files (pptx, pptm, ppsx, ppsm, potx, potm, ppt, pps, pot)
- Microsoft Word files (docx, docm, dotx, dotm, doc, dot)
- OpenDocument files (odt, ott, ods, odp)
- PDF files
- RTF files
- Text files (txt)
- Visio Drawings (vsd, vdx, vss, vsx, vst, vtx, vdw)

Using Annotations

The annotation options are shown in the Alt menu and in the task area on the left-hand side of the M-Files Desktop user interface.

▶ Video: *Annotations*

Enabling annotations in the user interface

To make sure that annotations are enabled in your user interface:

1. Open M-Files Desktop and access your vault.
2. Press the Alt key on your keyboard.
3. Open the *View* menu.
4. Enable the *Show Annotations* option.

Creating a new annotation object

To start creating new annotations to a document:

1. Select a document in suitable format (for instance, a *.doc* or *.pdf*).
2. Make sure the *Preview* tab (not, for example, the *Metadata* tab) is selected in the right pane.
3. Select the *New Annotations* command via the task area on the left-hand side of the user interface.

This should create a new *Annotation* object under your document, visible via the listing view, and open the annotation toolbar in the preview window.

> 📄 **Note:** The task area displays the *New Annotations* option only for documents that do not yet have any annotations. If you want to create another annotation object, you can do so by pressing the Alt key and

selecting **New** > **Annotation...** from the menu. It is, however, recommended to have only one annotation object for each document.

Adding annotations

The annotation toolbar includes a number of different ways for you to highlight parts of the document.
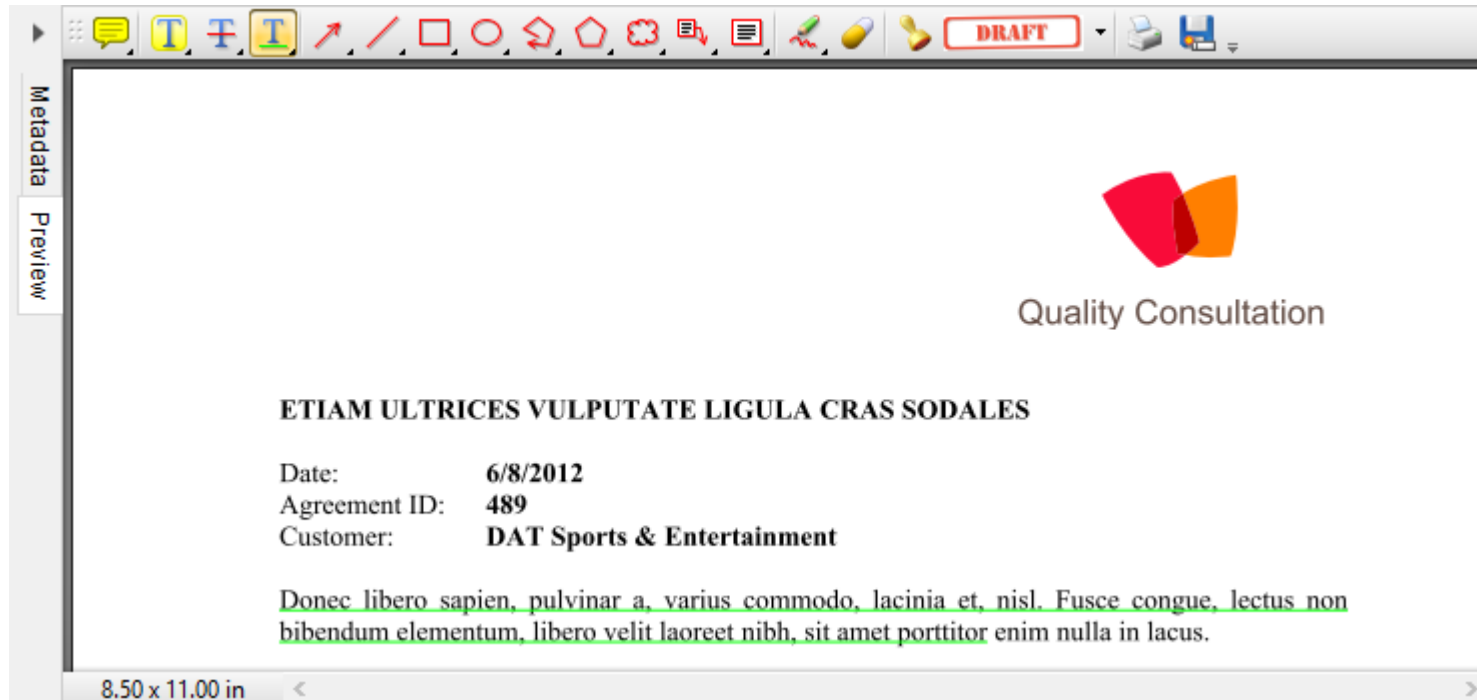
Figure 27: The annotation toolbar in the preview window.

You can add comments as well as text emphasis in the form of text highlighting, strikethrough text and text underlines. You can also add arrows, lines, rectangles and various other shapes for emphasis, including text boxes. In addition to these elements, there is a pencil tool coupled with an eraser in case you make a mistake. Finally, you can add various built-in stamps, such as "Draft", "Approved" or "Final".

Saving and printing annotated documents

The toolbar also displays icons for printing and saving. You can use these functions to print the annotated document or to save a copy to people with no access to your document vault. Saving a copy is also a convenient way for embedding all the annotations to a single PDF file.

Saving annotations

Once you have finished making annotations, you can save your changes by selecting the *Save Annotations* option via the task area. Alternatively, you can select another document, which triggers M-Files to ask if you want to check in the annotated document. The modifications are saved once the document has been checked in.

Editing annotations

To edit previously added annotation objects:

1. Select the annotated document or the annotation object.
2. Make sure the *Preview* tab is active.
3. Select *Edit Annotations* via the task area.

This should open the annotation toolbar in the preview window.

Showing and hiding annotations

When you have an annotated document selected, the task area should display the options to display or hide the annotations.

To hide the annotations, select the *Hide Annotations* option via the task area. Alternatively, select the *Show Annotations* if they are not visible.

4.11. Version History

Whenever you reserve a document or an object by checking it out, a new version of the object is created.

M-Files offers the possibility to return to the previous, unchanged version via the object's *version history* even after you have saved the changes to your document, closed it and checked it in. This is done by highlighting the object and selecting **History** from the task area. Version history is stored for all objects.

📄 **Tip:** You can restore a previous version of the document by using the *Roll Back* function of the *History* dialog. Versions can be labeled easily by using the *Add Label to This Version* function.

4.12. Using Views

Your day-to-day use of M-Files will mainly involve using M-Files Desktop for browsing views in which documents and other objects have been grouped according to the desired criteria, such as a project or a customer, based on the metadata contained in the objects.

For example, all documents for which the *Project* metadata has been specified can be grouped by project. The documents and other objects related to the same project will then be displayed in the project's virtual directory. For more information on configuring views and grouping levels, refer to *New View* on page 90.

▶ Video: *Views Overview*

4.13. Finding Documents and Other Objects

The most efficient way of finding your documents and other objects is to use the M-Files search functions. This is especially useful when you remember only a single detail about the document or object, such as the creation date or the user who created the document.

Quick search

With the *quick search* function (at the top of the M-Files user interface), you can search for certain words associated with the object.

Advanced search

The *advanced search* allows you to define more search criteria related to the status and properties of the object. For example, if you want to view the documents that a certain user has checked out during the last month, this is easier to do by performing an advanced search than by creating a new view.

📄 **Tip:** The more search criteria you use in the advanced search, the more likely you are to find the exact document or object you want.

Display the most relevant result first

The following information is of primary importance for providing search results:

- When was this document or other object **created**?
- When and how many times was the document or other object **edited**?
- When and how many times was it **processed**?

By using this information, the you will find relevant data on **the organization's newest and most commonly used documents** or other objects. If several years have passed since the creation of the document and the document has not been updated for a long time, the document is perhaps not considered very relevant for the user and it is not included among the first search results.

In addition to the information related to document handling mentioned above, the occurrence of the search string in metadata and/or file contents influences the order of the search results.

An item's location among the search results is influenced by the search string appearing in the following:

1. The name or title of the document or other object
2. Other metadata than the name or title of the document or other object
3. File contents

The name is of special importance because the document or object name often contains essential information about the content. Additionally, M-Files ignores certain metadata that tend to decrease the relevance of the search results. Full-text search in files is influenced by, for example, the length of the file in such a way that the shorter document is given more importance than the long one when the two have the same number of matches for the search string. In any case, the order of the search results is always more dependent on metadata than file content.

> 📝 **Note:** The set of search results is naturally influenced by the search criteria, which may include search of the metadata, full-text search, or both.

Search result definitions can be modified via the Windows registry settings.

For more information, see *Search Functions* on page 139.

4.14. Show Status

In M-Files, the documents are kept on the M-Files server, and they are transferred to the caches of M-Files users' computers to make the use of M-Files as fast as possible.

With the *Show Status* component, you can monitor the file transfers from the server to your computer and find out how long it will take to download a document. This tool is particularly useful if you are using M-Files over a slow connection. In regular local area network use, documents are usually transferred so quickly that there is no time to check the status information.

File transfer

The *Status* column indicates whether the file has been transferred or is being transferred. The status is indicated as a percentage. You can stop the transfer by highlighting the document and clicking **Stop**.
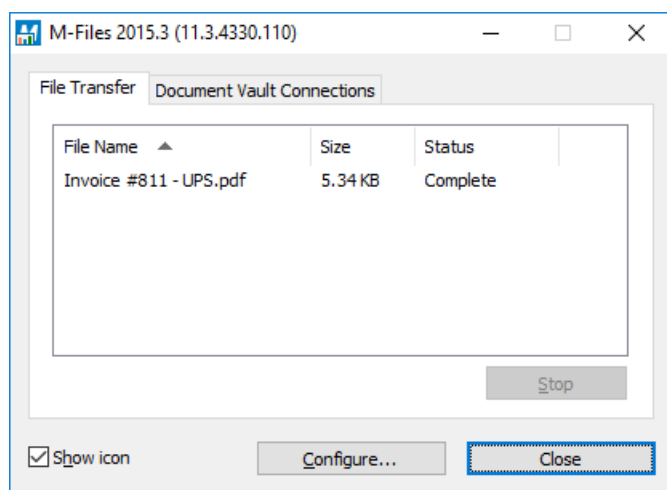
Figure 28: The "File Transfer" tab of the "Show Status" component.

The **Configure...** button opens M-Files Desktop Settings. For more information, refer to *M-Files Desktop Settings* on page 34.

Document vault connections

On the *Document Vault Connections* tab, you can see which document vault connections are available and whether the vault is online.
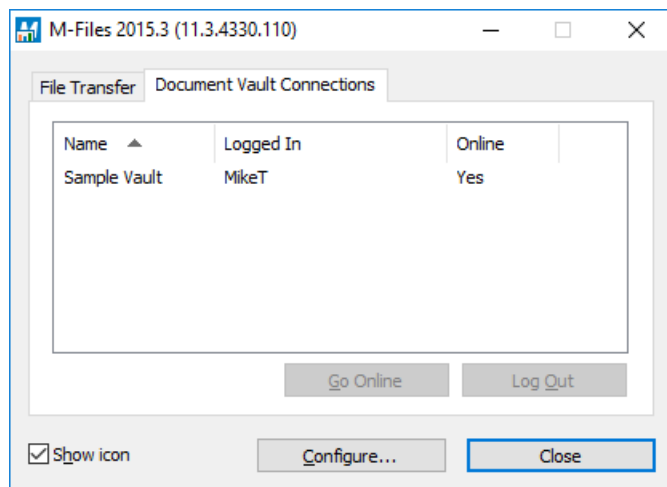
Figure 29: The "Document Vault Connections" tab of the "Show Status" component.

Go Online, Go Offline

These functions allow you to switch between the *Offline* and *Online* modes. The function of the button changes according to the current status. For more information, refer to *Go Offline* on page 126 and *Go Online* on page 126.

Log Out, Log In

If you are *logged in* to a document vault, you can use the **Log Out** button to log out and quit M-Files Desktop. The function of the button changes according to your current status.

4.15. Office and AutoCAD Functions

Documents stored in M-Files can be edited in external software in the same way as any document stored on your computer. M-Files also offers access to its functions in the Microsoft Office and AutoCAD software.

Utilizing M-Files with Microsoft Office and AutoCAD software is easy:

- Documents can be opened from and stored into M-Files directly.
- The M-Files menu offers quick and easy access to M-Files functions.
- Document metadata can be edited directly in Microsoft Office and AutoCAD.
- Document metadata stored in M-Files can be partially included in document contents.
- E-mail messages and attachments can be saved to M-Files in various file formats.
- Saving of e-mail messages can also be automated, meaning that the messages are automatically saved with their metadata by means of Outlook rules and M-Files features.
- Contact persons and customers can be automatically associated with e-mail messages.

For more information about using these M-Files functions, refer to *M-Files Functions in Microsoft Office and AutoCAD* on page 162.

5. Basic Functions in M-Files Desktop

This chapter describes the basic functions in M-Files Desktop via the menus *View*, *New*, *Operations* and *Settings*. The M-Files functions can be accessed either via the Windows menu bar activated by pressing the *Alt* key on your keyboard, from the task area or via the context menus activated with the right mouse button. You can choose the method that suits you best.

5.1. "View" Menu

This topic presents the options available via the *View* menu.

Clean View, Hide View and Unhide Views

Clean View is a function that a user logged in to the document vault can perform for any view. It is used for removing temporary local files and all empty folders automatically.

Some views of the *Demo Vault* cannot be removed, but they can be hidden. A regular user cannot remove views that have been created in the M-Files Admin. In such cases, you can highlight the view on the listing area and use the context menu function *Hide View*. To unhide views, open the *Unhide Views* dialog under the *View* menu or in the context menu for the listing area.

> 📄 **Tip:** You can create a view showing all the deleted objects if you have any of the following permissions: *full control of vault*, *permission to see all objects*, or *permission to see deleted objects*. Just create a view with the filter *Deleted = Yes*. See also *Status* on page 148.

Display Mode

With the **Display Mode** options you can:

- Choose whether you want objects to be displayed as icons or as a details list.
- Move the metadata card from the right side of the user interface to the bottom, and vice versa.
- Turn the Windows Explorer navigation pane on and off.
- Change the right pane and the bottom pane to be displayed in the minimized mode, or turn them off completely.
- Choose whether M-Files annotations are shown or not.
- Enable or disable object type based object grouping as well as view and folder grouping.
- Choose between a normal and a compact layout for the user interface.

Save as common display settings

M-Files allows you to save the display settings of a function as *common display settings*. To use this function, you need administrative rights to the relevant vault. The function saves the display settings common to users view-specifically. You can choose whether the function is to be applied for all users or only those users who have not yet modified their own display settings.

With the function, you can, for example, define specific columns to be displayed for all users.

Reset display settings to default

By using this function, you can reset modified display setting values to the defaults set by the system administrator. Alternatively, you can reset the display settings to the M-Files software defaults.

Binding a report to the view

You can bind the report for example to the view *Sales by customer* or *Proposals by salesperson*. With the *Reports* function in the *View* menu, you can bind the report to the view and specify its location. If you want this setting to apply for all users, select the option *Common to all users* in the view settings. In order to define a common view, however, you need the permissions for managing the document vault's common views.

For more information on reports, see *Reporting and Data Export* on page 367.

5.2. "New" Menu

This section offers a brief description of the *New* menu's functions.

New Annotation

Selecting **New** > **Annotation...** creates a new annotation object for the document. This opens the *Preview* tab of the document, including the annotation toolbar above the document preview.

For more information about using annotations, see the topics *Annotations and Redlining* on page 72 and *Using Annotations* on page 73.

New Document

The *New Document* function is one way of creating new documents in M-Files. M-Files document consists of two components: zero or more files and the metadata. A single Word file is not a document by itself, but becomes one when metadata is added. Selecting a document class automatically provides the document with certain properties that have been specified for the *class* in question via M-Files Admin.

For a basic description on document creation in M-Files, refer to *Creating a Document* on page 58.

Class

The *Class* field is used to categorize the document as part of a certain predefined class. This mostly affects what metadata is specified for the document or object. For more information about classes, refer to *Classes* on page 307.

Use Template

You can create a new document by using a predefined template. When you select a template in the new document creation wizard, the metadata card is populated with the data contained in the template. You can also edit and add metadata. The new document contains the contents of the template.

Examples of useful templates include *Proposal template*, *Order template* and *PowerPoint presentation template*.

To specify a document or other object as a template, add the property *Is template* and set it to *Yes.* Templates are class-specific, but you can specify the template to affect several classes by adding the *Additional Classes* property for the object.

> 📝 **Note:** When you want to save a document as a document template to be used in M-Files, save the document as an Microsoft Office document – i.e. in the format *.doc(x)*, *.ppt(x)*, *.xls(x)* or similar. Do not use the template formats offered by Microsoft Office applications (for instance the Word template, *.dotx*).

▶ Video: *Document Templates*

For more information, refer to *New Class* on page 308, as well as to *Automatic Values* on page 292 for information on using document templates with automatic values.

Single-File and Multi-File Documents

In M-Files, you can create *multi-file* or *single-file documents*.

⊙ Video: *Multi-File Documents*

A multi-file document usually contains several files, i.e. files that together with the metadata constitute one multi-file document. You can view the contents of a multi-file document by double-clicking it. In other words, a multi-file document is a fixed entity that contains several document files. For example, it is a good idea to include a proposal and its attachment in the same multi-file document.

You can later convert a single-file document to a multi-file document and vice versa. For more information, refer to *Convert to Single-file Document* on page 120.

Name	Date Modified	Score ▼	
▲ Documents (3)			
🅆 Employment Agreement Template.doc	6/22/2011 6:53 PM	82335	
◢ 📁 Employment Agreement / Alex Kramer	6/22/2011 6:53 PM	81924	
🅆 Editable version.doc	6/22/2011 6:53 PM		
📄 Signed copy.pdf	6/10/2008 4:29 PM		
› 👤 Employees (1)			
› 🅆 Employment Agreement / Kimberley Miller.doc	6/22/2011 6:52 PM	81704	

Figure 30: Multi-file document and single-file Word documents in the listing view.

File Extension

The file extension of a new document is predefined by the template chosen in the new document creation wizard (see *Creating a Document* on page 58).

📄 **Tip:** If you want to see all the available file extensions and create a blank document, select the category *Blank* in the wizard.

Properties

You can edit the metadata directly by modifying the property values in the metadata card. In addition to being able to directly edit property values, you can add or remove properties, change workflow-related information and modify permissions of the selected item(s).

Clicking on a property on the metadata card activates the edit mode, which displays the *Save* and *Discard* options at the bottom of the page. Clicking the **Save** button saves the changes, creates a new version of the object and returns the metadata card to view mode. Selecting **Discard** returns the metadata card to view mode without saving any modifications.

M-Files fills in the *Created* and *Added by* fields automatically on the basis of the current M-Files user information and timestamp data. M-Files is also able to fill in other fields, depending on where you save the document. The *Name* or *Title* field must be filled in, as the title constitutes the name displayed in various lists. An asterisk (*) next to a field indicates that the field must be filled in for you to be able to create the object.

A toolbar is displayed for properties that can have additional functionalities. Only the functions available for the chosen property are displayed.

Figure 31: The five functions of the toolbar: Add field, Remove Field, Refresh, Add value and Edit.

You can use the + and - icons to add or remove fields in a multi-select property. This enables you to link a document to multiple properties, such as a number of various projects.

The *Refresh* icon updates the values of a property based on a value list. Additionally, you can create more values to a property by selecting the *Add value* icon. With the *Edit* icon you can open a dialog for modifying the chosen value.

> **Tip:** You can use keyboard shortcuts while editing the metadata. See *Efficient Use of the Metadata Card* on page 57.

You can easily add metadata fields to the metadata card by clicking the *Add property* label at the end of the property list. If you want to create new properties, open the *M-Files Admin* on page 127 and refer to *Property Definitions* on page 288.

Editing properties of multiple objects at once

You can select multiple objects in M-Files by doing any of the following:

- Hold down the ⇧ Shift key while selecting objects in the listing area to select a group of consecutive objects.
- Hold down the Ctrl key while selecting objects in the listing area to select multiple individual objects.
- Click and drag a box around the objects that you want to select in the listing area.

When you have multiple objects selected, you should see the collective metadata of the objects you have selected on the metadata card:

(varies)

Customer
ID (varies) Version (varies)

Created (varies) (M-Files Server)
Last modified (varies) (varies)

Class*	Customer
Customer name*	(varies)
Address (line 1)	(varies)
Address (line 2)	(varies)
City	(varies)
State/province	(varies)
ZIP/postal code	(varies)
Country	☐ Canada
	◪ China
	☐ France
	◪ Germany
	☐ United Kingdom
	☑ USA
Telephone number	(varies)
Web site	http://www.m-files.com
Is supervisor?	◕ Not specified
	◕ Yes
	○ No

🔒 Full control for all internal users

The metadata card shows all the properties of the selected objects. If the objects have the same value for a property, the value is shown in the property field. If, on the other hand, the objects have differing values for a property, the property looks something like one of the following:

Example property	Explanation
Telephone number (varies)	The selected objects have varying values for the property.

Example property	Explanation
Country □ Canada ◪ China □ France ◪ Germany □ United Kingdom ☑ USA	The selected objects have different values selected for the property: • If the check box is unchecked, it means that *none* of the selected objects have the value selected. • If the check box is checked, it means that *all* of the selected objects have the value selected. • If half of the check box is filled with gray, it means that *some* of the selected objects have the value selected.
Is supervisor? ◐ Not specified ◐ Yes ○ No	The selected objects have different values selected for the property: • If the radio button is not selected, it means that *none* of the selected objects have the value selected. • If the radio button is selected, it means that *all* of the selected objects have the value selected. • If half of the radio button is filled with gray, it means that *some* of the selected objects have the value selected.

Now, when you edit a property value, you change the value for all the selected objects collectively. If you enter a new value in place of `(varies)`, the same property value is set for all the selected objects. Or, if you check or uncheck a check box, or select or unselect a radio button, the value is added or removed for all the selected objects collectively.

Permissions

To open the permissions dialog, click the permissions area at the bottom of the metadata card.

▶ Video: *Permissions*
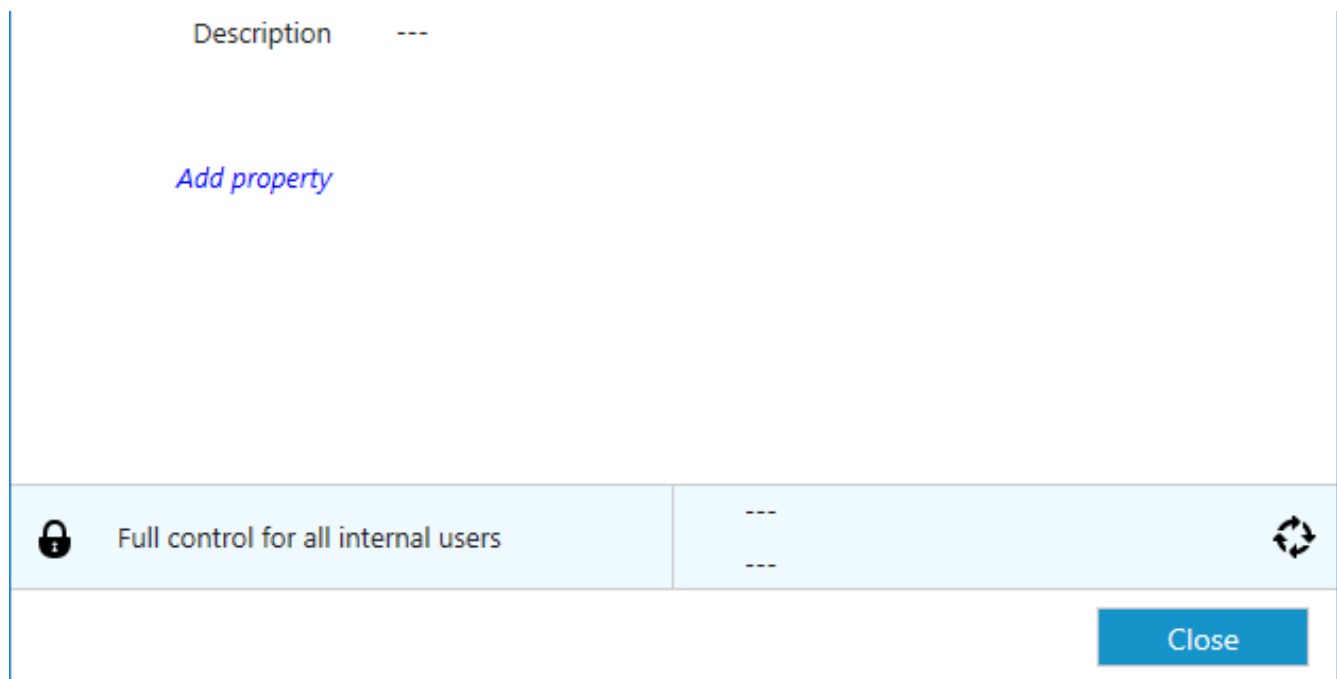
Figure 32: The permissions area is displayed at the bottom of a metadata card.

You can quickly select the document permissions from the pull-down menu in the *Permissions* dialog. These predefined permissions, or named access control lists, can be modified with the M-Files Admin (refer to *Named Access Control Lists* on page 339). An access control list consists of various user groups or users and definitions of their permissions.

Editing permissions

You can edit the permissions by first clicking the *Permissions* area on the metadata card and the clicking the **Edit...** button in the *Permissions* dialog.

When you want to edit the permissions, first deselect the *Use named access control list* checkbox. By clicking the **Add...** button, you can display all users, user groups, and pseudo-users registered in M-Files and edit the permissions for each of them. With the **Remove** button, you can remove users, user groups, and pseudo-users from the access control list. If you want to edit this user list, open M-Files Admin and refer to *Users* on page 251 or *User Groups* on page 256.

Also refer to the specification of pseudo-users in *Pseudo-users* on page 88.

Multilevel permission system

You can view and modify the permissions of the object via the permissions area at the bottom of the metadata card. The options available are *All*, *Change permissions*, *Remove*, *Edit*, and *Read*. You can allow a permission by selecting *Allow* and deny it by selecting *Deny*.

A user with *Read* permissions is allowed to open the files contained by the object, as well as to view its properties. The user cannot check out the document, and is thus not able to make any changes to it. If the user does not have *Read* permissions to the document, it will not be visible to the user in views or search results.

Edit permissions enable users to freely edit the document. These permissions automatically include *Read* permission and *Edit* permissions. *Edit* permissions do not encompass any deletion rights.

Remove permissions allow users to delete the document but not *destroy* on page 229 it altogether. Deletion rights do not encompass any other rights.

The right to *Change permissions* determines whether the user is allowed to change the permissions for the document in question. These permissions do not include any other permissions, and they can be used independently of the other permissions.

> **Note:** Users with the right to *Change permissions* enable them to specify any other permission for themselves.

Example

Denied permissions always take precedence over allowed permissions. This means, for instance, the following: *User A* is a member of *user group B*. *User group B* has the *Edit* permission for *document C*. *User A*, on the other hand, does not have *Edit* permissions for *document C*. Even though *user A* has *Edit* permissions for *document C* by means of *user group B*, *user A* cannot modify the document, because it has been separately denied from *user A*.

Selected permissions

The document or object may have its own permissions, and the object may also have different automatic permissions via its properties. Any given permissions must be granted by all these settings in order to be effective.

On the *Permissions* tab for the object, the user can check the permissions that influence the final permissions of the object. In order for any specific permission, such as read or edit access, to be granted for a specific user, all of the permissions in effect, at all levels, must allow it simultaneously.

For more information on internal restrictions to permissions and valid permissions, refer to *Effective Permissions* on page 86.

Source

The "Source" column indicates the source from which the object has received a given permission. In the example, the object has automatic permissions granted via the project (*Project name [Project])*, and the object's own permissions (*This object*). Both of them restrict the final permissions of the object.

Description

The "Description" column provides descriptive text for the permission. Note: If you have created an automatic permission by value, value list, or object type and named it, the name is displayed in this column.

Active

If the users have been allowed to bypass the automatic permissions when they are specifying automatic permissions for the relevant value, value list, or object type, the user can deactivate the automatic permissions granted via the value by deselecting the permission in question. Then the permission is not active anymore and it does not influence the object's final permissions.

Details

You can enter the Permissions dialog box either via the ... icon or *Details* icon. Use the *Add* and *Remove* buttons to add or remove users.

Effective Permissions

For more information on internal restrictions to permissions and valid permissions, refer to *Effective Permissions* on page 86.

Effective Permissions

An object may have various permissions of its own, as well as automatic permissions. All these permissions restrict the use of the object when the extended automatic permissions have been activated. In order for specific access rights, such as read or edit permissions, to be granted to a certain user, all settings must allow it simultaneously. That is, any given permission must be granted by all active settings in order for it to be effective.

Example 1: Automatic permissions for objects via any project

The access that was specified for the object itself may cover full control of the document for all users while the automatic permissions via a project may restrict the use of the document in such a way that full control is granted to project managers only and all other users have read-only access.
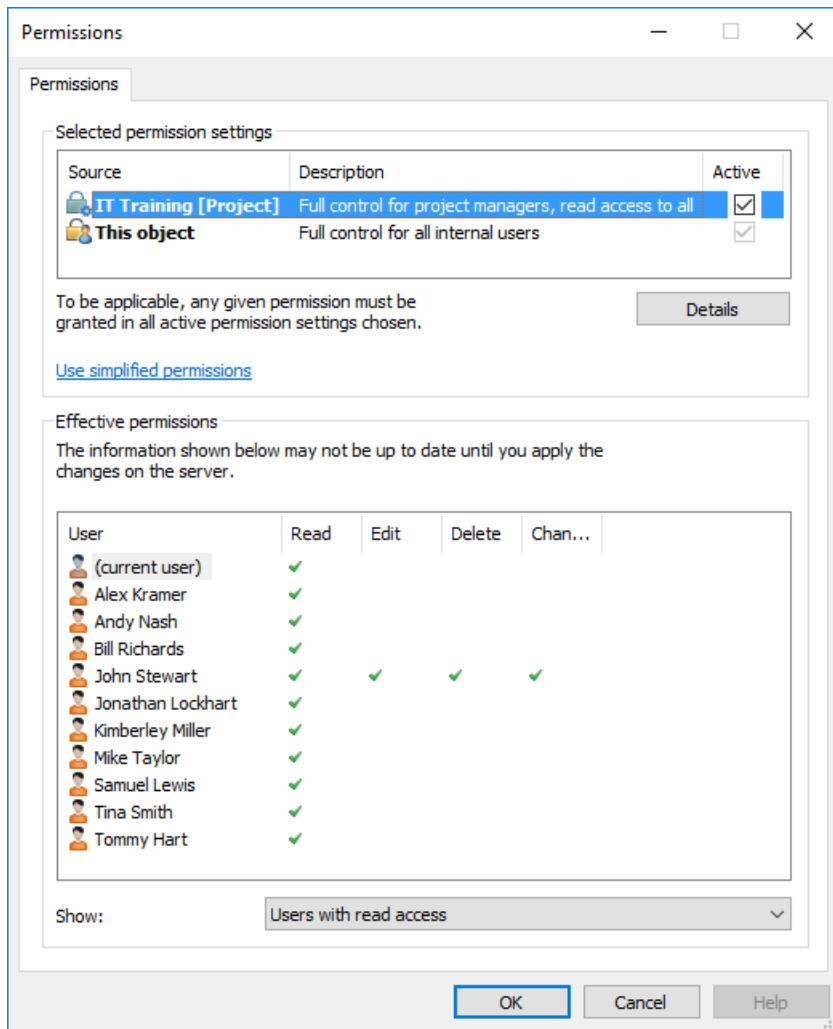
Figure 33: Automatic permissions via a project may restrict the object's permissions.

> 📄 **Tip:** You can quickly check the effective permissions by user and access right via the table shown in the *Permissions* dialog.

Example 2: Internal restrictions to permissions

- The permission settings of the object allow full control for all users.
- Via its class, the object has been granted permissions that give full control to management and read-only access to all other users.
- Via its safety class property, the object has been granted permissions that give full control to management and edit rights to the HR department.

Since any given right must be allowed by all of these settings in order to be valid, the settings mentioned above restrict each other in such a way that the following permissions are ultimately valid:

- Full control for the management.
- Read-only access to the HR department.
- No rights at all for other users.

The final restrictions are always determined by the strictest settings. As explained further above, all settings must allow the permissions simultaneously in order for them to be effective.

Changing the final permissions of the document or other the object

Because all permissions restrict the use of the objects, changes to final access rights can be made in different ways. In the client software, you can change access rights as follows:

You can change the object's own permissions from the *Permissions* dialog. If the object has permissions granted via properties, the *Details* button is displayed on the *Permissions* tab. The button can be used to change the object's own permissions (activate *This object* first).

If deactivation of the automatic permissions is allowed, you can deactivate the automatic permissions by property.

You can change the object's properties via which automatic permissions were granted to the object (if allowed).

If you cannot change the permissions or properties associated with the object itself and the automatic permissions granted via them, you should contact the administrator for changes of access rights.

Pseudo-users

Instead of just adding users or user groups to the permissions of an object, you can also add so-called pseudo-users, or *users from metadata*, as well.

You can specify pseudo-users directly for the object and use these automatic pseudo-users for automatic permissions and named access control lists. Pseudo-users that are specified via properties can also be used in workflows when you want to specify people for tasks, send a notification to users, or define permissions for different states.

You can specify pseudo-users via only those properties that are based on a *Users* or *User groups* value list.

▶ Video: *Dynamic Access Control Entries*

Example: You can specify that the project manager for a certain project always has access to an object if this project is indicated in the object's metadata. Then the project manager information is automatically delivered to the object with the project and, on the basis of automatic permissions, the user is granted project manager access rights to the object. In case the project manager is changed, the project manager information can easily be changed for the project. This information is transferred to the documents or other objects, so updating their project manager information separately is not necessary.

You can also perform multilevel user definitions via properties. For example, you can define the project manager via the related project property (see the image below). This way, the project manager information is kept up to date constantly, as it is associated with the project instead of each separate document. You can specify access for these pseudo-users by object or utilize them when defining automatic permissions.
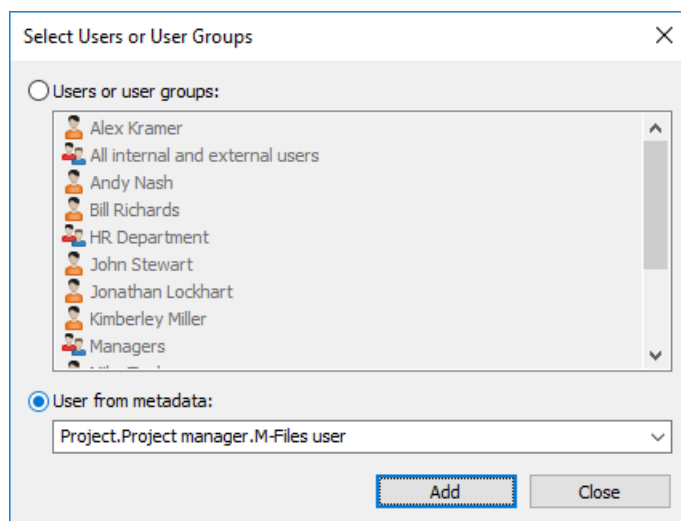
Figure 34: Select "User from metadata" when you want to specify pseudo-users.

You can specify automatic permissions and utilize the pseudo-user definitions in, for example, the "contract of employment" class, which grants specific rights automatically to, for instance, an employee's supervisor. In this case, the supervisor is automatically found with the employee information and the supervisor is granted the appropriate rights. If the employee's supervisor changes, these rights are automatically granted to the new supervisor.

For more information on automatic permissions, see *Automatic Permissions* on page 275.

New Document Collection

A document collection is a set of interrelated documents. The difference from a multi-file document is that each member of a document collection is independent and has its own metadata. In addition, the document collection has a collective set of metadata that is independent of the member documents. By contrast, in a multi-file document, all document files share the document's properties.

To create a document collection in M-Files, use the *New Document Collection* function. First select a class and then fill in the collection's shared metadata. Now you can include members in the collection using the *Members* function.

Example of a document collection: A company is preparing a new marketing authorization application. A marketing authorization application consists of the following separate documents: cover letter, general product description, technical product specification, statement by the safety authorities, and the company's financial statement. Because the company wants to utilize the application's member documents in other document collections and as separate documents, it makes sense to create a document collection for the application.

 Video: *Document Collections*
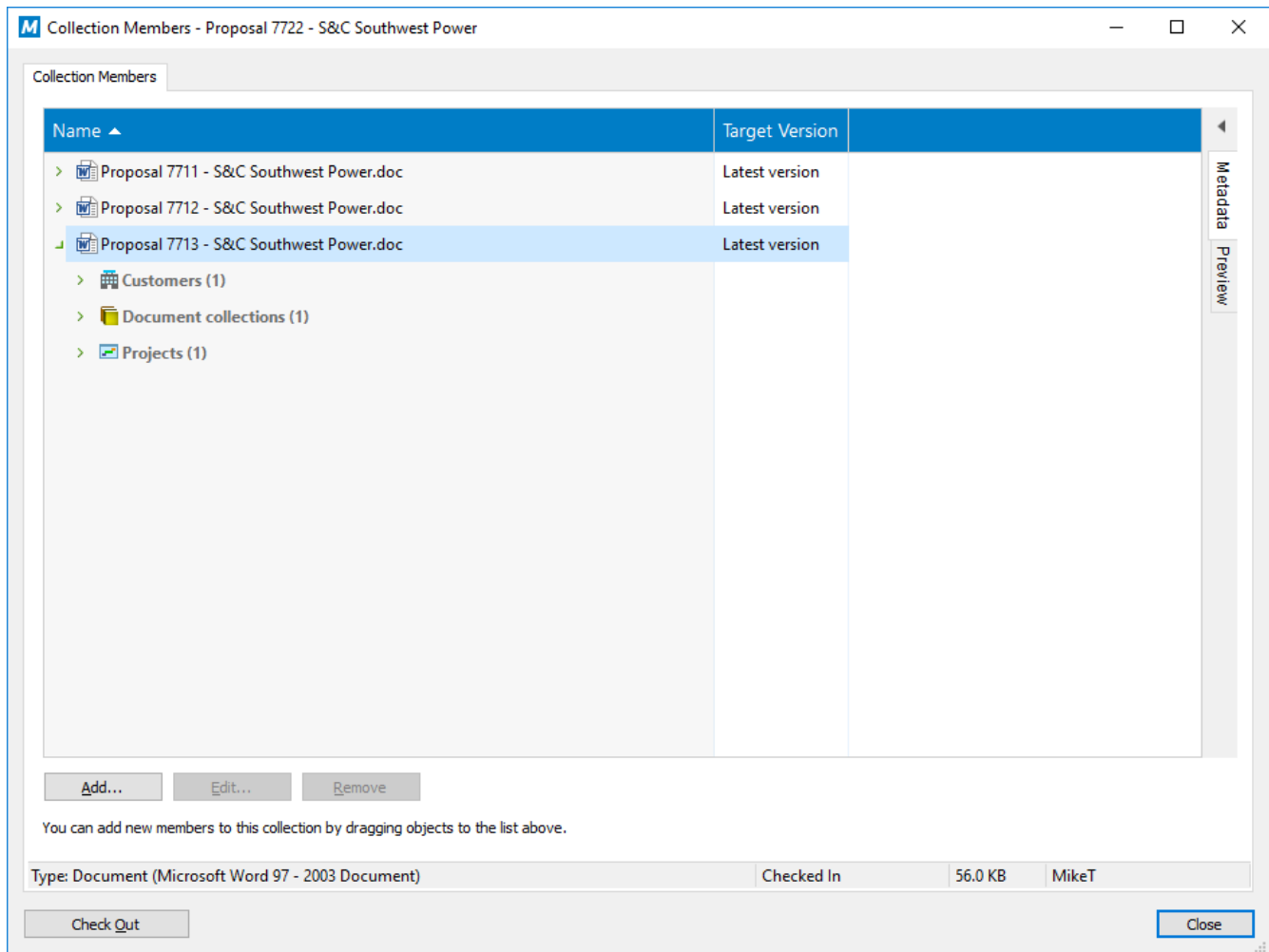
Figure 35: The "Collection Members" dialog.

Add, Edit, Remove

Use the buttons along the bottom of the dialog to add, edit, and remove collection members. To add several objects at once, you can drag and drop members from the listing view.

> 📄 **Note:** You can edit and remove documents only by first checking out the document collection.

Latest version, Specific version

When you add a relationship, M-Files prompts for the desired behavior regarding the version of the added document. You can set the relationship to always apply to the latest version or to the current version. In the latter case, further editing of the document will not be reflected in the document inside the document collection.

New Object

Besides documents, you can also create other objects defined by the system administrator. In the *New* menu, select an object type (such as *Customer*). For more information on creating an object other than a document, refer to *Creating Other Objects* on page 68.

New View

In M-Files, documents and other objects can be categorized into different views according to their metadata. The creation of views is largely based on specifying the metadata used to searching and categorizing documents.

▶ Video: *New Views*

Views allow you to save frequently used searches and define grouping levels. For information about searching for documents, refer to *Search Functions* on page 139.

There are two phases in determining a view:

1. Specify a *filter* to ensure that the view only displays objects you want to see. Specifying filters is similar to performing searches.
2. Determine the folder structure of the objects. This is useful when you have a large number of objects and you want to group them into different levels according to specific *properties*.
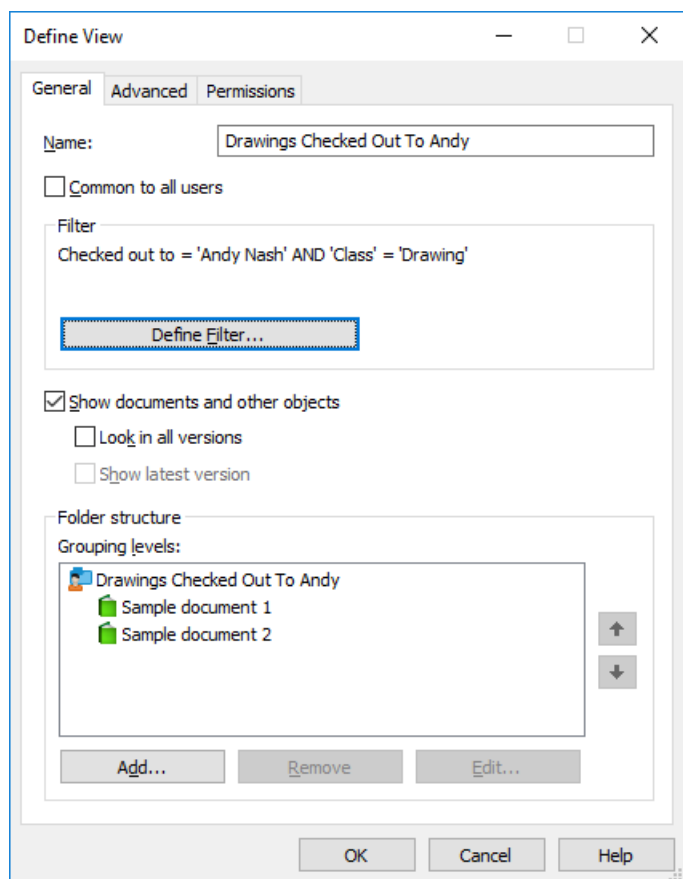
Figure 36: The "Define View" window.

In the example shown above, the documents must be checked out to the user Andy Nash, they must not have been deleted, and they must be of the type *Drawing* or *Model*. No properties have been added to the display hierarchy in this window, so all documents that meet the criteria are displayed in the same folder.

Name

Start by assigning a name to the view. The name should be as descriptive of the contents of the view as possible, so that users can deduce from the name of the view what kind of objects it contains.

Common to all users

Normally, views are created for personal use only. If you wish, you can define the view to be a common view visible to a desired user group. In order to define a common view, you need the document vault permission for managing the common document vault's common views.

You should carefully consider which views are needed by all M-Files users. For instance, the *Documents by Projects* view is often necessary. The users of the client software can hide unnecessary views from their own computers, and the administrator can restrict the visibility of the views by setting appropriate permissions. The views also can be assembled in groups *(view bundles)* from which, for example, the views used by the sales department are easy to find.

Show documents and other objects

By default, the view shows documents and objects according to the filter settings and folder structure. This option can be deselected if, for instance, new views are created under the current view. Note: When creating a new view inside the current view, the conditions of the upper view remain simultaneously valid. In other words, the sub-view results only include objects that also meet the conditions of the upper view.

Look in all versions

If you leave the *Look in all versions* box unchecked, the view will only list those objects whose latest version meets the specified criteria.

If you check the box, the filtered search will be performed on all versions of each document. Only the newest version meeting the criteria will be displayed. For example, if TinaS has modified versions 1 and 2 of a document, and AndyN has updated the document to version 3, search criterion *Last Modified By = TinaS* will return version 2 of the document.

Show latest version

If the option *Show latest version* is on, M-Files will show the newest version of each returned object instead of showing the old version that actually matched the search conditions.

Example: Creating a New View for French Customers

1. In M-Files, open the document vault to which you want to create the view.

2. Press **ALT** to open the menu bar.

3. Select **New** > **View...**

   ✅ The **Define View** dialog is opened.

Define View

General Advanced Permissions

Name: |

☐ Common to all users

Filter
Not deleted

Define Filter...

☑ Show documents and other objects
☐ Look in all versions
☐ Show latest version

Folder structure
Grouping levels:

View Name
Sample document 1
Sample document 2

Add... Remove Edit...

OK Cancel Help
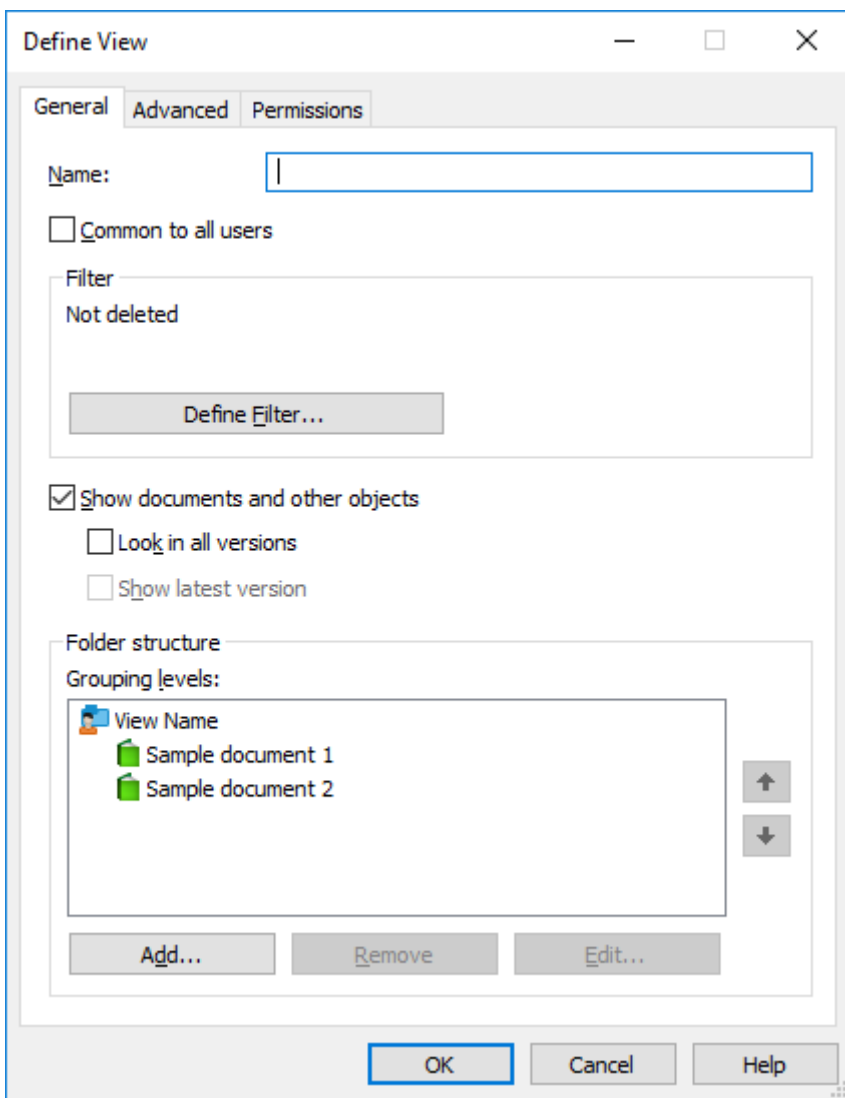
4. In the **Name** field, enter the name `French customers`.

ⓘ The name will appear in the listing area under **My Views**.

5. Optional: Check the **Common to all users** option check box if you want to define this view as a common view.

6. Click **Define Filter...** to specify the conditions that objects must meet to be shown in this view.

✓ The **Define Filter** dialog is opened.

7. On the **Status** tab, check the **Object type** check box, select the equal (=) operator from the adjacent drop-down menu, and select the *Customer* from the rightmost drop-down menu.

8. Go to the **Properties** tab.

   ✅ The **Properties** tab is opened.

9. Click **Add Condition** and add the following condition:
   a) Use the **Property** drop-down menu to select the **Country** property.
   b) Use the **Operator** drop-down menu to select the equal (=) operator.
   c) Use the **Value** drop-down menu to select **France** as the country.

10. Click **OK** to close the **Define Filter** dialog and to return to the **Define View** dialog.

11. Check the **Show documents and other objects** option check box.

12. Click **OK** to finish creating the view.

The view you have just defined appears in the listing area under **My Views** and it contains all the objects and documents that meet the conditions that you have specified in the filter settings of your view.

Example: Creating a Common View Containing All the Documents Created by the Current User

You must be either a vault administrator or a system administrator to be able to define a common view.

1. In M-Files, open the document vault to which you want to create the view.

2. Press **ALT** to open the menu bar.

3. Select **New** > **View...**

   ☑ The **Define View** dialog is opened.
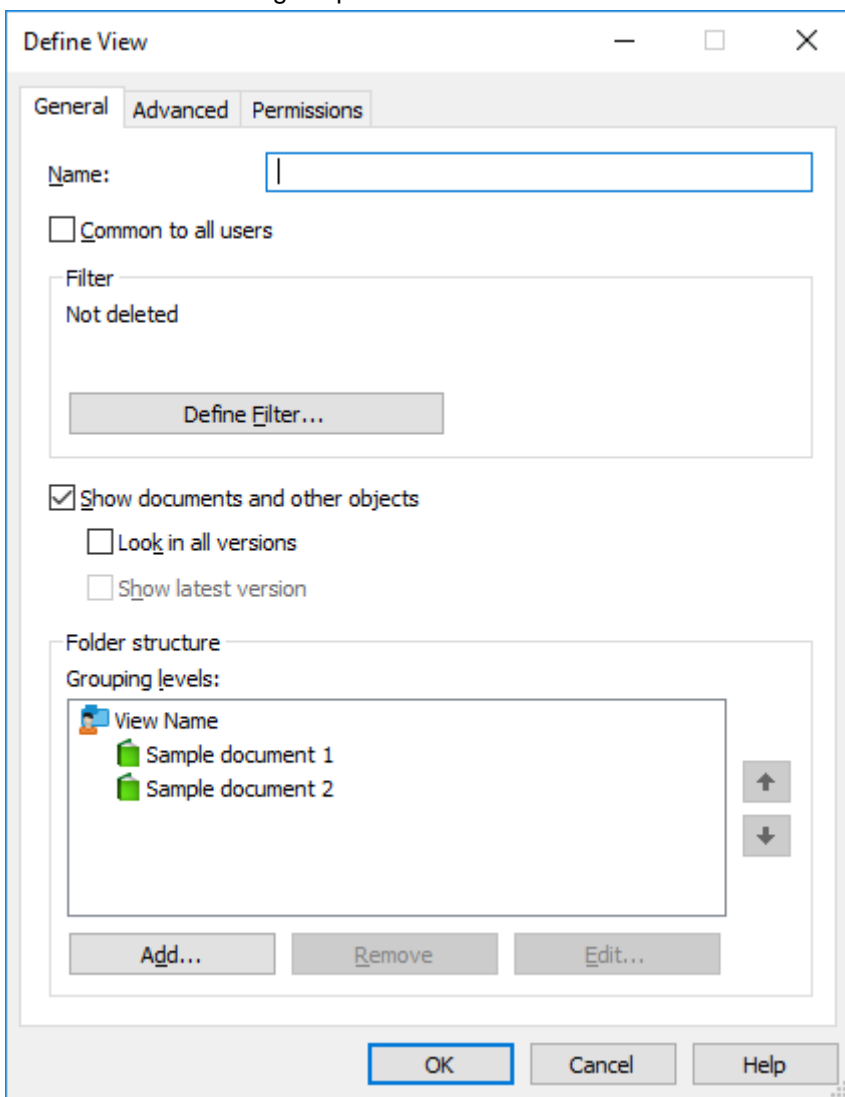
4. In the **Name** field, enter a descriptive name for the view.

   ✎ The name of the view can be, for example, `Documents Created by Me`.

5. Check the **Common to all users** option check box.

6. Click the **Define Filter...** button.

   ☑ The **Define Filter** dialog is opened.

   Define Filter   ✕

   Specify the conditions that objects must meet in order to be shown in this view.

   [Status] Properties   Files   Permissions

   ☐ Object type: = ⌄   ⌄
   ☐ Object ID: = ⌄
   ☑ Checked out: Yes ⌄
   ☐ Checked out to: = ⌄   ⌄
   ☐ Checked out between: ☐ 9/20/2016 ▦⌄ - ☐ 9/20/2016 ▦⌄
   ☐ Object flags: None ⌄
   ☑ Deleted: No ⌄

   [Reset Filter]   [OK]   [Cancel]
   ---

7. Go to the **Properties** tab.

   ☑ The **Properties** tab is opened.

   Define Filter   ✕

   Specify the conditions that objects must meet in order to be shown in this view.

   Status   [Properties]   Files   Permissions

Property	Operator	Value	Options

   [Add Condition]   [Remove Condition]

   [Reset Filter]   [OK]   [Cancel]
   ---

8. Click **Add Condition** and add the following condition:
   a) Use the **Property** drop-down menu to select the **Created by** property.
   b) Use the **Operator** drop-down menu to select the equal (=) operator.
   c) Use the **Value** drop-down menu to select the **(current user)** option.

9. Click **OK** to close the **Define Filter** dialog.

10. Click **OK** to close the **Define View** dialog and to finish creating the view.

All users of the vault should now have a new view under **Common Views**. They can use the view to list all the documents that they have created in the vault.

Define Filter

When defining a filter for the view, you specify the conditions according to which the objects are to be listed in the view. You can define criteria for the view on the *Status*, *Properties*, *Files* and *Permissions* tabs.
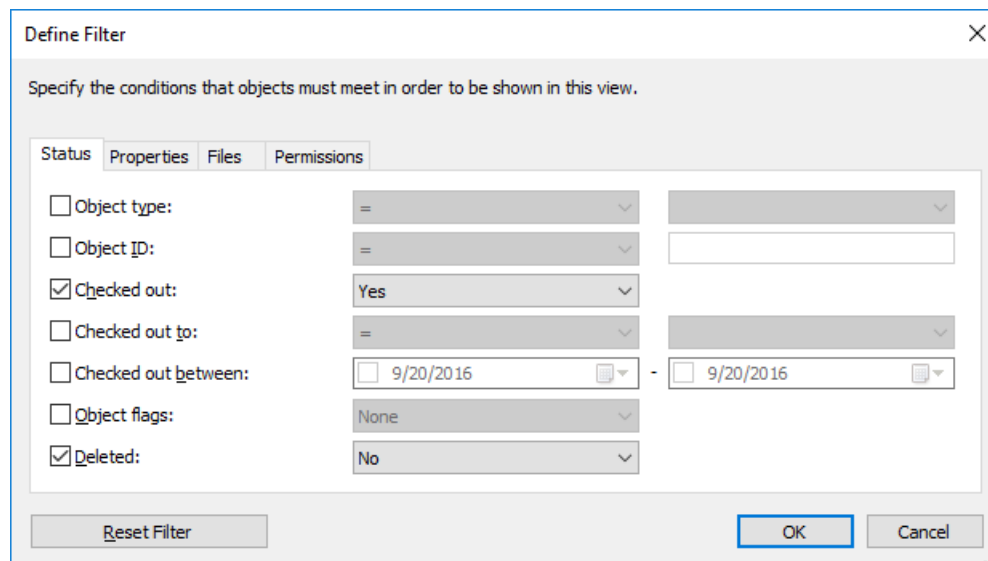
Figure 37: The "Define Filter" dialog.

Status, Properties, Files, Permissions

Refer to *Filter Settings* on page 148 under *Search Functions* on page 139.

Grouping Levels

Use the **Add...** button in the *Define View* dialog to start adding a new grouping level to your view.
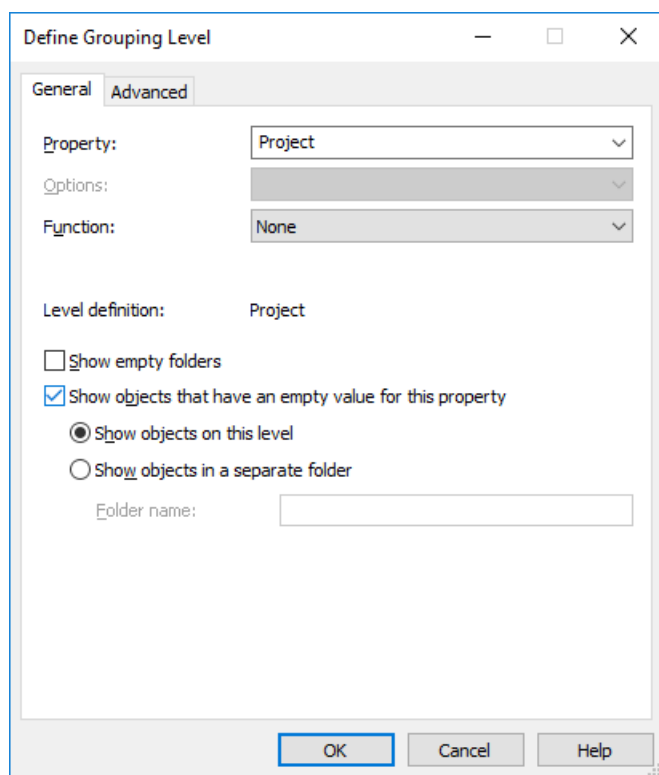
Figure 38: The "Define Grouping Level" window.

Property

When creating a new view that contains documents or other objects, you can use predefined properties to group documents. For example, to create a view that shows folders for all customers, select the property *Customer'* from the pull-down menu. You can modify this list with M-Files Admin. For more information on this, refer to *Property Definitions* on page 288.

Options

When working with properties based on value lists, use *Options* to select whether the folder for a certain value should also display documents for which one of the value's subitems or parent items is selected. For more information on hierarchical value lists, refer to *Value Lists* on page 269.

Function

You can use *Function* to specify how M-Files should treat properties like dates and timestamps, such as grouping them into months or years. Other data types can be grouped by first letters or letter ranges.

Show empty folders

By deselecting *Show empty folders*, folders with no contents will not be displayed in the grouping level.

Show objects that have an empty value for this property

To display objects of empty value with respect to this property in the grouping level, select this option. You can then specify whether the objects are displayed as a list in this level or in a separate folder.

Indirect views

Views can also be created by means of property relationships: the object itself does not have to include all of the properties defined for the grouping level in order to be included in the filtered view. Instead, the properties may be properties of other objects that have a relationship with the object in question (such as project or customer properties).

For example, *viewing documents by Country, Customer, and Project* is possible by means of indirect views, even if not all of these properties have been defined for the actual document. It is sufficient that the document be associated with the project, the project be associated with the customer, and a country be specified for the customer.

▶ Video: *Indirect Views*

You can easily specify these indirect views by clicking the plus-sign buttons in the property list and then selecting the property of a related object according to which you wish to create and group the internal structure of the view. In the example, first *Project* has been selected from the property list as the highest grouping level, then the project's property *Customer* was chosen, and finally the project customer's property *Country* was chosen, resulting in the property "*Project.Customer.Country*" with the periods. This way, the document has been linked all the way to the country information, which enables the creation of an indirect view by country. After this, the internal structure of the view has been defined to be distributed by customer, and by project on the last level (see the figure).
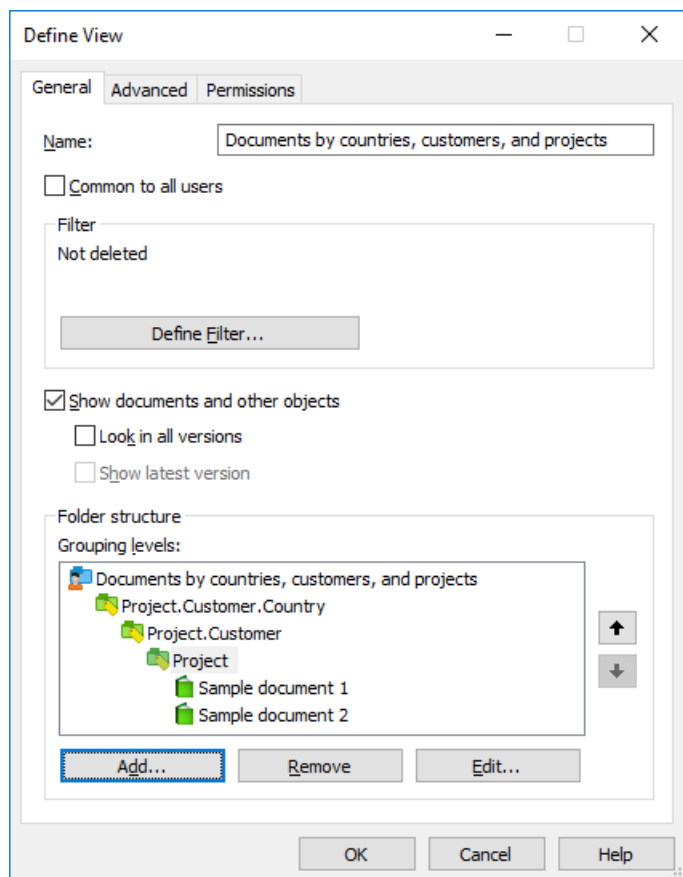
Figure 39: Creating an indirect view.

Grouping Level Advanced Options

Filter

When defining a filter for the level, you specify the conditions for including folders in the grouping level. For more information on defining the conditions, refer to *Filter Settings* on page 148. You can also utilize indirectness in specifying filter settings (for more information, refer to *Advanced Search* on page 144).

User-specific folder selection in a view

In the advanced settings for the view grouping level, you can specify whether the user is to be shown all virtual folders belonging to the level or whether the user may select the folders to be used. Folder selection is useful when the view or virtual folder includes a large number of subfolders (more than 500). By means of folder selection, the user can easily select the folders to be modified. The use of folder selection is significantly quicker than, for example, grouping by first letter when the number of objects is large (more than 10,000).

For example, if the view has been defined *By Customer* or *By Project* and the company has thousands of customers or projects, user-specific folder selection makes it easier for users to perform their daily tasks in the required customer or project folders. In this case, the user employs the *Select Folder* function to select only the folders that should be used.

If the retrieval of the subfolder listing is slow, try each algorithm in order to determine which is fastest for this type of search.

Folder limitation can be used if the grouping level is specified on the basis of a property that utilizes a value list.

> 📄 **Note:** The setting is specific to each grouping level.

For common views, folder limitation can be specified by a user with at least the right to manage common views.
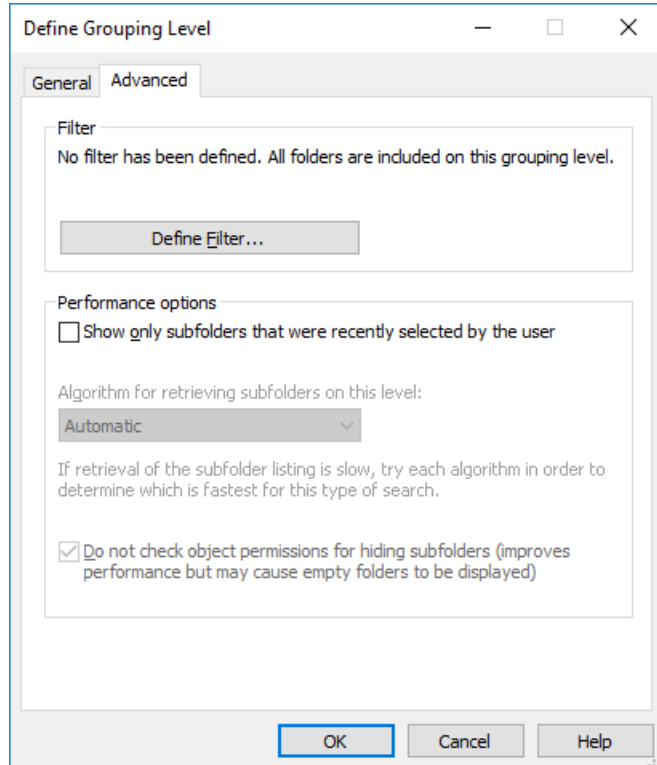
Figure 40: The advanced options for a grouping level.

Group By and Add Grouping Level

In the M-Files Desktop user interface, you can also add grouping levels by using the *Group By* or *Add Grouping Level* functions under the *View menu* on page 79. For instance in the *All Documents* view, it is possible to group the objects by their first letter or group projects by customers. You can remove and add new levels according to your needs.

View Advanced Settings

You can create a subview in a virtual folder of a certain view, for instance *By Project > Example Project > Recently Modified* (see *Creating a View in a Folder* on page 102).

When you create a new view in a virtual folder, you can determine whether the view is also displayed in other folders on the same level.

> **Note:** If the same level contains views and folders, views created in the folders will not be created in the views of the same level. The selection applies only to the folders of the level.
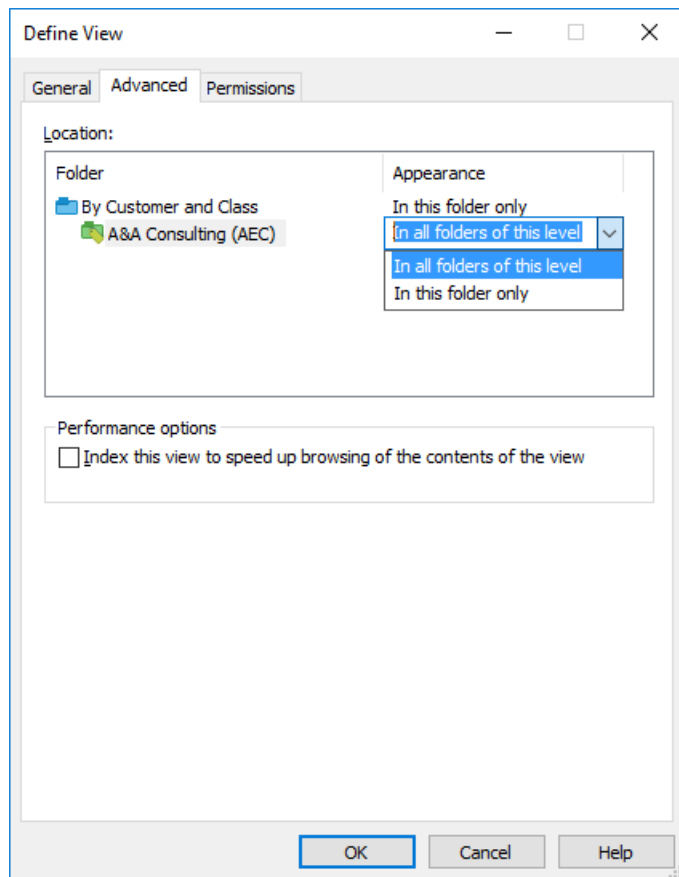
Figure 41: The advanced options for an M-Files view.

To display your view in all the other folders of the same level, select the *In all folders of this level* option. In the above example, the newly created view would be visible in all the virtual folders under the view *By Customer and Class*.

Indexing the view

Indexing of the view can be used to speed up the use of certain important views in a large document vault, if the filter criteria for the view sufficiently filter the group of objects. Indexing of the view is recommended only if the view does not include many objects (for instance, 10,000 objects in a vault with a total of 1,000,000 objects) and if the view is used daily and is working slowly.

Indexing of views should be used sparingly and only for views that benefit significantly from it, since each indexed view in the vault slightly slows down the creation and editing of documents and other objects.

View-specific indexing can be activated by a user with at least the right to manage common views.

Permissions

Define the users who will be able see this view. This tab is visible only when you are defining common views.

Creating a View in a Folder

New views can also be created in virtual folders. Open the virtual folder where you want to create a new view. Select *New View* and define the settings. For example, you can create a *Proposals that expire this week* view in the *Proposals* folder.

▶ Video: *Virtual Folders*

> 📝 **Note:** When creating a new view in a folder, the parent view and folder conditions are valid at the same time. This means that the new view only accepts objects that also meet the conditions of the parent view and folder.

Customizing a Folder as a View

Virtual folders can also be converted into views via the *Customize* tab of the virtual folder *Properties* dialog, or by right-clicking a virtual folder and selecting **Customize Folder**.

After the customization, you can modify the display settings of the new view and create grouping levels in the same way as for other views. Then, for example, in the *Memo* view, which has been customized from the *Memo* folder, you can group documents according to meeting types.

Because views can be created in folders, and folders can be converted to views, views and virtual folders may be available parallel in the listing area. Views can therefore contain folders as well as views, and folders can contain views as well as folders.

A folder that has been customized as a view can be restored as a folder by clicking the right mouse button on top of it and by then selecting *Remove Folder Customization*. The same option can also be found via the *menu bar* on page 79: **Operations** > **Remove Folder Customization**.

New Offline Filter

Navigate to the *Offline* view (accessed via *Other Views* of the home screen). In this view, you can define filters ensuring that all important objects are accessible even without a network connection.

Example: You can define all the documents of a certain project to always be available – even when no network connection is available. Just start creating a new filter, press the **Define filter...** button and add your project as a property filter.

To remove the offline filter, select *Remove* from the filter context menu.

Example: Creating an Offline Filter for a Project

1. On the M-Files home screen, navigate to **Other Views** > **Offline**.

2. Press **Alt** to open the menu bar.

3. Select **New** > **Offline Filter**.

   ☑ The **Offline Filter Properties** dialog is opened.

4. In the **Name** field, enter a name for your offline filter.

   ℹ The name will appear in the listing area under **Other Views** > **Offline**.

5. Click **Define Filter...** to specify the conditions that objects must meet to be shown in this view.

☑ The **Define Filter** dialog is opened.

Define Filter				×

Specify the conditions that objects must meet in order to be shown in this view.

Status · Properties · Files · Permissions

☐ Object type: =   ⌄   ⌄

☐ Object ID: =   ⌄

☑ Checked out: Yes   ⌄

☐ Checked out to: =   ⌄   ⌄

☐ Checked out between: ☐ 9/20/2016 ▦⌄ - ☐ 9/20/2016 ▦⌄

☐ Object flags: None   ⌄

☑ Deleted: No   ⌄

Reset Filter   OK   Cancel
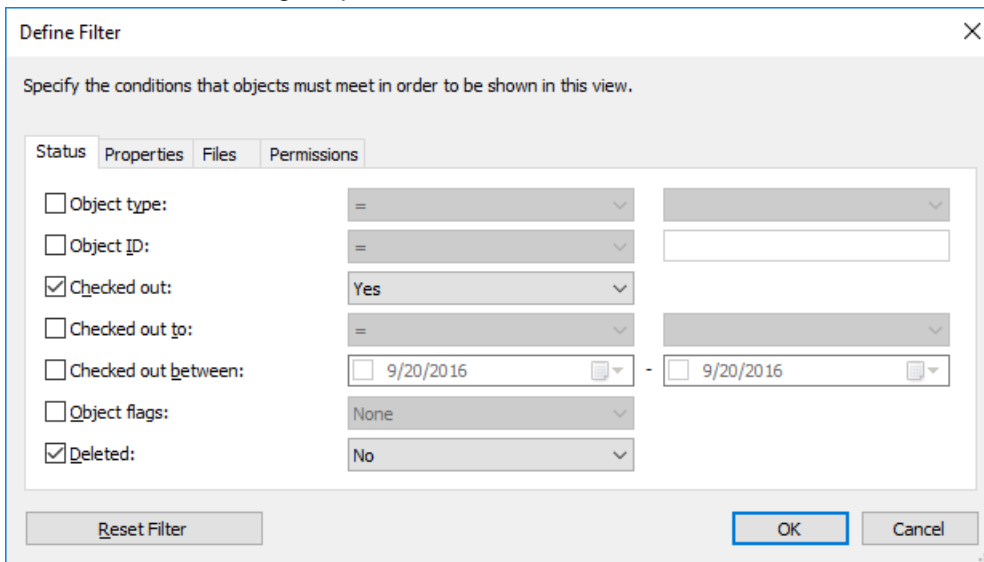
6. On the **Properties** tab, click **Add Condition** and add the following condition:

   a) From the **Property** drop-down menu, select **Project**.
   b) Select **=** from the **Operator** drop-down menu.
   c) From the **Value** drop-down menu, select a desired project.

7. Click **OK** to close the **Define Filter** dialog and to return to the **Offline Filter Properties** dialog.

8. If unchecked, check the **Show documents and other objects** check box.

9. Click **OK** to finish creating the offline filter.

The offline filter you have created appears under **Other Views** > **Offline**. Every document and object in this view can be accessed even when the connection to M-Files Server in unavailable.

New Traditional Folder

You can create *traditional folders* in M-Files. These folders do not have the additional properties provided by views. Traditional folders are comparable to, for example, folders on your `C:\` drive and can be used for importing files to M-Files. Traditional folders allow you to retain the original folder structure of the imported files. For more information about traditional folders, refer to *Import Files and Folders* on page 104.

Creating a New Traditional Folder

1. In M-Files Desktop, press `ALT` to display the menu bar and select **New** > **Traditional Folder** from the menu.

2. Optional: Right-click the traditional folder that you have just created and select **Rename** to rename the folder.

A new traditional folder is created and added in the **Traditional Folders** view. You can use the folder for importing files and folders to M-Files.

Add File

The *Add File* function is used for creating new document files for a *multi-file document*.

It should be noted, however, that a multi-file document in M-Files does not equal to a folder in Windows. A multi-file document is a single document that contains zero or more document files and one common set of metadata.

A document file is a fixed component of a multi-file document. For example, a contract scanned from a paper copy can be a multi-file document and its pages can be the document files.

📄 **Note:** Use the *Import File...* function to add an existing file to the multi-file document. Alternatively, you can drag and drop a file on top of a multi-file document.

Check out the multi-file document to which you want the new document file to belong, and select an extension for the new document file. In this case, any metadata for the new file does not need to be filled in as the document file is part of an entity.

Name ▲	Size	Date Modified	
▲ 📗 Employment Agreement / A...		6/22/2011 6:52 PM	

Open
Windows Commands >
New >
Make Copy...
Add File >
   🖼 bmp: BMP File
   📇 contact: Contact File
   📄 docx: Microsoft Word Document
   📁 library-ms: Folder
   📄 mdb: Microsoft Access Database
   📄 pptx: Microsoft PowerPoint Presentation
   📄 pub: Microsoft Publisher Document
   📄 rtf: Rich Text Format
   📄 txt: Text Document
   📄 xlsx: Microsoft Excel Worksheet
   📄 zip: Compressed (zipped) Folder

   Other Extension...
   Add File from Scanner...
   Import File...

Check Out Ctrl+O
Offline Availability >
History Ctrl+H
Relationships Ctrl+L
Comments Ctrl+M
Workflow >
Archiving >
Scanning and Text Recognition (OCR) >
Cut Ctrl+X
Copy Ctrl+C
Sharing, E-mail and PDF >
Get Hyperlink...
Share Public Link...
Add to Favorites
Delete Del
Rename F2
Properties Alt+Enter

Figure 42: The "Add File" function.

Import Files and Folders

Import Files and Folders allows you to easily import even large numbers of files to M-Files. Selecting this function (*New* > *Import Files and Folders...* from the menu bar) opens a dialog box where you can specify which files and folders are to be imported and how they should be organized.

📄 **Note:** You can also drag and drop files straight to M-Files Desktop. After dropping the file(s), M-Files reacts as you would be creating a new object or new objects (see *Creating a Document* on page 58).
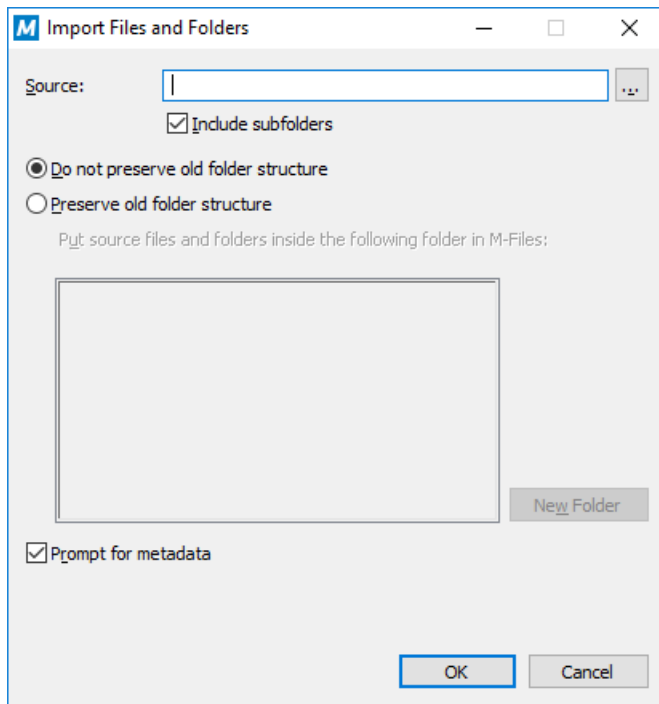
Figure 43: The "Import Files and Folders" dialog.

Source

Select the source from which you wish to import files or folders to M-Files.

Include subfolders

If you wish to also import the subfolders and their contents from the selected source, activate *Include subfolders*.

Do not preserve old folder structure

If you wish to transfer the files to M-Files without preserving the folder structure, select *Do not preserve old folder structure*. The imported documents will now appear, as usual, in M-Files views sorted by their metadata.

Preserve old folder structure

When you select *Preserve old folder structure*, you can continue to use the old folder structure also in M-Files. Select the traditional folder where you wish to import the files or folders. To create a new traditional folder, click **New Folder**. M-Files will now preserve the folder structure of the files and folders that are transferred. You can explore the structure by going to the traditional folder where you imported the material. The imported documents appear both in traditional folders and in M-Files view folders sorted by their metadata.

Prompt for metadata

If you wish to enter metadata for the documents when transferring them, select *Prompt for metadata*. For example, if you are transferring memos to M-Files, select the document class *Memo* in the metadata card, then select *OK to all*. All imported documents will now be classified as *Memos*.

If you leave this box unchecked, all imported files will be assigned to the document class *Unclassified Document*. This way, you may add document metadata later on.

Permissions

Specify permissions for the imported files and folders. The *Permissions* field is visible only if no other properties are defined for the documents. Otherwise, permissions are defined on the metadata card.

Transferring Folders to M-Files by Using the Import Files and Folders Dialog

1. In M-Files, press **ALT** to open the menu bar.

2. Select **New** > **Import Files and Folders...**

3. Click **...** to select the folder you want to import.

4. Select:

   a. **Do not preserve old folder structure** to discard the folder structure of the folder you are importing.

      or

   b. **Preserve old folder structure** to preserve the folder structure of the folder you are importing. You need to select a folder in M-Files for the content to be imported. You can create a new folder by clicking **New Folder**.

5. Optional: Uncheck the **Prompt for metadata** check box if you do not want to add metadata for the content you are importing.

6. Click **OK**.

   If you checked the **Prompt for metadata** check box, do the steps from 7 to 9 for every file you are importing.

7. In the **New Document** dialog, select an appropriate class for the file from the **Class** drop-down menu.

8. Enter other optional property values.

   ⓘ Click **Add property** to add additional properties.

9. Click **Create**.

The folder is imported to M-Files. If you chose the **Preserve old folder structure** option, the imported folder appears as a new traditional folder in M-Files.

Convert to Document

If documents are imported to M-Files in some unusual manner, such as by using a command prompt, M-Files indicates these temporary local files with a grayed-out icon. If you want to convert a temporary local file into a regular M-Files document, choose the temporary local file and select the *Convert to Document* function.

5.3. "Operations" Menu

This section describes the functions under the *Operations* menu.

Make Copy

To copy an object in the document vault, use the *Make Copy...* function. This function creates an entirely new object using the metadata and contents of the source object. The version history is not copied to the new object.

Check Out

Checking an object out for editing is an M-Files function that prevents the concurrent editing of an object. A checked out object can be viewed by other users (is read-only while checked out).

▶ Video: *Editing Documents*

When you are opening a document that has not yet been checked out, the following message is displayed:
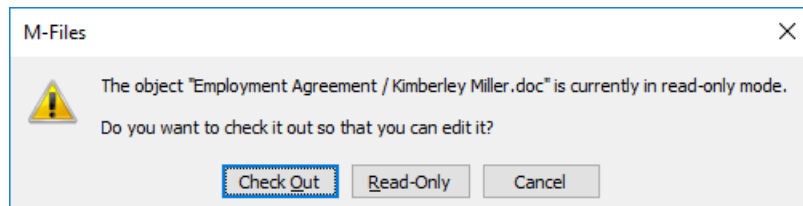
Figure 44: The check out message.

When you check out a document, a small check mark appears on the document icon to indicate that it has been checked out to you. A red sign indicates that the document has been checked out to someone else, in which case you are only able to open it in the read-only mode.

Figure 45: An object checked out to someone else and an object checked out to you.

Functions without checkout

You can add files to and remove files from a multi-file document without checking it out for editing. You can also rename and replace files without checking them out.

Check Out for Co-authoring

M-Files also allows for co-authoring, meaning that several users can edit the same document simultaneously. Even a person without an M-Files account can participate in the co-authoring process. This type of co-authoring is possible via the *Microsoft OneDrive* service.

▶ Video: *Co-Authoring*

By modifying the registry settings, co-authoring can be enabled for SharePoint as well. In this case, sharing is performed via SharePoint instead of OneDrive.

Checking out for co-authoring and check-in to M-Files

When you want to share the file for editing in OneDrive, use the *Check Out for Co-authoring* function. If you want to share a file in a multi-file document for co-authoring, use the *Begin Co-authoring* function. If you already have checked out a single-file document, you can start co-authoring from this state with the *Begin Co-authoring* function.

When the file is uploaded to OneDrive for co-authoring, it becomes available to several people.

