User Guide for Classic M-Files Desktop and M-Files Admin

Contents

1. Introduction

This section contains common M-Files terminology and information about this user guide.

The M-Files® knowledge work automation platform 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 is stored.

Instead of the traditional folder-based method, you have instant access to all of your content with search or dynamic views. It is simple, dynamic, and flexible. From managing a wide variety of content to ensuring regulatory compliance, M-Files has you covered.

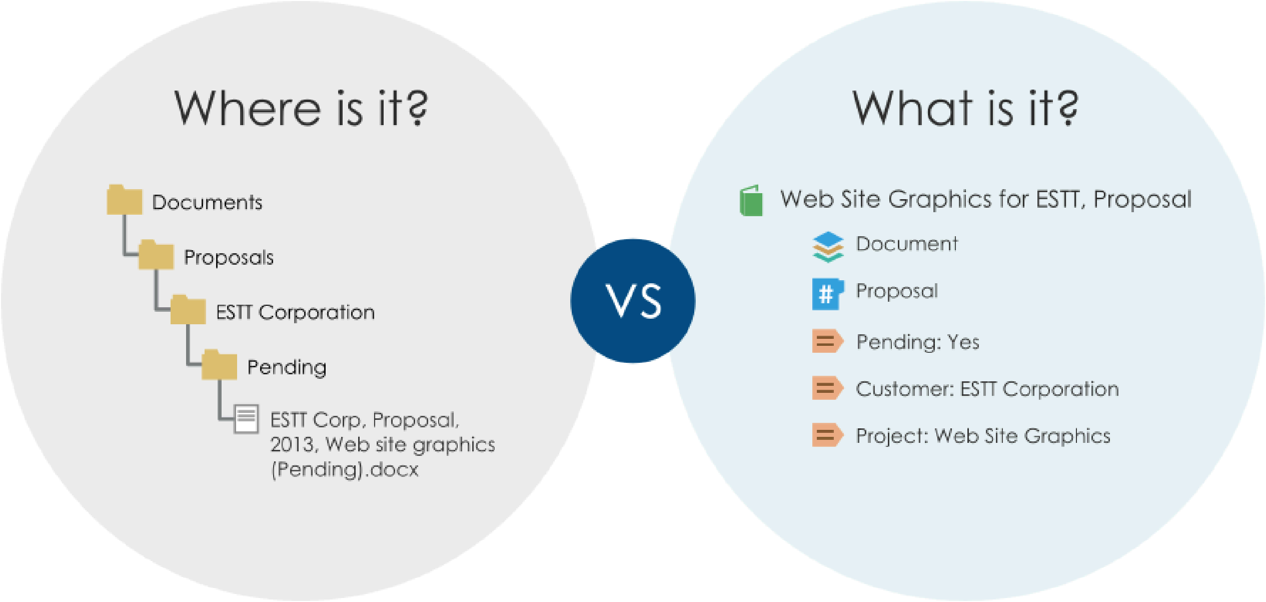

Where is it?
Documents
Proposals
ESTT Corporation
Pending
ESTT Corp, Proposal, 2013, Web site graphics (Pending).docx
VS
What is it?
Web Site Graphics for ESTT, Proposal
Document
Proposal
Pending: Yes
Customer: ESTT Corporation
Project: Web Site Graphics

Figure 1: M-Files organizes content based on what something is (and what it relates to) instead of where it is stored.

You can deploy M-Files on-premises, in the cloud, or a hybrid of both. For more information, see System Overview.

In this chapter

1.1. About This User Guide

This user guide is a comprehensive manual for effective use of M-Files. It includes detailed, step-by-step instructions for the core functionalities of M-Files, covering both everyday use and system administration tasks.

In addition to the M-Files user guide, there are separate guides available for M-Files Web, M-Files Hubshare, and M-Files Manage, each designed to help users get the most value out of these products. You can find all the user guides from the M-Files User Guides page.

Other useful resources

Refer to the Product Support section in M-Files Community for a full list of useful resources for users, admins, and developers.

In M-Files Community, you can interact with other users, ask questions, share tips and best practices, and ask help from M-Files experts. M-Files Help Center is a great resource especially for new M-Files users.

Technical product documentation

- M-Files knowledge base
- M-Files Support Portal
- M-Files Developer Portal

The M-Files knowledge base is a comprehensive collection of product guides for administrators who set up and manage M-Files solutions or need technical information about the product. The knowledge base has configuration instructions for the official M-Files add-ons and extensions.

The product guides tell you everything you need to know to set up and maintain an M-Files environment best suited for your organization. The knowledge base includes detailed instructions and information about a wide range of topics, such as collaboration, compliance, connectors, intelligence services, M-Files clients, searches and indexing, security, permissions, authentication, server installation and maintenance, and user synchronization.

You can find the product guides also in M-Files Support Portal. In the portal, you can also explore support articles for useful tips, recommendations, and answers to previously asked questions. If you need more help with your question, contact our customer support or your M-Files reseller.

If you are a developer or an M-Files system administrator, visit M-Files Developer Portal to find guides, tutorials, and samples for software development.

1.2. Accessing This User Guide

To open this user guide when M-Files is active press the F1 key on your keyboard. When you open the user guide with F1, you see a topic that is related to what you do at the moment in M-Files.

You can also open the user guide with the M-Files icon on the Windows notification area, and with help buttons in M-Files.

The user guide is also available as a PDF version. You can download it from the PDF icon in the upper right corner of the web user guide.

1.3. Conventions Used in M-Files User Guides

The M-Files user guides contain a number of typographic and writing conventions as well as visual elements that will help you to better understand information and to do tasks.

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`, 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 must open the menu bar and select the **Applications** item from the **Settings** menu.
Optional	Indicates that a step in a task is optional and up to the users to decide if they will complete the step.
Info	Highlights important information related to a specific step in a task. This information is always under the related step.
Example	Highlights an example of how a given step is completed. This information is always under the related step.
Result	Highlights a description of the expected results after you have completed a task step.
Bold	Bolded text indicates user interface elements, such as buttons, menu items, and dialog names. Examples: Click **OK** to continue. The **Object Type Properties** dialog is opened.

1.4. M-Files Terminology

The following table describes daily M-Files terminology.

Term	Definition
M-Files software	The M-Files software consists of these 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 (see Accessing M-Files Web) or a mobile device (see Accessing M-Files Mobile).
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. Once you have installed 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.

Term	**Definition**
Multi-file document	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.
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 and 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. They can be used to organize content or import files to M-Files.
Client	A *client* is the regular M-Files user's computer or mobile device and the software installed on it. The regular user performs operations like creating documents and exploring the document vault.

Term	Definition
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 user guide often represents operations as being performed on documents, but the same operations are available for 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 (compare with 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. 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 on workflows, see Configuring Workflows.
Server	M-Files Server runs on a server computer. 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.

Term	Definition
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.
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 login account. Compare with login accounts.
Intelligent Metadata Layer	Intelligent Metadata Layer, abbreviated as IML, is a repository-neutral approach to intelligent information management that unifies information across the enterprise based on context, not on the system or folder in which the information is stored. In addition, IML categorizes documents and records automatically and provides metadata suggestions with the aid of artificial intelligence. See Intelligent Metadata Layer for more information.
Managed object	A managed object is either an internal M-Files object stored in a document vault or a promoted external repository object. Managed objects have metadata in M-Files and can be managed using various M-Files functionalities, such as version history or workflows. A managed external repository object can be demoted to an unmanaged object by removing its metadata. Compare with unmanaged object and see Unmanaged and Managed Objects.
Unmanaged object	An unmanaged object in M-Files represents a file in an external repository. An unmanaged object does not have M-Files metadata and it cannot be managed with the M-Files version history or workflows. An unmanaged object can be promoted into a managed object by adding metadata to it. Compare with managed object and see Unmanaged and Managed Objects.
Repository	A repository is any accessible place where information can be stored and accessed, such as an M-Files document vault, or an external location such as a network folder or a SharePoint site. Compare with external repository.
External repository	A repository that is other than an M-Files vault and the contents of which are displayed and can be edited via the M-Files user interfaces. Compare with repository.

Term	Definition
Connector	A vault application that lets an external repository to be shown and accessed with M-Files. See Connectors for more information.
Intelligence service	An intelligence service is a vault application that attempts to understand vault content the way humans do. They can, for instance, be used to analyze file content and existing metadata for automatically categorizing content or for providing end users with metadata suggestions. See Intelligence Services for more information.
Vault application	Vault applications are pieces of software that are installed to a document vault to extend the functionality of the vault. See Installing and Managing Vault Applications for more information.
Quick view area	The area on the left side of the home screen, containing a number of quick views, such as **Recently Accessed by Me**, **Assigned to Me**, and **Checked Out to Me**.

1.5. Getting Started with M-Files

If you are a new M-Files user, we recommend that you start with the content in M-Files Help Center and then come back to the user guide.

The table given here contains links to help you get started with the use of M-Files. Many of the linked sections put focus on the use of the classic M-Files Desktop, but many of the concepts and procedures are usable in all M-Files clients. There is a separate user guide for M-Files Web and the new M-Files Desktop.

Task	Links to instructions
Opening M-Files clients and accessing vaults	• Accessing M-Files Desktop • Accessing M-Files Web • Accessing M-Files Mobile
Learning the basics of the classic M-Files Desktop	Using the Classic M-Files Desktop
Using metadata and the metadata card	• Object Metadata • Metadata Card
Adding content to M-Files	Adding Content to Vault
Editing content in M-Files	Editing Content
Finding content with searches	Searching

Task	Links to instructions
Finding content with views	Using Views
Using document templates	Using Document Templates
Working offline	Using the Classic M-Files Desktop Offline

1.6. Contacting Support

If you cannot find a solution to your problem in the user guide, refer to M-Files Support Portal or the M-Files knowledge base.

You can also log in to M-Files Support Portal to create a support ticket. For instructions on the details to include in the ticket, refer to the article Basic Information to Submit for M-Files Support. If you purchased your M-Files subscription from an M-Files reseller or partner, contact the reseller instead.

If phone support is included in your subscription, you can call our customer support. See the phone numbers at https://www.m-files.com/about/contact.

For information about our support scope, service availability, response times, and priority levels, refer to https://www.m-files.com/product-support-policy.

2. Daily Use

This section gives information about the day-to-day use of M-Files.

This section tells you how to access M-Files, use the classic M-Files Desktop, and manage, share, and find content in M-Files. You can also find information about the user settings for M-Files Desktop.

If you are a new M-Files user, we recommend that you visit M-Files Help Center to learn the basics of M-Files.

In this chapter

2.1. Accessing M-Files

Before you use your M-Files vault, make sure that your M-Files system administrator has done these operations:

- The M-Files system has been set up.
- A vault connection or vault connections have been added for you.

In this chapter

2.1.1. Accessing M-Files Desktop

When M-Files Desktop is installed and your vault connections are set up, you see all the vault connections on your M-Files drive in File Explorer. To use M-Files, click the icon on your desktop. You can also use the Windows start menu or the M-Files drive in File Explorer.

M-Files Desktop versions

There are two versions of M-Files Desktop that you can use: the classic M-Files Desktop (this user guide) and the new M-Files Desktop (refer to the user guide for M-Files Web and the new M-Files Desktop).

To switch between the two versions, use the NEW toggle in the top area.

Logging in

To log in, double-click a vault on the M-Files drive. To log in as a different user, right-click the vault and select **Log In as**. If M-Files cannot use your Windows credentials for the login, the system asks you for your credentials when you open the vault.

Logging out

To log out, click your initials in the top-right corner of the user interface and select **Log Out**.

2.1.2. Accessing M-Files Web

You can go to M-Files vaults also with M-Files Web. M-Files Web is a browser-based M-Files client that lets you use the basic M-Files functions.

There are two versions available: the classic M-Files Web and the new M-Files Web. For basic guidance on how to use the classic M-Files Web, see the Using the Classic M-Files Desktop. For guidance on the use of M-Files Web, refer to the user guide for M-Files Web and the new M-Files Desktop.

You can get the address of M-Files Web in your organization from your system administrator.

Editing content in M-Files Web

In M-Files Web, you can use M-Files Web Companion to edit content with desktop applications. With the classic M-Files Web, you can use the M-Files for Chrome extension.

Logging in to the classic M-Files Web

1. In your web browser, go to the M-Files Web address given by your system administrator or an M-Files consultant.

   If the name of your vault is *Sales Tracker*, the address can be *https://sales-tracker.cloudvault.m-files.com* for cloud-based deployments or *http://sales-tracker.mydomain.com* for on-premises vaults. In your corporate network, the connection protocol can be *HTTP* instead of *HTTPS*.

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

3. Optional: If you have access to many vaults, select the vault to which to connect.

   If you have access to only one vault, you are automatically connected.

2.1.3. Accessing M-Files Mobile

M-Files is also available as a mobile application for iOS and Android devices.

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)

Application language

M-Files mobile applications use the language settings of your device.

Editing Office documents with M-Files Mobile

For information about editing Office 365 documents with M-Files Mobile, refer to Editing Office Documents in M-Files Mobile with O365 Integration in M-Files Support Portal.

Logging in to M-Files Mobile

1. Contact your vault administrator or an M-Files consultant to get the login information of the vault.

2. Open the M-Files mobile app on your device.

3. On the login screen, enter the full server address, your username, and password.

   If the name of your vault is *Sales Tracker*, the address can be *https://sales-tracker.cloudvault.m-files.com* for cloud-based deployments or *http://sales-tracker.mydomain.com* for on-premises vaults. In your corporate network, the connection protocol can be *HTTP* instead of *HTTPS*.

   For cloud vaults hosted in M-Files Cloud, M-Files recognizes the server address even if you only enter the *sales-tracker* part. However, to make sure that the correct protocol and address are used, we recommend to always use the full server address.

4. Tap **Log in**.

5. Optional: If you have access to many vaults, select the vault to which to connect.

   If you have access to only one vault, you are automatically connected.

Adding a vault connection with QR code

You can add a vault connection for M-Files Mobile with a QR code shown in M-Files Desktop and in M-Files Web.

To add vault connection with QR code:

1. Open M-Files Desktop or M-Files Web and the vault to which you want to connect with M-Files Mobile.

2. Click your initials in the top-right corner of the user interface and select **Use with M-Files Mobile**.

✓ A window with a QR code opens.

3. Open the QR code scanner:

   a. Long-press the M-Files app icon on your mobile device and select **Scan Barcode**.

      or

   b. Open the M-Files app on your device and start to add a new vault connection. Tap the QR code icon () in **Server address**.

4. Scan the QR code.

   ✓ M-Files fills the **Server address** automatically.

5. Tap **Connect**.

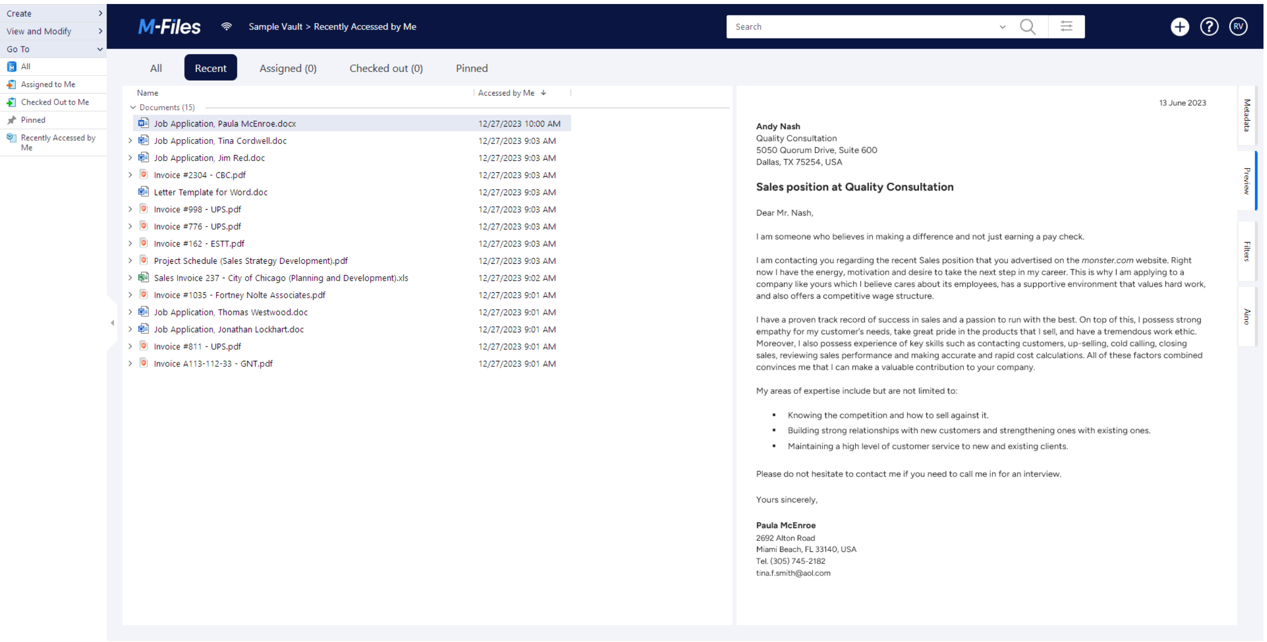
6. Enter your username and password.

7. Tap **Log in** to open the vault in M-Files Mobile.

For more information, refer to Connecting to Vaults with QR Codes in M-Files Mobile in M-Files Support Portal.

2.2. Using the Classic M-Files Desktop

This section tells about the user interface for the classic M-Files Desktop. Click on different parts of the screenshot below for a description of the areas in the user interface.



Name	Accessed by Me
Documents (15)	
Job Application, Paula McEnroe.docx	12/27/2023 10:00 AM
Job Application, Tina Cordwell.doc	12/27/2023 9:03 AM
Job Application, Jim Red.doc	12/27/2023 9:03 AM
Invoice #2304 - CBC.pdf	12/27/2023 9:03 AM
Letter Template for Word.doc	12/27/2023 9:03 AM
Invoice #998 - UPS.pdf	12/27/2023 9:03 AM
Invoice #776 - UPS.pdf	12/27/2023 9:03 AM
Invoice #162 - ESTT.pdf	12/27/2023 9:03 AM
Project Schedule (Sales Strategy Development).pdf	12/27/2023 9:03 AM
Sales Invoice 237 - City of Chicago (Planning and Development).xls	12/27/2023 9:02 AM
Invoice #1035 - Fortney Nolte Associates.pdf	12/27/2023 9:01 AM
Job Application, Thomas Westwood.doc	12/27/2023 9:01 AM
Job Application, Jonathan Lockhart.doc	12/27/2023 9:01 AM
Invoice #811 - UPS.pdf	12/27/2023 9:01 AM
Invoice A113-112-33 - GNT.pdf	12/27/2023 9:01 AM

13 June 2023

Andy Nash
Quality Consultation
5050 Quorum Drive, Suite 600
Dallas, TX 75254, USA

Sales position at Quality Consultation

Dear Mr. Nash,

I am someone who believes in making a difference and not just earning a pay check.

I am contacting you regarding the recent Sales position that you advertised on the *monster.com* website. Right now I have the energy, motivation and desire to take the next step in my career. This is why I am applying to a company like yours which I believe cares about its employees, has a supportive environment that values hard work, and also offers a competitive wage structure.

I have a proven track record of success in sales and a passion to run with the best. On top of this, I possess strong empathy for my customer's needs, take great pride in the products that I sell, and have a tremendous work ethic. Moreover, I also possess experience of key skills such as contacting customers, up-selling, cold calling, closing sales, reviewing sales performance and making accurate and rapid cost calculations. All of these factors combined convinces me that I can make a valuable contribution to your company.

My areas of expertise include but are not limited to:

- Knowing the competition and how to sell against it.
- Building strong relationships with new customers and strengthening ones with existing ones.
- Maintaining a high level of customer service to new and existing clients.

Please do not hesitate to contact me if you need to call me in for an interview.

Yours sincerely,

Paula McEnroe
2692 Alton Road
Miami Beach, FL 33140, USA
Tel. (305) 745-2182
tina.f.smith@aol.com

1. Top area
2. View navigation

3. Listing area
4. Right pane
5. Task area

Top area

The top area of contains these items:

- M-Files logo
- Connection status
- Navigation path
- Search field and search options
- Object creation icon
- Link to M-Files Help Center
- User menu icon

M-Files logo

Click the M-Files logo to go to your home tab. To change which tab the logo link opens, see Setting Your Home Tab.

Connection status

The connection status icon (📶) shows the status of your connection to the vault. The connection is measured with the round-trip time to the server that hosts the vault. Click the connection status icon to open the **Connection Status** dialog. If your connection is slow or there is no connection to the server, contact your M-Files system administrator. Click **Refresh** to refresh the information of your connection status or **Analyze Connection** to see details about your connection.

Navigation path

The navigation path shows you where you are. In practice, it contains the name of the current view and of all its parent views. The path can be, for example, **Sample Vault** > **Documents** > **By Customer** > **A&A Consulting**.

Searching

Use the search bar to find your documents and other objects. For more information, see Searching.

Creating objects

Click **Create** (⊕) to create an object. For more information, see Creating Documents and Creating Non-Document Objects.

M-Files Help Center

M-Files Help Center is a great resource for new M-Files users. Click the question mark icon (?) to get started.

View navigation

The bar below top area contains a number of useful views. For example, these views:

- **Recent**: Objects that you have recently used.
- **Assigned**: Objects that are assigned to you.
- **Checked Out**: Objects that you have checked out for editing.
- **Pinned**: Objects that you have pinned.

Listing area

The listing area usually contains views and objects. For more information, see Listing Area.

Right pane

The contents of the **Metadata**, **Preview**, **Filters**, and **Aino** tabs are shown in the right pane. To hide the right pane, click the active tab. For example, **Metadata** or **Preview**. You can drag the left border of the metadata card and preview window to resize them.

Metadata card

To see and change the metadata of the selected object, use the metadata card. For more information, see Object Metadata and Metadata Card.

Preview

In the preview mode, you can browse and copy the content of the selected document. For more information, see Document Preview.

Filters

When you search for an object or a document, you can use the advanced search features on the **Filters** tab. In the **Filters** tab, you can give more specific search criteria for your search. For more information, see Search Filters.

Aino

To summarize a selected document or to get responses of the document content, use M-Files Aino. For more information, see Using M-Files Aino.

Note: If the M-Files Aino tab is not shown, it can be that M-Files Aino is not available in your platform edition or not set up. The setup instructions for M-Files admins are available in M-Files Catalog.

Task area

In the task area, you can see shortcuts to different operations. For more information, see Task Area. Click the handle on the right edge of the task area to hide it.

User menu

Click your initials in the top-right corner to see these items:

- About M-Files
- Set your home tab (in User Settings)
- Set a default tab for the objects selected in the listing area (in User Settings)
- Notification Settings (in User Settings)
- Substitute Users (in User Settings)

- Change Language (in User Settings)
- Use with M-Files Mobile
- Shared by Me
- Go Offline
- Log Out
- External Repositories

In this chapter

2.2.1. Listing Area

The listing area in M-Files Desktop usually contains views and objects. The listing area and Windows File Explorer operate very similarly. One difference is that for an object in M-Files Desktop, you can use the arrowheads to show and hide related objects and files. There are two types of arrowheads: The filled arrowhead (▶) shows that the object contains files and the hollow arrowhead (›) shows that the object has metadata-based relationships to other objects.

Sorting objects in the listing area

Objective	Instructions
Change the sort order of the objects in the listing area.	Click a column heading in the listing area.
Change the sort order to ascending or descending.	Right-click a column heading and select a sort order.
Select secondary, tertiary, and other sort orders.	Hold down the Ctrl key and click another column heading.
Add more columns to the listing area.	Right-click on the column heading area and select **Choose Columns**.

For information on how the search results are grouped, see Search result grouping.

Listing area troubleshooting

If an item name in the listing area is shown in gray text, the full item path is too long for Windows (more than 259 characters). It is thus necessary to rename parts of it to make sure that the content operates properly. If you use Microsoft Windows 10 or later, you can ask your system administrator to enable longer item paths.

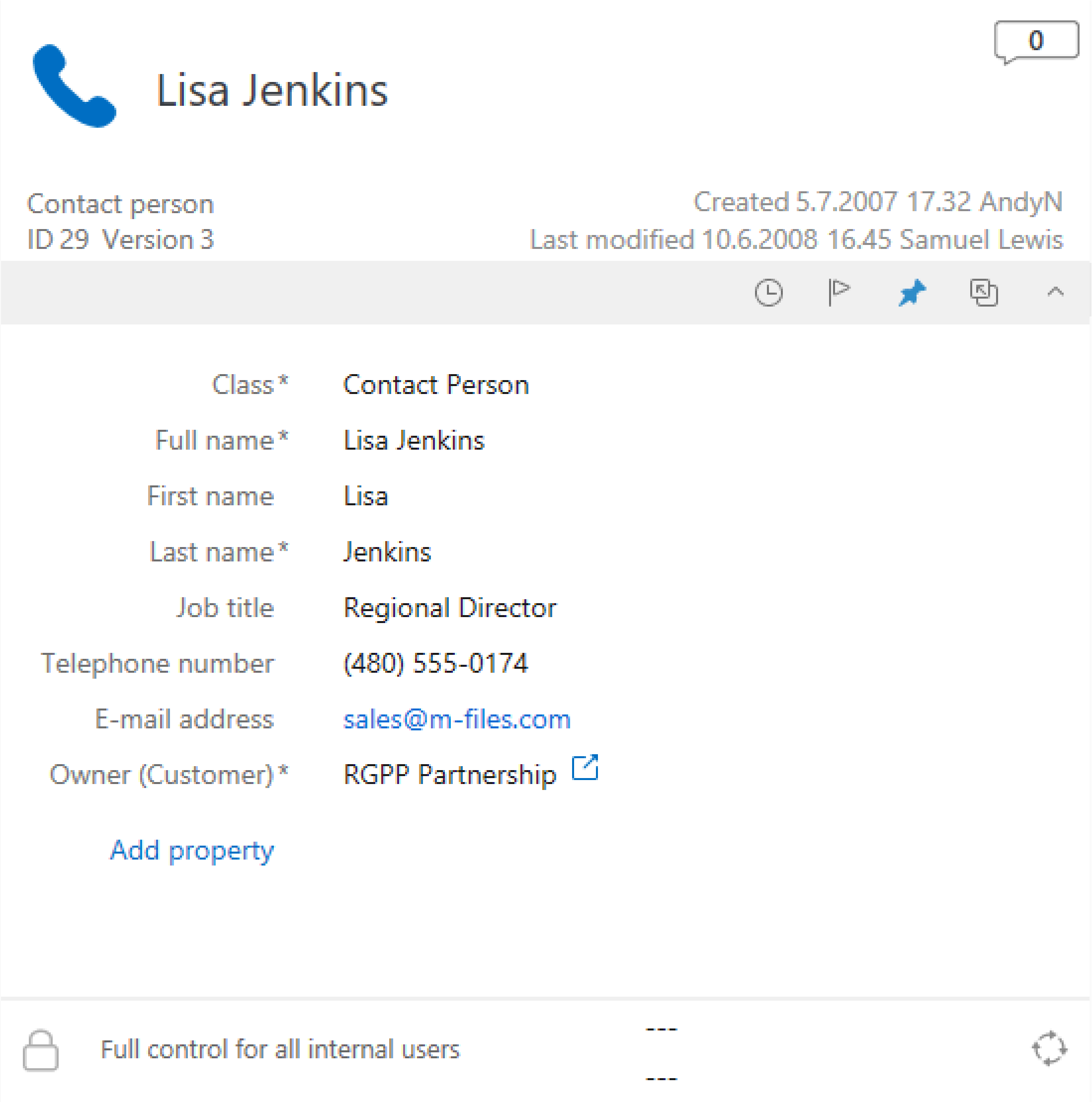
If the **Size** column for an object is empty, the size of the object is temporarily unknown. When the object is opened, the size of the object is updated in the **Size** column.

2.2.2. Metadata Card

The metadata card contains important information about the object. For example, the title, creation time, author, and class of a document. Click the **Metadata** tab to open or close the metadata card or drag the left border of the window to resize it.

Tip: To open the metadata card in a separate window in the classic M-Files Desktop, select an object in the listing area and press Alt + Enter. For more keyboard shortcuts, see Keyboard Shortcuts in the classic M-Files Desktop.

Click the different parts of the screenshot for a description of the metadata card sections.



Lisa Jenkins

Contact person
ID 29 Version 3

Created 5.7.2007 17.32 AndyN
Last modified 10.6.2008 16.45 Samuel Lewis

Class*	Contact Person
Full name*	Lisa Jenkins
First name	Lisa
Last name*	Jenkins
Job title	Regional Director
Telephone number	(480) 555-0174
E-mail address	sales@m-files.com
Owner (Customer)*	RGPP Partnership

Full control for all internal users

1. Object comments
2. Metadata card option ribbon
3. Object metadata
4. Object permissions
5. Object workflow

Object comments

Click the comments icon (💬) to see the comment view. In the comment view, you can see and add comments to the object. For more information, see Object Comments.

Metadata card option ribbon

The option ribbon contains options related to the selected object and the metadata card.

Icon	Action
🕒	Opens the **History** dialog of the object.
⚐	Sets the object as followed or unfollowed. When the object is set as followed, you get an email notification when someone changes the document. For more information on notifications, see Editing Notification Settings in the Classic M-Files Desktop. **Note:** The person who changed the object does not get a notification.
📌	Pins or unpins the object.
⧉	Opens the metadata card in a new window.
^	Hides or shows the title area of the metadata card.

Object metadata

Metadata helps you to find objects in M-Files. Metadata is the information related to an object. For more information, see Object Metadata.

Object permissions

Click the permissions area to open the **Permissions** dialog. In the dialog, you can change the permissions for the object. For more information, see Object Permissions.

Object workflow

Use the workflow options select a workflow and a workflow state for an object. For more information, see Workflows.

2.2.3. Document Preview

The preview option lets you see the content of the selected object. M-Files shows the document preview for the file types listed on this page. Click the **Preview** tab to open or close the document preview or drag the left border of the window to resize it.

To zoom PDF files on the **Preview** tab, right-click and select **Zoom In Tool**. Right-click again to use the different zoom tools.

To edit the object, check out the document and make necessary changes, or add annotations in the preview mode.

On the **Preview** tab, you can see the content of these file types:

- 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 (vsdx, vsx, vtx, vdx, vssx, vstx, vsdm, vssm, vstm, vdw, vsd, vss, vst)

- Video files (mp4, webm, ovg) *
- Audio files (mp3, ogg, wav) *

*) Supported only in M-Files Web

It is possible to extend the support for other file types. For example, DWG files. To do this, you must have a compatible third-party application set up and set it as the default application for that file type. However, this is necessary only for file types that are not listed here.

The maximum file size for document preview in M-Files Web

File type	Maximum file size
Email files	10 MB
Image files	100 MB
Video files	1 GB
Audio files	500 MB
Microsoft Word files	25 MB
Microsoft PowerPoint files	10 MB
Microsoft Excel files	10 MB
Visio drawings	10 MB

2.2.4. Pinned Content

The **Pinned** tab lets you collect items that you frequently use into a single tab. Click the **Pinned** tab in the view navigation bar to see your pinned items.

Click the arrow in front of a group name to expand or collapse a group of pinned items. Use the options at the top of the **Pinned** tab to filter pinned items by name, add a group to the **Pinned** tab, or expand or collapse all groups.

Click an item on the **Pinned** tab to see its metadata or preview in the right pane. Double-click the item to do the default action of the object. To move a pinned item on the **Pinned** tab, drag and drop the item.

Click the three dots icon (⋮) to show more options. For example, you can rename a pinned item. This changes the name of the shortcut but not the name of the item.

The **Pinned** tab can contain a maximum of 200 items.

Favorites and Pinned tab

The **Favorites** functionality is no longer part of the most recent versions of M-Files. You can instead pin items and move content from **Favorites** to the **Pinned** tab.

Pinning an item

To pin an item to the **Pinned** tab:

1. In the classic M-Files Desktop, find and select the item that you want to pin.
2. Complete one of these steps:

    a. Drag and drop the item from the listing area to the **Pinned** tab in the view navigation bar.

    or

    b. Right-click the item and click **Pin**.

    or

    c. Click the **Pin** icon (📌) on the option ribbon of the metadata card.

The selected item is pinned to the **Pinned** tab.

By default, the item is pinned to the **Ungrouped** group. To unpin an item, click the three dots icon (⋮) and select **Unpin**.

Adding groups to the Pinned tab

You can divide the pinned items into groups.

To add a group:

1. In the classic M-Files Desktop, click the **Pinned** tab.
2. Click the plus icon (+) at the top of the **Pinned** tab.
3. Enter a name for the group.

    ☑ The group is added to the **Pinned** tab.

4. Optional: Drag and drop items to the group.

Editing groups on the Pinned tab

To change the position of a group:

1. On the **Pinned** tab, drag and drop a group.

To rename a group:

2. Click the three dots icon (⋮) and select **Rename**.
3. Enter a new name.

To remove a group:

4. Click the three dots icon (⋮) and select **Remove**.
5. Optional: If the group contains pinned items, select one of these options in the **Remove Group** dialog:

Option	Action
Unpin	Removes the group and unpins the pinned items that it contains.
Keep Pinned	Removes the group and moves the pinned items to the **Ungrouped** group.

Moving content from your favorites to the Pinned tab

1. In the classic M-Files Desktop, open the **All** tab.
2. Open **Other Views** > **Favorites**.
3. In the **Favorites** view, select the items that you want to move.
4. Right-click one of the selected items.
5. Select **Move from Favorites to Pinned**.

The selected items are moved to the Pinned tab.

2.2.5. Task Area

The task area in the classic M-Files Desktop contains shortcuts to different operations. Click the gray vertical handle on the left side of the user interface to show or hide the task area.

Section	Content
Create	Quick links for object creation. For more information on how to create objects, see Creating Documents and Other Objects.
Go To	A list of predefined links to the most commonly used views.

When you have selected an object in the listing area, you can see also the sections **View and Modify** and **State transition** in the task area.

Section	Content
View and Modify	A list of object-specific operations. For example, **Check Out** and **Check In**.
State transition	A list of the available state transitions for the selected object. For more information, see Changing the Workflow State in the Task Area. **Note:** The **Change State** command is shown in the task area only if the object has a workflow and you have the permission to change the workflow state.

Customizing the task area

You can customize the shortcuts of the **View and Modify** and **Go To** sections.

Objective	Instructions
Add or hide shortcuts in the **View and Modify** section.	Right-click an empty space in the task area and select or unselect a shortcut from **Commands**.
Add an object shortcut to the **Go To** section.	Select the object, open the menu bar with the Alt key, and select **Operations** > **Add Shortcut to Task Area**.
Add a view or virtual folder shortcut to the **Go To** section.	Right-click on a view or virtual folder and select **Add Shortcut to Task Area**.
Rename, remove, or move shortcuts in the **Go To** section.	Right-click a shortcut in the task area and select a command.

2.2.6. Customizing the User Interface of the classic M-Files Desktop

You can change display settings with the **Display Mode** options. Right-click an empty space in the listing area and select **Display Mode** to see the settings.

With the **Display Mode** options, you can do these operations:

- Select if the objects are shown as icons or as a details list.
- Select if the Windows File Explorer navigation pane is shown or not.
- Select if the task area, the right pane, and the bottom pane are shown as usual, minimized, or not at all.
- Show or hide annotations.
- Enable or disable the options for object grouping by object type and view and folder grouping.
- Select a normal or a compact layout for the user interface.

You can also set the **Metadata card** or the **Preview** tab to be used as the default tab. For more information, see Setting Default Tab for Object.

2.2.7. Keyboard Shortcuts in the classic M-Files Desktop

Shortcuts in the listing area

Use these shortcuts when the listing area is active:

Quick Search	Ctrl + F	See Quick Search.
New Document	Ctrl + N	See Creating Documents.
Refresh the object listing	F5	Updates only the objects that have changes.
Fully refresh the object listing	Shift + F5	Updates all the objects in the listing area.

Shortcuts for the selected objects

Use these shortcuts when an object is selected in the listing area:

Open the metadata card	Alt + Enter	See Metadata Card.

Check Out	Ctrl + O	See Checking Out a Document.
Check In	Ctrl + I	See Checking In a Document.
Check in with comments	Ctrl + ⇧ Shift + I	See Checking In a Document.
Relationships	Ctrl + L	See Object Relationships.
Collection members	Ctrl +⇧ Shift + L	See Managing Document Collections.
Comments	Ctrl + M	See Object Comments.
Subobjects	Ctrl + J	See Subobjects.
History	Ctrl + H	See Version History.

Shortcuts for the metadata card

Use these shortcuts on the metadata card:

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.
Ctrl + S	Save metadata.

2.3. Managing Content

This section tells you how to manage content in the classic M-Files Desktop.

In this chapter

2.3.1. Adding Content to Vault

This section tells you how to add content to your M-Files vault.

In this chapter

- Making Copies of Existing Objects
- Making PDFs of Objects
- Functions in Microsoft Outlook

Saving to M-Files

When you save files to your M-Files drive, the information is not usually stored on your personal hard drive. With M-Files Desktop, you see the M-Files drive in File Explorer like your other hard drives.

To save files to your M-Files drive, use one of these methods:

- Drag and drop
- Copy and paste
- **Save As** function in an application
- Import Files and Folders dialog

When you save a file to M-Files, M-Files asks you to add metadata. For more information, see Object Metadata.

Saving many files to M-Files

You can save many files to M-Files with drag and drop, copy and paste, and the **Import Files and Folders** dialog.

Tip: To save many files with the same metadata, enable **Use these values as defaults for the next document**.

Tip: Use **Skip This** to select not to save a file to M-Files. You can do this when you save many files to the vault.

Detecting duplicate file contents

If you try to save a file that is already in the vault, M-Files lets you know. M-Files shows you the duplicate documents to which you have permissions. For information on how the detection is done, see the How does the duplicate detection feature work? page.

Duplicate file content is shown in the listing area and when you add new content to the vault.

- Listing area: To see the documents with duplicate file content, expand the object. The duplicate documents are shown under the **Duplicate File Content** node.
- When you add new vault content: If M-Files detects documents with duplicate file content in the vault, it shows the **Duplicate File Content** dialog. In the dialog, select **Do Not Create** or **Create Anyway**.

If you save many files, enable **Do this for the next duplicate documents** to use the same selection for all the duplicate documents that M-Files finds during the operation. This option is not available with the **Save As** function.

In this chapter

- Dragging and Dropping Files to M-Files
- Copying and Pasting Files to M-Files
- Saving to M-Files from Application
- Saving Folders to M-Files

Dragging and Dropping Files to M-Files

To add content to the vault with drag and drop:

1. In File Explorer, find the file that you want to save.
2. Drag and drop the file to an empty space in the listing area in M-Files.

   ☑ The **New Document** dialog opens.

   > **Note:** In some views opened through the **Browse relationships** feature, M-Files can usually fill in all the mandatory properties, for example, based on the associated project. When this happens, the **New Document** dialog is not shown when you drag and drop files to the vault.

3. Select a class for the file from the **Class** drop-down menu.
4. Optional: Enter other optional property values.

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

5. Click **Create**.

Copying and Pasting Files to M-Files

1. In File Explorer, find the file that you want to save.
2. Right-click the file and select **Copy**.
3. Go to the M-Files window, right-click on an empty space in the listing area, and select **Paste**.

   ☑ The **New Document** dialog opens.

4. Select a class for the file from the **Class** drop-down menu.
5. Optional: Enter other optional property values.

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

6. Click **Create**.

Saving to M-Files from Application

For information on how to save your work from a Microsoft Office application (Office 2013 or later) to M-Files, see Example: Saving a Microsoft PowerPoint Presentation to M-Files with the M-Files Tab. For information on how to save your work from other desktop applications to M-Files, see Example: Saving a Microsoft PowerPoint presentation to M-Files.

Example: Saving a Microsoft PowerPoint Presentation to M-Files with the M-Files Tab

1. In Microsoft PowerPoint, create a new presentation or open one.
2. Make changes to the document.
3. Open the **M-Files** tab in the Microsoft PowerPoint ribbon.
4. Click **Save to M-Files**.

5. Click the vault where you want to save your presentation.

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

6. Select a class for the file from the **Class** drop-down menu.
7. Optional: Enter other optional property values.

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

8. Click **Create**.

Your presentation is saved to M-Files.
Example: Saving a Microsoft PowerPoint presentation to M-Files

1. In Microsoft PowerPoint, create a new presentation or open one.
2. Make changes to the document.
3. Click **File** > **Save As** > **Computer** > **Browse**.

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

4. In the left pane of the **Save As** dialog:

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

      or

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

5. Double-click the vault where you want to save your presentation.
6. In **File name**, enter a file name for your presentation.
7. Select **Save**.

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

8. Select a class for the file from the **Class** drop-down menu.
9. Optional: Enter other optional property values.

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

10. Click **Create**.

Your presentation is saved to M-Files.
Saving Folders to M-Files

> **Note:** Your administrator can use external repository connectors to import files from a network drive. Before you import files or folders, make sure that the same content is not already in the vault.

When you save a folder with subfolders or many individual files together, M-Files can keep the old folder structure. If you want the folder structure to stay the same, M-Files organizes the saved contents into traditional folders. To do this:

1. In the classic M-Files Desktop, press Alt to open the menu bar.
2. Select **Create** > **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.

    or

    b. **Preserve old folder structure** to keep the folder structure. To import the content, select a folder for it in M-Files. To create a new folder, click **New Folder**.

5. Optional: If you do not want to add metadata for the imported content, disable **Prompt for metadata**.
6. Click **OK**.

If you checked the **Prompt for metadata** check box, do the steps from 7 to 9 for each file you import.

7. Select a class for the file from the **Class** drop-down menu.
8. Optional: Enter other optional property values.

    Click **Add property** to add more 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.

Creating Documents and Other Objects

This section tells you how to create new objects in the vault. For information on differences between documents and other object types, see the definition of an object.

In this chapter

Object Metadata

Metadata helps you to find objects in M-Files. Metadata is the information related to an object. For example, the creation date, the class, and the name of an object are all metadata. The more you enter metadata for an object, the easier it is to find the object when you need it.

Editing the metadata

You can edit the object metadata on the metadata card:

Objective	Instructions
Edit property values	Click a property. Mandatory fields show an asterisk (*).
Add properties	Click **Add property** at the end of the property list.
Remove added properties	Click the remove icon (⊗) next to the property name.
Change the workflow state	See Changing the Workflow State on the Metadata Card.
Change permissions of the selected items	See Editing object permissions.

Click **Save** to save the changes and create a new version of the object.

Tip: You can use keyboard shortcuts when you edit object metadata. For more information, see Shortcuts for the metadata card.

Metadata suggestions

When Intelligent Metadata Layer and intelligence services are set up, M-Files shows metadata suggestions for a new document.

Click a suggestion to add it as a value for the property above the suggestion. If there is a plus sign (+) on the left of the suggested value, the value is added as a new object or value list item. Some property types let you add more than one of the suggested values.

Using the metadata card toolbar

Click a property to activate the metadata card toolbar. The toolbar is available for properties that use a value list. The toolbar can include these options:

Icon	Action
+	Adds a field to a multi-select property.
−	Remove a field from a multi-select property.
↻	Refresh the values of the property.
⊞	Open a dialog to create a new property value.
✎	Open a dialog to edit the selected property value.

Editing the properties of many objects

To select many objects in the listing area, do one of these operations:

Objective	Instructions
Select a list of objects	Click the first object, hold down the ⇧ Shift key, and click the last object.

Objective	Instructions
Select many individual objects	Click the first object, hold down the Ctrl key, and select the other objects.
Select all objects	Use the shortcut Ctrl + A.

Tip: When you edit the permissions of many objects, we recommend for performance reasons that you do not make other metadata changes at the same time.

The metadata card shows all the properties of the selected objects. See this table for descriptions of the special property values used when you have selected objects that have a different value for the same property:

Value	Description
(varies)	The values of the selected objects are different.
□ ○	None of the selected objects have the value selected.
◪ ◐	Some of the selected objects have the value selected.
☑ ●	All the selected objects have the value selected.

When you edit a value, you change the value for all the selected objects. For example, if you replace `(varies)` with a new value, it is set for all the selected objects.

Creating Documents

You can create documents normally and save them directly to the M-Files drive. You can also create other types of objects, such as customers or assignments. See Creating Non-Document Objects and Creating and Completing Assignments for more information.

To start the creation of a document click **Create** (⊕) and select **Document**. The new document dialog helps you to select the correct template and class for the document. You can also use search to find a template, or select a class to show only the templates available for that class.

Select **All** to show all available templates and file formats. **Recently Used** shows all the templates you have recently accessed. **Blank** shows all file formats available for a document.

Click **Next** to open the metadata card for the new document. Properties marked with an asterisk (*) are mandatory.

Tip: You can use keyboard shortcuts when you edit object metadata. For more information, see Shortcuts for the metadata card.

Tip: Use permissions to specify who can view, open, or edit the document.

When you are ready with the metadata, select whether you want the document to be opened for editing (**Open for editing**) or available to others immediately (**Check in immediately**). Finally, click **Create** to save your changes.

When you create a document in another application, you enter the metadata when you save the document to the vault on the M-Files drive.

Converting a temporary local file to a document

The **Convert to Document** operation is available for files that are imported to M-Files with an unusual procedure, for example with command prompt. M-Files shows these temporary local files with a gray icon. To convert a temporary local file to an M-Files document, right-click the file and click **Convert to Document**.

In this chapter

Example: Creating a Document

1. Open M-Files Desktop and go to a vault.
2. Click **Create** (⊕).
3. Click **Document**.
4. Select a template:

   a. Enter a search term to the search field and select a template.

      or

   b. From the **Select class** drop-down menu, select a class and select a template.

      or

   c. Select a template from the **Recently Used**, **All**, or **Blank** quick lists.
5. Click **Next**.
6. In the **Name or title** field, enter a name.
7. Enter the object metadata. Mandatory fields are shown with an asterisk (*).

   To add more metadata fields, click **Add property** below the last metadata property on the list.
8. Optional: Click the permission options at the bottom of the dialog to set permissions for your document.

For more information, see Object Permissions.

9. Optional: Click the workflow options to select a workflow and a workflow state for the document.

10. Select one of these options:

    a. Select **Open for editing** to change the content before you check in the document.

    or

    b. Select **Check in immediately** to add the content to the vault after you click **Create**.

11. Click **Create**.

Using Document Templates

You can use templates when you create documents in M-Files. Templates can be specified to add a predefined set of metadata and content to the document. For example, a proposal template or an order template.

To set a document or other object to be a template, add the property **Is template** to the metadata and set the value to **Yes**. Templates are class-specific, but you can specify the template to be used for other classes with the **Additional classes** property.

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, that is, 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*).

For more information, see New Class, as well as Automatic Values for information on using document templates with automatic values.

Single-File and Multi-File Documents

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

A single-file document contains only one file. For example, a PDF or a Word document.

A multi-file document (🗐) usually contains many files. For example, you can include a proposal and its attachments, which are single-file documents, in the same multi-file document. You can double-click the multi-file document to see its content.

Converting a multi-file document to a single-file document

When a multi-file document contains only one file, you can convert it to a single-file document: Right-click a multi-file document and click **Convert to Single-file Document**.

Converting a single-file document to a multi-file document

To convert a single-file document to a multi-file document, right-click a single-file document and click **Convert to Multi-file Document**.

In this chapter

Adding New Files to Multi-File Documents

The **Add File** function can be used for creating new document files for a multi-file document.

Note, 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. You can also drag and drop a file to a multi-file document.

Do the following steps to add a new file to a multi-file document:

1. Right-click the multi-file document of your choice.
2. Select **Add File** to show a list of file types.
3. Select a type for the new file.

   ✓ The document is checked out to you and a new file representing the type of your choice is added to the multi-file document.
4. Enter a name for the added file.

Creating Non-Document Objects

In addition to documents, you can create other objects like customers and projects. You can therefore 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.

When you start to create a new object, the first thing you see is the metadata card. After you have entered the values for the mandatory fields (marked with an asterisk), the object can be saved with **Create**.

The **Check in immediately** option is selected by default to make sure that the new object is saved to the repository immediately after you click **Create**. You can leave the object checked out to you to add metadata to it before you save the information to the vault.

Object types are specified with M-Files Admin. For more information, see Object Types.

Example: Creating a New Customer

1. Click **Create** > **Customer**.
2. In the **Customer name** field, enter the customer's name.
3. Optional: Enter other customer details in the available fields.
4. Click **Create**.

A new customer object is added to the vault.

Adding Content from Scanner

This section offers instructions on how to add new files to the vault or to replace existing vault content from a scanner.

In this chapter

- Adding Documents from the Scanner
- Adding Documents from the Scanner to a Multi-File Document
- Replacing a Document with a Document from the Scanner
- Scanning and Text Recognition (OCR)

Adding Documents from the Scanner

1. In M-Files, click **Create** and select **Add Document from Scanner** .

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:

Option:	**Objective:**
Scanning done	You do not want to scan additional documents.
Scan more pages to the current document	You want to scan another document and combine it with the previously scanned document.
Scan another document	You want to scan another document and do not want 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**.

   ℹ For more information on converting scanned documents to searchable PDFs, see Scanning and Text Recognition (OCR).

6. When the **New Document** dialog is shown, enter the metadata and click **Create**.

The scanned document or documents are added to M-Files.

Adding Documents from the Scanner to a Multi-File Document

Complete the steps given here to add documents from a scanner to a multi-file document. For instructions on converting single-file documents to multi-file documents, see Single-File and Multi-File Documents.

1. In M-Files, locate the multi-file document for which to add a file from the scanner.

2. Right-click the multi-file document and select **Add File** > **Add 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:

Option:	Objective:
Scanning done	You do not want to scan additional documents.
Scan more pages to the current document	You want to scan another document and combine it with the previously scanned document.
Scan another document	You want to scan another document and do not want 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**.

   For more information on converting scanned documents to searchable PDFs, see Scanning and Text Recognition (OCR).

The scanned document or documents are added to the multi-file document.

Note: The multi-file document only has one set of metadata. The files in the document do not have separate metadata.

Replacing a Document with a Document from the Scanner

1. In M-Files, locate and select the document that you want to replace with a document from the scanner.

   Single-file documents and documents in a multi-file document can be replaced with a document from the scanner.

2. Press Alt to show the menu bar and select **Operations** > **Scanning and Text Recognition (OCR)** > **Replace with File from Scanner**.

   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:

Option:	Objective:
Scanning done	You do not want to scan additional documents.
Scan more pages to the current document	You want to scan another document and combine it with the previously scanned document.
Scan another document	You want to scan another document and do not want 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**.

   For more information on converting scanned documents to searchable PDFs, see Scanning and Text Recognition (OCR).

The existing document in M-Files is replaced with the document from the scanner.
Scanning and Text Recognition (OCR)

You can add paper documents to M-Files with a scanner. To use the scanning features, in the classic M-Files Desktop, press Alt and select **Operations** > **Scanning and Text Recoginition (OCR)**. When a document scan is complete, M-Files suggests the scanned file to be converted to a searchable PDF with optical character recognition (OCR).

M-Files automatically suggests the character recognition if you drag and drop an image to M-Files. You can also convert non-searchable PDFs and images to searchable PDFs manually with the context menu of the file.

You can use optical character recognition with these file formats:

- TIF
- TIFF
- JPG
- JPEG
- BMP
- PNG
- PDF

TIFF files that use an alpha channel or JPEG compression are not supported.

Important information for admins

Note: When you use the OCR feature in M-Files on a signed PDF, the entire document is rewritten. Because digital signatures validate the content, any edits made by OCR will invalidate the existing signature. This can result in the signature's removal.

- The OCR features in M-Files do not support mass operations. They are meant for conversions of a small number of files at a time.
- For information about network scanning, see Scanner Sources.
- The scanner integration uses TWAIN and WIA technologies. Only scanners with a TWAIN or WIA driver are supported.
- System administrators can change settings for scanning and optical character recognition in Advanced Vault Settings. The settings are in the section **Configuration** > **Scanning & OCR**.
- If text recognition is done to an image that is not saved to M-Files, the file is saved as a PDF. Otherwise, you can find the original image file in the version history of the object.

Importing Image Files as Searchable PDFs

To import a picture file to the vault as a searchable PDF:

1. Drag and drop an image file to the classic M-Files Desktop.
2. Optional: In the **Conversion to Searchable PDF** dialog, check the **Use automatic language detection** checkbox to set M-Files to automatically detect the document language.
3. Optional: In the **Conversion to Searchable PDF** dialog, click **Advanced** to improve the quality of the text recognition by selecting primary and secondary language options to match the language used in the image.

   Opening the advanced options disables the option to use automatic language detection.

4. Click **Convert** to start the conversion.
5. Once the conversion is complete, the **New Document** dialog appears. Finish importing the image by filling in the metadata and clicking **Create**.

The image file is imported to to the vault as a searchable PDF, allowing you to locate it by using the M-Files search functions.

Converting an Image File Stored in M-Files to a Searchable PDF

1. In M-Files, locate 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.
3. Optional: In the **Conversion to Searchable PDF** dialog, check the **Use automatic language detection** checkbox to set M-Files to automatically detect the document language.
4. Optional: In the **Conversion to Searchable PDF** dialog, click **Advanced** to improve the quality of the text recognition by selecting primary and secondary language options to match the language used in the image.

   ⓘ Opening the advanced options disables the option to use automatic language detection.
5. Click **Convert** to start the conversion.

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.

Replacing the Content of a Document File

You can use the **Replace with File** command to select another document or file whose content (data in the file) is to replace the content of the selected document.

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 command affects the contents of the file only. You can view the version history by opening the **History** dialog (see Version History).

To replace the content of a document with that of another one:

1. Right-click the document file the content of which you want to replace.
2. Press the Alt key and select **Operations** > **Replace with File**.
3. Locate and select the file that you want to use for replacing the original file content.
4. Click **OK**.

The content of the original file is replaced with the content of the file that you selected. Document metadata is unaffected.

Object Permissions

To open the **Permissions** dialog of an M-Files object, click the permissions area at the bottom of the metadata card.

You can quickly select the document permissions with named access control lists.

Editing object permissions

To edit the object permissions, click the **Permissions** area on the metadata card. The object has automatic permissions if the **Selected permission settings** section of the **Permissions** dialog shows a list with columns **Source**, **Description**, and **Active**. To edit these permissions, see Permissions from many sources.

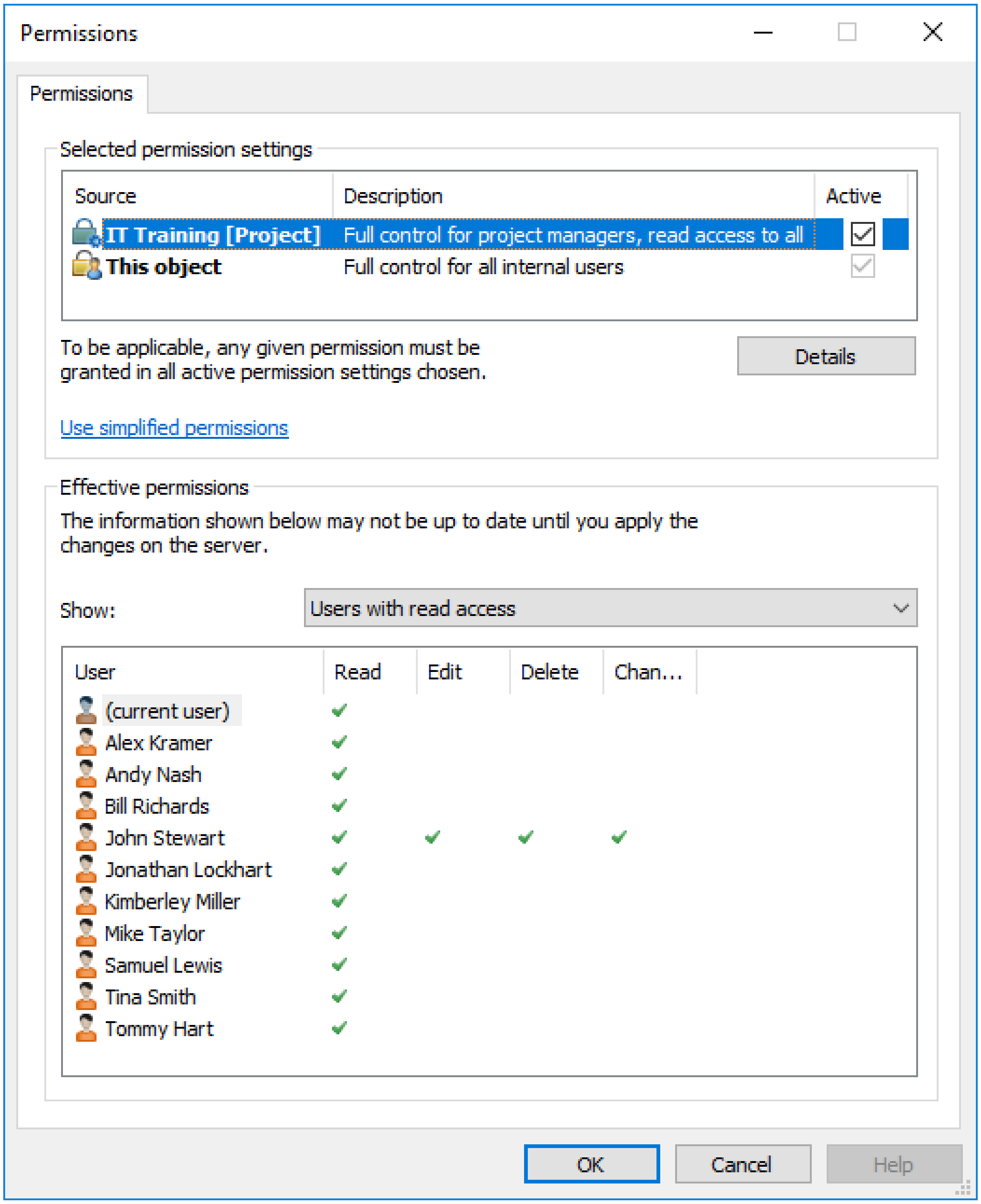
If the object does not have automatic permissions, you can select **Full control for all internal users**, **Only for me**, or the drop-down menu to use a named access control list.

To specify other permissions, click **Edit**. In the dialog that opens, unselect **Use named access control list**. Click **Add** to show all users, user groups, and pseudo-users registered in M-Files, and edit the permissions for them. Click **Remove** to remove users, user groups, and pseudo-users from the access control list. To specify what the users can do with the object, see Allowing and denying permissions.

Tip: When you edit the permissions of many objects, we recommend for performance reasons that you do not make other metadata changes at the same time.

Permissions from many sources

If the effective permissions of the object come from many sources, meaning that – in addition to its own permissions settings – its access rights are affected by automatic permissions, the **Permissions** dialog displays the sources in the **Selected permission settings** section.



Selected permission settings

Source	Description	Active
IT Training [Project]	Full control for project managers, read access to all	☑
This object	Full control for all internal users	☑

To be applicable, any given permission must be granted in all active permission settings chosen.

Use simplified permissions

Effective permissions

The information shown below may not be up to date until you apply the changes on the server.

Show: Users with read access

User	Read	Edit	Delete	Chan...
(current user)	✓			
Alex Kramer	✓			
Andy Nash	✓			
Bill Richards	✓			
John Stewart	✓	✓	✓	✓
Jonathan Lockhart	✓			
Kimberley Miller	✓			
Mike Taylor	✓			
Samuel Lewis	✓			
Tina Smith	✓			
Tommy Hart	✓			

Figure 2: Effective permissions from many sources.

In the **Permissions** dialog, you can select 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.

The **Selected permission settings** section contains the columns explained below.

Source

The **Source** column indicates the source from which the object has received a given permission. In the example image further above, the object has automatic permissions granted through the project *IT Training*, 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. If you have created an automatic permission rule based on a value, a value list, or an object type and named it, the name is displayed in this column.

Active

If you can bypass the automatic permissions when you specify automatic permissions for the relevant value, value list, or object type, you can deselect the permission in question to deactivate the automatic permissions given through the value. This causes the permission setting to no longer be active and influence the final permissions of the object.

Allowing and denying permissions

To specify what the users are allowed to do with the object, go to the **Permissions** dialog and click **Edit**. The available options 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 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*.

In this chapter

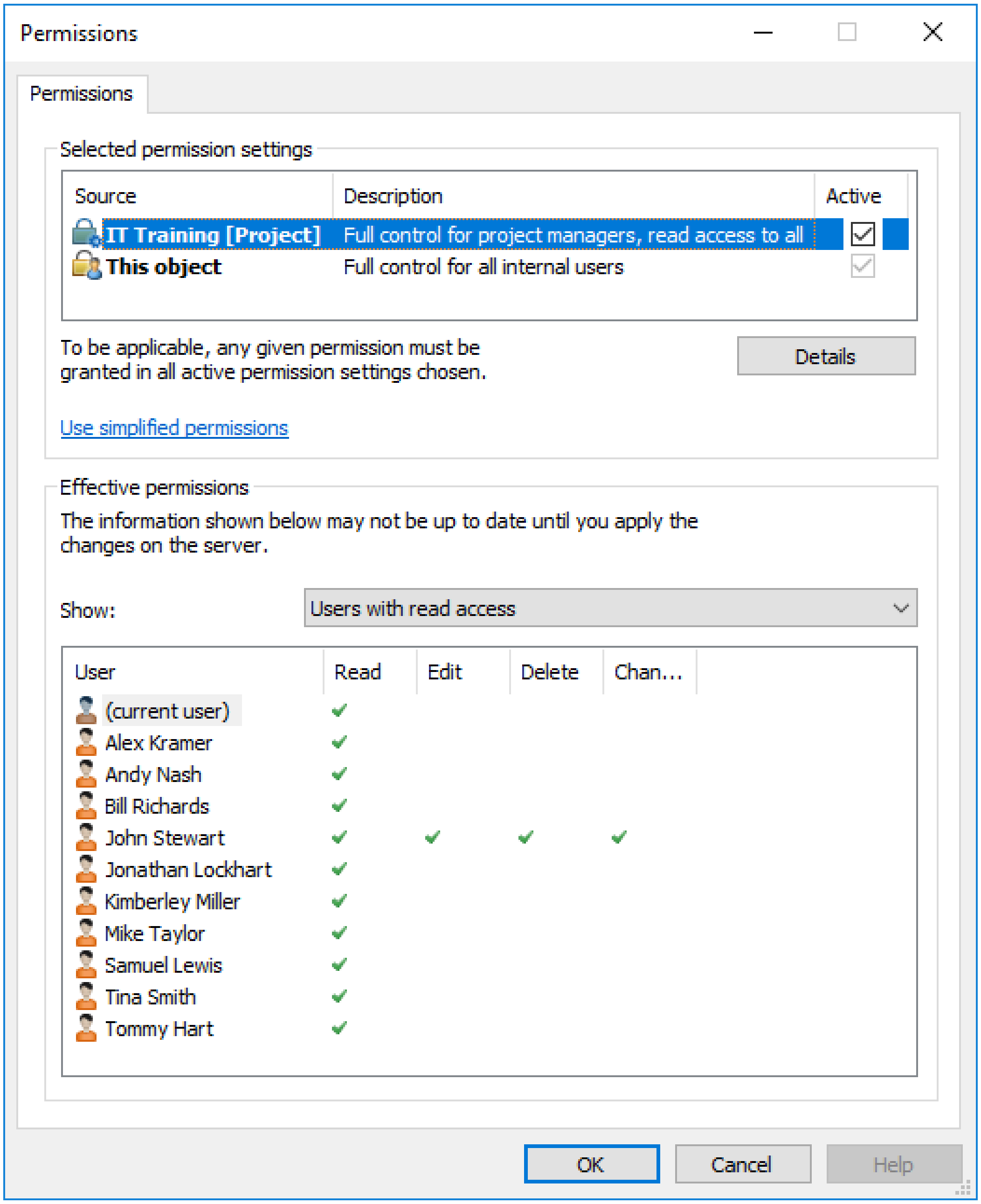
- Effective Permissions
- Pseudo-users

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:
Automatic permissions for objects through any project

The access that was specified for the object itself can cover full control of the document for all users while the automatic permissions through a project can 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.



Selected permission settings

Source	Description	Active
IT Training [Project]	Full control for project managers, read access to all	☑
This object	Full control for all internal users	☑

To be applicable, any given permission must be granted in all active permission settings chosen.

Effective permissions

The information shown below may not be up to date until you apply the changes on the server.

Show: Users with read access

User	Read	Edit	Delete	Chan...
(current user)	✓			
Alex Kramer	✓			
Andy Nash	✓			
Bill Richards	✓			
John Stewart	✓	✓	✓	✓
Jonathan Lockhart	✓			
Kimberley Miller	✓			
Mike Taylor	✓			
Samuel Lewis	✓			
Tina Smith	✓			
Tommy Hart	✓			

Figure 3: Automatic permissions through a project can restrict the object permissions.

Tip: You can see the effective permissions by user and access right in the table in the **Permissions** dialog.

Example:
Internal restrictions to permissions

- The permission settings of the object allow full control for all users.

- Through its class, the object has been granted permissions that give full control to management and read-only access to all other users.
- Through 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 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 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 through 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 through 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 through them, ask your system administrator to change the 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 through metadata 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.

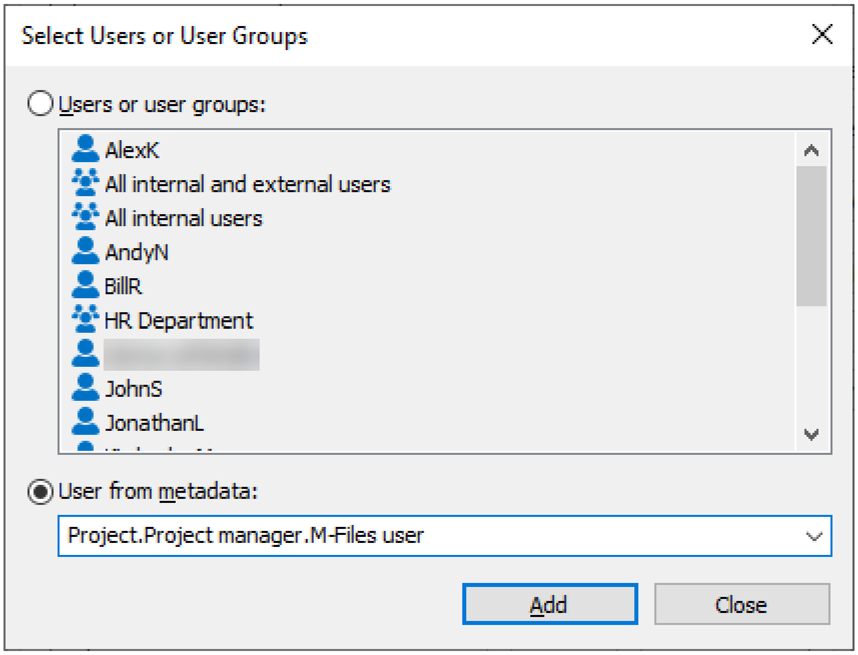
You can specify pseudo-users only through properties that are based on a **Users** or **User groups** value list.

For information on how this feature is supported in different M-Files clients, refer to M-Files Client Feature Comparison.

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. If 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 as a background task (see this note), so updating their project manager information separately is not necessary.

You can also do multi-level user definitions through metadata. For example, you can specify the project manager in 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.



● User from metadata: Project.Project manager.M-Files user

Figure 4: 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.

> **Note:** Object permissions are updated as an asynchronous background task. Object permissions may be updated when, for example, a named access control list, a user, a user group, or the value of a pseudo-user (such as a project manager) is modified. You may monitor the progress of the task in M-Files Admin in the **Background Tasks** section. For more information, see Monitoring Background Tasks.

For more information on automatic permissions, see Automatic Permissions for Value List Items.

Creating and Completing Assignments

Assignments transfer information and responsibility for task execution to the correct person. Assignments 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 Assign to user.

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, and therefore only a user who has reading rights to the document can mark the assignment completed. The user does not need to have rights to edit the document, meaning that users with a read-only license to M-Files can also mark the assignment completed.

You can add contextual information to assignments with different methods:

- Create an assignment and add objects to it either with drag and drop or the **Add File** function from the context menu.
- Select one or more documents and select **Assignment** in the **Create** menu.
- Create an assignment without adding an object to it and define the entire task in the description field of the assignment.

Metadata related to assignments

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 Creating a View.

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.

> **Note:** If a user creates the assignment, only this user and users with the **Full control of vault** rights can edit the **Assigned to** property value. If the assignment is created through a workflow, only users with full control of the vault can edit the property value.

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 **Create** > **Assignment**.

3. In **Name or title**, enter a descriptive title for the assignment.
4. In **Assignment description**, enter a detailed description of the assignment to ensure that the assignee is properly informed about the details of the assignment.
5. In **Assigned to**, select the person to whom this assignment is assigned.
6. Optional: In **Deadline**, select a deadline by which the assignment must be completed.
7. Optional: With the workflow controls at the bottom of the **New Assignment** dialog, select a workflow for the assignment.
8. Click **Create**.

The new assignment is shown in the **Assigned to Me** view of the assignee and they are informed by email about the new assignment.

Creating a New Assignment for a New Document

1. In the classic M-Files Desktop, click the **Create** button and select **Assignment**.
2. In **Name or title**, enter a descriptive title for the assignment.
3. In **Assignment description**, enter a detailed description of the assignment to ensure that the assignee is properly informed about the details of the assignment.
4. In **Assigned to**, select the person to whom this assignment is assigned.
5. Optional: In **Deadline**, select a deadline by which the assignment must be completed.
6. Optional: With the workflow controls at the bottom of the **New Assignment** dialog, select a workflow for the assignment.
7. Click **Create**.
8. When the new assignment has been created, right-click the assignment in the listing area and select **Add File**.
9. Select a format for the new file.
10. Rename the new file.
11. Optional: Double-click the newly added file to edit it.

The new assignment is shown in the **Assigned to Me** view of the assignee and they are informed by email about the new assignment.

Completing an Assignment

To mark complete an assignment:

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

   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 with one of these methods:

   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**.

   ✓ The **Mark Complete** dialog is opened.

4. Optional: Write a comment to the **Comment** field.
5. Click **OK** to close the **Mark Complete** dialog.
6. 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

To complete an approval assignment:

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

   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:

   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**.

   or

   d. Approve or reject the assignment with the notification email.

   Note: To complete approval assignments with email links, your M-Files system administrator must add the **New Approval Assignment Message** template section to **Notifications** > **Notification Templates** > **Email Templates** in Advanced Vault Settings.

   ✓ The **Mark Complete** dialog is opened.

4. Optional: Write a comment to the **Comment** field.
5. Click **OK** to close the **Mark Complete** dialog.
6. 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.

Making Copies of Existing Objects

To create a copy of an existing object, right-click an object and select **Make Copy**. This command creates a new object with the metadata and contents of the source object. The version history is not copied to the new object.

Making PDFs of Objects

You can make PDFs of the files in M-Files.

Here are some solutions for issues that occur often when making PDFs:

- If you cannot convert documents to the PDF format, see Why can't I convert a document to PDF format or annotate a document?
- If there are problems with non-English content, your M-Files administrator can try to enable the Advanced Vault Settings option **PDF Conversion** > **Word Files** > **Extended Language Support**.

Saving as PDF

To save a file as a PDF:

1. Right-click an object in the listing area and select **Save as PDF** > **Save as PDF**.

   ✓ When the PDF is created, the **Save As** dialog opens.

2. In the **Save As** dialog, select the location for the PDF file.

   ⓘ If you save a single-file document, the dialog shows the vault as the default save location. If you save a file in a multi-file document, the dialog shows the multi-file document as the default save location.

3. Click **Save**.
4. Optional: If you save the PDF as a single-file document, the object's metadata card opens. Fill in the necessary metadata and click **Create**.

The PDF version of the file is saved to the vault.

Converting to PDF

To convert a file into PDF format, right-click an object in the listing area, click **Save as PDF**,and select one of these options:

Option	Description
Convert to PDF (replaces original file)	M-Files converts the selected file to PDF format and replaces the original file (for example, a Word file) with the PDF file.
Convert to PDF (adds separate file)	M-Files converts the selected file to PDF format and keeps the original version of it. If you convert a single-file document, M-Files converts it to a multi-file document and adds the PDF file to it.

Functions in Microsoft Outlook

M-Files has two add-ins for the classic Microsoft Outlook and one for the new Microsoft Outlook:

- M-Files Outlook Standard for the classic Microsoft Outlook
- M-Files for Outlook for the classic Microsoft Outlook
- M-Files for Outlook Pro for the new Microsoft Outlook

This section and the subsections tell you about the M-Files Outlook Standard add-in which is for the classic Microsoft Outlook. This add-in is included to all M-Files subscriptions.

To use the other two add-ins, M-Files for Outlook and M-Files for Outlook Pro, you must have a separate license. For more information, refer to Configuring M-Files for Outlook, Using M-Files for Outlook, and Setting Up M-Files for Outlook Pro in M-Files Support Portal.

Features of the standard integration with Microsoft Outlook

- You can save email messages and attachments to M-Files in many file formats.
- You can send an email message and, at the same time, save it to an M-Files vault.
- You can create Outlook rules and use M-Files features to save email messages automatically.
- The email messages that have been saved to M-Files show an M-Files flag.
- Email messages related to a specific subject have a relationship in M-Files. With the relationships, you can easily find and read the entire email conversation in M-Files.
- You can open a stored email message in M-Files directly from the classic Microsoft Outlook.
- M-Files can automatically associate contact persons and customers with email messages.
- The document date in M-Files is automatically the same as the email date in the classic Microsoft Outlook.

Optional settings

To disable the **Send and Save to M-Files** button in the classic Microsoft Outlook, configure this registry setting on the client computer:

Key	**HKEY_CURRENT_USER\SOFTWARE\Motive\M-Files\<version>\Client\Common\<vault name>\MSOutlookRibbon**	
Value name	`ShowSendAndSaveInMFilesTab`	
Value type	`REG_DWORD`	
Description	When enabled, the **Send and Save to M-Files** button is visible in the M-Files ribbon.	
Default value	`1`	Enabled
Value	`0`	Disabled
	`1`	Enabled

To add the **Send and Save to M-Files** button to the default composer window in the classic Microsoft Outlook, configure this registry setting on the client computer:

Key	**HKEY_CURRENT_USER\SOFTWARE\Motive\M-Files\<version>\Client\Common\<vault name>\MSOutlookRibbon**
Value name	`ShowSendAndSaveInBuiltInTab`

Key	`HKEY_CURRENT_USER\SOFTWARE\Motive\M-Files\<version>\Client\Common\<vault name>\MSOutlookRibbon`	
Value type	`REG_DWORD`	
Description	When enabled, the **Send and Save to M-Files** button is visible in the default composer window of the classic Microsoft Outlook.	
Default value	`0`	Disabled
Value	`0`	Disabled
	`1`	Enabled

The M-Files system administrator can also apply these settings to multiple client computers. For more information, see Configuration Options for the "Send and Save to M-Files" Button.

In this chapter

- Saving Email Messages in the classic Microsoft Outlook to M-Files
- Storage Formats
- Creating a Microsoft Outlook Rule for M-Files
- Saving messages in M-Files Folders
- Associating Messages with Contacts
- The M-Files Flag

Saving Email Messages in the classic Microsoft Outlook to M-Files

1. In the classic Microsoft Outlook, do one of these steps:

   a. Locate the email message that you want to save to M-Files, right-click the message and select **Save to M-Files**, and then select the vault where you want to save the selected email message.

      or

   b. Locate the email message that you want to save to M-Files, and then drag and drop the message to the preferred M-Files folder in the navigation pane of the classic Microsoft Outlook.

      or

   c. First compose a new email message, then, in the **Message** window, open the **M-Files** tab and click **Send and Save to M-Files**, and finally select the appropriate vault from the drop-down menu.

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

2. From the **Save as type** drop-down menu, select the format in which the email message is saved.

   ℹ For more information about email message storage formats, see Storage Formats.

3. Fill in the metadata for the email message and click **Create**.

   ℹ Note that some properties may be automatically populated. For more information, see Automatically Populated Metadata.

The selected email message is added to the selected vault in M-Files. An M-Files flag is also added to the message in the classic Microsoft Outlook as an indication that the message has been saved to M-Files.

Storage Formats

Email messages and attachments can be saved from the classic Microsoft Outlook directly to M-Files. The M-Files capabilities described in this section are available in the classic Microsoft Outlook versions 2016 and 2019, and in versions of Microsoft 365 Apps for enterprise that Microsoft supports.

The classic Microsoft Outlook has these options for the **Save to M-Files** feature:

Microsoft Outlook message (*.msg)

The email message and any attachments are stored in M-Files in MSG format. The stored file and its attachments open as a message in the classic Microsoft Outlook.

Microsoft Outlook message; separate attachments (*.msg; *.*)

The email 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 the classic Microsoft Outlook. The attachments open in the applications associated with the file format.

Text only; no attachments (*.txt)

The email message is stored as a text file. The stored file opens in, for example, Notepad. Attachments are not saved.

Text only; separate attachments (*.txt; *.*)

The email 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 email 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 email 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 email attachments. The attachments are stored in their native file formats. If an email 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: To store multiple attachments as separate documents rather than as a single multi-file document, contact your M-Files consultant for additional information.

Creating a Microsoft Outlook Rule for M-Files

With Microsoft Outlook rules, you can automate saving specific kinds of email messages to M-Files on the basis of, for example, the sender, subject, or recipient of a message. For example, you can specify that all proposal messages that you send are saved to M-Files on the basis that the subject field contains the word `proposal`.

Note: These instructions are for Microsoft Outlook 365. If you use a different version of Microsoft Outlook, there can be minor differences in how rules are created.

To create a Microsoft Outlook rule for M-Files:

1. Open the classic Microsoft Outlook and select an email 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**.

   The **Create Rule** dialog is opened.

3. Click **Advanced Options**.

   The **Rules Wizard** dialog is opened.

4. Check the condition or conditions that an email message must meet for this rule to be applied.

   To create a rule that applies to messages that are sent by the selected sender, check the **from <sender>** check box.

5. Optional: 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** check box.

   You can also move the messages themselves directly to M-Files so that they are deleted from Microsoft Outlook when they are moved. The best practice normally is to move a copy of the message to M-Files. With this method, 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: 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.

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** check boxes and click **Finish**.

The email messages in Microsoft Outlook that match the rule that you 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 with the 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 the classic Microsoft Outlook.
- M-Files folders are automatically available to you in the classic Microsoft 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 the classic Microsoft Outlook: messages are not removed from their original Microsoft Outlook folder when you move them to the M-Files folder.
- You can specify automatically populated metadata for each M-Files folder.

The functions described in this section are available in the classic Microsoft Outlook versions 2016 and 2019, and in versions of Microsoft 365 Apps for enterprise that Microsoft supports.

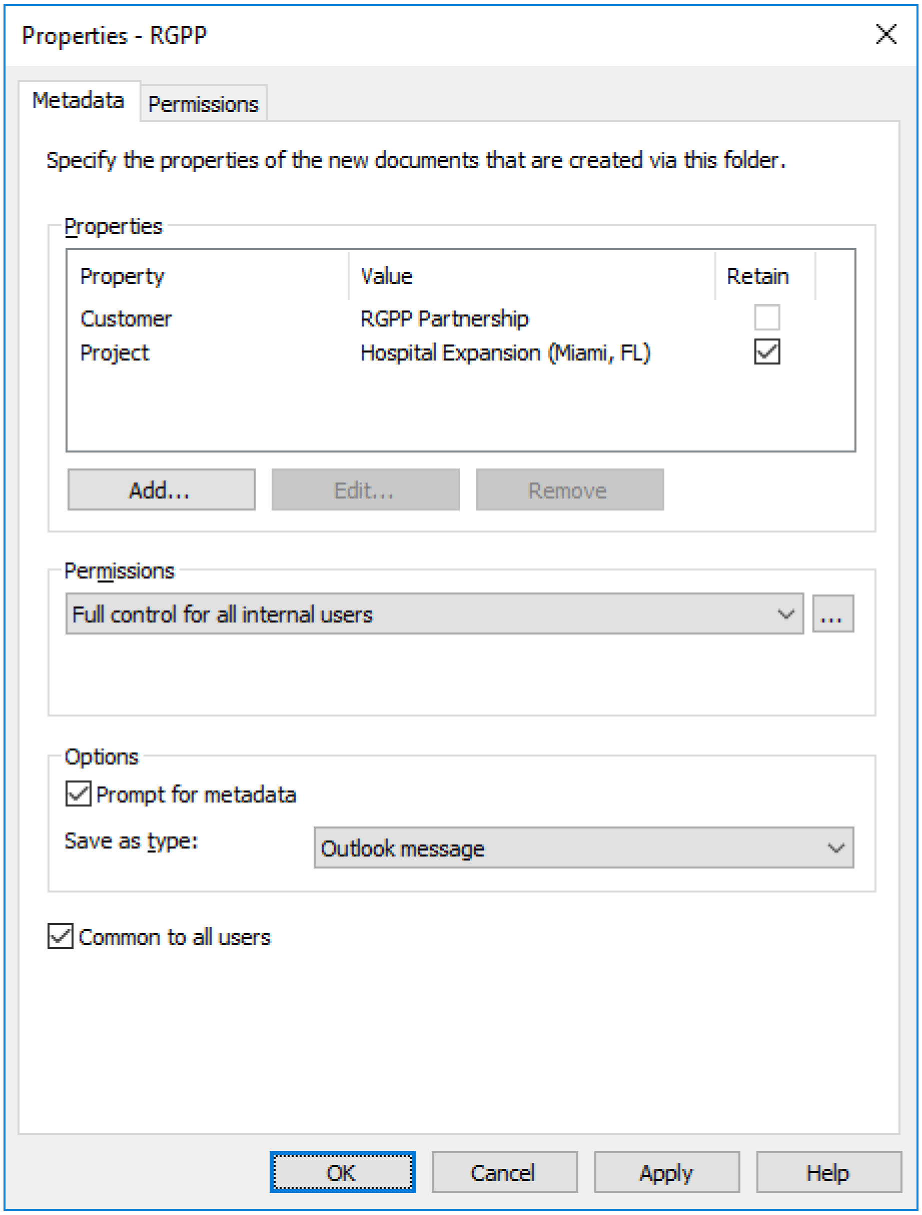
In this chapter

Automatically Populated Metadata

You can specify automatically populated properties to be added to email messages when you save them to M-Files by dragging them to M-Files folders in the classic Microsoft Outlook. The settings are folder-specific, and thus let you use many subfolders for different use cases. The function is available in the classic Microsoft Outlook versions 2016 and 2019, and in versions of Microsoft 365 Apps for enterprise that Microsoft supports.

Note: These folders must 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 Microsoft Outlook folder, for which you cannot specify M-Files properties.

You can find the **Specify M-Files Properties** function in the classic Microsoft Outlook by right-clicking an M-Files folder.



Specify the properties of the new documents that are created via this folder.

Properties

Property	Value	Retain
Customer	RGPP Partnership	□
Project	Hospital Expansion (Miami, FL)	☑

Permissions: Full control for all internal users

Options

☑ Prompt for metadata

Save as type: Outlook message

☑ Common to all users

Figure 5: 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 *Hospital Expansion (Miami, FL)*. This way, the messages dragged into that folder are automatically associated with the *Hospital Expansion (Miami, FL)*. 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 can also specify M-Files folder properties to be read from the email 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 emails 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. This means that the folder is shown in the classic Microsoft Outlook to all users. You can set up a common M-Files subfolder if you have 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 the classic Microsoft 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 email header field to read information from by using the **Field** drop-down menu if you want to populate the property value with information read from the imported email 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. With the **Permissions** drop-down menu, specify the permissions for documents created through this folder.
7. Optional: Select the **Prompt for metadata** if you want to display the metadata card and prompt for additional metadata when an email message is dragged and dropped to this folder.
8. Using the **Save as type** drop-down menu, select the email 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 email 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

In M-Files Admin, you can set M-Files to automatically associate the sender and recipient information of email messages with contact persons and customers saved in the vault. For example, M-Files can automatically associate a message from `matt.bay@estt.com` with the contact person Matt Bay and the customer ESTT Corporation. For instructions on how to specify the properties in M-Files Admin, see Email Client Integration Settings.

Note: This feature is available in the classic Microsoft Outlook versions 2016 and 2019, and in versions of Microsoft 365 Apps for enterprise that Microsoft supports.

The automation is activated when you save an email to a vault-specific M-Files folder in the classic Microsoft Outlook. This also applies to all subfolders of that M-Files folder.

The M-Files Flag

The M-Files flag shown in the classic Microsoft Outlook message listing tells that you have already saved the message to M-Files.

If another user (for example, another recipient) has saved the same message to M-Files, M-Files confirms whether to save that message again. Even if you do not save the message again, the M-Files flag will now be shown in the classic Microsoft Outlook for that message.

With the **Update M-Files Status** function in the context menu of the message, you can easily show all M-Files flags. Also messages saved in M-Files by other users will then have an M-Files flag.

2.3.2. Removing and Archiving Content

This section deals with ways you can remove objects from your vault, as well as with archiving vault content.

In this chapter

- Deleting, Undeleting, and Destroying Objects
- Archiving Content

Deleting, Undeleting, and Destroying Objects

Deleting objects

To delete an object, right-click it and select **Delete**. The object is not destroyed permanently, but it will become deleted.

Note: You can see the deleted objects in the vault only if you have at least one of these permissions:

- **System administrator** permissions
- **Vault administrator** permissions
- The permission **See and read all vault content (including deleted objects)**
- The permission **See and undelete deleted objects**

To show deleted objects, you can create a view for them or use a filtered search.

Undeleting objects

To restore a deleted object, right-click it and select **Undelete**. To find deleted objects, see Deleting objects.

Destroying objects

To permanently remove an object, right-click a deleted object and select **Destroy**. You can also select **Destroy permanently** in the confirmation dialog when you delete an object. To find the deleted objects, see Deleting objects.

Archiving Content

Vault content that is no longer in active use can be archived to a separate archive file. The file can later be used to restore the archived content back to the vault.

Note: Only vault admins can use the archiving commands, and they are only supported in the classic M-Files Desktop.

Marking content for archiving

To set objects to be archived:

1. In the classic M-Files Desktop, select the objects on the listing area.
2. Click one of the selected objects with the secondary mouse button.
3. Select **Archiving** > **Mark for Archiving**.

Clearing the archiving status

To remove the archiving marker:

1. In the classic M-Files Desktop, select the objects on the listing area.
2. Click one of the selected objects with the secondary mouse button.
3. Select **Archiving** > **Clear Archiving Marker**.

Archiving and restoring content in M-Files Admin

The archiving operation done with M-Files Admin moves the marked objects from the vault to a separate archive file. See Archiving Old Versions.

You can restore the archived content to the vault with Content Replication and Archiving.

2.3.3. Editing Content

This section tells you how documents are edited in M-Files. Documents are first checked out for editing or co-authoring. After edits are done, documents are checked back in to the vault. The section also tells you how to enable and use the Annotations and Redlining feature, how to use object comments, workflows, and version history, and how to compare document content.

Editing Office documents with M-Files Mobile

For information about editing Office 365 documents with M-Files Mobile, refer to Editing Office Documents in M-Files Mobile with O365 Integration in M-Files Support Portal.

In this chapter

Checking Out a Document

Checking out a document is an M-Files function that prevents concurrent editing. A checked out document can still be viewed and opened in read-only mode by other users.

When you check out a document, a small check mark (✓) is shown on the document icon. A red icon (⛔) means that the document has been checked out to someone else.

Note: When you check out a document in M-Files Desktop, M-Files Web shows that the same document is checked out to someone else. The same applies the other way around. This happens because the two clients use a different client cache. You can, however, use the **Undo Checkout** command.

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.

Sending a check-in request

You can also send a check-in request to the user who has checked out a document: Right-click the document and select **Send Check-in Request**. The user gets an email message about the request. The message also contains a link to the document. The check-in request is sent to the email address associated with the user's login account.

Undoing Document Checkout

With the **Undo Checkout** function, you can undo checking out a document without saving the changes on the server. In this case, you 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.

Checking Out a Document for Web Co-Authoring

With M-Files, many users can edit a document at the same time. You can check out a document for co-authoring with Microsoft Office for the web when the Microsoft Office for the web tools and web co-authoring have been enabled for your vault or vaults.

Note: Office for the web has limits for the maximum size of the files. For more information, refer to Microsoft documentation.

Editing an Office Document in the Co-Authoring Mode

You must have an Office 365 account and editing permissions to the document that you want to edit in co-authoring mode.

To check out a document for co-authoring:

1. Locate the object that you want to make available for co-authoring in M-Files Desktop or M-Files Web.
2. Right-click the document and select **Check Out for Co-authoring** in the context menu.

Note: Co-authoring is only available for single-file DOCX, XLSX, XLSM, and PPTX documents.

✓ In the classic M-Files Desktop, a security warning is opened about who can view and modify the file during co-authoring. If you do not use the classic M-Files Desktop, skip to step 4.

3. In the **Security Warning** dialog in the classic M-Files Desktop, click **Begin Co-authoring**.

   ✓ The document is opened in Microsoft Office for the web.

   Tip: If you use Google Chrome and the browser cannot load the editor, check if the address bar contains an icon informing the user about a blocked redirection. If it does, click it and allow the redirection to be completed. Finally, close the browser window or tab and double-click the document in M-Files to reopen the editor.

4. Edit the document in the browser.

   Microsoft Office automatically saves your document when you make changes to it.

5. When you are done, close the editor tab.
6. To end co-authoring, right-click the object in M-Files Desktop or M-Files Web and select **Check In**.

   The user who checks out the document for co-authoring must be the one who also checks it in. 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.

   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, unless you selected **Undo Checkout** instead of checking in the document.

Participating in Co-Authoring

When a document has been checked for co-authoring, you can participate in the authoring process:

1. Locate the co-authored document in M-Files Desktop or M-Files Web and double-click it to open it in the co-authoring mode.

   A co-authored document is marked with a yellow icon that contains a checkmark.

   ✓ A dialog about editing the document in the co-authoring or opening it in read-only mode is opened.

2. Select **Edit (Co-authoring)**.

   ✓ The document is opened in Microsoft Office for the web.

   Tip: If you use Google Chrome and the browser cannot load the editor, check if the address bar contains an icon informing the user about a blocked redirection. If it does, click it and allow the redirection to be completed. Finally, close the browser window or tab and double-click the document in M-Files to reopen the editor.

3. Edit the document in the browser.

   Microsoft Office automatically saves your document when you make changes to it.

4. When you are done, close the editor tab.

The changes you made to the document are saved to M-Files when the user who started the co-authoring has ended the co-authoring and checked in the document.

Checking Out a Document for Co-Authoring with Microsoft SharePoint

If you do not use Microsoft Office for the web, you can use the co-authoring functionality with Microsoft SharePoint. In co-authoring with Microsoft SharePoint, also a person without an M-Files account can participate in the co-authoring process. For instructions on how to set the co-authoring features to be used with Microsoft SharePoint, see the knowledge base article Customizing Co-Authoring and Sharing Features.

Editing an Office Document in the Co-Authoring Mode with Microsoft SharePoint

You must 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.

      Note: By default, co-authoring is available for DOCX, XLSX, and PPTX files only.

   ✓ A security warning is opened about who can view and modify the file during co-authoring.
3. Click **Begin Co-authoring** in the **Security Warning** dialog.
4. In the **Co-authoring** dialog, click **Send Link** to send the shared object link to co-authoring participants with 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.
5. Double-click the object in the listing area to begin co-authoring.

   ✓ The document is opened in Microsoft Office for the web.
6. 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.
7. 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.
8. Save your changes if you are using the desktop application.

Microsoft Office automatically saves your document when you make changes to it.

9. Close the document.

10. Right-click the object in M-Files, and select **End Co-authoring** from the context menu.

11. 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.

    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. If you want to share the document for co-authoring again, check out the file for co-authoring and send a new link to the file.

Participating in Co-Authoring with Microsoft SharePoint

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.

    Microsoft Office 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.

Checking In a Document

When you no longer edit a document, you can check it in to make it available for others. To do this, right-click the document and select **Check In**.

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

Checking in with comments

You can comment on changes you made when you check in a document. Right-click the object and select **Check In with Comments**. In the **Check In** dialog, you can enter a description of the changes you made. The comments are displayed in the Comments view of the object.

Note: Comments keep their permission settings. Only users defined in the permission settings, when the comment was added, can see these comments.

Annotations and Redlining

You can add comments and stamps, and draw arrows, boxes and other shapes to your documents. The feature supports most common file types, including Microsoft Word, Microsoft Excel, Microsoft PowerPoint and Visio documents, email files, RTF files, HTML and web archive files as well as OpenDocument files and PDF documents. When you select an annotated document, the task area shows the options to show or hide the annotations.

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

Note: The M-Files system administrator must first enable the annotations and redlining feature before documents can be annotated. For more information, see Annotations and redlining.

Enabling annotations in the user interface

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

1. Open your vault with the classic M-Files Desktop.
2. Press Alt.
3. Open the **View** menu.
4. Enable the **Show Annotations** option.

Annotation objects

Your annotations are saved as separate Annotation objects under the main document. M-Files automatically creates these objects every time you 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.

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 (vsdx, vsx, vtx, vdx, vssx, vstx, vsdm, vssm, vstm, vdw, vsd, vss, vst)

Troubleshooting

If you are running into issues with annotations or are unable to use them, see Why can't I convert a document to PDF format or annotate a document? for assistance.

In this chapter

Adding Annotations to Documents

Use these instructions to create an annotation object and add annotations to a document in the classic M-Files Desktop and the classic M-Files Web. For instructions on how to add annotations with M-Files Desktop and M-Files Web, refer to the user guide for M-Files Web and the new M-Files Desktop.

1. Select a document in the listing area.
2. Make sure that the **Preview** tab is selected in the right pane.
3. Do one of these steps:

   a. Right-click the document and select **Create** > **Annotation**.

      or

   b. Click **New Annotations** in the task area under the **Annotations** section.

      Note: This option is only available for documents that do not have annotations.

   ✓ An annotation object is added to the document's related objects in the listing area.

4. Use the annotation controls at the top of the preview to add annotations.

   ⓘ The annotation controls include different ways for you to highlight parts of the document and icons for saving and printing the annotated document.

5. In the task area, click **Save Annotations**.

   ✓ In the classic M-Files Desktop, the annotation object is checked in. In the classic M-Files Web, select **Check in** to make your changes visible to other users.

Editing Annotations

To edit an annotation object:

1. Select an annotated document or an annotation object in the listing area.
2. Make sure that the **Preview** tab is selected in the right pane.
3. Click **Edit Annotations** in the task area under the **Annotations** section.
4. Use the annotation controls at the top of the preview to add annotations.

   ⓘ The annotation controls include different ways for you to highlight parts of the document and icons for saving and printing the annotated document.

5. In the task area, click **Save Annotations**.

   ✓ In the classic M-Files Desktop, the annotation object is checked in. In the classic M-Files Web, select **Check in** to make your changes visible to other users.

Object Comments

You can add comments to objects with the **Comments** function. Click the comments icon (🗨) on the metadata card to see the comments of an object.

You can only add comments for objects for which you have edit permissions, and only when you are not using a read-only license. As an exception, you can add a comment for an object when you change its workflow state.

> **Note:** Comments keep their permission settings. Only users defined in the permission settings, when the comment was added, can see these comments.

Workflows

During the lifecycle of a document, different contributors can change, edit, and make different decisions on the document. It is important that each person that participates in the process knows their responsibilities and the working stages.

The M-Files workflows let you model document lifecycles to real world processes. The workflows are divided into states that represent the working stages of the document or other object.

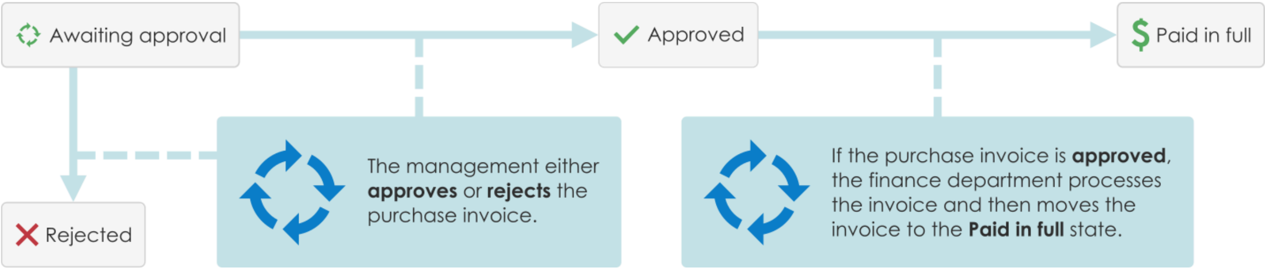

Awaiting approval
Approved
Paid in full
Rejected
The management either approves or rejects the purchase invoice.
If the purchase invoice is approved, the finance department processes the invoice and then moves the invoice to the Paid in full state.

Figure 6: Workflows make routine tasks of the organization easier. For example, purchase invoice process.

Workflows are created and changed in M-Files Admin by M-Files system administrators. To create and edit workflows, see Configuring Workflows.

To select a workflow and a workflow state for an object, use the workflow controls on the metadata card.

Changing the Workflow State on the Metadata Card

1. Select an object in the listing area.
2. Click the workflow state field at the bottom of the metadata card.
3. Select the workflow state.

   ✓ The **Change State** dialog is opened.

4. Optional: In **Comment**, add comments about the state transition to the object.
5. Select one of these options:

Option	Description
OK	The state transition is made and the possible comment is added.
Cancel	The state transition is made but no comment is added.

✓ The **Change State** dialog is closed.

6. Select **Save**.
7. Optional: If the **Electronic Signature** dialog is opened, complete one of these steps:

   a. If the **Username** and **Password** fields are shown, enter your user credentials and click **Sign**.

   or

   b. If the **Username** and **Password** fields are not shown, click **Sign** to enter your user credentials.

Changing the Workflow State with the Context Menu

1. In the listing area, right-click an object and click **Workflow** > **Change State**.

   ✓ The **Change State** dialog is opened.

2. In **State Transition**, select the workflow state.
3. Optional: In **Comment**, add comments about the state transition to the object.
4. Click **OK**.

   ✓ The **Change State** is closed and the state transition is made.

5. Optional: If the **Electronic Signature** dialog is opened, complete one of these steps:

   a. If the **Username** and **Password** fields are shown, enter your user credentials and click **Sign**.

   or

   b. If the **Username** and **Password** fields are not shown, click **Sign** to enter your user credentials.

Changing the Workflow State in the Task Area

1. In the listing area, select an object that has a workflow.
2. In the task area, click the new state in the **State transition** section.

   ✓ The **Change State** dialog is opened.

3. Optional: In **Comment**, add comments about the state transition to the object.
4. Click **OK**.

   ✓ The **Change State** is closed and the state transition is made.

5. Optional: If the **Electronic Signature** dialog is opened, complete one of these steps:

   a. If the **Username** and **Password** fields are shown, enter your user credentials and click **Sign**.

      or

   b. If the **Username** and **Password** fields are not shown, click **Sign** to enter your user credentials.

Conflict History

When automatic conflict resolution is enabled, M-Files automatically resolves conflicts that occur during data synchronization between vaults. Vault users can then use the **Conflict History** dialog to see and restore discarded object versions. For instructions on how to configure automatic conflict resolution, refer to Configuring Automatic Resolution of Replication Conflicts.

The configuration specifies if you are told when changes you made to an object are discarded in conflict resolution. The options are:

- You get a notification.
- A task is assigned to you.
- There is no indication of discarded changes.

Showing and Restoring Discarded Object Versions

To show the discarded object versions:

1. In the classic M-Files Desktop, right-click an object and select **Conflict History**.

   ✓ The **Conflict History** dialog is opened.

   Note: If there are many discarded object versions, it is possible that the oldest ones are not shown.

To compare document versions:

2. Press and hold Ctrl and select two document versions.

3. Right-click a selected version and select **Compare Selected Documents**.

To restore a discarded object version:

4. Select a discarded object version.

5. Click **Restore Object Version**.

6. In the confirmation dialog that is opened, click **Yes**.

   ✓ M-Files uses the contents of the object version to create a new version of the object.

Comparing Documents

When the setup for Advanced Document Compare feature is completed (refer to Setting Up M-Files Advanced Document Compare), you can use the classic M-Files Desktop to compare the content of two documents or two versions of a document. This section gives examples on how you can use the feature.

Note: The file extension of the compared documents must be DOC, DOCX, PDF, or RTF, and their total file size must be less than 16 MB.

Using the Listing Area to Compare Document Content

To compare the content of the latest version of a document with a different version or document, do the steps in this section. To compare two previous versions of a document with each other, see Comparing Document Content with the History Dialog.

1. Log in to a vault.
2. Use a search or a view to find the document that you want to compare.
3. Right-click the document on the listing area, and select one of these options:

   a. Click **Compare** > **Compare with Previous Version** to compare the current document version with the previous version.

      or

   b. Click **Compare** > **Compare with Another Version** to compare the current document version with a previous version. This command opens the History dialog where you can select a document version with which to compare the content.

      or

   c. Click **Compare** > **Compare with Another Document** to compare the current document version with a different document. This command opens the Windows **Open** dialog where you can select a document with which to compare the content.

   ✓ The **Document Compare** window is opened.

4. To examine the changes, use the **Previous Change** and **Next Change** buttons, the navigation links in the **Change Summary** list, or simply scroll through the document.
5. Optional: To save a copy of the comparison in PDF or DOCX format, use the commands **Save as PDF**, **Save as DOCX**, or **Track Changes**.

   ⓘ **Save as DOCX** creates a simple Microsoft Word rendition of the comparison that you see in the **Document Compare** dialog, but **Track Changes** creates a document that lets you control the tracked changes from the **Review** tab in Microsoft Word.

Comparing Document Content with the History Dialog

When you start to compare content in the listing area, you can compare the latest version of the selected document with a different version or document. To compare two previous versions of a document, start the comparison in the History dialog.

To compare the document content of two previous document versions:

1. Log in to a vault.
2. Use a search or a view to find the document that you want to compare.
3. Right-click the document and select **History**.

   ✓ The **History** dialog is opened.

4. Press and hold down the Ctrl key and select the two versions that you want to compare.

5. Right-click a selected version and click **Compare Selected Documents**.

   ✓ The **Document Compare** window is opened.

6. To examine the changes, use the **Previous Change** and **Next Change** buttons, the navigation links in the **Change Summary** list, or simply scroll through the document.
7. Optional: To save a copy of the comparison in PDF or DOCX format, use the commands **Save as PDF**, **Save as DOCX**, or **Track Changes**.

   ℹ **Save as DOCX** creates a simple Microsoft Word rendition of the comparison that you see in the **Document Compare** dialog, but **Track Changes** creates a document that lets you control the tracked changes from the **Review** tab in Microsoft Word.

Comparing Document Content with the Microsoft Word Ribbon

The **Compare** functionality is only available for documents that are stored in M-Files.

To compare the content of the document opened in Microsoft Word with that of a different document or document version:

1. In the Microsoft Word menu ribbon, open the M-Files tab.
2. Click **Compare**.
3. Select one of these options:

   a. Click **Compare** > **Compare with Previous Version** to compare the current document version with the previous version.

      or

   b. Click **Compare** > **Compare with Another Version** to compare the current document version with a previous version. This command opens the History dialog where you can select a document version with which to compare the content.

      or

   c. Click **Compare** > **Compare with Another Document** to compare the current document version with a different document. This command opens the Windows **Open** dialog where you can select a document with which to compare the content.

   ✓ The **Document Compare** window is opened.

4. To examine the changes, use the **Previous Change** and **Next Change** buttons, the navigation links in the **Change Summary** list, or simply scroll through the document.
5. Optional: To save a copy of the comparison in PDF or DOCX format, use the commands **Save as PDF**, **Save as DOCX**, or **Track Changes**.

   ℹ **Save as DOCX** creates a simple Microsoft Word rendition of the comparison that you see in the **Document Compare** dialog, but **Track Changes** creates a document that lets you control the tracked changes from the **Review** tab in Microsoft Word.

Functions in Microsoft Word, Microsoft Excel and Microsoft PowerPoint

The M-Files functions in Microsoft Word, Microsoft Excel and Microsoft PowerPoint for Microsoft Windows make it easy to manage documents. You can access the functions from the **File** menu, **Office** menu, or **M-Files** menu.

The M-Files functions in this section are available in Microsoft Word, Microsoft Excel, and Microsoft PowerPoint 2016 and 2019, and in versions of Microsoft 365 Apps for enterprise that Microsoft supports.

Open From M-Files	You can open a document from the vault to read or edit it. If you have many vaults, use the **Open from M-Files** function to select the correct one. This function is also available in the **File** and **Office** menus.
Save to M-Files	**Save** is the easiest way to save a document to M-Files. When you save to M-Files directly, the metadata card opens for editing. For more information, see Creating Documents. If you use many vaults, select the correct vault in the **Save** submenu. This function is also available in the **File** and **Office** menus.
Explore M-Files	If the opened file is in M-Files, the **Explore M-Files** function shows it in M-Files. This makes it is easier to use other M-Files functions on the file.
Check Out	The **Check Out** function converts a previously read-only document into an editable document. **Note:** If the document is edited in read-only mode, all changes are lost when you **Check Out** the document.
Check In	The **Check In** function saves the edited document to the vault and closes it in Microsoft Word.
Check In Changes	The **Check In Changes** function checks in your changes and immediately checks out the document to you. This lets other vault users see your changes but lets you continue to edit the document.
Undo Checkout	The **Undo Checkout** function closes the current document and cancels the checkout. If the **Undo Checkout** function is done on an edited document, all changes made after the document was checked out are lost. **Note:** It is not possible to use **Undo Checkout** on a single file of a multi-file document. The function is also not available in the M-Files menu.

Compare	With the standard **Compare** function, you can compare the content of the current document to a previous version of the same document. The **Compare** function opens the document version history where you can select a previous version with which to compare the current one. If the Advanced Document Compare feature is used in your vault, document comparison operates differently. You can also compare the content to a different document. For more information, see Comparing Document Content with the Microsoft Word Ribbon. **Note:** **Compare** is available in Microsoft Word only.
Insert Property	See Add M-Files Property.
Properties	The **Properties** function opens the document's metadata card. See also Object Metadata.

In this chapter

- Add M-Files Property

Add M-Files Property

To add object metadata to the content of a Microsoft Word, Microsoft Excel, or Microsoft PowerPoint document, click **Insert Property** in the M-Files tab. You can also add an electronic signature to a Microsoft Word document. For more information, see Electronic Signatures.

Note: For Microsoft PowerPoint, the **Insert Property** function is available in versions 2016 and 2019, and in versions of Microsoft 365 Apps for enterprise that Microsoft supports.

By default, the metadata fields in a Microsoft Word, Microsoft Excel, or Microsoft PowerPoint document are updated when someone opens the document in a Microsoft Office desktop application. It is also possible to enable automatic updates for metadata fields on check-in. When this setting is enabled, the metadata fields are updated when metadata is changed in M-Files. To enable this feature, tell your M-Files system administrator to enable automatic updates for metadata fields.

Using Insert Property with document templates

The **Insert Property** function can be very helpful when you create document templates. M-Files automatically fills text fields or cells in the template with the selected properties when a user creates a new document. If a property does not have a value, the text fields or cells in the document templates stay empty.

To set a document to be used as a template in M-Files, use the Is template property. To control which users can set documents as templates, see Property Definition Permissions. It is, however, not necessary to set a document to be a template to add metadata to the document.

An M-Files property added into a Microsoft Word document shows as a text field, which turns gray when clicked. In Microsoft Excel documents, M-Files properties show as cell formulas. Microsoft PowerPoint documents show the properties as text areas.

Additional information about properties with date and time information

- Properties of the **Timestamp** data type added to Microsoft Word documents always use the time `0:00`. To have the timestamp include the correct time, ask your administrator to set up a property of the **Text** data type to contain the timestamp value. Then, use that **Text** property in your template.
- For instructions on how to change how date and time information is shown in the inserted properties, refer to the article How to change the date and time formats in Word templates.

Example: Inserting M-Files Properties in Microsoft Word

1. Find a Microsoft Word document in M-Files.
2. Double-click the document and click **Check Out**.

   ✓ The selected document is opened in Microsoft Word.

3. In Microsoft Word, place the cursor where you want the M-Files property to be added.
4. Open the M-Files ribbon and click **Insert Property**.

   ✓ The **Insert M-Files Property** dialog is opened.

5. Click the name of a property.
6. Click **OK** to close the **Insert M-Files Property** dialog.

The value of the selected property is added to the selected location of the document.

Version History

M-Files keeps previous versions of objects. You can return to a previous version from the object history. To open the **History** dialog, click the history icon (🕒) in the option ribbon of the object's metadata card.

When you create a document and check it in, the first version of the document is saved on the server. When you check out the document, make changes, and check it back in, the second version of the document is saved on the server. You can roll back to one of these document versions.

In the **History** dialog, the icon identifies a previous version of the object. In this example, a Microsoft Word document is shown. You cannot change the content or metadata of previous versions.

Add label to this version

You can add a label to an object version. The label is shown in the **Version label** column in the **History** dialog.

To add a label to the selected object version:

1. Click **Add Label to This Version**.
2. Select a label from the drop-down menu.

To create a version label:

1. Click **Add Label to This Version**.
2. Click the arrowhead next to the drop-down menu.

3. Click **New Value (Version label)**.

Clear this label from the other versions of the object

Only system administrators and users with the **Full control of vault** administrative permissions can use this option.

To remove the selected label from other object versions, enable **Clear this version label from the other versions of the object**. For example, you can make sure that only one version of a contract has the label "Approved".

Modify version details

With the **Modify Version Details** option, you can add one or more version labels to an object version and add a comment that will show in the **History** dialog. These comments are also shown in the comments view of the object's metadata card and in the comment history of the **Comments** function (see Object Comments).

Roll back

In the **History** dialog, object versions are recorded from oldest to newest. You can restore old versions with the **Roll Back** option.

When you do a rollback, M-Files uses the contents and metadata of the selected version to create a new version of the object. Rollback does not have an effect on the versions in between. You can use the **Roll Back** option only when the object is not checked out. Be careful when you roll back to an object version that has a workflow state, because the workflow state can cause unwanted actions.

> **Note:** You must have the correct permissions for the object to restore a previous version of it. If you roll back to a version where the permission settings and the metadata of the object are changed, you must have **change permissions** and **edit** rights to the object. If only the metadata or the contents of the object are changed, you must have **edit** rights to the object.

Compare selected documents

To compare document content:

1. Press and hold the Ctrl key and select two document versions.
2. Right-click a selected version and click **Compare Selected Documents**.

For more information, see Comparing Documents.

Version history and permissions

To see a previous version of an object, you must have have access rights to that version and to the latest checked-in version.

Functions in AutoCAD

To make work with CAD drawings easy, users get access to the M-Files functions directly in Autodesk AutoCAD. You can access the functions from the **File** menu or the **M-Files** menu.

M-Files functions in AutoCAD:

- Open from M-Files

- Save to M-Files
- Check Out
- Check In
- Undo Checkout

These functions are not supported in AutoCAD LT. The supported AutoCAD versions are specified in the M-Files Lifecycle Policy.

For more information about these functions, see Functions in Microsoft Word, Microsoft Excel and Microsoft PowerPoint .

Properties

See Properties.

Insert Field

With the **Insert Field** option, you can add M-Files metadata to drawings and AutoCAD fields. In AutoCAD, you can find the M-Files metadata fields in the M-Files **field category** in the **Field** selection dialog. For more information, see Add M-Files Property.

2.3.4. Object Relationships

You can create relationships between objects to link related documents. For example, an offer can contain an offer document, a related price list, and a company brochure. Each object has a separate version history and you can update them separately. Relationships do not create copies of linked objects but establish references between them.

With relationships, you can specify metadata connections between objects the same way you do with the metadata card. For example, you can link a customer with a document, which will then show in the metadata of the object. Relationships added with the metadata card are also shown in the **Relationships** dialog.

Tip: You can use the properties of a related object to create indirect views and searches or to specify filter settings. For more information, see Indirect searches.

In this chapter

- Relationship Operations
- Relationships Between Objects in Separate Vaults
- Subobjects

Relationship Operations

In the classic M-Files Desktop, right-click an object in the listing area and select **Relationships** to manage the relationships of an object.

Adding Object Relationships

To add a relationship to the selected object:

1. On the **Relationships From This Object** or **All Relationships** tab, click **Add Relationship**.
2. In the **Select Target Object** dialog, select the target object.

For a specific version, right-click an object and click **History**.

Tip: You can also drag and drop objects from other windows to the **Relationships** dialog to create many relationships at once.

3. Click **Open**.
4. In the **Define Relationship** dialog, select one of these options:

Option	Description
Latest version	The relationship always points to the latest version of the target object.
Specific version	The relationship points to the selected version of the target object. The relationship does not show updates to the object.

5. Click **OK**.
6. In the **Relationships** dialog, click **Close**.

Editing Object Relationships

To edit a relationship of the selected object:

1. In the **Relationships** dialog, click **Check Out**.
2. On the **Relationships From This Object** or **All Relationships** tab, select the relationship.
3. Click **Edit Relationship**.
4. In the **Relationship Properties** dialog, select one of these options:

Option	Description
Latest version	The relationship always points to the latest version of the target object.
Specific version	The relationship points to the selected version of the target object. The relationship does not show updates to the object.

5. Click **OK**.
6. In the **Relationships** dialog, click **Check In**.
7. Click **Close**.

Removing Object Relationships

To remove a relationship of the selected object:

1. In the **Relationships** dialog, click **Check Out**.
2. On the **Relationships From This Object** or **All Relationships** tab, select the relationship.
3. Click **Remove Relationship**.
4. In the confirmation dialog that is opened, click **Yes**.
5. In the **Relationships** dialog, click **Check In**.
6. Click **Close**.

Relationships Between Objects in Separate Vaults

You can also create a relationship between objects that are saved to two different vaults. The objects are not exported from one vault to the other but a link is created between them. To create the relationship, drag an object from one vault to the other or use the **Relationships** function.

The relationship between the two objects is shown as a shortcut. When you double-click the shortcut, M-Files shows the actual object in a new window. When you select the shortcut, you can see some of the related object's metadata and a link to the object in the target vault. You can also rename the shortcut. This does not change the name of the original object or cause any conflicts between the vaults.

Note: If you have problems with the creation of relationships between vaults, contact your system admin to make sure that the metadata definitions of the object types are matched between vaults.

Shortcut permissions

The shortcuts have their own permissions. By default, M-Files uses permissions for a new object in the vault that you are currently logged in.

Shortcuts created with synchronization

When data is synchronized between vaults, sometimes the metadata of the imported objects creates shortcuts. For example, if a document related to a project is imported without the project, M-Files creates a shortcut for the project in the target vault. This shortcut is now a link to the object in the source vault.

Subobjects

In addition to relationships, objects can also have subobjects. For example, a customer object can have a contact person as a subobject. Object types and the relationships between them are specified by the system administrator in M-Files Admin. The Ctrl + J shortcut shows the object's subobjects and lets you edit and remove them. You can add a new contact person directly from the vault with the **Subobjects** option.

2.3.5. Document Collections

A document collection is a set of related documents. Unlike a multi-file document, each member of a document collection is independent and has its own metadata. Also the document collection has its own metadata. In a multi-file document, all files share the same metadata.

In this chapter

Creating Document Collections

To create a document collection:

1. In M-Files, click the **Create** button.
2. Select **Document collection**.

   If this object type is not shown in the context menu, click an empty area in the listing area and select **Create** > **Document collection**.

✓ The **New - Document Collection** dialog is opened.

3. Select a class and click **Next**.
4. Optional: Select a template.
5. Fill in the necessary metadata.
6. Click **Create**.

The document collection is created. Next, you can add document collection members.

Managing Document Collections

Right-click a document collection in the listing area and select **Collection Members** to open the document collection and manage its content.

Adding Document Collection Members

To add a document collection member:

1. In the **Collection Members** dialog, click **Add**.

   Tip: You can also drag and drop objects from other windows to the **Collection Members** dialog to add many document collection members at once.

   ✓ The **Select Member Object** dialog is opened.

2. Find and select the object that you want to add to the document collection.
3. Click **Open**.
4. In the **Define Membership** dialog, select one of these options:

Option	Description
Latest version	The relationship always points to the latest version of the target object.
Specific version	The relationship points to the selected version of the target object. The relationship does not show updates to the object.

5. Click **OK**.
6. In the **Collection Members** dialog, click **Close**.

Editing Document Collection Members

To edit the membership of a document collection member:

1. In the **Collection Members** dialog, click **Check Out**.
2. Click **Edit**.
3. In the **Define Membership** dialog, select one of these options:

Option	Description
Latest version	The relationship always points to the latest version of the target object.

Option	Description
Specific version	The relationship points to the selected version of the target object. The relationship does not show updates to the object.

4. Click **OK**.

5. In the **Collection Members** dialog, click **Check In**.

6. Click **Close**.

Removing Document Collection Members

To remove a document collection member:

1. In the **Collection Members** dialog, click **Check Out**.

2. Click **Remove**.

3. In the confirmation dialog that is opened, click **Yes**.

4. In the **Collection Members** dialog, click **Check In**.

5. Click **Close**.

2.3.6. Using the Classic M-Files Desktop Offline

This section tells you how to make content available offline, how to edit documents in the offline mode, and what happens when you are back online.

In this chapter

- Offline Availability
- Going Offline
- Going Online

Offline Availability

You can make objects available in the offline mode with the **Mark for Offline Availability** function or with Offline filters. For information on how to go offline and online, see Going Offline and Going Online.

Marking for Offline Availability

You can make individual objects, a group of objects, views, or virtual folders available offline. If you make a view or virtual folder available offline, M-Files creates a new offline filter for it. This way, all new objects that meet the filter conditions are automatically updated to the offline view. For information on how to edit the offline filter that you created, see Offline filters.

To mark objects, views, or virtual folders for offline availability:

1. Select the objects, views, or virtual folders that you want to make available offline.
2. Press Alt and select **Operations** > **Offline Availability** > **Mark for Offline Availability** from the menu bar.

   The selected documents are shown in the **Offline** view.

Removing Offline Availability

To remove the offline availability from individual objects:

1. Select the objects that you want to remove from the **Offline** view.
2. Press Alt and select **Operations** > **Offline Availability** > **Remove Offline Availability** from the menu bar.

   The selected documents are removed from the **Offline** view.

> **Note:** To remove the offline availability from views or virtual folders, you must remove the offline filter. See Offline filters.

Offline filters

You can define filters to make sure you have access to important objects without a network connection from **Other Views** > **Offline**. See Example: Creating an Offline Filter for a Project.

To remove an offline filter, go to the **Offline** view, right-click the offline filter and select **Delete**. In the confirmation dialog that is opened, click **Yes**.

> ! **Important:** When you remove the offline availability from a view or virtual folder, make sure that you run the **Delete** operation in the **Offline** view. Otherwise, M-Files deletes the whole view.

Example: Creating an Offline Filter for a Project

1. In the **All** view (see View navigation), go to **Other Views** > **Offline**.

2. Press Alt to open the menu bar.

3. Select **Create** > **Offline Filter**.

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

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

   ℹ The name is shown in the **Offline** listing area.

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

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

6. On the **Properties** tab, click **Add Condition** and add these conditions:
   a) From the **Property** drop-down menu, select **Project**.
   b) From the **Operator** drop-down menu, select **=**.
   c) From the **Value** drop-down menu, select a project.

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

8. Select **Show documents and other objects**.

9. Click **OK**.

The offline filter is shown in **Other Views** > **Offline**. This lets you access all the documents and objects in this view when the connection to M-Files Server is not available.

Going Offline

You can use M-Files without a network connection.

To use M-Files without a network connection, click your initials in the top-right corner of the user interface and select **Go Offline**. You will then have access to the **Offline** view, which shows all the objects that are available offline.

You can make objects available offline with the **Mark for Offline Availability** command. For more information, see Offline Availability . Collection members, relationship objects, and subobjects are also available offline if they are related to objects that are available offline.

In offline mode, you can create new objects and edit objects that are available offline.

Going Online

To go online from the offline mode, click your initials in the top-right corner and select **Go Online**. When you are online, M-Files restores all other views and you can continue to browse the vault normally. You can also check in documents shown in the **Offline** view and save the changes to the server.

Because users can edit a document on the server when you edit it offline, M-Files makes sure that you can check in your changes when you go online. If other users did not edit the document, you can save the offline version as the new version. If new versions were saved on the server when you were offline, M-Files lets you know. You can then select how to continue:

- Save the version edited offline as a new document. The document on the server stays the same.
- Reject the changes made offline, and accept the new version on the server.
- Cancel **Go Online**.

Tip: If you check out the document before you go offline, other users can see that you checked out the document. When you edit the document, other users cannot make changes to it.

2.3.7. Using M-Files Aino

M-Files Aino is an AI assistant that can summarize documents and give responses about document contents. Click the **M-Files Aino** tab to open or close the interaction with M-Files Aino, or drag the left border of the window to resize the discussion area.

Note: If the M-Files Aino tab is not shown, it can be that M-Files Aino is not available in your platform edition or not set up. The setup instructions for M-Files admins are available in M-Files Catalog.

Note: If you have read-only access to M-Files, M-Files Aino is not available.

M-Files Aino can process documents that contain textual information. M-Files Aino cannot process images, audio, or video. Scanned documents must be converted to a searchable PDF with optical character recognition (OCR) before M-Files Aino can process them. M-Files Aino uses only the information found in the vault content, no external knowledge or internet resources are used.

The supported file formats for M-Files Aino include but are not limited to these formats:

- Microsoft Word files (docx, docm, dotx, dotm, doc, dot)
- Microsoft Excel files (xlsx, xlsm, xltx, xltm, xlsb, xls, xlt)
- Microsoft PowerPoint files (pptx, pptm, ppsx, ppsm, potx, potm, ppt, pps, pot)

- PDF files

Note: The responses can contain inaccuracies or be incomplete. If you see mistakes, please give feedback.

Summarizing documents

To summarize a single document, select the document in the listing area and click **Summarize this document** in the Aino tab. Click **Add details** or **Condense** to view more or less information in the summary.

Note: M-Files Aino summarizes the document in the software language. See Selecting the Software and Vault Language. Click **Translate** to have the summary in your preferred language.

Asking questions

You can use M-Files Aino to find answers from a single document, from objects that are related to your current location, for example a view, or from the entire vault. To ask questions about the content, write your question to the **Ask anything** field on the **Aino** tab and click **Ask** or press Enter.

If you have selected a single document, M-Files Aino gives you answers related to that document only. If you click, for example, a view name or open a view, M-Files Aino looks for answers from that content. If M-Files Aino cannot find the answer with these options, use the **Look for answers in** option to tell M-Files Aino to find answers from the entire vault.

M-Files Aino uses your vault permissions when it creates the answer. This means that if you do not have the necessary permissions for the content that M-Files Aino would use in the answer, the content is not included in the answer. M-Files Aino shows the answer's source documents below the answer.

Your administrator can specify that some content is left out from M-Files Aino's answers. This means that not all documents will be considered when M-Files Aino searches for an answer from multiple documents. When this feature is active, you will see a notification message with an explanation from your administrator in the **Aino** tab. Nevertheless, you can still select a single document and ask Aino questions about that document even if it is left out from vault-wide search.

Note: To ask questions from many documents or from the entire vault, your M-Files admin must have set a separate configuration. This separate configuration is available for an additional cost.

Note: M-Files Aino answers in the same language as the question. The document language and the software language can be different. See Selecting the Software and Vault Language. If you want to have an answer in certain language, you must ask the question in that language.

Saving responses

You can save M-Files Aino's responses to the clipboard or to the document's metadata. Click **Copy to clipboard** to copy the summary or the answer to the clipboard. Click **Save as metadata** to save the summary or the answer as metadata. Use the suggested metadata property from M-Files or select a property to which you want save the response.

Chat history

M-Files Aino saves all your chats automatically to the chat history. The chat history is shown only to you.

To see the chat history, click the clock icon (🕒) at the top of the **Aino** section. In the chat history, you can continue your old chats or delete them.

- To continue a chat, click a chat.
- To delete a chat, click the bin icon (🗑). To confirm the deletion, click **Delete**.

> **Note:** When you continue previous chats, it is possible that the source documents have changed. This can have an effect on the previous answers.

Giving feedback

You can give feedback to help improve M-Files Aino. If you think that the response is useful, click the thumbs up icon (👍). If you think that the responses are unsatisfactory or erroneous, click the thumbs down icon (👎), enter your feedback, and click **Send**. Your feedback is anonymous, and you will not be contacted.

Limitations and user quota

M-Files Aino has these limitations:

- M-Files Aino cannot process very large documents (approximately 100 pages or more).
- M-Files Aino can sometimes give incorrect or incomplete information.
- M-Files Aino is trained to decline unsuitable requests.

Each user has a vault-specific quota on how much content they can have M-Files Aino process within 24 hours. The quota use depends on, for example, document language, complexity of the text, and formatting details.

M-Files lets you know when you have used 90% of your quota. If you use all your quota, M-Files Aino will be temporarily unavailable. When enough time has passed, you can use M-Files Aino again.

For more details about these limits, refer to the platform editions page on the M-Files website.

Admin aid

Refer to these documents for more technical information:

- M-Files Aino - Getting started
- M-Files Aino - Administrator Guide
- M-Files Aino - FAQ
- M-Files Aino - Security and Data Protection Features

Related M-Files solutions

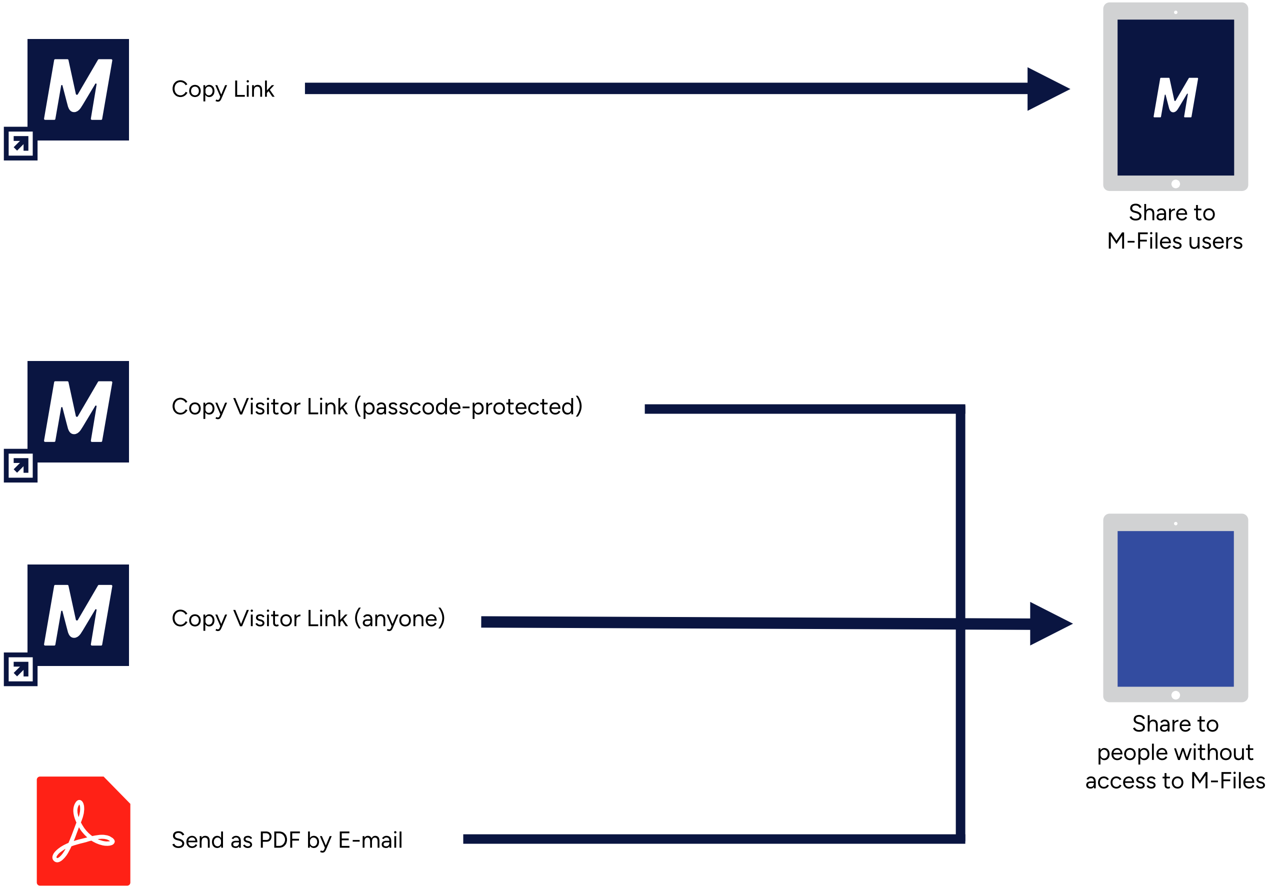
Refer to these documents for information on related M-Files add-ins and extensions:

- Setting Up M-Files Copilot Connector

2.4. Sharing Content

This section tells you how to share vault content in the classic M-Files Desktop to people with access to the same vault as you, and to people outside your organization. Click on different parts of the image for information about the sharing options.

Note: To use these sharing options, M-Files Web must be enabled.


Copy Link
Share to M-Files users
Copy Visitor Link (passcode-protected)
Copy Visitor Link (anyone)
Send as PDF by E-mail
Share to people without access to M-Files

1. Sharing to M-Files Users
2. Sharing passcode-protected visitor links
3. Sharing to M-Files Users
4. Sharing to People without Access to M-Files
5. Sharing visitor links for anyone
6. Send as PDF by E-mail

Admin aid

Refer to these documents for more technical information:

- Configuring M-Files Links
- Creating URLs for the Classic M-Files Web

Related M-Files solutions

Refer to these documents for information on related M-Files add-ins and extensions:

- Setting Up and Using M-Files for Microsoft Teams

In this chapter

2.4.1. Sharing to M-Files Users

Note: To use the **Copy Link** operation in the classic M-Files Desktop, M-Files Web must be enabled.

You can share links to other M-Files users with the **Copy Link** option. The recipient must have access to the vault and the object or view to open the link.

To share a link to an M-Files user with the **Copy Link** option:

1. In the listing area, do one of these operations:

   a. Right-click an object.

      or

   b. Right-click a view.

      or

   c. Select many objects and right-click one of them.

2. Select **Copy Link**.

The link is copied to your clipboard and you can share the link to other M-Files users. If you selected many objects, M-Files creates a separate link for each object.

Sharing links to previous object versions

To share a link to a previous object version:

1. Click the history icon (🕓) in the option ribbon of the object's metadata card.

   ✓ The **History** dialog opens.

2. In the dialog, do one of these operations:

   a. Right-click an object.

      or

   b. Select many objects and right-click one of them.

3. Select **Copy Link**.

The link is copied to your clipboard and you can share the link to other M-Files users. If you selected many objects, M-Files creates a separate link for each object.

2.4.2. Sharing to People without Access to M-Files

Important information

Your visitor link is usable when these requirements are met:

- Your user account is enabled.
- You have at least read permissions to the document.

For security reasons, the link is no longer usable if either requirement is not met. To share documents with a large number of people without access to M-Files, you can use these alternative sharing methods:

- M-Files Hubshare offers more control and security.
- Anonymous vault access lets users access a vault without credentials.

You can use visitor links to share M-Files objects for people without access to M-Files. With passcode-protected visitor links, you can specify the people who can open the link. With visitor links for anyone, anyone with the link can open it. In addition to visitor links, you can share content with the **Send as PDF by E-mail** option.

If you do not see the **Create Visitor Link** option in the context menu of an object, ask your M-Files admin to make sure that these operations are done:

- Public links have been configured.
- M-Files Web has been set up.
- The M-Files Web home page has been specified in **Document Vault Properties**.

Sharing passcode-protected visitor links

With passcode-protected visitor links, you can specify the people who can open the link.

To copy a passcode-protected visitor link in M-Files:

1. In the listing area, right-click an object and select **Create Visitor Link**.

   ✓ The **Create Visitor Link** dialog opens.

2. In the **Create a passcode-protected visitor link** section of the dialog, enter the email address of the link receiver and click **Add**.

   ✓ The email address is added to the list of people's addresses that can open the link.

3. Click **Copy link**.

   ✓ The link is copied.

You can now paste the link, for example, to emails and chats. Only people whose email addresses are on the list can open the link with the passcode that was sent to them. If no receivers get passcodes to visitor links that you have created, ask your administrator to make sure that notifications are enabled in the vault.

Note: A passcode-protected visitor link expires after three months. Every time the list of email addresses is edited, the expiration date is set again to three months. You can see the expiration date in the **Shared by Me** dialog.

Sharing visitor links for anyone

With visitor links for anyone, anyone with the link can open it.

To create a visitor link for anyone:

1. In M-Files, find the object to share.
2. Right-click the object or the object version and select **Create Visitor Link**.

   The **Create Visitor Link** dialog opens.
3. In the **Create a visitor link for anyone** section, click **Create**.

   The **Create Visitor Link for Anyone** dialog opens.
4. Select the target version.
5. Use **Expiration date (local time)** to select the date and time after which the visitor link for anyone will no longer be active.
6. Optional: In **Description**, enter a description.

   The description is shown in the **Shared by Me** dialog.
7. Click **Create Visitor Link for Anyone**.

   The link is added to the **Visitor link for anyone** field.
8. Click **Copy** to copy the link.
9. Click **Close**.

You can now paste the link, for example, to emails and chats.

Managing visitor links

In the **Shared by Me** dialog, you can manage the visitor links that you have shared. For example, you can stop sharing a link. Users with the **Full control of vault** or **See and read all vault content** administrative rights can see and manage the visitor links shared by all vault users.

To manage shared visitor links:

1. In the classic M-Files Desktop, click your initials in the top-right corner and select **Shared by Me**.

   If you have the **Full control of vault** or **See and read all vault content** rights, you can also select **Shared Files (All Users)**.

   All the visitor links shared by you are shown in the **Shared by Me** dialog.
2. Do the necessary operations.

Link type	Option	Description
Visitor (Passcode-protected)	**Copy Link**	Copies a shared passcode-protected visitor link to the clipboard.

Link type	Option	Description
Visitor (Passcode-protected)	**Edit**	Opens the **Copy visitor link** dialog. Click **Remove all** to stop sharing the passcode-protected visitor link.
Public (For anyone)	**Copy Link**	Copies a shared visitor link for anyone to the clipboard.
Public (For anyone)	**Stop Sharing**	Removes a shared visitor link for anyone.

3. Click **Close**.

Send as PDF by E-mail

With this option, M-Files converts the selected file to PDF format and creates an email message with the PDF file attached. The file in M-Files stays in its original format. To use the option, right-click a file in the listing area and select **Save as PDF** > **Send as PDF by E-mail**.

2.5. Finding Content

This section tells you how to find content with the M-Files search functions and views.

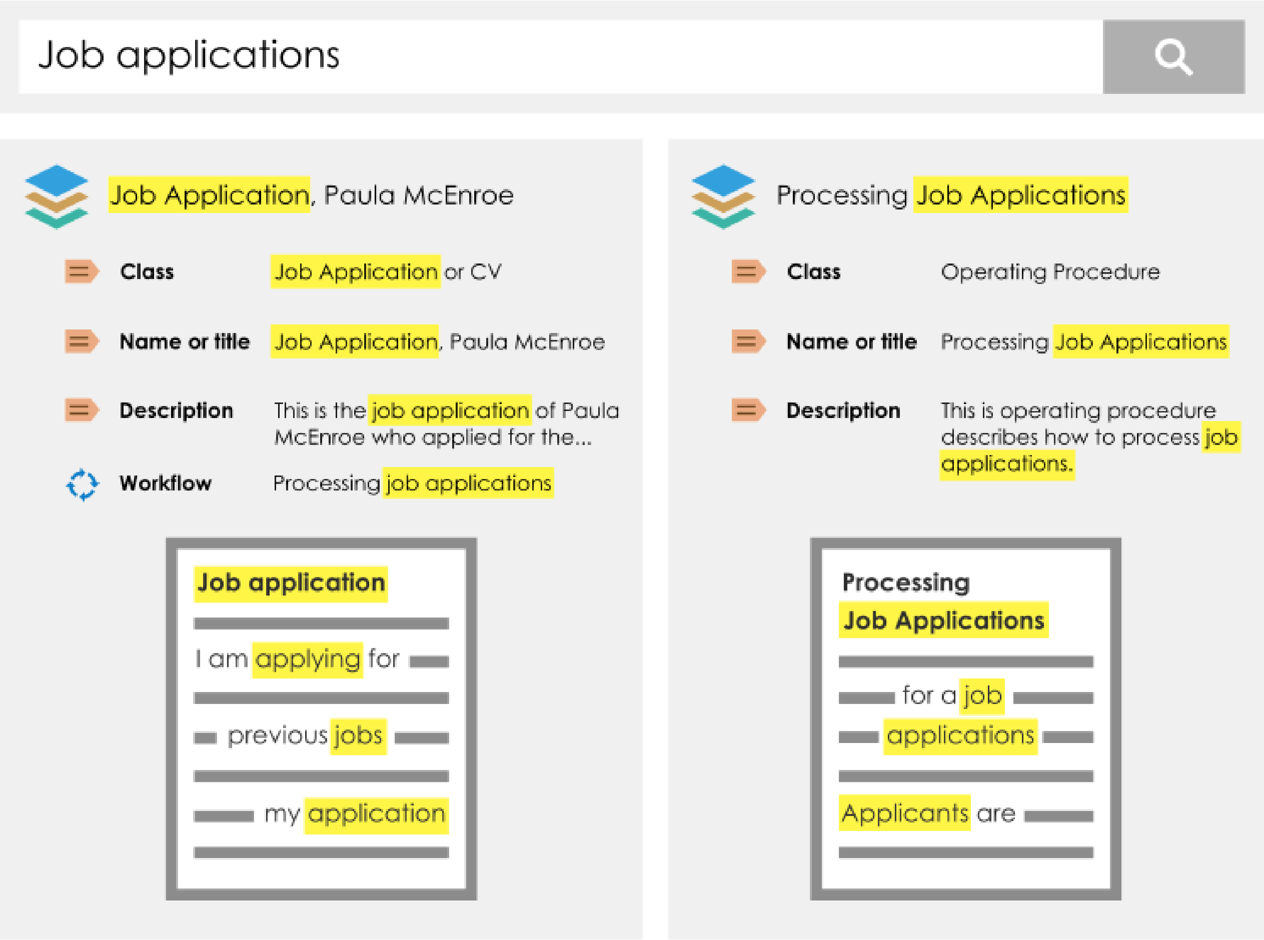

Job applications
Job Application, Paula McEnroe
Class
Job Application or CV
Name or title
Job Application, Paula McEnroe
Description
This is the job application of Paula McEnroe who applied for the...
Workflow
Processing job applications
Job application
I am applying for
previous jobs
my application
Processing Job Applications
Class
Operating Procedure
Name or title
Processing Job Applications
Description
This is operating procedure describes how to process job applications.
Processing
Job Applications
for a job
applications
Applicants are

Figure 7: As an example, when you search for job applications, M-Files looks for your search term in the titles, metadata, and contents of objects in the vault. You can also find inflected forms of your search term.

In this chapter

2.5.1. Searching

The best way to find objects is to use the search. This is especially helpful if you only know one detail about the object. For example, the creation date or creator of a document.

Search options and filters

The search options and filters let you specify more search criteria.

Search result sorting

M-Files shows the search results in a sequence of most frequently or recently used objects. This way, objects that are most related to the user are shown first. M-Files uses the criteria in this list to create the sequence:

- When the object was created
- When and how many times the object was edited
- When and how many times the object was processed
- How many times the search string is found in metadata or file contents, which includes:

  - The name or title of the object
  - Metadata other than the title
  - File contents

M-Files ignores some metadata that decreases the precision of the search results. For the sequence of the search results, metadata is always more important than the file content.

Tip: If your M-Files system administrator has enabled translated object titles, you can use the translated object titles in searches. The translated object titles are also shown in the title area of the metadata card, in the listing area, in notifications, and in value lists.

Disabling relevance sorting

The M-Files system administrator can disable the default relevance settings so that each user can sort the results independently. For more information, see Disabling the Sorting of Search Results by Their Relevance.

Search result grouping

M-Files automatically groups search results by object type.

If there is a large number of search results in a grouping, M-Files only shows a part of the search results. To see more search results, click **Show more results**. To change the number of results shown on a page, right-click an empty space in the listing area and select **Display Mode** > **Objects per Group**.

Search word emphasis in the results

Your search terms are highlighted in yellow on the listing area and the metadata card. When preview is used, search terms are highlighted in the file contents.

Note: Search word emphasis is not available for file previews if your admin has set the classic M-Files Desktop to use the Windows default previewer.

Contents of these file types are highlighted in the **Preview** tab:

- Email files (eml, emlx, msg)
- HTML and web archive files (htm, html, mht, mhtml)
- 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)

Note: If you use the exact match search with quotation marks, for example `"dat sports"`, partial matches can also be highlighted. See Exact match.

Admin aid

Refer to these documents for more technical information:

- M-Files Smart Search - Frequently Asked Questions
- Solution Description - Smart Search
- Configuring Faceted Search
- Editing Settings for dtSearch Relevancy Ranking in M-Files Admin
- Setting Up High Availability for IDOL Searches

In this chapter

Quick Search

To do a quick search, enter a search string to the search field in the top area and click the search button. The words and phrases that you use in searches are kept in the search drop-down menu. It is thus easy to do recent searches again.

The search tries to find objects that contain the search word in the metadata or file contents. You can also set M-Files to use only metadata or file contents. M-Files remembers your selection until you close the window or log out. For more information about search refinements, see Search Filters.

By default, quick search scans the entire vault. However, your M-Files administrator can change the default behavior and limit the quick search to the currently active view. In this case, you can widen the search to the entire vault. To do this in the classic M-Files Desktop, go to the **Filters** tab and unselect the view. In M-Files Web and the new M-Files Desktop, you can change the setting in the search bar.

If you cannot find the correct information, try these features or methods:

- Quotation marks or other operators and special characters

- Search options for quick search
- More accurate search terms
- The **advanced search features**

In the classic M-Files Desktop, you can also disable Look for different inflected forms of the words in Quick Search in the Additional Conditions dialog. This causes the search results to only contain objects that match this word accurately.

Search options for Quick Search

Click the search options button (☰) in the classic M-Files Desktop to open three more options:

- Search type
- Property conditions
- Additional conditions

Some search conditions operate differently with different search engines.

Search type

To set how your search queries are matched, select:

All words Matched objects contain all the search words.

Any word The search shows all objects that contain at least one of the search words.

Boolean The search lets you use more specific search phrases and different operators. For the list of operators, see Boolean operators.

> **Note:** Boolean search is available in vaults that use dtSearch or Micro Focus IDOL as the search engine.

Property conditions

Each object has property values that you can use as search criteria. For example, the value of the property Project can be Hospital Expansion (Florida). If you do a search with these values, the search shows all object in which the Project property contains the value Hospital Expansion (Florida).

To set a property condition, select a property, a condition, and a property value with the drop-down menus in the search options section. You can set more property conditions with additional conditions.

Subordination of search criteria

You can use search subordination criteria to make sure that previous filter selections are used before the property values are shown in the drop-down menu. For example, if you select a workflow as the search criterion, you can then only use workflow states related to the selected workflow as search criteria. Corresponding filtering is done automatically for other interdependent value lists. For example, contact persons are filtered by the customer if these value lists have a hierarchical relationship.

You can use subordinate search criteria with the "is" operator. In the **Additional Conditions** dialog, it is also possible to use the operator "one of".

Indirect searches

You can also use property relationships in your search criteria. Thus, the property selected as the search criterion can be the property of a related object. For example, with indirect search you can find agreements related to a country without the Country criterion. It is sufficient if it is found through a customer related to the agreement. The search criterion is specified like this: `Customer.Country`.

To set indirect search properties, click the plus sign in the property list and select the property of a related object. With additional conditions, you can create three-level indirect search criteria.

Tip: You can create indirect views with the properties of related objects. You can also use indirectness when you create a filter. For more information about how to create views, see Creating a View.

In this chapter

- Operators and Special Characters

Operators and Special Characters

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.

Note: M-Files Smart Search does not support wildcard characters, but you can use property conditions with the `Contains` operator. You can read more about Smart Search in M-Files Smart Search - Frequently Asked Questions.

Search type	Operator or special character	Description
Exact match	Quotation marks: `"phrase"`	Search words inside quotation marks find objects that contain all of the search terms in the given order. Example search: `"functional specification"` The exact match search operates differently with the different search engines available for M-Files. M-Files Smart Search and dtSearch always find the exact form of the phrase inside the quotation marks. Micro Focus IDOL finds the exact forms, inflected forms, and decompounded forms (for example, `"smartphone"` also finds `"smart"` and `"phone"`). To know which search engine your organization uses, contact your M-Files administrator or try different searches in the vault. To have Micro Focus IDOL operate in the same manner as M-Files Smart Search and dtSearch, your M-Files administrator must disable the search engine's language analyzer. This can be done in the settings of the search index with Advanced Vault Settings. For the new setting to be used, the search index must be rebuild (refer to Rebuilding the dtSearch Full-Text Search Index). For performance reasons, the exact match search for M-Files Smart Search only uses approximately 950 to 1,000 of the first words in a document.
Any single character	Question mark: `appl?`	The `?` character matches any single character except a whitespace or underscore 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 single digit	Hash: `201#`	The `#` character matches any single digit in its position. Example search: `201#` matches, for example, "2017" and "2018". **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.

Search type	Operator or special character	Description
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` **Note:** Fuzzy search is disabled by default and must be enabled by the M-Files system administrator. See Enabling Phonic and Fuzzy Searches for more information.
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:** To use this feature, your search engine must be dtSearch. **Note:** Phonic search is disabled by default and must be enabled by the M-Files system administrator. For more information, see Enabling Phonic and Fuzzy Searches. **Note:** Phonic searches are inclusive by nature, and therefore they may occasionally produce too many search results or their search precision may be low.
Synonym search		Documents containing synonyms of a word included in your search query may also be listed in the search results. For example, if you search for `announcement`, the search results may also list documents containing words such as `notice`, `bulletin`, `publication`, or `statement`, in addition to the word `announcement`. **Note:** Synonym search is disabled by default and must be enabled by the M-Files system administrator. See Setting Up Synonym Search for more information.
	Underscore: `2018_01`	The _ character matches a whitespace. Consequently, the next character starts a search term and cannot be a wildcard character `?`, `#`, or `*`. Example search: `2018_01` matches both "2018_01" and "2018 01".

Boolean operators

Click the search options icon (☰) and select **Boolean** to use the Boolean operators in your search.

Note: Boolean search is available in vaults that use dtSearch or Micro Focus IDOL as the search engine.

Search type	Operator	Description
All of the search terms must be found	AND	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	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	The `NOT` operator excludes a search term from the search results. It can be used in conjunction with `AND`, `OR` or `W/N`. Example search: `agenda AND NOT minutes`
Required search term and an optional search term	AndAny	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	( )	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	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`

Search Filters

With the advanced search features, you can use more specific search criteria for the document or object you are looking for. In the classic M-Files Desktop, the criteria is in the **Filters** tab. In M-Files Web and the new M-Files Desktop, they are shown in the **Search** tab.

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. Your search results are updated in real time according to the selected search filters.

The filters can contain, for example, these search options:

- Scope
- Object type
- View (in the classic M-Files Desktop)
- Search refinements

Scope

In **Search in**, you can select whether to search metadata, file contents, or both. By default, both metadata and file contents are searched.

Object type

You can select one or more of the object types to narrow down your search.

View

When you have a specific view open, you can select to search only within the view that you are currently in. The **View** option is shown only if you currently have a view open on the listing area.

The **View** option is shown also for external views. If it is not shown, ask your system administrator to rebuild the search index of the external repository.

Search refinements

Note: This functionality is available only if your vault uses the Smart Search or Micro Focus IDOL search engine.

You can refine your search results by selecting one or more of the available criteria in this section. For more information, see Search Refinements.

Default search filters

In the classic M-Files Desktop, you can set frequently used search options to be remembered by M-Files. For more information, see Default Search Filters.

In this chapter

- Search Refinements
- Default Search Filters

Search Refinements

Note: This functionality is available only if your vault uses the Smart Search or Micro Focus IDOL search engine. You can read more about Smart Search in M-Files Smart Search - Frequently Asked Questions.

You can select one or more of the available criteria in the section below the **Search in**, **Object type**, and **Repository** options on the **Filters** tab to refine your search results. You can, for example, select to only search for objects that were created in 2022, modified within the last week, and that refer to a specific vault user.

Click the **Show more** option to view more criteria in a specific category.

Note: Search refinements only apply to objects with M-Files metadata. Any objects that do not have metadata (for example, unmanaged objects) are hidden in the search results if search refinements are selected.

When your search results have been refined to match your search query and the selected criteria, you can refine your search even more. To do this, select additional criteria. The criteria for which there are no longer matches are grayed out.

Default Search Filters

You can set default search filters that will be remembered by M-Files always when you log in to the vault with the classic M-Files Desktop. This is useful, if you often select the same search options on the **Filters** tab when searching for documents or objects.

Do the following steps to set default search filters:

1. In the classic M-Files Desktop, do a search.

   The **Filters** tab is opened in the right pane.

2. On the **Filters** tab, hover over the the search criterion you want to select as your default search filter.

   Note: If your vault uses Micro Focus IDOL or Smart Search, you can set any search filter as default. If dtSearch is used instead, the filter selection is limited.

   The open lock icon (🔓) appears in front of the check box.

3. Click the open lock icon (🔓).

   The search criterion is shown in bold and it appears with closed lock icon (🔒) under **Your default filters** at the top of the **Filters** tab.

4. Set as many filters as desired by repeating the steps 2 and 3.
5. Optional: To unselect a default search filter, click it under **Your default filters**.

   The search filter is removed from the list.

When searching for documents and objects in the classic M-Files Desktop, the set default filters are automatically used as search criteria.

You can view your current default search filters and refine them on the **Filters** tab. The default search filters are shown in bold and they are listed under **Your default filters**.

To remove all default filters, click **Reset default filters**.

Additional Conditions

To open the **Additional Conditions** dialog in the classic M-Files Desktop, click the search options button (☰) and then **Additional Conditions**. After you have applied additional conditions and closed the dialog, the number of active conditions is shown in parentheses in the **Additional Conditions** button.

> **Note:** Some search conditions operate differently with different search engines.

Look for different inflected forms of the words in Quick Search

To search for a particular word form, disable the option **Look for different inflected forms of the words in Quick Search** in the **Additional Conditions** dialog. 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*, and so on.

> **Note:** The search for inflected forms is enabled by default. If needed, the M-Files system administrator can disable this option for all vault users. For more information, see Disabling the Search for Inflected Forms.

Look in the metadata of all versions

When you select the **Look in the metadata of all versions** option, the search operation looks for results in the metadata of all object versions instead of only the latest ones.

Two limitations apply to this option:

- The option is not used in quick searches.
- The property definition setting **Do not search for old object versions** can have an effect on the results.

Show latest version

When you select **Look in the metadata of all versions**, the search will be performed on all versions of each object. If the option **Show latest version** is on as well, M-Files shows the newest version of each returned object instead of showing the old version that actually matched the search conditions.

Exporting search conditions

You can use the *Export Conditions* function to save the search criteria. To access this search-related function, press Alt 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, see the M-Files API documentation.

In this chapter

- Status-Based Conditions

- Property-Based Conditions
- File Information Based Conditions
- Permissions-Based Conditions

Status-Based Conditions

You can find the search criteria listed in this section on the **Status** tab of the **Additional Conditions** dialog.

Object type

Specify the object type or object types to include in the search results. If you do not select anything here, the results include all object types in the vault.

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 Property-Based Conditions.

Checked out

If you specify as a search criterion that the document has been *checked out* and select *Yes* from the drop-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. M-Files preserves all deleted documents. In order to perform this search, you need permissions for viewing deleted documents.

In this chapter

- Example: Searching Only for Deleted Projects

Example: Searching Only for Deleted Projects

You need to have permissions to see deleted objects.

1. Click the advanced search options button (☰) in the search bar.
2. Click the **Additional Conditions** button.

   ✓ The **Additional Conditions** dialog is opened.
3. Select the **Object type** check box, select **=** from the first drop-down menu, and finally select **Projects** from the rightmost drop-down menu.
4. Select 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 search field or leave it empty if you do not want to filter your search further.
7. Press Enter or click the search button.

The search results show the deleted projects for your search term or all the deleted projects if you omitted the search term.

Property-Based 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.

On the **Properties** tab of the **Additional Conditions** dialog, click **Add Condition** to specify a property-based condition. To remove the selected property condition, click **Remove Condition**. Note that the checkbox next to the property name does not indicate selection for this purpose, but instead specifies whether or not the condition is in use.

Note: Any disabled conditions are automatically removed when the properties dialog is closed.

Properties

The criterion defined in the **Property** column can either refer to the value of 1) a certain, single property or 2) that of all properties that have been defined to show values from a certan value list (see below for an example).

What does any property in the property name mean?

Many of the properties are accompanied by the expression **any property**. If you use this type of property as a search criterion, it means that the search results will include all objects where the property value matches your search term *no matter what the name of the property is* as long as it has been defined to show values from the specified list. This is perhaps best explained with an example:

Example: If you have installed M-Files for evaluation, the properties *Supervisor* and *Project manager* in the sample vault both show values from the list *Employees*. If you now select *Employee (any property)* as a search criterion, the search returns all objects where the *Supervisor* or *Project manager* property has the value that you searched for. If, on the other hand, you use the *Supervisor* property as your search criterion, the search only returns objects that contain the *Supervisor* property with the specified value.

Operators

In the *Operator* field, you can also determine other criteria than *equal to*. See the table below for the list of available operators.

Operator	Description
=	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.

Operator	Description
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. If you want to include wildcards in your search criterion, use the *Matches wildcard pattern* option.
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. See further below for an example.
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 right-clicking **Filter: *** and selecting **Set Filter** from the context menu. Enter a suitable filter word in the **Set Filter to List** dialog. Note that you can enter only one filter value in the text field. If you need to select multiple values from the **Value** column, you can try extending your filter by using wildcards. If not applicable, you must select the values without a filter.

Note: You can select multiple values by holding down the Ctrl key while clicking values.

For instance, when you search for projects with the **Matches wildcard pattern** operator and the search term `????house*`, the results include all the objects whose **Project** property value begins with any four-character string, followed by the word `house`, and then a string with any number of any characters. If the vault has a document with a **Project** property `Warehouse Management System Development`, it is shown in the search results.

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 = 18.12.2021	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. You can also use negative numbers. For example: • `DaysFrom > 5` is the same as `DaysTo < -5`. • `DaysFrom < 5` is the same as `DaysTo > -5`.
DaysTo()	Effective through < 10	Returns objects with a given timestamp property containing a date within a given number of days *following* the current date. You can also use negative numbers. For example: • `DaysFrom > 5` is the same as `DaysTo < -5`. • `DaysFrom < 5` is the same as `DaysTo > -5`.
Month()	Created = 05	Returns objects that have a given timestamp property containing a date with a given month. Use the format `MM`.
Year()	Document date = 2022	Returns objects that have a given timestamp property containing a date with a given year. Use the format `YYYY`.
YearAndMonth()	Created = 2021-12	Returns objects that have a given timestamp property containing a date with a given year and month. Use the format `YYYY-MM`.

Also refer to **Subordination of search criteria** and **Indirect searches** under Search Filters. You can always utilize indirectness for specifying the properties in filter settings.

In this chapter

Example: Searching for Ongoing Projects for American Customers

1. Click the advanced search options button (☰) in the search bar.
2. Click the **Additional Conditions** button.

   ✓ 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.

   ℹ 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**.
11. Click **OK** to close the **Additional Conditions** dialog.
12. Enter a search term in the search field or leave it empty if you do not want to filter your search further.
13. Press Enter or click the search button.

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.

File Information Based Conditions

An M-Files object contains metadata and zero or more files. You can use the **Files** tab of the **Additional Conditions** dialog to specify search criteria related to files.

Contains files

Set this condition to **Yes** to search only documents that contain files. If you select **No**, only objects without files are included in the search results.

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. For more information on the available operators, see Property-Based Conditions.

File size (KB)

If you want to search files of a specific size, enter the minimum and maximum file size here.

File created, File changed

You can also make searches according to the creation and modification time of the files. For more information, see Status-Based Conditions.

Linked to external location

You can make 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, see External File Sources.

Show duplicates only

Use the **Show duplicates only** option to create a view that contains only duplicate content. This is useful, for example, when you want to remove duplicate files from the vault.

In this chapter

Example: Searching for PNG Images

1. Click the advanced search options button (☰) in the search bar.
2. Click the **Additional Conditions** button.

   ✓ 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.
6. Click **OK** to close the **Additional Conditions** dialog.
7. Enter a search term in the search field or leave it empty if you do not want to filter your search further.
8. Press Enter or click the search button.

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-Based Conditions

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. To do this, go to the **Permissions** tab of the **Additional Conditions** dialog. Select a condition or click **Add Condition** to specify a permission-based condition.

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.

> **Note:** When you use the condition **Access control list** and select a named access control list that uses pseudo-users through metadata, it can be that the search results are not accurate or that there are no results. For more information, see Pseudo-users and Named Access Control Lists.

In this chapter

- Example: Searching for Objects That Are Visible to the HR Department

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 the advanced search options button (☰) in the search bar.
2. Click the **Additional Conditions** button.

   ✓ 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 search field or leave it empty if you do not want to filter your search further.
8. Press Enter or click the search button.

The search results show the objects that match your search term and are visible only to the HR department.

Exporting Search Results

Before you export search results, make sure that all the necessary search results are shown. Use **Show more results**, **Next**, and **Previous** to see more results.

The number of exported results is specified with a registry setting. Contact your system administrator about necessary changes.

To start the export:

1. Right-click an empty area in the listing area and select **Export**.
2. Select the information that you want to export.

3. Select one of these options:

    a. To export a list of the search results as a CSV file, unselect **Export files**.

    or

    b. To export a list of the search results as a CSV file and the object files, select **Export files**.

4. Click **OK**.
5. Select the file location and enter the file name.
6. Select **Save**.

    ✓ The confirmation dialog is opened.

7. Click **Yes**.

Search Results in Other Vaults

When you do a search in M-Files, the **Search Results in Other Vaults** pane below the search results listing shows the number of results in other vaults. If the vault icon is blue, there are matches in that vault. If the vault icon is gray, the search results are not available or there are no matches in that vault. When you click a vault in this pane, you go to that vault and see the search results.

Search results in other vaults are not updated if your search is filtered by additional conditions or search refinements.

Tip: The search results are gotten from the vaults to which you are logged in. You can click **Show all** to also see the vaults to which you are not logged in. You can set your login account to be automatically logged in to a vault when Windows is started. For instructions, see Log in automatically when Windows is started.

To hide or show the **Search Results in Other Vaults** pane, right-click an empty space in the listing area and select **Display Mode** > **Show Search Results in Other Vaults**.

You can also minimize the **Search Results in Other Vaults** pane. This only shows the heading of the pane until you expand it. To do this, right-click an empty space in the listing area and select **Display Mode** > **Bottom Pane** > **Minimized**. This setting changes all the panes shown at the bottom of the listing area.

Disabling the pane with registry settings

To disable the **Search Results in Other Vaults** pane automatically, you can ask your administrator to change this registry setting on the client computer:

Key	`HKEY_CURRENT_USER\SOFTWARE\Motive\M-Files\<version>\Client\MFShell\ <vault>`	
Value name	`MultiVaultSearchEnabled`	
Value type	`REG_DWORD`	
Description	Enables or disables the **Search Results in Other Vaults** pane.	
Valid values	`0`	The **Search Results in Other Vaults** pane is disabled.
	`1`	The **Search Results in Other Vaults** pane is enabled.

2.5.2. Using Views

Views organize objects in the vault by metadata. This makes the correct information easy to find. Views can use, for example, object types (such as **Customer** or **Project**) and they can be further grouped by properties (such as **Country** or **Customer**).

For instructions on how to set up views and grouping levels, see Creating a View.

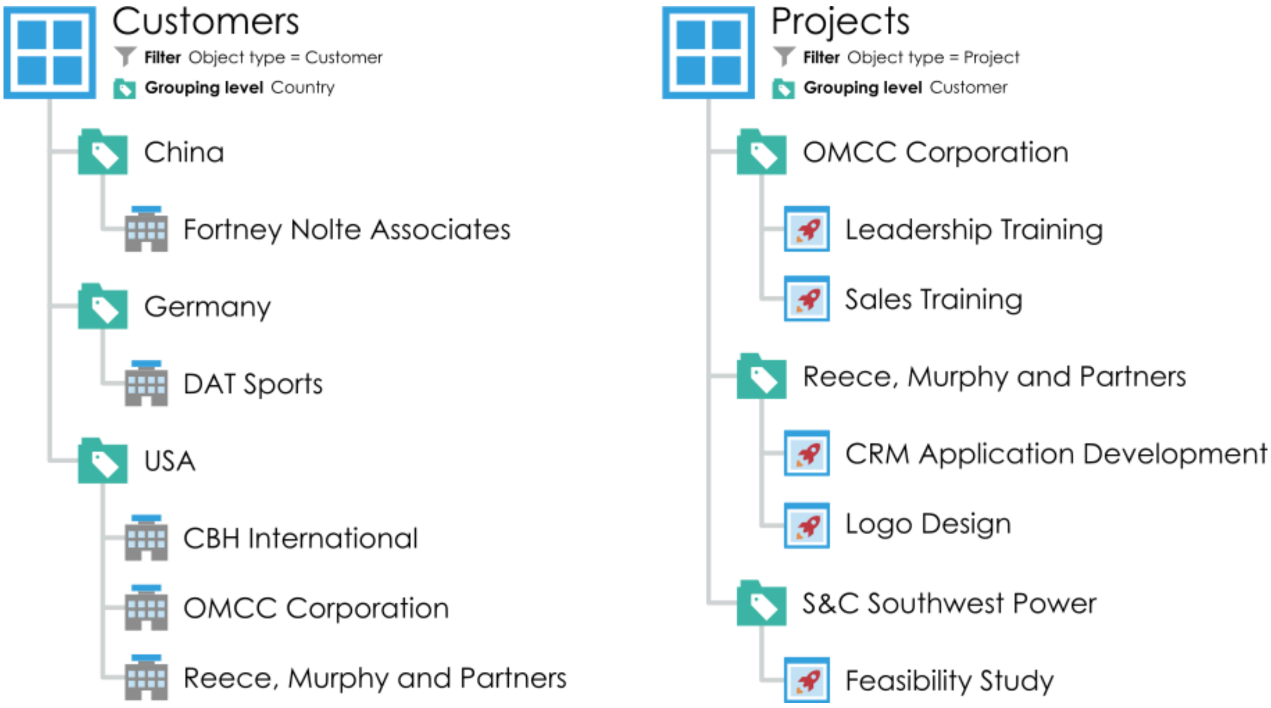


Figure 8: These examples use customer, project, and country information to group objects.

In this chapter

- Creating a View
- Traditional Folders
- View-Specific Operations

Creating a View

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

Views allow you to save frequently used searches and define grouping levels. For information about searching for documents, refer to Searching.

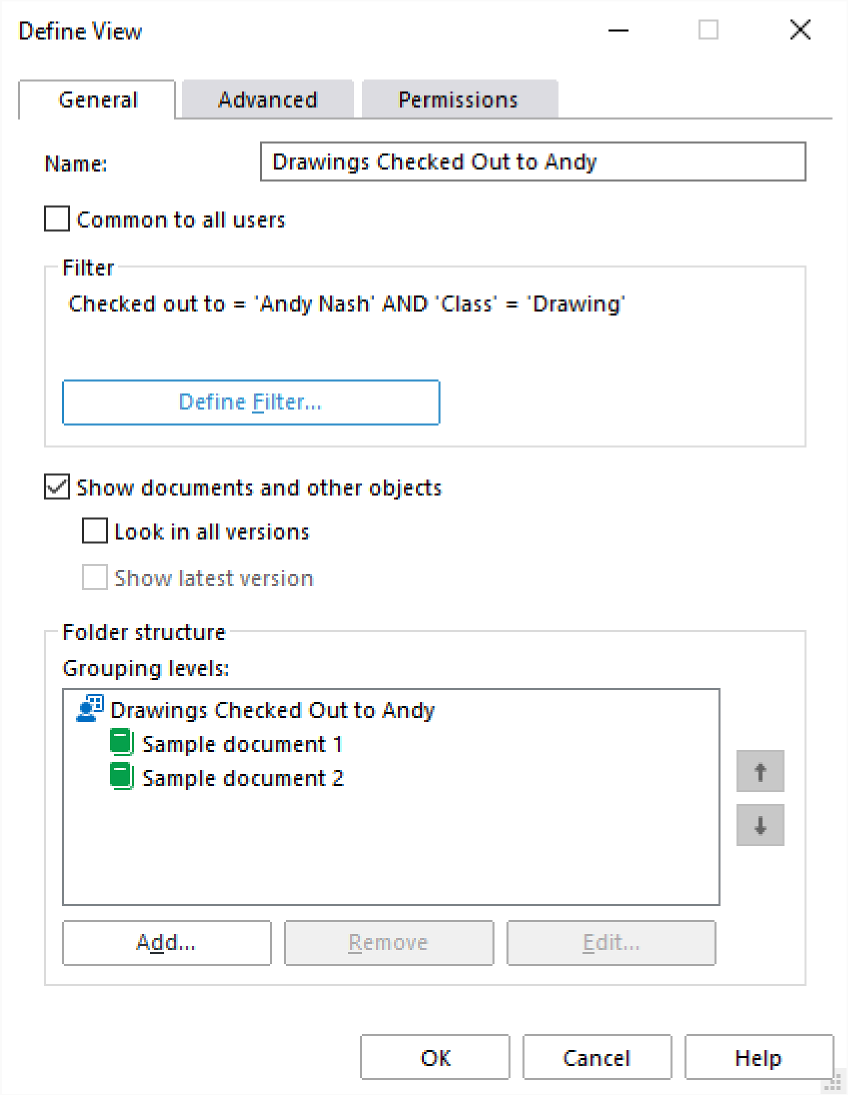
To create a view:

1. In M-Files, open the document vault to which you want to create the view.
2. Click the **Create** button and select **View**.

   The **Define View** dialog is opened.

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 defining search criteria.
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.



Define View

General | Advanced | Permissions

Name: Drawings Checked Out to Andy

□ Common to all users

Filter

Checked out to = 'Andy Nash' AND 'Class' = 'Drawing'

☑ Show documents and other objects

□ Look in all versions

□ Show latest version

Folder structure

Grouping levels:

- Drawings Checked Out to Andy
  - Sample document 1
  - Sample document 2

Figure 9: 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*. No properties have been added to the display hierarchy in this window, so all documents that meet the criteria are displayed in a single list.

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. You can also set the view to be a common view visible to all vault users. To create a common view, your user account must have permissions to manage common views or the **Full control of vault** rights.

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.

Defining the filter

See Defining a Filter for a View.

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.

Folder structure

See Grouping Levels.

In this chapter

Defining a Filter for a View

The filter settings for a view use the same filters that are used for searches. With the settings, you can specify the conditions to use for the view. You can specify criteria on the **Status**, **Properties**, **Files** and **Permissions** tabs of the **Define Filter** dialog.

For more information about the available search filters, see Status-Based Conditions, Property-Based Conditions, File Information Based Conditions, and Permissions-Based Conditions.

Grouping Levels

When you create a view that contains documents or other objects, you can use properties to further group objects in the view. For example, you can create a view that shows documents grouped in folders by customers.

To define a grouping level for a view:

1. In the classic M-Files Desktop, do one of these steps:

   a. Right-click a view for which you want to define a grouping level and select **Properties**.

      or

   b. To define a new view, click the **Create** button and select **View**. For more instructions, see Creating a View.

2. In the **Properties** dialog of the view, in the **Folder structure** section, complete one of these steps:

   a. Select a grouping level in the **Grouping levels** list and click **Add** to create a new grouping level.

      or

   b. Select an existing grouping level and click **Edit** to edit the selected grouping level.

   ✓ The **Define Grouping Level** dialog is opened.

3. Use the **Group by** drop-down menu to select the object type, value list, or function by which you want to group objects on the selected level.

4. Optional: If you selected an object type for grouping the selected level, you can click **Define Filter** to specify the conditions for including folders in the grouping level. For more information on defining the conditions, see Status-Based Conditions, Property-Based Conditions, File Information Based Conditions, and Permissions-Based Conditions.

5. If you selected an object type for grouping the selected level, use the **Reference direction** option to select the metadata reference direction between the object type of the grouping level and the objects in the view:

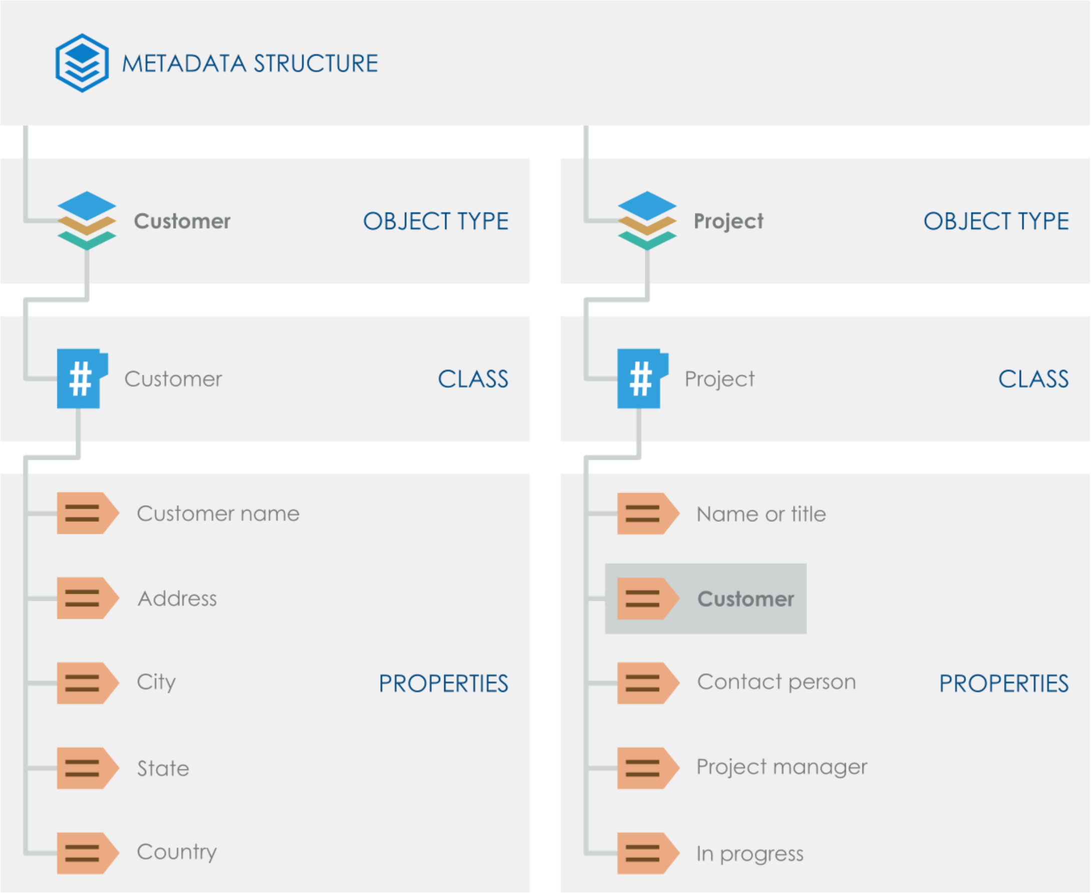
   a. **To <selected object type>**: The objects in this view have metadata that refer to the object type used as the grouping level. In other words, the reference direction is from the objects in the view **to** the object type used as the grouping level (see the example further below).

      or

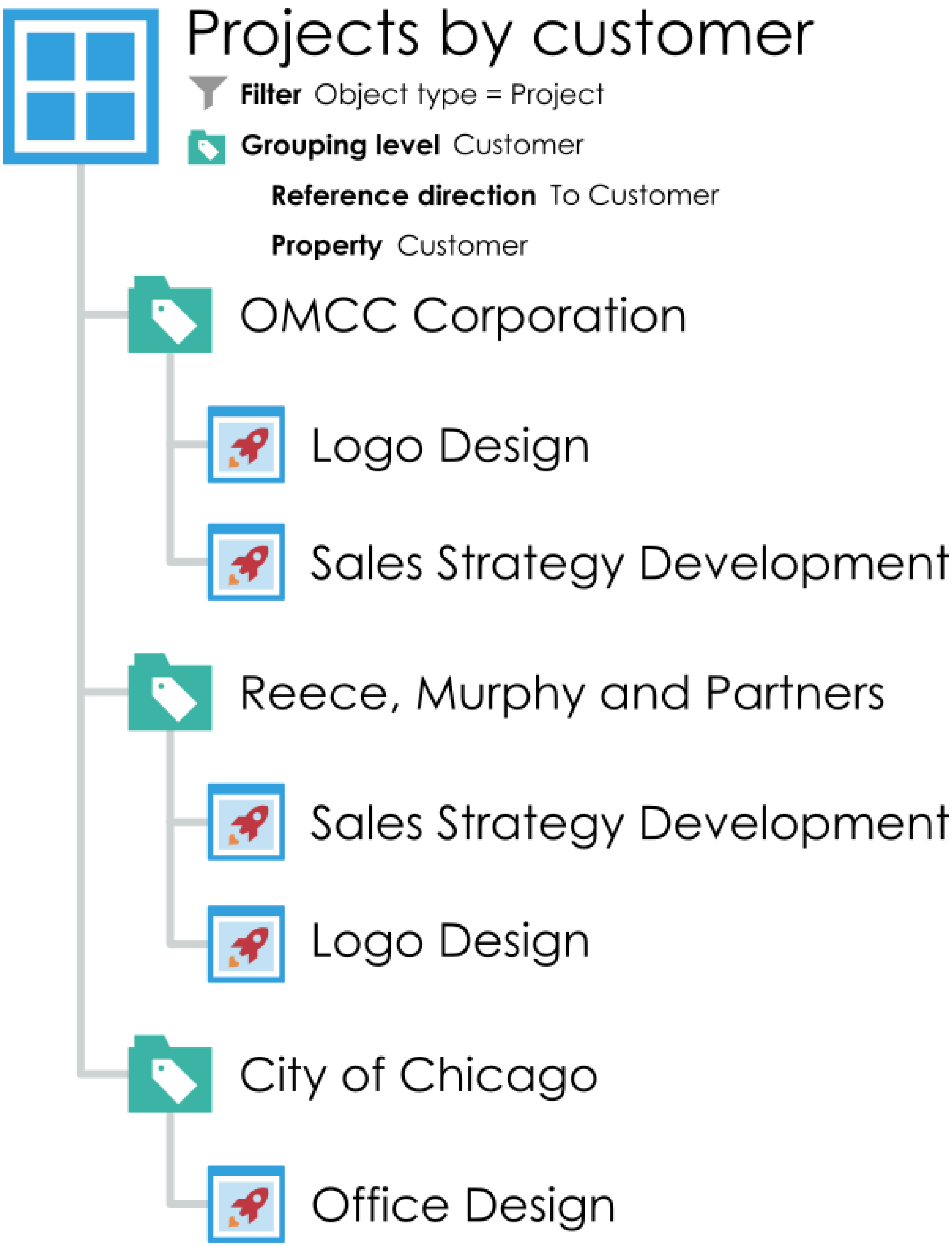
   b. **From <selected object type>**: The object type used as the grouping level has metadata that refers to the objects in this view. In other words, the reference direction is to the objects in this view **from** the object type used as the grouping level. This option is used when the objects in the view do not have metadata references to the object type used for grouping the view (see the example further below).

   Note: Views and virtual folders that use property references of the **From <selected object type>** type cannot be marked for offline availability.

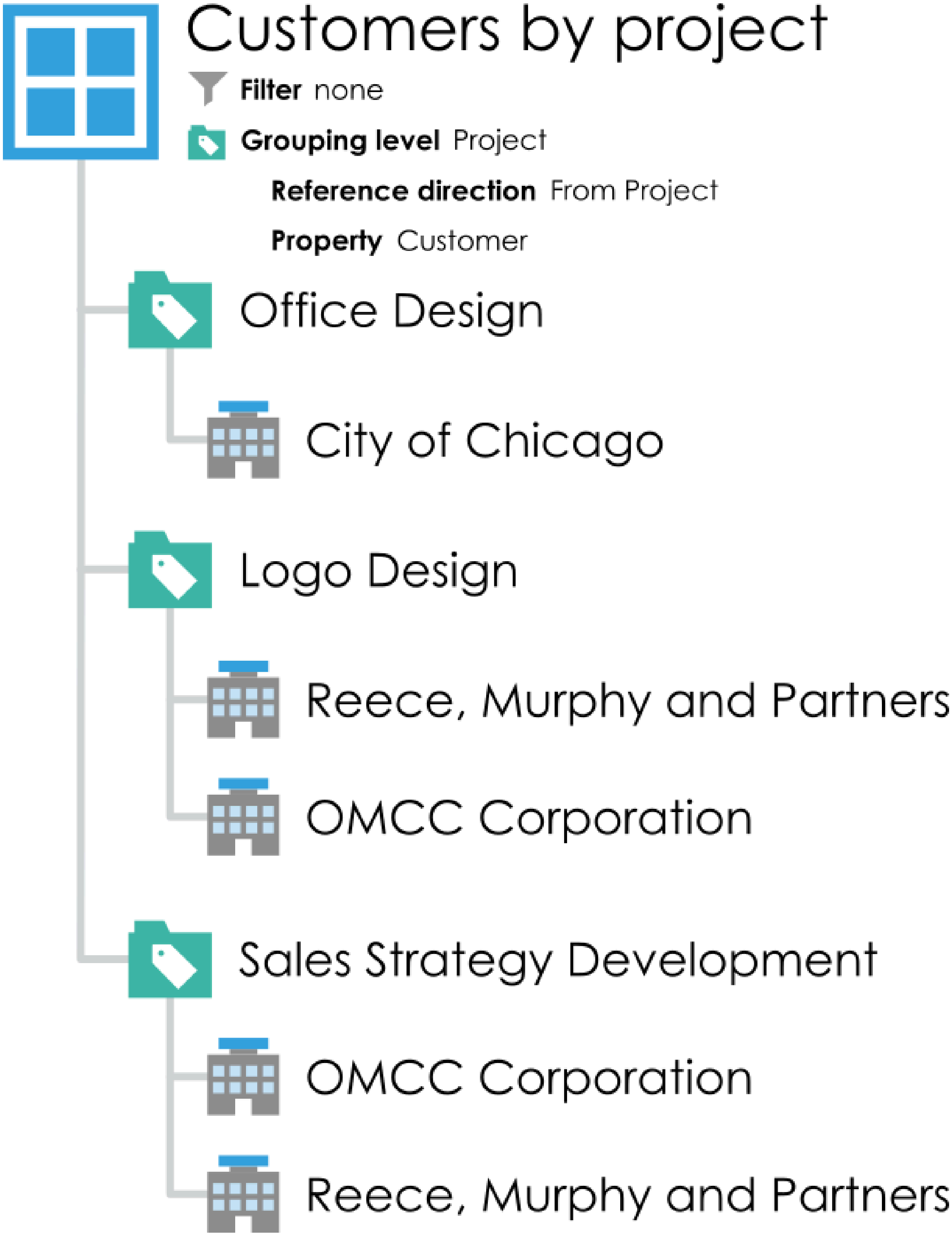
   The **Reference direction** selection is dependent on the metadata structure of the vault. As an example, take a look at this graphical representation of a simple vault metadata structure:



Say that you want to have a view that contains **projects grouped by customers**. You would then filter the view by the *Project* object type and add the *Customer* object type as a grouping level with **To Customer** as the reference direction because the *Project* objects in the view refer **to** the object type used for grouping the view (*Customer*).


Projects by customer
Filter Object type = Project
Grouping level Customer
Reference direction To Customer
Property Customer
OMCC Corporation
Logo Design
Sales Strategy Development
Reece, Murphy and Partners
Sales Strategy Development
Logo Design
City of Chicago
Office Design

On the other hand, say that you want to have a view that contains **customers grouped by projects**. The first thing to note here is that the *Customer* object type does not have any metadata information about projects (as seen in the metadata structure image further above). This means that the reference direction needs to be **from** the grouping object type, *Project*, to the *Customer* objects. So, in this scenario, you would add the *Project* object type as a grouping level with **From Project** as the reference direction, and select *Customer* as the property used by the grouping level object type. Filtering the view separately in this instance is not necessary because the *Customer* property selected for the grouping level filters the view to contain only customers.



Note: If you would like to disable the **Reference direction** setting in the vault, see Disabling the Reference Direction Setting for Grouping Levels.

6. Use the **Property** drop-down menu to select the property that is utilized by the item selected in the **Group by** drop-down menu. This selection defines the property that you want to group by on this grouping level.

7. Optional: If you selected **IntegerSegment()** in the **Group by** drop-down menu and a property of the **Number (integer)** or **Number (real)** data type in the **Property** drop-down menu, in the **Segment size** field, define a segment size that you want to group objects by on the selected grouping level.

   If you set, say, 10 as the segment size, objects are grouped into virtual folders by segments 0-9, 10-19, 20-29, and so on. If you set 100 as the segment size, objects are grouped by segments 0-99, 100-199, 200-299, and so on.

8. Optional: Check the **Show empty folders** check box if you want to include empty virtual folders on this grouping level, that is, virtual folders that do not contain any objects because the object on which the virtual folder is based is not referenced by any other object or it does not refer to any other object in the view.

9. Optional: Check the **Show objects that have an empty value for this property** check box if you want to include on this grouping level objects that do not have a value for the property selected in the **Property** drop-down menu as the grouping property, and then select either:

   a. **Show objects on this level**: Select this option if you want to list within the grouping level the individual objects that do not have a value for the selected grouping property.

      or

   b. **Show objects in a separate folder**: Select this option if you want to list objects that do not have a value for the selected grouping property in a separate folder in the grouping level. In the **Folder name** field, enter the name of the folder under which such objects are listed.

10. Optional: Open the **Advanced** tab to modify the performance options for viewing and accessing the virtual folders in this grouping level. Modifying these settings may be beneficial for views or virtual folders that contain a large number of folders. For more information, see Grouping Level Advanced Options.

11. Click **OK** to finish creating the grouping level.

The objects in the selected view are now grouped by the grouping level that you have just defined.

In this chapter

- Grouping Level Advanced Options
- Grouping Options in the classic M-Files Desktop

Grouping Level Advanced Options

The **Advanced** tab of the grouping level settings contains performance options for viewing and accessing virtual folders. Modifying these settings may be beneficial for views or virtual folders that contain a large number of folders.

Show only subfolders that were recently selected by the user

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 instance, 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.

Important remarks

- The set of folders selected for each grouping level is cleared when the user session ends. In other words, the folders need to be reselected, for instance, after the user logs out from the vault.
- The setting is specific to each grouping level.
- Folder limitation can be used if the grouping level is specified on the basis of a property that utilizes a value list.
- For common views, folder limitation can be specified by a user with at least the right to manage common views.

Other performance options

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

Activate the **Do not check object permissions for hiding subfolders** option to improve browsing performance. This may, however, cause empty folders to be displayed in the listing.

Grouping Options in the classic M-Files Desktop

You can add, change, or remove grouping levels directly in the classic M-Files Desktop. To do this:

1. In the classic M-Files Desktop, open a view.
2. Right-click an empty space in the listing area.
3. Do one of these options:

Objective	Instructions
Add a grouping level to a view that does not yet have any grouping defined	**a.** Open the **Group By** menu. **b.** Select the grouping level from the list of choices or select **Define** to define your own.
Add an additional grouping level to a view	**a.** Open the **Add Grouping Level** menu. **b.** Select the grouping level from the list of choices or select **Define** to define your own.
Change the current grouping level	**a.** Open the **Current Grouping Level** menu. **b.** Select a new grouping level to replace the current one or select **Define** to create a new grouping level.
Remove the current grouping level	**a.** Select **Remove Current Grouping Level**.

4. Optional: If you want to categorize the objects or virtual folders alphabetically, right-click an empty space in the listing area and select **Group by First Letter(s)** or **Group Folders by First Letter(s)**.

For the **Group by First Letter(s)** command to work, the **Allow this property to be used as a grouping level in views** option of the **Name or title** property has to be enabled.

View Advanced Settings and Permissions

In the **Advanced** tab of the **Define View** dialog, you can specify these settings:

- Set whether a subview of a virtual folder is shown in other virtual folders of the same level.
- Set M-Files to index the view to make it faster to use.
- Set searches in the view to be done for the content of the view only.

Visibility setting of subviews in virtual folders

You can set a view created in a virtual folder to be shown in that virtual folder only or in all virtual folders of the same level. See Creating a View in a Virtual Folder for instructions on how to create views in virtual folders. This setting is shown only for views in virtual folders.

Note: If the same level contains views and virtual folders, views created in the virtual folders are not shown in the views of the same level.

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 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.

Setting searches to be done within the view

With the **Search within this view by default**, you can specify that searches done in this view are normally done for the content of the view only. Users can still use the **View** setting on the **Filters** tab to change the searches to be done in the entire vault instead.

Sorting objects across all pages

The objects of the view can be shown on many pages. The **Sort objects across all pages** setting specifies whether the objects are sorted across the page open in the listing area or across all the pages.

Permissions tab

In the **Permissions** tab of the **Define View** dialog, you can specify the users who can see the view. The tab is shown for common views.

Creating a View in a Virtual Folder

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

Note: When you create 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.

Converting a Virtual Folder into a View

Virtual folders can also be converted into views in 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, created on the basis of the **Memo** virtual folder, you can group documents according to meeting types.

Note: 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 converted into a view can be restored as a folder by right-clicking it and selecting **Remove Folder Customization** from the context menu.

Example: Creating a New View for French Customers

1. Go to a vault with the classic M-Files Desktop.
2. Click the **Create** button and select **View**.

   ✓ The **Define View** dialog is opened.
3. In the **Name** field, enter the name `French customers`.

   The name will appear in the listing area under **My Views**.
4. Optional: Check the **Common to all users** check box if you want to define this view as a common view.
5. Click **Define Filter** to specify the conditions that objects must meet to be shown in this view.

   ✓ The **Define Filter** dialog is opened.
6. 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.
7. Go to the **Properties** tab.
8. 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.
9. Click **OK** to close the **Define Filter** dialog and to return to the **Define View** dialog.

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

11. Click **OK**.

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. Go to a vault with the classic M-Files Desktop.

2. Click the **Create** button and select **View**.

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

3. In the **Name** field, enter a descriptive name for the view.

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

4. Check the **Common to all users** check box.

5. Click the **Define Filter** button.

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

6. Go to the **Properties** tab.

7. 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.

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

9. 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.

Traditional Folders

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. They can be used to organize content or import files to M-Files.

Organizing Content with Traditional Folders

In the classic M-Files Desktop, it is possible to create traditional folders in some views opened through the **Browse relationship** feature. If your M-Files administrator has enabled this feature, you can double-click a non-document object to open the related objects in the listing area. For example, double-clicking a customer to see their projects and then double-clicking a project to see the project documents.

With traditional folders, you can create a custom structure for this type of view to simplify daily tasks especially when there is a large number of objects. The traditional folders are visible to all users who double-click the non-document object, such as a project or customer.

To create a content structure with traditional folders:

1. In the classic M-Files Desktop, open a view that supports the double-click functionality. If the view has many levels, double-click the next grouping levels or views to see the contents.
2. Double-click a non-document object, such as a project or customer. Repeat this until the objects that you want to organize in folders are shown.
3. Right-click an empty space in the listing area and select **New Traditional Folder**.
4. Enter a name for the traditional folder.
5. Drag and drop objects to the traditional folder.
6. Repeat steps from 3 to 5 until you are ready with the content structure.

To move an object to another traditional folder:

7. In the traditional folder, right-click the object and select **Remove from This Folder**.
8. In the confirmation dialog that is opened, click **Yes**.
9. Go to the view level that has the traditional folders. The object that you removed from the folder is shown here.
10. Drag and drop the object to another traditional folder.

> **Note:** The objects in a traditional folder must match the view conditions to be shown in the folder. If an object no longer meets the view conditions, it is not visible in the traditional folder.

Creating a Traditional Folder to Import Files

Traditional folders allow you to keep the original folder structure of the imported files.

To create a traditional folder for this purpose:

1. In the classic M-Files Desktop, press Alt to show the menu bar.
2. Select **Create** > **Traditional Folder**.
3. Optional: Right-click the traditional folder 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 to import files and folders to M-Files. For instructions, see Saving Folders to M-Files.

View-Specific Operations

This page contains information about different view-specific commands and features.

Using the Clean View, Hide View, and Unhide Views commands

Clean View is a command available for all views in the classic M-Files Desktop. It removes temporary local files and all empty folders. To do this, right-click a view and select **Clean View**.

Some views cannot be removed but can be hidden. For example, most vault users do not have rights to remove common views. To hide a view, right-click it and select **Hide View**. To unhide views, right-click an empty space in the listing area and select **Unhide Views**.

Tip: You can create a view that shows all deleted objects if you have any of these permissions: **Full control of vault**, **Permission to see all objects**, or **Permission to see deleted objects**. Create a view with the filter `Deleted = Yes` (see Status-Based Conditions).

Saving the display settings of a view as common display settings

M-Files allows you to save the display settings of a view 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.

To do this, press Alt and select **View** > **Save As Common Display Settings**.

Resetting the display settings to their defaults

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.

To do this, right-click an empty space in the listing area and select **Reset Display Settings to Defaults**.

Binding a report to a view

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

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

Exporting a view

You can export the contents of a view in the same way that you export search results. For instructions, see Exporting Search Results.

Sharing views

You can share your views with other users in the same vault. You cannot share common views. If you share a subview of a view, the filters of the view will not affect the shared subview.

To share a view, right-click a view and select **Share View by Email**. To share many views, hold down the Ctrl key and click the views that you want to share. Then right-click a selected view and select **Share View by Email**.

In both cases, a new email message is opened in your email client.

Note: The email message contains an M-Files shortcut to the view as an attachment. By default, the shortcut expires in 14 days. To change the default expiration time, contact your M-Files administrator.

2.6. User Settings

This section contains information about different settings available for users.

In this chapter

2.6.1. M-Files Desktop Settings

M-Files Desktop Settings let you add, edit, remove, and test vault connections. Additionally, on the **Settings** tab, you can edit options related to the user- and computer-specific behavior of the client software.

Before you set up your vault connection, your M-Files system admin must have set up the M-Files system and the vault.

To open M-Files Desktop Settings:

1. In the Windows system tray, click the M-Files icon (M) with the secondary mouse button.

   ℹ The system tray is normally in the bottom-right corner of your Windows desktop.

2. Select **Settings** > **M-Files Desktop Settings**.

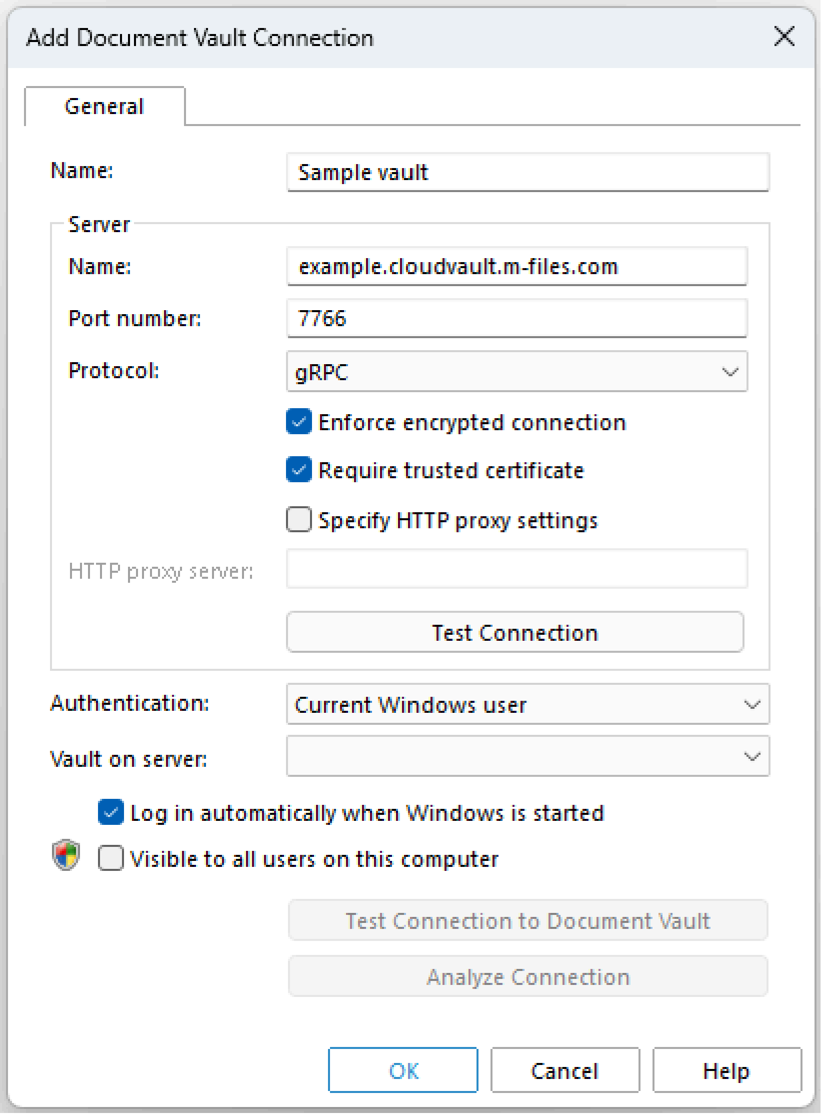
In this chapter

Adding a Vault Connection

Important information

- When you use the gRPC protocol for connections between the M-Files server and M-Files clients, a valid TLS certificate must be in use on the server for connection security and encryption. For instructions, see Managing Server Certificates.
- For RPC encryption to operate, 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.

To open the dialog for a new vault connection, click **Add** in the M-Files Desktop Settings main window.


Add Document Vault Connection
General
Server
Test Connection
Test Connection to Document Vault
Analyze Connection
OK
Cancel
Help

Name: Sample vault

Server

Name: example.cloudvault.m-files.com

Port number: 7766

Protocol: gRPC

☑ Enforce encrypted connection

☑ Require trusted certificate

☐ Specify HTTP proxy settings

HTTP proxy server:

Authentication: Current Windows user

Vault on server:

☑ Log in automatically when Windows is started

☐ Visible to all users on this computer

To create the connection, enter the necessary information to the dialog.

Name

The name of the connection can be anything, but it is a good idea to make it descriptive. The name will be shown on the `M` drive as a directory that contains the contents of the 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

Specify the port to connect to on the server. The default gRPC port for M-Files is 443.

Server/Protocol

Define the protocol to be used for the network connection. The following protocols are available:

- gRPC
- Local gRPC
- TCP/IP
- SPX
- Local Procedure Call (LPC)
- HTTPS

Enforce encrypted connection

Enable this option to secure the communication between M-Files Desktop and M-Files Server with RPC encryption.

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 the client software and M-Files Server in the organization's internal network.

The option is available for the TCP/IP and gRPC protocol. 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.

For more information on encrypted connections, refer to Protecting Data in Transit with Encryption in M-Files.

Require trusted certificate

Please ignore this setting. The setting is preparation for future capabilities. It is possible that in the future, it will be renamed or removed. In most cases the setting is inactive, but if you do disable it, TLS certificates cannot be used for encrypted connections.

Specify HTTP proxy settings

You can specify an explicit forward proxy server for vault connections that use the gRPC or HTTPS protocol. This can be necessary if all traffic in your organization must be routed through a forward proxy server.

To do this, enable the option **Specify HTTP proxy settings** and do one of these options in the **HTTP proxy server** field:

- If you selected **gRPC** as the protocol, enter the protocol, the address of the proxy server, and optionally the port number in this format: *<protocol>://<server address>*:*<port number>*. For example, `http://exampleserver.com:80`.
- If you selected **HTTPS** as the protocol, the protocol is `HTTPS` by default and you must only enter the address of the proxy server and optionally the port number in this format: *<server address>*:*<port number>*. For example, `exampleserver.com:80`.

Server / Test Connection

You can use this button to check that the 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	You can use the *Current Windows user* method to log in with your current Windows credentials.
Specific Windows user	Selecting *Specific Windows user* means that you need to enter your Windows username, password, and domain information when you log in. This option allows you to log in with a different account than the one you used for accessing Windows.
M-Files user	The M-Files authentication method allows you to log in to M-Files only. If your organization does not have a Windows domain or you do not have access to it, you should select *M-Files authentication* for logging in.

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.

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.

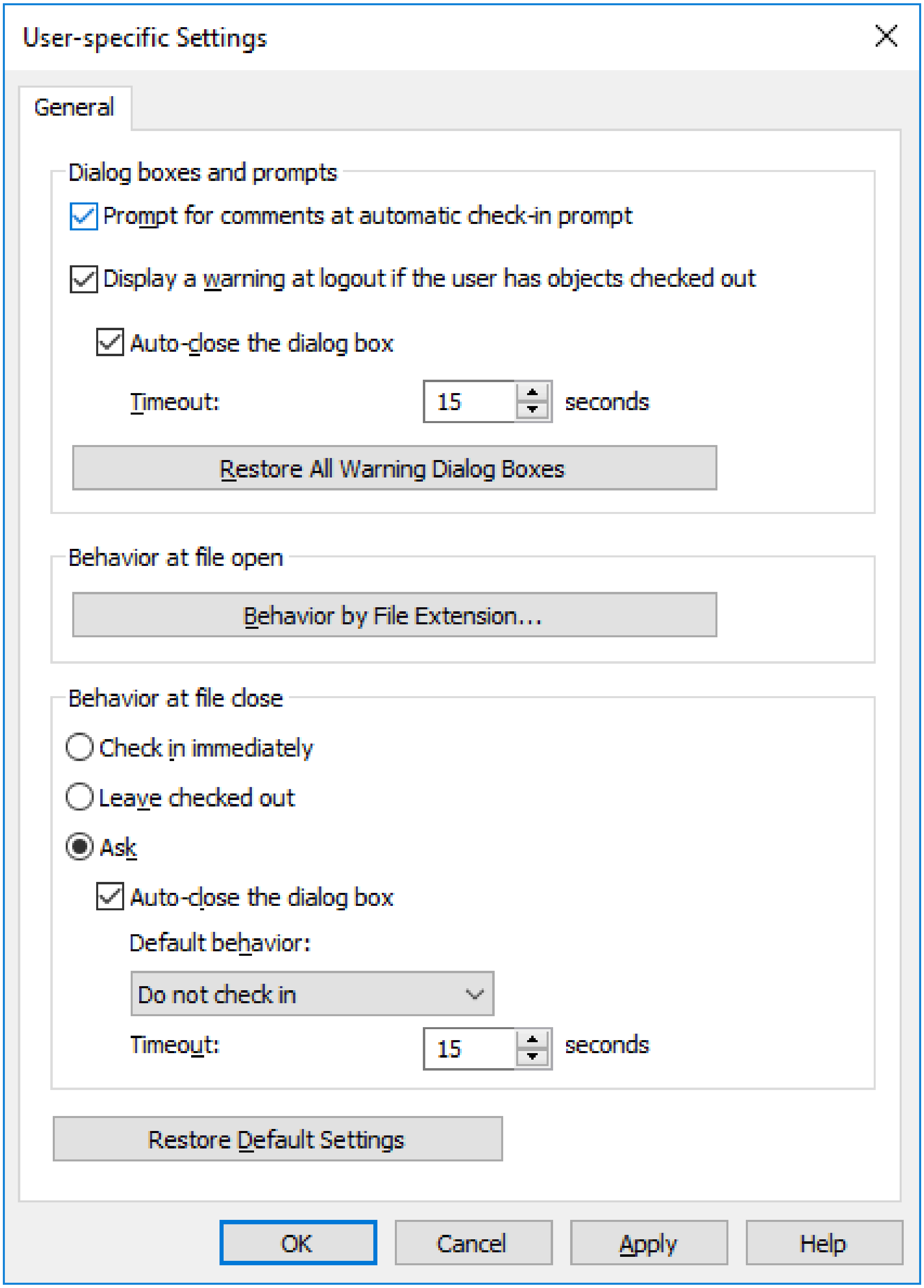
Analyze connection

When you have created the vault connection and open the **Document Vault Connection Properties** dialog by double-clicking the vault connection in the M-Files Desktop Settings dialog, you can use the **Analyze Connection** button to display further details about the connection. The analysis measures the round-trip time between the client and the server, as well as the download and upload speeds.

User-Specific Settings

These settings let you edit M-Files Desktop behavior specific to your Windows user account. To open the **User-specific Settings** dialog:

1. Open M-Files Desktop Settings.
2. Open the **Settings** tab.
3. Click **User-specific Settings**.



User-specific Settings

General

Dialog boxes and prompts

☑ Prompt for comments at automatic check-in prompt

☑ Display a warning at logout if the user has objects checked out

☑ Auto-close the dialog box

Timeout: 15 seconds

Behavior at file open

Behavior at file close

○ Check in immediately

○ Leave checked out

● Ask

☑ Auto-close the dialog box

Default behavior: Do not check in

Timeout: 15 seconds

Figure 10: 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.

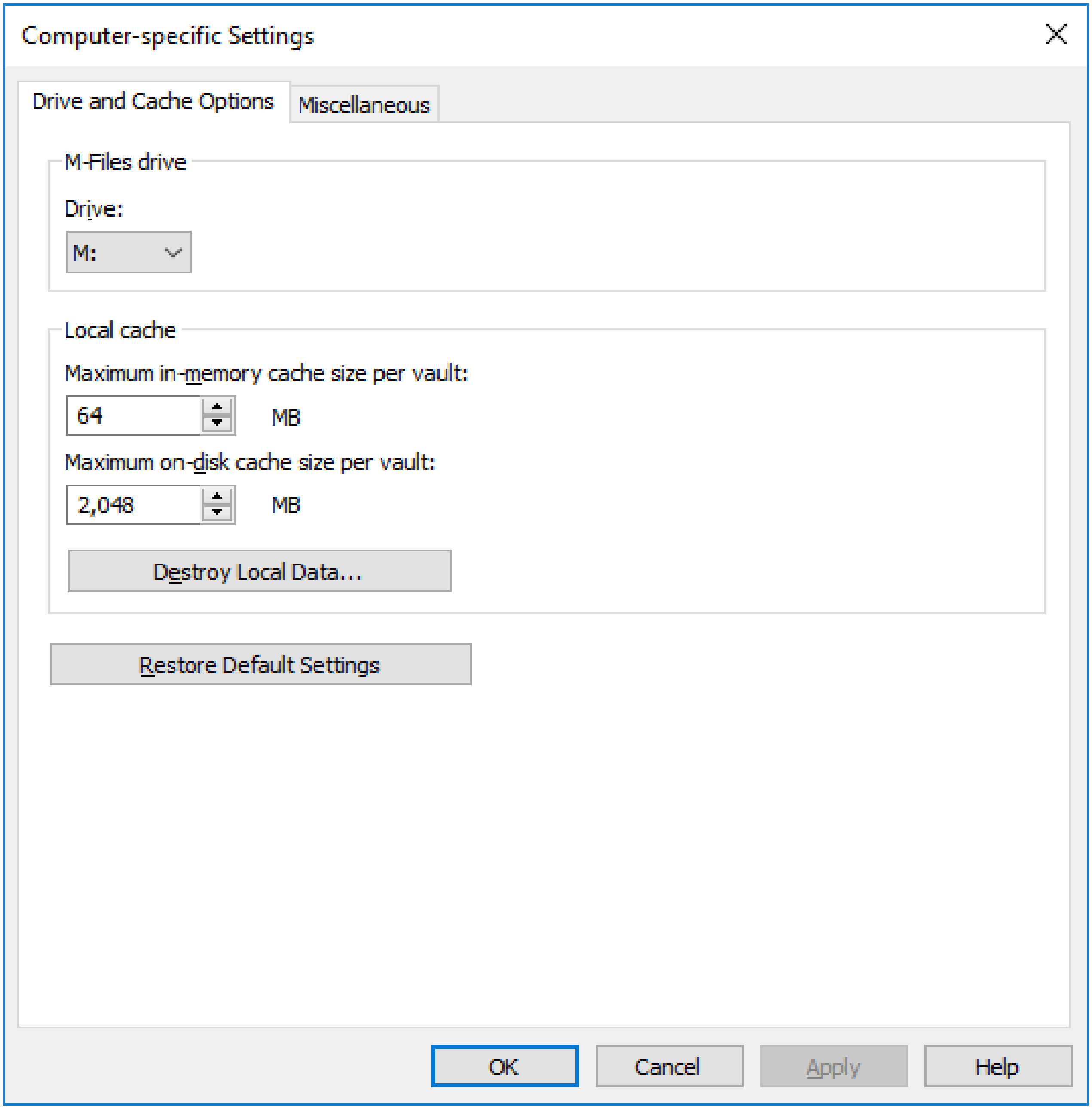
Behavior at file close

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

These workstation-specific settings allow you to change the M-Files drive letter and to control options related to the local data cache. To open these settings:

1. Open M-Files Desktop Settings.
2. Open the **Settings** tab.
3. Click **Computer-specific Settings**.



Drive: M:

Maximum in-memory cache size per vault: 64 MB

Maximum on-disk cache size per vault: 2,048 MB

Figure 11: 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 your 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.

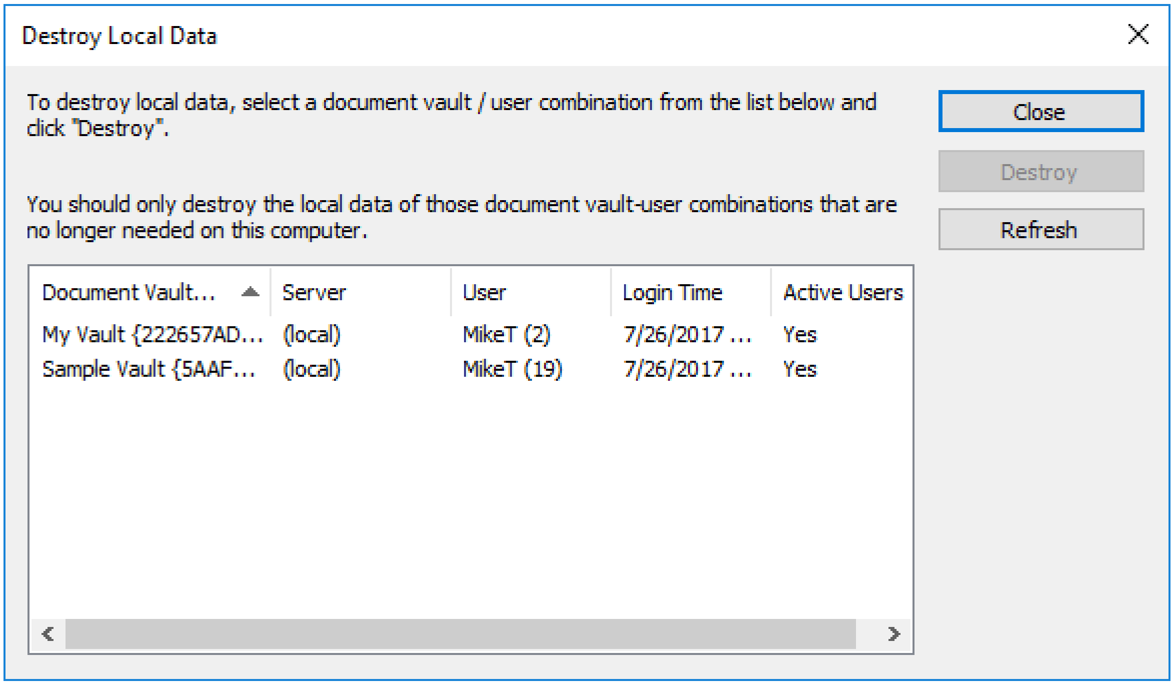
Maximum on-disk cache size per vault

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 vault contents locally in the computer 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 locally cached data by user and by document vault.

Note that the **Destroy Local Data** function may delete data that cannot be restored from the M-Files server such as currently checked-out files on your computer, offline content, and temporary local files. Therefore it is important to ensure that you have saved and checked in all the documents that you need before destroying local data.



To destroy local data, select a document vault / user combination from the list below and click "Destroy".

You should only destroy the local data of those document vault-user combinations that are no longer needed on this computer.

Document Vault...	Server	User	Login Time	Active Users
My Vault {222657AD...	(local)	MikeT (2)	7/26/2017 ...	Yes
Sample Vault {5AAF...	(local)	MikeT (19)	7/26/2017 ...	Yes

Figure 12: The local vault and user combinations are listed in the **Destroy Local Data** dialog.

Note:

If you only want to delete temporary local files and empty the metadata cache, see Clearing the Local Cache of the Vault.

The table below compares the locally cached elements that are either deleted or preserved when **Clear Local Cache** or **Destroy Local Data** is run.

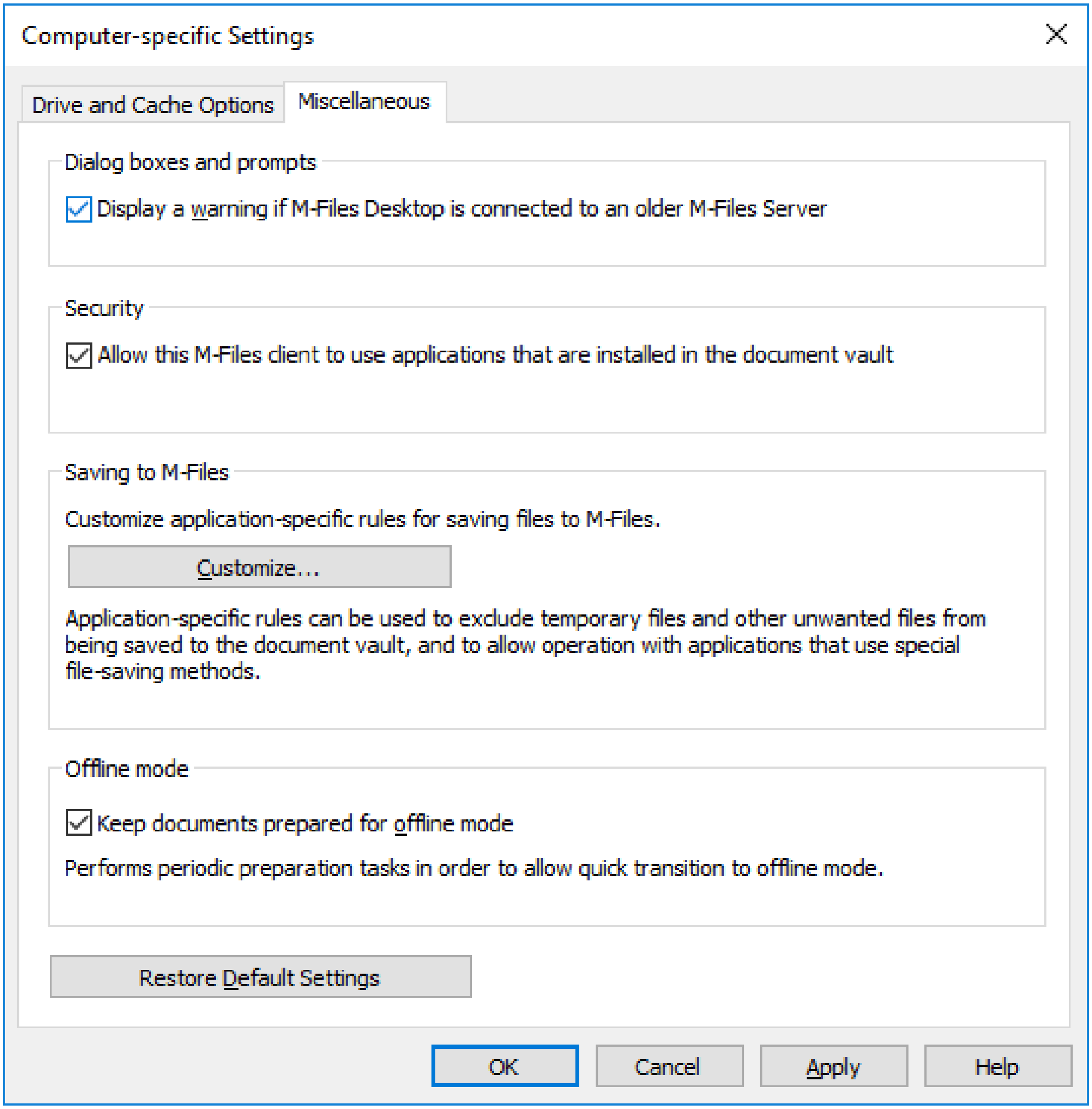
Cached content	Clear Local Cache	Destroy Local Data
Temporary local files	Optional	Delete
Metadata	Delete	Delete
Checked-out documents	Keep	Delete
Document preview data	Keep	Delete

Cached content	Clear Local Cache	Destroy Local Data
Offline content	Keep	Delete

Other Computer-Specific Settings

These workstation-specific settings let you change M-Files Desktop behavior related to dialog boxes and prompts, vault security, file saving, and offline mode. To open these settings:

1. Open M-Files Desktop Settings.
2. Open the **Settings** tab.
3. Click **Computer-specific Settings**.
4. Open the **Miscellaneous** tab.



Computer-specific Settings

Drive and Cache Options | Miscellaneous

Dialog boxes and prompts

☑ Display a warning if M-Files Desktop is connected to an older M-Files Server

Security

☑ Allow this M-Files client to use applications that are installed in the document vault

Saving to M-Files

Customize application-specific rules for saving files to M-Files.

Customize...

Application-specific rules can be used to exclude temporary files and other unwanted files from being saved to the document vault, and to allow operation with applications that use special file-saving methods.

Offline mode

☑ Keep documents prepared for offline mode

Performs periodic preparation tasks in order to allow quick transition to offline mode.

Figure 13: The **Miscellaneous** tab contains different computer-specific settings.

Dialog boxes, prompts, and security

By default, these settings are enabled:

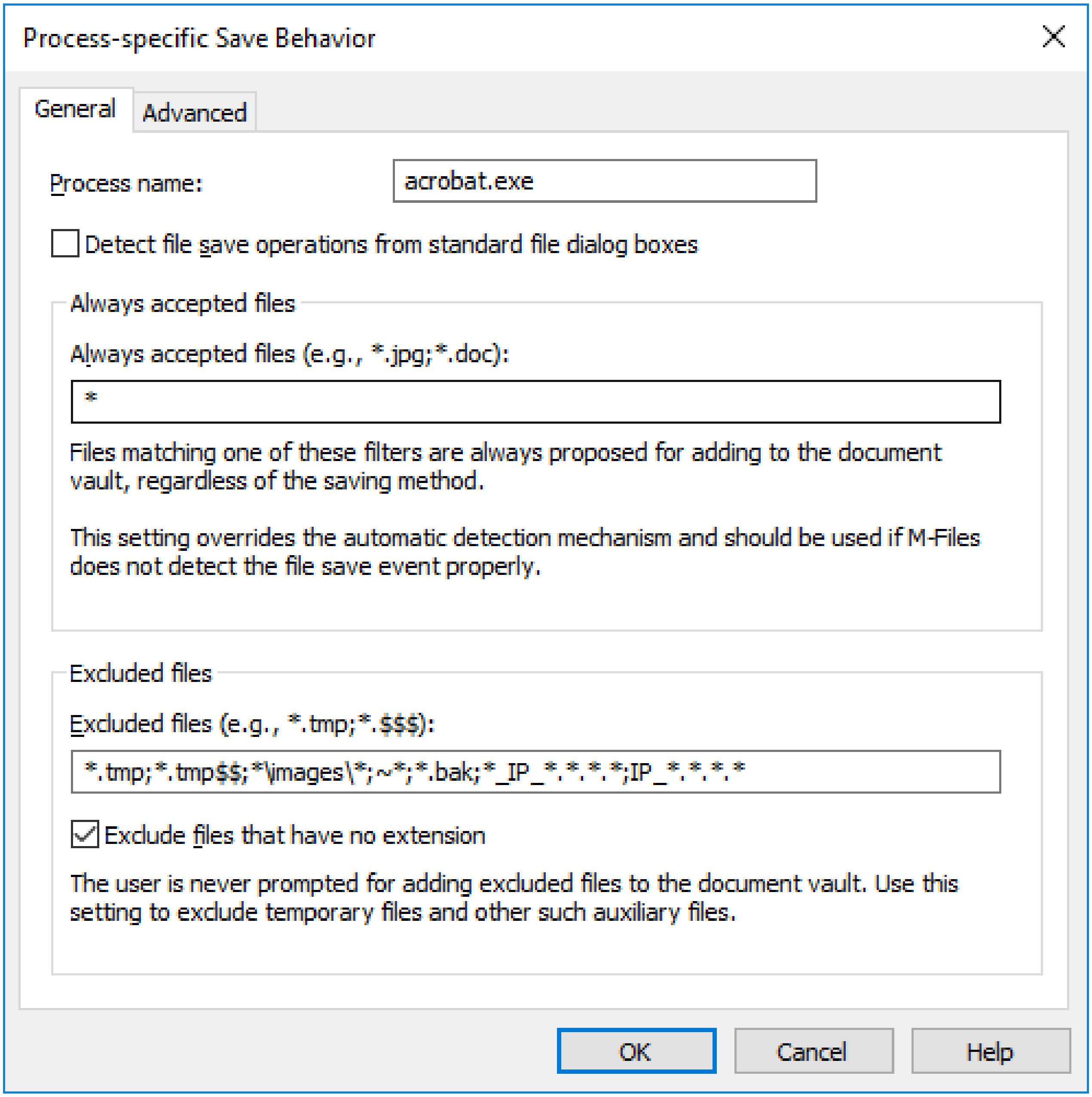
- **Display a warning if M-Files Desktop is connected to an older M-Files Server**
- **Allow this M-Files client to use applications that are installed in the document vault**

Saving to M-Files

In this section, 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 vault. Rules can also be used to allow operation with applications that use special file saving methods. The rules make sure that, for example, a metadata card of new files is displayed if automatic identification does not function.

Process-specific Save Behavior

Click first **Customize** and then **Add** to add a new rule. The **Process-specific Save Behavior** dialog is opened.



Process-specific Save Behavior

Process name: acrobat.exe

☐ Detect file save operations from standard file dialog boxes

Always accepted files

Always accepted files (e.g., *.jpg;*.doc):

*

Files matching one of these filters are always proposed for adding to the document vault, regardless of the saving method.

This setting overrides the automatic detection mechanism and should be used if M-Files does not detect the file save event properly.

Excluded files

Excluded files (e.g., *.tmp;*.$$$):

.tmp;.tmp$$;*\images*;~*;*.bak;*_IP_*.*.*.*;IP_*.*.*.*

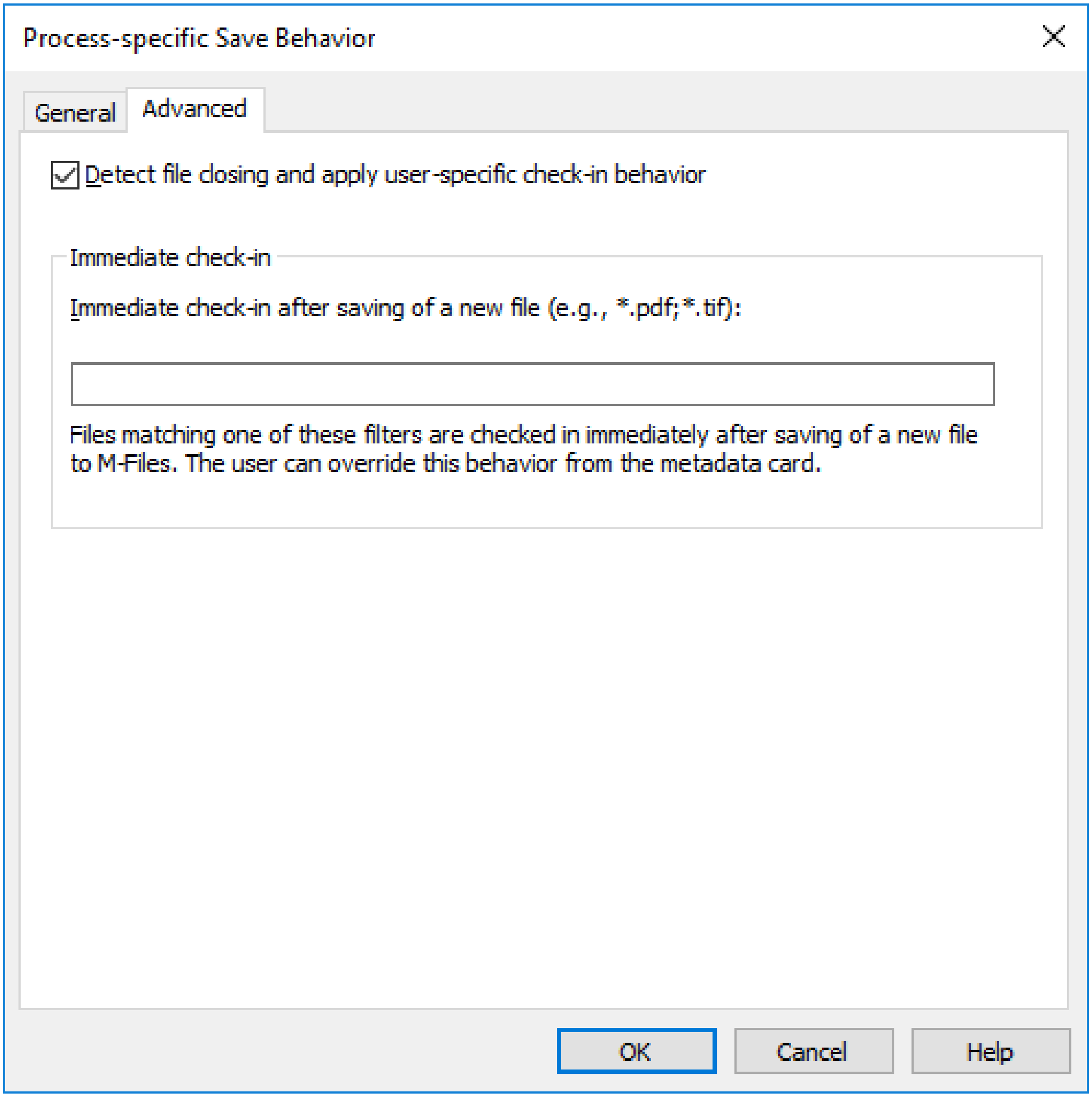
☑ Exclude files that have no extension

The user is never prompted for adding excluded files to the document vault. Use this setting to exclude temporary files and other such auxiliary files.

Figure 14: General process-specific settings.

On the **General** tab, you can enable or disable the setting **Detect file save operations from standard file dialog boxes**. By default, the setting is enabled.

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



☑ Detect file closing and apply user-specific check-in behavior

Immediate check-in

Immediate check-in after saving of a new file (e.g., *.pdf;*.tif):

Files matching one of these filters are checked in immediately after saving of a new file to M-Files. The user can override this behavior from the metadata card.

Figure 15: Advanced process-specific settings.

On the **Advanced** tab, you can enable or disable the setting **Detect file closing and apply user-specific check-in behavior**. By default, the setting is enabled.

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.

Offline mode

By default, the documents are kept ready for the offline state for a quick transition to the offline mode. When the computer-specific setting **Keep documents prepared for offline mode** is enabled, M-Files downloads the necessary objects at specified intervals. Disable the setting if you do not use the offline mode or the feature causes additional load for the machine.

Exporting Vault Connections and Settings

Vault connections and settings can be exported to a Windows registry file. By running the exported registry file on other computers, you can use the same M-Files configuration data on several computers.

To export vault connections and settings:

1. Open M-Files Desktop Settings.
2. Open the **Settings** tab.
3. In the **Export** section, select the components that you want to export by checking the appropriate check boxes.
4. Click the **Export** button.

   ☑ The **Save As** dialog is opened.
5. Specify the target location and file name for the REG file.
6. Select **Save**.

The settings for the components of your choice are saved to a REG file and stored to the location that you defined in the **Save As** dialog.

2.6.2. Setting Your Home Tab

You can change the tab that the classic M-Files Desktop opens when you go to a vault or click the M-Files logo in the top area.

To set your home tab:

1. Click your username in the upper right corner.
2. Click **User Settings** > **Home Tab**.
3. Select the home tab.

2.6.3. Setting Default Tab for Object

In the right pane, the Metadata tab, the Document Preview tab, or both are shown when you click an object. You can set the default tab in the classic M-Files Desktop.

To open the **Default Tab for Object** setting:

1. Click your username in the upper right corner.
2. Click **User Settings** > **Default Tab for Object**.
3. Select one of these options:

Select the option...	If you want to...
Automatic Selection	See the same tab that you viewed the previous object with. If there is no preview available for the object, the metadata card is shown.

Select the option...	If you want to...
Metadata and Preview	See the metadata card and the preview of the object when you click an object. If there is no preview available for the object, the preview tab is empty.
Metadata	See the metadata card of the object when you click an object.
Preview	See the preview of the object when you click an object. If there is no preview available for the object, the metadata card is shown.

2.6.4. Editing Notification Settings in the Classic M-Files Desktop

You can set M-Files to inform you by email about some events, for example changes made to objects. This can be useful when you want to keep track of modifications made to a specific document.

Note: You must have read permissions to an object to get notifications about it.

Note: To use this feature, event logging and notifications must be enabled on the M-Files server. For more information about server settings, see Editing Notification Settings in M-Files Admin.

To open the **Notification Settings** dialog, click your username in the upper right corner and select **User Settings** > **Notification Settings**.

Unselect **Enable notification messages** to disable your notification rules.

Note: Your M-Files system administrator can set specified notification messages to be sent to all users. This means that you can get some notifications, for example, for assignments even if you have disabled notification messages.

Creating a new notification rule

Click **Add** in the **Notification Settings** dialog to open the **New Notification Rule** dialog.

Give the rule a name. Under **Notification sent**, select **When a selected event occurs** or **When object matches the conditions of the filter**. The content of the dialog changes based on your selection.

Message delivery

Select one of the message delivery options explained in the table below.

Option	Description
Notification messages disabled	Select this option to disable notification messages.

Option	Description
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:** This option is not available if you selected **When object matches the conditions of the filter** under **Notification sent**.
A digest message once a day	Select this option to be informed of events with a digest message once a day. If you selected **When object matches the conditions of the filter** under **Notification sent**, select the days on which you wish to receive the digest message. The time when the message is sent is set by the system administrator in M-Files Admin. For more information, see Editing Notification Settings in M-Files Admin.

Notification recurrence

Select whether you want to get a notification for an object only once or on each day that you selected in **Message delivery**. The selection is available only if you selected **When object matches the conditions of the filter** under **Notification sent**.

Filter

Define a filter. The filter determines the group of objects to which the notification rule applies. For more information about filters, see Defining a Filter for a View.

Event subscriptions

If you selected **When a selected event occurs**, select the check box for all the events for which you want a notification message.

Exclude notifications of events caused by the current user

Select this option if you do not want to be informed of events caused by yourself, such as modifications that you have made to an object. This option is available only if you selected **When a selected event occurs** under **Notification sent**.

Private and common rules

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, see **Manage common views and notification rules** in this table.

Recipients

Specify the users or user groups who will receive notifications on the basis of this rule.

Enabling push notifications for the M-Files mobile apps

To enable push notifications for M-Files Mobile, see Setting Up Push Notifications for the M-Files Mobile Apps.

In this chapter

- Example: Daily Notifications for New Orders
- Example: Reminder Messages for Contracts

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 use this feature, event logging and notifications must be enabled on the M-Files server. For more information about server settings, see Editing Notification Settings in M-Files Admin.

1. Open the classic M-Files Desktop.

2. Click your username in the upper right corner.

3. Click **User Settings** > **Notification Settings**.

✓ The **Notification Settings** dialog is opened.

4. Click the **Add** button.

5. In the **Name** field, give your rule a name, such as *New orders*.

6. In **Notification sent**, select **When a selected event occurs**.

7. In **Message delivery**, select **A digest message once a day**.

8. Click the **Define Filter** button.

9. Open the **Properties** tab.

10. Click **Add Condition**.

11. For the newly added property condition, select *Class* as the property, = as the operator, and *Order* as the value.

12. Click **OK**.

✓ The property condition *'Class'* = *'Order'* is now shown in the **Filter** field of the **Notification Rule Properties** dialog.

13. Enable notifications for the event *New document or other object*.

14. 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**.

15. When you are done, click **OK**.

The new notification rule is added to the list in the **Notification Settings** dialog.

Example: Reminder Messages for Contracts

This example shows how you can create a common notification rule for contracts that have their deadline in 30 days. You will be notified every day starting 30 days before the deadline until the deadline is met.

Note: To use this feature, event logging and notifications must be enabled on the M-Files server. For more information about server settings, see Editing Notification Settings in M-Files Admin.

1. Open the classic M-Files Desktop.
2. Click your username in the upper right corner.
3. Click **User Settings** > **Notification Settings**.

   ✓ The **Notification Settings** dialog is opened.
4. Click the **Add** button.
5. In the **Name** field, give your rule a name, such as *Contract reminder*.
6. In **Notification sent**, select **When object matches the conditions of the filter**.
7. In **Message delivery**, select **A digest message once a day**.

   All days of the week are selected by default.
8. In **Notification recurrence**, select **Notify of each matching object repeatedly**.
9. Click the **Define Filter** button.
10. Open the **Properties** tab.
11. Click the **Add Condition** button three times.
12. For the first condition, select *Assignees* as the property, = as the operator, and *(current user and users for whom the current user is a substitute)* as the value.
13. For the second condition, select *Deadline* as the property, <= as the operator, *DaysTo()* as the option, and *30* as the value.
14. For the third condition, select *Deadline* as the property, > as the operator, *DaysTo()* as the option, and *0* as the value.

    If you do not set this condition, you will get notifications also after the deadline.
15. Click **OK**.

    ✓ The property condition *'Assignees' = '(current user and users for whom the current user is a substitute)' AND DaysTo('Deadline') <= 30 AND DaysTo('Deadline') > 0* is now shown in the **Filter** field of the **Notification Rule Properties** dialog.
16. When you are done, click **OK**.

The new notification rule is added to the list in the **Notification Settings** dialog.

2.6.5. Managing Vault Applications in the Classic M-Files Desktop

Various third-party applications can be used for modifying and extending client and server behavior. Information on how to manage and install the applications is available for admins in Installing and Managing Vault Applications.

Managing the vault applications

After a vault-specific client application has been installed with M-Files Admin, it is available for end users. When you log in to the vault, M-Files asks 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.

To manage computer-specific client applications in the classic M-Files Desktop, press Alt and select **Settings** > **Applications** in the menu bar.

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. Click **Computer-specific Settings**.
4. Select the **Miscellaneous** tab.
5. Enable or disable the application setting under the **Security** heading.

2.6.6. 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. For step-by-step instructions on how to assign yourself a substitute user, see Appointing a Substitute User.

Assignments and user permissions

Assignment and document permissions may differ. 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 (see License type)

For more information about assignments, see Creating and Completing Assignments.

Assignment notifications

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.

Viewing assignments

You can see all the tasks assigned to you in the **Assigned to Me** view. To open it, click the **Assigned** tab in M-Files Desktop or M-Files Web.

In this chapter

- Appointing a Substitute User

Appointing a Substitute User

1. Click your username in the upper right corner.
2. Click **User Settings** > **Substitute Users**.

   ✓ The **Substitute Users** dialog is opened.
3. Click **Add** to select the substitute user or users.

   ✓ The **Select Users** dialog is opened.
4. Select the preferred user or users and click **Add**.

   You can select more than one item at once. Hold down the Ctrl key to select multiple individual items or hold 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.
5. 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.

2.6.7. Changing the Software and Vault Language

You can change the M-Files software and vault language. For a list of the supported software languages, see Language Versions of the M-Files Software. For instructions on how your vault admin can create vault localizations, see Translating the Metadata Structure.

To change the software and the vault language in the classic M-Files Desktop:

1. Click your username in the upper right corner.
2. Click **User Settings** > **Change Language**.

   ✓ The **Change Language** dialog is opened.
3. Use the **Software language** drop-down menu to change the language of the M-Files user interface.
4. 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.
5. Click **OK** to change the languages and to close the **Change Language** dialog.

2.6.8. Changing the 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. Go to a vault with the classic M-Files Desktop.
2. Click your initials in the top-right corner of the user interface to open the user menu and select **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.

2.6.9. Clearing the Local Cache of the Vault

To remove temporary local files from a vault in the classic M-Files Desktop, press the Alt key and select **Settings** > **Clear Local Cache**.

Select the temporary local files that you want to delete and click **Delete**, or click **Delete All** to delete all temporary local files in the vault. When you click **Finish**, the metadata cache in the vault is cleared. The cache is used to store data such as property values and object references.

For instructions on converting temporary local files into documents, see Converting a temporary local file to a document.

Note:

If you want to delete all locally cached data in a vault, see Destroy local data. Note that the **Destroy Local Data** function may delete data that cannot be restored from the M-Files server such as currently checked-out files on your computer, offline content, and temporary local files.

The table below compares the locally cached elements that are either deleted or preserved when **Clear Local Cache** or **Destroy Local Data** is run.

Cached content	Clear Local Cache	Destroy Local Data
Temporary local files	Optional	Delete
Metadata	Delete	Delete
Checked-out documents	Keep	Delete
Document preview data	Keep	Delete

Cached content	Clear Local Cache	Destroy Local Data
Offline content	Keep	Delete

2.6.10. Show Status

In M-Files, objects are kept on the M-Files server and transferred to the caches of M-Files users' computers to make sure using M-Files Desktop is 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 or any reason to even check the status information.

To open the **Show Status** dialog, click the M-Files icon (M) in the Windows system tray with the secondary mouse button and select **Show Status**.

The File Transfer tab

The **Status** column in the **File Transfer** tab indicates whether the file has been transferred or is being transferred. The status is indicated as a percentage. You can stop the transfer by selecting the document and clicking **Stop**.

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

Document vault connections

On the **Document Vault Connections** tab, you can see which document vault connections are available and whether the vault is online.

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. See also Going Offline and Going Online.

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.

2.6.11. Refreshing External Objects

M-Files can 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 user interface of the external database. You can refresh data automatically in both directions.

To make sure that M-Files contains up-to-date external object information: In the classic M-Files Desktop, press Alt and select **Settings** > **Refresh External Objects**.

For more information on external objects, see Connections to External Databases for Object Types.

2.6.12. Updating M-Files

Automatic updates keep the M-Files software up to date. If a newer version of M-Files becomes available, it is downloaded and installed automatically. You can delay automatic updates for a limited time if you are working on something important when an automatic update becomes available.