M-Files displays the following message:
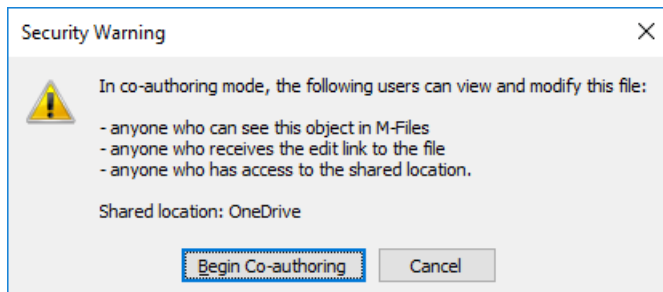
Figure 46: Individual users and user-specific rights cannot be individualized in co-authoring.

M-Files then directs you to enter your Windows Live ID. When you move to OneDrive, you will be presented with verification questions. You can proceed by answering *Yes* to these. You get a message when the file is ready to be shared via OneDrive and you can send the OneDrive link to other users. Please note that anyone with the link can view and modify the file.

When you perform the *Send Link* function, M-Files automatically creates an e-mail message that includes the filename and a link to the file in OneDrive.

After making the necessary changes, or if for some other reason you do not want to keep the file in co-authoring mode anymore, return from co-authoring mode so that other M-Files users can check it out for editing in M-Files or OneDrive.

The M-Files user who checks the document out for co-authoring must be the one who checks it in. Other M-Files users cannot check the document in from co-authoring. This M-Files user is responsible for the changes made in the document: the changes made from co-authoring mode are logged against the M-Files user who checked the document out for co-authoring and checked in the new version of the document in M-Files.

You can reject the changes made in co-authoring mode with the *Undo Checkout* function during check-in.

After checking in of the document in M-Files, it is no longer available in OneDrive. If you want to share the document in co-authoring mode again, check the file out for co-authoring and send a new OneDrive link to the file.

Editing in co-authoring mode

When you have received a link to a file that is in co-authoring mode, you can edit it normally in, for example, Word or PowerPoint.

With the co-authoring mode, you can edit mainly Office files in Microsoft Office 2010 (or later) or by using Office Web Apps. More than one user can, for example, edit the same Word file at the same time in Microsoft Office. A PowerPoint presentation can be edited by several users simultaneously in Microsoft Office's PowerPoint 2010 (or later).

The M-Files functions (for instance adding metadata to the content) are not available during editing in OneDrive.

M-Files users can also take part in co-authoring with the OneDrive link or directly from M-Files. When the object is checked out for co-authoring in M-Files, other M-Files users can also edit it via co-authoring mode in OneDrive or open its latest version in read-only state.

Editing an Office Document in the Co-Authoring Mode

You need to have a Microsoft account for co-authoring Office documents. If you do not have one, you can create the account the first time you check out an object for co-authoring.

1. Locate the object you want to make available for co-authoring in M-Files.

2. Either:

a. Right-click the object and select **Check Out for Co-authoring** from the context menu.

    or

b. Right-click the object and select **Begin Co-authoring** from the context menu if the file is part of a multi-file document or if it is already checked out to you.

☑ The **Security Warning** dialog is opened.
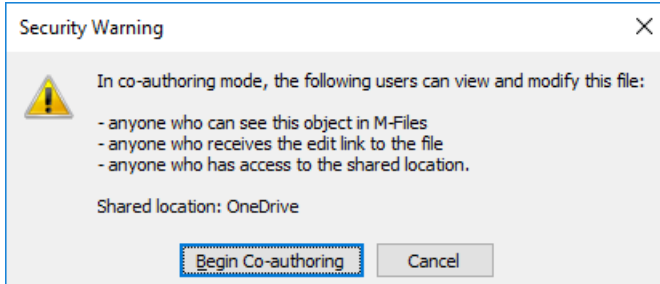
3. Click **Begin Co-authoring** in the **Security Warning** dialog.

4. Optional: If you are not yet logged in to OneDrive, enter your Microsoft account credentials in the login dialog and click **Sign in**, and when M-Files asks for your permission to access your information and to access and edit your OneDrive, click **Yes**.

5. In the **Co-authoring** dialog, click **Send Link** to send the shared object link to co-authoring participants via your mail client.

    ⓘ You can also right-click the object you have checked out for co-authoring and select **Send Co-authoring Link...** whenever you want to share the co-authoring link to someone.

    ⓘ Please note that anyone with the link can view and modify the file.

6. Double-click the object in the listing area to begin co-authoring.

    ☑ The document is opened in a web browser in Office Online.

7. Click **Edit in Browser** in the upper right corner to begin editing in the co-authoring mode.

    ⓘ M-Files functions (such as adding metadata to the content) are not available during co-authoring.

8. Optional: Click **Open in Word** (or **Open in Excel** or **Open in PowerPoint**) above the Office ribbon to begin co-authoring in the desktop application.

9. Save your changes if you are using the desktop application.

    ⓘ Office Online automatically saves your document when you make changes to it.

10. Close the document.

11. Right-click the object in M-Files, and select **End Co-authoring** from the context menu.

12. Finally, right-click the object again and select **Check In** to check in the changes.

    ⓘ The user who checks out the document for co-authoring must be the one who also checks it in. This M-Files user is responsible for the changes made in the document. The changes made during co-authoring are attributed to the user who checked out the document for co-authoring and checked in the new version.

ℹ️ You can reject the changes made in co-authoring by right-clicking the object and selecting **Undo Checkout** from the context menu.

The changes made by you and anyone else during co-authoring are saved to M-Files. After checking in the document, it is no longer available in OneDrive. If you want to share the document for co-authoring again, check out the file for co-authoring and send a new OneDrive link to the file.

Participating in Co-Authoring

When a document has been checked for co-authoring, there are two ways you can take part in co-authoring the document.

1. Either:

   a. If you receive a link to a co-authored document, click the link to open the document in the co-authoring mode.

      or

   b. Locate the co-authored document in M-Files and double-click it to open it in the co-authoring mode (a co-authored document is marked with a red cloud on top of its icon) and click **Edit (Co-authoring)** in the **Co-authoring** dialog.

2. Click **Edit in Browser** in the upper right corner to begin editing in the co-authoring mode.

3. Optional: Click **Open in Word** (or **Open in Excel** or **Open in PowerPoint**) above the Office ribbon to begin co-authoring in the desktop application.

4. Save your changes if you are using the desktop application.

   ℹ️ Office Online automatically saves your document when you make changes to it.

5. Close the document.

The changes you made to the document are saved to M-Files once the user who started the co-authoring has ended the co-authoring and checked in the document.

Check In

When you have edited and saved a document and are no longer using it, you should save the changes on the server with the **Check In** function. After this, other users will be available to check the document out and edit it. The easiest way to see all documents checked out to you is to open the *Checked Out to Me* view, which can be found in every document vault.

Check in with comments

You can easily comment on changes you made when checking in an object. The *Check In with Comments* option opens a text box for entering a free-form description of the changes you made. The comments are displayed in the *Comments* view of the object's metadata card.

📄 **Note:** Comments retain their permission settings. This means that they are visible only to the users defined in the permission settings that were in use when the comment was added.

Undo Checkout

With the **Undo Checkout** function, you can undo checking a document out without saving the changes on the server. In this case, you will lose all changes you made to the document during the checkout. This function is

useful when you have checked a document out, made changes and saved the document, but do not want the changes to take effect. In other words, you want to restore the document to how it was before you checked it out.

If the document has never been checked in, it is deleted when the *Undo Checkout* function is used.

Properties

This function opens the object's metadata card in a detached window.

Offline Availability

You can mark objects to be available in the offline mode. See also *New Offline Filter* on page 102.

Mark for Offline Availability

You can use the *Mark for Offline Availability* function to specify the documents and other objects to be available without a network connection. The selected documents will be shown in the *Offline* view.

You can select individual objects, a group of objects, view entities, or virtual folders to be available offline. If you select a view or virtual directory to be available offline, M-Files creates a new offline filter corresponding to the view in question. This way, all new objects conforming to the filter conditions will automatically be available offline according to the filter settings. You can also edit the offline filter you have created. For more information about off-line filters, refer to *New Offline Filter* on page 102.

You can move between the offline and online modes by using the **Go Online** and **Go Offline** functions. For more information, refer to *Go Offline* on page 126 and *Go Online* on page 126.

Remove Offline Availability

You change an object so that it is no longer available offline by using the *Remove Offline Availability* function.

History

One of the many advantages of M-Files is the fact that the earlier versions of objects are retained. You can go back in the object history according to the times the object has been checked out and checked back in.

▶ Video: *Version History*

When you create a document and check it in, the first version of the document is saved on the server. When you later check out the document and open it, make changes, save the document and check it back in, the second version of the document is saved on the server. You can later return to either of these two versions.
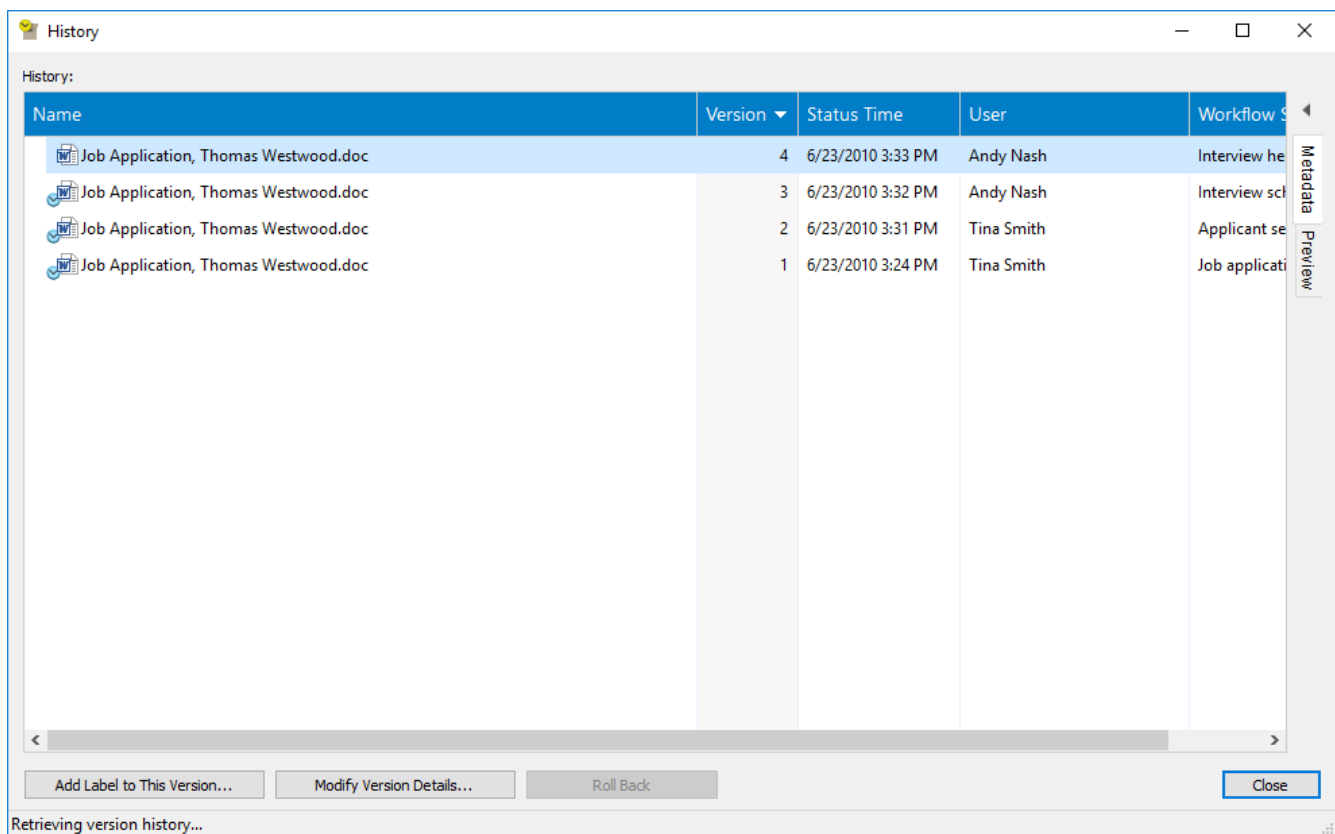
Figure 47: The "History" window.

Add label to this version

You can assign a label to a document version. The label will be displayed under Version Label in the History window. To assign a label, click **Add Label to This Version** and select a label from the pull-down menu. You can also add a new version label to the list by clicking the small arrow by the field and selecting the *Add New Value to List* function. As a default, no labels are assigned to any version.

Clear this label from the other versions of the object

If you have the **System administrator** server role or the **Full control of vault** vault user rights and if you want the selected label to be cleared from the other versions, check the *Clear this version label from the other versions of the object* box. This is useful if you want only one version of a contract to be labeled as approved.

Modify version details

The *Modify Version Details* function allows you to assign one or more version labels to the document version and to add a free-form comment that will be displayed in the History window. These comments are also displayed in the comments view of the object's metadata card and in the comment history of the *Comments* function (see *Comments* on page 116).

Roll back

As a default, the different versions of an object are listed from the oldest to the newest on the basis of their creation date. You can restore old versions of documents with the *Roll Back* function.

The function creates a new version of the document with the contents of the old version while preserving any intermediate versions. This function is useful when you have made and saved changes in a document but do not want them to take effect. You can use the *Roll Back* function only when the document is not checked out.

📄 **Note:** You need to have the appropriate permissions on the object in order to be able to restore a previous version of it. For example, if you are rolling back to a previous version where the permission settings and the metadata of the object have changed, you need to have the *change permissions* and *edit* rights on the object. If, on the other hand, only the metadata or the contents of the object have changed, you must have at least *edit* rights on the object.

Version History and Permissions

To be able to access a previous version of an object, the user needs to have access rights to the version in question as well as to the latest checked in version.

▶ Video: *Version History and Permissions*

Relationships

You can define relationships between objects in order to link interrelated documents. For instance, an offer could contain an offer document and a related price list along with a company brochure. Each object can be updated separately and they have separate version histories. The objects do not need to be copied unnecessarily.

You can access the **Relationships** dialog either via the context menu of an object or by selecting an object, then pressing the *Alt* key on your keyboard, and selecting **Operations** > **Relationships**.

📄 **Note:** You need to have the object checked out to make any modifications to its relationships.
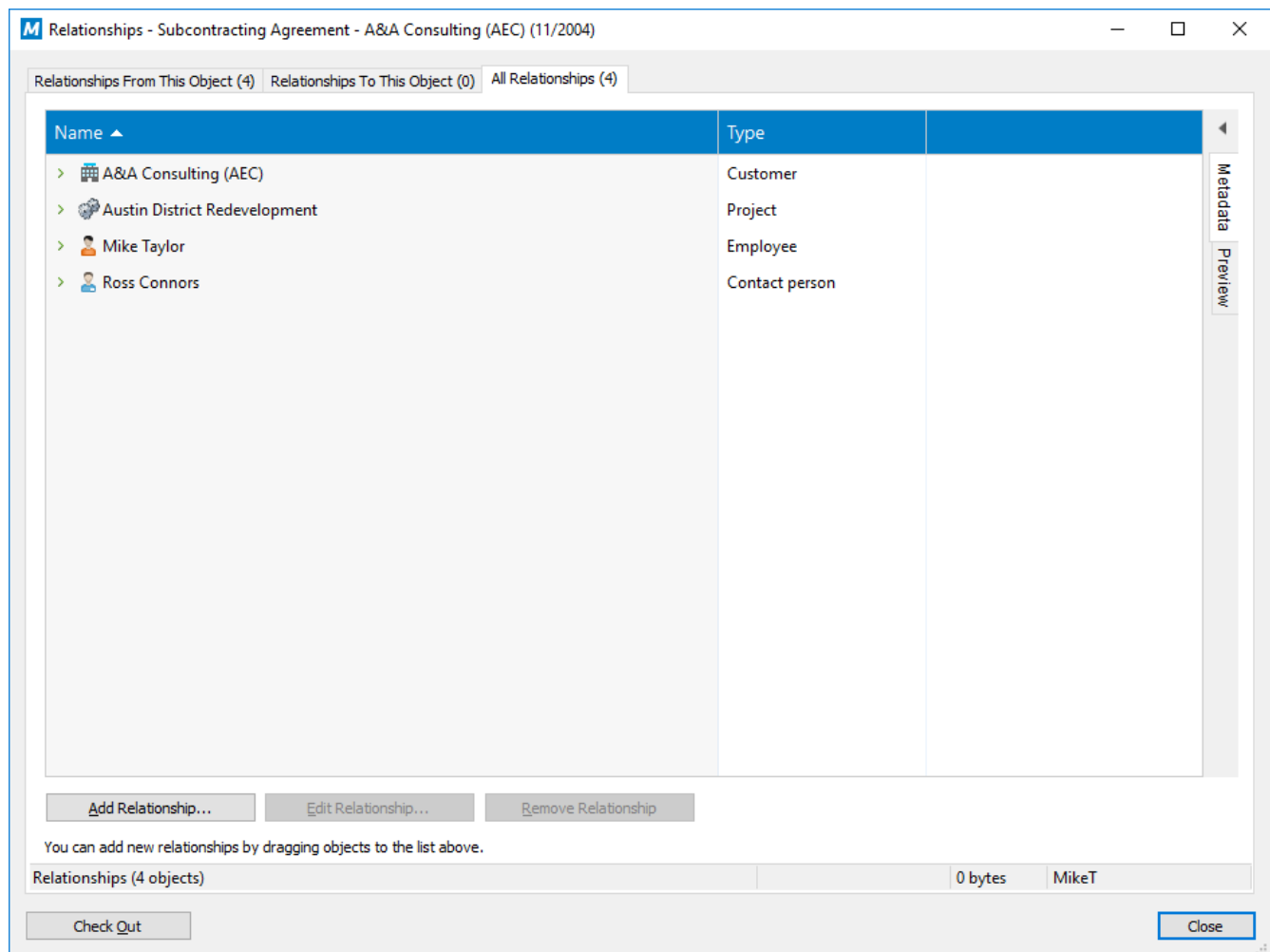
Figure 48: The "Relationships" dialog.

By using relationships, you can define metadata connections between objects, just as via the metadata card. For example, you can link a customer with an object. The customer then also appears in the object's metadata. Likewise, the relationships entered via the metadata card will appear in the *Relationships* window.

The dialog window contains three tabs representing the relationships *from* and relationships *to* the object, as well as one for *all relationships*.

> 📝 **Tip:** You can utilize the properties of a related object in creating indirect views and searches or in defining filter settings (see *Indirect searches* under *Advanced Search* on page 144).

Add Relationship, Edit Relationship, Remove Relationship

Use the buttons along the bottom of the dialog to add, edit, and remove relationships. To add several objects at once, you can drag and drop objects from other windows.

Latest version, Specific version

When you add a relationship, M-Files prompts for the desired behavior regarding the version of the added object. You can set the relationship to always apply to the latest version or to the current version.

Adding a Relationship Between Two Objects

1. In M-Files, locate and highlight the object from which you want to add a relationship to another object.

2. Either:

   a. Press ALT to display the menu bar and select **Operations** > **Relationships**.

      or

   b. Right-click the object and select **Relationships**.

3. Either on the **Relationships From This Object** or **All Relationships** tab, click the **Add Relationship...** button.

4. In the **Select Target Object** window, locate the object to which you want to add a relationship from this object and click **Open**.

5. Select either:

   a. **Latest version** if you want the relationship to always point to the latest version of the object.

      or

   b. **Specific version** if you want to add a relationship to the current version of the object, so that if the object is updated, the relationship still points to the object version that was the latest version of the object when the relationship was created.

6. Click **OK** to create the relationship.

The objects between which you have added the relationship should now have relationship links to each other. When you expand either of the objects in the listing area, you should see the linked object under the node representing the type of the referenced object, for instance **Documents** or **Customers**.

Relationships Between Objects in Separate Vaults

Relationships can also be created between objects residing in different vaults. Then the objects are not exported from a vault to another but the relationship is created by referring to an object in another vault, that is, a link is created to the original object.

You can create a relationship by dragging an object from one vault to another or by using the *Relationships* function in the same way as when adding a relationship to an object in the same vault.

In addition, you can replace a file with a file in another vault as if the two files were in the same vault.

Shortcuts

The related object in another vault is displayed as a shortcut in the target vault. When you double-click this object, M-Files shows the object in the original vault in the same way as when M-Files shortcuts are used.

In the target vault, you can see the basic properties of the related object (shortcut) and information for the original vault, but the actual changes and opening of the object are performed in the original vault. You must have permissions for the original vault and original object if you want to view and edit the related object in the original vault.

You can rename the shortcut in the target vault if so desired; this change does not change the name of the original object in the source vault and does not cause any conflicts between vaults.

Shortcut permissions

The shortcuts have their own permissions. The default setting is the target vault's default permission for new objects set by object type.

Shortcuts created through synchronization

When data is synchronized between vaults, for such purposes as archiving or publishing, shortcuts are created in certain cases through metadata of the imported objects. For example, if a document related to a certain project is imported to the target vault but the project is not imported, M-Files creates a shortcut for the project in the target vault. Then this shortcut is a link to an object in the other vault. The requirement is that the *Project* property definition be associable between the source and target vaults. The metadata definitions themselves must always be associable so that their related objects and values can be displayed or imported as shortcuts.

Requirements

M-Files automatically creates a relationship to objects that have a built-in object type (for instance, *Document* or *Document collection*). If the object type of the object is created by the user (*Customer*, *Project*, etc.), you should ensure that the metadata definitions of the object types can be matched between vaults.

Collection Members

The "Collection Members" function opens a dialog for viewing and editing document collection members. For more information about document collections and editing them, refer to *New Document Collection* on page 89.

Subobjects

Objects can also have subobjects. For example, a customer object may have a contact person as a subobject. The system administrator can define object types and relationships between them via M-Files Admin.

The *Ctrl+J* shortcut displays the object's subobjects and allows you to edit and remove them if necessary. This function enables, for instance, adding a new contact person directly by finding the desired customer from the document vault and using the *Subobjects* function to create a new contact person.

Browsing Relationships

Objects frequently have relationships with other objects. For example, a document is often attached to a project or a customer. Relationships are defined separately for each object. For more information, refer to *Relationships* on page 113.

The objects related to the current object can be viewed by right-clicking the object and selecting **Subobjects** (or the name of the subobject if the object has only one subobject specified), if relationships between object types have been specified in M-Files Admin (disabled by default). For more information, refer to *Creating a New Object Type* on page 259.

Related objects are always shown in the listing view (search result or view), regardless of whether relationships between the object types have been specified in M-Files Admin. This allows you to easily browse, for example, documents and contact persons related to the project, directly from the listing view. You can also move from one object to another by using relationships. For example, you can move from a document to the related object, from a project to the customer, or from a customer to the contact.

Comments

You can attach free-form comments to objects in the document vault with the *Comments* function. Saved comments are saved and displayed in the comment history.

> **Note:** Comments retain their permission settings. This means that they are visible only to the users defined in the permission settings that were in use when the comment was added.

The *Comments* function can be accessed by right-clicking an object and selecting *Comments* from the context menu or via the metadata card.

Also refer to *Check in with comments* under *Check In* on page 110.

Workflow

Each document has a lifecycle, during which it is processed and edited. During the lifecycle, the contributors may change and different persons may be responsible for different decisions. However, it is important that every person participating in the process is aware of their own areas of responsibility and the working stage.

The M-Files workflows enable modeling document lifecycles according to real world processes. The workflows are grouped into states that represent the working stages of the document or other object.

Workflows can be created and modified via the M-Files Admin. For more information about workflows, refer to *Workflows* on page 313 under *Document Vault Administration* on page 223.

Workflows and workflow state transitions can be selected in M-Files Desktop via the workflow controls at the bottom of the metadata card.

Change state

The *Change state* function enables you to select a state transition for the object, thus moving it to a new workflow state. If a workflow has been defined for the object, you can also change its state with the state transition name commands directly in the context menu. By using the *Change state* function, you can also add comments to the object while you are moving the object to a new workflow state.

Electronic signatures

If an electronic signature has been defined for the state transition, you must give your authentication data (user ID and password) and log in in order to perform a state transition. In order for the state to change, the object must be checked in. Transitions requiring a signature can only be performed one object at a time.

The electronic signature does not refer to an electronic "fingerprint"; it always requires entering the user identification and logging in. For more information, see *Electronic Signature* on page 329.

Scanning and Text Recognition (OCR)

Paper documents can be added to M-Files by using a network scanner or a local scanner. For more information on network scanning, refer to *Scanner Sources* on page 358. When using local scanning, the scanner must be

directly connected to the computer that is used to add the scanned file to M-Files. The scanning functions are located under the **Operations** menu.

> 📄 **Note:** Scanner integration in M-Files Desktop uses the TWAIN and WIA technologies. Only scanners that can be equipped with a TWAIN or WIA driver are supported.

> 📄 **Note:** The text recognition functionality requires the *M-Files OCR module*, an M-Files add-on product available for an extra fee. It can be activated with a license code. You also need to have installed the necessary files for the OCR module. Refer to *Enabling the M-Files OCR Module* for more information.

Adding Documents from the Scanner

1. In M-Files, press ALT to display the menu bar and select **Operations** > **Scanning and Text Recognition (OCR)** > **Add Document from Scanner...**

   > ⓘ Alternatively, you can right-click an empty space in the listing area and select **Scanning and Text Recognition (OCR)** > **Add Document from Scanner...** from the context menu.

2. Optional: If the **Select Source** dialog appears, select your scanner from the list and click **Select**.

3. Scan your document using the scanner application.

   > ✅ When the scanning is complete, the **Scanner Job** dialog appears.

4. Select one of the following options:

Select the option...	If you...
Scanning done	do not want to scan additional documents.
Scan more pages to the current document	want to scan another document and combine it with the previously scanned document.
Scan another document	want to scan another document and do not wish to combine it with the previously scanned document.

5. Optional: If the **Conversion to Searchable PDF** dialog appears, select **Convert** if you want to convert the scanned document into a searchable PDF. Otherwise, click **Skip Conversion**.

6. When the **New Document** dialog appears, fill in the metadata and click **Create** once you are done.

The scanned document or documents are added to M-Files.

Adding Documents from the Scanner to a Multi-File Document

1. In M-Files, locate the multi-file document for which you want to add a file from the scanner.

2. Right-click the multi-file document and select **Add File** > **Add File From Scanner...** from the context menu.

3. Optional: If the **Select Source** dialog appears, select your scanner from the list and click **Select**.

4. Scan your document using the scanner application.

   > ✅ When the scanning is complete, the **Scanner Job** dialog appears.

5. Select one of the following options:

Select the option...	If you...
Scanning done	do not want to scan additional documents.
Scan more pages to the current document	want to scan another document and combine it with the previously scanned document.

Select the option...	If you...
Scan another document	want to scan another document and do not wish to combine it with the previously scanned document.

6. Optional: If the **Conversion to Searchable PDF** dialog appears, select **Convert** if you want to convert the scanned document into a searchable PDF. Otherwise, click **Skip Conversion**.

The scanned document or documents are added to the multi-file document.

📝 **Note:** The multi-file document only has one set of metadata and separate files belonging to the multi-file do not have any separate metadata.

Replacing a Document with a Document from the Scanner

1. In M-Files, locate and highlight the document that you want to replace with a document from the scanner.

   ℹ Single-file documents and documents in a multi-file document can be replaced with a document from the scanner.

2. Press ALT to display the menu bar and select **Operations** > **Scanning and Text Recognition (OCR)** > **Replace with File from Scanner...**

   ℹ Alternatively, you can right-click the document and select **Scanning and Text Recognition (OCR)** > **Replace with File from Scanner...**

3. Optional: If the **Select Source** dialog appears, select your scanner from the list and click **Select**.

4. Scan your document using the scanner application.

   ☑ When the scanning is complete, the **Scanner Job** dialog appears.

5. Select one of the following options:

Select the option...	If you...
Scanning done	do not want to scan additional documents.
Scan more pages to the current document	want to scan another document and combine it with the previously scanned document.
Scan another document	want to scan another document and do not wish to combine it with the previously scanned document.

6. Optional: If the **Conversion to Searchable PDF** dialog appears, select **Convert** if you want to convert the scanned document into a searchable PDF. Otherwise, click **Skip Conversion**.

The existing document in M-Files is replaced with the document from the scanner.

Text Recognition (OCR) and Searchable PDFs

If the M-Files OCR module is enabled, M-Files suggests that the scanned file can be converted to a searchable PDF by text recognition once the scanning is completed. You can activate the text recognition or ignore it. You can also define advanced settings for the text recognition.

You can also convert an image file to a searchable PDF. The text recognition is performed on the image file in order to enable full-text searching across the file. After the conversion, you can find, for example, a contract document converted from an image by performing a search using the names of the contracting parties or any other text included in the original image file.

M-Files also automatically suggests the text recognition if you drag an image file to M-Files, provided that you have the M-Files OCR module installed.

Text recognition can be performed on the following file formats: TIFF, JPEG, BMP, PNG, and PDF. TIFF files using an alpha channel or JPEG compression are not supported. For more information, see *Searchable PDF* on page 355.

> 📝 **Note:** If the text recognition is performed on an image file which was not saved and returned to M-Files, the file will only be saved as a PDF. Otherwise, the original image file can be found in the document version history.

Importing and Converting an Image File to a Searchable PDF

1. Drag and drop an image file to M-Files.

2. Once the **Conversion to Searchable PDF** dialog appears, click **Convert**.

> ℹ️ By clicking **Advanced** in the **Conversion to Searchable PDF** dialog, you can improve the quality of the text recognition by selecting primary and secondary language options to match the language used in the image.

3. Once the conversion is complete, the **New Document** dialog appears. Finish importing the image by filling in the metadata and clicking **Create**.

Converting an Existing Image File in M-Files to a Searchable PDF

1. In M-Files, locate and highlight the image file that you want to convert to a searchable PDF.

2. Right-click the file and select **Scanning and Text Recognition (OCR)** > **Convert to Searchable PDF...** from the context menu.

> ℹ️ Alternatively, you can press ALT to display the menu bar and select **Operations** > **Scanning and Text Recognition (OCR)** > **Convert to Searchable PDF...**

3. When the **Conversion to Searchable PDF** dialog appears, click **Convert** to convert the image file.

The image file is converted into a searchable PDF and any textual content in the image can be found using the search functions of M-Files.

Archiving

When documents are no longer actively needed in the document vault, they can be archived. For example, the system administrator can store all documents marked for archiving by users in a separate archive file, from which they can also be restored to active use.

Mark for archiving

With the *Mark for Archiving* function, you can specify documents to be archived. The archiving, which is performed in M-Files Admin, moves the marked documents from the document vault to a separate archive file. For more information, refer to *Content Replication and Archiving* on page 375.

Clear archiving marker

You can remove a document's archive definition by using the *Clear Archive Marker* function.

Undelete

The *Undelete* function can be used to restore deleted objects. First find the deleted item either from the *Deleted* view or with the detailed search, and then select *Undelete* from the item's context menu.

You can see deleted objects only if you have *full control of the document vault*, *permission to see all objects* or *permission to see deleted objects*.

▶ Video: *Delete, Undelete, Destroy*

Convert to Single-file Document

You can convert a multi-file document to a regular single-file document by selecting *Convert to Single-file Document* from the item context menu. This can be done only if the original multi-file document contains exactly one document file.

Convert to Multi-file Document

You can convert a single-file document to a multi-file document with the *Convert to Multi-file Document* function. Multiple files can be included in the new multi-file document.

Replace with File

You can use the *Replace with File* function to select another document or file whose contents (data in the file) are to replace the contents of the document file selected earlier.

The first version of the replaced document file will nevertheless be kept, as M-Files made a new version of the document when it was checked out. The metadata remains unchanged, so the function affects the data in the file only. You can view the versions by using the *History* function (see *History* on page 111).

Get Hyperlink

M-Files users may have document vault connections with different names, and each user may have different views. M-Files provides a function to create shortcuts that are not affected by these factors. Such links might be used for instance in e-mail messages with references to the organization's documents.

Select the *Get Hyperlink* function from the object's context menu. The dialog offers four different ways to share your link.
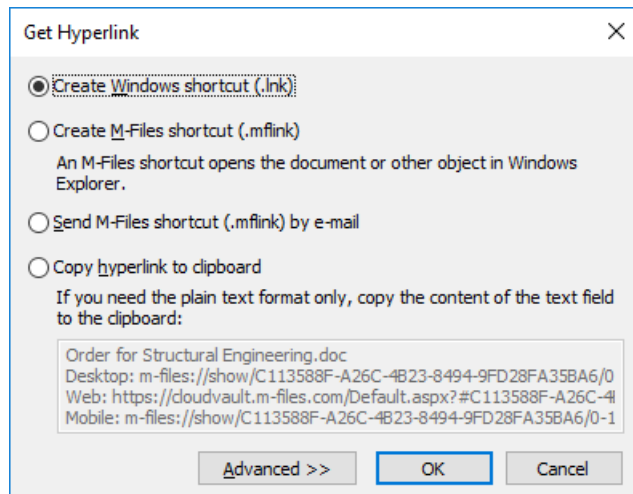
Figure 49: The "Get Hyperlink" dialog.

▶ Video: *Creating Object Links*

Create Windows shortcut and Create M-Files shortcut

Use these options to create a shortcut to your Windows desktop. Opening the Windows shortcut opens the document in the default application for the document type, and the M-Files shortcut opens the document or object in M-Files Desktop.

Send an M-Files shortcut by e-mail

This option automatically creates and opens a new e-mail message with a shortcut included in the message. The *Send Link by E-Mail* function under *Sharing, E-mail and PDF* creates a new e-mail message with shortcuts in the same way.

Copy hyperlink to clipboard

This option enables you to copy an object hyperlink to your clipboard. By using this option, you can ensure that the link remains usable even if the document is renamed. You can paste the link to e-mail messages in HTML format, or open the document directly in M-Files by entering the path in the Windows *Run* function.

If you need the link – or, for example, just the M-Files Desktop link – in plain text format only, you can copy the URL from the text field to your clipboard.

> 📝 **Tip:**
>
> The command in the plain text URL can also be manually changed if you want the link to do something else than to just open the object or file. The available commands are: *show*, *showmetadata*, *open*, *view* and *edit*. The table below describes how these commands function.
>
> | Command | Action |
> |---|---|
> | *show* | Displays the object in M-Files Desktop. |
> | *showmetadata* | Shows the metadata card for the object. |
> | *open* | Shows the check-out dialog and opens the document in the default application. |
> | *view* | Opens the document in the default application in read-only mode without prompting the user to check it out. |
> | *edit* | Checks out the object and opens it for editing in the default application. |
>
> For instance, the command *m-files://**edit**/<vault GUID>/<object name>-<id>* would check out the document and open it for editing in the associated default program.
>
> For more information about M-Files URL properties, refer to *this knowledge base article*.

Advanced

The advanced settings enable you to specify whether you want the link to always point to the latest version of the document (*Latest version*) or to the version that you have selected (*This version*).

Modifying the appearance of the hyperlinks

The appearance of the hyperlinks can be modified with a few registry settings. The registry settings can be added either to `HKEY_LOCAL_MACHINE`, `HKEY_CURRENT_USER`, or both. If both are used, `HKEY_CURRENT_USER` takes precedence.

In `HKEY_LOCAL_MACHINE`, the key name is: `HKEY_LOCAL_MACHINE\Software\Motive\M-Files \<`*version*`>\Common\Settings\Hyperlinks`.

In `HKEY_CURRENT_USER`, the key name is: `HKEY_CURRENT_USER\Software\Motive\M-Files \<`*version*`>\Client\MFShell\<`*vault*`>\Hyperlinks`.

For both keys, the actual settings are as described in the tables below.

Value name: `FriendlyNameModeForHTML`	
Value Type	REG_DWORD

Value name: `FriendlyNameModeForHTML`	
Description	Defines whether the object title acts as a link in the HTML version of the hyperlink. Values from 1 to 3 also define the type of the link.
Value Data	• 0: No hyperlink • 1: Desktop hyperlink (default) • 2: Web hyperlink • 3: Mobile hyperlink

📄 **Tip:** M-Files also adds the link to your clipboard in the XML Spreadsheet format for pasting the link to, for example, a cell in Microsoft Excel. The type of the link is specified via the `FriendlyNameModeForHTML` value. If its value has either been set to `0` or not been specified at all, the link opens the object in M-Files Desktop.

Value name: `CanShowSpecificLinks`	
Value Type	`REG_DWORD`
Description	Controls whether the HTML version of the hyperlink can include client-specific links after the object title.
Value Data	• 0: No client-specific links are appended. • 1: Client-specific links are appended as specified via the "SpecificLinksMode" value (see further below).

Value name: `SpecificLinksMode`	
Value Type	`REG_DWORD`
Description	If `CanShowSpecificLinks` is set to "1", controls which of the client-specific links are appended to the HTML version of the hyperlink after the object title.
Value Data	• 0: None • 1: Desktop • 2: Web • 3: Desktop and Web • 4: Mobile • 5: Desktop and Mobile • 6: Web and Mobile • 7: Desktop, Web, and Mobile

Value name: `PlainTextModeForClipboard`	
Value Type	`REG_DWORD`
Description	Controls the content of the plain-text version of the hyperlink copied to the clipboard.
Value Data	• 0: All hyperlinks • 1: Desktop hyperlink only • 2: Web hyperlink only • 3: Mobile hyperlink only

Send M-Files shortcut by e-mail

You can add or drag documents from M-Files to the e-mail in the same way as any other documents. You can also use the *Send M-Files shortcut by e-mail* function. With this function, M-Files creates a new e-mail message with a copy of the file attached.

Web links

It is also possible to use web links to share documents contained in M-Files. M-Files can be used as a content management system for sharing documents with interested parties. For more information, see *Document-specific Publishing via a Web Link* on page 191.

Creating Shortcuts

1. In M-Files, right-click the object for which you want to create a link and select **Get Hyperlink...** from the context menu.

   ☑ The **Get Hyperlink** dialog is opened.

2. Select one of the following options and click **OK**:

Select...	If you...
Create Windows shortcut (.lnk)	want to create a shortcut that opens the selected object in the default application for the file type.
Create M-Files shortcut (.mflink)	want to create a shortcut that displays the selected object in M-Files Desktop.

3. Click **Yes** when you are prompted to place the shortcut on your desktop.

The shortcut that you have just created is placed on your desktop. Double-clicking the shortcut, depending on the shortcut type, either opens the object in the default application for the file type or displays the object in M-Files Desktop.

Sending Shortcuts

1. In M-Files, right-click the object for which you want to create a link and select **Get Hyperlink...** from the context menu.

   ☑ The **Get Hyperlink** dialog is opened.

2. Select the **Send M-Files shortcut (.mflink) by e-mail** option.

A new e-mail message is opened in your e-mail client, containing the M-Files shortcut as an attachment.

Copying Hyperlinks

1. In M-Files, right-click the object for which you want to create a link and select **Get Hyperlink...** from the context menu.

   ☑ The **Get Hyperlink** dialog is opened.

2. Select the **Copy hyperlink to clipboard** option.

3. Either:

   a. If you want the link in HTML format, click **OK** to copy the hyperlink to the clipboard.

      or

b. If you want the link in plain text format, select and copy the text in the text field and click **Cancel**.

You now have the link to the selected object copied to your clipboard. If you chose the HTML format and you paste the link, for example, to a new Outlook message, the link is pasted to the message in the following HTML format, provided that you have HTML formatting enabled in Outlook:

Order for Structural Engineering.doc (Desktop, Web, Mobile)

If you copied the plain text format instead, or you paste the link in HTML format to an editor or e-mail client that does not support HTML formatting, the link is pasted as plain text.

Web Links

It is also possible to use web links to share documents contained in M-Files. This can be achieved in two ways:

- M-Files Web can be used as a content management system for sharing documents with interested parties. For more information, see *Document-specific Publishing via a Web Link* on page 191.
- Documents in M-Files can be shared publically by creating temporary public links to specific documents, making the documents available to anyone who is given the link. For more information, see *Share Public Link* on page 124.

Share Public Link

Documents in M-Files can be shared publically by creating temporary public links to selected documents, making the documents available to anyone who is given the link.

Before you begin, make sure that M-Files Web is up and running. See *Web and Mobile Access* on page 185 for instructions.

Do the following steps to create a public link:

1. In M-Files locate the object that you want to share using the search or views.

2. Optional: If you want to share an earlier version of the object, right-click the object and select **History**.

3. Right-click the object (or the object version) and select **Share Public Link...** from the context menu.

✅ The **Share Public Link** dialog is opened.

4. Use the **Expiration date (local time)** date and time picker to select the expiration date after which the public link will no longer be active.

5. Optional: In the **Description** field, enter a description for your shared item.

6. Click **Create Public Link**.

✅ The public link is created in the **Public link** field.

7. Click **Copy** to copy the public link to the clipboard.

8. Click **Close** to close the **Share Public Link** dialog.

You can now share the public link to anyone who may be interested. The link becomes inactive after the set expiration date. If you want to view or remove your shared public links, see *Managing and Removing Shared Public Links* on page 125.

Managing and Removing Shared Public Links

You can view and remove public links that you have shared in the **Shared by Me** window. Users with the administrative rights *Full control of vault* or *See and read all vault content* can see and manage the public links shared by all vault users.

1. In M-Files, click your username in the top-right corner and select **Shared by Me** from the context menu.

   ☑ The **Shared by Me** window is opened, displaying all the public links that you have shared.

2. To copy a shared public link to the clipboard, locate the desired link in the list, and click **Copy Link**.

3. To remove a shared public link, locate the desired link in the list, and click **Stop Sharing**.

   ☑ A confirmation dialog is opened.

4. Click **Yes** to confirm removing the public link.

The link that you have just removed is no longer active and can no longer be used to access the previously public object.

Sharing, E-mail and PDF

Share via OneDrive

Instead of using e-mail attachments, you can share individual files for reading and editing in *Microsoft OneDrive* also to people without an M-Files user account. In this case the editor/reader does not need to have a Windows Live ID either.

Share the file with these functions under *Sharing, E-mail and PDF*: *Share via OneDrive* or *Share via OneDrive as PDF*. The files can be shared in their original format (for instance *.docx*) or as PDF files.

The link can be sent in its full or in a shortened form. The shortened form is more convenient, but with confidential files, you should use the full form. Everyone who has access to the link, can read and edit the file. You can also copy the link from the dialog box for other uses.

> 📝 **Note:** If changes to a file are made in M-Files, the version of the file that is shared is not automatically updated in OneDrive. If you want the modifications made in M-Files to be visible in the OneDrive version, you need to share the file again and send a new link to the recipients.

You can manage the shared files via your OneDrive account (*https://onedrive.live.com/*). Previously shared files and currently redundant files should be deleted from time to time.

If you want to share, for instance, brochures and price lists in a way that the shared versions are automatically updated, you should utilize the *interaction between vaults* on page 202 for this kind of publication.

Send link by e-mail

With this function, M-Files creates a new e-mail message with a link to the file. The recipient must have access to the M-Files vault and the file.

Send (original or PDF version) by e-mail

You can send the file directly in PDF format, whereby the file will be converted to PDF format prior to sending. When the PDF file is ready, M-Files creates a new e-mail message with the PDF file already attached. Alternatively, you can send the file in its original format by choosing *Send Copy by E-mail*. In both cases, the file is sent as an e-mail attachment without any linking to M-Files.

Save as PDF

You can save a file directly as a PDF file by using the M-Files functions. This enables you to save the file in M-Files using the *Save as PDF* function without needing to open the file.

If you save a single-file document as a PDF file, M-Files creates a new document in PDF form with a metadata card. If you save a file in a multi-file document as a PDF file, M-Files suggests saving the file in the same multi-file document by default.

Convert to PDF

You can also convert a file to PDF. In this case, the original file (e.g., a Word file) is replaced with the corresponding PDF file.

You can use the function *Convert to PDF (adds separate file)*, when you want to keep the original version and then have a PDF of it. If converting a single-file document using this function, M-Files will convert it to multi-file document at the same time with PDF converting.

Go Offline

You can use M-Files without a network connection as well.

▶ Video: *Offline Mode*

Start using M-Files without a network connection by selecting the *Go Offline* function. You will then have access to the *Offline* view, which shows all documents and other objects that have been made available offline. In other words, the documents and objects in this view can be accessed even when a connection to M-Files Server is unavailable.

The *Go Offline* command prepares M-Files so that it can also be used offline. The same preparation procedures are performed during a normal logout and when Windows is being shut down.

For example: A sales representative is leaving the office to give a presentation to a customer. She makes a PowerPoint presentation and intends to present it offline. She will have no access to the corporate network from the customer premises, but M-Files offers access to the PowerPoint document through the *Offline* view.

You can make the desired documents and other objects available offline by using the *Mark for Offline Availability* function. For more information, refer to *Offline Availability* on page 111. Collection members, relationship objects, and subobjects are also automatically available offline if they are associated with objects marked as available offline.

When you are using the offline mode, you can create new objects and edit objects available offline.

Go Online

You can move back online from the offline mode by using the *Go Online* function. Once you are back in the online mode, M-Files restores all other views and you can continue browsing the document vault normally. You can also, for example, check in documents shown in the *Offline* view and thus save the changes on the server.

When switching to online mode, M-Files detects whether the changes made offline cannot be checked in to the server directly. For instance, somebody may have edited the document on the server while you were editing it offline. If the latest version checked in to the server matches the version you started to edit offline, the version edited offline can be saved as the new document version. In this case, no changes have been made to the object in question during offline editing. However, if the server contains a new versions created during the time offline, M-Files notifies the user, who can then choose from the following procedures:

- Save the version edited offline as a new document (the document on the server remains unchanged).
- Reject the changes made (accepts the new version on the server and rejects changes made offline).
- Cancel *Go Online*.

📝 **Tip:** If you check out the document online, editing offline should not create unclear situations. The user can edit the document normally while offline, and other users can see that the document is checked out to the user in question.

Log Out

You can log out from the document vault with the *Log Out* function. You can also log out via the menu in the upper-right corner of the user interface.

5.4. "Settings" Menu

This section offers a brief description of the *Settings* menu's functions.

M-Files Admin

Here you can start the M-Files Admin tool. For more information, refer to *M-Files Admin* on page 175.

Notification Settings (M-Files Desktop)

You can set M-Files to inform you by e-mail about certain events, for instance about changes made to objects. This is useful, for example, when you wish to keep track of modifications made to a certain document.

▶ Video: *Notifications Overview*

📝 **Note:** To be able to use this feature, event logging and notifications must be enabled on the M-Files server. For more information about server settings, refer to *Notification Settings (M-Files Admin)* on page 181.

You can access the *Notification Settings* dialog in M-Files Desktop by pressing the *Alt* key on your keyboard, and then selecting **Settings** > **Notification Settings** via the menu bar.

Notification Settings (MikeT)			✕
☑ Enable notification messages			
Notification rules			
Name ▲	ID	Type	Message Delivery
Assigned to me	1	Common	Separately
Monitored by me	3	Common	Disabled
New Documents	101	Common	As a digest message
New Requests for Proposal	102	Common	Separately
Reminder: Assigned to me	2	Common	As a digest message

Add...   Edit...   Remove

OK   Cancel
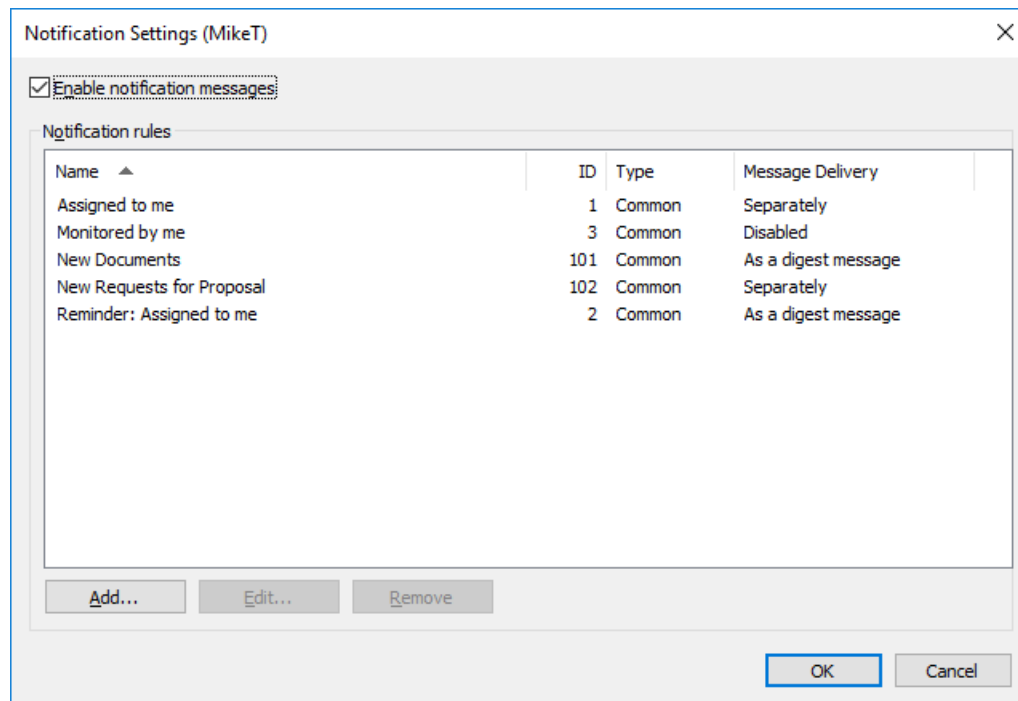
Figure 50: You can set M-Files to inform you by e-mail of modifications made to objects.

Notification rules

Open the *New Notification Rule* dialog by clicking the **Add...** button in the *Notification Settings* window.

Give the rule a name, and define a filter. The filter determines the group of objects to which the notification rule applies. For more information about filters, refer to *Define Filter* on page 97.

Then select the events that you wish to be reported about by e-mail.

▶ Video: *Creating Notification Rules*

Figure 51: The "New Notification Rule" dialog.

Message delivery: Notification messages disabled

Select this option to disable notification messages.

Message delivery: A separate notification message for each event

Select this option if you wish to receive a separate message for every event that meets the rule. The message is sent immediately whenever the notification rule is met.

📝 **Note:** If the option **Document or other object matches the conditions of the filter** is enabled in conjunction with this option, the notification message is delivered once a day at the same time as the digest message.

Message delivery: A digest message once a day

Select this option if you wish to be informed of events via a digest message once a day. The time when the message is sent is set by the system administrator in M-Files Admin. For more information, refer to *Notification Settings (M-Files Admin)* on page 181.

Private rule vs. common rule

If you want a notification message to be sent only to you, select *Private rule*. If you want a notification message to be sent to several selected recipients, select *Common rule*. M-Files Admin is used for specifying the permissions for creating a common rule. For more information, refer to *Creating a User* on page 31.

Recipients

Specify the users or user groups who will receive notifications on the basis of this rule.

Exclude notifications of events caused by the current user

Select this option if you do not wish to be informed of events caused by yourself, such as modifications that you yourself have made to an object.

📝 **Note:** This option has no effect if the option **Document or other object matches the conditions of the filter** is enabled.

Example: Daily Notifications for New Orders

This example shows how you can create a private notification rule for sending you a daily digest message of all the new order objects in the vault.

📝 **Note:** To be able to use this feature, event logging and notifications must be enabled on the M-Files server. For more information about server settings, refer to *Notification Settings (M-Files Admin)* on page 181.

1. Open M-Files Desktop.

2. Press the *Alt* key on your keyboard.

3. In the menu bar, select **Settings** > **Notification Settings**.

   ✅ The **Notification Settings** dialog is opened.

Notification Settings (MikeT)   ✕

☑ Enable notification messages

Notification rules

Name ▲	ID	Type	Message Delivery
Assigned to me	1	Common	Separately
Monitored by me	3	Common	Disabled
New Documents	101	Common	As a digest message
New Requests for Proposal	102	Common	Separately
Reminder: Assigned to me	2	Common	As a digest message

Add...   Edit...   Remove

OK   Cancel

4. Click the **Add...** button.

☑ A dialog for creating a new notification rule is opened.

Notification Rule Properties - New Notification Rule   ✕

General

Name: | |

Message delivery: | A separate notification message for each event ⌄ |

◉ Private rule. Applies to the current user only.

○ Common rule. Applies to the specified recipients only.

            Recipients...

Filter
Not deleted

            Define Filter...

Event subscriptions

Event	Notify
New document or other object	☐
Document or other object changed	☐
The state of a document or other object changed	☐
Document or other object matches the conditions of the filter	☐
Checkout	☐
Check-in	☐
Undo checkout	☐
Rollback	☐
File downloaded	☐
Document or other object deleted	☐
Document or other object destroyed	☐
One version of a document or other object destroyed	☐

☐ Exclude notifications of events caused by the current user

            OK   Cancel   Help

5. In the **Name** field, give your rule a name, such as *New orders*.

6. Change the **Message delivery** setting to **A digest message once a day**.

7. Click the **Define Filter...** button.

☑ The **Define Filter** dialog is opened.
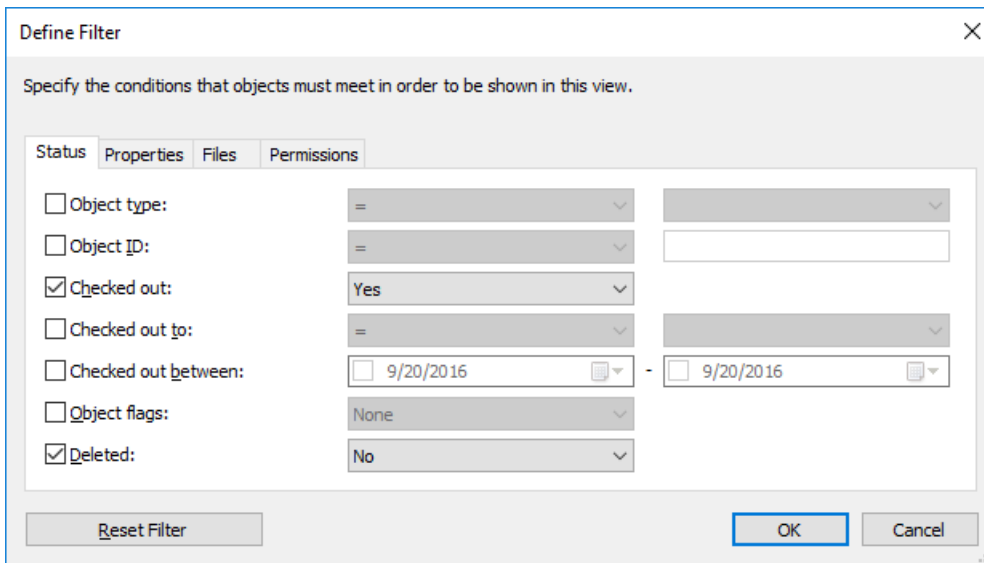
8. Open the **Properties** tab.

9. Click **Add Condition**.

10. For the newly added property condition, select *Class* as the property, = as the operator, and *Order* as the value.

11. Click **OK** to close the **Define Filter** dialog.

   ✓ You should now see the property condition *'Class' = 'Order'* in the **Filter** field of the **Notification Rule Properties** dialog.

12. Enable notifications for the event *New document or other object*.

13. Optional: If you do not want to receive notifications for order objects created by yourself, enable the option **Exclude notifications of events caused by the current user**.

14. Once you are done, click **OK** to save the rule and close the dialog.

The new notification rule is added to the list in the **Notification Settings** dialog.

Example: Reminder Messages for Assignments

This example shows how you can create a common notification rule for assigments that have their deadline in two days.

   📄 **Note:** To be able to use this feature, event logging and notifications must be enabled on the M-Files server. For more information about server settings, refer to *Notification Settings (M-Files Admin)* on page 181.

1. Open M-Files Desktop.

2. Press the *Alt* key on your keyboard.

3. In the menu bar, select **Settings** > **Notification Settings**.

   ✓ The **Notification Settings** dialog is opened.

Notification Settings (MikeT)   ✕

☑ Enable notification messages

Notification rules

Name ▲	ID	Type	Message Delivery
Assigned to me	1	Common	Separately
Monitored by me	3	Common	Disabled
New Documents	101	Common	As a digest message
New Requests for Proposal	102	Common	Separately
Reminder: Assigned to me	2	Common	As a digest message

Add...   Edit...   Remove

OK   Cancel

4. Click the **Add...** button.

☑ A dialog for creating a new notification rule is opened.

Notification Rule Properties - New Notification Rule   ✕

General

Name: |

Message delivery: A separate notification message for each event ⌄

◉ Private rule. Applies to the current user only.

○ Common rule. Applies to the specified recipients only.

    Recipients...

┌─ Filter ───┐
│ Not deleted   │
│   │
│   │
│   Define Filter...   │
│   │
└───┘

┌─ Event subscriptions ─────────────────────────────────────┐
│ Event   Notify   │
│ New document or other object   ☐   │
│ Document or other object changed   ☐   │
│ The state of a document or other object changed   ☐   │
│ Document or other object matches the conditions of the filter ☐ │
│ Checkout   ☐   │
│ Check-in   ☐   │
│ Undo checkout   ☐   │
│ Rollback   ☐   │
│ File downloaded   ☐   │
│ Document or other object deleted   ☐   │
│ Document or other object destroyed   ☐   │
│ One version of a document or other object destroyed ☐   │
└───┘

☐ Exclude notifications of events caused by the current user

            OK   Cancel   Help

5. In the **Name** field, give your rule a name, such as *Assigment reminder*.

6. Click the **Define Filter...** button.

✓ The **Define Filter** dialog is opened.
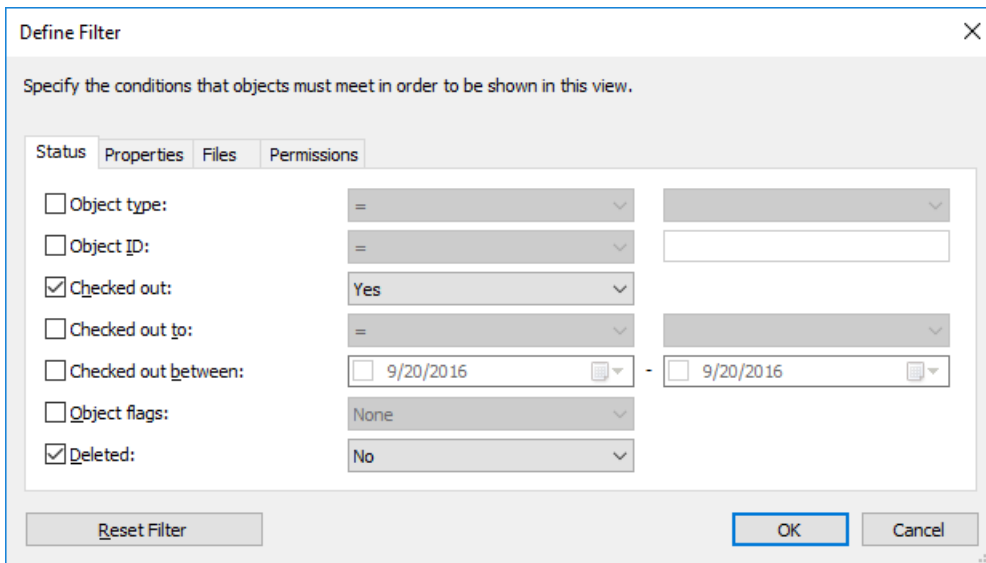
7. Open the **Properties** tab.

8. Click the **Add Condition** button twice.

9. For the first condition, select *Assigned to* as the property, = as the operator, and *(current user and users for whom the current user is a substitute)* as the value.

10. For the second condition, select *Deadline* as the property, <= as the operator, *2* as the value, and *DaysTo()* as the option.

11. Click **OK** to close the **Define Filter** dialog.

   ☑ You should now see the property condition *'Assigned to' = '(current user and users for whom the current user is a substitute)' AND DaysTo('Deadline') <= 2* in the **Filter** field of the **Notification Rule Properties** dialog.

12. Enable notifications for the event *Document or other object matches the conditions of the filter*.

13. Optional: If you do not want to receive notifications for order objects created by yourself, enable the option **Exclude notifications of events caused by the current user**.

14. Once you are done, click **OK** to save the rule and close the dialog.

The new notification rule is added to the list in the **Notification Settings** dialog.

Refresh External Objects

M-Files can also be connected to external databases. This way, a two-way connection can be set up between M-Files and, for example, a customer database. Customer data can be accessed through M-Files as well as through the customer system's own user interface. You can refresh data automatically in both directions.

Using the *Refresh external objects* function enables you to ensure that M-Files contains the current external object information.

Substitute Users

You can define substitute users for periods of absence. The substitute users you specify have the rights to carry out assignments given to you during this period.

▶ Video: *Substitute Users*

> 📄 **Note:** Assignment and document permissions may differ. So, if the assignment requires the assignee to edit a document, the substitute user of the assignee must have:
>
>   • edit rights to the document
>   • either a named user license or a concurrent user license
>
> For more information about assignments, see *Creating and Completing Assignments* on page 64.

If the assignment is created after the substitute user has been specified, the substitute user will also receive notification of the assignment. If the substitute user is specified after creating the assignment, the substitute user will not receive any separate notification of the assignment. By using the *Assigned to Me* shortcut in the task area, the substitute user can view all uncompleted assignments.

Appointing a Substitute User

1. In M-Files Desktop, press `ALT` to display the menu bar and select **Settings** > **Substitute Users** from the menu.

   ℹ️ Alternatively, you can click your user name in the upper right corner and select **Substitute Users** from the context menu.

   ✅ The **Substitute Users** dialog is opened.
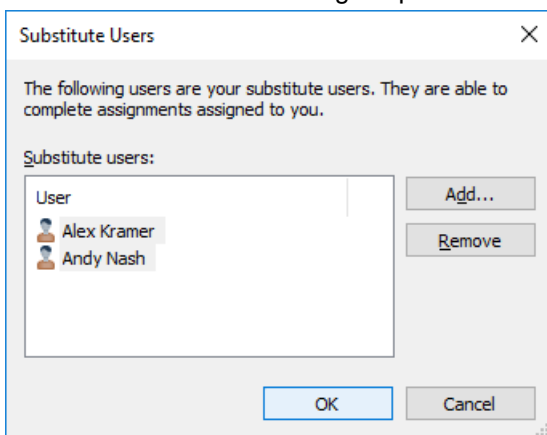
2. Click **Add...** to select the substitute user or users.

   ✅ The **Select Users** dialog is opened.

3. Highlight the preferred user or users and click **Add**.

   ℹ️ You can select more than one item at once by holding down the Ctrl key to select multiple individual items or by holding down the ⇧ Shift key to select adjacent items on the list.

   ✅ The **Select Users** dialog is closed and the selected user or users are added to the **Substitute users** list.

4. Click **OK** to close the **Substitute Users** dialog.

The users who you have just appointed as your substitute users will now be able to complete assignments assigned to you and will receive notifications about such assignments.

Applications (M-Files Desktop)

Various third-party application can be used in order to modify and extend the behavior of your M-Files Desktop and M-Files Server. For information on managing and installing the applications, see *Applications (M-Files Admin)* on page 220.

Using the applications

After a vault-specific client application has been installed via M-Files Admin, it is available for M-Files Desktop users. Upon logging into the vault, M-Files prompts you to enable the new application. If the administrator requires the application to be enabled, you cannot log in and use the vault until you have approved the use of the application.

You can manage computer-specific client applications via the Alt menu **Settings** > **Applications**.

Computer-specific settings

Note that the computer-specific settings influence the use of the applications as well. By default, the user computer-specifically allows M-Files to use applications that are installed in the document vault. If this setting is disabled, neither the optional nor compulsory vault-specific applications are available.

To enable or disable this setting:

1. Open M-Files Desktop Settings.
2. Select the *Settings* tab.
3. Open *Computer-specific Settings*.
4. Select the *Miscellaneous* tab.
5. Enable or disable the application setting under the *Security* heading.

Change M-Files Password

If you are using M-Files authentication, you can change your password by completing the steps provided below.

> 📄 **Note:** If you cannot see this option, it means that your login account is not using M-Files authentication, and thus you have no separate M-Files password for the selected vault.

To change your M-Files password:

1. Enter a vault via M-Files Desktop.

2. Either:

   a. Click your username in the top-right corner of the user interface to open the user menu and select **Change Password...**

   or

   b. Press the Alt key on your keyboard and select **Settings** > **Change Password...**

   ✅ The **Change M-Files Password** dialog is opened.

3. Enter your current password in the **Old password** field.

4. Enter a new password in the **New password** field.

5. Confirm your new password by retyping it in the **Confirm new password** field.

6. Click **OK** to save your changes.

Your M-Files password should now be changed to the one you specified in the **New password** field.

Change Language

You can change both the *software language* and *vault language*. For more information, see *Selecting the Software and Vault Language* on page 238. For a list of the supported user interface languages, see *Language Versions of the M-Files Software* on page 15.

Clear Local Cache

You can remove all temporary local files from a document vault with the *Clear Local Cache* function under the *Settings menu bar* on page 79 item.

All data in the local cache will be cleared at the same time. The cache is used to store data such as document listings and property values. Also refer to *Convert to Document* on page 106 and *M-Files Terminology* on page 8.

5.5. Export Results of Views or Searches

The *Export* function enables you to save the results of views or searches in CSV (comma-separated values) format.

Use this command to export properties (metadata) and, optionally, object files from M-Files. You can find it in the *File* menu and the listing view context menu. After exporting the metadata, you can view the CSV files, for instance, with Microsoft Excel or Open Office Calc.

> **Note:** The number of exported results can be modified by using a registry setting. Contact M-Files consulting services for additional information if you need to limit or expand the number of exported search results.

Video: *Export Views*

6. Search Functions

M-Files supports quick searches and advanced searches.

▶ Video: *Searching*

General search criteria

Search all objects: With the default setting, *Search all objects*, M-Files searches for all objects on the basis of the search strings (unless more specific search criteria have been defined in the advanced search).

Predefined search criteria

Predefined search criteria can be used to speed up the search. You can search for objects according to a certain object type or the modification date:

- Search only: by object type
- Search only: documents modified today or within the last week/month/year
- Search only: documents I have accessed today or within the last week/month/year

Other search functions

You can make the results more specific by enabling the *Search within this view* checkbox. In this case, the search only covers the view that you are in, whereas M-Files would normally search from the entire vault.

📄 **Note:** The *Search within this view* option is only available for views and virtual folders, and is thus not displayed, for instance, in the *Home* view.

You can clear all search criteria with the *Reset All* button in the top-right corner of the user interface.

Search results

The order in which the search results are listed is based mainly on frequency or recency of use. The main idea is to emphasize things that are relevant for the user. The following information is of primary importance for providing search results:

1. When was this document or other object **created**?
2. When and how many times was the document or other object **edited**?
3. When and how many times was it **processed**?

For more information, see *Finding Documents and Other Objects* on page 75.

Emphasizing the search words

When you make a search in M-Files, your search terms are marked in yellow on the listing area as well as on the metadata card and file content (preview). When preview is in use, M-Files highlights the search terms in yellow in the file contents for common file formats (Word, Excel, PowerPoint, Outlook, etc.).

Figure 52: Results of a quick search in the user interface.

Contents of the following types of files can be highlighted in the **Preview** tab:

- Email files (eml, emlx, msg)
- HTML and web archive files (htm, html, mht, mhtml)
- Image files (tif, tiff, jpg, jpeg, bmp, gif, png)
- Microsoft Excel files (xlsx, xlsm, xltx, xltm, xlsb, xls, xlt)
- Microsoft PowerPoint files (pptx, pptm, ppsx, ppsm, potx, potm, ppt, pps, pot)
- Microsoft Word files (docx, docm, dotx, dotm, doc, dot)
- OpenDocument files (odt, ott, ods, odp)
- PDF files
- RTF files
- Text files (txt)
- Visio Drawings (vsd, vdx, vss, vsx, vst, vtx, vdw)

Search results in other vaults

When you do a search in M-Files, the **Search Results in Other Vaults** pane at the bottom of the search results listing shows you the number of results in any other vaults you are connected to. If the M-Files logo next to the vault name is blue, it means that there are matches to your query in the vault. If, on the other hand, the M-Files logo is grey, it means that the search results are not yet available or there are no matches to your query in the vault. The search results are retrieved only from the vaults that you are currently logged in to. You can click **Show all** to view also the vaults you are currently *not* logged in to.

> 📝 **Tip:** You can set your login account to be automatically logged in to a vault when Windows is started. For instructions, see *Adding a Document Vault Connection* on page 35.
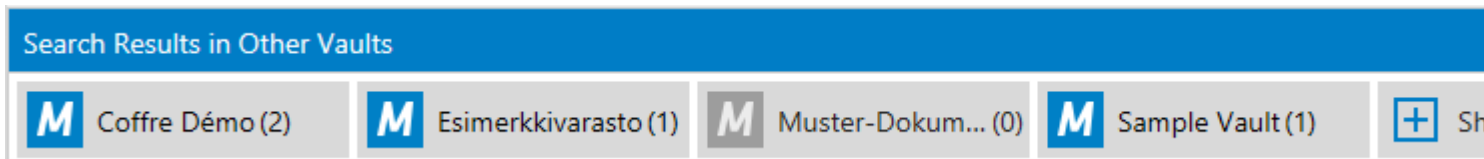
When you click any of the vaults in this pane, you are taken to the vault in question and the search results for your query are displayed.

The **Search Results in Other Vaults** pane can be hidden or displayed by right-clicking on an empty space in the listing area and selecting **Display Mode** > **Show Search Results in Other Vaults** from the context menu.

You can also show the **Search Results in Other Vaults** pane minimized by default, so that only the heading of the pane is displayed until you expand the pane. To display the pane minimized by default, right-click on an empty space in the listing area and select **Display Mode** > **Bottom Pane** > **Minimized** from the context menu. Note that this setting affects all the panes that are displayed at the bottom of the listing area.

6.1. Quick Search

Quick Search is a useful way to search for documents and other objects in the vault. Quick Search looks for objects that contain the search word in the file contents or metadata. You can determine whether to search metadata, file contents, or both. By default, both metadata and file contents are searched. If you change the setting, M-Files will use your setting for all subsequent searches.

In the search field, enter a search string that has to do with the object, such as the title, the login account of a person who has edited it, or a customer related to it, and click the arrow button. The search string does not need to be a whole word – you can truncate the word by using an asterisk. For example, when you search for data in the *Demo Vault* with the search string *specific**, you will find a document named *Technical Specifications*, because the name contains the string searched for.

To search for a particular word form, remove the selection from *Look in different inflected forms of the words in Quick Search* in the advanced search options. This option is selected by default. When you do this to search for, say, the word "corporation," the search results include only those objects that match this exact word, not *corporate, incorporated*, etc.

Words and phrases searched for are saved in a pull-down menu, making it easy to repeat the searches.
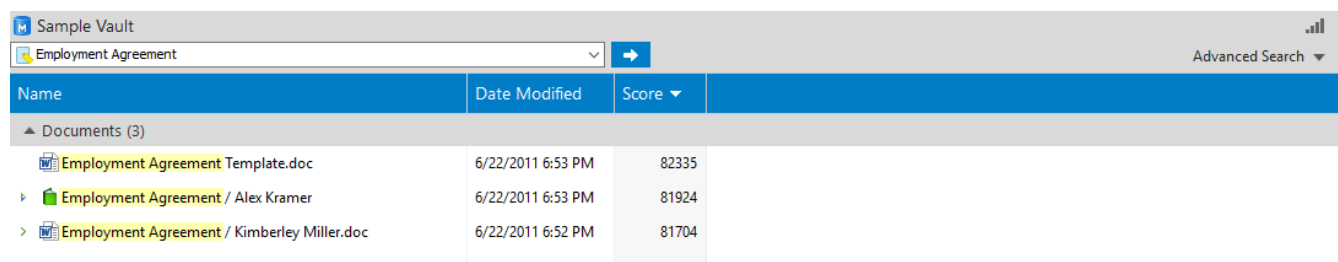
Figure 53: In the quick search, you only need to enter the search word.

Advanced options for quick search

By clicking **Advanced Search** to the right of the search field and selecting one of the three search types, you can specify the way your search queries are matched. You can select one of the following options:

All words	Matched objects contain all the specified search words.
Any word	The search will return all objects that contain at least one of the specified search words.

Boolean	The search allows you to use more specific search phrases and different operators.

You can also use different operators and special characters in your search query to find documents and objects that strictly meet your search criteria. The table below lists the operators and special characters that can be used to broaden or narrow a search.

Search type	Operator or special character	Description
Exact match	Quotation marks: `"phrase"`	Enclose the search words in double quotation marks to find objects where the words appear adjacent to each other. Example search: `"functional specification"`
Any single character	Question mark: `appl?`	The ? character matches any single character in its position. Example search: `appl?` matches both "apply" and "apple". **Note:** This character cannot be used as the first character in a search term.
Any number of characters	Asterisk: `market*`	The * character matches any number of characters in its position. Example search: `market*` matches "markets", "marketing", and so on. **Note:** This character cannot be used as the first character in a search term.
All of the search terms must be found	AND (Boolean search only)	The AND operator combines two search terms. Documents found contain both terms. Example search: `functional AND specification`
One of the search terms must be found	OR (Boolean search only)	The OR operator retrieves all documents which contain at least one of the terms entered. Example search: `agenda OR minutes`
Exclude a search term	NOT (Boolean search only)	The NOT operator exludes a search term from the search results. It can be used as a standalone operator or in conjunction with AND, OR or W/N. Example search: `agenda AND NOT minutes`
Required search term and an optional search term	AndAny (Boolean search only)	The AndAny operator combines required search terms with optional ones. Search terms before the AndAny operator are required and terms appearing after the operator are optional. In other words, search terms after the AndAny operator are considered as matches only if the search terms before the operator are also found in the document. Example search: `agenda AndAny minutes`
Faceted query	( ) (Boolean search only)	Brackets are used to group search terms together. Example search: `(agenda OR minutes) AND market*`

		This search returns all objects which contain the word "agenda" or "minutes" and which also contain a word or words beginning with "market".
Proximity search	W/N (Boolean search only)	The W/N operator retrieves objects that contain two words or phrases within a certain distance of one another. The N value indicates the number of intervening words between the search words or phrases. Example search: `agenda W/4 2015`
Fuzzy search	Vertical bar: `que|ry`	Vertical bars can be used for searching for spelling variations of the search term. The number of | characters used indicates how many characters in the search term will be ignored. Characters to the left of the first vertical bar must have an exact match in the search results. Example search: `release s||chedule`
Phonic search	The grave accent mark (`): `` `query ``	You can use the grave accent mark (` ) for searching for words that sound like the word in your search query and begins with the same letter. Add the ` character in front of the search word to search for its phonic matches. Example search: `` `John Doe `` 📄 **Note:** Phonic searches are inclusive by nature, and therefore they may occasionally produce too many search results or their search precision may be low.

📄 **Note:**

Phonic and fuzzy searches are disabled by default and are enabled by setting a registry key. The tables below list the registry key and values that must be set if phonic or fuzzy searches are to be used.

To enable fuzzy or phonic searches at the server level, add the following registry key:

Key
HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files*<version>*\Server\MFServer\FullTextSearch\

To enable fuzzy or phonic searches at the vault level, add the following registry key:

Key
HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files*<version>*\Server\MFServer\Vaults*<vault GUID>*\FullTextSearch\

Add one or both of the following values under the key defined above:

Value name	Valid values	Type	Description
Phonic	1 0 (default)	REG_DWORD	`1` enables phonic searching.

Value name	Valid values	Type	Description
Fuzzy	1 0 (default)	REG_DWORD	`0` disables phonic searching. `1` enables fuzzy searching. `0` disables fuzzy searching.

6.2. Advanced Search

With the advanced search features, you can define more specific search criteria for the document or object you are looking for. The more search criteria you use in the advanced search, the more likely you are to find the exact object you want. This way, you can prevent the search from returning too many results. Advanced search features can be opened by clicking **Advanced Search** to the right of the search field.

Advanced search

Each object has property values that can be used to search for documents in a precise manner. The value of the property *Project* can be for instance *Hospital Expansion (Florida)*. If you perform an advanced search with these values, the search returns all the documents in which the *Project* property contains the value *Hospital Expansion (Florida)*. You can also restrict the search to a specific object type, such as *Customer* or *Contact person*.
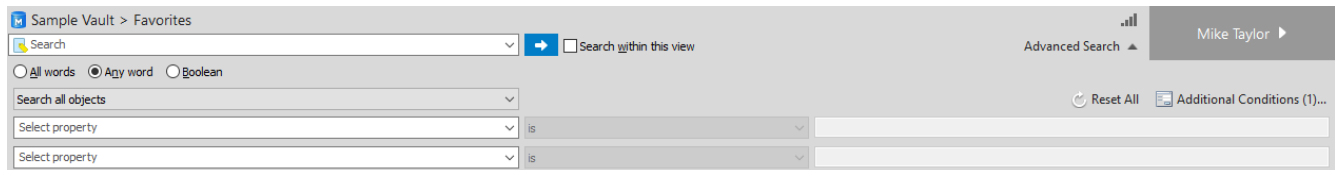
Figure 54: Advanced search features.

Subordination of search criteria

You can easily specify search criteria by utilizing their subordination, so the options shown in the lists are filtered on the basis of other list choices. For example, if you have selected a certain workflow as the search criterion, the state options are filtered in such a way that only the states related to your selected workflow are visible and selectable. Corresponding filtering will be performed automatically for other interdependent value lists as well. For example, contact persons are filtered by customer if these value lists have a hierarchical relationship.

Subordinate search criteria can be used with the "is" operator. In additional conditions, the operator "one of" can also be used.

Indirect searches

You can specify search criteria also by means of *property relationships*, which means that the object itself need not have the property in question. Instead, the property selected as the search criterion is in this case the property of a related object.

By using indirect search, you can, for example, find agreements related to a specific country; even if the *Country* property has not been defined for the actual agreement, it is enough if it can be found via a customer associated with the agreement. In this case, the search criterion is specified as "*Customer.Country*" combination.

You can specify these indirect search properties by clicking the plus-sign button in the list and then selecting the property of a related object to be used as the search criterion. In the example below, *Customer* was selected

from the list first, and then the customer's *Country* property, which resulted in the search criterion with a period, "*Customer.Country*", being displayed in the search field.

By using additional conditions, you can create three-level indirect search criteria.

Figure 55: Indirect search criteria.

> 📋 **Tip:** You can specify indirect views in the same manner, by using the properties of related objects. You can utilize indirectness in specification of filter settings as well.

6.3. Refining Your Search

> 📋 **Note:** This functionality is available only if your document vault is using the IDOL search engine.

You can refine your search results on the **Search** tab by selecting one or more of the available criteria and clicking **Refine Search**. You can view more criteria in a specific category by clicking **Show more**.

Refine your search

Object type

☐ Document (13519)
☐ Project (85)
☐ Assignment (57)
☐ Account (21)
☐ Contact Person (12)

Show more

Class

☐ Agreement (272)
☐ Brochure (150)
☐ Confirmation of Or... (757)
☐ Instruction (330)
☐ Invoice (562)

Show more

File extension

☐ PDF (3351)
☐ DOC (3145)
☐ DOCX (3142)
☐ XLS (2165)
☐ MSG (2012)

Show more

Created

☐ 2016 (340)
☐ 2015 (590)
☐ 2014 (810)
☐ 2013 (843)
☐ 2012 (838)

Show more

Last Modified

☐ today (2)
☐ within the last week (48)
☐ within the last month (106)
☐ within the last year (920)

User

☐ Michael Scott (1357)
☐ Donald Brander (1348)
☐ Jessica James (1341)
☐ Helen Roy (679)
☐ Andy Nash (584)

Show more

Account

☐ M-Files Oy (4871)
☐ M-Files Inc. (1383)

Refine Search

Once your search results have been refined to match your search query as well as the criterion or criteria you have selected, you can refine your search even more by selecting additional criteria and clicking **Refine Search** again. Note that after you have refined your search, the criteria for which there are no longer matches are now greyed out.

6.4. Additional Conditions

The *Additional Conditions* dialog can be launched via the link in the top-right corner of the user interface. In addition to the filter settings, the window contains a few options.

Look in all versions

When you select *Look in all versions*, the search will be performed on all versions of each document and object. If this option is not selected, the search is performed on the latest versions only.

Look in different inflected forms of the word in Quick Search

To search for a particular word form, remove the default selection from *Look in different inflected forms of the words in Quick Search* in the advanced search options. When you do this to search for, say, the word *corporation*, the search results include only those objects that match this exact word, not *corporate*, *incorporated*, etc.

Show latest version

When you select *Look in all versions*, the search will be performed on all versions of each object. If the option *Show latest version* is on, M-Files will show the newest version of each returned object instead of showing the old version that actually matched the search conditions.

Example: Searching for a Particular Word Form

1. Click **Advanced Search** on the right side of the search bar to bring up the advanced search options.

2. Click **Additional Conditions...**

    ✅ The **Additional Conditions** dialog is opened.
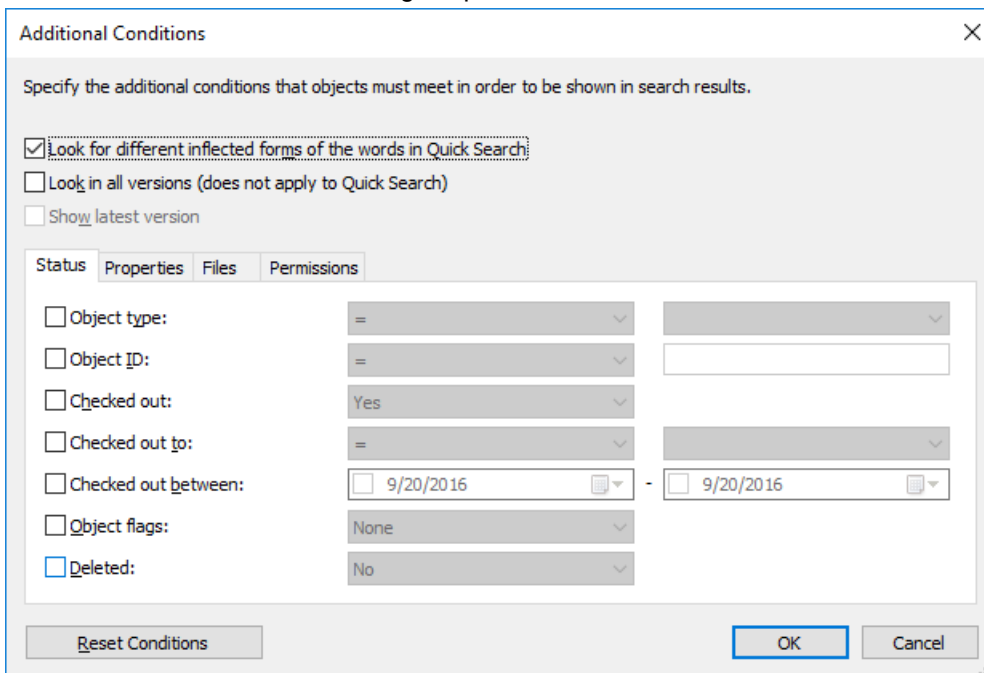
3. Uncheck the **Look for different inflected forms of the words in Quick Search** check box.

4. Click **OK** to close the **Additional Conditions** dialog.

5. Enter a search string in **Quick Search** and press Enter to search.

The search results should include only objects that contain the specific word or words that you searched for.