Note: For the automatic updates to run, local administrative permissions on your computer are not necessary.

When a new M-Files version becomes available, you see a notification in the top area of M-Files Desktop. Click **Options** to schedule or start the M-Files software update.

The feature gets the latest update information from the update server using HTTPS on TCP port 443. This means that normally it is not necessary for you to change any firewall settings.

For information on updating M-Files manually, see Manually Updating M-Files.

Settings for automatic updates

To open the settings for automatic updates, right click the M-Files icon () in the Windows system tray and select **Settings** > **Automatic Updates**.

Note: If your M-Files system admin manages the settings for automatic updates, you cannot change them and all options are not necessarily visible.

For a high-level description on how M-Files downloads the update packages when the **Download updates automatically** option on the **Settings** tab is enabled, see Update Download Process. To make sure that your M-Files software is always up to date, do not disable automatic updates.

To check for updates manually, open the **Installation** tab and click **Check Now**. If an update package is available, it is downloaded to your computer.

Note: If automatic updates are disabled, you must have local administrative permissions on your computer to install an available update.

To disable the automatic installation of updates, open the **Settings** tab and unselect the **Install updates automatically** check box. To start the installation of available updates manually, open the **Installation** tab and click **Install**. If the **Install** button is disabled, there are no updates available for installation.

In the **Installation schedule** section of the **Installation** tab, you can select the preferred days and time of installing M-Files updates. It is recommended that you select a date and time that is outside of working hours so that installations do not interrupt M-Files operations in your organization. Note that the computer must be running and not in sleep or hibernate mode when the update is scheduled to be installed. If the computer is not running when the scheduled installation time occurs, the update is attempted to be installed or scheduled the next time the computer is started.

For more information on scheduling update installations and disabling automatic updates, see Configuring Automatic Updates with Registry Settings.

3. System Administration

This section, intended mainly for M-Files system administrators, explains how to manage, maintain, and configure the M-Files system.

This section, intended mainly to M-Files system administrators, explains how to manage, maintain, and configure the M-Files system.

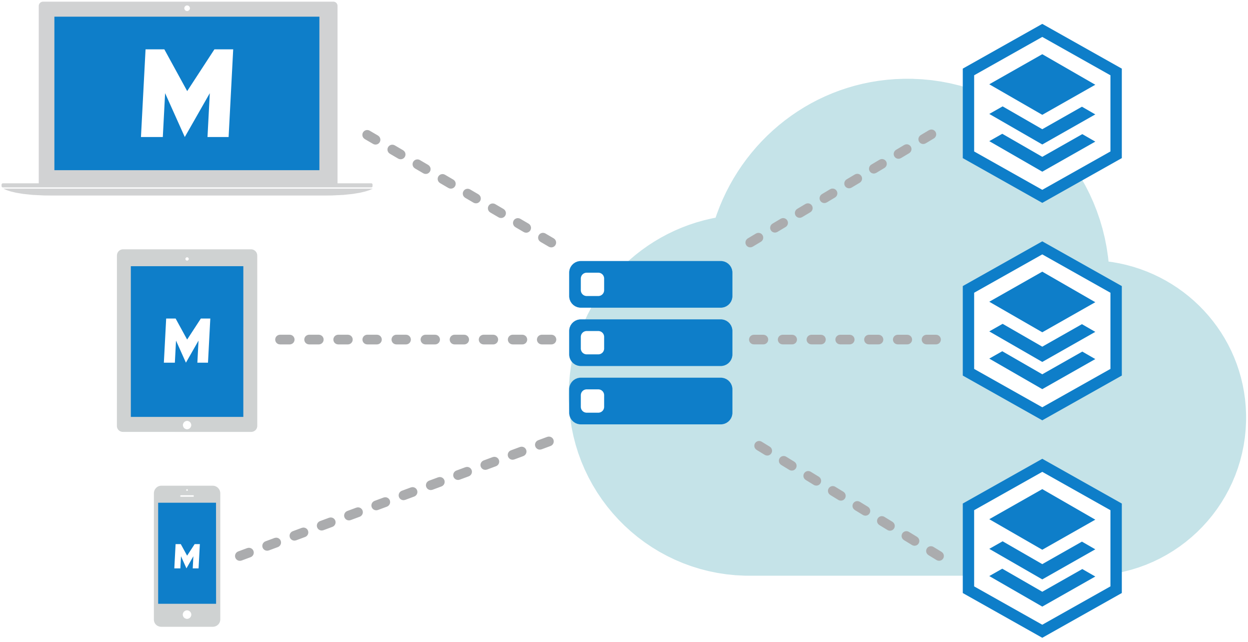


Figure 16: M-Files clients (on the left) are used for accessing M-Files Server (in the center), which manages the vaults (on the right).

The first subsection, Setting Up and Maintaining M-Files, introduces the M-Files system, provides instructions for installing and upgrading the system, and explains how server connections and vaults are managed.

The second subsection, Configuring M-Files, discusses the various ways you can configure and personalize your system to match your specific requirements and processes. It includes themes such as modifying the metadata structure of the vault, configuring workflows, using vault applications, making use of event handlers and scripts, and so forth.

In this chapter

3.1. Setting Up and Maintaining M-Files

This section describes what the M-Files system consists of, how you can set it up, and how to make sure everything is running as intended. For instructions on how to, for instance, modify the vault metadata structure, object workflows, or the metadata card behavior, or on how to install and use vault applications, see Configuring M-Files.

In this chapter

3.1.1. Before Taking M-Files into Use

It is recommended that you familiarize yourself with these operations and tasks before you take M-Files into use.

- Read the M-Files Product Support Policy.
- Make sure that your system meets the operating system requirements.
- Make sure that the server hardware setup meets the requirements.
- Decide the correct deployment option for your organization.
  - If you select the cloud deployment, make sure that the cloud requirements are met.
- Make sure that the firewall settings and your anti-virus software are up to date.
- See the technical details before you install M-Files.
- Get to know how M-Files is updated.
- Add connections to the server and create a vault.
- Add, change, or test vault connections in desktop settings.
- Read the instructions in Getting started with M-Files.

3.1.2. System Overview

An M-Files system consists of these components:

1. A server computer (or multiple servers) with the *M-Files Server* component that contains the vaults
2. M-Files clients used to show and edit the vault-stored information with the end-users' devices

You can access vaults with these methods:

- Install M-Files Desktop on your device.
- Access M-Files Web with a web browser.
- Use the M-Files mobile apps for iOS and Android.

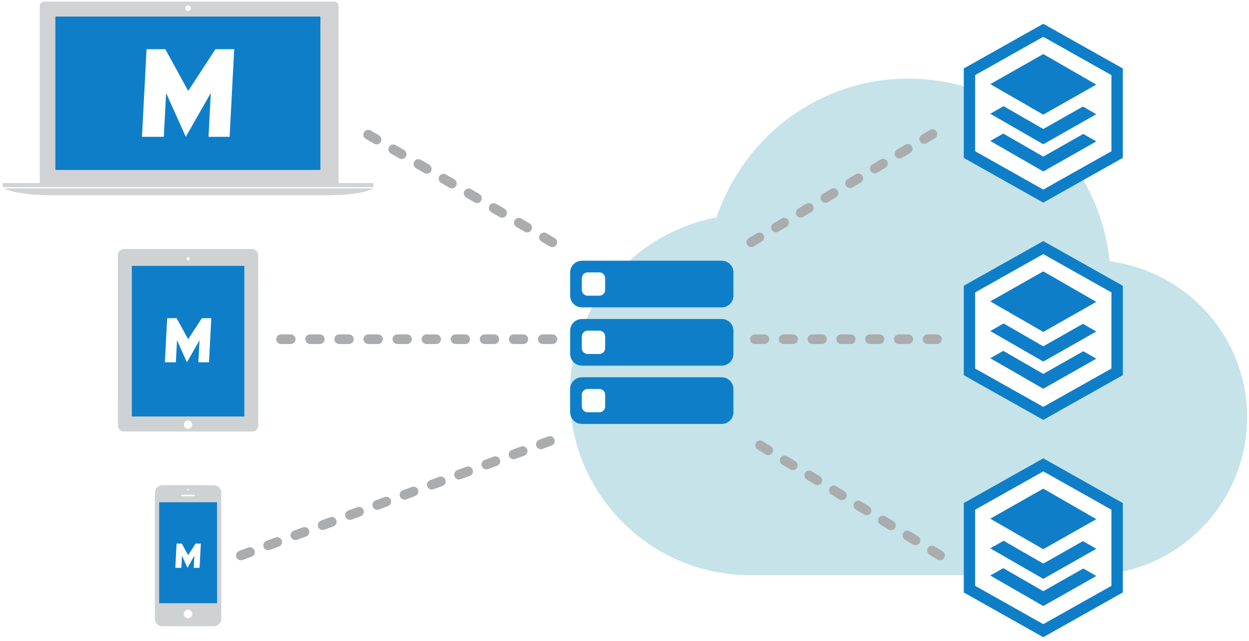


Figure 17: M-Files clients (on the left) are used for accessing M-Files Server (in the center), which manages the vaults (on the right).

This is a high-level description of the M-Files system: The clients on the left access the server computer (center of the image), which manages one or more vaults (on the right). Alternatively, M-Files Server and the vaults can be located on a cloud-based server (see M-Files Deployment Options).

You can edit server settings and the vault structure with M-Files Admin. With M-Files Desktop Settings, you can add, remove and edit vault connections. For more information about using M-Files Web and the mobile applications, see the topics Accessing M-Files Web and Accessing M-Files Mobile.

In this chapter

System Components

Your M-Files software includes these components:

- *M-Files Setup:* Use this to install M-Files.
- *M-Files Desktop:* The M-Files client most tightly integrated into Windows. There are two versions of M-Files Desktop available: the classic M-Files Desktop and the new M-Files Desktop.
- *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. There are two versions available: the classic M-Files Web and the new M-Files Web.
- *M-Files Mobile:* To access M-Files with your mobile device, you can use the M-Files mobile apps for iOS and Android.
- *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 (refer to M-Files Web Service). The M-Files API and its documentation are included within the installation of the M-Files software.

Differences between clients

Refer to the document M-Files Client Feature Comparison for a comprehensive list of features available in each M-Files client.

M-Files Deployment Options

M-Files offers many deployment options that give you the flexibility to use M-Files the way that best suits your organization's business needs and budget. This section gives you a high-level description of each deployment option. Contact M-Files sales at sales@m-files.com to find the best solution for your organization.

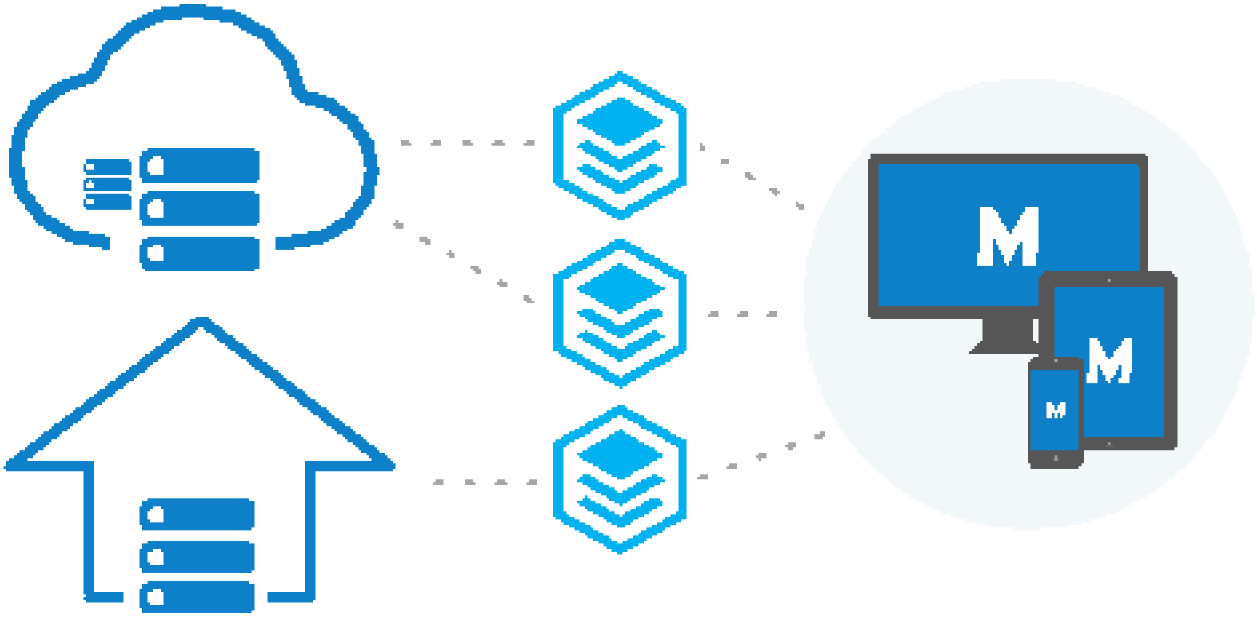


Figure 18: You can access your vaults with all M-Files clients regardless of the deployment solution.

Cloud deployment

M-Files Cloud is a fully managed cloud environment for knowledge work automation. With M-Files Cloud, you can manage your content without investing in local server infrastructure and maintenance. M-Files Cloud uses industry-leading cloud services by Microsoft Azure that are designed for high availability, accessibility, reliability, and security.

M-Files Cloud services can easily be scaled up and down based on your business needs. Thanks to the flexible and transparent pricing model, you only pay for the number of user licenses and the amount of storage you need. End users can use the web browser, the desktop client, or the mobile app to view, edit, and share documents anytime, anywhere.

For more information, refer to M-Files Cloud - Service Description in the M-Files Support Portal. See also M-Files Cloud Requirements.

M-Files Manage

M-Files Manage is a web application for centralized user and license management of your M-Files subscription.

With M-Files Manage, you can do, for example, these operations:

- Add and remove users.
- Add and remove licenses.
- Change user information and license types.
- Control user access to vaults.
- Connect an identity provider, such as Microsoft Entra ID, to your subscription to import and synchronize user groups to M-Files.
- Manage license types for user groups gotten from your identity provider.
- Download M-Files installers.

For more information, refer to M-Files Manage User Guide.

On-premises deployment

An on-premises deployment is best suited for organizations that have already invested in IT infrastructure, 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 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 with M-Files Web, M-Files mobile applications, or M-Files Desktop (with a VPN connection) in any location.

Self-managed cloud deployment

You can set up M-Files in a Windows Server virtual machine running on a cloud platform, such as Microsoft Azure, Amazon Web Services, or Google Cloud. These cloud deployments are self-managed in the same way as M-Files on-premises deployments.

The managed instance deployment option of Microsoft Azure SQL Database lets your organization set up a cloud-based environment to control the M-Files server and vault database engine. A managed instance of the Microsoft Azure SQL Database is a fully managed SQL Server Database Engine instance hosted in Azure cloud.

Hybrid deployment

With a hybrid solution, organizations can both leverage their existing on-premises technology investments and take advantage of M-Files Cloud – the award-winning knowledge work automation platform. It also eliminates the need for data migration and lets organizations keep legacy content where it is.

M-Files Cloud can be seamlessly integrated with on-premises ERP or CRM systems, 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, and M-Files mobile applications) are available also for hybrid deployments.

M-Files Platform Editions

M-Files is available in different platform editions. Each platform edition contains a different set of M-Files features. For more information, refer to the platform editions page.

Note: It can be that all features in this user guide are not available in your platform edition.

Language Versions of the M-Files Software

The 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
- Macedonian
- Mongolian
- Norwegian
- Polish
- Portuguese (Brazil)
- Romanian
- Russian
- Serbian (Cyrillic)
- Serbian (Latin)
- Slovak
- Slovenian
- Spanish
- Swedish
- Thai
- Turkish
- Ukrainian
- 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.

Security and Authentication

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

Admin aid

Refer to these documents for more technical information:

- Best Practices for Data Security and High Availability in M-Files
- Protecting Data in Transit with Encryption in M-Files
- Protecting File Data at Rest with Encryption in M-Files
- Setting Up M-Files to Use gRPC
- Enabling RPC over HTTPS connections to M-Files Server
- Using Federated Authentication with M-Files

In this chapter

- M-Files and Virus Scanning
- Accessing M-Files Vaults without VPN
- Encrypted Connections to M-Files Server
- HTTPS Connections to M-Files Server
- M-Files and Federated Authentication

M-Files and Virus Scanning

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

Make sure that the virus scanners on the users' computers do not do scheduled scanning for the virtual M-Files drive (the `M:` drive by default). A scheduled scan for the M-Files drive loads all the content from the M-Files server to the user's client and unnecessarily puts strain on the network and the server.

For best performance, disable real-time scanning for the M-Files drive and the M-Files installation folder (`C:\Program Files\M-Files\` by default) on the server and clients computers. This prevents 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, add their paths to the correct exclusion lists or exception lists in the anti-virus software. For example, with Symantec Endpoint Protection Manager (SEPM), this is done with an "exceptions policy". Other commonly used anti-virus software products can use terminology such as "excluded items list", "exclude objects", or "exclude from scanning". There are usually separate exclusion lists for scheduled scanning and real-time scanning.

If you cannot exclude the M-Files drive in the anti-virus software, use M-Files Admin to set the antivirus scanning processes not to have access to scan the drive. To do this, in the **Advanced Vault Settings** section of M-Files Admin, go to **Client** > **Desktop** > **Excluded Antivirus Scanning Processes**. To get access to this setting, the **Manage Client Settings Centrally** setting must be set to **Yes**. Before you set it to **Yes**, read the setting description on the **Info** tab.

Click **Add Process** and enter the name of the antivirus scanning process. For example, `scan64.exe`. Add as many processes as is necessary. Finally, click **Save**.

You can use Microsoft's Process Monitor to make sure that the M-Files drive and installation folder are excluded from virus scanning. For instructions, refer to this article.

Excluding the M-Files Client process from virus scanning

If your anti-virus software lets you exclude processes by name, it can be a good idea to exclude `MFClient.exe` from real-time scanning on the client computers. It can improve performance because it makes sure that the virus scanner does not scan the same files twice: once when the application opens the file and a second time when `MFClient.exe` does an internal **Open** operation on the same file.

The default path to `MFClient.exe` is `C:\Program Files\M-Files\<version>\Bin\x64\MFClient.exe`.

- If you use Microsoft Windows Defender, refer to the support article Excluding M-Files Client from Windows Defender.
- If you use SEPM, refer to the Symantec knowledge base article Exceptions: User-defined Exceptions.

Excluding M-Files server processes and vault data from virus scanning (on-premises only)

Note: These instructions are only for on-premises environments.

Note: If the processes and folders given in this section are not excluded from virus scanning on the M-Files server machine, users can experience poor vault performance. This can also cause faulty backups of vault data.

On the M-Files server machine, make sure that these processes are excluded from real-time virus scanning:

Process name	Default location
`MFServer.exe`	`C:\Program Files\M-Files\<version>\Bin\x64\`
`MFServerAux.exe`	`C:\Program Files\M-Files\<version>\Bin\x86\`
`MFIndexer.exe`	`C:\Program Files\M-Files\<version>\Bin\x64\`
`MFIndexingManager.exe`	`C:\Program Files\M-Files\<version>\Bin\x64\`
`MFDataExport.exe`	`C:\Program Files\M-Files\<version>\Bin\x64\`
`mf-grpc-web-server.exe`	`C:\Program Files\M-Files\<version>\Server\Web\GRPC\`

Make also sure that these folders are excluded:

- The M-Files installation folder (`C:\Program Files\M-Files\` by default)
- The vault data folder (`C:\Program Files\M-Files\Server Vaults\` by default)

Excluding other processes (on-premises only)

Note: These instructions are only for on-premises environments.

The exclusion of the `pdfSaver.exe` process from real-time virus scanning can improve performance when the user converts documents to PDF. Its default location is `C:\Program Files\PDF-XChange\PDF-XChange Standard`.

Antimalware support (on-premises only)

Note: These instructions are only for on-premises environments.

M-Files Server supports antimalware checks on Microsoft Windows 10 and later, and Microsoft Windows Server 2016 and later. Files uploaded to the M-Files server can be scanned for viruses and malware before they are saved to the repository. To do this, you must use an anti-virus software that is compatible with Windows Antimalware Scan Interface (AMSI). For example, Microsoft Windows Defender. Real-time scanning must also be enabled.

To take the antimalware checks into use, add these Microsoft Windows registry settings on the M-Files Server computer:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Server\MFServer**
Value name	`EnableAntimalwareScanner`
Value type	`REG_DWORD`
Value	`1`
Description	Enables antimalware scanning on Microsoft Windows 10 and later, and Microsoft Windows Server 2016 and later.

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Server\MFServer**	
Value name	`TreatAntimalwareScannerErrorsAsTransferBlockingErrors`	
Value type	`REG_DWORD`	
Description	Specifies whether file transfers to M-Files Server are blocked if the antimalware software is not available or has not been correctly configured. The default value is `0`.	
Value	`0`	Do not block file transfers if antimalware software is not available or is misconfigured.
	`1`	Block file transfers if antimalware software is not available or is misconfigured.

For the changes to take effect, you must restart the M-Files Server service.

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 enables 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) to ensure that only authorized devices can attempt to connect to the system. Cloud-based servers, M-Files Web, and the mobile applications use the HTTPS protocol by default.

Together, the HTTPS encryption and the use of a strong authentication mechanism by a compatible identity provider (for example, Microsoft Entra ID and Okta) provide similar security as VPN but without the complexity and compatibility challenges of VPN. However, the approach is not identical to VPN from the security point of view. 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.

Encrypted Connections to M-Files Server

M-Files clients can use different protocols when they communicate with M-Files Server. If users access data from outside the organization's private network, encrypting the network communication is usually mandatory. M-Files clients support end-to-end encrypted connections to the server.

For details on available protocols and how to create the connection, see Adding a Vault Connection.

M-Files Cloud server

The connection is always end-to-end encrypted with HTTPS protocol, which is implemented with a public Transport Layer Security (TLS) certificate.

The desktop client always uses the gRPC protocol to encode the data. When you configure the protocol, you will see gRPC and not HTTPS. gRPC steps on HTTPS as the network carrier protocol and for encryption.

On-premises server

With on-premises server configurations, you can select more connection protocol options:

- gRPC - recommended
- RPC over HTTPS - obsolete
- TCP/IP - obsolete

gRPC - recommended

> **Note:** M-Files recommends that you use the gRPC connection protocol with all new M-Files implementations for all client connections.

You can configure the gRPC connection with or without encryption. To require an encrypted connection, a valid TLS certificate must be in use on the server. To learn more about server certificates, see Managing Server Certificates, or refer to Setting Up M-Files to Use gRPC in M-Files Support Portal.

RPC over HTTPS - obsolete

> **Note:** RPC over HTTPS protocol is obsolete and it is not recommended for new installations. M-Files recommends that you use the gRPC connection protocol with all new M-Files implementations and also set up gRPC on existing installations.

The classic M-Files Desktop can use the RPC over HTTPS to communicate with M-Files Server.

RPC over HTTPS steps on the HTTPS encryption provided by an old IIS feature. The IIS feature must be present between the M-Files client and M-Files Server. RPC over HTTPS encapsulates the underlying RPC protocol inside HTTPS for encryption. For more information, refer to Enabling RPC over HTTPS Connections to M-Files Server in M-Files Support Portal.

TCP/IP - obsolete

> **Note:** TCP/IP protocol is obsolete and it is not recommended for new installations. M-Files recommends that you use the gRPC connection protocol with all new M-Files implementations and also set up gRPC on existing installations.

When both computers are connected to the same domain, TCP/IP uses RPC protocol and is encrypted by default. Because no additional configuration steps are needed for this communication mode, it is usually an easier way to communicate inside the organization's internal network. Please make a note that it is not recommended to use TCP/IP outside internal networks. For more information, refer to Protecting Data in Transit in M-Files in M-Files Support Portal.

Other clients

You can also encrypt the M-Files Web and M-Files Mobile connections. In M-Files Cloud, the connection is always end-to-end encrypted with HTTPS protocol, which is implemented with a public TLS certificate. In an on-premises environment, make sure that the server requires HTTPS and has a valid certificate that the client trusts. For more information, see Setting Up Web and Mobile Access to M-Files.

M-Files Web

M-Files Web and the classic M-Files Web use HTTP or HTTPS protocol to connect to the server. Both clients use the web browser when setting up the connection and encrypting it.

M-Files Mobile

By default, M-Files Mobile tries to use gRPC protocol for the server communication. If gRPC is not available, M-Files Mobile uses the REST API of the server or vault. Both protocols use HTTPS for encryption.

HTTPS Connections to M-Files Server

This topic describes the outdated Remote Procedure Call (RPC) over HTTPS protocol. See Encrypted Connections to M-Files Server for recommended connections and protocols.

The classic M-Files Desktop uses the TCP/IP, HTTPS, or gRPC protocol to communicate with M-Files Server. The classic M-Files Web uses HTTP or HTTPS, the new M-Files Web and the new M-Files Desktop use gRPC, and M-Files Mobile uses HTTP, HTTPS, or gRPC for server communication.

gRPC is used for all vault connections in M-Files Cloud and it is recommended for all new on-premises server implementations as a future-proof connection protocol. However, the default way for the classic M-Files Desktop to communicate with an on-premises M-Files server is to use the 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, it is preferable to enable the classic M-Files Desktop to communicate with M-Files Server through the HTTPS protocol instead of RPC. This is especially useful if clients connect 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 the classic 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 the classic 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.

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. Federated authentication allows M-Files users to be authenticated using third-party services called identity providers, such as Google or Microsoft Entra ID. 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.

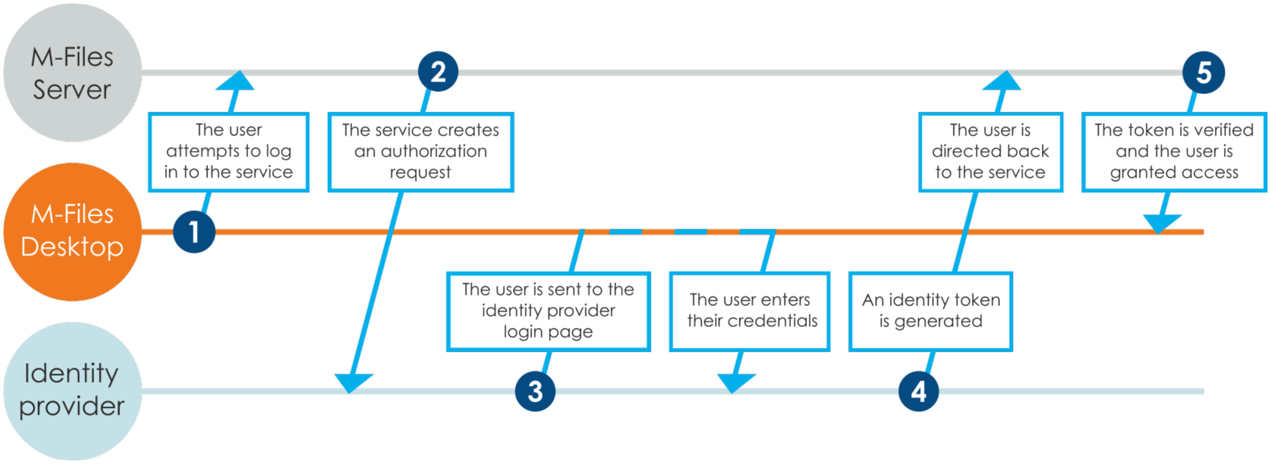

M-Files Server
M-Files Desktop
Identity provider
1
The user attempts to log in to the service
2
The service creates an authorization request
3
The user is sent to the identity provider login page
The user enters their credentials
4
An identity token is generated
The user is directed back to the service
5
The token is verified and the user is granted access

Figure 19: Authentication flow in a federated authentication system.

The figure gives an overview of the federated authentication process:

1. An M-Files user tries to log in to a vault, and the client sends an authentication request to M-Files Server.
2. M-Files Server creates an authorization request, which it sends to the identity provider.
3. The user is then redirected to the identity provider's login page where the user provides her credentials.
4. After the identity provider has validated the credentials, it returns a response to M-Files Server in the form of an identity token, which contains an assertion affirming that the user has been authenticated.
5. M-Files Server verifies the identity token and grants the user access to the vault.

You may use the configurations editor in M-Files Admin to enable federated authentication in your vault. For more information, see Using the Configurations Editor.

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

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:

- ISO 9001 series
- FDA 21 CFR Part 11
- EU GMP Annex 11
- HIPAA
- 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.

Note:

It is important to understand the login process used for electronic signing in M-Files:

- Normally, users must at least enter their password. It can also be necessary to use multi-factor authentication.
- With federated authentication, the login is done through the identity provider's process, not in M-Files.
  - By default, M-Files sends the Login Prompt parameter as `prompt=login`.

The full login process can also be a legal requirement for electronic signing.

Activation

The Electronic Signatures and Advanced Logging module includes the event logging extensions mentioned above and the electronic signature functionality. The module is available for a separate fee.

In most environments, the module is automatically activated if your subscription includes it. If licenses are managed manually on your on-premises M-Files server, refer to Managing Server Licenses.

In addition to the module, also the audit trail features of the vault must be activated (see Document Vault Advanced Properties). If you do not have M-Files Compliance Kit installed, you also need to add the electronic signature metadata structure to your vault manually (for instructions, see Metadata Definitions for an Electronic Signature Object).

More information

For more information on the Electronic Signatures and Advanced Logging module related extensions for event logging and electronic signatures, refer to Vault Event Log and Electronic Signatures.

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.

3.1.3. Installing and Upgrading M-Files

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

See Important Tasks after Installation, Vault Creation, or Vault Migration for a checklist of tasks that we recommend to be done with installation. It is especially important to make sure that the necessary virus scanning exclusions are in place. See M-Files and Virus Scanning for instructions.

In this chapter

- Manually Updating M-Files

System Requirements and Technical Details

This section contains hardware and software requirements and guidelines for the M-Files implementation. The Technical Details page includes information about special environments, file data encryption, and third-party applications.

In this chapter

- Operating System Requirements
- Server Hardware Guidelines
- M-Files Cloud Requirements
- M-Files Mobile and M-Files Web Requirements
- Microsoft SQL Server Requirements
- Technical Details

Operating System Requirements

We recommend that you use the desktop versions of Microsoft Windows for M-Files Desktop and the server versions for M-Files Server. If possible, do not use Microsoft Windows operating systems that are in the Extended support phase. Please refer to Microsoft's documentation for details about their support phases and product lifecycle.

Supported operating systems for M-Files Desktop

- Microsoft Windows 11 (64-bit) (recommended)
- Microsoft Windows 10 (64-bit)
- Microsoft Windows Server 2025 (64-bit)
- Microsoft Windows Server 2022 (64-bit)
- Microsoft Windows Server 2019 (64-bit)
- Microsoft Windows Server 2016 (64-bit)

Supported operating systems for M-Files Server

- Microsoft Windows Server 2025 (64-bit) (recommended)
- Microsoft Windows Server 2022 (64-bit) (recommended)
- Microsoft Windows Server 2019 (64-bit)
- Microsoft Windows Server 2016 (64-bit)
- Microsoft Windows 11 (64-bit)
- Microsoft Windows 10 (64-bit)

Note: In production environments, we recommend that you use M-Files Server always with a server operating system.

The version of the operating system can be Workstation or Server. You can install M-Files Server on a physical or a virtualized server. For example, you can use Hyper-V or VMWare ESXi for server virtualization. However, you cannot use M-Files in a Windows Container or in an Nano Server environment.

For data security reasons, do not install M-Files Server on a computer that is also used as a Microsoft domain controller.

Using Linux and macOS

Linux and macOS users can get access to M-Files with M-Files Web. The recommended browser is Google Chrome. macOS users can also install M-Files Web Companion to edit content with desktop applications.

With the classic M-Files Web, you can use the M-Files for Chrome extension.

.NET Framework requirements

The server and client computers must have Microsoft .NET Framework (not .NET) 4.7.2, 4.8.x, or later installed for M-Files to operate correctly. You can download it at: https://dotnet.microsoft.com/en-us/download/dotnet-framework. Normally, the Runtime version is sufficient, but you can alternatively install the Developer Pack version.

Server Hardware Guidelines

The M-Files system can be set up on a single server or on dedicated database, application, and search servers. If you use M-Files Ground Link, see the hardware setup guidelines for the Ground Link proxy server.

Plan the server architecture and especially the memory capacity and the CPU of the server so that it is easy to upgrade the server machine later.

M-Files Desktop, M-Files Admin, and M-Files Server cannot be used on computers with an ARM processor. End users that use this type of computer can access vaults with M-Files Web.

> **Important:** The configurations that this section gives are examples only. There are many things that have an effect on the system performance. For example, the degree of concurrent activity and the type of operations that users do in the vault.
>
> The disk space requirements for the metadata database are dependent on the complexity of the metadata structure and the number of object versions in the database. You can use the estimates of this section in typical document management use cases.
>
> In large M-Files implementations, contact M-Files to help you with the implementation plan.

In this chapter

Hardware Guidelines for Single-Server Environments

This section lists the minimum hardware requirements and hardware guidelines for environments where the M-Files server machine runs the M-Files Server application and the database server (Firebird or Microsoft SQL Server).

> **Important:** The configurations that this section gives are examples only. There are many things that have an effect on the system performance. For example, the degree of concurrent activity and the type of operations that users do in the vault.

The disk space requirements for the metadata database are dependent on the complexity of the metadata structure and the number of object versions in the database. You can use the estimates of this section in typical document management use cases.

In large M-Files implementations, contact M-Files to help you with the implementation plan.

Minimum requirements

CPU	2 cores
Memory	1 GB
Storage	300 MB disk space for M-Files Server

Environments with up to 50,000 objects

CPU	4 cores
Memory	4 GB
Storage	RAID 1 or RAID 5 disks and enough disk space for files, database, and backups

Environments with up to one million objects

CPU	8 cores
Memory	16 GB
Storage	RAID 1 or RAID 5 disks and enough disk space for files, database files, and backups. Database files, Microsoft SQL Server transaction logs, and search index files must be stored on solid state drives (SSD) for optimal performance.
Operating system	64-bit operating system
Database management system	Microsoft SQL Server 2019 or later, Standard or Enterprise Edition

Hardware Guidelines for Environments with Multiple Servers

For environments with a large number of objects and users, we recommend to have separate dedicated server machines for the M-Files Server application, the vault database, and full-text search indexing. For better scalability and availability, it is also possible to have multiple application, vault database, and full-text search indexing servers.

In Multi-Server Mode environments, each application server must have hardware that meet the server requirements.

Important: The configurations that this section gives are examples only. There are many things that have an effect on the system performance. For example, the degree of concurrent activity and the type of operations that users do in the vault.

The disk space requirements for the metadata database are dependent on the complexity of the metadata structure and the number of object versions in the database. You can use the estimates of this section in typical document management use cases.

In large M-Files implementations, contact M-Files to help you with the implementation plan.

Environments with up to one million objects when Microsoft SQL Server is on a separate server

We recommend to have a separate SSD drive for indexing on the M-Files Server. In this example, file data is stored on the application server.

System component	Database server	Application server
CPU	8 cores	8 cores
Memory	32 GB	16 GB
Storage	2 TB SSD drive	10 TB in total (4 TB for files + 4 TB for indexing + 20% as a buffer)
Database management system	Microsoft SQL Server 2019 or later, Standard or Enterprise Edition	

Environments with up to five million objects and five terabytes of files

Note: In these types of environments, configurations without a separate full-text search indexing server can be sufficient.

System component	Database server	Application server	Full-text search indexing (distributed IDOL installation on 1 server)
CPU	16 cores	8 cores	8 cores
Memory	32 GB	16 to 32 GB	16 to 32 GB
Storage	256 GB SSD drive for operating system SSD disks for database data and database transaction log Use RAID 1 or similar	256 GB SSD drive for operating system 15 TB HDD for file data. The file storage can be attached to the application server or the application server can connect to a separate file server. Use RAID 1 or similar	256 GB SSD disk for operating system 256 GB HDD/SSD disks for IDOL installations: • 1 disk for DIH/DAH engine • 1 disk for daily index content engine • 5 disks for main index content engines Use RAID 1 or similar

System component	Database server	Application server	Full-text search indexing (distributed IDOL installation on 1 server)
Operating system	Microsoft Windows Server 2019	Microsoft Windows Server 2019	Microsoft Windows Server 2019
Database management system	Microsoft SQL Server 2019 or later, Standard or Enterprise Edition		

Environments with up to 15 million objects and 8 terabytes of files

			The full-text search indexing (distributed IDOL installation on 3 servers)	
System component	Database server	Application server	Frontend server	2 backend servers
CPU	32 cores	16 cores	8 cores	16 cores per server
Memory	128 GB	32 GB	128 GB	128 GB per server
Storage	256 GB SSD disk for operating system Two 512 GB SSD disks for database data Two 128 GB SSD disks for database transaction log Use RAID 1 or similar	256 GB SSD disk for operating system 25 TB HDD for file data. The file storage can be attached to the application server or the application server can connect to a separate file server. Use RAID 1 or similar	256 GB SSD disk for operating system 256 GB HDD/SSD disks for IDOL installations: • 1 disk for DIH/DAH engine • 1 disk for daily index content engine Use RAID 1 or similar	256 GB SSD disk for operating system 256 GB HDD/SSD disks for IDOL installations: • 10 disks for main index content engines Use RAID 1 or similar
Operating system	Microsoft Windows Server 2019	Microsoft Windows Server 2019	Microsoft Windows Server 2019	Microsoft Windows Server 2019

			The full-text search indexing (distributed IDOL installation on 3 servers)	
System component	**Database server**	**Application server**	**Frontend server**	**2 backend servers**
Database management system	Microsoft SQL Server 2019 or later, Standard or Enterprise Edition			

Environments with up to 50 million objects and 10 terabytes of files

			The full-text search indexing (distributed IDOL installation on 6 servers)	
System component	**Database server**	**Application server**	**Frontend server**	**5 backend servers**
CPU	32 cores	16 cores	8 cores	16 cores per server
Memory	512 GB	64 GB	128 GB	128 GB per server
Storage	256 GB SSD disk for operating system Two 1 TB SSD disks for database data Two 256 GB SSD disks for database transaction logs Use RAID 1 or similar	256 GB SSD disk for operating system 30 TB HDD for file data. The file storage can be attached to the application server or the application server can connect to a separate file server. Use RAID 1 or similar	256 GB SSD disk for operating system 256 GB HDD/SSD disks for IDOL installations: • 1 disk for DIH/DAH engine • 1 disk for daily index content engine Use RAID 1 or similar	256 GB SSD disk for operating system 256 GB HDD/SSD disks for IDOL installations: • 10 disks for main index content engines Use RAID 1 or similar
Operating system	Microsoft Windows Server 2019	Microsoft Windows Server 2019	Microsoft Windows Server 2019	Microsoft Windows Server 2019

System component	Database server	Application server	The full-text search indexing (distributed IDOL installation on 6 servers)	
			Frontend server	**5 backend servers**
Database management system	Microsoft SQL Server 2019 or later, Standard or Enterprise Edition			

Hardware Guidelines for Ground Link Proxy Servers

In environments for Ground Link proxy services, we recommend this setup.

Note: Ground Link proxies do not support Multi-Server Mode.

Environments with one Ground Link proxy

CPU	4 cores
Memory	8 GB
Storage	10 GB disk space for M-Files Server and temporary files

If the same server machine is used for multiple Ground Link proxies, multiply the hardware resources by two.

M-Files Cloud Requirements

This section contains the minimum requirements and guidelines for an M-Files Cloud deployment.

Supported client applications and interfaces

You can connect to M-Files Cloud with these applications and application interfaces:

- M-Files Desktop
- M-Files Admin
- M-Files Mobile apps for iOS and Android
- M-Files Web
- M-Files Web based add-ins (for example, M-Files Add-in for Teams and SharePoint Online)
- M-Files Web Service API (restrictions can apply)
- M-Files API (restrictions can apply)
- M-Files UI Extensibility Framework

Supported M-Files Desktop and M-Files Admin versions

For information on the product versions that M-Files supports, refer to M-Files Lifecycle Policy.

We strongly recommend that you always use the latest available version of M-Files Desktop and M-Files Admin unless your cloud environment is updated with a custom upgrade schedule. In this case, use the same M-Files Long-Term Support version that the cloud vault uses.

For more information about software requirements, see Operating System Requirements.

Requirements for M-Files Mobile and M-Files Web

See M-Files Mobile and M-Files Web Requirements.

In this chapter

Requirements for M-Files Cloud Connections

Before you connect to M-Files Cloud, read these requirements and restrictions.

Requirements

- Allowed protocol: gRPC
- Allowed port: 443
- There is no restriction for the IP range. Contact M-Files customer support or your M-Files reseller to determine your static IP address or check the IP range here: Azure IP Ranges and Service Tags. Also refer to How to get IP address or range of M-Files DNS name.
- Connections from the local network to M-Files Cloud vaults must be allowed by the firewall.
- Connections from the local network to M-Files Cloud vaults must support the TLS 1.2 protocol.

    - This includes Microsoft Windows operating systems, API solutions, client computers, and integration systems.

        Note: TLS 1.2 must be used in on-premises environments if replication with cloud storage is used.
    - Refer to How to Enable TLS 1.2.
- You must have an internet connection. For the best performance, the latency between the client and the M-Files Cloud server must be less than 50 milliseconds. You can use the connection status tool in the classic M-Files Desktop to analyze the connection quality.

Restrictions

Site-to-site, point-to-site, Azure Express Route, and other VPN solutions are not supported in M-Files Cloud. You can use Ground Link when secure connection to local data is necessary. Ground Link supports external repository connectors and external object types.

Pre-shared keys are not supported in M-Files Cloud.

Adding a vault connection

See Adding a Vault Connection for instructions on how to add a connection to the vault.

Requirements for On-Premises to Cloud Migrations with Cloud Storage

When you plan to migrate on-premises vaults to M-Files Cloud, contact M-Files.

Before you create a replication package to cloud storage, read these requirements and restrictions.

Requirements

The minimum software requirement for the on-premises M-Files Server is M-Files 2015.1. We recommend that M-Files Server uses the latest available version. For more information, refer to M-Files version compatibility regarding API and Replication.

> ! **Important:** Do not update M-Files Server to the latest available M-Files version if you have purchased a long-term support (LTS) service for M-Files Cloud. Refer to our release notes for information about the latest available LTS version.

The TLS 1.2 protocol must be used in the on-premises environment.

All scripts and custom code must be disabled in the vaults. Custom code is automatically removed from replication packages during import, unless your M-Files Cloud environment is an isolated service. The removed code includes these components:

- Calculated values of property definitions (VBScript)
- Validation scripts of property definitions (VBScript)
- Advanced preconditions and postconditions for workflow states (VBScript)
- Workflow state scripts (VBScript)
- Workflow state transition scripts (VBScript)
- Event handlers

> **Tip:** After the migration to a shared M-Files Cloud environment, you can install signed vault applications and custom vault applications and scripts that M-Files has validated. In isolated services, code validation is not necessary.

Restrictions

These components cannot be transferred with replication:

- Vault applications and UI extensions
- Settings stored in Custom Vault Data
- Advanced Vault Settings
- External mail sources and file sources
- Data exports for reporting
- Login accounts

After the migration, user provisioning and authentication must be reconfigured in the M-Files Cloud vault.

Server-level configurations are not supported and cannot be migrated to M-Files Cloud. Server-level configurations can include these components:

- Microsoft Windows registry settings
- PowerShell scripts
- Microsoft Windows Task Scheduler tasks
- Custom Open Database Connectivity (ODBC) drivers
- Software installed to the local Microsoft Windows server

Requirements for On-Premises to Cloud Migrations with Vault Backups

When you plan to migrate on-premises vaults to M-Files Cloud, contact M-Files.

Before you create a backup of a local vault, read these requirements and restrictions.

Requirements

The on-premises M-Files Server must be upgraded to the latest available version. See System Requirements and Technical Details.

> ! **Important:** Do not update M-Files Server to the latest available M-Files version if you have purchased a long-term support (LTS) service for M-Files Cloud. Refer to our release notes for information about the latest available LTS version.

If you use Microsoft SQL Server to host the vault database:

- The server software must be upgraded to Microsoft SQL Server 2016 or later with the latest service pack installed.
- The file data location must be changed from the vault database to a file system folder.

Error detection:

- The database optimization and verify and repair operations must be successfully completed in the thorough mode in all the local vaults. If errors are found, they must be resolved before you create the backups. Report unresolved errors to M-Files.
- The Microsoft Windows event log of the on-premises server must not contain errors that prevent the M-Files Cloud deployment. Report unresolved errors to M-Files.

User management:

- A local synchronization and authentication system of Windows users on the M-Files server must be replaced with an M-Files Cloud compatible solution. For example, a local active directory to Microsoft Entra ID. For more information, see Document Vault Authentication.
- Login accounts must be converted to vault-specific accounts on the local M-Files server. After this, existing server-specific login accounts must be transferred to the appropriate vaults.

Vault applications and scripts:

- Custom vault applications installed to the local M-Files server must be upgraded to support Multi-Server Mode.
- All the installed custom vault applications, scripts, and code must be validated. If you migrate to an isolated service in M-Files Cloud, this is not necessary.
- Official M-Files add-ons installed to the local M-Files server must be upgraded to their latest version.

Restrictions

Server-level configurations are not supported and cannot be migrated to M-Files Cloud. Server-level configurations can include these components:

- Microsoft Windows registry settings
- PowerShell scripts
- Microsoft Windows Task Scheduler tasks
- Custom Open Database Connectivity (ODBC) drivers

- Software installed to the local Microsoft Windows server

Supported Backup Formats for M-Files Cloud

Before you create a backup of a local vault, make sure that these requirements are fulfilled: Requirements for On-Premises to Cloud Migrations with Vault Backups.

These formats are supported for M-Files Cloud backups:

- MFB file with file data included in the file (Firebird backup)
- MFB file with separate file data folders (Firebird backup)
- BACPAC file with separate file data folders (SQL backup)

These formats are not supported:

- BAK file with separate file data folders (SQL backup)
- Any SQL backup file with file data included in the file
- ZIP file

M-Files Mobile and M-Files Web Requirements

Supported operating systems for the M-Files Mobile apps

App name	Required OS version
M-Files Mobile for iOS	iOS 14 or later
M-Files Mobile for Android	Android 9 or later
M-Files for MobileIron	iOS 15 or later, Android 7 or later
M-Files for BlackBerry	iOS 17 or later, Android 10 or later
M-Files for Intune	iOS 16 or later, Android 9 or later

Supported browsers for M-Files Web

Always use the latest available version of the browser.

Web browser	Operating system
Google Chrome	Microsoft Windows, macOS
Mozilla Firefox	Microsoft Windows
Safari	macOS
Microsoft Edge	Microsoft Windows

With M-Files Web, you can use M-Files Web Companion to edit content with desktop applications.

Supported browsers for the classic M-Files Web

For optimal user experience with the classic M-Files Web, use the M-Files for Chrome extension. The extension is available in the Chrome Web Store for Chromium-based browsers. These include Google Chrome and Microsoft Edge. As an alternative to the extension, your M-Files admin can set up Microsoft Office for the web.

Always use the latest available version of the browser.

Web browser	Operating system
Google Chrome **(recommended)**	Microsoft Windows, macOS
Microsoft Edge **(recommended)**	Microsoft Windows
Mozilla Firefox	Microsoft Windows
Safari	macOS

Microsoft SQL Server Requirements

You can use Microsoft SQL Server as the vault database engine. Refer to our lifecycle policy for information about the supported versions. These editions are supported: Microsoft SQL Server Express, Standard, and Enterprise. Refer to Microsoft documentation to make sure that your Microsoft SQL Server edition has the necessary features and capabilities for your environment. M-Files supports the use of Microsoft SQL Server on Microsoft Windows.

With a cloud-based M-Files environment that you manage yourself, you can also use Microsoft Azure SQL Database Managed Instance as the vault database engine.

Important information

Please take note of these details before you set up Microsoft SQL Server:

- Some editions of Microsoft SQL Server can have a hard limit for the size of a database. If all the space of the database is used, the vault can become unusable.

  - For example, if you use the Express edition, it is extremely important to make sure that the database space is never completely used. This can cause that it is no longer possible to log in to the vault with any login account.
- Do not use performance tuning advisor tools for M-Files vault databases or create additional indices or statistics. This can slow down the system and cause a vault to be unusable during an update.
- We recommend M-Files Server and Microsoft SQL Server to be used in the same subnetwork to reduce latency.
- For best performance, limit the Microsoft SQL Server memory use so that the operating system does not use the paging file in normal operation.

Enabling Microsoft SQL Server features

Enable the features given here 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)

Loading the Microsoft SQL Server assembly (M-Files February '23 Update and earlier)

M-Files February '23 Update and earlier versions use an SQL server assembly that must be used in the SQL server instance. Usually, M-Files loads this assembly to the SQL server instance automatically. However, it can be necessary to manually allow the use of the assembly, if, for example, M-Files does not have the necessary permissions in the SQL server instance. For instructions, refer to the support article M-Files and SQL Server 2017 compatibility). If the SQL server assembly is updated, you must repeat the process.

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, you can use Microsoft SQL Server as the database engine for better performance and support for larger repositories. Refer to our lifecycle policy for information about the supported versions.

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. Microsoft 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.

If your organization wants to use a self-managed cloud environment with a SQL database, you can use the managed instance deployment option of the Microsoft Azure SQL Database. A managed instance of the Microsoft Azure SQL Database is a fully managed SQL Server Database Engine instance hosted in Azure cloud.

It is strongly recommended that the data saved in the file system is encrypted. The file data encryption at rest feature uses the AES-256 algorithm. The encryption is compliant with the Federal Information Processing Standard (FIPS) publication 140-2. For more information, refer to Protecting File Data at Rest with Encryption in M-Files.

M-Files uses Unicode and thus supports storing and finding data in East Asian languages as well.

Network communication

The classic M-Files Desktop uses the TCP/IP, HTTPS, or gRPC protocol to communicate with M-Files Server. The classic M-Files Web uses HTTP or HTTPS, the new M-Files Web and the new M-Files Desktop use gRPC, and M-Files Mobile uses HTTP, HTTPS, or gRPC for server communication.

Use encrypted connections in all client-to-server communication. For more information, refer to Protecting Data in Transit with Encryption in M-Files.

Special environments

M-Files can be used with virtualization and remote desktop technologies. M-Files has been proven to be compatible with these environments:

- Remote Desktop Services (Terminal Services)
- Citrix XenApp

  - M-Files is Citrix Ready for Citrix XenApp 7.6. See Using M-Files with Citrix XenApp or Microsoft RDS for the configuration details.
- Linux file servers
- Novell networks

> **Note:** M-Files is not responsible for the configuration of virtualization and remote desktop technologies, or application errors caused by their use. If a known issue cannot be resolved in a virtual or remote desktop environment, you must set up a non-virtual environment for more assistance.

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 an active directory (LDAP).
Federated authentication	Users are authenticated against an external Identity Provider (IdP), such as Microsoft Entra ID. See Using Federated Authentication with M-Files for more information.
M-Files authentication	Users are authenticated with usernames and passwords specified within M-Files.

Database connections

M-Files Server can be integrated with existing databases, such as CRM and ERP databases. Most databases with an OLE DB or ODBC driver are supported (includes SQL Server, Oracle, and MySQL). The use of the Access ODBC driver is not supported.

Integrations with third-party applications

Numerous third-party applications can be integrated 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 (refer to M-Files Web Service).

> **Note:** When you develop new extensions or edit existing ones, we recommend that you replace VBScript content with Vault Application Framework (VAF) compatible code for future compatibility. For more information on the benefits of VAF development over VBScript, refer to The Vault Application Framework in M-Files Developer Portal.

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

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

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 a single M-Files installation. For advanced installation options, refer to the document Installing M-Files Desktop, M-Files Server, and M-Files Admin with Advanced Options.

Tip: During the M-Files installation progress, it can be a good idea to see M-Files and Virus Scanning.

Read this information before you start the installation:

- The server and client computers must have Microsoft .NET Framework (not .NET) 4.7.2, 4.8.x, or later installed for M-Files to operate correctly. You can download it at: https://dotnet.microsoft.com/en-us/download/dotnet-framework. Normally, the Runtime version is sufficient, but you can alternatively install the Developer Pack version.
- You can get the M-Files setup file from your system admin, or download it on the M-Files download page.
- System admins: See Important Tasks after Installation, Vault Creation, or Vault Migration for a checklist of tasks that we recommend to be done with the installation. It is especially important to make sure that the necessary virus scanning exclusions are in place. See M-Files and Virus Scanning for instructions.

For a single M-Files installation:

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.

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

   If you are not an M-Files system administrator in your organization, you can install M-Files Desktop only. In this case, M-Files Server has been installed for you, and your M-Files system administrator has M-Files Server Tools (M-Files Admin) installed. After the normal installation, you can connect to the vaults on your M-Files server with M-Files Desktop Settings.

   The evaluation installation includes all the software components and a sample vault, which you can start to use after the installation.
6. Click **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 to see the Guided Tour and click **Finish**.

The M-Files software has been installed. It is recommend to see the Getting Started with M-Files section next.

In this chapter

Example: Single-Instance Installation of M-Files

This is a short description of a basic M-Files installation to a single computer that, in this case, serves as both the server machine and the client. The purpose of this example is to provide the main steps of setting up the elementary components of an M-Files system.

Complete the following steps:

1. Install the M-Files software as instructed in Installing the Software.
2. Create a document vault as instructed in Creating a Vault.

   Note, however, that with the evaluation installation option, two vaults are automatically deployed. **Sample Vault** contains a reference metadata structure and views for some common information management processes as well as sample files to help you to easily evaluate the search. **My Vault** contains the same metadata structure and views as **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 the sample structure from the M-Files Server installation folder (`C:\Program Files\M-Files\<version>\Server\sample\My Vault.mfb` by default).

3. Create a new login account to the server as instructed in Creating a Login Account.
4. Create a new user (or multiple users) to your vault as instructed in Creating a User.

   At this point, the following tasks should be completed:

   - M-Files Server, M-Files Admin, and M-Files Desktop have been installed.
   - There is a document vault on the server – either one of the vaults that come with the evaluation installation or one that you have created from scratch.
   - There is at least one login account on the server.
   - There is at least one user in your vault.

5. Open M-Files Desktop Settings and create a connection to the vault as instructed in Adding a Vault Connection.

You should now have a vault on the M-Files server with a user whose credentials you can use to log in to the vault and start browsing the content with M-Files Desktop.

Updating M-Files

Automatic updates keep the M-Files software up to date. If a newer version of M-Files becomes available, it is downloaded and installed automatically. You can delay automatic updates for a limited time if you are working on something important when an automatic update becomes available.

Note: For the automatic updates to run, local administrative permissions on your computer are not necessary.

When a new M-Files version becomes available, you see a notification in the top area of M-Files Desktop. Click **Options** to schedule or start the M-Files software update.

The feature gets the latest update information from the update server using HTTPS on TCP port 443. This means that normally it is not necessary for you to change any firewall settings.

For information on updating M-Files manually, see Manually Updating M-Files.

Settings for automatic updates

To open the settings for automatic updates, right click the M-Files icon (M) in the Windows system tray and select **Settings** > **Automatic Updates**.

> **Note:** If your M-Files system admin manages the settings for automatic updates, you cannot change them and all options are not necessarily visible.

For a high-level description on how M-Files downloads the update packages when the **Download updates automatically** option on the **Settings** tab is enabled, see Update Download Process. To make sure that your M-Files software is always up to date, do not disable automatic updates.

To check for updates manually, open the **Installation** tab and click **Check Now**. If an update package is available, it is downloaded to your computer.

> **Note:** If automatic updates are disabled, you must have local administrative permissions on your computer to install an available update.

To disable the automatic installation of updates, open the **Settings** tab and unselect the **Install updates automatically** check box. To start the installation of available updates manually, open the **Installation** tab and click **Install**. If the **Install** button is disabled, there are no updates available for installation.

In the **Installation schedule** section of the **Installation** tab, you can select the preferred days and time of installing M-Files updates. It is recommended that you select a date and time that is outside of working hours so that installations do not interrupt M-Files operations in your organization. Note that the computer must be running and not in sleep or hibernate mode when the update is scheduled to be installed. If the computer is not running when the scheduled installation time occurs, the update is attempted to be installed or scheduled the next time the computer is started.

For more information on scheduling update installations and disabling automatic updates, see Configuring Automatic Updates with Registry Settings.

In this chapter

Configuring Automatic Updates with Registry Settings

In addition to using the **Automatic Updates** dialog, you can configure automatic updates on the server computer and client computers with Microsoft Windows registry settings. For the changes to take effect, you must restart the M-Files Server service. For more information on automatic updates, see Updating M-Files.

> **Note:** If automatic updates are disabled, you must have local administrative permissions on your computer to install an available update.

> **Tip:** In Microsoft Windows, you can use Group Policy Objects to distribute registry settings to multiple computers.

Disabling or enabling automatic updates

Add or edit the following Windows registry setting to disable or enable the automatic updates. To make sure that your M-Files software is always up to date, do not disable automatic updates.

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\Common\Updates`**	
Value name	`Enabled`	
Value type	`REG_DWORD`	
Description	If the value is set to `0`, automatic updates are disabled on the target computer, including manual update checks with the **Automatic Updates** dialog. You can update the software by downloading and running the installation package by hand.	
Default value	The default value is `1`.	
Valid values	`1`	Updates are enabled on the computer.
	`0`	Updates are disabled on the computer.

Disabling or enabling automatic update features

Add or edit the Windows registry settings in this section to disable or enable specific features of automatic updates.

Disabling or enabling the setting for automatic update installation

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Common\MFAUClient`**	
Value name	`AllowToUseAutoInstallationFeature`	
Value type	`REG_DWORD`	
Description	If the value is set to `0`, installing automatic updates is disabled and only the **Download updates automatically** option is visible on the **Settings** tab in the **Automatic Updates** dialog. You can still install updates in the **Installation** tab of the **Automatic Updates** dialog.	
Default value	The default value is `1`.	
Valid values	`1`	The setting **Install updates automatically** is shown on the **Settings** tab.
	`0`	The setting **Install updates automatically** is not shown and updates are not automatically installed.

Disabling or enabling automatic update installation

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Common\MFAUClient`**
Value name	`EnableAutoInstallation`
Value type	`REG_DWORD`
Description	With this setting, you can specify whether automatic updates are automatically installed. If the setting `AllowToUseAutoInstallationFeature` is set to `0`, this setting has no effect.
Default value	The default value is `0`.

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common\MFAUClient**	
Valid values	0	Automatic updates are not automatically installed. The **Install updates automatically** option is disabled on the **Settings** tab of the **Automatic Updates** dialog.
	1	Automatic updates are automatically installed. The **Install updates automatically** option is enabled on the **Settings** tab of the **Automatic Updates** dialog.

Disabling or enabling automatic update downloads

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common\MFAUClient**	
Value name	EnableUpdates	
Value type	REG_DWORD	
Description	If the value is set to 0, M-Files no longer downloads updates automatically, but you can run the update check manually in the **Installation** tab of the **Automatic Updates** dialog.	
Default value	The default value is 1.	
Valid values	1	M-Files automatically checks for updates and downloads a new version if one is available.
	0	M-Files does not check for new versions automatically.

Disabling or enabling automatic update options in the user interface

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common\MFAUClient**	
Value name	CanConfigureAutoInstallingViaUi	
Value type	REG_DWORD	
Description	If the value is set to 0, the settings shown on the **Settings** tab in the **Automatic Updates** dialog cannot be changed.	
Default value	The default value is 1 for Microsoft Windows Server operating systems and 0 for other operating systems.	
Valid values	1	Settings shown on the **Settings** tab in the **Automatic Updates** dialog can be changed.
	0	Settings shown on the **Settings** tab in the **Automatic Updates** dialog cannot be changed.

Controlling the installation deadline

If necessary, you can adjust the installation deadline and the amount of time by which users can delay the installation. Add the following registry settings on the target computer to adjust the installation deadline:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common\MFAUClient**
Value name	PostponeDurationInHours

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common \MFAUClient**	
Value type	REG_DWORD	
Description	Users can delay the installation process once before it is started. Edit this value to change the number of hours by which users can delay the installation process by selecting **Update Later** in the options dialog.	
Default value	10	The default value for the additional delay is 10 hours.
Valid values	Any number of hours.	

Defining the installation schedule

You can select the preferred days and time of installing M-Files updates. It is recommended that you select a date and time that is outside working hours so that installing updates does not interrupt daily M-Files tasks in the organization.

Note that the computer must be running and not in sleep or hibernate mode when the update is scheduled to be installed. If the computer is not running when the scheduled installation time occurs, the update is attempted to be installed or scheduled the next time the computer is started.

Add the following registry settings on the target computer to define an installation schedule:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common \MFAUClient**	
Value name	AutoInstallDays	
Value type	REG_SZ	
Description	One or more days when automatic updates are attempted to be installed. Separate multiple values with a semicolon.	
Default value	mon;tue;wed;thu;fri;sat;sun	By default, automatic updates are attempted to be installed every day of the week.
Valid values	mon	Monday
	tue	Tuesday
	wed	Wednesday
	thu	Thursday
	fri	Friday
	sat	Saturday
	sun	Sunday

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common \MFAUClient**
Value name	AutoInstallTimeOfDay
Value type	REG_SZ
Description	The time of day in 24-hour format when automatic updates are attempted to be installed.

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common \MFAUClient**	
Default value	`02:00`	By default, automatic updates are attempted to be installed at 02:00.
Valid values	Any valid time of day.	

Defining the maximum random added delay before the update

You can add random delay to the beginning of the automatic updates by adding the following registry setting on the target computer:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common \MFAUClient**	
Value name	`AdditionalMaxRandomSleepingPeriod`	
Value type	`REG_DWORD`	
Description	The maximum value for the random delay (in other words sleeping) added to the main sleeping period (default: one hour) at the beginning of the automatic updates poll-download-install cycle. The randomness establishes a crude form of load balancing in a network. When defining the value, take into consideration that too large values may impact polling frequency and that also several other registry settings affect the sleeping period and installation. Their combined effect can result in unwanted consequences, such as preventing a user from postponing the installation during office hours or delaying the download to occur only after a weekly installation day. With the default settings, the poll-download-install cycle restarts every 1-2 hours with a mean value of 1.5 hours.	
Default value	`3600`	The default maximum added delay value is one hour (3600 seconds).
Valid values	`0`	No random added delay.
	`<1-86400>`	Maximum random added delay in seconds.

Update Download Process

When the **Download updates automatically** option is enabled, M-Files automatically requests for an update package from the default update server (`findupdates.m-files.com`) every hour. If a new version is available, the automatic update server sends the new version number and an HTTPS URL for the update package to M-Files.

Note: Update packages for new versions are made available gradually after an update is released.

After receiving the download URL, M-Files checks that it starts with `https`, and if it does, downloads the digitally signed update package with Background Intelligent Transfer Service (BITS). M-Files then proceeds to verify that the update package has been created and signed by M-Files and that it has not been tampered with, therefore making sure that it can be safely installed, and finally makes the new version available for installation.

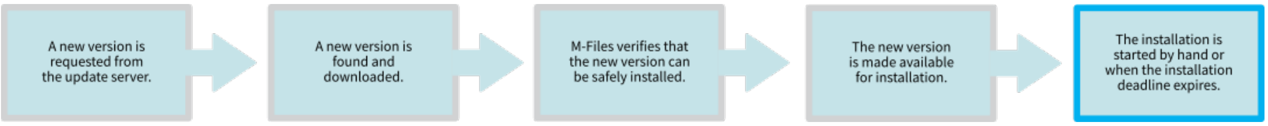

A new version is requested from the update server.
A new version is found and downloaded.
M-Files verifies that the new version can be safely installed.
The new version is made available for installation.
The installation is started by hand or when the installation deadline expires.

Figure 20: The download and installation process of an M-Files update.

Manually Updating M-Files

Note: By default, M-Files is automatically updated and manual update is not necessary. For more information, see Updating M-Files.

Before you start the update, do not uninstall previous versions of M-Files. The M-Files installer automatically detects the previous versions of the software and migrates the settings to the new version.

To update M-Files to a newer version:

1. Start the M-Files installer for the new version.
2. Select the **Simple upgrade** option.

When you select the **Simple upgrade** option, the setup installs the new version and transfers the M-Files settings and all the local data from the previous version to the new version. Finally, the setup uninstalls the previous version.

Installation preconditions

For information on the product versions that M-Files supports, refer to M-Files Lifecycle Policy.

All M-Files Server instances in a replication setup must have the same build number. For example, `12628` in `23.5.12628.4`.

To verify compatibility with M-Files API and replication, refer to M-Files version compatibility regarding API and Replication.

If you have recently done the Verify and Repair (Quick) operation and issues were found, make sure that they are fixed before you upgrade the software.

Before you install the upgrade on the M-Files server, make sure that the conditions listed here are met.

- Your server fulfills the requirements of the new version. See System Requirements and Technical Details.
- Recent backups of the vaults are available and usable. The backups can be useful if an unexpected error occurs during the upgrade.
- Recent backups of the master database are available.

  - It is recommended that the backups are on a disk that is separate from the main system.

If an error occurs, create a support case in M-Files Support Portal or contact your M-Files reseller immediately. Do not try to resolve the situation yourself.

Note: In some cases, you must disable your antivirus software for the duration of the upgrade process.

Installation order

When you update M-Files frequently, you can upgrade the client computers and the server computer in any order. Otherwise, it is recommended to upgrade first the server and then the client computers.

Note: It is possible that some new options and features of the newer version are not available until the server and the clients have been upgraded.

Upgrading offline vaults

The internal database structure of the vault changes during the upgrade. This is why also the vaults must be upgraded. All online vaults are upgraded automatically during a software upgrade. However, you must upgrade vaults in the offline state manually.

Service releases

Service releases are small software upgrades that share the same main version number (for example, `22.3`). After the main version number comes the four- or five-digit version ID for the service release. For example, `23.3.12441.9` and `23.3.12441.10` are service releases for the version `23.3.12441.6`.

Service releases do not usually contain new features. They are released if significant issues are detected in the released version or if compatibility with newer versions of other software requires changes to M-Files.

Service releases are compatible between each other and can be installed in any order.

Centralized deployment with Windows Group Policy

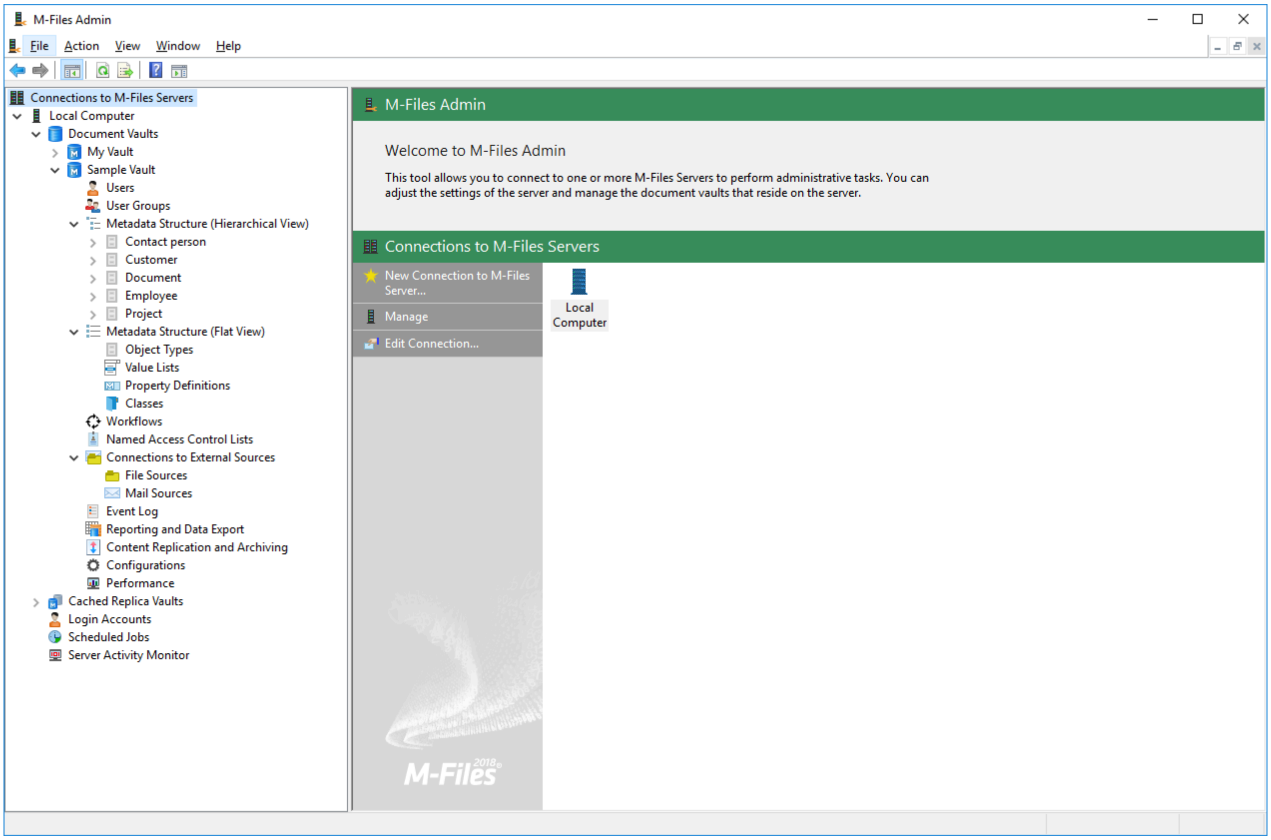
You can use the Windows Group Policy feature to automatically distribute M-Files to client computers. You can also use any other centralized deployment mechanism that you are familiar with. To customize the behavior of the M-Files setup program, refer to Installing M-Files Desktop, M-Files Server, and M-Files Admin with Advanced Options.

3.1.4. M-Files Admin

M-Files Admin is a tool that 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 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.



Welcome to M-Files Admin

This tool allows you to connect to one or more M-Files Servers to perform administrative tasks. You can adjust the settings of the server and manage the document vaults that reside on the server.

Figure 21: The M-Files Admin main window displaying the different levels inside a document vault.

M-Files Admin Terminology

Login account

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.

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. Compare with M-Files Terminology.

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.

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).

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.

System administrator

A system administrator is a user who has been assigned the role of system administrator. This means that the user's login account has the server role **System administrator**. With this role, the user gets all the permissions to each vault on the server and the user has server-level access to do all possible functions in M-Files. A system administrator can add the role of system administrator to other login accounts.

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.

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, that is, to specify the users who may access it.

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*.

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. See also M-Files Terminology.

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.

3.1.5. Connections to M-Files Server

This section offers an information about various operations and settings related to connections to M-Files server.

Note: In M-Files Cloud, only M-Files employees can make changes on the server level.

The M-Files Cloud service includes managing server licenses, backups, and server certificates. Customer administrators do not have access to the related sections in M-Files Admin.

Note: It is recommended to use Universal Naming Convention (UNC) paths (such as `\\ServerName\`) when you are defining a connection to a network drive, as the letter assigned to the drive may not be visible to the M-Files server. In addition, Windows drive letter assignments are frequently user-specific. A network drive may, for example, contain an external database for a value list.

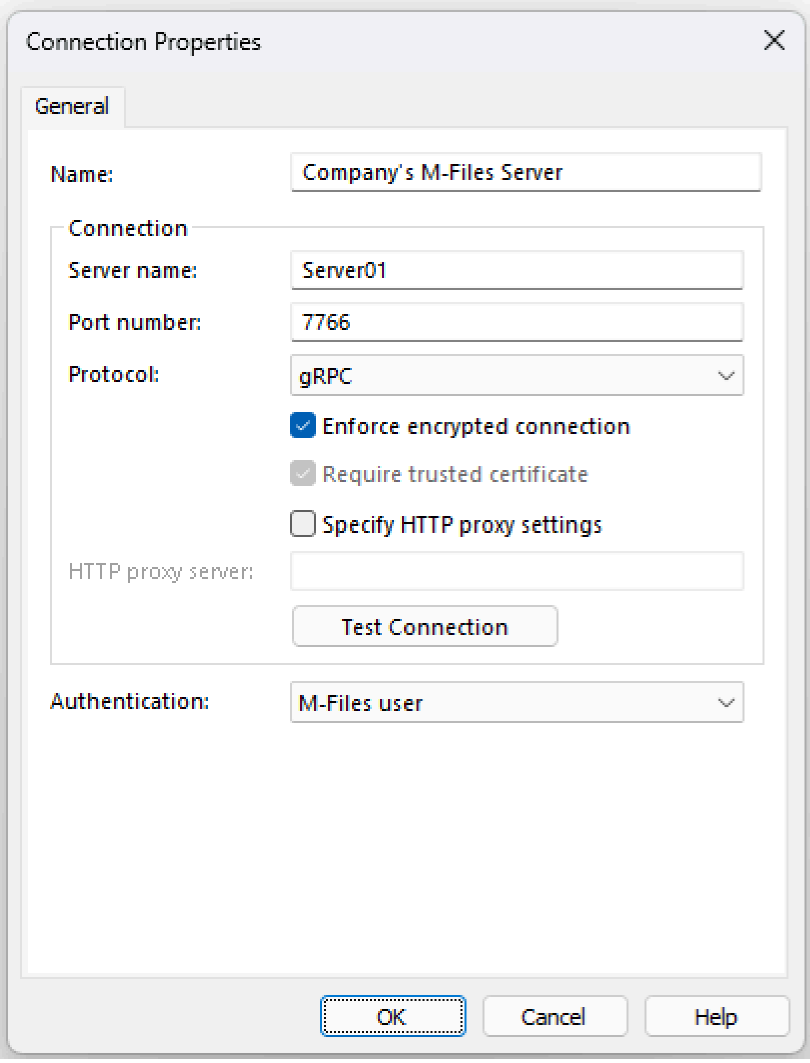
In this chapter

Adding a New Connection to M-Files Server

Important information

- When you use the gRPC protocol for connections between the M-Files server and M-Files clients, a valid TLS certificate must be in use on the server for connection security and encryption.For instructions, see Managing Server Certificates
- For RPC encryption to operate, 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.

To set up a new connection to M-Files server in M-Files Admin, select **Connections to M-Files Servers** in the left-side tree view. In the task area, click **New Connection to M-Files Server**.



Name: Company's M-Files Server

Server name: Server01

Port number: 7766

Protocol: gRPC

☑ Enforce encrypted connection

☑ Require trusted certificate

□ Specify HTTP proxy settings

HTTP proxy server:

Authentication: M-Files user

Name

First assign a name to the 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 following protocols are available:

- gRPC
- Local gRPC

- TCP/IP
- SPX
- Local Procedure Call (LPC)
- HTTPS

Enforce encrypted connection

Enable this option to secure communication between M-Files Admin and M-Files Server with RPC encryption.

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 the client software and M-Files Server in the organization's internal network.

The option is available for the TCP/IP and gRPC protocol. 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.

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

Specify HTTP proxy settings

You can specify an explicit forward proxy server for a server connection that uses the gRPC or HTTPS protocol. This can be necessary if your organization wants to route all traffic through a forward proxy server.

To do this, enable the option **Specify HTTP proxy settings** and do one of these options in the **HTTP proxy server** field:

- If you selected **gRPC** as the protocol, enter the protocol, the address of the proxy server, and optionally the port number in this format: *<protocol>://<server address>*:*<port number>*. For example, `http://exampleserver.com:80`.
- If you selected **HTTPS** as the protocol, the protocol is `HTTPS` by default and you must only enter the address of the proxy server and optionally the port number in this format: *<server address>*:*<port number>*. For example, `exampleserver.com:80`.

Connection / Test Connection

You can test the operation of the connection to M-Files server 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*.

In this chapter

Connecting to and Disconnecting from the Server

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. Open M-Files Admin.
2. Select a connection to M-Files server.
3. Open the **Action** menu.
4. Select **Disconnect**.

To reconnect:

1. Open M-Files Admin.
2. Select a connection to M-Files server.
3. Open the **Action** menu.
4. Select **Connect**.

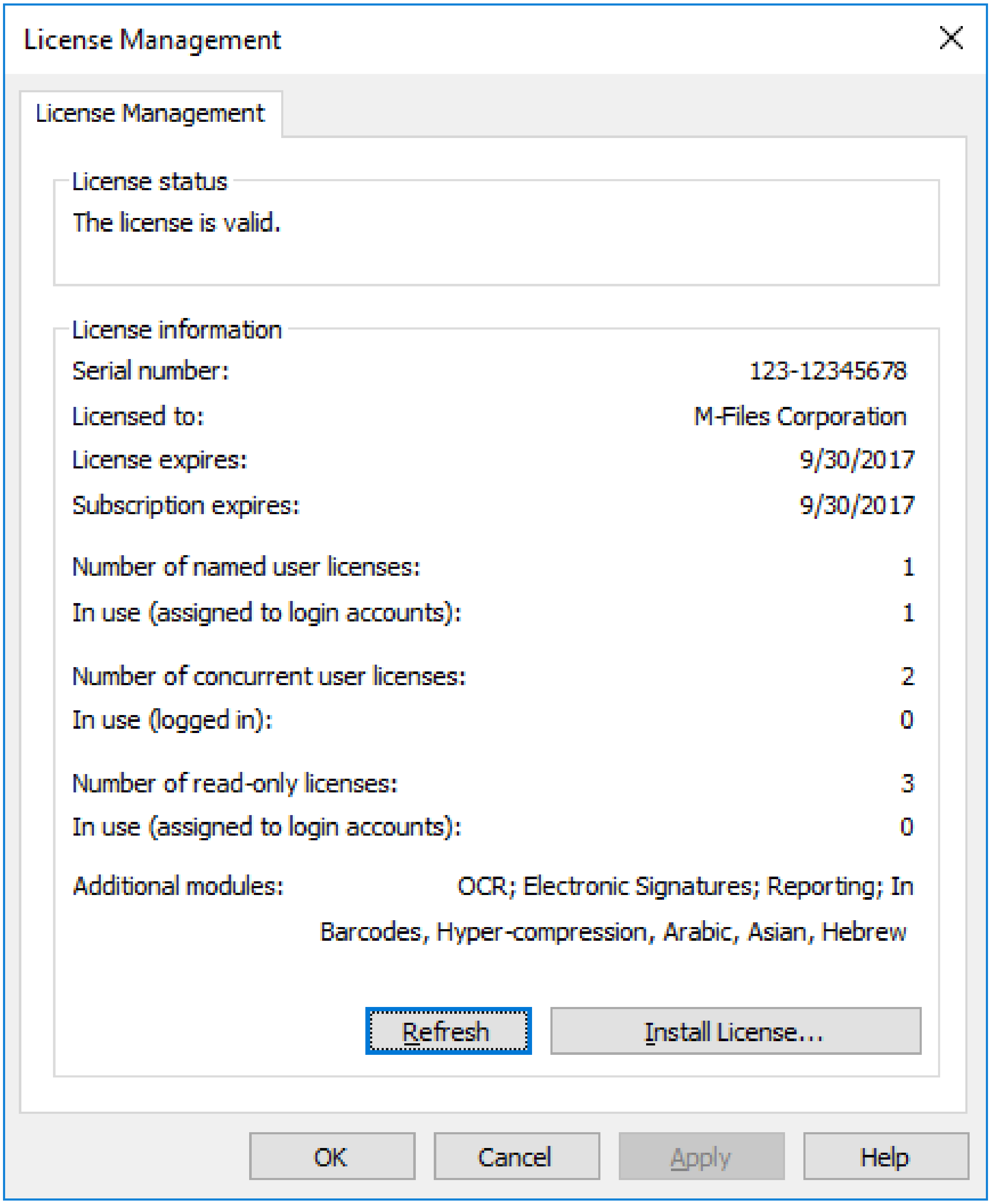
Managing Server Licenses

Note: The information on this page is applicable to on-premises environments only.

Important: If your on-premises subscription uses license automation, it is not necessary to manage server and vault application licenses manually.

To use license automation, make sure that the server's firewall allows outbound traffic to the M-Files licensing server at `https://mfmgmtapiprod.cloudvault.m-files.com` on port 443.

To open license management settings in M-Files Admin, right-click your M-Files server in the left-side tree view and click **License Management**.



License Management

License Management

License status

The license is valid.

License information

Serial number: 123-12345678

Licensed to: M-Files Corporation

License expires: 9/30/2017

Subscription expires: 9/30/2017

Number of named user licenses: 1

In use (assigned to login accounts): 1

Number of concurrent user licenses: 2

In use (logged in): 0

Number of read-only licenses: 3

In use (assigned to login accounts): 0

Additional modules: OCR; Electronic Signatures; Reporting; In

Barcodes, Hyper-compression, Arabic, Asian, Hebrew

Figure 22: 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

If your on-premises subscription uses license automation, the server license is valid for the next 30 days, unless your subscription expires sooner. The validity is refreshed automatically each day.

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 License type.

Number of concurrent user licenses / In use

The number of *concurrent user licenses* in use is determined by the number of currently logged in users 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 of M-Files, the license becomes available. For more information about license types, refer to License type.

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 type.

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, a license is necessary to use M-Files. To install your license, click **Install License** and enter the serial number and license code you have obtained. Then click **OK**.

Login Accounts

The 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 vaults as users. The same server login can be added to several vaults.

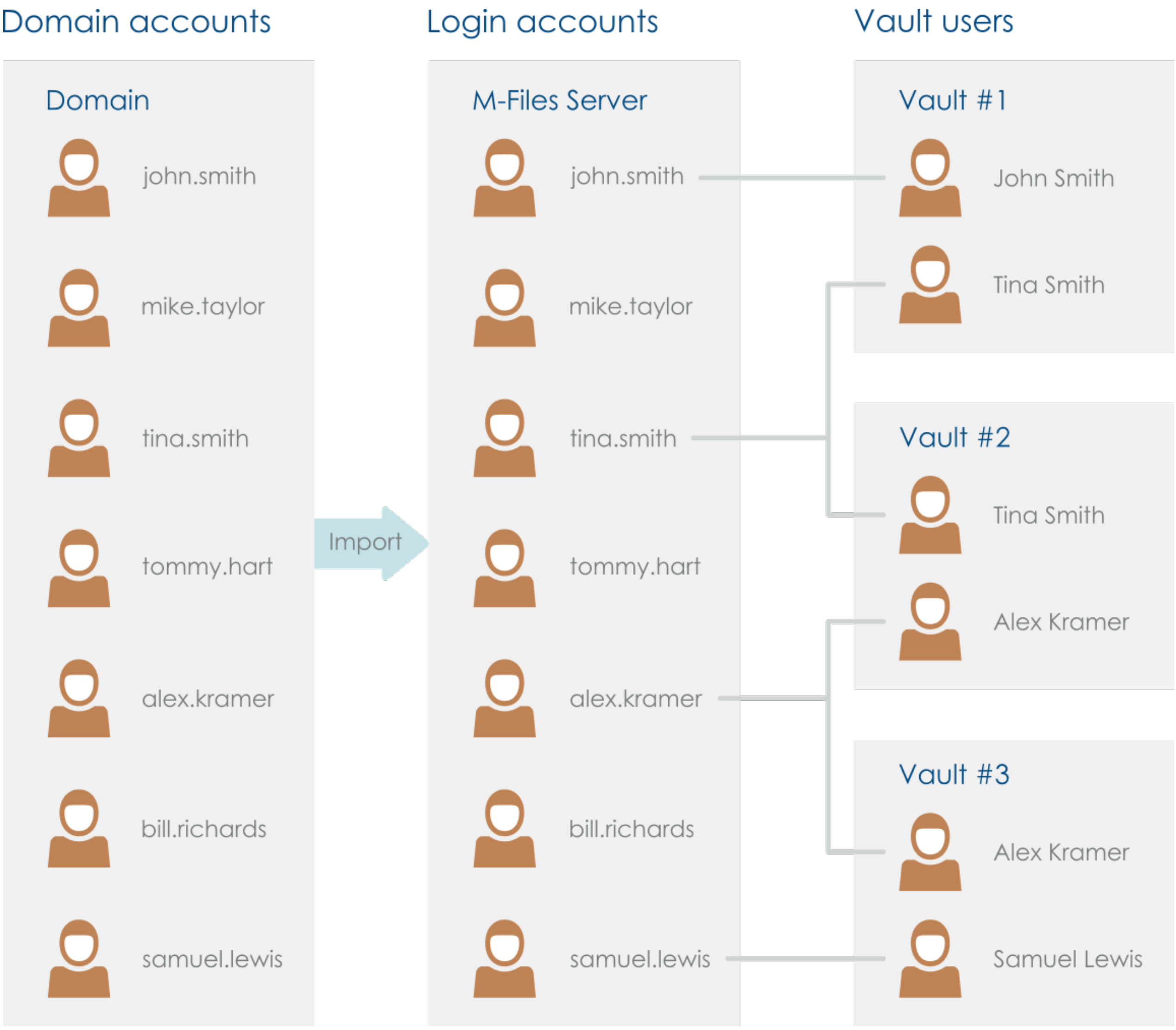


Figure 23: Login accounts are used for authenticating M-Files users to M-Files Server. They can be imported from a domain to M-Files Server. Login accounts are associated with vault-specific users.

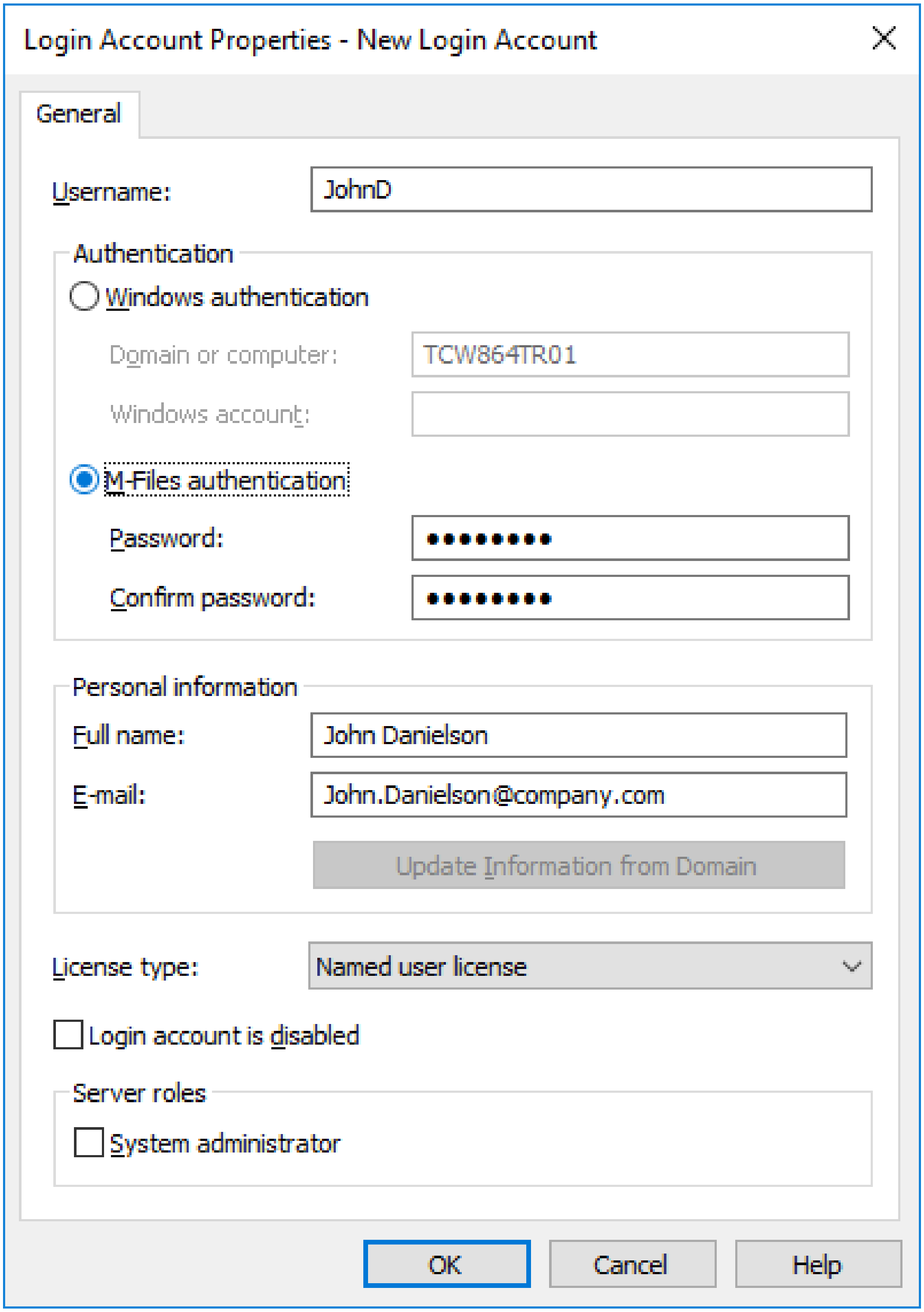
In this chapter

- Login Account Properties
- Creating a Login Account
- Importing Login Accounts
- Creating Application Accounts
- Changing the Login Account of a User
- Editing Many Login Accounts
- Showing Logged-In Users

Login Account Properties

You can create a login account in M-Files Admin when you right-click **Login Accounts** in the left-side tree view and select **New Login Account**. For a step-by-step guide, see Creating a Login Account.

Tip: You can also import Windows login accounts to M-Files. For more information, see Importing Login Accounts.


Login Account Properties - New Login Account
General

Username: JohnD

Authentication

○ Windows authentication

Domain or computer: TCW864TR01

Windows account:

● M-Files authentication

Password: •••••••••

Confirm password: •••••••••

Personal information

Full name: John Danielson

E-mail: John.Danielson@company.com

Update Information from Domain

License type: Named user license

□ Login account is disabled

Server roles

□ System administrator

Figure 24: The new login account creation dialog.

Windows authentication

Windows authentication can be used for authentication on M-Files Server. In this case, the user logs in to the vault with the same login information used to log in to Windows or the domain of the organization.

Domain login is the quickest and easiest authentication method. This means that new passwords and logins are not necessary, which makes this a user-friendly method. For more information, see Differences between the various user authentication methods.

Note: If your organization uses federated identity management, refer to Using Federated Authentication with M-Files.

M-Files authentication

With the M-Files authentication method, the user can log in to M-Files only. If the organization does not have a Windows domain or the user must not have access to it, it is a good idea to use M-Files authentication for the vault.

Personal information

Enter an email address and a full name for the login account. This information is used for sending notifications. For more information about notifications, see Editing Notification Settings in M-Files Admin. If the authentication method used is Windows authentication, you can retrieve the personal information from the domain when you click **Update Information from Domain**.

License type

Select a license type for the login account.

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. Users with a read-only license can only read documents, not create or edit them. However, they can mark an assigment complete and change the workflow state of an object.

External Connector license

External Connector licenses enable third-party systems to anonymously read from or write to M-Files vault through a service account. The license type is necessary, for example, when M-Files data is published programmatically in an intranet or extranet environment to an unrestricted number of users. Anonymous authentication for the new M-Files Web and M-Files Mobile is an example of such use.

You cannot select this license type in the user interface. To get an External Connector license, contact sales@m-files.com.

Account is disabled

This function provides an easy way to specify whether the user can 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

With this role, the user can make any changes on the server level. The user can *change the server logins* and *create* and *delete vaults*. In other words, a system administrator can do any operation on a vault.

Note: In M-Files Cloud, only M-Files employees can make changes on the server level. Thus, you cannot have the system administrator server role in M-Files Cloud. Customer administrators get the **Full control of vault** rights to their vaults.

See the table for a comparison between the permissions of a system administrator and a user with the **Full control of vault** administrative rights. For a description of the administrator permissions in the **Advanced Vault Settings** section of the M-Files Admin configurations editor, see this table.

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
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	Allowed with M-Files Cloud, not allowed on on-premises servers
Migrate to Microsoft SQL Server	Allowed	Not allowed
Manage content replication and archiving settings	Allowed	Allowed to manage cloud storage based replication jobs
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

Operation	System administrator	Vault administrator
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 login accounts	Allowed	Allowed
Manage common views and notification rules	Allowed	Allowed
Manage vault applications	Allowed	Not allowed
Edit scripts (for example related to event handlers, workflow states, and automatic property values)	Allowed	Not allowed
Manage connections to external mail sources	Allowed	Allowed
Manage connections to external file sources	Allowed	Not allowed
Disable or enable vault event logging	Allowed	Not allowed
See and manage scheduled jobs	Allowed	Not allowed
Restart vault	Allowed	Allowed
Enable the Annotations and redlining feature	Allowed	Allowed
Change the vault icon	Allowed	Allowed
See the vault unique ID	Allowed	Allowed

For a system administrator to log in to a vault on the server with M-Files Admin, a user account in that vault is not necessary. However, you can set the system administrator to not have access to vaults and rights to create users in vaults where they do not have a user account. To do this, a specific license is necessary. To get the license, contact licensing@m-files.com. For more information about this feature, contact our customer support in M-Files Support Portal or your M-Files reseller.

Creating a Login Account

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.

3. Click **Login Accounts**.
4. In the task area, click **New Login Account**.

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

5. In **Username**, enter a username.
6. Select an authentication method 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.

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

8. In **License type**, select a license.

   i For information about the license types, see License type.

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**.

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 a connection to M-Files server.
3. Click **Login Accounts**.
4. In the task area, click **Import Login Accounts**.

   ✓ The **Import Login Accounts** dialog is opened.

5. Select either:

   a. **Choose from list** to select the user group using drop-down menus. In **Domain**, select the desired domain. In **Organizational unit**, select the desired organizational unit within that domain. Finally, in **User group**, select the user group that you want to import.

      or

   b. **Enter Name**. This option is especially useful if you have so many user groups that searching the correct one from list is hard. Enter the name of the user group in the format *<domain>**<user group>* and click **Show**.

✓ The list area in the dialog is populated with the members of the selected user group.

6. Optional: Check the **Include users from nested groups** check box to be able to import login accounts from nested groups within the selected user group.

   ✓ The list area in the dialog is populated with the members of the selected user group and the members of any user group nested within the selected user group.

7. Select the login account or login accounts by clicking a login account on the list.

   You can select more than one item at once. Hold down the Ctrl key to select multiple individual items or hold down the ⇧ Shift key to select adjacent items on the list.

8. 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 type.

9. 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 click **Login Accounts** in the left-side tree view in M-Files Admin.

Creating Application Accounts

Application accounts are special login accounts that you can use to set up federated authentication for machine-to-machine integrations. For more information, refer to Application Accounts in the M-Files Manage user guide.

In an on-premises environment, application accounts are created and edited in the **Login Accounts** section in M-Files Admin. For configuration instructions, refer to Configuring OAuth Authentication for Application Accounts in M-Files Support Portal

Changing the Login Account of a User

Sometimes it can be necessary to change the login account for a user. For example, when a user's last name has changed or when login accounts are moved between domains. To keep the user history and the user's personal settings in the vault, do not delete the vault user. Instead, change its login account where necessary. For the differences of these two, see the descriptions of login account and user.

In the M-Files June '24 Update and later, the events that are related to users also include a user account ID. The user account ID stays the same even when the account name is changed.

> ! **Important: Changing login accounts when users are synchronized from Microsoft Entra ID**
>
> If new login accounts are synchronized from Entra ID, M-Files automatically creates new users for the new login accounts. To associate the new login account with the correct existing user, you must first delete the new, automatically created user. Before you do this, make sure that the user has not used the automatically created user account. Otherwise, user settings and history are lost.

Before you begin, make sure that the new login account has been created in M-Files. To change a login account of a user:

1. Open M-Files Admin.

2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Users**.

   ✓ The **Users** list is opened in the right-side pane.
6. Right-click the user whose login account you want to change and select **Properties**.
7. In the **User Properties** dialog, use the **Login account** drop-down menu to select a new login account for the user.
8. Click **OK**.

The new login account is now associated with the existing user. When the user logs in with the new user credentials, their previous user history and personal settings in the vault are available.

Editing Many Login Accounts

You can do some operations on many login accounts at the same time. This is useful if you have a lot of login accounts in M-Files and you want to, for example, change the license type of many login accounts. When you have selected many login accounts, the operations **Enable**, **Disable**, **Delete**, and **Change License Type** are available.

To edit many login accounts:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Click **Login Accounts**.
4. In the list of login accounts, do one of these steps:

   a. To select a range of login accounts, click the first login account, hold down the ⇧ Shift key, and click the last login account.

      or

   b. To select many individual login accounts, click the first login account, hold down the Ctrl key, and select the other login accounts.
5. In the task area, select the action.
6. Optional: If you selected **Delete**, click **Yes** in the dialog that is opened to confirm the operation.

Showing Logged-In Users

In on-premises environments, you can see the currently logged-in users and their license types server-specifically. With cloud vaults, you can see the same information vault-specifically.

Showing logged-in users (on-premises)

To see the users who are currently logged in to an on-premises server:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.

3. Click **Login Accounts**.
4. In the task area, click **Show Logged-in Users**.

   You must have server administrator rights to do this.

The **Logged-in Users** dialog is opened. It shows the users who are currently logged in.

You can also force specific users to log out. To do this, select the user and click **Force Logout**. This can be useful, for example, when concurrent licenses are used: The operation lets you to force the logout of idle users to release the license for someone else to use. Forcing active users to log out, however, normally does not affect them at all. Active users immediately get a license if available licenses exist.

Showing logged-in users (cloud)

To see the users who are currently logged in to a cloud vault:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand the **Document Vaults** section.
4. Select a vault.
5. Click **Show Logged-in Users**.

The **Logged-in Users** dialog is opened. It shows the users who are currently logged in.

You can also force specific users to log out. To do this, select the user and click **Force Logout**. This can be useful, for example, when concurrent licenses are used: The operation lets you to force the logout of idle users to release the license for someone else to use. Forcing active users to log out, however, normally does not affect them at all. Active users immediately get a license if available licenses exist.

Scheduled Jobs

Backups can be automated with **Scheduled Jobs** that you can find at the bottom of the left-side tree structure in M-Files Admin. Backups can be restored later if necessary (see Restoring a Vault).

In this chapter

- Creating a New Scheduled Job
- Scheduled Backup Jobs

Creating a New Scheduled Job

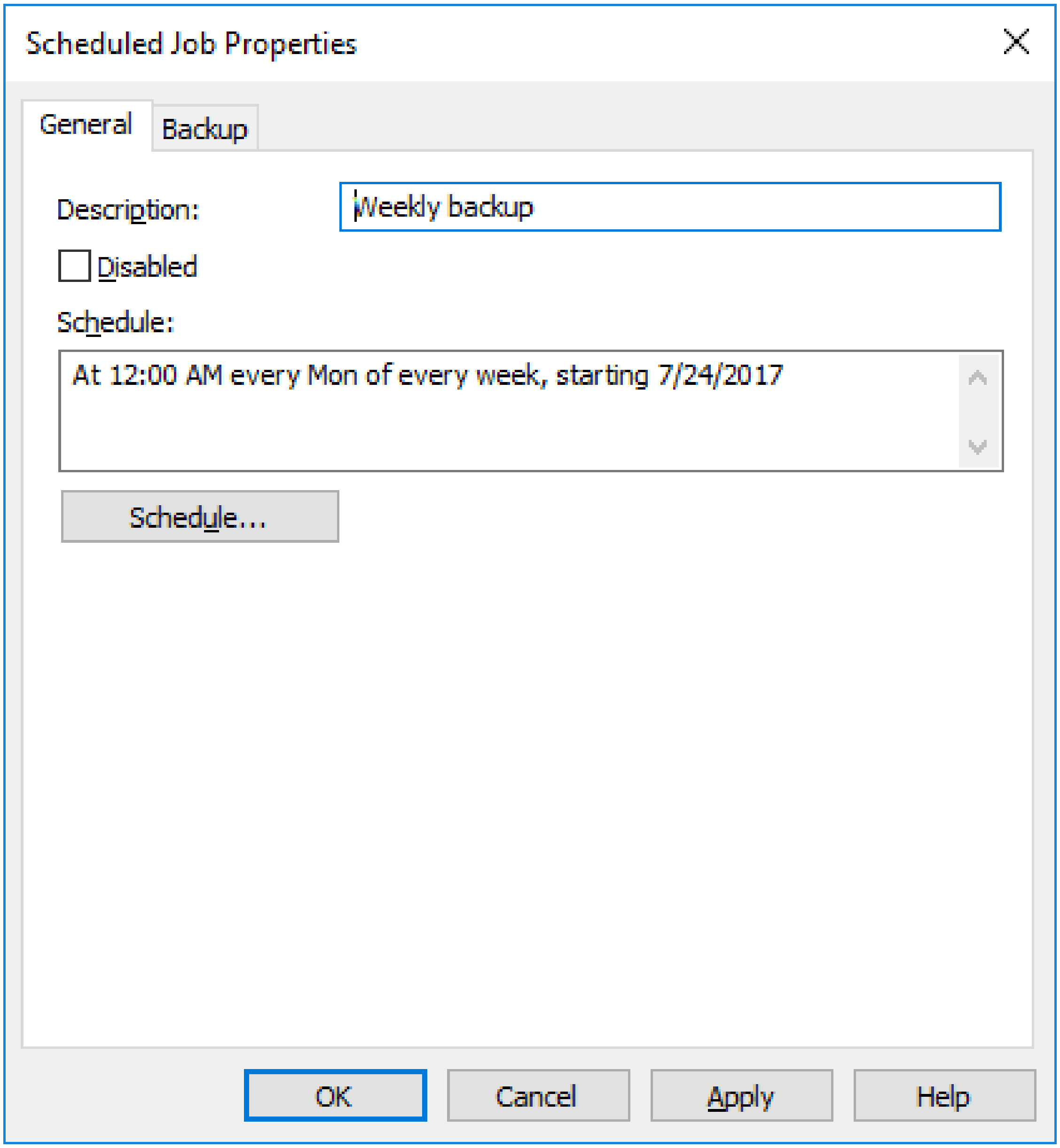
Note: If you are looking for information on scheduled export and import jobs, see Scheduled Export and Import.

Complete the following steps to define a new scheduled backup job:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Click **Scheduled Jobs**.

4. In the task area, click **New Scheduled Backup Job**.

   ✓ The **Scheduled Job Properties** dialog is opened.



Scheduled Job Properties

Description: Weekly backup

□ Disabled

Schedule:

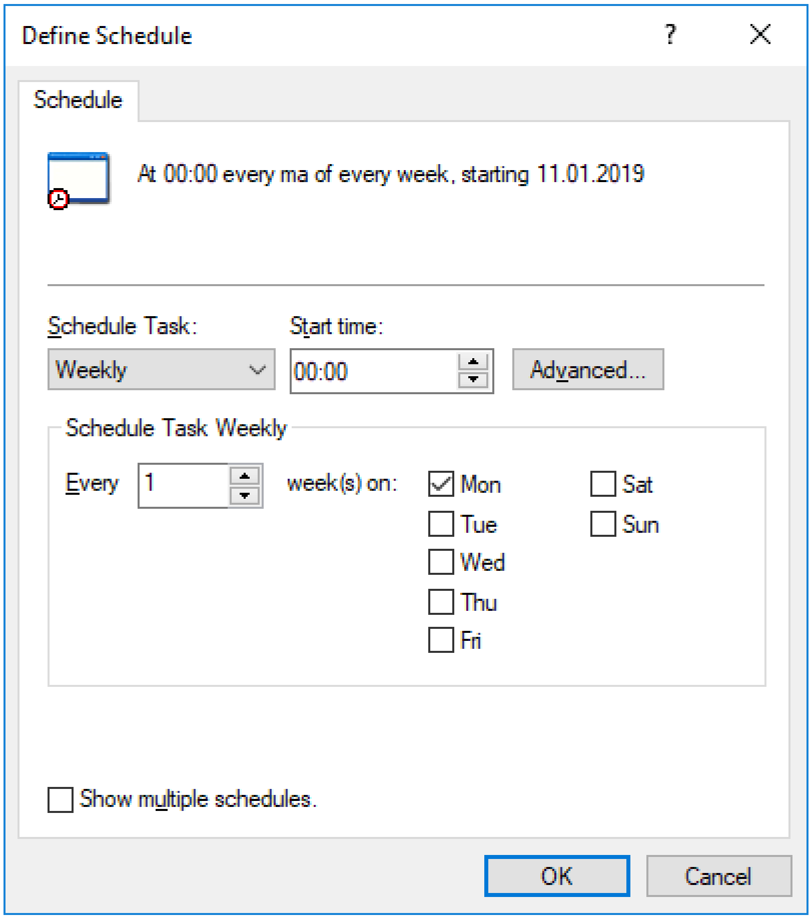
At 12:00 AM every Mon of every week, starting 7/24/2017

5. In the **Description** field, enter a description for the new scheduled job.

6. To define a schedule for this task:

   a) Click **Schedule**.

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



At 00:00 every ma of every week, starting 11.01.2019

Schedule Task: Weekly

Start time: 00:00

Every 1 week(s) on: ☑ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

□ Show multiple schedules.

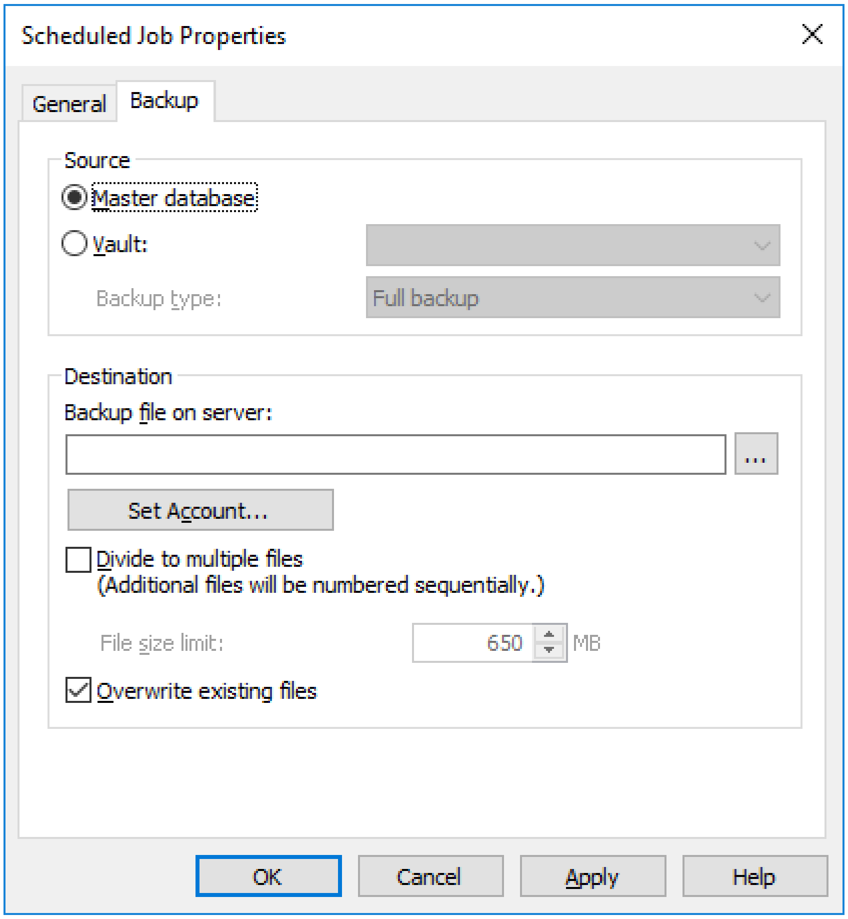
b) Specify the schedule with the available options.

The schedule option **When idle** is not supported in M-Files.

c) Click **OK** to close the **Define Schedule** dialog.

7. Click **Backup** to open the **Backup** tab.

The **Backup** tab is opened.



Source

● Master database

○ Vault:

Backup type: Full backup

Destination

Backup file on server:

□ Divide to multiple files
(Additional files will be numbered sequentially.)

File size limit: 650 MB

☑ Overwrite existing files

8. Select either:

a. **Master database**: Select this option if you want to schedule a backup job for the master database.

or

b. **Vault:** Select this option if you want to schedule a backup job for a document vault. Use the **Vault** drop-down menu to select the vault that you want to back up and the **Backup type** drop-down menu to select either the **Full backup** or **Differential backup** backup type.

> **Note:** 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.

9. Click the **...** button to select the destination of the M-Files backup file (MFB).

10. Optional: Click **Set Account...** to run the task with another account than the Local System account. If the file location is on a network drive that the Local System account cannot get access to, you must set another account. On the **Set Account** dialog:

a) Select **This account**.
b) In **This account**, enter the name of the user account.
c) In **Password** and **Confirm password**, enter the password of the user account.
d) Click **OK** to close the **Set Account** dialog.

11. Optional: If you want to divide the vault backup into multiple files, check the **Divide to multiple files** check box and set the file size limit.

The names of the backup files should not be modified as they might no longer be recognized during a backup operation later on.

12. Optional: Check the **Overwrite existing files** check box if you want your new backup files to replace any existing files with the same file name.

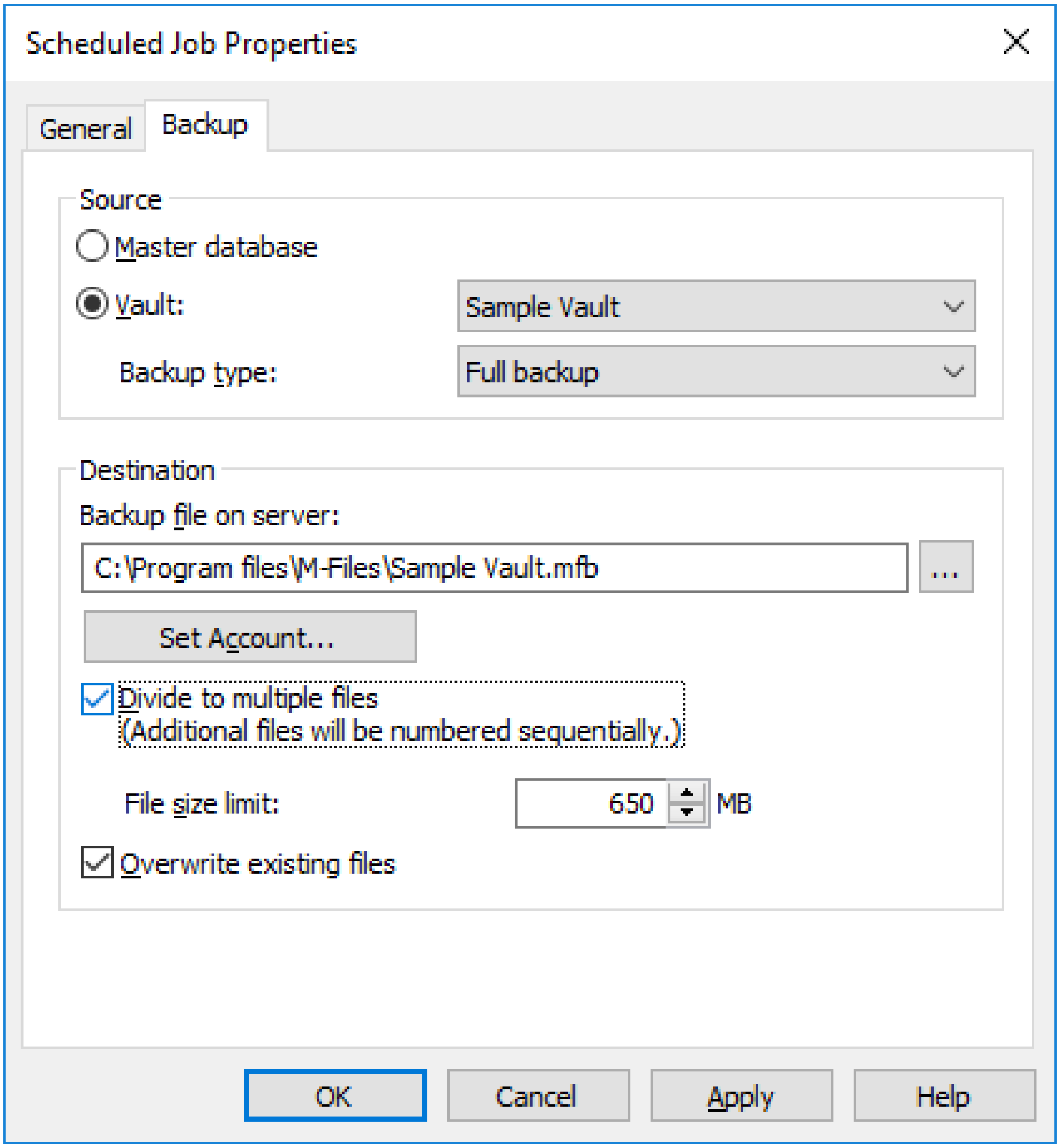
13. Click **OK** to finish creating the scheduled backup job.

The scheduled backup job you have defined is added to the **Scheduled Jobs** list and it is run according to the specified schedule.

Scheduled Backup Jobs

The **Backup** tab of the **Scheduled Job Properties** dialog 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 Vault.



Scheduled Job Properties

General | Backup

Source

○ Master database

● Vault: Sample Vault

Backup type: Full backup

Destination

Backup file on server:

C:\Program files\M-Files\Sample Vault.mfb

Set Account...

☑ Divide to multiple files (Additional files will be numbered sequentially.)

File size limit: 650 MB

☑ Overwrite existing files

Figure 25: 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.

Server Activity Monitor

M-Files Admin includes a tool called Server Activity Monitor for observing events, processes, and tasks executed by vault users or M-Files Server. 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.

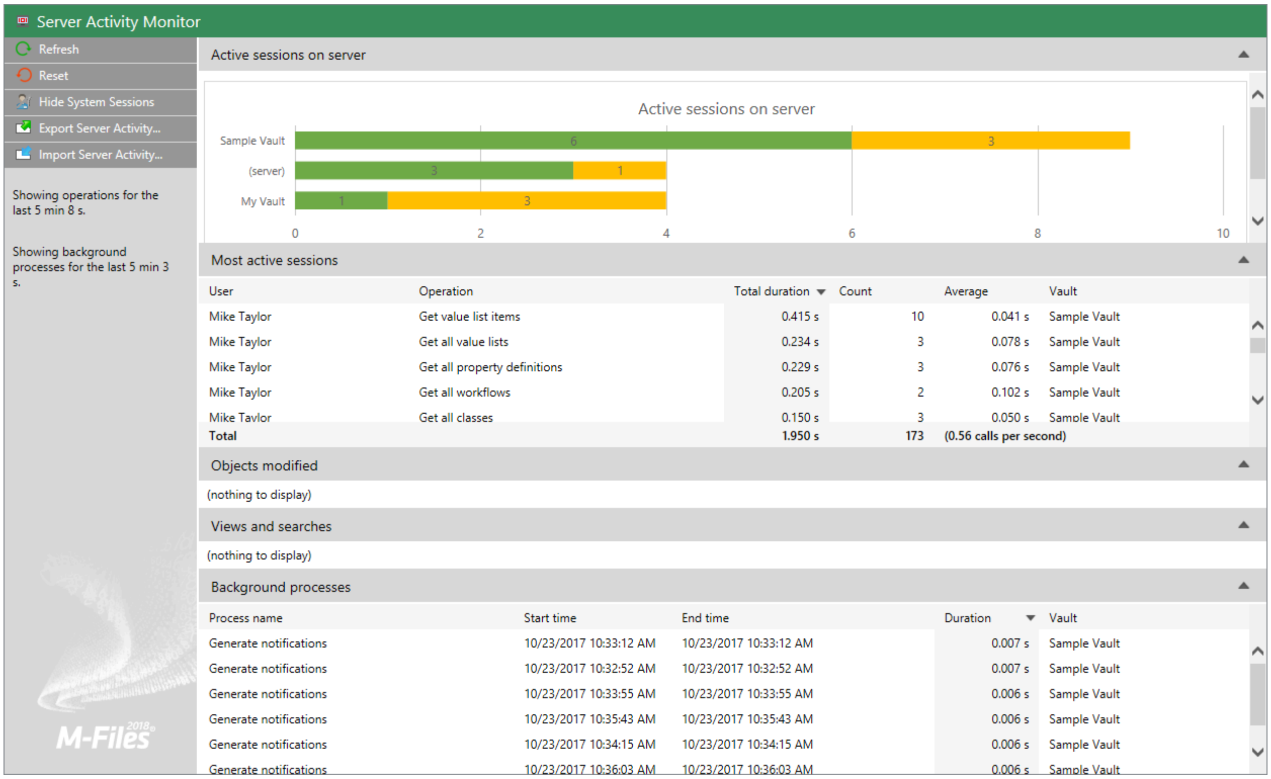
This topic describes the various views included in the monitoring tool, but let's first see how to access Server Activity Monitor in M-Files Admin.

To open the server monitoring tool:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Click **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.



Showing operations for the last 5 min 8 s.

Showing background processes for the last 5 min 3 s.

Most active sessions

User	Operation	Total duration	Count	Average	Vault
Mike Taylor	Get value list items	0.415 s	10	0.041 s	Sample Vault
Mike Taylor	Get all value lists	0.234 s	3	0.078 s	Sample Vault
Mike Taylor	Get all property definitions	0.229 s	3	0.076 s	Sample Vault
Mike Taylor	Get all workflows	0.205 s	2	0.102 s	Sample Vault
Mike Taylor	Get all classes	0.150 s	3	0.050 s	Sample Vault
Total		**1.950 s**	**173**	**(0.56 calls per second)**	

Objects modified

(nothing to display)

Views and searches

(nothing to display)

Background processes

Process name	Start time	End time	Duration	Vault
Generate notifications	10/23/2017 10:33:12 AM	10/23/2017 10:33:12 AM	0.007 s	Sample Vault
Generate notifications	10/23/2017 10:32:52 AM	10/23/2017 10:32:52 AM	0.007 s	Sample Vault
Generate notifications	10/23/2017 10:33:55 AM	10/23/2017 10:33:55 AM	0.006 s	Sample Vault
Generate notifications	10/23/2017 10:35:43 AM	10/23/2017 10:35:43 AM	0.006 s	Sample Vault
Generate notifications	10/23/2017 10:34:15 AM	10/23/2017 10:34:15 AM	0.006 s	Sample Vault
Generate notifications	10/23/2017 10:36:03 AM	10/23/2017 10:36:03 AM	0.006 s	Sample Vault

Figure 26: 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.

Backing Up the Master Database

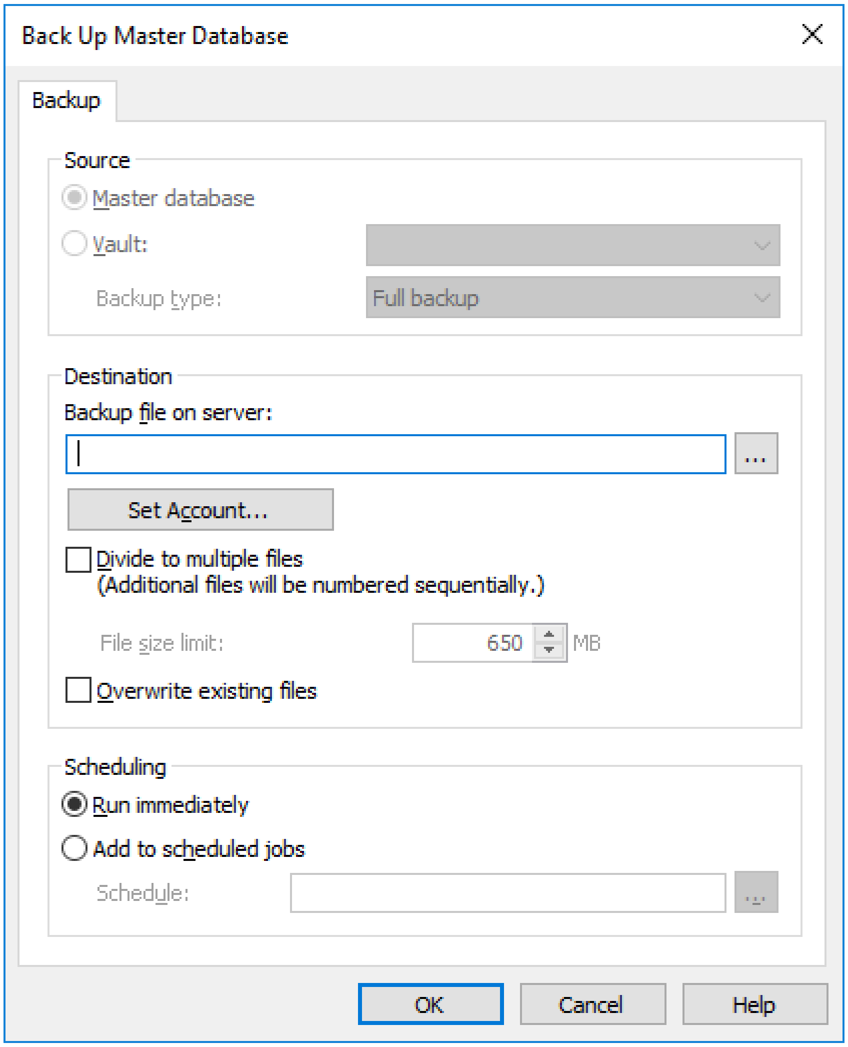
Note: The information on this page is applicable to on-premises environments only.

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.

Complete the following steps to back up the master database:

1. Open M-Files Admin.
2. Right-click a connection to M-Files server.
3. Click **Back Up Master Database**.

   ✓ The **Back Up Master Database** dialog is opened.



Back Up Master Database

Backup

Source

● Master database

○ Vault:

Backup type: Full backup

Destination

Backup file on server:

Set Account...

□ Divide to multiple files
(Additional files will be numbered sequentially.)

File size limit: 650 MB

□ Overwrite existing files

Scheduling

● Run immediately

○ Add to scheduled jobs

Schedule:

4. In the **Destination** section, click **...** to browse for the location where you would like to have the backup file placed.

5. Optional: Click **Set Account...** to run the task with another account than the Local System account. If the file location is on a network drive that the Local System account cannot get access to, you must set another account. On the **Set Account** dialog:
   a) Select **This account**.
   b) In **This account**, enter the name of the user account.
   c) In **Password** and **Confirm password**, enter the password of the user account.
   d) Click **OK** to close the **Set Account** dialog.

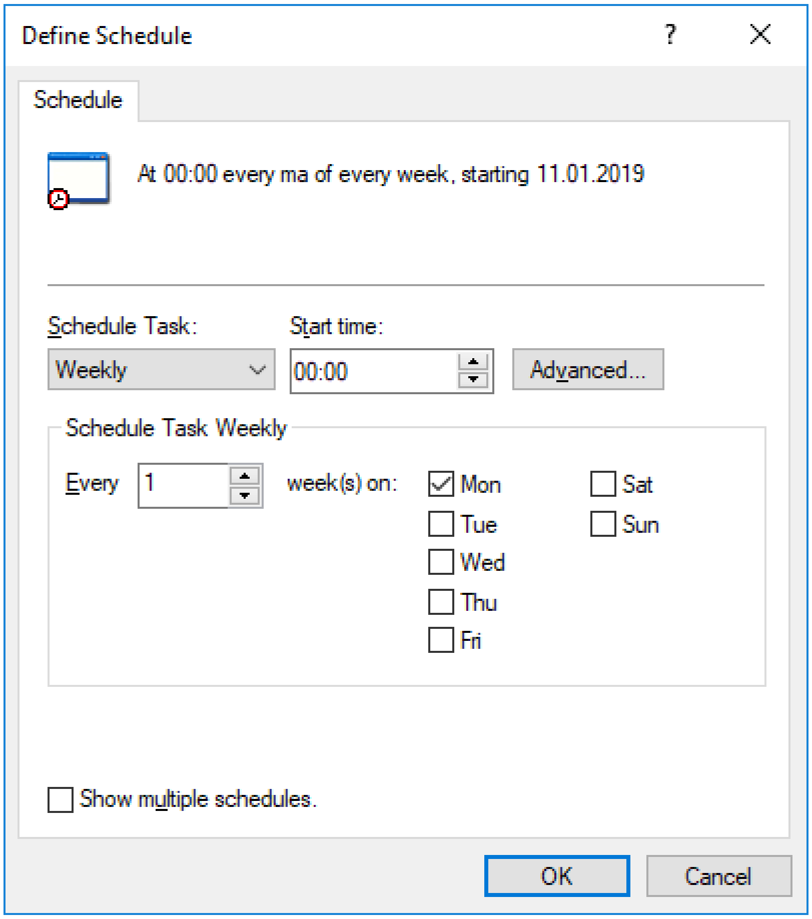
6. Optional: Check the **Divide to multiple files** check box if you want to divide the backup into multiple files of given size.

   ⓘ Use the **File size limit** spinner to specify the size of the split backup files.

7. Optional: Check the **Overwrite existing files** check box if you want to overwrite any existing backup files in the location you have selected.

8. Optional: In the **Scheduling** section, select the **Add to scheduled jobs** option if you want to specify a recurring schedule for backing up the master database.
   a) Click the **...** button.

The **Define Schedule** dialog is opened.



At 00:00 every ma of every week, starting 11.01.2019

Schedule Task: Weekly

Start time: 00:00

Every 1 week(s) on:

☑ Mon
□ Tue
□ Wed
□ Thu
□ Fri
□ Sat
□ Sun

□ Show multiple schedules.

b) Specify the schedule with the available options.

The schedule option **When idle** is not supported in M-Files.

c) Click **OK** to close the **Define Schedule** dialog.

9. Click **OK** to back up the master database.

The master database backup is stored in the location you have selected.

Restoring the Master Database

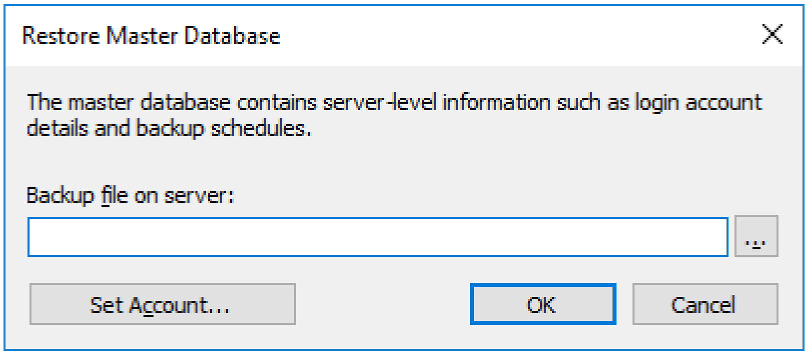
Complete the following steps to restore the master database:

1. Open M-Files Admin.

2. In the left-side tree view, right-click a connection to M-Files server.

3. Click **Restore Master Database**.

The **Restore Master Database** dialog is opened.



Restore Master Database

The master database contains server-level information such as login account details and backup schedules.

Backup file on server:

4. Click **...** to browse for the location of the master database backup file.
5. Optional: Click **Set Account...** to run the task with another account than the Local System account. If the file location is on a network drive that the Local System account cannot get access to, you must set another account. On the **Set Account** dialog:
   a) Select **This account**.
   b) In **This account**, enter the name of the user account.
   c) In **Password** and **Confirm password**, enter the password of the user account.
   d) Click **OK** to close the **Set Account** dialog.
6. Click **OK** to restore the master database.

A confirmation message is displayed after the master database has been restored.

Managing Server Certificates

Note: The information on this page is applicable to on-premises environments only.

Before you set up a server certificate, refer to Setting Up M-Files to Use gRPC in M-Files Support Portal to learn more about server certificates.

Important information

- When you use the gRPC protocol for connections between the M-Files server and M-Files clients, a valid TLS certificate must be in use on the server for connection security and encryption. If the certificate cannot be found, it is outdated, or it will become outdated in a week or less, a warning icon (⚠) is shown in the M-Files Admin user interface.
- Make sure that you have a TLS certificate and a private key for the certificate. For information about digital certificates, refer to information given by certificate authorities. For example, Verisign, IdenTrust, or DigiCert. You can also create your own certificate, for example, with OpenSSL.
- The best practice is to use certificates by well-known public authorities, such as certificates that are commonly used in public web servers. Otherwise, when you use self-signed certificates, you must add the corresponding public keys to the Trusted Root Certification Authorities certificate store of the client computers. This way the signatures can be properly verified on systems that access the M-Files server with gRPC. Make sure that you add the signing certificate under the **Local Computer** and **Current User** certificate stores. The client computer must be able to verify the entire certificate chain. If any of the signatures cannot be verified, the connection cannot be opened.

To set up a server certificate:

1. Open M-Files Admin.
2. Right-click a connection to M-Files server.

3. Click **Manage Server Certificate**.

   ☑ The **Server Certificate Management** dialog is opened.

4. Enable the option **Use a TLS certificate**.
5. Under the **Private Key** section, click **Change**.

   ☑ An **Open** dialog for selecting the private key is opened.

6. Locate and double-click a valid private key (a `KEY` file) to put it to use.

   ⓘ EC and RSA certificates are supported. EC keys must be in the PKCS#8 format and RSA keys in the PKCS#1 format.

   ⓘ For more information, refer to the server certificate section in Setting Up M-Files to Use gRPC.

7. Under the **Certificate** section, click **Change**.

   ☑ An **Open** dialog for selecting the certificate file is opened.

8. Locate and double-click a valid TLS certificate (a `CRT` file) to put it to use.

   ⓘ The certificate must be in `PEM` (Privacy-Enhanced Mail) format.

9. Make sure the certificate details are as expected and click **OK**.

The certificate is now in use for connections between the M-Files server and M-Files clients.

3.1.6. Managing Document Vaults

This section describes how you can create, operate and maintain document vaults, and deals with various other aspects closely related to document vaults, such as content replication, vault languages, and connections to external databases.

In this chapter

Vault Operations

This section provides instructions for various administrative document vault operations, such as creating, copying, backing up, or restoring a document vault, or restarting a vault, which is an operation that must be occasionally carried out to make vault configuration changes effective.

In this chapter

Creating a Vault

Creating a vault in M-Files Cloud

In M-Files Cloud, you can create a vault in M-Files Manage. For instructions, refer to Creating a Cloud Vault in the M-Files Manage user guide.

Creating a vault in on-premises environments

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 with Windows Task Manager before you create the vault. For instructions on changing the software language, see Selecting the Software and Vault Language.

See Important Tasks after Installation, Vault Creation, or Vault Migration for a checklist of tasks that we recommend to be done with vault creation.

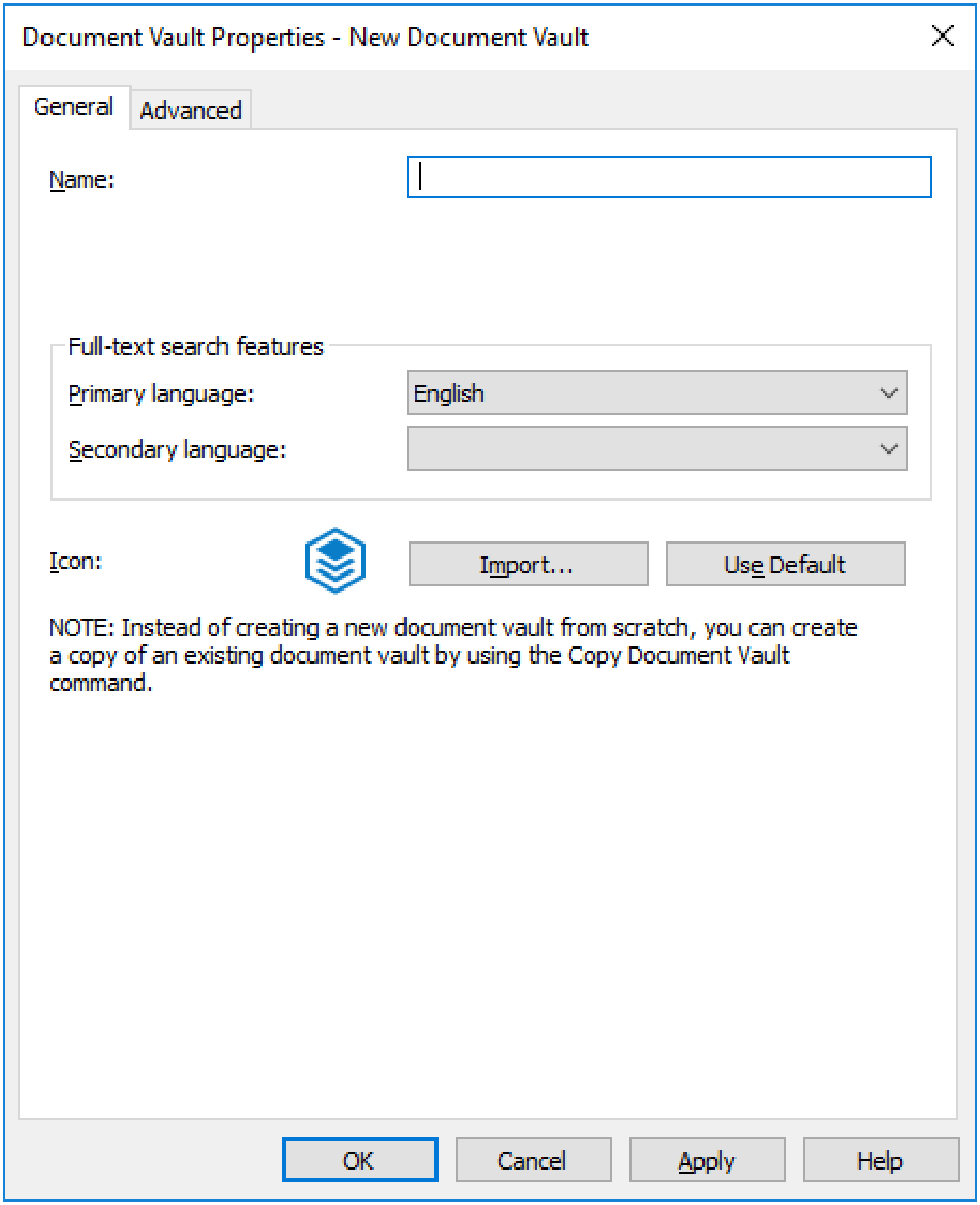
To create a vault:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Click **Document Vaults**.

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

4. In the task area, click **New Document Vault**.

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



Name:

Full-text search features

Primary language: English

Secondary language:

Icon:

NOTE: Instead of creating a new document vault from scratch, you can create a copy of an existing document vault by using the Copy Document Vault command.

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 if 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 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. For instructions, see Adding a Vault Connection.

In this chapter

- Document Vault Advanced Properties
- Document Vault Authentication

Document Vault Advanced Properties

On the **Advanced** tab of the **Document Vault Properties** dialog, you can define whether you want to use 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 can cause faulty operation of the software and loss of data. The structure and contents of the document vault may only be modified with the M-Files clients, M-Files Admin, and M-Files API.

Firebird

See Using Firebird as the Database Engine.

Microsoft SQL Server

See Using Microsoft SQL Server as the Database Engine.

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 for Value List Items. You can activate the automatic permissions by value, value list, object type, or class. To use the automatic permissions through a specific property, also allow this in the property definition's properties. For more information, see New Property Definition.

Enable file data encryption at rest

This option lets you 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. For more information, refer to Protecting File Data at Rest with Encryption in M-Files.

Before you enable the feature, please take note of this important information:

- Make sure that you have enough disk space. See Disk space needed for encrypting file data at rest.
- This option only encrypts file data that is stored to the vault after the feature has been enabled. Thus, after you have enabled the feature, you must run the **Update encryption status of existing files** operation to encrypt all existing files in the vault.
- We recommend that you make sure that the users of the vault have no objects checked out to them.

Objects that contain at least one file and have never been checked in can no longer be checked in after the vault file data has been encrypted. If this issue occurs, the files are still available on the client machine, but they cannot be made available for other vault users. Additionally, M-Files Server stores the files in unencrypted format and no vault maintenance operation will delete them.

After you have enabled the feature, do these steps to encrypt the 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**.
3. Manually run the **Optimize Database (Thorough)** operation to remove the unencrypted file data of the vault. If the option **Delete the files of destroyed objects** is available, select it.

   > **Note:** The scheduled automatic optimization does not remove the unencrypted file data.

File data encryption is not visible for the users.

Especially when encryption is enabled, it is crucial to have thorough and frequent backup 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.

Advanced Event Log features

With this option, you can activate the audit trail features for this vault. M-Files supports the administration of electronic records and signatures in compliance with FDA 21 CFR Part 11. Electronic signing requires the Electronic Signatures and Advanced Logging module, which is available for a separate fee. The module includes event logging extensions and the electronic signature functionality. For more information, see Electronic Signing and Compliance.

For a list of the event types recorded to the event log, see Event Types.

Tip: If you want to give system administrators more visibility into actions that vault users perform in a vault, see User Action Log.

Annotations and redlining

The *Annotation and redlining* feature enables you to add annotations to documents in the document vault. You can enable the annotations and redlining feature by checking the **Annotations and redlining** check box in the **Document Vault Properties** dialog. For more information about annotations in M-Files, see Annotations and Redlining.

M-Files Web

Enter the URL to your M-Files Web home page. M-Files requires this to include M-Files Web URLs in hyperlinks and M-Files Web links in notification messages.

Make sure that the URL starts either with `http://` or `https://`. For example: `https://myserver.mydomain.com`.

Classic M-Files Web

Enter the URL to your classic M-Files Web home page. M-Files requires this to include classic M-Files Web URLs in hyperlinks and classic M-Files Web links in notification messages.

Make sure that the URL starts either with `http://` or `https://`. For example: `https://myserver.mydomain.com`.

In this chapter

Using Firebird as the Database Engine

Firebird is an SQL database engine integrated in M-Files.

M-Files uses Firebird as the default vault database engine. We recommend that Microsoft SQL Server is used if the vault contains 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 and the size of the metadata file has since then significantly increased, migrate the vault database to Microsoft SQL Server.

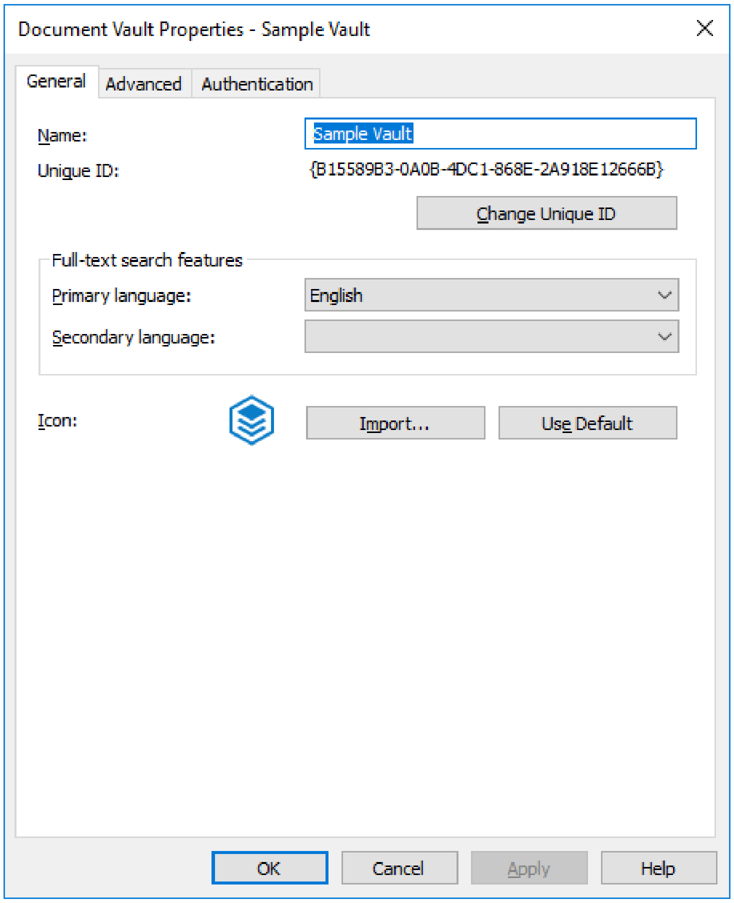
We recommend that you start to plan migration to Microsoft SQL Server when the size of the metadata file for a vault is close to 1 GB. For instructions on checking the metadata file size, see Checking the Size of a Firebird Metadata File.

You can apply a registry setting to extend Firebird usability to 2 GB per vault. You can use Firebird also after this limit has been exceeded, but, for performance reasons, Microsoft SQL Server is in this case the recommended database engine.

To open the vault settings for the Firebird engine:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Right-click a vault.
5. Click **Properties**.

   ✓ The **Document Vault Properties** dialog is opened.



Document Vault Properties - Sample Vault

Name: Sample Vault

Unique ID: {B15589B3-0A0B-4DC1-868E-2A918E12666B}

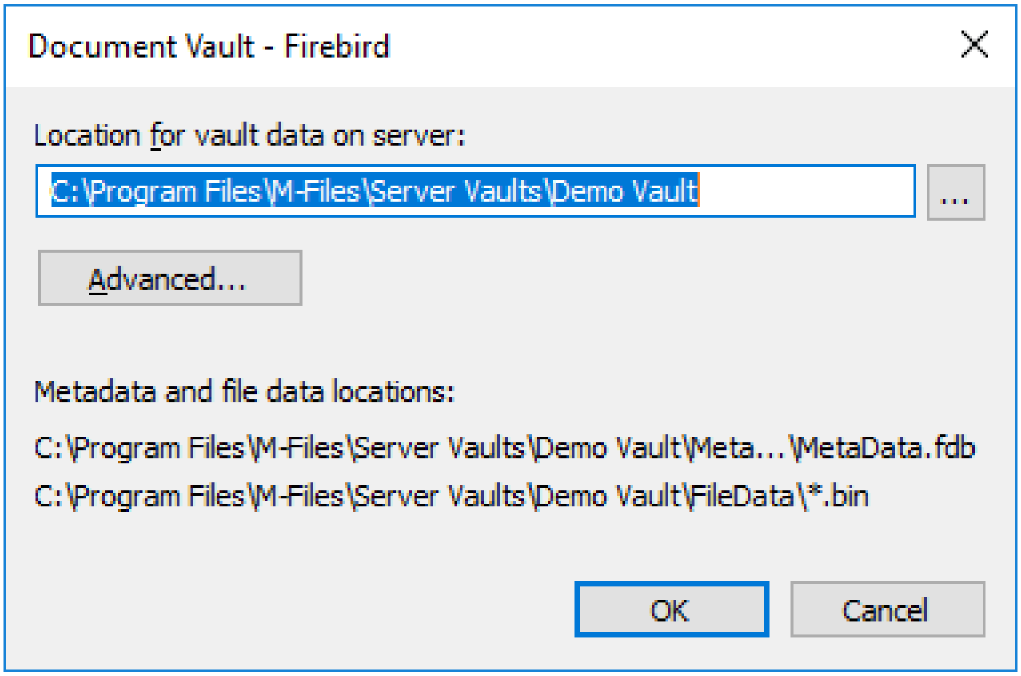
Full-text search features

Primary language: English

Secondary language:

6. Open the **Advanced** tab.
7. Click **Define...** under the **Use Firebird** option to open the settings for the Firebird engine.

   ✓ The Firebird settings dialog is opened.



Location for vault data on server: C:\Program Files\M-Files\Server Vaults\Demo Vault

Metadata and file data locations:

C:\Program Files\M-Files\Server Vaults\Demo Vault\Meta...\MetaData.fdb

C:\Program Files\M-Files\Server Vaults\Demo Vault\FileData*.bin

On the Firebird settings dialog, you can do these operations:

- Changing the Location of the Vault Data
- Defining A Separate Location for Vault File Data

Changing the Location of the Vault Data

If necessary, you may change the default location of the vault data, that is, the *file data* and the *metadata* of the vault. Note that the vault metadata must be stored on the local drive of the M-Files Server computer. If you wish to store the *file data* of the vault in a separate location (which can be, for example, a network drive), see Defining A Separate Location for Vault File Data.

Before you begin, take the vault offline for the duration of the operation. For instructions, see Taking a Vault Offline.

To change the location of vault data:

1. Open the vault database engine settings.

   The current location of the vault data is shown in the vault database engine settings dialog.

2. Using File Explorer or any other file manager, copy the `FileData` and the `MetaData` folders from their current location to the new location.
3. Click the **...** button to browse for the new file data location.

   The **Browse For Folder** dialog is opened.

4. Select the new location for vault data, and then click **OK** to close the **Browse For Folder** dialog.

   Note that the selected location should be on the local drive of the M-Files Server computer and it should contain the `FileData` and `MetaData` folders.

5. Click **OK** to close the vault database engine dialog, and finally click **OK** to close the **Document Vault Properties** dialog.

After the operation is complete, bring the vault back online. For instructions, see Bringing a Vault Online.

Defining A Separate Location for Vault File Data

By default, vault file data is stored in the same folder as vault metadata. If necessary, you can define a separate location for the file data of the vault. This enables you to locate your file data on a large network drive or file server. It is, however, recommended to store the metadata and files in the same location.

Before you begin, take the vault offline for the duration of the operation. For instructions, see Taking a Vault Offline.

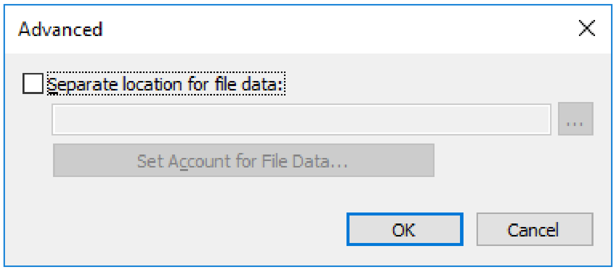
To define a separate location for file data:

1. Open the vault database engine settings.

   The current location of the vault file data is shown in the vault database engine settings dialog.

2. Using File Explorer or any other file manager, copy the folder `FileData` from its current location to the new location.
3. Click the **Advanced...** button.

   ✓ The **Advanced** dialog is opened.


Advanced
□ Separate location for file data:
...
Set Account for File Data...
OK
Cancel

4. Enable the **Separate location for file data** option.
5. Click the **...** button to browse for the new file data location.

   ✓ The **Browse For Folder** dialog is opened.

6. Select the new location for vault file data, and then click **OK** to close the **Browse For Folder** dialog.

   Note that the selected location should contain the `FileData` folder. The location can also be a UNC path to a network drive.

7. Optional: Click **Set Account for File Data...** to select the account that M-Files Server uses for accessing the vault file data. This may be necessary if the local system account does not have permission to access the selected location.
   a) Select the **This account** option.
   b) In the **This account** field, specify the account that M-Files Server should use for accessing vault file data in the selected location.
   c) In the **Password** and **Confirm password** fields, enter the password of the account.
   d) Click **OK** to close the **Set Account** dialog.
8. Click **OK** to close the **Advanced** dialog.
9. Click **OK** to close the vault database engine dialog, and finally click **OK** to close the **Document Vault Properties** dialog.

After the operation is complete, bring the vault back online. For instructions, see Bringing a Vault Online.

Using Microsoft SQL Server as the Database Engine

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

With Microsoft SQL Server, the database server memory can be more efficiently used and the backup storage of large data vaults is improved. You can also switch to the mirrored database server without delay if necessary.

Note: Microsoft SQL Server licenses are not included in M-Files licenses. They must be purchased separately.

Migration to Microsoft SQL Server

See Migrating the Vault Database to Microsoft SQL Server.

In this chapter

Supported Microsoft SQL Server Versions

You can use Microsoft SQL Server as the vault database engine. Refer to our lifecycle policy for information about the supported versions. These editions are supported: Microsoft SQL Server Express, Standard, and Enterprise. Refer to Microsoft documentation to make sure that your Microsoft SQL Server edition has the necessary features and capabilities for your environment. M-Files supports the use of Microsoft SQL Server on Microsoft Windows.

With the Microsoft SQL Server Enterprise Edition versions 2008–2017 table data and indexes can be compressed. 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 2016 Service Pack 1 and later support updateable columnstore indexes (in earlier versions, columnstore indexes are only available in Enterprise Edition). This enables better performance with sub-levels of views (such as **Documents by project**). This is especially beneficial when empty virtual folders are set to be hidden.

Guidelines for version selection, updates, and upgrades

- When you take Microsoft SQL Server into use as the database engine, we recommend that you use the latest version of Microsoft SQL Server that M-Files and your operating system support. For Microsoft SQL Server software requirements, refer to Microsoft documentation.
- Make sure that the server machine always has the latest service pack and cumulative updates installed. To do this, refer to Latest updates for Microsoft SQL Server.
- To upgrade your version of Microsoft SQL Server, refer to Upgrade SQL Server.

Configuring Microsoft SQL Server Databases

M-Files supports the use of Microsoft SQL Server on Microsoft Windows. With a cloud-based M-Files environment that you manage yourself, you can also use Microsoft Azure SQL Database Managed Instance as the vault database engine.

Microsoft SQL Server can 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. For instructions on the efficient operation of SQL Server, refer to Microsoft SQL Server documentation.

Make sure 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.

Before you take Microsoft SQL Server into use as the database engine, see Microsoft SQL Server Requirements and Database engine and data storage.

> ❗ **Important:** If your SQL Server does not use the default port, `1433`, you must give the server name in the format *<server name>*`,`*<port>*.

M-Files Server stores data in the vault in the associated database. Certain secondary data that do not require a backup, such as search indexes, are left outside the database.

Instructions for specialized setups

Refer to these documents in specialized Microsoft SQL Server environments:

- Setting M-Files to Operate Without Sysadmin Role in Microsoft SQL Server
- Setting up M-Files vault databases to SQL Server AlwaysOn Availability Group

File data location

File data can be saved in the Microsoft SQL Server database or other location, such as a network drive.

Select one of these options:

- **Store file data in the vault database**
- **Store file data in a file-system folder**: With this option, you can specify the location for saving the files to a network drive or to another location. You can set a specific account for processing the file data to keep the file data secure.

  > ❗ **Important:** If you want to use a network drive for storing file data, you must use the format `//`*`<server>`*`/`*`<path>`* to specify the file data location.

  > **Note:**
  >
  > The vault remains online and fully operational for the majority of the duration of changing the file data location. Only when the new file data location is taken into use, is the vault offline for the duration of taking the new location into use. If you cancel the operation of changing the file data location, you can always resume it by selecting the same location as you previously selected for file data.

For more instructions, see Changing the Location of the Vault File Data for Microsoft SQL Server.

Backing Up Microsoft SQL Server Databases

The administrator is responsible for making backup copies and timing the backup copies of the vault database. Backup copying is done with SQL Server's own management tools and backup copying solutions offered by third parties. When restoring a backup copy, the administrator first returns the vault database to the SQL Server, and then reattaches the vault to M-Files with the Attach Document Vault function.

If your file data is stored on the file system separately from the database, you must back up both the Microsoft SQL database and the files on the file system separately.

For more instructions, see the M-Files knowledge base article M-Files Backup Policy.

Important information

- Always back up the SQL database (metadata) first and then the file system data (object files) to avoid references to non-existing object files. Do not run M-Files Server optimization after you have backed up the SQL database. Otherwise, the files that have been marked for destruction are removed.
- Do not back up an active M-Files system with a snapshot of the file system where its data is stored. This can create a damaged or unusable backup because write operations to files (most importantly, the database engine files) can be ongoing and, thus, incomplete. If you use full virtual machine (VM) snapshots for backups, make sure that the VM software fully supports creation of snapshots of an active system. This means that the software can restore the system to exactly the same state, including the memory and CPU states.

Changing the Location of the Vault File Data for Microsoft SQL Server

If you use Microsoft SQL Server and your file data of the vault is stored either in the vault database or the file system, you may change the location of the vault file data.

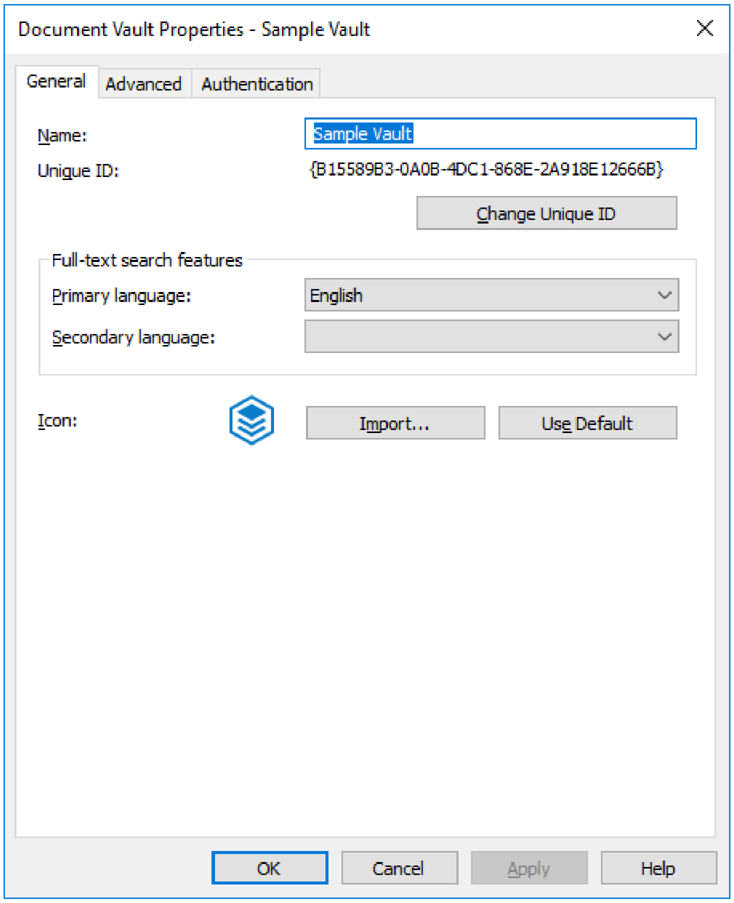
Note:

The vault remains online and fully operational for the majority of the duration of changing the file data location. Only when the new file data location is taken into use, is the vault offline for the duration of taking the new location into use. If you cancel the operation of changing the file data location, you can always resume it by selecting the same location as you previously selected for file data.

To change the location of the vault file data:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Right-click a vault.
5. Click **Properties**.

   ✓ The **Document Vault Properties** dialog is opened.


Document Vault Properties - Sample Vault

Name: Sample Vault

Unique ID: {B15589B3-0A0B-4DC1-868E-2A918E12666B}

Full-text search features

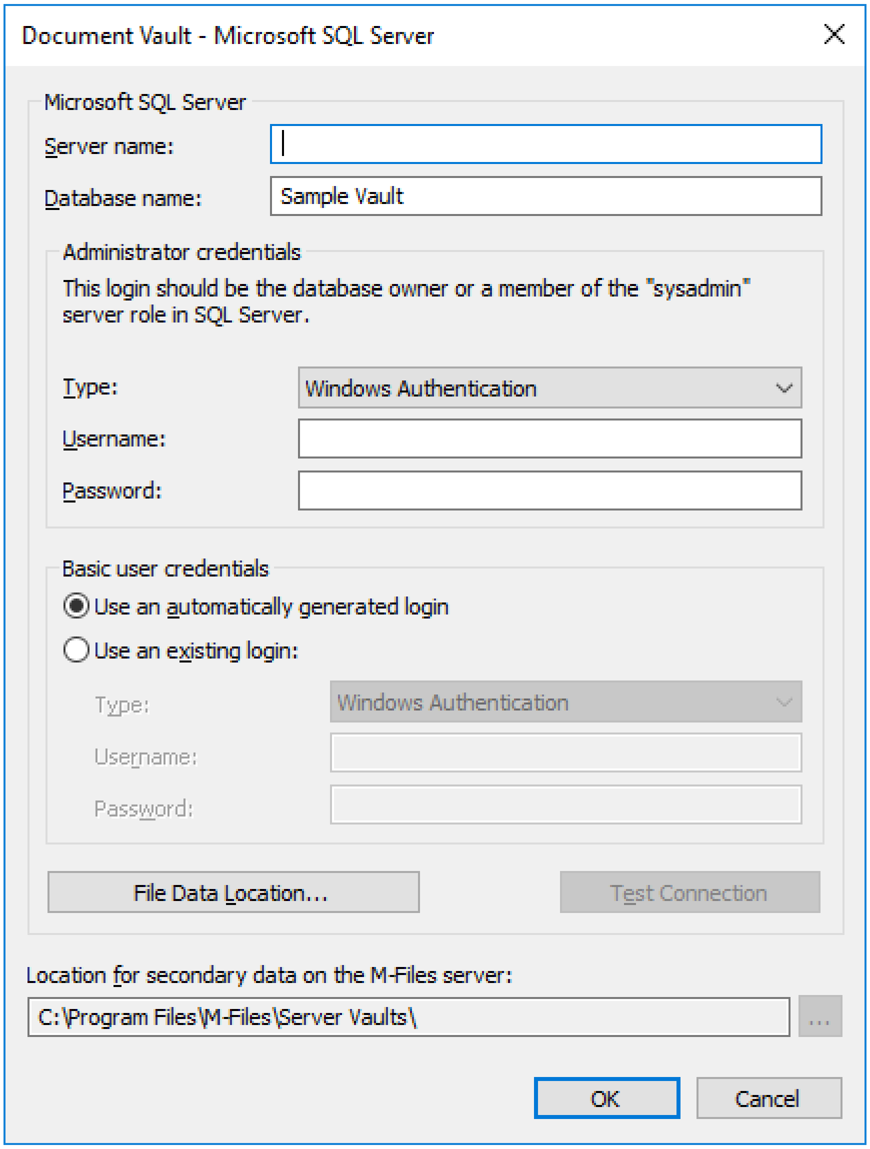
Primary language: English

Secondary language:

Icon:

6. Open the **Advanced** tab.
7. Under the **Use Microsoft SQL Server** option, click the **Define...** button.

✓ The **Document Vault - Microsoft SQL Server** dialog is opened.



Document Vault - Microsoft SQL Server

Microsoft SQL Server

Server name:

Database name: Sample Vault

Administrator credentials

This login should be the database owner or a member of the "sysadmin" server role in SQL Server.

Type: Windows Authentication

Username:

Password:

Basic user credentials

● Use an automatically generated login

○ Use an existing login:

Type: Windows Authentication

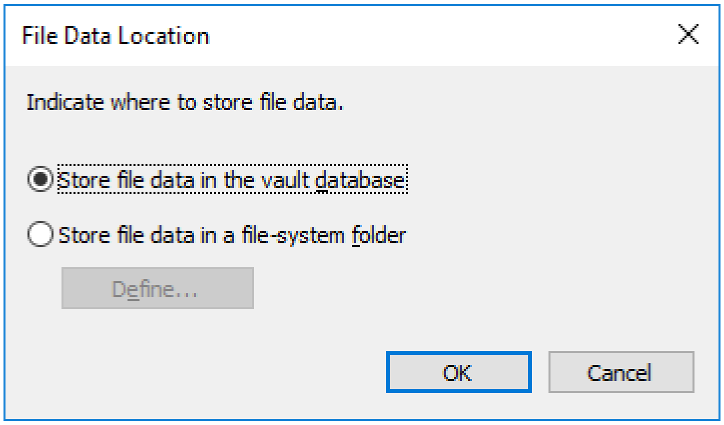
Username:

Password:

Location for secondary data on the M-Files server: C:\Program Files\M-Files\Server Vaults\

8. Click the **File Data Location...** button.

✓ The **File Data Location** dialog is opened.



File Data Location

Indicate where to store file data.

● Store file data in the vault database

○ Store file data in a file-system folder

9. Either:

a. If you want to change the location of the vault file data from the vault database to the file system, or from one folder in the file system to another, select the option **Store file data in a file-system folder** and then click the **Define...** button.

   or

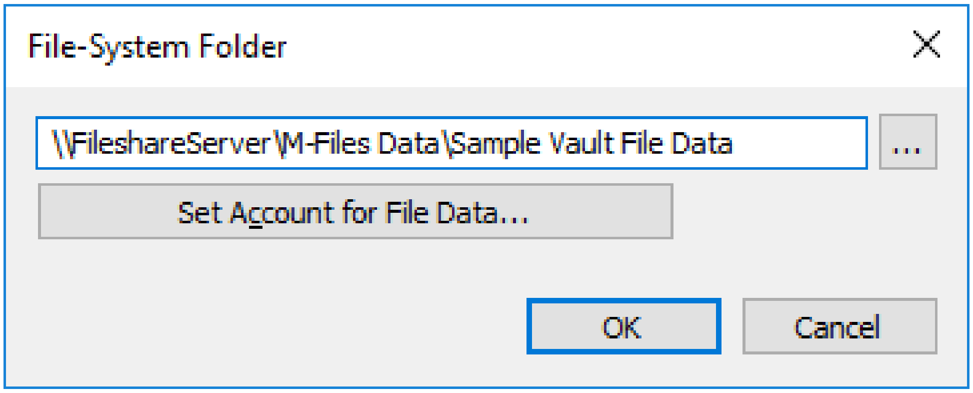
b. If you want to change the location of the vault file data from the file system to the vault database, select the option **Store file data in the vault database** and then click **OK**.

10. If you selected the option **Store file data in a file-system folder**, complete the following steps:

a) Optional: If you are changing the vault file data location from one folder in the file system to another, using File Explorer or any other file manager, copy the `FileData` folder from its current location to the new location.

b) In the **File-System Folder** dialog, click the **...** button to browse for the new file data location, or type in the location in the text field.

   ⓘ The location can also be a UNC path to a network drive.



File-System Folder

\\FileshareServer\M-Files Data\Sample Vault File Data

c) Optional: Click **Set Account for File Data...** to use an account other than the Local System account for accessing file data.

   ⓘ Setting the account may be necessary especially if the file data is located on a network drive that the Local System account cannot access.

d) Click **OK** to close the **File-System Folder** dialog.

11. Click **OK** to close the **File Data Location** dialog and the vault database engine dialog, and finally click **OK** to close the **Document Vault Properties** dialog.

12. If you are changing the vault file data location from the vault database to the file system, or from the file system to the vault database, you are prompted to confirm that you want to change the file data location. Click **Yes**.

☑ The file data of the vault is then copied to the new location.

Your vault now uses the specified location for storing and accessing the file data of the vault.
Document Vault Authentication

The **Authentication** tab of the **Document Vault Properties** dialog contains settings related to vault user synchronization and authentication with Microsoft Entra ID. The tab is available in the **Document Vault Properties** dialog of existing vaults. When you create a vault, you cannot see this tab.

User synchronization

For information about user synchronization, see User Synchronization with Microsoft Entra ID.

User authentication

Refer to the specified instructions in this table to set up user authentication in your environment:

Deployment	Instructions
M-Files Cloud and Microsoft Entra ID	Setting up federated authentication with Microsoft Entra ID in the M-Files Manage user guide.
On-premises server and Microsoft Entra ID	Configuring Vault Authentication with Microsoft Entra ID in On-Premises Environments
Any environment and any OAuth 2.0 or OpenID Connect compliant identity provider	Configuring OpenID Connect and OAuth 2.0 for M-Files Authentication

Additional information:

- In M-Files Cloud, Entra ID is automatically configured for vaults created in M-Files Manage.
  - In M-Files Cloud, refer to Configuring Vault Authentication with M-Files Login Service to manually set up authentication through M-Files Login Service.
  - If the vault has been migrated from on-premises, see M-Files Cloud Requirements.
- If you use M-Files Web or the add-ins based on M-Files Web, also refer to Setting Up OAuth 2.0 for the New M-Files Web and Web-Based Add-Ins.
- In on-premises environments, also refer to Configuring OpenID Connect and OAuth 2.0 for M-Files Authentication.

Anonymous authentication

On the **Authentication** tab of the **Document Vault Properties** dialog, you can also find the **Use anonymous authentication** setting. It lets you set M-Files Web and M-Files Mobile users to have read-only access to this vault without username and password.

When the feature is enabled, M-Files adds an anonymous user to the vault. The user has no login account on the server, but you can use it to set permissions, and add it to user groups. The anonymous user is created as an external user. However, you can change it to an internal user.

> **Important:** When this feature is enabled, the vault always uses anonymous authentication and personal credentials cannot be used with M-Files Web and M-Files Mobile.

Prerequisites to set up the feature:

- You must have External Connector license.
- You must be a system administrator or have full control of the vault.
- In on-premises and self-managed cloud environments, you must set up mappings between incoming connections and your vaults.

Remarks:

- The classic M-Files Desktop and classic M-Files Web do not use this setting. To set up anonymous authentication for the classic M-Files Web, see Optional: Changing Publication Settings.
- The anonymous user does not decrease the number of your read-only licenses.

Copying a Vault

You can use the **Copy Document Vault** operation to create a copy of a vault. You can copy the vault fully or select the data components that are copied.

Note: The **Copy Document Vault** operation copies the vault first fully and then deletes the data components that have not been selected. For large vaults, the operation time can be long.

It is possible to copy the structure of a vault without the actual content to a new vault. You can use for example the sample vault, that is included in the M-Files installation, in this operation. To copy the structure of a large vault, we recommend exporting the structure. For more information, see Exporting Content.

To copy a vault:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Right-click a vault.
4. Click **Operations** > **Copy Document Vault**.

   ✓ The **Copy Document Vault** dialog is opened.

5. In the **Name** field, enter a name for the copy of the vault.
6. Click **Define** to define the vault data location on the server to which the copy is saved.

   ✓ The **Document Vault** dialog is opened.

7. Click the **...** button to browse for the vault data location.
8. Optional: To define a separate location for file data:
   a) Click **Advanced**.

      ✓ The **Advanced** dialog is opened.

   b) Select the **Separate location for file data** check box.
   c) Click the **...** button to browse for the file data location.
   d) To define a separate account for copying file data, click **Set Account for File Data**.
   e) Click **OK** to close the **Advanced** dialog.
9. 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.

    ⓘ Click **All** to select all components or **Structure Only** to select only the structure components of the vault.

    ⓘ If the **Documents and other objects** check box is selected, you can exclude file data from the vault copy for troubleshooting purposes. Click **Advanced** and select the **Exclude file data from the vault copy** check box.

11. Click **OK** to copy the vault.

Attaching a Vault

A vault can be detached from M-Files Server (see Detaching a Vault). This means that all data in the vault is kept in a file folder on a hard drive but the vault is not registered on the server. If you know the name of the vault and want to start to use it again, attach the vault back to M-Files Server with M-Files Admin.

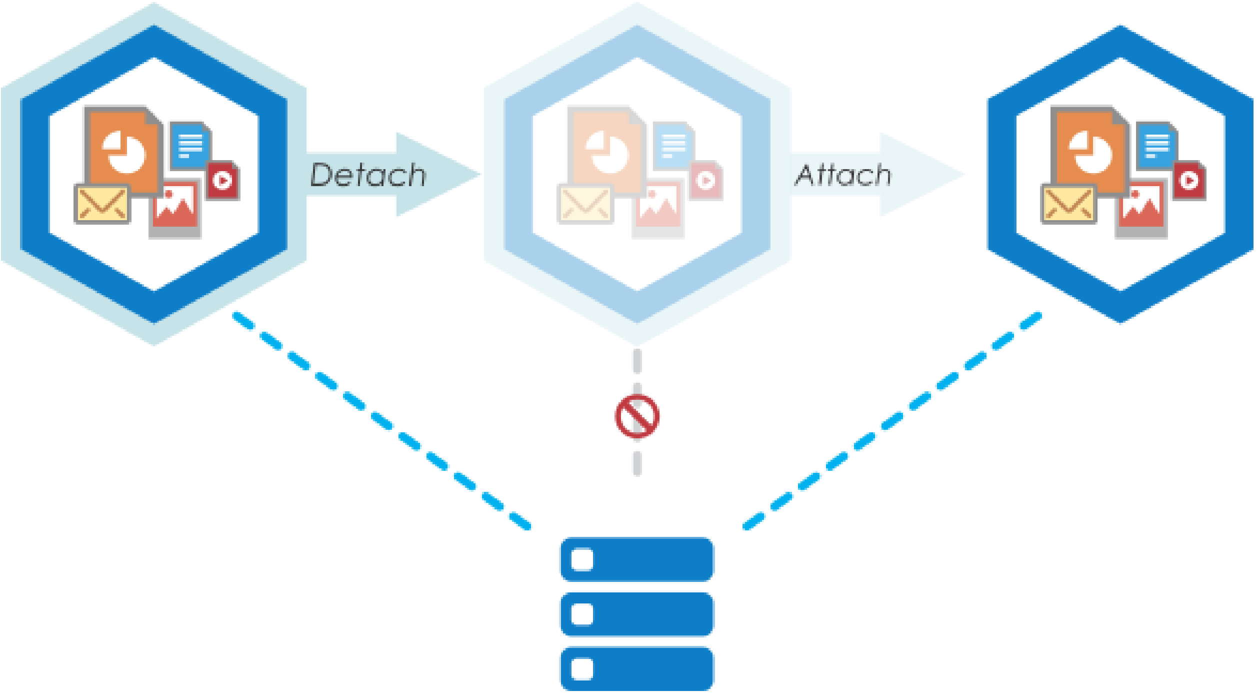


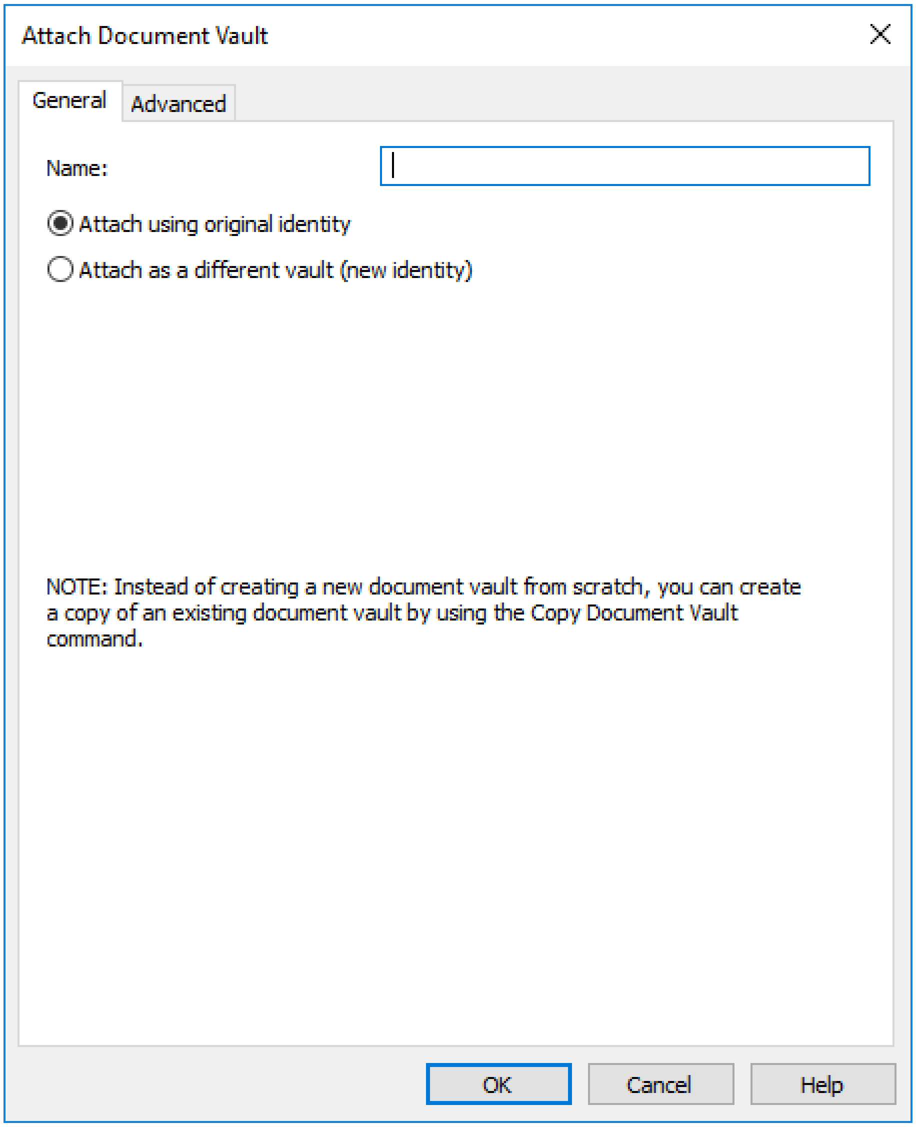
Figure 27: When the vault is detached from the server, it is not displayed in the list of available vaults in M-Files Admin and users cannot access it, but all the data stored in the vault stays intact. You can, for instance, move a detached vault to a another server machine and take it back into use by attaching it to the new server.

If, for example, lack of space makes it necessary to move a vault from one server to another, this can be done with the **Detach** and **Attach** functions: simply detach the vault on server A, copy the vault data to server B, and attach the vault on server B.

To attach a vault:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Select **Document Vaults**.
4. In the task area, click **Attach Document Vault**.

   ☑ The **Attach Document Vault** dialog is opened.



Name:

● Attach using original identity

○ Attach as a different vault (new identity)

NOTE: Instead of creating a new document vault from scratch, you can create a copy of an existing document vault by using the Copy Document Vault command.

5. In the **Name** field, enter the name of the detached vault.

ℹ You may look for the name of the detached vault on the server computer in the folder `C:\<M-Files installation directory>\Server Vaults`.

6. Select either:

a. **Attach using original identity**: Select this option if you want to use the existing ID of the vault.

or

b. **Attach as a different vault (new identity)**: Select this option if you want to create a new unique ID for the vault.

ℹ The vault identity is used in establishing vault connections to the server.

7. Optional: On the **Advanced** tab, you may select and configure the database engine for storing vault data.

See Using Firebird as the Database Engine and Using Microsoft SQL Server as the Database Engine for more information.

8. Click **OK**.

   ✓ The **Attach Vault Options** dialog is opened.

9. Select the features to be disabled in the attached vault:

   - External object types and value lists: Connections to external databases for object types and value lists
   - Connections to external sources
   - Reporting and metadata export data sets
   - Scheduled export and import jobs
   - Active Directory user group synchronization
   - Event handlers
   - Vault applications
   - Remote full-text search indexes: Search indexes that are not used by dtSearch
   - Anonymous login

   If you do not know which features to disable, do not make changes.

   Change the setting **Ignore vault options listed below for multi-server mode vault that is already attached to at least one server** only if you have a good reason to do so. If the vault is not part of multi-server mode setup, the setting has no effect even when it is enabled.

10. Click **Disable selected**.

    ✓ A dialog is displayed listing the features that will be in use in the attached vault.

11. In the **Attach Vault** dialog, click **Attach**.

The selected vault is attached to M-Files Server and can be accessed again.

The users of the vault must add a connection to it with M-Files Desktop settings. For instructions, see Adding a Vault Connection.

Detaching a Vault

You can detach a vault from a connection to M-Files server, in which case the vault data is not destroyed but kept on the hard drive of the server computer. You can later restore the server connection with the **Attach Document Vault** operation.

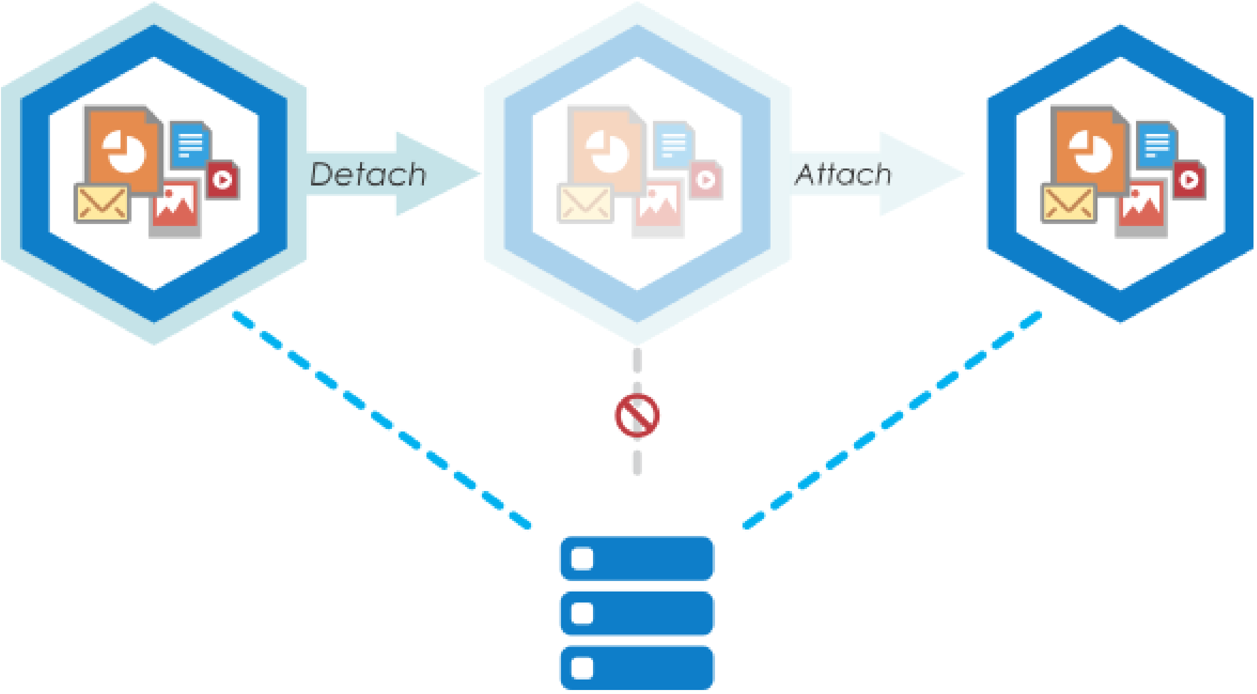


Figure 28: When the vault is detached from the server, it is not displayed in the list of available document vaults in M-Files Admin and users cannot access it, but all the data stored in the vault stays intact. You can, for instance, move a detached vault to another server machine and take it back into use by attaching it to the new server.

Do the following steps to detach a document vault:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Click **Document Vaults**.
4. Select a document vault that you want to detach and click **Detach** on the task area.
5. Click **Yes** at the prompt to confirm your action.

The selected document vault is detached from M-Files Server.

Backing Up a Vault

The vault backup function can be used for backing up an on-premises vault or for scheduling a recurring vault backup job. For more information about scheduled backups, refer to Scheduled Backup Jobs.

Important information

- M-Files Cloud vaults are backed up daily as a standard service. In M-Files Cloud, it is not necessary to schedule other vault backup jobs.
- It is very important to also regularly create master database backups, not only vault backups.
- You can restore the backup only on a server whose M-Files Server version is the same as or later than the version on the server that is used to create the backup. If you restore the backup on a server that has a later version, see Upgrading Vaults.
- If you use Microsoft SQL Server as the database engine of your vault, see Backing Up Microsoft SQL Server Databases for instructions on how to back up and restore your vault data.
- Do not back up an active M-Files system with a snapshot of the file system where its data is stored. This can create a damaged or unusable backup because write operations to files (most importantly, the database engine files) can be ongoing and, thus, incomplete. If you use full virtual machine (VM)

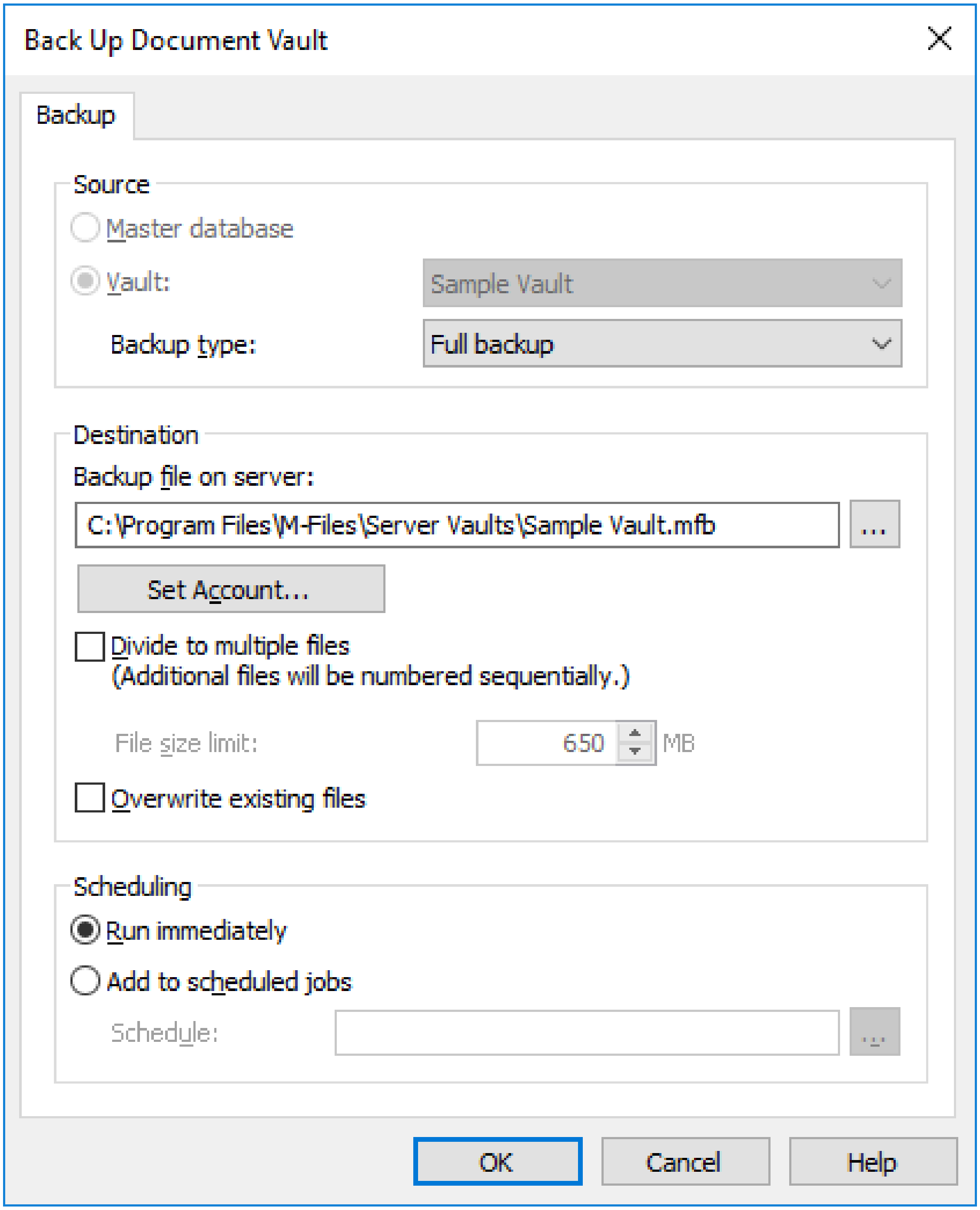
snapshots for backups, make sure that the VM software fully supports creation of snapshots of an active system. This means that the software can restore the system to exactly the same state, including the memory and CPU states.

It also is important to note that M-Files stores on the hard drive of the server machine a vault-specific set of secondary data that is not included in a vault backup, but instead re-recreated after the vault backup has been restored. This data includes PDF renditions for hit-highlighting and preview, thumbnails, and most importantly, the search index of the vault. As rebuilding the search index for a large vault can take a significant amount of time, you should always consider backing up and restoring the search index as well. For instructions, see Backing Up and Restoring the Vault Search Index.

To back up a document vault, do the following steps:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Right-click a vault
4. Click **Operations** > **Back Up**.

   ☑ The **Back Up Document Vault** dialog is opened.



Source

○ Master database

● Vault: Sample Vault

Backup type: Full backup

Destination

Backup file on server: C:\Program Files\M-Files\Server Vaults\Sample Vault.mfb ...

Set Account...

□ Divide to multiple files
(Additional files will be numbered sequentially.)

File size limit: 650 MB

□ Overwrite existing files

Scheduling

● Run immediately

○ Add to scheduled jobs

Schedule: ...

5. Using the **Backup type** drop-down menu, select either *Full backup* or *Differential backup*.

   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: Click **Set Account...** to run the task with another account than the Local System account. If the file location is on a network drive that the Local System account cannot get access to, you must set another account. On the **Set Account** dialog:

a) Select **This account**.
b) In **This account**, enter the name of the user account.
c) In **Password** and **Confirm password**, enter the password of the user account.
d) Click **OK** to close the **Set Account** dialog.

8. Optional: If you want to divide the vault backup into multiple files, check the **Divide to multiple files** check box and set the file size limit.

   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** 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.

11. Click **OK** to either start the backup process or to add the scheduled task to the list of scheduled jobs.

The vault backup should now be run or added to the list of scheduled jobs, depending on your choice under the **Scheduling** header of the dialog.

Restoring a Vault

If a vault is destroyed or the vault data is corrupted, you can restore a healthy version of the vault from a backup. For more information about how to create backups, see Backing Up a Vault and Scheduled Backup Jobs. If you use Microsoft SQL Server as the database engine of your vault, see Backing Up Microsoft SQL Server Databases for instructions on how to back up and restore your vault data.

To restore an M-Files Cloud vault, contact our customer support in M-Files Support Portal or your M-Files reseller.

Note: You can restore the backup only on a server whose M-Files Server version is the same as or later than the version on the server that is used to create the backup. If you restore the backup on a server that has a later version, see Upgrading Vaults.

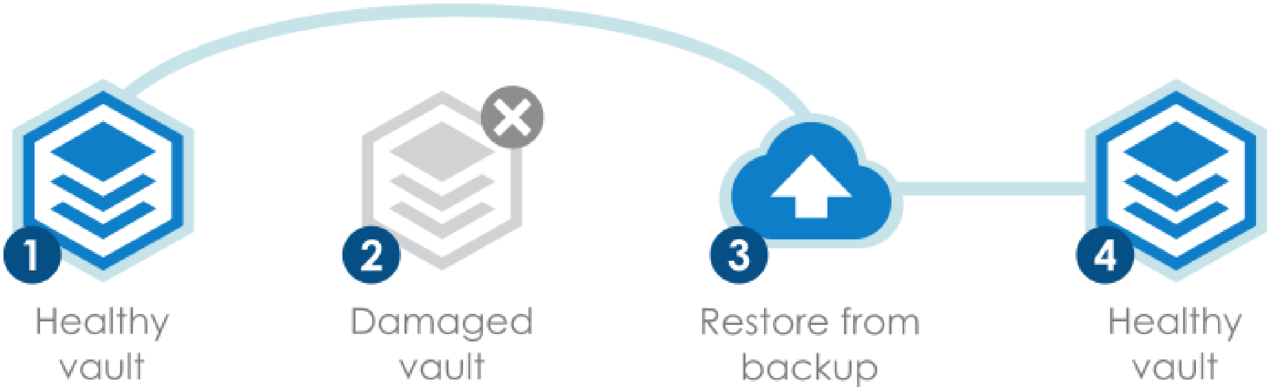
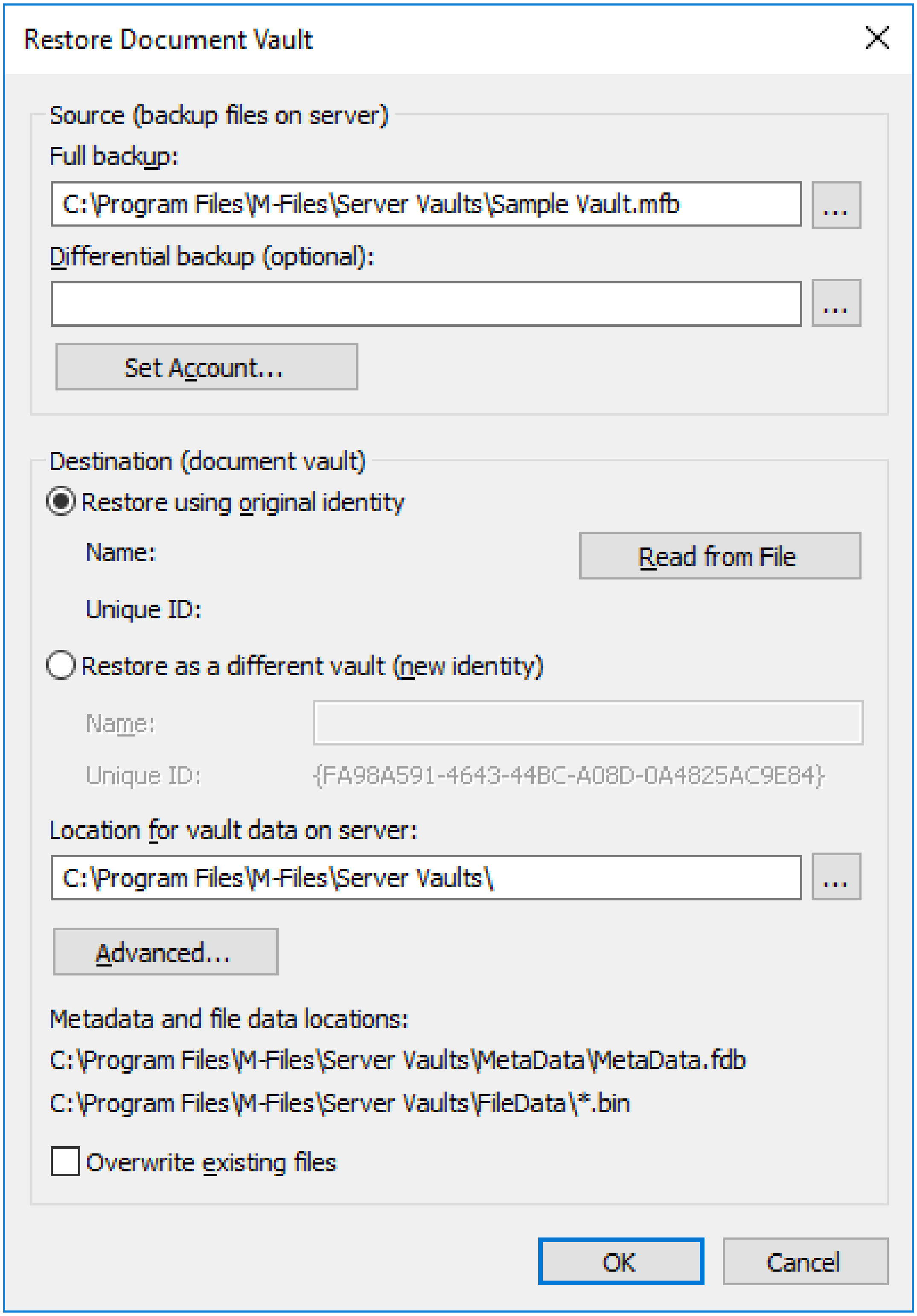


Figure 29: You can restore a backup of a document vault with M-Files Admin.

Do the following steps to restore a document vault from a backup file:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Click **Document Vaults**.
4. In the task area, click **Restore Document Vault**.

   ☑ The **Restore Document Vault** dialog is opened.



Restore Document Vault

Source (backup files on server)

Full backup: C:\Program Files\M-Files\Server Vaults\Sample Vault.mfb

Differential backup (optional):

Destination (document vault)

● Restore using original identity

Name:

Unique ID:

○ Restore as a different vault (new identity)

Name:

Unique ID: {FA98A591-4643-44BC-A08D-0A4825AC9E84}

Location for vault data on server: C:\Program Files\M-Files\Server Vaults\

Metadata and file data locations:

C:\Program Files\M-Files\Server Vaults\MetaData\MetaData.fdb

C:\Program Files\M-Files\Server Vaults\FileData\*.bin

□ Overwrite existing files

5. In the **Full backup** field, specify the location of the backup file on the server from which the full backup is to be restored.

6. Optional: In the **Differential backup (optional)** field, specify the location of the differential backup file to restore a differential backup on top of the full backup.

7. Select either:

a. **Restore using original identity**: Select this option to use the existing ID of the document vault.

   or

b. **Restore as a different vault (new identity)**: Select this option to generate a new unique ID and to specify a new name for the vault to be restored.

   ⓘ The identity is used in establishing document vault connections to the server. The name of the vault can be changed on the server, and the document vault connection can have any name in the client software of the end user.

8. In the **Location for vault data on server** field, specify the location where the data of the document vault is saved.
9. Optional: Click **Advanced...** if you want to define a separate location for file data.
10. Optional: Select the **Overwrite existing files** check box if you want to overwrite existing files in the selected metadata and file data locations.
11. Click **OK**.

    ☑ The **Attach Vault Options** dialog is opened.
12. Select the features to be disabled in the attached vault:

    ⓘ
    - External object types and value lists: Connections to external databases for object types and value lists
    - Connections to external sources
    - Reporting and metadata export data sets
    - Scheduled export and import jobs
    - Active Directory user group synchronization
    - Event handlers
    - Vault applications
    - Remote full-text search indexes: Search indexes that are not used by dtSearch
    - Anonymous login

    If you do not know which features to disable, do not make changes.

    Change the setting **Ignore vault options listed below for multi-server mode vault that is already attached to at least one server** only if you have a good reason to do so. If the vault is not part of multi-server mode setup, the setting has no effect even when it is enabled.
13. In the **Attach Vault** dialog, click **Attach**.

A document vault is restored from the selected backup file.

The users of the vault must add a connection to it. For instructions, see Adding a Vault Connection.

Creating a Search Index

You must create a new search index for a vault for example when you take a new search engine in use. This page tells you how to create a search index in an on-premises installation when your search engine is Smart Search or Micro Focus IDOL. If you use M-Files Cloud, contact our customer support in M-Files Support Portal or your M-Files reseller.

Only a system administrator can create a search index.

For instructions on how to create a search index when your search engine is dtSearch, refer to Rebuilding the dtSearch Full-Text Search Index.

Note: Version 1.2 of the TLS protocol is mandatory for Smart Search.

To create a search index when your search engine is Smart Search or Micro Focus IDOL:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **Search** > **Indexes**.

3. Click **Add Index**.

4. Expand the created index.

5. Give the index a name.

   ⓘ The name must be unique. The length of Smart Search index names must be 34 characters or shorter. Index names for Micro Focus IDOL have no character limit, but we recommend that you try to keep the name as short as possible.

6. Change the remaining settings where necessary.

   a. If you use the default service type, Smart Search, fill in **Application ID** and **API Key** under **Smart Search Options**.

      To get the application ID and API key, write to licensing@m-files.com and include the vault GUID in the request. Tell also the search index location that you will use, for example the United States or European Union. If your data must be in a specified country, contact our customer support in M-Files Support Portal or your M-Files reseller to make sure that the location is available.

      or

   b. Define the Micro Focus IDOL settings with the instructions in Installing Micro Focus IDOL 12 for M-Files.

7. To use the search index as the active index, write the name of the newly created search index in the **Search** > **Active Combined Index** field.

8. In the new search index, set **Enabled** to **Yes**.

9. Click **Save**.

10. Restart the vault.

11. Make sure that the indexing is done with a few full-text searches in M-Files Desktop or M-Files Web.

12. When you are sure that the new index works correctly, disable the previously used index.
    a) In **Advanced Vault Settings**, go to **Configuration** > **Search** > **Indexes** > **<index name>**.
    b) Set **Enabled** to **No**.

With the new search index, you can take search facets in use. For more information, see Configuring Search Facets.

Backing Up and Restoring the Vault Search Index

As the search index of the vault is not included in a vault backup, and since re-creating the index for a large vault can take a large amount of time, you should always consider backing up the search index together with a vault backup. This section provides instructions for backing up and restoring the search index of your vault.

Backing up and restoring the vault search index (dtSearch)

Do the following steps to back up the vault search index when you are using dtSearch as your search engine:

1. Copy the `Indexes` folder from the location of the vault data on the server (for example `C:\Program Files\M-Files\Server Vaults\<vault name>\Indexes`).

2. Store the copied folder in a safe place.

   ℹ The index itself stores its state, and your backup of the index does not need to be as new as the vault backup.

Once you have a backup of your search index, do the following steps to restore the backed up search index:

3. Take the vault offline.

   ℹ For instructions, see Taking a Vault Offline.

4. Delete the `Indexes` folder and replace the folder with the backup.

5. Bring the vault online.

   ℹ For instructions, see Bringing a Vault Online.

The indexing begins to catch up until the search index is completely up-to-date.

Backing up and restoring the vault search index (IDOL)

Do the following steps to back up the vault search index when you are using Micro Focus IDOL version 12 as your search engine:

1. Use Windows Task Manager to stop the **MFIndexingManager** service.

   ℹ When the indexing service is stopped, no new material is added to the index.

   > **Note:** In M-Files May '20 Update or later, M-Files Server migrates the index log files to IDOL and deletes the index log files from M-Files Server. If you use M-Files May '20 Update or later, you do not need to do the following step.

2. Copy the existing index log files `IndexFLog.log` and `IndexMLog.log` or `IndexCLog.log` (in case of an external repository) and store the copied files in a safe place.

The usual location of the log files is in the `FileData` and `MetaData` folders in `C:\Program Files\M-Files\Server Vaults\<vault name>\Indexes\Combined\M-Files`.

3. Wait until all IDOL indexing queues in each content engine are empty.

   The queues are empty when the folders in the IDOL indexing queue are empty. The location of the IDOL indexing queue is for example `E:\IDOL12\data\PROD1-content-12000\index\status`.

4. On the IDOL frontend server, open a browser.

   Note: If you have existing backup files created by the DREEXPORT command and you have not deleted them, you have to give new names to the backup files because the process does not overwrite.

   Note: You need to perform the following step on each backend engine and the daily index content engine.

5. On the address bar of the browser, give the command `http://<content engine IP address>:<content engine indexing port number>/DREEXPORTIDX?FileName=<optional path and backup file name>`.

   Example: `http://192.168.75.130:10001/DREEXPORTIDX?FileName=BU`

   The command generates a file called `<file name>-0.idx.gz` into the folder of the content engine, for example in `E:\IDOL12\data\PROD1-content-12000\index`. The file includes all index data to the point of last full indexing batch.

6. Start the **MFIndexingManager** service.

7. Copy the backup files of the content engines from `<IDOL installation directory or drive>\<content engine>\bin\single<content engine port range>\content` into a safe place.

Once you have the backup of your search index in place, you can start the restore process. By default, the restore process uses the same folders as the backup. Do the following steps to restore the backed up search index:

8. Use Windows Task Manager to stop the **MFIndexingManager** service.

   When the indexing service is stopped, no new material is added to the index.

9. Wait until all IDOL indexing queues in each content engine are empty.

   The queues are empty when the folders in the IDOL indexing queue are empty. The location of the IDOL indexing queue is for example `E:\IDOL12\data\PROD1-content-12000\index\status`.

10. On the IDOL frontend server, open a browser.

    Note: You need to perform the following step on each backend engine and the daily index content engine.

11. To clear the whole index, give the command `http://<content engine IP address>:<DIH/DAH indexing port>/DREINITIAL?` on the address bar of the browser.

    Note: You need to perform the following step on each backend engine and the daily index content engine.

12. Add the index from the corresponding backup by giving the command `http://`*<content engine IP address>*`:`*<content engine indexing port>*`/DREADD?`*<optional backup file path and file name>*`-0.idx.gz`.

Example: `http://192.168.75.120:10001/DREADD?BU-0.idx.gz`

13. Check the number of documents with MFAutonomyConsole using the `getstatus` action against the DIH and DAH engines.

Note: If the backup has been taken before the M-Files May '20 Update, you have the index log files in addition to the IDOL index. In this case, perform the following step. If the backup has been taken after the M-Files May '20 Update, you do not need to perform the following step.

14. Overwrite the index log files `IndexFLog.log` and `IndexMLog.log` or `IndexCLog.log` (in case of an external repository) with the backup files.

The usual location of the log files is in the `FileData` and `MetaData` folders in `C:\Program Files\M-Files\Server Vaults\`*<vault name>*`\Indexes\Combined\M-Files`.

15. Start the **MFIndexingManager** service.

You can run multiple backups or restores simultaneously with a PowerShell script in the backend engines and the daily index content engine.

Example of a backup script:

```
$navOpenInBackgroundTab = 0x1000;
$ie = new-object -com InternetExplorer.Application
$ie.Navigate2("http://192.168.75.128:9001/DREEXPORTIDX?FileName=BU");
# backup from Daily

$ie.Navigate2("http://192.168.75.130:10001/DREEXPORTIDX?FileName=BU",
 $navOpenInBackgroundTab);
# backup from backend server 1, engine 10001

$ie.Navigate2("http://192.168.75.131:20001/DREEXPORTIDX?FileName=BU",
 $navOpenInBackgroundTab);
# backup from backend server 2, engine 20001
$ie.Visible = $true;
```

Example of a restore script:

```
$navOpenInBackgroundTab = 0x1000;
$ie = new-object -com InternetExplorer.Application
#$ie.Navigate2("http://192.168.75.128:9001/DREADD? BU-0.idx.gz ");
# restore Daily

$ie.Navigate2("http://192.168.75.130:10001/DREADD?BU-0.idx.gz",
 $navOpenInBackgroundTab);
#restore backend server 1, engine 10001

$ie.Navigate2("http://192.168.75.131:20001/DREADD?BU-0.idx.gz",
 $navOpenInBackgroundTab);
# restore backend server 2, engine 20001
$ie.Visible = $true;
```

Destroying a Vault

The **Destroy** function in M-Files Admin can be used to permanently destroy all data from a vault.

To delete a cloud vault, refer to Deleting a Cloud Vault in the M-Files Manage user guide.

Warning: When you destroy a vault, the following operations are carried out:

- All the vault file data on the M-Files server is permanently deleted.
- The vault database is permanently deleted.

To destroy a vault:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Click **Document Vaults**.
4. Right-click the document vault that you want to destroy, and then select **Operations** > **Destroy** from the context menu.

   ✓ You are prompted to make sure that you want to destroy the selected vault.
5. Click **Yes** at the prompt.

The selected document vault, including its file data and its database, are permanently deleted and the vault can no longer be accessed by users.

Note: The **Destroy** function naturally does not affect backups located on the hard drive. The document vault can thus be restored if backups have been made.

Upgrading Vaults

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, right-click a vault in M-Files Admin and select **Operations** > **Upgrade** from the context menu.

Important information

- The vault upgrade makes it incompatible with older M-Files Server versions.
- If you have recently done the Verify and Repair (Quick) operation and issues were found, make sure that they are fixed before you upgrade the vault.

Migrating the Vault Database to Microsoft SQL Server

In M-Files Cloud, vaults use Microsoft Azure SQL Database as the default database engine.

In an on-premises environment, M-Files uses Firebird as the default vault database engine. For vaults that contain several hundreds of thousands of objects, we recommend you to use Microsoft SQL Server. If a vault uses Firebird but the number of objects in the vault greatly increases, it can 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 in M-Files Admin.

Note: You can only migrate the document vault database engine from Firebird to Microsoft SQL Server. Migrations from Microsoft SQL Server to Firebird are not supported.

Before you start, make sure that these prerequisites are completed:

- Your vault uses Firebird as the database engine.
- You have a Microsoft SQL Server connection.
- See Important Tasks after Installation, Vault Creation, or Vault Migration for a checklist of tasks that we recommend to be done with vault migration.

After the migration, the file data location is the same as with Firebird. If you want to change the file data location before or after the migration, do these steps:

1. Take the vault offline.
2. Move the file data to a different location.
3. Specify the location of the vault file data.
4. Bring the vault back online.

To migrate your vault database from Firebird to Microsoft SQL Server:

1. Open M-Files Admin.

2. In the left-side tree view, expand a connection to M-Files server.

3. Right-click a vault.

4. Click **Operations** > **Take Offline**.

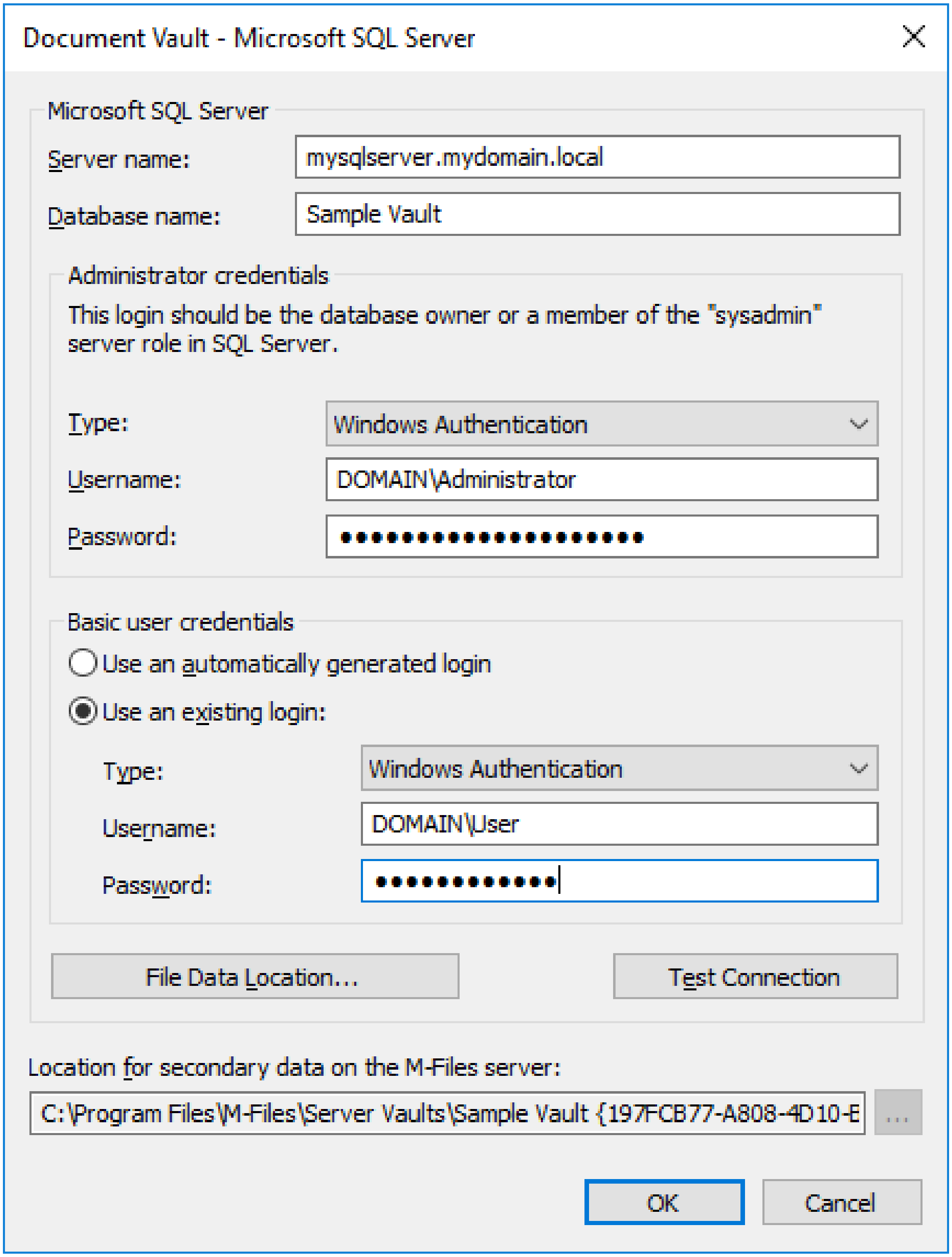
5. Click **Yes** to confirm that you want to take the document vault offline.

6. Optional: It is recommended that you back up the document vault at this point.

   For instructions on backing up the document vault, see Backing Up a Vault.

7. In the left-side tree view, right-click the vault again and select **Operations** > **Migrate to Microsoft SQL Server** from the context menu.

   ✓ The **Document Vault - Microsoft SQL Server** dialog is opened.



Document Vault - Microsoft SQL Server

Microsoft SQL Server

Server name: mysqlserver.mydomain.local

Database name: Sample Vault

Administrator credentials

This login should be the database owner or a member of the "sysadmin" server role in SQL Server.

Type: Windows Authentication

Username: DOMAIN\Administrator

Password: ••••••••••••••••••••

Basic user credentials

○ Use an automatically generated login

● Use an existing login:

Type: Windows Authentication

Username: DOMAIN\User

Password: ••••••••••••

Location for secondary data on the M-Files server:

C:\Program Files\M-Files\Server Vaults\Sample Vault {197FCB77-A808-4D10-E

8. In **Server name**, enter the connection address to your Microsoft SQL Server, such as `mysqlserver.mydomain.local`.

9. In **Database name**, enter 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.

10. In the **Administrator credentials** and **Basic user credentials** sections, fill in the credentials 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.	**a.** In the **Administrator credentials** section, enter the credentials for a login that has the *sysadmin* server role on your Microsoft SQL Server. **b.** In the **Basic user credentials** section, select the **Use an automatically generated login** option.
Manually create the Microsoft SQL Server database and login accounts (without the *sysadmin* server role) and use the non-*sysadmin* credentials for M-Files Server.	**a.** By using Microsoft SQL Server Management Studio, create an empty database for the vault. **b.** Still in Microsoft SQL Server Management Studio, create two login accounts without the *sysadmin* server role, for example `User A` and `User B`. **c.** Back in M-Files Admin and the **Document Vault - Microsoft SQL Server** dialog, in the **Administrator credentials** section, enter the credentials for `User A`. **d.** In the **Basic user credentials** section, first select the **Use an existing login** option and then enter the credentials for `User B`.

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 login accounts need to be created manually (the second option). For detailed instructions, refer to the document How to Configure M-Files to Operate Without Sysadmin Role in MS SQL Server.

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 login accounts – for some of the maintenance operations.

11. Optional: Click **Test Connection** to test the connection to your Microsoft SQL Server.

12. Click **OK**.

A warning dialog is opened to tell you that the operation cannot be undone.

13. Click **Yes** to close the warning dialog and start the migration.

14. After the migration is complete, in the left-side tree view, right-click the vault.

15. Click **Operations** > **Bring Online**.

Once the migration process is complete, the database of your M-Files vault is located on the Microsoft SQL Server that you specified.

After migrating the vault database to Microsoft SQL Server, you need to create a backup job for the database in Microsoft SQL Server Management Studio. For more details and recommendations, see M-Files Backup Policy.

In this chapter

Migrating the Vault Database from One Microsoft SQL Server to Another

When migrating from one Microsoft SQL Server to another, the new Microsoft SQL Server should be running the same or newer version of Microsoft SQL Server, and the Microsoft SQL Server edition (Enterprise or Standard) should also be the same or higher than that of the old Microsoft SQL Server.

In other words, do not migrate vault databases from Microsoft SQL Server to an older version or lower edition of Microsoft SQL Server.

See also Important Tasks after Installation, Vault Creation, or Vault Migration for a checklist of tasks that we recommend to be done with vault creation.

To migrate a vault database from one Microsoft SQL Server to another:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Right-click a vault.
4. Click **Operations** > **Take Offline**.
5. Open Microsoft SQL Server Management Studio and take a full backup of the vault database.
6. Restore the database to the new Microsoft SQL Server as a new database.
7. In M-Files Admin, right-click the document vault and select **Properties** from the context menu.

   ✓ The **Document Vault Properties** dialog is opened.
8. Open the **Advanced** tab.
9. Under the **Use Microsoft SQL Server** option, click the **Define...** button.

   ✓ The **Document Vault - Microsoft SQL Server** dialog is opened.
10. In the **Server name** field, specify the name of the new Microsoft SQL Server.
11. In the **Database name** field, specify the name of the new database.
12. In the **Administrator credentials** and **Basic user credentials** sections, specify the new authentication settings.
13. Click **OK** to close the **Document Vault - Microsoft SQL Server** dialog and then click **OK** to close the **Document Vault Properties** dialog.
14. In the left-side tree view, right-click the vault.
15. Click **Operations** > **Bring Online**.

From this point forward, the M-Files server will access the vault database from the new Microsoft SQL Server.

After migrating the vault database to the new Microsoft SQL Server, you need to create a backup job for the new database in Microsoft SQL Server Management Studio on the new Microsoft SQL Server. For more details and recommendations, see M-Files Backup Policy.

Restarting a Vault

The restart operation takes the vault offline and brings it back online in one go. With this operation, you avoid the risk of leaving the vault accidentally offline. When a vault is offline, also any open sessions that users may have are closed. Users cannot check in objects or log in to a vault until the vault is back online.

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Right-click a vault which is in the online state.
4. Select **Operations** > **Restart**.
5. Click **Yes** at the prompt.

Taking a Vault Offline and Bringing a Vault 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.

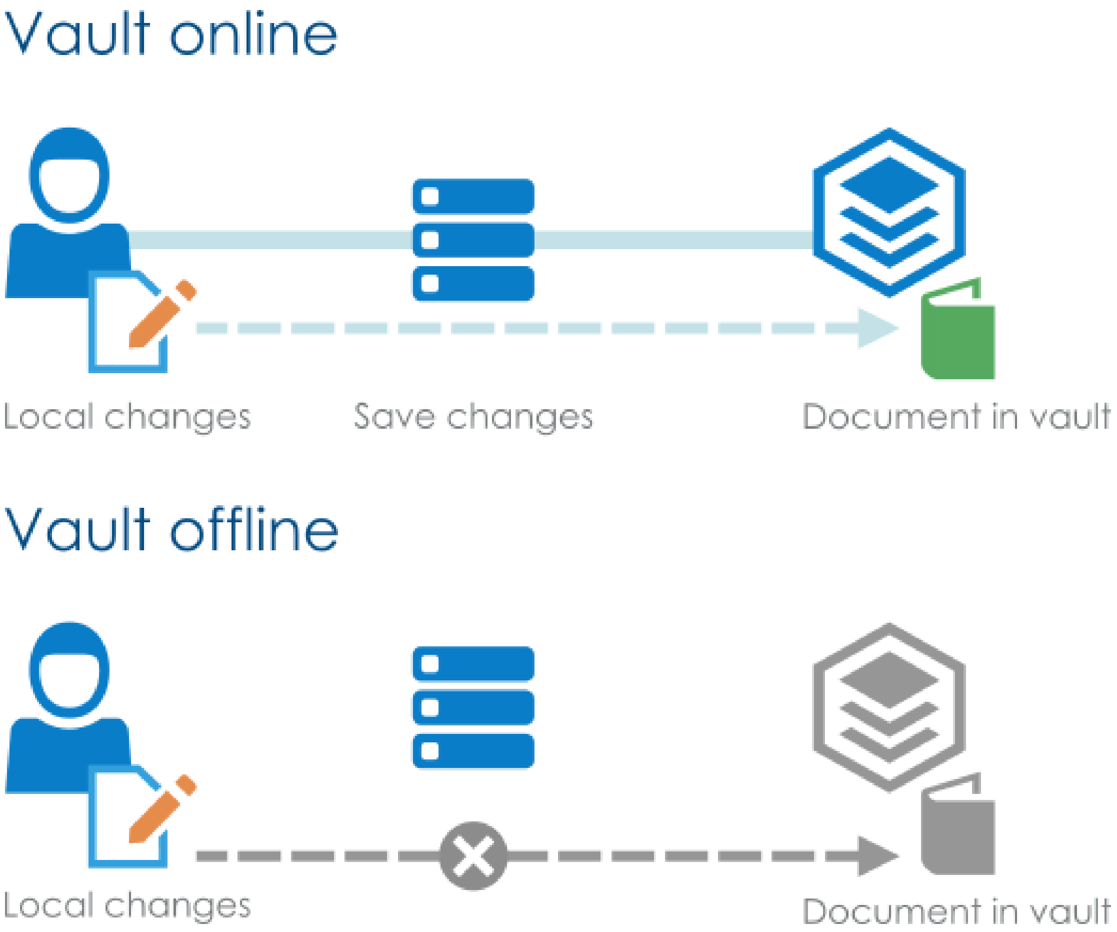


Figure 30: When a vault is taken offline, all vault users are disconnected. If a user checks out a document for editing and makes modifications to the content, during which the vault administrator takes the vault offline, the user is unable to check in the document until the vault is brought back online. It is therefore not recommended to carry out unscheduled operations that require the vault to be taken offline.

Taking a Vault Offline

To take a vault offline:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Right-click a vault which is in the online state.
4. Select **Operations** > **Take Offline**.

Bringing a Vault Online

To bring a vault online:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Right-click a vault which is in the offline state.
4. Click **Operations** > **Bring Online**.

Logging in to and out of a Vault in M-Files Admin

To log out of a vault on the server level, select the vault in the left-side tree view in M-Files Admin, and then select **Action** > **Log Out** from the menu bar.

When you have logged out from the document vault, the name of this function changes to **Log In**, allowing you to log back in.

Vault Maintenance

Regular vault maintenance makes sure that even vaults with a large number of objects have high performance.

Most of the information on this page is applicable to on-premises environments only. The M-Files Cloud service includes regular vault maintenance. In M-Files Cloud, customer administrators can only see and do the operations in M-Files Admin that are not included in the service.

In an on-premises environment, the **Maintenance** submenu for a vault in M-Files Admin contains functions to, for example, verify and optimize the integrity of the internal database structure. It is also important to regularly verify the integrity of your vault and master database backups.

It can be helpful to see the Why is my M-Files not as fast as it used to be? FAQ article. It contains many frequently encountered issues that can cause system slowness.

> ! **Important:** M-Files does continuous database maintenance during use, especially with the thorough optimization process. If you use Microsoft SQL Server, do not use any maintenance operations with Microsoft SQL Server Management Studio. At best, they have no effect, but they can cause negative effects on the performance of your M-Files system. With some Microsoft SQL Server editions, manually used maintenance operations can even prevent the use of M-Files during the operation.

Maintenance recommendations for M-Files Cloud vaults

Summary of the recommended maintenance operations:

- Use the **Reset Thumbnail Images** operation only if the thumbnail images do not work correctly.
- Rebuild the full-text search index only if you think that the search index is corrupted or if the search operations are significantly slower than usual.
- Archive M-Files event logs at least once a year.

Maintenance recommendations for on-premises vaults

Summary of the recommended maintenance operations:

- Use the **Reset Thumbnail Images** operation only if the thumbnail images do not work correctly.
- Rebuild the full-text search index only if you think that the search index is corrupted or if the search operations are significantly slower than usual.
- Use the **Verify and Repair (Quick)** operation twice a year for all repositories.
- Clean the vaults at least once a year.
- Archive M-Files event logs at least once a year.
- Verify the integrity of your master database backups at least two to four times a year.

  - Refer to M-Files Backup Policy for further guidelines and best practices related to backups.
- Verify the integrity of your vault backups at least two to four times a year.

  - If Microsoft SQL Server is used, refer to the documentation of the backup tools you use to create the backups for instructions.
  - If Firebird SQL database is used, see Backing Up a Vault and Restoring a Vault for instructions.
  - When you restore test vaults, make sure that you do not accidentally overwrite the production vault. In addition, when you restore a vault with a new GUID, make sure that you do not let the restored vault, when asked, use any external connections. This can cause problems if the production vault uses the same connections. Finally, please make note that the restored vault can cause, for example, scripts to be executed and assignment emails to be sent.
  - Refer to M-Files Backup Policy for further guidelines and best practices related to backups.

For a recommended maintenance schedule, see the table in How do I maintain the M-Files server machine?.

See Important Tasks after Installation, Vault Creation, or Vault Migration for a checklist of tasks that we recommend to be done with operations listed in the section.

Optimizing the database

The **Optimize Database (Thorough)** operation tries to improve the performance of the vault database. The operation defragments indexes, updates database statistics, and compresses the full-text search index.

By default, M-Files does the **Optimize Database (Thorough)** operation once every week. To change the default schedule or specify a timeout for the optimization, see Scheduled Optimization.

Normally, it is not necessary to do the operation yourself. However, if the vault operates more slowly than usual, it can be necessary to do it. The vault can respond slowly after a large number of objects is imported to the vault. For example, if the number of objects in a vault that uses Firebird quickly increases from 0 to 10,000 objects.

You can do the operation in the quick mode first, but we recommend to use the thorough mode in most cases. For instructions, see Manual Optimization.

These tasks are done when you run the **Optimize Database (Quick)** operation:

1. Rebuilding metadata indexes
2. Recalculating relevance scores for objects
3. Clearing the change logs of object types
4. Updating the statistics for database objects

See Task Order in Thorough Optimization for the list of tasks done during the thorough operation.

Updating encryption status of existing files

The selection of the setting **Enable encryption for file data at rest** on the **Advanced** tab of the **Document Vault Properties** dialog has an effect on the functionality of the **Update encryption status of existing files** operation:

- If the **Enable encryption for file data at rest** is selected, all the files in the vault previously not encrypted are now encrypted as well.
- If the **Enable encryption for file data at rest** is not selected, the encryption of all the encrypted files in the vault is removed.

After you have run the **Update encryption status of existing files**, you must manually run the **Optimize Database (Thorough)** operation to remove the old file data of the vault. If the option **Delete the files of destroyed objects** is available, select it.

Rebuilding the full-text search index

This operation is to be done only if you think that the search index is corrupted or if the search operations are significantly slower than usual. For use instructions, see Managing Vault Indexing.

The best practice is to create a duplicate index in the background. Please contact our customer support in M-Files Support Portal or your M-Files reseller for further assistance.

Please take note of this important information before you start the operation:

- This operation completely rebuilds the full-text search index and it can require a very large amount of time. For example, with vaults that contain a million, millions, or tens of millions of documents, indexing can take days or even weeks. Many factors, such as the used indexer, hardware resources, and type of data in the vault can have a considerable effect on the indexing speed.
- During the rebuild process, search operations can be used but the search results can be limited because the search index is not complete. For instructions on how to have the search operate normally during the process, refer to Rebuilding the dtSearch Full-Text Search Index.

Resetting thumbnail images

You can reset the thumbnail image cache for the vault if you use the thumbnail view in M-Files Desktop and if the images are not working correctly. This can happen, for instance, after installing a software capable of displaying thumbnails that could not previously be shown.

Cleaning the vaults

When you clean the vaults, you release disk space for new objects.

To clean a vault:

1. In M-Files Admin, export the content that you want to remove from the vault.

   Example filter:

   - **Status** tab: **Deleted** set to **No**
   - **Properties** tab: **Created** property with the **<=** operator and the value set to a date
2. In M-Files Desktop or M-Files Web, delete the objects that you have already exported and enable **Destroy permanently**.

   Note: When you search for objects to delete and destroy, use the same filters as in step 1. This makes sure that you only destroy content that you have exported.
3. In M-Files Admin, manually optimize the database.

   Enable **Delete the files of destroyed objects**.

   Note: The scheduled automatic optimization does not remove the destroyed files.

In this chapter

Important Tasks after Installation, Vault Creation, or Vault Migration

This section gives M-Files administrators critical information about important tasks to be done with these operations:

- M-Files installation
- Vault creation
- Vault migration (to a new location or a new database provider)

To reduce the risk of data loss, make sure that you are familiar with the information given here and that the guidance is carefully followed.

When you install M-Files:

- Make sure that the necessary antivirus exclusions are in place. See M-Files and Virus Scanning.
- For a production system, implement and test a backup policy for the master database. Refer to M-Files Backup Policy.
- Make sure that shutdowns and restarts are not forced. Refer to Do not force a shutdown of an M-Files/ SQL Server process or computer.

After a vault is created or migrated:

- When you change the database engine from Firebird to Microsoft SQL Server or create a vault in that uses Microsoft SQL Server, make sure that its memory limit is set correctly. See Changing the Memory Limit for a Microsoft SQL Server Instance.
- For a production system, implement and test a backup policy for the vault content. Refer to M-Files Backup Policy.
- Make sure that the antivirus exclusions include the vault data (file data, metadata, and indexes). This is especially important if you do not use the default paths for them. See M-Files and Virus Scanning.

Periodically:

- Monitor your Firebird vault sizes and plan to change the database engine to Microsoft SQL Server according to these guidelines: Using Firebird as the Database Engine.
- Familiarize yourself with the system requirements and make sure that they are met over the lifetime of the system. When the vaults grow, the requirements change. See System Requirements and Technical Details.
- Do not do database optimization tasks manually for Microsoft SQL Server because M-Files does them. Refer to Manual SQL Maintenance.
- Use the **Verify and Repair (Quick)** operation. See Using Verify and Repair.
- To clean up files from destroyed objects, do a manual run of the **Optimize Database (Thorough)** process. See Manual Optimization.
- If the vault uses dtSearch as the search engine, rebuild the indexes. Refer to Rebuilding the dtSearch Full-Text Search Index.

    - If the vault grows to around million objects, switch to a more scalable search engine. For example, Smart Search.

Task Order in Thorough Optimization

The order and number of tasks done during the **Optimize Database (Thorough)** operation is different in different contexts. This page gives you the list of tasks done in the most frequently used contexts.

Manual optimization with Firebird

1. Taking the vault offline
2. Clearing the quick indexing table
3. Resetting the help tables
4. Deleting the contents of temporary files
5. Resetting the ID generator for file uploads
6. Changing the local time zone of the vault
7. Rebuilding metadata indexes
8. Recalculating relevance scores for objects
9. Removing unused access control lists
10. Removing old records from object type change logs
11. Processing the full-text search compatibility of views
12. Upgrading the vault database to improve performance
13. Optimizing the vault database
14. Optimizing the process memory
15. Backing up metadata
16. Restoring metadata
17. Bringing the vault online
18. Compressing the full-text search indexes

Manual optimization with Microsoft SQL Server ("Delete the files of destroyed objects" not enabled)

1. Clearing the quick indexing table
2. Resetting the help tables
3. Deleting the contents of temporary files
4. Resetting the ID generator for file uploads
5. Changing the local time zone of the vault
6. Rebuilding metadata indexes

7. Recalculating relevance scores for objects
8. Taking the vault offline

    - This step is done only if dtSearch is used as the search engine.
9. Bringing the vault online

    - This step is done only if dtSearch is used as the search engine.
10. Removing unused access control lists
11. Removing old records from object type change logs
12. Processing the full-text search compatibility of views
13. Upgrading the vault database to improve performance
14. Optimizing the vault database
15. Rebuilding database indexes
16. Updating the statistics for database objects
17. Optimizing the process memory
18. Compressing the full-text search indexes

Manual optimization with Microsoft SQL Server ("Delete the files of destroyed objects" enabled)

1. Taking the vault offline
2. Clearing the quick indexing table
3. Resetting the help tables
4. Deleting the contents of temporary files
5. Resetting the ID generator for file uploads
6. Changing the local time zone of the vault
7. Rebuilding metadata indexes
8. Recalculating relevance scores for objects
9. Removing unused access control lists
10. Removing old records from object type change logs
11. Processing the full-text search compatibility of views
12. Upgrading the vault database to improve performance
13. Optimizing the vault database
14. Rebuilding database indexes
15. Updating the statistics for database objects
16. Optimizing the process memory
17. Bringing the vault online
18. Compressing the full-text search indexes

Scheduled optimization with Firebird

1. Taking the vault offline
2. Clearing the quick indexing table
3. Resetting the help tables
4. Deleting the contents of temporary files
5. Resetting the ID generator for file uploads
6. Rebuilding metadata indexes
7. Recalculating relevance scores for objects
8. Removing unused access control lists
9. Removing old records from object type change logs
10. Processing the full-text search compatibility of views
11. Upgrading the vault database to improve performance

12. Optimizing the vault database
13. Optimizing the process memory
14. Backing up metadata
15. Restoring metadata
16. Bringing the vault online
17. Compressing the full-text search indexes

Scheduled optimization with Microsoft SQL Server

1. Clearing the quick indexing table
2. Resetting the help tables
3. Deleting the contents of temporary files
4. Resetting the ID generator for file uploads
5. Rebuilding metadata indexes
6. Recalculating relevance scores for objects
7. Taking the vault offline

   - This step is done only if dtSearch is used as the search engine.
8. Bringing the vault online

   - This step is done only if dtSearch is used as the search engine.
9. Removing unused access control lists
10. Removing old records from object type change logs
11. Processing the full-text search compatibility of views
12. Upgrading the vault database to improve performance
13. Optimizing the vault database
14. Rebuilding database indexes
15. Updating the statistics for database objects
16. Optimizing the process memory
17. Compressing the full-text search indexes

Nightly Maintenance

Nightly maintenance is an M-Files operation that does important maintenance tasks to keep your vault healthy. By default, M-Files starts the nightly maintenance every night at 4:30 AM server time. The number of tasks done during the nightly maintenance is different in different contexts. Additionally, you can control which operations are included in the nightly maintenance of a vault.

Nightly maintenance does, for example, these tasks for all vaults where it is enabled:

- Does the full refresh operation for external object types
- Deletes old relogin session IDs
- Starts nightly maintenance for full-text search indices

If the vault uses Microsoft SQL Server as the database engine, nightly maintenance also does these tasks:

- Updates database statistics from Microsoft SQL Server and starts SQL Server database optimization
- Removes outdated server tasks
- Stops SQL queries that have not completed in the time specified in the **Time Limit for SQL Queries** nightly maintenance setting

You can configure nightly maintenance to also do these tasks:

- Run automatic workflow state transitions
    - To enable this task, set **Run Automatic State Changes During Maintenance** nightly maintenance setting to **Yes**.
- Synchronize Microsoft Entra ID user groups and external repository user groups
    - To enable this task, set the **Run User Group Synchronization Only During Nightly Maintenance** nightly maintenance setting to **Yes**.

Editing nightly maintenance settings

You can control when and how M-Files does nightly maintenance for a vault.

Recommendations:

- In production environments, do not disable nightly maintenance.
- Set nightly maintenance to be done when the vault is not used. Otherwise, it can cause performance issues. By default, nightly maintenance starts at 4:30 AM server time.
- If you have large Microsoft Entra ID user groups, enable **Run User Group Synchronization Only During Nightly Maintenance** to set the synchronization to be done outside working hours. The synchronization can otherwise have a negative impact on system performance.
- Have one of these two settings enabled:
    - **Run Automatic State Changes During Maintenance**
    - **Run Automatic State Changes in the Background**

To open the nightly maintenance settings of a vault:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
    a) Open M-Files Admin.
    b) In the left-side tree view, expand an M-Files server connection.
    c) Expand **Document Vaults**.
    d) Expand a vault.
    e) Click **Configurations**.
    f) In the navigation area, click **Advanced Vault Settings**.
    g) Open the **Configuration** tab.

    ✓ The advanced vault settings are shown.

2. Expand **Database** > **Nightly maintenance**.

    For more information, select a setting and see the **Info** tab.

    Note: M-Files updates the starting time settings only after the current cycle is finished or after you restart the M-Files Server service. You can restart the service with Windows Task Manager or the Windows Services app.

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 change to any software language with the language setting. For intructions on how to translate the vault metadata structure to the language of your choice, see section Translating the metadata structure.

Changing the Windows display language depends on your Windows version. For instance in Windows 10, you can change the display language in **Control Panel** > **Language**.

Note: The classic M-Files Web has different requirements for a fully localized user experience. See this note for more information. The new M-Files Web uses your browser language setting to select the language of the user interface.

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, and so on. 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 for further information on how to create a localized version of the metadata structure of your vault.

Tip: If your M-Files system administrator has enabled translated object titles, you can use the translated object titles in searches. The translated object titles are also shown in the title area of the metadata card, in the listing area, in notifications, and in value lists.

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 languages, it can be difficult for the user to understand why some information is displayed in different languages. 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.

In this chapter

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

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, complete the following steps:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)** and then select **Value Lists**.

   ✓ The **Value Lists** list is opened in the right pane.
6. Double-click the value list that you want to edit.

   ✓ The **Value List Properties** dialog is opened.
7. Open the **Advanced** tab.
8. Enable the option **The contents of this value list can be translated**.

9. Click **OK** to close the **Value List Properties** dialog.

The contents of the selected value list can now be translated.

In this chapter

- Translating the Metadata Structure

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.

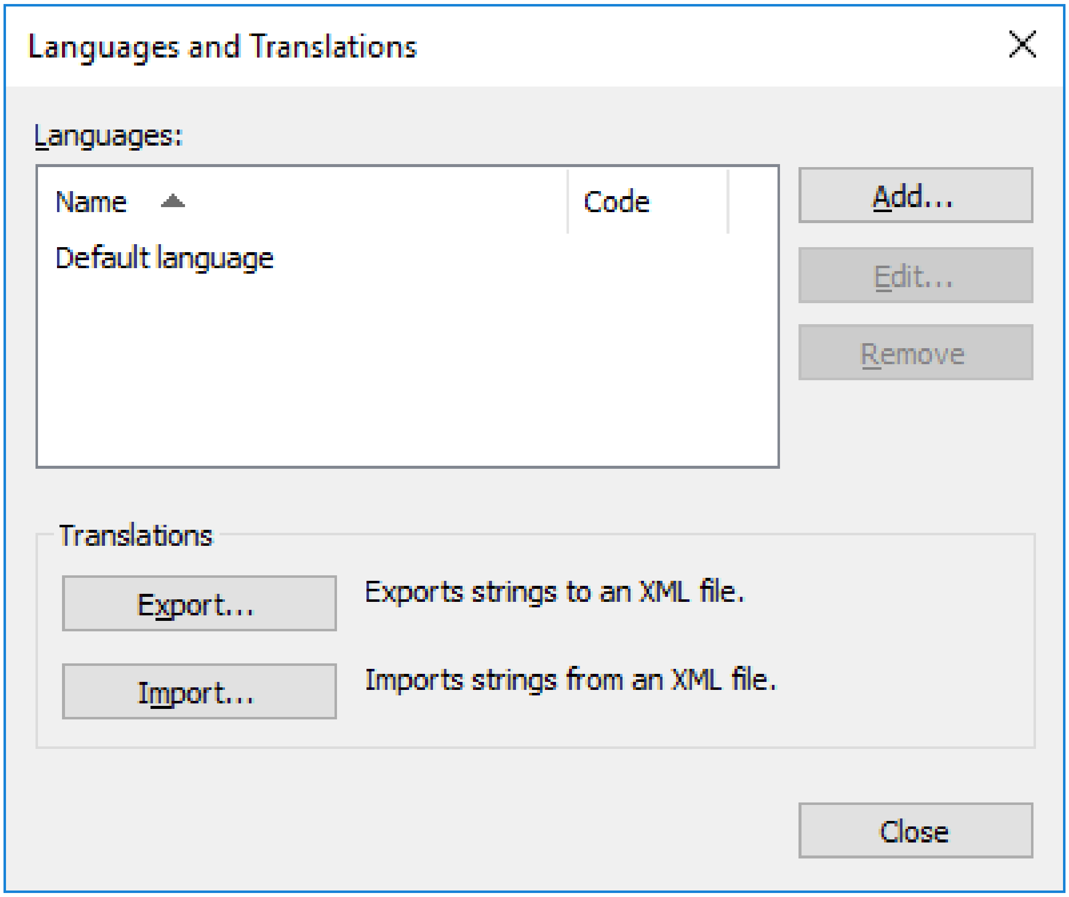
1. Open M-Files Admin.

2. In the left-side tree view, expand a 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.


Languages and Translations
Languages:
Name
Code
Default language
Add...
Edit...
Remove
Translations
Export...
Exports strings to an XML file.
Import...
Imports strings from an XML file.
Close

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.

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 Microsoft Excel.

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.