Export Conditions

You can use the *Export Conditions* function to save the search criteria. To access this search-related function, press the *Alt* key on your keyboard and select **File** > **Export Conditions...**.

The generated text file contains the search criteria as a string that can be used with the M-Files API method *SearchForObjectsByExportedSearchConditions*. For more information on the method, refer to the M-Files API documentation.

Filter Settings

With filter settings you can add additional filters and conditions for your search. You can define the following criteria for the objects to be searched:

Status

The search criteria related to the *object status* are specified on this tab.

Object type

Define the object type of the objects being searched for. If the object type is not specified, the search will be performed on all objects.

Object ID

Each object has an *individual ID* that M-Files Server automatically creates for each new object using consecutive numbers. With the ID search criterion, you can find the objects efficiently according to their ID numbers. You can make the ID search more specific by using *operators*. For more information, refer to *Properties (Additional Conditions)* on page 150.

Checked out

If you specify as a search criterion that the document has been *checked out* and select *Yes* from the pull-down menu, the search returns all documents that have been checked out for editing. This search criterion is useful, for example, when you want to see all documents in the vault that have been checked out to any user.

Checked out to

You can also search for documents that have been *checked out to* specific *users* of the document vault. For example, if you want to find all the documents in the *Demo Vault* that have been checked out to the user *AndyN*, choose = as the operator and select *AndyN* from the user list. You can also select *!=,* in which case you will see all the documents that have been checked out by users other than *AndyN*. *Checked Out to Me* shows all the documents that have been checked out to the user logged in to the document vault.

Checked out between

When you *check out* a document, it remains checked out until you *check it in*. Thus you can also search for documents that have been checked out earlier but have not been checked back in. For example, if you want to find all documents that were checked out between February 16 and 17, 2013, select 2/16/2013 as the start date and 2/17/2013 as the end date.

Object flags

Interaction between vaults has imported special objects to M-Files which are used to process data between vaults. These are described as conflicts and shortcuts. Conflicts are created when the versions in separate vaults differ. Shortcuts refer to objects that are located in different vaults.

When a filter is used, these special objects can be included in the search or omitted from it.

Deleted

If you specify as a search criterion that the document has been deleted, you will see all deleted documents. As stated earlier in this manual, M-Files preserves even deleted documents. In order to perform this search, you need permissions for viewing deleted documents.

Example: Searching Only for Deleted Projects

You need to have permissions to see deleted objects.

1. Click **Advanced Search** on the right side of the search bar to bring up the advanced search options.

2. Click **Additional Conditions...**

   ☑ The **Additional Conditions** dialog is opened.

3. Check the **Object type** check box, select **=** from the first drop-down menu, and finally select **Projects** from the rightmost drop-down menu.

4. Check the **Deleted** check box and select **Yes** from the drop-down menu.

5. Click **OK** to close the **Additional Conditions** dialog.

6. Enter a search term in the **Quick Search** field or leave it empty if you do not want to filter your search any further.

7. Press **Enter** or click the arrow button next the **Quick Search** field to start your search.

The search results show the deleted projects for your search term or all the deleted projects if you omitted the search term.

Properties (Additional Conditions)

Each object has property values that are assigned to it in the metadata card. These property values can be used to search for documents in a precise manner. A document property can be for example *Project*, and the value of this project can be *Hospital Expansion (Florida)*. If you perform an advanced search with these values, the search returns all documents for which *Hospital Expansion (Florida)* has been defined as the value of the *Project* property.

Properties

A property can be an object property or an *Item from a list* selection. *Item from a list* selections affect all property definitions that have been defined using the selected value list. For example, if you have installed M-Files for evaluation, the properties *Buyer* and *Supplier* in the demo vault are both defined using the value list *Customers*. If you now select *Item from list 'Customers'* as a search criterion, the search returns all documents where the *Buyer* or *Supplier* property has the value that was searched for. If, on the other hand, your search criterion is, for example, the *Buyer* property only, the M-Files search is limited to the *Buyer* property of documents.
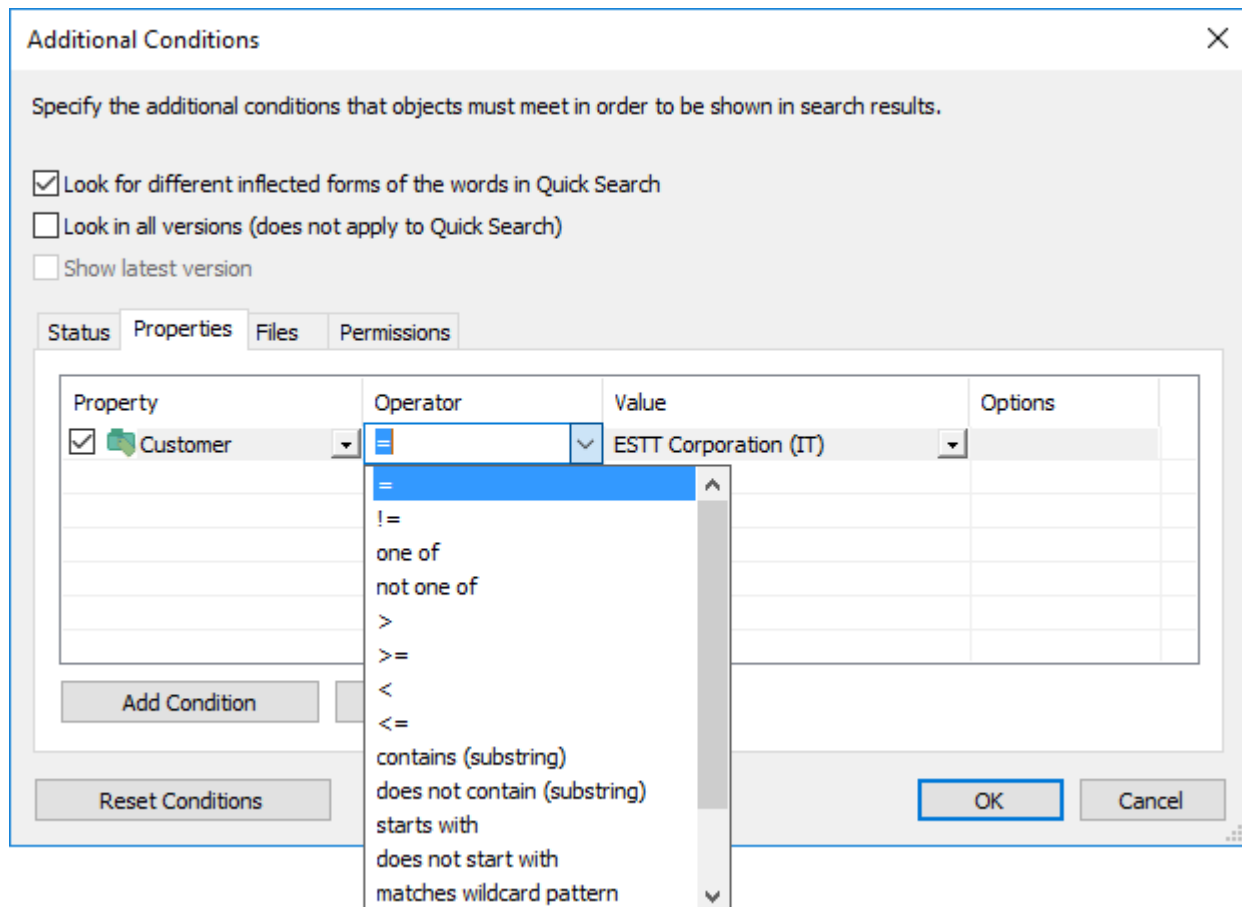
Figure 56: The properties tab of the additional search conditions dialog.

Operators

In the *Operator* field, you can determine criteria other than *equal to*. See the table below for the list of available operators.

=	Equal to
!=	Unequal to
>	Greater than
	This operator is useful when the *value* to be selected contains numbers. You can easily find all values that are greater than the value you have specified. For example, if your document vault contains the data type of the *Department* property as numbers, the search criterion > 10 returns the documents whose *Department* value is greater than 10.
>=	Greater than or equal to
<	Less than
<=	Less than or equal to
One of	You can select some property values for the search, for instance certain projects but not all of them. In this case, the search results are just the documents whose Project property has one of the values you selected with the *One of* operator. For example, the Project property of the document *Window Chart E12.dwg* is *"Hospital Expansion (Florida)"*.
Not one of	This search option is the opposite of the previous one.
Contains	When you want to search for documents by letter combination, for instance a word, you can use the *Contains* operator. For example, if you want to find all documents in the *Demo Vault* whose *Project* property value contains the letters *pan*, the search results include the document Window Chart E12.dwg, whose *Project* property is *"Hospital Expansion (Florida)"*. The word *Expansion* contains the letters *pan* that were determined as the search criterion.
Does not contain	This search option is the opposite of the previous one.
Starts with	The *Starts with* option works in almost the same way as the *Contains* option. Here, the word must start with the value specified.
Does not start with	This search option is the opposite of the previous one.
Matches wildcard pattern	The **matches wildcard pattern** option can be used with the wildcards ? and *. The ? character replaces any single character, and the * character replaces any number of characters. For example, if you want to find documents whose **Project** property value starts with the string *Web Site* followed by *any number of any characters* and ends with the string *ESTT*, you would select the **Project** property and specify `web site * estt` as the search string for the **matches wildcard pattern** operator. The **Project** property value of documents returned by this search could be, for example, *Web Site Graphics for ESTT* or *Web Site Design for ESTT*.
	Note: Wildcard characters cannot be used as the first character in a search term.
Does not match wildcard pattern	This search option is the opposite of the previous one.
Is empty	In some cases, the properties of a document have no value. This happens when no value is specified for the property at the stage of filling in the metadata card – e.g., when no value has been specified for the *Project* property. The *Is empty* operator utilizes the

	missing value in the search. For example, you can easily find all documents whose *Project* property has no value.
Is not empty	This search option is the opposite of the previous one.

Values

From the **Value** column, you select the value for the selected property that is used as the search criterion. You can filter the list of available values by selecting the **Filter** option and entering a suitable filter word in the **Set Filter to List** dialog.

📄 **Note:** You can select multiple values by holding down the Ctrl key while clicking values.
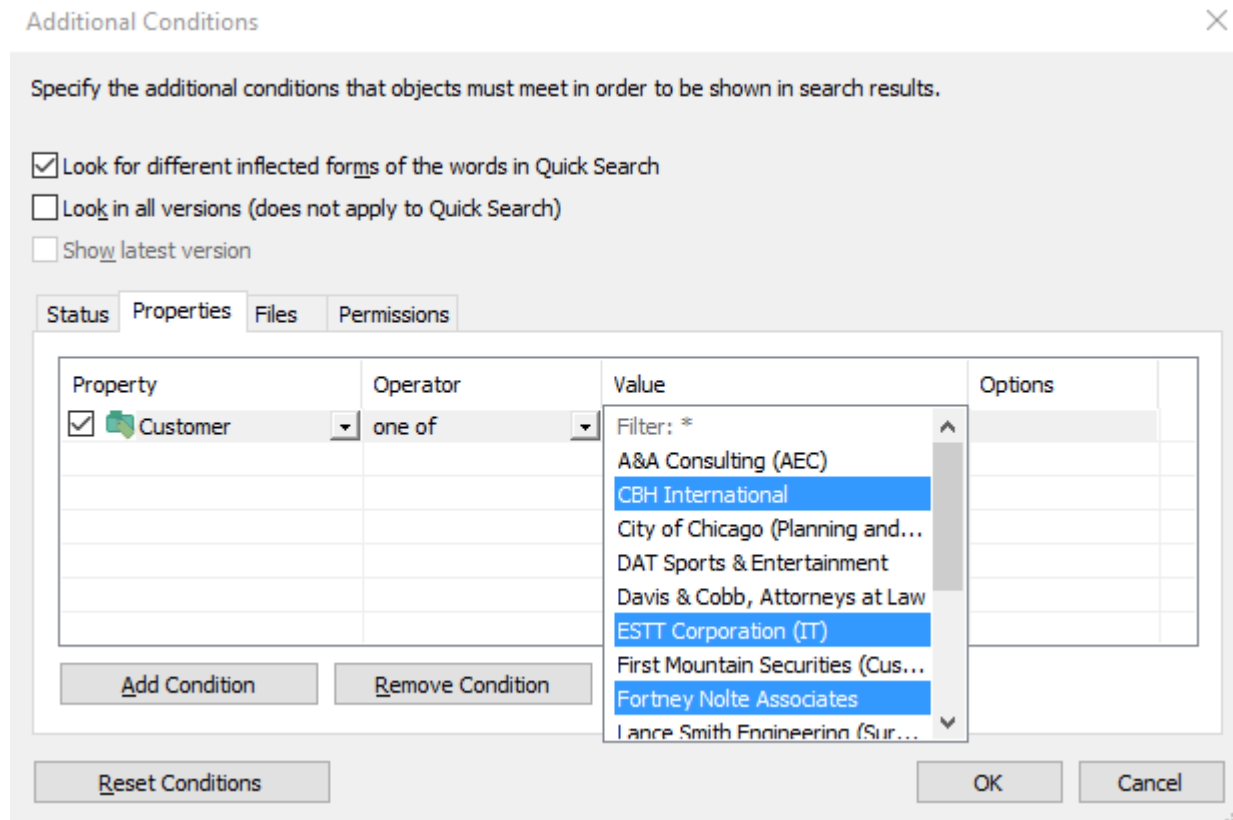
Figure 57: Selecting properties for the search filter.

When you search for Projects with the *Matches wildcard pattern* operator (`????house*`), one of the documents returned from the *Demo Vault* is the document *Functional Specification.doc*, whose Project property has the value *Warehouse Management System Development*. The word Warehouse begins with *any four character string*, followed by the word *house* and then any character string.
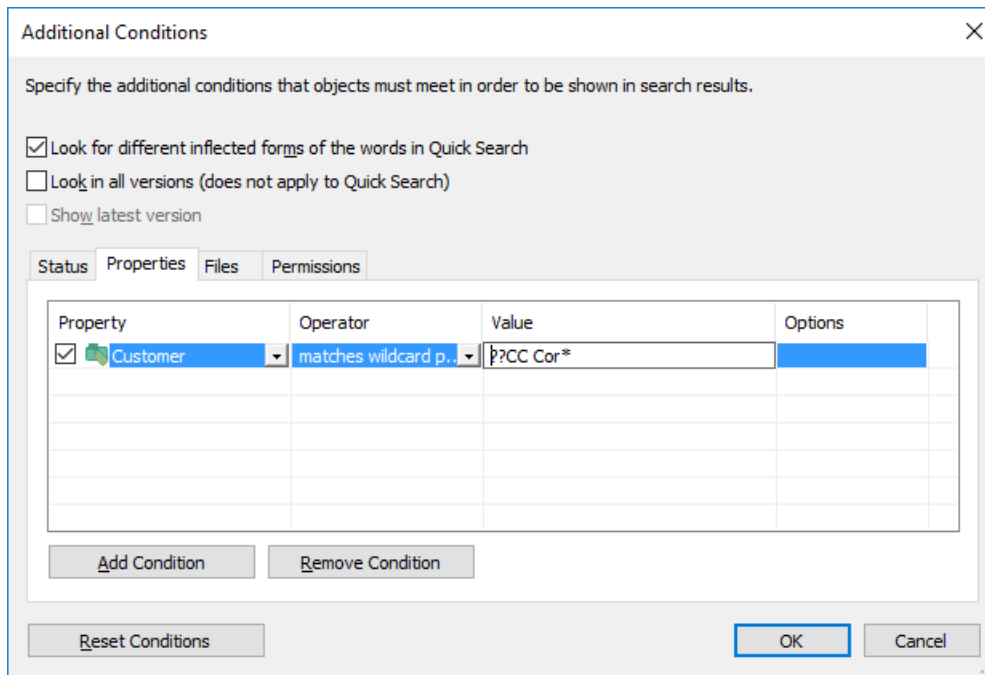
Figure 58: Utilizing the"Matches wildcard pattern" operator.

If a property definition based on a hierarchical value list is selected as the search criterion, you can also select whether to include the values higher and lower in the hierarchy in the search.

Options

If your search criteria includes a property containing a timestamp, you can make the search more specific by selecting an option from the **Options** column, selecting an operator, and entering a suitable value in the **Value** field. For example, you can find all recently created documents. Give "Created < 7" as your search criterion, and select the option `DaysFrom()`. The search will return all documents created over the last seven days. See the table below for the list of available options for timestamp properties and their descriptions.

Option	Example	Description
Date()	Created = 18.12.2015	Returns objects that have a given timestamp property containing a given date.
DaysFrom()	Created < 7	Returns objects with a given timestamp property containing a date within a given number of days *preceding* the current date.
DaysTo()	Effective through < 10	Returns objects with a given timestamp property containing a date within a given number of days *following* the current date.
Month()	Created = 05	Returns objects that have a given timestamp property containing a date with a given month. Use the format *MM*.

Option	Example	Description
Year()	Document date = 2015	Returns objects that have a given timestamp property containing a date with a given year. Use the format *YYYY*.
YearAndMonth()	Created = 2015-12	Returns objects that have a given timestamp property containing a date with a given year and month. Use the format *YYYY-MM*.
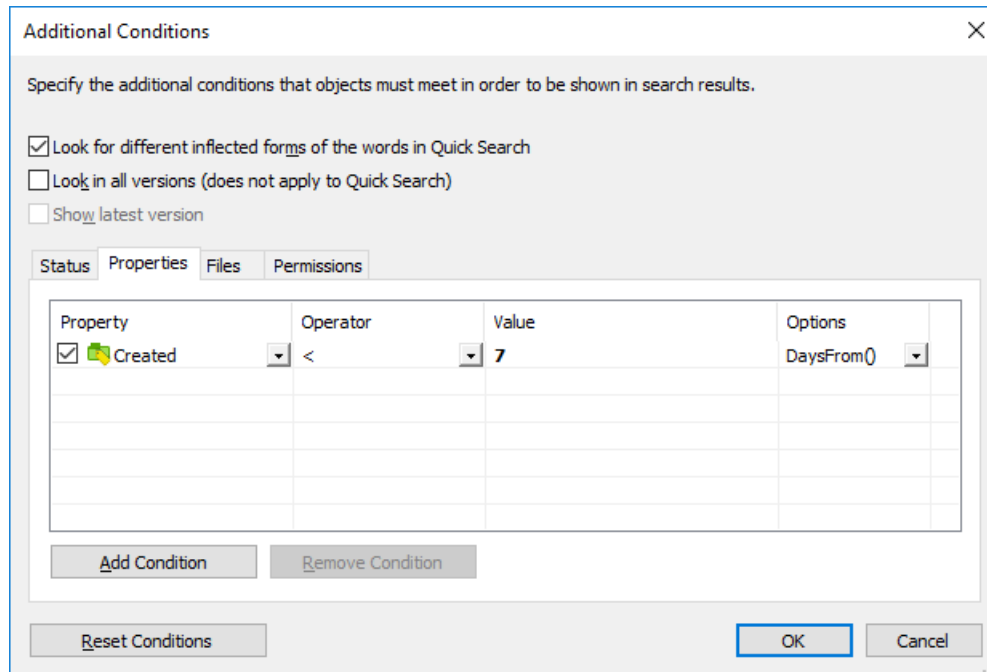
Figure 59: Utilizing options for properties of the timestamp data type.

Also refer to **Subordination of search criteria** and **Indirect searches** under *Advanced Search* on page 144. You can always utilize indirectness for specifying the properties in filter settings.

Example: Searching for Ongoing Projects for American Customers

1. Click **Advanced Search** on the right side of the search bar to bring up the advanced search options.

2. Click **Additional Conditions...**

☑ The **Additional Conditions** dialog is opened.

3. Go to the **Properties** tab and click **Add Condition** to add a property condition.

4. From the topmost **Property** drop-down menu, select **In progress**.

5. From the topmost **Operator** drop-down menu, select **=**.

6. From the topmost **Value** drop-down menu, select **Yes**.

7. Click **Add Condition** again to add another property condition.

8. Locate **Customer** in the next **Property** drop-down menu and click the plus sign next to **Customer** to expand its properties and select the **Country** customer property.

   ⓘ This creates an indirect property association that uses the **Country** property of the customer object to define a country for the project. As the project object does not include country data in this case, the customer object can be used indirectly to provide it.

9. From the **Operator** drop-down menu, select **=**.

10. From the **Value** drop-down menu, select **USA**.

   ☑ The **Additional Conditions** dialog should now look like this:

11. Click **OK** to close the **Additional Conditions** dialog.

12. Enter a search term in the **Quick Search** field or leave it empty if you do not want to filter your search any further.

13. Press **Enter** or click the arrow button next the **Quick Search** field to start your search.

The search results show the projects (for the search term or all the projects if no search term was given) that are in progress for customers from the United States.

Files

As described earlier in this manual, an M-Files document consists of metadata and zero or more files. This tab in the detailed search is used to specify search criteria for just the document files – i.e., not the metadata, which was specified on the *Properties* and *Status* tabs.
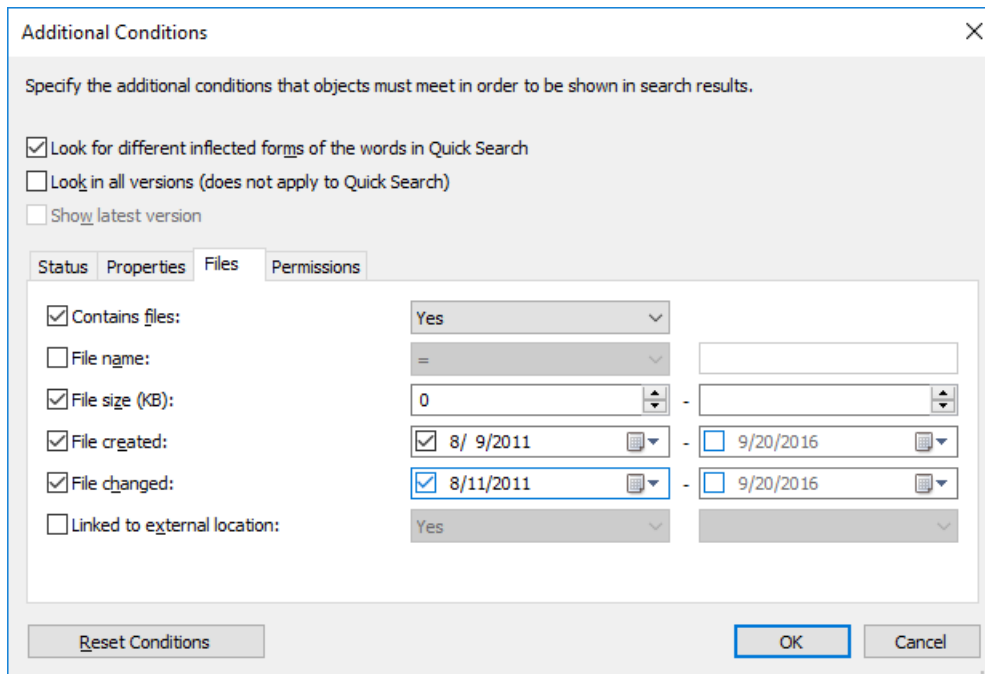
Figure 60: The Files tab allows you to specify search criteria for document files.

File name

If you can remember the file name or parts of it, *File name* is an efficient search criterion. If you remember the exact name, select the *equals* sign and enter the name of the file in the next field. If you cannot remember the exact name, you can use other operator settings than the *equals* sign; refer to *Properties (Additional Conditions)* on page 150.

File size (KB)

If you want the search to return files of a certain size, you can specify the minimum and maximum file size here.

File created, File changed

Searches can also be performed according to the time stamps of files, i.e., creation date and change date. The use of dates as search criteria works in the same manner in all searches. For more information about the use of dates as search criteria, refer to *Status* on page 148.

Linked to external location

You can also perform a search on files that are linked to an external location. You can choose to search within files that are all linked to one and the same external location, or within all linked files that are external to M-Files. For more information about linking files, refer to *External File Sources* on page 343.

Example: Searching for PNG Images

1. Click **Advanced Search** on the right side of the search bar to bring up the advanced search options.

2. Click **Additional Conditions...**

✅ The **Additional Conditions** dialog is opened.

3. Go to the **Files** tab, check the **Contains files** check box, and select **Yes** from the adjacent drop-down menu.

4. Check the **File name** check box and select **matches wildcard pattern** from the adjacent drop-down menu.

5. Enter `*.png` in the text field next to the drop-down menu.

✅ The **Files** tab should now look like this:

6. Click **OK** to close the **Additional Conditions** dialog.

7. Enter a search term in the **Quick Search** field or leave it empty if you do not want to filter your search any further.

8. Press **Enter** or click the arrow button next the **Quick Search** field to start your search.

The search results show the PNG images found for your search term or all the PNG images in the vault if you omitted the search term.

Permissions

Each object has permission settings that are assigned to it on the *Permissions* tab of the metadata card. Objects can also be searched according to their permission settings. You can, for example, create a search listing all objects that are visible to the company management only. This way, you can also change the permissions of specific objects.
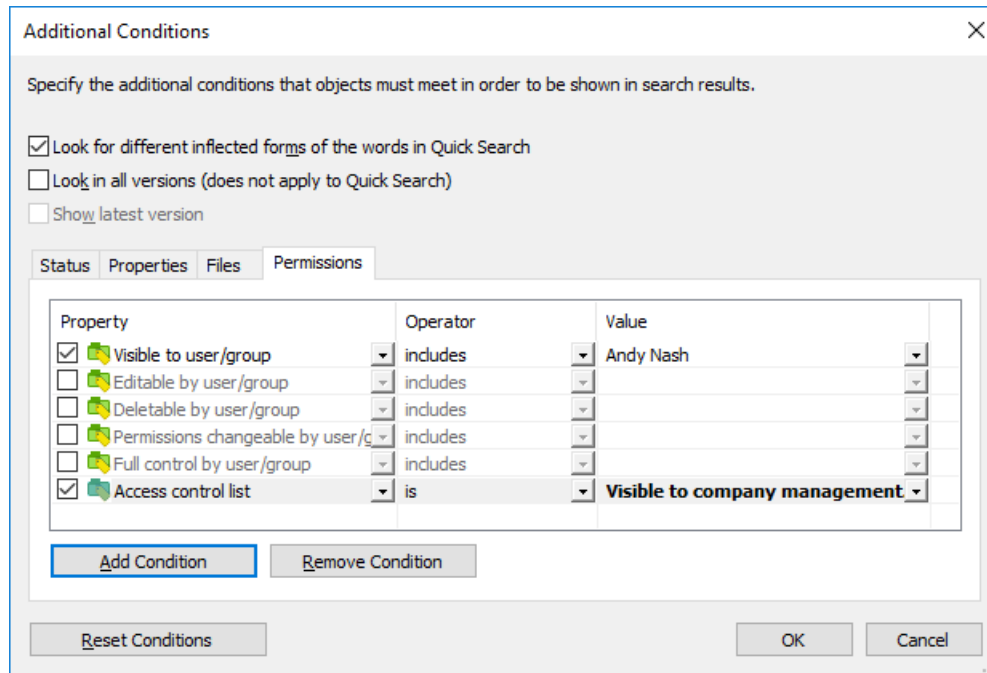
Figure 61: You can also search objects by specific permissions.

Example: Searching for Objects That Are Visible to the HR Department

Your vault needs to have the **HR Department** user group and you need to be a member of that group.

1. Click **Advanced Search** on the right side of the search bar to bring up the advanced search options.

2. Click **Additional Conditions...**

☑ The **Additional Conditions** dialog is opened.

3. Go to the **Permissions** tab and check the **Visible to user/group** check box.

4. From the **Operator** drop-down menu, select **includes**.

5. From the **Value** drop-down menu, select **HR Department**.

6. Click **OK** to close the **Additional Conditions** dialog.

7. Enter a search term in the **Quick Search** field or leave it empty if you do not want to filter your search any further.

8. Press **Enter** or click the arrow button next the **Quick Search** field to start your search.

The search results show the objects that match your search term and are visible only to the HR department.

6.5. Search Results Groupings

M-Files automatically groups search results by object type. Thanks to this, you can quickly and easily find the desired object, regardless of whether you are looking for, for example, a document or a project.

If there is a "+" sign in addition to the number beside the object type title, there are more search results than are being shown (for instance *Documents (50+)*). You can display more search results by clicking on *Show more results*.

Figure 62: M-Files groups the search results by object type.

Try new searches

If needed, M-Files guides the user toward the desired search result by displaying various quick tips. For example, M-Files may suggest the use of another search string or making the search broader with the * character.

7. M-Files Functions in Microsoft Office and AutoCAD

This chapter describes how M-Files has been integrated into your Microsoft Office and AutoCAD.

7.1. Functions in Word, Excel and PowerPoint

The M-Files functions accessible directly in Word, Excel, and PowerPoint make it easy to work with documents. You can access the functions from the *File menu*, *Office menu*, or *M-Files menu*. The menus may look a little different, depending on the software versions in use.
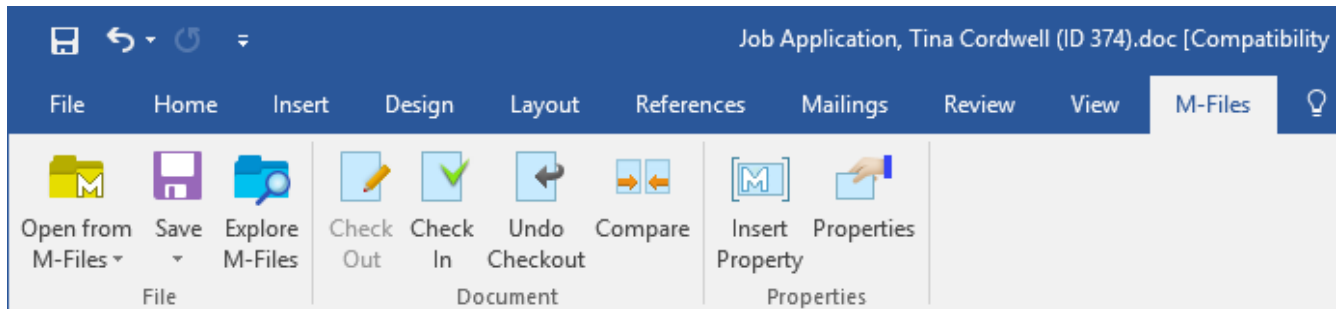
Figure 63: All M-Files functions are available through the M-Files menu.

The M-Files functions presented below are available in Microsoft Word, Excel, and Powerpoint versions 2007, 2010, 2013, and 2016.

Open From M-Files

You can open a document for reading or editing directly from the document vault. If you are using several document vaults, use the *Open from M-Files* function to select the desired document vault. This function is also available on the *File* and *Office* menus.

Save to M-Files

Save is the handiest way to save a new or edited document to M-Files. When you save to M-Files directly, the metadata card opens for editing just as it does when you create a new document via M-Files Desktop. For more information, refer to *New Document* on page 80. If you are using several document vaults, choose the target document vault in the *Save* submenu. This function is also available on the *File* and *Office* menus.

Explore M-Files

You can open the M-Files user interface at the same time. If the opened file is in M-Files, the *Explore M-Files* function displays the file in M-Files, making it is easier to perform other M-Files functions on the file (such as copying or sending a link by E-mail).

Check Out

The *Check Out* function checks out for editing a document that has been opened as read-only. This function converts the document from read-only mode to edit mode.

> **Note:** If the document is in read-only mode and has been edited, and the *Check Out* function is performed, all changes are lost.

Undo Checkout

The *Undo Checkout* function closes the current document and cancels its checkout without saving changes. If the *Undo Checkout* function is performed on a document that has been edited, all changes made after the document was *checked out* will be lost.

> 📄 **Note:** *Undo Checkout* cannot be used on a single file of a multi-file document. In this case, the function is not available in the M-Files menu.

Compare

With the *Compare* function, the content of the current document can be compared to an earlier version of the same document. The *Compare* function opens the document version history, which allows you to select the earlier version to compare the current one to. The results are displayed with the changes visible.

Insert Property

For more information, refer to *Insert M-Files Property* on page 163.

Properties

For more information, refer to *M-Files Properties* on page 163.

M-Files Properties

The document properties defined in M-Files can also be displayed in Word, Excel and PowerPoint via the *Properties* function. This function can be found in the *M-Files menu* on page 162. The metadata card opened by means of the Properties function is the same as the metadata card in M-Files.

The document properties can be edited and saved as in M-Files. For more information, refer to *Document Properties* on page 81.

Insert M-Files Property

Document metadata stored in M-Files can be included in document contents by using the **Insert Property** function.
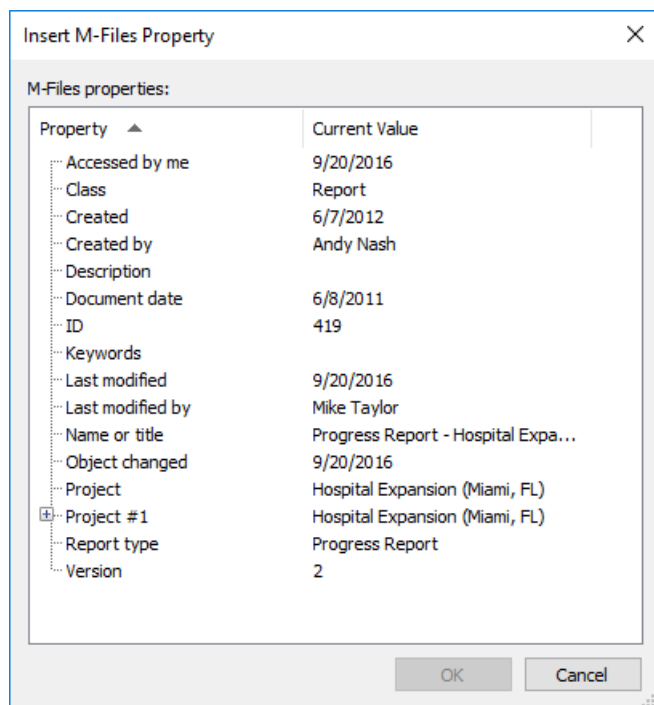
Figure 64: List of properties that can be inserted to the document.

You can set up text fields or cells in Word, Excel, and PowerPoint in which the selected M-Files properties are filled in automatically. For example, you can select a customer name and address from the document properties and insert them as the recipient's contact information in a proposal.

Other M-Files properties can be added in a similar way. For example, you might insert the name of your proposal document as the heading of the cover letter or add product information to the proposal.
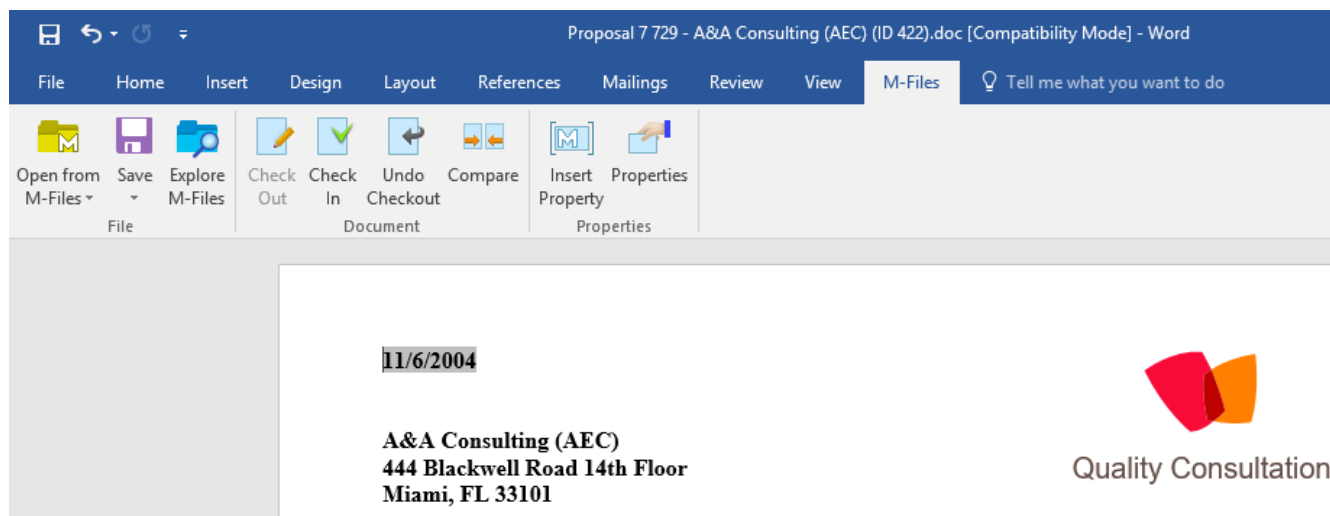
Figure 65: The "Insert Property" function automatically inserts selected document properties into the document content.

You can also add an electronic signature to an Office document by selecting the **Insert property** function. For more information, see *Electronic Signature* on page 329.

Document metadata can also be edited by using the **Properties** function when the document is processed in Word, Excel, or PowerPoint. For more information, refer to *M-Files Properties* on page 163.

> 📄 **Note:** In PowerPoint, the **Insert Property** function is available in versions 2007, 2010, 2013, and 2016 only.

Utilizing "Insert Property" with document templates

The **Insert Property** function can be used to conveniently create document templates. Text fields or cells defined in the template are automatically populated with the selected properties when a new document is created. For example, a proposal template can be set up to include fields for the properties *Customer*, *Contact*, *Address*, and *Country*. When a new proposal is created using the template, the customer information in the metadata is automatically inserted into the fields. This means that address information no longer has to be separately copied from the customer contact information.

An existing document can be defined as a document template in M-Files by selecting the *Is template option* on page 80. The *property definition permissions* on page 306 in M-Files Admin are used for controlling which users are able to set documents as templates.

If a property does not have a value, the text fields or cells in the document templates may also be left empty. When a user creates a new document using the template, these text fields and cells are automatically populated with the current property values.

An M-Files property inserted into a Word document is displayed as a text field, which by default turns gray when clicked. In Excel documents, M-Files properties are displayed as cell formulas and in PowerPoint documents as text areas.

Note, however, that inserting metadata in a document does not in itself require the document to be defined as a *template*.

Example: Inserting M-Files Properties in Microsoft Word

1. In M-Files, locate a Microsoft Word document of your choice, double-click it, and then click the **Check Out** button.

   ☑ The selected document is opened in Microsoft Word.

2. In Microsoft Word, place the cursor where you want the M-Files property to appear in the document.

3. Open the M-Files ribbon and click **Insert Property**.

   ☑ The **Insert M-Files Property** dialog is opened.

4. The properties and property values of the current document are listed in the **M-Files properties** list. Select a property by clicking the name of the property.

5. Click **OK** to close the **Insert M-Files Property** dialog.

The property value of the selected property is inserted in the selected location of the Microsoft Word document.

7.2. Functions in Outlook

M-Files offers several features and diverse benefits for the daily handling of e-mail messages and for their utilization in customer relationships. For example, you can automate storing messages in M-Files by utilizing Outlook rules and M-Files features. Extensive integration with Outlook provides you with, for example, the following features:

- E-mail messages and attachments can be saved to M-Files in various file formats.
- E-mail messages can also be saved automatically with their metadata by means of Outlook rules and M-Files features.
- Contact persons and customers can be automatically associated with e-mail messages.
- The M-Files flag indicates messages that have been saved to M-Files.

- Messages related to a particular message are interlinked in M-Files. Thanks to this, the entire message thread is easily accessible and readable in M-Files.
- The *Show in M-Files* function allows you to open a stored message in the M-Files user interface.
- When an e-mail message is saved to M-Files in Outlook, the document date will automatically be the same as the e-mail date, no matter when the message is saved to M-Files.

▶ Video: *Email Integration*

Saving An E-Mail Message in Outlook to M-Files

1. In Microsoft Outlook, locate the e-mail message that you want to save to M-Files.

2. Either:

    a. Right-click the e-mail message and select **Save to M-Files**, and then select the vault where you want to save the selected e-mail message.

    or

    b. Drag and drop the e-mail message to the preferred M-Files folder located in the Microsoft Outlook navigation pane.

    ☑ The **New Document** dialog is opened.

3. From the **Save as type** drop-down menu, select the format in which the e-mail message is saved.

    ⓘ For more information about e-mail message storage formats, see *Storage Formats* on page 166.

4. Fill in the metadata for the e-mail message and click **Create** once you are done.

    ⓘ Note that some properties may be automatically populated. For more information, see *Automatically Populated Metadata* on page 169.

The selected e-mail message is added to the selected vault in M-Files. An M-Files flag is also added to the message in Microsoft Outlook as an indication that the message has been saved to M-Files.

Storage Formats

E-mail messages and attachments can easily be saved from Outlook directly to M-Files. The following M-Files functions are available in Microsoft Outlook 2007, 2010, 2013, and 2016.

Outlook offers the following save options for *Save to M-Files*:
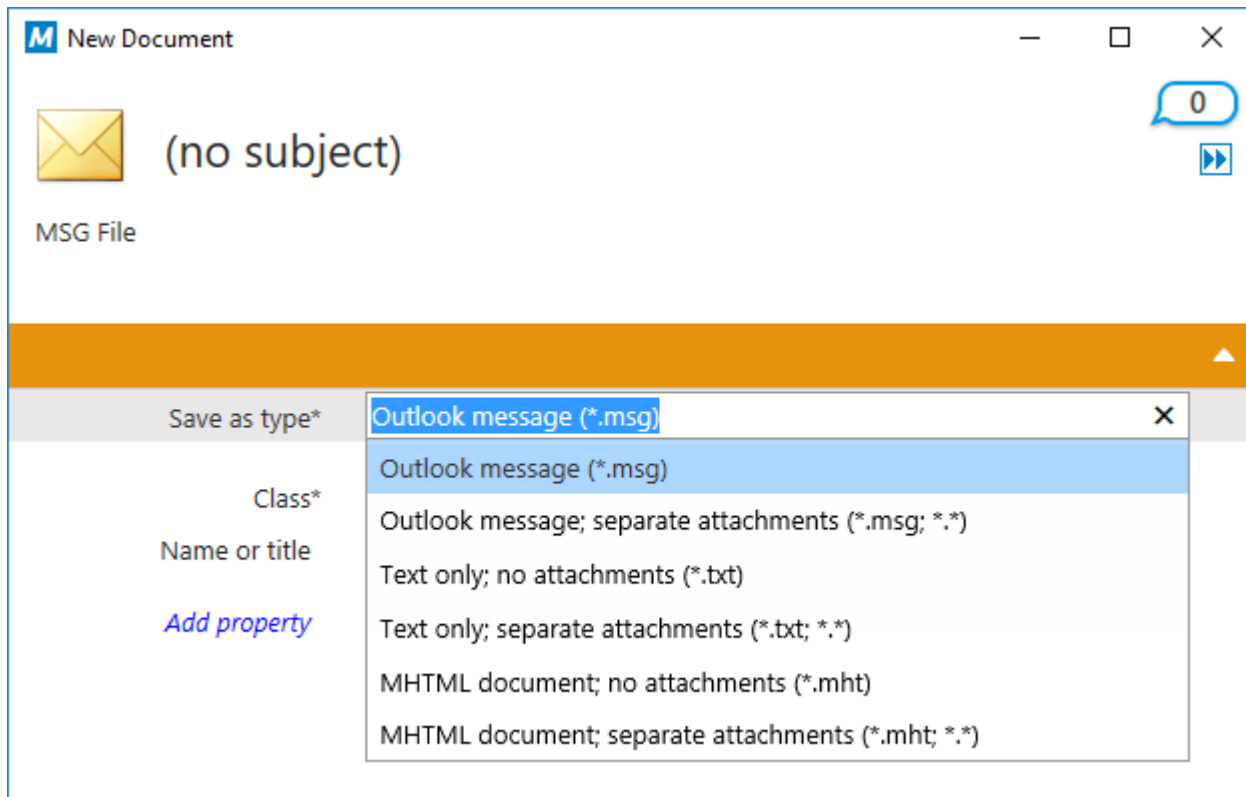
Figure 66: E-mail messages can be saved to M-Files in many formats.

Outlook message (*.msg)

The e-mail message and any attachments are stored in M-Files in MSG format. The stored file and its attachments open as a message in Outlook.

Outlook message; separate attachments (*.msg; *.*)

The e-mail message is stored as a multi-file document: message text is stored in MSG format and the attachments in their native file formats. The stored MSG file opens as a message in Outlook. The attachments open in the applications associated with the file format.

Text only; no attachments (*.txt)

The e-mail message is stored as a text file. The stored file opens in, e.g., Notepad. Attachements are not saved.

Text only; separate attachments (*.txt; *.*)

The e-mail message is stored as a multi-file document: message text is stored as plain text and the attachments in their native file formats. The attachments open in the applications associated with the file format.

MHTML document; no attachments (*.mht)

The e-mail message is stored in M-Files in MHT format. The stored file is opened in a program that supports reading of MHT files such as Internet Explorer.

MHTML document; separate attachments (*.mht; *.*)

The e-mail message is stored as a multi-file document: the content of the message is stored in MHT format and the attachments in their native file formats. The attachments open in the applications associated with the file format.

Save Attachments to M-Files

The *Save Attachments to M-Files* function stores only e-mail attachments. The attachments are stored in their native file formats. If an e-mail message contains several files as attachments, these files are saved as a

multi-file document. If the message contains one attachment, the file is saved as a single-file document. The attachments open in the applications associated with the file format.

> 📄 **Note:** If you would prefer to store multiple attachments as ZIP archives rather than as multi-file documents, please contact your M-Files consultant for additional information.

Creating a Microsoft Outlook Rule for M-Files

By utilizing Microsoft Outlook rules, you can easily automate saving specific kinds of e-mail messages to M-Files on the basis of, for example, the sender, subject, or recipient of a message. For instance, you can specify that all proposal messages that you send are to be saved to M-Files on the basis that the subject field contains the word *proposal*.

> 📄 **Note:** These instructions are for Microsoft Outlook 2013. If you are using a different version of Microsoft Outlook, there may be minor differences in how rules are created.

Complete the following steps to create a Microsoft Outlook rule for M-Files:

1. Open Microsoft Outlook and select an e-mail message that represents the type of message for which you want to create a rule.

   > ✏️ You can select the message and create the rule on the basis of, for example, the sender of the message, text in the subject field, or the recipient of the message.

2. On the **Home** tab, in the **Move** section, click **Rules** and the select **Create Rule...** from the menu.

   > ✅ The **Create Rule** dialog is opened.

3. Click the **Advanced Options...** button.

   > ✅ The **Rules Wizard** dialog is opened.

4. Check the condition or conditions that an e-mail message must meet for this rule to be applied.

   > ✏️ For example, if you want to create a rule that applies to messages that are sent by the selected sender, check the **from <sender>** option check box.

5. Optional: If necessary, click an underlined value in the rule description field to edit the rule condition.

6. Click **Next**.

7. Check the **move a copy to the specified folder** option check box.

   > ℹ️ You can also move the messages themselves directly to M-Files so that they are deleted from Microsoft Outlook once they are moved, but the best practice normally is to *move a copy* of the message to M-Files, in which case the actual message remains in the original folder, such as the *Inbox* or *Outbox* folder.

8. Click **specified** in the rule description field.

   > ✅ The **Rules and Alerts** dialog is opened.

9. Expand the **M-Files** node and then select the vault to which you want to move copies of messages that match this rule.

10. Click **OK** to close the **Rules and Alerts** dialog and then click **Next**.

11. Optional: If you need to make exceptions to this rule, check any exception check box that you want to be applied and edit the exception in the rule description field, if necessary.

12. Click **Next**.

13. In the text field, enter a descriptive name for the rule.

14. Check the **Run this rule now on messages already in...** and **Turn on this rule** option check boxes and click **Finish** to finish creating the rule.

The e-mail messages in Microsoft Outlook that match the rule that you have just specified are moved automatically to the selected vault in M-Files.

> **Note:** If Microsoft Outlook is not open when you receive a message that matches this rule and would therefore be automatically saved to M-Files, M-Files will suggest that you *Save pending messages now* when Microsoft Outlook is opened the next time.

Saving messages in M-Files Folders

In addition to using the *Save to M-Files* function, you can save messages to M-Files by using M-Files folders. This offers several additional features for saving messages:

- You can save messages quickly and easily by dragging them to M-Files folders in Outlook.
- M-Files folders are automatically available to you in Outlook if M-Files has been installed on your computer. Automatically used M-Files folders correspond to the M-Files vaults to which you have added a document vault connection.
- The messages are always copied from their original folder in Outlook: messages are not removed from their original Outlook folder when you move them to the M-Files folder.
- You can specify automatically populated metadata for each M-Files folder.

The above functions are available in Microsoft Outlook 2007, 2010, 2013, and 2016.

Automatically Populated Metadata

You can specify automatically populated properties to be added to e-mail messages when you save them to M-Files by dragging them to M-Files folders in Outlook. These settings are folder-specific, allowing you to utilize multiple subfolders for a variety of use cases. The function is available in Microsoft Outlook 2007, 2010, 2013 and 2016.

> **Note:** These folders need to be added as subfolders under the automatically created M-Files folders (representing your M-Files vault connections). If you create a folder directly on the main level, you create a normal Outlook folder, for which you cannot specify M-Files properties.

You can find the *Specify M-Files Properties* function in Microsoft Outlook by right-clicking an M-Files folder.
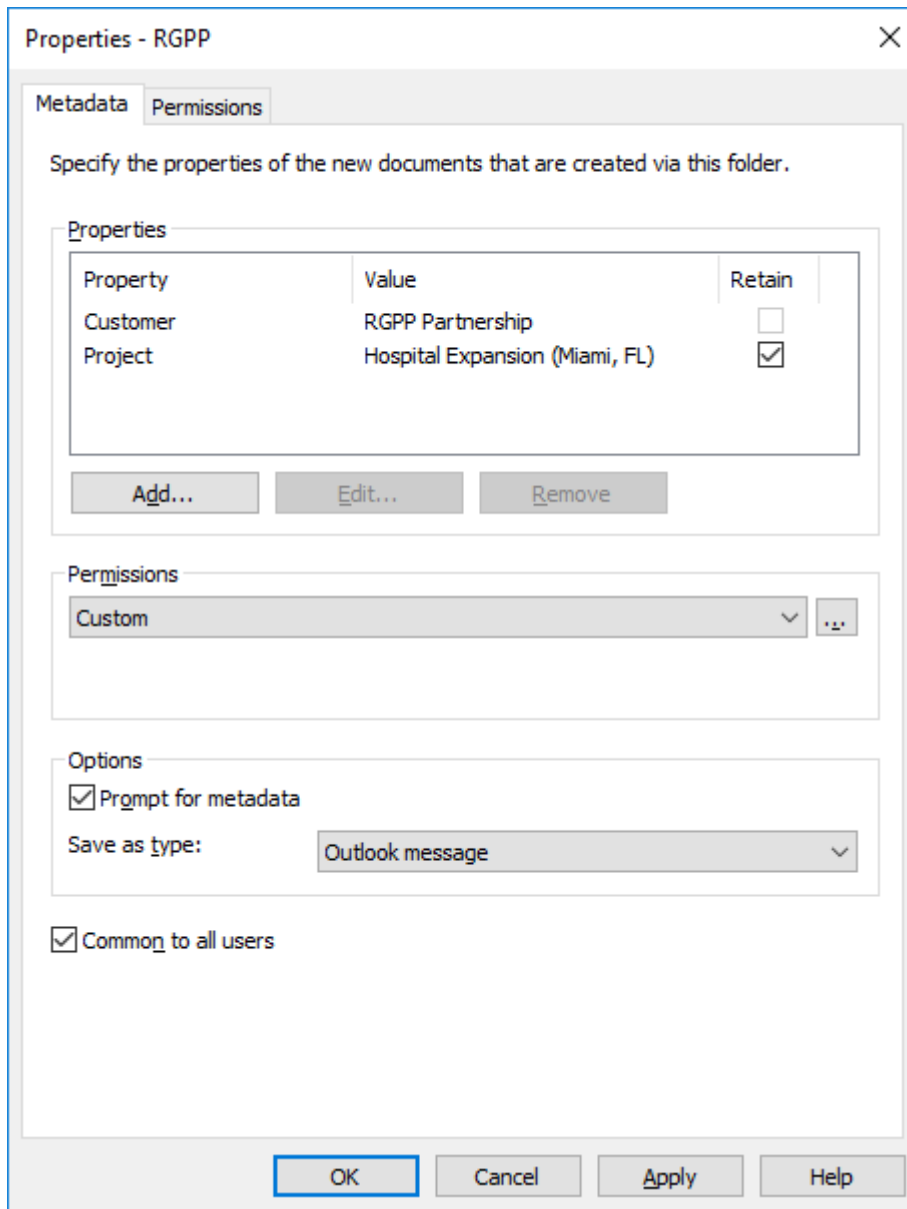
Figure 67: Properties dialog for setting up automatically populated, folder-specific metadata.

Click the **Add...** button to define a new property.

You can, for instance, use the property *Project* and set it to have the fixed value *Zenith Construction Project*. This way, the messages dragged into that folder are automatically associated with the *Zenith Construction Project*. Alternatively, if you wish to save all job applications in the *Job application* class, select the folder property *Class* and set its value to *Job application*.

You may also specify M-Files folder properties to be read from the e-mail message itself. In this case, select **Add...**, then the *Read from the e-mail message* option and choose a suitable field from the drop-down menu.

Allow users to retain the property value for this folder

This setting (visible only to users with at least the right to manage common views) adds a *Retain* column to the folder properties dialog. The *Retain* option is available for all users, and also controlled by each individual user. Activating the *Retain* option for a property tells M-Files to remember the latest value provided by the user, ignoring the original fixed value set by the administrator.

Let's say the organization is connected to two projects with the same customer, and the default project has been set to *Alpha*. The project manager for project *Beta* would probably want to enable the *Retain* option, because this way the property needs to be changed only once. After this, M-Files remembers that the project manager wants to associate his e-mails with project *Beta*, not *Alpha*, even though the default project was set to *Alpha*.

Permissions

The *Permissions* option enables you to define user permissions for the messages that are saved in this M-Files folder. This should not be confused with the view permissions for common folders (see below).

Prompt for metadata

You can specify whether the metadata card is to be displayed when messages are dragged into the M-Files folder. The metadata card should be displayed if you wish to check or modify automatically populated metadata during saving, or if you have not defined any folder-specific properties.

Specifying common M-Files folders

You can also specify that the M-Files subfolder you created is common to all users, in which case the folder will be displayed in Outlook to all users. A common M-Files subfolder can be created and specified by a user with at least the right to manage common views. When the user drags a message to a common folder, the message automatically receives the metadata (properties) that have been specified for the common folder.

The common folder settings are applied once the user starts Outlook while being logged into the vault.

Common folder view permissions

As soon as the *Common to all users* option has been enabled, the *Permissions* tab appears next to the *Metadata* tab. This allows you to select view permissions for the common folder. This should not be confused with the *Permissions* option on the *Metadata* tab (see above).

Defining Automatically Populated Metadata

1. In Microsoft Outlook, select an existing M-Files folder or create a new M-Files folder:

If you want to...	Do the following...
Define automatically populated metadata for an existing M-Files folder	Right-click an existing M-Files folder in the navigation pane and select **Specify M-Files Properties** from the context menu.
Define automatically populated metadata for a new M-Files folder	Right-click a vault in the navigation pane, select **New Folder...** from the context menu, name the folder and press the Enter key.

   ☑ The **Properties** dialog is opened.

2. Click **Add...** to define a new property.

   ☑ The **Define Property** dialog is opened.

3. From the **Property** drop-down menu, select an M-Files property that you want to automatically populate, and then select either:

   a. **Use a fixed value** and enter or select a value in the field below if you want to populate the property value with a fixed value.

      or

b. **Read from the e-mail message** and select an e-mail header field to read information from by using the **Field** drop-down menu if you want to populate the property value with informaton read from the imported e-mail message.

4. Click **OK** to close the **Define Property** dialog.

   ☑ The automatically populated property is added to the **Properties** list in the **Properties** dialog.

5. Optional: On the **Properties** list in the **Properties** dialog, check the **Retain** check box of an automatically populated property if you wish M-Files to always remember the most recent value set by any user for this property, ignoring the original value set in this dialog.

6. Using the **Permissions** drop-down menu, define the permissions for documents created via this folder.

7. Optional: Check the **Prompt for metadata** check box if you wish to display the metadata card and prompt for additional metadata whenever an e-mail message is dragged and dropped to this folder.

8. Using the **Save as type** drop-down menu, select the e-mail message format for the messages saved to this folder.

9. Optional: Check the **Common to all users** check box if you wish to display this folder to all vault users in Microsoft Outlook.

   ⓘ If the **Common to all users** option is enabled, you can specify the users who may see this folder on the **Permissions** tab.

When an e-mail message is dragged and dropped to the Microsoft Outlook folder for which you have just set automatically populated metadata definitions, the message is saved to M-Files with automatically populated metadata.

Associating Messages with Contacts

You can use M-Files Admin for specifying messages to be automatically associated with contact persons and customers saved in M-Files on the basis of the sender and recipient information. A message from, for example, *matt.bay@estt.com* can be automatically associated with the contact person *Matt Bay* and the customer *ESTT*.

When the user is saving an e-mail message to M-Files in Outlook, M-Files looks for similarity between the e-mail addresses in the message and the properties that have been specified in M-Files Admin. On the basis of similarity and the properties specified by the administrator, M-Files automatically associates the message with customers or contact persons when the message is saved in the M-Files folder in Outlook.

   📄 **Note:** The association is possible only if the message is saved in Microsoft Outlook 2007, 2010, 2013, or 2016.

This automation takes place on a vault-specific basis (with a vault-specific M-Files folder in Outlook), also applying to all subfolders of the M-Files folder in question. The message must be saved via the *Save to M-Files* function or by dragging the message to the M-Files folder in Outlook. If you drag the message directly to the M-Files user interface, it will not be associated with the customer or contact person.

E-mail Client Integration Settings

To open E-Mail Client Integration Settings:

1. Open M-Files Admin.
2. Select a vault in the left-side tree view.
3. Select **Action** > **E-Mail Client Integration Settings**.

Contact persons

M-Files looks for a full match with a contact person's e-mail address. M-Files associates the message with the contact person *Matt Bay* if *Matt Bay*'s properties have exactly the same e-mail address as the message does (*matt.bay@estt.com*).

Customers

If customer information has been specified in the e-mail integration settings:

1. M-Files looks for customer matches via the contact person (the *Customer* object type must be the owner of the *Contact person* object type): M-Files associates the message with the customer *ESTT* if Matt Bay is the contact person for *ESTT*.
2. M-Files looks for similarity between the domain name in the e-mail address and the customer's properties: M-Files associates the message with the customer *ESTT* on the basis of the e-mail address domain, *matt.bay@**estt.com*** or *patsy.bay@**estt.com*** if the domain *estt.com* can be found in the customer's properties. The message will not be associated with any contact person in this case, unless a full match is found with the contact person information.

E-Mail Client Integration Settings - Advanced

The **Advanced** tab of the **E-Mail Client Integration Settings** dialog allows you to further specify associations between e-mail information and M-Files metadata. M-Files automatically populates the metadata card according to the mappings defined in these settings.

First, you can select a default class for all the e-mail messages that are saved to M-Files via Outlook. Secondly, the options allow you to define an appropriate metadata property for each e-mail header field value.

For instance, if you want the information contained in the *From* field to be automatically inserted to a certain property on the metadata card of the e-mail object, select the appropriate property from the drop-down menu.

The M-Files Flag

The M-Files flag, shown in Outlook's message list, indicates that you have already saved the message to M-Files.

If some other user (for instance another recipient) has saved the same message to M-Files, M-Files prompts you to confirm whether you wish to save that message again. Even if you do not save the message again, the M-Files flag will now be displayed in Outlook for that message.

With the *Update M-Files Status* function (in the message's context menu), you can easily display all M-Files flags. Also messages saved in M-Files by other users will then have an M-Files flag in Outlook.

7.3. Functions in AutoCAD and AutoCAD LT

The M-Files functions accessible directly in AutoCAD and AutoCAD LT make it easy to work with CAD drawings. You can access the functions from the *File menu* or the *M-Files menu*. The menus may look a little different, depending on the version of AutoCAD or AutoCAD LT in use.

The following M-Files functions are available in Autodesk AutoCAD and AutoCAD LT versions 2007–2017. The functions are also available in discipline-specific products based on these versions of AutoCAD, such as AutoCAD Architecture, AutoCAD Civil 3D, AutoCAD Map 3D, and AutoCAD MEP.

M-Files functions in AutoCAD and AutoCAD LT are:

- Open from M-Files
- Save to M-Files
- Check Out
- Check In

- Undo Checkout

For more information about these functions, see *Functions in Word, Excel and PowerPoint* on page 162.

Properties

For more information about this function, see *M-Files Properties* on page 163

Insert Field

With the *Insert Field* function, you can add M-Files metadata to drawings along with AutoCAD fields. The M-Files metadata fields are located in the M-Files *field category* in the *Field* selection dialog in AutoCAD.

For more information, see *Insert M-Files Property* on page 163.

8. M-Files Admin

This chapter describes the functionality of the M-Files Admin tool by examining the tree structure in the left pane and the options in the *Action* menu.

The application is used for administrating and maintaining M-Files document vaults and M-Files Server connections.

M-Files Server is the backbone of the M-Files system. It saves all objects (such as documents, employees and customers), controls access rights, registers object modifications (version history), and allows the system administrator to configure connections also to other systems (such as a customer registry). Basically, M-Files Server saves and controls all information related to the M-Files system.

Technically, M-Files Server, like M-Files Desktop, is a *service*. This means that M-Files Server starts automatically when the server computer starts. The M-Files server software is run even if there are no users logged in on the computer running the M-Files server software.
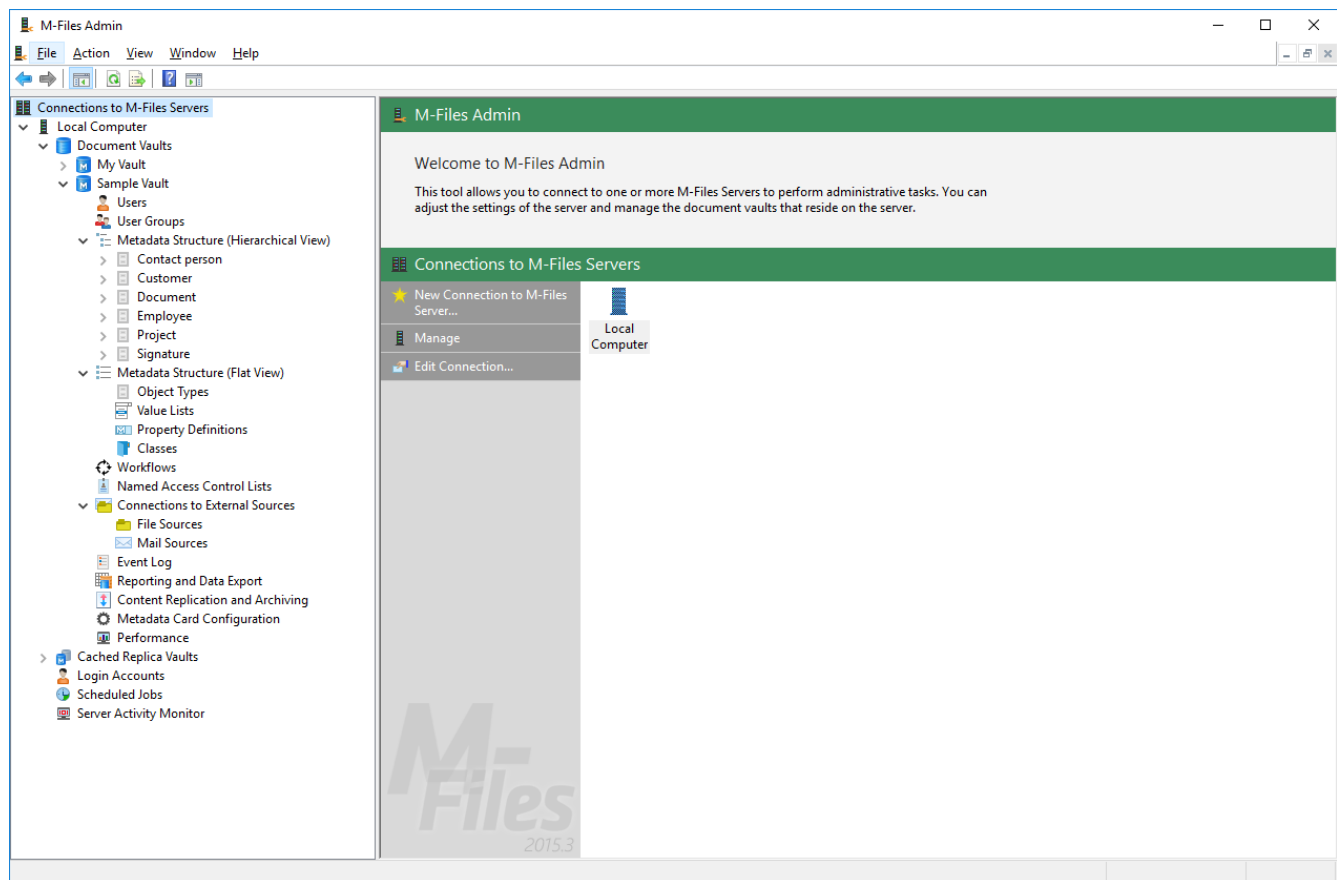
Figure 68: The M-Files Admin main window displaying the different levels inside a document vault.

Terminology

Vault	The *document vault* is managed with M-Files Admin. This is where you can add users to the document vault, change the metadata structures of objects, and edit views visible to all users. Also refer to the table *Daily M-Files terminology* on page 8.
Login account name	The M-Files Server login account that is used to log in to M-Files Server and on the basis of which a new user can be added to the document vault.

User	The M-Files user, who, at the server level, can be either a regular user or a system administrator. Users can be added to the desired document vaults, and a user's document vault administration permissions depend on the document-vault-level roles assigned to the user. On the document vault level, roles mainly determine the user's permissions to document vault administration. A regular user's basic permissions are also assigned by means of roles. Users can be grouped into external and internal users. For example, you can define your customers as external users. External users can only see and access documents and objects specifically marked for them. By default, they do not have permissions to view any documents.
System administrator	A system administrator is a user who has been assigned the role of system administrator. A system administrator automatically receives all permissions to every document vault, i.e., basically he can perform all possible functions in M-Files. A system administrator can add the role of system administrator to any other user. However, a system administrator cannot log in to a document vault if he has not been added as a user of that particular vault.
User group	You can create *user groups* on the M-Files server to which individual users can be added. Each user automatically belongs to the user group *All internal and external users*. In addition, each internal user automatically belongs to user group *All internal users*. User groups are specified on the document vault level. User groups can be used to define the permissions to an object, i.e., to specify the users who may access it.
Role	Roles can be used to provide users with permissions that mainly affect M-Files Server Administration. The permissions gained through roles always take precedence over document and object permissions. User who has all permissions to a document vault can access any object, even if the access of a particular user to a document has been denied by means of object-specific permissions.
Value List	A value list is a list that contains various values, such as the names of all customers. The same value list can be utilized in several different *properties*.
Property Definition	*Property definitions* are used to determine properties associated with *document classes*. A property definition is used to define the property name (which should be descriptive) and *data type*, which determines the type of the data entered (in relation to the property).
Workflow	Workflows define how the organization manages a process. An example of a workflow is *invoice circulation*. The workflow has related states and definitions regarding the task performer, permissions, and state transitions.
Object type	Besides documents, you can also manage other objects, such as *customers* and *projects*. These data set definitions are called object types. *Document* is one object type.
Metadata	In M-Files Admin, you can change the structures of metadata (for example, value lists, property definitions, document classes, and document class groups) and create new metadata, whereas you just specify values for these metadata items in the day-to-day use of M-Files. Cf. the table *Daily M-Files terminology* on page 8.

Connections to external databases

M-Files offers flexible approaches for information presentation and transfer also from external sources. Databases, for example, are required to support *OLE DB* or Open Database Connectivity (*ODBC*) connections. The type of a database connection can be either read-only or two-way. With a read-only connection, M-Files is reading from an external database, such as a customer database, but you are not allowed to enter new data via M-Files. With a two-way connection, changes and additions made in M-Files are saved in the external database.

A good example of an external database connection is a connection between M-Files and an external customer database. Many organizations already have a vast database of customer information, consisting of tables populated with customer information. When the user creates a new offer document in M-Files, it makes sense to add the existing customer information to it. M-Files can be set to import customer information from an external database. The information can then be accessed directly from, for example, the metadata card when a new document is created.

You can also import and link existing files from external objects. This function makes deploying M-Files easy and quick, since all existing files can be accessed via M-Files without a separate time-consuming transfer process. When one is accessing files via M-Files, it makes sense to add metadata for them at the same time. Furthermore, among other things, version history is created in M-Files; concurrent editing is avoided; and, thanks to M-Files scheduled jobs, backups are easy to manage. Adding metadata also enables you to better take advantage of the search capabilities of M-Files.

Saving and managing e-mail messages

M-Files provides the opportunity to save, manage, and share important e-mail in a controlled manner. The messages can be transferred directly from the mail server to the document vault without the need for separate actions by the user.

For example, messages and their attachments sent to the organization's common e-mail box can be transferred directly to the document vault. In the document vault, imported messages can be handled in a controlled manner via, for example, the workflow features. The purpose of use might be central, controlled handling of orders or saving of sent offers. This way, important information can be managed in M-Files so that the information does not disappear or get forgotten in e-mail boxes.

For more information about these and many other possibilities, refer to *Functions in Outlook* on page 165.

8.1. New Server Connection

Start setting up a new server connection by selecting *Connections to M-Files Servers* in the left-side tree structure of the M-Files Admin and selecting *Action > New Connection to M-Files Server...* Connecting to the server with this function is quite similar to establishing a document vault connection (see *Adding a Document Vault Connection* on page 35).

Figure 69: Server Connection Properties.

Alias

First assign a name to the server connection.

Connection / Server Name

Enter the network name or IP address of the server on which M-Files Server has been installed and that contains the document vault.

Connection / Port Number

The server was specified in the previous field, and in this field you specify the port to connect to on the server. Enter the server port number to connect to. M-Files uses port 2266 by default.

Connection / Protocol

Specify the protocol to be used for the network connection. The available protocols are *TCP/IP*, *SPX*, *Local Procedure Call (LPC)* and *HTTPS*.

Encrypted connection

Activate this option to enable RPC encryption between M-Files Admin and M-Files Server.

The option is available for the TCP/IP protocol only. If the protocol is HTTPS, the connection is always encrypted at the HTTPS protocol level. For connections from outside the organization's internal network, HTTPS or VPN should still be used, as RPC communication to the default TCP port, 2266, is often blocked by firewalls.

> **Note:** 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.

For more information on encrypted connections and for instructions on how to configure the server to require encrypted connections, refer to *Protecting Data in Transit with Encryption in M-Files*.

Connection / Test Connection

You can test the operation of the server connection with the **Test Connection** button.

Authentication

Specify the method M-Files Server is to use for authenticating the user. The authentication options are *Current Windows user*, *Specific Windows user* and *M-Files user*.

8.2. M-Files Server

This section offers a brief description of M-Files servers.

It is recommended to use Universal Naming Convention (UNC) paths (such as `\\ServerName\`) with network drives, because letters assigned to these drives may not necessarily be visible to the M-Files server; in Windows, drive letter assignments are frequently user-specific. A network drive may contain an external database for a value list, among other things. Also refer to *Value Lists* on page 269.

Note that, in a network, the M-Files server uses by default the identity of the computer running the M-Files server software (DOMAIN\COMPUTER$). Backup to a network drive, for example, is possible as long as the DOMAIN \COMPUTER$ Windows user, representing the server, has write permissions to this drive. In certain functions, it is possible to enter the logins that the function is to use during the procedure.

Disconnect, Connect

You can use the **Disconnect** function to disconnect the network connection to the server. You can reconnect the connection later without having to specify the server registration properties again.

To disconnect:

1. Highlight the server connection.
2. Open the **Action** menu.
3. Select **Disconnect**.

To reconnect:

1. Highlight the server connection.
2. Open the **Action** menu.
3. Select **Connect**.

License Management

License management settings are accessed by right-clicking the server and selecting *License Management*. For more information about licenses and assigning licenses to login accounts, refer to *License types* on page 181.
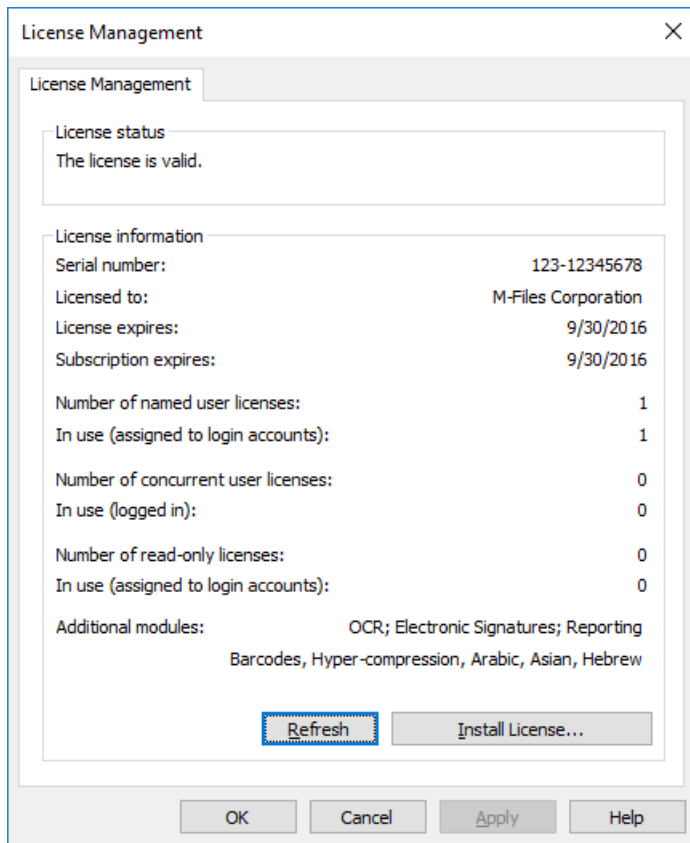
Figure 70: M-Files license management window.

License Status

The status of the license is shown here. Users receive a notification before the license expires.

Serial number

This is your M-Files serial number.

Licensed to

The license holder is displayed here. This confirms that your organization is the registered user of the software.

License expires

License expiry date. Normally, the license never expires.

Subscription expires

Subscription expiry date. During the subscription period, you are entitled to all M-Files version updates free of charge. You also need to have an active M-Files subscription for receiving customer support free of charge.

Number of named user licenses / In use

The number of licenses installed is displayed for each license type separately. Below that you can see the number of licenses in use. *Named user licenses* are assigned to individual login accounts. For more information about license types, refer to

Number of concurrent user licenses / In use

The number of *concurrent user licenses* in use is determined by the number of currently logged in logins using this license type. A license is reserved when a user using this license type logs in to M-Files. When the user *logs out* on page 127 of M-Files, the license becomes available. For more information about license types, refer to *License types* on page 181.

Number of read-only licenses / In use

A read-only license allows the user only to read content. It does not allow the user to create or modify documents in the document vault. For more information about license types, refer to *License types* on page 181.

Additional modules

Here you can see the additional modules to which you have access, such as the OCR module.

Refresh

The **Refresh** button brings the "in use" license data up to date.

Install License

When the evaluation period expires, you need a license to be able to use M-Files. Install your license by selecting **Install License**. Enter the serial number and license code you have obtained, and then click **OK**.

License types

Select a license type for the login account. The different license types are listed below. For more information about licenses, refer to *License Management* on page 179.

▶ Video: *Licenses and Login Accounts*

Named user license

Named user licenses are assigned to individual login accounts. This license allows the login account to use M-Files any time, independent of other users.

Concurrent user license

When a login account entitled to a concurrent user license logs in, one license of this type is taken up. When the login account logs out, the license becomes available for use by other login accounts that use this same license type.

Read-only license

Read-only licenses are assigned to individual login accounts. This license allows the login account to use M-Files at any time, independent of other users. The license is limited in the sense that not all M-Files features are available for use: the user is only able to read but not to create or modify documents.

Notification Settings (M-Files Admin)

M-Files can be requested to send e-mail notifications to end users about object-related actions. Users can create new notification rules via M-Files Desktop (see *Notification Settings (M-Files Desktop)* on page 127 and *"Follow this object" functionality* on page 55).

📄 **Note:** In addition to enabling notifications via M-Files Admin, for the end users to receive e-mail notifications, *event logging* on page 364 and *M-Files Desktop notifications* on page 127 must be enabled.

Do the following steps to enable e-mail notifications on the M-Files Server computer:

1. Open M-Files Admin.

2. In the left-side tree view, right-click the desired connection to M-Files Server and select **Notification Settings** from the context menu.

   ✅ The **Notification Settings** dialog is opened.

3. Check the **Enable notifications** option check box.

4. In the **SMTP server** field, enter the address of the SMTP server to be used for sending notification e-mail messages.

   ✏️ For example, `mail.company.com`. Ask your network administrator for the e-mail server name used by your company.

5. Optional: Check the **Use encrypted connection (SSL/TLS)** option check box if the connection to the SMTP server is encrypted.

6. In the **SMTP server port** field, enter the port number that the SMTP server is using.

   ℹ️ The default ports are 25 (without SSL), and 587 (with SSL). The most commonly used ports are 25, 465, and 587.

7. Optional: Check the **SMTP server requires authentication** option check box if the SMTP server requires the sender to be authenticated.

   a) In the **Account name** field, enter the username of the sender's e-mail account.

   b) In the **Password** field, enter the password of the sender's e-mail account.

8. In the **Sender's e-mail address** field, enter the e-mail address for the notification sender.

   ✏ For example, `m-files@company.com`. The e-mail address does not have to actually exist.

9. In the **Sender's display name** field, enter the name for the notification sender to be displayed in the *From* field of notification messages.

   ✏ For example, `M-Files`.

10. In the **Digest message** field, specify the time when the daily digest messages are sent.

   ⓘ M-Files users can choose to receive their notifications as individual messages or as a daily digest message. For more information, see *Notification Settings (M-Files Desktop)* on page 127.

11. Click **OK** to save your changes and to close the **Notification Settings** dialog.

Notifications are now enabled on the M-Files server.

- Users must enable notifications in M-Files Desktop to be able to receive notifications. For instructions, see *Notification Settings (M-Files Desktop)* on page 127.
- The administrator and users can also create notification rules on the basis of which notification messages are sent. See *Notification Settings (M-Files Desktop)* on page 127 for more information.
- You can customize your notification messages. For instructions, see *Personalizing Notification Messages* on page 183.

Personalizing Notification Messages

M-Files uses customizable templates for e-mail notifications. The notification templates can be modified to match the requirements of your organization.

The M-Files installation directory contains a server-level template file as well as various vault-specific template files.

📄 **Note:** Modifications to the server-level notification templates are reset when M-Files Server is updated. Modifications to vault-specific templates are preserved during the migration to a new M-Files version, but as they are not saved to the vault database, the templates are not included in a *vault backup* on page 224 or a *copy of a vault* on page 225.

Do the following steps to personalize notification messages:

1. Either:

   a. If you wish to modify the server-level template, navigate to the directory `C:\Program Files \M-Files\<M-Files version>\Server` on the M-Files server computer and open the file `notifications_template.txt` in a text editor of your choice.

   or

   b. If you wish to modify a vault-specific template, navigate to the directory `C:\Program Files\M-Files \<version>\Server\Data\Notifications\<vault GUID>\<notification rule ID>` on the M-Files server computer and open the file `notifications_template.txt` in a text editor of your choice.

   or

c. If you wish to create and modify a template for a notification rule, take note of the notification rule ID, create the folder `C:\Program Files\M-Files\<version>\Server\Data\Notifications \<vault GUID>\<notification rule ID>` on the M-Files server computer, and create a new `notifications_template.txt` file in the folder.

> 📝 **Note:** Your M-Files installation directory may vary from the example given.

> 📝 **Note:** You can view the *notification rule ID* via the M-Files Desktop *Notification Settings* on page 127 dialog, and the *vault GUID* under the name of an existing vault in the *Document Vault Properties* on page 28 dialog.

2. Edit the lines that begin with a colon (`:`) to customize the content of the notification messages. Make sure to preserve the colon at the beginning of each line that you edit.

ℹ️ View the template files for additional instructions. Editing the templates requires a basic understanding of HTML and CSS.

ℹ️ The notification messages can include placeholders. For example, to include an object ID in the message, add the string `%OBJID%` to the template in the appropriate location. The available placeholders are described in the table below.

Placeholder	Description
CAUSEDBY	The name of the user who caused the event.
CAUSEDBYACCOUNT	The account name for the user who caused the event.
FILENAME	The name of the file.
HYPERLINKFRAGMENTHTML	An HTML formatted hyperlink containing URLs to the object for M-Files Desktop, M-Files Web, and M-Files Mobile.
HYPERLINKFRAGMENTPLAIN	A plain-text formatted text fragment containing URLs to the object for M-Files Desktop, M-Files Web, and M-Files Mobile.
INTERNALID	The (internal) ID of the object. The internal ID is always unique for each object of a single object type and within a single vault (see also *OBJID*).
MFILESURL	An M-Files URL that shows the latest version of the object in question.
MFILESURLTOVERSION	An M-Files URL that shows the specific version of the object in question.
MOBILEURL	M-Files Mobile URL that shows the latest version of the object in question.
MOBILEURLTOVERSION	M-Files Mobile URL that shows the specific version of the object in question.
NOTIFICATIONRULENAME	The name of the notification rule that caused the event. Available for notification templates.
OBJID	The (external) ID of the object (see also *INTERNALID*).
OBJTITLE	The name or title of the object.

Placeholder	Description
OBJTYPE	Object type.
OBJVER	Object version.
ROLLEDBACKTOVERSION	The version that the object was rolled back to.
TIMESTAMP	The time when the event occurred.
USERCAUSEDWORKFLOWSTATE_Z	The user who moved the object into a specific state, Z being the ID of the workflow state.
VAULTNAME	The name of the document vault.
VAULTGUID	The unique identifier (GUID) of the vault.
WEBURL	An M-Files Web URL that shows the latest version of the object in question.
WEBURLTOVERSION	An M-Files Web URL that shows the specific version of the object in question.
PROPERTY_<ID>	The value of the specified property of the object. (Replace <ID> in the placeholder with the ID of the property definition.)
OLDPROPERTY_<ID>	The old value of the specified property of the object. (Replace <ID> in the placeholder with the ID of the property definition.)
OBJTYPE_<ID>	Values of all the properties that can refer to the specified object type. (Replace <ID> in the placeholder with the ID of the object type.)

3. Save your changes to the template file.

4. Use Windows Task Manager to restart the **MFServer** service.

   ℹ This makes sure M-Files Server detects your newly introduced changes to the notification templates.

Your notifications are now personalized.