18. Click **OK**.
19. Once the import is complete, click **Close** to close the **Languages and Translations** dialog.

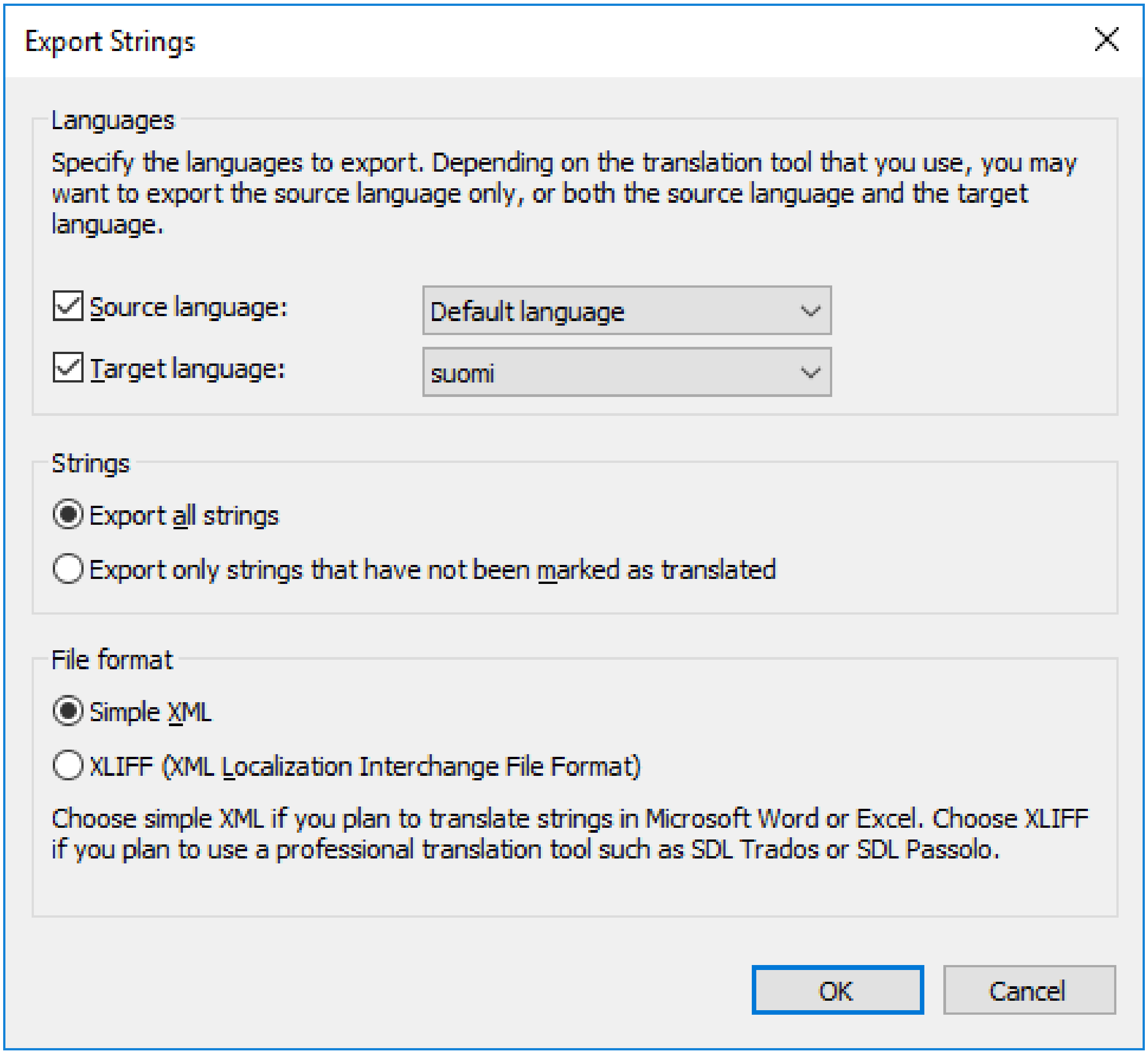
Translations for the newly added language have been imported to M-Files and you can select the vault language in M-Files Desktop and M-Files Web.

In this chapter

- Translating in Microsoft Excel
- Importing Translations

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:



Export Strings

Languages

Specify the languages to export. Depending on the translation tool that you use, you may want to export the source language only, or both the source language and the target language.

☑ Source language: Default language

☑ Target language: suomi

Strings

● Export all strings

○ Export only strings that have not been marked as translated

File format

● Simple XML

○ XLIFF (XML Localization Interchange File Format)

Choose simple XML if you plan to translate strings in Microsoft Word or Excel. Choose XLIFF if you plan to use a professional translation tool such as SDL Trados or SDL Passolo.

Figure 31: 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.

If 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 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 Microsoft Excel

Translating the metadata structure into the target language in Excel is straightforward. Simply open the XML file in Excel: Select 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, meaning 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.

The **source** column contains the concepts to be translated. Add the translation to the **target** column and change `0` in the **translated** column to `1`. This tells M-Files that the string has been translated.

Naming convention of the identifiers

The identifiers are formed as follows: `TableID_ResourceID1_ResourceID2_StringID`.

- `TableID`: Identifies the type of the metadata structure element in question.
  - `PropertyDef`
  - `ObjectType`
  - `Item` (referring to any translatable value list item)
  - `NamedACL`
  - `View`
  - `Language`
- `ResourceID1`: 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 resource ID 1. The resource ID 2 is always `0` for elements other than `Item`.
- `ResourceID2`: 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 that identifies the item in the **Workflows** value list.

- `StringID` (`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 Microsoft 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: If 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 Microsoft Excel, save the translated XML file in Microsoft 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

You can change the M-Files software language and the vault language. The software language is used in the texts and labels that you see in M-Files. For example, button texts, dialog titles, and warning messages. The vault language is used as the metadata structure language, which is always vault-specific.

To change the software and the vault language in the classic M-Files Desktop:

1. Click your username in the upper right corner.
2. Click **User Settings** > **Change Language**.

   ✓ The **Change Language** dialog is opened.
3. Use the **Software language** drop-down menu to change the language of the M-Files user interface.

4. 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.

5. 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 with 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*", and so on. 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 a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Users**.

   The **Users** list is opened in the right-side pane.

6. 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.

7. Use the **Vault language** drop-down menu to change the default vault language for the selected user.

8. 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.

Enabling Translatable Object Titles

To use translatable object titles, you need to have the desired languages added as vault languages in the Languages and Translations dialog. However, it is not required that the metadata structure is translated into those languages.

Note: This feature is not supported in the M-Files add-ins such as M-Files Add-in for Teams and SharePoint Online.

The translatable object title configuration allows you to give objects titles in different languages. When an object has multilingual titles, the translated names can be used as search criteria. You can search for and find documents and other objects in your own language regardless of the original object's language. The language version that matches the **Vault language** in the Change Language dialog is used on the title area of the metadata card, listing area as well as in notifications and value lists.

To enable translatable object titles, do the following steps:

1. Check that the desired languages with language codes are listed in the **Languages and Translations** dialog.

   If a language or a code is missing from the list, add it according to the instructions in Translating the Metadata Structure. Note down of the language codes.

2. Open M-Files Admin and go to a vault.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.

3. Expand **Metadata Structure (Flat View)**.

4. Click **Property Definitions**.

   ✓ The **Property Definitions** dialog is opened.

5. In the task area, click **New Property Definition** to create property definitions for the desired object title languages.

   Note: The data type of the property definitions must be **Text**.

   For instructions on creating property definitions, see Creating a New Property Definition.

   If you want to allow adding a Finnish title for an object, you can create a property definition called `Title in Finnish`.

6. Select **Configurations** and expand **Advanced Vault Settings**.

7. Expand the **Configuration** node and select **Translatable Object Titles**.

8. Specify the settings according to the information in the following table.

Setting name	Description	Example value
Object Types Using Translated Titles	Specify the object types that can use translated title properties.	**Document**
Translated Title Properties	Specify the property definitions that are used as an alternative language title, each with their corresponding language code. Use the language codes noted down from the **Languages and Translations** dialog.	**Language Code**: **fi** **Title Property**: `Title in Finnish`

9. Click **Save**.

Now you are ready to enter translated titles for objects of the specified object type. After you have added the properties to the metadata of an object and entered the translated names, the title is shown according to the selected vault language on the title area of the metadata card, listing area as well as in notifications and value lists. Translated object titles do not affect pinned shortcuts or notifications sent to unknown or multiple recipients.

Note: After you have saved the changes and M-Files Server has been restarted, end users must log out from and log back in to the vault to be able to use translatable object titles. To log out all vault users, restart the vault. However, taking a vault offline must always be done in a controlled manner and the vault users must be notified beforehand.

Tip: You can use metadata card configuration rules to show the translated object titles after the actual **Name or title** property.

Connections to External Sources

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 can read from an external database, but you cannot enter new data with 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 makes deploying M-Files easy and quick, because all existing files can be accessed with M-Files without a separate transfer process. When you access files with M-Files, it makes sense to enrich them with metadata 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.

Warning: A large number of connections to external sources with short synchronization intervals can cause performance issues.

In this chapter

External File Sources

You can import or link files from external sources to M-Files. With a link between a folder on a network drive and an M-Files vault, you can modify files both in M-Files and on the network drive. If you want to make changes in M-Files only, you can import the files to the vault.

You can also use external repository connectors to import content to your vault. See Connectors. Make sure that you do not use both features to import the same content.

In M-Files Cloud, this feature is only supported for Azure file shares. In a shared M-Files Cloud environment, contact our customer support in M-Files Support Portal or your M-Files reseller if you want to connect your cloud vault to an Azure file share. They can also give you information on other options to link and import files.

> ❗ **Warning:** A large number of connections to external sources with short synchronization intervals can cause performance issues.

In this chapter

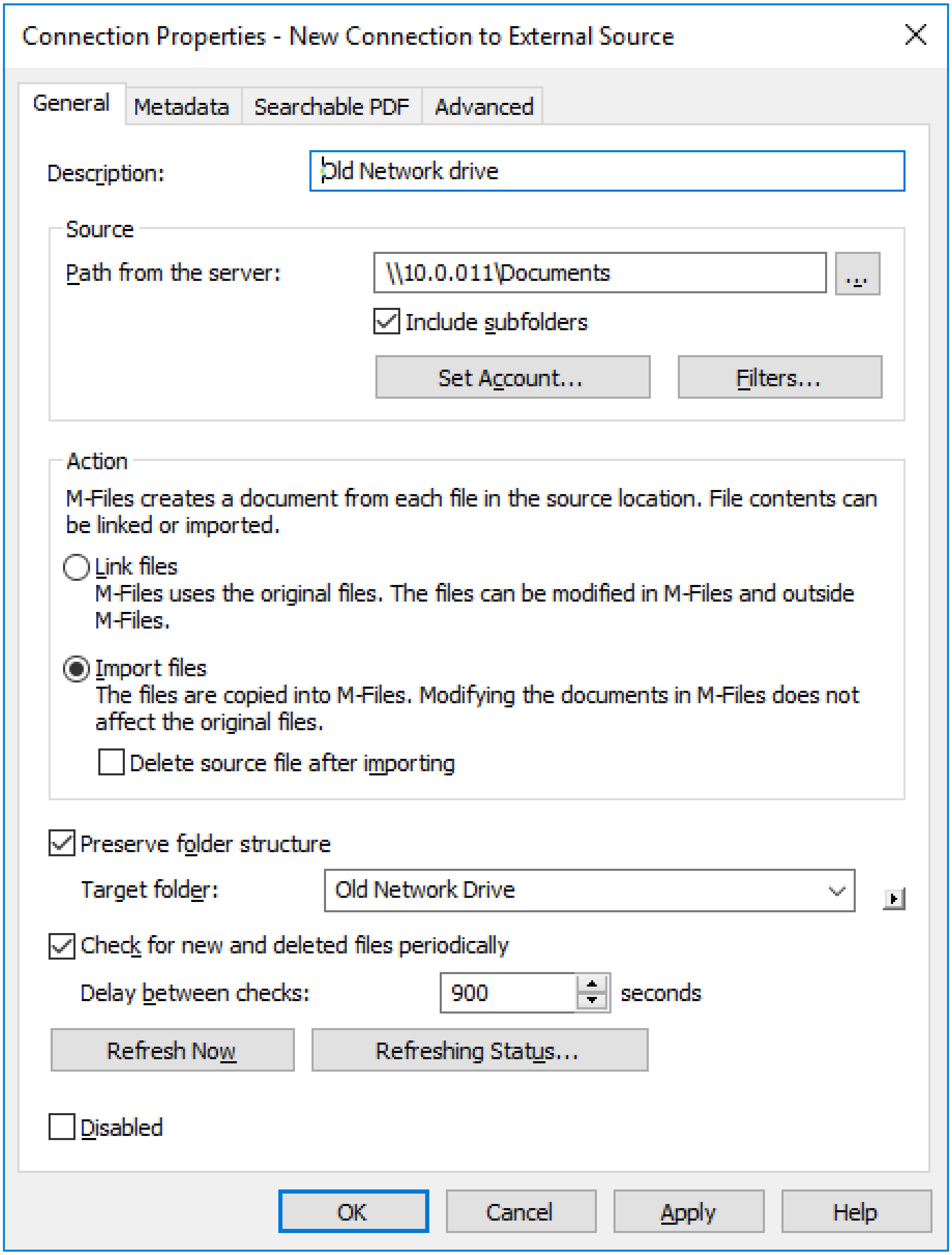
Creating a New Connection to an External Source

Before you begin, see this note if you plan to use the **Link files** option and to preserve the original files in the external location. You can also use external repository connectors to import content to your vault. See Connectors. Make sure that you do not use both features to import the same content.

Follow these instructions to define a new connection to an external source.

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Connections to External Sources** and then select **File Sources**.
6. In the task area, click **New File Source** to start creating a new connection to an external source.

   ☑ The **Connection Properties** dialog is opened.



Description: Old Network drive

Path from the server: \\10.0.011\Documents

☑ Include subfolders

M-Files creates a document from each file in the source location. File contents can be linked or imported.

○ Link files
M-Files uses the original files. The files can be modified in M-Files and outside M-Files.

● Import files
The files are copied into M-Files. Modifying the documents in M-Files does not affect the original files.

□ Delete source file after importing

☑ Preserve folder structure

Target folder: Old Network Drive

☑ Check for new and deleted files periodically

Delay between checks: 900 seconds

□ Disabled

7. 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.

8. 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.

9. Optional: Check the **Include subfolders** check box if you wish to include in the connection the entire folder structure of the specified path.

10. 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.

11. 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 with 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 (`;`).

12. Select either:

    a. **Link files**: Select this option to edit the files of the external source in M-Files and externally. Changes made in M-Files are shown to external users and changes made outside M-Files are shown in M-Files.

       Important: If the M-Files user group **All internal users** or **All internal and external users** does not have edit access to a linked document, the document is deleted from the external file source when it is added to M-Files. If this happens, you can copy the file back to the external location by adding edit access to either the **All internal users** or **All internal and external users** user group (see Object Permissions).

       This behavior can be prevented with a registry setting. For instructions, see Preventing Linked Documents from Being Removed.

       Note: Normally, M-Files only stores the latest external file version. To change this behavior, refer to the article Linked external file source documents only keep the latest file version in M-Files.

       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** 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.

13. Optional: Select the **Preserve folder structure** check box 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.

14. Optional: Select the **Check for new and deleted files periodically** 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.

Warning: Short synchronization intervals can cause performance issues if there are many connections to external sources.

15. 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.

16. 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.

17. Optional: On the **Advanced** tab, you can specify an alias for the new connection.

Use semicolons (;) to separate many aliases.

For more information, see Associating the Metadata Definitions.

When automatic aliases are in use and you write a name on the **General** tab, the **Aliases** field on the **Advanced** tab is automatically filled in. The alias has the format <*predefined prefix*>.<*name*>. Configure automatic aliases for your vault in Advanced Vault Settings.

18. Click **OK**.

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.
Defining Metadata for an External File Source

To define automatic metadata for externally created documents:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Connections to External Sources** and click **File Sources**.
6. On the **File Sources** list, double-click the file source that you want to edit.

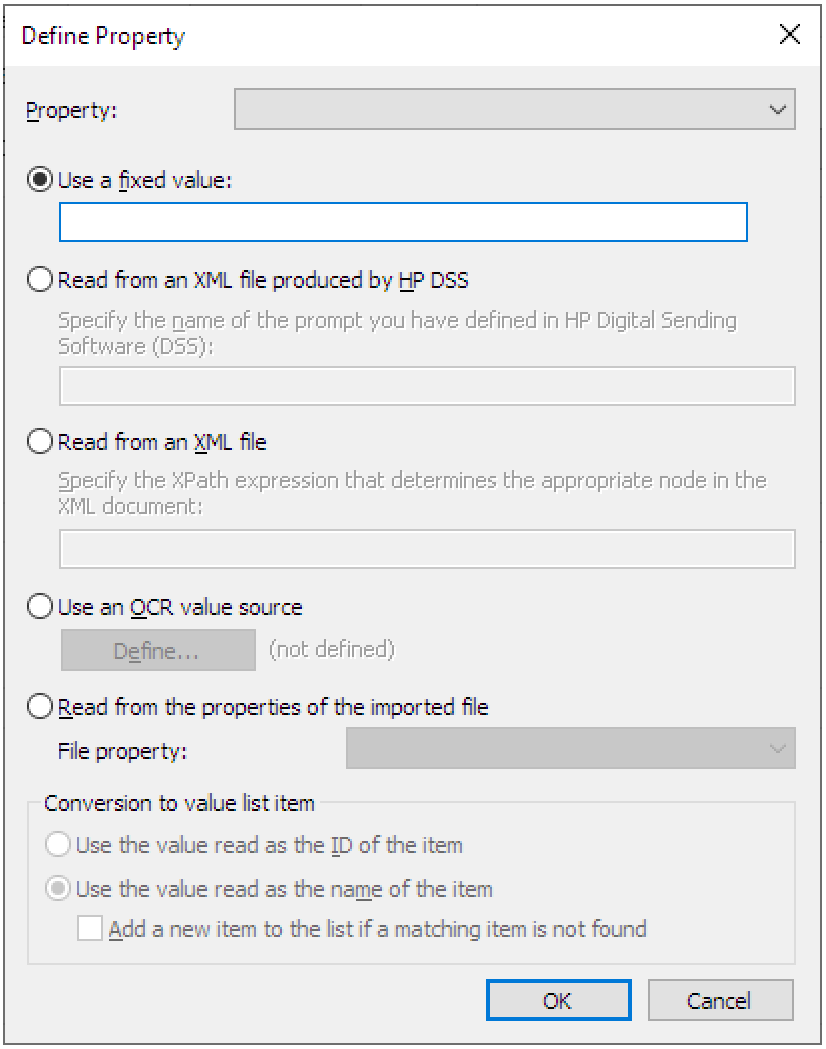
   ✓ The **Connection Properties** dialog is opened.
7. Click **Metadata**.

   ✓ The **Metadata** tab is opened.
8. In **Object type**, select the object type that the external objects get when they are imported or linked to M-Files.

The selected object type must have the **Objects of this type can have files** setting enabled.

9. 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.



Define Property

Property:

● Use a fixed value:

○ Read from an XML file produced by HP DSS

Specify the name of the prompt you have defined in HP Digital Sending Software (DSS):

○ Read from an XML file

Specify the XPath expression that determines the appropriate node in the XML document:

○ Use an OCR value source

Define... (not defined)

○ Read from the properties of the imported file

File property:

Conversion to value list item

○ Use the value read as the ID of the item

● Use the value read as the name of the item

□ Add a new item to the list if a matching item is not found

OK Cancel

10. Use the **Property** drop-down menu to select the property for which you want to define a value.

11. In the **Define Property** dialog, select one of the following options:

   a. **Use a fixed value**: Use this option to specify 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. The name of the XML file must match the name of the file to be imported. For instance, when the name of the file is `filename.txt` the XML file must be named `filename.xml`.

For example, say you have the following XML file:

```
<?xml version="1.0" encoding="UTF-8"?>
<document>
    <name>The name of the document</name>
    <keywords>Keywords in an XML file</keywords>
</document>
```

Now, to use the text inside the `keywords` element in the XML file as the value for the selected property, you would enter `document/keywords` in the **Read from an XML file** field, and thus you would get *Keywords in an XML file* as the property value. The string `document/keywords` is a simple XPath expression that selects all `keywords` elements that are children of the `document` element.

XPath is a W3C standard syntax for defining locations in an XML document. For detailed information on XPath syntax, see the W3Schools XPath Tutorial.

Note: If the XML file uses namespaces, you need to take them into account in the XPath expression. You can use the namespace prefixes in the expression. Note that the default namespace, however, has no prefix. Selecting from the default namespace is possible, for instance, by using the `namespace-uri()` or the `local-name()` XPath function, or both, in the expression. Multiple namespaces with the same prefix are not supported.

For example:

```
mynamespace:document/keywords
```

or

```
//*[namespace-uri()='http://www.exampleuri.com' and local-
name()='document']/[namespace-uri()='http://www.exampleuri.com' and
local-name()='keywords']
```

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.

or

e. **Read from the properties of the imported file**: Use this option to populate the property value with a Microsoft Windows file property value. Use the **File property** drop-down menu to select the appropriate file property. The accepted data types for the file properties are as follows:

- **Name**: Text, Text (multi-line)
- **Directory**: Text, Text (multi-line)
- **Extension**: Text, Text (multi-line), Choose from list
- **Created at**: Timestamp
- **Last modified**: Timestamp
- **Last accessed**: Timestamp
- **Read-only**: Boolean (yes/no)
- **Hidden**: Boolean (yes/no)
- **Archive**: Boolean (yes/no)

12. 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** check box if you want to add a new value list item whenever a new value is captured.

13. Click **OK** to close the **Define Property** dialog.

14. Use the **Permissions** drop-down menu to set the permissions for new objects created through the external source.

    ⓘ You can click the **...** button to refine the permission settings.

15. Optional: Check the **Read values from an XML file** check box if you want property values to be read from an XML file. Check also the **Delete the XML file after use** 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. For instance, when the name of the file is `filename.txt` the XML file must be named `filename.xml`. The supported XML formats are:

    - Regular XML data
    - XML data output by HP Digital Sending Software (DSS)

16. Click **OK** to finish defining the metadata.

The metadata that you specified is assigned to new objects created through this external source.

In this chapter

- Defining an OCR Value 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.

You can use optical character recognition with these file formats:

- TIF
- TIFF
- JPG
- JPEG
- BMP
- PNG

- PDF

TIFF files that use an alpha channel or JPEG compression are not supported.

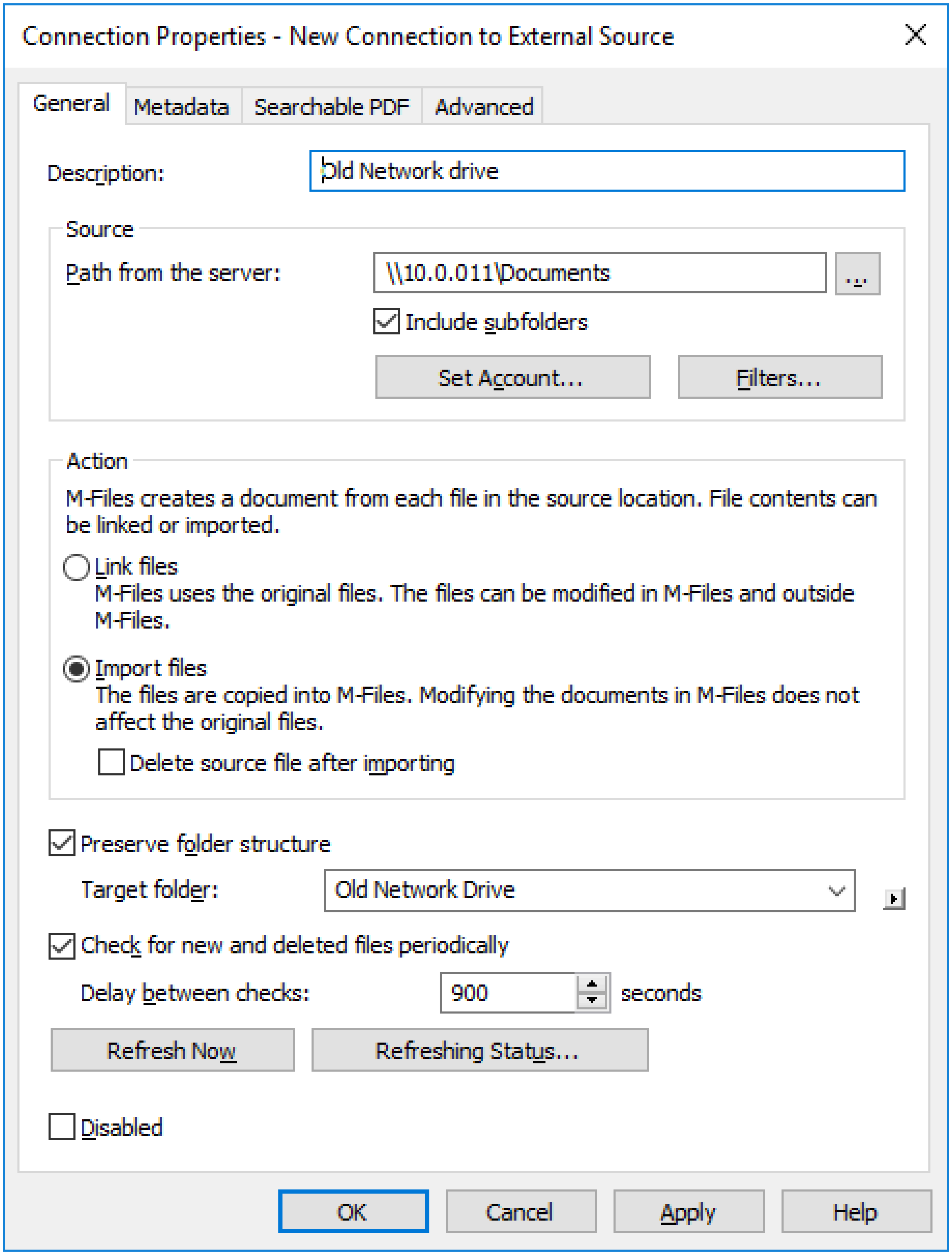
The use of an OCR value source is only possible when using an external source.

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 a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Connections to External Sources**
6. Click **File Sources**.
7. On the **File Sources** list, double-click the file source that you want to edit.

   ✓ The **Connection Properties** dialog is opened.



Connection Properties - New Connection to External Source

Description: Old Network drive

Source

Path from the server: \\10.0.011\Documents

☑ Include subfolders

Action

M-Files creates a document from each file in the source location. File contents can be linked or imported.

○ Link files
M-Files uses the original files. The files can be modified in M-Files and outside M-Files.

● Import files
The files are copied into M-Files. Modifying the documents in M-Files does not affect the original files.

□ Delete source file after importing

☑ Preserve folder structure

Target folder: Old Network Drive

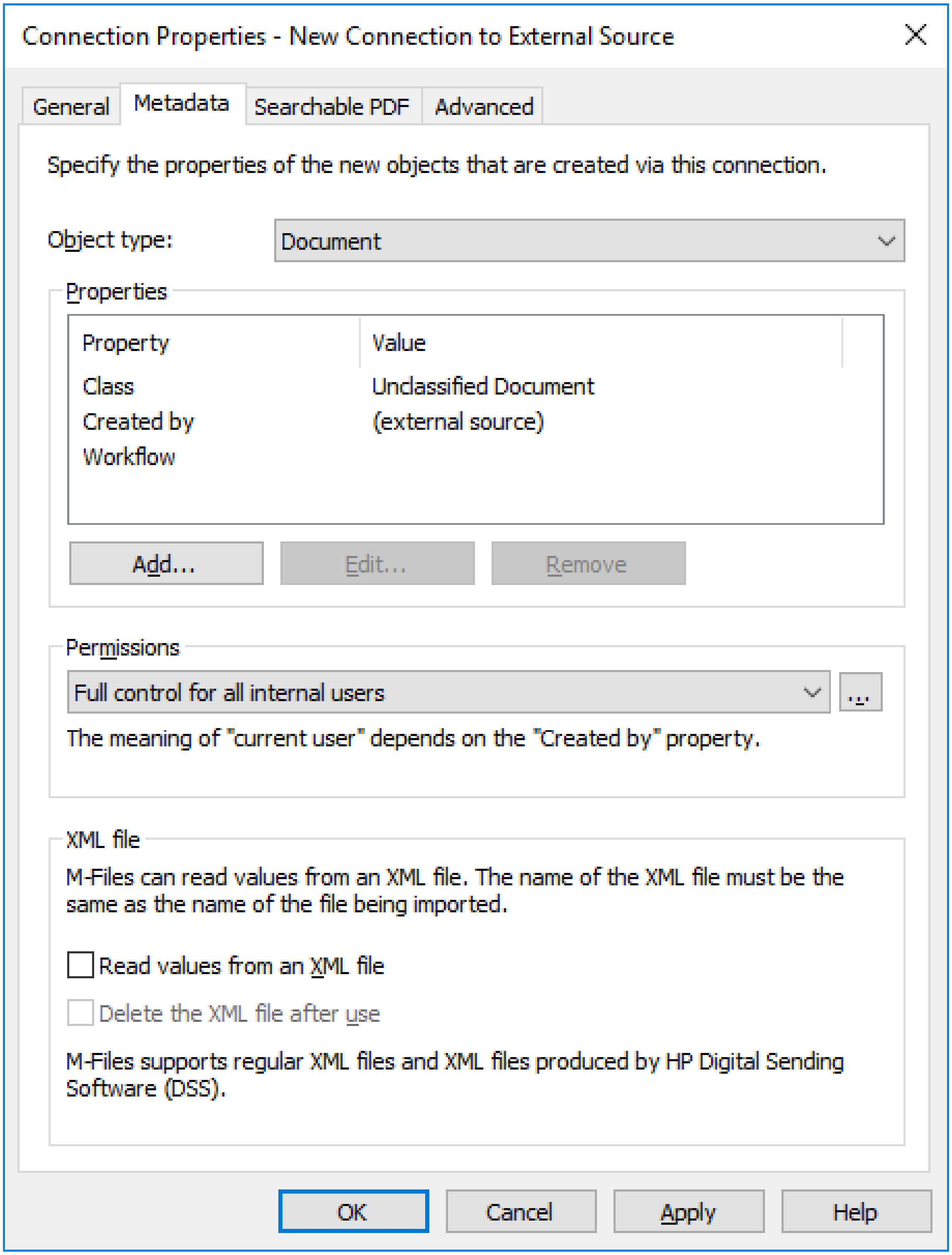
☑ Check for new and deleted files periodically

Delay between checks: 900 seconds

□ Disabled

8. Click the **Metadata** tab.

✓ The **Metadata** tab is opened.



Connection Properties - New Connection to External Source

Specify the properties of the new objects that are created via this connection.

Object type: Document

Properties

Property	Value
Class	Unclassified Document
Created by	(external source)
Workflow	

Permissions

Full control for all internal users

The meaning of "current user" depends on the "Created by" property.

XML file

M-Files can read values from an XML file. The name of the XML file must be the same as the name of the file being imported.

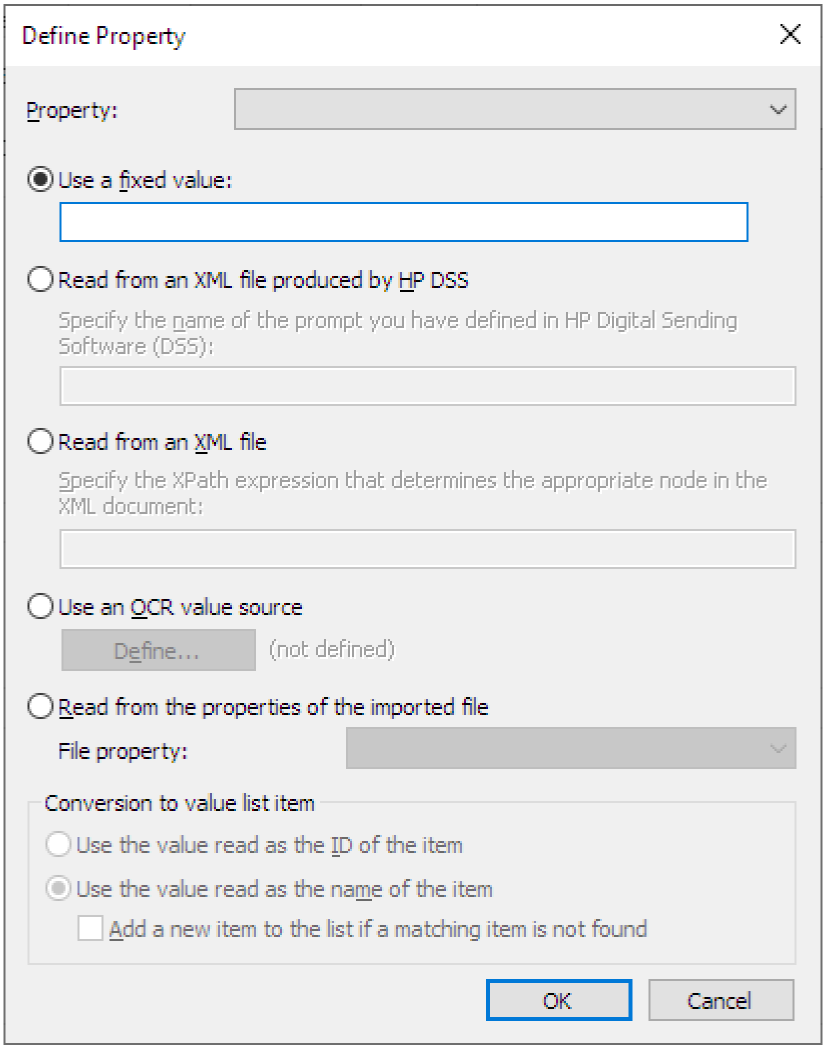
□ Read values from an XML file

□ Delete the XML file after use

M-Files supports regular XML files and XML files produced by HP Digital Sending Software (DSS).

9. 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.



Define Property

Property:

● Use a fixed value:

○ Read from an XML file produced by HP DSS

Specify the name of the prompt you have defined in HP Digital Sending Software (DSS):

○ Read from an XML file

Specify the XPath expression that determines the appropriate node in the XML document:

○ Use an OCR value source

Define... (not defined)

○ Read from the properties of the imported file

File property:

Conversion to value list item

○ Use the value read as the ID of the item

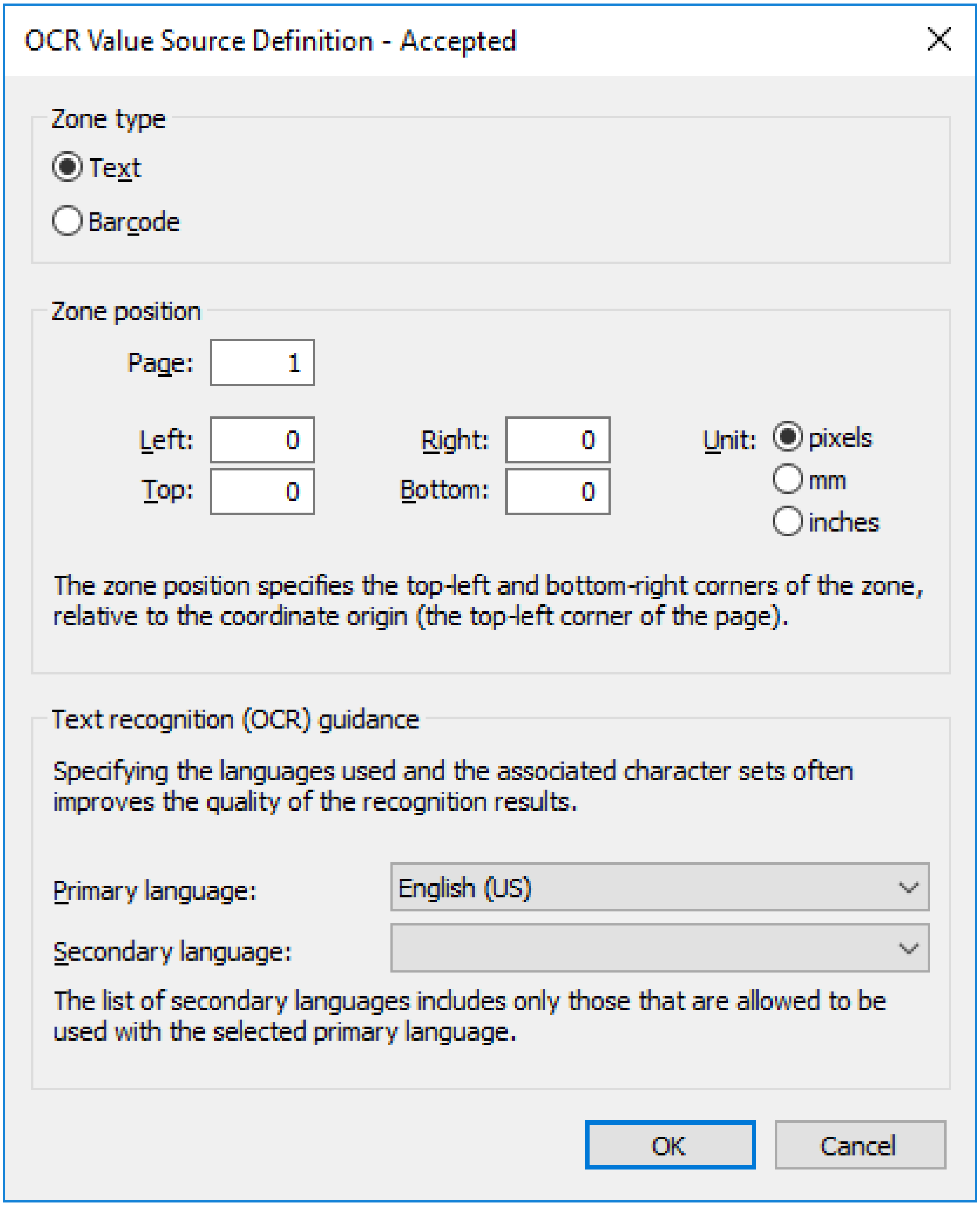
● Use the value read as the name of the item

□ Add a new item to the list if a matching item is not found

OK Cancel

10. Select the option **Use an OCR value source** and click the **Define...** button.

✓ The **OCR Value Source Definition** dialog is opened.



OCR Value Source Definition - Accepted

Zone type

● Text

○ Barcode

Zone position

Page: 1

Left: 0 Right: 0 Unit: ● pixels ○ mm ○ inches

Top: 0 Bottom: 0

The zone position specifies the top-left and bottom-right corners of the zone, relative to the coordinate origin (the top-left corner of the page).

Text recognition (OCR) guidance

Specifying the languages used and the associated character sets often improves the quality of the recognition results.

Primary language: English (US)

Secondary language:

The list of secondary languages indudes only those that are allowed to be used with the selected primary language.

11. In the **Zone type** section, select either:

a. **Text**: Select this option if the OCR zone contains text.

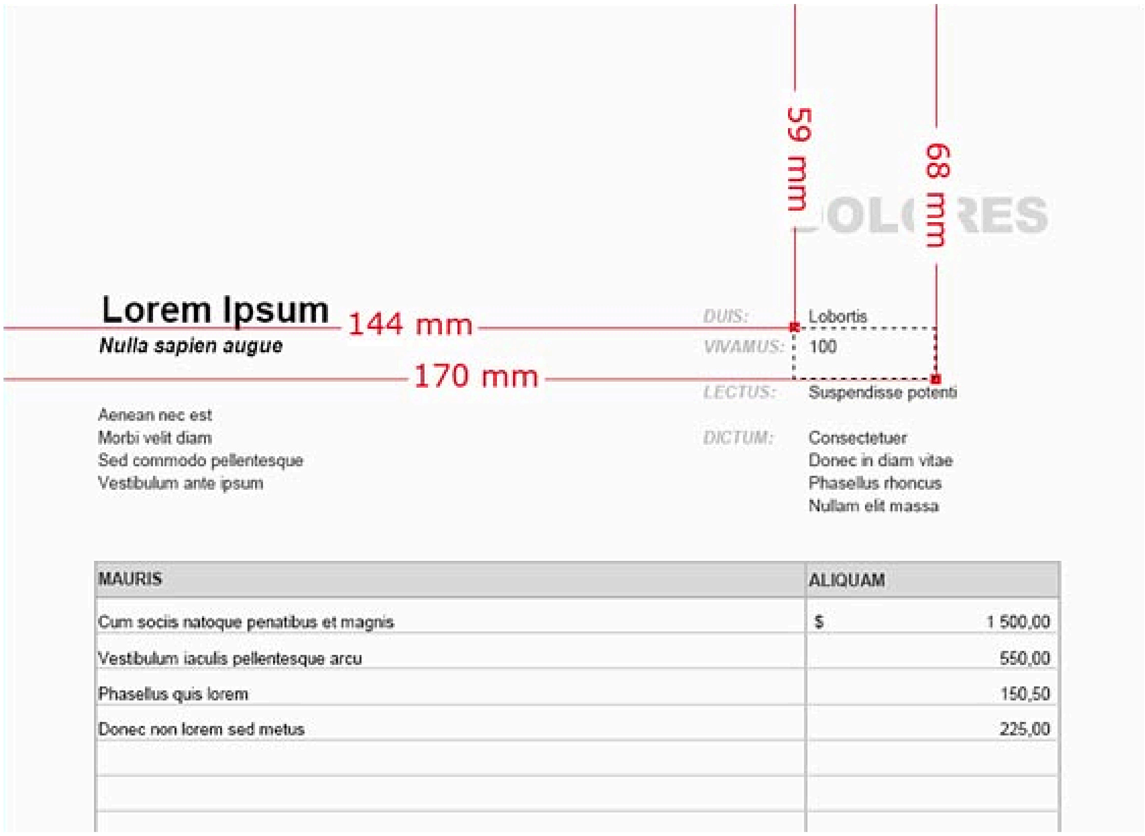
or

b. **Barcode**: Select this option if the OCR zone contains a barcode.

Note: For the supported barcode types, see Supported Barcode Types.

12. 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:

    Lorem Ipsum
    Nulla sapien augue

    Aenean nec est
    Morbi velit diam
    Sed commodo pellentesque
    Vestibulum ante ipsum

    DUIS: Lobortis
    VIVAMUS: 100
    LECTUS: Suspendisse potenti
    DICTUM: Consectetuer
    Donec in diam vitae
    Phasellus rhoncus
    Nullam elit massa

MAURIS	ALIQUAM
Cum socis natoque penatibus et magnis	$ 1 500,00
Vestibulum iaculis pellentesque arcu	550,00
Phasellus quis lorem	150,50
Donec non lorem sed metus	225,00

    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.

13. With the **Primary language** and **Secondary language** drop-down menus, select the primary and secondary language of the scanned documents 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.

14. Click **OK** to close the **OCR Value Source Definition** dialog.

15. 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** check box if you want to add a new value list item whenever a new value is captured.

16. 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 make sure that the specified zone is correctly positioned, in most cases the document to be scanned must be placed onto the scanner glass by hand.

In some cases, the OCR can give an incorrect recognition result of the text. For example, depending on the font type or size, the number `1` can be interpreted as the letter `I`. To make sure that the characters are added correctly to 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.

Supported Barcode Types

The M-Files OCR module supports the following barcode types:

- QR Code
- Data Matrix
- Aztec Code
- EAN-13
- EAN-8
- EAN-5
- EAN-2
- MSI Plessley
- MSI Pharma
- UPC-A
- UPC-E
- Codabar
- Interleaved 2 of 5
- Discrete 2 of 5
- Code 39
- Code 39 Extended
- Code 39 HIBC
- Code 93
- Code 128
- PDF 417

- Postnet
- Postnet 32
- Postnet 52
- Postnet 62
- Patchcode
- UCC-128
- UPCE Extended
- IATA 2 of 5
- Datalogic 2 of 5
- Reverse 2 of 5
- Code 39 (out-of-spec)
- Code 128 (out-of-spec)
- Codabar (out-of-spec)

Searchable PDF

M-Files can convert images imported from external file sources into *searchable PDFs* using optical character recognition (OCR). This makes full-text search of scanned documents possible. After conversion, you can find the PDF document by searching the actual document content.

You can use optical character recognition with these file formats:

- TIF
- TIFF
- JPG
- JPEG
- BMP
- PNG
- PDF

TIFF files that use 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: When you use the OCR feature in M-Files on a signed PDF, the entire document is rewritten. Because digital signatures validate the content, any edits made by OCR will invalidate the existing signature. This can result in the signature's removal.

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 a connection to M-Files server.

3. Expand **Document Vaults**.

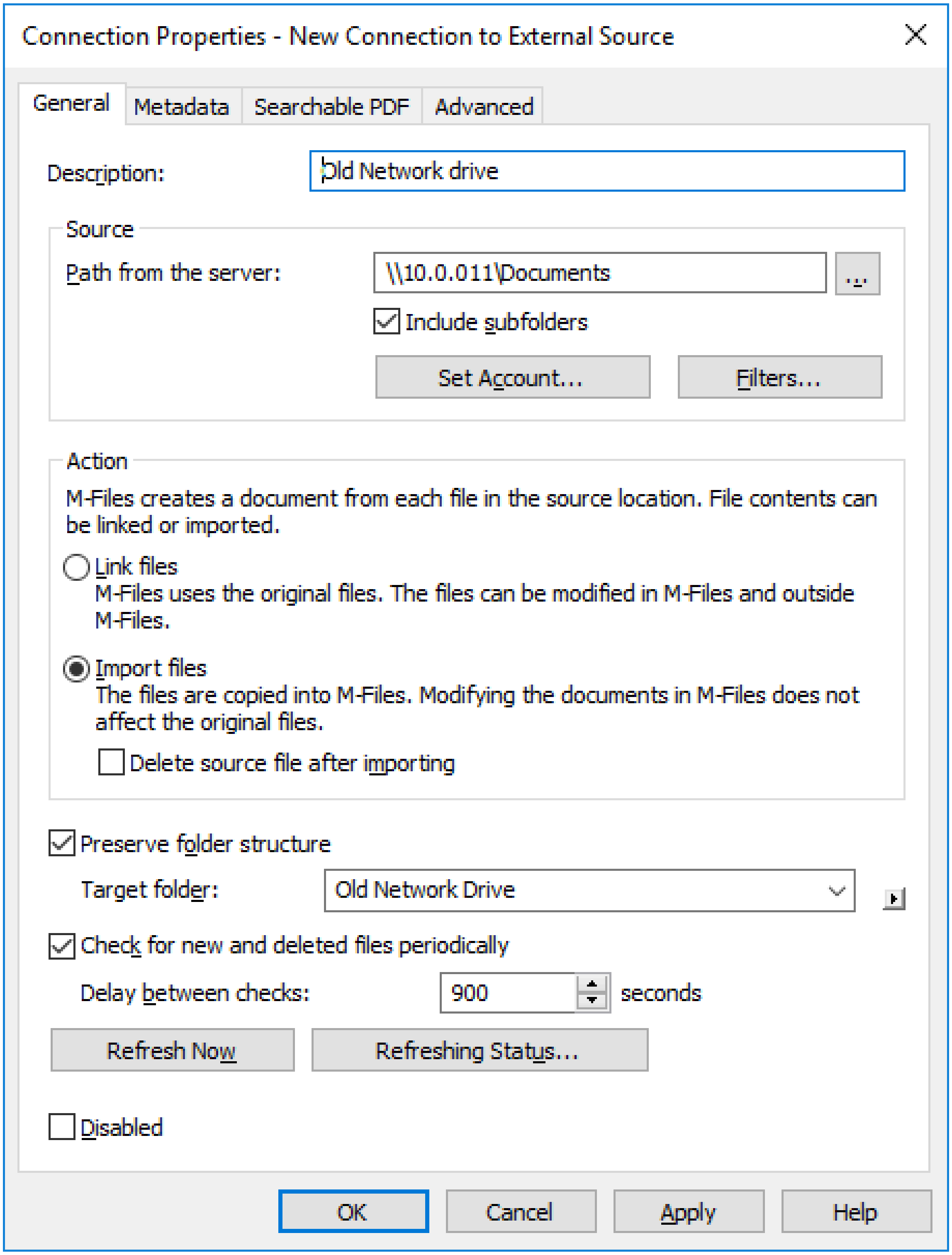
4. Expand a vault.

5. Expand **Connections to External Sources**.

6. Click **File Sources**.

7. On the **File Sources** list, double-click the file source that you want to edit.

   ✓ The **Connection Properties** dialog is opened.



Connection Properties - New Connection to External Source

Description: Old Network drive

Source

Path from the server: \\10.0.011\Documents

☑ Include subfolders

Action

M-Files creates a document from each file in the source location. File contents can be linked or imported.

○ Link files
M-Files uses the original files. The files can be modified in M-Files and outside M-Files.

● Import files
The files are copied into M-Files. Modifying the documents in M-Files does not affect the original files.

□ Delete source file after importing

☑ Preserve folder structure

Target folder: Old Network Drive

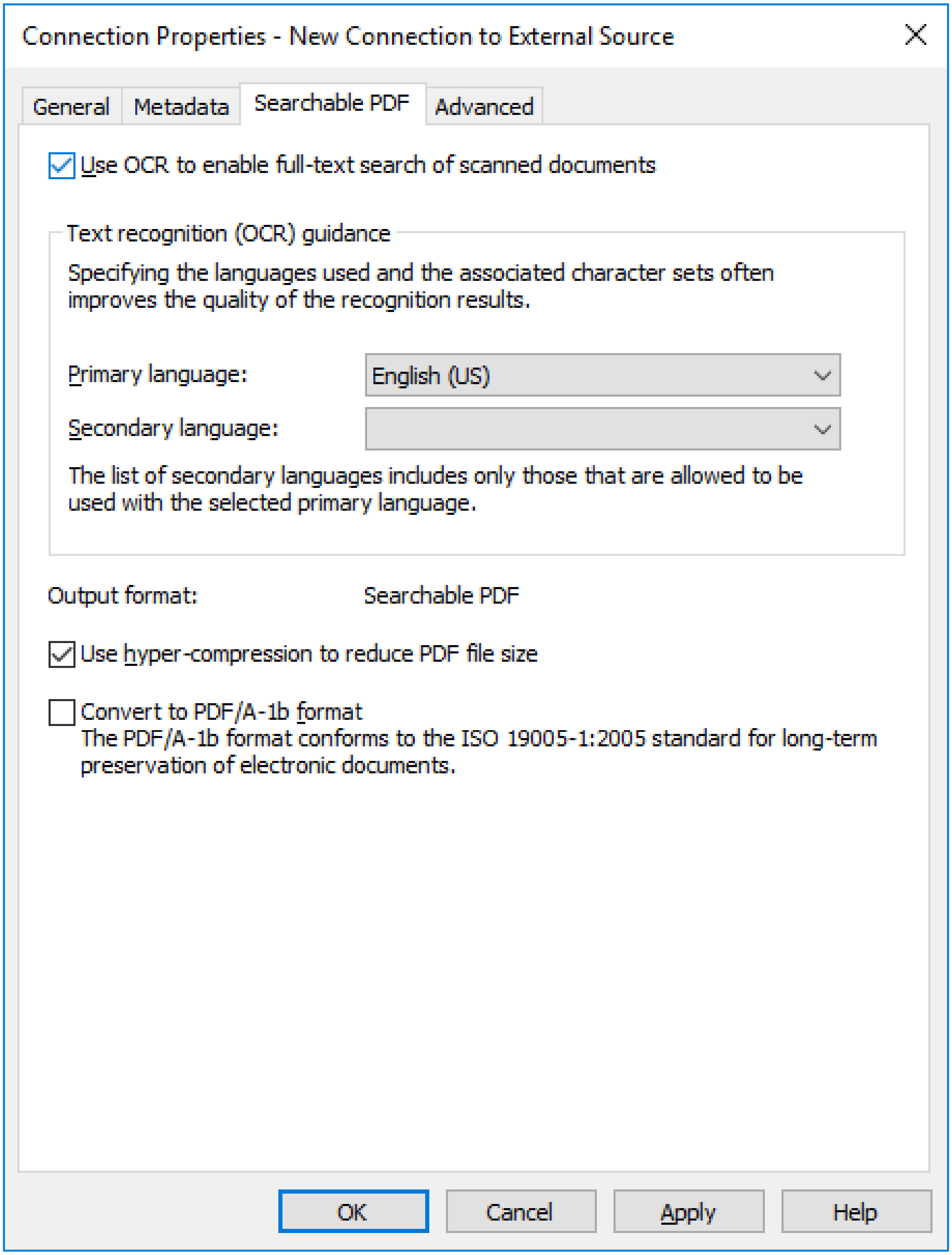
☑ Check for new and deleted files periodically

Delay between checks: 900 seconds

□ Disabled

8. Click the **Searchable PDF** tab.

   ✓ The **Searchable PDF** tab is opened.



☑ Use OCR to enable full-text search of scanned documents

Text recognition (OCR) guidance

Specifying the languages used and the associated character sets often improves the quality of the recognition results.

Primary language: English (US)

Secondary language:

The list of secondary languages includes only those that are allowed to be used with the selected primary language.

Output format: Searchable PDF

☑ Use hyper-compression to reduce PDF file size

□ Convert to PDF/A-1b format
The PDF/A-1b format conforms to the ISO 19005-1:2005 standard for long-term preservation of electronic documents.

9. Check the **Use OCR to enable full-text search of scanned documents** check box.

10. With the **Primary language** and **Secondary language** drop-down menus, select the primary and secondary language of the scanned documents 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.

11. Optional: Check the **Use hyper-compression to reduce PDF file size** check box if you want to reduce the file size of the searchable PDFs created via this connection.

12. Optional: Check the **Convert to PDF/A-1b format** 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.

13. Click **OK** to close the **Connection Properties** dialog.

The documents scanned with 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 done in the classic M-Files Desktop. For more information, see Scanning and Text Recognition (OCR). 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 our customer support in M-Files Support Portal or your M-Files reseller.

Deleting a Connection to an External Source

Complete the following steps to delete a connection to an external source:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Connections to External Sources** and then select **File Sources**.
6. Right-click the connection that you want to delete and select **Delete** from the context menu.
7. Click **Yes** at the prompt to confirm the deletion.
8. Optional: If the type of the connection you are about to delete is **Link**, you must select between these options:

    a. **Import Linked Files**: The documents obtained via the connection are imported to M-Files, but the link between the documents in M-Files and the files on the file system will be disabled. When you select this option, the connection imports the files from the file source and after the import is complete, you may delete the connection. The files on the file system and the documents in M-Files will continue to live their own lives independently of each other.

or

b. **Destroy Documents**: The documents added to M-Files through the connection are destroyed in M-Files, but the previously linked files stay in the file system. The external folder will no longer be linked to M-Files and the files previously added to M-Files through this connection are available in the external location only.

   or

c. **Cancel**: This option cancels the operation.

The selected connection is deleted and files are no longer imported or linked from the selected file system location to M-Files.

Scanner Sources

With a scanner connection, you can save paper documents to the vault in digital format. This lets the M-Files search capabilities to be used with 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.

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 with 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 through 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.

Note: Text recognition can also be done with the M-Files OCR module. You can also scan using a local scanner that is directly connected to your computer. For more information, see Scanning and Text Recognition (OCR).

Mail Sources

You can use external mail sources to save, manage, and share important email, and to make sure that important information does not get lost in email boxes. For example, you can set a designated archive account to import all email to the vault and to then delete the messages from the mail server. In the vault, you can manage the imported messages with the M-Files features. Example use cases include managing orders or archiving sent offers. You can use the `Cc` and `Bcc` fields to save sent email to the vault as well, for example proposals and order confirmations. To avoid junk mail, you can set the email account to accept email only from users in your organization.

Warning: A large number of connections to external sources with short synchronization intervals can cause performance and other issues. One solution is to set a limit for simultaneous mail source updates. To do this, configure the setting **Maximum Number of Simultaneous Updates** in the **Connections to External Sources** > **Mail Sources Common** section of Advanced Vault Settings.

In this chapter

Connecting to a New Mail Source

To connect to a new mail source:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Connections to External Sources** and select **Mail Sources**.
6. In the task area, click **New Mail Source**.

   ✓ The **Connection Properties** dialog is opened.
7. In **Description**, enter a description for the new connection.
8. In **Service type**, select one of these options:

   - **Generic POP3 service**: Use the POP3 protocol to connect to a mail service that is not listed here.
   - **Generic IMAP4 service**: Use the IMAP4 protocol to connect to a mail service that is not listed here.
   - **Microsoft Exhange Online**: Connect to Microsoft Exchange Online.

     Refer to this document for instructions on how to set up an OAuth application in Azure Portal: Azure Portal Configuration for Microsoft Exchange Online as External Mail Source. You will need the application details in step 9.

     Note: Microsoft Exchange Online connections cannot be set up or edited with Microsoft Windows Server 2016. You can do the setup and editing remotely with a supported Microsoft Windows operating system.
   - **Google Mail (IMAP4)**: Connect to Google Mail with the IMAP4 protocol.
9. In the **Configuration** section, enter the necessary information for your service type. See the information in the table.

Service	Setting name	Description
Generic POP3 service	Mail server	The IP address or domain name of the mail server.

Service	Setting name	Description
	Use encrypted connection (SSL/TLS)	Specifies whether the connection to the server is encrypted. In most cases, encrypted connection is necessary. **Note:** The M-Files server and the mail server must use TLS (Transport Layer Security) 1.2 or later.
	Port number	The communication endpoint of the mail server.
	Username	The username to access the mail server.
	Password	The password for the user.
Generic IMAP4 service	Mail server	The IP address or domain name of the mail server.
	Use encrypted connection (SSL/TLS)	Specifies whether the connection to the server is encrypted. In most cases, encrypted connection is necessary. **Note:** The M-Files server and the mail server must use TLS (Transport Layer Security) 1.2 or later.
	Port number	The communication endpoint of the mail server.
	Folder	The folder from which M-Files reads and imports the mail to the vault.
	Username	The username to access the mail server.
	Password	The password for the user.
Microsoft Exchange Online	Tenant ID	The tenant ID (also called directory ID) of your Microsoft Entra ID application. For example: `00112233-4455-6677-8899-aabbccddeeff`
	Client ID	The client ID (also called application ID) of your Microsoft Entra ID application. For example: `00112233-4455-6677-8899-aabbccddeeff`
	Client secret	The client secret of your Microsoft Entra ID application. For example: `sXXtFz1UtYMRCVc.2.23TMC-94-T.yK-84`

Service	Setting name	Description
	Folder	The email address and folder from which M-Files reads and imports the mail to the vault. For example: `mail@example.com/Inbox` or `mail@example.com/Important/Sales`.
	HTTP proxy	This is an optional setting. For authentication and email requests to use a proxy server, enter the address and port of the server. For example: `192.168.1.1:8080`. The proxy server must support the SSL protocol.
Google Mail (IMAP4)	Client ID	The client ID of your OAuth application. For more information, refer to Google Cloud Platform Configuration for Gmail as External Mail Source.
	Client secret	The client secret of your OAuth application. For more information, refer to Google Cloud Platform Configuration for Gmail as External Mail Source.
	Folder	The folder from which M-Files reads and imports the mail to the vault.
	HTTP proxy	This is an optional setting. For authentication and email requests to use a proxy server, enter the address and port of the server. For example: `192.168.1.1:8080`. The proxy server must support the SSL protocol.

10. Optional: In the **Action** section, select the appropriate options:

Select the option...	If you want to...
Include attachments	Import attachments with email messages.
Import only messages that have attachments	Import only the email messages that have attachments.
Delete messages from server after importing	Remove the messages from the mail server automatically when they have been imported to M-Files. Make sure that any information only supported by the email server is not lost.
Remove attachments from server after importing	Remove the attachments from the mail server when the email messages have been imported to M-Files. This option is available only if the selected service type is not **Generic POP3 service** and the option **Include attachments** is enabled.
Save in Outlook message format (*.msg)	Save the email messages to M-Files in the Outlook message format (MSG). Attachments are stored in the MSG file and the messages appear in M-Files as single-file documents (see Single-File and Multi-File Documents). **Note:** This functionality requires Microsoft Exchange Server or a 32-bit MAPI client to be installed on the M-Files server. If you want to save the email messages as RFC 822 compliant EML files, configure the registry setting that follows on the M-Files server computer.

<table>
<tr><th>Select the option...</th><th>If you want to...</th></tr>
<tr><td></td><td>
<table>
<tr><td><b>Key</b></td><td colspan="2"><b><code>HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<i>&lt;version&gt;</i>\Server\MFServer\Vaults\<i>&lt;vault GUID&gt;</i>\ MailSources\<i>&lt;external mail source name&gt;</i></code></b></td></tr>
<tr><td>Value name</td><td colspan="2"><code>StoreEmailInRawEmlFormat</code></td></tr>
<tr><td>Value type</td><td colspan="2"><code>REG_DWORD</code></td></tr>
<tr><td>Description</td><td colspan="2">When this is enabled, M-Files stores new email messages as EML files.</td></tr>
<tr><td>Default value</td><td><code>0</code></td><td>Disabled</td></tr>
<tr><td rowspan="2">Valid values</td><td><code>1</code></td><td>Enabled</td></tr>
<tr><td><code>0</code></td><td>Disabled</td></tr>
</table>
This registry setting overrides the selected storage format option. For the changes to take effect, you must restart the M-Files Server service.
</td></tr>
<tr><td><b>Separate attachments from the message</b></td><td>Save attachments separately from the body of the message. This option can be enabled only if the option <b>Save in Outlook message format (*.msg)</b> is enabled. The message without its attachments is saved to 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.</td></tr>
</table>

11. Optional: Select the **Check for new and deleted files periodically** check box to enable M-Files to synchronize with the mail server at predefined intervals.

a) In **Delay between checks**, enter the time interval in seconds between synchronizations.

Warning: Short synchronization intervals can cause performance issues if there are many connections to external sources.

12. Optional: Click **Refresh Now** to synchronize the vault with the mail server right away.

Click **Refreshing Status...** to see the current status of the refreshing process.

13. Optional: On the **Metadata** tab, specify properties for new objects created through this connection.

For more information, see Defining Automatic Metadata for a Mail Source.

14. Optional: On the **Advanced** tab, set an alias for this connection.

Use semicolons (;) to separate many aliases.

For more information, see Associating the Metadata Definitions.

When automatic aliases are in use and you write a name on the **General** tab, the **Aliases** field on the **Advanced** tab is automatically filled in. The alias has the format <*predefined prefix*>.<*name*>. Configure automatic aliases for your vault in Advanced Vault Settings.

15. Click **OK**.

This locks the **Service type** setting. Create a new connection to change the service type.

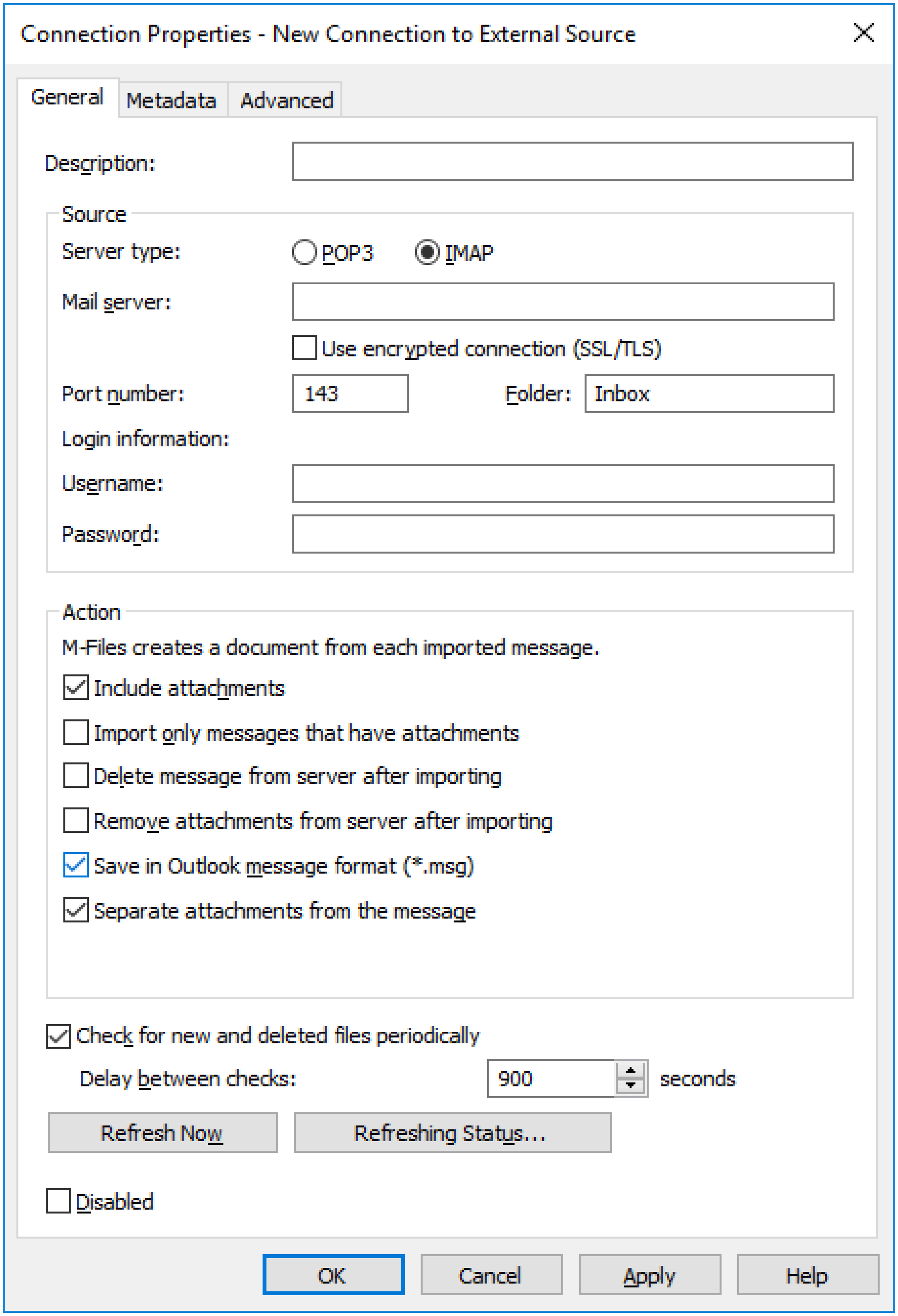
Email messages are imported to M-Files from the mail source with the specified settings. You can optionally change advanced settings for a Microsoft Exchange Online or Google Mail mail source in the **Connections to External Sources** > **Mail Sources Common** section of Advanced Vault Settings.
Defining 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 a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Connections to External Sources** and then select **Mail Sources**.
6. 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

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

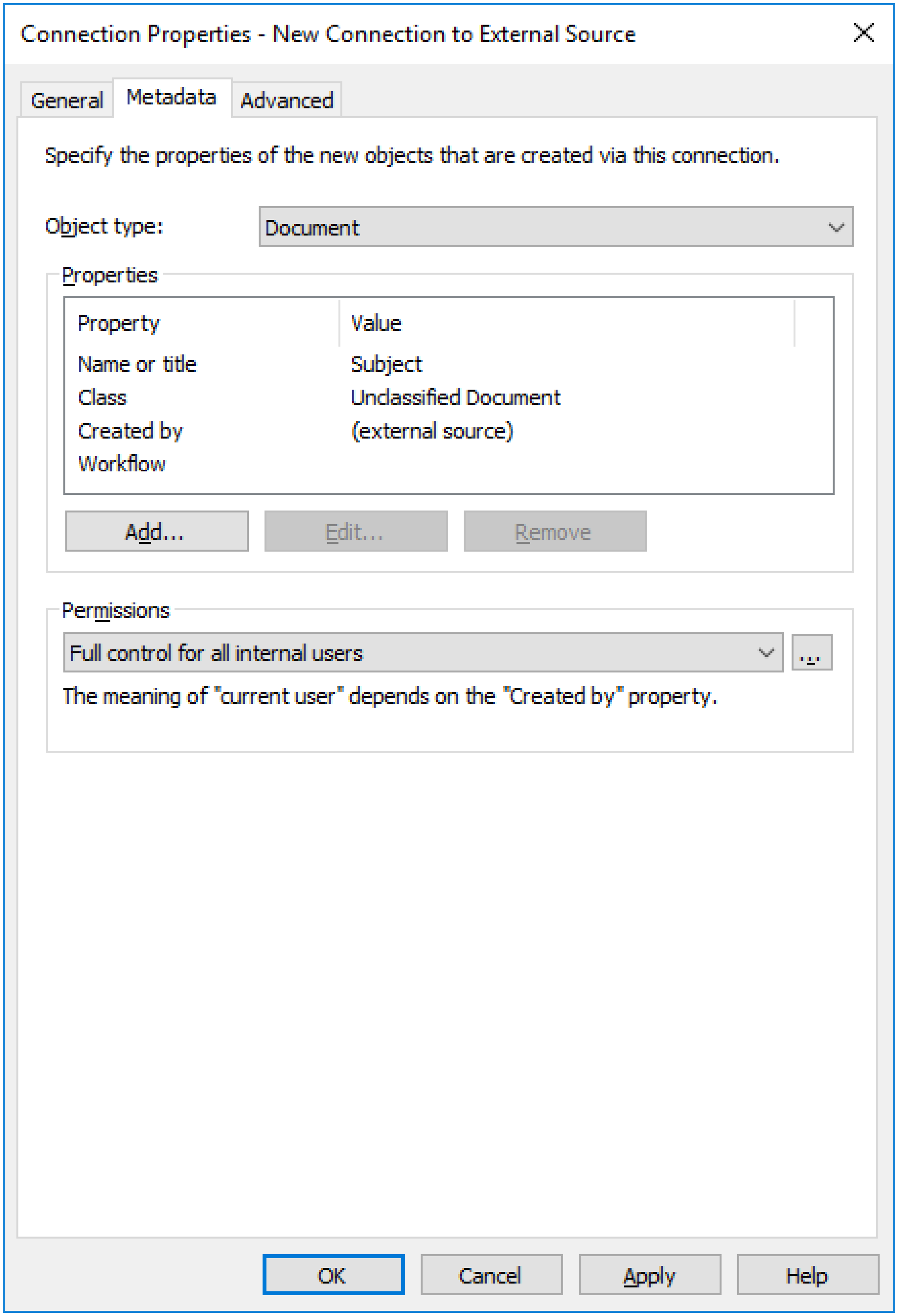
☑ Check for new and deleted files periodically

Delay between checks: 900 seconds

□ Disabled

7. Click the **Metadata** tab.

☑ The **Metadata** tab is opened.



Connection Properties - New Connection to External Source

Specify the properties of the new objects that are created via this connection.

Object type: Document

Properties

Property	Value
Name or title	Subject
Class	Unclassified Document
Created by	(external source)
Workflow	

Permissions

Full control for all internal users

The meaning of "current user" depends on the "Created by" property.

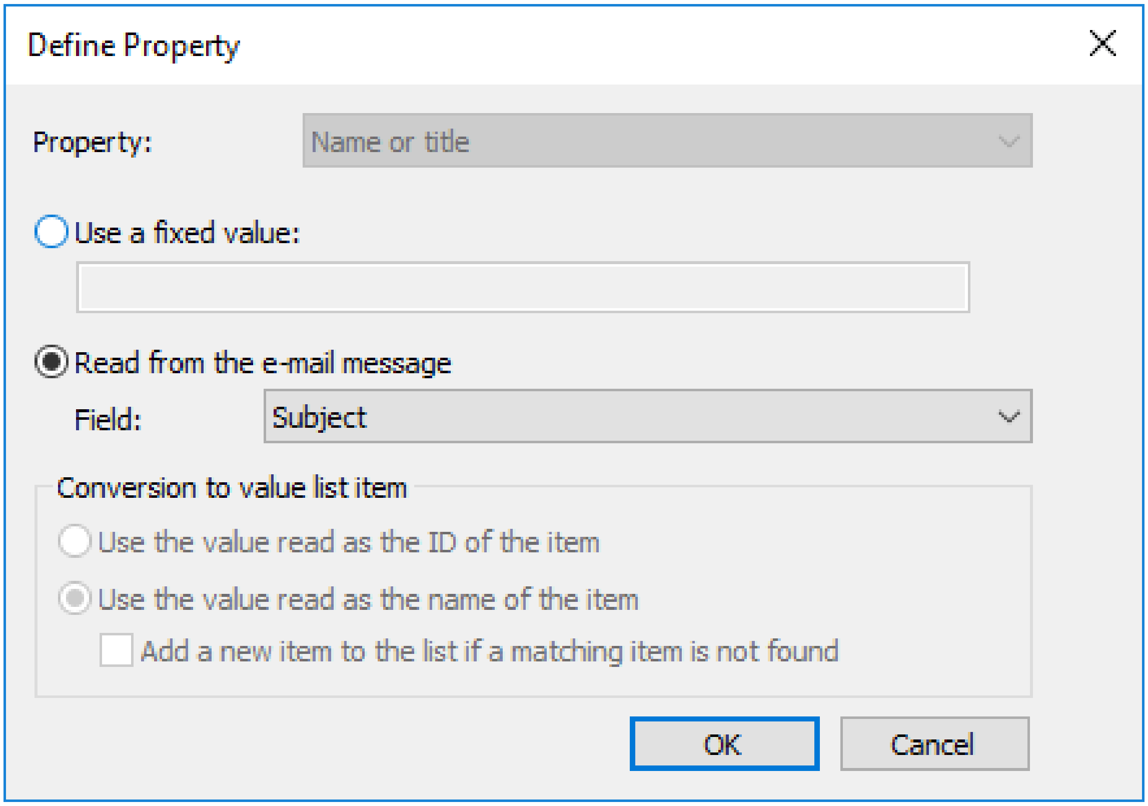
8. Use the **Object type** drop-down menu to select the object type for new objects created through this connection.

9. Use the **Permissions** drop-down menu to select the permissions for new objects created through this connection.

You can click the **...** button to refine the permission settings.

10. In the **Properties** section, click **Add** to add a new automatic property for objects created through this connection or select one of the existing properties and click **Edit** to edit it.

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



Define Property

Property: Name or title

○ Use a fixed value:

● Read from the e-mail message

Field: Subject

Conversion to value list item

○ Use the value read as the ID of the item

● Use the value read as the name of the item

□ Add a new item to the list if a matching item is not found

11. 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.

Note: If you select the **Date** field as the source of the property value, the data type of the property must be **Time**. It is not recommended to select a property of the **Timestamp** data type for the **Date** field because **Timestamp** values are adjusted by the time zone settings on client computers.

12. 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** check box if you want to add a new value list item whenever a new value is extracted.

13. Click **OK** to close the **Define Property** dialog.

The email messages imported to M-Files through this connection are assigned automatic properties according to the settings that you have defined.

Email Client Integration Settings

You can specify messages to be automatically associated with contact persons and customers in M-Files. M-Files does this on the basis of the sender and recipient information when the messages are saved to your vault in Microsoft Outlook. For an introduction to this feature, see Associating Messages with Contacts.

For information on how this feature is supported in different M-Files clients, refer to M-Files Client Feature Comparison.

To open the **Email Client Integration Settings** dialog:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Right-click a vault and select **Email Client Integration Settings**.

Contact persons

M-Files looks for a match with a contact person's email address. M-Files associates the message with the contact person Matt Bay if the properties of the contact person object have the same email address as the message (matt.bay@estt.com).

Customers

If you have specified customer information in the email integration settings:

1. M-Files looks for customer matches through the contact person information (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 email address and the customer's properties: M-Files associates the message with the customer ESTT on the basis of the email address domain, matt.bay@**estt.com** or patsy.bay@**estt.com**, if the domain `estt.com` is found in the customer's properties. The message is not associated with any contact person, unless a full match is found with the contact person information.

Advanced Settings

On the **Advanced** tab, you can further specify associations between email information and M-Files metadata. M-Files automatically populates the metadata card according to the defined mappings.

Note: These settings are in use in these situations:

- You drag and drop the email from Microsoft Outlook to M-Files.
- You select **Save to M-Files** from the Microsoft Outlook ribbon.

You can select a default class for all the email messages that are saved to M-Files with Microsoft Outlook. If you use the standard Microsoft Outlook integration, specify the default class here. If you use M-Files for Outlook, the user selects the default class in the add-in options in Microsoft Outlook. In other words, M-Files for Outlook does not use the default email class that is specified in **Email Client Integration Settings**.

With the other options on the **Advanced** tab, you can define an appropriate metadata property for the value of each email header field.

For example, if you want M-Files to automatically insert the information from the **From** field to a certain property on the metadata card of the email object, select the appropriate property from the drop-down menu.

Accepted data types

There are limitations for the data types of the properties that are assigned to object metadata with these settings. You can see the accepted data types in the table. You must also allow the properties to be used with the Document object type (or with all object types).

Email header field	Accepted data types
To	• Text (multi-line)
From	• Text • Text (multi-line)
Cc	• Text (multi-line)
Subject	• Text • Text (multi-line)
Received	• Timestamp
Sent	• Timestamp
Importance	• Text • Text (multi-line)

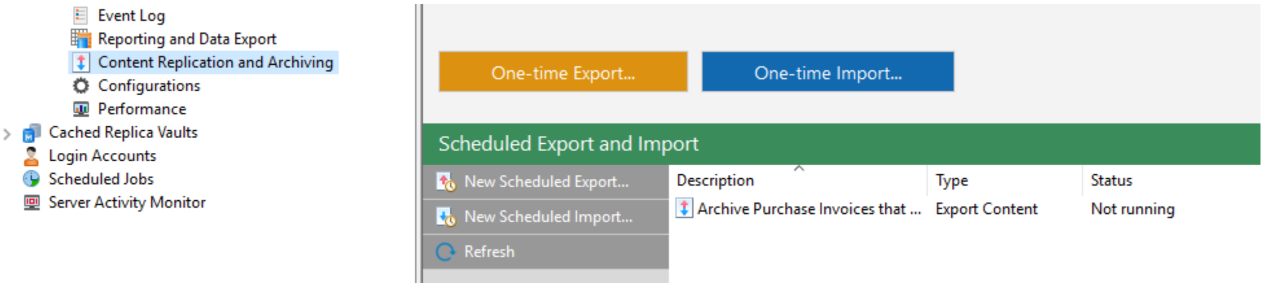
Email header field	Accepted data types
Sensitivity	• Text • Text (multi-line)

M-Files for Outlook

If you use M-Files for Outlook, specify the settings on the **M-Files for Outlook** tab. For more information, refer to Configuring M-Files for Outlook.

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 and import operations available in M-Files Admin.



Description	Type	Status
Archive Purchase Invoices that ...	Export Content	Not running

Figure 32: The replication features in M-Files Admin.

Note: Accessing these settings requires you to log in to the server with a login account that has the System administrator server role. Vault users with the Full control of vault rights are allowed to manage cloud storage based replication jobs.

Ways to utilize replication and archiving

With content replication and archiving, you can, for instance:

- 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).

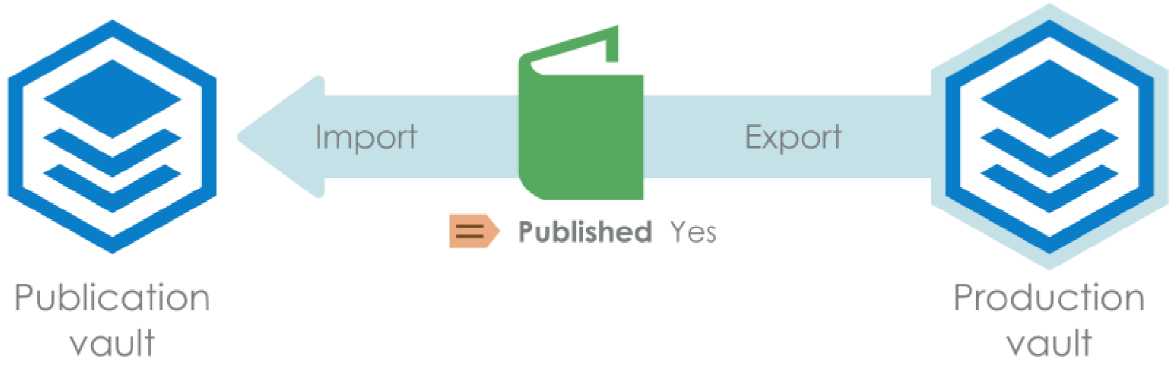


Figure 33: You can, for example, replicate documents from a production vault to a publication vault according to given property values of documents. For instance, a document may be replicated to a publication vault when the property Published is set to Yes.

For in-depth information on replication and archiving, see 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 associable between vaults. For more information, see Associating the Metadata Definitions.
- 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, each server must have a unique server license installed.
- All M-Files Server instances in a replication setup must have the same build number. For example, `12628` in `23.5.12628.4`.
- Two-directional replication of metadata structure is highly discouraged as the structure of the target vault is always overwritten with the structure in the content package, even if the metadata structure of the vault is more recent than the one in the content package. Thus, if two-directional replication of metadata structure is enabled, it may overwrite changes made to the metadata structure of any vault in the replication scheme.

  An exception to the above recommendation are value list items, as they are provided with timestamp information to indicate when they have been created or modified. Therefore replicating value list items does not have the same shortcomings as replicating other metadata structure items, as value list timestamps assure that the most recent value list items are always preserved during replication.
- Replication from a vault to another vault is not supported if the vaults have the same GUID. Two vaults must never share the same GUID. It is possible to generate such a situation, for example if a copy or a backup of a vault is attached to another server using the original GUID.
- It is highly discouraged to compress M-Files content packages using the ZIP archive format. ZIP archives do not specify the character encoding that is used for the file names stored in the archive, and therefore it may not be possible to import content packages that have been compressed using ZIP to systems that use different system language and code page settings than the system from which the content package was exported. If you wish to compress the content package, it is recommended to use a format that retains the character encoding information of file names, such as 7Z.

In this chapter

- Scheduled Export and Import
- Archiving Old Versions

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:

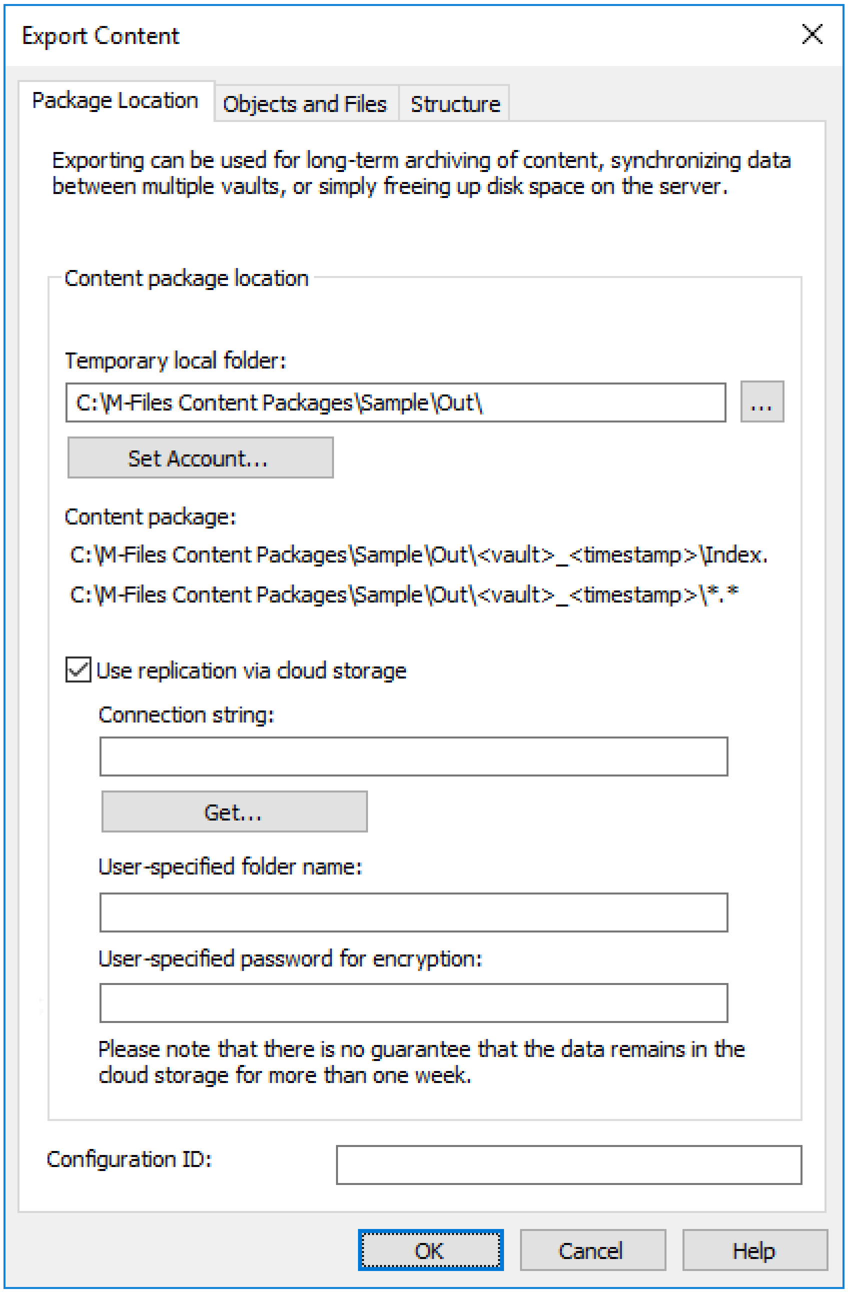
1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Content Replication and Archiving**.

   ✓ The content replication and archiving features are displayed in the right-side pane.

6. Click the **One-time Export...** button.

   ⓘ For information about creating a recurring export operation, see Defining a Scheduled Export.

   ✓ The **Export Content** dialog is opened.



Export Content

Exporting can be used for long-term archiving of content, synchronizing data between multiple vaults, or simply freeing up disk space on the server.

Content package location

Temporary local folder: C:\M-Files Content Packages\Sample\Out\

Content package:

C:\M-Files Content Packages\Sample\Out\<vault>_<timestamp>\Index.

C:\M-Files Content Packages\Sample\Out\<vault>_<timestamp>*.*

☑ Use replication via cloud storage

Connection string:

User-specified folder name:

User-specified password for encryption:

Please note that there is no guarantee that the data remains in the cloud storage for more than one week.

Configuration ID:

7. 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.

8. 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** or **Request**. The functionality is different in different M-Files environments.

Option	Description
Get	The connection string is automatically filled.
Request	An email message to M-Files customer support is opened. Remove unwanted locations from the line **Preferred location** and send the email.

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.

9. Optional: In the **Configuration ID** field, you can enter any string of characters for identifying this replication job.

M-Files automatically creates a numeric ID for each scheduled replication job. You can enter an additional ID for the job to the **Configuration ID** field. The configuration ID can be any string of characters. If a configuration ID cannot be found when the jobs are processed, M-Files uses the job ID.

10. On the **Objects and Files** tab, select **Export objects and files** and **Export existing objects**.

For more information about the options on this tab, see Export Objects and Files.

Note:

When the **Export only changes since latest run** option is enabled, only new objects and content that has versioning or non-versioning changes since the given date and time are exported. If you export also metadata structure elements, the elements are not exported unless there are changes to files or objects.

If you want to export metadata structure elements regardless of whether objects or files have been changed, do one of these operations:

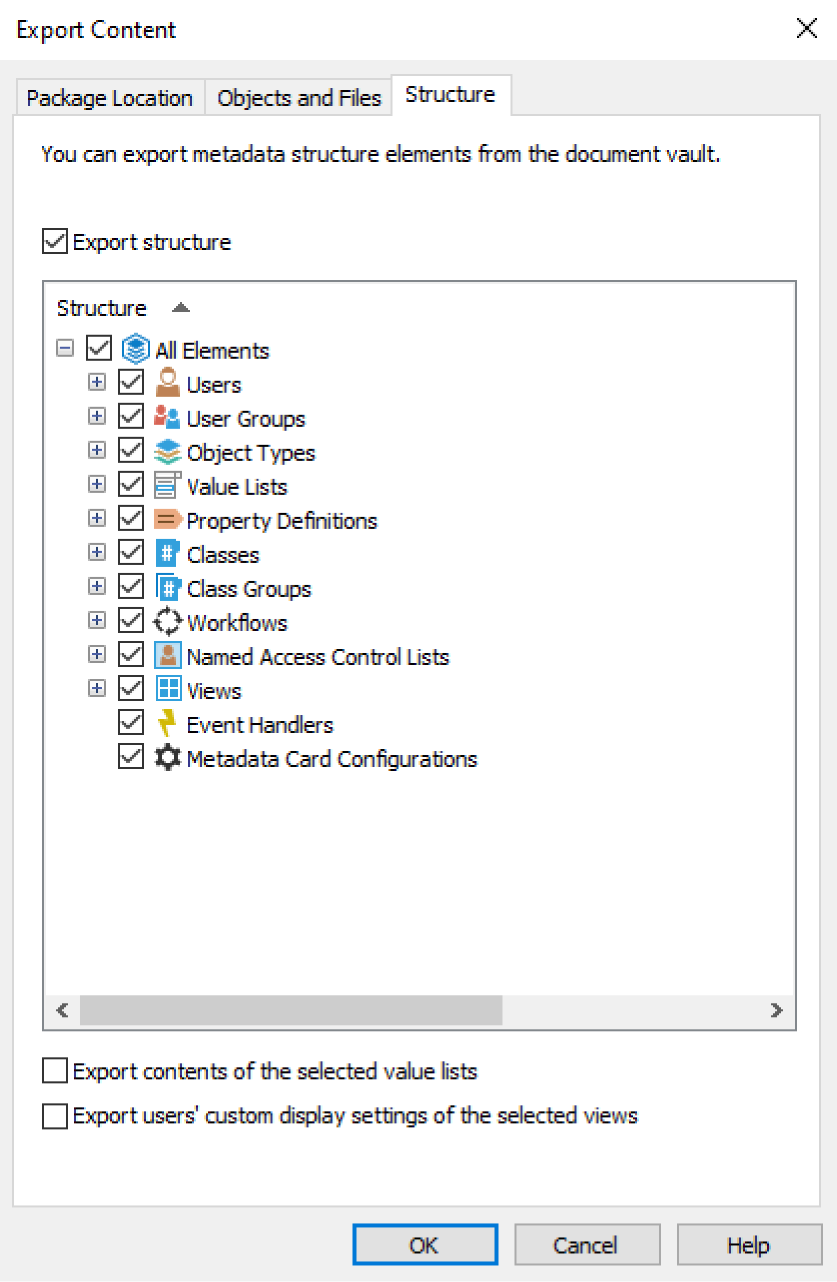
- Export the metadata structure separately.
- Disable the **Export only changes since latest run** option. However, if you do not limit the scope of the export in any way, it can take a considerable amount of time to complete the export job.

11. Optional: To define the conditions that objects must meet to be exported, select **Use a search filter** and click the **Define** button.

a) In the **Define Filter** dialog, define the conditions that objects must meet to be exported and click **OK** once you have defined all the necessary conditions.

12. Click the **Structure** tab.

✓ The **Structure** tab is opened.



Export Content

Package Location | Objects and Files | Structure

You can export metadata structure elements from the document vault.

☑ Export structure

Structure

- ☑ All Elements
  - ☑ Users
  - ☑ User Groups
  - ☑ Object Types
  - ☑ Value Lists
  - ☑ Property Definitions
  - ☑ Classes
  - ☑ Class Groups
  - ☑ Workflows
  - ☑ Named Access Control Lists
  - ☑ Views
  - ☑ Event Handlers
  - ☑ Metadata Card Configurations

□ Export contents of the selected value lists

□ Export users' custom display settings of the selected views

13. 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.

For more information about the options on this tab, see Export Structure.

14. Click **OK** to close the **Export Content** dialog and to start the export.

Note: Make sure that the export operation is complete before you take any actions in the vault.

When the export operation is complete, you can use the export package to import the exported content to another vault. See Importing Content.

In this chapter

- Export Package Location
- Export Objects and Files
- Export Structure

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**.

M-Files automatically creates a numeric ID for each scheduled replication job. You can enter an additional ID for the job to the **Configuration ID** field. The configuration ID can be any string of characters. If a configuration ID cannot be found when the jobs are processed, M-Files uses the job ID.

Use replication via cloud storage

You can also use replication through 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

Click **Get** to update the connection string for the cloud storage location. Use the same string for export and import. If there is no **Get** button, click **Request** to send an email to our customer support, and wait for them to send you the connection string.

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 lets you to change settings for exporting object and file content.

> ! **Important:** When you export objects, make sure that the target vault does not refer to the same external repositories as the source vault. Vaults that refer to the same repositories can cause duplicate objects in the target vault.

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 for example certain price lists from a vault designed for partner use, you need to make sure that this setting has been enabled and that the price lists 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 set M-Files to destroy the exported objects after the export. You cannot select this setting if you have selected to export the latest versions or changes since the latest run only.

Export migrated objects as internal objects

When this option is enabled, objects from external repositories are exported without their external repository ID. It can be useful to enable this option if external repository IDs contain sensitive data. For example, customer names.

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 select to export only the changes made since the latest export. This means that only new objects and content that has versioning or non-versioning changes are exported. Thus, also objects whose **Last modified** timestamp has not changed can be included in the export job.

For example, these content changes are included in the export package when **Export only changes since latest run** is selected:

- Object created
- File content edited
- Object metadata edited
- Object deleted
- Object undeleted
- Object checked out
- Checkout undone
- Conflict resolved
- Object version label changed
- Comment added for object version
- New object version imported to vault

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).

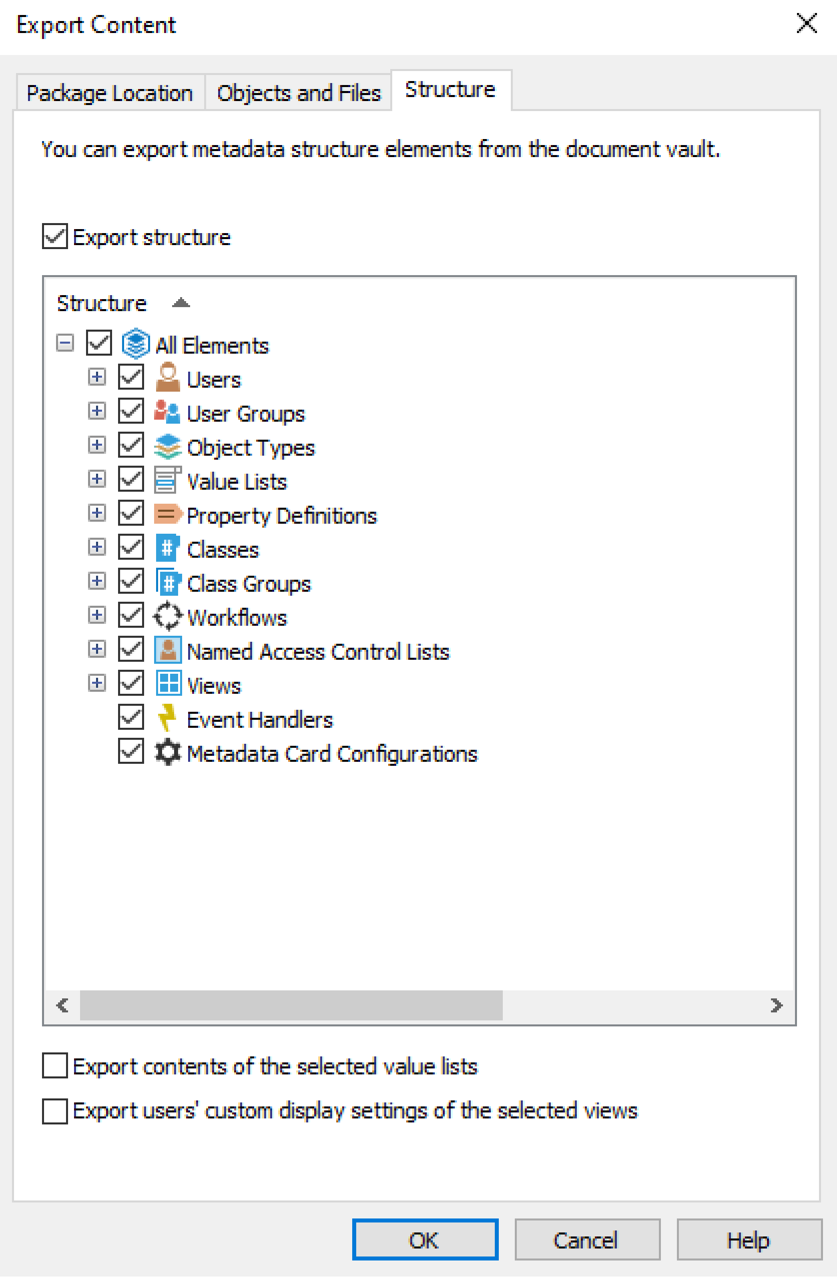
> **Note:**
>
> When the **Export only changes since latest run** option is enabled, only new objects and content that has versioning or non-versioning changes since the given date and time are exported. If you export also metadata structure elements, the elements are not exported unless there are changes to files or objects.
>
> If you want to export metadata structure elements regardless of whether objects or files have been changed, do one of these operations:
>
> - Export the metadata structure separately.
> - Disable the **Export only changes since latest run** option. However, if you do not limit the scope of the export in any way, it can take a considerable amount of time to complete the export job.

Preview

Click the **Preview** button to see the number of objects to be affected by the export process.

Export Structure

The **Structure** tab enables you to select which parts of the metadata structure you want to export.



Export Content

You can export metadata structure elements from the document vault.

☑ Export structure

Structure

- ☑ All Elements
  - ☑ Users
  - ☑ User Groups
  - ☑ Object Types
  - ☑ Value Lists
  - ☑ Property Definitions
  - ☑ Classes
  - ☑ Class Groups
  - ☑ Workflows
  - ☑ Named Access Control Lists
  - ☑ Views
  - ☑ Event Handlers
  - ☑ Metadata Card Configurations

□ Export contents of the selected value lists

□ Export users' custom display settings of the selected views

Figure 34: The **Structure** tab of the **Export Content** dialog.

Export structure

You can select the metadata structure elements of the selected vault to be exported or select all elements with **All Elements**.

Important remarks

- Built-in elements are always created in M-Files by default. They include, for example, the property definitions **Name or title**, **Created by**, and **Keywords**. In addition to these, administrators can create user-defined elements.
- It is recommended to use aliases or GUIDs in event handlers and metadata card configurations. This is because they are exported as-is and because the metadata element IDs can be different in the source and the target vaults.

- The imported metadata card configurations are visible in the target vault after you either restart M-Files Admin or do a forced refresh (Ctrl + F5) in the configurations editor.

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 deleted values in the source or target vault with 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, you can import its content to a vault. 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:

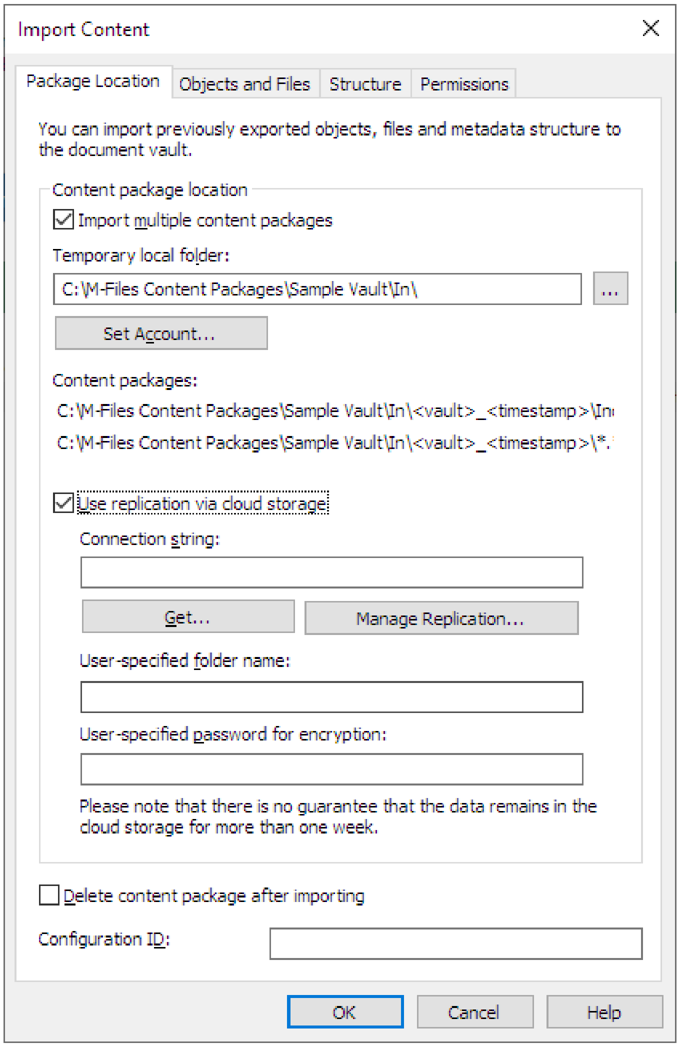
1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click **Content Replication and Archiving**.

   ☑ The content replication and archiving features are displayed in the right-side pane.

6. Click the **One-time Import...** button.

   ⓘ For information about creating a recurring import operation, see Defining a Scheduled Import.

   ☑ The **Import Content** dialog is opened.



Import Content

You can import previously exported objects, files and metadata structure to the document vault.

Content package location

☑ Import multiple content packages

Temporary local folder: C:\M-Files Content Packages\Sample Vault\In\

Content packages:

C:\M-Files Content Packages\Sample Vault\In\<vault>_<timestamp>\In

C:\M-Files Content Packages\Sample Vault\In\<vault>_<timestamp>*.

☑ Use replication via cloud storage

Connection string:

User-specified folder name:

User-specified password for encryption:

Please note that there is no guarantee that the data remains in the cloud storage for more than one week.

☐ Delete content package after importing

Configuration ID:

7. 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.

8. 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** or **Request**. The functionality is different in different M-Files environments.

Option	Description
Get	The connection string is automatically filled.

Option	Description
Request	An email message to M-Files customer support is opened. Remove unwanted locations from the line **Preferred location** and send the email.

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.

9. Optional: Select **Delete content package after importing** if you want the content package to be removed after the operation has been completed.

Use this option only if you import the content package to one vault. Otherwise, the content package is deleted before it is imported to all the vaults.

10. Optional: In the **Configuration ID** field, you can enter any string of characters for identifying this replication job.

M-Files automatically creates a numeric ID for each scheduled replication job. You can enter an additional ID for the job to the **Configuration ID** field. The configuration ID can be any string of characters. If a configuration ID cannot be found when the jobs are processed, M-Files uses the job ID.

11. On the **Objects and Files** tab, you can specify how objects and files are imported.

For more information, see Import Objects and Files.

12. On the **Structure** tab, you can specify how metadata structure is imported.

For more information, see Import Structure.

13. On the **Permissions** tab, you can specify the permission settings for the imported objects.

For more information, see Permissions (Importing Content).

14. 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 should be reviewed carefully before proceeding with the import operation.

In this chapter

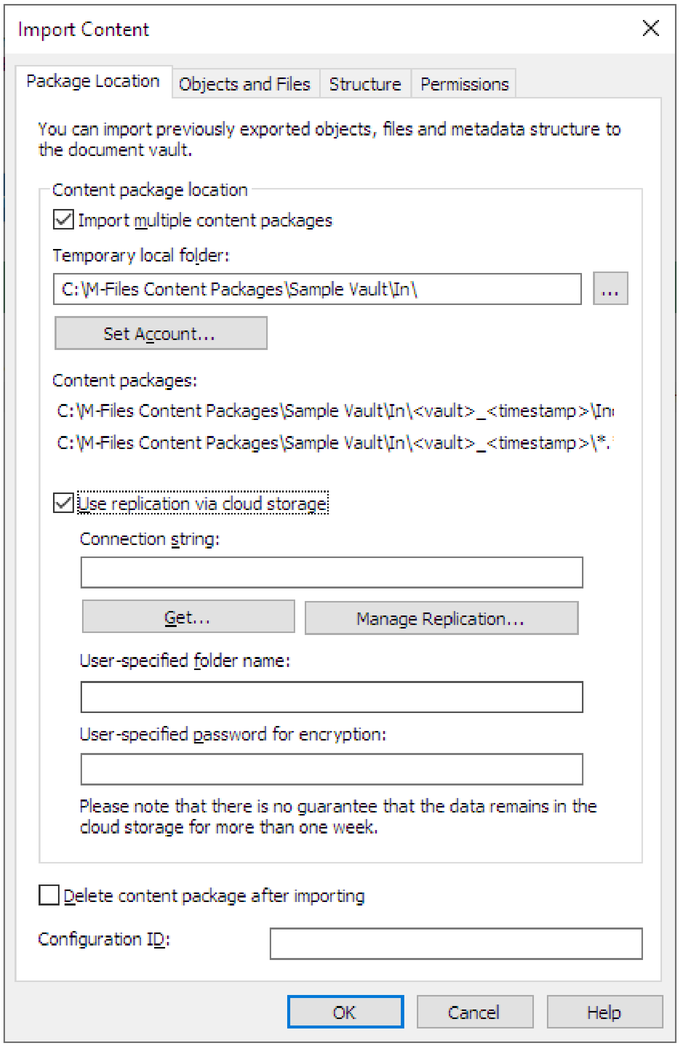
- Import Package Location
- Import Objects and Files
- Import Structure
- Permissions (Importing Content)
- Import Summary Report

Import Package Location

The **Package Location** tab displays options related to the package containing the objects, files, and metadata structure to be imported. See the corresponding settings in Exporting Content 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 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.



Import Content

Package Location | Objects and Files | Structure | Permissions

You can import previously exported objects, files and metadata structure to the document vault.

Content package location

☑ Import multiple content packages

Temporary local folder: C:\M-Files Content Packages\Sample Vault\In\

Content packages:
C:\M-Files Content Packages\Sample Vault\In\<vault>_<timestamp>\In
C:\M-Files Content Packages\Sample Vault\In\<vault>_<timestamp>*.

☑ Use replication via cloud storage

Connection string:

User-specified folder name:

User-specified password for encryption:

Please note that there is no guarantee that the data remains in the cloud storage for more than one week.

☐ Delete content package after importing

Configuration ID:

Figure 35: 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** check box. 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 this option only if you import the content package to one vault. Otherwise, the content package is deleted before it is imported to all the vaults.

M-Files automatically creates a numeric ID for each scheduled replication job. You can enter an additional ID for the job to the **Configuration ID** field. The configuration ID can be any string of characters. If a configuration ID cannot be found when the jobs are processed, M-Files uses the job ID.

Use replication via cloud storage

You can also use replication through 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).

Manage Replication

Click **Manage Replication...** to open a dialog listing the queued import packages. This allows you to easily remove any erroneous packages that may be blocking the queue.

User-specified folder name

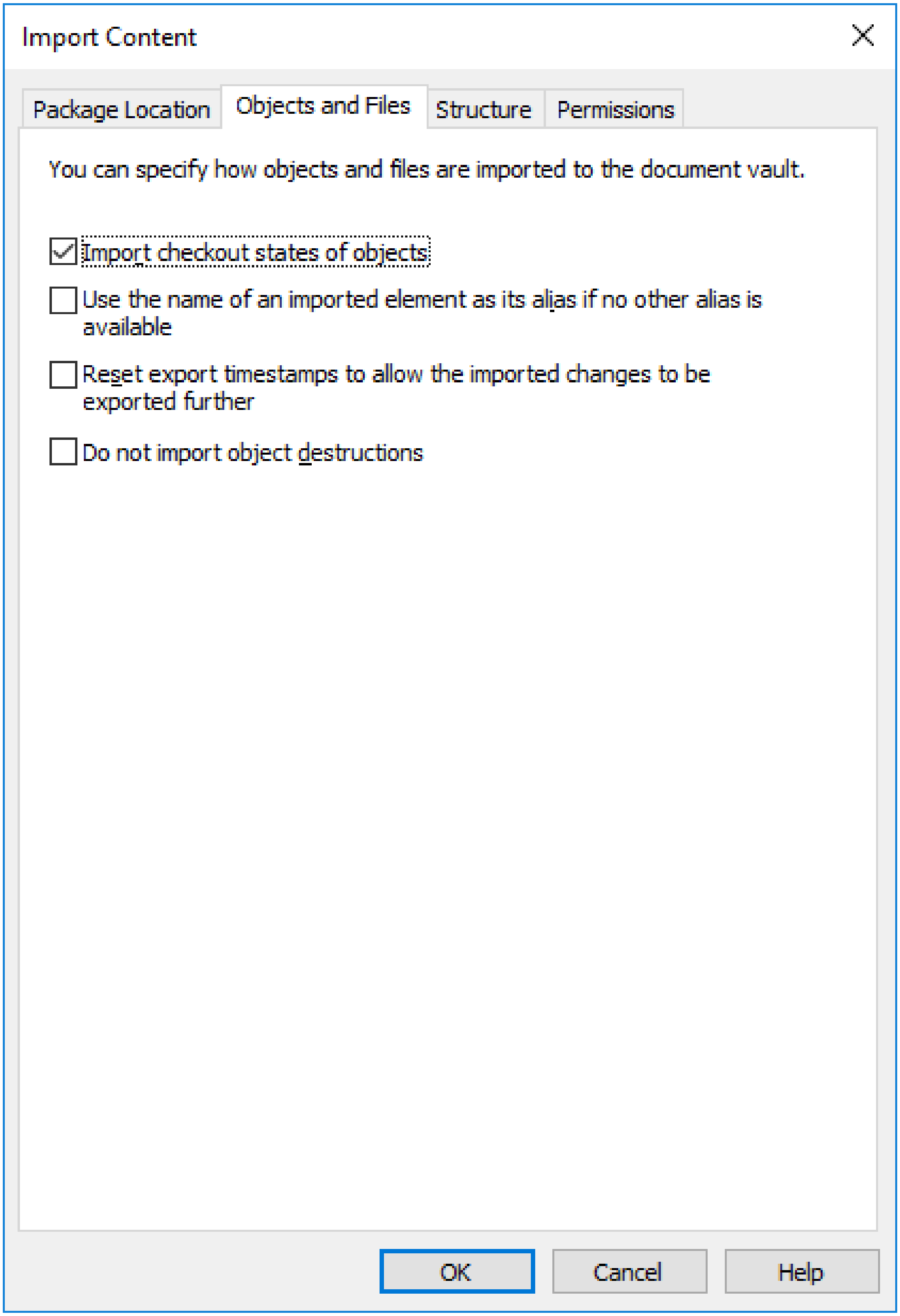
The folder name is unique for one export-import pair. For instance, replication from the master vault to a secondary vault could be named `MasterOut` and replication from the secondary vault to the master vault `MasterIn`.

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.

Import Objects and Files

The **Objects and Files** tab enables you to change settings related to importing object and file content.



You can specify how objects and files are imported to the document vault.

☑ Import checkout states of objects

□ Use the name of an imported element as its alias if no other alias is available

□ Reset export timestamps to allow the imported changes to be exported further

□ Do not import object destructions

Figure 36: The **Objects and Files** tab of the **Import Content** dialog.

Import checkout 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 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.

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

On the **Structure** tab, you can see which features are set to be disabled in the imported structure. By default, external connections and new and changed scripts are disabled. To clear these selections, you must have the system administrator permissions.

New and changed scripts to disable

In a shared M-Files Cloud environment, users with the **Full control of vault** administrative rights can change the import behavior of the new and changed scripts that are set to be disabled. By default, the selected scripts are disabled only if they are unsigned. Unsigned scripts have not been validated by M-Files. In **New and changed scripts to disable**, select **Always disable** to set all the new and changed scripts to be disabled, including signed scripts.

Views

In one-time import, the setting **Import views with an older last modified date and time** is available. Enable this setting to import views whose corresponding view in the target vault has been modified later than the view in the import package.

When you click **OK**, M-Files creates a report that shows all the changes 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 a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click **Content Replication and Archiving**.

   ✓ The content replication and archiving features are displayed in the right-side pane.
6. Either:

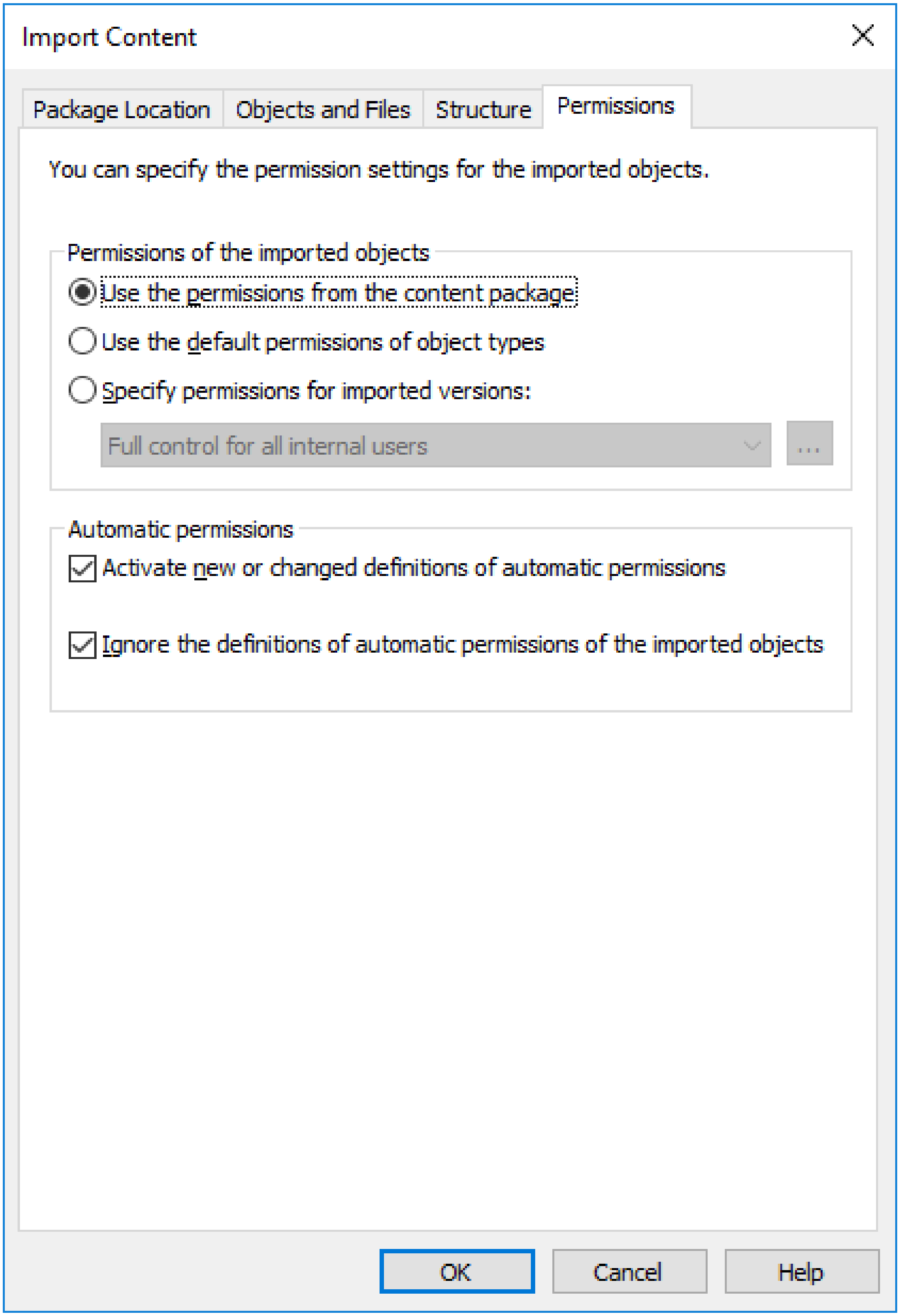
   a. Click **One-time Import...** if you want to modify the permissions of a single import package.

      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.
7. Select the **Permissions** tab.

   ✓ The **Permissions** tab of either the **Import Content** or the **Scheduled Job Properties** dialog is opened.



You can specify the permission settings for the imported objects.

Permissions of the imported objects

● Use the permissions from the content package

○ Use the default permissions of object types

○ Specify permissions for imported versions:

Full control for all internal users

Automatic permissions

☑ Activate new or changed definitions of automatic permissions

☑ Ignore the definitions of automatic permissions of the imported objects

8. 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 to have the imported objects use the default permissions specified in the properties dialog 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.

9. Optional: Check or uncheck the **Activate new or changed definitions of automatic permissions** option checkbox.

   ⓘ 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.

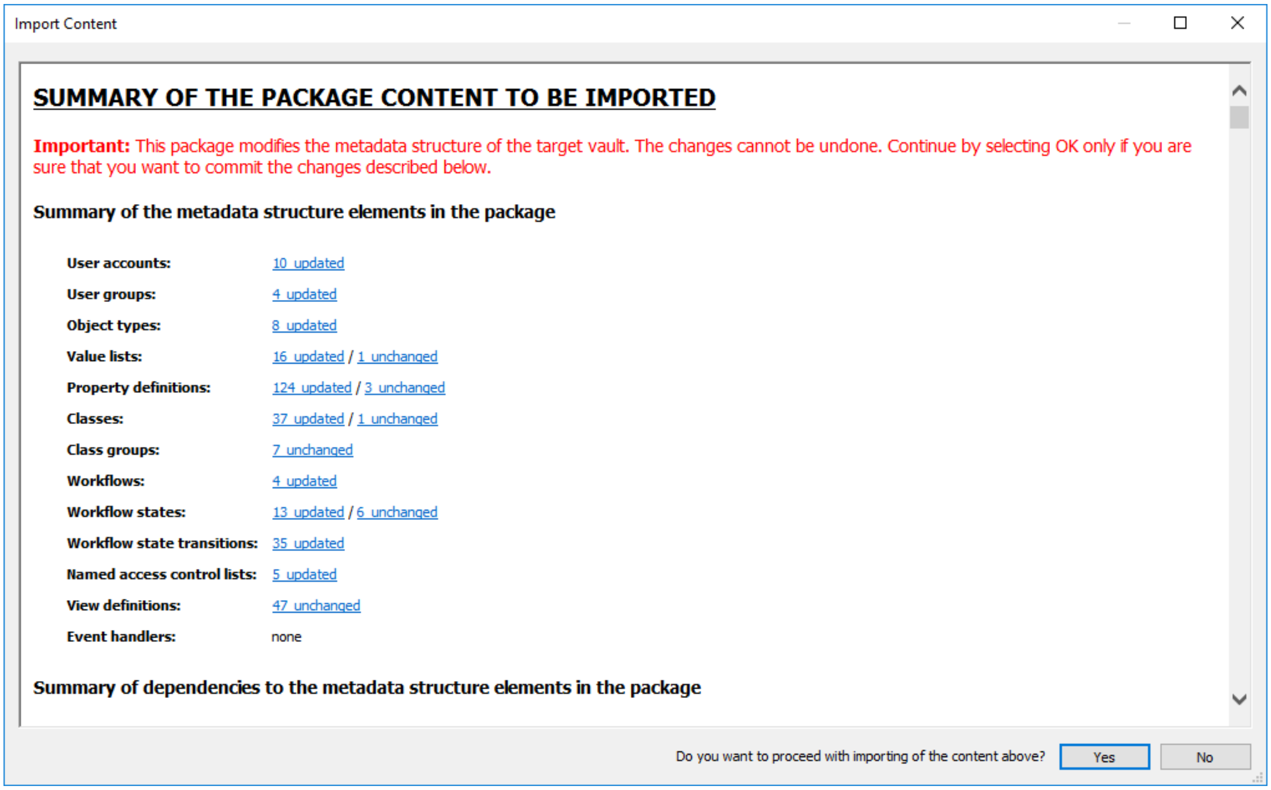
10. Optional: Check or uncheck the **Ignore the definitions of automatic permissions of the imported objects** option checkbox.

    ⓘ 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.

11. 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.



SUMMARY OF THE PACKAGE CONTENT TO BE IMPORTED

Important: This package modifies the metadata structure of the target vault. The changes cannot be undone. Continue by selecting OK only if you are sure that you want to commit the changes described below.

Summary of the metadata structure elements in the package

User accounts:	10 updated
User groups:	4 updated
Object types:	8 updated
Value lists:	16 updated / 1 unchanged
Property definitions:	124 updated / 3 unchanged
Classes:	37 updated / 1 unchanged
Class groups:	7 unchanged
Workflows:	4 updated
Workflow states:	13 updated / 6 unchanged
Workflow state transitions:	35 updated
Named access control lists:	5 updated
View definitions:	47 unchanged
Event handlers:	none

Summary of dependencies to the metadata structure elements in the package

Do you want to proceed with importing of the content above?

Figure 37: 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.

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 before defining any export or import jobs.

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. 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.

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 Vaults.

In this chapter

- Defining a Scheduled Export
- Defining a Scheduled Import

Defining a Scheduled Export

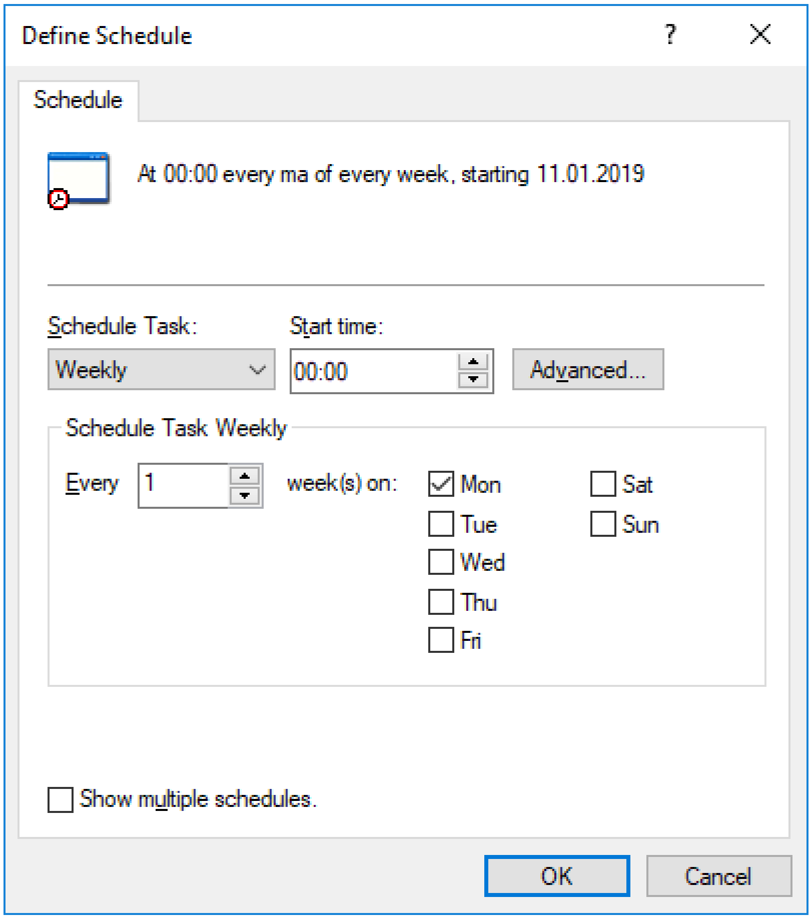
1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Content Replication and Archiving**.

   ✓ The content replication and archiving features are displayed in the right-side pane.
6. In the task area, click **New Scheduled Export**.

   ✓ The **Scheduled Job Properties** dialog is opened.
7. In the **Description** field, type in a name for the scheduled export job.
8. To define a schedule for this task:

   a) Click **Schedule**.

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



Define Schedule

Schedule

At 00:00 every ma of every week, starting 11.01.2019

Schedule Task: Weekly

Start time: 00:00

Schedule Task Weekly

Every 1 week(s) on:

☑ Mon
☐ Tue
☐ Wed
☐ Thu
☐ Fri
☐ Sat
☐ Sun

☐ Show multiple schedules.

b) Specify the schedule with the available options.

The schedule option **When idle** is not supported in M-Files.

c) Click **OK** to close the **Define Schedule** dialog.

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.

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.

If you do not yet have the connection string, click **Get** or **Request**. The functionality is different in different M-Files environments.

Option	Description
Get	The connection string is automatically filled.
Request	An email message to M-Files customer support is opened. Remove unwanted locations from the line **Preferred location** and send the email.

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. Optional: In the **Configuration ID** field, you can enter any string of characters for identifying this replication job.

M-Files automatically creates a numeric ID for each scheduled replication job. You can enter an additional ID for the job to the **Configuration ID** field. The configuration ID can be any string of characters. If a configuration ID cannot be found when the jobs are processed, M-Files uses the job ID.

12. On the **Objects and Files** tab, select **Export objects and files** and **Export existing objects**.

For more information about the options on this tab, see Export Objects and Files.

Note:

When the **Export only changes since latest run** option is enabled, only new objects and content that has versioning or non-versioning changes since the given date and time are exported. If you export also metadata structure elements, the elements are not exported unless there are changes to files or objects.

If you want to export metadata structure elements regardless of whether objects or files have been changed, do one of these operations:

- Export the metadata structure separately.
- Disable the **Export only changes since latest run** option. However, if you do not limit the scope of the export in any way, it can take a considerable amount of time to complete the export job.

13. Optional: To define the conditions that objects must meet to be exported, select **Use a search filter** and click the **Define** button.

a) In the **Define Filter** dialog, define the conditions that objects must meet to be exported and click **OK** once you have defined all the necessary conditions.

14. 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.

15. 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 a connection to M-Files server.

3. Expand **Document Vaults**.
4. Expand a vault.
5. Click **Content Replication and Archiving**.

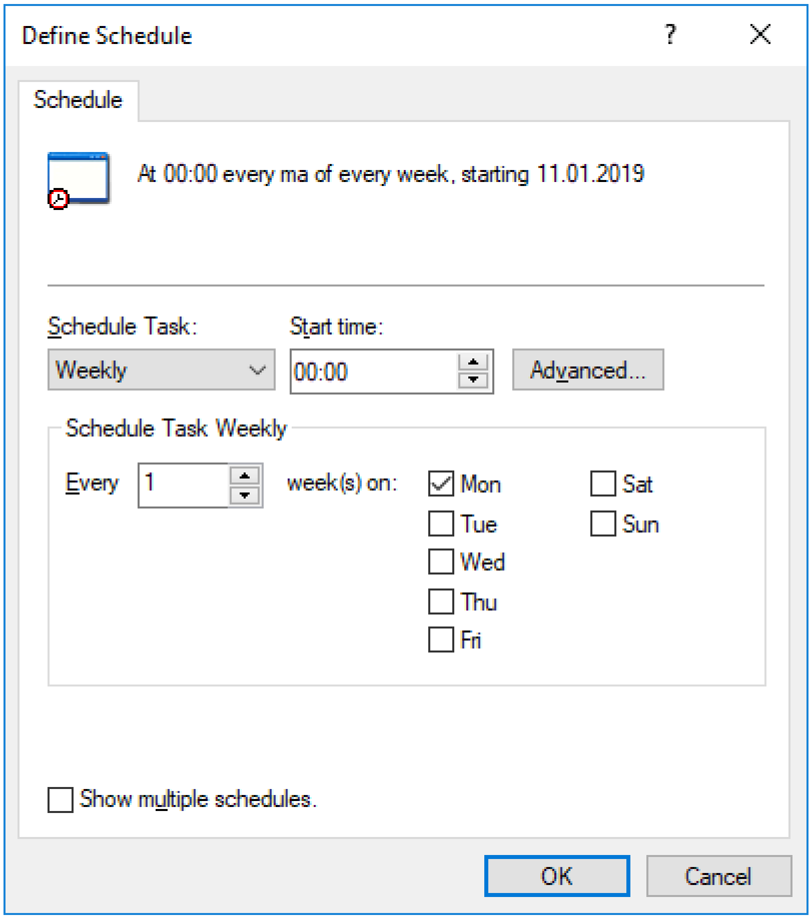
   ✓ The content replication and archiving features are displayed in the right-side pane.

6. In the task area, click **New Scheduled Import**.

   ✓ The **Scheduled Job Properties** dialog is opened.

7. In the **Description** field, type in a name for the scheduled import job.
8. To define a schedule for this task:
   a) Click **Schedule**.

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



At 00:00 every ma of every week, starting 11.01.2019

Schedule Task: Weekly

Start time: 00:00

Schedule Task Weekly

Every 1 week(s) on:

☑ Mon
☐ Tue
☐ Wed
☐ Thu
☐ Fri
☐ Sat
☐ Sun

☐ Show multiple schedules.

   b) Specify the schedule with the available options.

   ℹ The schedule option **When idle** is not supported in M-Files.

   c) Click **OK** to close the **Define Schedule** dialog.

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.

ℹ 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.

ℹ If you do not yet have the connection string, click **Get** or **Request**. The functionality is different in different M-Files environments.

Option	Description
Get	The connection string is automatically filled.
Request	An email message to M-Files customer support is opened. Remove unwanted locations from the line **Preferred location** and send the email.

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. Optional: Select **Delete content package after importing** if you want the content package to be removed after the operation has been completed.

Use this option only if you import the content package to one vault. Otherwise, the content package is deleted before it is imported to all the vaults.

12. Optional: In the **Configuration ID** field, you can enter any string of characters for identifying this replication job.

M-Files automatically creates a numeric ID for each scheduled replication job. You can enter an additional ID for the job to the **Configuration ID** field. The configuration ID can be any string of characters. If a configuration ID cannot be found when the jobs are processed, M-Files uses the job ID.

13. On the **Objects and Files** tab, you can specify how objects and files are imported.

ℹ For more information, see Import Objects and Files.

14. On the **Structure** tab, you can specify how metadata structure is imported.

ℹ For more information, see Import Structure.

15. On the **Permissions** tab, you can specify the permission settings for the imported objects.

ℹ For more information, see Permissions (Importing Content).

16. 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

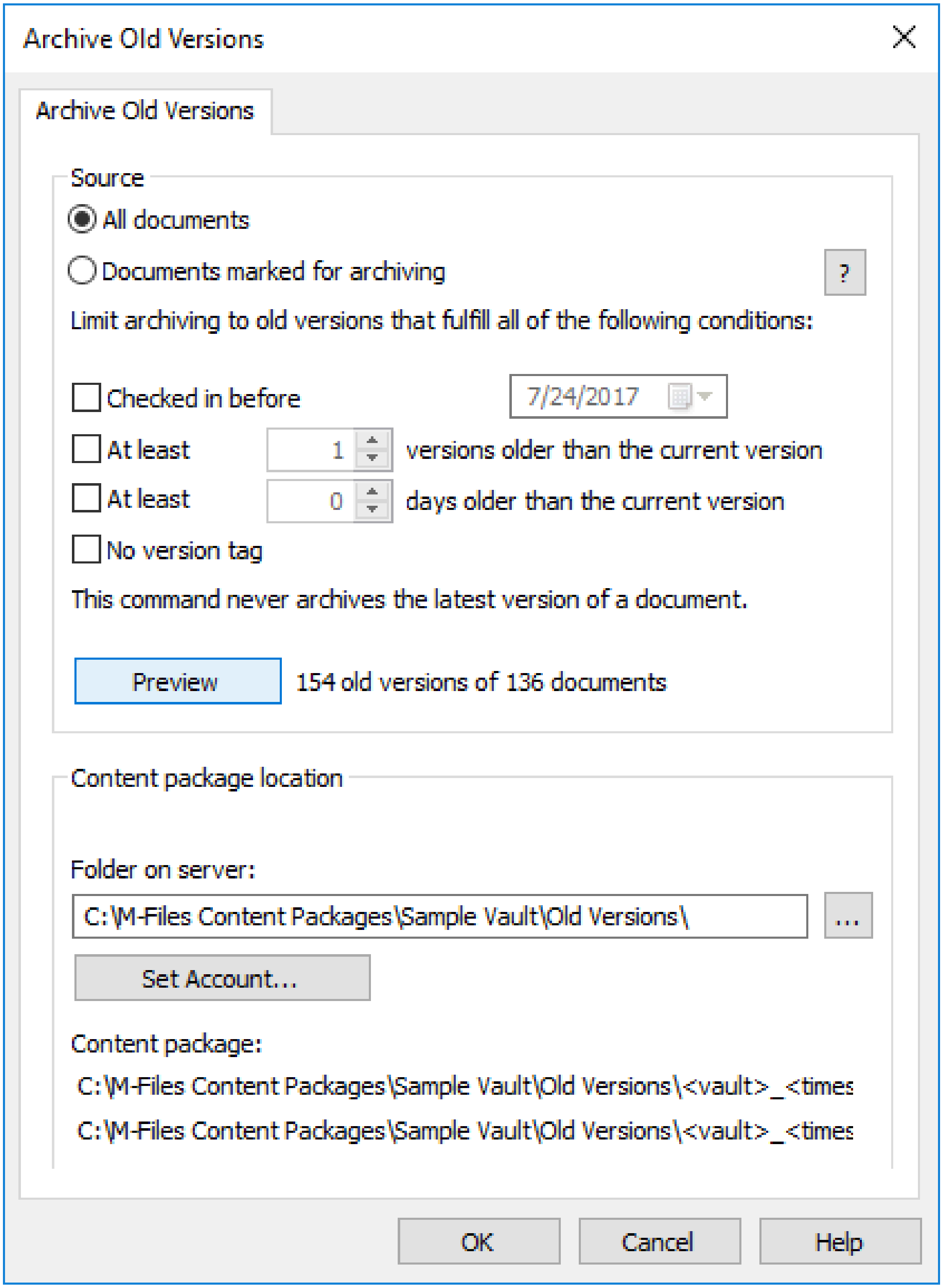
You can archive old versions of documents that you no longer need. When you archive old versions of documents, the selected document versions are transferred from the document vault to the archive file.

Do the following steps to archive old versions of documents:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click **Content Replication and Archiving**.
6. In the menu bar, click **Action** > **Archive Old Versions**.

   ℹ You can also right-click an empty area in the **Scheduled Export and Import** list and select **Archive Old Versions**.

   ☑ The **Archive Old Versions** dialog is opened.



Archive Old Versions

Archive Old Versions

Source

● All documents

○ Documents marked for archiving

Limit archiving to old versions that fulfill all of the following conditions:

□ Checked in before 7/24/2017

□ At least 1 versions older than the current version

□ At least 0 days older than the current version

□ No version tag

This command never archives the latest version of a document.

Preview 154 old versions of 136 documents

Content package location

Folder on server:

C:\M-Files Content Packages\Sample Vault\Old Versions\

Set Account...

Content package:

C:\M-Files Content Packages\Sample Vault\Old Versions\<vault>_<times

C:\M-Files Content Packages\Sample Vault\Old Versions\<vault>_<times

7. 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.

> **Tip:** You can mark a document for archiving in the classic M-Files Desktop. For instructions, see Archiving Content.

8. Select the conditions (you can select all that apply) for limiting the number of old versions to be archived:

> 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.
No version tag	Select this option to exclude versions that have a version label from the archive.

9. In the **Content package location** section, click the **...** button to select the location to save the archive.

10. Optional: Click **Set Account...** to run the task with another account than the Local System account. If the file location is on a network drive that the Local System account cannot get access to, you must set another account. On the **Set Account** dialog:

a) Select **This account**.
b) In **This account**, enter the name of the user account.
c) In **Password** and **Confirm password**, enter the password of the user account.
d) Click **OK** to close the **Set Account** dialog.

11. 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 specified.

You can restore the archived content to the vault with Content Replication and Archiving.

> **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.

Vault Event Log

The vault event log records vault events. For example, object creations and user logins. When the event log is enabled, you can monitor the vault events and use filter criteria or sort order to show only events that you are interested in. For more information, see Configuring the Vault Event Log and Using the Vault Event Log.

Note: The event log must be enabled for notifications to be sent. For information about notifications, see Editing Notification Settings in M-Files Admin.

These components specify what event types are recorded:

- The **Event types to include** setting
- The Electronic Signatures and Advanced Logging module that adds event types to the event log and lets you enable these event log features:
  - User Action Log
  - Advanced Event Log features

For a list of all event types, see Event Types.

The Electronic Signatures and Advanced Logging module

Some event types are only recorded if you have purchased and activated the Electronic Signatures and Advanced Logging module. For a list of these event types, see Event Types. This module also lets you use User Action Log, Advanced Event Log features, and electronic signatures.

To activate the Electronic Signatures and Advanced Logging module, see Activation.

Event logging and virus scanning exclusions

The event log can sometimes show an unexpectedly large number of file downloads during a short time period. If this occurs, it can be useful to make sure that the necessary virus scanning exclusions are in place. See M-Files and Virus Scanning for instructions.

In this chapter

- Event Types
- Configuring the Vault Event Log
- Using the Vault Event Log
- User Action Log

Event Types

The table on this page contains the standard event types and shows which event types are only part of the Electronic Signatures and Advanced Logging module. See the event types that User Action Log adds to the event log in Event types with User Action Log.

You can use the arrowheads in the table headers to sort the information and the search field to filter the table content.

Event type name	Standard event type	Included with Electronic Signatures and Advanced Logging
Backup started	✔	✔
Backup completed	✔	✔
Check-in	✔	✔
Check-out	✔	✔

Event type name	Standard event type	Included with Electronic Signatures and Advanced Logging
Check-in request	✔	✔
Conflict resolved	✔	✔
Conflict object restored as a new version	✔	✔
Conflicting changes discarded	✔	✔
Custom event	✔	✔
Document or other object changed	✔	✔
Document or other object deleted	✔	✔
Document or other object destroyed	✔	✔
Document vault created	✔	✔
Document vault created as a copy of another vault	✔	✔
Event log cleared	✔	✔
Event log exported	✔	✔
Event logging disabled	✔	✔
Event logging enabled	✔	✔
File downloaded	✔	✔
File downloaded via public link	✔	✔
Free-form request	✔	✔
Login	✔	✔
Logout	✔	✔
New document or other object	✔	✔
Object undeleted	✔	✔
One version of a document or other object destroyed	✔	✔
Operation denied (incompatible license)	✔	✔
Public link accessed	✔	✔
Public link created	✔	✔
Public link deleted	✔	✔
Restoration from backup completed	✔	✔
Rollback	✔	✔

Event type name	Standard event type	Included with Electronic Signatures and Advanced Logging
The state of a document or other object changed	✔	✔
Undo checkout	✔	✔
User group created	✔	✔
User group deleted	✔	✔
User group modified	✔	✔
User group member added	✔	✔
User group member removed	✔	✔
User created	✔	✔
User deleted	✔	✔
User modified	✔	✔
Vault settings modified	✔	✔
Vault variable modified	✔	✔
Application installed	✘	✔
Application disabled	✘	✔
Application enabled	✘	✔
Application uninstalled	✘	✔
Application license changed	✘	✔
Class created	✘	✔
Class changed	✘	✔
Class deleted	✘	✔
Common view created	✘	✔
Common view changed	✘	✔
Common view deleted	✘	✔
Content package exported	✘	✔
Content package import started	✘	✔
Content package import completed	✘	✔
Event handler created	✘	✔
Event handler changed	✘	✔
Event handler deleted	✘	✔
Event handler index changed	✘	✔
Named ACL created	✘	✔

Event type name	Standard event type	Included with Electronic Signatures and Advanced Logging
Named ACL changed	✘	✔
Named ACL deleted	✘	✔
Object type created	✘	✔
Object type changed	✘	✔
Object type deleted	✘	✔
Property definition created	✘	✔
Property definition changed	✘	✔
Property definition deleted	✘	✔
State created	✘	✔
State changed	✘	✔
State deleted	✘	✔
State transition created	✘	✔
State transition changed	✘	✔
State transition deleted	✘	✔
Value list created	✘	✔
Value list changed	✘	✔
Value list deleted	✘	✔
Value list item created	✘	✔
Value list item changed	✘	✔
Value list item deleted	✘	✔
Value list item undeleted	✘	✔
Workflow created	✘	✔
Workflow changed	✘	✔
Workflow deleted	✘	✔

Configuring the Vault Event Log

1. In M-Files Admin, go to the **Advanced Vault Settings** section.

a) Open M-Files Admin.
b) In the left-side tree view, expand an M-Files server connection.
c) Expand **Document Vaults**.
d) Expand a vault.
e) Click **Configurations**.
f) In the navigation area, click **Advanced Vault Settings**.
g) Open the **Configuration** tab.

✓ The advanced vault settings are shown.

2. Expand **Event Log**.
3. Specify the settings.

   See the information in the table. For more information, select a setting and see the **Info** tab.

   Note: When the Advanced Event Log feature is enabled in Vault Properties, the configurations under **Advanced Event Log** are used. When the feature is not enabled, the configurations under **Event Log** are used.

Setting name	Description
Advanced Event Log > **Exclude ACL Change Events Done by M-Files Server**	This setting specifies whether the log includes events that are related to changed ACL permissions and done by M-Files Server.
Event Log > **Enabled**	This setting specifies whether events are recorded in the vault event log. **Note:** You cannot disable the event log with this setting if Advanced Event Log features are enabled. **Note:** The event log must be enabled for notifications to be sent. For information about notifications, see Editing Notification Settings in M-Files Admin.
Event Log > **Event Types to Include**	Settings in this section specify which event types are included in the vault event log. The event types that are set to **No**, are not recorded and thus not included in event log exports. **Warning:** Specific event types are necessary for other M-Files functions to operate correctly. Do not disable event types if you do not know the effects. **Note:** If Advanced Event Log features are enabled, these settings have no effect. Instead, all the event types are recorded.
Event Log > **Maximum Number of Events**	M-Files Server removes the oldest events when the number of events is close to the value specified here unless the Electronic Signatures and Advanced Logging module and Advanced Event Log features are in use. By default, the maximum number of events is 10,000.
Maximum Size of Event Log Data to Retrieve	Specifies, in kilobytes, the maximum data size for getting event log data. If the request exceeds the maximum data size, M-Files Server doesn't return any event log data.

Setting name	Description
User Action Log	This section contains settings related to User Action Log. To use this feature, the Electronic Signatures and Advanced Logging module must be active on the M-Files server. Set **Enabled** to **Yes** and specify the settings in **Event Settings** as necessary to take User Action Log into use.

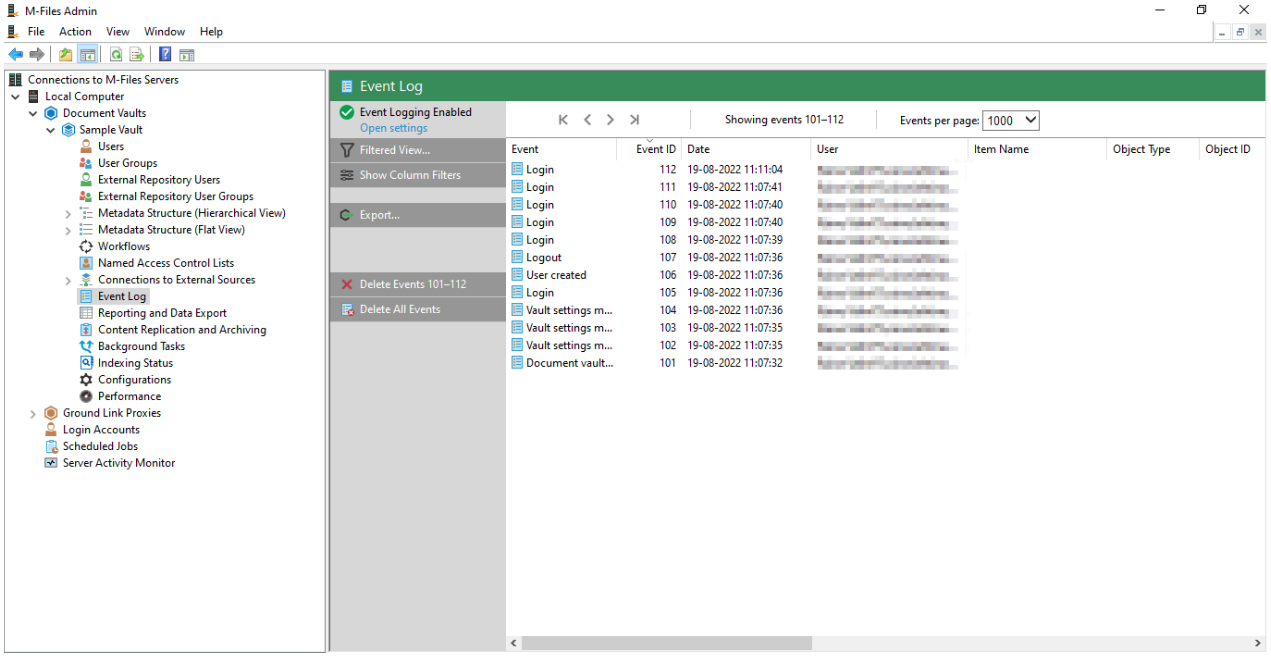
4. Click **Save**.

Your changes are saved. If you enabled User Action Log, M-Files starts to record the events for the vault users that have logged out and logged back in. To log out all vault users, restart the vault. However, taking a vault offline must always be done in a controlled manner and the vault users must be notified beforehand.

Using the Vault Event Log

This section tells you what functions are available in the vault event log and how to use them. To open the event log, in M-Files Admin, go to a vault, and select **Event Log**.

Click on different parts of the screenshot below for a description of the areas in the user interface.



Showing events 101–112

Events per page: 1000

Event	Event ID	Date	User	Item Name	Object Type	Object ID
Login	112	19-08-2022 11:11:04	[redacted]			
Login	111	19-08-2022 11:07:41	[redacted]			
Login	110	19-08-2022 11:07:40	[redacted]			
Login	109	19-08-2022 11:07:40	[redacted]			
Login	108	19-08-2022 11:07:39	[redacted]			
Logout	107	19-08-2022 11:07:36	[redacted]			
User created	106	19-08-2022 11:07:36	[redacted]			
Login	105	19-08-2022 11:07:36	[redacted]			
Vault settings m...	104	19-08-2022 11:07:36	[redacted]			
Vault settings m...	103	19-08-2022 11:07:35	[redacted]			
Vault settings m...	102	19-08-2022 11:07:35	[redacted]			
Document vault...	101	19-08-2022 11:07:32	[redacted]			

1. Task area
2. Top pane
3. List of events
4. Vault event log

Task area

At the top of the task area, you can see the status of the vault event log.

- **Event logging enabled**: The standard event types are recorded.

- **Advanced event logging**: The Electronic Signatures and Advanced Logging module is active.
- **Partial event logging**: Some event types are not recorded because they are disabled in **Event Types to Include**.
- **Event logging disabled**: No event types are recorded.

Click...	To...
Open Settings	Go to the **Event Log** settings in the **Advanced Vault Settings** section in M-Files Admin. Do this to check which event types are included in the event log.
Filtered View	Specify filter criteria or select a filtered view to show only specific events. You can filter the events, for example, by object type, event type, user, or time range. You can save frequently used filter criteria to **My Filtered Views**. This is useful if you often use the same criteria when you examine the vault event log. To do this, enter filter criteria and click **Save as**. Enter a name for the filtered view, select whether you want to use it as the default view, and click **Save**. To use a filtered view, click **My Filtered Views**, select a filtered view from the list, and click **Apply** > **Close**. In the **Filtered View** dialog, click **OK**. In **My Filtered Views**, select a view and click **Use as Default View** to set a filtered view to be applied by default when you open the vault event log.
Show Column Filters **Disable Column Filters**	Show or disable column filters. With the column filters, you can enter filter text for a column to show only specific events.
Export	Export and archive all or selected events in the XML format. For more information on archiving, see Archiving M-Files Event Logs. After the export, you can select to delete the exported events from the event log.
Delete Event IDs X–XXXX	Delete the events on the opened page. If you have filtered the events, also events that are not shown are deleted. In the confirmation dialog, you can select to export the events before they are deleted.
Delete All Events	Delete all events. In the confirmation dialog, you can select to export the events before they are deleted.

Top pane

Here you can see which event IDs are shown and change the page and the number of events shown on one page.

List of events

To see more information about an event, double-click it to open the **Event Details** dialog.

Note: Some event details are available only if have the Electronic Signatures and Advanced Logging module is active on the M-Files server.

User Action Log

The User action log feature gives more visibility to the actions that M-Files users do in a vault. User action log adds event types listed in the table below into the vault event log. To enable the feature, see Configuring the Vault Event Log.

Important remarks

- To use this feature, the Electronic Signatures and Advanced Logging module must be active on the M-Files server.
- Actions done in M-Files Mobile or M-Files API based custom clients are not recorded.
- Actions done in offline mode are not recorded.
- Using this feature considerably increases the size of the vault log.
- For compliance reasons, User action log also records global search events.

Event types with User Action Log

Event type	Description
Collection Members dialog opened	An event of this type is recorded when the **Collection Members** dialog is opened. The entry contains these details: • The name and ID of the user who opened the dialog • The timestamp of the event • The name and ID of the object This event is only recorded in the classic M-Files Desktop.
Column added	An event of this type is recorded when a column is added to a listing. The entry contains these details: • The name and ID of the user who performed the modification • The timestamp of the event • The column that was added
Column removed	An event of this type is recorded when a column is removed from a listing. The entry contains these details: • The name and ID of the user who performed the modification • The timestamp of the event • The column that was removed

Event type	Description
Column settings modified	An event of this type is recorded when columns are added or removed in the **Choose Columns** dialog. The entry contains these details: • The name and ID of the user who performed the modification • The timestamp of the event • The columns that are visible to the user after the modification This event is only recorded in the classic M-Files Desktop.
Data exported	An event of this type is recorded when data is exported from the vault. The entry contains these details: • The name and ID of the user who did the export operation • The timestamp of the event • The export settings and the number of exported objects • The name and ID of the exported objects • This behavior must be enabled in Advanced Vault Settings.
File opened	An event of this type is recorded when a file is opened. The entry contains these details: • The name and ID of the user who opened the file • The timestamp of the event • The name and ID of the object
File opened for document comparison	An event of this type is recorded when a user compares document content in the classic M-Files Desktop. The entry contains these details: • The name and ID of the user who compared document content • The timestamp of the event • The name and ID of the compared document This event is only recorded in the classic M-Files Desktop.

Event type	Description
Metadata card opened	An event of this type is recorded when the metadata card is shown in the right pane or in a new window for an object. The entry contains these details: • The name and ID of the user who opened the metadata card • The timestamp of the event • The property IDs, name, and ID of the object The property IDs are shown only if you have enabled this behavior with the feature settings.
Object copied to clipboard	An event of this type is recorded when an object is copied to the Windows clipboard. The entry contains these details: • The name and ID of the user who copied the object • The timestamp of the event • The name and ID of the object If multiple objects are copied, all items are separately logged. This event is only recorded in the classic M-Files Desktop.
Object dragged from M-Files	An event of this type is recorded when an object is dragged and dropped from M-Files. The entry contains these details: • The name and ID of the user who exported the object • The timestamp of the event • The name and ID of the object If multiple objects are exported, all items are logged.
Object history opened	An event of this type is recorded when the **History** dialog is opened. The entry contains these details: • The name and ID of the user who opened the dialog • The timestamp of the event • The name and ID of the object
Object listing invoked	An event of this type is recorded when a search is done in M-Files. The entry contains these details: • The name and ID of the user who invoked the listing • The timestamp of the event • The search terms and search criteria

Event type	**Description**
Object listing requested from server	An event of this type is recorded when a search is done M-Files. The entry contains these details: • The name and ID of the user who requested the listing • The timestamp of the event • The search terms and search criteria For M-Files to start recording events of this type, you must restart the vault after enabling the feature.
Object relationships opened	An event of this type is recorded when the relationships of an object are browsed in the listing area. The entry contains these details: • The name and ID of the user who browsed the relationships • The timestamp of the event • The name and ID of the object
Object or objects marked to be available offline	An event of this type is recorded when M-Files is used to mark an object to be available in the offline mode. The entry contains these details: • The name and ID of the user who marked the object to be available offline • The timestamp of the event • The name and ID of the object This event is only recorded in the classic M-Files Desktop.
Preview tab opened	An event of this type is recorded when the preview tab is displayed for a document or a non-document object containing one or more files. The entry contains these details: • The name and ID of the user who opened the preview pane • The timestamp of the event • The name and ID of the document (or, alternatively, the name of the file and the name and ID of the object containing the file)

Event type	Description
Relationships dialog opened	An event of this type is recorded when the **Relationship** dialog is opened. The entry contains these details: • The name and ID of the user who opened the dialog • The timestamp of the event • The name and ID of the object This event is only recorded in the classic M-Files Desktop.
Search initiated	An event of this type is recorded when a search is done in a vault or with global search. The entry contains these details: • The name and ID of the user who performed the search • The search terms • The timestamp of the event • The columns shown in the listing area
View or folder marked to be available offline	An event of this type is recorded when the M-Files is used to mark a view or folder to be available in offline mode. The entry contains these details: • The name and ID of the user who marked the view or grouping level to be available offline • The timestamp of the event • The name and ID of the object This event is only recorded in the classic M-Files Desktop.
View or folder opened	An event of this type is recorded when a view or grouping level is opened. The entry contains these details: • The name and ID of the user who opened the view or grouping level • The timestamp of the event • The name and ID of the object • The columns shown in the listing area

Scheduled Optimization

In the **Scheduled Optimization** section, you can control and monitor the scheduled automatic optimization. This can be helpful, for example, to see the the status of the optimization job or the last time that the job was run in the vault.

The **Optimize Database (Thorough)** operation tries to improve the performance of the vault database. The operation defragments indexes, updates database statistics, and compresses the full-text search index. For more information, see Optimizing the database.

To open the **Scheduled Optimization** section:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Scheduled Optimization**.

Note: The section is available in offline mode only when optimization is in progress.

Select the **Optimize Database (Thorough)** job to show these options in the task area: **Start Job**, **Stop Job**, and **Properties**.

Editing the scheduled optimization job

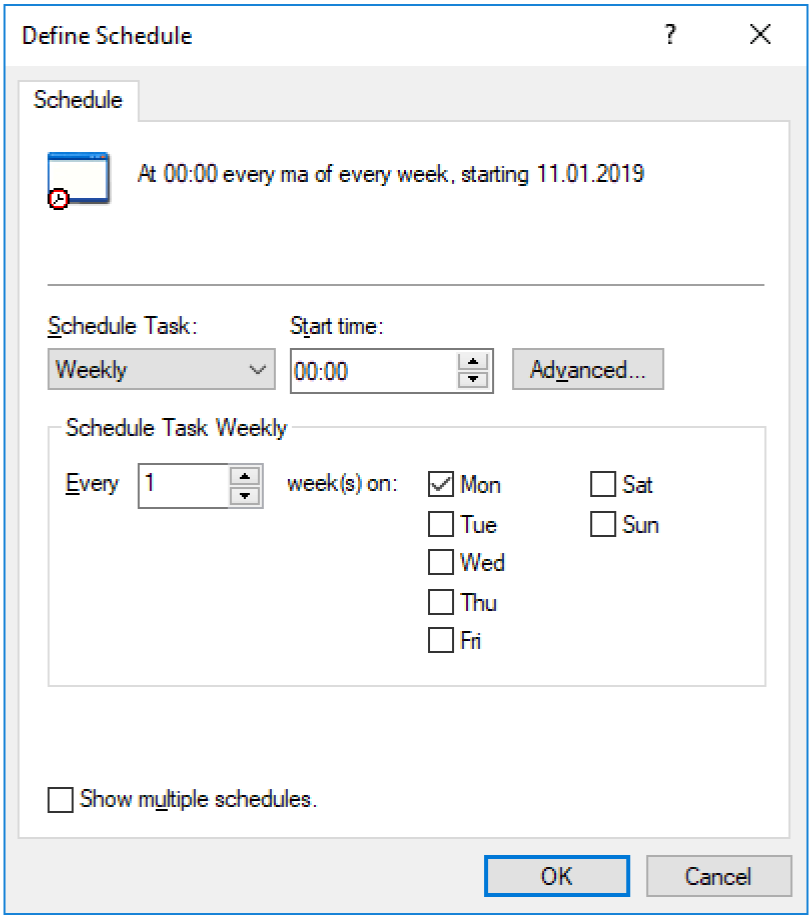
1. In the **Scheduled Optimization** section, double-click the **Optimize Database (Thorough)** job.

   ✓ The **Scheduled Job Properties** dialog is opened.

2. Optional: Edit the description.

3. Optional: To edit the schedule:
   a) Click **Schedule**.

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



At 00:00 every ma of every week, starting 11.01.2019

Schedule Task: Weekly

Start time: 00:00

Every 1 week(s) on:

☑ Mon
☐ Tue
☐ Wed
☐ Thu
☐ Fri
☐ Sat
☐ Sun

☐ Show multiple schedules.

b) Specify the schedule with the available options.

The schedule option **When idle** is not supported in M-Files.

c) Click **OK** to close the **Define Schedule** dialog.

4. Optional: In the **Automatic cancelation** section, specify a timeout for the scheduled job to improve system performance.

5. Click **OK**.

Monitoring Background Tasks

M-Files Server performs various tasks for your document vault in the background. You may monitor the progress of these operations in M-Files Admin.

Background tasks are complex and time-consuming processes that are processed in the background so that they can be executed in parallel with other M-Files Server tasks without interfering or stalling other ongoing processes.

Complete the following steps to monitor background tasks in your document vault:

1. Open M-Files Admin.

2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Select **Background Tasks**.

✓ The **Background Tasks** view is opened.

You can browse the background tasks page by page by using the arrow icons.

If the list contains a large number of items, you might want to filter it. To filter the view, open the **View** menu and click **Filter**. Enter a desired text to filter the column contents.

The background tasks that are currently in progress are listed in the **Background Tasks** view. You can click **Refresh** in the task area to refresh the view.

Managing Vault Indexing

You can use M-Files Admin to manage vault indexing. This can be helpful, for example, when you want to do one of these:

- Start the reindexing process and monitor the status of the index rebuild.
- Make sure that indexing for the vault has completed.
- See when the last object of the indexing round was processed.

The **Index Management** section in M-Files Admin divides indices into three categories: **Active Index**, **Used for Indexing**, and **Disabled**.

Index category	Description	Available operations
Active Index	• Active indices are used for searches in the vault. • dtSearch uses two active indices: metadata index and file data index. • Micro Focus IDOL and Smart Search use one active index. • Active indices are always enabled. • Active indices cannot be disabled. • Active index configurations cannot be deleted. • To set a new active index, select an index in the **Used for Indexing** category and click **Set as Active**.	• **Reindex** (Micro Focus IDOL and Smart Search only) • **Delete and Reindex**
Used for Indexing	**Used for Indexing** indices are enabled for indexing but are not active. In other words, they are not used for searches in the vault.	• **Reindex** (Micro Focus IDOL and Smart Search only) • **Delete and Reindex** • **Disable** • **Set as Active** • **Remove Configuration** (not available for default indices)

Index category	Description	Available operations
Disabled	Disabled indices are not indexed or used for searches in the vault.	- **Enable** - **Set as Active** - **Remove Configuration** (not available for default indices)

For a description of the operations, see this table.

When an index rebuild process is ongoing, a blue notification icon (◌) is shown next to the name of the index. When it is necessary to rebuild an index, a yellow notification icon (⚠) is shown.

More technical information about the feature is available in Index Management in M-Files Admin.

Viewing indexing information

To see information about the indexing status:

1. Open M-Files Admin and go to a vault.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
2. Click **Index Management**.
3. In the task area, click the name of the index.
4. On the **Status** tab, expand an indexing scenario.

   For example, **Reindexing** or **New or Modified**.

   The indexing status information is shown.

For a description of a piece of information, click the information icon (ⓘ).

Using indexing operations with index management

To use the operations in **Index Management**:

1. Select an index in the left-side navigation area.
2. In the top-right corner of the user interface, select one of the commands available for the index.

   The table given here contains a description for all available commands. The availability of the operations depends on the state of the index, the search engine that the vault uses, and your user rights.

Command	Description	Necessary access rights
Set as Active	Active indices are used for searches in the vault. With Micro Focus IDOL and Smart Search, only one index can be active at a time. With dtSearch, one metadata and one file data index are active at the same time.	System admin
Enable	Enabled indices are kept up to date with changes in the vault data. In other words, they are indexed.	System admin
Disable	Disabled indices are not kept up to date with changes in the vault data. In other words, they are not indexed.	System admin
Delete and Reindex	! **Important:** The process can take a large amount of time. With vaults that contain a million, millions, or tens of millions of documents, indexing can take days or even weeks. There are many things that have an effect on the indexing speed. For example, used indexer, hardware resources, and type of data in the vault. This operation deletes the selected index and then builds it from scratch. The operation is available for all search engines. If you use dtSearch, we recommend that you also refer to Rebuilding the dtSearch Full-Text Search Index.	System admin or vault admin

Command	Description	Necessary access rights
Reindex	! **Important:** The process can take a large amount of time. With vaults that contain a million, millions, or tens of millions of documents, indexing can take days or even weeks. There are many things that have an effect on the indexing speed. For example, used indexer, hardware resources, and type of data in the vault. This operation is available for Micro Focus IDOL and Smart Search only. Micro Focus IDOL: • Timestamps are deleted. • Objects are reindexed completely (file data and metadata) on top of the old data. • The index is not deleted. Thus, some old unnecessary content can be left in the index. • Rebuild information is written from scratch (occurs when the timestamp is zero). Smart Search: • Timestamps are deleted. • Only metadata is reindexed for the vault. External repositories are always reindexed completely (file data and metadata). • The index is not deleted. Thus, some old unnecessary content can be left in the index. • Rebuild information is written from scratch (occurs when the timestamp is zero). • If something has not been indexed correctly before, only metadata is indexed.	System admin or vault admin
Remove Configuration	This operation removes only the configuration. Index data must be deleted separately.	System admin

Measuring Vault Performance

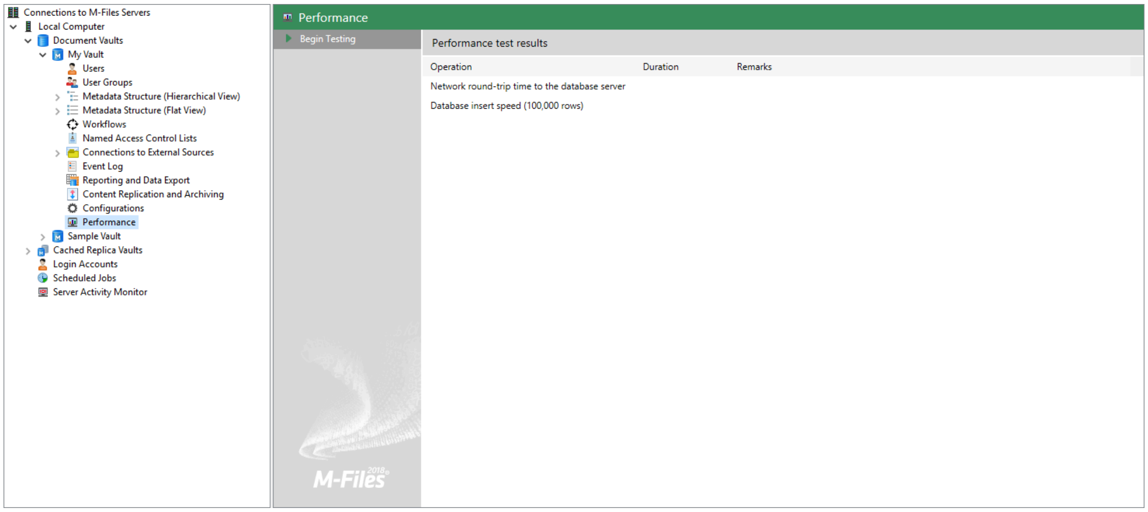
You can use M-Files Admin to measure the performance of a specific vault to detect problems or bottlenecks in the performance of the vault. The performance tests measure the network round-trip time to the database server of the vault as well as the time it takes to insert 100,000 rows into the vault database.

Do the following steps to measure vault performance:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.

5. Click **Performance**.

   ✓ The **Performance** view is opened in the right-side pane.



Performance test results

Operation	Duration	Remarks
Network round-trip time to the database server		
Database insert speed (100,000 rows)		

6. In the task area, click **Begin Testing**.

   You can stop the test at any time by clicking **Stop Testing** in 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.

> **Note:** The vault performance tests have predefined threshold times. The default threshold time for the network round-trip test is 1,500 microseconds, and for the database insert speed test, it is 6,000 milliseconds. For instructions on modifying the default threshold values, see Settings for Vault Performance Measurement.

Interaction Among Several Vaults

M-Files enables a multi-level interaction between several document vaults. The interaction enables you, for instance, to:

- 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 documents with 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, each server must have a unique server license installed. For example, if you want to replicate information between vaults on separate servers, unique server licenses must be installed for all the 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.

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.

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.

In this chapter

Associating the Metadata Definitions

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) 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*, and so on. 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 with 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 Aliases for Associating Metadata Between Vaults.
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 done with aliases.

5. You can also use the **name of imported metadata definition as its 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.
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` and `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 you want, such as `Telephone number` or `dc.PhoneNumber`, with the exception that it cannot contain both dots and spaces.

The alias is not shown to the users in the M-Files clients. 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 a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.
5. Expand **Metadata Structure (Flat View)** 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.

6. 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.

7. Go to the **Advanced** tab.
8. In the **Aliases** field, type in the name of the alias for the selected metadata definition.

   ℹ Use the same aliases for semantically equivalent metadata in both the source and the target vault.

   ℹ Use semicolons (;) to separate many aliases.

9. 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.

Synchronization of Objects and Their Values Between Vaults

This section provides further information on synchronization of objects and their values. We recommend you to read this section before you specify synchronization jobs. Synchronization is done with Content Replication and Archiving.

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 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.

Conflicts and their resolution

If users edit an object at the same time in multiple vaults, a conflict can occur during synchronization of data between vaults. For example, from source vault A to target vault B. When M-Files detects a conflict, it creates a conflict object.

If automatic conflict resolution is enabled, M-Files resolves conflicts automatically. For instructions on configuring automatic conflict resolution, refer to Configuring Automatic Resolution of Replication Conflicts in M-Files knowledge base. To restore a discarded object version, see Showing and Restoring Discarded Object Versions.

Unresolved conflicts are shown in object relationships. In the listing area, expand an object with the arrow button. If the object has unresolved conflicts, they are shown under the **Conflicts** node.

To see all conflict objects of the vault, go to the **Conflicts** view. By default, the view is hidden. For information on unhiding views, see Using the Clean View, Hide View, and Unhide Views commands.

In manual conflict resolution, you decide which object version you want to keep. To resolve a conflict, you must have editing rights to the object and the conflict object in the same vault. Right-click the conflict object and click **Resolve Conflict: Keep These Changes** to replace the local changes with the contents of the conflict object or **Resolve Conflict: Discard These Changes** to keep the local version.

If two-way synchronization (replication of contents) is used, you must resolve the conflict in both vaults.

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 can be shown regardless of its permissions in the source vault. For example, the name of the document creator can be shown in the metadata of the published document as "Created by: User XYZ (deleted)". 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 Object Relationships.

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.

3.2. Configuring M-Files

This section offers guidance on personalizing the system to function and behave according to the requirements of your organization. In addition to instructions on modifying the metadata structure of your vault, the topics under this section deal with themes such as adding and editing workflows, installing and using vault applications, editing notification settings, and making use of event handlers and scripts.

In this chapter

3.2.1. Editing the Vault Metadata Structure

M-Files Admin enables you to modify the metadata elements of the vault, 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, and therefore the metadata structure of the vault should be carefully planned.

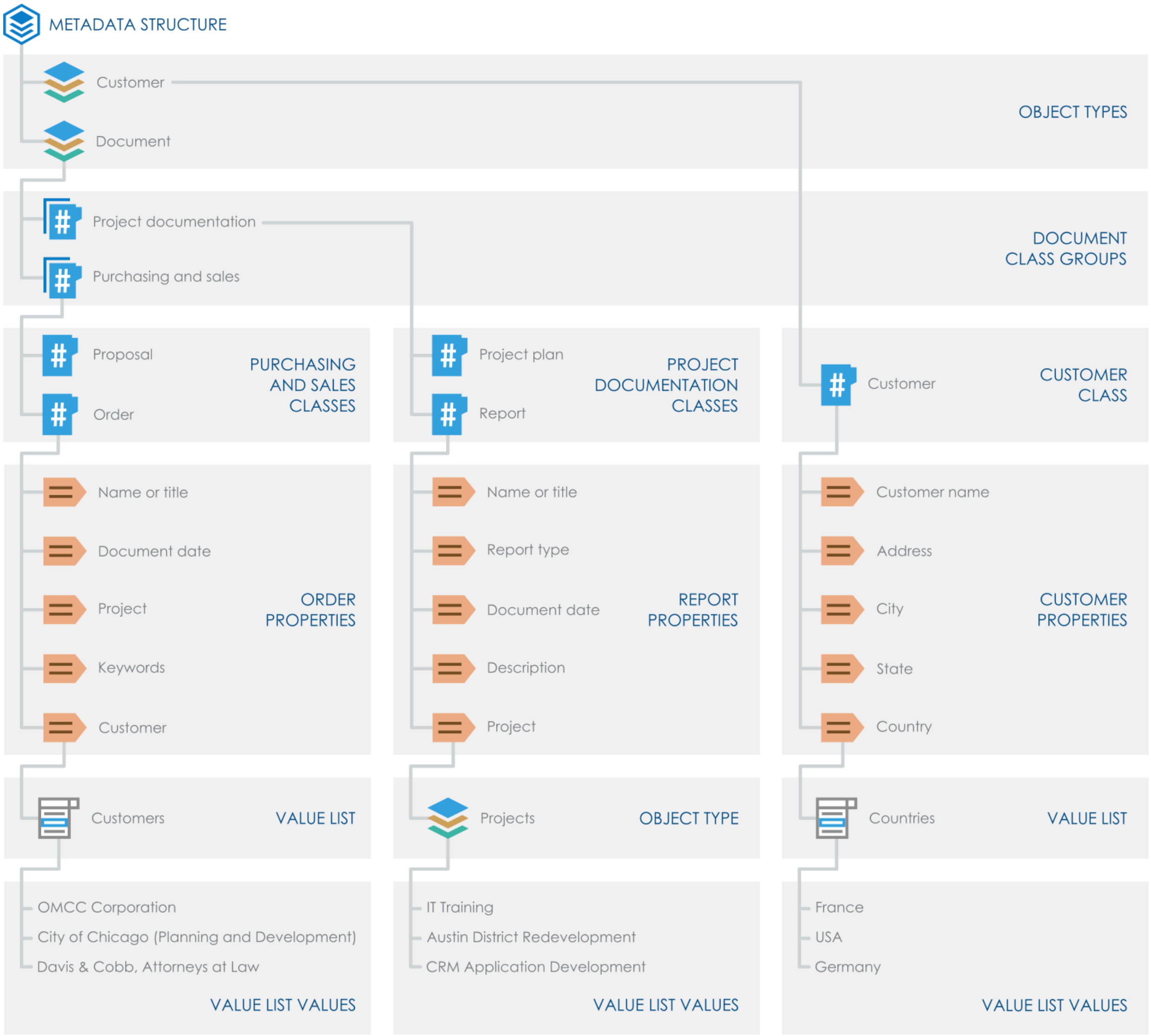


Figure 38: The vault metadata structure consists of object types, class groups, classes, property definitions, and value lists. The example above illustrates the hierarchy of a metadata structure that contains the Customer and Document object types and various classes for the two object types.

You can browse and edit the vault metadata structure either as a hierarchical view or as a flat view.

Complete the following steps to browse and edit your vault metadata structure:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Hierarchical View)** or **Metadata Structure (Flat View)**.

In the **Metadata Structure (Hierarchical View)** and **Metadata Structure (Flat View)** sections, you can create new metadata elements, such as object types, to the vault metadata structure or modify existing ones. See the subtopics in this section for further information on different types of metadata elements and how you can specify them.

In this chapter

- Object Types
- Value Lists
- Property Definitions
- Classes
- Class Groups

Object Types

M-Files uses object types to specify the stored objects. The built-in object types are document, document collection, and share. You can also specify more object types, for example, customer, contact, or project.

> **Note:** Currently, you can use the share object type only with the M-Files for Microsoft Teams integration. For more information on the share object type, refer to section 1.5 in Setting Up and Using M-Files for Microsoft Teams.

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).

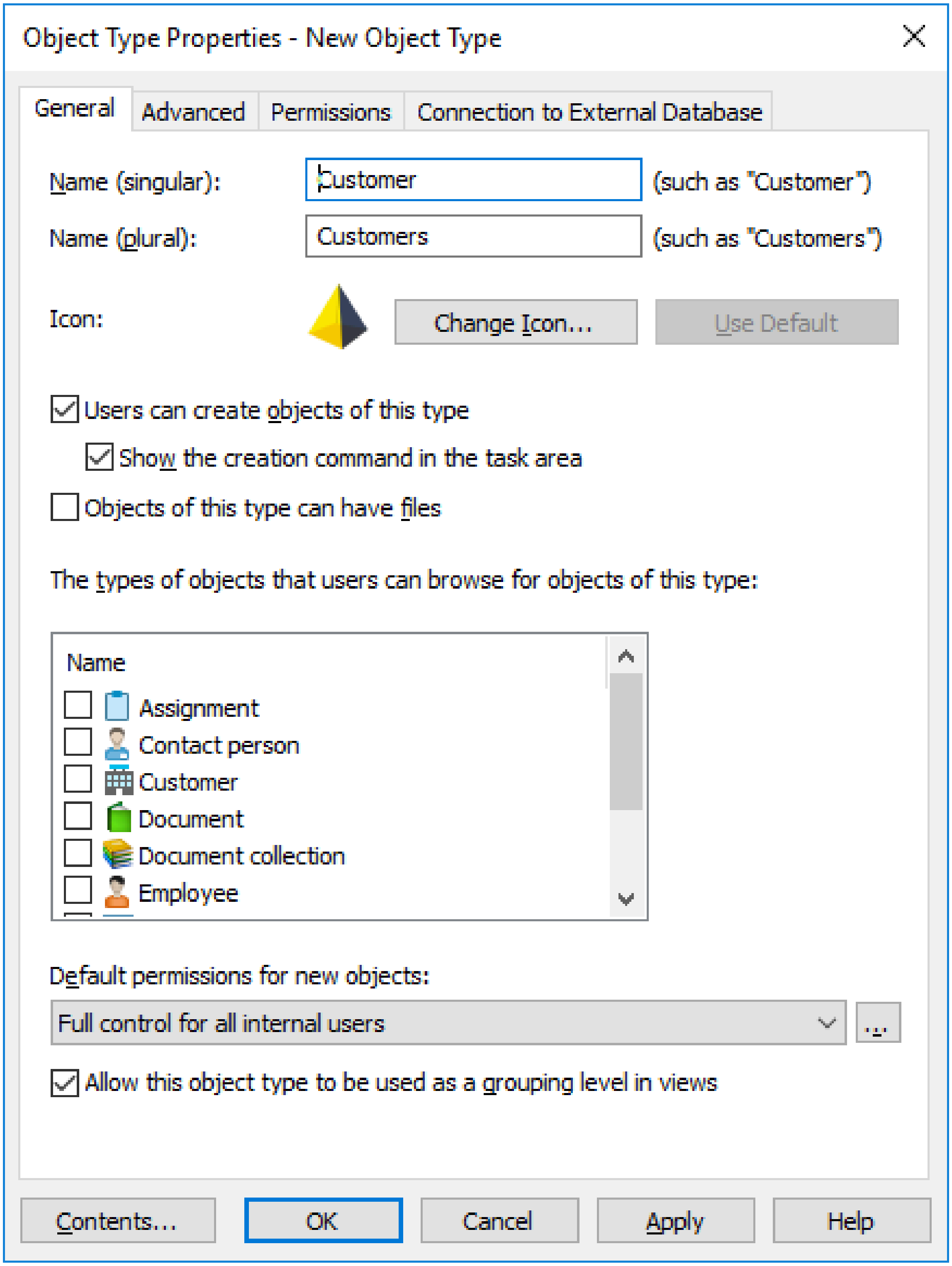
In this chapter

- Creating a New Object Type
- Advanced Object Type Properties
- Object Type Permissions
- Connections to External Databases for Object Types

Creating a New Object Type

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)**.
6. Click **Object Types**.
7. In the task area, click **New Object Type**.

   ✓ The **Object Type Properties** dialog is opened.



Name (singular): Customer (such as "Customer")

Name (plural): Customers (such as "Customers")

Icon:

☑ Users can create objects of this type

☑ Show the creation command in the task area

□ Objects of this type can have files

The types of objects that users can browse for objects of this type:

Name
□ Assignment
□ Contact person
□ Customer
□ Document
□ Document collection
□ Employee

Default permissions for new objects: Full control for all internal users

☑ Allow this object type to be used as a grouping level in views

8. In the **Name (singular)** field, write a name for the object type in the singular form.

9. In the **Name (plural)** field, write the same name in the plural form.

10. Optional: To change the icon of the object type, click **Change Icon**.

a) Select an icon from the list or click **Browse** to browse for a different icon file.
b) Click **OK**.

If you want to restore the default icon, click **Use Default**.

11. Optional: If you want that users can create objects of this type in M-Files, select the **Users can create objects of this type** check box.
    a) If you want the object type to appear under the **Create** menu in the top area and the task area, select **Show the creation command in the task area**.

12. Optional: If you want that users can add files into objects of this type, select **Objects of this type can have files**.

13. Optional: In the **The types of objects that users can browse for objects of this type** list, select the object types that users can browse when they double-click an object of this type or right-click an object and select **Browse Relationships** in M-Files.

    This setting does not affect the related objects displayed in the listing view (search results or a view) below the main object.

14. In the **Default permissions for new objects** drop-down menu, select the default permissions for new objects of this type.

    To adjust any permission settings, click the **...** button.

15. Optional: Select the **Allow this object type to be used as a grouping level in views** check box so that users can use this object type to define a grouping level within a view.

16. Optional: To define an object type hierarchy, automatic permissions, a separate metadata search index, or aliases for the object type, click the **Advanced** tab.

    For more instructions, see Advanced Object Type Properties.

17. Optional: To refine the permissions for the new object type, click the **Permissions** tab.

    For more instructions, see Object Type Permissions.

18. Optional: To use an external database as the source of the objects for the new object type, define the external database connection on the **Connection to External Database** tab.

    For more instructions, see Connections to External Databases for Object Types.

19. Click **OK**.

You can see the object type that you have just created in the **Object Types** list. You can now create objects of this type in M-Files.

Advanced Object Type Properties

On the **Advanced** tab of the **Object Type Properties** dialog, for the selected object type, you can:

- define an object type hierarchy
- define automatic permissions
- enable a separate metadata search index
- define aliases

Defining an Object Type Hierarchy

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.

To define an object type hierarchy:

1. In M-Files Admin, go to the **Advanced** tab of the **Object Type Properties** dialog for the object type that you want to modify.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Expand **Metadata Structure (Flat View)** and then select **Object Types**.

      ✓ The **Object Types** list is opened in the right pane.

   f) Double-click the object type that you want to modify.

      ✓ The **Object Type Properties** dialog is opened.

   g) Click the **Advanced** tab.
2. Do one or both of the following:

If you want to	Do the following task
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. Hold down the Ctrl key to select multiple individual items or hold down the ⇧ Shift key to select adjacent items on the list. **Note:** To remove a subtype, click **Remove**.
Define this object type as a subtype of another object type	Select the **This object type is a subtype of the following object type** check box and select the object type from the drop-down menu.

3. Click **OK**.

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.

Defining Automatic Permissions for an Object Type

An object receives automatic permissions when a value with automatic permissions is added to the object metadata. You can define automatic permissions for an object type so that when an object of the selected type is referred to in the metadata of another object, the object inherits the permissions of the object that it references.

Note: The automatic permission settings that are specific to a value list item always have priority over the settings made at value list and object type level. For more information on automatic permissions for value list items, see Automatic Permissions for Value List Items.

Note: Micro Focus IDOL and Smart Search: If more than four automatic ACL sources control the permissions of an object, only administrators can see it in search results.

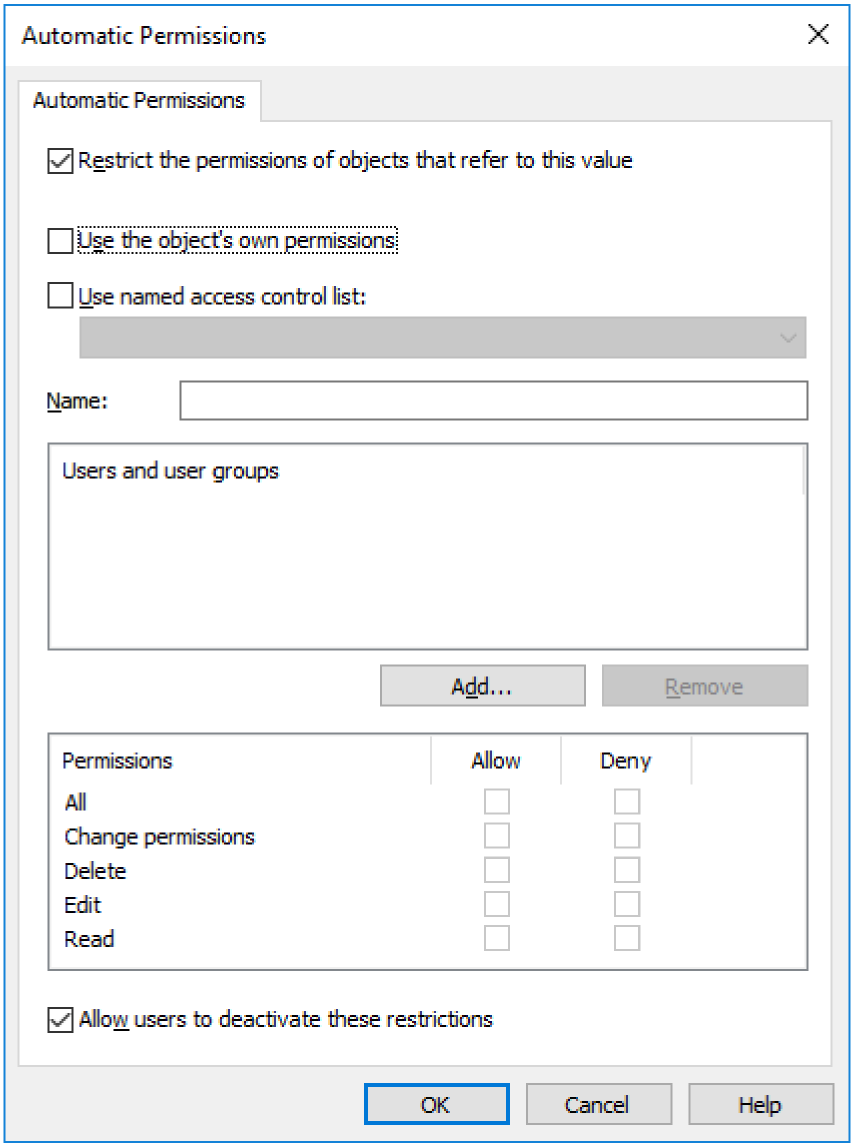
To define automatic permissions for an object type:

1. In M-Files Admin, go to the **Advanced** tab of the **Object Type Properties** dialog for the object type that you want to modify.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Expand **Metadata Structure (Flat View)** and then select **Object Types**.

      ✓ The **Object Types** list is opened in the right pane.
   f) Double-click the object type that you want to modify.

      ✓ The **Object Type Properties** dialog is opened.
   g) Click the **Advanced** tab.
2. Click the **Define** button next to **Default automatic permissions from this object type**.

   ✓ The **Automatic Permissions** dialog is opened.



Automatic Permissions

☑ Restrict the permissions of objects that refer to this value

□ Use the object's own permissions

□ Use named access control list:

Name:

Permissions	Allow	Deny
All	□	□
Change permissions	□	□
Delete	□	□
Edit	□	□
Read	□	□

☑ Allow users to deactivate these restrictions

3. Select the **Restrict the permissions of objects that refer to this value** check box to enable automatic permissions for the selected object type.

4. Do one of the following:

If you want to	Do the following task
Use the object permissions defined on the metadata card as automatic permissions	Select the **Use the object's own permissions** check box.
Use a predefined named access control list as automatic permissions	Select the **Use named access control list** check box and then select a predefined named access control list from the drop-down menu.
Use custom permission settings as automatic permissions	Click the **Add** button, then select the users or user groups to be added to the custom permission settings, and click **Add**.

If you want to	Do the following task
	Note: You can select more than one item at once. Hold down the Ctrl key to select multiple individual items or hold down the ⇧ Shift key to select adjacent items on the list. **Note:** To remove a user or group from the settings, click **Remove**. Select a user or group in the **Users and user groups** list and grant permissions in the **Permissions** list with the **Allow** and **Deny** check boxes.

5. Optional: Select the **Allow users to deactivate these restrictions** check box if you want vault users to be able to disable the automatic permissions granted by these settings.

6. Click **OK** to close the **Automatic Permissions** dialog.

7. Back in the **Object Type Properties** dialog, click **Apply** or **OK**.

The selected object type now has automatic permissions. Now when an object of this object type is referred to in the metadata of another object, the referring object inherits the permissions of the object that has automatic permissions set.
Using a Separate Metadata Search Index for an Object Type

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 example, 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*, and *Contact person*.

If you select this option, M-Files uses 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 if 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 and the users cannot access the vault.

To enable a separate metadata search index for an object type:

1. In M-Files Admin, go to the **Advanced** tab of the **Object Type Properties** dialog for the object type that you want to modify.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Expand **Metadata Structure (Flat View)** and then select **Object Types**.

The **Object Types** list is opened in the right pane.

f) Double-click the object type that you want to modify.

The **Object Type Properties** dialog is opened.

g) Click the **Advanced** tab.

2. Select the **Use a separate metadata search index for this object type** check box.

3. Click **OK**.

M-Files now uses a separate search index for the objects of the selected object type.
Defining Aliases for an Object Type

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, names, or both 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 you define 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.

To define aliases for an object type:

1. In M-Files Admin, go to the **Advanced** tab of the **Object Type Properties** dialog for the object type that you want to modify.

a) Open M-Files Admin.
b) In the left-side tree view, expand an M-Files server connection.
c) Expand **Document Vaults**.
d) Expand a vault.
e) Expand **Metadata Structure (Flat View)** and then select **Object Types**.

The **Object Types** list is opened in the right pane.

f) Double-click the object type that you want to modify.

The **Object Type Properties** dialog is opened.

g) Click the **Advanced** tab.

2. In the **Aliases** field, enter the aliases for the selected object type.

Use semicolons (;) to separate many aliases.

ObjectType.Customers; OT.Customers

When automatic aliases are in use and you write a name on the **General** tab, the **Aliases** field on the **Advanced** tab is automatically filled in. The alias has the format <*predefined prefix*>.<*name*>. Configure automatic aliases for your vault in Advanced Vault Settings.

3. Click **OK**.

Object Type Permissions

On the **Permissions** tab, you can specify the access rights for viewing this object type and creating objects of this type.

If the user does not have the permission to view the name of the object type, it is not available for selection in the M-Files clients. 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.

Editing Permissions

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click a node that contains items that you want to edit.

   Permission settings are available for these items:

   - **Users**
   - **User groups**
   - **Metadata Structure (Flat View)** > **Object types**
   - **Metadata Structure (Flat View)** > **Value lists**
   - **Metadata Structure (Flat View)** > **Property definitions**
   - **Metadata Structure (Flat View)** > **Classes**
   - **Metadata Structure (Flat View)** > **Class groups**
   - **Workflows**
   - **Named access control lists**
6. Select an item in the listing area.
7. Right-click the item and click **Properties**.
8. Open **Permissions**.
9. In **Users and user groups**, select the user or user group whose permissions to change.

   If the user or user group is not on the list, click **Add**.
10. Specify the permissions for the selected user or user group.

    Allow: Enable this to explicitly give the permission to the selected user or user group.

    Deny: Enable this to explicitly deny the permission from the user or user group.

The **Deny** setting is normally used to specify an exception to an **Allow** setting. For example, when John Doe is part the group **HR Managers**, you can set **Allow** for the group and **Deny** for John Doe.

You can also leave both settings unselected.

11. Repeat steps 9 and 10 for the rest of the permissions.

12. Click **OK**.

Connections to External Databases for Object Types

You can set M-Files to update object types to and from an external database. Objects that use an external database connection can also contain properties that are not synchronized with the external database.

This section tells you how to set object types to use an application connection to an external database. To use the legacy database connection, see the section "Using the Legacy Database Connection for Object Types".

Prerequisites

Take note of this important information before you start the setup:

- Before you set up an application connection to an external database, you must have an external object type connector installed and enabled.
  - The connector must support the application connection. You can use M-Files OLE DB External Object Type Connector, which is normally installed to the vault but is disabled.
    - To use the connector, a license is not necessary.
    - For instructions on adding connectors and managing vault applications, see Adding a Connector and Installing and Managing Vault Applications.
  - If you use the Ground Link service, the connector must be enabled on the Ground Link proxy. For instructions, see Configuring External Object Types over Ground Link. If you use a local service, the connector must be enabled in the vault.
- If you use replication and application connection to an external database service, you must configure the connection separately for each vault in the replication scheme. Make sure that the necessary configuration changes are also made to each vault. We also recommend that you read the section **Replication of External Objects** of the document Replication and Archiving - User's Guide.
- It is not possible to include the configuration for **External Object Type Connector** to replication packages.
- In `SELECT FROM` statements, the columns are selected in order of appearance. There is no relation between column and property names, which is why the order must be the same in the `SELECT FROM` and `INSERT INTO` statements, and `SELECT FROM` and `UPDATE` statements. Also, columns not used in the `INSERT INTO` and `UPDATE` statements must always be listed last in the `SELECT FROM` statement.

To use a connection to external database and to open the service configuration:

1. Open M-Files Admin and go to a vault.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.

2. Expand **Metadata Structure (Flat View)**.

3. Click **Object Types**.

   ✓ The object type listing is opened in the right pane.

4. In the right-pane listing, double-click the object type.

   ✓ The **Object Type Properties** dialog is opened.

5. Go to the **Connection to External Database** tab and enable the option **Use a connection to an external database to import and modify objects that reside in the external database**.

6. Select **Application connection**.

7. In **Service**, select the service.

Option	Description
`M-Files OLE DB at vault <name of the vault>`	Select this option to use the local service.
`M-Files OLE DB from Ground Link proxy <name of the Ground Link proxy>`	Select this option to establish the connection with a remote service through Ground Link.

   ℹ The services that have the `(OK)` suffix, have a configuration for the object type.

   ✓ Information of the service configuration with possible errors is shown.

8. Click **Configure**.

   ✓ The **External Object Type Connector** dialog is opened.

To specify the connection settings and to get the source columns:

9. Expand **Service-Specific Settings** > **Connection to External Database**.

10. In **Provider**, select the provider for the external database connection.

    ✎ **Microsoft OLE DB Driver for SQL Server**.

    ℹ **Note:** The list of providers shows all the available providers on the server machine that runs the external object type connector. Thus, it can include providers that cannot be used in external database connections.

    ℹ The syntax of the connection string is different for each Object Linking and Embedding Database (OLE DB) supplier used for establishing the connection to the external database. If Open Database Connectivity (ODBC) is necessary to create the connection, the data store must be accessed over OLE DB and ODBC. For a list of recommended providers, see Provider Recommendations for External Database Connections.

11. Optional: If you selected **Custom provider (manual configuration)**, in **Custom provider**, specify the provider.

12. Under **Connection to External Database**, complete one of these steps:

Option	Description
Specify the other settings.	The correct values are different for each provider and external database. For more information, select a setting and see the **Info** tab.
In Advanced Options, enter the connection string.	Use this option if it is not possible to use the other settings with the selected provider. When you enter the connection string, make sure that all values are correctly enclosed and the connection string has the necessary formatting.

13. Optional: Under **Optional SELECT Statements**, define the settings.

    Note: The application connection does not support the **Connections to External Databases** settings in the **Advanced Vault Settings** section in M-Files Admin. To use these settings, define them here.

14. Under **Service-Specific Settings**, in **SELECT Statement**, write the SELECT statement for getting source columns from the external database.

    Examples of SELECT statements:

    ```
    SELECT CustomerNumber, CustomerName FROM Customer
    ```

    ```
    SELECT ID, Name + ' ' + Department FROM Company
    ```

    ```
    SELECT ID, Name, CustomerID FROM Contacts
    ```

    ```
    SELECT * FROM Customer
    ```

    Tip: You can write a multi-line statement.

15. Click **Save**.

16. Optional: To configure a remote service:
    a) Click **Apply**.

       ✓ The **Enter Password** dialog is opened.

    b) Enter the password that is defined in the Ground Link proxy configuration.
    c) Click **OK**.

17. To authenticate the common user, open the **Dashboard** tab and click **Authenticate**.

    ✓ The **Log In** dialog is opened.

18. Enter the common user credentials and click **Log In**.

    Note: The ODBC driver does not support all special characters. If your connection uses ODBC, the values that contain special characters must be enclosed in curly brackets. The correct format is `{`*`username or password`*`}`.

19. In the dialog that is opened, click **OK**.

20. Click **Save** to get the source columns.

    a) Optional: To configure a remote service, repeat step 16.

    Note: You cannot save the configuration if there are no changes.

    ✓ The dialog closes and the configuration refreshes. On the **Configuration** tab, the **Column Mappings** section shows the source columns that your SELECT statement returned from the external database.

To map the source columns with M-Files properties:

21. On the **Configuration** tab, go to **Column Mappings** and expand a source column node.

22. In **Mapping Type**, specify how the source column is mapped to M-Files. Complete one of these steps:

    a. To map a source column as the external ID, select **Object ID**.

       or

    b. To map the source column to an M-Files property, select **Property**. In **Target Property**, select the M-Files property.

    Note: When you want to map multiple values to a property of the **Choose from list (multi-select)** data type, the values must be recorded on their own rows in the external database. For example, if you want to map multiple values to the **Industry** property, the values must be recorded like this:

ID	Customer name	City	Industry	Active
ABC-123	ESTT Corporation	New York	100	1
ABC-123	ESTT Corporation	New York	101	1
ABC-123	ESTT Corporation	New York	108	1

    In this case, however, data can only be read from, not recorded to the external database.

23. Optional: If the **Mapping Type** is **Property**, specify the settings **Use in Update Operation** and **Use in Insert Operation** and define the related statements.

If you want to...	Complete the following steps:
Allow read-only access	Set the **Use in Update Operation** and **Use in Insert Operation** settings to **No**. Do not specify the statements in this table.
Allow users to update but not create or delete information	**a.** Set the **Use in Update Operation** to **Yes**. **b.** Under **Service-Specific Settings**, in **UPDATE statement**, write the UPDATE statement.
Allow users to update, create, and delete information	**a.** Set the **Use in Update Operation** and **Use in Insert Operation** settings to **Yes**.

If you want to...	Complete the following steps:
	b. Under **Service-Specific Settings**, write the four statements in this table.

Statement	Definition	Examples

UPDATE	When a user edits 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.
	Note: Make sure that the columns are in the same order as they are in the SELECT statement.
		`UPDATE Customers SET CustomerName = ? WHERE CustomerID = ?`
		`UPDATE Contact SET Name = ?, CustomerID = ? WHERE ContactID = ?`

INSERT INTO	When a user creates 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: Make sure that the columns are in the same order as they are in the SELECT statement.
	Note: The INSERT INTO statement input to M-Files does not define a value for the ID column. The external 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. If the external database cannot produce new ID values, the INSERT INTO statement cannot be used.
		`INSERT INTO Customers( CustomerName ) VALUES( ? )`
		`INSERT INTO ContactPersons( Name, CustomerID ) VALUES( ?, ? )`

Get ID SELECT	After a new record has been created with the INSERT INTO statement, M-Files Server gets the ID of the created record with this SELECT statement.	`SELECT MAX( CustomerID ) FROM Customer`
		`SELECT ID FROM Customers WHERE CustomerName = ?`

Statement	Definition	Examples

DELETE	When a user deletes 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 = ?`

24. Repeat the steps from 21 to 23 for all the necessary source columns.

To take the configuration into use:

25. Under **General Settings**, set **Enabled** to **Yes**.

> **Tip:** You can enable and disable the external database connection also with the **Disabled** check box on the **Connection to External Database** tab of the **Object Type Properties** dialog.
>
> If the connection is disabled, information between the vault and the external database is not synchronized.

26. Optional: To configure a remote service:

a) Click **Apply**.

✓ The **Enter Password** dialog is opened.

b) Enter the password that is defined in the Ground Link proxy configuration.

c) Click **OK**.

27. Click **OK** to close the **Object Type Properties** dialog.

The object type is now updated to and from the external database.

In this chapter

- Using the Legacy Database Connection for Object Types
- Refreshing External Object Types
- Provider Recommendations for External Database Connections
- Configuring Logging for External Object Type Connectors

Using the Legacy Database Connection for Object Types

Before you start, take note of this information:

- In `SELECT FROM` statements, the columns are selected in order of appearance. There is no relation between column and property names, which is why the order must be the same in the `SELECT FROM` and `INSERT INTO` statements, and `SELECT FROM` and `UPDATE` statements. Also, columns not used in the `INSERT INTO` and `UPDATE` statements must always be listed last in the `SELECT FROM` statement.
- In the `SELECT` statement used to get the ID of the records, `WHERE` must refer to the first column of the `SELECT FROM` statement.

1. Do the steps from 1 to 5 in Connections to External Databases for Object Types.

2. In M-Files Admin, in the **Connection to External Database** tab of the **Object Type Properties** dialog, select **Legacy database connection**.

3. Click **Configure**.

   ✓ The **Configure Connection to External Database** dialog is opened.

4. Click the **Define** button next to the **OLE DB connection string (from server)** field.

   The syntax of the connection string is different for each Object Linking and Embedding Database (OLE DB) supplier used for establishing the connection to the external database. If Open Database Connectivity (ODBC) is necessary to create the connection, the data store must be accessed over OLE DB and ODBC. For a list of recommended providers, see Provider Recommendations for External Database Connections.

   Note: M-Files Admin only displays OLE DB providers that are available on the computer running M-Files Admin. If your M-Files Server resides on a different host, make sure that the selected OLE DB connection string works from the computer running M-Files Server as well.

   ✓ The **Data Link Properties** dialog is opened.

5. On the **Provider** tab, select **Microsoft OLE DB Driver for SQL Server** from the list and click **Next >>**.

   Other providers can have different options on the **Connection** and **Advanced** tabs. The **All** tab contains all the available connection properties as a name–value table.

   Note: We do not recommend the use of Microsoft Access Database Engine Redistributables to import value lists or object types from an Excel file.

   ✓ The **Connection** tab of the **Data Link Properties** dialog is opened.

6. To the **Select or enter a server name** field, write the name of your Microsoft SQL Server.

7. In the **Enter information to log on to the server** section, select:

   a. **Windows Authentication**: Select this option to use a Microsoft Windows account for logging in. In this case, the connection uses the credentials that are used for running the M-Files Server service.

      or

   b. **SQL Server Authentication**: Select this option to use a Microsoft SQL Server login. Enter the credentials in the **User name** and **Password** fields, and select the **Allow saving password** check box.

   Note: The ODBC driver does not support all special characters. If your connection uses ODBC, the values that contain special characters must be enclosed in curly brackets. The correct format is `{username or password}`.

8. For the **Select the database** section, complete one of these steps:

   a. Use the drop-down menu to select the database on the specified server.

      or

   b. Enter a database name to the **Attach a database file as a database name** field and click the **...** button to select a Microsoft SQL Server Database (MDF) file.

9. Optional: Click **Test Connection** to make sure that your database connection operates correctly.

10. Optional: On the **Advanced** tab, define a timeout period for the database connection.
11. Click **OK** to close the **Data Link Properties** dialog.

    The connection string is added to the **OLE DB connection string (from server)** field.

12. In the **Configure Connection to External Database** dialog, to the **SELECT statement** field, enter the SELECT statement for getting source columns from the external database.

    Examples of SELECT statements:

    ```
    SELECT CustomerNumber, CustomerName FROM Customer

    SELECT ID, Name + ' ' + Department FROM Company

    SELECT ID, Name, CustomerID FROM Contacts

    SELECT * FROM Customer
    ```

13. Click **Refresh Columns** to get the source columns.

    The **Columns** listing shows correspondences between columns retrieved from the external database (**Source Column**) and M-Files properties (**Target Property**).

14. Map the **Source Column** properties with properties in your M-Files vault (listed in the **Target Property** column).

    Note: When you want to map multiple values to a property of the **Choose from list (multi-select)** data type, the values must be recorded on their own rows in the external database. For example, if you want to map multiple values to the **Industry** property, the values must be recorded like this:

ID	Customer name	City	Industry	Active
ABC-123	ESTT Corporation	New York	100	1
ABC-123	ESTT Corporation	New York	101	1
ABC-123	ESTT Corporation	New York	108	1

    In this case, however, data can only be read from, not recorded to the external database.

15. Select the check boxes in the **Update** and **Insert** columns and define the four statements below the **Columns** listing.

If you want to...	Complete the following steps:
Allow read-only access	Do not select the check boxes and leave the statements empty.
Allow users to update but not create or delete information	**a.** Select the check boxes in the **Update** column for the necessary properties. **b.** Click the **Default** button next to the UPDATE statement field. You can also enter your statements to the fields.

If you want to...	Complete the following steps:
Allow users to update, create, and delete information	**a.** Select the check boxes in the **Update** and **Insert** columns for the necessary properties. **b.** Click the **Default** button next to the UPDATE, INSERT INTO, SELECT, and DELETE statement fields. You can also enter your statements to the fields.

The table below explains the use of the four statements mentioned above.

Statement	Definition	Examples

UPDATE	When a user edits 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.
	Note: Make sure that the columns are in the same order as they are in the SELECT statement.
		`UPDATE Customers SET CustomerName = ? WHERE CustomerID = ?`
		`UPDATE Contact SET Name = ?, CustomerID = ? WHERE ContactID = ?`

INSERT INTO	When a user creates 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: Make sure that the columns are in the same order as they are in the SELECT statement.
	Note: The INSERT INTO statement input to M-Files does not define a value for the ID column. The external 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. If the external database cannot produce new ID values, the INSERT INTO statement cannot be used.
		`INSERT INTO Customers( CustomerName ) VALUES( ? )`
		`INSERT INTO ContactPersons( Name, CustomerID ) VALUES( ?, ? )`

Statement	Definition	Examples

SELECT	After a new record has been created with the INSERT INTO statement, M-Files Server gets the ID of the created record with this SELECT statement.	`SELECT MAX( CustomerID )`
		`FROM Customer`
		
		`SELECT ID FROM Customers`
		`WHERE CustomerName = ?`

DELETE	When a user deletes 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 = ?`

16. Click **OK** to close the **Configure Connection to External Database** dialog.

17. Optional: Select the **Disabled** check box to temporarily disable the external database connection.

If the connection is disabled, information between the vault and the external database is not synchronized.

18. Click **OK** to close the **Object Type Properties** dialog.

The object type is now updated to and from the external database.
Refreshing External Object Types

There are two types of refresh operations for external object types:

- full refresh
- quick refresh

A full refresh detects new items, compares and updates existing items, and deletes items that have disappeared from the external database. A quick refresh, by default, only detects new items in the external database. It does not compare existing items. It does not delete items, either, because undeleting them would require a full refresh.

The quick refresh operation is notably quicker than the full refresh operation. For reference, the full refresh operation for 120,000 items takes about two minutes, while the quick refresh operation finishes in about seven seconds. For simple value lists, refreshing data is fast even with large amounts of data and therefore a full refresh is always used. This guarantees up-to-date data.

Refreshing external object types manually

External object types can be refreshed in the classic M-Files Desktop by pressing Alt and selecting **Settings** > **Refresh External Objects** and then by selecting a suitable external object type from the submenu. You can select either the **Quick Refresh** or the **Full Refresh** operation.

If you try to refresh an external object type at the same time with M-Files Server, the operation started by you begins after the one started by M-Files Server.

Refreshing external object types with M-Files Admin

To start or stop the full refresh operation for an external object type in M-Files Admin, right-click the object type in **Metadata Structure (Flat View)** and click **Refresh Now**. This gets the up-to-date column data from the external database.

The full refresh operation is also started when you edit the object type definitions in M-Files Admin. If you update the object type definition before the previous refresh operation has completed, M-Files starts the operation again.

Automatic refresh operations and configuration options

The quick refresh operation is started automatically if an external object type is requested by a client (for instance, the metadata card containing a property that uses an external object type is viewed) and if the latest refresh was executed more than 15 minutes ago.

A full refresh operation is initiated for all external object types at 4:30 AM server time every night. This operation is executed as one part of the nightly maintenance routine.

A full refresh operation is automatically triggered instead of a quick refresh operation if an external object type is requested by the client and if a full refresh has not been performed within the last 25 hours.

For configuration options available for refreshing external object types automatically, see the document Default Refresh Logic and Configuration Options for External Value Lists and Object Types.

Automatic property values ignored during refresh operations

When M-Files updates objects to and from an external database, it compares object properties in the external database to the ones in the vault. If M-Files finds differences in the properties, it updates the objects. During the comparison, properties with an automatically calculated value are ignored, which causes these scenarios:

- If all the object's property values to be updated to or from an external database are set to have an automatically calculated value in M-Files, the object is not updated.
- If the refresh operation creates an object in M-Files, all property values of the object are filled with the values from the external database. This includes properties that are set to have an automatically calculated value.
- If the refresh operation updates the object's properties in M-Files, all the object's property values to be updated get their value from the external database. This includes properties that are set to have an automatically calculated value.

Provider Recommendations for External Database Connections

The table below lists the recommended OLE DB providers to be used for an external database connection (see Connections to External Databases for Object Types).

Database	Provider
Microsoft SQL Server Azure SQL Server Azure SQL Managed Instance	Microsoft OLE DB Driver for SQL Server (`MSOLEDBSQL`) **Note:** Using the following, deprecated providers is not recommended: • Microsoft OLE DB Provider for SQL Server (`SQLOLEDB`) • SQL Server Native Client OLE DB Provider (`SQLNCLI`)
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: M-Files Server only supports 64-bit drivers for External Object Types and External Value Lists. Make sure that you download and install 64-bit versions of custom drivers, for example MySQL.

Configuring Logging for External Object Type Connectors

- This is an advanced feature for advanced users only.
- Logging is only available for some External Object Type connectors. Check your connector documentation to see if logging is available for it.
- To use logging, you must first configure an External Object Type connection. For instructions, see Connections to External Databases for Object Types.
- In production environments, it is recommended that logging is disabled or set to only log errors and enabled temporarily to diagnose specific issues.

Administrators and developers can enable logging to help diagnose connector behavior and common issues. You can configure logging to include only warnings and errors, and some connectors let you include more details. For example, exact queries that are run against the external database.

To configure logging for an External Object Type connector:

1. In M-Files Admin, go to **Document vaults** > **A vault** > **Configurations** > **External Repositories**
2. Click your connector with the secondary mouse button and select **Show Application Diagnostics** from the list.

   ✓ A new diagnostics section appears.

3. Go to **Diagnostics** > **Logging** and open the **Configuration** tab.
4. Set **Enabled** to `Yes`.
5. Set at least one of the target categories.

   Default Target saves the log files in the vault's temporary folder. For more information about specific settings, click the information icon next to the setting (ⓘ).

6. Set the **Default Log Level**.

   `Trace` level logs the all possible events while `Fatal` logs only critical errors.

7. Click **Save**.

Logging is now configured, and log files will start accumulating into your target folder.
Downloading log files

To download the log files as a compressed .zip file:

1. In the left-hand pane, click **Logging** with the secondary mouse button.
2. Select **Download Logs** from the list.

   ✓ **Download Log Files** window opens.

3. Select the files you want to download.
4. Click **Download**.
5. Select a location for the .zip file.
6. Click **Save**.

Value Lists

A value list contains various values, such as city names. The same value list can be utilized in several different properties.

A value list is one of the M-Files data types. 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.

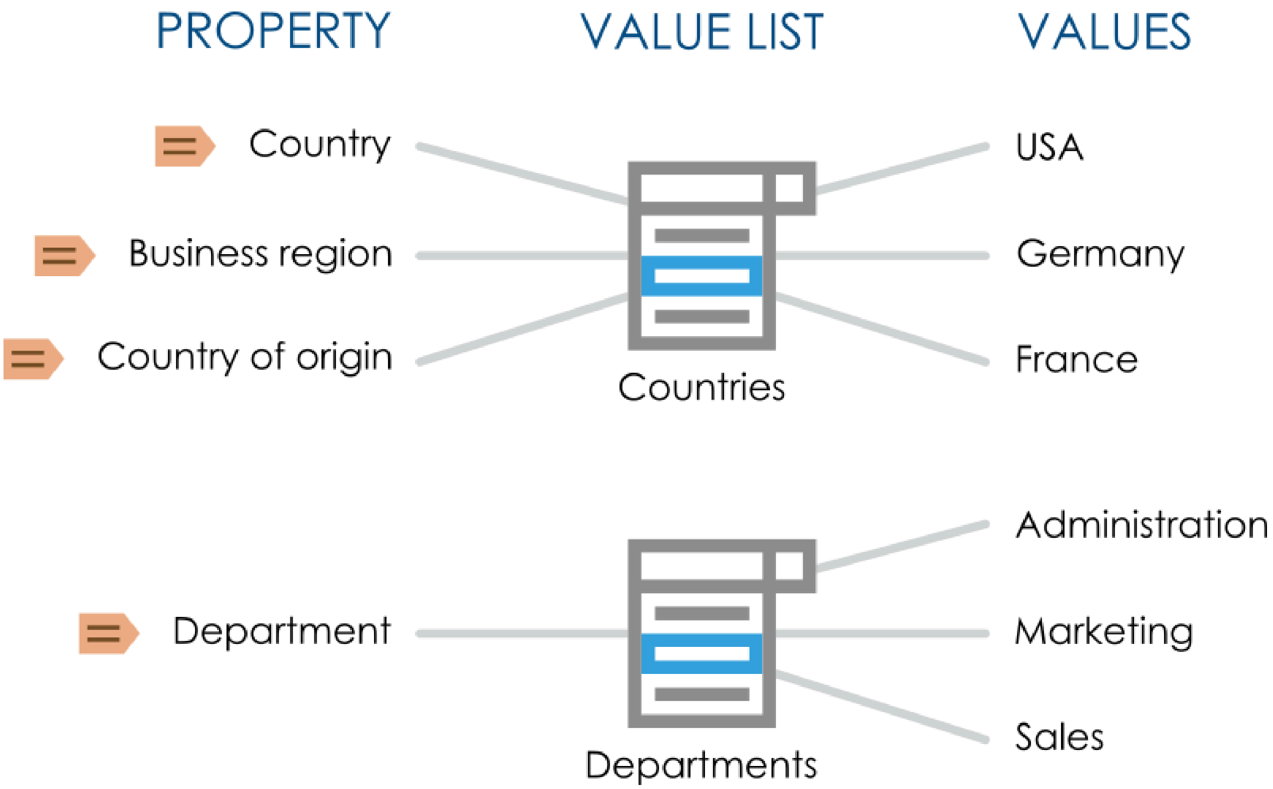


Figure 39: Value lists can be used for storing and selecting preset values for metadata properties. Several different properties can be based on the same value list.

Complete the steps below to view the value lists in your vault:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)** and then 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** in the task area.

In this chapter

New Value List

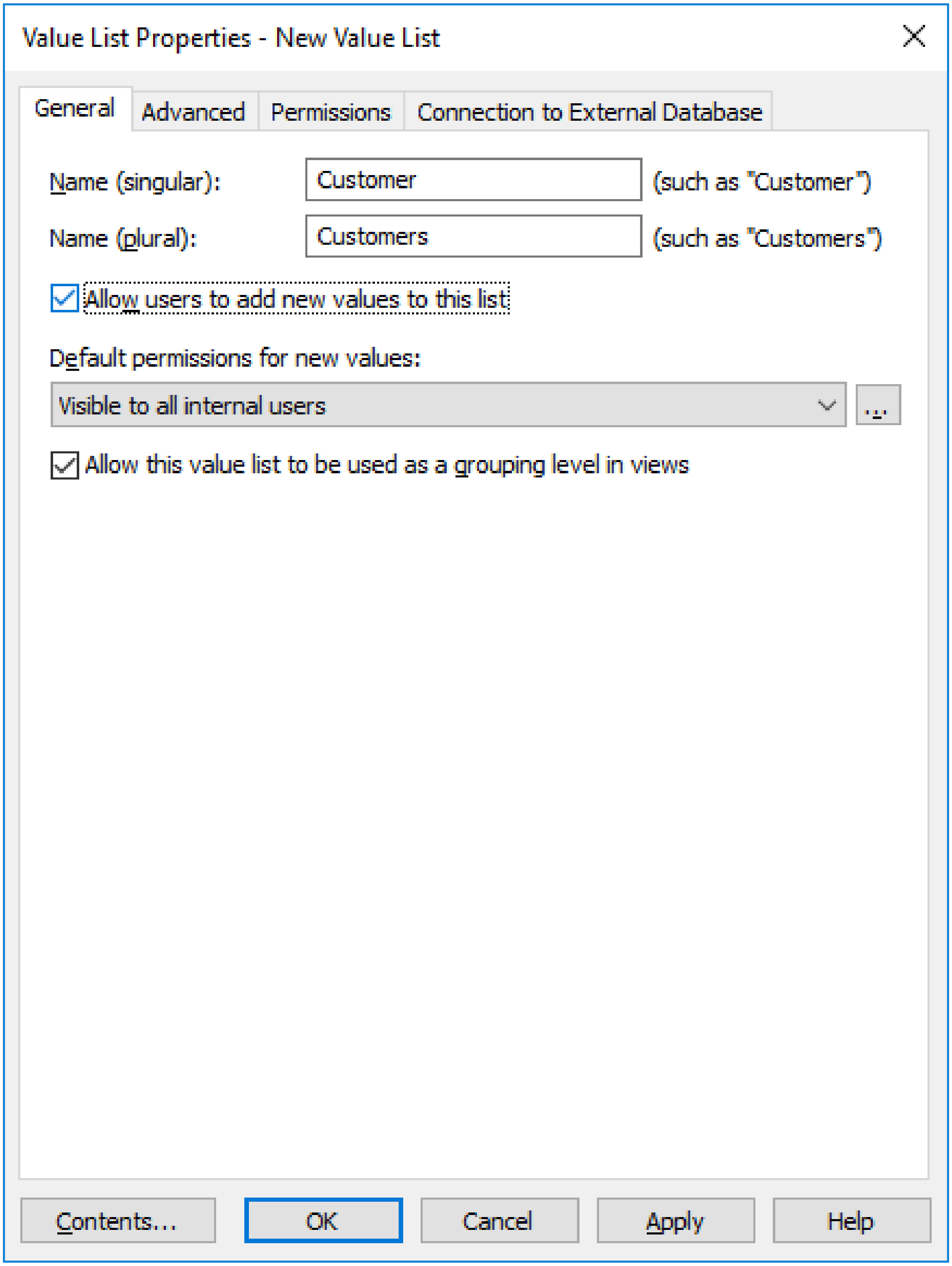
A value list can either be *internal* or *external*.

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. See Connections to External Databases for Value Lists.

Creating a New Value List

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)**, and then select **Value Lists**.
6. In the task area, click **New Value List**.

   ☑ The **Value List Properties** dialog is opened.



Value List Properties - New Value List

Name (singular): Customer (such as "Customer")

Name (plural): Customers (such as "Customers")

☑ Allow users to add new values to this list

Default permissions for new values: Visible to all internal users

☑ Allow this value list to be used as a grouping level in views

7. 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.
8. 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.
9. From the **Default permissions for new values** drop-down menu, select the default permissions for new values in this value list.

10. Optional: Check the **Allow this value list to be used as a grouping level in views** check box to allow this value list to used for defining a grouping level within a view.

11. Optional: On the **Advanced** tab, set hierarchical relationships for the value list.

    See Advanced Value List Properties for more information.

12. Optional: On the **Permissions** tab, you can specify the users who may see this value list or add new values to it.

    See Value List Permissions for more information.

13. Optional: On the **Connection to External Database**, set the connection to an external database for importing value list contents from an external database source.

    For further instructions, Connections to External Databases for Value Lists.

14. 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 a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Expand **Metadata Structure (Flat View)** and then select **Value Lists**.

6. From the **Value Lists** list, select the value list that you want to convert to an object type.

7. In the task area, click **Convert to Object Type**.

    ✓ The **Convert to Object Type** dialog appears.

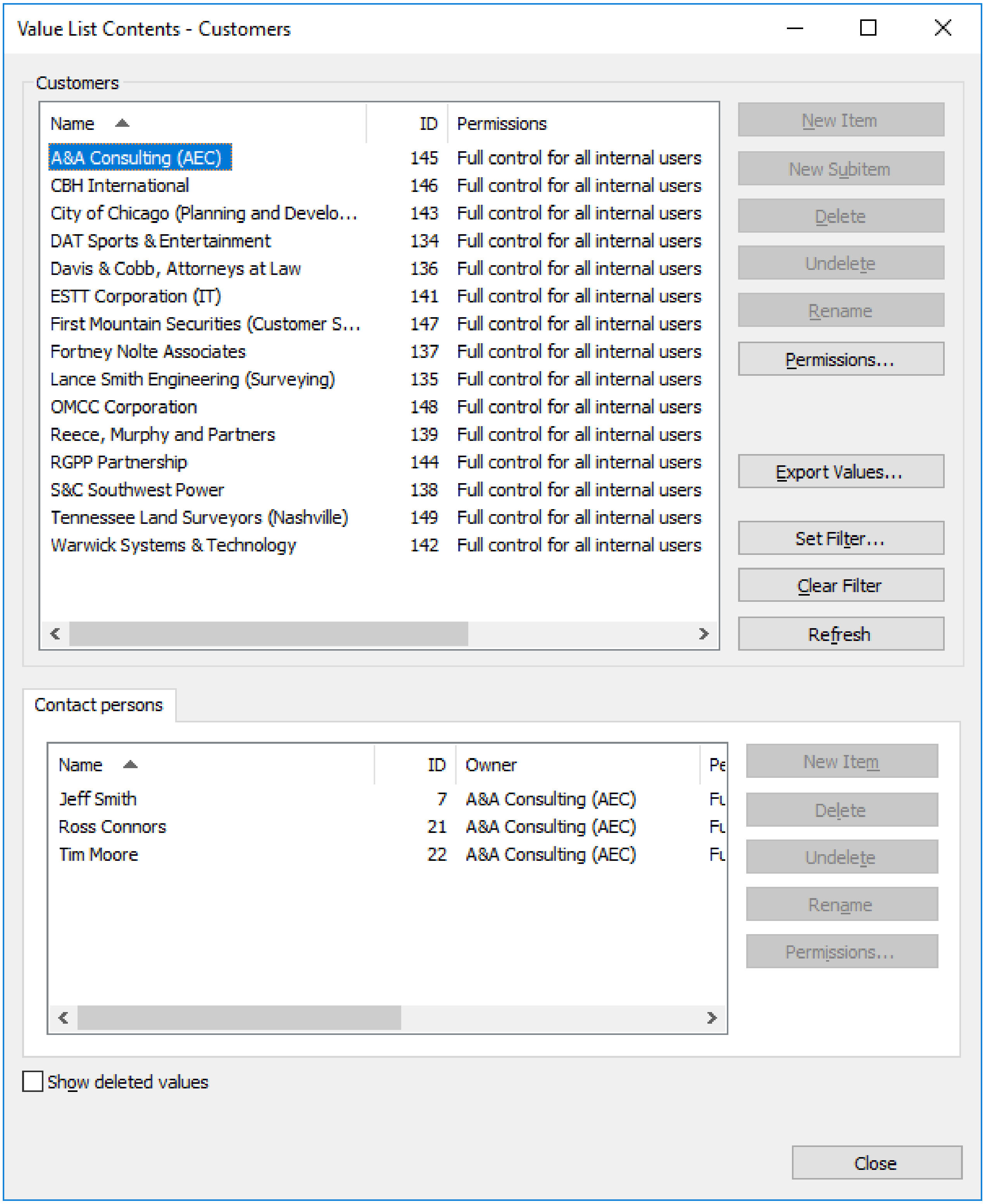
8. You are prompted to confirm that you want to convert the selected value list to an object type. Click **Yes**.

    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). Additionally, you can set value-specific permissions as well as default permissions for objects that use the item.



Name	ID	Permissions
A&A Consulting (AEC)	145	Full control for all internal users
CBH International	146	Full control for all internal users
City of Chicago (Planning and Develo...	143	Full control for all internal users
DAT Sports & Entertainment	134	Full control for all internal users
Davis & Cobb, Attorneys at Law	136	Full control for all internal users
ESTT Corporation (IT)	141	Full control for all internal users
First Mountain Securities (Customer S...	147	Full control for all internal users
Fortney Nolte Associates	137	Full control for all internal users
Lance Smith Engineering (Surveying)	135	Full control for all internal users
OMCC Corporation	148	Full control for all internal users
Reece, Murphy and Partners	139	Full control for all internal users
RGPP Partnership	144	Full control for all internal users
S&C Southwest Power	138	Full control for all internal users
Tennessee Land Surveyors (Nashville)	149	Full control for all internal users
Warwick Systems & Technology	142	Full control for all internal users

Name	ID	Owner	Pe
Jeff Smith	7	A&A Consulting (AEC)	Fu
Ross Connors	21	A&A Consulting (AEC)	Fu
Tim Moore	22	A&A Consulting (AEC)	Fu

Figure 40: The "Contact persons" value list used as a sublist for the "Customers" value list.

Permissions

By selecting a value list item and clicking the **Permissions...** button, 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

An object receives automatic permissions when a value with automatic permissions is added to the object metadata.

You can activate the automatic permissions by value, value list, object type, or class by clicking **Permissions...** in the **Value List Contents** dialog and then selecting the **Automatic Permissions** tab. For more information, see Automatic Permissions for Value List Items.

In this chapter

- Adding Values to a Value List
- Automatic Permissions for Value List Items

Adding Values to a Value List

1. Open M-Files Admin.

2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Expand **Metadata Structure (Flat View)**.

6. Click **Value Lists**.

☑ The **Value Lists** list is opened in the right pane.

7. 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.

8. Click the **New Item** button.

☑ A new value titled **New Item** is added to the selected value list.

9. 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.

10. Optional: Click **Permissions** to specify the users who may see this value list item.

ⓘ For detailed instructions, see Value List Permissions and Automatic Permissions for Value List Items.

11. 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 more instructions, see Changing the Icon of a Value in a Value List.

12. Optional: Repeat steps from 6 to 9 to add another value.

13. 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 a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Expand **Metadata Structure (Flat View)** and then select **Value Lists**.

   ✓ The **Value Lists** list is opened in the right pane.

6. Optional: To show the built-in value lists, click **Show All Value Lists**.

7. Right-click a value list that you want to edit and select **Contents** from the context menu.

   ✓ The **Value List Contents** dialog is opened.

8. Select a value from the list and click the **Change Icon** button.

   ✓ The **Change Icon** dialog is opened.

9. Either:

   a. Select an icon from the list of icons.

      or

   b. Click **Browse** to browse for a different icon file and then select an icon from the list of icons.

10. Click **OK** to change the icon and close the **Change Icon** dialog.

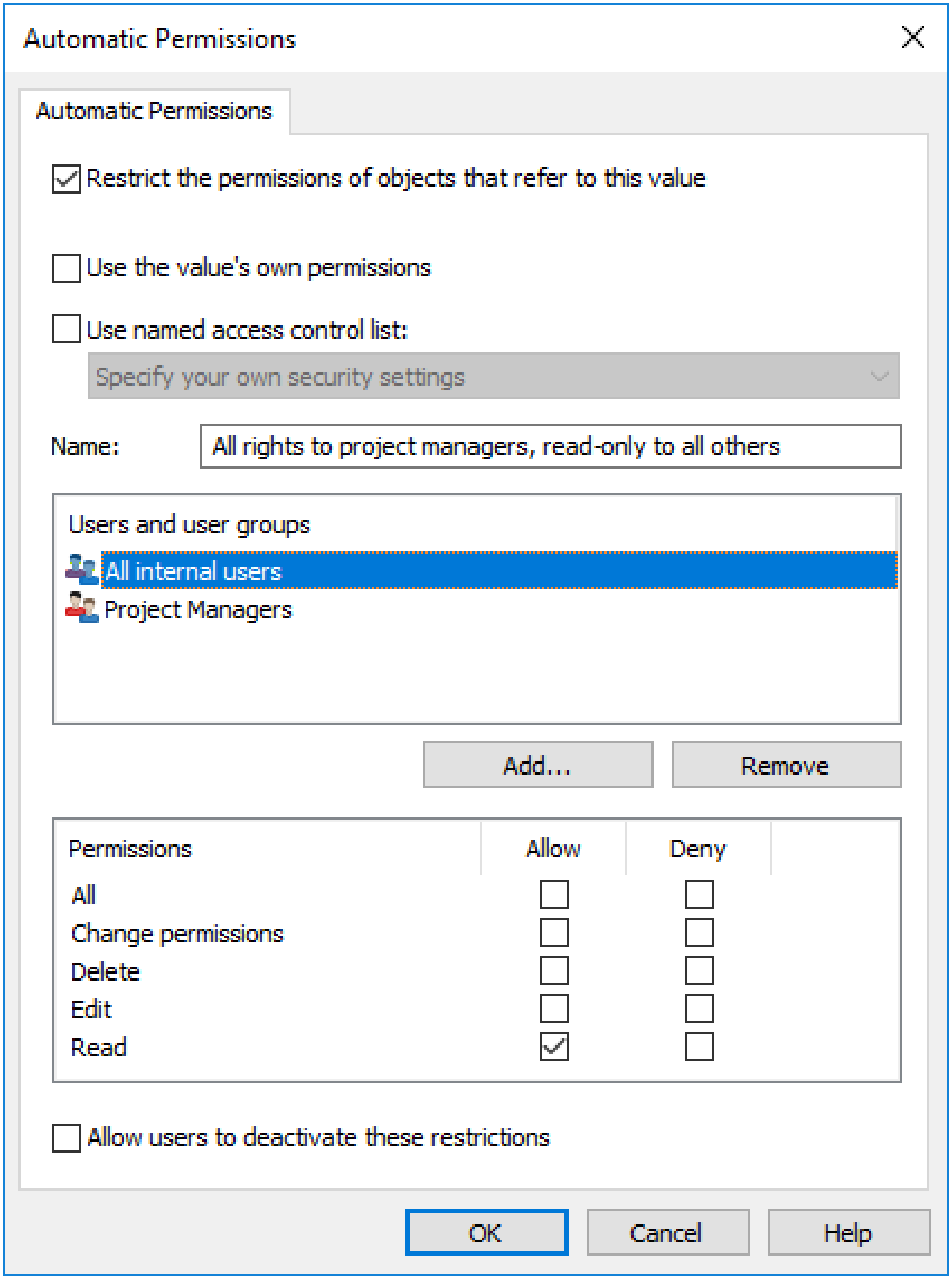
11. Repeat the steps from 6 to 8 to change the icon for another value.

12. Click **Close** when you are done to close the **Value List Contents** dialog.

Automatic Permissions for Value List Items

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 to the object metadata.

Note: Micro Focus IDOL and Smart Search: If more than four automatic ACL sources control the permissions of an object, only administrators can see it in search results.



Automatic Permissions

☑ Restrict the permissions of objects that refer to this value

□ Use the value's own permissions

□ Use named access control list:

Specify your own security settings

Name: All rights to project managers, read-only to all others

Users and user groups

- All internal users
- Project Managers

Permissions	Allow	Deny
All	□	□
Change permissions	□	□
Delete	□	□
Edit	□	□
Read	☑	□

□ Allow users to deactivate these restrictions

Figure 41: 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 project plan inherits the permissions of the project that is added as a value to the metadata of the project plan. For example, the user has defined permissions for the project *House project Haven* that allow access for the project manager and project group only. When this project is added to the metadata of a project plan, the same permissions are granted to the plan.

Note: Automatic permissions are not inherited indirectly. For example, we can have an object "Hugh Brent" that inherits automatic permissions from 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 Object Permissions. Also refer to the specification of pseudo-users in Pseudo-users.

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 through this value, so that the users can delete the preset automatic permissions if necessary.

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.

Note: The value-specific settings always have priority over the settings made at value list and object type level.

Enabling Automatic Permissions for a Value List Item

1. Open M-Files Admin.

2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)** and then select **Value Lists**.

   ✓ The **Value Lists** list is opened in the right pane.
6. Right-click a value list that you want to edit and select **Contents...** from the context menu.

   ✓ The **Value List Contents** dialog is opened.
7. Select a value list item that you want to edit and click the **Permissions...** button.

   ✓ The **Permissions** dialog is opened.
8. On the **Automatic Permissions** tab, check the **Restrict the permissions of objects that refer to this value** check box.
9. 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** check box.
Use an existing named access control list as automatic permissions	Check the **Use named access control list** 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 select the appropriate **Allow** or **Deny** check boxes on the **Permissions** list.

10. Optional: Select the **Allow users to deactivate these restrictions** check box if you want to give users the option to disable the automatically set permissions and employ user-defined permissions instead.
11. Click **OK** to close the **Permissions** dialog.
12. 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 a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)**.
6. Select **Property Definitions**.

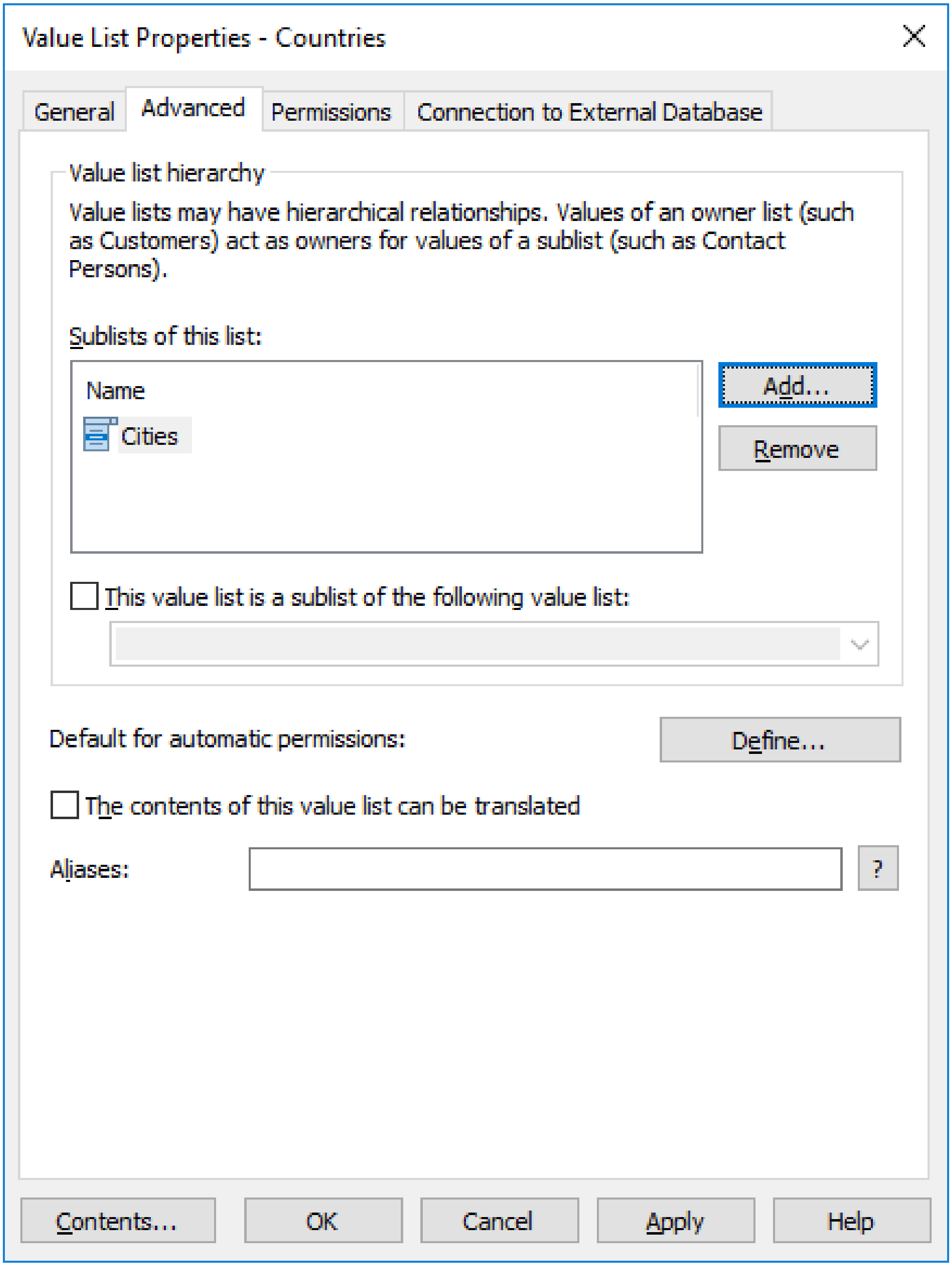
You can see which properties have automatic permissions enabled in the *Automatic Permissions* column of the listing area.

Advanced Value List Properties

Value list hierarchy

Value lists can have two types of hierarchical relationships:

- Internal hierarchies withing individual value lists
- Hierarchies between separate value lists



Value List Properties - Countries

Value list hierarchy

Value lists may have hierarchical relationships. Values of an owner list (such as Customers) act as owners for values of a sublist (such as Contact Persons).

Sublists of this list:

Name
Cities

□ This value list is a sublist of the following value list:

Default for automatic permissions:

□ The contents of this value list can be translated

Aliases:

Figure 42: 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 a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Expand **Metadata Structure (Flat View)** and then select **Value Lists**.

✓ The **Value Lists** list is opened in the right pane.

6. Double-click the value list that you want to edit.

✓ The **Value List Properties** dialog is opened.

7. Open the **Advanced** tab, and check **This value list is a sublist of the following value list** check box.

8. Using the drop-down menu, select the **Same list (defines a value list with internal hierarchy)** option.

9. Click the **Contents...** button.

✓ The **Value List Contents** dialog is opened.

10. Select an item on the list for which you want to create a subitem and click **New Subitem**.

11. Type in an appropriate name for the new item.

ⓘ You can also rename the item later by selecting the item in the list and clicking **Rename**.

12. Optional: If you want to create additional subitems, repeat the steps 10 and 11.

13. Click **Close** when you are ready.

The value list items that you have just created are added 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 a connection to M-Files server.

3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)** and then select **Value Lists**.

   ✓ The **Value Lists** list is opened in the right pane.

6. Double-click the value list that you want to define as a sublist of a higher-level list.

   ℹ Make sure that the property definition using this value list uses automatic filtering. For more information, see Property Definitions.

   ✓ The **Value List Properties** dialog is opened.

7. Open the **Advanced** tab, and check **This value list is a sublist of the following value list** check box.
8. Using the drop-down menu, select the value list that you want to set as the owner of this value list.
9. Click **OK** to save your changes and close the **Value List Properties** dialog.
10. 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.

11. In the upper list, select the owner item for which you want to add a subitem.
12. Next to the lower list, click **New Item**.

    ✓ A new value list item is added to the lower list.

13. Type in an appropriate name for the new subitem.

    ℹ You can also rename the item later by selecting the item in the list and clicking **Rename**.

14. Optional: If you want to create additional subitems, repeat the steps from 11 to 13.
15. 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.
Default for automatic permissions

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.

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

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.

Value list aliases

Using the **Aliases** field, you can define an alias for the value list. For more information, see Associating the Metadata Definitions. Use semicolons (;) to separate many aliases.

When automatic aliases are in use and you write a name on the **General** tab, the **Aliases** field on the **Advanced** tab is automatically filled in. The alias has the format <*predefined prefix*>.<*name*>. Configure automatic aliases for your vault in Advanced Vault Settings.

Value List 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.

Editing Permissions

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click a node that contains items that you want to edit.