Web and Mobile Access

M-Files Web provides a way of accessing your document vaults via a web browser. It is thus possible to use M-Files on any computer that provides the capability for web browsing.

The M-Files Web interface is managed with the M-Files Server computer. In a normal implementation, M-Files Web is set to listen on TCP port 80 for the HTTP protocol, but there are other possibilities as well. For more information, contact M-Files customer support.

M-Files Web has been implemented with standard languages, such as HTML, DHTML, JavaScript, and CSS. This makes it possible to use M-Files with various browsers, among them Chrome, Internet Explorer, Mozilla Firefox, Opera, and Safari. Please see the *System Requirements and Technical Details* on page 21 for details.

Enabling the Necessary Internet Information Services (IIS) Components

The following Internet Information Services (IIS) components need to be enabled on the M-Files Server computer before web and mobile access can be enabled:

- ASP.NET features
- Dynamic Content Compression

- Windows Authentication
- IIS Metabase and IIS 6 configuration compatibility
- Static Content

1. In Microsoft Windows open **Control Panel** and then open **Programs and Features**.

   ☑ The **Programs and Features** dialog is opened.

2. On the task pane on the left, click **Turn Windows features on or off**.

   ☑ The **Windows Features** dialog is opened.

3. Navigate to **Internet Information Services** > **World Wide Web Services** and enable the **Common HTTP Features** feature.

4. Navigate to **Internet Information Services** > **World Wide Web Services** > **Application Development Features** and enable the **ASP.NET** features.

5. Navigate to **Internet Information Services** > **World Wide Web Services** > **Performance Features** and enable the **Dynamic Content Compression** feature.

6. Navigate to **Internet Information Services** > **World Wide Web Services** > **Security** and enable the **Windows Authentication** feature.

7. Navigate to **Internet Information Services** > **Web Management Tools** > **IIS 6 Management Compatibility** and enable the **IIS Metabase and IIS 6 configuration compatibility** feature.

8. Navigate to **Services** > **World Wide Web Services** > **Common HTTP Features** and enable the **Static Content** feature.

9. Click **OK** to close the **Windows Features** dialog.

You should now have the neccesary components installed and you are ready to enable web and mobile access on the selected server computer.

Enabling Web and Mobile Access

M-Files Web uses Microsoft Internet Information Services and .NET framework version 4.0 (or higher). These applications must be installed on the computer running the M-Files Server in order to enable M-Files Web.

1. Open M-Files Admin on the server computer on which you intend to host web and mobile access.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Still in the left-side tree view, right-click the connection and select **Configure Web and Mobile Access...** from the context menu.

   ☑ The **Configure Web and Mobile Access** dialog is opened.
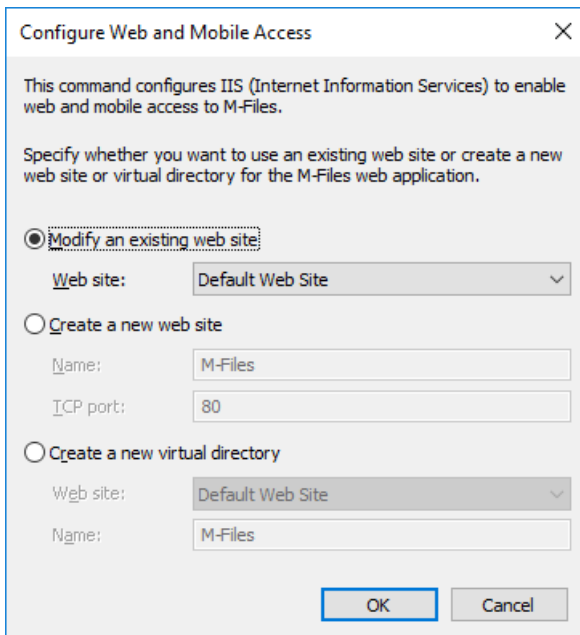
4. Select one of the following options:

Select the option...	If you want to...
Modify an existing web site	Modify an existing M-Files Web site. Select the existing site using the **Web site** drop-down menu.
Create a new web site	Create a new M-Files Web site within IIS. Enter the name of the site in the **Name** field and the TCP for connecting to the site in the **TCP port** field. The TCP port is 80 by default as it is the most common TCP port for web servers. If you use any other port, you need to indicate the port in the URL (`http://<domain name>:<port>`) to access the site.
Create a new virtual directory	Create a new M-Files Web site under a virtual directory within an existing web site. Use the **Web site** drop-down menu to select the preffered existing web site and, in the **Name** field, enter the name of the virtual folder. The URL for accessing the site is thus `http://<domain name>/<virtual folder name>`.

5. Click **OK** to close the **Configure Web and Mobile Access** dialog.

You should now have web and mobile access to the vaults under the selected connection. You can test to see if your site is online by typing the URL of your site into your web browser.

M-Files Web Publication Settings

When documents are published online for customers or other interest groups, it is usually a good idea to hide some of the object properties. For example, if the user has read-only access, the functions for editing need not be displayed at all. With the publication settings, the users can be granted suitable and sufficient functions that facilitate and simplify accessing and processing the published information.

> 📄 **Note:** You can use the *Get Hyperlink* function in the task area when you want to send a link to the document from the M-Files Web interface.

Site for definition of the publication settings (site and vault specific)

You can specify different publication settings specific to the site and vault by using a separate configuration site.

Log in to the configuration page by using your company's M-Files Web URL (for instance "http://www.publications.company.com") and by adding "/configuration.aspx" at the end of the address. For example,

"http://www.publications.company.com/configuration.aspx". If you have already logged in to M-Files Web in the browser, M-Files does not ask you to log in again.

📝 **Note:** You must have system administrator's rights in order to be able to edit the publication settings

Site-specific settings

From the site-specific settings, you can make selections that apply to the configuration site and all vaults of the site.

Figure 71: The publication settings configuration site.

Restrict access to configuration pages

You can specify the configuration site to be accessible for a certain IP address range only. Access to the configuration site is usually allowed only for connections from inside the company.

Display options

Page title: You can freely name the page of the web site you are offering. The default title is "M-Files Web".

Language: By default, M-Files uses *Automatic* as the language selection. This means that the M-Files Web language is determined by the language of the user's browser settings. If the language in the browser settings is not supported by M-Files, the language installed on the M-Files server will be used.

Alternatively, you can set a *Specific language* to be the M-Files Web language. For example, if your company's instructions refer to functions that are in English or the users work in different languages, you can specify English as the M-Files Web language. You can choose from all languages supported by M-Files.

📝 **Note:** This applies to the user interface language only. For the full M-Files Web experience to be in the language defined by a specific user, four prerequisites need to be met:

- The vault has been *localized to the target language* on page 233.
- The vault language has been *set for the vault user* on page 32.
- The language setting has been set to *Automatic* as described further above.
- The language preference settings of the user's browser have been set to the desired language. For more information, see *this W3C article*.

Windows SSO

With Windows authentication enabled, M-Files Web can automatically use the user's Windows credentials for login. The administrator can configure the single sign-on (SSO) setting so that the login credentials are no longer required when users navigate to M-Files Web.

The automatic authentication is disabled by default, but can be enabled by setting the single sign-on value to *Use automatically*. Alternatively, the choice of using single sign-on can be displayed on the login page by selecting *Show on login page*.

Force M-Files User Login

Select this setting if you do not want to display the Windows login option to users. Then the user does not have to consider which login option is appropriate and M-Files suggests logging in as an M-Files user. For data security reasons, it may be advisable to disable Windows login in some cases.

📄 **Note:** This does not prevent logging in to the configuration site with your Windows user account.

Automatic Login

Select *Automatic Login* and enter the authentication information if you do not wish to require the users to enter their user ID for M-Files Web. This means that any user can access the site's vaults if authorized by the user ID.

Authentication (username, password and domain): If automatic login is enabled, this is the authentication information that M-Files uses for the automatic login. If you want M-Files to offer a specific ID for the user by default, save the default ID in the authentication information and disable automatic login. The user is still able to use other IDs, possibly granting more extensive web-based access.

Vault: You can also specify the vault to which the user is to be connected to. If the vault is not specified, the users can see all the vaults accessible with the credentials.

Vault-specific settings

You can specify, for example:

* Whether the vault is to be available for use via M-Files Web.
* The vault-specific default view.
* The configuration of the vault user interface.

Allow access to this vault

Select this if you want the vault to be accessible via M-Files Web.

📄 **Note:** In order to use a vault, the user must always have permissions for that vault.

Default View

You can specify which view is to be opened by default. The home view is opened by default.

Layout

You can choose the layout elements to be displayed – or hidden – in the vault. You can, for instance, hide the task area or choose to display the listing area only.

Prevent navigation outside default view

You can prevent navigation beyond the default view by choosing *Prevent navigation outside default view*. In this case, navigation is not possible, even if the breadcrumb is used.

Default search criteria and settings

You can select whether the latest search criteria and settings selected by users are to be kept or if you would prefer to use a specific criterion and setting. The same options as in M-Files Desktop are available.

Navigation within the vault

You can display or hide the top menu (*New*, *Operations*, and *Settings*) and/or breadcrumb.

> 📄 **Note:** When M-Files Web is displayed in the "Listing pane only" mode, object metadata and search functions are hidden from the users. This allows the users to only read and edit objects displayed in the listing pane, according to their permissions.

Vault controls

These settings allow you to control which functions are available for the users of the vault.

- *Save view settings*. If several users have the same user ID (for example, during automatic login), it is recommended to prevent saving of the column settings.

- *Workflow shortcut in properties pane*.

- *Checkout prompt*. If the M-Files Web users are granted *read-only* access and no edit permission, displaying the *Check Out* dialog is not necessary.

- *Hidden properties*. Some properties may be hidden from external users. In these cases, the information *(hidden)* is displayed in the properties pane or on the metadata card. It is recommended to hide this *(hidden)* information.

- *State transition prompt*.

- *Save search terms*.

- *Context menu*.

- *Advanced Search*.

- *Search in right pane*. With this option enabled, the search functions can be placed into the right pane.

Task area operations

The options in the task area settings allow you to decide which links are to be displayed in the task pane.

> 📄 **Note:** If you hide the *New* commands, users cannot create new objects. Additionally, if the *View and Modify* commands are hidden, they are not accessible via the context menu either.

Example: Modifying the Appearance of M-Files Web

1. Open the M-Files Web configuration page by entering the URL `http://<Your M-Files Web domain>/configuration.aspx` into your web browser and then enter your credentials if you are not already logged in.

   ✅ If you are already logged in, you will be redirected directly to the configuration page. Otherwise the configuration page will be opened after the login screen.

2. From the left-side tree view, under **Vault-specific settings**, expand the additional settings of the vault that you want to modify by clicking the arrow before the vault icon.

3. By clicking the folder beneath the selected vault in the left-side tree view, select the category that you want to modify:

   a. Select the **Controls** folder, if you want to show or hide various M-Files Web user interface controls.

   or

   b. Select the **Task area** folder, if you want to show or hide various elements on the M-Files Web task area.

4. Select the **Show** or **Allow** radio button for the elements that you want to enable.

   ✏️ For example, if you want to show the **Log Out** button on the task area, go to the **Task area** settings, and select **Show** for the **Log Out** option.

5. Select the **Hide** or **Disallow** radio button for the elements that you want to disable.

Document-specific Publishing via a Web Link

You can use M-Files for sharing documents with interested parties through direct web links. This feature makes it possible to, for example, provide a company web site with a direct link to a price list in M-Files. The link can be made to always refer to the latest version of the document, to be able to provide up-to-date information at all times. The link works in the same way as any ordinary web URL.

Normally, M-Files Web always requires a login name and a password to be entered. However, if the system is used for publishing, it may often be necessary to allow users to view documents without entering any credentials. To enable this, M-Files can be set to use a predetermined login account with, for example, read permissions for certain documents.

Enabling document-specific publishing via a web link

In order to enable document-specific publishing via a web link, the following steps have to be taken:

1. Create a login account, such as *Publishing*, on the server. Select **M-Files authentication** as the authentication method, and enter a password and other necessary data.

    For instructions, see *Creating a Login Account for Publishing* on page 191 below.
2. Assign the user to the desired document vault and define the user as an external user.

    For instructions, see *Assigning the Login Account to the Desired Vault* on page 192 below.
3. Provide the user with read permissions for published documents.

    For instructions, see *Providing the User with Read Permissions to Published Documents* on page 192 below.
4. Enable the login account to log in automatically.

    For instructions, see *Enabling the Login Account to Log In Automatically* on page 193 below.
5. After this you can create direct web links to the vault.

    For instructions, see *Creating Direct Web Links* on page 194 below.

Creating a Login Account for Publishing

In order to allow users to view documents without entering credentials, you must first create a login account that will be used to automatically log in to a specific vault.

1. Open M-Files Admin on the M-Files Server computer used for publishing content.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Highlight the **Login Accounts** node and click **New Login Account...** on the task pane.

    ☑ The **Login Account Properties** dialog is opened.

4. In the **Username** field, enter a suitable username for the login account, such as `Publishing`.

5. Select **M-Files authentication** as the authentication method, and enter a password of your choice in the **Password** and **Confirm password** fields.

6. Optional: Enter personal information of the login account in the **Full name** and **E-mail** fields.

7. Using the **License type** drop-down menu, select a license type for the login account.

8. Click **OK** to finish creating the login account.

The newly created login account is added to the **Login Accounts** list.

Assigning the Login Account to the Desired Vault

Next, the login account needs to be assigned to the vault that contains the published documents.

1. Open M-Files Admin on the M-Files Server computer used for publishing content.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand **Document Vaults**, then expand the desired vault and finally select the **Users** node.

4. Click **New User...** on the task pane.

   ☑ The **User Properties** dialog is opened.

5. Using the **Login account** drop-down menu, select the login account that you previously created.

6. Check the **External user** check box.

7. Optional: Check the **User cannot create documents or other objects** check box, if you wish to prevent users from creating documents or other objects with this user account.

8. Optional: Check the **User cannot create or modify** check box, if you wish to prevent users from creating or modifying traditional folders with this user account.

9. Click **OK** to finish creating the user.

The user is added to the **Users** list.
Providing the User with Read Permissions to Published Documents

The user needs to be provided with appropriate permissions in order to access published documents.

1. Open M-Files Admin on the M-Files Server computer used for publishing content.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. In the left-side tree view, select the **Named Access Control Lists** node under the selected vault.

5. Either:

   a. Click **New Named Access Control List...** to define a new named access control list containing read permissions for the newly created user account.

   or

   b. Double-click an existing named access control list on the **Named Access Control Lists** list to define read permissions for the newly created user account.

   ☑ The **Named Access Control List Properties** dialog is opened.

6. If you are creating a new named access control list, enter a suitable name for it in the **Name** field.

7. Click **Add...** to add the newly created user to the **Users and user groups** list.

   ☑ The **Select Users or User Groups** dialog is opened.

8. Select the newly created user from the **Users or user groups** list and click **Add** to add the user to the named access control list and to close the **Select Users or User Groups** dialog.

9. Back in the **Named Access Control List Properties** dialog, highlight the newly added user and provide the user the following permissions using the check boxes below in the dialog:

Permission	Allow / Deny
Change Permissions	Deny
Delete	Deny
Edit	Deny
Read	Allow

10. Optional: If your named access control list already has all permissions set to **Allow** for the **All internal users** user group, you can skip these steps. Do the following steps to allow all permissions for **All internal users**:

    a) Click **Add...** to add the **All internal users** user group to the **Users and user groups** list.

    ☑ The **Select Users or User Groups** dialog is opened.

    b) Select **All internal users** from the **Users or user groups** list and click **Add**.

    c) Highlight **All internal users** on the **Users and user groups** and check the **Allow** check box next to the **All** option on the **Permissions** list.

11. Click **OK** to close the **Named Access Control List Properties** dialog.

12. Assign the named access control list you just created or modified to all the public documents intended to be accessed without credentials.

If you have created a new named access control list, it is added to the **Named Access Control Lists** list. Otherwise your changes are saved to the existing named access control list that you have modified.

Enabling the Login Account to Log In Automatically

To make it possible to view published documents without logging in, M-Files must be set to log in automatically through M-Files Web. This way, published documents can be viewed without entering a username and password.

Before you begin, make sure M-Files Web is configured properly. For more information, refer to *Web and Mobile Access* on page 185. To ensure sufficient permissions, an *unlimited read-only license* is required.

1. On the M-Files Server computer, use Registry Editor to create the following registry key, where `<version>` is the M-Files version number (for example *11.1.4310.92*) and `<web site ID>` is a unique ID assigned to the M-Files Web site by Internet Information Services (IIS):

    ℹ `HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFWA\Sites\<web site ID>\`

    - If there is only one web site, the site ID is usually *1*.
    - If the M-Files Web site is running in the virtual directory of the web site, add a colon and the name of the virtual directory after the site ID. For example, if the application is accommodated in the M-Files Web virtual directory of this single web site, the web site ID is *1:MFWA*.
    - The IIS server software in Windows 2003 displays the ID as one column.

2. Specify the registry key values to be used for automatic login. The table below lists the values available for specification.

ℹ
Value	Type	Description
Domain	REG_SZ	If the authentication method used is Windows authentication, use this value to specify the domain.

Value	Type	Description
Password	REG_SZ	Login password.
UserName	REG_SZ	Login account name, for example "publishing".
Vault	REG_SZ	The document vault ID. The value can be for instance `{A8DCB561-913F-4318-A276-E7E171EAFBE6}`. The value can be found in the *Document Vault Properties* window of M-Files Admin.
WindowsUser	REG_DWORD	Specifies the authentication method. *0* means M-Files authentication, *1* means Windows authentication.

3. Close Registry Editor.

The selected login account can now be used to automatically log in to M-Files Web and the account can be used for accessing published documents without entering a username and password.

Creating Direct Web Links

Once automatic login is enabled, you can create direct web links between, for example, the company web site and document files. The opening page, `openfile.aspx`, can be assigned the following parameters:

Parameter	Description
objtype	Object type ID of the object to which the file to be opened belongs. This parameter is required. You can see the list of object type IDs by completing the first four steps of the *Creating a New Object Type* on page 259 task.
docid	ID of the document containing the file to be opened. This parameter is required.
docver	Version of the document containing the file to be opened. This parameter is not required. If this parameter is not used, the link always refers to the latest version of the document.
fileid	ID of the file to be opened. This parameter is not required unless the document containing the file is a multi-file document.
filever	File version.
showopendialog	This parameter specifies whether or not the web browser displays an opening dialog. If the value assigned to this parameter is 0, the dialog is not displayed.

As described above, you can provide your web site with a link that refers directly to a document. Below are examples of such web links. Replace *<server>* with the web address of your own server.

```
http://<server>/openfile.aspx?objtype=0&docid=71
```

```
http://<server>/openfile.aspx?objtype=0&docid=71&docver=7
```

```
http://<server>/openfile.aspx?objtype=0&docid=71&docver=7&fileid=71
```

```
http://<server>/openfile.aspx?objtype=0&docid=71&showopendialog=0
```

Sharing documents via OneDrive

In addition, you can use *Share via OneDrive* on page 125 links for version-specific publication of individual documents.

Back Up and Restore Master Database

The M-Files master database contains the server login accounts and scheduled backup jobs. For example, in case of a hardware failure, the master database can be restored from the backup so that login information and server-specific settings like scheduled backup jobs are not lost.

8.3. Document Vault Overview

This section offers a brief overview on document vaults. For a more detailed description, refer to *Document Vault Administration* on page 223.

Creating a New Document Vault

▶ Video: *New Document Vault*

If you want to create a new vault in a language other than the currently selected software language, you must first change the software language and restart the M-Files Server service via Windows Task Manager before creating the vault. For instructions on changing the software language, see *Selecting the Software and Vault Language* on page 238.

Do the following steps to create a new document vault:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Select **Document Vaults** in the left-side tree view.

☑ The **Document Vaults** list is opened in the right-side pane.

4. Click **New Document Vault...** on the task area.

☑ The **Document Vault Properties** dialog for a new vault is opened.

5. In the **Name** field, enter a name for the new document vault.

6. Use the **Primary language** and **Secondary language** drop-down menus to select the primary and secondary languages for full-text search features.

   > ℹ These selections affect, for example, the way inflected or irregular forms of words or compounds are dealt with in searches. If the document vault is to contain material in several languages, it is recommended to select the language that is used most as the primary language and a less commonly used language as the secondary language.
   >
   > Selecting a language or languages improves the probability of finding the right search results. Even if a certain language was not selected as the primary or secondary language, the full-text search will nevertheless return results if words in this language were used in the search.

7. Optional: Click **Import...** to change the vault icon to facilitate finding the right vault in case you are using multiple vaults.
   a) In the **Change Icon** dialog, select an item from the list or click **Browse...** to search for a different icon.
   b) Click **OK** once you have selected the new icon.

   > ℹ You can revert back to the default icon by clicking **Use Default**.

8. Optional: Change the *advanced settings* on page 197 on the **Advanced** tab.

9. Click **OK** once you are done.

You should now have created the document vault and it should appear on the left-side tree view of M-Files Admin under **Document Vaults**.

> 📄 **Note:** When you create a document vault, M-Files automatically creates an ID for it. The ID can be changed later in the **Document Vault Properties** dialog of the vault by clicking the **Change Unique ID** button.

After you have created the vault, the users of the vault must add a connection to it via M-Files Desktop settings. For instructions, see *Adding a Document Vault Connection* on page 35.

Document Vault Advanced Properties

In the document vault advanced settings, you need to define whether you are using Firebird or Microsoft SQL Server for saving document vault information.

Firebird is a SQL database engine integrated in M-Files. As part of the M-Files Server service, it requires no separate installation and is therefore very easy to use. Choose Firebird as the database engine, unless you have a particular reason to choose Microsoft SQL Server. Switching from Firebird to Microsoft SQL Server can be easily done later on if necessary. Changing from Microsoft SQL Server to Firebird is not, however, possible.

Microsoft SQL Server is a SQL database engine that requires purchasing and separate installation. It is recommended to use Microsoft SQL Server with large document vaults, but it also requires that the administrator is already familiar with the Microsoft SQL Server management.

> 📄 **Note:** Never modify the content structure of the document vault database directly using, for instance, database system management tools. The database contents may be modified with the M-Files Server service only. Other modifications endanger the logical integrity of the database, which may cause faulty operation of the software and loss of data. The structure and contents of the document vault may only be modified via M-Files Desktop, M-Files Admin tool, and M-Files API.
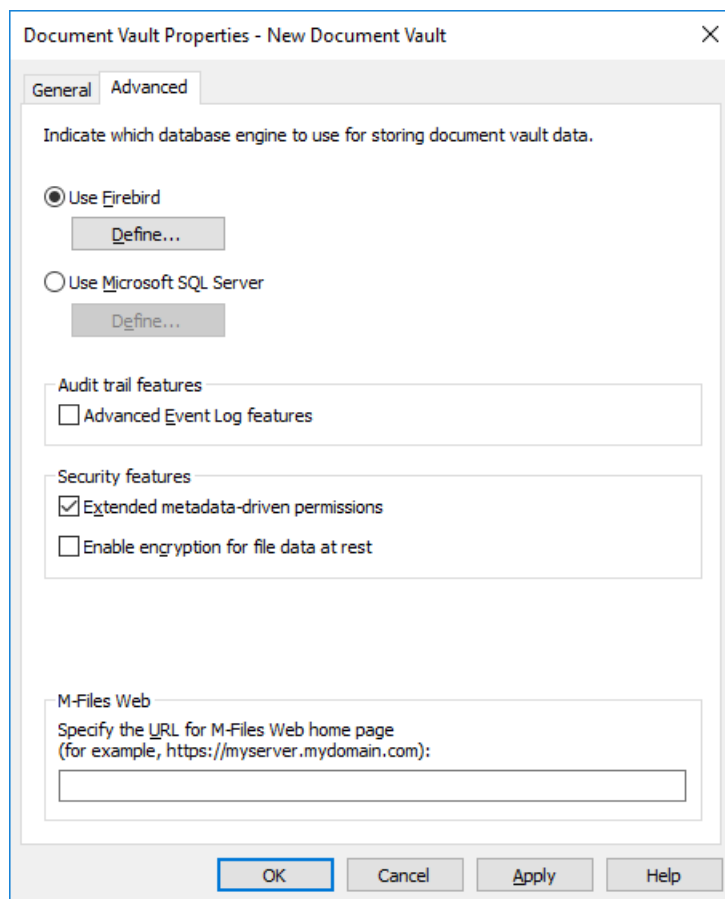
Figure 72: The advanced options of the "Document Vault Properties".

Use Firebird

See *Using Firebird as the Database Engine* on page 199.

Use Microsoft SQL Server

See *Using Microsoft SQL as the Database Engine* on page 199.

Audit trail features

M-Files supports the administration of electronic records and signatures in compliance with FDA 21 CFR Part 11. Electronic signing requires the Electronic Signatures module, which is available for a separate fee. The module includes event logging extensions and electronic signature functionality. The module is activated with an appropriate license code.

In addition to this, vault-specific properties of the audit trail must be activated. Open the *Properties* dialog of the vault for which you want to activate these features and, on the *Advanced* tab, enable *Advanced Event Log features* under *Audit trail features*. Electronic signatures are automatically enabled as soon as the license code is activated. For more information, see *Electronic Signing and Compliance* on page 222.

Security features

Extended metadata-driven permissions

For vaults created with version 8.0 (or later), the extended metadata-driven permissions are active by default. Otherwise they need to be manually activated. Please bear in mind that you cannot undo the operation.

> 📝 **Note:** If you have assigned automatic permissions to values in earlier versions of M-Files, it is strongly recommended to check that the permissions are still working as desired.

For more information on automatic permissions, refer to *Automatic Permissions* on page 275. You can activate the automatic permissions by value, value list, object type, or class. For you to be able to use the automatic permissions via a specific property, you should also allow this in the property definition's properties. For more information, see *New Property Definition* on page 288.

Enable file data encryption at rest

This option allows you to use the AES-256 algorithm for encryption of the vault file data at rest. The encryption is compliant with the Federal Information Processing Standard (FIPS) publication 140-2.

This option only encrypts file data that is stored to the vault *after* the feature has been turned on. If you want to encrypt existing data:

1. Select the vault in the left-side tree view of M-Files Admin.
2. Select **Action** > **Maintenance** > **Update encryption status of existing files**.

From the perspective of the end-user, file data encryption is not visible in any way.

> 📝 **Note:** Especially when encryption is enabled, it is crucial for the administrator to have thorough and frequent back-up processes in place. The combination of encrypted file data, hard drive failure and inadequate backup system could eventually lead to the loss of all data.

Other features

The *Annotation and redlining* feature enables you to add annotations to documents in the document vault. For more information about annotations in M-Files, see the topics *Annotations and Redlining* on page 72 and *Using Annotations* on page 73.

M-Files Web

The text field in this section should contain the URL to your M-Files Web home page. Creating M-Files hyperlinks for documents and objects stored in the vault requires this to be able to include M-Files Web URLs in the hyperlinks.

Make sure the URL starts either with *http://* or *https://*. For example: *https://myserver.mydomain.com*.

Using Firebird as the Database Engine

Firebird is a SQL database engine integrated in M-Files. Select Firebird as the database engine, unless you have a particular reason to choose Microsoft SQL Server.

Click the **Define...** under the *Advanced* tab of the *Document Vault Properties* to open settings for the Firebird engine.
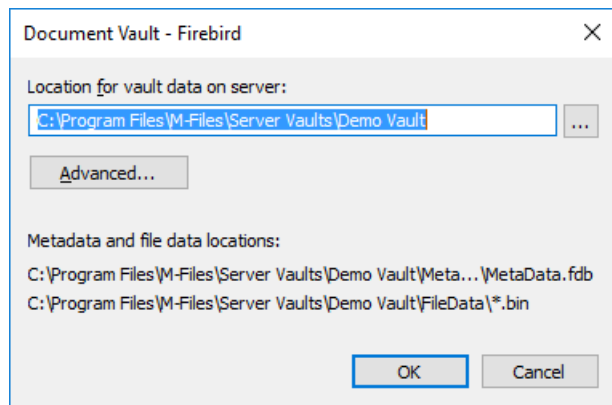
Figure 73: Location of metadata and file data when using Firebird.

Here you can define the vault folder on the server in which all of the document vault data is to be physically stored.

By default, *files* are stored in the same folder as the *metadata*. With the *Separate location for file data* option under **Advanced...**, you can define a location for file data that is different from the metadata location. This enables you to locate your file storage at a storage facility on a large network drive or file server. It is, however, recommended to store the metadata and files in the same location.

Using Microsoft SQL as the Database Engine

In addition to Firebird, you can use Microsoft SQL Server (2008, 2008 R2, 2012, 2014, or 2016) as the database system. M-Files supports all the SQL Server editions (Express, Standard, Enterprise, etc.).

> 📝 **Note:** For new installations, we recommend using Microsoft SQL Server Enterprise Edition 2016. If you are already using Microsoft SQL Server as the database engine for one or more vaults, and are interested in upgrading to a newer version for performance reasons, we recommend consulting our customer support at *support@m-files.com* before upgrading.
>
> The Microsoft SQL Server Enterprise Edition versions 2008–2016 provide the possibility for compressing table data and indices. This reduces the input/output activity of the disk, but also increases the CPU load by about 10 percent. Typically this means reduced database sizes.
>
> Microsoft SQL Server Enterprise Edition 2016 uses columnstore indices, which speeds up opening sub-levels of views, such as *Documents by project*. This is especially beneficial when empty virtual folders are set to be hidden.

Using SQL Server means that the database server memory can be more efficiently used and the backup storage of large data vaults is improved. In the event of problems, errors etc., you can switch to the mirrored database server without delay.

We recommend using Microsoft SQL Server with large document vaults that contain several hundreds of thousands or more documents or other objects. With large document vaults, Microsoft SQL Server provides better overall efficiency than Firebird. However, use of the Microsoft SQL Server database engine requires that the administrator is already familiar with the Microsoft SQL Server management.

> 📝 **Note:** Microsoft SQL Server licenses are not included in M-Files licenses and must be purchased separately.

Microsoft SQL Server may be located on the same machine as the M-Files Server, or it can be installed on another server. If SQL Server is installed on another server, M-Files Server and SQL Server must be linked with a fast network connection. Instructions for ensuring the efficient operation of SQL Server can be found in the Microsoft SQL Server documentation. Firstly, it is recommended to ensure that the SQL Server machine has a sufficient amount of memory. The number and speed of processors and hard drives also have a significant impact on the efficiency.

Figure 74: The Microsoft SQL Server properties dialog.

> 📝 **Note:** If your SQL Server does not use the default port (1433), the server name must be given as *<server name>,<port>*.

When Microsoft SQL Server is used as the document vault database engine, M-Files Server stores data in the document vault in the associated database. Certain secondary data that do not require a backup, such as search indices, are left outside the database.

Location of file data

File data can be saved in the Microsoft SQL Server database or other location, such as a network drive.

You can choose to:

- *Store file data in the vault database*.

- *Store file data in a file-system folder*.

  - With this option, you can freely specify the location for saving the files, on a network drive or in another location. You can keep the file data secure by designating a specific account for processing the file data.

Backing Up

The administrator is responsible for making backup copies and timing the backup copies of the document vault database. Backup copying is performed using SQL Server's own management tools and backup copying solutions offered by third parties. When restoring a backup copy, the administrator first returns the document vault database to the SQL Server using the desired method, and then reattaches the document vault to M-Files using the *Attach Document Vault* function.

▶ Video: *SQL Server Backups*

For more comprehensive backup instructions, please see the M-Files Knowledgebase article *M-Files Backup Policy*.

Migrating to Microsoft SQL Server

The document vault database engine can also be changed from Firebird to Microsoft SQL. Refer to *Migrate to Microsoft SQL Server* on page 227.

Attach Document Vault

A document vault may have been detached from M-Files Server (see *Detach* on page 229), in which case all data in the document vault is kept in a file folder on a hard drive but the document vault is not registered on the server. If you know the name of the document vault and want to start using it again, you can do so by attaching the vault back to *M-Files Server* with the *Attach Document Vault* function. You can find it by opening the *Document Vaults* section in M-Files Admin's tree-view.

If, for example, lack of space makes it necessary to move a document vault from one server to another, this can be done with the **Detach** and **Attach** functions – simply detach the vault on server A, and attach it on server B. The **Advanced** tab enables you to further specify information related to the database connection, such as vault data location for a Firebird vault, or Microsoft SQL Server connection details.

You can select whether to attach the vault with its *original identity* or with a *new identity*. For the difference between these two, see *Restoring a document vault* on page 202.

Restore Document Vault

A *full backup* and *differential backup* (see *Scheduled Backup Jobs* on page 216) of the document vault can be restored with the *Restore Document Vault* function. You can find it by opening the *Document Vaults* section in the M-Files Admin's tree-view.

▶ Video: *Restore Backups*
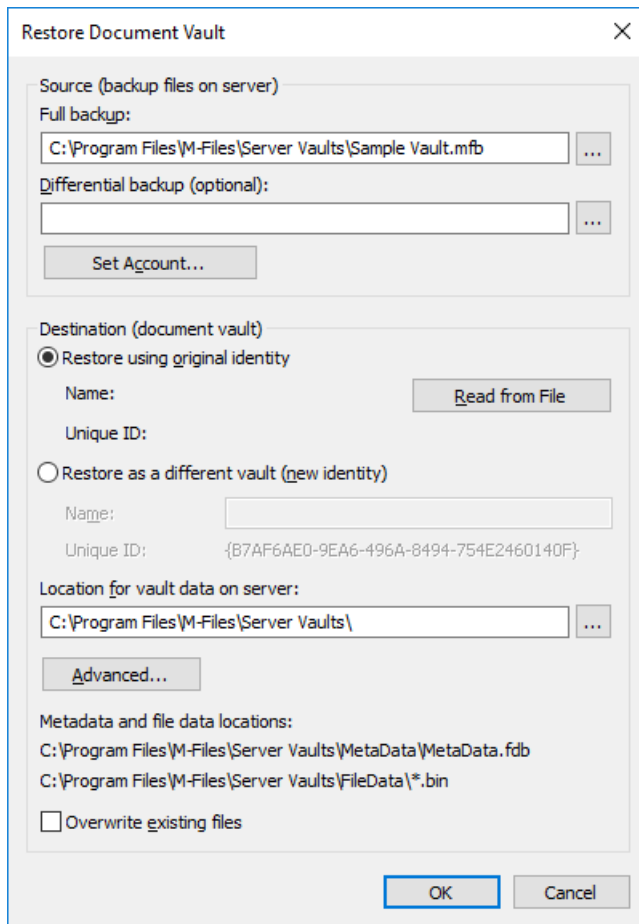
Figure 75: The "Restore Document Vault" dialog.

Restoring a document vault

Specify the *source* (backup files on the server) from which the *full backup* (and *differential backup*, if desired) is to be restored.

You can also determine whether the document vault is to be restored as a *different vault* (in which case M-Files creates a new unique ID for the vault) or with the *original identity* of the vault. The identity is used in establishing document vault connections to the server.

> 📄 **Tip:** The name of the vault can be changed on the server, and the document vault connection can have any name in the end user's client software.

You can also define the location for vault data, a separate location for file data under *Advanced...*, and whether or not to overwrite existing files.

Even if the document vault is *destroyed*, you can *restore* it if a backup has been made. For more information about backups, refer to *Scheduled Backup Jobs* on page 216.

8.4. Interaction Among Several Vaults

M-Files enables a multi-level interaction between several document vaults. The interaction enables you, for instance, to:

* Replicate data across several locations, which enables work that spans a variety of locations at all times, even if network connections are slow or get interrupted.
* Archive data from an actively used vault to an archive vault.

- Back up data from the vault on your server to the vault in the cloud service so that the users can immediately connect to the cloud service if they face problems with the vault installed on your server.
- Centralize data from several M-Files vaults to a single vault.
- Use several vaults, separating the various functions of the company so that content, metadata structures, and the permissions for the vaults can be customized to match the needs of various operations and business units.
- Publish certain documents via a separate vault for interest groups.
- Create relationships between objects in different vaults so that objects in other vaults can be found as the company's operations require.

With interaction, you can share documents and other objects efficiently between separate vaults. You can, for example, specify certain documents for sharing from the company's vault with a publishing vault. This enables you to easily provide your customers and other cooperation partners with up-to-date price lists, product descriptions, brochures, and other material from this publishing vault at all times without any manual copying or outdated information.

> **Note:** If M-Files is installed on several servers, there must be an *M-Files Additional Server License* installed on the additional servers. For example, if you want to replicate information between vaults on separate servers, this license must be installed on the additional servers.

Settings required for the interaction

Associations for the metadata definitions

In order for you to associate and synchronize metadata between vaults, the metadata definitions must also be associatable between vaults. For more information, refer to *Associating the Metadata Definitions* on page 203.

Synchronization of objects and values between vaults

In addition to associations for the metadata, the objects and values need to be updated or synchronized regularly so that the data content is up to date across vaults. Synchronization of data between vaults is performed with *replication* of contents, with data then exported from the source vault and imported to another vault.

The synchronization of this content can be performed with scheduled export and import operations. The content can be synchronized, for example, every 15 minutes. With this approach, the data in the target vault will always be up to date. For more information, refer to *Content Replication and Archiving* on page 375.

Two-way synchronization is possible between vaults, but synchronization can also be performed among many individual vaults. When defining the export, you can use a filter if you want to export and publish only certain documents or another objects for the target vault.

Associating the Metadata Definitions

In order to associate and synchronize objects and their metadata between different vaults, the metadata definitions must also be associatable between different vaults.

Associations between metadata definitions can be made in several ways depending on how the vaults are used. Certain metadata definitions are always associated automatically. Some of them are associated automatically according to the vault structure, but for some of them, it must be done manually using aliases.

Purpose of the Vault vs. Metadata Associations

Associations between metadata can be created in several ways, depending on the purpose of use of the vaults. The target vault can be used in archiving, replication, backups, and publication. For this reason, you should consider – before creating a vault that might be used as a target vault – which implementation is the easiest and best for creation of the desired vault.

If the association and synchronization is performed between two or more existing vaults, check the association of the metadata definitions and define the scheduled export and import between vaults.

Perfect copy (for example replication, archiving, and backup)

If you want the vaults to be perfect – full and complete – copies of each other in terms of both metadata and contents, you should first create a target vault through backup or copy of the relevant vault and then define the export and import. This way, especially the metadata definitions are automatically matched with the names and IDs and any separate definition of aliases need not be performed one metadata definition at a time.

> 📄 **Note:** Metadata definitions created after creation of the vault must be manually associated between vaults by using aliases.

Partially the same metadata structure and partially the same contents (for example vaults intended for different purposes in the company)

If you want the metadata largely matching each other between vaults, you should consider first creating the metadata structure of the target vault through metadata structure export (see *Export Structure* on page 382) and then define the export and import. After this, you should verify in the target vault that the metadata structure corresponds to the use of the target vault.

> 📄 **Note:** Metadata created after creation of the vault must be manually associated between vaults by using aliases.

Different metadata structure but partially the same content (for example, publication of certain objects from one vault to another)

If you want to publish only certain objects and metadata in the so-called publishing vault, you should create the metadata structure of the publishing vault separately from that of the source vault.

In this case, aliases must be defined for all other metadata structures than built-in ones, so that metadata can be associated when the synchronization is performed.

Associating Metadata

By default, M-Files associates metadata by the following methods (in order of relevance):

1. **The built-in metadata definitions are always automatically associated,** regardless of the manner of creation of the vault metadata structures or methods of performing the association. These metadata definitions might be *Name or title*, *Created by*, *Last modified by*, *Keywords*, etc. In publishing operations, you may want to hide some of these; for example, you may not want to show the document creator in the publishing vault. You can edit the built-in metadata to suit the publishing operation via the registry settings and permissions.
2. All the items have a **GUID (globally unique identifier)**. If there is a GUID match across vaults, the metadata definitions are always mapped automatically.
3. If the **aliases match** between the vaults, the association of the metadata definitions is always performed. The alias must be manually defined in each vault for the metadata definition in question. For more information, refer to the section *Aliases for association of the metadata between vaults* below.
4. If **both metadata definition's ID and the name match**, the association of the metadata is performed automatically. This default setting can be changed from the registry settings. Note that when the association is performed with name, the names in line with the default languages for vaults are used. Also note that if the metadata structures have been separately created in different vaults, the IDs are not the same and the association must be performed via aliases.
5. You can also use the **name of imported metadata definition as it's alias** if there are no other aliases available. In this case, you need to define the alias only in the target vault using the name of the metadata definition from the source vault. For more information, refer *Use the name of an imported element as its alias if no other alias is available* under *Importing Content* on page 384.
6. If, in addition to those mentioned above, you want to **have associations using the name only**, you can include this definition in the registry settings. Then the name of the metadata definition, such as *Telephone number*, must be the same across vaults. When default settings are used, the name alone is not sufficient for

association of the metadata. Note that when the association is performed by means of name, the names in line with the default languages for the vaults are used.

Aliases for Associating Metadata Between Vaults

Because only the built-in metadata definitions and those matching the GUID or ID and name are associated automatically, for other metadata definitions the association must be performed by using aliases.

Aliases can be used for identifying semantically equivalent metadata. For example, when importing objects from another vault, their *Date* and *Description* properties can be mapped to the target vault's equivalent properties on the basis of aliases even if the properties' internal IDs and/or names are different. That is, the aliases refer to semantically equivalent metadata in different vaults. In other words, **alias is a common identifier for the same metadata definition between several vaults**.

The alias is defined as a common ID with the same name in both source and target vault.

When defining the alias, you can use various external data type and archive standards, such as SÄHKE2, MoReq2, and Dublin Core.

Check that there are sufficient definitions for all desired metadata definitions so that the association can be performed. Check the following: object types, value lists, property definitions, classes and class groups, workflows and workflow states, user groups, and named access control lists. In the properties of these metadata definitions, you can find the *Advanced* tab, where you can define the alias(es) for the metadata definitions.

For example, the source vault has the property definition *Telephone number*, whose vault-specific ID is *1001*. The semantically equivalent property definition is also in the target vault, but the vault-specific ID is *1005* – the name can be the same *("Telephone number")* or different (for example, *"Phone" or "Phone number")*, in the default language. If you want to associate these, you must define a common alias for this property definition in both vaults. The alias can be anything, such as *Telephone number* or *dc.PhoneNumber*, as long as it is the same in both vaults.

The alias is not shown to the users in M-Files Desktop; that is, the users see the name of the vault-specific property definition, just as before.

> 📝 **Note:** If there are several metadata definitions with the same alias in the target vault, the association is bypassed for these and the data will not be imported to the target vault.

Assigning Aliases for Metadata Definitions

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand the **Metadata Structure (Flat View)** node and select the type of metadata definition, for example **Property Definitions**, for which you want to assign an alias or aliases.

   ✅ The list of metadata definitions is opened in the right-side panel.

5. From the list, right-click the instance for which you want to assign an alias and select **Properties** from the context menu.

   ✅ The **Properties** dialog for the selected metadata definition is opened.

6. Go to the **Advanced** tab.

7. In the **Aliases** field, type in the name of the alias for the selected metadata definition.

   ℹ️ Use the same aliases for semantically equivalent metadata in both the source and the target vault.

8. Click **OK** to close the **Properties** dialog.

The alias is displayed in the **Aliases** column of the metadata definition listing.

Login Accounts

Depending on the purpose of use of the target vault, the users of the target vault may be the same as, or entirely different from, those of the source vault. If you want to grant certain users permissions for both vaults, synchronize the metadata for the *Users* value list, or do both, you should create user accounts with the same name for these users for both vaults. User accounts are not automatically synchronized between vaults.

Related Objects in Separate Vaults

The interaction between several vaults enables creation of relationships between objects across vaults. The objects are not exported from one vault to another; instead, the relationship is created by reference to an object in another vault; that is, a link is created to the original object. The object types of the objects must be associatable, but synchronization of the objects (replication of content) is not required, because the objects are not transferred from one vault to another. For more information, see *Relationships Between Objects in Separate Vaults* on page 114.

Synchronization of Objects and Their Values Between Vaults

This section provides further information on synchronization of objects and their values. We recommend studying this section before defining any synchronization jobs. Synchronization is implemented via *Content Replication and Archiving* on page 375.

Synchronizing Objects

When the metadata structures of vaults have been defined according to your needs and the required metadata definitions can be associated with them, the actual synchronization of objects and values can be performed between vaults. Synchronization of data between vaults is performed with replication of content. For more information, refer to *Content Replication and Archiving* on page 375 and *Replication and Archiving User's Guide*.

> 📄 **Note:** Only the values for which there is a built-in object type are synchronized automatically. For other object types, either the alias or the combination of ID and name must match, so that objects of this object type are imported to the target vault during import. You should check that these definitions are in proper order. For more information, see *Associating the Metadata Definitions* on page 203.

Conflicts and their resolution

If objects are edited at the same time in multiple vaults, conflicts may result during synchronization of data, for example, from source vault A to target vault B. When detecting a conflict, M-Files creates a so-called conflict object, from which the conflict can be resolved in favor of either the source or the target vault.

You can find these conflict objects through relations: if the object has conflicts, you can find them under the *Conflicts* grouping title. You can also find all conflict objects by means of the *Conflicts* view (hidden by default).

Resolve conflicts by keeping the changes in the target vault (*Keep These Changes*) or discarding them (*Discard These Changes*), as appropriate. The latter chooses the version in the source vault. When resolving the conflict, you must have editing rights to the actual object and the conflict object in the same vault.

If two-way synchronization (replication of contents) is performed, you must resolve the conflict in both vaults in order to rectify the conflict situation.

Publishing selected objects of one vault in another vault

If you want to publish only certain objects from a vault by using another vault, you can do this by using a search filter when defining the content export. You should also check that the object types of the published objects can be associated either automatically or based on aliases.

Synchronizing Metadata Values

Value-list values

When the metadata structures of vaults have been defined according to your needs and the required metadata definitions can be associated, the actual synchronization of objects and their values can be performed between vaults. Data synchronization between different vaults is performed with replication of contents.

However, you should note that if the value does not exist in the target vault or you cannot create it as a normal value-list value during import (for example, in the case of built-in values, such as classes, workflows, and users), the value name is displayed in metadata in the form "Value name XYZ *(deleted)*". In other words, if the value does not exist in the metadata structure of the target vault after import, it is shown as a "Value name XYZ *(deleted)*" value.

> 📝 **Note:** The default permissions for the imported values are the target vault's default permissions for new values set from value lists. This means that the name of the value may be shown regardless of its permissions in the source vault. For example, the name of the document creator is shown in the metadata of the published document via the "*Created by:* User XYZ *(deleted)*" value. If necessary, check the permissions and association of the metadata definitions if you do not want to display this information in the other vault.

Related objects

The object metadata contains information on other, related objects. For example, a document might be related to a project or a customer.

When objects are exported to another vault, you may not want to export their related objects to the target vault. For example, you export documents to the target vault but not projects or customers (for instance, in publishing operations, you publish price lists and brochures but not customer information). Then the related object is shown as a shortcut in the object's metadata (or, less frequently, with the "Value name XYZ *(deleted)*" value). The object refers to the source vault and has not been imported as a genuine object to the target vault. For further information, refer to *Relationships between objects in separate vaults* under *Relationships* on page 113.

> 📝 **Note:** The default permissions for the related object are the target vault's default permissions for new objects set in the import by object type. This means that the name of the related object is shown in the metadata of the imported/published object regardless of its permissions in the source vault. For example, the name of the customer or project may be shown in metadata of the published document as a shortcut or as a "Value name XYZ *(deleted)*" value. If necessary, check the permissions and association of the metadata definitions if you do not want to display this information in the other vault.

8.5. Cached Replica Vaults

Document vaults can be replicated from the main server to geographically separate *replica servers*. Opening objects from replica servers often makes it quicker to open documents for editing, because the connection to the main server may be slow. Therefore, replication makes accessing frequently used documents on client computers in geographically separate facilities much faster.

Cached replica vaults need a connection to the main server, but full replication can be used even if the connection to the main server is cut off. For more information on implementation of full replication, refer to *Interaction Among Several Vaults* on page 202.

The document vault is replicated from the main server to the replica server. The document vault on the replica server is called a *cached replica vault*.

> 📝 **Note:** The files on the cached replica server are not encrypted.

In M-Files Desktop Settings, the connection to the cached replica vault is created in the same way as any other document vault connection. The M-Files Desktop user only sees the name of the cached replica vault. In other words, the user does not know whether the vault is replicated or not.

▶ Video: *Cached Replica Vaults*

Creating a Cached Replica Vault

- Make sure you have administrator rights on the computer that servers as the replica server.
- Install M-Files Server and M-Files Admin with the same minor release level as the main server (for instance, 11.1.x and 11.1.x).
- Make sure you have a user ID with access to the document vault on the main server.

  📝 **Note:** Administrator rights are only required for accessing the replica server. The main server does not require administrator rights at any stage of specifying the replication.

For more information about administrator rights, see *Server roles: System administrator* on page 211.

1. Open M-Files Admin on the computer that serves as a replica server.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Still in the left-side tree view, highlight **Cached Replica Vaults** and then click **New Cached Replica Vault...** on the right pane.

   ☑ The **Cached Replica Vault Properties** dialog is opened.

4. In the **Server name** field, enter the network name or IP address of the server on which M-Files Server has been installed and that contains the document vault.

5. In the **Port number** field, enter the port to connect to the server. M-Files uses the port 2266 by default.

6. Using the **Protocol** drop-down menu, select the protocol to be used for the network connection. You can select between TCP/IP, SPX, or HTTPS.

7. Using the **Document vault** drop-down menu, select the document vault to be replicated.

   ✅ The **Name** field is updated with the name of the source vault and the **Unique ID** field is updated with the unique ID of the source vault. The **Unique ID** value is used as storage identification of the cached replica vault. M-Files Server uses the IDs to tell document vaults apart, which prevents, for instance, the same vault being replicated twice to the same server.

8. Optional: Click **Test Connection to Document Vault** to check whether you can successfully connect to the document vault. If the connection test is successful, proceed to the next step. If the test fails, check the connection properties and try again.

9. Optional: Using the **Name** field, you can change the name of the cached replica vault. By default, the cached replica vault has the same name as the source vault.

   ⓘ If the name of the source vault is changed, you can click **Update** to update the name of the cached replica vault with the updated name of the source vault.

10. Click the **...** button next to the **Cache location on server** field to specify the directory where the replica vault is stored on the server.

   ✅ The **Location for cached file data** field is updated with the path to the replicated files in the cache directory.

11. Optional: Click **Set Account...** to select the login account used to connect to the server cache.

   ⓘ M-Files Server uses the specified account to store information in the server cache or open files from it. The account must be specified when the server cache is on, for example, a file server requiring authentication for connection.

12. Click **OK** to finish creating the cached replica vaults.

The cached replica vault that you have just created is added to the **Cached Replica Vaults** list and it now acts as a cached replica vault of the specified source document vault.

8.6. Login Accounts

The document vault has users who must first authenticate themselves to M-Files Server. Before creating the users, you must create *login accounts on M-Files Server*. These login accounts are added to document vaults as *users*. Different users can be selected for document vaults from among the login accounts.

▶ Video: *Vault Users and Login Accounts*

New Login Account

You can start creating a new login account by right-clicking on the *Login Accounts* in the left-side tree view of M-Files Admin and by selecting *New Login Account...*

Figure 76: The new login account creation dialog.

Windows authentication

Windows authentication can be used for authentication on M-Files Server, in which case the user logs in to the document vault with the same login information used to log in to Windows or the organization's domain.

Using the domain logins is the quickest and easiest authentication method. This means that new passwords and logins are not needed, which makes this a rather user-friendly method. For more information, refer to table *Differences between the various user authentication methods* on page 35.

> 📄 **Note:** In case your organization is using federated identity management, refer to *Using Federated Authentication with M-Files*.

M-Files authentication

The M-Files authentication method allows the user to log in to M-Files only. If the organization does not have a Windows domain or the user is not to have access to it, it is a good idea to use M-Files authentication for the document vault.

Personal information

Enter an e-mail address and a full name for the login account. This information is used for sending notifications. For more information about notifications, refer to *Notification Settings (M-Files Admin)* on page 181. If the authentication method used is Windows authentication, you can retrieve the personal information from the domain by clicking **Update Information from Domain**.

License type

Select a license type for the login account. The different license types are listed below. For more information about licenses, refer to *License Management* on page 179.

Named user license

Named user licenses are assigned to individual login accounts. This license allows the login account to use M-Files any time, independent of other users.

Concurrent user license

When a login account entitled to a concurrent user license logs in, one license of this type is taken up. When the login account logs out, the license becomes available for use by other login accounts that use this same license type.

Read-only license

Read-only licenses are assigned to individual login accounts. This license allows the login account to use M-Files at any time, independent of other users. The license is limited in the sense that not all M-Files features are available for use: the user is only able to read but not to create or modify documents.

External Connector license

External Connector licenses enable 3rd party systems to anonymously read M-Files database. The license type is needed for example when M-Files data is published programmatically in an intranet or extranet environment to an unrestricted number of users.

Account is disabled

This function provides an easy way to specify whether the user is allowed to log in to the server or not. This function is useful if you do not want to remove the login account altogether, but to disable it for the time being.

Server roles: System administrator

This role entitles the user to make any changes on the server level. These include *changing the server logins* and *creating* and *deleting document vaults*. In other words, a system administrator can perform any operation on a document vault.

See the table below for a comparison between the permissions of a system administrator and a vault administrator with a full control of a vault:

Operation	System administrator	Vault administrator
Create a vault	Allowed	Not allowed
Attach a vault	Allowed	Not allowed
Restore a vault	Allowed	Not allowed
Detach a vault	Allowed	Not allowed
Back up a vault	Allowed	Not allowed
Copy a vault	Allowed	Not allowed
Destroy a vault	Allowed	Not allowed
Optimize the database	Allowed	Not allowed
Back up the master database	Allowed	Not allowed

Operation	System administrator	Vault administrator
Restore the master database	Allowed	Not allowed
Take a vault offline	Allowed	Not allowed
Rebuild the full-text search index	Allowed	Allowed
Reset thumbnail images in a vault	Allowed	Allowed
Verify and repair a vault	Allowed	Not allowed
Migrate to Microsoft SQL Server	Allowed	Not allowed
Create a cached replicate vault	Allowed	Not allowed
Create or import a login account	Allowed	Not allowed
Create a scheduled job	Allowed	Not allowed
Change M-Files Server notification settings	Allowed	Not allowed
Manage M-Files licenses	Allowed	Not allowed
Configure web and mobile access	Allowed	Not allowed
Shut down M-Files Server	Allowed	Not allowed
Log in to any vault	Allowed	Not allowed
Create and import users	Allowed	Not allowed
Import user groups	Allowed	Not allowed
Create user groups	Allowed	Allowed
See and read all vault content (including deleted objects)	Allowed	Allowed
See and undelete deleted objects	Allowed	Allowed
Destroy objects	Allowed	Allowed
Force undo checkout	Allowed	Allowed
Change permissions for all objects	Allowed	Allowed
Change metadata structure	Allowed	Allowed
Manage workflows	Allowed	Allowed
Manage user accounts	Allowed	Allowed
Manage common views and notification rules	Allowed	Allowed

Creating a Login Account

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Highlight **Login Accounts** in the left-side tree view.

4. Click **New Login Account...** on the task area.

   ✓ The **New Login Account** dialog is opened.

5. Enter a username.

6. Select an authentication method by clicking the appropriate radio button and enter authentication details in the fields below the selected authentication method.

7. Enter an email address and a full name in the personal information fields.

   ⓘ If you are using Windows authentication, you can click **Update Information from Domain** to retrieve personal information from the domain's directory service.

8. Select a license from the **License type** drop-down menu to set an appropriate license for the login account.

9. Optional: Check the **Login account is disabled** check box if you want to disable the login account for the time being.

10. Optional: Check the **System administrator** check box if you want to assign a system administrator role for the login account. This role entitles the user to make any changes on the server level, including *changing the server logins* and *creating and deleting document vaults*.

11. Click **OK** once you are done.

You should now have a new login account and it should appear in the **Login Accounts** list when you highlight **Login Accounts** in the left-side tree view in M-Files Admin.

Importing Login Accounts

Do the following steps to import login accounts to M-Files Server:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Highlight **Login Accounts** in the left-side tree view.

4. Click **Import Login Accounts...** on the task area.

   ✓ The **Import Login Accounts** dialog is opened.

5. Using the **Domain** drop-down menu, select the domain from which you wish to import login accounts.

6. Using the **Organizational unit** drop-down menu, select the organizational unit within the domain from which you wish to import login accounts.

7. Using the **User group** drop-down menu, select the user group within the organizational unit from which you wish to import login accounts.

   ✓ The members of the selected user group are listed in the **Select the users to import** list box.

8. Optional: Check the **Include users from nested groups** option check box to be able to import login accounts from nested groups within the selected user group.

9. Select the login account or login accounts by clicking a login account on the **Select the users to import** list box.

> ⓘ You can select more than one item at once by holding down the Ctrl key to select multiple individual items or by holding down the ⇧ Shift key to select adjacent items on the list.

10.Using the **License type for new login accounts** drop-down menu, select the license type for the login accounts to be imported.

> ⓘ For more information about license types, see *License types* on page 181.

11.Click **OK** to import the selected login accounts.

The selected login accounts are imported to M-Files Server and should now appear in the **Login Accounts** list when you highlight **Login Accounts** in the left-side tree view in M-Files Admin.

Changing the User Login Account

Sometimes it may be necessary to change the *login account* on page 209 for a user. The user's login account may have to be changed when, for example, the user needs a new login account due to his or her last name being changed or when login accounts are moved from one domain to another.

When a user login account must be changed, it is important to preserve the *vault user* on page 251 associated with the original login account and to associate the same user with the new login account in order to preserve the user history and the user's personal settings in the vault.

> 📝 **Note:** It is important to distinguish between *login accounts* on page 209 and *users* on page 251:
>
> - Login accounts are server-level (or in some cases vault-level) accounts that are used for authenticating users to M-Files Server. A login account can be associated with multiple users, but only one user per vault.
> - Users are vault-level objects that store user-specific settings and user history and that have permissions to perform specific operations in a vault. A user is linked to one and only one login account.

Do the following steps to correctly change a login account for a user *after new login accounts have been created in M-Files*:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select **Users**.

   > ☑ The **Users** list is opened in the right-side pane.

5. Right-click the user whose login account you need to change and select **Properties** from the context menu.

   > ⓘ If new login accounts are synchronized from an Active Directory source, M-Files automatically creates new users for the new login accounts. In order to associate the new login account with the correct existing user, you must first delete the new, automatically created user.

   > ☑ The **User Properties** dialog is opened.

6. Use the **Login account** drop-down menu to select a new login account for the user.

7. Click **OK** to close the **User Properties** dialog and to save your changes.

The new login account is now correctly associated with the existing user. Now when the user logs in using the new credentials, his or her previous user history and personal settings in the vault are available.

Show Logged-in Users

You can server-specifically view the currently logged-in users and their license types.

Do the following steps to view the users who are currently logged in to the server:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Highlight **Login Accounts** in the left-side tree view.

4. Click **Show Logged-in Users** on the task area.

   ✓

The **Logged-in Users** dialog is opened, showing the users who are currently logged in. You can click **Refresh** to update the view.

If necessary, you can also force certain users to log out by selecting the user and clicking **Force Logout**. This might be very useful, for instance, when concurrent licenses are used: The operation enables you to force the logout of idle users in order to release the license to be used by someone who actually needs it at the moment. Forcing active users to log out, however, normally does not affect them at all. Active users immediately get a license if available licenses exist.

   Note: Displaying the logged-in users and forcing their logout requires you to have administrator rights.

8.7. Scheduled Jobs

Backups can be made automatic with *Scheduled Jobs*, which you can find at the bottom of the left-side tree structure in M-Files Admin. Backups are saved on the hard drive or a network drive, from which they can be transferred to, for instance, a tape drive. If necessary, backups can be restored with M-Files Admin (see *Restore Document Vault* on page 201).

The jobs also include other scheduled tasks, such as the database optimization. The operation performs, for example, database search index maintenance ensuring that document vault access remains fast regardless of the amount of changes made to the data.

New Scheduled Job

To start defining a new scheduled backup job:

1. Select *Scheduled Jobs* from the left-side tree structure in M-Files Admin.
2. Select *New Scheduled Backup Job...* via the task area.
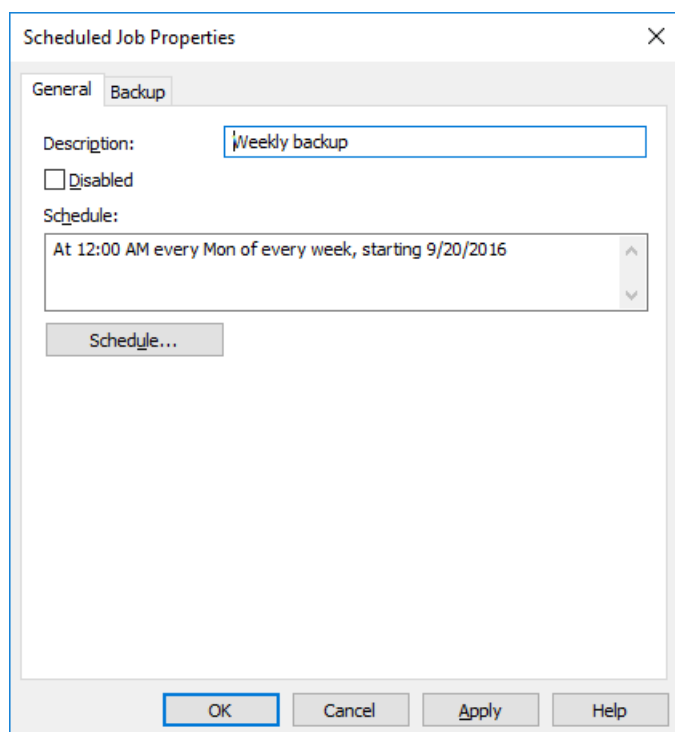
Figure 77: The "Scheduled Job Properties" dialog.

Scheduling a backup job is quite similar to defining a scheduled task in the Windows Control Panel. The **Schedule...** button opens a dialog for defining the job schedule. The *Schedule* text field can be used for a free-form textual description.

If you opened this page via a *New Scheduled Export/Import* dialog, you might be looking for *Content Replication and Archiving* on page 375.

Scheduled Backup Jobs

The *Backup* tab of the *Scheduled Job Properties* window enables you to define what needs to be backed up and to which location. You can also specify whether to divide the backup into multiple files and whether to overwrite existing backup files.

For step-by-step instructions on how to create a vault backup, see *Backing Up a Document Vault* on page 224.

▶ Video: *Backups*
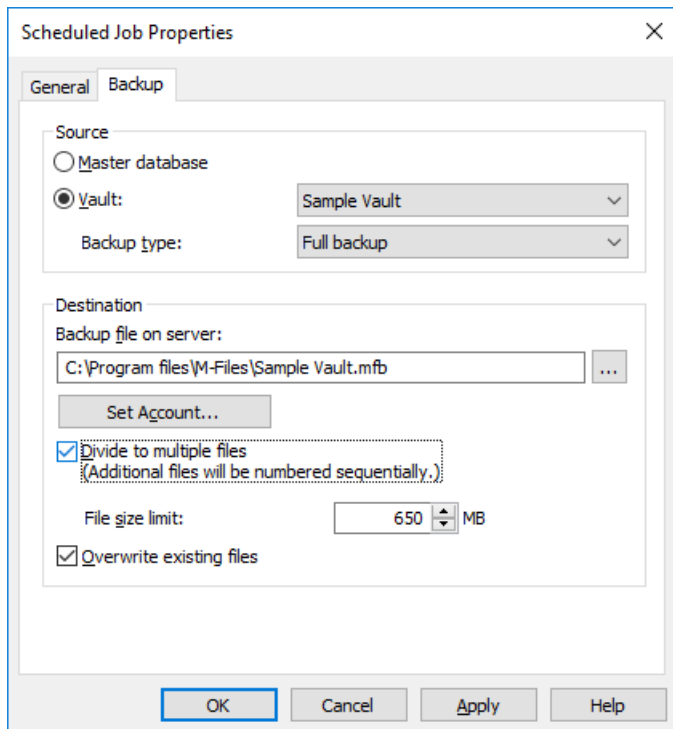
Figure 78: The "Backup" tab of the "Scheduled Job Properties" dialog.

Backup types

Two kinds of backups can be made of document vaults: *full backups* and *differential backups*. Only full backups can be made of the master database.

A full backup is the most complete copy that can be produced with M-Files. It contains, for example, the *history information* of all documents. You cannot make a differential backup if you have not made a full backup first.

To save disk space, full backups should be scheduled to occur less frequently, for instance once a week, and differential backups for example once a day. Be sure to specify backups separately for both the *document vault* and the *master database*.

The differential backup contains all data that has been changed after the last full backup. When restoring a differential backup, you will need the full backup and the files from the last differential backup.

Also refer to *M-Files Server* on page 179.

8.8. Server Activity Monitor

M-Files Admin contains a tool called Server Activity Monitor for observing the various events taking place on your M-Files Server computer. The tool enables you to easily identify possible issues related to operations taking place on the server.

> 📄 **Note:** The activity monitor records a limited number of events. This means that once the record is full, every time a new event is recorded, the oldest event is removed from the list.

This topic describes the various views included in the monitoring tool, but let's first see how to access Server Activity Monitor in M-Files Admin.

To open the server monitoring tool:

1. Open M-Files Admin.
2. Expand the server connection node.

3. Select **Server Activity Monitor**.

As a result, you should see the activity monitor on the right side window of M-Files Admin.

> 📄 **Note:** The views are not updated in real time. You can use the **Refresh** and **Reset** commands on the task pane to update and clear the views. The activity monitor is always on, so you do not need to separately activate it.
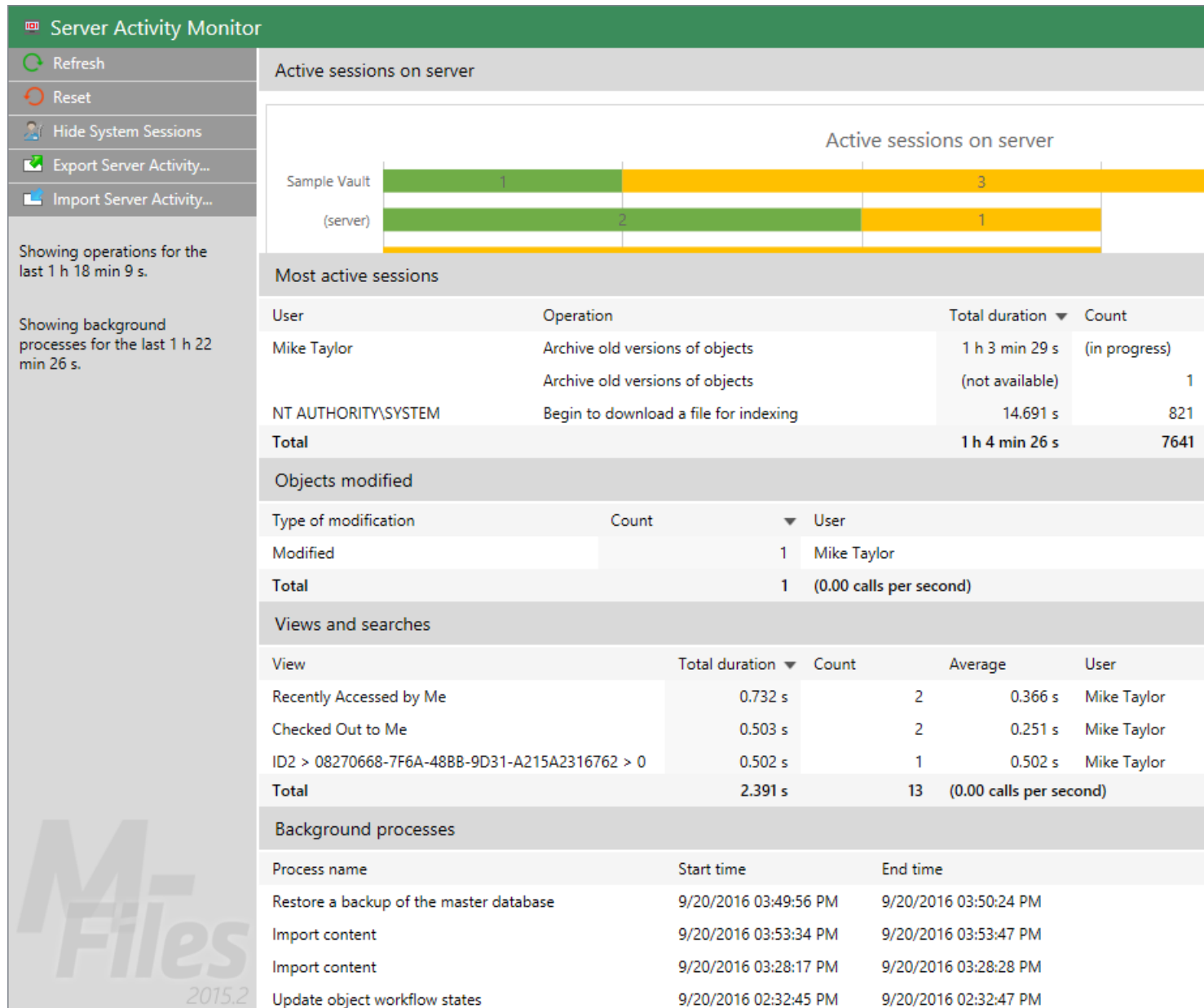
Figure 79: Server Activity Monitor in M-Files Admin.

> 📄 **Tip:** You can sort the information by any numerical column in any of the views by clicking the column heading of you choice.

> 📄 **Tip:** You can easily copy any of the server activity listings shown by selecting and copying a listing and pasting the selection into, say, Microsoft Excel or Microsoft Word. If you paste the selection into a Microsoft Excel worksheet, the copied listing is separated into multiple cells, preserving the original row and column format.

Task pane commands

The commands on the task pane allow you to perform various operations in Server Activity Monitor:

- **Refresh** updates the server activity data with up-to-date information.
- **Reset** removes all the existing server activity data and restarts the monitoring.
- **Show System Sessions** / **Hide System Sessions** shows or hides active system sessions and operations. If system sessions are hidden, only user activity is shown.
- **Export Server Activity...** allows you to export the current server activity data to a JSON file.
- **Import Server Activity...** allows you to import and view server activity data previously exported to a JSON file.

Active sessions on server

This view lists all the active user and system sessions by vault connection. If the connection is listed as *(server)*, the connection is not to any of the vaults, but to the server itself.

Most active sessions

This view lists the total number (**Count**) and duration of operations (**Total duration**) by user, the description of the operation (**Operation**), the average duration per operation (**Average**), and the vault connection (**Vault**).

The **Total** row shows the total duration and number of operations for the entire period server activity has been monitored, and the number of operation calls made per second during the monitoring period.

> **Note:** This view lists only thirty operations at a time, whereas the **Total** row displays the total number and duration of operations for the entire period of time server activity has been monitored. Therefore the calculated total number and duration of the operations visible in the view may not be equal to the figures shown in the **Total** row.

Objects modified

This view displays the number of object modifications by user and vault.

The types of modification listed in this view are:

- object creation
- object modification
- object deletion

The **Total** row shows the total number of object modifications for the monitoring period and the average number of object modifications made per second.

> **Note:** This view lists only thirty operations at a time, whereas the **Total** row displays the total number of operations for the entire period of time server activity has been monitored. Therefore the calculated total number of the operations visible in the view may not be equal to the figures shown in the **Total** row.

Views and searches

This section lists the views accessed and searches initiated by the user. It displays the total duration, the number of uses, and the average duration per use of a single view (such as *Recently Accessed by Me*) or a search. Each row displays the user who accessed the view or performed the search, as well as the vault in which the operation was performed.

The **Total** row shows the total duration it has taken to open views and perform searches during the monitoring period. It also displays the total number of searches performed and views opened, and the average number of such operations made per second.

📋 **Note:** This view lists only thirty operations at a time, whereas the **Total** row displays the total number and duration of operations for the entire period of time server activity has been monitored. Therefore the calculated total number and duration of the operations visible in the view may not be equal to the figures shown in the **Total** row.

Background processes

The *Background processes* view lists activities automatically executed by M-Files Server, such as scheduled maintenance tasks and processing of automatic state transitions. In addition to the name of the process, the view displays the affected vault, as well as the duration, the last start time, and – for periodic events – the next start time of the process.

8.9. Applications (M-Files Admin)

You can manage vault-specific client and server applications via M-Files Admin. These applications allow you to modify and extend the behavior of your M-Files Desktop and M-Files Server. This way you can choose to give priority to the functions that are the most important for the efficiency of your organization.

The application can either be a *client application* or a *server application*:

• Client applications run in M-Files client computers and can affect the behavior of M-Files Desktop.
• Server applications run on the M-Files server computer, and can affect M-Files server behavior.

📋 **Note:** Creating applications requires advanced programming skills. Instructions for the programming are available from the M-Files technical staff for a separate fee. For more documentation and sample applications, see the guide to *M-Files UI Extensibility Framework*.

Do the following steps to manage the applications of the selected document vault:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Still in the left-side tree view, right-click the desired document vault and select **Applications** from the context menu.

☑ The **Applications** dialog is opened.

```
Applications                                                              ×

Name              Version      Description                    License     Publ
  🖥 Home Screen        1.0          The M-Files Desktop home view.    -          M-Fi
  🖥 M-Files QMS UI      2.0.127.0    User Interface for M-Files QMS    -          M-Fi
  🖥 SentinelInbox       1.0.11.6     M-Files SentinelInbox             -          M-Fi
  🖥 TaskPaneTemplates   1.0.0.12     M-Files TaskPaneTemplates         -          M-Fi




<                                                                         >

Install...      Uninstall      Export...      Enable      License        Close
```
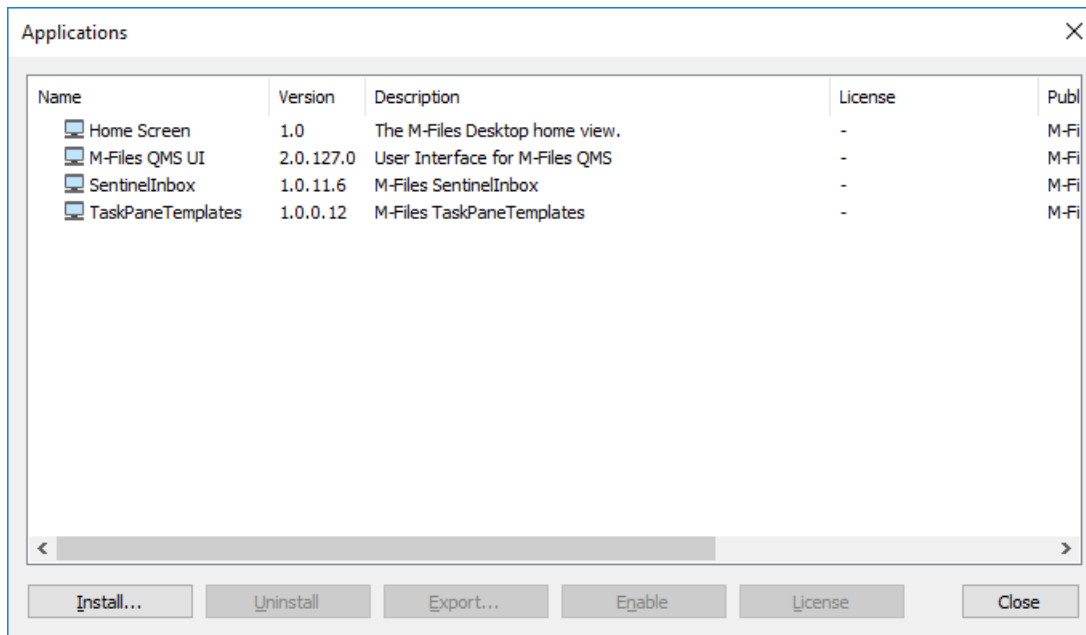
4. Perform one or more of the following operations, as necessary:

If you want to...	Do the following steps:
Install a new application	1. Click the **Install...** button. 2. Browse for the application package and click **Open**. 3. Click **Yes** to restart the document vault.
Uninstall an application	1. Select the application that you want to uninstall in the applications listing. 2. Click **Uninstall**. 3. Click **Yes** to confirm uninstalling the application. 4. Click **Yes** to restart the document vault.
Export an application	1. Select the application that you want to export in the applications listing. 2. Click the **Export...** button. 3. Select the location and the file name for the export package and click **Save**.
Disable an application and uninstall it from all users	1. Select the application that you want to disable in the applications listing. 2. Click **Disable**. 3. Click **Yes** to confirm uninstalling the application. 4. Click **Yes** to restart the document vault.
Enable a disabled application	1. Select the disabled application in the application listing. 2. Click **Enable**. 3. Click **Yes** to restart the document vault.
See the license status, or install or change the license of an application	1. Select the desired application in the applications listing.

If you want to...	Do the following steps:
	2. Click the **License** button to open the **Application License Management** dialog and to view the license status and information of the selected application.
	3. If necessary, click the **Install License...** button, browse for the license file, and then click **Open**.

5. Click **Close** once you are done.

The changes you have made to the selected document vault should now be effective.

For information on enabling the applications in M-Files Desktop, see *Applications (M-Files Desktop)* on page 136.

8.10. Electronic Signing and Compliance

Companies using M-Files can manage their documents and processes efficiently and with quality. M-Files can be used for compliance with various specifications, good manufacturing practices, general procedures, and documentation according to standards. Moreover, M-Files provides functions to manage and monitor general documents associated with daily business.

M-Files also meets the special requirements related to records and following various specifications and standards. For example, M-Files complies with the following standards and guidelines: the ISO 9001 series, FDA 21 CFR Part 11, EU GMP Annex 11, HIPAA, and Sarbanes-Oxley. M-Files can also be used to implement TLL-4-compliant data systems (TLL-4 is a data security classification used in public administration and defense forces).

M-Files supports the administration of electronic records and signatures in compliance with FDA 21 CFR Part 11. This involves maintenance of the detailed audit trail of actions performed on the documents, secure monitoring of individual actions, and certification of electronic signatures with usernames.

Activation

The Electronic Signatures module includes the event logging extensions mentioned above and electronic signature functionality. The module is available for a separate fee.

For you to activate the module, an appropriate license code must be activated on your system. The license is provided on a subscription basis. Activate or update the license code in M-Files Admin (for more information, refer to *License Management* on page 179). In addition to this, vault-specific properties of the audit trail must be activated (see *Document Vault Advanced Properties* on page 197). Electronic signatures are automatically enabled with the license code.

More information

For more information on the Electronic Signatures module related extensions for event logging and electronic signatures, refer to *Event Log* on page 364 and *Electronic Signature* on page 329.

M-Files can also be used to address other standards, quality management systems, compliance requirements, guidelines, and procedures and processes in different fields. Log entries, audit trails, version history, and electronic signatures form one set of functions that M-Files can offer. To find out how M-Files can support your business by complying with applicable standards and specifications, please contact us at *sales@m-files.com*.

9. Document Vault Administration

This chapter describes all the available operations and settings available for a single document vault via M-Files Admin.

Note: It is also possible to distribute vault settings via M-Files Server, so that the settings are read from the server when a user logs in and written to the Windows registry of the client computer. For more information, refer to *Distributing Vault-Specific Registry Settings from M-Files Server*.
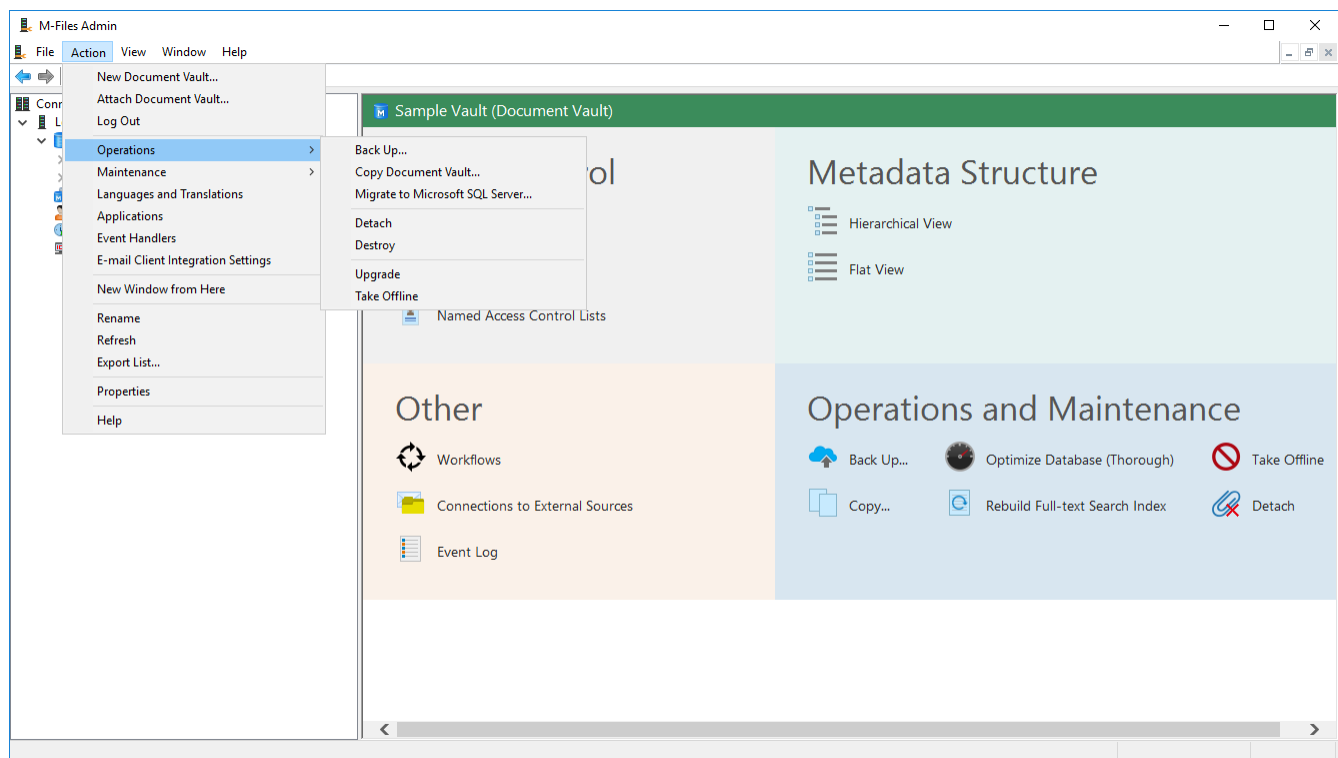
Figure 80: Document vault operations.

9.1. Document Vault Action Menu

There are a number of actions related to document vault management that you can find by highlighting a vault and opening the *Action* menu in M-Files Admin. This chapter offers a description of those actions as well as information on translating M-Files and using the software in a variety of languages.

Creating and Attaching a Document Vault

For information on creating and attaching document vaults, and on document vault properties, refer to *Document Vault Overview* on page 195.