   Permission settings are available for these items:

   - **Users**
   - **User groups**
   - **Metadata Structure (Flat View)** > **Object types**
   - **Metadata Structure (Flat View)** > **Value lists**
   - **Metadata Structure (Flat View)** > **Property definitions**
   - **Metadata Structure (Flat View)** > **Classes**
   - **Metadata Structure (Flat View)** > **Class groups**
   - **Workflows**
   - **Named access control lists**
6. Select an item in the listing area.
7. Right-click the item and click **Properties**.
8. Open **Permissions**.
9. In **Users and user groups**, select the user or user group whose permissions to change.

   If the user or user group is not on the list, click **Add**.
10. Specify the permissions for the selected user or user group.

Allow: Enable this to explicitly give the permission to the selected user or user group.

Deny: Enable this to explicitly deny the permission from the user or user group.

The **Deny** setting is normally used to specify an exception to an **Allow** setting. For example, when John Doe is part the group **HR Managers**, you can set **Allow** for the group and **Deny** for John Doe.

You can also leave both settings unselected.

11. Repeat steps 9 and 10 for the rest of the permissions.
12. Click **OK**.

Connections to External Databases for Value Lists

You can set M-Files to update value lists to and from an external database.

This section tells you how to set value lists to use an application connection to an external database. To use the legacy database connection, see the section "Using the Legacy Database Connection for Value Lists".

Prerequisites

Take note of this important information before you start the setup:

- Before you set up an application connection to an external database, you must have an external object type connector installed and enabled.
  - The connector must support the application connection. You can use M-Files OLE DB External Object Type Connector, which is normally installed to the vault but is disabled.
    - To use the connector, a license is not necessary.
    - For instructions on adding connectors and managing vault applications, see Adding a Connector and Installing and Managing Vault Applications.
  - If you use the Ground Link service, the connector must be enabled on the Ground Link proxy. For instructions, see Configuring External Object Types over Ground Link. If you use a local service, the connector must be enabled in the vault.
- If you use replication and application connection to an external database service, you must configure the connection separately for each vault in the replication scheme. Make sure that the necessary configuration changes are also made to each vault. We also recommend that you read the section **Replication of External Objects** of the document Replication and Archiving - User's Guide.
- It is not possible to include the configuration for **External Object Type Connector** to replication packages.
- In `SELECT FROM` statements, the columns are selected in order of appearance. There is no relation between column and property names, which is why the order must be the same in the `SELECT FROM` and `INSERT INTO` statements, and `SELECT FROM` and `UPDATE` statements. Also, columns not used in the `INSERT INTO` and `UPDATE` statements must always be listed last in the `SELECT FROM` statement.

To use a connection to external database and to open the service configuration:

1. Open M-Files Admin and go to a vault.

   a) Open M-Files Admin.

   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.

2. Expand **Metadata Structure (Flat View)**.

3. Click **Value Lists**.

   The value list listing is opened in the right pane.

4. In the right-pane listing, double-click the value list.

   The **Value List Properties** dialog is opened.

5. Go to the **Connection to External Database** tab and enable the option **Use a connection to an external database to import and modify objects that reside in the external database**.

6. Select **Application connection**.

7. In **Service**, select the service.

Option	Description
`M-Files OLE DB at vault` ***`<name of the vault>`***	Select this option to use the local service.
`M-Files OLE DB from Ground Link proxy` ***`<name of the Ground Link proxy>`***	Select this option to establish the connection with a remote service through Ground Link.

   The services that have the `(OK)` suffix, have a configuration for the value list.

   Information of the service configuration with possible errors is shown.

8. Click **Configure**.

   The **External Object Type Connector** dialog is opened.

To specify the connection settings and to get the source columns:

9. Expand **Service-Specific Settings** > **Connection to External Database**.

10. In **Provider**, select the provider for the external database connection.

   Microsoft OLE DB Driver for SQL Server.

   Note: The list of providers shows all the available providers on the server machine that runs the external object type connector. Thus, it can include providers that cannot be used in external database connections.

   The syntax of the connection string is different for each Object Linking and Embedding Database (OLE DB) supplier used for establishing the connection to the external database. If Open Database Connectivity (ODBC) is necessary to create the connection, the data store must be accessed over OLE DB and ODBC. For a list of recommended providers, see Provider Recommendations for External Database Connections.

11. Optional: If you selected **Custom provider (manual configuration)**, in **Custom provider**, specify the provider.

12. Under **Connection to External Database**, complete one of these steps:

Option	Description
Specify the other settings.	The correct values are different for each provider and external database. For more information, select a setting and see the **Info** tab.
In Advanced Options, enter the connection string.	Use this option if it is not possible to use the other settings with the selected provider. When you enter the connection string, make sure that all values are correctly enclosed and the connection string has the necessary formatting.

13. Optional: Under **Optional SELECT Statements**, define the settings.

Note: The application connection does not support the **Connections to External Databases** settings in the **Advanced Vault Settings** section in M-Files Admin. To use these settings, define them here.

14. Under **Service-Specific Settings**, in **SELECT Statement**, write the SELECT statement for getting source columns from the external database.

Examples of SELECT statements:

```
SELECT CustomerNumber, CustomerName FROM Customer

SELECT ID, Name + ' ' + Department FROM Company

SELECT ID, Name, CustomerID FROM Contacts

SELECT * FROM Customer
```

Tip: You can write a multi-line statement.

15. Click **Save**.

16. Optional: To configure a remote service:
    a) Click **Apply**.

    ✓ The **Enter Password** dialog is opened.

    b) Enter the password that is defined in the Ground Link proxy configuration.
    c) Click **OK**.

17. To authenticate the common user, open the **Dashboard** tab and click **Authenticate**.

✓ The **Log In** dialog is opened.

18. Enter the common user credentials and click **Log In**.

Note: The ODBC driver does not support all special characters. If your connection uses ODBC, the values that contain special characters must be enclosed in curly brackets. The correct format is `{username or password}`.

19. In the dialog that is opened, click **OK**.

20. Click **Save** to get the source columns.

    a) Optional: To configure a remote service, repeat step 16.

Note: You cannot save the configuration if there are no changes.

✓ The dialog closes and the configuration refreshes. On the **Configuration** tab, the **Column Mappings** section shows the source columns that your SELECT statement returned from the external database.

To map the source columns with M-Files properties:

21. On the **Configuration** tab, go to **Column Mappings** and expand a source column node.

22. In **Mapping Type**, specify how the source column is mapped to M-Files.

- To map a source column as the external ID, select **Object ID**.
- To map the source column as the name of the value list item, select **Name or Title**.
- To map the the source column as the ID of the owner value list item, select **Owner**.
- To map the the source column as the ID of the value list's parent item, select **Parent**.

For more information on value list hierarchy, see Value list hierarchy.

23. Optional: If the **Mapping Type** is **Name or Title**, specify the setting **Use in Insert Operation** and define the related statements.

If you want to...	**Complete the following steps:**
Allow read-only access	Set the **Use in Insert Operation** setting to **No**. Do not specify the statements in this table.
Allow users to create but not update or delete information	**a.** Set the **Use in Insert Operation** to **Yes**. **b.** Under **Service-Specific Settings**, in **INSERT INTO statement**, write the two statements in this table.

Statement	**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 = ?`

Statement	Definition	Examples

INSERT INTO	When you create a new value list item 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 Microsoft SQL Server databases, set the type of the ID column as identity. If the external database cannot produce new ID values, the INSERT INTO statement cannot be used.
		`INSERT INTO`
		`Customers( CustomerName )`
		`VALUES( ? )`
		
		`INSERT INTO`
		`ContactPersons( Name,`
		`CustomerID )`
		`VALUES( ?, ? )`

Get ID 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 = ?`

24. Repeat the steps from 21 to 23 for all the necessary source columns.

To take the configuration into use:

25. Under **General Settings**, set **Enabled** to **Yes**.

    Tip: You can enable and disable the external database connection also with the **Disabled** check box on the **Connection to External Database** tab of the **Value List Properties** dialog.

    If the connection is disabled, information between the vault and the external database is not synchronized.

26. Optional: To configure a remote service:
    a) Click **Apply**.

    The **Enter Password** dialog is opened.

    b) Enter the password that is defined in the Ground Link proxy configuration.

c) Click **OK**.

27. Click **OK** to close the **Value List Properties** dialog.

The value list is now updated to and from the external database.

In this chapter

- Using the Legacy Database Connection for Value Lists
- Refreshing External Value Lists
- Provider Recommendations for External Database Connections

Using the Legacy Database Connection for Value Lists

Before you start, take note of this information:

- In `SELECT FROM` statements, the columns are selected in order of appearance. There is no relation between column and property names, which is why the order must be the same in the `SELECT FROM` and `INSERT INTO` statements, and `SELECT FROM` and `UPDATE` statements. Also, columns not used in the `INSERT INTO` and `UPDATE` statements must always be listed last in the `SELECT FROM` statement.
- In the `SELECT` statement used to get the ID of the records, `WHERE` must refer to the first column of the `SELECT FROM` statement.

1. Do the steps from 1 to 5 in Connections to External Databases for Object Types.

2. In M-Files Admin, in the **Connection to External Database** tab of the **Value List Properties** dialog, select **Legacy database connection**.

3. Click **Configure**.

✓ The **Configure Connection to External Database** dialog is opened.

4. Click the **Define** button next to the **OLE DB connection string (from server)** field.

The syntax of the connection string is different for each Object Linking and Embedding Database (OLE DB) supplier used for establishing the connection to the external database. If Open Database Connectivity (ODBC) is necessary to create the connection, the data store must be accessed over OLE DB and ODBC. For a list of recommended providers, see Provider Recommendations for External Database Connections.

Note: M-Files Admin only displays OLE DB providers that are available on the computer running M-Files Admin. If your M-Files Server resides on a different host, make sure that the selected OLE DB connection string works from the computer running M-Files Server as well.

✓ The **Data Link Properties** dialog is opened.

5. On the **Provider** tab, select **Microsoft OLE DB Driver for SQL Server** from the list and click **Next >>**.

Other providers can have different options on the **Connection** and **Advanced** tabs. The **All** tab contains all the available connection properties as a name–value table.

Note: We do not recommend the use of Microsoft Access Database Engine Redistributables to import value lists or object types from an Excel file.

☑ The **Connection** tab of the **Data Link Properties** dialog is opened.

6. To the **Select or enter a server name** field, write the name of your Microsoft SQL Server.

7. In the **Enter information to log on to the server** section, select:

a. **Windows Authentication**: Select this option to use a Microsoft Windows account for logging in. In this case, the connection uses the credentials that are used for running the M-Files Server service.

or

b. **SQL Server Authentication**: Select this option to use a Microsoft SQL Server login. Enter the credentials in the **User name** and **Password** fields, and select the **Allow saving password** check box.

Note: The ODBC driver does not support all special characters. If your connection uses ODBC, the values that contain special characters must be enclosed in curly brackets. The correct format is `{`*`username or password`*`}`.

8. For the **Select the database** section, complete one of these steps:

a. Use the drop-down menu to select the database on the specified server.

or

b. Enter a database name to the **Attach a database file as a database name** field and click the **...** button to select a Microsoft SQL Server Database (MDF) file.

9. Optional: Click **Test Connection** to make sure that your database connection operates correctly.

10. Optional: On the **Advanced** tab, define a timeout period for the database connection.

11. Click **OK** to close the **Data Link Properties** dialog.

☑ The connection string is added to the **OLE DB connection string (from server)** field.

12. In the **Configure Connection to External Database** dialog, to the **SELECT statement** field, enter the SELECT statement for getting source columns from the external database.

Examples of SELECT statements:

```
SELECT CustomerNumber, CustomerName FROM Customer

SELECT ID, Name + ' ' + Department FROM Company

SELECT ID, Name, CustomerID FROM Contacts

SELECT * FROM Customer
```

13. Click **Refresh Columns** to get the source columns.

☑ The **Columns** listing shows correspondences between columns retrieved from the external database (**Source Column**) and M-Files properties (**Target Property**).

14. Map the **Source Column** properties with properties in your M-Files vault (listed in the **Target Property** column).

Note: When you want to map multiple values to a property of the **Choose from list (multi-select)** data type, the values must be recorded on their own rows in the external database. For example, if you want to map multiple values to the **Industry** property, the values must be recorded like this:

ID	Customer name	City	Industry	Active
ABC-123	ESTT Corporation	New York	100	1
ABC-123	ESTT Corporation	New York	101	1
ABC-123	ESTT Corporation	New York	108	1

In this case, however, data can only be read from, not recorded to the external database.

15. Select the check boxes in the **Insert** column and define the two statements below the **Columns** listing.

If you want to...	Complete the following steps:
Allow read-only access	Do not select the check boxes and leave the statements empty.
Allow users to create but not update or delete information	**a.** Select the check boxes in the **Insert** column for the necessary properties. **b.** Click the **Default** button next to the INSERT INTO and SELECT statement fields. You can also enter your statements to the fields.

The table below explains the use of the two statements mentioned above.

Statement	Definition	Examples

INSERT INTO	When you create a new value list item 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 Microsoft SQL Server databases, set the type of the ID column as identity. If the external database cannot produce new ID values, the INSERT INTO statement cannot be used.
		`INSERT INTO Customers( CustomerName ) VALUES( ? )`
		`INSERT INTO ContactPersons( Name, CustomerID ) VALUES( ?, ? )`

Statement	Definition	Examples
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.	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.

16. Click **OK** to close the **Configure Connection to External Database** dialog.

17. Optional: Select the **Disabled** check box to temporarily disable the external database connection.

> ℹ If the connection is disabled, information between the vault and the external database is not synchronized.

18. Click **OK** to close the **Object Type Properties** dialog.

The object type is now updated to and from the external database.
Refreshing External Value Lists

There are two types of refresh operations for external value lists:

- full refresh
- quick refresh

A full refresh detects new items, compares and updates existing items, and deletes items that have disappeared from the external database. A quick refresh, by default, only detects new items in the external database. It does not compare existing items. It does not delete items, either, because undeleting them would require a full refresh.

The quick refresh operation is notably quicker than the full refresh operation. For reference, the full refresh operation for 120,000 items takes about two minutes, while the quick refresh operation finishes in about seven seconds. For simple value lists, refreshing data is fast even with large amounts of data and therefore a full refresh is always used. This guarantees up-to-date data.

Refreshing external value lists manually

External value lists can be manually refreshed with the metadata card in the classic M-Files Desktop and the classic M-Files Web. Select a property that uses an external value list and click the **Refresh** icon (↻).

If you try to refresh an external value list at the same time with M-Files Server, the operation started by you begins after the one started by M-Files Server.

Refreshing external value lists with M-Files Admin

To start or stop the full refresh operation for an external value list in M-Files Admin, right-click the value list in **Metadata Structure (Flat View)** and click **Refresh Now**. This gets the up-to-date column data from the external database.

The full refresh operation is also started when you edit the value list definitions in M-Files Admin. If you update the value list definition before the previous refresh operation has completed, M-Files starts the operation again.

Automatic refresh operations and configuration options

The quick refresh operation is started automatically if an external value list is requested by a client (for instance, the metadata card containing a property that uses an external value list is viewed) and if the latest refresh was executed more than 15 minutes ago.

A full refresh operation is automatically triggered instead of a quick refresh operation if an external value list is requested by the client and if a full refresh has not been performed within the last 25 hours.

For configuration options available for refreshing external value lists automatically, see the document Default Refresh Logic and Configuration Options for External Value Lists and Object Types.

Automatic property values ignored during refresh operations

When M-Files updates objects to and from an external database, it compares object properties in the external database to the ones in the vault. If M-Files finds differences in the properties, it updates the objects. During the comparison, properties with an automatically calculated value are ignored, which causes these scenarios:

- If all the object's property values to be updated to or from an external database are set to have an automatically calculated value in M-Files, the object is not updated.
- If the refresh operation creates an object in M-Files, all property values of the object are filled with the values from the external database. This includes properties that are set to have an automatically calculated value.
- If the refresh operation updates the object's properties in M-Files, all the object's property values to be updated get their value from the external database. This includes properties that are set to have an automatically calculated value.

Provider Recommendations for External Database Connections

The table below lists the recommended OLE DB providers to be used for an external database connection (see Connections to External Databases for Value Lists).

Database	Provider
Microsoft SQL Server Azure SQL Server Azure SQL Managed Instance	Microsoft OLE DB Driver for SQL Server (`MSOLEDBSQL`) **Note:** Using the following, deprecated providers is not recommended: • Microsoft OLE DB Provider for SQL Server (`SQLOLEDB`) • SQL Server Native Client OLE DB Provider (`SQLNCLI`)

Database	Provider
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: M-Files Server only supports 64-bit drivers for External Object Types and External Value Lists. Make sure that you download and install 64-bit versions of custom drivers, for example MySQL.

Property Definitions

Property definitions are used for determining properties associated with classes. A property definition specifies the property name (which should naturally be as descriptive as possible) and the 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). 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.

In this chapter

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**.

Property definition data types

Text	Any typed text, for instance, a heading. This type of property accepts a maximum of 100 characters entered in the user interface. More characters can be entered with the M-Files API but values of over 100 characters will be cut and the full value is lost.
Text (multi-line)	Any typed text. The text can have multiple lines. This type of property accepts a maximum of 10,000 characters entered in the user interface. More characters can be entered with the M-Files API, but this may cause the value to not be shown in its entirety, as well as other unwanted behavior in the user interface. For instance, attempting to insert property values containing more than 10,000 characters into a Microsoft Office document causes an error.
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 enter a time.
Timestamp	You can select a date and time.
Number (integer)	You can enter the desired integer. The value can be anything between -2,147,483,648 and 2,147,483,647.
Number (real)	You can enter the desired real number. The value can be anything between -1,79 x 10^{308} and 1,79 x 10^{308}. You can enter the value in the format `XEY`, where `X` is the number to be multiplied, `E` represents the base number 10 and `Y` is the exponent. For instance, entering `–12E3` would result in the value `–12,000`. **Note:** This data type can present a wider range of numbers than **Number (integer)** but at the cost of precision. Consequently, **Number (real)** should not be used when the number value has to be absolutely accurate, such as with values representing money. In those cases, it is recommended to use **Number (integer)** as the data type.

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

You can set the values of a value list based property to be filtered with another property. This causes the values to be dynamically filtered with the user's choices on the metadata card.

Example: The user adds the properties Customer and Contact Person on the metadata card. The value that the user selects for Customer causes the values available for Contact Person to only contain contact persons of the selected customer. The Customer property uses the Customers value list and Contact Person the Contact Persons value list. The Contact Persons value list is set to be filtered by the Customer property.

You can also select an automatic filter to let M-Files use the best filter for the property. For example, two-way filtering between ZIP codes and cities can be used in a user-friendly manner: On the metadata card, you can select a ZIP code first, and M-Files selects a suitable city from the list automatically. If you select the city first, M-Files filters the available ZIP codes automatically according to the city.

Show only filtered values on the metadata card

Enable this setting to make sure that the value list on the metadata card is strictly filtered with the property selected in **Filter the list by using the value of the following property**. Otherwise, the list can also contain values filtered on the basis of other properties that 1) are in the object's metadata and 2) show values of the same list.

Example: The Project Manager property shows values of the Employees value list and is filtered with the External Project property. A Project object contains a value for the properties Project Manager, External Project, and Internal Project. If this setting is enabled, only managers for external projects can be selected for Project Manager. Otherwise, managers for external and internal projects can be selected.

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

To use the automatic permissions through a property, you must allow this in the property definition's properties. For the Class property definition, the automatic permissions are active by default.

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.

Allow searching for objects by this property

If you disable this option, searches based on the values of the selected property do not generate any results. However, the property can still be shown in the list of additional property conditions. If you enable this option and use the **Do not search for old object versions** suboption, users can only search for the latest versions of objects on the basis of the values of this property.

If you think the property is a relevant search criterion, this option should be enabled. Otherwise, it is best to leave it disabled to allow the search to perform optimally.

Aliases (Advanced tab)

In the **Advanced** tab, you can specify an alias for the property definition. For more information, see Associating the Metadata Definitions. Use semicolons (;) to separate many aliases.

When automatic aliases are in use and you write a name on the **General** tab, the **Aliases** field on the **Advanced** tab is automatically filled in. The alias has the format <*predefined prefix*>.<*name*>. Configure automatic aliases for your vault in Advanced Vault Settings.

Creating a New Property Definition

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)** and then select **Property Definitions**.

   ✓ The **Property Definitions** list is opened in the right pane.
6. Click **New Property Definition...** on the task pane.

   ✓ The **Property Definition Properties** dialog is opened.
7. 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.
8. 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.

   > **Note:** You cannot change the data type if the vault has at least one object that uses the property in its metadata. However, you can change the data type **Choose from list** to **Choose from list (multi-select)** and **Text** to **Text (multi-line)** or vice versa. If you change **Choose from list (multi-select)** to **Choose from list**, only the first value is kept in the metadata of existing objects. If you change **Text (multi-line)** to **Text**, the value in the metadata of existing objects can be cut if it is too long.
9. 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.
10. Optional: If you chose **Choose from list** or **Choose from list (multi-select) as the data type,** do the steps from 10.a to 10.e:

    a) In **Show values from the following list**, select the value list from which a value is to be chosen for the property.

    ⓘ You can also click **Filter** and set the conditions to filter the values available in the value list.

    b) Optional: In **Filter the list by using the value of the following property**, you can 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.

    c) Optional: Enable **Show only filtered values on the metadata card** to make sure that the value list on the metadata card is strictly filtered with the property selected in **Filter the list by using**

the value of the following property. For more information, see Show only filtered values on the metadata card.

d) Optional: Use the **Sort values in the list in the following order** drop-down menu to select the sorting order for the values.
e) Optional: Enable **Enable automatic permissions via this property** to allow automatic permissions for this property.

   For more information, see Automatic Permissions for Value List Items.

11. 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.

12. Optional: Check the **Allow this property to be used as a grouping level in views** 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.

13. Optional: Check the **Allow searching for objects by this property** check box to allow the values of this property to be used as criteria for searching for objects and object versions.

   a) Optional: Select the **Do not search for old object versions** check box to allow the values of this property to be used as criteria for searching for the latest versions of objects only.

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.

Property Definition 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, see New Class) and in automatically including metadata in document content (for more information, see Add M-Files Property).

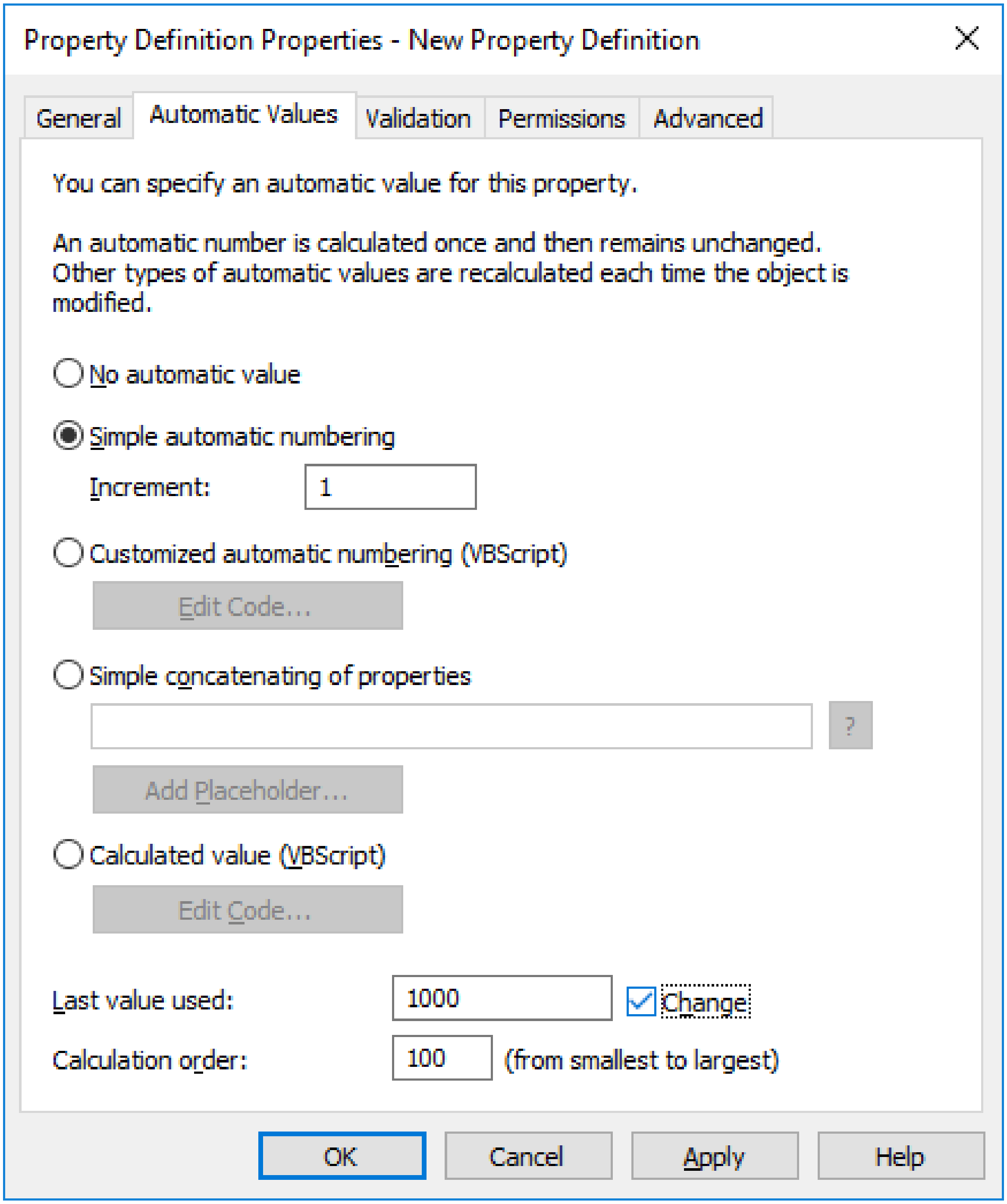
> **Warning:** VBScript execution errors can cause new object versions to not be created. They can also cause external object type synchronization to not complete. This prevents updates also to other objects of the same object type. VBScript execution errors are recorded in the Windows event log.

Automatic numbers and values

A property can have an automatic number or an automatic value.

An **automatic number** is calculated once and it does not change. Ths is useful, for example, in different company's internal processes and record-keeping.

An **automatic value** is calculated always when a new object version is created. It can contain other properties, usually by concatenating two or more properties. For example, if a document name (automatic value) is defined as *Class (Customer)*, the document name can get the value *Proposal (ESTT)*. If the automatic value is created with the class and customer name *(Proposal (Customer A))*, the automatic value changes to *(Proposal (Customer B))* when another customer is selected.



Property Definition Properties - New Property Definition

You can specify an automatic value for this property.

An automatic number is calculated once and then remains unchanged. Other types of automatic values are recalculated each time the object is modified.

○ No automatic value

● Simple automatic numbering

Increment: 1

○ Customized automatic numbering (VBScript)

○ Simple concatenating of properties

○ Calculated value (VBScript)

Last value used: 1000 ☑ Change

Calculation order: 100 (from smallest to largest)

Figure 43: 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 in the **Increment** field. The default value is one (1).

Customized automatic numbering (VBScript)

Generates an automatic number that can contain letters, numbers, or both. Creating a customized automatic number is specified in more detail with M-Files API and generic features of VBScript.

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 Available VBScript Variables.

The desired custom value is assigned to the `Output` variable, for example `Output = "Automatic value"`. For more information on specifying customized automatic numbering, see Specifying an Automatic Property Value Using VBScript.

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.

Besides the ID, you can also add the placeholders using aliases. To specify an alias placeholder, use the syntax `%PROPERTY_{Property.Definition.Alias}%`. For more information on defining aliases, see Assigning Aliases for Metadata Definitions.

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*.

Alternatively, you can add indirect placeholders using aliases. In the previous example, the syntax with aliases would be `%PROPERTY_{PD.Customer}.PROPERTY_{PD.Country}%` , where *PD.Customer* is the alias for the *Customer* property definition and *PD.Country* is the alias for the *Country* property definition.

Calculated value (VBScript)

Creating an automatic value can be specified in more detail with M-Files API and generic features of VBScript.

These 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 Available VBScript Variables.

The custom value is assigned to the `Output` variable, for example `Output = "Automatic value"`. For more information on specifying calculated values, see Specifying an Automatic Property Value Using VBScript.

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.

Recalculate

The **Recalculate** command is available in M-Files Admin task area (or by right-clicking a property in the **Property Definitions** list and selecting **Recalculate**) when a property with an automatic value is selected. You can choose between recalculating empty values or recalculating all values.

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** field, 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 Using Document Templates and New Class.

In this chapter

- Specifying an Automatic Value for a Property
- Specifying an Automatic Property Value Using VBScript

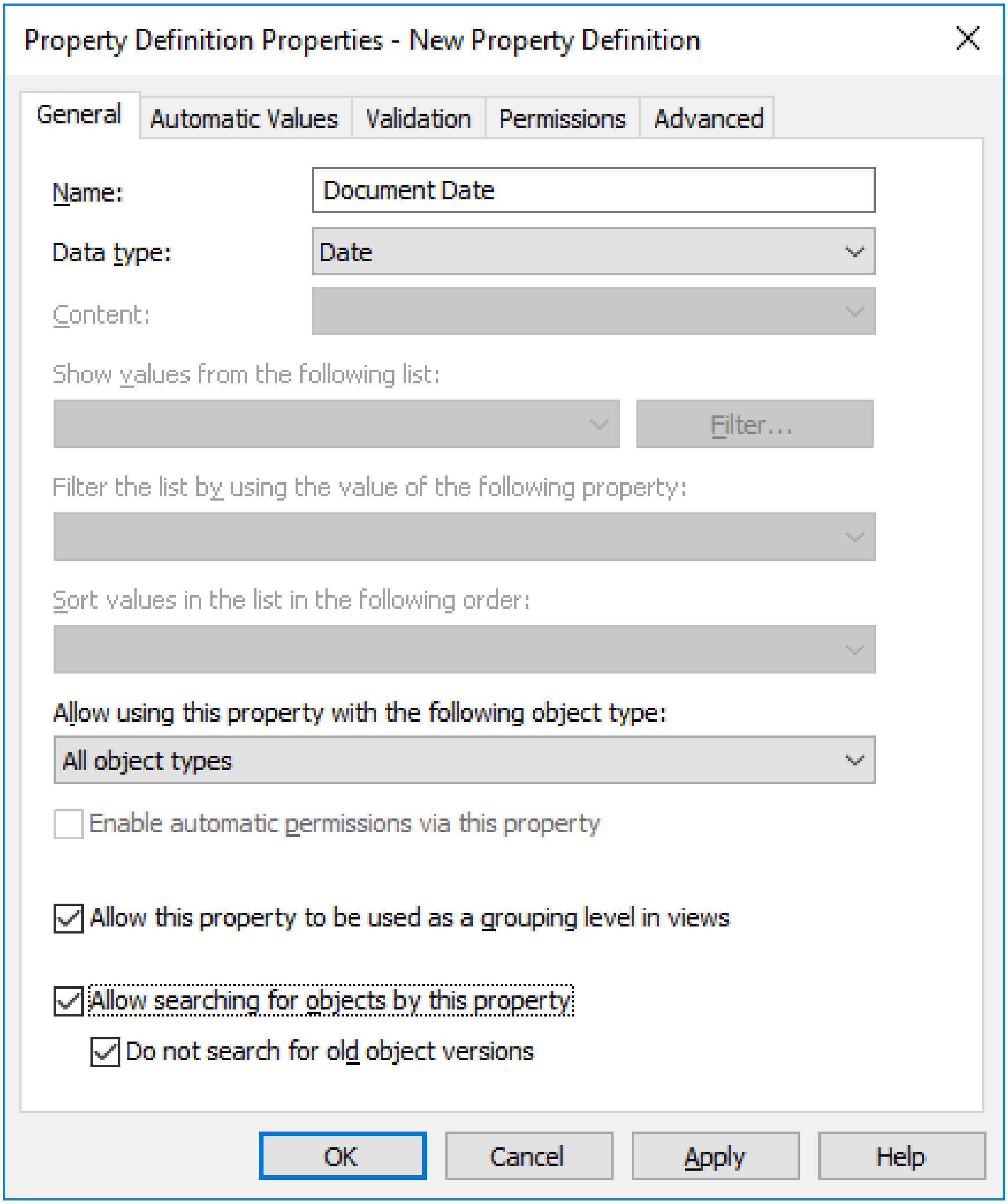
Specifying an Automatic Value for a Property

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)** and then select **Property Definitions**.

   ✓ The **Property Definitions** list is opened in the right pane.

6. Double-click the property definition that you want to edit.

   ✓ 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

☑ Allow searching for objects by this property

☑ Do not search for old object versions

7. 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.

If you want to	Do the following
	Note: For more information, see Specifying an Automatic Property Value Using VBScript.
Specify a combination of text and property placeholders as an automatic property value.	Select the **Simple concatenation 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. **Note:** For more information on placeholders, see Simple concatenation of properties.
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.

8. 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).
9. 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.

10. 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 with M-Files API and generic features of VBScript ("Microsoft Visual Basic Scripting Edition"). This section gives instructions on how to use VBScript with automatic values. For the VBScript user's guide and language reference, see the VBScript MSDN article.

Note: When you develop new extensions or edit existing ones, we recommend that you replace VBScript content with Vault Application Framework (VAF) compatible code for future compatibility. For more information on the benefits of VAF development over VBScript, refer to The Vault Application Framework in M-Files Developer Portal.

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 use the property values and basic information of the same or another object with these VBScript variables:

- `CurrentUserID`
- `DisplayID`
- `LastUsed`
- `MFScriptCancel`
- `ObjVer`
- `Output`
- `PropertyDef`
- `PropertyValues`
- `Vault`
- `VaultSharedVariables`

For the variable descriptions, see Available VBScript Variables.

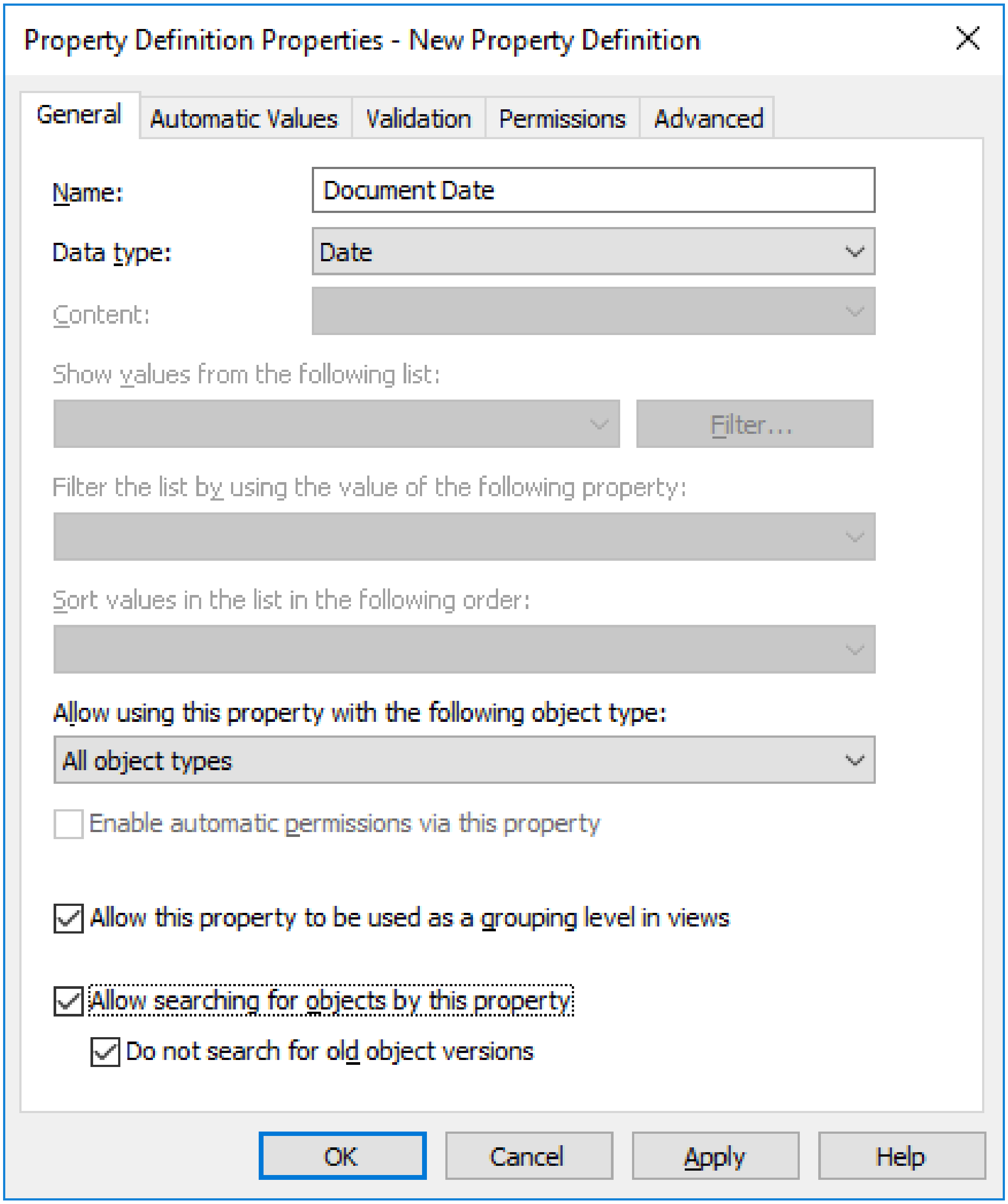
Note: Some property definitions are not shown when using the `PropertyValues` variable in scripts (see Property definitions not shown for scripts).

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 a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)** and then select **Property Definitions**.

   ✓ The **Property Definitions** list is opened in the right pane.
6. Double-click the property definition that you want to edit.

   ✓ The **Property Definition Properties** dialog is opened.



Name: Document Date

Data type: Date

Content:

Show values from the following list:

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

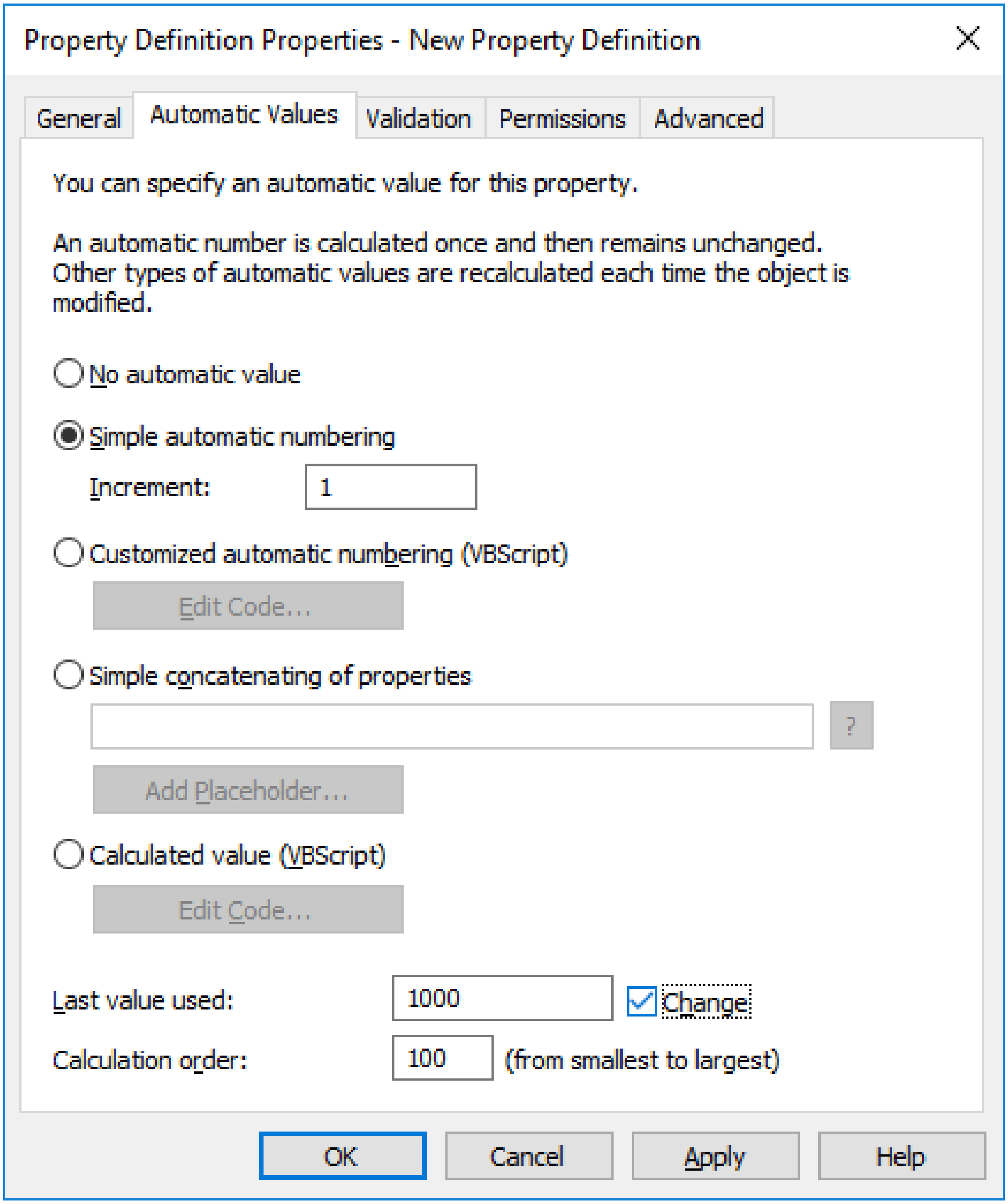
☑ Allow this property to be used as a grouping level in views

☑ Allow searching for objects by this property

☑ Do not search for old object versions

7. Go to the **Automatic Values** tab.

✓ The **Automatic Values** tab is opened.



Property Definition Properties - New Property Definition

You can specify an automatic value for this property.

An automatic number is calculated once and then remains unchanged. Other types of automatic values are recalculated each time the object is modified.

○ No automatic value

● Simple automatic numbering

Increment: 1

○ Customized automatic numbering (VBScript)

○ Simple concatenating of properties

○ Calculated value (VBScript)

Last value used: 1000 ☑ Change

Calculation order: 100 (from smallest to largest)

8. Select either:

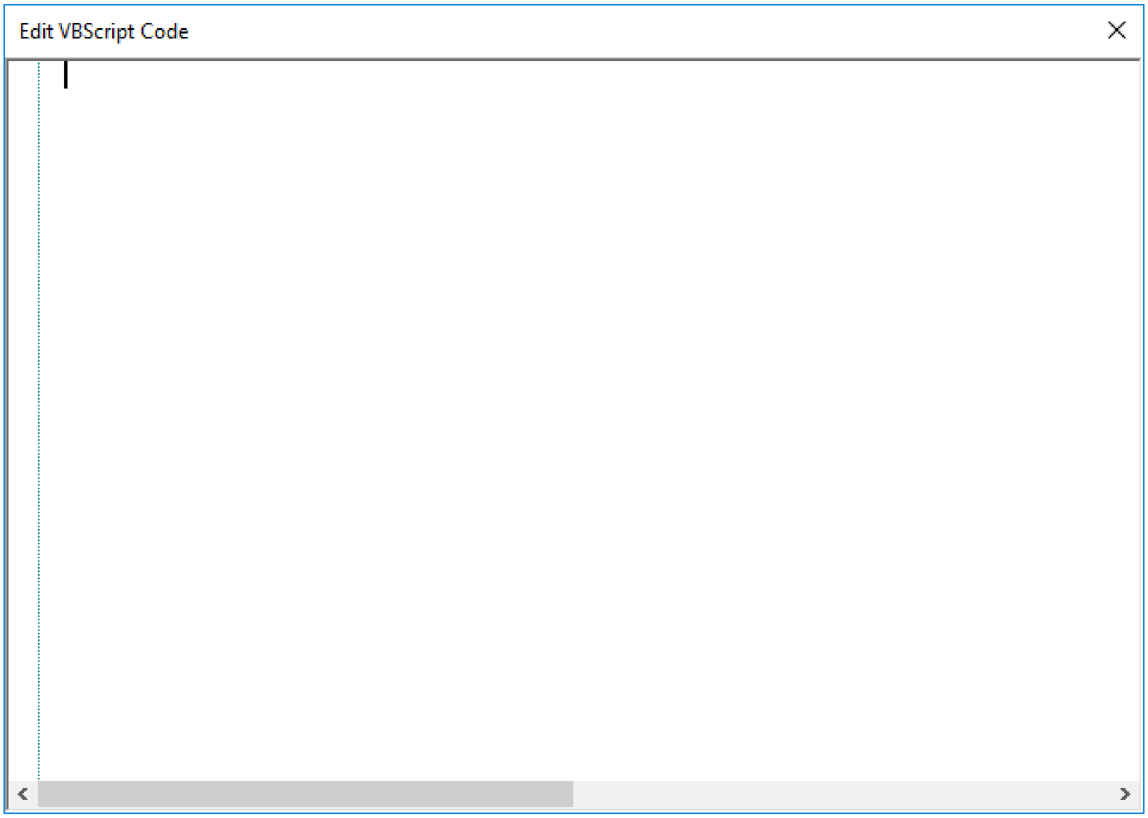
a. **Customized automatic numbering (VBScript)**: Select this option if you want to define automatic numbering using VBScript.

or

b. **Calculated value (VBScript)**: Select this option if you want to define any other type of automatic value using VBScript.

9. Click **Edit Code**.

The **Edit VBScript Code** window is opened.



10. Specify the VBScript code for calculating the automatic value. For instructions, see Specifying an Automatic Property Value Using VBScript.

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"*.

```
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
```

11. Close the **Edit VBScript Code** window once you are done.

12. 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 Available VBScript Variables.

Note: When you develop new extensions or edit existing ones, we recommend that you replace VBScript content with Vault Application Framework (VAF) compatible code for future compatibility. For more information on the benefits of VAF development over VBScript, refer to The Vault Application Framework in M-Files Developer Portal.

By default, validation is considered successful. Invalid values are thus detected using conditional statements and should any of the conditions specified in the validation be met, then an error should be raised, prompting the user to correct the invalid value (for instance, `Err.Raise MFScriptCancel, "The property must have a value of at least 10 characters."`).

Complete the following steps to add value validation for a property:

1. Open M-Files Admin.

2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Expand **Metadata Structure (Flat View)**.

6. Click **Property Definitions**.

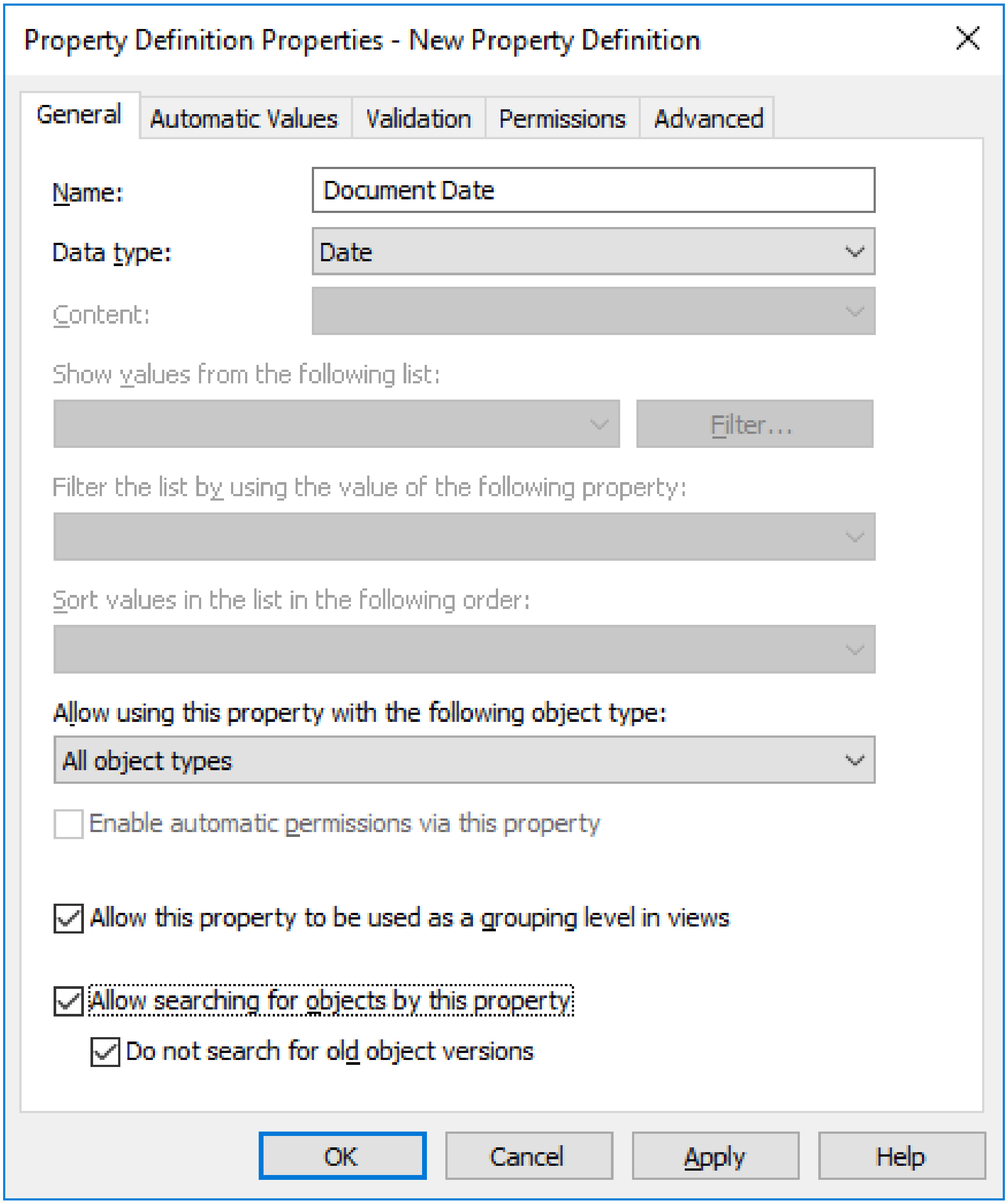
7. Either:

    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. In the task area, click **New Property Definition** to create a new property definition with automatic value validation.

✓ The **Property Definition Properties** dialog is opened.



Name: Document Date

Data type: Date

Content:

Show values from the following list:

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

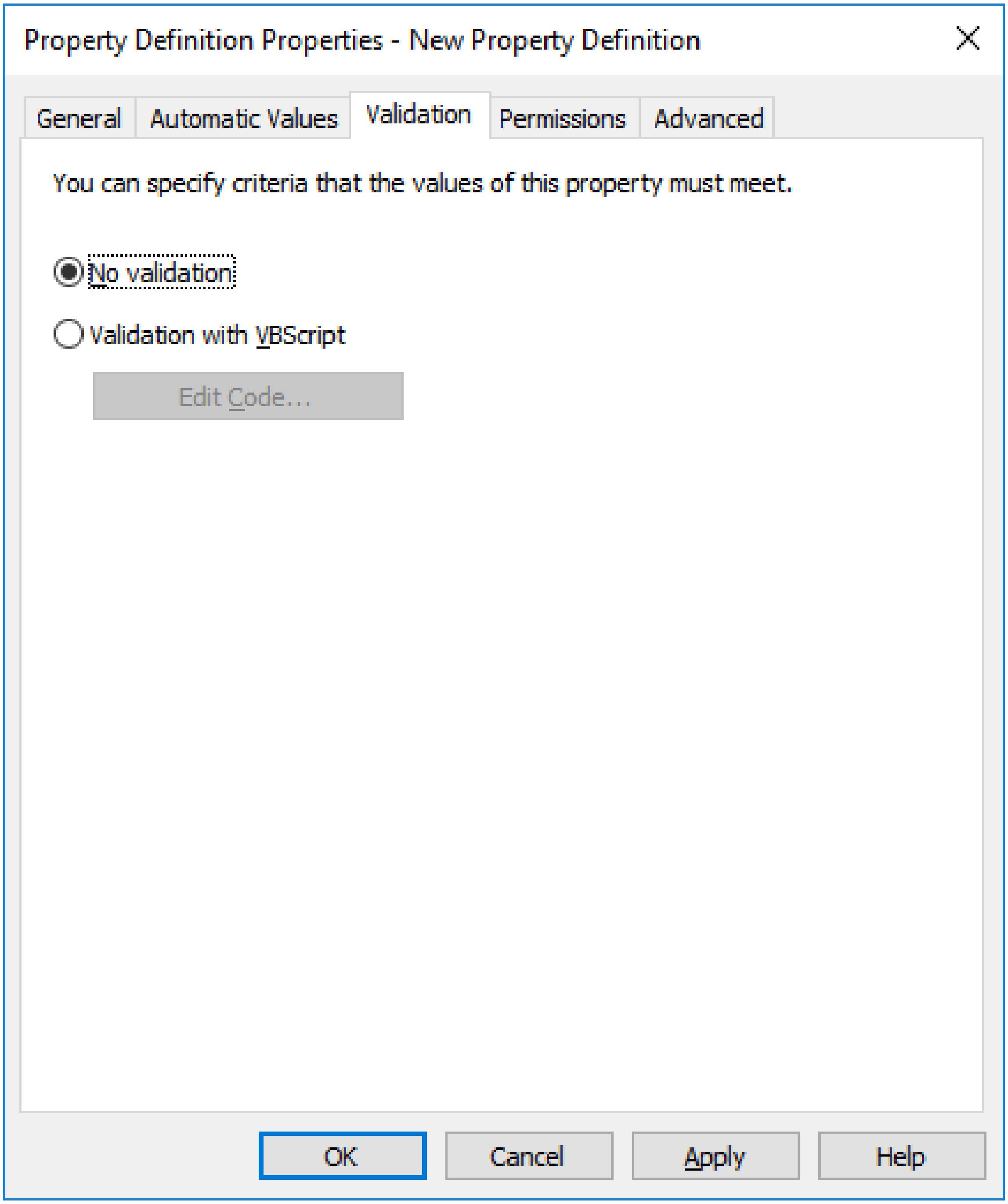
☑ Allow this property to be used as a grouping level in views

☑ Allow searching for objects by this property

☑ Do not search for old object versions

8. Go to the **Validation** tab.

✓ The **Validation** tab is opened.



Property Definition Properties - New Property Definition

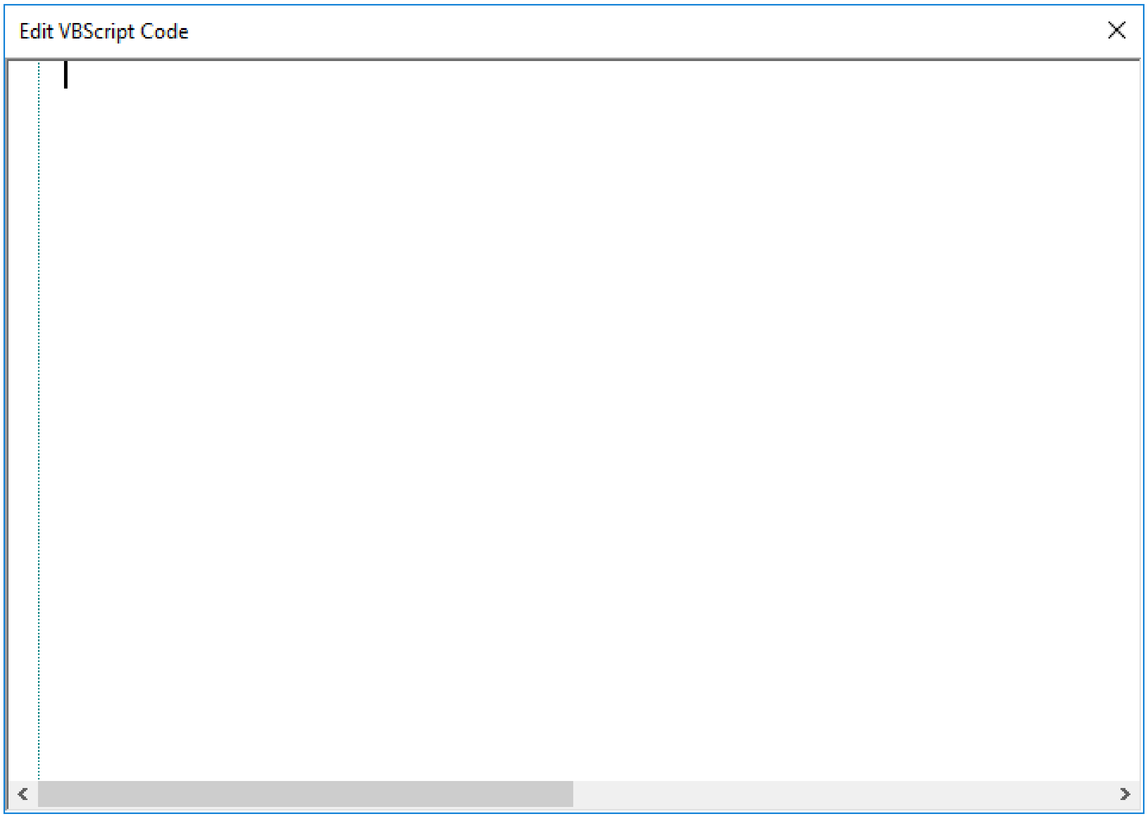
You can specify criteria that the values of this property must meet.

● No validation

○ Validation with VBScript

9. Select the **Validation with VBScript** option and click the **Edit Code...** button.

✓ The **Edit VBScript Code** window is opened.



10. In the **Edit VBScript Code** window, type in the VBScript code for validating the values of this property.

    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 M-Files API documentation is available online: M-Files API.

11. 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 following table 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.
Conflicted version	Number (integer)	Indicates the conflicted object version. When M-Files detects a conflict in the vault, M-Files creates a conflict object and adds this property to it. The conflict object is automatically removed when the conflict has been resolved.
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.

Built-in property definition	Data type	Description
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.
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.

Built-in property definition	Data type	Description
Name or title	Text	The name of title of the current object. **Tip:** If your M-Files system administrator has enabled translated object titles, you can use the translated object titles in searches. The translated object titles are also shown in the title area of the metadata card, in the listing area, in notifications, and in value lists.
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.
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.

Built-in property definition	Data type	Description
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.
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.

Built-in property definition	Data type	Description
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.

Property Definition 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.

Editing Permissions

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click a node that contains items that you want to edit.

   Permission settings are available for these items:

   - **Users**
   - **User groups**
   - **Metadata Structure (Flat View)** > **Object types**
   - **Metadata Structure (Flat View)** > **Value lists**
   - **Metadata Structure (Flat View)** > **Property definitions**
   - **Metadata Structure (Flat View)** > **Classes**
   - **Metadata Structure (Flat View)** > **Class groups**
   - **Workflows**
   - **Named access control lists**
6. Select an item in the listing area.

7. Right-click the item and click **Properties**.
8. Open **Permissions**.
9. In **Users and user groups**, select the user or user group whose permissions to change.

   If the user or user group is not on the list, click **Add**.

10. Specify the permissions for the selected user or user group.

    Allow: Enable this to explicitly give the permission to the selected user or user group.

    Deny: Enable this to explicitly deny the permission from the user or user group.

    The **Deny** setting is normally used to specify an exception to an **Allow** setting. For example, when John Doe is part the group **HR Managers**, you can set **Allow** for the group and **Deny** for John Doe.

    You can also leave both settings unselected.

11. Repeat steps 9 and 10 for the rest of the permissions.
12. Click **OK**.

Hierarchical Property Values

Instead of having the property value selection field show a flat list of values, you can set it to show a hierarchically ordered list, which can be built either on top of value lists or real object types. This section explains how you can set up the property value selection field to show an object type based hierarchy. If you would like to specify and use hierarchical value lists instead, see Value list hierarchy.

Tip: The values of a real object type based value list consist of actual objects in your vault, whereas a simple value list only contains items that are added to the list manually, with M-Files Admin or in the M-Files clients by users.

Before you can set a hierarchy to be used by a property, you of course must have one available to you. See the example in Creating an Object-Based Hierarchy to get started. After you have finished creating the hierarchy, you can put it to use as explained in Specifying Hierarchical Properties.

In this chapter

Creating an Object-Based Hierarchy

This example describes a scenario where a construction company wants to use a single hierarchically ordered list of values for three separate properties referring to the location of a construction site. They want the hierarchical value list to be based on actual objects in their vault.

To create the required metadata structure and objects for this kind of scenario, follow the steps provided below. The names of the structure elements are examples only, and you can freely name them as you like.

First, open M-Files Admin and create the required metadata structure elements as instructed below.

1. Create an object type with the names `Area` (singular) and `Areas` (plural).

   For instructions on creating object types, see Creating a New Object Type.

2. Create four property definitions that have the names listed below. All of them should be of the data type **Choose from list** and should show values from the value list **Areas**, essentially consisting of various **Area** objects in your vault.

   - Belongs to area
   - Construction site continent
   - Construction site country
   - Construction site city

   For instructions on creating property definitions, see Creating a New Property Definition.

   Tip: You can optionally set the following filters for the continent and country properties if you want the continent property to only show continents and the country property to hide cities from the list:

   - Construction site continent: Class = Continent
   - Construction site country: Class != City

3. Create the following three classes:

   - Continent
   - Country
   - City

   As the value of the **Object type** setting for each one, select **Area**.

   Under the **Properties** section, add the **Belongs to area** property for all the three classes. This way, the property is automatically added to the metadata card when you are creating these objects later on.

   For detailed instructions on creating classes, see Creating a New Class.

Next, open M-Files Desktop or M-Files Web and create a hierarchy of continent, country, and city objects.

4. Create a set of continents:

   a) Click the **Create** button in the top area and select **Area**.
   b) To the **Class** field, enter `Continent`.
   c) To the **Name or title** field, enter the name of the continent, such as `Asia`.
   d) Leave empty the value of the **Belongs to area** field as this is a top-level object.

      The top-level object must contain this property as well because it defines that it belongs to the same hierarchy as its descendant objects (in this example, countries and cities).

   e) Click **Create** once you are done.
   f) Repeat these steps for as many objects of this class as you require.

5. Create a set of countries:

   a) Click the **Create** button in the top area and select **Area**.
   b) To the **Class** field, enter `Country`.
   c) To the **Name or title** field, enter the name of the country, such as `India`.
   d) To the **Belongs to area** field, enter the name of the continent in which this country is located, such as `Asia`.

e) Click **Create** once you are done.
f) Repeat these steps for as many objects of this class as you require.

6. Create a set of cities:

a) Click the **Create** button in the top area and select **Area**.
b) To the **Class** field, enter `City`.
c) To the **Name or title** field, enter the name of the city, such as `Mumbai`.
d) To the **Belongs to area** field, enter the name of the country in which this city is located, such as `India`.
e) Click **Create** once you are done.
f) Repeat these steps for as many objects of this class as you require.

Finally, open M-Files Admin again and, by following the instructions in Specifying Hierarchical Properties, set the property definitions **Construction site continent**, **Construction site country**, and **Construction site city** to use the **Belongs to area** hierarchy. The configuration should look similar to the one presented below.

- Hierarchies
    - Construction site continent
        - Hierarchy Name = Construction site continent
        - Target Property = Construction site continent
        - Hierarchy Property = Belongs to area
    - Construction site country
        - Hierarchy Name = Construction site country
        - Target Property = Construction site country
        - Hierarchy Property = Belongs to area
    - Construction site city
        - Hierarchy Name = Construction site city
        - Target Property = Construction site city
        - Hierarchy Property = Belongs to area

7. Click **Save** and close M-Files Admin once you are done.

Now, when you add the properties **Construction site continent**, **Construction site country**, and **Construction site city** to the metadata of an object, they all show the same hierarchical list of areas that you can use to select the location of the construction site.

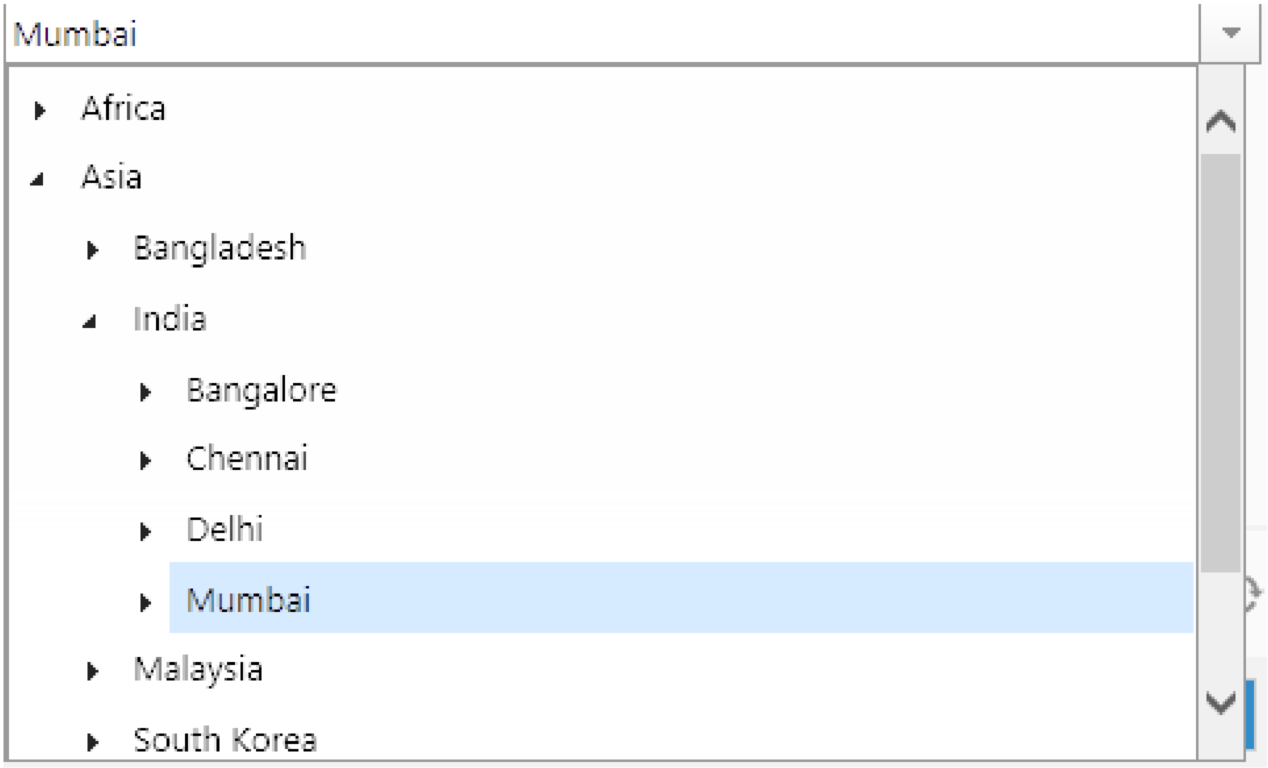


Figure 44: An example of a hierarchical, object-based value list.

Specifying Hierarchical Properties

To set a property of your choice to use an object-based hierarchy, do the following steps:

1. Open M-Files Admin and go to a vault.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
2. Select **Configurations** and expand **Advanced Vault Settings**.
3. Expand the **Configuration** node and select **Real Object Type Hierarchies**.
4. Select the **Hierarchies** > **Add Hierarchy**.
5. Expand the newly created node and specify the values according to the information in the table below.

Setting name	Description	Example value
Hierarchy Name	The name of this hierarchy definition. The name is only shown in the configurations editor.	Construction site continent
Target Property	The property that uses the value list hierarchy specified in the **Hierarchy Property** setting. Can be the same as **Hierarchy Property**. The property must be of the data type **Choose from list** or **Choose from list (multi-select)**.	Construction site continent

Setting name	Description	Example value
Hierarchy Property	Specifies the real object type based value list hierarchy to be used. The property selected here is automatically set to be hierarchical as well. The property must be of the data type **Choose from list**.	Belongs to area

6. Click **Save**.

When the property specified in the **Target Property** setting is added to object metadata, the value selection drop-down menu shows a hierarchically ordered list of values based on the property specified in the **Hierarchy Property** setting. For an example, see Creating an Object-Based Hierarchy.

Note: After the changes have been saved and M-Files Server has been restarted, end users must log out from and log back in to the vault to be able to use these type of lists. To log out all vault users, restart the vault. However, taking a vault offline must always be done in a controlled manner and the vault users must be notified beforehand.

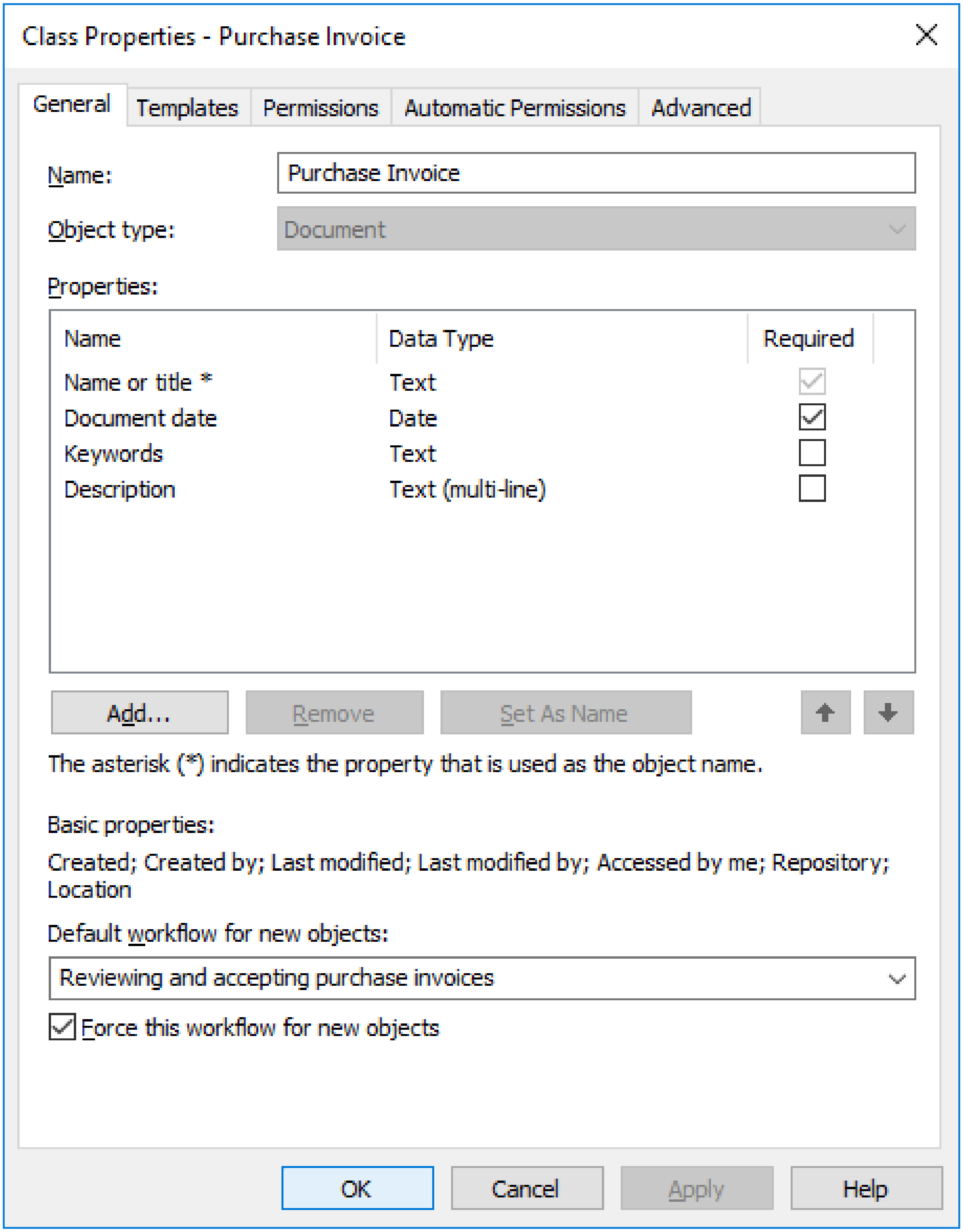
Classes

A class is a metadata structure element designed to help categorize objects, improve consistency, and make it easier for users to add object metadata. You can create classes and specify properties for each class in M-Files Admin. When you select the class in the client, M-Files shows on the metadata card the properties that the system administrator has specified for the class.

In this chapter

New Class

To create a new class in M-Files Admin, go to a vault in the left-side tree view and expand **Metadata Structure (Flat View)** > **Classes**. In the task area, click **New Class**.



Name: Purchase Invoice

Object type: Document

Properties:

Name	Data Type	Required
Name or title *	Text	☑
Document date	Date	☑
Keywords	Text	□
Description	Text (multi-line)	□

The asterisk (*) indicates the property that is used as the object name.

Basic properties:

Created; Created by; Last modified; Last modified by; Accessed by me; Repository; Location

Default workflow for new objects:

Reviewing and accepting purchase invoices

☑ Force this workflow for new objects

Figure 45: The properties dialog of a new "Purchase Invoice" class.

In this **Class Properties** dialog, you can add new properties with the **Add** button. If the **Required** checkbox for the property is active, users must give a value for the property when they create an object with that class. The settings in this example make sure that **Name or title** and **Document date** are given for all **Purchase Invoice** objects.

The properties of a class can be a combination of normal M-Files properties and properties that are read from an external database. However, make sure that the external database connection is enabled before you add internal properties to a class.

Set As Name

Any property of the class can be set to specify the name of the object. This makes the naming of objects in a class more consistent. This property can be very useful when you work with automatic values (see Property Definition Automatic Values). For example, the automatic value of the property can be set to be the name of the proposal document.

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)

In the **Advanced** tab, you can specify an alias for the class. For more information, see Associating the Metadata Definitions.

Creating a New Class

To create a new class to your M-Files vault:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)**, and then select **Classes**.
6. In the task area, click **New Class**.

✓ 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.

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.

    ⓘ For more information, see Permissions and Automatic Permissions.

12. Optional: On the **Automatic Permissions** tab, you can specify whether or not objects of this class receive automatic permissions.

    ⓘ For more information, see Permissions and Automatic Permissions.

13. Optional: On the **Advanced** tab, you can define aliases for the class using the **Aliases** field.

    ⓘ Use semicolons (;) to separate many aliases.

    ⓘ For more information, see Aliases for Associating Metadata Between Vaults.

    When automatic aliases are in use and you write a name on the **General** tab, the **Aliases** field on the **Advanced** tab is automatically filled in. The alias has the format <*predefined prefix*>.<*name*>. Configure automatic aliases for your vault in Advanced Vault Settings.

14. Click **OK**.

The new class is added to the list of classes and can be selected for objects in the M-Files clients.
Assignment 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.

Assignment types

There are two types of assignments, task assignments and approval assignments. The assignees of the task assignments simply mark the assignment complete when they have successfully carried out the task, whereas the assignees of approval assignments have more say in the actual approval process: they can use the assignment 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.

Permissions and Automatic Permissions

Permissions

On the **Permissions** tab, you can specify who can see this class and set the class for objects. System and vault administrators can always see all classes and set them for objects.

Automatic permissions

An object receives automatic permissions when a class with automatic permissions specified is added to the object metadata.

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 Enabling Automatic Permissions for a Value List Item.

Note: Micro Focus IDOL and Smart Search: If more than four automatic ACL sources control the permissions of an object, only administrators can see it in search results.

Editing Permissions

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click a node that contains items that you want to edit.

   Permission settings are available for these items:

   - **Users**
   - **User groups**
   - **Metadata Structure (Flat View)** > **Object types**
   - **Metadata Structure (Flat View)** > **Value lists**
   - **Metadata Structure (Flat View)** > **Property definitions**
   - **Metadata Structure (Flat View)** > **Classes**
   - **Metadata Structure (Flat View)** > **Class groups**
   - **Workflows**
   - **Named access control lists**
6. Select an item in the listing area.
7. Right-click the item and click **Properties**.
8. Open **Permissions**.
9. In **Users and user groups**, select the user or user group whose permissions to change.

   If the user or user group is not on the list, click **Add**.

10. Specify the permissions for the selected user or user group.

    Allow: Enable this to explicitly give the permission to the selected user or user group.

    Deny: Enable this to explicitly deny the permission from the user or user group.

    The **Deny** setting is normally used to specify an exception to an **Allow** setting. For example, when John Doe is part the group **HR Managers**, you can set **Allow** for the group and **Deny** for John Doe.

    You can also leave both settings unselected.

11. Repeat steps 9 and 10 for the rest of the permissions.

12. Click **OK**.

Class Groups

You can create class groups to combine document classes into categories. This makes it easier to select a class when you create documents. You can create class groups for the document object type only.

To create a class group:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Hierarchical View)**.
6. Right-click **Document** and select **New Class Group**.
7. In **Name**, enter a name for the group.

   The name can be, for example, `4. Meetings` for a class group that contains classes for documents related to meetings, such as Memo, Meeting Notice, or Agenda. Class groups are shown in the class selection drop-down menu in alphabetical order. You can use numbers at the start of the group names to change the order of the list.

8. Click **Add** to add a class to the new group.
9. Optional: To create a class and add it to the class group, click **New Class**.

   For instructions, see Creating a New Class.

10. Select the classes that you want to add to the new class group and then click **Add**.

    You can select more than one item at once. Hold down the Ctrl key to select multiple individual items or hold down the ⇧ Shift key to select adjacent items on the list.

11. Optional: In **Members**, you can select a class and click the ↑ or the ↓ button to rearrange the classes.

    The ordering changes the order in which the classes are shown in the class selection drop-down menu in the classic M-Files Desktop.

12. Optional: In **Members**, select a class and click **Edit** to change its properties.

    ℹ For more information on class properties, see New Class.

13. Optional: To remove a class from the class group, in the **Members** list, select the group to be removed and click **Remove**.

    ℹ This only removes the class from the class group. It does not delete the class.

14. Optional: Select one or more classes and click **Add properties** to add one or more properties to the selected classes.

    ℹ To change the order of the added properties, you must edit each class separately.

15. Optional: Open the **Permissions** tab to specify the users who may see the new class group.

    ℹ For instructions, see Editing Permissions.

16. Click **OK** to create the class group.

In this chapter

- Editing Permissions

Editing Permissions

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click a node that contains items that you want to edit.

   ℹ Permission settings are available for these items:

   - **Users**
   - **User groups**
   - **Metadata Structure (Flat View)** > **Object types**
   - **Metadata Structure (Flat View)** > **Value lists**
   - **Metadata Structure (Flat View)** > **Property definitions**
   - **Metadata Structure (Flat View)** > **Classes**
   - **Metadata Structure (Flat View)** > **Class groups**
   - **Workflows**
   - **Named access control lists**
6. Select an item in the listing area.
7. Right-click the item and click **Properties**.
8. Open **Permissions**.
9. In **Users and user groups**, select the user or user group whose permissions to change.

ⓘ If the user or user group is not on the list, click **Add**.

10. Specify the permissions for the selected user or user group.

ⓘ **Allow**: Enable this to explicitly give the permission to the selected user or user group.

ⓘ **Deny**: Enable this to explicitly deny the permission from the user or user group.

ⓘ The **Deny** setting is normally used to specify an exception to an **Allow** setting. For example, when John Doe is part the group **HR Managers**, you can set **Allow** for the group and **Deny** for John Doe.

ⓘ You can also leave both settings unselected.

11. Repeat steps 9 and 10 for the rest of the permissions.

12. Click **OK**.

3.2.2. Managing Users and User Groups

This section deals with managing vault users and user groups in M-Files Admin.

In this chapter

Users

Under the **Users** node of a vault in M-Files Admin, you can add users to the 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).

M-Files assigns each user a unique ID, which can be found in the user's properties in M-Files Admin.

Deleting users

As a general rule, users should not be deleted from the vault because they contain a lot of information that might still be needed later on. The user objects hold, among other things, user interface preferences, information about the favorite objects of the user, and records about notifications related to the user. M-Files Admin does not allow the delete operation to be undone, so it should be carried out only if you are absolutely certain the user information will no longer be needed. You might, instead, want to consider disabling the user. For more information about disabled users, go to Creating a User and search for `disabled` in step 9.

In this chapter

- Enabling or Disabling Many Users

Creating a User

Creating a user in M-Files Cloud

In M-Files Cloud, you can create a user in M-Files Manage. For instructions, refer to Creating Users in the M-Files Manage user guide.

Creating a user in other M-Files environments

To create a user to a selected vault:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click **Users**.

   Tip: If the list contains a large number of items, you might want to filter it. To filter the view, open the **View** menu and click **Filter**. Enter a desired text to filter the column contents.

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

   The **New User** dialog is opened.

7. 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 Creating a Login Account.

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

8. 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.

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

Option	Description
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.

Option	Description
	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. **Note:** Object permissions are updated as an asynchronous background task. Object permissions may be updated when, for example, a named access control list, a user, a user group, or the value of a pseudo-user (such as a project manager) is modified. You may monitor the progress of the task in M-Files Admin in the **Background Tasks** section. For more information, see Monitoring Background Tasks.
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 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.
User cannot create or modify private views or notification rules	The user cannot create or modify private views or private notification rules. Private views and notification rules are visibile only to the user who created them, whereas common ones are visible to all vault users.
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

Option	Description
	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. **Note:** With this permission, users may be allowed to view metadata structure items and other vault information that they would not otherwise be permitted to view, such as value lists, object types, and named access control lists.
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	With this permission, you can create views visible to all vault users. You can also specify common notification rules. You can create common views and notification rules in the classic M-Files Desktop. **Note:** For more information on common views, see Using Views. For more information on common notification rules, see Editing Notification Settings in the Classic M-Files Desktop.

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

The system administrator and all users with full control of the document vault in question always see all users.

a) On the **Users and user groups** list, select 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** check box to modify the permissions of the selected user.

11. 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.

Importing Users

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click **Users**.
6. In the task area, click **Import Individual Users**.

   ✓ The **Import Individual Users** dialog is opened.

7. Select either:

   a. **Choose from list** to select the user group using drop-down menus. In **Domain**, select the desired domain. In **Organizational unit**, select the desired organizational unit within that domain. Finally, in **User group**, select the user group that you want to import.

      or

   b. **Enter Name**. This option is especially useful if you have so many user groups that searching the correct one from list is hard. Enter the name of the user group in the format *<domain>**<user group>* and click **Show**.

   ✓ The list area in the dialog is populated with the members of the selected user group.

8. Optional: Check the **Include users from nested groups** check box to be able to import login accounts from nested groups within the selected user group.

   ✓ The list area in the dialog 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. Hold down the Ctrl key to select multiple individual items or hold 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 type.

11. Click **OK** to import the selected users.

The users are imported to the selected vault and added to the **Users** list.

Vault User 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.

Editing Permissions

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click a node that contains items that you want to edit.

   Permission settings are available for these items:

   - **Users**
   - **User groups**
   - **Metadata Structure (Flat View)** > **Object types**
   - **Metadata Structure (Flat View)** > **Value lists**
   - **Metadata Structure (Flat View)** > **Property definitions**
   - **Metadata Structure (Flat View)** > **Classes**
   - **Metadata Structure (Flat View)** > **Class groups**
   - **Workflows**
   - **Named access control lists**
6. Select an item in the listing area.
7. Right-click the item and click **Properties**.
8. Open **Permissions**.
9. In **Users and user groups**, select the user or user group whose permissions to change.

   If the user or user group is not on the list, click **Add**.
10. Specify the permissions for the selected user or user group.

    Allow: Enable this to explicitly give the permission to the selected user or user group.

    Deny: Enable this to explicitly deny the permission from the user or user group.

    The **Deny** setting is normally used to specify an exception to an **Allow** setting. For example, when John Doe is part the group **HR Managers**, you can set **Allow** for the group and **Deny** for John Doe.

    You can also leave both settings unselected.
11. Repeat steps 9 and 10 for the rest of the permissions.

12. Click **OK**.

Enabling or Disabling Many Users

You can enable and disable many users at the same time. This is especially useful if you have a lot of users. You can also delete many users at once, but user deletion is not recommended.

To enable or disable many users:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Click **Users**.
4. In the list of users, do one of these steps:
    a. To select a range of users, click the first user, hold down the ⇧ Shift key, and click the last user.

       or

    b. To select many individual users, click the first user, hold down the Ctrl key, and select the other users.
5. In the task area, select **Enable** or **Disable**.
6. If you selected **Disable**, click **Yes** in the dialog that is opened to confirm the operation.

User Groups

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).

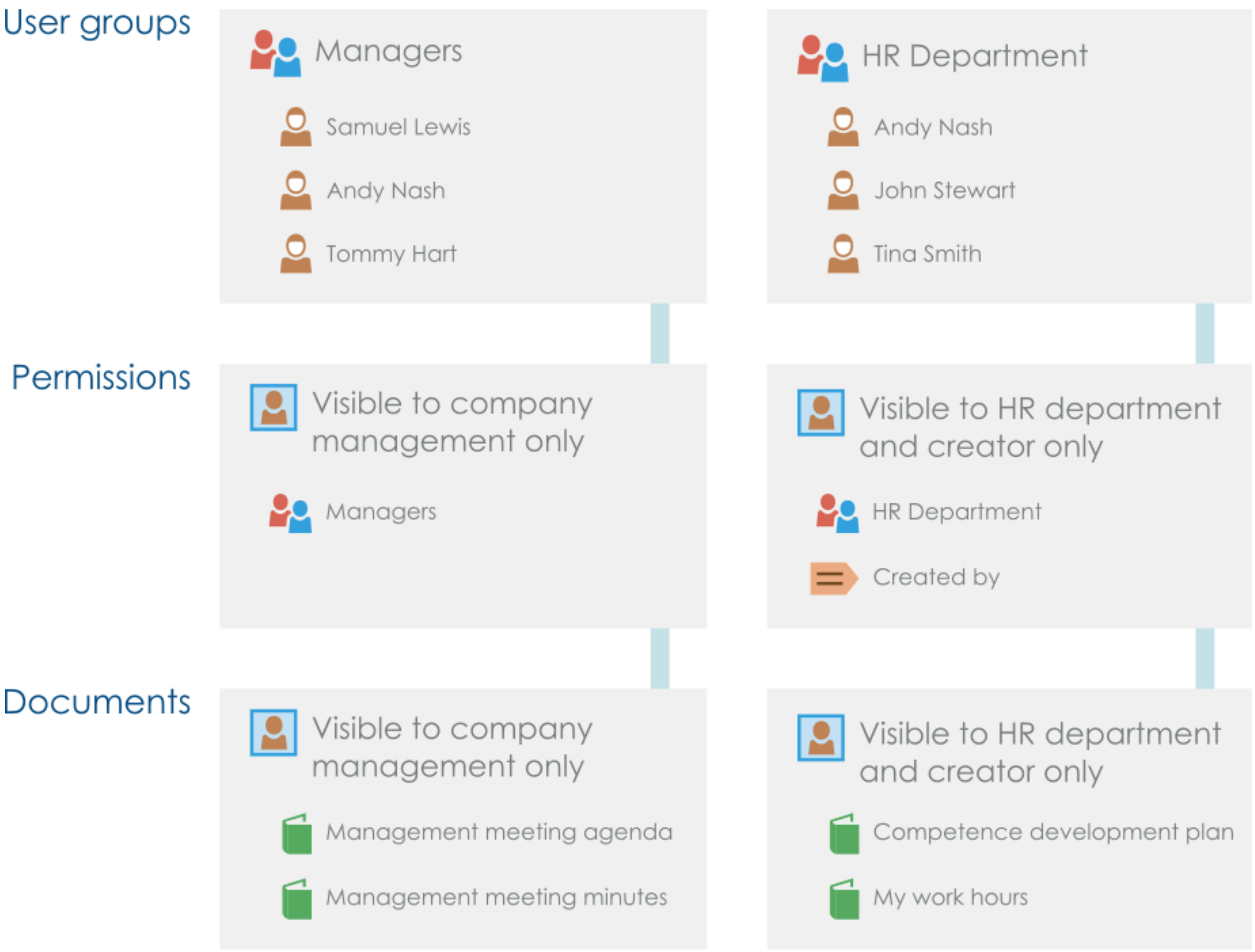

User groups
Managers
Samuel Lewis
Andy Nash
Tommy Hart
HR Department
Andy Nash
John Stewart
Tina Smith
Permissions
Visible to company management only
Managers
Visible to HR department and creator only
HR Department
Created by
Documents
Visible to company management only
Management meeting agenda
Management meeting minutes
Visible to HR department and creator only
Competence development plan
My work hours

Figure 46: User groups simplify the management of access rights.

You can manage the user groups in your vault by completing the following steps:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **User Groups**.

In this chapter

- Creating a User Group
- Importing User Groups
- User Group Permissions

Creating a User Group

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.

4. Expand a vault.

5. Click **User Groups**.

   Tip: If the list contains a large number of items, you might want to filter it. To filter the view, open the **View** menu and click **Filter**. Enter a desired text to filter the column contents.

6. On the task pane, click **New User Group...**.

   ✓ The **User Group Properties** dialog is opened.

7. In the **Name** field, enter a name for the new user group.

8. Click **Add...** to add users to this group.

   ✓ The **Select Users or User Groups** dialog is opened.

9. Select the users to be added to the user group and click **Add**.

   You can select more than one item at once. Hold down the Ctrl key to select multiple individual items or hold down the ⇧ Shift key to select adjacent items on the list.

10. Optional: Enable the **Group members are synchronized from the domain** and click **Define...** if you want to retrieve the users from a domain.

    For more information, see Importing User Groups.

11. Optional: On the **Advanced** tab, define an alias for the user group.

    Use semicolons (;) to separate many aliases.

    For more information, see Associating the Metadata Definitions.

    When automatic aliases are in use and you write a name on the **General** tab, the **Aliases** field on the **Advanced** tab is automatically filled in. The alias has the format <*predefined prefix*>.<*name*>. Configure automatic aliases for your vault in Advanced Vault Settings.

12. Click **OK** to finish creating the user group.

The user group that you have just created is added to the **User Groups** list.

Note: Object permissions are updated as an asynchronous background task. Object permissions may be updated when, for example, a named access control list, a user, a user group, or the value of a pseudo-user (such as a project manager) is modified. You may monitor the progress of the task in M-Files Admin in the **Background Tasks** section. For more information, see Monitoring Background Tasks.

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.

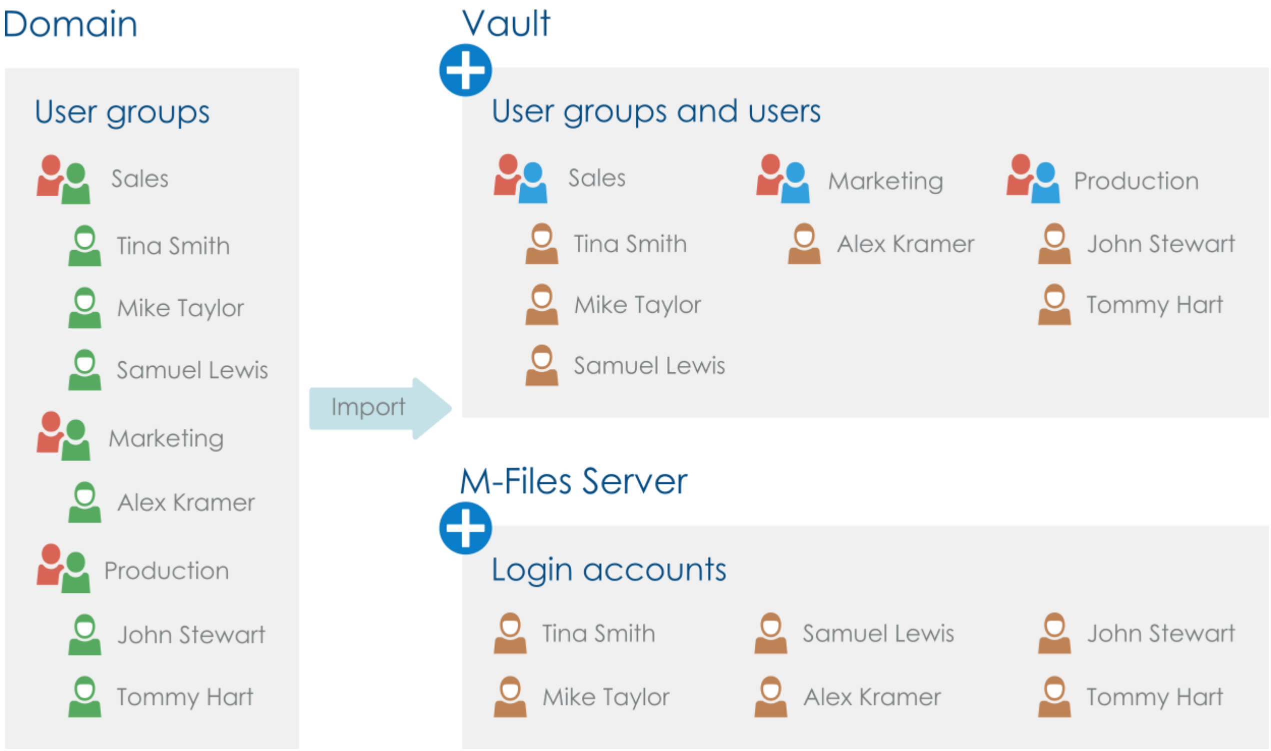


Figure 47: User groups can be imported from the domain to the vault, allowing existing user groups in the domain to be used for specifying permissions to vault content.

Complete the following steps to import user groups:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click **User Groups** and then click **Import User Group** in the task area.

   ✓ The **Import User Group** dialog is opened.

6. Select either:

   a. **Choose from list** to select the user group using drop-down menus. In **Domain**, select the desired domain. In **Organizational unit**, select the desired organizational unit within that domain. Finally, in **User group**, select the user group that you want to import.

      or

   b. **Enter Name**. This option is especially useful if you have so many user groups that searching the correct one from list is hard. Enter the name of the user group in the format *<domain>**<user group>* and click **Show**.

   ✓ The list area in the dialog is populated with the members of the selected user group.

7. Optional: Check the **Include users from nested groups** check box to be able to import login accounts from nested groups within the selected user group.

✓ The list area in the dialog is populated with the members of the selected user group and the members of any user group nested within the selected user group.

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.

9. Optional: Select the **Check for new and deleted members every 15 minutes** 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. In addition, new login accounts are created for new users.

In this chapter

- Defining, Editing, or Disabling Import Settings of Existing User Groups
- User Synchronization with Microsoft Entra ID
- User Synchronization Details

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 a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Click **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.

6. Either:

If you want to	Do the following
Import to users an existing user group	Check the **Group members are synchronized from the domain** check box, click the **Define...** button and then define the import settings in the dialog that is opened. See Importing User Groups

If you want to	Do the following
	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 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** check box.

7. Click **OK** to save your changes and close the **User Group Properties** dialog.

User Synchronization with Microsoft Entra ID

This page tells you how you can set up user group synchronization between M-Files and Microsoft Entra ID.

If you use M-Files Cloud, we strongly recommend subscription-level user provisioning. With on-premises servers, the recommended setup is the vault-specific plugin method.

Subscription-level user provisioning

In M-Files Cloud, user provisioning with M-Files Manage is the recommended method to synchronize user groups with Microsoft Entra ID. User provisioning uses the SCIM protocol. This means that the user group management is done in Entra ID, and Entra ID pushes the users to M-Files. The process creates users to the M-Files subscription, which lets you easily link an Entra ID user group to many vaults.

Note: This method is available only in M-Files Cloud and on-premises environments where the server is joined to M-Files Manage. To use this method, you must have a Microsoft Entra ID Premium license. For more information and configuration instructions, refer to the M-Files Manage user guide.

Vault-level user synchronization

On the vault level, there are two methods to set up user synchronization with Entra ID. With both methods, user group management is done in Entra ID, but they are different in how users are brought to M-Files.

With the plugin method, you specify the user groups in M-Files Admin, and M-Files periodically pulls the users from Entra ID. With the SCIM method, Entra ID pushes the users to M-Files.

- Plugin method: Importing User Information from Entra ID with the User Synchronization Plugin
  - In on-premises environments, we strongly recommend this method over the SCIM method.
  - In addition to the Azure AD synchronization plugin, you can also use the Okta user group synchronization plugin. For instructions, refer to Configuring Okta User Group Synchronization Plugin in M-Files Support Portal.
- SCIM method: Synchronizing Users from Microsoft Entra ID to M-Files with SCIM
  - To use this method, you must have a Microsoft Entra ID Premium license.
  - In an on-premises environment, this method lets you use Entra ID authentication only for M-Files Desktop.

Optional settings for Active Directory importing with the vault-level plugin method

After you have configured the synchronization plugin, you can adjust the behavior of the user group synchronization. This is especially useful in environments with large vaults and Active Directory groups.

To open the settings, in the **Advanced Vault Settings** section of M-Files Admin, go to **User Groups** > **Active Directory Importing**.

If the M-Files server has many vaults, we recommend that you set the synchronization to start at a different time in each vault to improve system performance. To do this, change the **Start Time of First Import** for each vault to specify different start times of the first import after the server startup.

User Synchronization Details

This information applies to user synchronization with local active directories and with the vault-level plugin method for Microsoft Entra ID. For synchronization details with M-Files Manage provisioning, refer to the M-Files Manage user guide.

Changes in AD group members

See the table for information on what occurs in M-Files when the members of the synchronized AD groups have changed.

Change	Effects
Users added to AD groups that are synchronized to M-Files	• The users are added as vault users to the vault that contains the user group. • 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. For example, if users have been assigned concurrent licenses, and they are added to a group with named licenses, the users keep the concurrent licenses.
Users removed from all the AD groups that are synchronized to M-Files	• The users are removed from the user group in M-Files. They lose all permissions that were granted to them through the group membership. • The user accounts stay in M-Files but are disabled. • The login accounts stay active. They keep the licenses that are assigned to them. **Note:** Users are not automatically disabled if they are members of at least one synchronized AD group.

Disabling and deleting synchronized users in M-Files

See the table for information on what occurs if you disable or delete synchronized users in the vault.

Change	Effects
Synchronized users disabled in M-Files	By default, the users stay disabled. To enable the users again, they must be enabled in M-Files. If you use a synchronization plugin, you can change the default behavior. To do this, go to the **Active Directory Importing** settings and set **Enable Disabled Users from Imported Groups** to **Yes**.
Synchronized users deleted in M-Files	The AD group synchronization does not create the deleted users again to the vault.

User Group 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.

Editing Permissions

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click a node that contains items that you want to edit.

   Permission settings are available for these items:

   - **Users**
   - **User groups**
   - **Metadata Structure (Flat View)** > **Object types**
   - **Metadata Structure (Flat View)** > **Value lists**
   - **Metadata Structure (Flat View)** > **Property definitions**
   - **Metadata Structure (Flat View)** > **Classes**
   - **Metadata Structure (Flat View)** > **Class groups**
   - **Workflows**
   - **Named access control lists**
6. Select an item in the listing area.
7. Right-click the item and click **Properties**.
8. Open **Permissions**.
9. In **Users and user groups**, select the user or user group whose permissions to change.

   If the user or user group is not on the list, click **Add**.
10. Specify the permissions for the selected user or user group.

Allow: Enable this to explicitly give the permission to the selected user or user group.

Deny: Enable this to explicitly deny the permission from the user or user group.

The **Deny** setting is normally used to specify an exception to an **Allow** setting. For example, when John Doe is part the group **HR Managers**, you can set **Allow** for the group and **Deny** for John Doe.

You can also leave both settings unselected.

11. Repeat steps 9 and 10 for the rest of the permissions.

12. Click **OK**.

External Repository Users

When you connect a document vault to an external repository using the Intelligent Metadata Layer technology, users in the external repository are imported to M-Files Server.

The **External Repository Users** view in M-Files Admin allows you to manage and refine associations between M-Files users and external repository users. When you associate an M-Files user with an external repository user, the M-Files user inherits the access rights of the external repository user. This way you can refine the access rights of an M-Files user to external repository content.

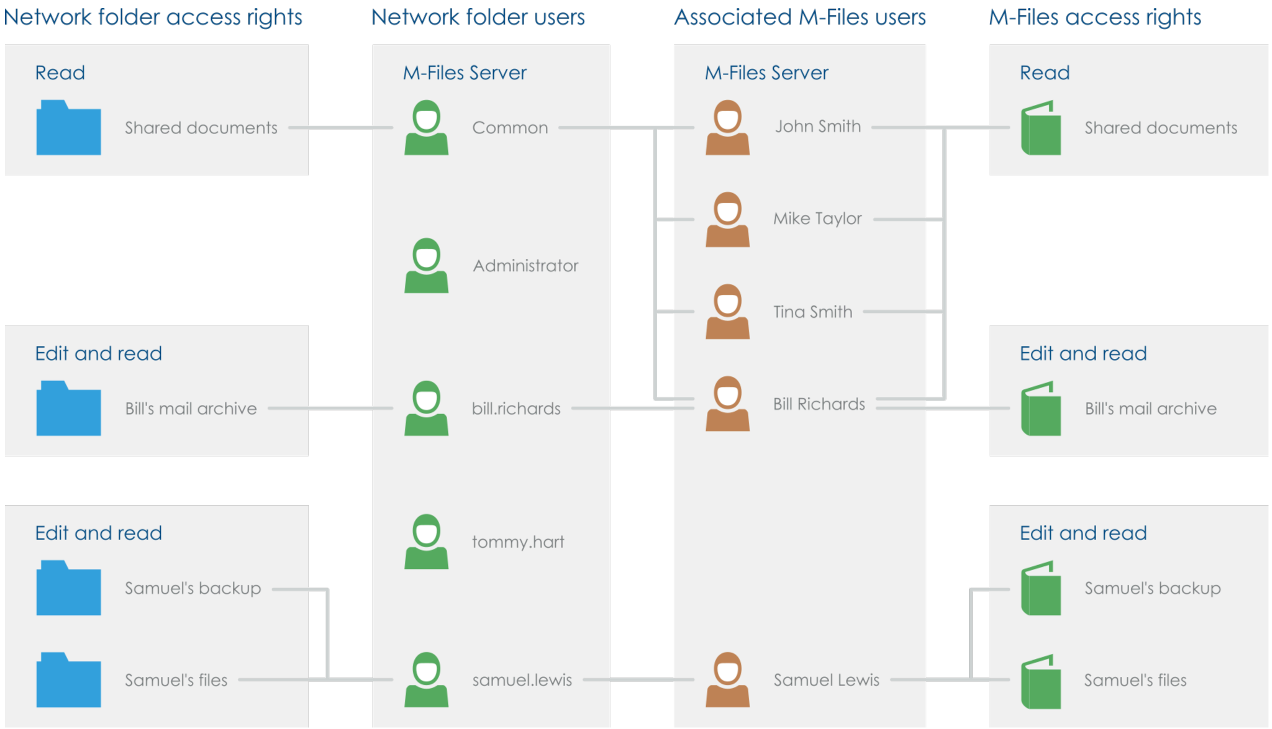


Figure 48: To refine access rights of external repository content, you must map external repository users with M-Files users in M-Files Admin.

Depending on your connector configuration, automatic associations between M-Files users and external repository users may be established in external repository connections. See Automatic Association for more information.

For more information on Intelligent Metadata Layer, see Intelligent Metadata Layer.

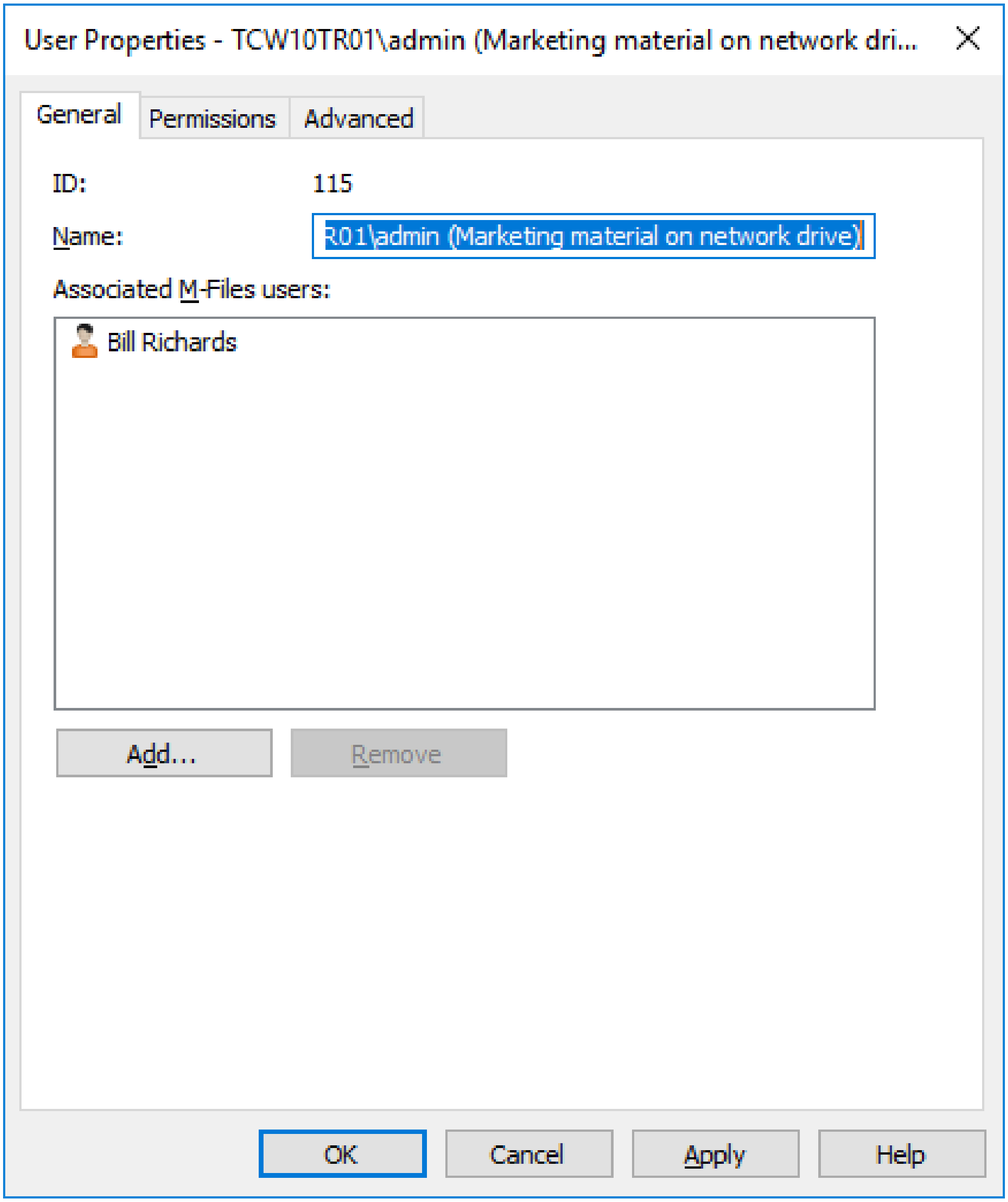
Note: External Repository Users is visible only if the selected vault has one or more active external repository connections.

Complete the following steps to associate an M-Files user with an external repository user:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **External Repository Users**.

   Tip: If the list contains a large number of items, you might want to filter it. To filter the view, open the **View** menu and click **Filter**. Enter a desired text to filter the column contents.
6. Double-click an external repository user.

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



User Properties - TCW10TR01\admin (Marketing material on network dri...

ID: 115

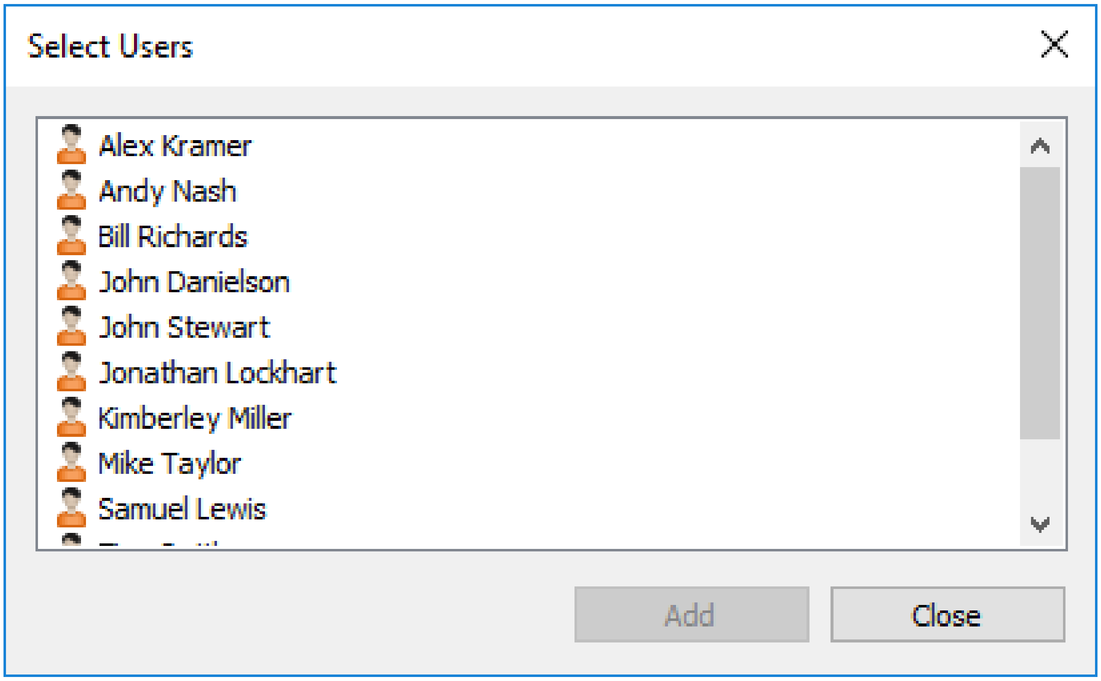
Name: R01\admin (Marketing material on network drive)

Associated M-Files users:

Bill Richards

7. To associate an M-Files user with the selected external repository user, click the **Add...** button.

   ✓ The **Select Users** dialog is opened.



Select Users

- Alex Kramer
- Andy Nash
- Bill Richards
- John Danielson
- John Stewart
- Jonathan Lockhart
- Kimberley Miller
- Mike Taylor
- Samuel Lewis

8. Select the M-Files user or users that you want to associate with the selected external repository user and then click **Add**.

   You can select more than one item at once. Hold down the Ctrl key to select multiple individual items or hold down the ⇧ Shift key to select adjacent items on the list.

9. Click **OK** to close the **User Properties** dialog.

The selected M-Files user is now associated with the selected external repository user, and the M-Files user has the same access rights to the external repository content as the external repository user when the M-Files user accesses the external repository with M-Files.

External Repository User Groups

When you connect a document vault to an external repository using the Intelligent Metadata Layer technology, all or some of the user groups in the external repository are imported to M-Files Server, depending on your connector configuration.

The **External Repository User Groups** view in M-Files Admin allows you to manage and refine associations between M-Files users or M-Files user groups and external repository users or external repository user groups. When you associate an M-Files user or user group with an external repository user group, the M-Files user or user group inherits the access rights of the external repository user group. This way you can refine the access rights of an M-Files user to external repository content.

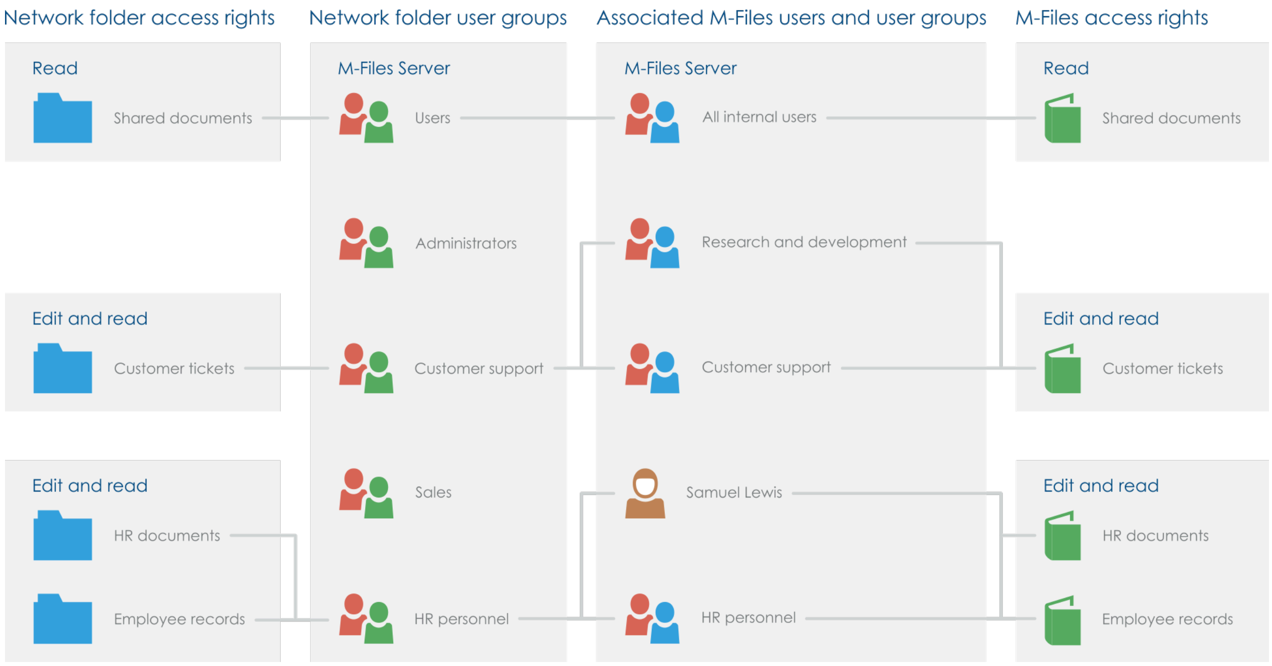


Figure 49: To refine access rights of external repository content, you must map external repository user groups with M-Files users and user groups in M-Files Admin.

Depending on your connector configuration, automatic associations between M-Files users or M-Files user groups and external repository users or external repository user groups may be established in external repository connections. See Automatic Association for more information.

For more information on Intelligent Metadata Layer, see Intelligent Metadata Layer.

Note: External Repository User Groups is visible only if the selected vault has one or more active external repository connections.

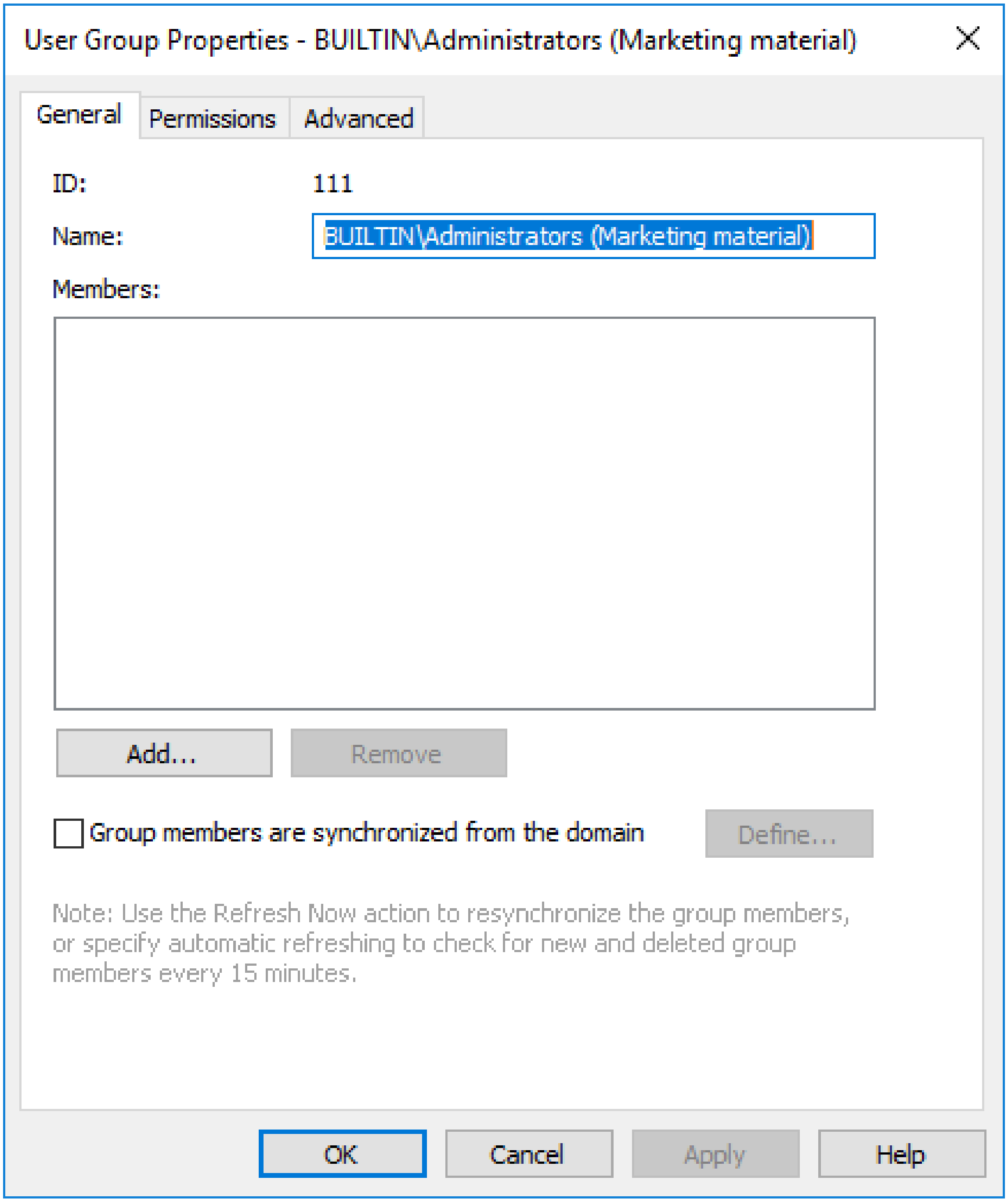
Complete the following steps to associate an M-Files user or user group with an external repository user group:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **External Repository User Groups**.