Log Out, Log In

You can use the *Action* > *Log Out* function to log out from the document vault on the server level. When you have logged out from the document vault, the name of this function will change to *Log In*, and you can use it to log in to the document vault on the server level.

Vault Operations

This chapter introduces the various vault actions under the *Operations* menu.

Backing Up a Document Vault

The vault backup function can be used for backing up the document vault or for scheduling a recurring vault backup job. For more information about scheduled backups, refer to *Scheduled Backup Jobs* on page 216.
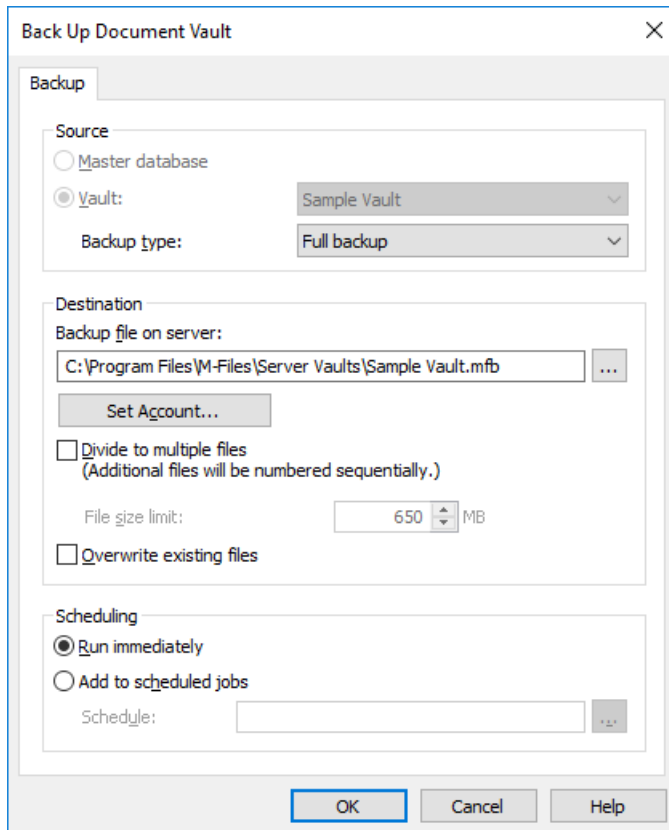
1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, select a vault of your choice.

4. Right-click the vault and select **Operations** > **Back Up...** from the context menu.

☑ The **Back Up Document Vault** dialog is opened.

5. Using the **Backup type** drop-down menu, select either *Full backup* or *Differential backup*.

ℹ A full backup is the most complete copy that can be produced with M-Files. It contains, for example, the history information of all documents. You cannot make a differential backup if you have not made a full backup first. A differential backup contains all data that has been changed after the last full backup.

6. Click the **...** button to select the destination of the M-Files backup file (MFB).

7. Optional: Use the **Set Account...** button to define a separate user account to have access rights to the backup file.

8. Optional: Check the **Divide to multiple files** option check box and set the file size limit if you want to divide the vault backup into multiple files.

ℹ The names of the backup files should not be modified as they might no longer be recognized during a backup operation later on.

9. Optional: Check the **Overwrite existing files** option check box if you want your new backup files to replace any existing files with the same file name.

10. Select either:

    a. **Run immediately** to start the backup job right away.

        or

    b. **Add to scheduled jobs** and click the **...** button to schedule the backup job as a recurring task.

        📝 **Note:** For more information about scheduled jobs, see *Scheduled Jobs* on page 215.

11. Click **OK** to either start the backup process or to add the scheduled task to the list of *scheduled jobs* on page 215.

The vault backup should now be run or added to the list of *scheduled jobs* on page 215, depending on your choice under the **Scheduling** header of the dialog.

Copying a Document Vault

You can use the **Copy Document Vault** operation to create a copy of a document vault. You can copy a document vault in its entirety or select specific data components to be included in the copy.

For example, if you have found the structure of an old document vault useful and want to copy it to a new vault without the actual content, you can easily do this by copying the vault structure only. This way you can utilize, for instance, the sample vault included in the M-Files installation.

Complete the following steps to copy a document vault:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, select the document vault of your choice.

4. Right-click the vault and select **Operations** > **Copy Document Vault...** from the menu bar.

    ☑ The **Copy Document Vault** dialog is opened.

5. In the **Name** field, enter a name for the copy of the document vault.

6. Click **Define...** to define the the vault data location on the server to which you want to copy the document vault.

    ✓ The **Document Vault** dialog is opened.

7. Click the **...** button to browse for the vault data location.

8. Optional: If you need to define a separate location for file data, do the following steps:

a) Click **Advanced**.

☑ The **Advanced** dialog is opened.

b) Check the **Separate location for file data** option check box.
c) Click the **...** button to browse for the separate location for file data.
d) Click **Set Account for File Data...** if you need to define a separate account for copying file data.
e) Click **OK** to close the **Advanced** dialog.

9. Once you have defined the location for the document vault copy, click **OK** to close the **Document Vault** dialog.

10. In the **Data to copy** section, select the vault data components that you want to copy.

ⓘ You can click **All** to select all components or **Structure Only** to select only the structure components of the vault.

ⓘ If the **Documents and other objects** option check box is checked, for troubleshooting purposes you may exclude file data from the vault copy by clicking **Advanced...** and checking the **Exclude file data from the vault copy** option check box.

11. Click **OK** to copy the vault.

The selected components of the document vault are copied to the location that you have defined.

Migrate to Microsoft SQL Server

M-Files uses Firebird as the default vault database engine. It is recommended, however, to use Microsoft SQL Server as the database engine for vaults that contain several hundreds of thousands of objects. If a vault has originally been set up to use Firebird but the number of objects in the vault has significantly increased, it might be beneficial to have the vault use Microsoft SQL Server as the database engine instead. You can migrate your vault database from Firebird to Microsoft SQL Server via M-Files Admin.

📝 **Note:** You can only migrate the document vault database engine from Firebird to Microsoft SQL Server. Migrating from Microsoft SQL Server to Firebird is not supported.

- Your vault must currently use Firebird as the database engine.
- You need to have a Microsoft SQL Server connection.

To migrate your vault database from Firebird to Microsoft SQL Server:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Still in the left-side tree view, right-click the vault of your choice and select **Operations** > **Migrate to Microsoft SQL Server...**

☑ The **Document Vault - Microsoft SQL Server** dialog is opened.

4. To the **Server name** field, insert the connection address to your Microsoft SQL Server, such as `mysqlserver.mydomain.local`.

5. To the **Database name** field, insert the name of the database to be created for the vault.

   ⓘ It is recommended to use the same name as the vault has on M-Files Server.

6. Fill in the credentials (the **Administrator credentials** and **Basic user credentials** sections) in one of the two following ways:

Option	Steps
Enter the credentials for a login that has the *sysadmin* server role on your Microsoft SQL Server, giving M-Files Server the rights to make the necessary migration-related operations.	1. To the **Administrator credentials** section, insert the credentials for a login that has the *sysadmin* server role on your Microsoft SQL Server. 2. For the **Basic user credentials** section, select the **Use an automatically generated login** option.
Manually create the Microsoft SQL Server database and logins (without the *sysadmin* server role) and use the non-*sysadmin* credentials for M-Files Server.	1. By using Microsoft SQL Server Management Studio, create an empty database for the vault. 2. Still in Microsoft SQL Server Management Studio, create two logins without the *sysadmin* server role, for example `User A` and `User B`. 3. Back in M-Files Admin and the **Document Vault - Microsoft SQL Server** dialog, enter the credentials for `User A` to the **Administrator credentials** section.

Option	Steps
	4. For the **Basic user credentials** section, first select the **Use an existing login** option and then enter the credentials for User B.

ℹ The easiest way is to select the first option, and to let M-Files Server make all the necessary changes on your Microsoft SQL Server. In some cases, however, system administrators may need to withhold Microsoft SQL Server *sysadmin* credentials from M-Files Server. In these cases, the vault database and the Microsoft SQL Server logins need to be created manually (the second option).

M-Files Server uses the basic user credentials for almost all vault operations, and the administrator credentials – in addition to creating the database and the logins – for some of the maintenance operations.

7. Optional: Click **File Data Location...** to specify the location for the file data of your vault.

ℹ In the **File Data Location** dialog, you can select to store the file data in the Microsoft SQL Server database (the first option) or to have it remain in its current file system folder (the second option).

8. Optional: Click **Test Connection** to test the connection to your Microsoft SQL Server.

9. Once you are done, click **OK**.

☑ A warning dialog about the irrevocability of the operation is shown.

10. Click **Yes** to close the warning dialog and to start the migration process.

Once the migration process is complete, the database of your M-Files vault is located on the Microsoft SQL Server that you specified.

Detach

You can detach a document vault from the server connection, in which case the data will not be destroyed but will be kept on the computer's hard drive. The *Detach* and *Attach* document vault functions are the opposites of each other. A document vault that has been *detached* can be *attached* back to the M-Files server from the hard drive. For more information on attaching a document vault, refer to

Destroy

The *Destroy* function can be used to permanently destroy all data from a document vault. The function naturally does not affect backups located on the hard drive. The document vault can thus be restored if backups have been made.

Upgrade

If the internal database structure of the document vault changes, which usually happens during a software upgrade, the document vault must be upgraded. During a software upgrade, this is done automatically for all the vaults that are in the online state. If the vault is offline during a software upgrade, it can only be used after it has been manually upgraded. To do this, open the vault context menu and select **Upgrade**.

📝 **Note:** Upgrading a document vault makes it incompatible with older M-Files Server versions.

Take Offline, Bring Online

When you take a document vault offline, M-Files closes the vault. This also closes any open sessions that users may have. Users cannot log in to a document vault that has been taken offline until the vault has been brought back online with the *Bring Online* function.

Vault Maintenance

The *Maintenance* submenu contains functions for verifying and optimizing the integrity of the internal database structure. Additionally, you can rebuild the full-text search index and reset thumbnail images in the vault. Regular vault maintenance ensures high performance even with vaults containing a large number of objects.

▶ Video: *Vault Maintenance - Optimization*

Optimize Database

The *Optimize Database (Thorough)* operation attempts to improve the performance of the vault database by defragmenting indexes, updating database statistics, and compressing the full-text search index.

M-Files automatically runs the *Optimize Database (Thorough)* operation once a week, so you do not normally need to do this yourself at all. If the vault is, however, responding more slowly than usual, you may want to try running the operation. This may happen, for instance, after a large number of objects has been imported to the vault (for instance if the number of objects in a vault using Firebird as the database engine quickly increases from 0 to 10,000 objects).

The operation can be run in the *Quick* mode first, but we recommend using the *Thorough* mode in most cases.

Update encryption status of existing files

Depending on the state of the setting **Enable encryption for file data at rest** in the *Document Vault Advanced Properties* on page 197, the **Update encryption status of existing files** does one of the following:

- If the **Enable encryption for file data at rest** has been enabled, all the files in the vault previously not ecrypted are now encrypted as well.
- If the **Enable encryption for file data at rest** has been disabled, the encryption of all the encypted files in the vault is removed.

Rebuild Full-text Search Index

This operation completely rebuilds the full-text search index, and may take up an extensive amount of time in large repositories (with hundreds of thousands of objects and hundreds of gigabytes of data).

We recommend running this operation if you think the search index might be corrupted or if the search operations are more sluggish than usual. In large repositories, especially if the objects get modified a lot, we recommend running this operation twice per year.

Reset Thumbnail Images

You can reset the thumbnail image cache for the vault if you are using the thumbnail view in M-Files Desktop and if the images are not working correctly. This might happen, for instance, after installing a software capable of displaying thumbnails that could not previously be shown.

Verify and Repair

This operation can be used for verifying that the database is intact and that all the data has been saved correctly to M-Files. The *Thorough* mode additionally checks whether the file sizes and the file checksums of the physical files in the vault data server location match those reported by the metadata database.

If errors are found, some of them can be repaired automatically by M-Files, but some errors might need additional user actions. If you have errors that cannot be resolved automatically, and that you cannot fix yourself, please contact our customer support at *support@m-files.com*.

We recommend running the *Verify and Repair (Thorough)* operation twice per year.

Maintenance recommendations

Here is a short roundup of the recommended maintenance operations:

- The *Optimize Database* operation does not need to be run regularly. It is automatically taken care of by M-Files.
- The *Rebuild Full-text Search Index* operation should be run twice a year for large repositories (with hundreds of thousands of objects and hundreds of gigabytes of data).
- The *Reset Thumbnail Images* operation only needs to be used if the thumbnail images are not working correctly.
- The *Verify and Repair (Thorough)* operation should be run twice a year for all repositories.

Languages and Translations

The language of the M-Files user interface depends on three factors:

- M-Files software language
- Vault language
- Windows display language

You can switch to using any of the software languages easily via the *language setting* on page 231 as described further below. For intructions on how to translate the vault metadata structure to the language of your choice, see section *Translating the metadata structure* on page 231.

Changing the Windows display language depends on your Windows version. For instance in Windows 8, you can change the display language via **Control Panel** > **Language**.

> 📄 **Note:** M-Files Web has different requirements for a fully localized user experience. See *this note* on page 188 for more information.

Changing the software language

M-Files software can be used in several different languages. Changing the language is easy and the change can also be done during use. You can open the **Change Language** dialog by clicking on the M-Files icon on the Windows notification area and by selecting **Settings** > **Change Language**. M-Files software offers these languages automatically.

If, for example, English is selected as the software language, the following options are displayed in English: **Check Out**, **Check In** and **Workflow**. If Finnish were to be chosen, the same options would be shown in Finnish: **Varaa muokattavaksi**, **Palauta muokkauksesta** and **Työnkulku**.

Additional language versions to those currently supported are available by separate agreement with M-Files.

Translating the metadata structure

The document vault metadata structure can be translated into different languages. The document vault metadata structure refers to the vault's object types, classes, property definitions, value lists, workflows, etc. The document class titles, such as *Proposal*, *Order* and *Contract*, can be translated into the desired languages.

The company can translate the metadata structure independently or have it translated by a third party. Managing the translation material is easy: the administrator can export the translation material in the XML file format. The material can then either be translated in-house or by a professional translation agency. The actual translation process is not dependent on M-Files Admin or its permissions.

Translating the metadata structure can be particularly beneficial for companies with operations in more than one country, or companies with more than one in-house language. This enables users to add documents and other objects using the metadata structure in their own language. The multilingual metadata structure can also be useful if the company uses several languages for other than geographical reasons.

See *Multilingual Metadata Structures* on page 233 for further information on how to create a localized version of the metadata structure of your vault.

Different language for software and metadata structure

Besides the M-Files functions, metadata specific to document vaults can be selected and edited in a user-specified language if the metadata structure has also been translated. If the metadata structure has not been translated into the relevant language(s), for instance, from Finnish to English, it can be difficult for the user to understand why some information is displayed in Finnish and some in English. Only users with administrator rights can view and edit the actual content of the metadata structure.

For example, the class *Proposal*, object type *Customer* and property definition *Document date* belong to the metadata structure. If the user has selected Finnish as the software language but the metadata structure has not been translated into Finnish, the user will see these options in English only because they have been added to the metadata structure and titled in English.

Thus, for instance, when creating a new document, some metadata card information will be displayed in Finnish (*Lisää ominaisuus*, *Avaa muokattavaksi* and *Luo*) and some in English (*Proposal*, *Customer* and *Project*). This is because some of the texts, such as *Luo*, are part of the M-Files software that has been already translated into Finnish but the *Proposal* concept in the metadata structure has not yet been translated.

Figure 81: A metadata card containing Finnish and English.

Multilingual Metadata Structures

The metadata structure is always specific to the document vault and the vault can have a multilingual metadata structure. For example, the following elements of the metadata structure can be translated:

- Names of classes and class groups.
- Names of object types.
- Names and values of value lists (for instance meeting types).
- Names of property definitions.
- Names of user groups and named access control lists.
- Names of workflows and their states.

- Names of views.

   📄 **Note:** Names of documents and other objects cannot be translated.

The default setting for value lists is that the contents of the value list are not translated. If you want to translate the contents of the value list, meaning the actual values, activate *The contents of this value list can be translated* option in the **Advanced** tab of the value list's properties.

Translating the Metadata Structure

Using the **Languages and Translations** dialog, you can export the translatable content of the metadata structure and translate the exported structure in Excel, Word, or a professional translation program, such as SDL Trados or SDL Passolo.

To translate the metadata structure of the vault, follow the steps provided below.

   First, you need to open the **Languages and Translations** dialog.

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. Select the desired vault.

4. Open the **Action** menu and select **Languages and Translations**.

   ✓ The **Languages and Translations** dialog for the selected vault is displayed.
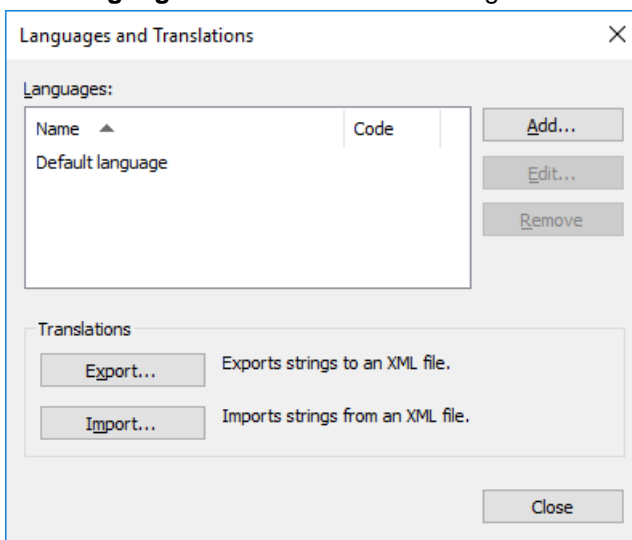
   Next, add your language to the list and export the list of terms to an XML or XLIFF file.

5. Click the **Add...** button.

   ✓ The **Language** dialog is opened.

6. In the **Name** field, enter the language name.

7. Optional: In the **Code** field, enter a code of your choice for the language.

   ✏ This can be, for instance, an ISO 639-1 code.

8. Click **OK** to close the **Language** dialog.

9. Select the newly added language from the list.

10. Click the **Export...** button.

☑ The **Export Strings** dialog is opened.

11. Define the settings for your language export.

ⓘ For more information, see *Adding and Exporting Languages* on page 235.

12. Define the location for your export file and click **Save**.

☑ The export file is saved as an XML or XLIFF file to the location you specified.

Once the export has completed, you can start working on the actual translation.

13. Open the exported file in the software of your choice and add the translations.

ⓘ For instructions on completing the process with Microsoft Excel, see *Translating in Excel* on page 236.

The final step is to import the completed translation back to M-Files.

14. Return to M-Files Admin and repeat the steps from 2 to 4 to open the **Languages and Translations** dialog.

15. Click the **Import...** button.

16. Select the target language and click **Open**.

17. Select whether you want to import all strings or just the ones that have been marked as translated.

ⓘ For more information, see *Importing Translations* on page 238.

18. Click **OK**.

19. Once the import is complete, click **Close** to close the **Languages and Translations** dialog.

Translations for the newly added language have been imported to M-Files and you can *select the vault language* on page 238 in M-Files Desktop.

Adding and Exporting Languages

The *Export* function of the *Languages and Translations* dialog can be used to specify the target language of the translation and the format of the material to be translated:
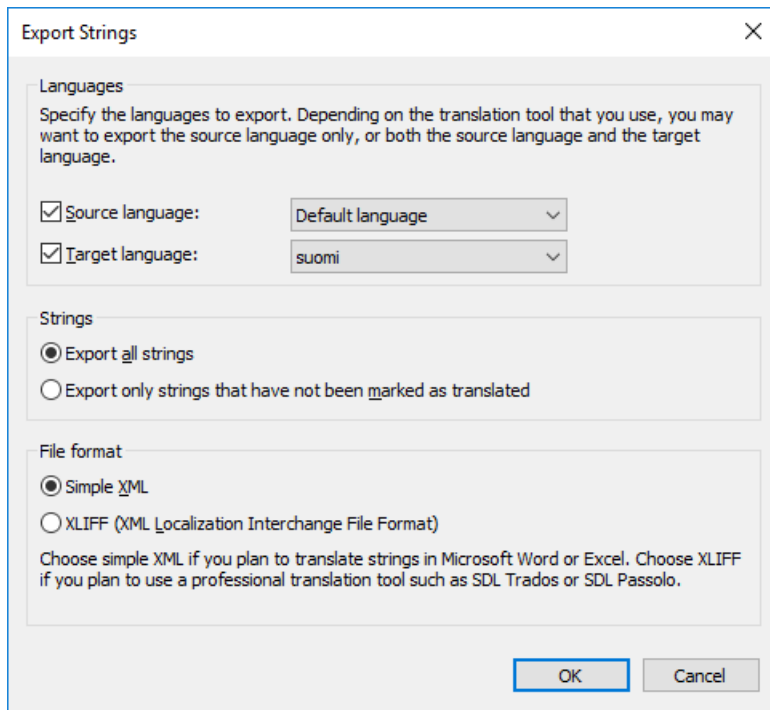
Figure 82: The "Export Strings" dialog.

Languages

Select the *source* and *target* languages. Note that you can translate the metadata structure only one language at a time.

In case you are working in Excel, both the source and target language need to be exported. The source language character strings, that is, the words to translate, are in their specific column and the target language translations are added to a column of their own.

You can also export the source language only. If you are using a translation agency or separate translation software for translating, you should determine the required format for the translation material.

Strings

When commencing the translation process for the first time, select *Export all strings.* A string refers to one concept or a specific attribute in the metadata structure, thus usually, a word or a phrase. Each language has its own strings, that is, a specific vocabulary for the metadata structure.

You can later use the *Export only strings that have not been marked as translated* option in order to export the new or changed strings only.

File format

The available file formats are *Simple XML* and *XLIFF*.

Select *Simple XML*, if you want to translate the strings in Microsoft Word or Excel. Select XLIFF, if you want to use a professional translation tool, such as SDL Trados or SDL Passolo.

Translating in Excel

Translating the metadata structure into the target language in Excel is quite straightforward. Simply open the XML file in Excel: choose the default settings *As an XML table* and *Excel will create a schema based on the XML source data*.

Identifier is the identifier of the concept, i.e. the word or phrase to be translated. For example, an identifier starting with *PropertyDef* indicates that it is a property definition name. *ObjectType* is an object type name and *UserGroup* is a user group name. M-Files creates these identifiers automatically. The translator does not need to pay much attention to these identifiers as such, although they can be helpful pointers when choosing a suitable translation. For a closer look at how the identifiers are named, see *Naming convention of the identifiers* on page 237.

The *Source* column contains the concepts to be translated. The *Target* column is empty. The translator enters the translations in this column.

	A	B	C	D	E
1	identifier	source	target	translated	source-version
2	PropertyDef_0_0_Name	Name or title		0	
3	PropertyDef_20_0_Name	Created		0	
4	PropertyDef_21_0_Name	Last modified		0	
5	PropertyDef_22_0_Name	Single file		0	
6	PropertyDef_23_0_Name	Last modified by		0	
7	PropertyDef_24_0_Name	Status changed		0	
8	PropertyDef_25_0_Name	Created by		0	
9	PropertyDef_27_0_Name	Deleted		0	
10	PropertyDef_28_0_Name	Deleted by		0	
11	PropertyDef_29_0_Name	Version label		0	
12	PropertyDef_30_0_Name	Size on server (this version)		0	
13	PropertyDef_31_0_Name	Size on server (all versions)		0	
14	PropertyDef_32_0_Name	Marked for archiving		0	
15	PropertyDef_33_0_Name	Comment		0	
16	PropertyDef_34_0_Name	Traditional folder		0	
17	PropertyDef_35_0_Name	Created from external location		0	
18	PropertyDef_36_0_Name	Additional classes		0	
19	PropertyDef_37_0_Name	Is template		0	
20	PropertyDef_38_0_Name	Workflow		0	
21	PropertyDef_39_0_Name	Workflow State		0	
22	PropertyDef_40_0_Name	Moved into current state		0	
23	PropertyDef_41_0_Name	Assignment description		0	
24	PropertyDef_42_0_Name	Deadline		0	
25	PropertyDef_43_0_Name	Monitored by		0	
26	PropertyDef_44_0_Name	Assigned to		0	
27	PropertyDef_45_0_Name	Marked as complete by		0	
28	PropertyDef_46_0_Name	Collection members (documents)		0	
29	PropertyDef_47_0_Name	Collection members (document collections)		0	

Sheet1

READY   100%

Figure 83: The exported XML table opened in Excel for translation.

In the above example, a translation from English to the target language has been started. The translation for each source language string is to be placed in the *target* column. When the translation has been added, the *0* in the *translated* column should be replaced with *1*. This tells M-Files that the strings has been translated.

Naming convention of the identifiers

The identifiers are formed as follows: `TableID_ResourceID1_ResourceID2_StringID`.

- **Table ID**: Identifies the type of the metadata structure element in question.

  - `PropertyDef`
  - `ObjectType`
  - `Item` (referring to any translatable value list item)
  - `NamedACL`
  - `View`

- `Language`
- **Record ID 1**: The ID number of the metadata element in question. For instance, the *Document* object type has the identifier `ObjectType_0_0_Name`, where `ObjectType` is the table ID and the first `0` is the record ID 1. The record ID 2 is always `0` for elements other than `Item`.
- **Record ID 2**: The ID number of the item in question. For example, the workflow *Processing job applications* in the M-Files sample vault has the identifier `Item_7_105_Name`, where `Item` is the table ID, `7` the record ID 1, and `105` the record ID 2 identifying the item on the *Workflows* value list.
- **String ID** (`Name` or `NamePlural`): The part of the identifier that specifies whether the translation should be in the singular or plural form.

Importing Translations

When translating in Excel, the string can be marked as translated by changing the cell value of the *translated* column from *0* to *1*. However, if the *Import all strings* option is selected when re-importing the translation back to M-Files, all strings are imported to M-Files regardless of whether the value of the *translated* column.

> 📄 **Note:** In case the *target* column is left empty and the value of the *translated* column is set to `1`, M-Files uses the source language string as the translation.

If you only want to import the strings marked as translated, select the *Import only strings that have been marked as translated* option. This way, only the strings with the value *1* in the *translated* column are imported to M-Files. For example, if new additions are made to the source language at a later stage, this selection can be used to import only the translations of the new additions to M-Files.

If changes are made in the source language, this version data can be found in the *source-version* column of the exported XML file: when changes are made to the source language string, the value of this string cell is always increased by one. The target language translation must then be checked and changed to correspond to the change in the source language.

Also, if the values of the translated strings in the *translated* column have previously been changed to *1*, they will be reset to *0* if changes are made to the source language of these strings. For this reason, it is recommended to instruct the translator to mark the translated and accepted translations as translated, after which the value *1* indicates that the target language translations are up to date.

To import the translation back to M-Files from Excel, save the translated XML file in Excel in *XML Data* format. You can then import the file to M-Files using the *Import* function of the *Languages and Translations* dialog. It is alright for the file to have different name when importing and exporting.

Importing a translation to M-Files is quite straightforward. Just select the appropriate target language and whether you want to import all the strings or just the ones marked as translated.

After importing, M-Files asks if you want to rebuild the *full-text search index* for the metadata. Edited translations cannot be used in searches until the search index is rebuilt. This may take several minutes or even hours depending on the number of objects in the document vault.

Selecting the Software and Vault Language

Users can change both the *software language* and *vault language* via M-Files Desktop. The *software language* refers to the texts and labels that you see in the M-Files user interface, such as button texts, dialog titles, warning messages, and so on. The *vault language* refers to the metadata structure language, which is always specific to a given document vault.

Do the following steps to change the software and the vault language:

1. In M-Files Desktop, press *Alt* and select **Settings** > **Change Language...** from the menu bar.

   ☑ The **Change Language** dialog is opened.

2. Use the **Software language** drop-down menu to change the language of the M-Files user interface.

3. Use the **Vault language** drop-down menu to change the language of the current vault.

ⓘ The vault language selection contains all languages that the document vault has been translated into.

4. Click **OK** to change the languages and to close the **Change Language** dialog.

The M-Files user interface language and the current vault language are changed accordingly.

If 1) the software installation language, 2) the vault language, and 3) the Windows display language are the same, all the M-Files functions and the metadata structure of the document vault are displayed in the language in question.

> 📄 **Note:** If you want to create a new vault in a language other than the currently selected software language, you must first change the software language and restart the M-Files Server service via Windows Task Manager before creating the vault.

> 📄 **Note:** If the user adds a new value to the value list, the new value (concept) will be added to the original metadata structure, that is, the source language contents, regardless of the user's vault language. For example, a user with Finnish as the vault language, can add a new value *LVI-piirustus* to the value list *Drawing Types/Piirustustyypit*. If the source language was English, the new Finnish value "*LVI-piirustus*" is displayed among the English values: " *Architectural*, *LVI-piirustus*, *Mechanical, Services*, etc. The name of this value can be changed in *Value List Properties* to correspond the source language, after which it can be re-translated into Finnish. Common views can be named in the same way according to the text added by the user, regardless of the source language.

> 📄 **Note:** If the metadata structure is translated into several languages, the software or the vault language selected by the user does not affect the search results. For example, if the user has selected Finnish as the language and added a document to class *Hinnasto*, the document in question is included in the search results when using the search criterion *Price List*. However, then the concepts *Price List* and *Hinnasto* must be translations of each other, that is, different translations of the same concept.

Changing the User-Specific Default Vault Language

Administrators can also change the default language of a vault for a specific user. The selected default language can be any of the vault languages. If neither the user nor the administrator changes the vault language, M-Files will use the vault source language as the default.

Do the following steps to change the default vault language for a specific user:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select **Users**.

> ✅ The **Users** list is opened in the right-side pane.

5. Right-click the user whose default vault language you want to change and select **Properties** from the context menu.

> ✅ The **User Properties** dialog is opened.

6. Use the **Vault language** drop-down menu to change the default vault language for the selected user.

7. Click **OK** to save your changes and to close the **User Properties** dialog.

The default language in the selected vault is changed for the selected user.

Event Handlers

With event handlers you can define different operations that are executed when certain events occur, such as after an object is modified or before a new value list item is created, and so on. The operations are specified using variables, generic features of VBScript, and M-Files API.

Examples of event handler use:

- Object permissions can be set to change automatically when the object properties are changed.
- Certain basic documents can be added to every new project via a pre-defined project model.
- Specified Word documents can always be saved as PDFs, so that when a Word file is checked in, it is saved to the server in PDF format as well.
- Data related to photos, such as date and image size, can be automatically added to the metadata of the photo document.
- If the user adds a new value to the value list, the event handler can be used to check that the added value is entered correctly.
- Logging in to M-Files can be prevented outside working hours, for instance during night time and weekends.
- Downloading certain files can be monitored, downloading large numbers of files can be prevented, or an alarm of suspicious downloads can be sent to the administrator.

> 📝 **Note:** The documentation for the M-Files API is located in **Start** > **Programs** > **M-Files** > **Documentation** > **M-Files API**. For more information about VBScript code and M-Files API, go to *www.m-files.com/api*. Instructions on writing VBScript code and working with the M-Files API are available for a separate fee from M-Files customer support (*support@m-files.com*).

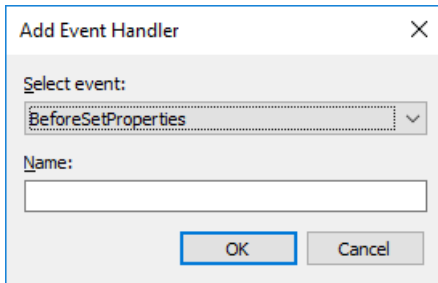Do the following steps to create a new event handler:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, right-click the desired document vault and select **Event Handlers** from the context menu.

   ✅ The **Event Handlers** dialog is opened.
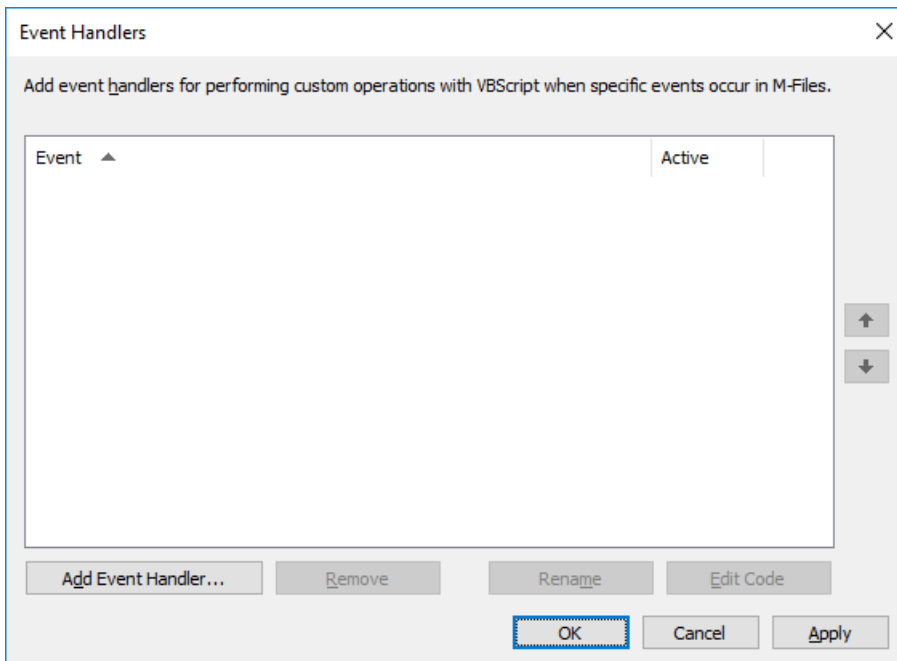
4. Click the **Add Event Handler...** button.

☑ The **Add Event Handler** dialog is opened.

```
Add Event Handler                      ✕

Select event:
BeforeSetProperties                    ⌄

Name:
[                                    ]

         OK            Cancel
```

5. Use the **Select event** drop-down menu to select the event for which you want to create an event handler.

🖉 For example, if you want to create an event handler that is invoked whenever a new object is about to be created, select the **BeforeCreateNewObjectFinalize** event.

ℹ For the list of available events and their descriptions, see *Available Event Handlers* on page 242

6. In the **Name** field, enter a descriptive name for the new event handler and click **OK** to close the **Add Event Handler** dialog.

🖉 For example, `Check for duplicate titles.`

7. Back in the **Event Handler** dialog, click **Edit Code**.

☑ The **Edit VBScript Code** window is opened.

```
Edit VBScript Code                                                        ✕

  |



















  <                                                            >
```
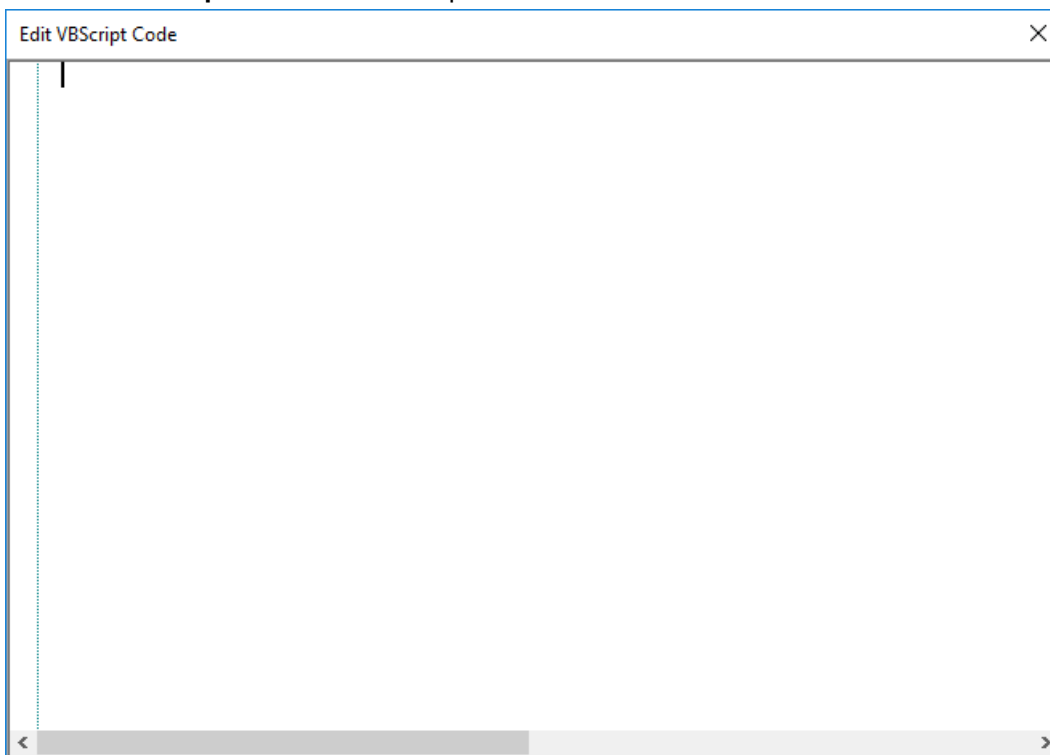
8. Enter the code to be executed when the event handler is invoked, and then close the **Edit VBScript** window.

🖉 For example, the following code in the **BeforeCreateNewObjectFinalize** event could be used to display an error message to the user when they are about to create a new object (that is, the

metadata card is filled with the necessary information and the user clicks the **Create** button) and the document vault already contains an object with the same title:

```vbscript
' The ID of the title property.

Dim titleProperty
titleProperty = MFBuiltInPropertyDefNameOrTitle

' Find the title property of the current object.

Dim currentTitleProp
currentTitleProp = PropertyValues.SearchForProperty(titleProperty)

' Get the title of the object.

Dim currentTitle
currentTitle = currentTitleProp.Value

' Search for objects on the basis of title.

Dim titleSearch
Set titleSearch = CreateObject("MFilesAPI.SearchCondition")
Dim titleExpression
Set titleExpression = CreateObject("MFilesAPI.Expression")
titleExpression.SetPropertyValueExpression titleProperty,
 MFParentChildBehaviorNone, Nothing
Dim titleTypedValue
Set titleTypedValue = CreateObject("MFilesAPI.TypedValue")
titleTypedValue.SetValue MFDatatypeText, currentTitle
titleSearch.Set titleExpression, MFConditionTypeEqual, titleTypedValue
Dim SearchResults
Set SearchResults
 = Vault.ObjectSearchOperations.SearchForObjectsByCondition(titleSearch, false)

' If an existing object with the same title was found, raise an error.

If SearchResults.Count > 1 Then

    Err.Raise MFScriptCancel, _
    "The document vault already contains an object with the same title.
 Please choose another title."

End if
```

9. Back in the **Event Handlers** dialog, click **OK** to save your changes and to close the **Event Handlers** dialog.

The new event handler is added to the selected document vault and the code that you have defined is executed whenever the event handler is invoked.

Available Event Handlers

Below you can find the available event handlers, with their variables and explanations. For more information about variables, refer to *VBScript Variables Explained* on page 402.

Document vault event handlers on page 243

Server event handlers on page 250

Document vault event handlers

`BeforeSetProperties` and `AfterSetProperties`	
Variables	`ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `PropertyValues`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`
Execution	The event handlers are executed when the property values of the object stored in the document vault are re-set. Properties can be inspected during `BeforeSetProperties` before they are set. It is not, however, recommended to modify properties during `BeforeSetProperties` as they may be overwritten after the event handler has been executed. Properties, on the other hand, can be modified during the `AfterSetProperties` event.

`BeforeCreateNewObjectFinalize` and `AfterCreateNewObjectFinalize`	
Variables	`ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `PropertyValues`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`
Execution	The event handlers are executed when a new object is created in the document vault, regardless of whether the new object has been checked in or not. When executing the `AfterCreateNewObjectFinalize` event handler, the object may have already been checked in. For this reason, the metadata or files can no longer be modified during operation of the event handler, and thus the event handler is only suitable for validating changes.

`BeforeCancelCreateObject` and `AfterCancelCreateObject`	
Variables	`ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`
Execution	The event handlers are executed when an object which has never been checked in is removed from the document vault. The execution takes place, for instance, when the user performs the "Undo Checkout" function on the object or removes the object from the document vault.

`BeforeCheckInChanges` and `AfterCheckInChanges`	
Variables	`ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`
Execution	The event handlers are executed when the user checks the object in. The event handlers are not executed if the object was not modified, in which case the `BeforeCancelCheckOut` and `AfterCancelCheckOut` event handlers are executed. It is still possible to modify the object during `BeforeCheckInChanges`. These event handlers are also executed when the user creates a new object with the **Check in immediately** option unchecked, and checks in the object without making any changes to the file. These event handlers are not executed when a new object is created with the **Check in immediately** option enabled. During the execution of the

BeforeCheckInChanges and **AfterCheckInChanges**	
	`AfterCheckInChanges` event handler, the object can no longer be modified as the object has already been checked in, and thus the event handler is only suitable for validating changes.

BeforeCancelCheckOut and **AfterCancelCheckOut**	
Variables	`ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`
Execution	The event handlers are executed when modifications of a checked out object are undone using, for example, the "Undo Checkout" function. The event handlers are also executed if the object is checked in without any modifications. During execution of the `AfterCancelCheckOut` event handler, the object cannot be modified as the object is no longer checked out.

AfterCancelCheckoutFinalize	
Variables	`ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`
Execution	An event triggered after the undo checkout operation is complete, meaning that the object is no longer checked out. A script can be used for performing the checkout operation and for performing further object operations with the checked out object version.

BeforeCheckOut and **AfterCheckOut**	
Variables	`ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`
Execution	The event handlers are executed when a document vault object is checked out. During execution of the `BeforeCheckOut` event handler, the object has not been checked out, so the object cannot be modified.

BeforeDeleteObject and **AfterDeleteObject**	
Variables	`ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`
Execution	The event handlers are executed when an object is marked as deleted.

BeforeDestroyObject and **AfterDestroyObject**	
Variables	`ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`

`BeforeDestroyObject` and `AfterDestroyObject`	
Execution	The event handlers are executed when an object is destroyed from the document vault.

`BeforeDestroyObjectVersion` and `AfterDestroyObjectVersion`	
Variables	`ObjVer, DisplayID, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handlers are executed when an individual version of the object is destroyed from the document vault.

`BeforeSetObjectPermissions` and `AfterSetObjectPermissions`	
Variables	`ObjectAccessControlList, ObjVer, DisplayID, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handlers are executed when the object permissions are changed.

`BeforeFileUpload`	
Variables	`FileTransferSessionID, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handler is executed when the user starts a file transfer to M-Files Server.

`AfterFileUpload`	
Variables	`FileTransferSessionID, FileVer, ObjVer, DisplayID, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handler is executed when the file transfer to the server is completed.

`BeforeFileDownload` and `AfterFileDownload`	
Variables	`FileTransferSessionID, ObjID, FileVer, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handlers are executed when the user loads the file from M-Files Server to the client machine's local cache. If necessary, these event handlers can be used to prevent transfer of certain files to the users' machines.

BeforeCreateNewValueListItem and **AfterCreateNewValueListItem**	
Variables	`ValueListItem, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handlers are executed when new values are added to a certain value list of the document vault. These event handlers can be used to, for example, ensure that all values entered in the value list are in a specified form as desired.

BeforeLoginToVault	
Variables	`LoginAccount, Vault, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handler is executed immediately prior to logging in of the user to the document vault. At this stage, the user has already been identified against M-Files Server, so the event handler is not executed, for instance, if a user who attempts to log in does not have a login account on the server.

AfterLoginToVault	
Variables	`LoginAccount, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handler is executed when the user has successfully logged in to the document vault.

BeforeLogoutFromVault	
Variables	`Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handler is executed immediately before the user is logged out of the document vault. The logout cannot be interrupted during this event handler. The client software does not react to any error messages received from this event handler.

AfterLogoutFromVault	
Variables	`LoggedOutUserID, Vault, VaultSharedVariables, SavepointVariables, TransactionCache, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handler is executed when the user has been logged out of the document vault. The logout cannot be interrupted during this event handler. The client software does not react to any error messages received from this event handler.

Replication: `AfterCheckInChanges`	
Variables	`RestoredVersions, Vault, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, ObjVer, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handlers are invoked when new versions are imported to the existing object from the content package or when a conflict between two objects is resolved in favor of the source-vault version. When the `AfterCheckInChanges` event handler is invoked, the object has already been checked in. For this reason, the metadata or files can no longer be modified during operation of the event handler.

Replication: `AfterCreateNewObjectFinalize`	
Variables	`RestoredVersions, Vault, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, ObjVer, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handler is invoked when a new object is imported to the document vault from the content package. On invoking of the `AfterCreateNewObjectFinalize` event handler, the object has already been checked in. For this reason, the metadata or files can no longer be modified during operation of the event handler.

`VaultExtensionMethod`	
Variables	`Input, Output, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event handler is invoked explicitly by the client (the so-called vault extension method).

`BeforeCreateLoginAccount` and `AfterCreateLoginAccount`	
Variables	`LoginAccount, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	`BeforeCreateLoginAccount`: an event that is triggered for all online vaults before a login account is created on the server. An exception in the event does not prevent the operation to be executed. `AfterCreateLoginAccount`: an event that is triggered for all online vaults after a login account is created on the server.

`BeforeModifyLoginAccount` and `AfterModifyLoginAccount`	
Variables	`LoginAccount, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	`BeforeModifyLoginAccount`: an event that is triggered for all online vaults before a login account is modified on the server. An exception in the event does not prevent the operation to be executed. `AfterModifyLoginAccount`: an event that is triggered for all online vaults after a login account is modified on the server.

`BeforeRemoveLoginAccount` and `AfterRemoveLoginAccount`	
Variables	`LoginAccount, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	`BeforeRemoveLoginAccount`: an event that is triggered for all online vaults before a login account is removed from the server. An exception in the event does not prevent the operation to be executed. `AfterRemoveLoginAccount`: an event that is triggered for all online vaults after a login account is removed from the server.

`BeforeCreateUserAccount` and `AfterCreateUserAccount`	
Variables	`UserAccount, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The `BeforeCreateUserAccount` event is triggered for all online vaults before a user account is created on the server. The `AfterCreateUserAccount` event is, in turn, executed for all online vaults after a user account is created.

`BeforeModifyUserAccount` and `AfterModifyUserAccount`	
Variables	`UserAccount, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The `BeforeModifyUserAccount` event is triggered for all online vaults before a user account is modified on the server. The `AfterModifyUserAccount` event is, in turn, executed for all online vaults after the modification.

`BeforeRemoveUserAccount` and `AfterRemoveUserAccount`	
Variables	`UserAccount, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The `BeforeRemoveUserAccount` event is triggered for all online vaults before a user account is removed from the server. The `AfterRemoveUserAccount` event is, in turn, executed for all online vaults after the removal.

`BeforeCreateUserGroup` and `AfterCreateUserGroup`	
Variables	`UserGroupAdmin, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The `BeforeCreateUserGroup` event is triggered for all online vaults before a user group is created on the server. The `AfterCreateUserGroup` event is, in turn, executed for all online vaults after the user group is created.

`BeforeModifyUserGroup` and `AfterModifyUserGroup`	
Variables	`UserGroupAdmin, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The `BeforeModifyUserGroup` event is triggered for all online vaults before a user group is modified on the server. The `AfterModifyUserGroup` event is, in turn, executed for all online vaults after the modification.

`BeforeRemoveUserGroup` and `AfterRemoveUserGroup`	
Variables	`UserGroupAdmin, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The `BeforeRemoveUserGroup` event is triggered for all online vaults before a user group is removed from the server. The `AfterModifyUserGroup` event is, in turn, executed for all online vaults after the removal.

`AfterBringOnline` and `BeforeTakeOffline`	
Variables	`Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The `AfterBringOnline` event is triggered after the vault is brought online. The `BeforeTakeOffline` event, in turn, is executed before the vault is taken offline. An exception in any of the two event handlers does not prevent the online/offline transition.

`AfterCheckInChangesFinalize`	
Variables	`ObjVer, DisplayID, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The event is triggered when an object has been completely checked in (or when an object is immediately checked in after it has been created) after all the operations occurring after the check-in, such as any automatic state transitions, have been completed.

`BeforeReturnView`	
Variables	`CurrentUserID,CurrentUserSessionInfo, View, Vault, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	This event handler is triggered after a view has been retrieved from the vault but before it is returned to the client. It enables you to modify a view, for instance, by filtering it with dynamic search conditions, such as ones based on the current user.

`BeforeUndeleteObject` and **`AfterUndeleteObject`**	
Variables	`ObjVer, DisplayID, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The `BeforeUndeleteObject` event handler is triggered before an object is undeleted. The `AfterUndeleteObject` event handler is triggered after an object is undeleted. A script can be used for performing the checkout operation and for performing further object operations with the checked out object version.

`AfterUndeleteObjectFinalize`	
Variables	`ObjVer, DisplayID, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	This event is triggered after the object undelete operation is complete and you are able to work with the undeleted object.

`BeforeModifyMFilesCredentials` and **`AfterModifyMFilesCredentials`**	
Variables	`Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MasterTransactionID, CurrentTransactionID, ParentTransactionID, ActivityID, GetExtensionObject`
Execution	The `BeforeModifyMFilesCredentials` event handler is triggered before the password of the M-Files login account is changed, and the `AfterModifyMFilesCredentials` event handler after the password of the M-Files login account is changed.

Server event handlers

`BeforeRunScheduledJob` and **`AfterRunScheduledJob`**	
Variables	`MFScriptCancel, CurrentUserID, ScheduledJob, ScheduledJobOutputInfo, CurrentUserSessionInfo, GetExtensionObject, GetExtensionObject`
Execution	The event handler is executed when one of the timed jobs of the server is performed. These event handlers can be used to automatically monitor the execution of the automatically timed jobs. In case of error, the event handler can automatically send an e-mail notification to the administrator to facilitate resolution of the problem.

`BeforeCreateLoginAccount` and **`AfterCreateLoginAccount`**	
Variables	`LoginAccount, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	`BeforeCreateLoginAccount`: an event that is triggered before a login account is created on the server. `AfterCreateLoginAccount`: an event that is triggered after a login account is created on the server.

`BeforeModifyLoginAccount` and `AfterModifyLoginAccount`	
Variables	`LoginAccount, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	`BeforeModifyLoginAccount`: an event that is triggered before a login account is modified on the server. `AfterModifyLoginAccount`: an event that is triggered after a login account is modified on the server.

`BeforeRemoveLoginAccount` and `AfterRemoveLoginAccount`	
Variables	`LoginAccount, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	`BeforeRemoveLoginAccount`: an event that is triggered before a login account is removed from the server. `AfterRemoveLoginAccount`: an event that is triggered after a login account is removed from the server.

`BeforeModifyMFilesCredentials` and `AfterModifyMFilesCredentials`	
Variables	`CurrentUserID, CurrentUserSessionInfo, GetExtensionObject`
Execution	The `BeforeModifyMFilesCredentials` event handler is triggered before the password of the M-Files login account is changed, and the `AfterModifyMFilesCredentials` event handler after the password of the M-Files login account is changed.

`BeforeCheckinChangesFinalize`	
Variables	`ObjVer, DisplayID, Vault, CurrentUserID, CurrentUserSessionInfo, VaultSharedVariables, SavepointVariables, TransactionCache, MFScriptCancel, GetExtensionObject, MasterTransactionID, CurrentTransactionID, ParentTransactionID`
Execution	The `BeforeCheckinChangesFinalize` event handler is triggered before an object is checked in, but after the state transitions and signatures have been finalized. Workflow changes are not allowed.

9.2. Users

Under *Users*, you can add users to the document vault, thus assigning a name to the user and specifying the user's permissions. Each user object is based on a *server login account* (see *Login Accounts* on page 209).

M-Files assigns each user a unique ID, which can be found via the user's properties in M-Files Admin.

Creating a User

▶ Video: *Configure User Properties*

Do the following steps to create a new user to a selected document vault:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight **Users**.

5. Click **New User...** on the task area.

   ☑ The **New User** dialog is opened.

   ┌───┐
   │ User Properties - New User   ✕ │
   │   │
   │ General Permissions   │
   │   │
   │ ID: <new>   │
   │ Login account: JohnD   ⌄   │
   │ Full name: │
   │ Vault language: Default language   ⌄   │
   │   │
   │ ☐ User account is disabled   │
   │ ☐ User cannot create documents or other objects │
   │ ☐ User cannot create or modify traditional folders │
   │ ☐ External user   │
   │   │
   │ ┌ Administrative rights in vault ─────────────┐ │
   │ │ ☐ Full control of vault   │ │
   │ │ ☐ See and read all vault content (including deleted objects) │ │
   │ │ ☐ See and undelete deleted objects   │ │
   │ │ ☐ Destroy objects   │ │
   │ │ ☐ Force undo checkout   │ │
   │ │ ☐ Change permissions for all objects   │ │
   │ │ ☐ Change metadata structure   │ │
   │ │ ☐ Manage workflows   │ │
   │ │ ☐ Manage user accounts   │ │
   │ │ ☐ Manage common views and notification rules │ │
   │ └───┘ │
   │   │
   │   OK   Cancel   Apply   Help   │
   └───┘

6. Use the **Login account** drop-down menu to select a login account for the user or select **New login account...** from the same drop-down menu to create a new login account for the user.

   ⓘ For instructions on creating a new login account, see *New Login Account* on page 30.

   ☑ The **Full name** field is updated with the full name information of the selected login account.

7. Use the **Vault language** drop-down menu to select the default vault language for the user from the list of available vault languages.

   ⓘ For instructions on adding a new vault language, see *Languages and Translations* on page 231.

8. Set the properties and administrative rights for the new user in the selected vault by checking or unchecking the relevant option check boxes:

Option	Description
User account is disabled	When the account is disabled, the user cannot access the document vault. Logging in to the document vault has been disabled, but the user information is retained. The account can be easily enabled again by unchecking this

Option	Description
	option check box when necessary. For example, you may want an employee's account to be disabled during her vacation for data security reasons.
User cannot create documents or other objects	The user cannot create documents or other objects in the vault but can, for example, read them if provided with the necessary permissions.
User cannot create or modify traditional folders	The user cannot create traditional folders in the vault or modify existing traditional folders.
External user	Users can be grouped into external and internal users. A user can be defined as an external user by enabling the **External user** option. External users cannot see or access any documents other than those specifically marked for them. By default, they do not have permissions to view any documents. For example, you can define your customers as external users and grant them access to customer-specific documents in the document vault.
	As stated above, external users do not, by default, have permissions for accessing any documents. To share a document with an external user, access must be explicitly granted in the permissions of the document.
Full control of vault	With this option, the user is assigned all *administrative permissions* in the vault.
See and read all vault content (including deleted objects)	Regardless of the permissions specified for a document or object, a user with this permission can see and read all objects, including deleted ones.
See and undelete deleted objects	The user has the permission to restore documents and other objects marked as deleted.
Destroy objects	The user has the permission to permanently destroy objects.
Force undo checkout	A user with this permission can undo the *checkout* made by another user. For example, if a user has forgotten to check in a document that others should be able to edit, a user with this permission can check in the document. In this case, the changes made to the document during the checkout will not be saved on the server.
Change permissions for all objects	The user has the right to change the permissions for any object that they are permitted to see. You can edit the permissions for an object, for instance, remove the write permission to a document from other users.
	📝 **Note:** The user with this permission has the power to obtain edit rights to documents that they would normally be able to only read.
Change metadata structure	The user has the permission to modify document vault metadata, such as add new document classes or value lists. For example, if you want to change the *Invoice* document class so that the *Project* property field must be filled in for each invoice, you can make the change if you have this permission. Even if the user does not have the permission to do this, the user can still add new metadata fields to individual objects using the metadata card.
Manage workflows	This permission enables the user to create, edit and delete workflows in M-Files Admin.

Option	Description
Manage user accounts	The user has the permission to manage login accounts in the selected document vault. With this permission, you can, for instance, add or remove users from the document vault.
Manage common views and notification rules	The user has the permission to manage the document vault views and notification rules. With this permission, you can create a document vault view visible to all users. You can also define common notification rules. Common views and notifications are created via M-Files Desktop.

> **Note:** For more information on common views, see *"View" Menu* on page 79. For more information on common notification rules, see *Notification Settings (M-Files Desktop)* on page 127.

9. Optional: On the **Permissions** tab, specify the users or user groups who may see this user.

   a) On the **Users and user groups** list, highlight the user or the user group for which you wish to set the permissions for seeing this user.

   > If the desired user or user group is not on the list, click **Add...** to add the user or user group to the **Users and user groups** list.

   b) Check either the **Allow** or **Deny** checkbox to modify the permissions of the selected user.

10. Click **OK** once you are done.

A new user is created and it is listed in the **Users** list. The new user can now access the selected document vault with the permissions that you have defined.

> **Note:** You can also import domain users to M-Files. For instructions, see *Importing Users* on page 255.

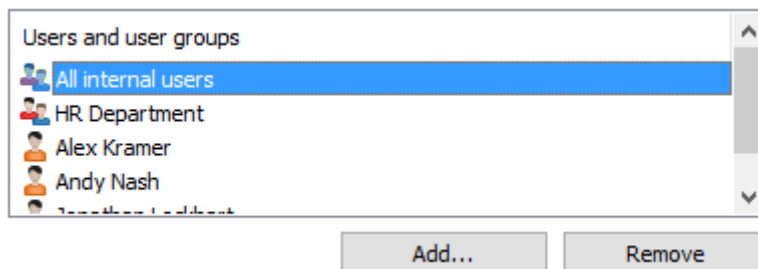## Permissions

The *Permissions* tab enables you to specify who may see this user.

> **Note:** The system administrator and all users with full control of the document vault in question always see all users.

▶ Video: *Configure Vault User Visibility*

Adjusting Permissions

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight the appropriate node or subnode of the vault and select the desired item from the list on the right.

5. Right-click the item and select **Properties** from the context menu.

6. Go to the **Permissions** tab.

7. From the **Users and user groups** list, select the user or user group whose permissions you want to adjust.

> ⓘ If the user or user group is not on the list, click **Add...** to add the user or user group to the list.

8. Either:

    a. Check the **Allow** check box to allow the selected user to see this item.

       or

    b. Check the **Deny** check box to deny the selected user from seeing this item.

9. Optional: If you want to adjust additional permissions, repeat the steps 7 and 8.

10. Click **OK** once you are done.

You have adjusted the view permissions of the selected item for the selected users.

Importing Users

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight **Users** and then click **Import Individual Users...** on the task pane.

    ☑ The **Import Individual Users** dialog is opened.

5. Using the **Domain** drop-down menu, select the domain from which you want to import users.

6. Using the **Organizational unit** drop-down menu, select the organizational unit from which you want to import users.

7. Using the **User group** drop-down menu, select the user group from which you want to import users.

    ☑ The **Select the users to import** list is populated with the members of the selected user group.

8. Optional: Check the **Include users from nested groups** option check box, if you want to import users from user groups nested within the selected user group.

    ☑ The **Selelect users to import** list is populated with the members of the selected user group and the members of any user group nested within the selected user group.

9. Select the user to be imported by clicking its username on the list.

> ⓘ You can select more than one item at once by holding down the Ctrl key to select multiple individual items or by holding down the ⇧ Shift key to select adjacent items on the list.

10. Using the **License type for new login accounts** drop-down menu, select the license type for the login accounts that are created for the imported users.

    ℹ For more information about license types, see *License types* on page 181.

11. Click **OK** to import the selected users.

The users are imported to the selected vault and added to the **Users** list.

9.3. User Groups

User groups can be managed by selecting the *User Groups* heading in the left-side tree view of M-Files Admin.

You can create, edit, remove and import user groups to your vault. Creating user groups makes it easier to specify permissions for documents. You can combine into user groups individual users with a certain common feature, such as their position in the organization (management, research and development, and so forth).

Creating a User Group

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight **User Groups** and then click **New User Group...** on the task pane.

    ☑ The **User Group Properties** dialog is opened.

5. In the **Name** field, enter a name for the new user group.

6. Click **Add...** to add users to this group.

    ☑ The **Select Users or User Groups** dialog is opened.

7. Select the users to be added to the user group and click **Add**.

    ℹ You can select more than one item at once by holding down the Ctrl key to select multiple individual items or by holding down the ⇧ Shift key to select adjacent items on the list.

8. Optional: Enable the **Group members are synchronized from the domain** and click **Define...** if you want to retrieve the users from a domain.

    ℹ For more information, see *Importing User Groups* on page 257.

9. Optional: On the **Advanced** tab, define an alias for the user group.

    ℹ For more information, see *Associating the Metadata Definitions* on page 203.

10. Click **OK** to finish creating the user group.

The user group that you have just created is added to the **User Groups** list.

Permissions

The *Permissions* tab enables you to specify who may see this user group.

📄 **Note:** The system administrator and all users with full control of the document vault in question always see all user groups.

Adjusting Permissions

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight the appropriate node or subnode of the vault and select the desired item from the list on the right.

5. Right-click the item and select **Properties** from the context menu.

6. Go to the **Permissions** tab.

7. From the **Users and user groups** list, select the user or user group whose permissions you want to adjust.

ℹ️ If the user or user group is not on the list, click **Add...** to add the user or user group to the list.

8. Either:

   a. Check the **Allow** check box to allow the selected user to see this item.

      or

   b. Check the **Deny** check box to deny the selected user from seeing this item.

9. Optional: If you want to adjust additional permissions, repeat the steps 7 and 8.

10. Click **OK** once you are done.

You have adjusted the view permissions of the selected item for the selected users.

Importing User Groups

User groups can be imported by domain and by organizational unit. This makes importing user groups into M-Files quicker and easier. M-Files can check for new and deleted user group members periodically.

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight **User Groups** and then click **Import User Group...** on the task area.

✓ The **Import User Group** dialog is opened.

5. Using the **Domain** drop-down menu, select the domain from which you want to import user groups.

6. Using the **User group** drop-down menu, select the user group that you want to import.

    ✓ The list area in the **Import User Group** dialog is populated with the members of the selected user group.

7. Optional: Check the **Include users from nested groups** option check box if you want to import the users from any nested user groups as well.

8. Using the **License type for new login accounts** drop-down menu, select the license type for the login accounts of the users to be imported.

    ⓘ For more information about license types, see *License type* on page 211.

9. Optional: Check the **Check for new and deleted members every 15 minutes** option check box if you want to keep the user group up to date and import new users automatically when they are added to the group.

10. Click **OK** to import the selected user group.

The selected user group is imported to the selected vault and it is added to the **User Groups** list.

Defining, Editing or Disabling Import Settings of Existing User Groups

You can also import users to existing user groups in M-Files.

Or you can edit the synchronization settings of previously imported user groups. If the user group on the domain is changed (it is for instance renamed or the grouping is changed), the earlier imported M-Files user group can be merged with the new user group on the domain. This preserves the identity of the M-Files user group regardless of changes in the domain user group, and the permissions related to it can remain the same.

if you no longer wish to import users to a specific user group, you can also disable user group synchronization altogether.

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight **User Groups** and then, on the **User Groups** list, double-click a user group that you want to edit.

    ✓ The **User Group Properties** dialog is opened.

5. Either:

If you want to	Do the following
Import to users an existing user group	Check the **Group members are synchronized from the domain** option check box, click the **Define...** button and then define the import settings in the dialog that is opened. See *Importing User Groups* on page 257 for specific instructions on import settings. After you are done, click **OK**.
Edit the import settings of a previously imported user group	Click **Define...** and modify the settings in the dialog that is opened. See *Importing User Groups* on page

If you want to	Do the following
	257 for specific instructions on import settings. After you are done, click **OK**.
Disable user group synchronization for a user group	Uncheck the **Group members are synchronized from the domain** option check box.

6. Click **OK** to save your changes and close the **User Group Properties** dialog.

Users in Synchronized Active Directory Groups

When new users are added to Active Directory (AD) groups that are synchronized to M-Files:

- The users are added as vault users to the vault in which the user group is located.
- If the added users do not yet have M-Files login accounts, new login accounts are automatically created for the users and the license specified in the synchronization settings is applied to the new login accounts.
- No changes are made to existing M-Files login accounts. If users have been assigned concurrent licenses, and they are added to a group for which named licenses are specified, the users retain their concurrent licenses.

When users are removed from AD groups that are synchronized to M-Files:

- The users are removed from the user group in M-Files, losing all permissions that were granted to them through the group membership.
- No other changes are made. The users retain their access to the document vault and their login accounts remain active, keeping the licenses assigned to them.

9.4. Metadata Structure

M-Files Admin enables you to modify the document vault's metadata elements, such as *object types*, *value lists*, *property definitions* and *classes*. Classes can also further be categorized into *class groups*. The document and object metadata is utilized almost everywhere in M-Files, such as in views and search functions, so the purpose of the metadata should be studied carefully.

You can browse the metadata structure either as a hierarchical view or as a flat view.

▶ Video: *Metadata Structure*

Object Types

M-Files uses object types to define the objects to be stored. Built-in object types include *documents* and *document collections*, but depending on the needs of the organization, you can also define object types like *customer*, *contact*, *project*, etc. in the document vault. They can then be managed via M-Files, storing the change history of these objects as well.

▶ Video: *Objects*

Besides versioning, M-Files enables sorting in dynamic views, protection against concurrent editing, easy-to-use permissions functionality, and extremely versatile search capabilities for all objects.

The metadata card is provided both for documents as well as for other object types. Other object types differ from documents in that they need not contain any files whereas documents are always based on at least one file (such as a Word document).

Creating a New Object Type

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Metadata Structure (Flat View)** and then select **Object Types**.

☑ The **Object Types** list is opened in the right pane.

5. Click **New Object Type...** on the task area.

☑ The **Object Type Properties** dialog is opened.

6. In the **Name (singular)** field, type in an appropriate name for the object type in the singular form.

7. In the **Name (plural)** field, type in the same name in the plural form.

8. Optional: Click **Change Icon...** to change the icon of the object type.
   a) Select an icon from the list or click **Browse...** to browse for a different icon file.
   b) Click **OK** to change the icon.

   ⓘ If you wish to restore the default icon, click **Use Default**.

9. Optional: If you want users to be able to create objects of this type in M-Files, check the **Users can create objects of this type** option check box.
   a) If you want to add in the task area a command for creating a new object of this type, check the **Show the creation command in the task area** option check box.

10. Optional: If you want users to be able to incorporate files into objects of this type, check the **Objects of this type can have files** option check box.

11. Optional: Check the object types in the **The types of objects that users can browse for objects of this type** list that you want users to be able to browse when they right-click an object of this type and select **Browse Relationships**.

    ℹ️ This setting does not affect the related objects displayed in the listing view (search results or a view) below the main object.

12. Using the **Default permissions for new objects** drop-down menu, select the default permissions for new objects of this type.

    ℹ️ You can click the **...** button to adjust any existing permission settings.

13. Optional: Check the **Allow this object type to be used as a grouping level in views** option check box to allow this object type to used for defining a grouping level within a view.

The object type that you have just created is added to the **Object Types** list. You can now create objects of this type in M-Files.

Advanced (Object Type Properties)
Object type hierarchy (Object Type Properties)

Object types can have hierarchical relationships. For example, the relationship between a customer company and its contact person can be defined so that the *Contact Person* object type is a subtype of the *Customer* object type. Viewing the value list for the *Customer* object type also displays the contact persons filtered by customer.

📋 **Note:** You cannot define an internal hierarchy for an object type.

Defining an Object Type Hierarchy

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Metadata Structure (Flat View)** and then select **Object Types**.

    ☑️ The **Object Types** list is opened in the right pane.

5. Double-click the object type for which you want to define a hierarchy.

    ☑️ The **Object Type Properties** dialog is opened.

6. On the **Advanced** tab, do one or both of the following:

If you want to	Do the following
Define subtypes for this object type	Click the **Add...** button, then select the object types to be added as subtypes of this object type, and click **Add**.
	📋 **Note:** You can select more than one item at once by holding down the Ctrl key to select multiple individual items or by holding down the ⇧ Shift key to select adjacent items on the list.
	📋 **Note:** You can remove a subtype by clicking **Remove**.

If you want to	Do the following
Define this object type as a subtype of another object type	Check the **This object type is a subtype of the following object type** option check box and select the object type using the drop-down menu.

7. Click **OK** to save your changes and close the **Object Type Properties** dialog.

An object type hierarchy is created between the selected object types. In M-Files, when you create a new object that you have defined as a subtype of another object type, you will need to select an owner object for it. Thus a relationship is created between the owner and the subobject when the new object is created.

Default for automatic permissions (Object Type Properties)

The actual final object receives automatic permissions when a value with automatic permissions specified is added for the object.

You can activate the automatic permissions by value, value list, object type or class. You can specify the automatic permissions for each object type in the same way as for each value.

> 📄 **Note:** The value-specific settings always have priority over the settings made at value list and object type level. For more information, see *Automatic Permissions* on page 275.

Aliases (Object Type Properties)

Aliases can be used for identifying semantically equivalent metadata. For example, when importing objects from another vault, their *Date* and *Description* properties can be mapped to the target vault's equivalent properties on the basis of aliases even if the properties' internal IDs and/or names are different. That is, the aliases refer to semantically equivalent metadata in different vaults, or in other words, alias is a common ID for the same metadata definition between several vaults.

The alias is defined as a common ID with the same name in both source and target vault.

When defining the alias, you can use various external data type and archive standards, such as SÄHKE2, MoReq2, and Dublin Core.

For more information, see *Associating the Metadata Definitions* on page 203.

Performance (Object Type Properties)

You might want to enable the **Use a separate metadata search index for this object type** option for essential object types that are frequently used and that are found in large number in the vault.

Since these essential object types vary from organization to organization, the option is disabled by default. In document management, for instance, the *Document* object type is naturally the most important object type. In CRM vaults, however, the most important object types are usually something different, such as *Customer*, *Project*, *Contact person*, and so on.

Enabling this option makes M-Files use a separate search structure for the objects of the selected object type. This improves search speed for both the objects of the selected object type and for other objects – especially in case the vault contains a high number of objects representing this key object type.

> 📄 **Note:** Enabling this option might take a long time to complete, from a couple of minutes up to a few hours. The vault is also taken offline for the duration of this operation, preventing any users from accessing the vault.

Permissions

Access for viewing this object type and creating objects of this type can be defined on the *Permissions* tab.

If the user does not have the permission to view the name of the object type, it is not available for selection in M-Files Desktop (for example when you are creating a new object or search). Even if the object type name is hidden, the user can see the objects themselves in views or search results, for example.

If you cannot see the object type name, you do not have the permission to create objects of this type either. However, the user may have the permission to see the name without having permission to create new objects.

Adjusting Permissions

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight the appropriate node or subnode of the vault and select the desired item from the list on the right.

5. Right-click the item and select **Properties** from the context menu.

6. Go to the **Permissions** tab.

7. From the **Users and user groups** list, select the user or user group whose permissions you want to adjust.

> ℹ If the user or user group is not on the list, click **Add...** to add the user or user group to the list.

8. Either:

   a. Check the **Allow** check box to allow the selected user to see this item.

      or

   b. Check the **Deny** check box to deny the selected user from seeing this item.

9. Optional: If you want to adjust additional permissions, repeat the steps 7 and 8.

10. Click **OK** once you are done.

You have adjusted the view permissions of the selected item for the selected users.

Connection to External Database (Object Types)
▶ Video: *Importing from Databases*

You can set M-Files to update any object type or a value list to and from an external database.

The example below describes how to define an object type to use an external database connection to SQL Server. The steps for specifying an external database connection for a value list are very similar.

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand the **Metadata Structure (Flat View)** node.

5. Select the **Object Types** node (or the **Value Lists** node if you are defining a value list to use an external database connection).

   ✔ The object type (or value list) listing is opened in the right pane.

6. In the right-pane listing, right-click the object type (or value list) of your choice and select **Properties** from the context menu.

7. Select the **Connection to External Database** tab.

   ✔ The **Connection to External Database** tab is opened.

Object Type Properties - New Object Type	✕

   General   Advanced   Permissions   Connection to External Database

   ☑ Use a connection to an external database to import and modify objects that reside in the external database.

   OLE DB connection string (from server):

   [　　　　　　　　　　　　　] [Define...] [?]

   SELECT statement:

   [　　　　　　　　　　　　　　　　] [?]

   [Refresh Columns]

   Columns:

Source Column	Target Property	Update	Insert

   If you want to allow users to modify the data in the external database from within M-Files, specify the SQL statements that M-Files Server can use to create, modify, or delete records in the external database:

   UPDATE statement for modifying an existing record:

   [　　　　　　　　　　　　] [Default] [?]

   INSERT INTO statement for creating a new record:

   [　　　　　　　　　　　　] [Default] [?]

   SELECT statement for getting the ID of the new record after insertion:

   [　　　　　　　　　　　　] [Default] [?]

   DELETE statement for deleting a record:

   [　　　　　　　　　　　　] [Default] [?]

   ☐ Disabled

   [Contents...] [OK] [Cancel] [Apply] [Help]

8. Enable the option **Use a connection to an external database to import and modify objects that reside in the external database**.

9. Click the **Define...** button next to the **OLE DB connection string (from server)** field.

   ⓘ The syntax of the connection string depends on the *OLE DB* (Object Linking and Embedding Database) supplier used for establishing the connection to the external database. If Open Database Connectivity (*ODBC*) is required to establish a connection, the data store has to be accessed over

OLE DB and ODBC. For a list of recommended providers, see *Provider Recommendations for External Database Connections* on page 269.

> 📄 **Note:** M-Files Admin only displays OLE DB providers that are available on the computer running M-Files Admin. In case your M-Files Server resides on a different host, ensure that the selected OLE DB connection string works from the computer running M-Files Server as well.

☑ The **Data Link Properties** dialog is opened.

10. On the **Provider** tab, select **Microsoft OLE DB Provider for SQL Server** from the list and click **Next >>**.

> ℹ️ The other providers may have slighlty different options on the **Connection** and **Advanced** tabs. The **All** tab contains all the available connection properties as a name–value table.

☑ The **Connection** tab of the **Data Link Properties** dialog is opened.

11. To the **Select or enter a server name** field, input the name of your SQL Server.

12. For the **Enter information to log on to the server** section, either:

    a. Select the **Use Windows NT Integrated security**.

    or

    b. Enter your credentials to the **User name** and **Password** fields, and check the **Allow saving password** check box.

13. For the **Select the database on the server** section, either:

    a. Use the drop-down menu to select the database on the server you defined above.

    or

    b. Enter a database name to the **Attach a database file as a database name** field and use the **...** button to select a Microsoft SQL Server Database (MDF) file.

14. Optional: Click **Test Connection** to ensure that your database connection is working properly.

15. Optional: On the **Advanced** tab, define a timeout period for the database connection.

16. Click **OK** to close the **Data Link Properties** dialog.

    ☑ The dialog is closed, the **Connection to External Database** tab of the **Objecty Type Properties** dialog is active, and your newly defined connection string is added to the **OLE DB connection string (from server)** field (not included in the screenshot).

17. Back on the **Connection to External Database** tab, enter the SELECT statement for retrieving properties from the database to the **SELECT statement** field.

    ⓘ Examples of SELECT statements:

    ```
    SELECT CustomerNumber, CustomerName FROM Customer

    SELECT ID, Name + ' ' + Department FROM Company

    SELECT ID, Name, CustomerID FROM Contacts

    SELECT * FROM Customer
    ```

18. Click the **Refresh Columns** button to fetch the data defined in your SELECT statement to the **Columns** listing.

    ☑ The **Columns** listing displays correspondences between columns fetched from an external database (**Source Column**) and document vault property definitions (**Target Property**).

19. Map the **Source Column** properties with properties in your M-Files vault (listed in the **Target Property** column).

20. Check the check boxes in the **Update** and **Insert** columns and define the four statements below the **Columns** listing according to the following table:

If you want to...	Complete the following steps:
Allow read-only access	Do not check any of the check boxes and leave the statements empty.
Allow users to update but not create or delete information	1. Check the check boxes in the **Update** column for the properties of your choice. 2. Click the **Default** button next to the UPDATE statement field – or enter your own statements to the field.
Allow users to update, create, and delete information	1. Check the check boxes in the **Update** and **Insert** columns for the properties of your choice. 2. Click the **Default** button next to the UPDATE, INSERT INTO, SELECT, and DELETE statement fields – or enter your own statements to these four fields.

ℹ The table below explains of use the the four statements mentioned above.

Stateme	Definition	Examples

UPDATE	When you edit an object in M-Files, M-Files Server edits the corresponding record in the external database using an UPDATE statement. Use a question mark (?) to signal columns to be updated.	`UPDATE Customers SET CustomerName = ? WHERE CustomerID = ?`
		
		`UPDATE Contact SET Name = ?, CustomerID = ? WHERE ContactID = ?`

INSERT INTO	When you create a new object in M-Files, M-Files Server adds a corresponding record into the external database using an INSERT INTO statement. Use a question mark (?) to indicate the value of each column.
	
	📝 **Note:** The INSERT INTO statement input to M-Files does not define a value for the ID column. The database should be set up to automatically provide an ID for new records. For example in SQL Server databases, set the type of the ID column as identity. In Access databases, use an `AutoNumber` type column for IDs. Because Excel cannot produce new ID values, the INSERT INTO statement cannot be used with Excel.
		`INSERT INTO Customers( CustomerName ) VALUES( ? )`
		
		`INSERT INTO ContactPersons( Name, CustomerID ) VALUES( ?, ? )`

SELECT	After a new record has been created with the INSERT INTO statement, M-Files Server gets the ID of the newly created record with this SELECT statement.	`SELECT MAX( CustomerID ) FROM Customer`

DELETE	When you delete an object from M-Files, M-Files Server deletes the corresponding record in the external database using a DELETE statement. Use a question mark (?) for the ID of the record to be deleted.	`DELETE FROM Customers WHERE CustomerID = ?`
		
		`DELETE FROM Contacts WHERE ContactID = ?`

21. Optional: Check the **Disabled** check box if you would like to temporarily disable the external database connection.

> ⓘ If the connection is disabled, any information between the vault and the external database is not synchronized. The synchronization can be re-enabled at any time by unchecking this check box.

22. Once you are done, click **OK** to close the dialog.

The value list or objects of the object type are now updated to and from an external database according to your connection definition.

Provider Recommendations for External Database Connections

The table below lists the recommended *OLE DB* providers to be used for an external database connection (see).

Database	Provider
MS SQL Server	Microsoft OLE DB Provider for SQL Server.
Access	Microsoft JET OLE DB Provider.
Excel	Microsoft JET OLE DB Provider. Also, set Extended Properties to *"Excel 8.0;"*. Use the *Define name* functionality to define the data area in Excel. This named Excel data area corresponds to a database table. The values in the first row of the data area become the column titles of a table.
MySQL	Microsoft OLE DB Provider for ODBC Drivers (MySQL Connector/ODBC). • Use the Data sources (ODBC) administrative tool to configure a new system data source. • Select MySQL Connector/ODBC as the ODBC driver. • Define the data source. • Under driver properties, select the *Disable Transactions* check box. In connection settings, select Microsoft OLE DB Provider for ODBC Drivers as the provider and the system data source you defined as the data source. The *default collection* in the connection settings remains empty. Thus you only define the database in the driver settings. You can also use MySql.OLEDB Provider with MySQL.

> 📄 **Note:** The Microsoft OLE DB Provider for Jet and the Jet ODBC driver are available in 32-bit versions only. If you need to use either of these in a 64-bit environment for connecting to an external Excel or Access resource, we recommend installing the 64-bit version of *Microsoft Access Database Engine 2010 Redistributable* or running M-Files Server in the 32-bit mode.

Value Lists

A value list contains various values, such as a list of city names. The same value list can be utilized in several different properties.

▶ Video: *Value Lists*

The following example illustrates the significance of value lists:

1. Log in to the *Demo Vault*.
2. Create a new document with the class *Proposal*.
3. When filling in the metadata card, select a value for the *Supplier* property (based on the *Customers* value list). The same value list can be utilized in several properties (for instance *Buyer*).

A value list is one of the M-Files *data types* on page 289. Creating and using value lists makes it significantly faster to specify metadata for a document. In many cases, selecting a value from the list is more sensible than typing it in each time. On the other hand, not all values can reasonably be selected from a list, such as the title of the object.

To view the available value lists in your vault:

1. Open M-Files Admin.
2. Expand the *Document Vaults* node on the left-side tree view.
3. Expand your document vault node.
4. Expand *Metadata Structure (Flat View)*.
5. Select *Value Lists*.

You should now be able to see the available value lists in the right-side listing view. To also display the built-in value lists, click **Show All Value Lists** on the task area.

New Value List

A value list can either be *internal* or *external*.

The contents of an internal value list are saved in the document vault database, meaning that the list is used only inside the document vault. An external value list, on the other hand, can be updated from an external database. In this case, you need to define how the server is to retrieve the value list contents from the other database. For example, an employee database running on an external database server can be connected to the M-Files value lists by defining the database connection. Also refer to *M-Files Server* on page 179.

Creating a New Value List

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand the **Metadata Structure (Flat View)** node and select the **Value Lists** node.

5. Click **New Value List...** on the task area.

   ☑ The **Value List Properties** dialog is opened.

6. In the **Name (singular)** and **Name (plural)** fields, enter the name of the new value list respectively in singular (for example, *Client*) and plural (for example, *Clients*) forms.

7. Optional: Check the **Allow users to add new values to this list** if you want to allow users to add new values to the value list.

8. From the **Default permissions for new values** drop-down menu, select the default permissions for new values in this value list.

9. Optional: Check the **Allow this value list to be used as a grouping level in views** option check box to allow this value list to used for defining a grouping level within a view.

10. Optional: On the **Advanced** tab, set hierarchical relationships for the value list.

   ⓘ See *Advanced (Value List Properties)* on page 278 for more information.

11. Optional: On the **Permissions** tab, you can specify the users who may see this value list or add new values to it.

   ⓘ See *Permissions* on page 281 for more information.

12. Optional: On the **Connection to External Database**, set the connection to an external database for importing value list contents from an external database source.

   ⓘ Connections to external databases for value lists are defined the same way as for object types. See *Connection to External Database (Object Types)* on page 263 for more information.

13. Click **OK** to finish creating the value list.

The new value list is added to the **Value Lists** list.
Converting a Value List to an Object Type

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand the **Metadata Structure (Flat View)** node and select the **Value Lists** node.

5. From the **Value Lists** list, select and highlight the value list that you want to convert to an object type.

6. Click **Convert to Object Type** on the task area.

    ☑ The **Convert to Object Type** dialog appears.

7. You are prompted to confirm that you want to convert the selected value list to an object type. Click **Yes**.

    ⓘ Once you have clicked **Yes**, you cannot undo the conversion.

The selected value list is converted to an object type and removed from the **Value Lists** list and added to the **Object Types** list.

Value List Contents (Individual Values)

You can create new items for the value list as well as new subitems for internally hierarchical values. You can also define hierarchical relationships between value list items (see *Defining a Hierarchical Relationship Between Value Lists* on page 280). Additionally, you can set value-specific permissions as well as default permissions for objects that use the item.
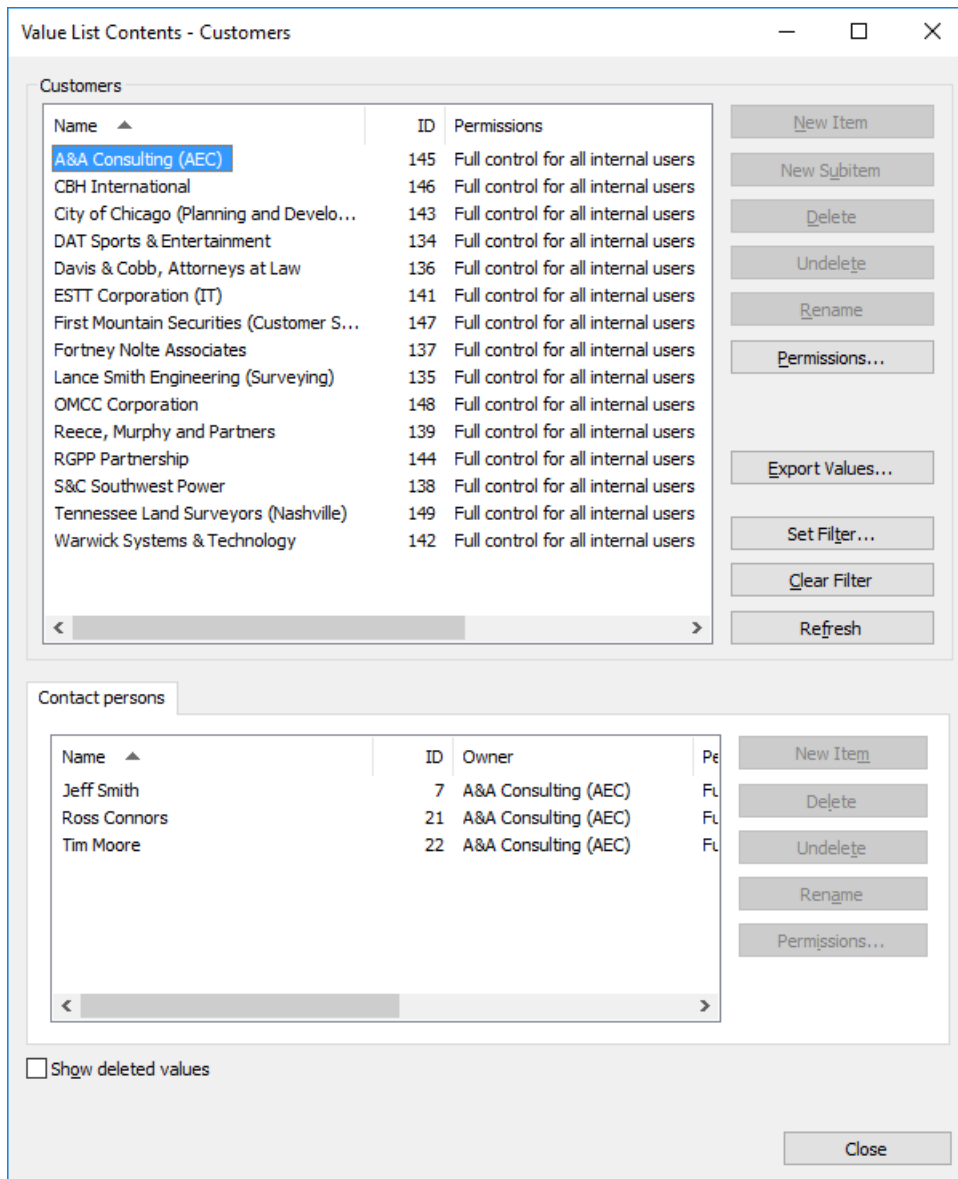
Figure 84: The "Contact persons" value list used as a sublist for the "Customers" value list.

Permissions

Via *Permissions*, you can specify the users who may see this value list item. This way, you can make a value list value to be visible to a specific target group only.

Automatic permissions

The actual final object receives automatic permissions when a value with automatic permissions specified is added for the object.
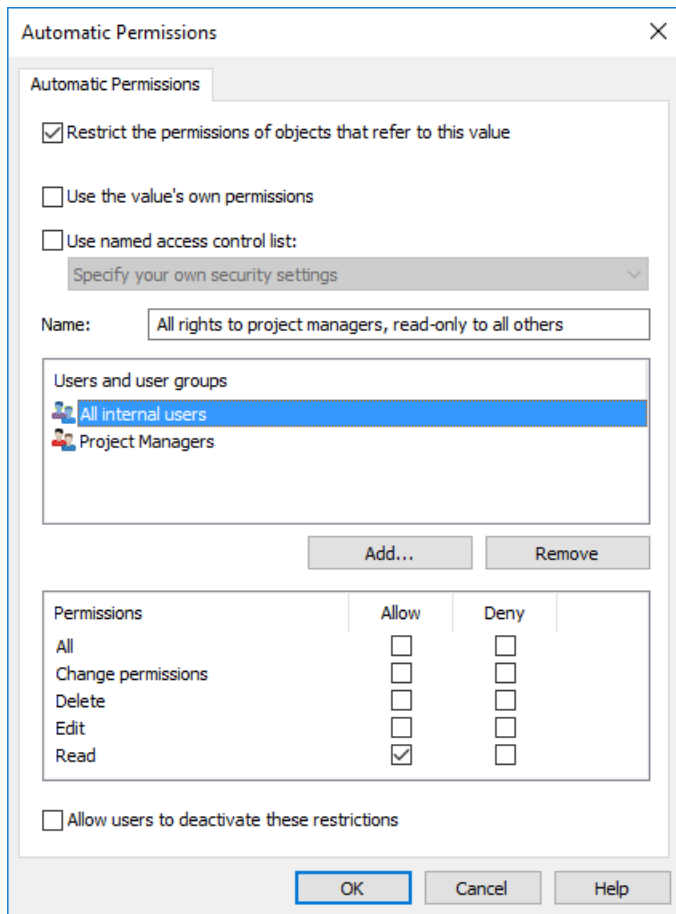
You can activate the automatic permissions by value, value list, object type, or class. For more information, see *Automatic Permissions* on page 275.

Versions older than 8.0: *Default Permissions for Objects* is a tab that enables you to set default permissions for any object that includes this item as a value. This makes it possible to implement permission settings that are based, for example, on the type of project selected.

Adding Values to a Value List

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Metadata Structure (Flat View)** and then select **Value Lists**.

   ☑ The **Value Lists** list is opened in the right pane.

5. Right-click a value list to which you want to add individual values and select **Contents...** from the context menu.

   ☑ The **Value List Contents** dialog is opened.

6. Click the **New Item** button.

   ☑ A new value titled **New Item** is added to the selected value list.

7. Type in an appropriate name for the new value.

   ⓘ You can rename existing values by selecting a value from the list and clicking the **Rename** button.

8. Optional: Click **Permissions...** to specify the users who may see this value list item.

   ⓘ For detailed instructions, see *Permissions* on page 281 and *Automatic Permissions* on page 275.

9. Optional: Click **Change Icon...** to change the icon of the value list item.

   ⓘ In addition to being able to add icons for object types, you can add, change, and remove icons for value list items. This allows you to further increase the clarity of the M-Files user interface. Specific icons can be assigned to, for instance, workflow states and meeting types. Since workflow states can be changed directly with the shortcuts in the task area or from the metadata card, icons can be used to make the states visually more distinguishable. For detailed instructions, see *Changing the Icon of a Value in a Value List* on page 274.

10. Optional: Repeat steps from 6 to 9 to add another value.

11. Click **Close** when you are done.

The new values are added to the selected value list.
Changing the Icon of a Value in a Value List

In addition to being able to add icons for object types, you can add, change, and remove icons for value list items. This allows you to further increase the clarity of the M-Files user interface.

Specific icons can be assigned to, for instance, workflow states and meeting types. Since workflow states can be changed directly with the shortcuts in the task area or from the metadata card, icons can be used to make the states visually more distinguishable.

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Metadata Structure (Flat View)** and then select **Value Lists**.

   ☑ The **Value Lists** list is opened in the right pane.

5. Right-click a value list that you want to edit and select **Contents...** from the context menu.

   ☑ The **Value List Contents** dialog is opened.

6. Select a value from the list and click the **Change Icon...** button.

   ☑ The **Change Icon** dialog is opened.

7. Either:

   a. Select an icon from the list of icons.

      or

   b. Click **Browse...** to browse for a different icon file and then selet an icon from the list of icons.

8. Click **OK** to change the icon and close the **Change Icon** dialog.

9. Repeat the steps from 6 to 8 to change the icon for another value.

10. Click **Close** when you are done to close the **Value List Contents** dialog.

Automatic Permissions

You can use automatic permission settings to pass permissions for an object when the object has a property value, object type or class that uses automatic permissions. The object receives automatic permissions when a value with automatic permissions specified is added for the object.

▶ Video: *Automatic Permissions*

Figure 85: The "Automatic Permissions" dialog for a value list item.

In the above example, automatic permissions have been activated. Read-only access has been granted to all users and a separate access to project managers.

Restrict the permissions of objects that refer to this value

Activate the function *Restrict the permissions of objects that refer to this value* when you want to activate the automatic permissions.

Use the value's own permissions

You can use the permissions of a value or object, such as a project, as automatic permissions.

In this type of case, for example, a plan for a house project would inherit the permissions of the project that is associated with the plan. For example, the *House project Haven* may have its own permissions that allow access for the project manager and project group only. When this project is associated with the house project plan, the same permissions are granted to the plan. The automatic permissions are then the same as the project's own permissions, so definition of separate automatic permissions for the project is not necessary.

> **Note:** Automatic permissions are not inherited indirectly. Let's say we have the object "Hugh Brent" that inherits automatic permissions via the "Look Up Company" property. These permissions are no longer inherited by the "CRM Application Development" object that has "Hugh Brent" as one of its property values.

Name

Give as descriptive a name as possible to the automatic permissions set, because this information will be displayed in the client software.

Specify permissions

You can then specify the automatic permissions that are always activated automatically for the object when a value, object, or class using automatic permissions is added to the object's metadata.

For more information on permissions, see *Permissions* on page 84. Also refer to the specification of pseudo-users in *Pseudo-users* on page 88.

> 📄 **Note:** If you do not explicitly allow any permissions, using this kind of value or object restricts all permissions for the final object.

Allow users to deactivate these restrictions

You can also specify whether the users are allowed to deactivate the automatic permission restrictions created via this value, so that the users can delete the preset automatic permissions if they so desire.

Remarks about using automatic permissions

The specified value providing automatic permissions must be selected on the metadata card for the explicit property definition for which you have enabled automatic permissions. See *Verifying Which Properties Have Automatic Permissions Enabled* on page 278.

> 📄 **Note:** The value-specific settings always have priority over the settings made at value list and object type level.

> 📄 **Note:** For you to be able to use the automatic permissions after you have updated the document vault from version 7.0 to a higher version, the extended metadata-driven permissions must be manually activated vault-specifically. For vaults created in version 8.0 (or higher), the extended automatic permissions are active by default and their activation is not needed. For more information, see *Document Vault Advanced Properties* on page 197.

Enabling Automatic Permissions

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Metadata Structure (Flat View)** and then select **Value Lists**.

   ✅ The **Value Lists** list is opened in the right pane.

5. Right-click a value list that you want to edit and select **Contents...** from the context menu.

   ✅ The **Value List Contents** dialog is opened.

6. Select a value list item that you want to edit and click the **Permissions...** button.

   ✅ The **Permissions** dialog is opened.

7. On the **Automatic Permissions** tab, check the **Restrict the permissions of objects that refer to this value** option check box.

8. Do one of the following:

If you want to	Do the following
Use the existing permissions of the value as automatic permissions	Check the **Use the value's own permissions** option check box.
Use an existing named access control list as automatic permissions	Check the **Use named access control list** option check box and, using the drop-down menu, select a named access control list.
Define new permissions to be used as automatic permissions	In the **Name** field, type in a name for the permissions, click **Add...** to add users or user groups affected by these permissions, and check the appropriate **Allow** or **Deny** option check boxes on the **Permissions** list.

9. Optional: Check the **Allow users to deactivate these restrictions** option check box if you want to give users the option to disable the automatically set permissions and employ user-defined permissions instead.

10. Click **OK** to close the **Permissions** dialog.

11. Click **Close** to close the **Value List Contents** dialog.

The selected value now has automatic permissions defined. When this value is added to the metadata of an object, the object receives the automatic permissions defined for the value.
Verifying Which Properties Have Automatic Permissions Enabled

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the tree view, expand **Metadata Structure (Flat View)**.

5. Select the **Property Definitions** node.

You can see which properties have automatic permissions enabled in the *Automatic Permissions* column of the listing area.

Advanced (Value List Properties)
Value List hierarchy (Value List Properties)

Value lists can have two types of hierarchical relationships:

- *Internal hierarchies withing individual value lists* on page 279
- *Hierarchies between separate value lists* on page 280
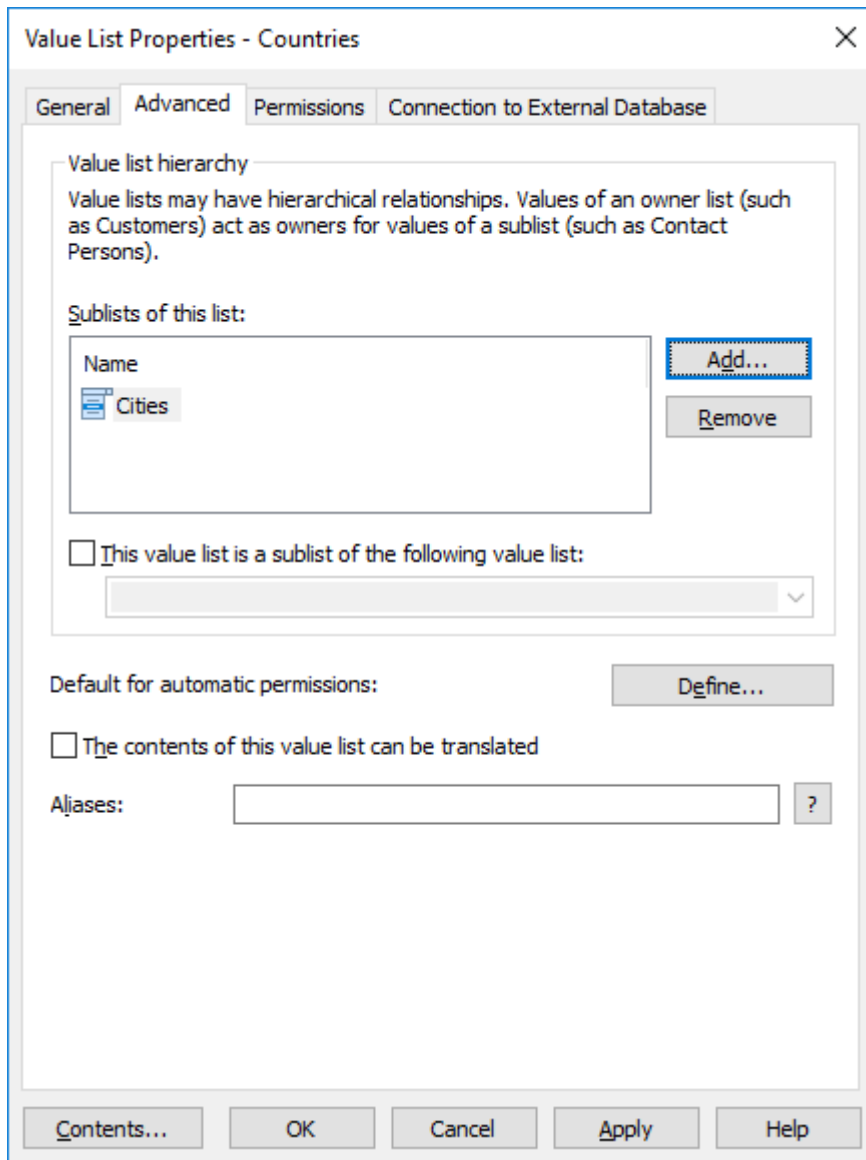
Figure 86: In the advanced settings, various hierarchical relationships can be defined.

Defining an Internal Hierarchy for a Value List

A value list can be *hierarchical in itself*, meaning that it can contain items and subitems. A parent item collects related subitems. This way, you can create, for example, a value list containing all drawing types hierarchically. The parent object can be for instance a floor plan, with floor plans in different scales as its subobjects. Regardless of their internal hierarchy, all items in the hierarchical value list represent the same concept (for example, the parent item *Floor plan* and its subitems *Floor plan 1:100* and *Floor plan 1:50*).

Do the following steps to define an internal hierarchy for a value list:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Metadata Structure (Flat View)** and then select **Value Lists**.

   ✅ The **Value Lists** list is opened in the right pane.

5. Double-click the value list that you want to edit.

   ✅ The **Value List Properties** dialog is opened.

6. Open the **Advanced** tab, and check **This value list is a sublist of the following value list** option check box.

7. Using the drop-down menu, select the **Same list (defines a value list with internal hierarchy)** option.

8. Click the **Contents...** button.

   ✅ The **Value List Contents** dialog is opened.

9. Select an item on the list for which you want to create a subitem and click **New Subitem**.

10. Type in an appropriate name for the new item.

    ℹ️ You can also rename the item later by selecting the item in the list and clicking **Rename**.

11. Optional: If you want to create additional subitems, repeat the steps .

12. Click **Close** when you are ready.

The value list items that you have just created are to the value list as subitems of the selected owner value list items. When you assign a value to a property from the aforementioned value list, you can select a subitem by clicking the down arrow next to a value list item to expand its subitems.
Defining a Hierarchical Relationship Between Value Lists

If a parent item and subitems represent different concepts, such as countries and their cities, separate value lists must be created for the items and the value lists must be defined as two hierarchically related value lists. In such a case, the item in the *Countries* value list (country name) is the owner value for the items in the *Cities* value list. The *Countries* value list is then the higher-level list and the *Cities* list is its sublist.

Do the following steps to define a hierarchical relationship between two value lists:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Metadata Structure (Flat View)** and then select **Value Lists**.

   ✅ The **Value Lists** list is opened in the right pane.

5. Double-click the value list that you want to define as a sublist of a higher-level list.

   ℹ️ Make sure that the property definition using this value list uses automatic filtering. For more information, see .

   ✅ The **Value List Properties** dialog is opened.

6. Open the **Advanced** tab, and check **This value list is a sublist of the following value list** option check box.

7. Using the drop-down menu, select the value list that you want to set as the owner of this value list.

8. Click **OK** to save your changes and close the **Value List Properties** dialog.

9. In the **Value Lists** list, find the value list that you have just set as the owner of the previous value list, right-click it, and select **Contents...** from the context menu.

    ☑ The **Value List Contents** dialog is opened.

10. In the upper list, select the owner item for which you want to add a subitem.

11. Next to the lower list, click **New Item**.

    ☑ A new value list item is added to the lower list.

12. Type in an appropriate name for the new subitem.

    ⓘ You can also rename the item later by selecting the item in the list and clicking **Rename**.

13. Optional: If you want to create additional subitems, repeat the steps from *10* on page 281 to *12* on page 281.

14. Click **Close** when you are ready to save your changes and close the **Value List Contents** dialog.

The selected value list is defined as a sublist of the selected owner value list. When you assign a value to a property from the owner value list in M-Files, you can then also assign any associated subvalues from the sublist, if you so wish.

Default for automatic permissions (Value List Properties)

You can activate the automatic permissions by value, value list, object type, or class. You can specify the automatic permissions for each value list in the same way as for each value. The automatic permissions are attached to an object when a value with automatic permissions is added for the object. For more information, see *Automatic Permissions* on page 275.

📄 **Note:** The value-specific settings always have priority over the settings made at value list and object type level.

The contents of this value list can be translated (Value List Properties)

Enable this option to allow the contents of the selected value list to be translated to different languages. For more information, see *Languages and Translations* on page 231.

Aliases (Value List Properties)

Using the **Aliases** field, you can define an alias for the value list. For more information, see *Associating the Metadata Definitions* on page 203.

Permissions

Access for viewing this value list and creating items to the list can be defined on the *Permissions* tab.

If the user does not have the permission to view the name of the value list, it is not available for selection in M-Files (for example, when you are creating a new search).

If the user cannot see the value list, the user does not have the permission to create items to it either. However, the user may have the permission to see the list without having the permission to create new items.

Adjusting Permissions

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight the appropriate node or subnode of the vault and select the desired item from the list on the right.

5. Right-click the item and select **Properties** from the context menu.

6. Go to the **Permissions** tab.

7. From the **Users and user groups** list, select the user or user group whose permissions you want to adjust.

> ⓘ If the user or user group is not on the list, click **Add...** to add the user or user group to the list.

8. Either:

    a. Check the **Allow** check box to allow the selected user to see this item.

    or

    b. Check the **Deny** check box to deny the selected user from seeing this item.

9. Optional: If you want to adjust additional permissions, repeat the steps 7 and 8.

10. Click **OK** once you are done.

You have adjusted the view permissions of the selected item for the selected users.

Connection to External Database (Value Lists)

▶ Video: *Importing from Databases*

You can set M-Files to update any object type or a value list to and from an external database.

The example below describes how to define an object type to use an external database connection to SQL Server. The steps for specifying an external database connection for a value list are very similar.

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand the **Metadata Structure (Flat View)** node.

5. Select the **Object Types** node (or the **Value Lists** node if you are defining a value list to use an external database connection).

    ☑ The object type (or value list) listing is opened in the right pane.

6. In the right-pane listing, right-click the object type (or value list) of your choice and select **Properties** from the context menu.

7. Select the **Connection to External Database** tab.

    ☑ The **Connection to External Database** tab is opened.

8. Enable the option **Use a connection to an external database to import and modify objects that reside in the external database**.

9. Click the **Define...** button next to the **OLE DB connection string (from server)** field.

   ⓘ The syntax of the connection string depends on the *OLE DB* (Object Linking and Embedding Database) supplier used for establishing the connection to the external database. If Open Database Connectivity (*ODBC*) is required to establish a connection, the data store has to be accessed over OLE DB and ODBC. For a list of recommended providers, see *Provider Recommendations for External Database Connections* on page 269.

   📄 **Note:** M-Files Admin only displays OLE DB providers that are available on the computer running M-Files Admin. In case your M-Files Server resides on a different host, ensure that the selected OLE DB connection string works from the computer running M-Files Server as well.

   ✅ The **Data Link Properties** dialog is opened.

10. On the **Provider** tab, select **Microsoft OLE DB Provider for SQL Server** from the list and click **Next >>**.

ⓘ The other providers may have slighlty different options on the **Connection** and **Advanced** tabs. The **All** tab contains all the available connection properties as a name–value table.

☑ The **Connection** tab of the **Data Link Properties** dialog is opened.

11. To the **Select or enter a server name** field, input the name of your SQL Server.

12. For the **Enter information to log on to the server** section, either:

    a. Select the **Use Windows NT Integrated security**.

    or

    b. Enter your credentials to the **User name** and **Password** fields, and check the **Allow saving password** check box.

13. For the **Select the database on the server** section, either:

    a. Use the drop-down menu to select the database on the server you defined above.

    or

    b. Enter a database name to the **Attach a database file as a database name** field and use the **...** button to select a Microsoft SQL Server Database (MDF) file.

14. Optional: Click **Test Connection** to ensure that your database connection is working properly.

15. Optional: On the **Advanced** tab, define a timeout period for the database connection.

16. Click **OK** to close the **Data Link Properties** dialog.

    ☑ The dialog is closed, the **Connection to External Database** tab of the **Objecty Type Properties** dialog is active, and your newly defined connection string is added to the **OLE DB connection string (from server)** field (not included in the screenshot).

Object Type Properties - New Object Type   ×

General | Advanced | Permissions | Connection to External Database

☑ Use a connection to an external database to import and modify objects that
reside in the external database.

OLE DB connection string (from server):

[   ] [Define...] [?]

SELECT statement:

[   ] [?]

[Refresh Columns   ]

Columns:

Source Column	Target Property	Update	Insert	

If you want to allow users to modify the data in the external database from
within M-Files, specify the SQL statements that M-Files Server can use to create,
modify, or delete records in the external database:

UPDATE statement for modifying an existing record:

[   ] [Default] [?]

INSERT INTO statement for creating a new record:

[   ] [Default] [?]

SELECT statement for getting the ID of the new record after insertion:

[   ] [Default] [?]

DELETE statement for deleting a record:

[   ] [Default] [?]

☐ Disabled

[Contents...]   [OK]   [Cancel]   [Apply]   [Help]

17. Back on the **Connection to External Database** tab, enter the SELECT statement for retrieving properties from the database to the **SELECT statement** field.

ⓘ Examples of SELECT statements:

```
SELECT CustomerNumber, CustomerName FROM Customer

SELECT ID, Name + ' ' + Department FROM Company

SELECT ID, Name, CustomerID FROM Contacts

SELECT * FROM Customer
```

18. Click the **Refresh Columns** button to fetch the data defined in your SELECT statement to the **Columns** listing.

☑ The **Columns** listing displays correspondences between columns fetched from an external database (**Source Column**) and document vault property definitions (**Target Property**).

19. Map the **Source Column** properties with properties in your M-Files vault (listed in the **Target Property** column).

20. Check the check boxes in the **Update** and **Insert** columns and define the four statements below the **Columns** listing according to the following table:

If you want to...	Complete the following steps:
Allow read-only access	Do not check any of the check boxes and leave the statements empty.
Allow users to update but not create or delete information	1. Check the check boxes in the **Update** column for the properties of your choice. 2. Click the **Default** button next to the UPDATE statement field – or enter your own statements to the field.
Allow users to update, create, and delete information	1. Check the check boxes in the **Update** and **Insert** columns for the properties of your choice. 2. Click the **Default** button next to the UPDATE, INSERT INTO, SELECT, and DELETE statement fields – or enter your own statements to these four fields.

ℹ The table below explains of use the the four statements mentioned above.

Stateme	Definition	Examples

UPDATE	When you edit an object in M-Files, M-Files Server edits the corresponding record in the external database using an UPDATE statement. Use a question mark (?) to signal columns to be updated.	`UPDATE Customers SET CustomerName = ? WHERE CustomerID = ?`
		
		`UPDATE Contact SET Name = ?, CustomerID = ? WHERE ContactID = ?`

INSERT INTO	When you create a new object in M-Files, M-Files Server adds a corresponding record into the external database using an INSERT INTO statement. Use a question mark (?) to indicate the value of each column.
	
	📝 **Note:** The INSERT INTO statement input to M-Files does not define a value for the ID column. The database should be set up to automatically provide an ID for new records. For example in SQL Server databases, set the type of the ID column as identity. In Access databases, use an `AutoNumber` type column for IDs. Because Excel cannot produce new ID values, the INSERT INTO statement cannot be used with Excel.
		`INSERT INTO Customers( CustomerName ) VALUES( ? )`
		
		`INSERT INTO ContactPersons( Name, CustomerID ) VALUES( ?, ? )`

SELECT	After a new record has been created with the INSERT INTO statement, M-Files Server gets the ID of the newly created record with this SELECT statement.	`SELECT MAX( CustomerID ) FROM Customer`

DELETE	When you delete an object from M-Files, M-Files Server deletes the corresponding record in the external database using a DELETE statement. Use a question mark (?) for the ID of the record to be deleted.	`DELETE FROM Customers WHERE CustomerID = ?`
		
		`DELETE FROM Contacts WHERE ContactID = ?`

21. Optional: Check the **Disabled** check box if you would like to temporarily disable the external database connection.

   ℹ If the connection is disabled, any information between the vault and the external database is not synchronized. The synchronization can be re-enabled at any time by unchecking this check box.

22. Once you are done, click **OK** to close the dialog.

The value list or objects of the object type are now updated to and from an external database according to your connection definition.

Property Definitions

Property definitions are used to determine properties associated with *classes.* A property definition is used to define the property name (which should be descriptive) and data type, which determines the type of the data entered (in relation to the property).

Various properties can be combined to create classes; refer to *Classes* on page 307. For example, *Contract of Employment* is a document class with the associated properties *Title*, *Document Date*, *Employee*, *Keywords* and *Description*.

The property definitions are used for determining the metadata on the metadata card. The properties that are associated with the document class are displayed on the metadata card after class selection.

New Property Definition

In a new property definition, you need to specify the data type after assigning a name to the property. For example, if you are creating a property with the name "Document Date," the logical data type choice is "Date".

Figure 87: The "New Property Definition" dialog.

Property definition data types

Text	Any typed text, for instance, a heading.
Text (multi-line)	Any typed text. The text can have multiple lines.
Choose from list	You can select one value from the options on the value list.
Choose from list (multi-select)	You can select several values from the options on the value list.
Date	You can select a date. As a default, M-Files suggests the current date.
Time	You can select a time.
Timestamp	This data type can be used for generating a timestamp with a script. 📄 **Note:** The timestamp needs to be defined as a calculated value. Go to the **Automatic Values** tab of the **Property Definition Properties** dialog and select the **Calculated value (VBScript)** option and click **Edit Code...** to add the VBScript code for generating the timestamp.
Number (integer)	You can enter the desired integer.
Number (real)	You can enter the desired real number.
Boolean (yes/no)	You can specify the Boolean value *yes* or *no* for the desired variable.

The data type indicates the type of the property. For example, if you create a new property named *Confidential* and specify *Boolean (yes/no)* as its data type, you need to select *yes* or *no* when filling in the *Confidential* field on the metadata card. This happens only if the property *Confidential* has been associated with the document class (*Report*, *Memo*, *Agenda*, etc.) to which the document you are creating belongs.

After creating this property, you can create a new view that lists the documents on the basis of whether they are confidential or not. You can group the documents into the *Yes* and *No* property folders by using the view hierarchy.

Value lists can be efficiently utilized in property definitions. For example, the *Customers* value list is utilized in several property definitions in the M-Files sample vault.

When specifying, for example, the *Author Organization*, the options are retrieved from the *Customers* value list, to which you can easily add new values (customers). This way, the same company names need not be entered again, but the existing list can be utilized instead. The lists decrease the number of input errors and make work more efficient.

Pre-filtering of properties

You can specify pre-filtering for property definitions to show a subset of the objects. This way, the list of objects to be displayed can be limited by certain criteria, and the user can more quickly find the desired object when, for example, adding a customer to the metadata card.

For example, pre-filtering can be used to divide:

- Customers into prospective and actual customers.
- Customers into buyers and suppliers.
- Customers into persons and companies.
- Projects into internal and external projects.
- Projects into current and past projects.

The customer class may also be used as a pre-filter for customer listing. Likewise, the project class, for example, may be used as a pre-filter for a project listing.

Filter the list by using the value of the following property

A property definition using a value list that is filtered by some other value list can be defined to be filtered by some other property definition that uses the main value list of the filtered one. This is a case of dynamic filtering, which depends on what the user selects in the metadata card.

Example: The properties *Customer (Buyer)* and *Customer's Contact Person* are filled in the metadata card. Selecting the correct *Customer (Buyer)* also filters values available in the *Customer's Contact Person* value list to show only contact persons of this selected customer. The *Customer (Buyer)* property may use the *Customers* value list and *Customer's Contact Person* may use the *Contact Persons* value list. The *Contact Persons* value list is filtered by customer.

In addition, the *Customer (Buyer)* property is defined to be filtered by the *Buyer* property. For more information about hierarchical relationships between value lists and object types, refer to *Value Lists* on page 269 and *Object Types* on page 259.

Also, you can select an *automatic filter* allowing M-Files to search for the best metadata card filter selection to filter the property in question. In this case, for example, the two-way filtering of value lists between ZIP codes and cities functions in a user-friendly manner: In the metadata card, you can choose a ZIP code first, and M-Files then chooses an appropriate city from the list automatically. If you choose the city first, M-Files filters the available ZIP codes automatically according to the city.

Sort values in the list in the following order

You can define whether you want the value list used for the property definition to be ascending or descending.

Allow using this property with the following object type

You can also limit the use of this functionality to just one object type.

Enable automatic permissions via this property

For you to be able to use the automatic permissions via a specific property, you should allow this in the property definition's properties. For the *Class* property definition, the automatic permissions are active by default, so activation is not needed in this case.

When you have added automatic permissions to a value, value list or object type, M-Files will display the property definitions in which the automatic permissions are enabled and those in which they are disabled. Make sure that the automatic permissions are enabled for the desired property definition.

Note that the specified value must be selected for the explicit property definition for which you have enabled automatic permissions.

Allow this property to be used as a grouping level in views

Enable this option to allow the property to be used for defining a grouping level within a view. It is advisable to disable this option for properties that may contain classified information.

Aliases (Advanced tab)

Via the *Advanced* tab, you can define an alias for the property definition. For more information, see *Associating the Metadata Definitions* on page 203.

Creating a New Property Definition

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Metadata Structure (Flat View)** and then select **Property Definitions**.

   ☑ The **Property Definitions** list is opened in the right pane.

5. Click **New Property Definition...** on the task pane.

   ☑ The **Property Definition Properties** dialog is opened.

6. In the **Name** field, enter a name for the new property definition.

   ⓘ The name will be displayed on the metadata card when you add this property to the metadata card.

7. Use the **Data type** drop-down menu to select the data type for the new property definition.

   ⓘ For more information on data types, see *Property definition data types* on page 289.

8. Optional: If you chose **Text** or **Text (multi-line)** as the data type, select a content type for the text data type using the **Content** drop-down menu.

9. Optional: If you chose **Choose from list** or **Choose from list (multi-select) as the data type,** carry out the steps from *9.a* on page 291 to *9.d* on page 291:

   a) Use the **Show values from the following list** drop-down menu to select the value list from which a value is to be chosen for the property.

      ⓘ You can also filter the values in the value list by clicking **Filter...** and specifying the conditions that must be met in order for a value list item to be a selectable value for the property.

   b) Use the **Filter the list by using the value of the following property** drop-down menu to select the property by which available values are filtered. If you do not want to filter the values, select **(no filtering)**.

      ⓘ For more information, see *Filter the list by using the value of the following property* on page 290.

   c) Use the **Sort values in the list in the following order** drop-down menu to select the sorting order for the values.

   d) Check the **Enable automatic permissions via this property** option check box if you want to allow automatic permissions for this property.

      ⓘ For more information, see *Automatic Permissions* on page 275.

10. Use the **Allow using this property with the following object type** drop-down menu to select the object type that this property is used with, or select the **All object types** option if you do not want to restrict the use of this property to a specific object type.

11. Optional: Check the **Allow this property to be used as a grouping level in views** option check box to allow this property to be used for defining a grouping level within a view.

    ⓘ It is advisable to disable this option for properties that may contain classified information.

The new property definition that you have just defined is added to the **Property Definitions** list and the property can be added to the metadata of objects in M-Files.

Automatic Values

An **automatic value** can be set for a property. This means that, for example, invoices can be consecutively numbered. An automatic value can also contain text, in which case it is a combination of other properties. For example, to create proposal headings in a set format such as *Class/Product/Customer*, these properties (*Proposal/Mach20A/ESTT Corporation*) can be used to automatically create the headings.

Automatic values offer increased utilization of document and object metadata in storing and searching for information. In addition, using automatic values makes the naming of documents and objects more consistent and reduces the need for repeated data entries.

Automatic values are especially useful for naming objects (for more information, refer to *New Class* on page 308) and in automatically including metadata in document content (for more information, refer to *Insert M-Files Property* on page 163).

Automatic numbers and values

A property can have an automatic number or value. An **automatic number** is calculated once and it does not change. Such automatic numbering is useful, for instance, in various company internal processes and record-keeping.

An automatic value can contain other properties, usually by concatenating two or more properties. For example, a document name (automatic value) can be defined as *Class (Customer)*, which would return, for instance, *Proposal (ESTT)*. The automatic value changes when the object is edited. If the automatic value is created using the class and customer name *(Proposal (Customer A))*, the automatic value changes when another customer is selected *(Proposal (Customer B))*.

Figure 88: Property definition with automatic numbering.

The example above illustrates a property with consecutive numbering in single whole number increments (increment: 1). The last value used is set as 1000. Thus, the next object to use this property will be numbered as 1001. The calculation order value is 100 (see *Calculation order* below).

Simple automatic numbering

Generates an incrementing numerical value. The increment can also be specified (*Increment*). The default value is one (1).

Customized automatic numbering (VBScript)

Generates an automatic number that can contain letters and/or numbers. Creating a customized automatic number is specified in more detail by using the M-Files API and generic features of VBScript. For more information, refer to *Specifying an Automatic Property Value Using VBScript* on page 296.

The following M-Files variables can be used with this script: `PropertyDef`, `Output`, `LastUsed`, `ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `PropertyValues`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`. For more information about the variables, refer to *VBScript Variables Explained* on page 402.

Simple concatenation of properties

Conjoins selected properties (for instance *Proposal/Device/Customer*). Any characters or text can be inserted between the selected properties. For example: *Proposal: Customer (Project)* or *Proposal, Customer, Project*.

A list of available placeholders can be opened when specifying an automatic value for a property. The **Add Placeholder…** button opens the list of property definitions and other placeholders available for use.

Alternatively, you can add the placeholders to the field manually. They are used by bracketing them with *%* characters. For instance, `%PROPERTY_23% (%PROPERTY_21%)` could give us "John Smith (09/25/2016 12:39 PM)", assuming that *23* is the ID for the *Last modified by* property and *21* the ID for the *Last modified* timestamp property.

Indirect placeholders

Indirect placeholders are metadata indirectly related to an object. For example, if a contract is related to a customer object, the country of the customer is indirect metadata for the document.

To specify the customer's country as an indirect placeholder the syntax `%PROPERTY_1079.PROPERTY_1090%` is used, where *1079* is the property definition ID for *Customer* and *1090* is the property definition ID for *Country*.

Calculated value (VBScript)

Creating an automatic value can be specified in more detail by using the M-Files API and generic features of VBScript. A calculated value is defined for the property. For more information about defining calculated values, refer to *Specifying an Automatic Property Value Using VBScript* on page 296.

The following M-Files variables can be used with this script: `PropertyDef`, `Output`, `ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `PropertyValues`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`. For more information about the variables, refer to *VBScript Variables Explained* on page 402.

▶ Video: *Calculated Value*

Last value used

The starting value for consecutive numbering or values. The default is zero (0). The value can be changed; for example, consecutive numbering can start at *3000*.

Calculation order

Calculation order determines the order in which automatic values are calculated (from smallest to greatest). This is significant when several automatic values are used and their combinations form new automatic values.

For example, calculation order is crucial if the name of an object is an automatic property value consisting of two other automatic values. These two automatic values should be calculated first and their combined value afterward.

The values themselves make no difference other than that the calculation order proceeds from smallest to greatest. The calculation order values for different properties can be, for example, 10, 12, 17 and 20. The property with the calculation order number 10 is thus calculated first, followed by the property with the calculation order number 12, and so on.

▶ Video: *Calculation Order*

Recalculate

The *Recalculate* function is available in M-Files Admin's task area (or by right-clicking) when a property with an automatic value is selected.

Recalculate Empty Values

Calculates automatic values for properties that have not been calculated yet. This is the default for calculating automatic values. Changes to settings only apply to new values. For example, if you edit the *Last value used*, only new objects will have the new value. Old values are preserved; that is, once defined, a value does not change.

Recalculate All Values

Recalculates the automatic values of all properties. *Recalculate All Values* thus also recalculates previously defined values. For example, if consecutive numbering is used and the *Last value used* is changed, this function renumbers all existing objects.

Naming a template without using automatic values

Document templates work differently when automatic values are used. All properties in the template metadata work without the calculation of an automatic value. Thus, in templates, automatic property values work as if they were not automatic. Their values can be defined normally and the server does not calculate an automatic value for the property.

For example, objects in the *Proposal* class may use automatic values in their titles (such as *Proposal <number> - <customer name>*). However, it makes sense to name the *Proposal* class templates as templates; titles using automatic properties only make sense for actual proposals, not templates. Thus, the template might be called *Proposal Template*, while the actual proposal documents created using the template will have names formulated with automatic values, such as *Proposal 35 - ESTT*.

For more information, refer to *Use Template* on page 80 and *New Class* on page 308.

Specifying an Automatic Value for a Property

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Metadata Structure (Flat View)** and then select **Property Definitions**.

   ☑ The **Property Definitions** list is opened in the right pane.

5. Double-click the property definition that you want to edit.

   ☑ The **Property Definition Properties** dialog is opened.

6. Go to the **Automatic Values** tab, and select one of the following:

If you want to	Do the following
Specify automatic incremental numbering for a property.	Select the **Simple automatic numbering** option, and specify the size of the increment for each new value in the **Increment** field.
Specify for a property customized automatic numbering using VBScript.	Select the **Customized automatic numbering (VBScript)** option, and click **Edit Code...** to add the code for automatic numbering. 📄 **Note:** For more information, see *Specifying an Automatic Property Value Using VBScript* on page 296.
Specify a combination of text and property placeholders as an automatic property value.	Select the **Simple concatenating of properties** option, and enter the combination of text and property placeholders in the text field. You can add property placeholders by clicking the **Add Placeholder...** button.

If you want to	Do the following
	📄 **Note:** For more information on placeholders, see *Simple concatenation of properties* on page 293.
Specify for a property an automatic calculated value using VBScript.	Select the **Calculated value (VBScript)** option, and click **Edit Code...** to add the code for calculating the property value. 📄 **Note:** For more information, see *Specifying an Automatic Property Value Using VBScript* on page 296.

7. Optional: In the **Last value used** field, enter the starting value for automatic numbering if you want to use some other value than the default zero (0).

8. In the **Calculation order** field, enter the number that determines the order in which this automatic value is calculated in relation to other automatic values. The smaller the number, the earlier the calculation order.

   ⓘ For more information, see *Calculation order* on page 294.

9. Click **OK** to save your changes and close the **Property Definition Properties** dialog.

The selected property now has an automatic value. When you add this property to the metadata card, the value is calculated and generated automatically.

Specifying an Automatic Property Value Using VBScript

Creating customized automatic values and calculated values can be specified in more detail by using M-Files API and generic features of VBScript ("Microsoft Visual Basic Scripting Edition"). This section provides instructions for using VBScript with automatic values.

📄 **Note:** For the VBScript user's guide and language reference, see the *VBScript* MSDN article.

The VBScript code for a calculated value is executed whenever a property value is edited. The VBScript code is used for calculating the automatic value, after which the result of the calculation must be assigned to a variable called *Output*. This value is stored as the value of the property in the object metadata.

The simplest piece of VBScript for formulating an automatic value might therefore look like this:

```
Output = "Automatic value"
```

Usually an automatic value uses other object properties, for example, by concatenating them. VBScript code can utilize the property values and basic information of the same or another object with the aid of the following VBScript variables:

- `CurrentUserID`
- `DisplayID`
- `LastUsed`
- `MFScriptCancel`

- `ObjVer`
- `Output`
- `PropertyDef`

- `PropertyValues`
- `Vault`
- `VaultSharedVariables`

For the variable descriptions, see *VBScript Variables Explained* on page 402.

Do the following steps to use VBScript for calculating an automatic value for a property:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Metadata Structure (Flat View)** and then select **Property Definitions**.

   ☑ The **Property Definitions** list is opened in the right pane.

5. Double-click the property definition that you want to edit.

   ☑ The **Property Definition Properties** dialog is opened.

6. Go to the **Automatic Values** tab.

   ☑ The **Automatic Values** tab is opened.

7. Select either:

   a. **Customized automatic numbering (VBScript)**: Select this option if you want to define automatic numbering using VBScript.

   or

   b. **Calculated value (VBScript)**: Select this option if you want to define any other type of automatic value using VBScript.

8. Click the **Edit Code...** button.

   ✓ The **Edit VBScript Code** window is opened.
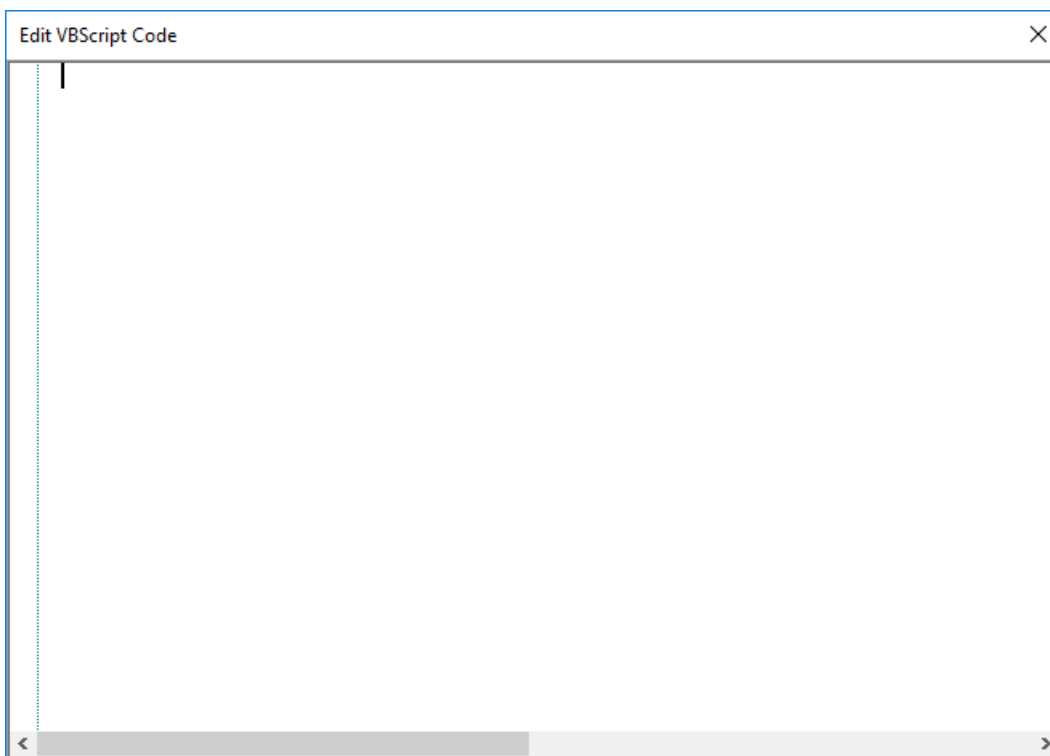
Edit VBScript Code   ✕

9. Specify the VBScript code for calculating the automatic value.

✎ For example, the following code creates an automatic value for the *"Proposal Title"* property by utilizing the proposal number and customer information in the object metadata. The ID of the *Proposal Number* property is 1156 and the ID of the *Customer* property is 1288. If a document has the proposal number 5577 and the customer is ESTT, the code below creates the following string as the title of the proposal: *"Proposal #5577 / ESTT"*.

```vbscript
Option Explicit

' Get proposal number.

Dim szNumber
szNumber = PropertyValues.SearchForProperty( 1156
 ).TypedValue.DisplayValue

' Get customer.

Dim szCustomer
szCustomer = PropertyValues.SearchForProperty( 1288
 ).TypedValue.DisplayValue

' Create proposal title.

Dim szName
szName = "Proposal #" & szNumber & " / " & szCustomer

' Set result.

Output = szName
```

10. Close the **Edit VBScript Code** window once you are done.

11. Back in the **Property Definition Properties** dialog, click **OK** to save your changes and to close the **Property Definition Properties** dialog.

The selected property now has an automatic value which is calculated by the VBScript code that you have specified.

Automatically Validating Property Values

On the **Validation** tab of the **Property Definition Properties** dialog, you can define the criteria that the values of a specific property should meet. For example, with validation you can ensure that the property value contains a required number of characters. In this way, you can verify that the customer phone number or invoice number is added correctly on the metadata card. You can also validate that, for instance, the value can be accepted in relation to other properties or that the value is not empty.

Validation is specified by using variables, generic features of VBScript, and M-Files API. The following M-Files variables can be used for validating property values: `PropertyDef`, `PropertyValue`, `ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`. For more information about the variables, refer to *VBScript Variables Explained* on page 402.

Complete the following steps to add value validation for a property:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Metadata Structure (Flat View)** and then select **Property Definitions**.

5. Either:

   a. In the **Property Definitions** list, right-click the property, the values of which you want to be automatically validated, and select **Properties** from the context menu.

   or

   b. Click **New Property Definition...** on the task area to create a new property definition with automatic value validation.

   ☑ The **Property Definition Properties** dialog is opened.

Property Definition Properties - New Property Definition   ✕

| General | Automatic Values | Validation | Permissions | Advanced |

Name: Document Date

Data type: Date

Content:

Show values from the following list:

     Filter...

Filter the list by using the value of the following property:

Sort values in the list in the following order:

Allow using this property with the following object type:

All object types

☐ Enable automatic permissions via this property

☑ Allow this property to be used as a grouping level in views

     OK   Cancel   Apply   Help

6. Go to the **Validation** tab.

   ✓ The **Validation** tab is opened.

Property Definition Properties - New Property Definition   ✕

| General | Automatic Values | Validation | Permissions | Advanced |

You can specify criteria that the values of this property must meet.

◉ No validation

○ Validation with VBScript

     Edit Code...

     OK   Cancel   Apply   Help

7. Select the **Validation with VBScript** option and click the **Edit Code...** button.

✓ The **Edit VBScript Code** window is opened.
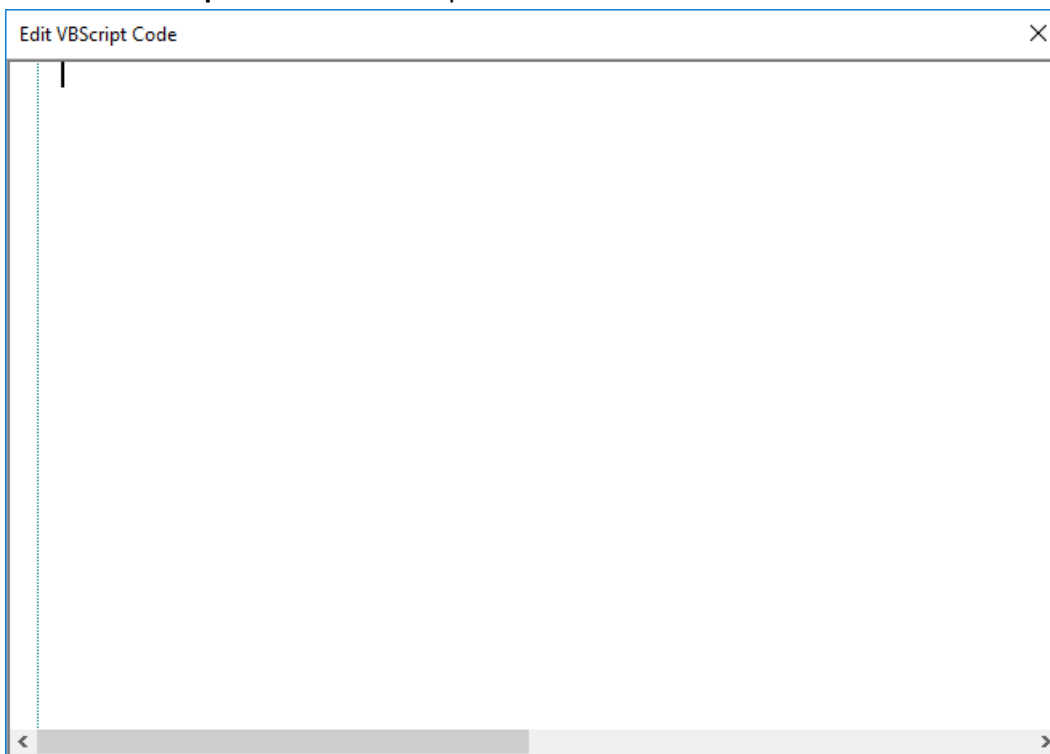
8. In the **Edit VBScript Code** window, type in the VBScript code for validating the values of this property.

✏ For example, if the values of this property must have at least 10 characters, you could use the following code:

```
Option Explicit

Dim propertyName, value

propertyName = PropertyDef.Name

value = PropertyValue.GetValueAsUnlocalizedText

If Len(value) < 10 Then

    Err.Raise MFScriptCancel, "The property """ + propertyName + """ must
 have a value of at least 10 characters."

End If
```

📄 **Note:** The documentation for the M-Files API is located in **Start** > **Programs** > **M-Files** > **Documentation** > **M-Files API**. For more information about VBScript code and M-Files API, go to *www.m-files.com/api*. Instructions on writing VBScript code and working with the M-Files API are available for a separate fee from M-Files customer support (*support@m-files.com*).

9. Close the **Edit VBScript Code** window and then click **Apply** in the **Property Definition Properties** dialog to save your changes.

The values entered for the selected property are now automatically validated. When entering a value for the property on the metadata card, the value is validated and if it does not meet the criteria specified, the action specified in the validation script is executed (such as displaying an error message).

Built-in Property Definitions

The table below lists the descriptions for built-in property definitions that come included in the metadata structure of every vault implementation. These property definitions are essential elements of every vault metadata structure, and therefore modifying these definitions is restricted by design.

Built-in Property Definition	Data type	Description
Accessed by me	Timestamp	The last time the object was accessed by the current user.
Additional classes	Choose from list "Classes" (multi-select)	A list of additional classes for the object.
Assigned to	Choose from list "Users" (multi-select)	A list of users to whom an assignment is assigned.
Assignment	Choose from list "Assignments" (multi-select)	An assignment related to the selected object.
Assignment description	Text (multi-line)	The assignment description for an assignment.
Class	Choose from list "Classes"	The class of the object.
Class groups	Choose from list "Class groups" (multi-select)	The class group of the object.
Collection members (document collections)	Choose from list "Document collections" (multi-select)	A list of document collections belonging to the document collection.
Collection members (documents)	Choose from list "Documents" (multi-select)	A list of documents belonging to the document collection.
Comment	Text (multi-line)	Comment text for an object.
Completed	Boolean (yes/no)	Specifies whether the assignment has been completed.
Conflict resolved	Timestamp	The date and time a conflict was last resolved in favor of the selected object.
Created	Timestamp	The creation date and time of an object.
Created by	Choose from list "Users"	Identifies the user who created the object in M-Files or imported the object into M-Files.
Created from external source	Choose from list "External sources"	The external source from which the object was imported.
Deadline	Date	The deadline date for the current assignment.
Deleted	Timestamp	The deletion date and time of the object.

Built-in Property Definition	Data type	Description
Deleted by	Choose from list "Users"	Identifies the user who deleted the object.
Deletion status changed	Timestamp	The date and time the object was last deleted or undeleted.
Document	Choose from list "Documents" (multi-select)	A document related to the selected object.
Document collection	Choose from list "Document collections" (multi-select)	A document collection related to the selected object.
Favorite view	Number (integer)	The ID of the *Favorites* view where the object is shown.
Is template	Boolean (yes/no)	A Boolean property identifying whether the object is a template.
Last modified	Timestamp	The last modification date and time of an object.
Last modified by	Choose from list "Users"	Identifies the user who last modified the object.
Marked as complete by	Choose from list "Users" (multi-select)	A list of users who have completed the current assignment.
Marked as rejected by	Choose from list "Users" (multi-select)	A list of users who have rejected the current assignment.
Marked for archiving	Boolean (yes/no)	A Boolean property identifying whether the object is marked for archiving.
Message ID	Text	The Message-ID value of an e-mail extracted from the Internet header.
Monitored by	Choose from list "Users" (multi-select)	A list of users who are monitoring the current assignment.
Moved into current state	Timestamp	The date and time when the object was moved to its current state.
Name or title	Text	The name of title of the current object.
Object changed	Timestamp	The date and time of the last change to the object.
Original path (1/3)	Text	The location from which the object was imported to M-Files.
Original path (2/3)	Text	The location from which the object was imported to M-Files (continued).
Original path (3/3)	Text	The location from which the object was imported to M-Files (continued).
Owner (Assignment)	Choose from list "Assignments"	The owner value of the selected object.

Built-in Property Definition	Data type	Description
Owner (Class group)	Choose from list "Class groups"	The owner value of the selected object.
Owner (Class)	Choose from list "Classes"	The owner value of the selected object.
Owner (Document collection)	Choose from list "Document collections"	The owner value of the selected object.
Owner (Document)	Choose from list "Documents"	The owner value of the selected object.
Owner (External source)	Choose from list "External sources"	The owner value of the selected object.
Owner (Report)	Choose from list "Reports"	The owner value of the selected object.
Owner (State transition)	Choose from list "State transitions"	The owner value of the selected object.
Owner (State)	Choose from list "States"	The owner value of the selected object.
Owner (Traditional folder)	Choose from list "Traditional folders"	The owner value of the selected object.
Owner (User group)	Choose from list "User groups"	The owner value of the selected object.
Owner (User)	Choose from list "Users"	The owner value of the selected object.
Owner (Version label)	Choose from list "Version labels"	The owner value of the selected object.
Owner (Workflow)	Choose from list "Workflows"	The owner value of the selected object.
Permissions changed	Timestamp	The date and time when the permissions of the object were last changed.
Reference	Choose from list "Documents" (multi-select)	A list of referenced documents.
Remote vault GUID	Text	
Reply to	Choose from list "Documents" (multi-select)	
Reply to (ID)	Text	
Report	Choose from list "Reports" (multi-select)	A report related to the selected object.
Report placement	Number (integer)	Specifies the placement of the selected report.
Report URL	Text	Specifies the URL of the selected report.

Built-in Property Definition	Data type	Description
Shared files	Text (multi-line)	The shared location paths of the shared files of the selected object.
Signature manifestation	Text (multi-line)	Electronic signature manifestation of the selected assignment.
Single file	Boolean (yes/no)	A Boolean property identifying whether the object is a single-file object.
Size on server (all versions)	Number (integer)	The total size of all versions of the selected object.
Size on server (this version)	Number (integer)	The size of the selected object version.
State	Choose from list "States"	The workflow state of the object.
State transition	Choose from list "State transitions"	The workflow state transition of the object.
Status changed	Timestamp	The date and time of the last status change of the object.
Traditional folder	Choose from list "Traditional folders" (multi-select)	A traditional folder containing the selected object version.
Version comment changed	Timestamp	The date and time of the last change to the comment of the object version.
Version label	Choose from list "Version labels" (multi-select)	The version label for the object.
Version label changed	Timestamp	The date and time of the last change to the version label of the object version.
Workflow	Choose from list "Workflows"	The workflow of the selected object.
Workflow Assignment	Choose from list "Assignments" (multi-select)	A property that indicates the assignment related to the workflow of the object.

Permissions

Access for viewing this property and editing the property in object metadata can be defined on the *Permissions* tab.

If the user does not have the permission to view the property, it is not available for selection in M-Files (for example, when you are creating a new search or when *More properties* is selected).

If the user cannot see the property, the user also does not have the permission to edit it. However, the user may have the permission to see the property without having the permission to edit it. Editing in this case refers to the user being able to edit the property in the object metadata in all possible ways: edit its value, or add or delete the property.

Adjusting Permissions

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight the appropriate node or subnode of the vault and select the desired item from the list on the right.

5. Right-click the item and select **Properties** from the context menu.

6. Go to the **Permissions** tab.

7. From the **Users and user groups** list, select the user or user group whose permissions you want to adjust.

    ℹ️ If the user or user group is not on the list, click **Add...** to add the user or user group to the list.

8. Either:

    a. Check the **Allow** check box to allow the selected user to see this item.

    or

    b. Check the **Deny** check box to deny the selected user from seeing this item.

9. Optional: If you want to adjust additional permissions, repeat the steps 7 and 8.

10. Click **OK** once you are done.

You have adjusted the view permissions of the selected item for the selected users.

Classes

A document class is an object type that combines several properties (see *Property Definitions* on page 288). Classes are designed to help categorize objects, to improve consistency as well as to speed up the process of filling in the object metadata.

You can create new classes and specify properties for each class via M-Files Admin. When the class is selected in M-Files Desktop, the properties that the system administrator has specified for the class will appear on the metadata card. M-Files users provide the properties with values when creating the new object.
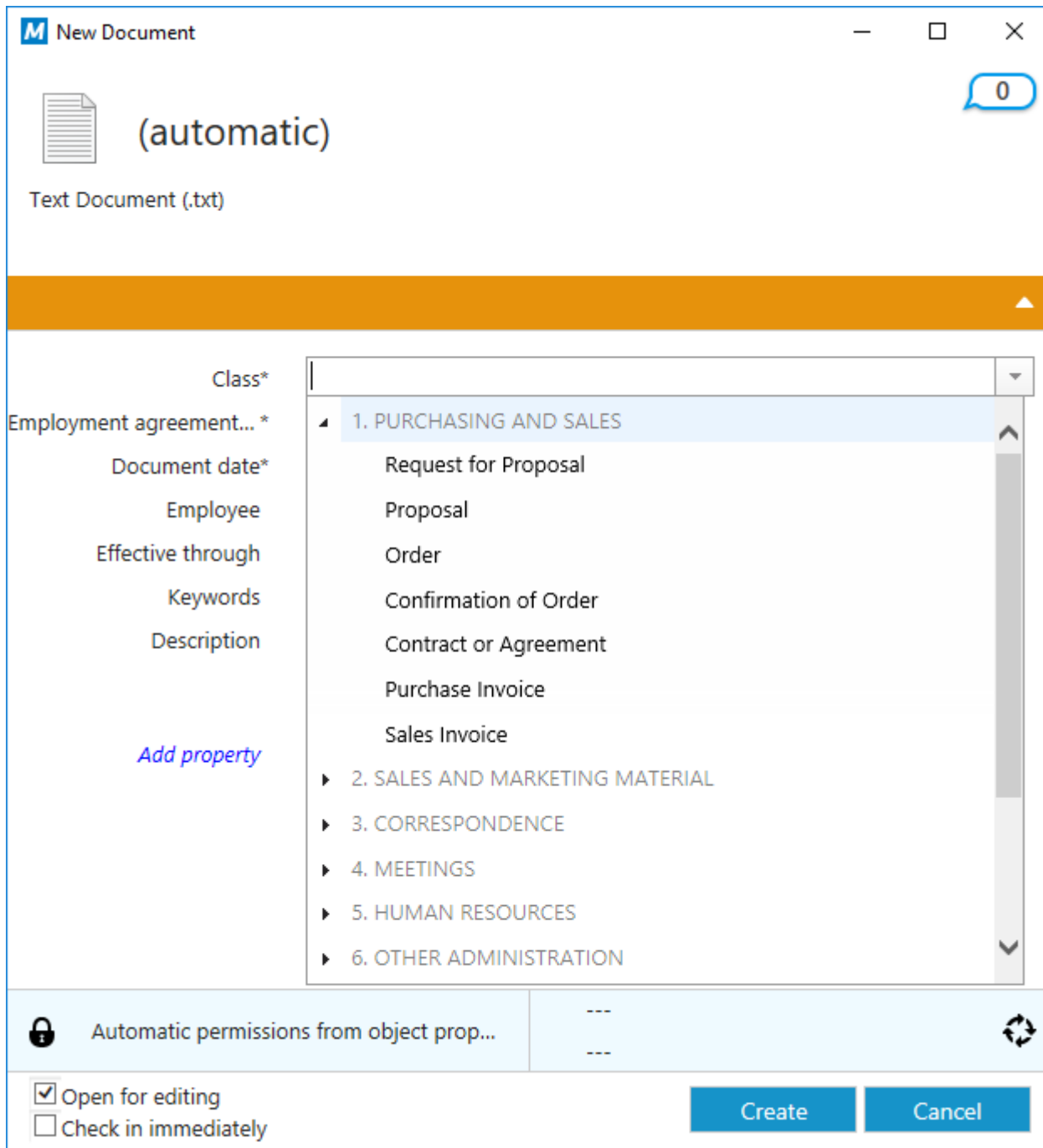
Figure 89: Classes shown on the metadata card for a new document.

New Class

You can start creating a new class by highlighting the *Class* heading in the left-side tree view of M-Files Admin and by clicking the *New Class...* link on the task area.

▶ Video: *Class Structure*

Figure 90: The properties dialog of a new "Purchase Invoice" class.

In the example shown above, a new class is being created. You can add new properties by clicking the **Add...** button. If the *Required* checkbox for the property is active, users need to assign a value for the property when creating a new object in that class. Otherwise, the object cannot be created. The *Purchase Invoice* class being created in the above image dictates that the *Name or title* and *Document date* properties would need to be filled in for users to be able to create a *Purchase Invoice* object.

▶ Video: *Class Properties*

Set As Name

Any property of the class can be defined as the name of the object; that is, the property is selected as the *name property* for the objects of this class. Then the name of the object does not have to be entered separately; instead, a certain property can be set up to always be the name or "title" of the object belonging to the class in question. This makes the naming of objects in a class more consistent.

This property is very useful for working with automatic values (see *Automatic Values* on page 292). The automatic value of the property may at the same time be the name of the proposal document ("Proposal/ESTT").

📄 **Note:** Templates are named without automatic values.

The *Update names* function (found on the M-Files Admin task area for a class) can be used to update the names of all existing objects in the class to conform to the new definition.

Default workflow for new objects

You can define a default workflow for new objects in this class. For example, all invoices can be set to use the *invoice circulation* workflow.

Force this workflow for new objects

If a specific workflow is forced for new objects in the class, the workflow cannot be deleted or changed. For example, the *Purchase Invoice Approval* workflow can be specified as compulsory for a new document created in the *Purchase Invoice* class.

Templates

You can define templates to be used when creating new objects in this class. To specify a document or other object as a template, add the property *Is template* and set it to *Yes*. Templates are class-specific. You can specify the template to be a part of several classes by specifying multiple classes for the object being used as a template, with the *Additional Classes* property.

Aliases (Advanced tab)

Via the *Advanced* tab, you can define an alias for the class. For more information, see *Associating the Metadata Definitions* on page 203.

Creating a New Class

Follow the steps provided below to create a new class to your M-Files vault.

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand the *Metadata Structure (Flat View)* node.

5. Select the *Classes* node.

6. Click **New Class...** on the task pane.

    ☑ The **Class Properties** dialog for a new class is opened.

7. In the **Name** field, type in a descriptive name for the new class.

8. Using the **Object type** drop-down menu, select the object type that the class is to be associated with.

    ⓘ The class can be selected only for objects of this type.

9. Optional: Using the **Properties** table, define which properties are to be automatically added to the metadata card when this class is selected.

    ⓘ For more information, see *New Class* on page 308.

10. Optional: Using the **Default workflow for new objects** drop-down menu, specify the default workflow to be associated with the class.

    ⓘ Enable *Force this workflow for new objects* to require the selected workflow to be used for any new objects with this class.

11. Optional: On the **Permissions** tab, you can specify the users who may see this class or attach objects to it.

ℹ For more information, see *Permissions and Automatic Permissions* on page 311.

12. Optional: On the **Automatic Permissions** tab, you can specify whether or not objects of this class receive automatic permissions.

ℹ For more information, see *Permissions and Automatic Permissions* on page 311.

13. Optional: On the **Advanced** tab, you can define aliases for the class using the **Aliases** field.

ℹ For more information, see *Aliases for Associating Metadata Between Vaults* on page 205.

14. Click **OK** to create the new class.

The new class is added to the list if classes in M-Files Admin and can be selected for objects in M-Files Desktop.
Assigment Class

When you are creating a new class with the object type *Assignment*, an additional tab appears to the **Class Properties** dialog, the **Assignment Details** tab. It enables you to select the assignment type and certain conditions related to the completion or approval of the assignment.

Assigment type

There are two types of assignments, task assignments and approval assignments. The assignees of the task assignments simply mark the assigment complete when they have successfully carried out the task, whereas the assignees of approval assigments have more say in the actual approval process: they can use the assigment for approving or rejecting the target object.

In both cases, you can set the completion of the assignment to require action from all or any assignees. You may also want to require an *Electronic Signature* on page 329.

Permissions and Automatic Permissions

Permissions

On the *Permissions* tab, you can specify the users who may see this class.

Automatic permissions

You can activate the automatic permissions by value, value list, object type, or class. You can specify the automatic permissions for each class in the same way as for each value. For more information, see *Automatic Permissions* on page 275.

Note: The actual final object receives automatic permissions when a class with automatic permissions specified is added for the object.

Versions older than 8.0: On the *Default Permissions for Objects* tab, you can set the default permissions to be applied when a new object in this class is created.

Adjusting Permissions

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight the appropriate node or subnode of the vault and select the desired item from the list on the right.

5. Right-click the item and select **Properties** from the context menu.

6. Go to the **Permissions** tab.

7. From the **Users and user groups** list, select the user or user group whose permissions you want to adjust.

> ℹ If the user or user group is not on the list, click **Add...** to add the user or user group to the list.

8. Either:

    a. Check the **Allow** check box to allow the selected user to see this item.

    or

    b. Check the **Deny** check box to deny the selected user from seeing this item.

9. Optional: If you want to adjust additional permissions, repeat the steps 7 and 8.

10. Click **OK** once you are done.

You have adjusted the view permissions of the selected item for the selected users.

Class Groups

Classes can be combined into class groups. This makes it easier to select a class while creating a new document.

You can create a new class group by right-clicking the *Document* heading under *Document Vaults > (Vault) > Metadata Structure (Hierarchical View)* and selecting *New Class Group...*

▶ Video: *Class Groups*

New Class Group

The image below displays the properties window for creating the class group *Meetings*. The *Members* field lists the classes that belong to this group.

The document classes are shown in the menu in numerical order when you fill in the metadata card. You can easily change the order of the list by using numbering.
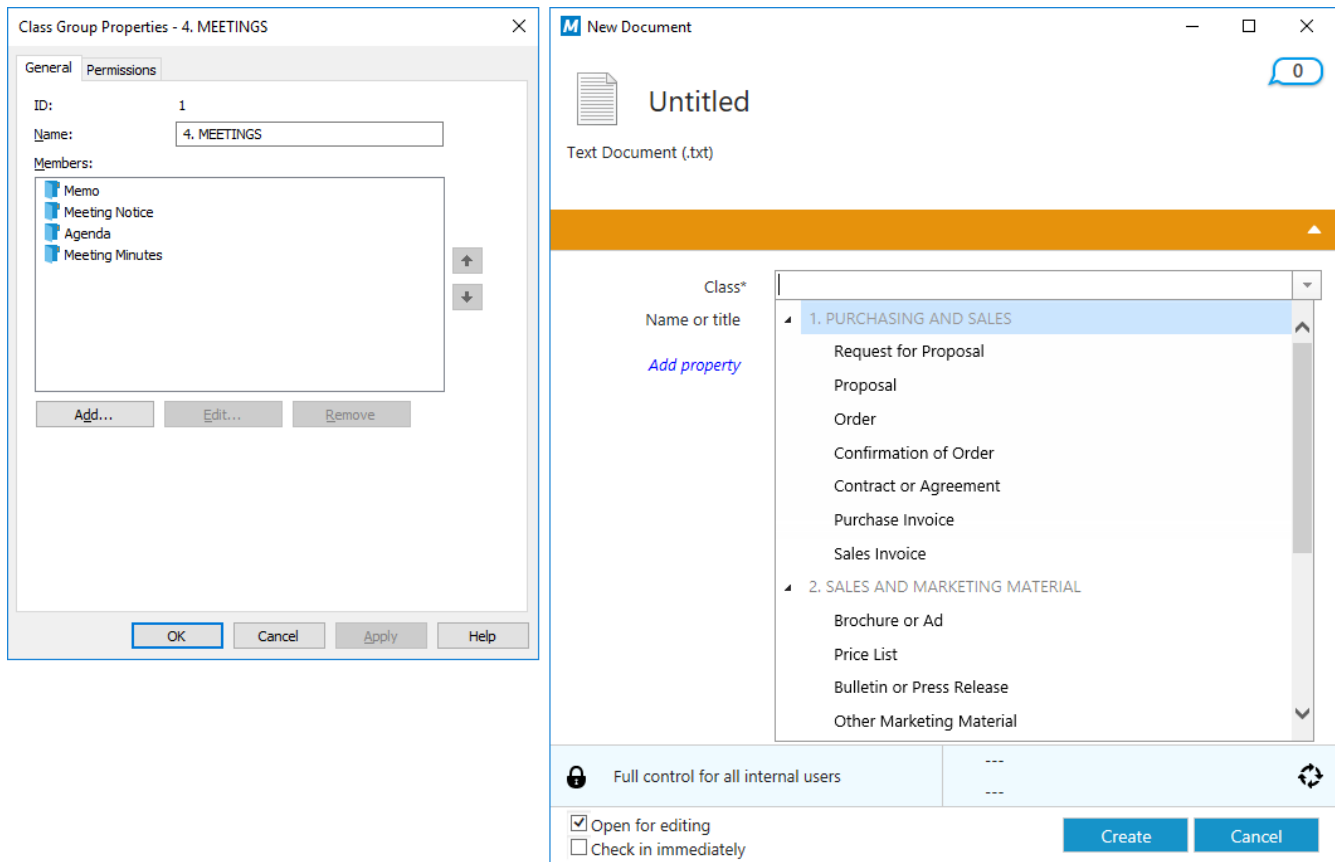
Figure 91: The "Class Group Properties" window and the new document creation dialog showing various class groups.

Permissions

You can specify the users who may see this class group via the *Permissions* tab of the *Class Group Properties* dialog.

9.5. Workflows

M-Files integrates with the organization's administrative and executive processes. Defining and monitoring tasks is easiest where the task documents are located. With the *Workflow* feature, the company's routines can be widely automated and tasks can be assigned to the right people at the right time. Users receive e-mail notifications about task-related issues, and managers can monitor task progress and approve completed tasks.

Workflows can be used, among many other processes, for purchase invoice circulation. Workflow states could in that case include:

- Awaiting approval
- Approved
- Rejected
- Paid in full

You can define who is allowed to transfer the object from one state to the next and who is responsible for the next workflow task. For example, invoices could only be approved for payment by a member of the management group.

When the invoice is in the *Approved* state, the department responsible for money transactions would automatically be informed that a new invoice is awaiting payment. When the invoice has been paid, it is transferred to the *Paid in full* state.

Graphical Workflow Designer

M-Files comes with a graphical user interface for managing workflows. See *Graphical Workflow Designer* on page 314 for more details.

Graphical Workflow Designer

In M-Files versions 2015 and later, you can use a graphical tool for creating and modifying workflows. The designer is an integral part of M-Files Admin. You can access the designer by selecting your vault connection from the left-side tree view and by navigating to *Workflows*.

📝 **Note:** The designer requires Internet Explorer 9 or later to be installed in the computer.

Workspace

The *Workflows* window has two sections:

- The top section lists the available workflows and the task area commands *New Workflow*, *Make Copy*, *Delete* and *Properties*.
- The bottom section displays the graphical workflow designer. The designer-related task pane commands are explained under *Using the designer* and *Task pane commands*.
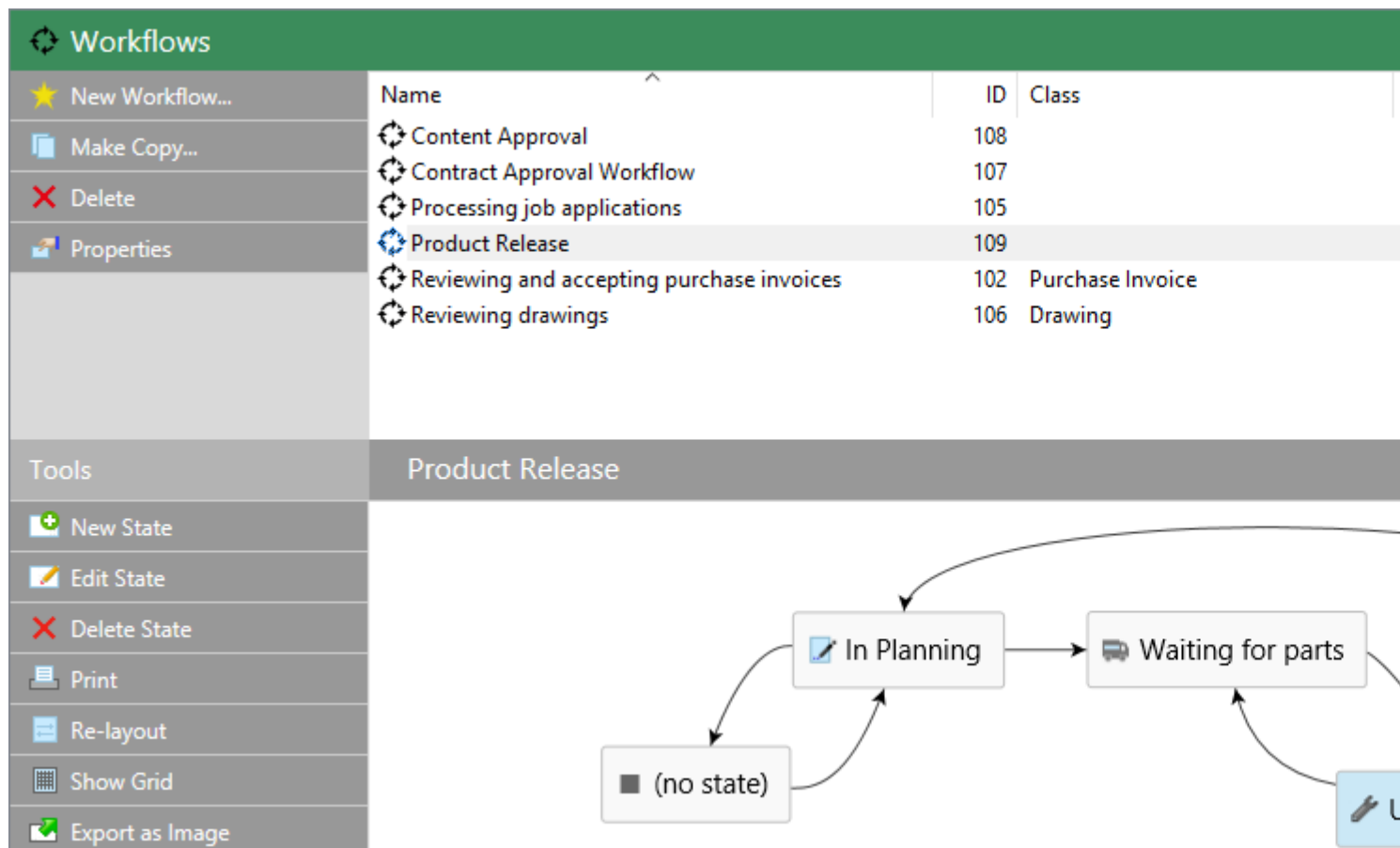
Figure 92: The graphical workflow designer in M-Files Admin.

The *Save* and *Discard* commands are located in the top-right corner of the workspace, on the title bar of the selected workflow. The *Save* command covers all the modifications to the workflow, including the layout of your graphical representation.

You can modify the workspace proportions by dragging the workflow title bar up or down.

Using the designer

The designer has been designed to work very intuitively. You can use the task area and/or interact with the graphical designer and context menus.

Creating new states

You can create new states either via the task area or by double clicking an empty space on the canvas. This opens up the dialog for a new workflow state.

Editing states

You can open the properties dialog for an existing state simply by double clicking the state, by selecting it and then clicking *Edit State* via the task area, or via the context menu for the state.

Deleting states

States can be deleted via the task area command *Delete*, via the state's context menu, or by selecting the state and pressing the *Delete* key on your keyboard.

Modifying the layout

The workflow states can be freely moved around on the canvas by dragging and dropping.

Connectors (state transitions)

You can add arrow connectors between the states by moving your cursor on the edge of a state rectangle and by using drag and drop. The state rectangle has green edges and the cursor changes into a cross (+) when a connector can be drawn. The connectors represent workflow state transitions.

Figure 93: A state transition being drawn from "Draft" to "Released".

Sometimes the connectors may overlap with each other or with the state rectangles. The connectors can also be modified to make the layout more readable. Just select a connector and use the two handles for re-shaping the connector.

The context menu for a connector allows you to *Edit* or *Delete* the state transition in question, as well as to *Straighten* the connector. Double clicking the connector opens the properties dialog for the state transition.

Zooming and dragging the canvas

You can zoom in and out by scrolling, as well as drag the canvas around. The context menu for an empty space on the canvas allows you to reset the zoom level.

Task pane commands

In addition to context-specific task area commands, such as *Edit State* or *Straighten*, there are also a few actions that affect the designer or your workflow as a whole.

Re-layout

With the *Re-layout* command you can "clean up" the canvas. This basically makes M-Files suggest a default positioning for the workflow components.

Show Grid

The *Show Grid* command toggles the grid shown on the background.

Print

You can create a paper copy of the workflow by using the *Print* command on the task area.

📄 **Note:** The print function uses Internet Explorer's *Page setup* settings for the page header and footer. You can set the settings for the header and footer to *empty* if you want to remove them from the printout. For instance with Internet Explorer 10, you can open the *Page setup* by clicking the tools button in the top-right corner of the browser and by selecting **Print** > **Page setup**.

Export as Image

In addition to creating a print-out, you can export the workflow as a PNG file. Clicking the *Export as Image* command opens the common Windows save dialog for the image file.

Tooltips

The state rectangles and connectors may display a tooltip while the cursor is hovered above them.

In addition to the title of the element, the tooltips may contain a description as well as information on the state transition conditions and special actions related to the transition or workflow state.

New Workflow

The Workflow feature enables automating company processes. You can start creating a new workflow by highlighting the *Workflows* heading in the left-side tree view of M-Files Admin and selecting *New Workflow...* on the task area.

Figure 94: The properties dialog for a workflow.

Name

Give a descriptive name for the workflow.

Description

A free-form description of the workflow.

States

Use the arrow keys along the right side of the dialog to change the order of the states. Use the **Add...**, **Edit...** and **Remove** buttons to manage the workflow states.

> 📄 **Note:** If you are creating a workflow that is going to be forced for new objects of a specific class (see *New Class* on page 308 for more information), make sure that the first state after *(no state)* in the graphical workflow designer is the topmost state in the **States** list.

Allow using this workflow with the following class

You can allow a given workflow to be used with all classes or with one class only. For example, you can define that the *Purchase Invoice Approval* workflow can be selected for documents in the *Purchase Invoice* class only. The workflow will in that case not be selectable for documents in any other class.

The Permissions tab

Access for viewing this workflow can be set on the *Permissions* tab. If the user does not have access for viewing the workflow, also the workflow states are hidden.

The Advanced tab

From the *Advanced* tab, you can define an alias for the workflow. For more information, see *Associating the Metadata Definitions* on page 203.

Creating a New Workflow

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select the **Workflows** node.

5. Click **New Workflow...** on the task area to start creating a new workflow.

   ✓ The **Workflow Properties** dialog is opened.

6. In the **Name** field, enter a name for the workflow and, in the **Description** field, enter an optional description for the workflow.

7. Optional: Click **Add...** to add states to the workflow.

   ℹ️ States can also be added later in the graphical workflow designer by selecting a workflow and clicking **New State** on the **Tools** pane.

8. Click **OK** to finish creating the workflow.

The workflow you have just created is added to the **Workflows** list. You can add workflow states and state transitions to it by selecting the workflow from the list and using the tools on the **Tools** pane.

- For instructions on adding workflow states to a workflow, see *Adding States to a Workflow* on page 318.
- For instructions on adding state transitions between states in a workflow, see *Adding State Transitions to a Workflow* on page 326.

Workflow States

Workflow states are used for dividing wokrflows into smaller stages. You can create a new workflow state by double clicking the canvas in the *Graphical Workflow Designer* on page 314 or by clicking the **Add...** button on the **General** tab of the **Workflow Properties** dialog (see *New Workflow* on page 316).

Individual states allow a variety of settings. The *General* tab contains the name and the description of the state. The properties dialog for a workflow state also includes the tabs *Conditions*, *Actions*, and *Advanced*. The *Advanced* tab allows you to assign an alias for the state. The tabs **Conditions** and **Actions** are presented in their own subtopics.

In versions 2015 and earlier, the **State Properties** dialog contains the **State Transition** tab. This can be enabled in M-Files 2015.1 and later by using a Windows registry setting. Ask your M-Files consultant for more information, or contact our customer support at *support@m-files.com*.

Adding States to a Workflow

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select the **Workflows** node.

5. Select a workflow from the **Workflows** list and click **New State** on the **Tools** pane to open the **State Properties** dialog.

6. In the **Name** field, enter a name for the workflow state and, in the **Description** field, enter an optional description for the state.

7. Optional: In the **Conditions** tab, specify the preconditions and postconditions that must be met before an object can be moved in or out of this state.

   ⓘ For more information on workflow state conditions, refer to *Conditions* on page 318.

8. Optional: In the **Actions** tab, specify the actions that are performed when an object is moved to this state.

   ⓘ For more information on workflow state actions, refer to *Actions* on page 320.

9. Click **OK** to close the **State Properties** dialog.

10. Click **Save** to save your changes.

The new state you have just defined is added to the workflow. The state can be seen in the graphical workflow designer.

• For instructions on adding state transitions between states in a workflow, see *Adding State Transitions to a Workflow* on page 326.
• For instructions on creating a new workflow, see *Creating a New Workflow* on page 317.

Conditions

On the *Conditions* tab you can specify different pre- and post-conditions for the state transitions. For example, you can define specific properties or their values that a document should meet before it can moved to this state. The conditions can also specify that, for instance, the basic documents related to the project (specification document, implementation and project timetable instructions, etc.) must be on a certain level before moving to the next level is possible.

▶ Video: *State Transition Conditions*

The conditions can be specified in broader scope and detail using variables, generic features of VBScript, m and M-Files API. The following variables can be used in advanced conditions: `VaultSharedVariables`, `MFScriptCancel`, `CurrentUserID`, `Vault`, `DisplayID`, `ObjVer`, `PropertyValues`, `StateID`, `PropertyDef`, `SavepointVariables`, `TransactionCache`, and `GetExtensionObject`. For more information about variables, refer to *VBScript Variables Explained* on page 402.

> 📝 **Note:** The documentation for the M-Files API is located in **Start** > **Programs** > **M-Files** > **Documentation** > **M-Files API**. For more information about VBScript code and M-Files API, go to *www.m-files.com/api*. Instructions on writing VBScript code and working with the M-Files API are available for a separate fee from M-Files customer support (*support@m-files.com*).
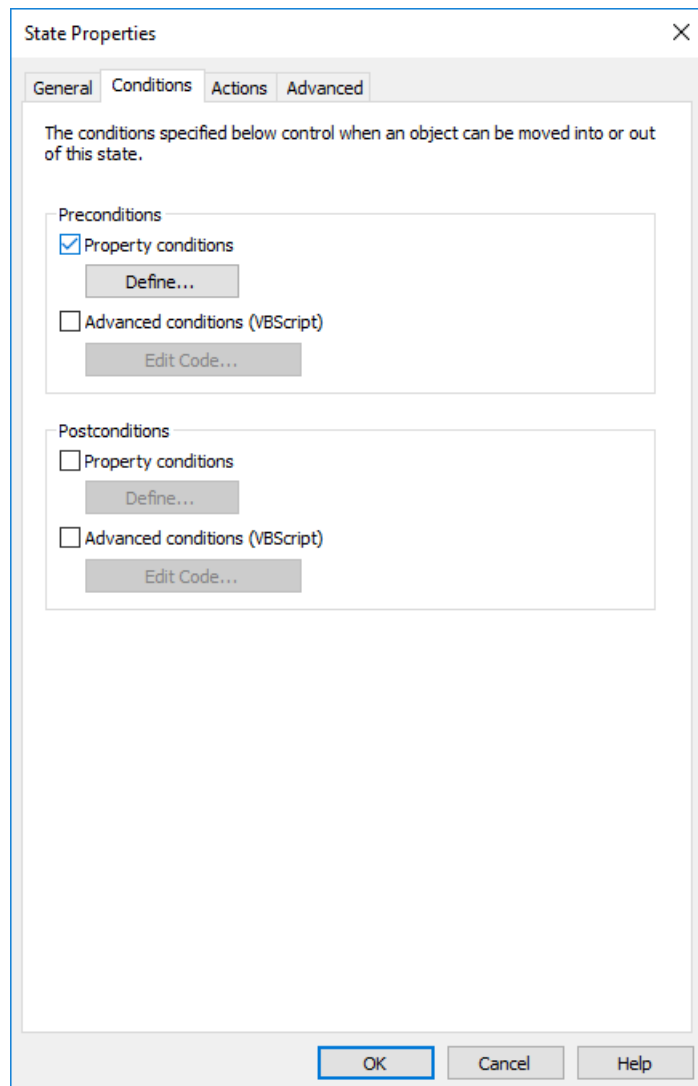
Figure 95: The "Conditions" tab of the workflow state properties.

Preconditions

The state preconditions specify the object properties that are required in order for the object to be moved to this state.

For example, you can specify that the *Approved by* information must be entered before the document can be moved to the *Approved* state.

Postconditions

The state postconditions specify the object properties that are required in order for the object to be moved out of this state.

For example, you can specify that the *Cost center* information in a purchase invoice must be entered before the document can be moved from the *Awaiting definition of cost center* state.

Actions

The *Actions* tab is used for setting the actions to be performed when the object enters to a certain state.

1. *Set permissions, Delete, and Mark for archiving* on page 321
2. *Send notification and Set properties* on page 321
3. *Convert to PDF format* on page 321
4. *Run script* on page 322
5. *Assign to user* on page 322
6. *Create separate assignments* on page 323

Set permissions, Delete, and Mark for archiving

You can define new permissions to be set, the object to be deleted, and/or archiving to be performed as a result of a state transition. Several options of the **Actions** tab can be selected at the same time.

Do not use automatic permissions

As a result of this state transition, the object bypasses the automatic permissions that would normally be applied to the object, and the effective permissions for the object version are configured with the **Set permissions** feature. However, if a user modifies the object, the automatic permissions are re-applied to the object.

Ignore the permissions of the latest checked-in version for this version

The permissions of the objects are version-specific in M-Files. In order for you to access the latest object version, you must have at least read access to it. To access any of the previous versions, you must have at least read access to that specific version *and* to the currently latest version. Enabling this checkbox ignores the permissions of the latest checked-in version and grants users access to prior versions of the object to which they have at least read access rights – regardless of the permission settings of the latest version.

This feature merits an example: Let's suppose that we have an SOP and an SOP workflow with the states *Draft*, *Waiting for Approval* and *Approved*. All three states have different permissions, as a draft is shown only to the user who created the document, and an approved document is shown to all users.

The document is now at version 3 and in the *Approved* state (and thus visible and accessible to all users). As modifications need to be introduced, it is moved back to the *Draft* state and the permissions are changed so that only the creator of the document can see it. If the check box **Ignore the permissions of the latest checked-in version for this version** was active when the new version was created, all users would still be able to access the document version 3, but not the newest one. If the check box was not active, however, only the creator of the document would be able to see the document version 3.

> 📝 **Note:** Even if the **Ignore the permissions of the latest checked-in version for this version** option was enabled, the document would still not be visible in searches and views if they do not have the *Look in all versions* on page 146 option enabled.

Send notification and Set properties

Send notification

To send a notification, first define the recipient users and user groups. Then enter the notification subject and the message. You can also specify the user from metadata or state transitions.

The **Add Placeholder...** buttons can be used to insert values from the object metadata to the subject line or message content (see also the placeholder descriptions under *Personalizing Notification Messages* on page 183).

▶ Video: *Notifications in Workflows*

Set properties

You can define different object properties and values to be applied when an object's state is changed. For example, you can make the *Published* version label to be assigned to a drawing when the drawing moves to the *Approved* state.

Convert to PDF format

Files of the object can be automatically converted into PDF form on the server when the object changes state. Conversion to PDF on the server can be done for files in such source formats as Word, Excel, PowerPoint, Outlook, and Visio, as well as RTF and OpenOffice files.

When converting to PDF, M-Files updates the M-Files property fields, if any, in Word and Excel documents by using the current metadata of the object.

Conversion settings

When you activate the **Convert to PDF** function from the **Actions** tab, M-Files converts the files in a single-file or multi-file document to PDF form automatically when the object's state changes. You can define advanced settings for the conversion.

Store each PDF file as a separate file next to the original file: If you also want to keep the file in its original format, select to store the PDF file next to the original file. Then the PDF file does not replace the original. The PDF file is created with the same name as the original file. If this function is applied to a single-file document, M-Files changes it into a multi-file document when creating the PDF file.

Overwrite existing PDF files: If there are already PDF files with this name in the multi-file document, select this option if you want to overwrite the identically named existing PDF files with the versions created via this function. If this option is not selected and the multi-file document already has a PDF file with the same name, M-Files will notify of the error and the PDF file will not be created.

Convert to PDF/A-1b: Select storage in PDF/A-1b form when you want to comply with ISO standard 19005-1:2005 for long-term preservation of electronic documents. PDF/A-1b is a more restricted format than that of standard PDF files, so files converted to PDF/A are often bigger than files converted to standard PDF. In addition, in export to PDF/A, certain advanced appearance settings may be omitted. You should use conversion to PDF/A form only if it is particularly necessary on account of, for example, requirements for long-term preservation.

Prevent state transition if the object contains files in an unsupported format: Select this if you want to prevent the state transition in cases wherein the PDF conversion function encounters files with formats that cannot be exported as PDF files (for instance, ZIP files). An error message is displayed and the state transition is prevented.

Run script

Operations can be specified in more detail using variables, generic features of VBScript, and M-Files API. For example, you can set consecutive numbers for different publication versions or add the send date for a document when it moves to the *Sent* state.

The following variables can be used in this script: `VaultSharedVariables`, `MFScriptCancel`, `CurrentUserID`, `Vault`, `DisplayID`, `ObjVer`, `PropertyValues`, `StateID`, `SavepointVariables`, `TransactionCache`, `PropertyDef`, and `GetExtensionObject`. For more information about variables, refer to *VBScript Variables Explained* on page 402.

> 📄 **Note:** The documentation for the M-Files API is located in **Start** > **Programs** > **M-Files** > **Documentation** > **M-Files API**. For more information about VBScript code and M-Files API, go to *www.m-files.com/api*. Instructions on writing VBScript code and working with the M-Files API are available for a separate fee from M-Files customer support (*support@m-files.com*).

Assign to user

Assignments are an important part of workflows. They transfer information and responsibility for task execution to the correct person automatically during a state transition. M-Files offers two types of assignments for use in connection with workflows.

▶ Video: *Assign to User*

By selecting **Assign to User**, you can create an assignment that does not result in a separate object. An assignment created with this option is switched to the "complete" state when one of the persons to whom the task was assigned changes the document state in the workflow (usually by moving the object to the next state).
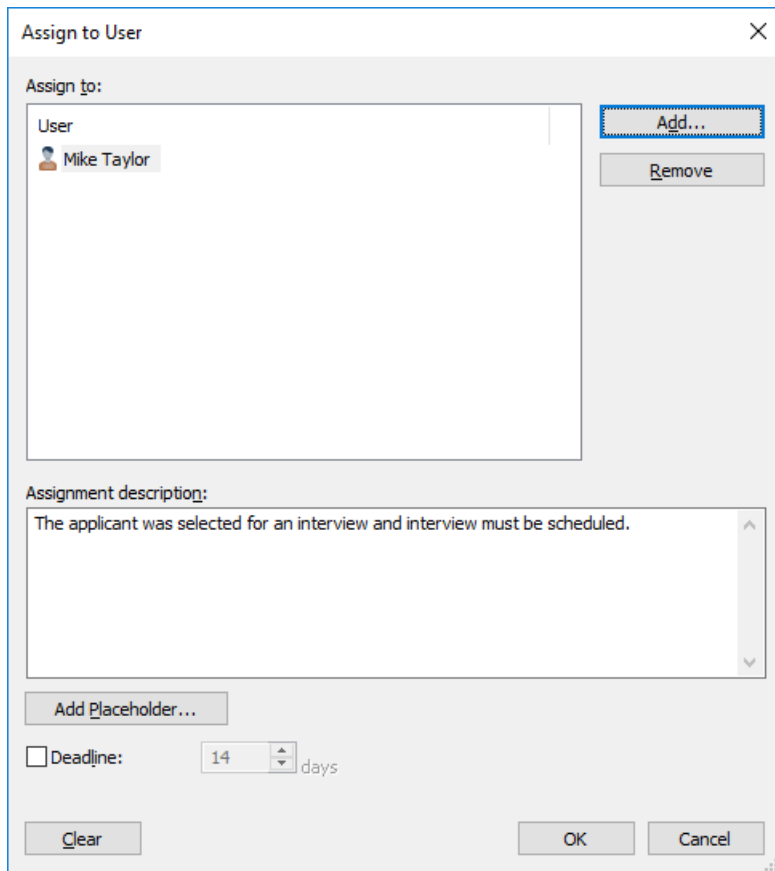
Figure 96: Define the task in the Assignment dialog.

In the object's properties, you can see whom it has been *assigned to*, provided that the object is in a state to which an assignment is related.

The person to whom the task was assigned can change the state by using the functions in the task area, metadata card or context menu.

Create separate assignments

You can also have separate assignments created once the object workflow is moved to a certain state. To create such assignments, enable **Create separate assignments** and click **Add...** on the **Actions** tab of the **State Properties** dialog.

If you want the workflow state to be automatically changed after the completion of the separate assignment(s), you need to define that in the *Trigger* on page 337 options of the state transition.

Adding and Removing users

You can manage the persons responsible for completing the task by using the **Add...** and **Remove** buttons in both the **Assign to User** dialog and the **Create separate assignment** dialog. In addition to adding users via the **Users or user groups** list, you can add users based on metadata or a state transition. For example, a person who has been specified in the property *Approved by* in the object's metadata can automatically be specified as the person to whom the task is assigned. For more information, see *Permissions* under *Permissions* on page 328 and *Pseudo-users* on page 88.
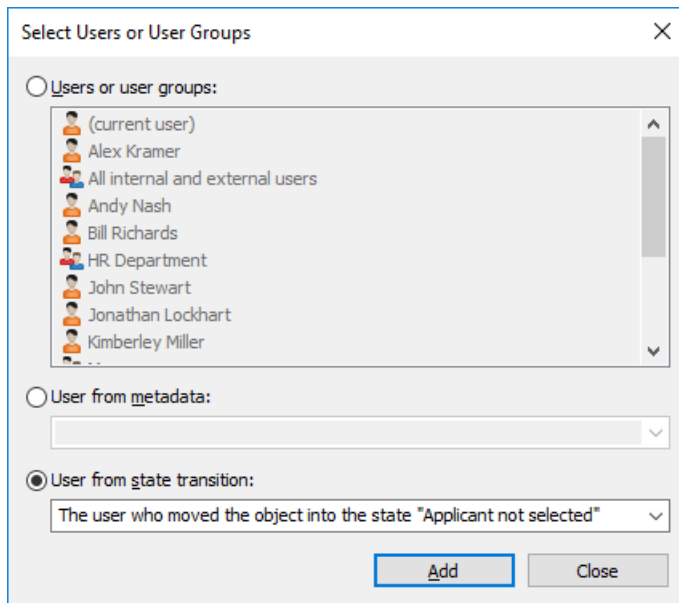
Figure 97: Selecting a user based on an earlier state transition.

Monitoring

In the **Monitoring** section (**Actions** > **Create separate assignments** > **Monitoring**), you can define the users that you want to notify each time a task has been completed. The assignment submitter is automatically defined as a task monitor.

There are separate icons for uncompleted and completed assignment objects, making it easy to distinguish between uncompleted and completed assignments.

Assignment class

The assigment class determines the assignment type and assignment completion conditions. See *Assigment Class* on page 311 for more information.

Assignment description

Add a free-form description of the task. The assignment notice by email displays the description to the person to whom the task was assigned. Notification templates supported by M-Files can also be included in the description. For more information on notification templates and placeholders, refer to *Notification Settings (M-Files Admin)* on page 181.

Deadline

If desired, you can specify a deadline for the assignment. An automatic reminder is sent if the assignment has not been marked complete when the deadline is approaching. The reminder will be sent using a common notification rule which can be deleted by the administrator.

> 📄 **Tip:** The deadline can also be useful for creating views. You can create a view to display any assignments with an approaching deadline. For more information about views, refer to *New View* on page 90.

Creating a Workflow State with a Separate Assignment

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select the **Workflows** node.

5. Select a workflow that you want to edit from the **Workflows** list.

☑ The workflow is opened in the graphical workflow designer.

6. In the graphical workflow designer, right-click a workflow state to which you want to add a separate assignment and select **Edit**.

☑ The **State Properties** dialog is opened.

7. In the **Actions** tab, check the **Create separate assignments** check box and click the **Add...** button.

☑ The **Create Separate Assignment** dialog is opened.

8. Click **Add...** to add the user or users the separate assignment is assigned to.

9. Optional: Click **Monitoring...** to add a user or users who will receive a notification once this assignment is marked complete, approved, or rejected.

10. From the **Select assignment class** drop-down menu, select the assignment class for the separate assignment.

11. In the **Title** field, enter a title for the assignment and, in the **Assignment description** field, enter an optional description for the assignment.

ⓘ By clicking the **Add Placeholder...** button, you can placeholders for metadata properties in the **Title** and **Assignment description** fields.

12. Optional: Check the **Deadline** check box and select the number of days to define a deadline for the separate assignment.

13. Click **OK** to close the **Create Separate Assignment** dialog.

14. Click **OK** to close the **State Properties** dialog.

15. Click **Save** to save your changes.

The separate assignment is added to the workflow state. When an assignment with the aforementioned workflow is moved to the aforementioned state, the separate assignment is created and added as a linked assignment under the primary assignment.

Workflow State Transitions

Workflow state transitions are used for moving from one workflow state to another. The transitions can be intiated manually by users or *triggered* on page 337 automatically by M-Files Server. They may also be set to require an *Electronic Signature* on page 329.

The General tab

The **General** tab contains the name of the state transition as well as an optional description for the state transition.

The Electronic Signature tab

The **Electronic Signature** tab allows you to enable eSigning for a state transition. If enabled, an electronic signature must be signed by the user before the state transition is performed. See *Electronic Signature* on page 329 for more information.

The Trigger tab

On the **Trigger** tab, you can define conditions for automatic state transitions. See *Trigger* on page 337 for more information.

The Advanced tab

On the **Advanced** tab, you can set an alias for the state transition. For more information about using aliases, see *Associating the Metadata Definitions* on page 203.

Adding State Transitions to a Workflow

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select the **Workflows** node.

5. Select a workflow that you want to edit from the **Workflows** list.

   ✅ The workflow is opened in the graphical workflow designer.

6. In the graphical workflow designer, place your cursor on the border of the state from which you want to create a state transition so that your cursor changes to a crosshair.

7. Holding down the left mouse button, draw a state transition by dragging the mouse cursor from the selected state to another.

8. Right-click the state transition arrow that you just created and select **Edit** from the context menu.

   ✅ The **State Transition** dialog is opened.

9. In the **Name** field, enter a name for the state transition and, in the **Description** field, enter an optional description for the transition.

10. Optional: In the **Electronic Signature** tab, you can specify an electronic signature that must be provided before completing this state transition.

    ℹ️ For more information on electronic signatures, refer to *Electronic Signature* on page 329.

11. Optional: In the **Trigger** tab, you can define a condition that triggers this state transition once the condition is fulfilled.

    ℹ️ For more information on triggers, refer to *Trigger* on page 337.

12. Click **OK** to close the **State Transition** dialog.

13. Click **Save** to save your changes.

The state transition is added to the workflow between the selected workflow states. This is manifested by the arrow between the states in the graphical workflow designer.

- For instructions on adding states to a workflow, see *Adding States to a Workflow* on page 318.
- For instructions on creating a new workflow, see *Creating a New Workflow* on page 317.

Parallel State Transitions

You can define multiple workflow state transitions between two states. This is useful, for instance, if you need to define multiple automatic transitions based on different criteria. For more information about creating state transitions, see *Adding State Transitions to a Workflow* on page 326.

Example: Creating a Workflow with a Parallel State Transition

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight **Workflows**.

5. In the **Workflows** list, select one of the existing workflows, such as *Reviewing drawings*.

   ✓ The workflow is shown as a flowchart in the graphical workflow designer below the **Workflows** list.

6. Click **New State** in the **Tools** pane to create a new state for the workflow.

   ⓘ If you already have a state called *Rejected* in your workflow, you can skip this and the next step, and proceed to step 8.

   ✓ The **State Properties** window is opened.

7. Enter the name *Rejected* in the **Name** field and click **OK** to close the **State Properties** window.

8. In the graphical workflow designer, place your cursor on the border of the *Listed for approval* state (or any other intermediary state, if your workflow does not have the *Listed for approval* state) so that your cursor changes to a crosshair.

9. Hold down the left mouse button and drag the crosshair to the *Rejected* state to draw a state transition between the *Listed for approval* and *Rejected* states.

10. Repeat step 8 to draw another state transition between the *Listed for approval* and *Rejected* states.

11. Right-click one of the state transition connector arrows and select **Edit**.

    ⓘ If you are seeing only one connector arrow between the states, the connectors are most likely on top of each other. Click the topmost connector to select it and click and drag the handles to reshape the connector.

12. Go to the **Trigger** tab, select the **Trigger the state transition after** option, and enter *10* in the **days** field.

13. Click **OK** to close the **State Properties** window.

14. Click **Save** in the upper-right corner of the graphical workflow designer to save the changes you have made to your workflow.

You should now have a workflow with two parallel state transitions from the *Listed for approval* state to the *Rejected* state: one that is initiated by users and another that is triggered automatically after 10 days, if it is not initiated by users in 10 days.

Permissions

You can access the state transition permissions by adding and selecting a state transition, clicking the **Edit Transition...** button and selecting the *Permissions* tab.

▶ Video: *State Transition Permissions*

Permissions

On the *Permissions* tab, you can specify which users are allowed to perform an explicit state transition.

Figure 98: Define permissions for changing state by means of state transitions.

The *Select Users or User Groups* dialog under the **Add...** button also contains the options *User from metadata* and *User from state transition*.

User from metadata

You can also utilize pseudo-users in state transitions. For example, you can specify that invoices are to be accepted only by the project manager of the project linked to the invoice. In other words, you can define users via the object's metadata. Then the right to perform state transitions is not bound to a certain named person; it is instead determined dynamically on the basis of an object's metadata.

User from state transition

You can also select users on the basis of previous state transitions. You can specify that the document can be moved from the *Approved* state to *Approval undone* only by the user who originally moved the document into the *Approved* state.

Electronic Signature

The electronic signature offered by the Electronic Signatures module expands the versatile workflows of M-Files: the state transition can be certified with a username. This function can easily be used to certify, for example, approval of documents.

The Electronic Signatures module is available for a separate fee. This module includes event logging extensions and electronic signature functionality. For more information, see *Electronic Signing and Compliance* on page 222.

Electronic signature for workflow state transitions

To incorporate an electronic signature with a workflow state transition:

1. Select a transition in the *Graphical Workflow Designer* on page 314.
2. Click **Edit Transition** in the left-side task pane.
3. Move to the **Electronic Signature** tab.

You should now have the **Electronic Signature** tab of a state transition in front of you.

Figure 99: The "Electronic Signature" tab for a state transition.

Enable the option **Require electronic signature for this action** to be able to modify the options.

Signature meaning

The **Signature meaning** options enable you to select either a predefined signature reason-meaning pair or to define multiple meanings for the signer to choose from. The signature reason is a brief heading-level description for the signature, such as *Approval of instruction document* or *Approval of invoice*. The signature meaning is a description that should enable the signer to understand what is being approved. The maximum number of

characters is 500, and placeholders can be used. The available placeholders are listed under *Placeholders for Signature meaning and Additional information fields* on page 333.

Figure 100: The signature reason and meaning displayed on an electronic signature prompt.

Signature metadata

The electronic signature can be set to require the signer to add a value for a selected metadata property, such as *Comment*. The text is saved either to a separate signature object (see below) or to the object using the workflow. You can also include additional information to the **Additional information** text box. The available placeholders are listed under *Placeholders for Signature meaning and Additional information fields* on page 333.

Create a separate signature object

Select this option if you want to create a new object for the signature. Then the signature object is automatically in relationship with the object to which the state transition applies.

> 📄 **Note:** In order for M-Files to be able to create the signature objects, certain metadata definitions have to be set up. See *Metadata Definitions for an Electronic Signature Object* on page 333 for more details.

Identifier

The identifier is free-form text. You can set, for example, *Purchase Invoice Approval* as the identifier. In creation of the signature object, the identifier becomes a part of the metadata for the object. The *Identifier* property can be utilized in, for example, scripts for state-transition functions or in searches to individualize a certain type of signature.

Figure 101: A signature object showing information on the signer, the signing date, the meaning of the signature and other elements.

Save signature manifestation as text to a property

Select the property that the signature is to be associated with. Then the content of the signature that has been defined is displayed as the property value in the object's metadata. The default property is *Signature manifestation*. The text content of the signature property consists of the *reason*, *meaning* and *additional information* for the signature.

> **Note:** If you use the same property for signatures of all state transitions in the workflow, such as the default property *Signature manifestation*, you can see only the latest signature manifestation in the metadata of the object's latest version. Other signatures with their contents (manifestations) can be found via the relevant object's version history.

You can also create a separate property definition of your own for each signature of the relevant state transition in the workflow. Then you can see all of the properties created and their signature content (manifestations) in the metadata of the object's latest version.

> **Note:** If you first create a property in the *Property definitions* area, specify its permissions in such a way that the users can see the property used in the signatures but cannot edit it.

Electronic signature for the state transition

If an electronic signature has been defined for the state transition, the signature is always required for the user before the change in state. In order for the state to change, the object must be checked in, and change of state with a signature can only be done one object at a time. Only users using Windows authentication can perform state changes that require an electronic signature. The user adds an electronic signature to the state transition by entering his or her identification data and logging in. The electronic signature does not refer to an electronic "fingerprint"; it always requires entering the user identification and logging in.

Placeholders for Signature meaning and Additional information fields

The available placeholders to be used with the *Signature meaning* and *Additional information* fields are listed in the table below.

Placeholder	Description
%SIGNED_AT_UTC%	The UTC time at the time of signing.
%SIGNED_AT_LOCAL%	The time on the client computer at the time of signing.
%SIGNED_AT%	The time on the server computer at the time of signing.
%SIGNED_BY%	The signer name.
%SIGNED_FROM_STATE%	The source state.
%SIGNED_TO_STATE%	The target state.
%SIGNED_FOR_STATETRANSITION%	The title of the state transition for which the electronic signature is required.
%SIGNED_BY_WITH_PROXY%	Displays the name of the signer and the user on behalf of whom an assignment has been electronically signed. For instance: "Preston Present, on behalf of Abraham Absent".

Metadata Definitions for an Electronic Signature Object

In order for automatic signature objects to be created in M-Files, aliases must be created for the new object type as well as for the required property definitions. The aliases are used for creating objects at the time of signing. If you are using the *Electronic Signatures module* on page 222, these definitions are already available. Otherwise, you should create the metadata definitions below in order to activate the separate signature objects.

Object type

Create a new object type and name it, for example, the *Signature* object type. In the advanced settings, specify the object type alias:

```
M-Files.QMS.Signature.ObjectType
```

Compulsory property definitions for the signature object

When you have created a new object type, M-Files automatically creates an equivalent property definition. Select this property definition in the property definitions and add the following alias:

```
M-Files.QMS.Signatures
```

In addition to this, add the aliases listed below:

Identifier	
Alias	`M-Files.QMS.Signature.Identifier`
Data Type	Text
Description	The identifier property is added to the electronic signature when the electronic signature object is created. The identifier property value is specified in the electronic signature settings in M-Files Admin.

Reason for signature	
Alias	`M-Files.QMS.Signature.Reason`
Data Type	Text
Description	A brief heading-level description for the signature.

Signature meaning	
Alias	`M-Files.QMS.Signature.Meaning`
Data Type	Text (multi-line)
Description	A description enabling the signer to understand what is being approved.

Signer	
Alias	`M-Files.QMS.Signature.Signer`
Data Type	Choose from list (select the *Users* value list)
Description	The vault user electronically signing the state transition.

User	
Alias	`M-Files.QMS.Signature.User`
Data Type	Choose from list (select the *Users* value list)
Description	The vault user to whose identity the signature is bound when the signature is used for moving an assignment to a terminal state, such as *Completed*, *Accepted*, or *Rejected*.

You can freely name the compulsory property definitions mentioned above, but you should use the most descriptive names possible, since this information is shown in the metadata of the signature object.

Optional property definitions for the signature object

You can also create various optional property definitions for the signature object. For example, you may want to create a new property definition for *additional signature information* with the data type *Text (multi-line)* and add the following alias:

`M-Files.QMS.Signature.AdditionalInfo`

The rest of the optional properties are listed below:

M-Files.QMS.Signature.Signer.Name	
Data Type	Text

M-Files.QMS.Signature.Signer.Name	
Description	Contains the full name of the signer.

M-Files.QMS.Signature.Signer.Account	
Data Type	Text
Description	Contains the M-Files account name of the signer.

M-Files.QMS.Signature.LocalTimestampText	
Data Type	Text
Description	The local time of the signature as text, including the timezone information.

M-Files.QMS.Signature.UTCTimestampText	
Data Type	Text
Description	The UTC time of the signature as text, including the timezone information.

M-Files.QMS.Signature.UTCTimestamp	
Data Type	Timestamp
Description	The UTC timestamp of the signature.

M-Files.QMS.Signature.Date	
Data Type	Date
Description	The signature date in local (server) time.

M-Files.QMS.Signature.FromState	
Data Type	Choose from list (select the *States* value list)
Description	The workflow state prior to the state transition. Available only when signing state transitions.

M-Files.QMS.Signature.ToState	
Data Type	Choose from list (select the *States* value list)
Description	The workflow state after the state transition. Available only when signing state transitions.

M-Files.QMS.Signature.StateTransition	
Data Type	Choose from list (select the *State Transitions* value list)
Description	The workflow state transition that has been executed. Available only when signing state transitions.

Executed, empty, and invalidated signature objects and how to utilize them

You can also create so-called empty signature objects and use them to monitor which signatures have not yet been signed and which signatures have already been executed. You can utilize these empty, executed, and invalidated signature objects creating different classes for the signature object type.

Here are the aliases which, if specified for classes of the *Signature* object type, are utilized by M-Files in various phases of electronic signing:

```
M-Files.QMS.Signature.Class.Empty
```

```
M-Files.QMS.Signature.Class.Executed
```

```
M-Files.QMS.Signature.Class.Invalidated
```

Permissions

Metadata definitions (object type and property definitions) created for the automatic signature object should be secure; it should not be possible to create signature objects manually or change their metadata. Also the property definition that binds the signed object to the signature must be secure. If you are using M-Files QMS, these definitions are already available.

Separate signature object

When you have created the necessary definitions and chosen creation of a separate object for the signature, the object will be automatically created after signing.

The name of the signature object is created automatically from the signature reason, signer and timestamp.

Other metadata for the signature object are created automatically on the basis of the signature definitions.

Inserting the Signature Property to Office Documents

The text content of the signature property can be added to a Word, Excel, or Powepoint document in the same way as other M-Files properties.

When the user selects the added property from the list, the property name, such as the name of the built-in property *Signature manifestation*, is displayed. This is why it is recommended to make the name of the property as unambiguous as possible.

When the property is selected, M-Files automatically adds the text content to the document. You should bear this in mind when you define the reason and meaning for the signature.
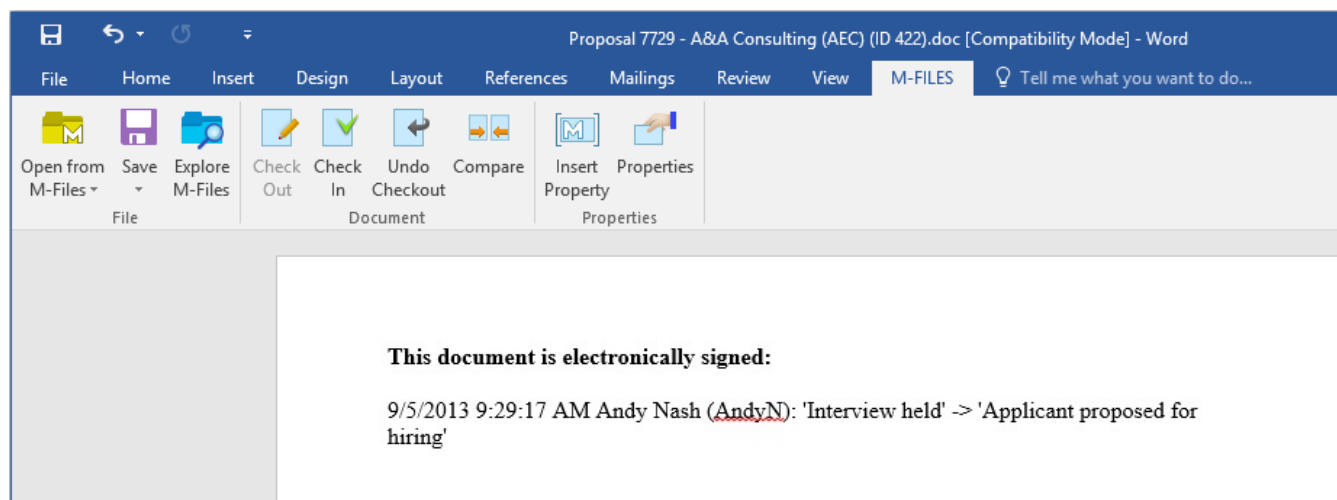
Figure 102: The signature content (manifestation) can be added to Office documents by using the "Insert Property" function.

> 📄 **Note:** If the signature is inserted in the Office document and you want to cancel the state transition, you should cancel it manually by removing the property value (signature manifestation) or the property itself, in order for the cancellation to apply for the document. In most cases, rolling back this kind of state transition to the previous state requires system administrator rights.

Trigger

You can define a trigger to automatically initiate a state transition when certain conditions are fulfilled. For example, you can set a state transition to take place when all the assignments of the current workflow state are completed or approved.

▶ Video: *Automatic State Transitions*

Automatic state transitions are executed by the server, ignoring user permissions. This means that permissions can be used to prevent users from manually initiating a state transition, ultimately executed by M-Files Server when all the assignees have completed the task.

Figure 103: Triggers can be used for automating workflow phases.

Using various criteria for the automatic transition

An automatic state transition can be configured to take place when an object fulfills certain conditions. You can configure, for example, the object to be moved to the next state when it is given a certain property or certain property value. For example, in the message process workflow, you can define that when a date is added to the *Sent* field for the document, the document will automatically be changed to the *Sent* state.

You can also set the state to be changed after all separate assignments are completed, approved, or rejected. Alternatively, you can specify custom criteria for the state change. For more information about filter settings, refer to *Filter Settings* on page 148.

Using a user-defined script for the automatic transition

The state transition can also be triggerd via a user-defined script. This allows you to specify the transition conditions in more detail by using variables, generic features of VBScript and M-Files API. For example, you can define several state transitions related to the properties and property values at the same time.

The following M-Files variables can be used in this script: `StateID`, `StateTransitionID`, `AllowStateTransition`, `NextStateID`, `ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `PropertyValues`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`. For more information about variables, refer to *VBScript Variables Explained* on page 402.

> 📄 **Note:** The documentation for the M-Files API is located in **Start** > **Programs** > **M-Files** > **Documentation** > **M-Files API**. For more information about VBScript code and M-Files API, go to *www.m-files.com/api*. Instructions on writing VBScript code and working with the M-Files API are available for a separate fee from M-Files customer support (*support@m-files.com*).

Evaluation priority

The evaluation priority enables you to define the priority in which parallel state transitions are evaluated on M-Files Server. The priority is sorted from the lowest to the highest number, zero (0) representing the highest priority.

9.6. Named Access Control Lists

A named access control list is a list of permissions that can be attached to an object. It is a list consisting of one or more subjects (users, user groups, or *pseudo-users* on page 88) and operations (delete, edit, read, or change permissions) that are either allowed or denied to those particular subjects. Named access control lists make managing permissions in M-Files very quick and effortless.

▶ Video: *Named Access Control List Permissions*

Creating a New Named Access Control List

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select the **Named Access Control Lists** node.

5. Click **New Named Access Control List...** on the task area.

   ✅ The **Named Access Control List Properties** dialog is opened.
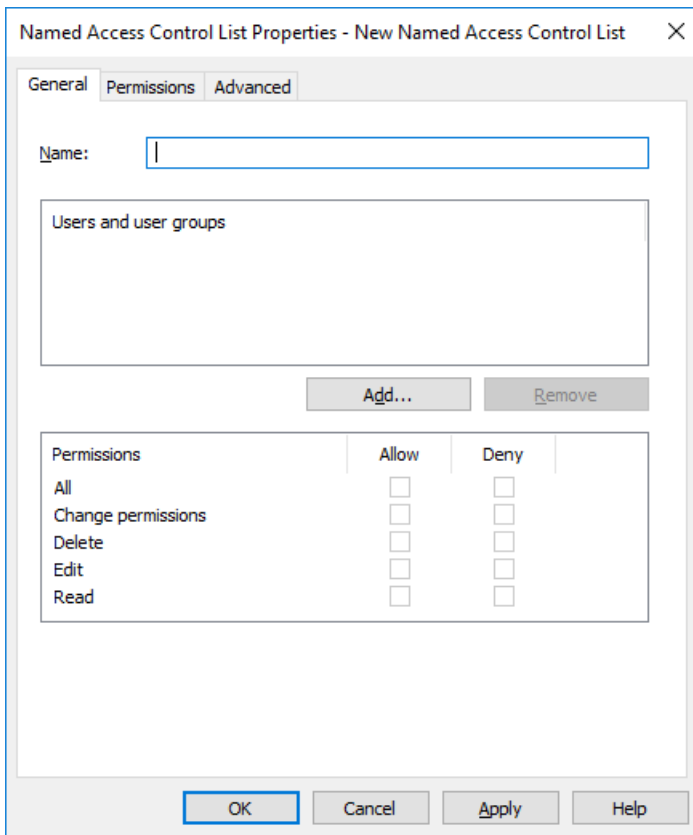
6. In the **Name** field, enter a descriptive name for the named access control list.

   ✎ It is recommended to name the named access control list according to the members of the list and the permissions given to them, such as *Visible to company management only* or *Full control for all internal users*.

7. Click **Add...** to add users or user groups to this named access control list.

   ☑ The **Select Users or User Groups** dialog is opened.
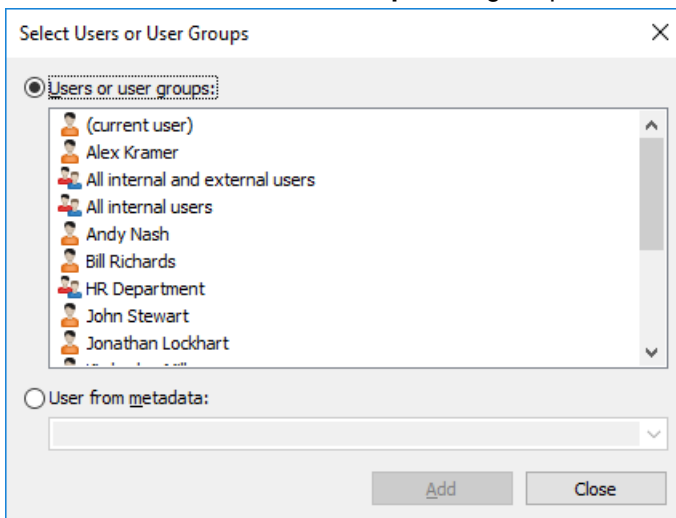
8. Select either:

    a. The **Users or user groups** option and select the users or user groups that you wish to add to this named access control list.

> 📄 **Note:** You can select more than one item at once by holding down the Ctrl key to select multiple individual items or by holding down the ⇧ Shift key to select adjacent items on the list.

    or

    b. The **User from metadata** option and use the drop-down menu to select the property containing users or user groups on the basis of which permissions are granted. For more information, see *Pseudo-users* on page 88.

9. Click **Add** to add the selected users or user groups to the named access control list and to close the **Select Users or User Groups** dialog.

10. Back in the **Named Access Control List Properties** dialog, select the user or user group whose permissions you want to adjust from the **Users and user groups** list.
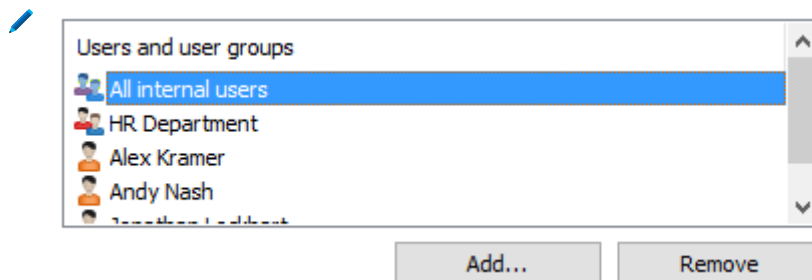
11. Select the permission that you want to adjust and check either:

    a. The **Allow** option check box if you want to allow the selected permission for the user or user group.

    or

    b. The **Deny** option check box if you wanto to deny the selected permission for the user or user group.

12. If you want to adjust additional permissions, repeat the steps *10* on page 341 and *11* on page 341.

13. Optional: On the **Permissions** tab, you can specify the users who can see this named access control list.

14. Optional: On the **Advanced** tab, you can specify an alias for the named access control list. For more information, see *Associating the Metadata Definitions* on page 203.

15. Click **OK** to finish creating the named access control list.

The new named access control list containing a set of permissions can now be attached to an object using the permission control on the metadata card.
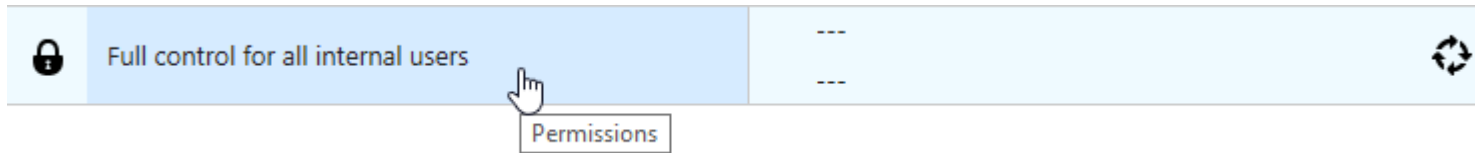
Modifying Named Access Control Lists

When you modify a named access control list, the modified permissions are applied to either new and existing objects to which the named access control list is already attached or to new objects only, depending on your choice.

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Highlight the **Named Access Control Lists** node.

   ✓ The list of named access control lists in the selected vault is opened in the right-side pane.

5. In the **Named Access Control Lists** list, right-click the item that you want to edit and select **Properties** from the context menu.

   ✓ The **Named Access Control List Properties** dialog is opened.

6. Optional: On the **General** tab, click **Add...** if you wish to add a new user or user group to this named access control list.

7. Select the user or user group whose permissions you wish to adjust from the **Users and user groups** list.

8. Depending on your choice, select either the **Allow** or **Deny** option for the desired operations.

9. Click **OK** once you are done to close the **Named Access Control List Properties** dialog.

10. Optional: If the selected named access control is already used in the permissions of one or more objects, the **Confirm Update** dialog is opened.

    a. Click **Change Objects' Permissions** if you *wish to apply your changes to the permissions of existing objects* that use the selected named access control list in their permissions.

       or

    b. Click **Preserve Objects' Permissions** if you *do not wish to apply your changes to the permissions of existing objects* that use the selected named access control list in their permissions.

The changes you have made are to the named access control list are saved and applied, depending on your choice, to new and existing objects that employ the selected named access control list or to new objects only.

Permissions

Access for viewing the selected access control list can be defined on the *Permissions* tab. The selected list can be made invisible to certain users.

📄 **Note:** The system administrator and all users with full administrative access to the document vault in question always see all the named access control lists.

Adjusting Permissions

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, highlight the appropriate node or subnode of the vault and select the desired item from the list on the right.

5. Right-click the item and select **Properties** from the context menu.

6. Go to the **Permissions** tab.

7. From the **Users and user groups** list, select the user or user group whose permissions you want to adjust.

ⓘ If the user or user group is not on the list, click **Add...** to add the user or user group to the list.

8. Either:

   a. Check the **Allow** check box to allow the selected user to see this item.

   or

   b. Check the **Deny** check box to deny the selected user from seeing this item.

9. Optional: If you want to adjust additional permissions, repeat the steps 7 and 8.

10. Click **OK** once you are done.

You have adjusted the view permissions of the selected item for the selected users.

9.7. Connections to External Sources

Here we look into using connections to external file, scanner and e-mail sources in conjunction with your M-Files vault, and for importing new content to the vault.

External File Sources

By using *connections to external sources*, you can import or link files from external file sources to M-Files and significantly speed up the launch of M-Files. You can, for example, create a link between an existing network drive and M-Files, which makes it possible to modify files both in M-Files and externally to M-Files, using the network drive.

You can also import files from an external source. Importing involves copying the files to M-Files. This means that modifying imported files to M-Files does not affect the original files.

You can also use this function to create a link between M-Files and, for example, a scanner. The M-Files server can be set to import new files from a source folder where scanned documents are saved. For more information, refer to *Scanner Sources* on page 358.

▶ Video: *Import Files*

Creating a New Connection to an External Source

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Connections to External Sources** and then select **File Sources**.

5. Click **New File Source...** on the task area to start creating a new connection to an external source.

   ☑ The **Connection Properties** dialog is opened.

6. In the **Description** field, provide a description for the new connection. You can, for example, describe the external source for which this connection is used.

7. In the **Path from the server** field, enter the path to the external location that you wish to connect to M-Files. The location can be, for example, a network drive of a scanner.

   ⓘ The path must be specified from the point of view of the M-Files server.

8. Optional: Check the **Include subfolders** option check box if you wish to include in the connection the entire folde structure of the path specified.

9. Click **Set Account...** to specify an account in M-Files to be used for processing files from the external location.

   ⓘ By default, M-Files uses the server identity (**Local System account**) as the account.

10. Optional: Click **Filters...** to define the files to be processed.
    a) In the **Include files that match any of the following filters** field, enter the filter or filters for the files that are to be included via this connection.
    b) In the **Exclude files that match any of the following filters field,** enter the filter or filter for the files that are to be excluded from this connection.

    ⓘ By default, all files are included except for BAK and TMP files.

    ⓘ You may use wildcards to define a filter (for example, `*.*` or `*.docx`). Multiple filters are separated with semicolons (`;`).

11. Select either:

    a. **Link files**: Select this option if you wish to modify the files of the external source both in M-Files and externally. Modifications made in M-Files are also visible to external users, and modifications made outside M-Files are visible in M-Files. M-Files will store a version history of the linked documents, so that at least all versions modified in M-Files will be available for future use.

       or

    b. **Import files**: Select this option if you want the files of the external source to be copied to M-Files. Modifying imported documents in M-Files will not have an effect on the original files.

       You may also check the **Delete source file after importing** option check box if you want the source files to be deleted after they have been imported to M-Files. This option may be useful, for example, when importing scanned documents to M-Files.

12. Optional: Check the **Preserve folder structure** option check and in the **Target folder** field, enter a target folder for the external files if you wish to preserve the original folder structure of the external source in M-Files using traditional folders.

    ⓘ You may click the ► (right-pointing triangle) icon to refresh the list of traditional folders or to add a new traditional folder to the vault.

13. Optional: Check the **Check for new and deleted files periodically** option check box if you want M-Files to automatically check the source folder at predefined intervals and update itself according to which files and folders are new and which have been deleted. Enabling this option makes any changes in the source folder automatically visible in M-Files as well.
    a) In the **Delay between checks** field, enter the interval in seconds between the automatic source folder checks to define how frequently you want M-Files to check the changes made to the source folder.

14. Optional: You may click **Refresh Now** to connect to the external source immediately.

    ⓘ Click **Refreshing Status...** to display additional information about the process of refreshing the external source.

15. Optional: On the **Metadata** tab, define the metadata to be added for externally created objects.

    ⓘ For more information, see *Defining Metadata for an External File Source* on page 346.

16. Optional: On the **Advanced** tab, you can specify an alias for the new connection.

> ⓘ For more information, see *Associating the Metadata Definitions* on page 203.

17. Click **OK** to finish creating the new connection.

The new connection to an external source is created and added to the **File Sources** list. Files are added from the external source to M-Files on the basis of the settings you have defined for the connection.

> 📄 **Note:** If the user groups *All internal users* or *All internal and external users* do not have edit permissions for a linked document, it will not be available in M-Files. This behavior can be prevented by enabling the following registry setting on the M-Files Server computer:

Key	`HKLM\Software\Motive\M-Files\<version>\Server\MFServer`
Value	`IgnoreACLsForExternalLinks`
Value type	REG_DWORD
Value data	`1`

The default behavior can be restored by setting the value data to `0`.

Defining Metadata for an External File Source

Follow these steps to define automatic metadata for externally created documents.

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Connections to External Sources** and then select **File Sources**.

5. On the **File Sources** list, double-click the file source that you want to edit.

> ✅ The **Connection Properties** dialog is opened.

6. Click the **Metadata** tab.

   ✓ The **Metadata** tab is opened.

7. Using the **Object type** drop-down menu, select the object type that the external objects get when they are imported or linked to M-Files.

8. Click **Add...** to define a new property and value to be added automatically for objects created from external files, or select one of the existing properties and click **Edit...** to edit it.

   ✓ The **Define Property** dialog is opened.

9. In the **Define Property** dialog, select one of the following options:

   a. **Use a fixed value**: Use this option to select a fixed property value.

      or

   b. **Read from an XML file produced by HP DSS**: Use this option if you want to obtain a property value from user-provided metadata when a document is scanned and OCRed using HP DSS.

      or

   c. **Read from an XML file**: Use this option to read a property value from an XML file using an XPath expression. XPath is a W3C standard syntax for defining locations in an XML document. For more information on XPath syntax, see *http://www.w3schools.com/xsl/xpath_syntax.asp*.

      or

   d. **Use an OCR value source**: Click **Define...** to define a zone in a scanned document from which to capture the property value. For detailed instructions, see *Defining an OCR Value Source* on page 350.

10. If the selected property is of the **Choose from list** data type, and you chose **Read from an XML file produced by HP DSS**, **Read from an XML file** or **Use an OCR value source** in the previous step, in the **Conversion to value list item** section, select either:

   a. **Use the value read as the ID of the item**: Select this option if you want to use the captured value as an identifier of the value list item with a separately defined name.

      or

   b. **Use the value read as the name of the item**: Select this option if you want to use the captured value as the name of the value list item. You can check the **Add a new item to the list if a matching item is not found** option check box if you want to add a new value list item whenever a new value is captured.

11. Click **OK** to close the **Define Property** dialog.

12. Use the **Permissions** drop-down menu to set the permissions for new objects created via the external source.

ⓘ You can click the **...** button to refine the permission settings.

13. Optional: Check the **Read values from an XML file** option check box if you property values to be read from an XML file. Check also the **Delete the XML file after use** option check box if you want the XML file to be deleted after the metadata has been read.

ⓘ The name of the XML file must match the name of the file to be imported. The supported XML formats are:

- Regular XML data
- XML data output by HP Digital Sending Software (DSS)

14. Click **OK** to finish defining the metadata.

The metadata that you have just defined is assigned to any new object created via this external source.

Defining an OCR Value Source

You can extract text or barcodes from a scanned document using optical character recognition (OCR) and use them as automatic property values for files imported from an external source, a scanner in this case. The OCR value source is a zone defined on a scanned page. For more information on defining different properties for objects imported from external file sources, see *Defining Metadata for an External File Source* on page 346.

The use of an OCR value source is only possible when using an external source. The OCR value source cannot be defined in M-Files Desktop.

📝 **Note:** The *M-Files OCR module* is an M-Files add-on product available for extra fee. It can be activated with a license code. The old license code must be replaced by the license code that enables the use of OCR. For more information, refer to *License Management* on page 179. In order to enable OCR, you need also to download and install some additional files to your M-Files Server (for further information, contact our *customer support*). The OCR related functions will then be available in M-Files Admin and M-Files Desktop. M-Files uses an OCR engine offered by I.R.I.S. For *the M-Files OCR module* purchase inquiries, please contact our sales team at *sales@m-files.com*.

📝 **Note:** You can use the OCR value source without enabling the **Use OCR to enable full-text search of scanned documents** option in the **Searchable PDF** tab.

Do the following steps to define an OCR value source:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Connections to External Sources** and then select **File Sources**.

5. On the **File Sources** list, double-click the file source that you want to edit.

☑ The **Connection Properties** dialog is opened.
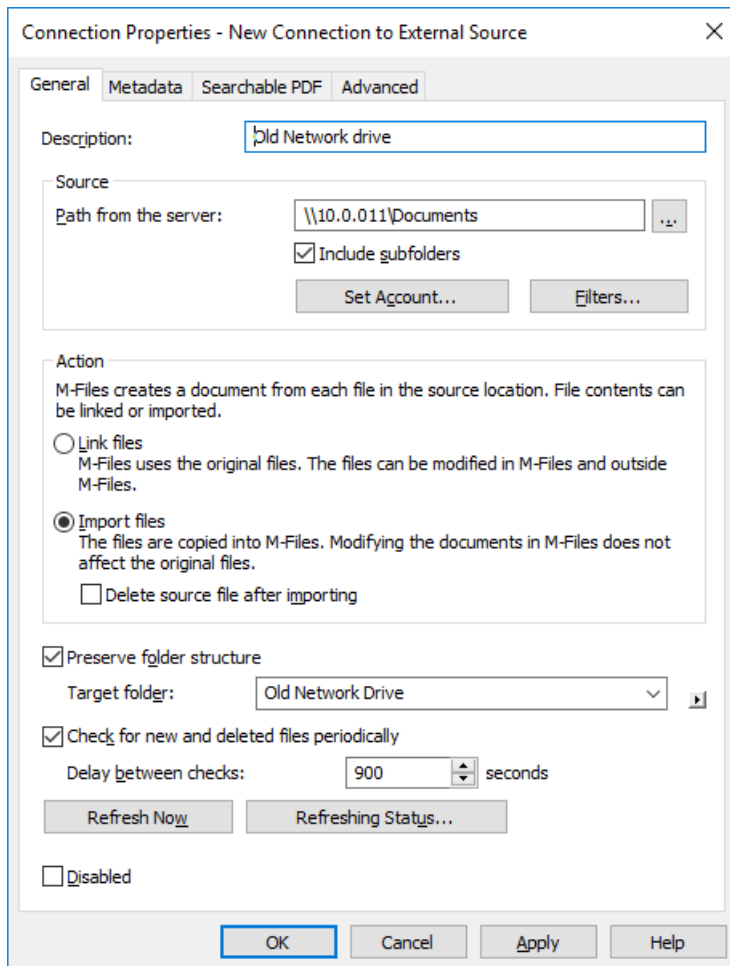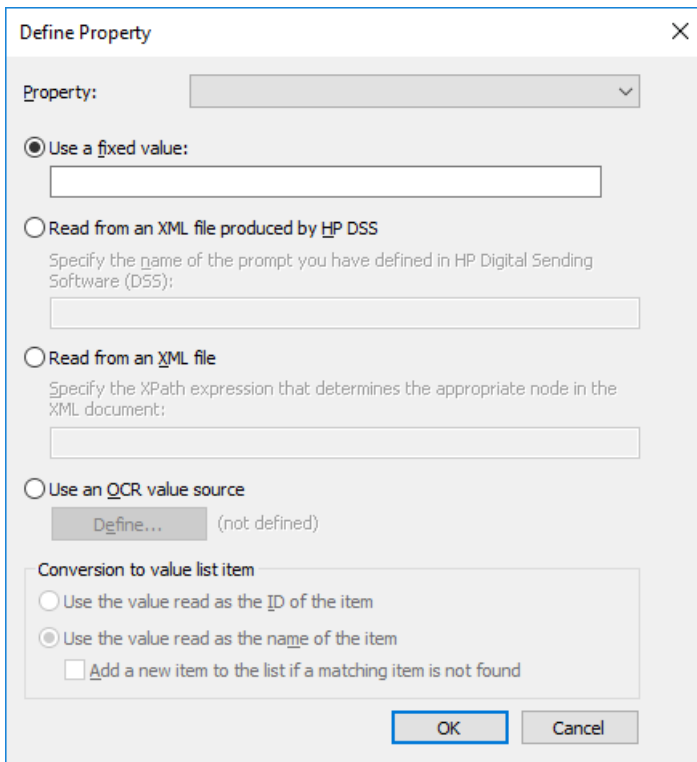
6. Click the **Metadata** tab.

☑ The **Metadata** tab is opened.
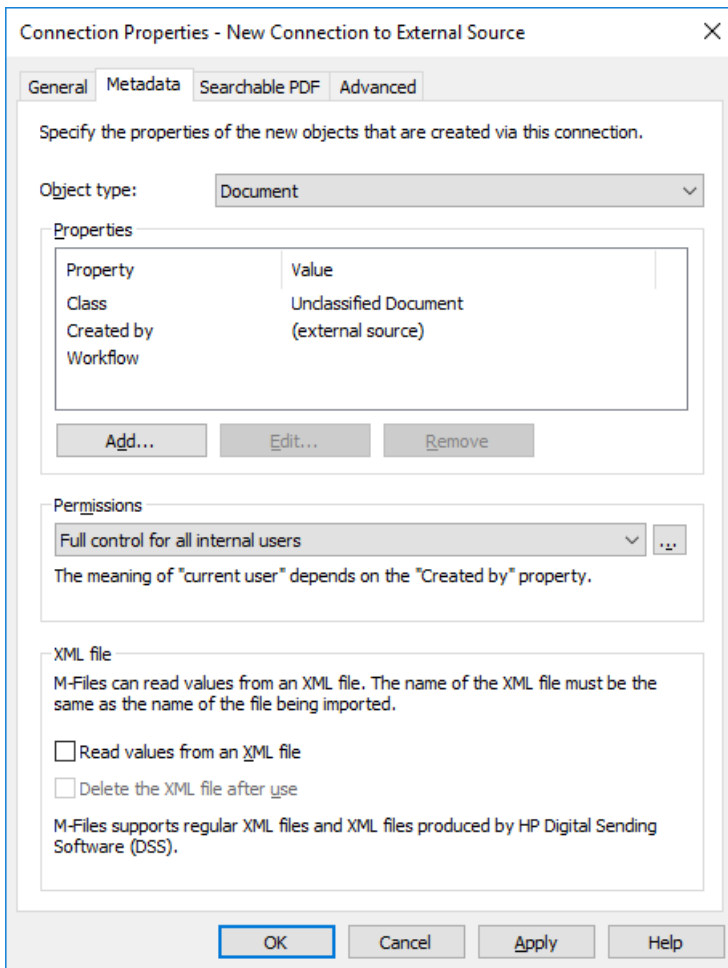
7. Click **Add...** to define a new property and value to be added automatically for objects created from external files, or select one of the existing properties and click **Edit...** to edit the existing property.

☑ The **Define Property** dialog is opened.

8. Select the option **Use an OCR value source** and click the **Define...** button.

   ☑ The **OCR Value Source Definition** dialog is opened.

9. In the **Zone type** section, select either:

a. **Text**: Select this option if the OCR zone contains text.
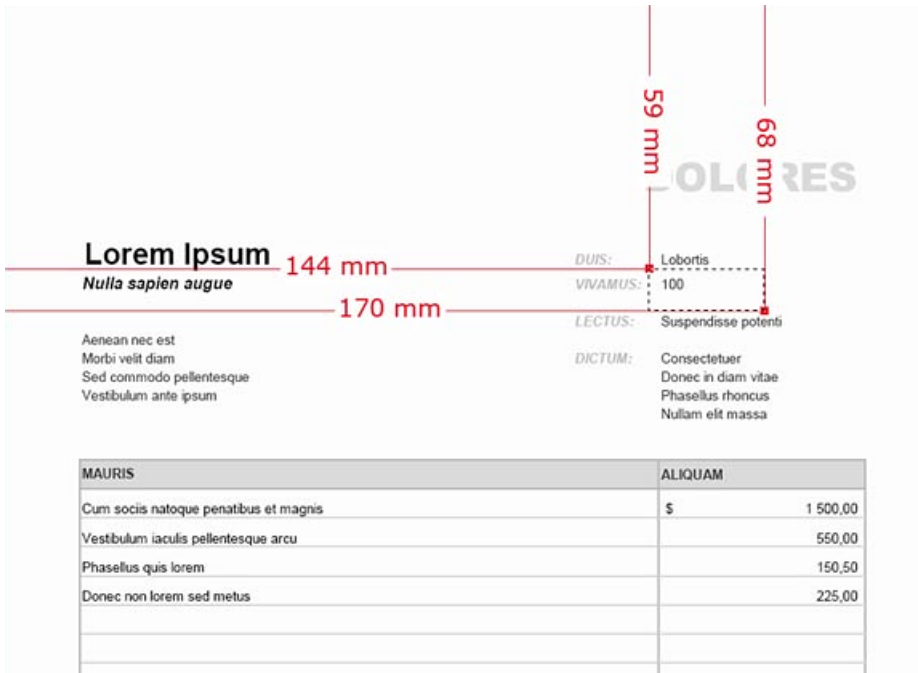
or

b. **Barcode**: Select this option if the OCR zone contains a barcode.

> 📄 **Note:** M-Files recognizes most of the 1D barcodes in use and two types of 2D bar code: PDF417 and QR Code. If you are using an OCR supported license code that has been delivered before the version 9.0, please ask our customer service to provide you a new license code if you want to use barcode recognition.

10. In the **Zone position** section, define a zone from which to extract a value for the selected property. The characters may include any letters, numbers or punctuation marks. For example, an invoice number shown on a page can be added as the *Invoice number* property value for the scanned document.

> ✏️ An example of a zone definition:

> ℹ️ If you are capturing a barcode and there is only one barcode to recognize on the page, you can specify the whole page as the zone. If there are several barcodes, restrict the zone in a such a way that it contains the desired barcode only. With QR codes, you should specify a zone larger than the actual barcode. If the specified zone has several barcodes, all of them are considered to be a property value.

a) In the **Page** field, enter the page number of the scanned document that you want to use as the OCR value source.
b) Using the **Unit** options, select the appropriate unit for defining the zone position.
c) In the **Left** field, enter the left corner position of the OCR zone. The left corner of the scanned document is considered "0".
d) In the **Right** field, enter the right corner position of the OCR zone.
e) In the **Top** field, enter the top corner position of the OCR zone. The top corner of the scanned document is considered "0".
f) In the **Bottom** field, enter the bottom corner position of the OCR zone.

11. Using the **Primary language** and **Secondary language** drop-down menus, select the primary and secondary language of the documents scanned via this external connection in order to improve the quality of

the recognition results. The list of secondary languages only contains languages that are allowed to be used with the selected primary language.

ⓘ Although the OCR automatically recognizes all Western languages and Cyrillic character sets, specifying a language selection often improves the quality of the text recognition results. In ambiguous cases, a problematic recognition result may be resolved by a language-specific factor, such as recognition of the letter 'Ä' in Finnish. The list of secondary languages only includes languages that are allowed to be used together with the selected primary language.

12. Click **OK** to close the **OCR Value Source Definition** dialog.

13. Back in the **Define Property** dialog, select either:

a. **Use the value read as the ID of the item**: Select this option if you want to use the captured value as an identifier of the value list item with a separately defined name.

or

b. **Use the value read as the name of the item**: Select this option if you want to use the captured value as the name of the value list item. You can check the **Add a new item to the list if a matching item is not found** option check box if you want to add a new value list item whenever a new value is captured.

14. Click **OK** to close the **Define Property** dialog.

The zone you have just defined is used to automatically extract a value for the selected property using OCR whenever a new object is created via the selected external file source.

To ensure that the defined zone is correctly positioned, in most cases the document to be scanned should be placed onto the scanner glass by hand rather than fed via an automatic sheet feeder.

In some cases, the OCR may give an incorrect recognition result of the text: for example, depending on the font type or size, the number *1* may be interpreted as the letter *I*. To ensure that the characters are added correctly to the document metadata, you can check the property values with event handlers and VBScript. You can then use VBScript to check, for example, that all added characters are numbers. For more information, see *Event Handlers* on page 240.

Searchable PDF

M-Files can convert images imported from external file sources into *searchable PDFs*. This makes full-text search of scanned documents possible. After conversion, you can find the PDF document by searching the actual document content.

Text recognition can be performed on the following file formats: TIFF, JPEG, BMP, PNG, and PDF. TIFF files using an alpha channel or JPEG compression are not supported.

📄 **Note:** Converting the file to a searchable PDF does not affect the outward appearance of the document when viewing it. The users still see the original scanned image. M-Files stores the automatic text recognition results in the PDF as invisible text, which is used when searching the file. Possible text recognition inaccuracies will not affect the appearance of the scanned document in any way when viewed on screen or printed.

📄 **Note:** The *M-Files OCR module* is an M-Files add-on product available for extra fee. It can be activated with a license code. The existing license code must be replaced by the new license code to enable use of the M-Files OCR. For more information, refer to *License Management* on page 179. The OCR related functions will then become available in M-Files Admin and M-Files Desktop. M-Files uses an OCR engine offered by I.R.I.S. To purchase the M-Files OCR module, please contact our sales team at *sales@m-files.com*.

Do the following steps to convert images from an external file source into searchable PDFs:
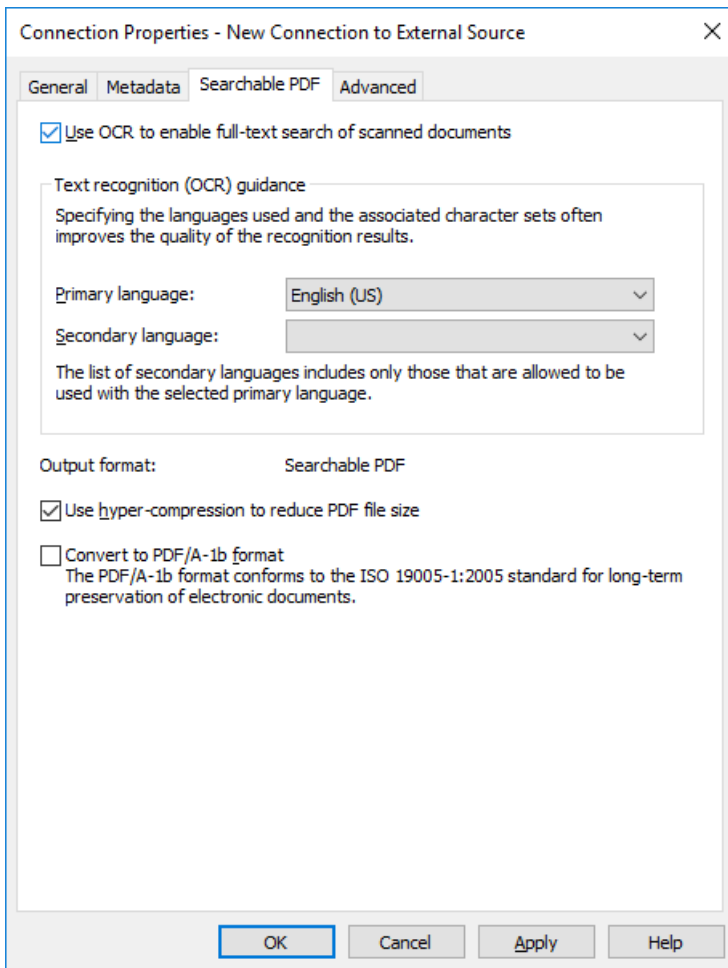
1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Connections to External Sources** and then select **File Sources**.

5. On the **File Sources** list, double-click the file source that you want to edit.

   ✓ The **Connection Properties** dialog is opened.

6. Click the **Searchable PDF** tab.

   ✓ The **Searchable PDF** tab is opened.

7. Check the **Use OCR to enable full-text search of scanned documents** option check box.

8. Using the **Primary language** and **Secondary language** drop-down menus, select the primary and secondary language of the documents scanned via this external connection in order to improve the quality of the recognition results. The list of secondary languages only contains languages that are allowed to be used with the selected primary language.

   ⓘ Although the OCR automatically recognizes all Western languages and Cyrillic character sets, specifying a language selection often improves the quality of the text recognition results. In ambiguous cases, a problematic recognition result may be resolved by a language-specific factor, such as recognition of the letter 'Ä' in Finnish. The list of secondary languages only includes languages that are allowed to be used together with the selected primary language.

9. Optional: Check the **Use hyper-compression to reduce PDF file size** option check box if you want to reduce the file size of the searchable PDFs created via this connection.

10. Optional: Check the **Convert to PDF/A-1b format** option check box if you want the converted PDF documents to comply with the ISO standard 19005-1:2005 for long-term preservation of electronic documents.

    ⓘ PDF/A-1b is a more restricted format than the format of standard PDF files, so the file size of documents converted to PDF/A is often larger than that of files converted to standard PDF. In addition, by exporting to PDF/A, certain advanced appearance settings may be omitted. You should use conversion to PDF/A form only if it is particularly necessary due to, for example, the requirements for long-term preservation.

11. Click **OK** to close the **Connection Properties** dialog.

The documents scanned via this connection are converted into searchable PDFs provided that they are in the applicable file format. After they have been imported or linked to M-Files, you can find them by searching for their content.

> 📄 **Note:** Text recognition can also be performed via M-Files Desktop. For more information, refer to *Scanning and Text Recognition (OCR)* on page 116. If you wish to use text recognition using external sources through the M-Files Admin only, this limitation can be set by changing the registry settings. The registry settings can be used to set other limitations as well. For more information on registry settings, contact M-Files customer support at *support@m-files.com*.

Scanner Sources

Via the scanner connection, it is easy to save paper documents into the document vault. This way, the M-Files search capabilities can be applied also to scanned paper documents.

When using external sources, M-Files does not communicate directly with the scanners but uses an external connection to read the file produced by the scanner from, for instance, the scanner's network drive. The connection is configured in M-Files Admin under *External File Sources* on page 343.

These connections can be made, for example, with Hewlett-Packard MFP series devices by using HP Digital Sending Software (DSS). In this case, the device is connected directly to the local area network and the user scans the paper document with the device.

It is also possible to enter metadata via the device's touchscreen. The scanned file and the metadata are sent to the DSS software performing optical character recognition (OCR) for the file. The scanned image and recognized text are combined into a PDF file. The PDF file and an XML metadata file are saved in a folder controlled by M-Files via external location configuration. On detecting new files, M-Files transfers the files to the document vault as documents with metadata.

For instructions on how to use a scanner as an external source for M-Files, see *Creating a New Connection to an External Source* on page 344.

> 📄 **Note:** Text recognition can also be performed with the M-Files OCR module. For more information, refer to *External File Sources* on page 343. You can also scan using a local scanner that is directly connected to your computer. For more information, refer to *Scanning and Text Recognition (OCR)* on page 116.

Mail Sources

M-Files provides the opportunity to save, manage, and share important e-mail in a controlled manner. The messages can be transferred directly and automatically from the mail server to the document vault.

For example, messages and their attachments sent to the organization's common e-mail box can be transferred directly to the document vault. In the document vault, imported messages can be handled in a controlled manner via, for example, workflow features. Example use cases include a centralized and controlled way for handling orders, and a systematic method for archiving sent offers. Important information can thus be managed in M-Files so that it does not get lost and forgotten in e-mail boxes.

The organization may also want to save important sent e-mail to M-Files. Such important messages could include, for instance, proposals and order confirmations. Your organization can use a designated *archive* e-mail account to which M-Files is connected. From this box, M-Files imports all e-mail to the document vault and then deletes the messages from the mail server. Important sent messages can be archived in M-Files by sending the message to the archive box via the *Cc* or *Bcc* fields. To avoid junk mail, it is possible to set the e-mail account to accept mail from internal users only.

▶ Video: *Email Monitoring*

Creating a New Connection to a Mail Source

Do the following steps to create a new connection to a mail source:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Connections to External Sources** and then select **Mail Sources**.

5. Click **New Mail Source...** on the task area.

   ☑ The **Connection Properties** dialog is opened.

Connection Properties - New Connection to External Source	✕

   General Metadata Advanced

   Description: [   ]

   ┌ Source ──────────────────────────────────────┐
   │ Server type: ○ POP3   ◉ IMAP   │
   │ Mail server: [   ] │
   │   ☐ Use encrypted connection (SSL/TLS) │
   │ Port number: [143]   Folder: [Inbox]   │
   │ Login information: │
   │ Username: [   ]   │
   │ Password: [   ]   │
   └──┘

   ┌ Action ──────────────────────────────────────┐
   │ M-Files creates a document from each imported message. │
   │ ☑ Include attachments   │
   │ ☐ Import only messages that have attachments   │
   │ ☐ Delete message from server after importing   │
   │ ☐ Remove attachments from server after importing │
   │ ☑ Save in Outlook message format (*.msg)   │
   │ ☑ Separate attachments from the message   │
   │   │
   └──┘

   ☑ Check for new and deleted files periodically
   Delay between checks: [900] ⬍ seconds
   [Refresh Now]   [Refreshing Status...]
   ☐ Disabled

   [OK]   [Cancel]   [Apply]   [Help]

6. In the **Description** field, enter a description for the new connection.

7. Select either:

   a. **POP3**: Use this option if the protocol for connecting to the mail server is POP3.

   or

    b. **IMAP**: Use this option if the protocol for connecting to the mail server is IMAP.

8. In the **Mail server** field, enter the network address of the mail server (the IP address or the domain name, such as *mail01.company.com*).

9. Optional: Check the **Use encrypted connection (SSL/TLS)** option check box to use an encrypted connection to the mail server.

10. In the **Port number** field, enter the port number of the mail server.

11. If you selected **IMAP** as the protocol, enter the folder on the server from which mail is read and imported in the **Folder** field.

12. In the **Username** field, enter the username for connecting to the mail server in the format *user@domain* (for example, *sam@company.com*).

13. In the **Password** field, enter the password for connecting to the mail server.

14. Optional: In the **Action** section, select the appropriate options:

Select the option...	If you want to...
Include attachments	Import attachments along with e-mail messages.
Import only messages that have attachments	Import to the vault only the e-mail messages that have attachments. Messages without attachments will not be imported.
Delete messages from server after importing	Remove the messages from the mail server automatically once they have been imported to M-Files.
Remove attachments from server after importing	Remove attachments from the mail server once e-mail messages have been imported to M-Files. This option can be enabled only if the selected protocol is **IMAP** and the option **Include attachments** is enabled.
Save in Outlook message format (*.msg)	Save the e-mail messages to M-Files in the Outlook message format (*MSG*). Attachments are stored inside the *MSG* file and the messages appear in M-Files as single-file documents (see *Single-File and Multi-File Documents* on page 80). 📄 **Note:** This functionality requires Microsoft Exchange Server or a 32-bit MAPI client to be installed on the server running M-Files Server.
Separate attachments from the message	Save attachments separately from the body of the message. This option can be enabled only if the option **Save in Outlook message format (*.msg)** is enabled. The message without its attachments is saved into an MSG file, and any attachments are stored beside the MSG file in their original file formats. If the message contains attachments, the message and its attachments appear in M-Files as a multi-file document.

15. Optional: Check the **Check for new and deleted files periodically** option check box to enable M-Files to synchronize with the mail server at predefined intervals.

    a) In the **Delay between checks** field, enter the time interval in seconds between synchronizations.

16. Optional: Click **Refresh Now** to synchronize the vault with the mail server right away.

    ℹ️ You can click **Refreshing Status...** to see the current status of the refreshing process.

17. Optional: On the **Metadata** tab you can define properties for new objects created via this connection.

    ℹ️ For more information, see *Defining Automatic Metadata for a Mail Source* on page 361.

18. On the **Advanced** tab you can set an alias for this connection.

    ℹ️ For more information, see *Associating the Metadata Definitions* on page 203.

19. Click **OK** to finish creating the connection.

E-mail messages are imported to M-Files from the defined mail source according to the settings specified.

Defining Automatic Metadata for a Mail Source

You can define automatic metadata for new objects created from an external mail source. You can use fixed property values or extract property values from the imported e-mail messages.

Do the following steps to define automatic metadata for objects created from an external mail source:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, expand **Connections to External Sources** and then select **Mail Sources**.

5. On the **Mail Sources** list, double-click the source that you want to edit.

    ☑ The **Connection Properties** dialog is opened.

Connection Properties - New Connection to External Source   ✕

General   Metadata   Advanced

Description: [   ]

┌─ Source ───┐
│ Server type: ○ POP3   ◉ IMAP   │
│ Mail server: [   ]│
│   ☐ Use encrypted connection (SSL/TLS)│
│ Port number: [143   ]   Folder: [Inbox   ]│
│ Login information: │
│ Username: [   ]│
│ Password: [   ]│
└───┘

┌─ Action ───┐
│ M-Files creates a document from each imported message.│
│ ☑ Include attachments   │
│ ☐ Import only messages that have attachments   │
│ ☐ Delete message from server after importing   │
│ ☐ Remove attachments from server after importing   │
│ ☑ Save in Outlook message format (*.msg)   │
│ ☑ Separate attachments from the message   │
│   │
└───┘

☑ Check for new and deleted files periodically
    Delay between checks: [900   ] ⬍ seconds

    [Refresh Now   ]   [Refreshing Status...]

☐ Disabled

        [OK]   [Cancel]   [Apply]   [Help]

6. Click the **Metadata** tab.

☑ The **Metadata** tab is opened.

7. Use the **Object type** drop-down menu to select the object type for new objects created via this connection.

8. Use the **Permissions** drop-down menu to select the permissions for new objects created via this connection.

   ⓘ You can click the **...** button to refine the permission settings.

9. In the **Properties** section, click **Add...** to add a new automatic property for objects created via this connection or select one of the existing properties and click **Edit...** to edit it.

   ✓ The **Define Property** dialog is opened.

10. Select either:

   a. **Use a fixed value**: Use this option to add a fixed value for the selected property.

      or

   b. **Read from the e-mail message**: Use this option to extract a value from the e-mail message for the selected property.

11. If the selected property is of the **Choose from list** data type, in the **Conversion to value list item** section, select either:

   a. **Use the value read as the ID of the item**: Select this option if you want to use the extracted value as an identifier of the value list item with a separately defined name.

      or

   b. **Use the value read as the name of the item**: Select this option if you want to use the extracted value as the name of the value list item. You can check the **Add a new item to the list if a matching item is not found** option check box if you want to add a new value list item whenever a new value is extracted.

12. Click **OK** to close the **Define Property** dialog.

The e-mail messages imported to M-Files via this connection are assigned automatic properties according to the settings that you have defined.

9.8. Event Log

The Event Log logs document vault events, such as new object creations and user logins.

To enable logging, select *Enable Event Logging* via the task area. Events can be viewed and organized in any desired order.

Event logging must be enabled to send notifications. For more information about notifications, refer to *Notification Settings (M-Files Admin)* on page 181.

Showing events X–XXXX

You can browse the events page by page by using the arrow icons. A single page can display 10,000 events at maximum.

Define Filter

You can specify the events to be displayed in the list by either object type or object ID.

Export

You can export and archive all or selected events in XML file format.

Delete events X–XXXX

In addition to being able to delete all events, you can select events for listing on the page and delete them (this does not apply to filtered lists).

▶ Video: *Event Logs*

Detailed information on an individual event

Event Details provides detailed information on the saved changes.

📄 **Note:** To view more detailed information on an individual event, you must have the *Electronic Signatures* on page 367 module activated.

Figure 104: The "Event Details" window.

Number of events, and event types

If the *Electronic Signatures* on page 222 module is in use and the *Advanced Event Log features* on page 198 have been enabled, the event log records all events without any restrictions. Otherwise, the M-Files server removes the oldest events automatically if the number of events exceeds 10,000. The maximum number of events can be changed via a registry setting (for more information, contact M-Files customer support).

While M-Files offers a versatile event log, several additional event types that can be covered by logging are enabled with the Electronic Signatures module.

The following event types are recorded in the M-Files Admin event log:

Assign request	Event log cleared	Object deleted	Signature settings deleted
Backup completed	Event log exported	Object destroyed	Signature settings modified
Backup started	Event logging disabled	Object undeleted	State changed
Check-in	Event logging enabled	Object version destroyed	The state of a document or other object changed
Check-in request	File downloaded	One version of a document or other object destroyed	User created
Checkout	File downloaded via public link	Property definition deleted	User deleted
Undo checkout	Free-form request	Public link accessed	User modified
Document or other object changed	Login	Public link created	User group created
Document or other object deleted	Logout	Public link deleted	User group deleted
Document or other object destroyed	New document or other object	Restoration from backup completed	User group modified
Document vault created	New object	Rollback	Vault variable modified
Document vault created as a copy of another vault	Object changed	Signature settings added	

The Electronic Signatures module adds the following event types to the M-Files Admin event log:

Metadata structure changes:

Class changed	Named ACL deleted	State transition changed	Value list item deleted
Class created	Object type changed	State transition created	Workflow changed
Class deleted	Object type created	State transition deleted	Workflow created
Common view changed	Object type deleted	Value list changed	Workflow deleted
Common view created	Property definition created	Value list created	
Common view deleted	Property definition changed	Value list deleted	

Named ACL changed	State created	Value list item changed
Named ACL created	State deleted	Value list item created

Vault property changes:

Event handler changed

Event handler created

Event handler deleted

Event handler index changed

Other:

Application installed

Application uninstalled

Content package exported

Content package import completed

Electronic Signatures module

The *Electronic Signatures* on page 222 module includes event logging extensions and electronic signature functionality. The module is available for a separate fee. For you to activate the Electronic Signatures module, the license code must be activated on your system. The license is provided on a subscription basis. Activate or update the license code in M-Files Admin (for more information, refer to *License Management* on page 179). In addition to this, properties of the audit trail must be activated that are specific to the vault. For more information, see *Document Vault Advanced Properties* on page 197.

9.9. Reporting and Data Export

Saving and protecting data is important, but the saved data must also be available for analysis. In addition to being able to save many types of data in M-Files, you can use it to create various reports.

The reports can be used to gather information on, for example, sales processes, completed projects, the size of the proposal base, volumes of orders, participation in training, and sales by each salesperson itemized by customer. Graphical reports make the data analysis quick and easy. In real-world operation, reports can be generated from any metadata.

Updating the license code for reporting

The reporting module is an M-Files add-on product available for a separate fee. It can be activated with an accompanying license code. The reporting module enables data export from M-Files to create reports and display them in the M-Files user interface.

For you to activate the reporting module, the license code must be activated on your system. The license is provided on a subscription basis. Activate or update the license code in M-Files Admin (for more information, refer to *License Management* on page 179).

To find out how M-Files can support your business with M-Files reports, please contact us at *sales@m-files.com*.

Report object type and class

To display the reports, M-Files has a built-in object type and class for reports. By default, the *Report* object type is hidden from the users. Provide the required access rights for the *Report* object type so that actual reports can be created in the client software.

Creating a New Data Set

M-Files Reporting Data Services enable data exporting from M-Files to external databases (SQL Server). The administrator can specify manually which data will be exported, or export data on a scheduled basis from M-Files for reporting or other purposes. The *M-Files Reporting Data Services* functionality is installed in conjunction with M-Files Server. Once you have exported a data set, you can use it to generate a report.

Start by specifying a data set that you want to export for reporting. Do the following steps to create a new data set:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select **Reporting and Data Export** and then click **New Data Set...** on the task area.

☑ The **Data Set Properties** dialog is opened.
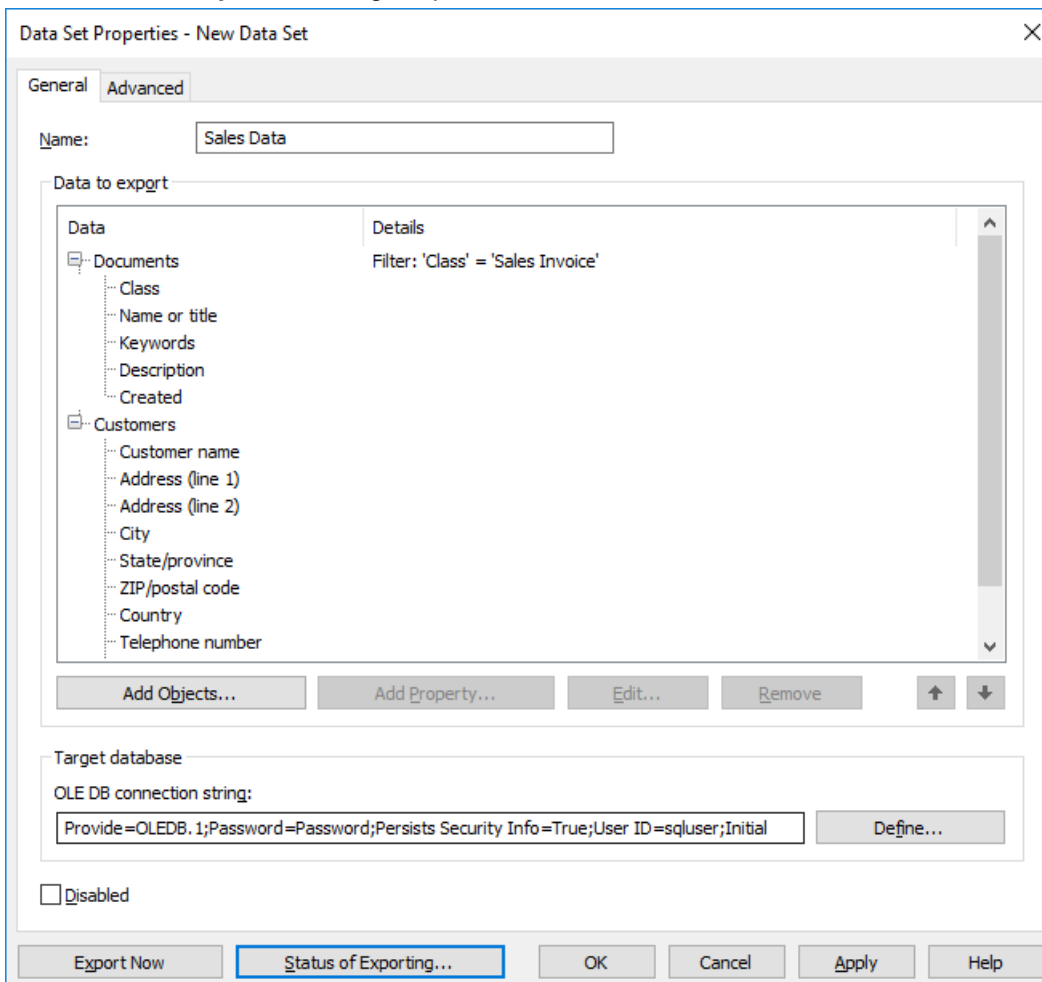
5. In the **Name** field, enter a name for the new data set.

6. In the **Data to export** section, click **Add Objects...** to select the objects to be exported.

> ✓ The **Add Objects to Data Set** dialog is opened.

7. Use the **Objects to export** drop-down menu to select the objects to be exported on the basis of the object type.

> ⓘ You can click **Filter Objects...** to refine the selected objects by specifying property conditions that the objects must meet to be exported. For more information on filtering objects by properties, see *Properties (Additional Conditions)* on page 150.

8. Optional: Select the object that you just added to the **Data to export** section and click **Add Property...** to add for the selected object type a property that you want to be exported.

   a) Use the **Property to export** drop-down menu to select the property to be exported.

   b) Go to the **History and Old Values** tab.

   > ⓘ On the **History and Old Values** tab you can define whether you want to export the change history and previous values of the selected property.

   > ✓ The **History and Old Values** tab is opened.

   c) Check the **Export the change history of this property** option check box if you want to export the change history of the selected property.

   > ⓘ The change history adds an entry of each change in the property value to the data set. This makes it possible to answer questions such as "What was the total value of deals closed in August?" by exporting the change history of the property value *Closed* and pinpointing the objects for which the value of said property changed from *No* to *Yes* during August.

   d) Check the **Export the old values of this property, using sampling** option check box if you want to export previous values of the selected property and use the **Sample at** drop-down menu to define the frequency of the sampling (daily, weekly, monthly, or yearly).

   e) Select either **Full history**, **Fixed-length period**, or **Starting from date** option to define the history length for the change history and old values of the selected property.

    ⓘ If the frequency of sampling is high (for instance daily), it is recommended to restrict the length of the history period in order to avoid expanding the database unnecessarily and to increase the speed of the export function.

  f) Click **OK** to close the **Property to Export** dialog.

9. In the **OLE DB connection string** field, enter the connection string for connecting to the target database or click **Define...** to define the connection string.

    ⓘ For more information on database connection strings, see *Connection to External Database (Object Types)* on page 263.

10. Go to the **Advanced** tab.

    ☑ The **Advanced** tab is opened.

11. Use the **Use the identity of the following user when reading data** drop-down menu to select the user whose identity you want to use for transferring data from M-Files to the reporting services.

    ⓘ The most suitable user is a "regular" user without any extended rights. If you use, for example, your own user identity that has a system administrator role, data that you do not want to expose to all users could end up in the reports displayed by the client software.

12. Optional: Check the **Export data on a scheduled basis** option check box and click **Schedule...** if you want to export this data set on a scheduled basis.

ⓘ It is recommended to schedule the data export to be performed once a day/week/month. The reports are updated at the same time. If you do not select scheduling, the data will not be updated after export. You can also create a separate update link in the reporting services so that the user can update the report in the client software whenever desired. For more information, please contact M-Files customer support at *support@m-files.com*.

13. Optional: Click **Export Now** to export the data set right away.

ⓘ You can click **Status of Exporting...** to view the status of the exporting process when the exporting is in progress.

14. Click **OK** to finish creating the new data set.

The data set that you have just defined is added to the **Reporting and Data Export** list. The data set is exported either automatically on a scheduled basis or manually, depending on the settings that you have provided.

Now that you have created a data set, you can use it to create a report (see *Creation of Reports and the Required Software* on page 372) and then create a report object in M-Files to read the report (see *Creating a Report Object for a Report* on page 373).
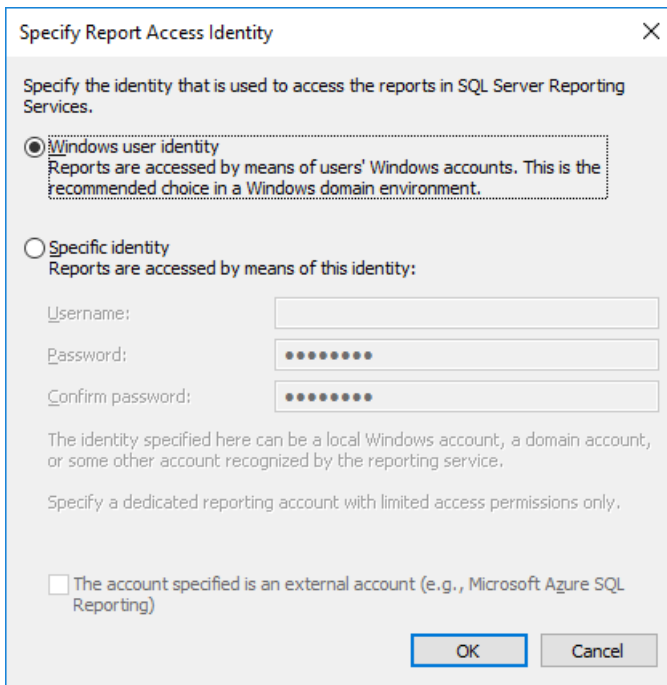
Specifying the Report Access Identity

The report access identity is the identity that is used for transferring reports from the reporting services to M-Files Desktop and for reading them.

Follow these steps to specify the report access identity:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select **Reporting and Data Export** and then click **Specify Report Access Identity** on the task area.

☑ The **Specify Report Access Identity** dialog is opened.

5. Select either:

   a. **Windows user identity**: Select this option to access reports via the Windows user account. This is the recommended choice in a Windows domain environment.

   or

   b. **Specific identity**: To define a specific identity for accessing reports, select this option and enter the username and password of the identity in the **Username** and **Password** fields. The identity can be a local Windows account, a domain account, or some other account recognized by the reporting service. The reporting account to be specified should have only limited access permissions to the reporting services. Check the **The account specified is an external account (e.g., Microsoft Azure SQL Reporting)** option check box if the specified account is an external account.

6. Click **OK** to close the **Specify Report Access Identity** dialog.

The report access identity that you have specified is now used for transferring reports from the reporting services to M-Files Desktop and for reading them.

Creation of Reports and the Required Software

The reports from M-Files to an external database are created by using the *Microsoft SQL Server Reporting Services* infrastructure, which must be implemented and configured correctly.

When reports have been created and they are to be used in M-Files, the *SQL Server Reporting Services* system contacts the database to which the data export was done from M-Files, creating a report when M-Files Desktop so requires.

Microsoft's SQL Server Reporting Services infrastructure can be installed with the SQL Server installation package (*SQL Server 2008* or *SQL Server 2008 R2*).

Also the SQL Server Express versions can be used in reporting. Then select the *SQL Server 2008 R2 Express with Advanced Services* installation package. You can download it via Microsoft's web site at *http://www.microsoft.com/express/Database*.

For more information, refer to *http://msdn.microsoft.com/en-us/library/ms159106.aspx* (SQL Server Books Online).

In planning the reports, you also need **Business Intelligence Development Studio** or, a simpler tool, **Report Builder**. The person planning the reports must be experienced in this and have the skills required for creating reports. Please contact our consulting services personnel, and we will be happy to help you with planning of the reports (*sales@m-files.com*).

For more information on installing Microsoft's reporting services, please consult Microsoft's web pages and the M-Files customer support staff at *support@m-files.com*.

> 📝 **Note:** Instructions for planning and creating reports and for using third-party software are available via the M-Files consulting services for a separate fee.

Creating a Report Object for a Report

When a report has been created (for more information, see *Creation of Reports and the Required Software* on page 372), it can be retrieved for use in M-Files Desktop.

For the reports to be displayed in M-Files, *.NET Framework 3.5 Service Pack 1* or *.NET Framework 4.0* must be installed on the computer of the user viewing the report. *.NET Framework Client Profile* is also a suitable solution. When necessary, M-Files will suggest installation, if the installation is possible.

Follow these steps to create a report object:

1. In M-Files, right-click on the listing area and select **New** > **Report...** from the context menu.

   ☑ The **New Report** dialog is opened.

2. In the **Name or title** field, enter a name describing the report.

   ✏ For example, if the report is used for calculating yearly revenue, the title of the report object could be *Revenue by Year*.

3. In the **Report URL** field, enter the URL to be used for retrieving the report from the reporting services to M-Files. The URL must be in the form `http://servername/instance?/report_path`.

   ℹ The same URL can be used to retrieve the report in the browser. Note, however, that this address will not be displayed in the browser address field after opening the report. For more information, please contact M-Files customer support at *support@m-files.com*.

4. Optional: To define the placement of the report in the M-Files user interface, click **Add property** and select **Report placement** from the drop-down menu, and the select an appropriate value for **Report placement** using the drop-down menu.

5. Click **Create** to create the report object.

The report object you have created is added to the vault. You can view the report by selecting the object in M-Files.

You can attach a report object to a specific view. For instructions, see *Attaching a Report Object to a View* on page 373.

Attaching a Report Object to a View

You can attach a report object to a specific view, such as *Sales by customer* or *Proposals by salesperson*. Do the following steps to attach a report object to a view:

1. In M-Files, navigate to the view to which you want to attach a report object.

2. Optional: If you want your settings to be applied for all users, right-click on an empty area in the view and select **Properties** from the context menu.

   a) In the **Properties** dialog, check the **Common to all users** option check box, if it is not already checked.

    b) Click **OK** to close the **Properties** dialog.

3. Press Alt and select one of the following options from the context menu:

    a. **View** > **Reports** > **Attach Report to This View (full view)...**: Select this option if you want the report to be displayed in the full view mode, covering the listing area and the right pane.

        or

    b. **View** > **Reports** > **Attach Report to This View (right)...**: Select this option if you want the report to be displayed in the right pane.

        or

    c. **View** > **Reports** > **Attach Report to This View (bottom)...**: Select this option if you want the report to be displayed at the bottom of the listing area.

    ☑ The **Select Report** dialog is opened.

4. Select the report object that you want to attach to the selected view and click **Open**.

The selected report is attached to the selected view. When you navigate to the view, the report is displayed automatically.

Associating the Report Object with Other Objects

You can associate the *Report* object with other objects, such as *Customers*. You can display the report data by customer by selecting a customer from the list if you so specify in the reporting services settings (see *Creation of Reports and the Required Software* on page 372). Then M-Files will show the data (for instance sales by month) for only this specific customer in the report. When you select another customer, the report will be updated with data related to the second customer.

Bringing the Report Up to Date

The data in the report is based on the latest data from M-Files to the reporting service. The data can exported either manually or on a scheduled basis. If a separate update link is created for a report in the reporting services, the report can be updated whenever desired via M-Files Desktop. For more information, please contact M-Files customer support at *support@m-files.com*.

Exporting a Report

Once a report is readable in M-Files, it can also be exported in various file formats. The supported file formats are:

* XML file with report data
* CSV (comma delimited)
* PDF
* MHTML (web archive)
* Excel spreadsheet.
* TIFF file
* Word document

    📄 **Note:** The exported report is static and cannot be edited in other applications.

Do the following steps to export a report:

1. In M-Files, locate the report that you want to export by using either the search or the views.

2. Right-click on the displayed report and select **Export** and then select a suitable file format from the context menu.

   ☑ The **Save As** dialog is opened.

3. Select a suitable directory and enter a suitable file name in the **File name** field and then click **Save**.

The report is exported in the selected file format.

9.10. Content Replication and Archiving

Content replication and archiving enables synchronization of objects between vaults. This helps in ensuring that data is up to date between various specified vaults. Replication and archiving can be carried out by using the *export* on page 376 and *import* on page 384 operations available in M-Files Admin.
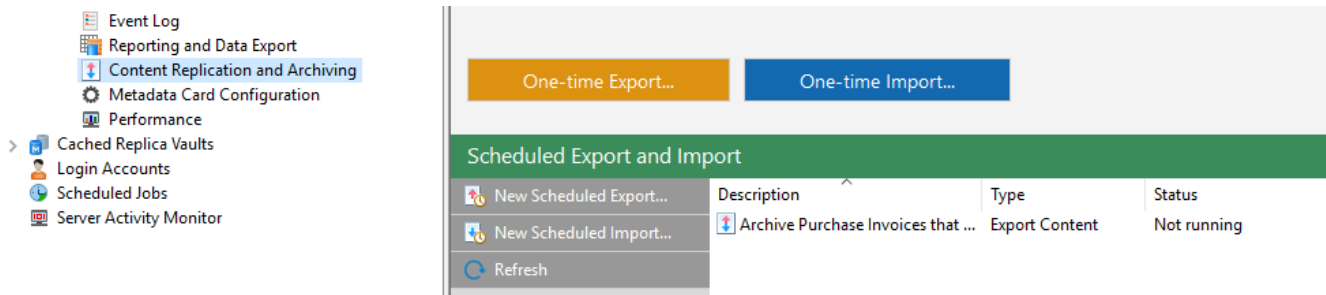
Figure 105: The replication features in M-Files Admin.

Ways to utilize replication and archiving

With content replication and archiving, you can, for instance:

- Replicate data between locations.

  - This allows, for example, global companies to replicate data to remote servers and, this way, ensure quick access to data even if the network connections to the main server are slow or cut off.
- Archive data from an actively used vault to an archive vault.
- Archive data for long-term preservation in XML or PDF/A form in compliance with standards.
- Collect data from several M-Files vaults within a single, centralized vault.
- Use specific vaults for each of the various operations of the company.
- Publish certain documents for interest groups, such as partners, customers, or subcontractors.
- Perform backups.
- Restore the system after an error reliably (as in disaster recovery).

▶ Video: *Replication Overview*

▶ Video: *Configure Replica Servers*

For a more extensive presentation on replication and archiving, refer to the *M-Files Replication and Archiving User's Guide*.

Important remarks

- For association and synchronization of objects and their metadata between separate vaults, the metadata definitions must also be associatable between vaults. For more information, refer to *Associating the Metadata Definitions* on page 203.

- It is advisable to check the permissions of confidential imported objects in the target vault after an import operation is complete, especially if the source and the target vaults have differing users or user groups.
- If M-Files is installed on several servers, an *M-Files Additional Server License* must be installed for the additional servers.
- In case you have archived documents in earlier versions of M-Files than 9.0, please note that you cannot restore archive files in the *.mfa* file format to a vault using version 9.0 or later. If you want to restore an archive file in the *.mfa* file format, you must use a vault that has version 8.0 or older installed. After this, you can upgrade the vault and perform archiving that is compatible with version 9.0 and newer.

Exporting Content

You can use content exporting for long-term archiving of content, synchronization of data among several vaults, or freeing up disk space on the server.

Do the following steps to export content:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select the **Content Replication and Archiving** node.

   ✓ The content replication and archiving features are displayed in the right-side pane.

5. Click the **One-time Export...** button.

   ⓘ For information about creating a recurring export operation, see *Defining a Scheduled Export* on page 393.

   ✓ The **Export Content** dialog is opened.

6. On the **Package Location** tab, define the location for the content package.
   a) Click the **...** button to define a temporary local folder for the content package.
   b) Optional: Click **Set Account...** to define the user account to be used for saving the content package to the selected local folder.

   > ⓘ You need to use a user account that has write permissions to the selected local folder.

7. Optional: Still on the **Package Location** tab, enable the **Use replication via cloud storage** option to export to a cloud storage location.
   a) In the **Connection string** field, enter the provided connection string for connecting to the cloud storage.

   > ⓘ If you do not yet have the connection string, click **Get...** to obtain one. This opens up a preformatted e-mail message to be mailed to M-Files customer support.
   b) In the **User-specified folder name** field, enter a folder location in the cloud storage that will be used for exporting from one vault and importing to another.
   c) In the **User-specified password for encryption** field, enter a password of your choice that will be used for encrypting content packages. The same password must be used for exporting and importing the same packages.

8. Click the **Objects and Files** tab.

   ✓ The **Objects and Files** tab is opened.

9. Enable the **Export objects and files** option by checking the check box and select the **Export existing objects** option.

    ⓘ For more information about the options on this tab, see *Export Objects and Files* on page 380.

    📄 **Note:**

    If the **Export only changes since latest run** option is enabled, only the files and objects that are new or have changed since the given date and time are exported. If you are exporting metadata structure elements while this option is enabled, the elements are not exported unless there have been changes made to files or objects.

    Thus if you want to export metadata structure elements regardless of whether objects or files have been changed, it is recommended to do either of the following operations:

    *   Export the metadata structure separately.
    *   Disable the **Export only changes since latest run** option if metadata structure elements are to be exported alongside objects and files. Note that if you do not limit the scope of the export in any way, it may take a considerable amount of time to complete the export job.

10. Optional: To define the conditions that objects must meet in order to be exported, enable the **Use a search filter** option by checking the check box and click the **Define...** button.

    a) In the **Define Filter** dialog, define the conditions that objects must meet in order to be exported and click **OK** once you have defined all the necessary conditions.

11. Click the **Structure** tab.

   ☑ The **Structure** tab is opened.
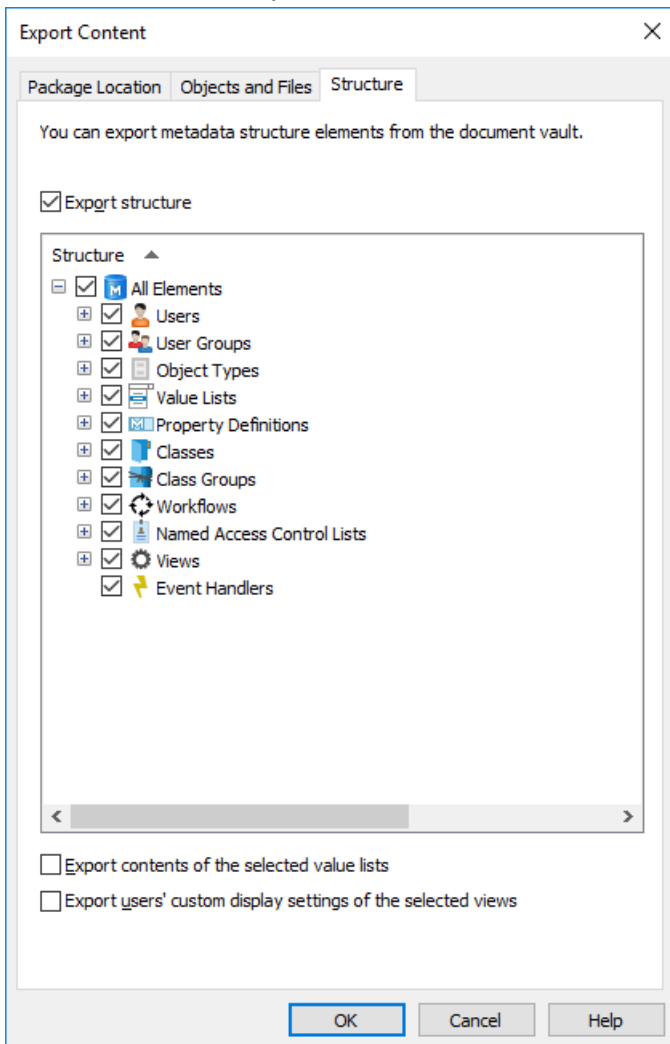
12. Enable the **Export structure** option and either:

   a. Check the **All Elements** option to export all metadata structure elements.

     or

   b. Check individual metadata structure elements on the list to define individually the elements to be exported.

   ℹ️ For more information about the options on this tab, see *Export Structure* on page 382.

13. Click **OK** to close the **Export Content** dialog and to start the export.

Once the export operation has been completed, you can use the export package to import the exported content to another vault. See *Importing Content* on page 384.

Export Package Location

On the *Package Location* tab of the *Export Content* dialog, you can change the location of the content package. M-Files names the files automatically according to the vault ID and timestamp, so that you can find the content package easily at a later time.

You can also modify the user account to be used. The user needs to have the rights to the specified saving location in order for the export to be successfully completed. The default selection is "Local System account".

Use replication via cloud storage

You can also use replication via a cloud storage location. When exported, the replication packages are locally encrypted with the AES-256 algorithm and then uploaded to the cloud storage location. When imported, the replication packages are downloaded from the cloud storage location and then decrypted locally. This functionality can be helpful when you are replicating data between different locations and want to be completely certain that only the appropriate persons can access the data.

Connection string

Use the **Get** button to obtain the connection string for the cloud storage location. Please make sure to use the same string for both export and import.

User-specified folder name

The folder name is unique for one export-import pair. For instance, replication from the master vault to a secondary vault could be named "MasterOut" and replication from the secondary vault to the master vault "MasterIn".

User-specified password for encryption

The replication password is used for encrypting the replication packages. The password can be whatever you decide. Just remember to use the same password for both export and import.

Export Objects and Files

The *Objects and Files* tab enables you to change settings for exporting object and file content.
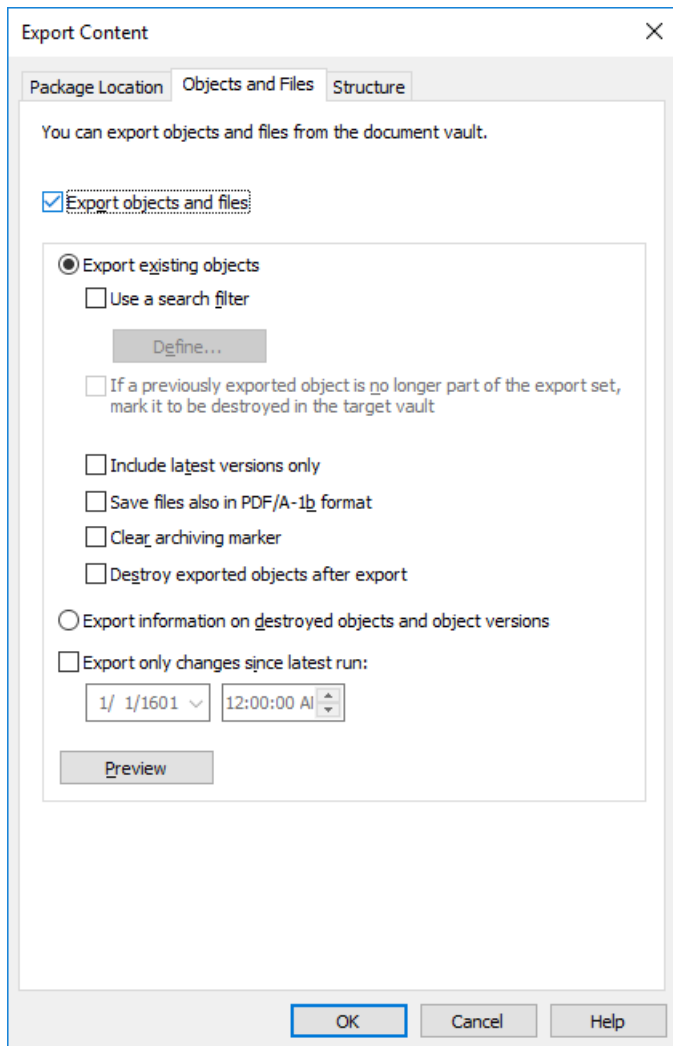
Figure 106: The "Objects and Files" tab of the "Export Content" dialog.

Export existing objects

Use a search filter

By using a filter, you can specify which existing objects you want to export. For example, you can export certain objects by object type or property. In particular, when publishing certain documents, such as brochures or press releases, for interest groups only, you can use the search filter for the publication when, for example, the requirement of a certain class or property is met.

If a previously exported object is no longer part of the export set, mark it to be destroyed in the target vault

By enabling this setting, any of the objects that were included in an earlier export set but are not in the current one will be deleted in the target vault upon import. If you wish to delete, say, certain price lists from a vault designed for partner use, you just need to make sure that this setting has been enabled and that they do not fit the criteria of the export set.

> **Note:** The setting is job-based and applies only for scheduled export and import jobs.

> **Note:** The setting *Do not import object destructions* in the properties of the import job overrides this setting.

Include latest versions only

You can choose to export only the latest versions of the selected objects for archiving. Older versions of the selected objects will not be archived.

Save files also in PDF/A-1b format

You can indicate whether you also want to save the files in PDF/A-1b format when archiving them. PDF/A-1b format complies with the standard ISO 19005-1:2005, on the long-term preservation of electronic documents.

Saving in PDF/A-1b format is possible with Office files and standard PDF files. Files in PDF/A-1b format are not imported during import. Saving in PDF/A-1b format slows down the export to some extent.

Clear Archiving Marker

If you have chosen to export objects with the *Marked for archiving* property defined, you can indicate that the property should be cleared after the content export. With this setting is enabled, the exported objects are no longer marked for archiving.

Destroy exported objects after exporting

You can specify whether you want to destroy the exported objects after the export. If you have selected to export the latest versions only, you cannot choose this setting.

Export information on destroyed objects and object versions

Instead of the existing objects, you can choose to export data from the destroyed objects and object versions only. This function is intended mainly for clearing the destroyed objects from the vault.

Export only changes since latest run

You can choose to export only the changes made since the latest run. By default, M-Files offers the date of the latest export (or of the last import of exported objects to the source vault with a timestamp older than the previous export).

> **Note:**
>
> If the **Export only changes since latest run** option is enabled, only the files and objects that are new or have changed since the given date and time are exported. If you are exporting metadata structure elements while this option is enabled, the elements are not exported unless there have been changes made to files or objects.
>
> Thus if you want to export metadata structure elements regardless of whether objects or files have been changed, it is recommended to do either of the following operations:
>
> • Export the metadata structure separately.
> • Disable the **Export only changes since latest run** option if metadata structure elements are to be exported alongside objects and files. Note that if you do not limit the scope of the export in any way, it may take a considerable amount of time to complete the export job.

Preview

The **Preview** button displays the number of objects affected by the export process.

Export Structure

The *Export Structure* tab enables you to select which parts of the metadata structure you want to export.
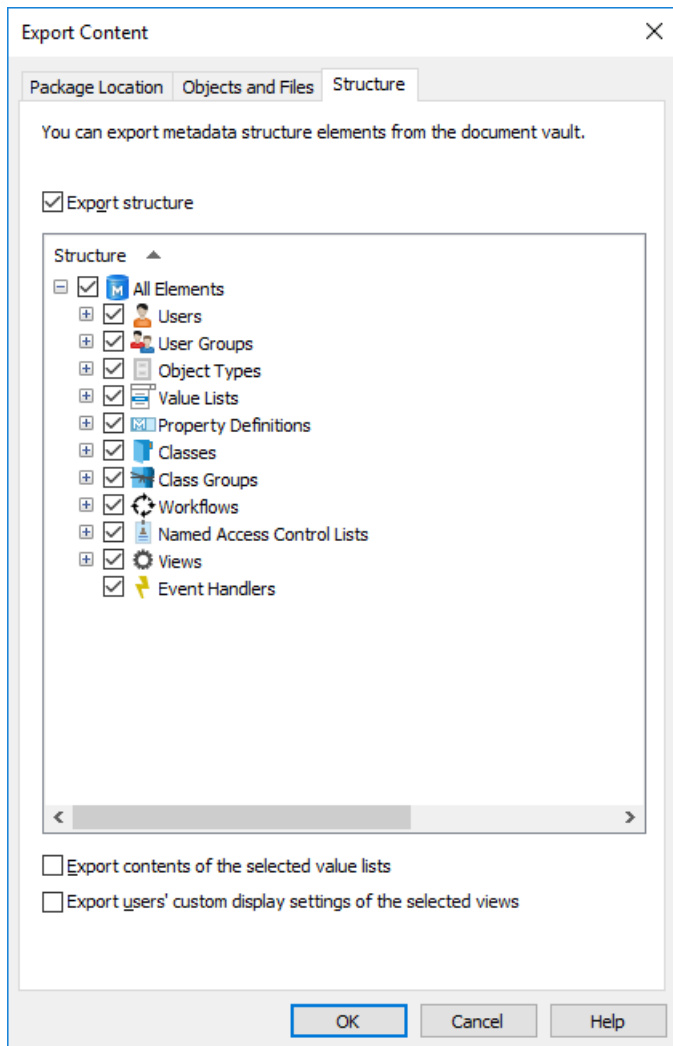
Figure 107: The "Structure" tab of the "Export Content" dialog.

Export Structure

You can choose the metadata structure elements of the selected vault to be exported or select all elements by activating *All Elements*.

> **Note:** Built-in elements are always created in M-Files by default and include, for example, the property definitions *Name or title*, *Created by*, *Last modified by*, and *Keywords*. In addition to these, administrators can create new, user-defined elements.

Export contents of the selected value lists

By selecting the *Export contents of the selected value lists* checkbox you can choose to export all value list content.

> **Note:** All the removed values are replicated as well. This means that values in the target vault may be deleted through a metadata structure import. The values are not deleted completely, however, but instead only marked as deleted. This enables the ability to search and re-enable any deleted values in the source or target vault via M-Files Admin.

Selecting **OK** creates an export package of the selected metadata to the location specified on the *Package location* tab.

Export users' custom display settings of the selected views

By enabling the **Export users' custom display settings of the selected views** checkbox you can choose to include users' custom display settings to the export package.

> 📄 **Note:** Exporting a view always includes the common display settings of the view.

Importing Content

After *creating an export package* on page 376, you can import its content to a vault of your choosing. You can use the **Import Content** function when you need to import data to another vault for example for replication, publication, archiving, or backup purposes. The objects and their metadata are imported and synchronized with those in the target vault. M-Files always imports versions that are new or changed compared to the current versions in the target vault.

Complete the following steps to import a content package:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select the **Content Replication and Archiving** node.

> ✅ The content replication and archiving features are displayed in the right-side pane.

5. Click the **One-time Import...** button.

> ℹ️ For information about creating a recurring import operation, see *Defining a Scheduled Import* on page 395.

> ✅ The **Import Content** dialog is opened.

6. On the **Package Location** tab, define the location for the content package.

    a) Optional: Enable the **Import multiple content packages** if you want to import multiple packages from the selected location.

    b) Click the **...** button to define the location of the content packages to be imported.

    c) Optional: Click **Set Account...** to define the user account to be used for retrieving the content package from the selected folder.

      ⓘ You need to use a user account that has read permissions to the selected folder.

7. Optional: Still on the **Package Location** tab, enable the **Use replication via cloud storage** option to import from a cloud storage location.

    a) In the **Connection string** field, enter the provided connection string for connecting to the cloud storage.

      ⓘ If you do not yet have the connection string, click **Get...** to obtain one. This opens up a preformatted e-mail message to be mailed to M-Files customer support.

    b) In the **User-specified folder name** field, enter a folder location in the cloud storage that will be used for importing to one vault and exporting from another.

    c) In the **User-specified password for encryption** field, enter a password of your choice that will be used for encrypting content packages. The same password must be used for exporting and importing the same packages.

8. Check the **Delete content package after importing** check box if you want the content package to be removed after the operation has been completed.

9. On the **Objects and Files** tab, you can specify how objects and files are imported.

   ⓘ For more information, see *Import Objects and Files* on page 388.

10. On the **Structure** tab, you can specify how metadata structure is imported.

    ⓘ For more information, see *Import Structure* on page 389.

11. On the **Permissions** tab, you can specify the permission settings for the imported objects.

    ⓘ For more information, see *Permissions (Importing Content)* on page 390.

12. Click **OK** to start the import operation.

    ✅ A summary of the package content to be imported is opened.

       📄 **Important:** It is essential to take into consideration that exporting and importing objects with relationships to other objects may, in some cases, produce a conflict. If the conflict cannot be resolved automatically, some of the selected objects might not be replicated. The *import summary report* on page 392 should be reviewed carefully before proceeding with the import operation.

Import Package Location

The *Package Location* tab displays options related to the package containing the objects and files and/or metadata structure to be imported. Refer to the corresponding settings in *Exporting Content* on page 376 when you are importing the content package to the selected vault.

The location must be the same as that of the content package exported from the source vault; that is, M-Files must find the exported data in order to perform the import. The location may be different, but in that case a separate data transfer between locations must be implemented.

   📄 **Note:** The exported package can contain different marker files. M-Files only imports content packages that have the *Ready* marker file but not the *Imported* marker file for the target vault.
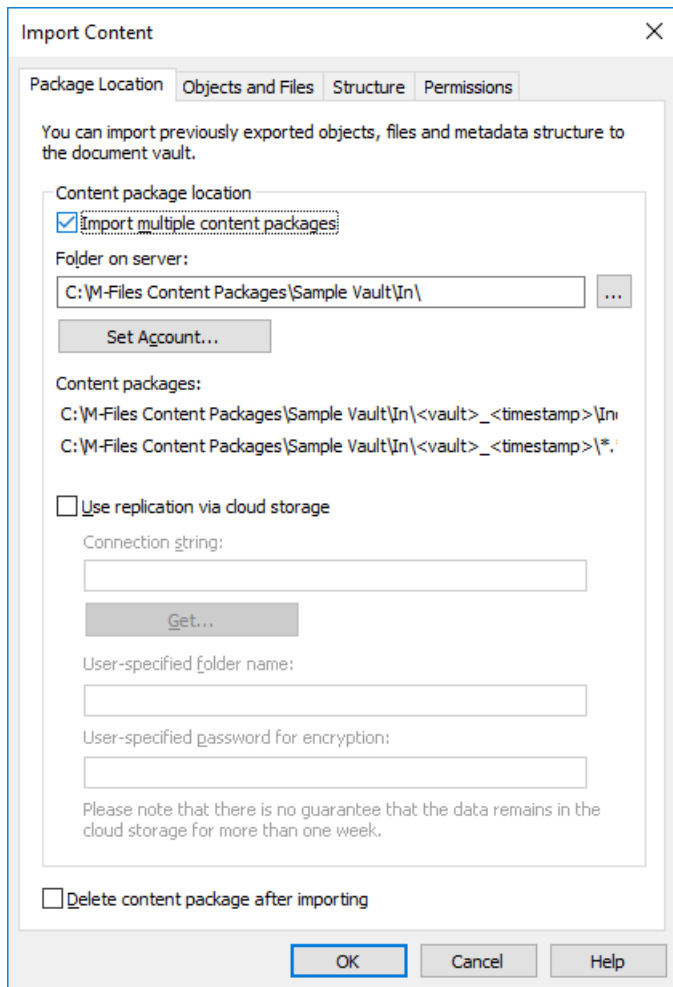
Figure 108: The Package Location tab of the Import Content dialog

You can also import several packages at a time by checking the *Import multiple content packages* checkbox. This enables you to select a folder instead of a single file.

The content package will be automatically deleted after importing if the *Delete content package after importing* option is enabled.

Use replication via cloud storage

You can also use replication via a cloud storage location. When exported, the replication packages are locally encrypted with the AES-256 algorithm and then uploaded to the cloud storage location. When imported, the replication packages are downloaded from the cloud storage location and then decrypted locally. This functionality can be helpful when you are replicating data between different locations and want to be completely certain that only the appropriate persons can access the data.

Connection string

The connection string contains the storage location information. Please make sure to use the same string for both export and import (see *Export Package Location* on page 379).

Folder name

The folder name is unique for one export-import pair. For instance, replication from the master vault to a secondary vault could be named "MasterOut" and replication from the secondary vault to the master vault "MasterIn".

Password for encryption

The replication password is used for encrypting the replication packages. The password can be whatever you decide. Just remember to use the same password for both export and import.

Import Objects and Files

The *Objects and Files* tab enables you to change settings related to importing object and file content.
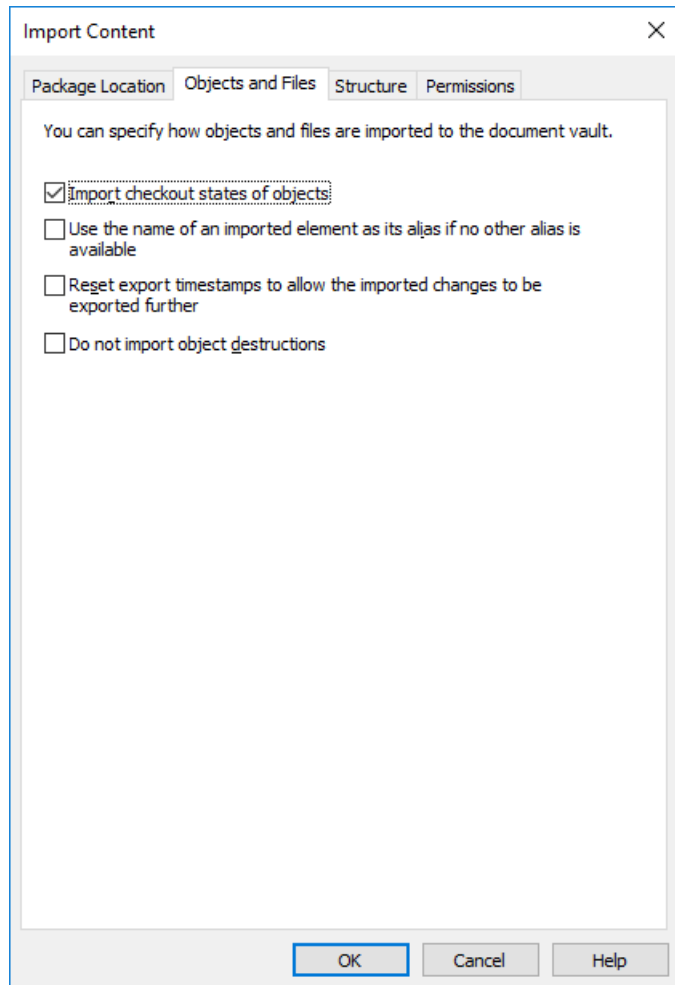
Figure 109: The "Objects and Files" tab of the "Import Content" dialog.

Settings

Import check-out states of objects

If the objects are checked out in the vault from which you are exporting, you can import the check-out states to the target vault as well. Then the object is also checked out in the target vault, which prevents other users from editing it. This reduces the possibility of conflicts, which could be caused by simultaneous editing in multiple vaults.

Use the name of an imported element as its alias if no other alias is available

Since only built-in, GUID and "ID+name" matching metadata definitions are automatically connected, other metadata definitions must be associated by using aliases. However, the necessary alias definitions may not have been made in the source vault. In the latter case, the data export can be facilitated by means of this setting. When this option has been selected, the alias need only be defined in the target vault as long as it is in line with the element's source vault name.

For example, you may want to import objects of the *Project* type but have not defined an alias for the *Project* object type in the source vault. By selecting this option and adding, in the target vault, an alias corresponding to the source vault's name for the project object type (in this case, the alias is "Project"), you will get the necessary definitions for the import.

> 📄 **Note:** You must use the default language names from the source vault as the aliases for the metadata definitions in the target vault in order to be able to perform connection of the metadata definitions.

> 📄 **Note:** This setting is valid only when the metadata definition in question (object type, property definition, value list, or similar) has no alias defined in the source vault.

Reset export timestamps to allow the imported changes to be exported further

If you want to export objects and their changes from one vault to another – for example, from vault A to vault B – and then onward (to vault C, D and so forth), enable this setting when you are importing from vault A to vault B. In this case, the corresponding objects and their changes can be exported from vault B to vault C as new information because the timestamps were reset.

In this case, make also sure that you have activated the *Export information on destroyed objects and object versions* selection in connection with the export to vault B.

Do not import object destructions

Select this option if:

* You do not want to destroy objects that you have destroyed in the source vault also in the target vault. For example, if you use the target vault for archiving destroyed objects, select this setting.
* You do not want to destroy objects that are no longer part of the export set. Please note that this setting nullifies the export setting *If a previously exported object is no longer part of the export set, mark it to be destroyed in the target vault*.

Import Structure

In the *Structure* tab, you can disable any external database connections to object types, value lists and to user groups, as well as disable any active event handlers to be replicated.
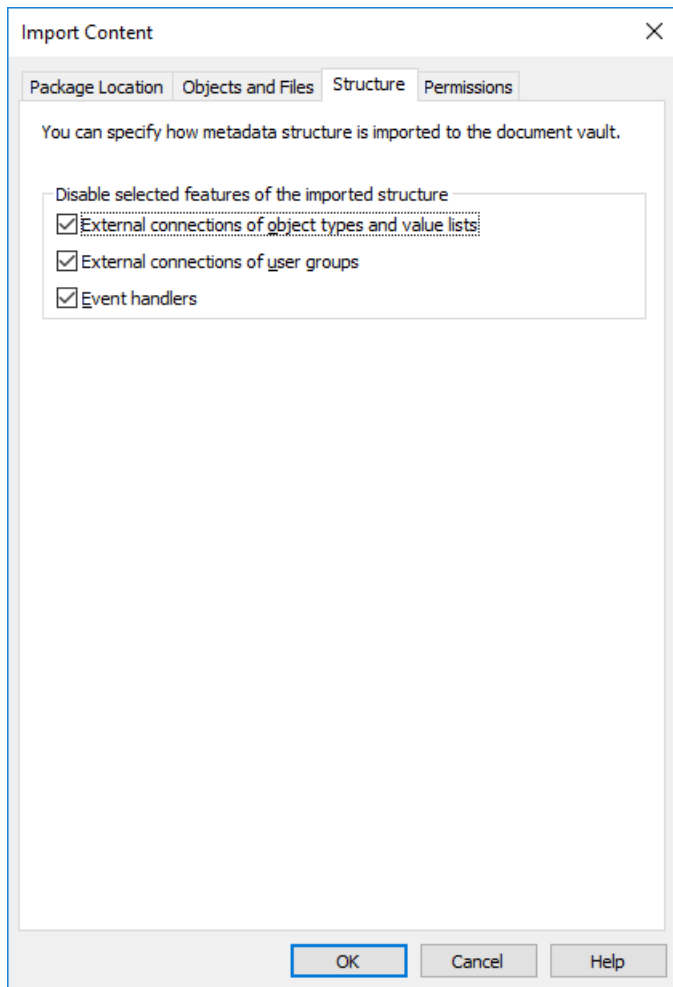
Figure 110: The Structure tab of the Import Content dialog

Selecting **OK** generates a report that displays all modifications to the target vault structure.

Permissions (Importing Content)

The *Permissions* tab of the importing dialog allows you to change the permission settings of the content to be imported.

Complete the following steps to modify the permissions:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select the **Content Replication and Archiving** node.

   ✅ The content replication and archiving features are displayed in the right-side pane.

5. Either:

   a. Click **One-time Import...** if you want to modify the permissions of a single import package.

      or

b. Click the task area item **New Scheduled Import...** if you want to modify the permissions of a recurring import job.

☑ Depending on your choice, either the **Import Content** or the **Scheduled Job Properties** dialog is opened.

6. Select the **Permissions** tab.

☑ The **Permissions** tab of either the **Import Content** or the **Scheduled Job Properties** dialog is opened.
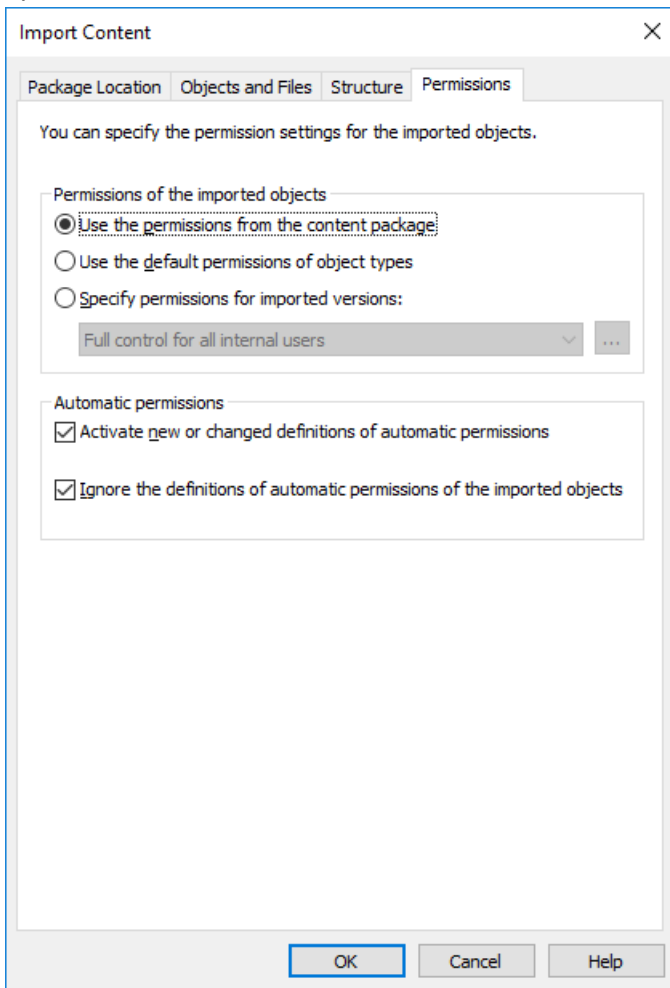
7. In the **Permissions of the imported objects** section, select one of the following options:

Option	Description
Use the permissions from the content package	Select this option if you want the imported objects to have the same permissions as the objects in the source vault.
Use the default permissions of the object types	Select this option if you want the imported objects to use the default permissions *defined via the properties dialog* on page 261 of each object type.
Specify permissions for imported versions	Select this option if you want to manually define permission settings that are to be applied to all the imported objects.

8. Optional: Check or uncheck the **Activate new or changed definitions of automatic permissions** option checkbox.

   ℹ️ If the content package contains any new or changed definitions of automatic permissions, importing the content package with this option enabled activates all the automatic permissions triggered by the imported definitions in the target vault. Importing the content package with this option unchecked still imports the automatic permission definitions to the target vault, but does not cause any new automatic permissions to be activated.

9. Optional: Check or uncheck the **Ignore the definitions of automatic permissions of the imported objects** option checkbox.

   ℹ️ When selected, this option makes the importing process bypass the definitions of automatic permissions of all the imported objects in the content package. This way you can choose to preserve the automatic permissions of all the objects in the target vault by leaving out any potential changes to the definitions of automatic permissions from the objects in the imported content package.

10. Click **OK** to close the dialog.

Import Summary Report

Before accepting any changes to the target vault, M-Files presents a detailed summary of the content package to be imported. It is highly recommended to carefully review the summary report explaining the results of the content import.

Figure 111: The summary report for the content to be imported.

It is very important to make sure that no unintended duplicate structure elements will be generated, and that all changes to the target vault's metadata structure will be as expected. In the event there are incorrect mappings, the process should be canceled and the names or aliases of the elements in the source and/or target vault modified accordingly.

> **Note:** The imported metadata structure elements overwrite their existing counterparts in the target vault. It is not recommended to configure similar object type structures in the master vault and replica vault if the vaults have different connections to external databases configured.

Scheduled Export and Import

For keeping vaults up to date between each other and in interaction, scheduled export and import must be defined for the vaults. With scheduled export and import, you can synchronize the objects and their metadata between vaults.

> **Note:** The schedule option *When idle* is not supported in M-Files.

> **Note:** It is recommended that you study the section *Interaction Among Several Vaults* on page 202 before defining any export or import jobs.

▶ Video: *Continuous Replication*

Scheduled export

Define the scheduled export in the source vault where you can save the content to be exported on a scheduled basis. The same settings are available as when defining an individual export. For further information, refer to *Export Content* on page 376. Exported data can be imported to another vault for publication, replication, archiving or backup.

Scheduled import

When you want to import the content to another vault for synchronization or other use, you should define the scheduled import to the target vault. The same settings are available as when defining an individual import. For further information, refer to *Import Content* on page 384.

Scheduling an export or an import job works the same way as scheduling tasks in the Windows Control Panel.

> **Note:** In addition to the content export and import, you should be able to associate the metadata definitions for the interaction between separate vaults, so that synchronization is possible through archiving. For further information, refer to *Interaction among several document vaults* on page 202.

Defining a Scheduled Export

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select the **Content Replication and Archiving** node.

   ☑ The content replication and archiving features are displayed in the right-side pane.

5. Click **New Scheduled Export...** on the task area.

   ☑ The **Scheduled Job Properties** dialog is opened.

6. In the **Description** field, type in a name for the scheduled export job.

7. Click **Schedule** to define a schedule for the export job.

✅ The **Define Schedule** dialog is opened.

8. Define the appropriate schedule using the available options and click **OK** to close the **Define Schedule** dialog.

   ℹ️ The schedule option **When idle** is not supported in M-Files.

9. On the **Package Location** tab, define the location for the content package.
   a) Click the **...** button to define a temporary local folder for the content package.
   b) Optional: Click **Set Account...** to define the user account to be used for saving the content package to the selected local folder.

      ℹ️ You need to use a user account that has write permissions to the selected local folder.

10. Optional: Still on the **Package Location** tab, enable the **Use replication via cloud storage** option to export to a cloud storage location.
    a) In the **Connection string** field, enter the provided connection string for connecting to the cloud storage.

       ℹ️ If you do not yet have the connection string, click **Get...** to obtain one. This opens up a preformatted e-mail message to be mailed to M-Files customer support.
    b) In the **User-specified folder name** field, enter a folder location in the cloud storage that will be used for exporting from one vault and importing to another.
    c) In the **User-specified password for encryption** field, enter a password of your choice that will be used for encrypting content packages. The same password must be used for exporting and importing the same packages.

11. On the **Objects and Files** tab, enable the **Export objects and files** option by checking the check box and select the **Export existing objects** option.

    ℹ️ For more information about the options on this tab, see *Export Objects and Files* on page 380.
    > 📄 **Note:**
    >
    > If the **Export only changes since latest run** option is enabled, only the files and objects that are new or have changed since the given date and time are exported. If you are exporting metadata structure elements while this option is enabled, the elements are not exported unless there have been changes made to files or objects.
    >
    > Thus if you want to export metadata structure elements regardless of whether objects or files have been changed, it is recommended to do either of the following operations:
    >
    > * Export the metadata structure separately.
    > * Disable the **Export only changes since latest run** option if metadata structure elements are to be exported alongside objects and files. Note that if you do not limit the scope of the export in any way, it may take a considerable amount of time to complete the export job.

12. Optional: To define the conditions that objects must meet in order to be exported, enable the **Use a search filter** option by checking the check box and click the **Define...** button.
    a) In the **Define Filter** dialog, define the conditions that objects must meet in order to be exported and click **OK** once you have defined all the necessary conditions.

13. On the **Structure** tab, enable the **Export structure** option and either:

    a. Check the **All Elements** option to export all metadata structure elements.

       or

    b. Check individual metadata structure elements on the list to define individually the elements to be exported.

**14.** Click **OK** to save the scheduled export job and close the **Scheduled Job Properties** dialog.

The scheduled export job that you have just defined is added to the **Scheduled Export and Import** list and will be run according to the defined schedule.

Defining a Scheduled Import

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select the **Content Replication and Archiving** node.

☑ The content replication and archiving features are displayed in the right-side pane.

5. Click **New Scheduled Import...** on the task area.

☑ The **Scheduled Job Properties** dialog is opened.

6. In the **Description** field, type in a name for the scheduled import job.

7. Click **Schedule** to define a schedule for the import job.

☑ The **Define Schedule** dialog is opened.

8. Define the appropriate schedule using the available options and click **OK** to close the **Define Schedule** dialog.

ⓘ The schedule option **When idle** is not supported in M-Files.

9. On the **Package Location** tab, define the location for the content package.
   a) Optional: Enable the **Import multiple content packages** if you want to import multiple packages from the selected location.
   b) Click the **...** button to define the location of the content packages to be imported.
   c) Optional: Click **Set Account...** to define the user account to be used for retrieving the content package from the selected folder.

    ⓘ You need to use a user account that has read permissions to the selected folder.

10. Optional: Still on the **Package Location** tab, enable the **Use replication via cloud storage** option to import from a cloud storage location.
   a) In the **Connection string** field, enter the provided connection string for connecting to the cloud storage.

   ⓘ If you do not yet have the connection string, click **Get...** to obtain one. This opens up a preformatted e-mail message to be mailed to M-Files customer support.
   b) In the **User-specified folder name** field, enter a folder location in the cloud storage that will be used for importing to one vault and exporting from another.
   c) In the **User-specified password for encryption** field, enter a password of your choice that will be used for encrypting content packages. The same password must be used for exporting and importing the same packages.

11. On the **Objects and Files** tab, you can specify how objects and files are imported.

   ⓘ For more information, see *Import Objects and Files* on page 388.

12. On the **Structure** tab, you can specify how metadata structure is imported.

> ℹ️ For more information, see *Import Structure* on page 389.

13. On the **Permissions** tab, you can specify the permission settings for the imported objects.

> ℹ️ For more information, see *Permissions (Importing Content)* on page 390.

14. Click **OK** to save the scheduled import job and close the **Scheduled Job Properties** dialog.

The scheduled import job that you have just defined is added to the **Scheduled Export and Import** list and will be run according to the defined schedule.

Archiving Old Versions

You can archive old versions of documents that you no longer need. When you archive old versions of documents, the selected document versions are transferred from the document vault to the archive file.

Do the following steps to archive old versions of documents:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select **Content Replication and Archiving**.

5. Select **Action** > **Archive Old Versions...** from the menu bar.

> ℹ️ You can also right-click on an empty area in the **Scheduled Export and Import** list and select **Archive Old Versions...** from the context menu.

> ✅ The **Archive Old Versions** dialog is opened.
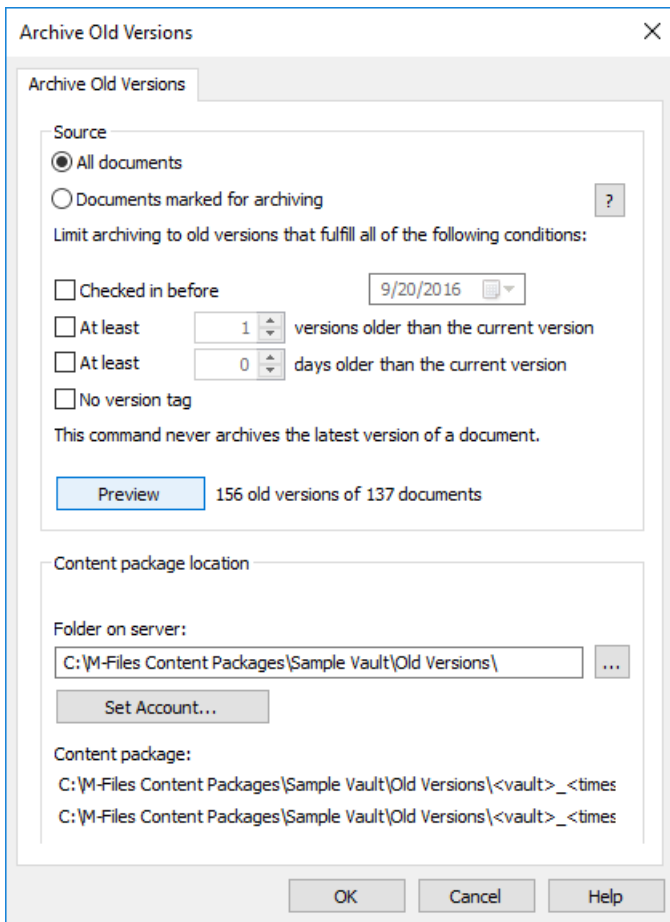
6. Select either:

a. **All documents**: Select this option if you want to archive old versions of all documents.

or

b. **Documents marked for archiving**: Select this option if you want to archive old versions of the documents that you have marked for archiving.

> 📄 **Note:** You can mark a document for archiving in M-Files Desktop by right-clicking a document and selecting **Archiving** > **Mark for Archiving** from the context menu. For more information, see *Archiving* on page 119.

7. Select the conditions (you can select all that apply) for limiting the number of old versions to be archived:

> ℹ️ You can click **Preview** to view the number of old versions to be archived with the selected settings.

Option	Description
Checked in before	Select this option to archive old versions that have been checked in before the given date.
At least *<number>* **versions older than the current version**	Select this option to archive old versions that are a given number of versions older than the current version.
At least *<number>* **days older than the current version**	Select this option to archive versions that are a given number of days older than the current version.

Option	Description
No version tag	Select this option to exclude versions that have a version label from the archive.

8. In the **Content package location** section, click the **...** to select the location to save the archive.

9. Optional: If the archive location you have selected requires access rights that the local system account does not have, click **Set Account...** to define a different user account for saving the archive.
    a) Select the **This account** option.
    b) In the **This account** field, enter the user account to be used for archiving.
    c) In the **Password** and **Confirm password** fields, enter the password of the account.
    d) Click **OK** to close the **Set Account** dialog.

10. Click **OK** to save your changes and to close the **Archive Old Versions** dialog.

The selected old versions of documents are archived to the location you have defined.

The archived documents can later be restored to the document vault via *Content Replication and Archiving* on page 375.

> 📄 **Note:** If you have archived documents in earlier versions of M-Files than 9.0, please note that you cannot restore archive files in the *.MFA* file format to a vault using version 9.0 or later. If you want to restore an archive file in the *.MFA* file format, you must use a vault that has version 8.0 or older installed. After this, you can upgrade the vault and perform archiving that is compatible with version 9.0 and newer.

9.11. Metadata Card Configuration

Via the left-side tree view of M-Files Admin, you can access a JSON-based editor for modifying the behavior of the metadata card.

> 📄 **Note:** The feature requires Internet Explorer 9 or later to be installed.

The editor enables you, for instance, to:

*   add an additional header, including text and an image, for a certain object type or a class.
*   add tooltips and description fields for individual properties.
*   create collapsible property groups.
*   control the order in which properties and groups are displayed on the metadata card.
*   assign default values for properties.
*   manage automatically added (mandatory and optional) properties based on, for instance, object type and class.
*   hide properties from the metadata card.

User interface

The user interface of the editor is comprised of four parts:

*   The hierachical rules list (left)
*   The rule name (top right)
*   The rule condition (middle right)
*   The rule behavior (bottom right)

Figure 112: The metadata card configuration tool.

You can add and remove rules by using the plus and cross icons at the top right corner of the rule list, or by right-clicking any of the rules. The list is hierachical, meaning that you can add subordinate rules for further specifying main rules (or any superordinate rules).

The **Name** field should contain a descriptive name for the rule. The name is only visible in the rule editor.

The **Condition** field defines the scope of the rule in JSON. You may want to, for example, hide certain properties from an object of certain class.

The **Behavior** field is used for specifying what happens when the above-defined condition is met. For instance, when the object class is *Customer*, you might want to add the property groups *Contact information*, *Subscription* and *Responsible employee* to the metadata card.

The hierarchical rule list is evaluated from top to bottom. The higher a rule is in the list, the earlier it is evaluated. You can change the evaluation order by right-clicking a rule and selecting **Move Up** to move it up in the list, or **Move Down** to move it down in the list.

📄 **Note:** When a rule becomes effective, it always overwrites any overlapping behaviors of rules that have previously come into effect. In other words, a rule always overwrites any overlapping behaviors of other rules higher up in the hierarchical rule list.

For more information on defining the rule condition and behavior, see the article *Configuring the Metadata Card (M-Files 2015.3)*.

9.12. Performance

You can use M-Files Admin to measure the performance of a specific document vault in order to detect problems or bottlenecks in the performance of the document vault. The performance tests measure the network round-trip time to the database server of the vault as well as the time it takes to insert 100,000 rows into the vault database.

Do the following steps to measure document vault performance:

1. Open M-Files Admin.

2. In the left-side tree view, expand the desired connection to M-Files Server.

3. In the left-side tree view, expand the document vault of your choice.

4. Still in the left-side tree view, select **Performance**.

✓ The **Performance** view is opened in the right-side pane.

Connections to M-Files Servers
- Local Computer
  - Document Vaults
    - Coffre Démo
    - Esimerkkivarasto
    - Muster-Dokumentenverwaltung
    - My Vault
      - Users
      - User Groups
      - Metadata Structure (Hierarchical View)
      - Metadata Structure (Flat View)
      - Workflows
      - Named Access Control Lists
      - Connections to External Sources
      - Event Log
      - Reporting and Data Export
      - Content Replication and Archiving
      - Metadata Card Configuration
      - Performance
    - Sample Vault
  - Cached Replica Vaults
  - Login Accounts
  - Scheduled Jobs
  - Server Activity Monitor

Performance

▶ Begin testing

Performance test results

Operation

Network round-trip time to

Database insert speed (100,0

M-Files
2015.3

5. Click **Begin Testing** on the task area.

ⓘ You can stop the test at any time by clicking **Stop Testing** on the task area.

☑ The network round-trip time to the database server as well as the database insert speed are measured.

The results of the tests are displayed in the **Duration** column. If there are no remarks displayed in the **Remarks** column, your vault should be performing optimally.

If one or more of the tests took longer than their expected duration, a remark is displayed in the **Remarks** column. If the network round-trip time to the database server took longer than expected, it may be indicative of a slow network connection or heavy traffic on the network. If the database insert speed test took longer than expected, your server hardware may be insufficient or there may be heavy load on the server.

10. VBScript Variables Explained

VBScript code is edited in the *Edit VBScript code* window available in the following dialogs:

- *Automatic Values* on page 292
- *Automatically Validating Property Values* on page 300
- *Trigger* on page 337
- *Actions* on page 320
- *Conditions* on page 318
- *Event Handlers* on page 240

The available variables are described in the table below.

> 📄 **Note:** The documentation for the M-Files API is located in **Start** > **Programs** > **M-Files** > **Documentation** > **M-Files API**. For more information about VBScript code and M-Files API, go to *www.m-files.com/api*. Instructions on writing VBScript code and working with the M-Files API are available for a separate fee from M-Files customer support (*support@m-files.com*).

ActivityID	
Data Type	`MFilesAPI.TypedValue`
Mode	In
Variable Use	The unique ID of the operation that is being processed. Can be used for identifying which events are caused by a certain server operation.

AllowStateTransition	
Data Type	Boolean
Mode	Out
Variable Use	Can be used to allow or deny automatic state transition when running the automatic state transition script.

CurrentTransactionID	
Data Type	`MFilesAPI.TypedValue`
Mode	In
Variable Use	The ID of the transaction. If event handlers are executed recursively (so that executing one causes another to be executed), the ID changes on every recursion level.

CurrentUserID	
Data Type	`MFilesAPI.Number`
Mode	In
Variable Use	Contains the ID of the user who performed the action that triggered the script.

CurrentUserSessionInfo	
Data Type	`MFilesAPI.SessionInfo`
Mode	In

CurrentUserSessionInfo	
Variable Use	Contains information about the login session of the user who caused the operation.

DisplayID	
Data Type	`MFilesAPI.TypedValue`
Mode	In
Variable Use	Contains the object's unique ID. This ID is displayed to users in the property area of M-Files Desktop when the object is selected in the list. `DisplayID` can contain both numbers and letters. Often, `DisplayID` is the same as the object's internal ID whose value can be retrieved with the `ObjVer` variable. The internal ID can only contain numbers. `DisplayID` and the internal ID are usually different when the object has been imported from an external database.

FileTransferSessionID	
Data Type	`MFilesAPI.Number`
Mode	In
Variable Use	Contains the user-specific data transfer identifier. The data transfer identifier is created when the data transfer is being started on the server and, at the same time, the same identifier is given to the `BeforeFileUpload` and `BeforeFileDownload` event handlers. After completion of the data transfer, the same data transfer identifier will be given to the `AfterFileUpload` and `AfterFileDownload` event handlers. This way it is possible to attach the event handlers of type "Before" to the event handlers of type "After".

FileVer	
Data Type	`MFilesAPI.FileVer`
Mode	In
Variable Use	Contains the complete unique ID of the target file, consisting of the file ID and file version.

GetExtensionObject	
Data Type	(Method)
Mode	N/A
Variable Use	A method for retrieving the extension object defined by the vault application. Use: `GetExtensionObject( <object name> [, application GUID])`, where the part `[, application GUID]` is optional. For example: `Set CK = GetExtensionObject("M-Files.ComplianceKit", "{0CAC5452-631F-4646-AC95-4A06BFB8147E}")` If the application GUID has not been specified, the extension object is searched from all the applications of the vault.

Input	
Data Type	`MFilesAPI.TypedValue`
Mode	In
Variable Use	A client-defined parameter for the `VaultExtensionMethod` event handler.

LastUsed	
Data Type	`MFilesAPI.TypedValue`
Mode	In
Variable Use	Available only if a *customized automatic number* is being calculated for a property. The value of an automatic number usually depends on the previous calculation. For example, in ordinary consecutive numbering, the automatic value is incremented by one each time. When you are setting up customized automatic numbering, the result of the previous calculation can be retrieved by using the `LastUsed` variable. For example, simple automatic numbering that increments by one could be implemented with the following simple VBScript code: `Output = LastUsed + 1`

LoggedOutUserID	
Data Type	`MFilesAPI.Number`
Mode	In
Variable Use	Contains the logged out user ID after logout.

LoginAccount	
Data Type	`MFilesAPI.LoginAccount`
Mode	In
Variable Use	Contains the user account data in the login.

MasterTransactionID	
Data Type	`MFilesAPI.TypedValue`
Mode	In
Variable Use	The ID of the transaction. If event handlers are executed recursively (so that executing one causes another to be executed), this transaction ID is the ID of the first transaction.

MFScriptCancel	
Data Type	`MFilesAPI.Number`
Mode	In
Variable Use	Contains the error code which is used by the scripts for displaying error messages to users. M-Files often adds detailed data to error messages; this can be prevented with the error code of the `MFScriptCancel` variable. Example: `Err.Raise MFScriptCancel, "This is the error message shown to the user."`

NextStateID	
Data Type	`MFilesAPI.Number`
Mode	Out
Variable Use	During the automatic state transition, the `NextStateID` variable contains the ID of the state for which the automatic state transition will be performed. By changing the value of this variable,

NextStateID	
	you can define the next state in the automatic state transition script. By default, the target state is the same as set in the *Next State* option in the user interface.

ObjectAccessControlList	
Data Type	MFilesAPI.ObjectAccessControlList
Mode	In
Variable Use	Contains the current permissions of the viewed object.

ObjID	
Data Type	MFilesAPI.ObjID
Mode	In
Variable Use	The ID of the object being processed.

ObjVer	
Data Type	MFilesAPI.ObjVer
Mode	In
Variable Use	Contains the complete unique ID of the target version, consisting of the object type ID, object internal ID, and object version.

Output	
Data Type	MFilesAPI.TypedValue
Mode	Out
Variable Use	Available only if a *customized automatic number* is being calculated for a property. When VBScript code starts to run, the Output variable contains the current value of the property being calculated (but not for automatic numbering).
	The main purpose of VBScript code is usually to create a new value and assign it to the Output variable, which is then stored in the object's metadata. If the VBScript code does not set the value of the Output variable, the property value in the metadata remains the same.
	The value of the Output variable can, in simple cases, be set with a simple statement, for example: Output = 123
	If the datatype of the value being calculated is, say, *Choose from list*, the SetValue method is recommended for setting the value of the Output variable (see M-Files API), for example, as follows: Output.SetValue MFDatatypeLookup, 101

ParentTransactionID	
Data Type	MFilesAPI.TypedValue
Mode	In
Variable Use	The ID of the transaction. If event handlers are executed recursively (so that executing one causes another to be executed), this transaction ID is the ID of the previous (calling) transaction.

PropertyDef	
Data Type	MFilesAPI.PropertyDef
Mode	In
Variable Use	Contains the information about the property value being calculated, such as the property value definition ID, name, and data type.

PropertyValue	
Data Type	MFilesAPI.PropertyValue
Mode	In
Variable Use	Contains a property value. Each property value is stored in the PropertyValues variable as a variable of the type PropertyValue. A certain property value can be retrieved with the SearchForProperty method.

PropertyValues	
Data Type	MFilesAPI.PropertyValues
Mode	In
Variable Use	Contains all the property values of the target version that were affected by the current action. Each property value is stored in the variable PropertyValues as a variable of the type PropertyValue. A certain property value can be retrieved with the SearchForProperty method.

RestoredVersions	
Data Type	MFilesAPI.IDs
Mode	In
Variable Use	Contains object versions of the exported object that were imported from the content package.

SavepointVariables	
Data Type	MFilesAPI.NamedValues
Mode	In/Out
Variable Use	A container for optional name-value pairs stored for the duration of a single transaction. The container automatically reverts the modifications caused by failed operations in the container.

ScheduledJob	
Data Type	MFilesAPI.ScheduledJob
Mode	In
Variable Use	Contains a description of the scheduled job which is being performed.

ScheduledJobOutputInfo	
Data Type	MFilesAPI.ScheduledJobOutputInfo
Mode	In
Variable Use	Contains information of the scheduled job result after the job has been performed.

StateID	
Data Type	`MFilesAPI.Number`
Mode	In
Variable Use	Contains the workflow state identifier which can be used to recognize the process state in scripts related to the workflows.

StateTransitionID	
Data Type	`MFilesAPI.Number`
Mode	In
Variable Use	The ID of the state transition.

TransactionCache	
Data Type	`MFilesAPI.NamedValues`
Mode	In/Out
Variable Use	A container for optional name-value pairs stored for the duration of a single transaction. The container retains all the modifications, even if they were caused by an operation that was later canceled due to an error.

UserAccount	
Data Type	`MFilesAPI.UserAccount`
Mode	In
Variable Use	Vault user information.

UserGroupAdmin	
Data Type	`MFilesAPI.UserGroupAdmin`
Mode	In
Variable Use	Vault user group information.

ValueListItem	
Data Type	`MFilesAPI.ValueListItem`
Mode	In
Variable Use	Contains the value list value which is being processed in the event handler.

Vault	
Data Type	`MFilesAPI.Vault`
Mode	In
Variable Use	Represents the document vault used in running the script. With the identifier, the script is able to handle the document vault contents in the same way as is possible with the M-Files API interface. In an error situation, all changes made to the document vault through the `Vault` entity will be cancelled.

Vault	
	The use of the `Vault` entity with scripts entails certain limitations. The scripts cannot, through the `Vault` entity, change the state of the object which the script is run to. The state change refers to checking out the object, checking in the object, undoing the check-out, and deleting and destroying the object. Also, all other objects that are checked out in the script must be checked in during running of the same script.

VaultSharedVariables	
Data Type	`MFilesAPI.NamedValues`
Mode	In/Out

Variable Use	A collection of named values stored in the document vault database. With the variable, the scripts can store their own values in the database so that they are also available to other scripts. The allowed data types for the named values are integer variables, Booleans, and strings.
	
	In the following example, the value 123 is stored as a named value and the number-based calculated value is then set as the value.
	
	`VaultSharedVariables( "Message" ) = 123`
	
	`Output = VaultSharedVariables( "Message" )`

11. Contacting Support

In case you cannot find a solution to your problem from this document, you can contact the M-Files customer support at *support@m-files.com*.

In addition to a verbal description of the problem, please include as much of the following information as possible to speed up the support process:

- Windows version and system type (64-bit or 32-bit).
- Complete M-Files version number (for instance, 11.2.4320.51).
- Number of affected users.
- Frequency and reproducibility of the problem/malfunction.
- Steps to reproduce the problem/malfunction.
- Application level error messages from the *Windows Event Viewer*.

    - *Event Viewer* is accessed via **Control Panel** > **Administrative Tools** > **Event Viewer**.
    - Include error messages for M-Files Server and M-Files Desktop separately.
- Name and complete version number of an installed antivirus software.
- Contents of a possible M-Files error message window (for instance, a screen capture including the error stack via the **Details >>** button).
- If a file cannot be opened via M-Files, can it be dragged to desktop and accessed on the local drive?

For Office products

- Microsoft Office version.
- The program (Word, Excel, Outlook, etc.) causing the problem/malfunction.

Status of the vault

- Is the vault Firebird or Microsoft SQL based?
- Is the file data included in the database or stored in a separate location?
- Has the vault been optimized recently?

    - Optimization procedure sets the vault to offline state.
- Has the vault been verified and repaired recently?
- If M-Files Admin is used for verifying and repairing the vault, does it report any errors?
- Has the vault been indexed lately?
- Does the M-Files installation include integrations or other add-ons (Dynamics, SharePoint, Salesforce, etc.)?

    - Provide full version information of any integrations or add-ons.

    📄 **Note:** Any relevant screen captures of the situation and settings are always helpful.

12. Frequently Asked Questions

This section deals with some of the most common questions related to the use of M-Files.

12.1. What are the hardware requirements and recommendations?

For technical specifications, refer to *System Requirements and Technical Details* on page 21.

In a system with fewer than 40 users, the M-Files server can be run on a computer meeting the Windows operating system requirements. The higher the number of concurrent users, the more is required of the hardware. Free space requirements depend on the number of documents and other objects. The version history, however, does not expand the disk space requirement in a linear fashion, because M-Files Server saves the data in the form of changes between different versions.

The M-Files server and its document vault can be easily transferred to another server machine as system requirements increase.

12.2. How often should I make backups?

The M-Files server is used to save important data, so it is very important to take care of backup procedures. A regular backup should be made of each document vault and master database on the server. Backups are easy to set up via the *scheduled jobs* on page 215 in the M-Files Admin tool. We recommend setting M-Files to run backups every night.

Each backup produces files that should be transferred to a safe place.

Example: Your organization has a separate disk server. The master database and document vault backups are run on the M-Files server every night using the scheduled jobs. The jobs are set up so that each produces a single file that replaces the older one. Backup files are set to be transferred to the disk server and from there to a tape drive. In the event of problems, like hardware failure, the backups allow quickly returning M-Files to working order.

12.3. What's new in this M-Files version?

For more information about new, version-specific M-Files features, refer to the M-Files web site *https://www.m-files.com/latest-ecm-features*.

12.4. How do the automatic updates work?

M-Files automatically checks for software updates. When an M-Files upgrade covered by your subscription becomes available, the upgrade is downloaded to your computer and can be installed whenever doing so is convenient for you. New M-Files versions normally become available as automatic updates about a month after a new version has been officially released.

> **Note:** See *Installation preconditions* on page 44 for ensuring version compatibility.

Automatic updates are a useful way to keep your software up to date. However, system administrators may opt to disable such functionality, because in larger organizations it is usually easier to handle updates in a centralized manner. For more information on how to do so, refer to *M-Files Setup: Advanced User's Guide*.

The feature obtains the latest update information from the update server using HTTP on TCP port 80. This means that normally you do not need to change any firewall settings.

See also *Automatic Updates* under *Installing M-Files Upgrades* on page 43.

12.5. Why can't I access the document vault?

The cause of the problem can be either authentication or the network connection.

If there are problems with the network connection, an error message usually reveals the cause of the problem. As regards authentication, there can be a few problems that should be solved by making the following checks.

1. Check that you have an active *login account* in M-Files Admin (refer to *Login Accounts* on page 209) and that a *user* (refer to *Users* on page 251) has been created for the login account in the document vault.
2. Ensure that your *password* is correct.
3. Check that you are using the *authentication method* (Windows/M-Files) specified for your login account. You can see your authentication method in the *Authentication* column in the login accounts.

If the problem cannot be solved, contact the M-Files system administrator.

12.6. Why can't I edit a document that has been checked out?

You cannot edit the document because it has been checked out by another user who has not yet checked the document back in. This is to prevent the creation of several different copies in M-Files. With system administrator permissions, the document can be forced to be checked in, but the changes made to the document during the checkout will then be lost.

12.7. How can I find the documents I have created myself?

You can search for documents based on certain specifications via additional conditions of the *Advanced Search* feature.

1. Open the *Advanced Search* pane and select **Additional Conditions...**
2. Open the *Properties* tab.
3. Click the **Add Condition** button.
4. Specify *document* as the object type, your own login account as the user, and select the equals sign (=) as the operator.
5. Perform the search by clicking **OK** and then the **Search** button.

Note: You can also create a view that shows only the documents you have created. Refer to *Properties (Additional Conditions)* on page 150 and *New View* on page 90.

12.8. How can I create a document that is only visible to me?

When filling in the metadata card, select *Only for me* in the *Permissions* field.

12.9. How can I add a new property to a class?

If you are a regular M-Files user, you can add properties while filling in the metadata card. You can select the *Add property* label in the metadata card to add a new property for the object. Please note that this property is only added to this particular object, not all objects of the class.

If you want to add a property to all documents of the class, go to *Classes* in M-Files Admin, right-click the desired class and select *Properties* from the context menu. You can add default properties for the class by clicking the **Add**... button. If the desired property cannot be found in the list, you need to create a new property definition (see *Property Definitions* on page 288).

12.10. Why did a file with a grayed-out icon appear on the M-Files drive when I saved a new document in Word?

The file became a temporary local file in the document vault. You can convert the *temporary local file to a document*; refer to *Convert to Document* on page 106.

12.11. How can I add a new item to a value list?

You can add values to a value list while filling in the metadata card via the **Add Value** button in the toolbar. This function is available only if it has been defined in the value list properties that regular users can add new values to this list.

If you are an M-Files system administrator, go to *Value Lists* in M-Files Admin, right-click the desired value list, and select *Properties* in the context menu. Click the **Contents**... button and add a new item by clicking the **New Item** button. If you do not have administrator rights, check with the system administrator that the *Allow users to add new values to this list* box is checked in the properties of the value list.

If the value list is object-type-based, the value list is edited through the object type. In this case, the new object type is created using the M-Files Desktop user interface.

12.12. How can I create a new view in which the objects are displayed by customer?

1. Move to the home view in the document vault.
2. Select **New View** from the shortcut menu. The *Define View* window should now be displayed.
3. Click the **Add...** button and select *Customer* from the property pull-down menu.
4. Click **OK**.
5. Define a name for your new view.
6. Click **OK**.

12.13. How can I add a new user to the document vault?

1. Go to *Users* in M-Files Admin.
2. Select the **New User** function from the task area. The *User Properties* window should now be displayed.
3. The *Login account name* pull-down menu shows all login accounts that have not been added to the document vault. If you want to create an entirely new login account, refer to *Login Accounts* on page 209.
4. Click **OK**.
5. Specify the permissions for the new user, click **Apply** and then **OK**.

12.14. Why can't I find the Checked Out to Me view?

Each user has the *Checked Out to Me* view, and it cannot be destroyed. However, the view may have been *hidden*.

To display hidden views:

1. In the view window, select the **Unhide Views** function from the shortcut menu.
2. Select the hidden view from the list and click **Unhide**.

Note: You can hide views by highlighting the view and selecting **Hide View** from the **View** menu.

12.15. Can I use M-Files programmatically?

M-Files includes an ActiveX/COM API. Supported languages include VB.NET, C#, Visual Basic, VBScript, and C++. Additionally, M-Files includes the M-Files Web Service API that allows programmatic access to M-Files through a REST-like interface. See *Application programming interface (API)* on page 26.

12.16. How do I change the name of a client computer without interfering with M-Files functionality?

If documents are checked out to the client in question when its name changes, edited information may be lost. This is because checkouts are user- and computer-specific. The computer is identified by its name. After the name is changed, M-Files considers the checkouts to belong to another computer and does not allow the user to access the edited information.

Check in all documents and items from the computer before changing the computer's name.

12.17. Where can I find more information when I need it?

In addition to this manual, you can look for help in the *Getting started with M-Files* guide or consult your organization's M-Files system administrator.

Customer Support

The M-Files upgrade agreement covers customer support (see also *Contacting Support* on page 409).

Customer support e-mail: *support@m-files.com*, tel.: +358 3 3138 7500.

Please note that customer support does not provide instructions on using the software.

More Information

If you are a developer or an M-Files system administrator, you might be interested in our documentation for:

- *M-Files API*
- *M-Files Web Service*
- *M-Files UI Extensibility Framework*

For a full list of M-Files documentation, please visit *m-files.com*.

Index