   Tip: If the list contains a large number of items, you might want to filter it. To filter the view, open the **View** menu and click **Filter**. Enter a desired text to filter the column contents.

6. In the task area, double-click an external repository user group.

   ✓ The **User Group Properties** dialog is opened.



User Group Properties - BUILTIN\Administrators (Marketing material)

ID: 111

Name: BUILTIN\Administrators (Marketing material)

Members:

□ Group members are synchronized from the domain

Note: Use the Refresh Now action to resynchronize the group members, or specify automatic refreshing to check for new and deleted group members every 15 minutes.

7. To associate an M-Files user or user group with the selected external repository user group, click the **Add...** button.

   ✓ The **Select Users or User Groups** dialog is opened.

8. Select the M-Files user or user group that you want to associate with the selected external repository user group and then click **Add**.

   You can select more than one item at once. Hold down the Ctrl key to select multiple individual items or hold down the ⇧ Shift key to select adjacent items on the list.

9. Click **OK** to close the **User Group Properties** dialog.

The selected M-Files user or user group is now associated with the selected external repository user group, and the M-Files user or user group has the same access rights to the external repository content as the external repository user group when the associated M-Files user accesses the external repository with M-Files.

3.2.3. Configuring Workflows

M-Files integrates with the organization's administrative and executive processes. With workflows, you can automate the routines of your organization and assign tasks to the correct people at the correct time. Users receive email notifications about task-related issues, and managers can monitor task progress and approve completed tasks.

You can use workflows for example for purchase invoice circulation. Workflow states can then include:

- Awaiting approval
- Approved
- Rejected
- Paid in full

You can select who can transfer the object from one state to the next and who is responsible for the next workflow task. For example, only a management group member can give its approval for payments.

When the invoice is in the *Approved* state, the department for money transactions will automatically know that a new invoice is awaiting payment. When the invoice is paid, it is moved to the *Paid in full* state.

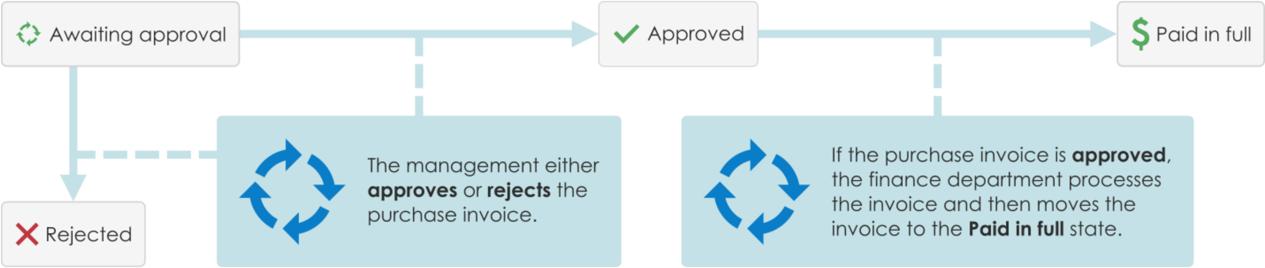

Awaiting approval
Approved
Paid in full
Rejected
The management either **approves** or **rejects** the purchase invoice.
If the purchase invoice is **approved**, the finance department processes the invoice and then moves the invoice to the **Paid in full** state.

Figure 50: Workflows make routine tasks of the organization easier. For example, purchase invoice process.

Graphical Workflow Designer

M-Files Admin includes a graphical user interface for workflow management. See Graphical Workflow Designer for more information.

In this chapter

- Graphical Workflow Designer
- Creating and Editing Workflows

Graphical Workflow Designer

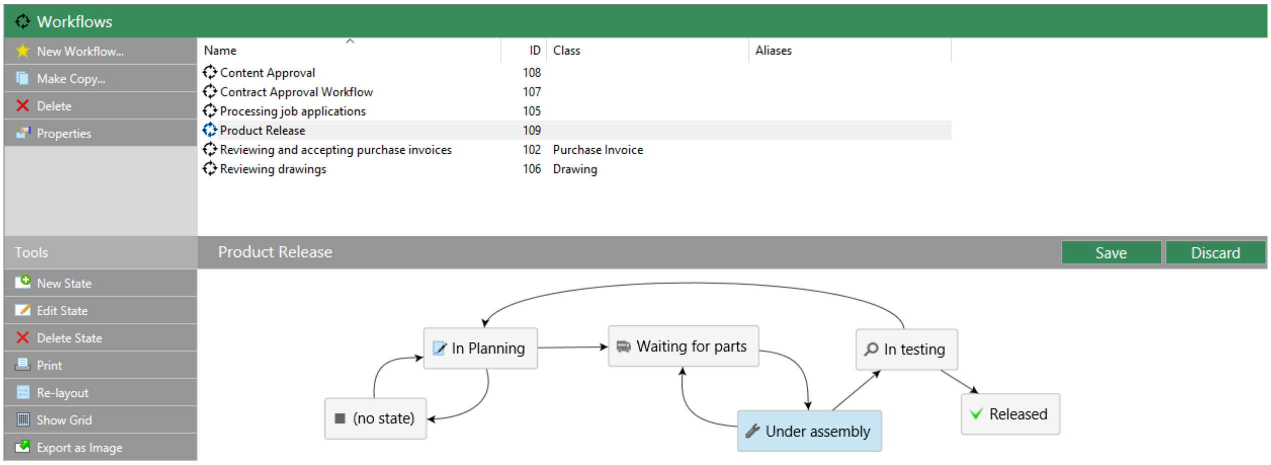
You can use the graphical workflow designer in M-Files Admin to create and edit workflows. Open M-Files Admin, select the vault connection and then the vault in the left-side tree view. Finally, click **Workflows**.

Note: Install Internet Explorer 9 or later on the computer for the designer to operate.

Workspace

The **Workflows** window has two sections:

- The top section shows the available workflows and the task area commands **New Workflow**, **Make Copy**, **Delete** and **Properties**.
- The bottom section shows the graphical workflow designer. See Using the designer and Task pane commands for explanations of the designer-related task area commands.



Name	ID	Class	Aliases
Content Approval	108		
Contract Approval Workflow	107		
Processing job applications	105		
Product Release	109		
Reviewing and accepting purchase invoices	102	Purchase Invoice	
Reviewing drawings	106	Drawing	

Figure 51: The graphical workflow designer in M-Files Admin.

The **Save** and **Discard** commands are in the top-right corner of the workspace, on the title bar of the selected workflow. The **Save** command saves all the changes to the workflow. This includes the layout of your graphical representation.

To change the workspace proportions, drag the workflow title bar up or down.

Using the designer

You can use the task area, the graphical designer area, and context menus.

Creating new states

To create new states, click **New State** in the task area or double-click an empty space on the canvas. The dialog for a new workflow state opens.

Note: If a class has a default workflow and a new object is created in the class, the first state is chosen automatically only if the first state is the first on the **States** list of the **Workflow Properties** dialog. The order of states on the list overrides the order of states in the graphical workflow designer.

Editing states

To edit states in the properties dialog, do one of these:

- Double-click the state.
- Select the state and click **Edit State** in the task area.
- Right-click the state and select **Edit** from the context menu.

Deleting states

To delete states, do one of these:

- Select the state and press the Delete key.
- Select the state and click **Delete State** in the task area.
- Right-click the state and select **Delete** from the context menu.

Editing the layout

Drag and drop the workflow states to move them around on the canvas.

Connectors (state transitions)

Arrow connectors between states show the workflow state transitions. To add connectors between the states, move your cursor on the edge of a state rectangle and use drag and drop. The state rectangle has green edges and the cursor changes into a cross (+) when you can draw a connector.

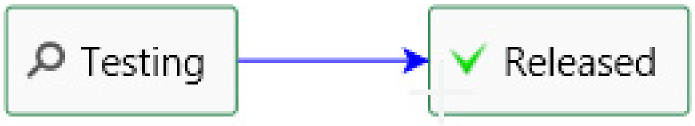


Figure 52: A state transition from **Testing** to **Released**.

Sometimes the connectors can overlap with each other or with the state rectangles. Edit the connector shape to make the layout easier to read. Select a connector and use the two handles to change the shape of the connector.

You can **Edit** or **Delete** the selected state transition from its context menu, and **Straighten** the connector. Double-click the connector to open the properties dialog for the transition.

Zooming and dragging the canvas

Scroll your mouse to zoom in and out or drag the canvas around. Right-click an empty space on the canvas to reset the zoom level.

Task pane commands

States and state transitions can have context-specific task area commands, for example **Edit State** and **Straighten**. The table below shows actions that are common for the designer and your entire workflow:

Click...	To do this...
Re-layout	Arrange workflow components to a default positioning.
Show Grid and Hide Grid	Show or hide the grid in the background.
Print	Make a paper copy of the workflow. **Note:** The print function uses the **Page setup** settings of Internet Explorer for the page header and footer. Set the settings for the header and footer to *empty* if you want to remove them from the printout. To open the **Page setup** dialog, for example with Internet Explorer 10, click the tools button in the top-right corner of the browser and select **Print** > **Page setup**.

Click...	To do this...
Export as Image	Export the workflow as a PNG file. When you click **Export as Image**, the common Windows save dialog for the image file opens.

Tooltips

Move the cursor over the state rectangles and connectors to see possible tooltips.

Tooltips can contain the element title, description, and information on the state transition conditions and special actions.

Creating and Editing Workflows

You can automate company processes with workflows. To create a workflow, click **Workflows** in the left-side tree view of M-Files Admin and select **New Workflow** in the task area.

In this chapter

- Creating a New Workflow
- Workflow States
- Workflow State Transitions

Creating a New Workflow

1. Open M-Files Admin.

2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Select **Workflows**.

6. In the task area, click **New Workflow**.

   ✓ The **Workflow Properties** dialog opens.

7. In **Name**, enter a name for the workflow.

8. Optional: In **Description**, enter a description.

9. Optional: Click **Add** to add states to the workflow.

   ⓘ You can also add states with the **New State** command in the graphical workflow designer. Use the arrow buttons to change the order of the states.

   ⓘ **Note:** If a class has a default workflow and a new object is created in the class, the first state is chosen automatically only if the first state is the first on the **States** list of the **Workflow Properties** dialog. The order of states on the list overrides the order of states in the graphical workflow designer.

10. Optional: In **Allow using this workflow with the following class**, select a class if you want to let users select this workflow for objects of that class only.

11. Optional: On the **Permissions** tab, select who can see the workflow.

12. Optional: On the **Advanced** tab, enter an alias for the workflow.

Use semicolons (;) to separate many aliases.

When automatic aliases are in use and you write a name on the **General** tab, the **Aliases** field on the **Advanced** tab is automatically filled in. The alias has the format *<predefined prefix>.<name>*. Configure automatic aliases for your vault in Advanced Vault Settings.

13. Click **OK**.

The new workflow is added to the list of workflows. Next, you can add workflow states and state transitions to it.

To do this, select the workflow from the list and use the tools on the **Tools** pane. For step-by-step instructions, see Adding States to a Workflow and Adding State Transitions to a Workflow.

Workflow States

Use workflow states to divide workflows into smaller stages. To add a state to a workflow, in the Graphical Workflow Designer, double-click the canvas or select **New State** in **Tools**. In the **State Properties** dialog, specify the settings. See the information in the table.

Open the tab	To...
General	Give a name and description for the state.
Conditions	Specify the preconditions and postconditions for the state.
Actions	Specify what happens when an object is moved to the state. For instructions, see Workflow State Actions.
Advanced	Assign an alias for the state. When automatic aliases are in use and you write a name on the **General** tab, the **Aliases** field on the **Advanced** tab is automatically filled in. The alias has the format *<predefined prefix>.<name>*. Configure automatic aliases for your vault in Advanced Vault Settings. For more information on aliases, see Associating the Metadata Definitions.

For step-by-step instructions, see Adding States to a Workflow.

In this chapter

- Adding States to a Workflow
- Workflow State Conditions
- Workflow State Actions

Adding States to a Workflow

1. Open M-Files Admin.

2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Select **Workflows**.

   ✓ The Graphical Workflow Designer is opened.

6. In the list of workflows, select a workflow.

   ✓ The workflow opens in the graphical workflow designer.

7. Click **New State** on the **Tools** pane.

   ✓ The **State Properties** dialog opens.

8. In the **Name** field, enter a name for the workflow state.
9. Optional: In the **Description** field, enter a description for the state.
10. Optional: On the **Conditions** tab, specify the preconditions and postconditions that must be met before an object can be moved to or out of this state.

    ℹ For more information, see Workflow State Conditions.

11. Optional: On the **Actions** tab, specify the actions that are done when an object is moved to this state.

    ℹ For more information, see Workflow State Actions.

12. Click **OK** to close the **State Properties** dialog.
13. Repeat steps from 7 to 12 to add more states to the workflow.
14. In the designer, click **Save**.

The states are added to the workflow and shown in the graphical workflow designer. Next, you can add state transitions between the states.

Tip: To change the icons of the workflow states, open **Metadata Structure (Flat View)** > **Value Lists**. Then click **Show All Value Lists**, double-click **Workflows**, and finally click **Contents**. Select the workflow and the state and click **Change Icon**. For more information, see Changing the Icon of a Value in a Value List

Workflow State Conditions

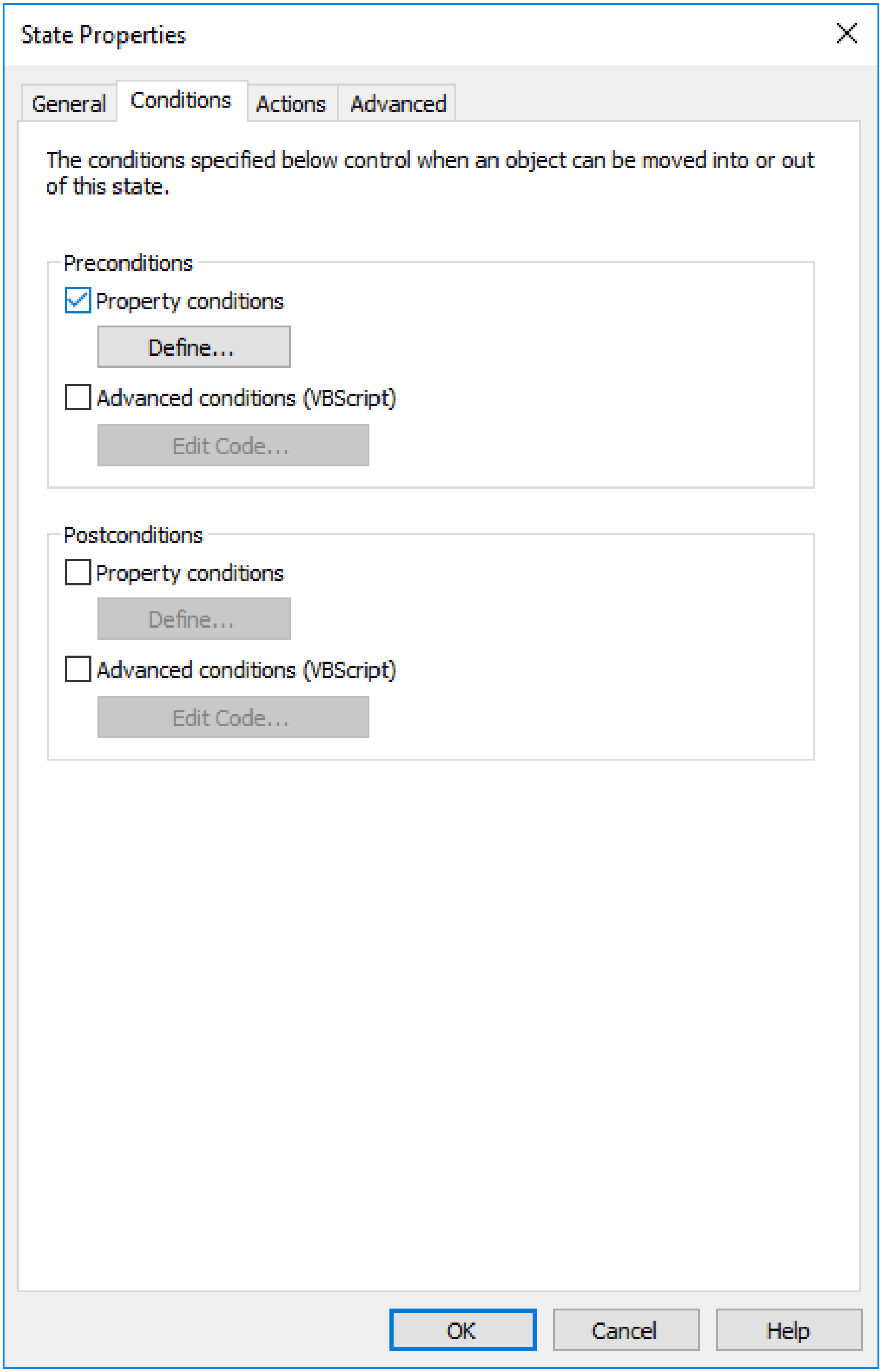
On the **Conditions** tab of the **State Properties** dialog, you can specify different preconditions and postconditions for the state transitions. For example, you can select properties or their values that a document must have before it is moved to a different state. The conditions can also show users that specified documents (for example, project documentation) must be on a certain level before it is possible to move them to the next level.

To open the dialog, see instructions on editing states.

It is possible to use variables, generic features of VBScript, and M-Files API to specify conditions that meet special needs.

You can use these variables: `VaultSharedVariables`, `MFScriptCancel`, `CurrentUserID`, `Vault`, `DisplayID`, `ObjVer`, `PropertyValues`, `StateID`, `PropertyDef`, `SavepointVariables`, `TransactionCache`, and `GetExtensionObject`. For more information about variables, see Available VBScript Variables.

Note: The M-Files API documentation is available online: M-Files API.



State Properties

The conditions specified below control when an object can be moved into or out of this state.

Preconditions

☑ Property conditions

□ Advanced conditions (VBScript)

Postconditions

□ Property conditions

□ Advanced conditions (VBScript)

Figure 53: The **Conditions** tab of the workflow state properties.

Preconditions

The state preconditions specify the properties that an object must have before it can be moved to this state.

For example, the document must contain the **Approved by** information before it is moved to the **Approved** state.

Postconditions

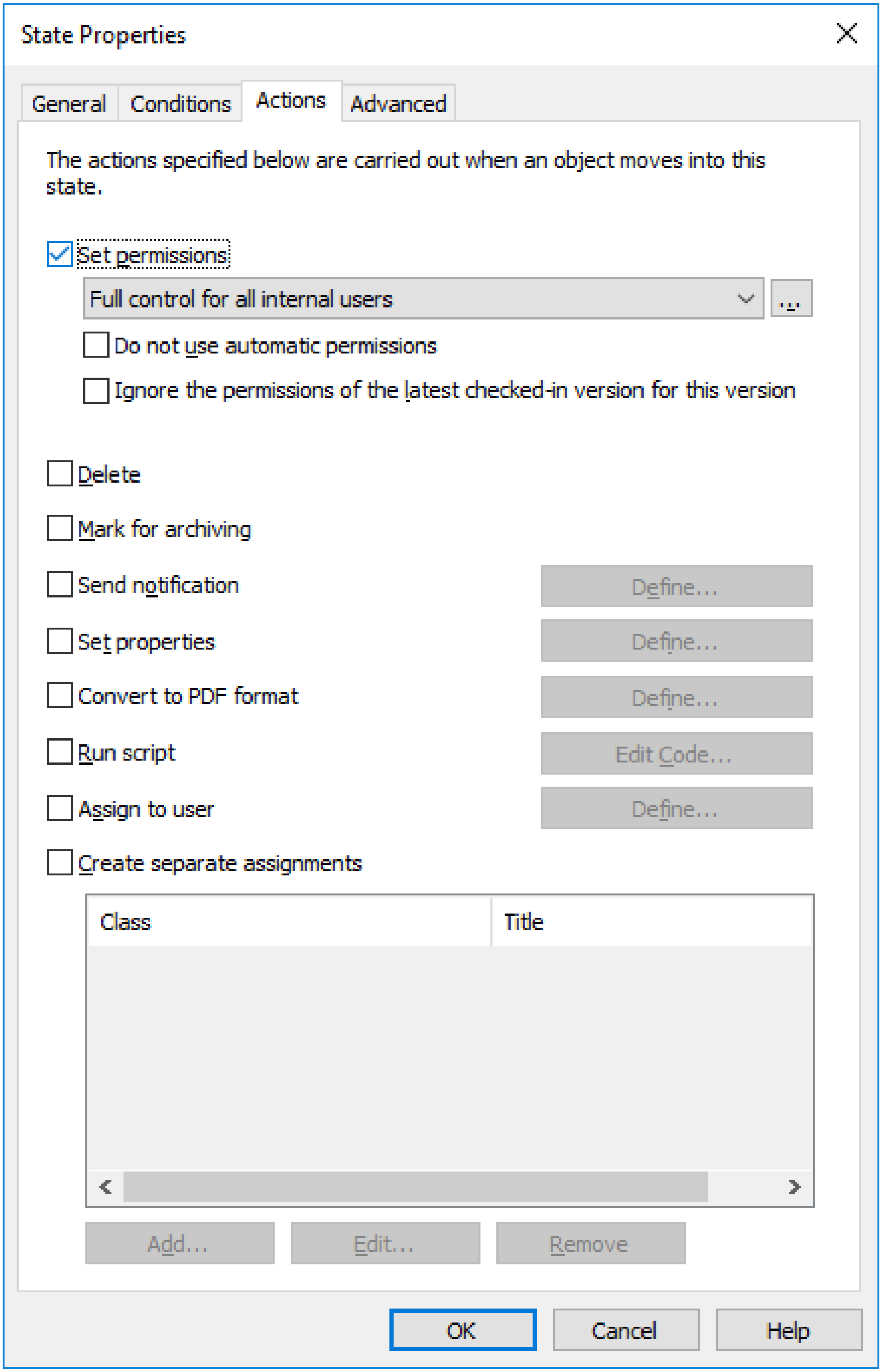
The state postconditions specify the properties that an object must have for it to be moved out of this state.

For example, the purchase invoice must have the **Cost center** information before it is moved from the **Awaiting definition of cost center** state.

Workflow State Actions

Use the **Actions** tab of the **State Properties** dialog to specify what happens when an object is moved to a specific workflow state. To open the dialog, see instructions on editing states.

Click on different parts of the screenshot below for a description of the settings.



The actions specified below are carried out when an object moves into this state.

☑ Set permissions

Full control for all internal users

□ Do not use automatic permissions

□ Ignore the permissions of the latest checked-in version for this version

□ Delete

□ Mark for archiving

□ Send notification

□ Set properties

□ Convert to PDF format

□ Run script

□ Assign to user

□ Create separate assignments

Class	Title

1. Set permissions, Delete, and Mark for archiving
2. Send notification and Set properties
3. Convert to PDF format
4. Run script
5. Assign to user
6. Create separate assignments

The actions are done in this order:

1. Mark for archiving
2. Assign to user
3. Create separate assignments
4. Send notification
5. Set properties
6. Convert to PDF format
7. Set permissions
8. Run script
9. Delete

In this chapter

Set permissions, Delete, and Mark for archiving

As a result of a state transition, new permissions can be specified, and the object can be deleted, and archived, or both. You can select several options of the **Actions** tab at the same time.

Set permissions

Do not use automatic permissions

If you select this option, the object bypasses the automatic permissions that would usually be applicable to the object. Use the **Set permissions** feature to change the effective permissions for the object version.

Ignore the permissions of the latest checked-in version for this version

The object permissions in M-Files are version-specific. To get access to the latest object version, you must have at least read access to it. To get access to a previous version, you must have at least read access to that specific version **and** to the latest version. If you select this option, M-Files ignores the permissions of the latest checked-in version and gives users access to older object versions where they have at least read access rights. The permission settings of the latest version do not change this access.

For example: There is an SOP and its workflow has the states **Draft**, **Waiting for Approval**, and **Approved**. All three states have different permissions. 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). It is moved back to the **Draft** state for changes and the permissions are changed so that only the document creator can see it. If the option **Ignore the permissions of the latest checked-in version for this version** is enabled, all users have access to the document version 3, but not to the latest one. If the option is disabled, only the document creator can see the document version 3.

Note: Even if the **Ignore the permissions of the latest checked-in version for this version** option is selected, the document is not visible in searches and views if the Look in the metadata of all versions option is disabled.

Send notification and Set properties

Send notification

To send a notification, enable **Send notification** on the **Actions** tab and click **Define**. In the **Notification** dialog, click **Add** to specify the recipient users and user groups. The **Select Users or User Groups** dialog has also options to select users from metadata or from state transition.

User from metadata

You can use pseudo-users in state transitions. For example, you can specify that only the project manager can accept invoices that are linked to the project. With pseudo-users, the right to do state transitions is not assigned to a specific person. Instead, object metadata specifies the right dynamically.

User from state transition

You can use previous state transitions to select the users. For example, only the user who originally moved the document to the **Approved** state can move the document from that state to **Approval undone**.

Subject and **Message**

Enter the notification subject and the message.

Use the **Add Placeholder** buttons to insert values from the object metadata to the subject line or message content (see also the placeholder descriptions under Personalizing Notification Messages).

Set properties

It is possible that different object properties and values are added or changed when an object's state is changed. For example, you can specify that the **Published** version label is given to a drawing when it is moved to the **Approved** state.

Use the properties of the data type **Date**, **Time**, or **Timestamp** to have M-Files use the time value of the state transition as the property value.

Convert to PDF format

When the object's state changes, M-Files can convert the object files automatically to the PDF format. Conversion to PDF is possible for these file types:

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft Visio

- RTF
- OpenOffice files

During the conversion, M-Files updates the M-Files property fields in Microsoft Word and Microsoft Excel documents with the object's current metadata.

Tip: If there are problems with non-English content, you can try to enable the Advanced Vault Settings option **PDF Conversion** > **Word Files** > **Extended Language Support**.

Conversion settings

When you activate the **Convert to PDF** option in the **Actions** tab, M-Files converts the files in a single-file or multi-file document to the PDF format automatically when the object's state changes.

Click **Define** to access these advanced settings for the conversion:

- **Store each PDF file as a separate file next to the original file**: Select this option to keep the original file. In this case, M-Files creates the PDF as a new file with the same name as the original file. If the document is a single-file document, M-Files changes it into a multi-file document and adds the PDF file to it.
- **Overwrite existing PDF files**: Select this option to overwrite existing PDF files with the same name in a multi-file document. In this case, these PDF files are replaced with the versions created with the workflow state action. If this option is not selected and a multi-file document already has a PDF file with the same name, M-Files notifies of the error and does not create the PDF file.
- **Convert to PDF/A-1b**: Select this option 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 standard PDF, and files converted to PDF/A are often larger than files converted to standard PDF. In addition, in export to PDF/A, certain advanced appearance settings can be ignored. Use the conversion to PDF/A form only if it is 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 option to prevent the state transition in cases where the PDF conversion is not possible (for example, ZIP files). If this option is selected and the PDF conversion is not possible, M-Files notifies of the error and prevents the state transition.

Run script

It is possible to use variables, generic features of VBScript, and M-Files API to specify operations in more detail. For example, you can set consecutive numbers for different publication versions or include the send date for a document when it moves to the **Sent** state.

To use this functionality, enable **Run script** on the **Actions** tab, click **Edit Code**, and enter the script.

You can use these variables: `VaultSharedVariables`, `MFScriptCancel`, `CurrentUserID`, `Vault`, `DisplayID`, `ObjVer`, `PropertyValues`, `StateID`, `PropertyDef`, `SavepointVariables`, `TransactionCache`, and `GetExtensionObject`. For more information about variables, see Available VBScript Variables.

Note: When you develop new extensions or edit existing ones, we recommend that you replace VBScript content with Vault Application Framework (VAF) compatible code for future compatibility. For more information on the benefits of VAF development over VBScript, refer to The Vault Application Framework in M-Files Developer Portal.

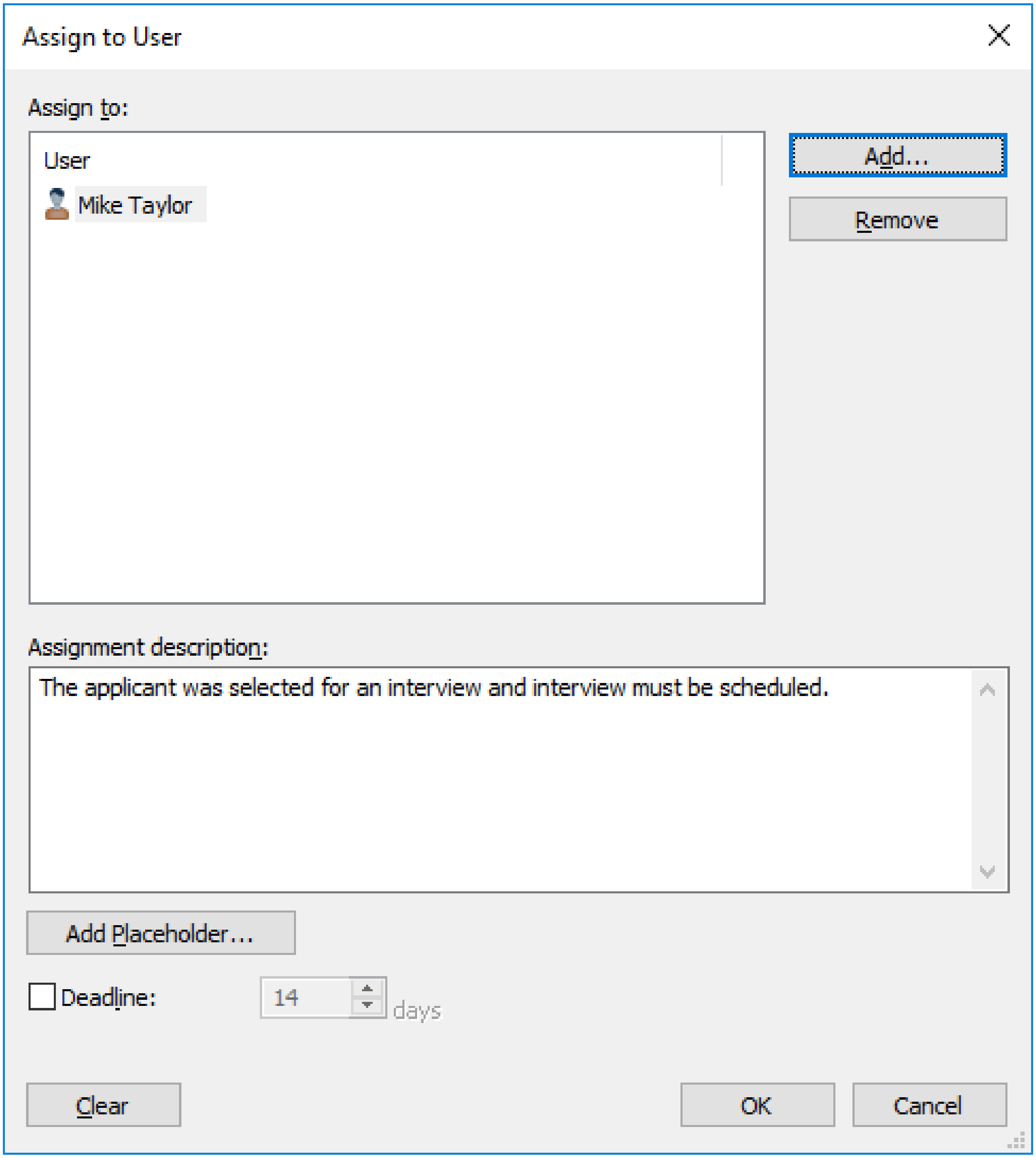
Note: The M-Files API documentation is available online: M-Files API.

Assign to user

Assignments are an important part of workflows. Assignments move information and responsibility for task completion to the correct person automatically during a state transition. M-Files has two types of assignments with workflows: **Assign to User** and **Create separate assignments**.

Select **Assign to User** on the **Actions** tab to create an assignment that does not result in a separate object. If an assignment is created with this option, it is switched to the completed state when one of the assignees changes the document state in the workflow (usually moves the object to the next state).

Click **Define** to specify the assignment.



Mike Taylor

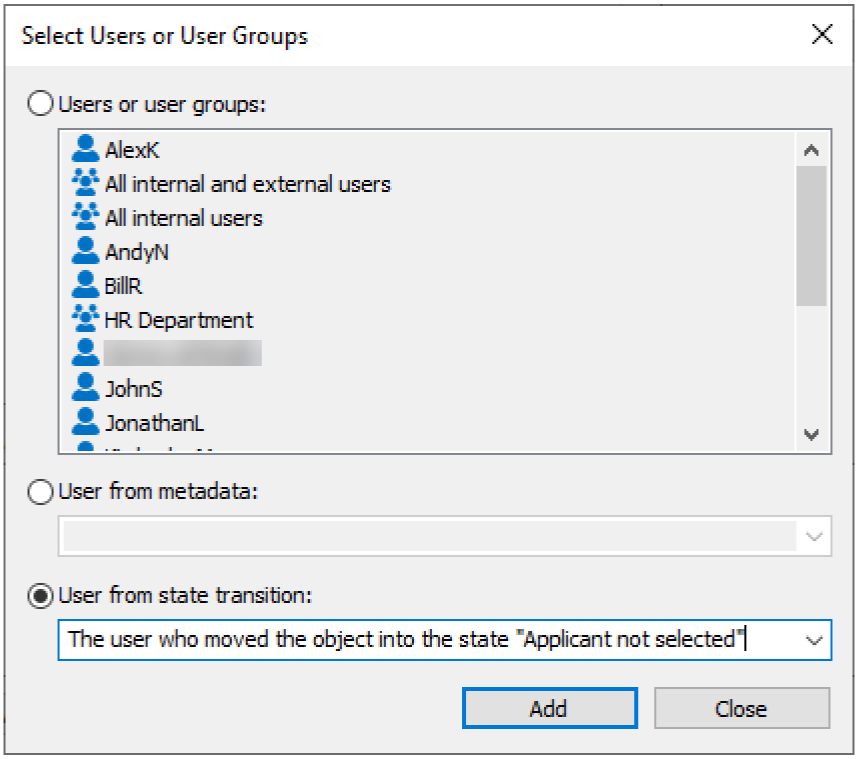
The applicant was selected for an interview and interview must be scheduled.

□ Deadline: 14 days

Figure 54: The **Assignment** dialog.

Adding and Removing users

You can manage the persons responsible for the task with the **Add** and **Remove** buttons. When you add users, select whether to add individual users from the **Users or user groups** list, users from metadata, or users from state transition. For example, a person specified in the **Approved by** property in the object metadata can automatically be set as the assignee. For more information on the **Select Users or User Groups** dialog, see Workflow State Transition Permissions.


Select Users or User Groups

○ Users or user groups:

- AlexK
- All internal and external users
- All internal users
- AndyN
- BillR
- HR Department
- [redacted]
- JohnS
- JonathanL

○ User from metadata:

● User from state transition:

The user who moved the object into the state "Applicant not selected"

Figure 55: Selecting a user based on an earlier state transition.

Managing the Assigned to property

If the object is in a state that created an assignment, the object's properties show whom the object has been assigned to. The assignee can change the state and complete the assignment with the functions in the task area, metadata card, or in the context menu. For step-by-step instructions, see Workflows and Completing an Assignment.

> **Note:** If a user creates the assignment, only this user and users with the **Full control of vault** rights can edit the **Assigned to** property value. If the assignment is created through a workflow, only users with full control of the vault can edit the property value.

Create separate assignments

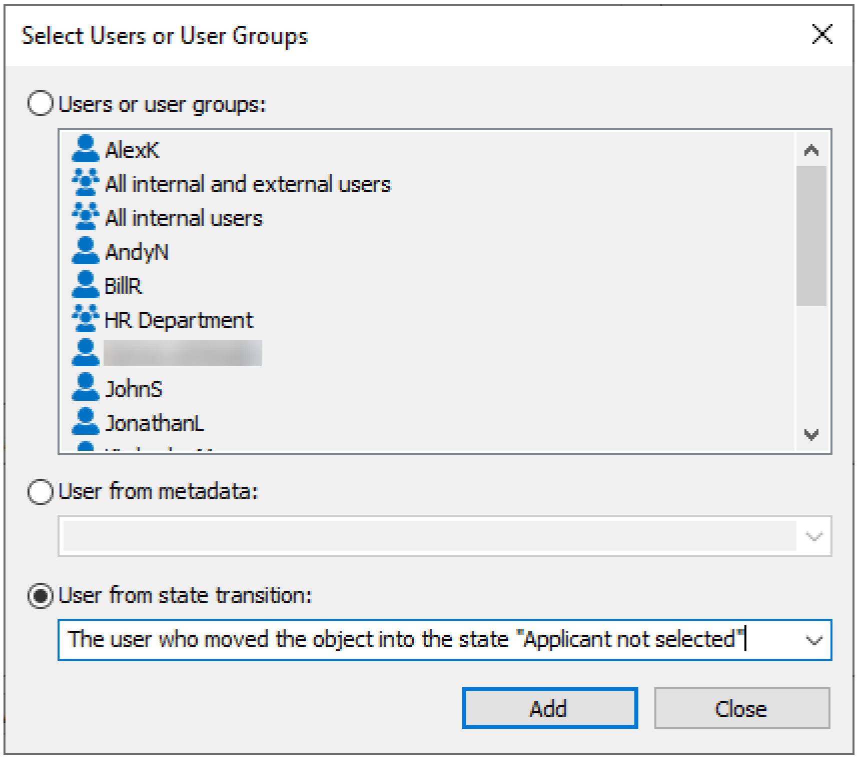
Assignments are an important part of workflows. Assignments move information and responsibility for task completion to the correct person automatically during a state transition. M-Files has two types of assignments with workflows: **Assign to User** and **Create separate assignments**.

You can specify M-Files to create separate assignments when the object workflow is moved to a certain state. To open the **Create Separate Assignment** dialog, enable the **Create separate assignments** option on the **Actions** tab and click **Add**.

To have the workflow state change automatically after the completion of the separate assignments, specify that in the Trigger options of the state transition.

Adding and Removing users

You can manage the persons responsible for the task with the **Add** and **Remove** buttons. When you add users, select whether to add individual users from the **Users or user groups** list, users from metadata, or users from state transition. For example, a person specified in the **Approved by** property in the object metadata can automatically be set as the assignee. For more information on the **Select Users or User Groups** dialog, see Workflow State Transition Permissions.



Select Users or User Groups

○ Users or user groups:

- AlexK
- All internal and external users
- All internal users
- AndyN
- BillR
- HR Department
- [redacted]
- JohnS
- JonathanL

○ User from metadata:

● User from state transition:

The user who moved the object into the state "Applicant not selected"

Figure 56: Selecting a user based on an earlier state transition.

Monitoring

You can specify M-Files to notify certain users each time a task is completed. To do this, click **Monitoring** in the **Create Separate Assignment** dialog and select the users. M-Files makes the assignment submitter automatically a task monitor.

Uncompleted and completed assignments are easy to identify, because their objects have separate icons.

Assignment class

The assignment class specifies the assignment type and assignment completion conditions. For more information, see Assignment Class.

Assignment description

Add a free-form description of the task. The description is shown in the notification email that is sent to the assignee. You can also include notification templates supported by M-Files in the description. For more information on notification templates and placeholders, see Editing Notification Settings in M-Files Admin.

Deadline

You can specify a deadline for the assignment. M-Files sends an automatic reminder if the assignment has not been marked complete when the deadline is approaching. The reminder is sent with a common notification rule. An administrator can also delete the rule.

Tip: It can be useful to create a view to show assignments with an approaching deadline. For more information about views, see Creating a View.

Creating a Workflow State with a Separate Assignment

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Workflows**.

   ✓ The Graphical Workflow Designer is opened.
6. In the list of workflows, select a workflow.

   ✓ The workflow opens in the graphical workflow designer.
7. In the designer, select a workflow state to which you want to add a separate assignment and select **Edit State** on the **Tools** pane.

   ✓ The **State Properties** dialog opens.
8. On the **Actions** tab, select **Create separate assignments** and click **Add**.

   ✓ The **Create Separate Assignment** dialog opens.
9. Add the user or users the separate assignment is assigned to.
10. Optional: Click **Monitoring** to add a user or users who will get a notification when this assignment is marked complete, approved, or rejected.
11. In the **Select assignment class** drop-down menu, select the assignment class for the separate assignment.
12. In the **Title** field, enter a title for the assignment. Click **Add Placeholder** to add placeholders for metadata properties.
13. In the **Assignment description** field, enter a description for the assignment.
14. Optional: Select **Deadline** and specify the number of days for the separate assignment deadline.
15. Click **OK** to close the **Create Separate Assignment** dialog.
16. Click **OK** to close the **State Properties** dialog.
17. In the designer, click **Save**.

The separate assignment is added to the workflow state. When an assignment with the related workflow is moved to this state, M-Files creates a separate assignment and adds it as a linked assignment under the primary assignment.

Workflow State Transitions

Workflow state transitions are used to move from one workflow state to another. Users can initiate the transitions manually or M-Files Server triggers them automatically. You can also specify that electronic signature is necessary to complete state transitions.

To see and edit the workflow state transition properties, in theGraphical Workflow Designer, select a state transition arrow and click **Edit Transition** in **Tools**. In the **State Properties** dialog, specify the settings. See the information in the table.

Tab	Description
General	This tab contains the name and description of the state transition.
Permissions	Here you can select the users who can complete the state transition. For more information, see Workflow State Transition Permissions.
Electronic Signature	Here you can turn on electronic signing for a state transition. In this case, users must confirm the state transition with an electronic signature. For more information, see Electronic Signatures.
Trigger	Here you can select conditions for automatic state transitions. For more information, see Trigger.
Advanced	Here you can set an alias for the state transition. Use semicolons (;) to separate many aliases. For more information about aliases, see Associating the Metadata Definitions.

In this chapter

Adding State Transitions to a Workflow

1. Open M-Files Admin.

2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Select **Workflows**.

✓ The Graphical Workflow Designer is opened.

6. In the list of workflows, select a workflow.

✓ The workflow opens in the graphical workflow designer.

7. In the designer, place your cursor on the border of the state from which you want to create a state transition.

   The cursor changes to a crosshair.

8. Hold the primary mouse button and drag the crosshair to the state to which you want to create the state transition.

   A state transition arrow is added between the workflow states.

9. Select the state transition arrow that you just created and select **Edit Transition** on the **Tools** pane.

   The **State Transition** dialog opens.

10. In the **Name** field, enter a name for the state transition.
11. Optional: In the **Description** field, enter a description for the transition.
12. On the **Permissions** tab, specify which users are allowed to do the state transition.

    For more information, see Workflow State Transition Permissions.

13. Optional: Use the settings on the **Electronic Signature** tab to set an electronic signature for the state transition.

    For more information, see Electronic Signatures.

14. Optional: Use the settings on the **Trigger** tab to specify a condition that triggers this state transition when the condition is fulfilled.

    For more information, see Trigger.

15. Click **OK** to close the **State Transition** dialog.
16. In the designer, click **Save**.

The state transition is added to the workflow between the selected workflow states. An arrow is shown between the states in the graphical workflow designer.

See also Adding States to a Workflow and Creating a New Workflow.

Parallel State Transitions

You can have many workflow state transitions between two states. This is useful, for example, to specify many automatic transitions based on different criteria. For information about creating state transitions, see Adding State Transitions to a Workflow.

Example: Creating a Workflow with a Parallel State Transition

Let's say that we want to edit an existing sample vault workflow, such as **Reviewing drawings**. The goal is to have an object automatically moved to the **Rejected** state if no one moves it from the **Listed for approval** state to the **Approved** (or **Rejected**) state within 10 days.

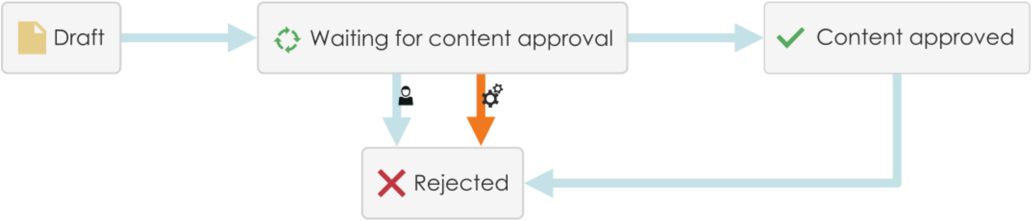


Figure 57: The workflow moves an object to the **Rejected** state automatically if no one moves it to the **Approved** state.

To edit the workflow:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Workflows**.

   ✓ The Graphical Workflow Designer is opened.

6. In the list of workflows, select a workflow. For example, **Reviewing drawings**.

   ✓ The workflow opens in the graphical workflow designer.

7. Click **New State** in **Tools**.

   ⓘ If you already have a **Rejected** state in your workflow, skip this and the next step, and go to step 9.

   ✓ The **State Properties** dialog opens.

8. In the **Name** field, enter `Rejected` and click **OK**.
9. In the designer, place your cursor on the border of the **Listed for approval** state.

   ✓ The cursor changes to a crosshair.

10. Hold the primary mouse button and drag the crosshair to the **Rejected** state.

    ✓ A state transition arrow is added between the workflow states.

11. Do the steps 9 and 10 again to draw one more state transition.
12. Select one of the state transition arrows and select **Edit Transition** in **Tools**.

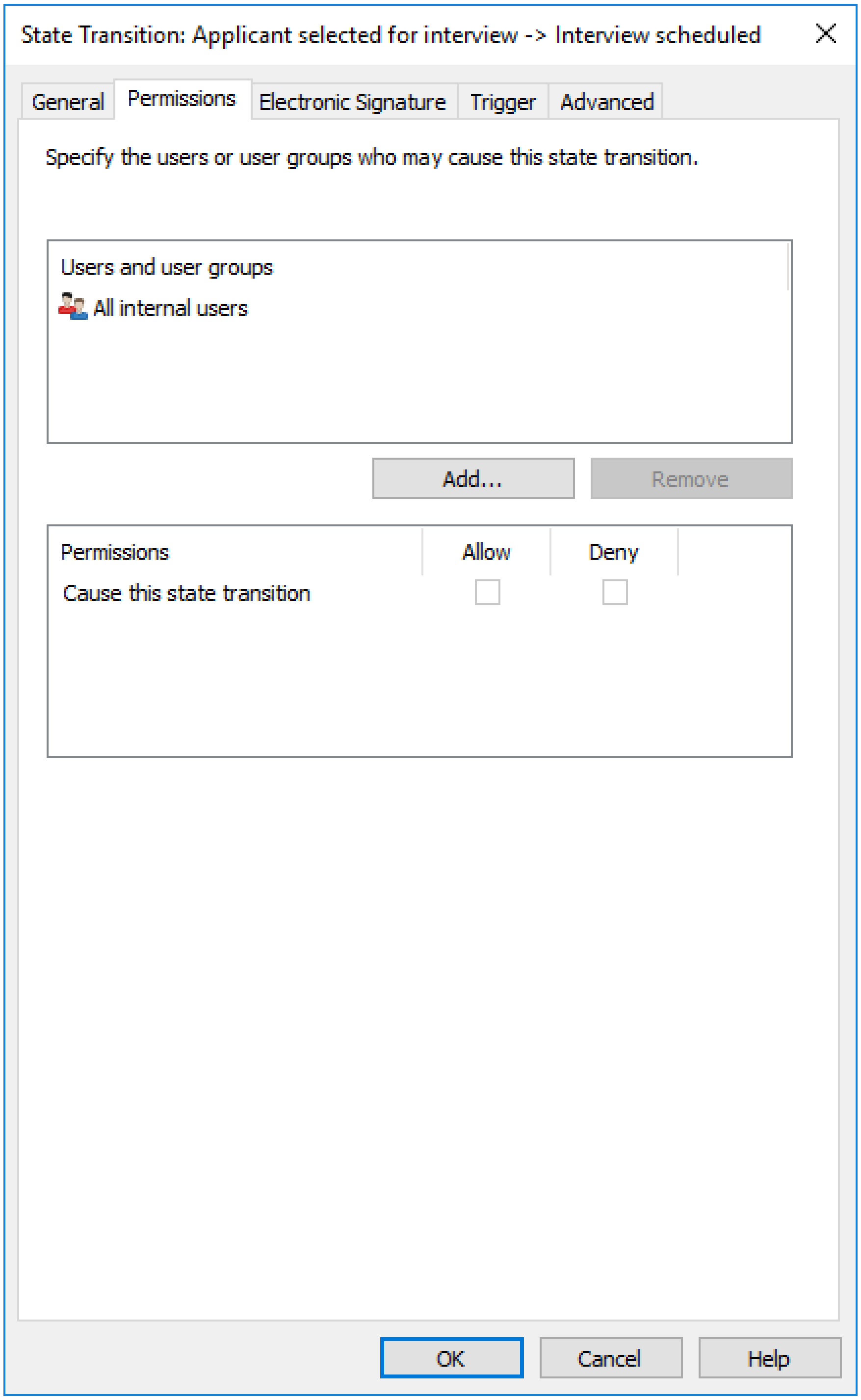
    ⓘ If you see only one arrow between the states, it is possible that the arrows are on top of each other. Click the topmost arrow and drag the handles to reshape the arrow.

13. Go to the **Trigger** tab.
14. Select the **Trigger the state transition after** option, and enter *10* in the **days** field.
15. Click **OK** to close the **State Transition** dialog.

16. In the designer, click **Save**.

You now have a workflow with two parallel state transitions from the **Listed for approval** state to the **Rejected** state. One state transition is initiated by users and another is triggered automatically if users did not initiate the parallel state transition in 10 days.
Workflow State Transition Permissions

On the **Permissions** tab of the **State Transition** dialog, you can specify which users are allowed to do the state transition.



State Transition: Applicant selected for interview -> Interview scheduled

Specify the users or user groups who may cause this state transition.

Users and user groups
All internal users

Permissions	Allow	Deny
Cause this state transition	□	□

Figure 58: The **Permissions** tab of the **State Transition** dialog.

Click **Add** to select users or user groups who can cause the state transition. The **Select Users or User Groups** dialog also has options to select users from metadata or from state transition.

User from metadata

You can use pseudo-users in state transitions. For example, you can specify that only the project manager can accept invoices that are linked to the project. With pseudo-users, the right to do state transitions is not assigned to a specific person. Instead, object metadata specifies the right dynamically.

User from state transition

You can use previous state transitions to select the users. For example, only the user who originally moved the document to the **Approved** state can move the document from that state to **Approval undone**.

Electronic Signatures

The Electronic Signatures and Advanced Logging module with the electronic signature feature expands the M-Files workflows. You can use electronic signatures to certify the state transition. For example, approval of documents.

When you set an electronic signature for a state transition, M-Files requires the signature to change the state. The user must enter their identification data and log in to add the electronic signature. The state is changed when the object is checked in.

You can change the state with a signature only one object at a time. Only users that use Windows authentication can do state changes that require an electronic signature. The electronic signature does not refer to an electronic "fingerprint".

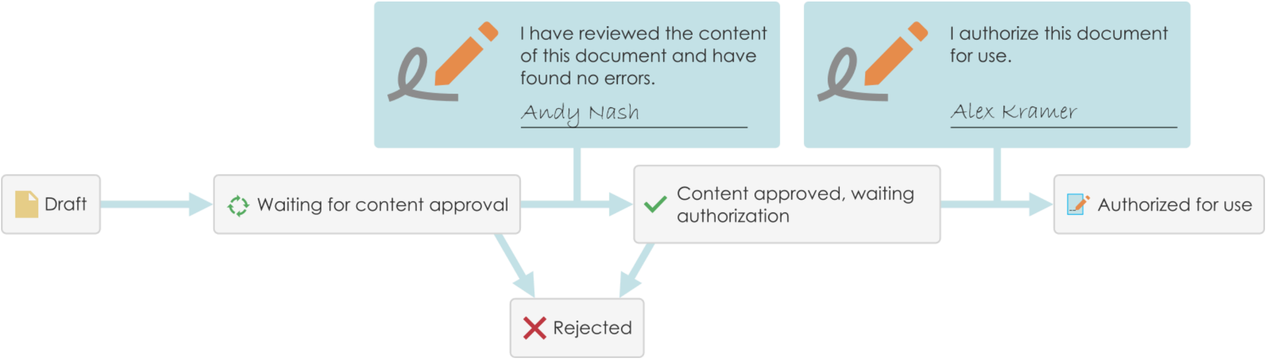

I have reviewed the content of this document and have found no errors.
Andy Nash
I authorize this document for use.
Alex Kramer
Draft
Waiting for content approval
Content approved, waiting authorization
Authorized for use
Rejected

Figure 59: You can require users to give their electronic signature before they can make a specific state transition in a workflow.

The Electronic Signatures and Advanced Logging module is available for a separate fee. This module includes event logging extensions and the electronic signature functionality. For more information, see Electronic Signing and Compliance.

Note:

It is important to understand the login process used for electronic signing in M-Files:

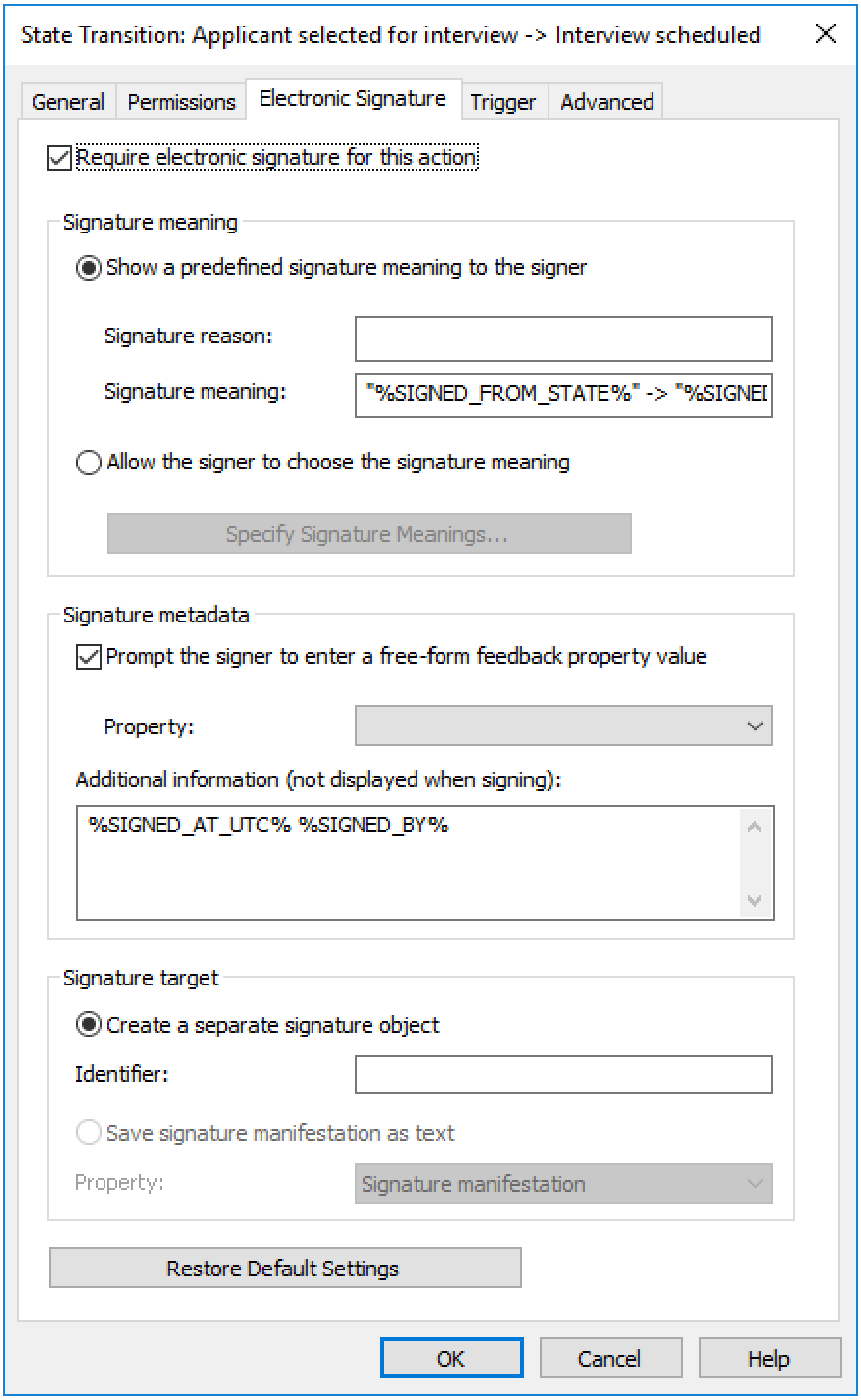
- Normally, users must at least enter their password. It can also be necessary to use multi-factor authentication.
- With federated authentication, the login is done through the identity provider's process, not in M-Files.
    - By default, M-Files sends the Login Prompt parameter as `prompt=login`.

The full login process can also be a legal requirement for electronic signing.

Electronic signature for workflow state transitions

To include an electronic signature in a workflow state transition:

1. Select a transition in the Graphical Workflow Designer.
2. In the task area, click **Edit Transition**.
3. Move to the **Electronic Signature** tab.



State Transition: Applicant selected for interview -> Interview scheduled
General
Permissions
Electronic Signature
Trigger
Advanced
Specify Signature Meanings...
Restore Default Settings
OK
Cancel
Help

☑ Require electronic signature for this action

Signature meaning

● Show a predefined signature meaning to the signer

Signature reason:

Signature meaning: "%SIGNED_FROM_STATE%" -> "%SIGNEI

○ Allow the signer to choose the signature meaning

Signature metadata

☑ Prompt the signer to enter a free-form feedback property value

Property:

Additional information (not displayed when signing):

%SIGNED_AT_UTC% %SIGNED_BY%

Signature target

● Create a separate signature object

Identifier:

○ Save signature manifestation as text

Property: Signature manifestation

Figure 60: The **Electronic Signature** tab for a state transition.

Select **Require electronic signature for this action** to modify the options.

Signature meaning

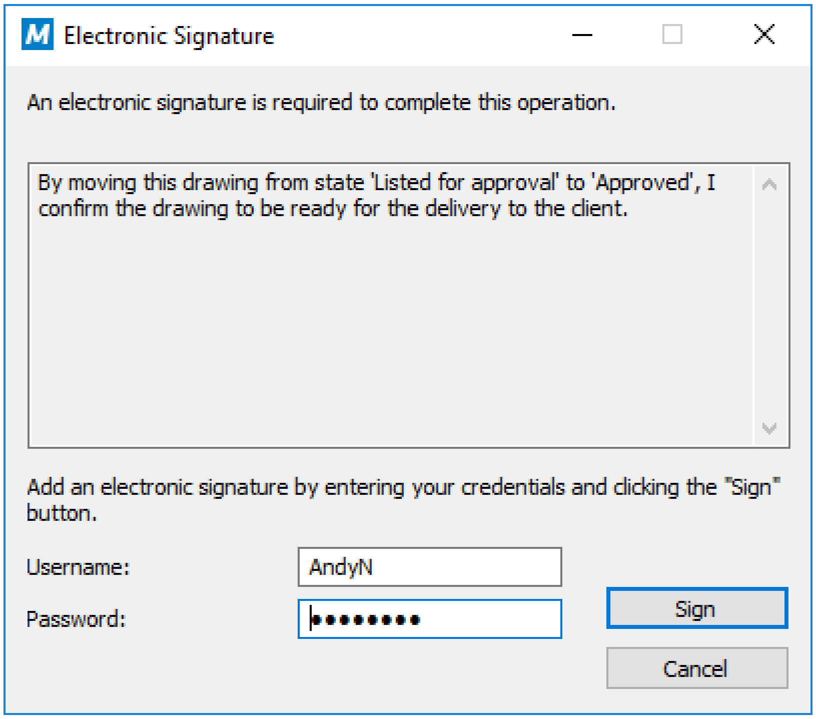
With the **Signature meaning** options, you can select either a predefined signature reason-meaning pair or specify multiple meanings for the signer to choose from. The signature reason is a brief heading-level description for the signature, such as *Approval of instruction document* or *Approval of invoice*. The signature meaning is a description that tells the signer what will be approved. The maximum number of characters is 500, and you can use placeholders. The placeholders are listed in Placeholders for Signature meaning, Signature reason, and Additional information fields.

Examples

If you entered "Signed by %SIGNED_BY%" in the **Signature meaning**, the actual signature description that the user sees is, for example, *Signed by Alex Kramer*.

If you want the substitute user's name to be shown, use the %SIGNED_BY_WITH_PROXY% placeholder. If you entered "Signed by %SIGNED_BY_WITH_PROXY%" in the **Signature meaning** and Alex Kramer signs, the signature description will be *Signed by Alex Kramer*. If the signer is a substitute user of Alex, the signature description will be *Signed by Andy Nash, on behalf of Alex Kramer*.

In the image, the user has defined this signature meaning: "By moving this drawing from state %SIGNED_FROM_STATE% to %SIGNED_TO_STATE%, I confirm the drawing to be ready for the delivery to the client."



An electronic signature is required to complete this operation.

By moving this drawing from state 'Listed for approval' to 'Approved', I confirm the drawing to be ready for the delivery to the client.

Add an electronic signature by entering your credentials and clicking the "Sign" button.

Username: AndyN

Password: ●●●●●●●●●

Figure 61: The signature meaning displayed on an electronic signature prompt.

Signature metadata

You can set the electronic signature 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 Create a separate signature object) or to the object with the workflow. You can also add more information to the **Additional**

information text box. In **Additional information**, you can use placeholders (listed in Placeholders for Signature meaning, Signature reason, and Additional information fields).

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 where the state transition is in use.

Note: M-Files can create the signature objects only when you set up certain metadata definitions. For more information, see Metadata Definitions for an Electronic Signature Object.

Identifier

The identifier is free-form text. You can set, for example, *Purchase Invoice Approval* as the identifier. In the creation of the signature object, the identifier becomes a part of the metadata for the object. The *Identifier* property can be used in, for example, scripts for state-transition functions or in searches to individualize a certain type of signature.

Save signature manifestation as text to a property

Select the property that you want the signature to be associated with. Then the specified content of the signature is shown as the property value in the metadata of the object. 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. You can find other signatures with their contents (manifestations) from the version history of the relevant object.

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.

Placeholders for Signature meaning, Signature reason, and Additional information fields

The available placeholders to be used with the **Signature meaning**, **Signature reason**, and **Additional information** fields are listed in this table.

Placeholder	Description
%SIGNED_AT_UTC%	The UTC time at the time of signing. You can use this placeholder only with the **Additional information** field.
%SIGNED_AT_LOCAL%	The time on the client computer at the time of signing. You can use this placeholder only with the **Additional information** field.
%SIGNED_AT%	The time on the server computer at the time of signing. You can use this placeholder only with the **Additional information** field.
%SIGNED_BY%	The signer name.

Placeholder	Description
%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%	Shows the name of the signer and the user on behalf of whom an assignment is electronically signed. For example: "Preston Present, on behalf of Abraham Absent". See the usage examples.

In this chapter

- Metadata Definitions for an Electronic Signature Object
- Inserting the Signature Property to Microsoft Office Documents

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 M-Files Compliance Kit, these definitions should already be available. Otherwise, you should create the metadata definitions below 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
```

Required property definitions for the signature object

When you have created the 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 property definitions listed below:

Suggested property name	Alias	Data type	Description
Identifier	M-Files.QMS.Signature.Identifier	Text	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	M-Files.QMS.Signature.Reason	Text	A brief heading-level description for the signature.

Suggested property name	Alias	Data type	Description
Signature meaning	M-Files.QMS.Signature.Meaning	Text (multi-line)	A description enabling the signer to understand what is being approved.
Signer	M-Files.QMS.Signature.Signer	Choose from list "Users"	The vault user electronically signing the state transition.
User	M-Files.QMS.Signature.User	Choose from list "Users"	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 required 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:

Alias	Data type	Description
M-Files.QMS.Signature.Signer.Name	Text	Contains the full name of the signer.
M-Files.QMS.Signature.Signer.Account	Text	Contains the M-Files account name of the signer.
M-Files.QMS.Signature.LocalTimestampText	Text	The local time of the signature as text, including the timezone information.
M-Files.QMS.Signature.UTCTimestampText	Text	The UTC time of the signature as text, including the timezone information.
M-Files.QMS.Signature.UTCTimestamp	Timestamp	The UTC timestamp of the signature.
M-Files.QMS.Signature.Date	Date	The signature date in local (server) time.
M-Files.QMS.Signature.FromState	Choose from list "States"	The workflow state prior to the state transition. Available only when signing state transitions.
M-Files.QMS.Signature.ToState	Choose from list "States"	The workflow state after the state transition. Available only when signing state transitions.
M-Files.QMS.Signature.StateTransition	Choose from list "State Transitions"	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 Compliance Kit, 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.

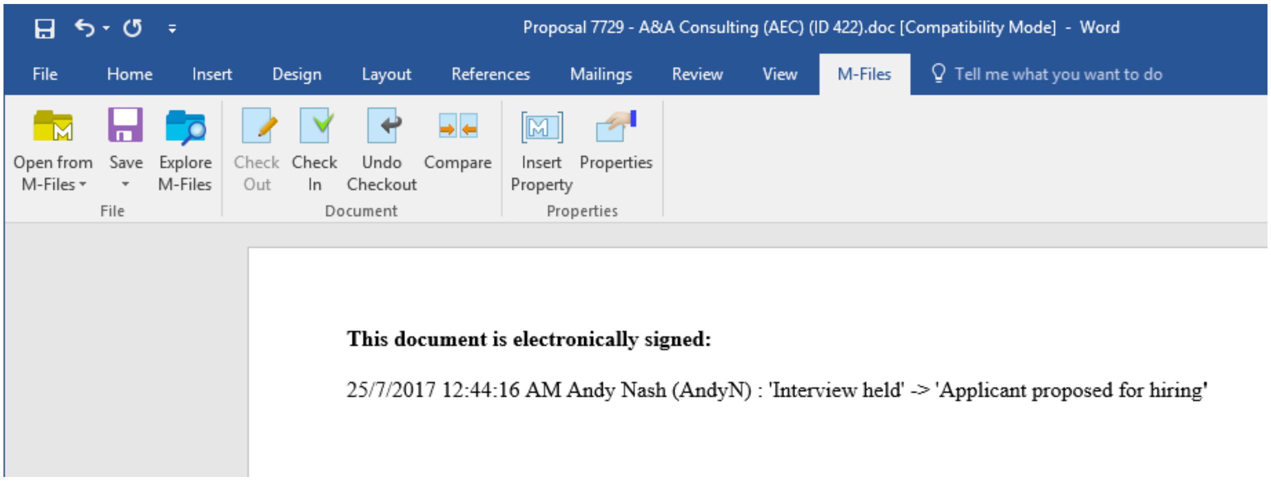
Other metadata for the signature object are created automatically on the basis of the signature definitions.

Inserting the Signature Property to Microsoft Office Documents

The text content of the signature property can be added to a Microsoft Word, Microsoft Excel, or Microsoft PowerPoint 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.



This document is electronically signed:

25/7/2017 12:44:16 AM Andy Nash (AndyN) : 'Interview held' -> 'Applicant proposed for hiring'

Figure 62: The signature content (manifestation) can be added to Microsoft Office documents by using the **Insert Property** function.

Note: If the signature is inserted in the Microsoft 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

On the **Trigger** tab of the **State Transition** dialog, you can define a trigger to automatically start a state transition when certain conditions are fulfilled. For example, you can define a state transition to occur when all the assignments of the current workflow state are completed or approved.

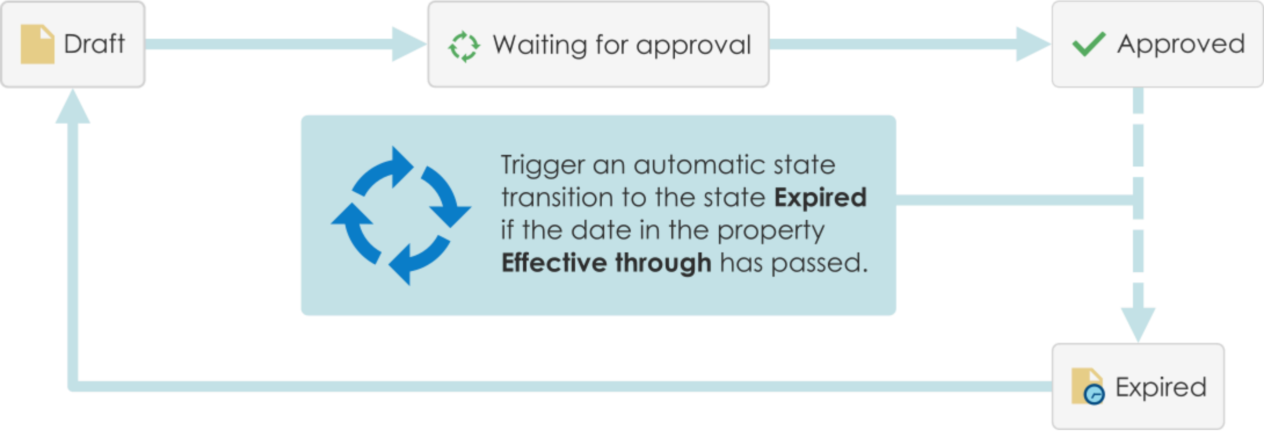

Draft
Waiting for approval
Approved
Trigger an automatic state transition to the state **Expired** if the date in the property **Effective through** has passed.
Expired

Figure 63: An automatic state transition for an object can occur for example on the basis of the property values of the object.

The server does automatic state transitions. User permissions are ignored. This means that you can use permissions to prevent users from manually starting a state transition. M-Files Server does the state transition when all the assignees have completed the task.

Using various criteria for the automatic transition

You can define an automatic state transition to occur when an object fulfills certain conditions. You can configure, for example,that the object is moved to the next state when a user gives it a certain property or certain property value. For example, in the message process workflow, you can define that when a user adds a date to the *Sent* field for the document, the document will automatically be moved to the *Sent* state.

You can also define that the state is changed after users have completed, approved, or rejected all separate assignments. As an alternative, you can specify custom criteria for the state change. For more information about filter settings, see Status-Based Conditions, Property-Based Conditions, File Information Based Conditions, and Permissions-Based Conditions.

Using a user-defined script for the automatic transition

You can also write a script that makes the state transitions occur. This allows you to specify the transition conditions in more detail with 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.

In this script, you can use these M-Files variables: `StateID`, `StateTransitionID`, `AllowStateTransition`, `NextStateID`, `ObjVer`, `DisplayID`, `Vault`, `CurrentUserID`, `CurrentUserSessionInfo`, `PropertyValues`, `VaultSharedVariables`, `SavepointVariables`, `TransactionCache`, `MFScriptCancel`, `GetExtensionObject`, `MasterTransactionID`, `CurrentTransactionID`, `ParentTransactionID`. For more information about variables, see Available VBScript Variables.

Note: The M-Files API documentation is available online: M-Files API.

Evaluation priority

With the evaluation priority, you can define the priority of parallel state transitions on M-Files Server. The priority is sorted from the lowest to the highest number. Zero (0) represents the highest priority.

Defining vaults for state transitions

You can define in which vaults the state transition occur. Enter the vault GUIDs separated by semicolons (;).

Evaluation of the triggering criteria

M-Files evaluates the state transition trigger every 60 minutes and every time the object is changed.

3.2.4. 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) 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.

Tip:

The best practice to specify access rights in named access control lists is through user groups instead of individual users.

Making changes to named access control lists in large vaults can be very slow and may therefore sometimes cause lock conflicts. Therefore, it is recommended that changes to named access control lists and, in turn, to object permissions are made during off-peak hours when user access to the vault is limited.

In this chapter

- Creating a New Named Access Control List

- Modifying Named Access Control Lists
- 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 a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click **Named Access Control Lists**.
6. In the task area, click **New Named Access Control List**.

   Tip: You can also use an existing access control list as a template. To do this, right-click one of the existing ones in the listing area and select **Create Copy**.

7. 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*.

8. Click **Add** to add users or user groups to this named access control list.

   ✓ The **Select Users or User Groups** dialog is opened.

9. Select one of these options:

   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.

      Tip:

      The best practice to specify access rights in named access control lists is through user groups instead of individual users.

      Making changes to named access control lists in large vaults can be very slow and may therefore sometimes cause lock conflicts. Therefore, it is recommended that changes to named access control lists and, in turn, to object permissions are made during off-peak hours when user access to the vault is limited.

      Tip: You can select more than one item at once. Hold down the Ctrl key to select multiple individual items or hold 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.

10. 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.

11. 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.

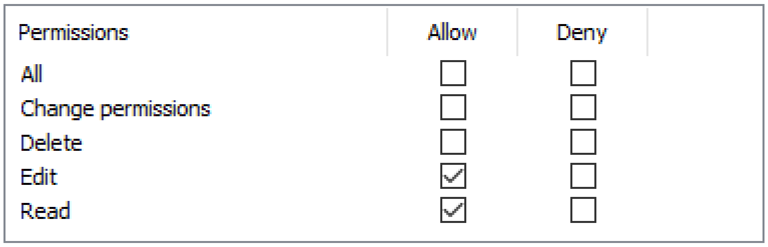
12. Select the permission that you want to adjust and check either:

    a. The **Allow** check box if you want to allow the selected permission for the user or user group.

    or

    b. The **Deny** check box if you wanto to deny the selected permission for the user or user group.

    Tip: For optimal performance in large vaults, named access control lists should only be used to allow access rights instead of explicitly denying them.



Permissions	Allow	Deny
All	□	□
Change permissions	□	□
Delete	□	□
Edit	☑	□
Read	☑	□

13. If you want to adjust additional permissions, repeat the steps 11 and 12.

14. Optional: On the **Permissions** tab, you can specify the users who can see this named access control list.

15. Optional: On the **Advanced** tab, you can specify an alias for the named access control list.

    Use semicolons (;) to separate many aliases.

    For more information, see Associating the Metadata Definitions.

    When automatic aliases are in use and you write a name on the **General** tab, the **Aliases** field on the **Advanced** tab is automatically filled in. The alias has the format <*predefined prefix*>.<*name*>. Configure automatic aliases for your vault in Advanced Vault Settings.

16. Click **OK**.

The new named access control list containing a set of permissions can now be attached to an object with 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 a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.

5. Click **Named Access Control Lists**.

   ✓ The list of named access control lists in the selected vault is opened in the right-side pane.

6. 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.

7. Optional: On the **General** tab, click **Add...** if you wish to add a new user or user group to this named access control list.

   a) Select the user or user group that you want to add to the named access control list.

      Tip:

      The best practice to specify access rights in named access control lists is through user groups instead of individual users.

      Making changes to named access control lists in large vaults can be very slow and may therefore sometimes cause lock conflicts. Therefore, it is recommended that changes to named access control lists and, in turn, to object permissions are made during off-peak hours when user access to the vault is limited.

      Tip: You can select more than one item at once. Hold down the Ctrl key to select multiple individual items or hold down the ⇧ Shift key to select adjacent items on the list.

   a) Optional: Select the **User from metadata** option if you want to add users based on metadata properties to the named access control list. Use the drop-down menu to select the desired property. For more information, see Pseudo-users.

   b) Click **Add** to add the users or user groups to the named access control list.

8. Select the user or user group whose permissions you wish to adjust from the **Users and user groups** list.

9. Depending on your choice, select either the **Allow** or **Deny** option for the desired operations.

10. Click **OK** once you are done to close the **Named Access Control List Properties** dialog.

11. 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.

       Note: Object permissions are updated as an asynchronous background task. Object permissions may be updated when, for example, a named access control list, a user, a user group, or the value of a pseudo-user (such as a project manager) is modified. You may monitor the progress of the task in M-Files Admin in the **Background Tasks** section. For more information, see Monitoring Background Tasks.

    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.

Named Access Control List 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.

Editing Permissions

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click a node that contains items that you want to edit.

   Permission settings are available for these items:

   - **Users**
   - **User groups**
   - **Metadata Structure (Flat View)** > **Object types**
   - **Metadata Structure (Flat View)** > **Value lists**
   - **Metadata Structure (Flat View)** > **Property definitions**
   - **Metadata Structure (Flat View)** > **Classes**
   - **Metadata Structure (Flat View)** > **Class groups**
   - **Workflows**
   - **Named access control lists**
6. Select an item in the listing area.
7. Right-click the item and click **Properties**.
8. Open **Permissions**.
9. In **Users and user groups**, select the user or user group whose permissions to change.

   If the user or user group is not on the list, click **Add**.
10. Specify the permissions for the selected user or user group.

    Allow: Enable this to explicitly give the permission to the selected user or user group.

    Deny: Enable this to explicitly deny the permission from the user or user group.

    The **Deny** setting is normally used to specify an exception to an **Allow** setting. For example, when John Doe is part the group **HR Managers**, you can set **Allow** for the group and **Deny** for John Doe.

You can also leave both settings unselected.

11. Repeat steps 9 and 10 for the rest of the permissions.

12. Click **OK**.

3.2.5. Installing and Managing Vault Applications

You can manage vault-specific client and server applications in M-Files Admin. These applications let you modify and extend client and server behavior. This way you can select to give priority to the functions that are the most important for the efficiency of your organization.

Creating applications requires advanced programming skills. Instructions for the programming are available from the M-Files technical staff for a separate fee. For documentation and sample applications, refer to M-Files Developer Portal.

Important information

- The maximum size for extracted files of a client application is 10 MB.
- A vault can have a maximum of 100 applications.
- The file format of a vault application to be installed must be MFAPPX. If the vault application has been given to you in another format, please contact the supplier.
- Signed applications have been validated by M-Files.
  - In a shared M-Files Cloud environment, vault administrators can install signed applications only. For more information on installing vault applications in M-Files Cloud, refer to Who can install vault applications in M-Files Cloud? in M-Files Support Portal.
  - To install a signed application in an on-premises environment, the server machine must use M-Files June '22 Update or later. Additionally, the server operating system must have the latest root certificate authority (CA) certificates. If you cannot install the signed application, try to install an unsigned version of the application if one is available.

To manage the applications of a vault:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Do one of these:

   a. Expand **Document Vaults**, and then right-click a vault.

      or

   b. Expand **Ground Link Proxies**, and then right-click a Ground Link proxy to configure the connector over Ground Link.
4. Select **Applications**.

   ✓ The **Applications** dialog is opened.
5. Do one or more of the operations listed here. Take note that, in most cases, it is necessary to restart the vault for the changes to take effect. Taking a vault offline should always be done in a controlled manner and the vault users should be notified beforehand.

If you want to...	Do the following steps:
Install a new application	**Warning:** Do not install applications from untrusted sources. **a.** Click the **Install** button. **b.** Browse for the application package and click **Open**. **c.** Click **Yes** to restart the vault.
Uninstall an application	**a.** Select the application that you want to uninstall in the applications listing. **b.** Click **Uninstall**. **c.** Click **Yes** to confirm uninstalling the application. **d.** Click **Yes** to restart the vault.
Export an application	**a.** Select the application that you want to export in the applications listing. **b.** Click the **Export** button. **c.** Select the location and the file name for the export package and click **Save**.
Disable an application and uninstall it from all users	**a.** Select the application that you want to disable in the applications listing. **b.** Click **Disable**. **c.** Click **Yes** to confirm uninstalling the application. **d.** Click **Yes** to restart the document vault.
Enable a disabled application	**a.** Select the disabled application in the application listing. **b.** Click **Enable**. **c.** Click **Yes** to restart the vault.
See the license status, or install or change the license of an application	**a.** Select the application in the applications listing. **b.** Click the **License** button to open the **Application License Management** dialog and to view the license status and information of the selected application. **Note:** In M-Files Cloud and on on-premises servers that use license automation, you get the license automatically for official M-Files add-ons. If necessary, click **Refresh** to activate the license.

If you want to...	Do the following steps:
	c. If necessary, click the **Install License** button, browse for the license file, and then click **Open**.

6. 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 the classic M-Files Desktop, see Managing Vault Applications in the Classic M-Files Desktop.

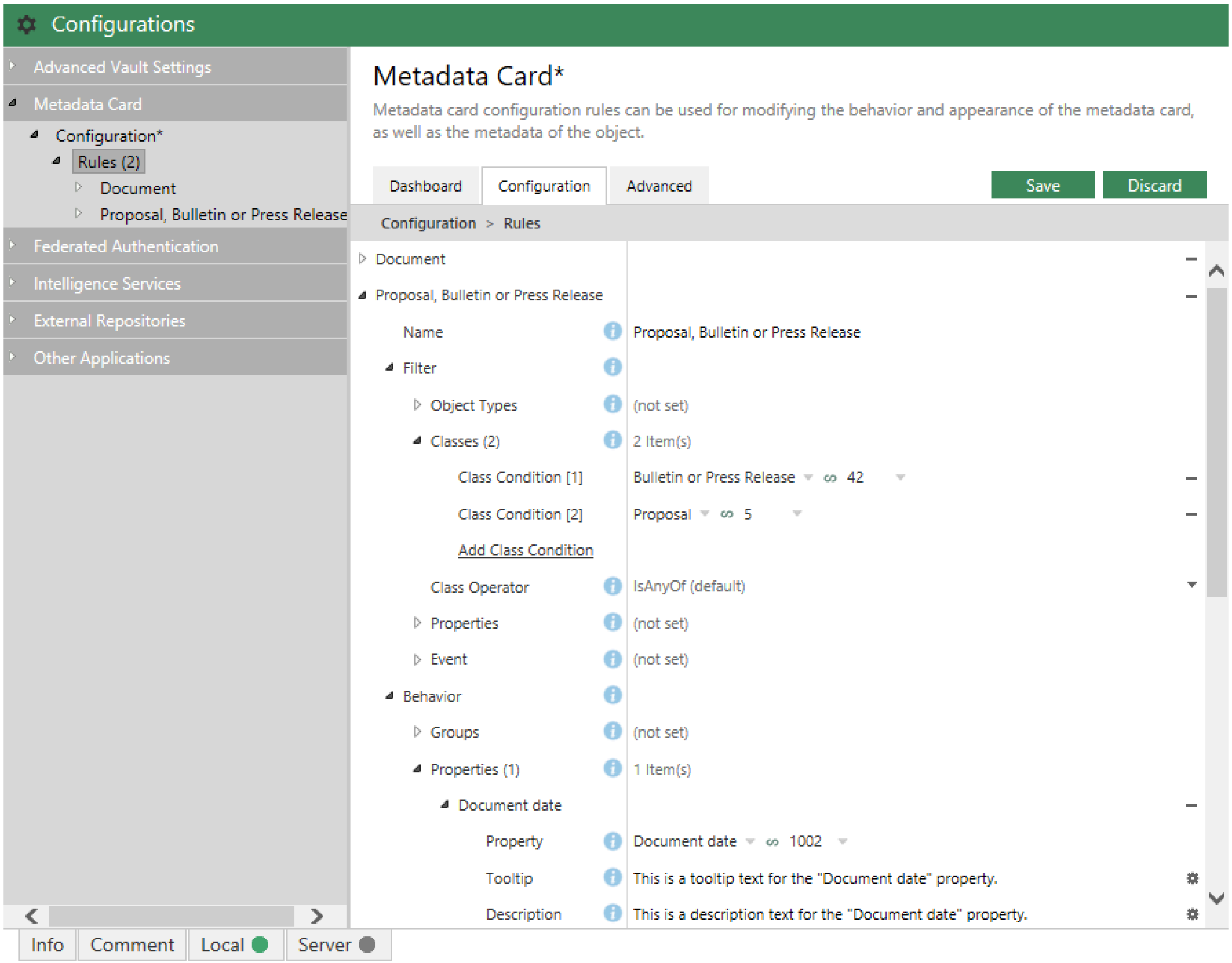
3.2.6. Using the Configurations Editor

The configurations editor in M-Files Admin allows you to define configurations for the following features of the vault:

- advanced vault settings
- custom vault data
- metadata card
- federated authentication
- intelligence services
- external connectors
- vault applications

Note: The configurations editor is available in English only. The editor requires Internet Explorer 9 or later to be installed.

Note: You must have the **Full control of vault** administrative right to use the configurations editor. For more information, see Users.



Configurations

- Advanced Vault Settings
- Metadata Card
  - Configuration*
    - Rules (2)
      - Document
      - Proposal, Bulletin or Press Release
- Federated Authentication
- Intelligence Services
- External Repositories
- Other Applications

Metadata Card*

Metadata card configuration rules can be used for modifying the behavior and appearance of the metadata card, as well as the metadata of the object.

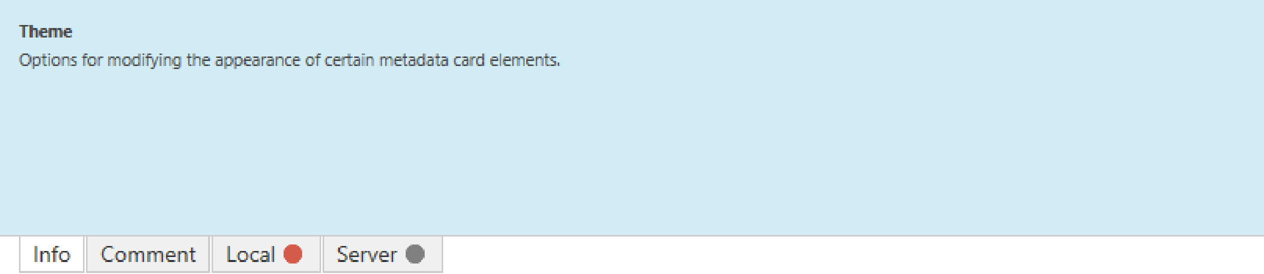
Configuration > Rules

```
▷ Document
◢ Proposal, Bulletin or Press Release
    Name                    Proposal, Bulletin or Press Release
  ◢ Filter
    ▷ Object Types          (not set)
    ◢ Classes (2)           2 Item(s)
        Class Condition [1] Bulletin or Press Release  42
        Class Condition [2] Proposal  5
        Add Class Condition
      Class Operator        IsAnyOf (default)
    ▷ Properties            (not set)
    ▷ Event                 (not set)
  ◢ Behavior
    ▷ Groups                (not set)
    ◢ Properties (1)        1 Item(s)
      ◢ Document date
          Property          Document date  1002
          Tooltip           This is a tooltip text for the "Document date" property.
          Description       This is a description text for the "Document date" property.
```

The configurations in the editor are hierarchical. You can select subsections of a configuration in the gray navigation area, and the scope of the configuration shown in the **Configuration** or the **Advanced** tab changes accordingly.

The configurations are defined in the **Configuration** tab. They may consist of configuration groups and subgroups, and configurations keys and subkeys. Subitems in a group or a key can be expanded or collapsed by clicking the arrow icon (▷ or ◢) next to the configuration key.

The **Info** tab provides you information about the use and purpose of the currently selected configuration key:

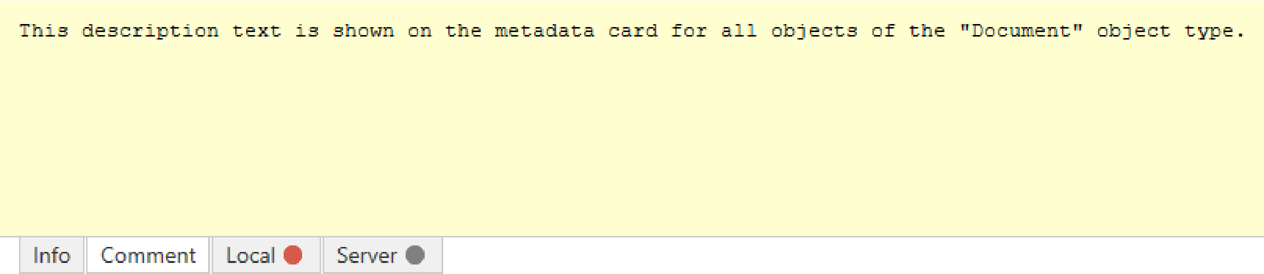


Theme

Options for modifying the appearance of certain metadata card elements.

You may also hover your mouse cursor over the information icon (ⓘ) next to the configuration key to see the same information.

You may comment a setting by selecting a setting and writing your comment in the **Comment** tab at the bottom of the **Configurations** pane:



```
This description text is shown on the metadata card for all objects of the "Document" object type.
```

Commenting a setting may be useful if you, for example, want to inform other administrators as to why a certain setting is used.

If there are errors in your configuration, they are shown in the **Local** or **Server** tab at the bottom of the **Configurations** pane.

The **Dashboard** tab provides you information on the selected configuration category. It may also contain an overview and status of your current configurations in the selected category.

The configurations are stored in JSON format. You may inspect, edit, as well as copy and paste the configurations in plain JSON format in the **Advanced** tab.

In this chapter

- Adding or Modifying Configurations
- Adding Translations for Configuration Values
- Exporting Configurations
- Importing Configurations
- Advanced Vault Settings
- Configuring Custom Vault Data
- Metadata Card Configuration

Adding or Modifying Configurations

Do the following steps to add or modify configurations in a vault:

1. Open M-Files Admin.

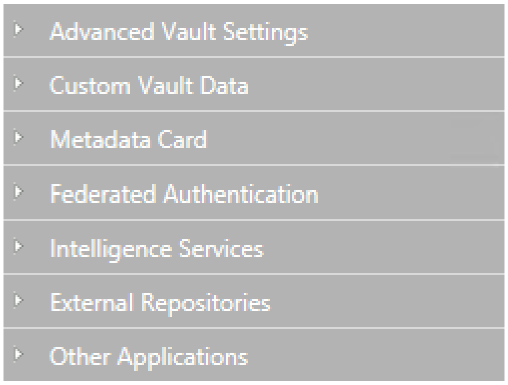
2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Document Vaults**.

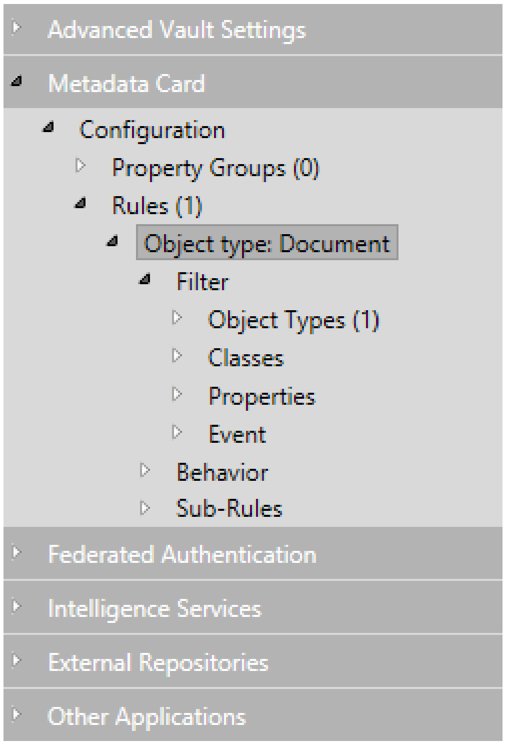
4. Expand a vault.

5. Select **Configurations**.

6. In the gray navigation area, expand the desired configuration category:



7. In the gray navigation area, locate and select the configuration key that you want to modify by expanding and navigating the configuration tree:



8. In the right pane, either:

   a. Modify the existing value.

      or

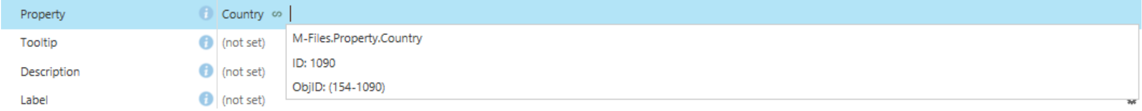
   b. Click the relevant **Add** button to add a new configuration value or subvalue.

      or

   c. Open the **Dashboard** tab and click the relevant **Add** button to add a new configuration.

   Configuration fields highlighted in red are required fields that must have a value.

If a configuration value requires a reference to a vault metadata structure item, you may enter the first few letters of the name of the item in the configuration field and the editor then suggests appropriate values. As you select an item from the available suggestions, the editor automatically resolves the reference by the alias or ID of the item. You may change the type of reference by clicking the value to the right of the equals sign and pressing the down arrow key:



Property	Country ∞	
Tooltip	(not set)	M-Files.Property.Country
Description	(not set)	ID: 1090
Label	(not set)	ObjID: (154-1090)

9. When ready, click the **Save** button.

Your configurations are saved and are now effective.

Adding Translations for Configuration Values

You can add translations for certain configuration values.

If you are for example configuring a metadata card description for a certain object type, you may add translations for the text used in the description, so that a vault user with the appropriate language settings can see the description on the metadata card in the correct language.

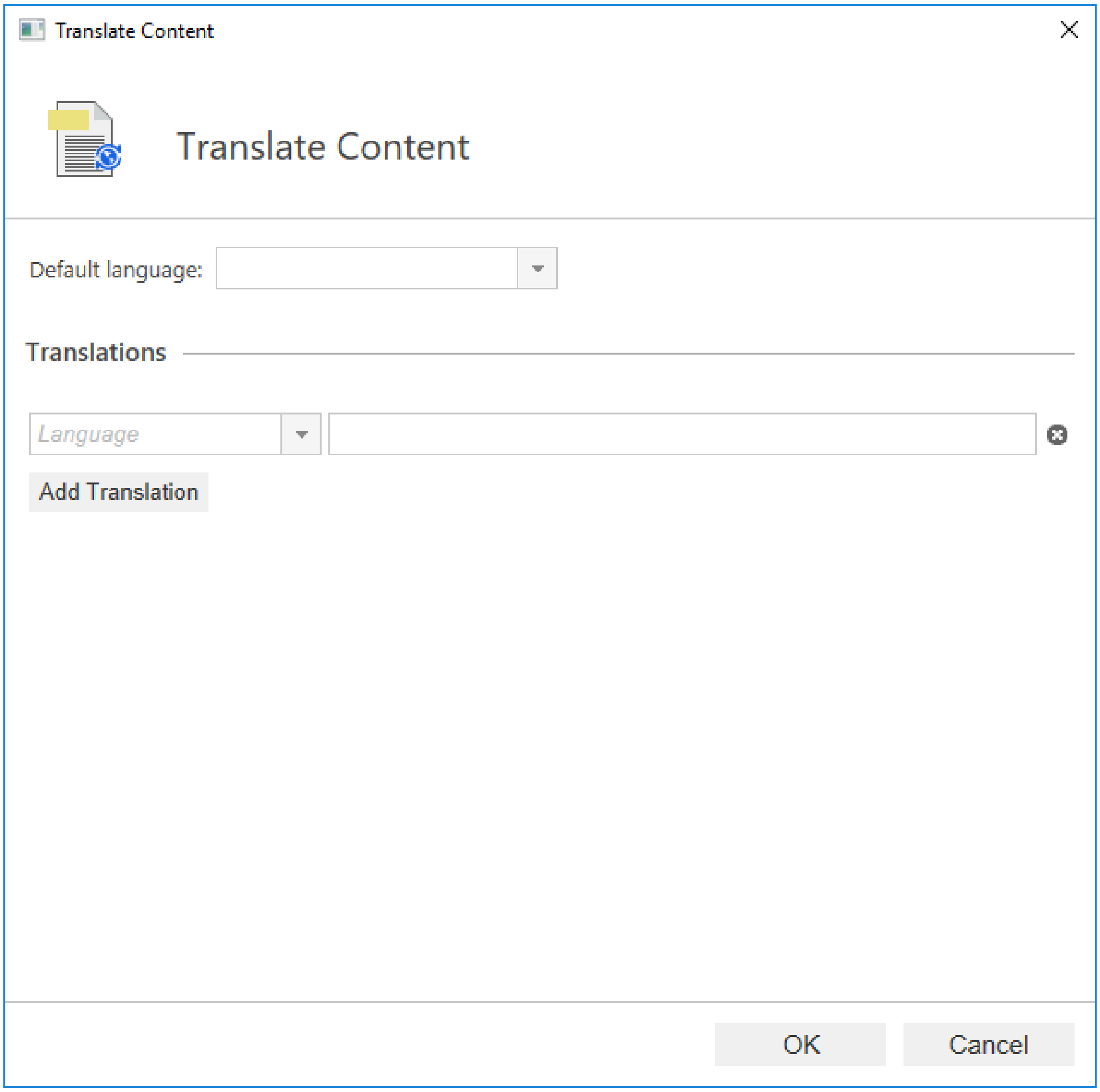
Do the following steps to add translations for a configuration value:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Configurations**.
6. In the gray navigation area, expand the configuration category that you want to edit and then locate the configuration key for which you want to add translations.

   The keys for which you can add translations can be identified by the cogwheel icon (⚙) shown in the value field.

7. Click the cogwheel icon (⚙) on the right side of the configuration value field.

   The **Translate Content** dialog is opened.



8. Use the **Default language** drop-down menu to select the default language.

   The translation for the default language is used if the requested translation is not available.

9. Use the **Language** drop-down menu to select the language of the value.

10. Enter the value in the text field in the selected value.

11. Click **Add Translation** to add a translation.

12. Repeat the steps 9 and 10.

13. Click **OK** when you are ready.

14. Click **Save** in the configurations editor to save your changes.

Exporting Configurations

You can export vault-specific configurations to a file and use the export file to import configurations, for example, to another server computer.

Do the following steps to export configurations:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Configurations**.
6. In the gray navigation area, expand the configurations that you want to export.
7. In the gray navigation area, right-click a setting node and select **Export to File...** from the context menu.

   ✓ The **Save As** dialog is opened.
8. Specify a location and file name, and then click **Save**.

   ✓ A confirmation dialog appears after the export is complete.
9. Click **OK**.

The configurations are exported to the specified location.

Importing Configurations

You can import vault-specific configurations from a configuration export file. This way you can, for example, import configurations from one M-Files server computer to another.

Do the following steps to import configurations from a configuration export file:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Configurations**.
6. In the gray navigation area, right-click a configuration category and select **Import from File...** from the context menu.

   ✓ The **Open** dialog is opened.
7. Locate and select the configuration export file, and then click **Open**.

   ✓ A confirmation dialog appears after the import is complete.
8. Click **OK**.
9. Right-click the category and select **Save All** from the context menu to save the imported configurations.

The selected configurations are imported to the server computer.

Advanced Vault Settings

The settings in the **Advanced Vault Settings** section of the M-Files Admin configurations editor allow you to control how the vault functions. These settings were previously available as Microsoft Windows registry settings. Settings added with the **Advanced Vault Settings** section are included in vault backups.

In the **Advanced Vault Settings** section, the system administrator can configure all the functionalities listed in the table below. The table gives an overview of which settings also a user with the **Full control of vault** administrative rights can adjust.

Configuration	Vault administrator
Assignments	Allowed
Automatic aliases	Allowed
Background tasks	Not allowed
Client **Note:** Set the **Manage Client Settings Centrally** setting to `Yes` only after you have read the description shown on the **Info** tab in M-Files Admin.	Partly allowed
Connections to external databases	Partly allowed
Connections to external sources	Partly allowed
Content replication and archiving	Partly allowed
Database	Partly allowed
Document comparison	Allowed
Duplicate detection	Allowed
Event log	Partly allowed
External repositories	Not allowed
File operations	Allowed
File previews	Not allowed
Ground Link	Partly allowed
M-Files add-in settings	Allowed
Multi-file documents	Allowed
Notifications	Partly allowed
PDF conversion	Partly allowed
Performance	Not allowed
Real object type hierarchies	Partly allowed
Reporting and data export	Not allowed
Scanning and OCR	Not allowed

Configuration	Vault administrator
Scripting	Not allowed
Search	Partly allowed
Security	Not allowed
Thumbnails	Partly allowed
Translatable object titles	Allowed
User groups	Allowed
Views	Allowed

Note: Some of the settings in the **Advanced Vault Settings** section are for advanced configuration and customization only, and therefore we recommend that you do not change any settings unless you know what you are doing.

Configuring Advanced Vault Settings

To configure vault settings:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand the section that you want to edit, and then edit settings that you want to change.

   For more information, select a setting and see the **Info** tab.

   Tip: Right-click a settings node to bring up a context menu with additional options, such as **Move Up**, **Move Down**, and **Make Copy**.

3. When you are done, click **Save** to save the vault settings.

4. Optional: Some of the settings require that you restart the vault for the changes to take effect. For instructions, see Restarting a Vault.

Example: Excluding *Employee* Objects from Metadata Searches

To configure your vault search engine so that *Employee* objects are not incuded in metadata searches:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.

e) Click **Configurations**.
f) In the navigation area, click **Advanced Vault Settings**.
g) Open the **Configuration** tab.

✓ The advanced vault settings are shown.

2. Expand **Search** > **Excluded Object Types** > **Metadata-Based Searches**.

3. Click **Add Object Type**.

4. In the **Object Type** field, press the down arrow key ↓ and then select *Employee*.

5. Click **Save** to save your settings.

After saving the setting, *Employee* objects are no longer included in metadata searches in the selected vault.

Configuring Custom Vault Data

The **Custom Vault Data** section in the M-Files Admin configurations editor allows you to add and modify custom vault data to affect the vault functionality. The most common type of custom vault data are custom settings of the vault that allow you to add custom functionality to the vault. Sets of custom vault data are registered within specific namespaces.

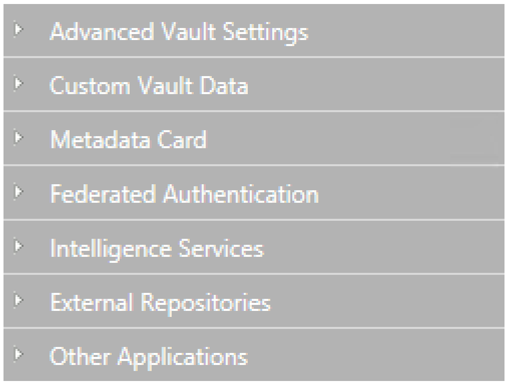
Note: This section of the configurations editor is intended for advanced configuration and customization only, and therefore we recommend that you do not add custom vault data unless you know what you are doing.

Registering a Namespace

To begin modifying custom vault data, you must first register a namespace for a new set of custom vault data. Complete the following steps to register a namespace:

1. In M-Files Admin, access the custom vault data section.

a) Open M-Files Admin.
b) In the left-side tree view, expand an M-Files server connection.
c) Expand **Document Vaults**.
d) Expand a vault.
e) Click **Configurations**.
f) In the navigation area, expand **Custom Vault Data**.



2. Select **Namespace Registry** > **Configuration**.

3. Expand the **Namespaces** node, click **Add Namespace**, and expand the newly added namespace node.

4. In the **Group** field, enter an internal name of your choice for the group that uses the namespace that you are about to register.

5. Use the **Storage Type** drop-down menu to select the storage type that the namespace uses.

6. In the **Namespace** field, enter the namespace that you are about to register, and in the **Namespace Label** field, enter a custom label for the namespace shown in the **Custom Vault Data** configuration.

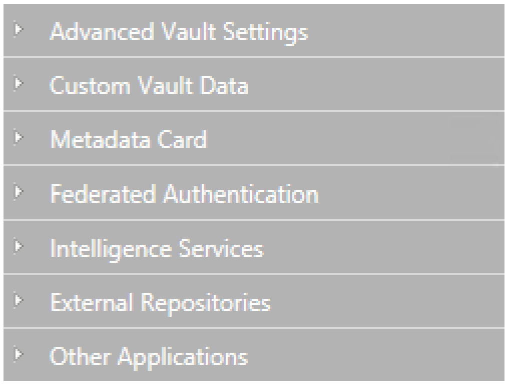
7. In the **Namespace Description** field, enter a description about the purpose of the namespace.

8. Click **Save** to save your configuration.

Adding Named Values

After you have registered a namespace, you can add named values within that namespace. Complete the following steps to add named values:

1. In M-Files Admin, access the custom vault data section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, expand **Custom Vault Data**.



2. In the gray navigation area, expand **Custom Vault Data** > **Named Values**, then expand a group that you have registered in Registering a Namespace, and finally select the namespace of the group.

3. Open the **Configuration** tab.

4. Click **Add Named Value**, and expand the newly created named value node.

5. In the **Name** field, enter the name part of the named value.

   The name can only contain letters, numbers, underscores, hyphens, and periods.

6. In the **Value** field, enter the value part of the named value.

7. Repeat the steps from 4 to 6 to add more named value pairs within the given namespace.

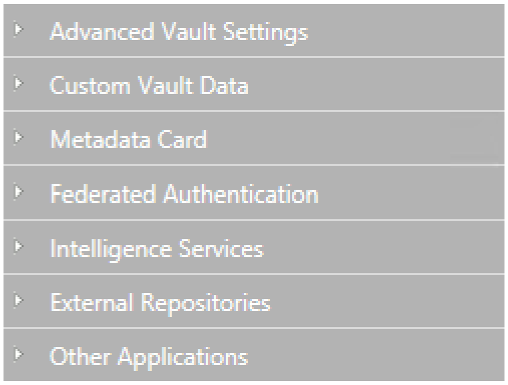
8. Click **Save** to save your configuration.

Example: Disabling the Sorting of Search Results by Their Relevance

By default, M-Files sorts search results by their relevance. For more information on how document relevance in relation to the search term is determined, see Search result sorting.

This behavior can be prevented so that search results are sorted by user preference instead. Make the following changes on the M-Files Server computer to prevent search results to be automatically sorted by their relevance:

1. In M-Files Admin, access the custom vault data section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, expand **Custom Vault Data**.

2. Select **Namespace Registry** > **Configuration**.
3. Expand the **Namespaces** node, click **Add Namespace**, and expand the newly added namespace node.
4. In the **Group** field, type `Search results`.
5. Use the **Storage Type** drop-down menu to select the **MFConfigurationValue** storage.
6. In the **Namespace** field, enter the following value: `M-Files.Core.Listing.SearchResults`
7. In the **Namespace Label** field, type `Search results`.
8. In the **Namespace Description** field, enter for example `Settings related to search results`.
9. Click **Save** to save the namespace settings.
10. In the gray navigation area, select **Named Values** > **Search results** > **Search results** > **Configuration**.
11. Click **Add Named Value**, and expand the newly created named value node.
12. In the **Name** field, enter the following value: `RememberSearchResultsSortingCriteria`
13. In the **Value** field, enter the following value: `true`
14. Click **Save** to save the configuration.

M-Files no longer forces search results to be sorted by their relevance, and therefore users can change the column by which search results are sorted and the user preference is retained in subsequent searches.

Metadata Card Configuration

You can use the configurations editor in M-Files Admin to modify the behavior and appearance of the metadata card. For instructions on how to use the configurations editor, see Using the Configurations Editor.

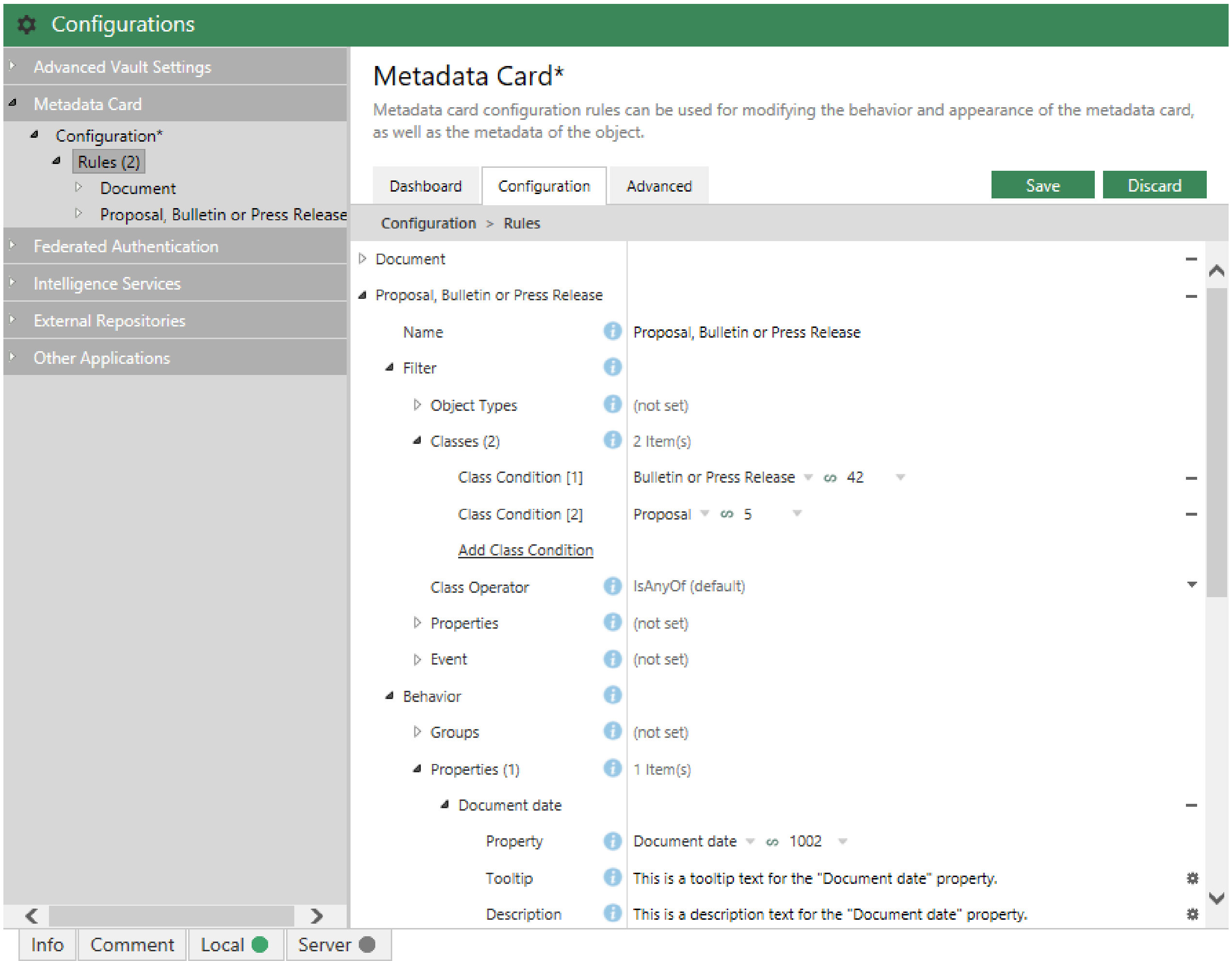
With metadata card configurations, you can:

- 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.

Important information to know before you use metadata card configurations

- Always use property definition permissions to protect sensitive information. Metadata card configuration rules can be used to hide property values from the display, but the values stay available to client applications. Property definition permissions, in turn, make sure that property values are not sent from the server to the client application of an unauthorized user.
- Do not use metadata card configurations for actual restrictions on metadata modifications because the configurations are effective at the user interface level only. For example, you can change the workflow state of an object with the Change State command without adding a required property value imposed by a configuration rule. Instead, use the workflow state preconditions or postconditions to make sure that certain property values are filled before state transitions occur.

For information on how this feature is supported in different M-Files clients, refer to M-Files Client Feature Comparison.



Configurations

- Advanced Vault Settings
- Metadata Card
  - Configuration*
    - Rules (2)
      - Document
      - Proposal, Bulletin or Press Release
- Federated Authentication
- Intelligence Services
- External Repositories
- Other Applications

Metadata Card*

Metadata card configuration rules can be used for modifying the behavior and appearance of the metadata card, as well as the metadata of the object.

Dashboard | Configuration | Advanced | Save | Discard

Configuration > Rules

- Document
- Proposal, Bulletin or Press Release
  - Name: Proposal, Bulletin or Press Release
  - Filter
    - Object Types: (not set)
    - Classes (2): 2 Item(s)
      - Class Condition [1]: Bulletin or Press Release 42
      - Class Condition [2]: Proposal 5
      - Add Class Condition
    - Class Operator: IsAnyOf (default)
    - Properties: (not set)
    - Event: (not set)
  - Behavior
    - Groups: (not set)
    - Properties (1): 1 Item(s)
      - Document date
        - Property: Document date 1002
        - Tooltip: This is a tooltip text for the "Document date" property.
        - Description: This is a description text for the "Document date" property.

Info | Comment | Local ● | Server ●

Figure 64: Metadata card configurations in the Configurations editor.

Metadata card configurations can be found in the **Metadata Card** section in the configurations editor.

You can add and remove rules by clicking the **Add New** button in the **Rules** section. The rules are hierarchical, meaning that you can add subordinate rules in the **Sub-Rules** section 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 **Filter** section defines the scope of the rule. You may want to, for example, apply a metadata card configuration of objects of a certain class only.

The **Behavior** section is 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 one of the following options:

- **Move Up** to move the rule up in the list
- **Move to Top** to move the rule to the top of the list
- **Move Down** to move the rule down in the list

- **Move to Bottom** to move the rule to the bottom of 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, refer to Configuring the M-Files Metadata Card.

3.2.7. Editing Notification Settings in M-Files Admin

M-Files can be set to send email notifications about object-related actions. Users can also create new notification rules in the classic M-Files Desktop (see Editing Notification Settings in the Classic M-Files Desktop and Metadata card option ribbon).

The email notifications contain a link to the related object. By default, the link is in the new M-Files link format. To use the classic link formatting, go to **Advanced Vault Settings** > **Configuration** > **Notifications** in M-Files Admin and set **Use Classic Link Formatting** to **Yes**. For more information on links in M-Files, refer to Configuring M-Files Links and M-Files URL Properties in M-Files Support Portal.

Note: In M-Files Cloud, email notifications are automatically enabled.

For the notifications to be sent, these features must be enabled:

- Event logging
- Vault notifications
- M-Files Desktop notifications

If you use Microsoft Exchange Online, you must also set up an OAuth application in Microsoft Azure Portal and have the details listed in the document Azure Portal Configuration for M-Files Notifications with Microsoft Exchange Online.

To enable email notifications in an on-premises environment, do these steps on the M-Files server computer:

1. Open M-Files Admin.
2. In the left-side tree view, right-click a connection to your M-Files server.
3. Select **Notification Settings**.
4. Select **Enable notifications**.
5. In **Service type**, select **SMTP server** or **Microsoft Exchange Online**.
6. Enter the connection information for the selected service type.

   The table given here contains the descriptions for the settings of both service types.

Service type	Setting name	Description
SMTP server	**SMTP server**	The address of the SMTP server that sends the notification email messages.

Service type	Setting name	Description
	Use encrypted connection (SSL/TLS)	Enable this setting if the SMTP server is ecrypted.
	SMTP server port	The port number for the SMTP server connection. The default ports are `25` (without encryption), and `587` (with encryption), but you can change the port number to, for example, `465`.
	SMTP server requires authentication	Enable this setting if the notification sender must be authenticated on the SMTP server. Then enter the name and password for the sender's account in **Account name** and **Password**.
	Sender's e-mail address	The email address of the sender to be shown in the notifications.
	Sender's display name	The name of the sender to be shown in the **From** field of the notifications.
Microsoft Exchange Online	**Tenant ID**	The tenant ID (also called directory ID) of your Microsoft Entra ID application. For example: `00112233-4455-6677-8899-aabbccddeeff`
	Client ID	The client ID (also called application ID) of your Microsoft Entra ID application. For example: `00112233-4455-6677-8899-aabbccddeeff`
	Client secret	The client secret of your Microsoft Entra ID application. For example: `sXXtFz1UtYMRCVc.2.23TMC-94-T.yK-84`
	HTTP proxy	This is an optional setting. For authentication and email requests to use a proxy server, enter the address and port of the server. For example: `192.168.1.1:8080`. The proxy server must support the SSL protocol.
	Sender's e-mail address	The email address of the sender to be shown in the notifications.
	Authentication timeout in seconds	If the sender cannot be authenticated in the time given in this setting, the authentication is canceled and the notification is not sent.
	Mail service timeout in seconds	If the mail service does not respond in the time given here, the process is canceled and the notification is not sent.

7. In **Digest message**, select the time when the daily digest messages are sent.

   ⓘ M-Files users can select to receive their notifications as individual messages or as a daily digest message. For more information, see Editing Notification Settings in the Classic M-Files Desktop.

8. Click **OK** to save your changes and to close the **Notification Settings** dialog.

Notifications are now enabled on the M-Files server.

- Make sure that notifications are enabled in the vault: In the **Advanced Vault Settings** in M-Files Admin, go to **Notifications** and make sure that **Enable Vault Notifications** is set to **Yes** (default value).
- Users must enable notifications in the classic M-Files Desktop to get notifications. See Editing Notification Settings in the Classic M-Files Desktop.
- The administrator and users can also create notification rules. See Editing Notification Settings in the Classic M-Files Desktop.
- You can customize your notification messages. See Personalizing Notification Messages.

In this chapter

- Personalizing Notification Messages
- Setting Up Push Notifications for the M-Files Mobile Apps

Personalizing Notification Messages

M-Files uses customizable templates for email notifications, which you can modify to match the requirements of your organization. You can, for instance, change the information provided along with notifications about new or modified objects, assignments, and so on.

Follow the instructions in this section to access and edit the notification templates in M-Files Admin.

Accessing the Notification Template Settings

To access the notification template settings:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **Notifications** > **Notification Templates**.

The list of available notification templates in this vault is displayed in the configurations editor. The templates are divided under two sections, **Email Templates** and **Push Notification Templates**. The latter are used for the M-Files mobile applications.

If the listing does not include at least a template called `Default`, try to restart the vault and M-Files Admin. Taking a vault offline should always be done in a controlled manner and the vault users should be notified beforehand.

Editing or Adding a Notification Template

To edit an existing notification template or to add a new one:

1. Under **Advanced Vault Settings** > **Notifications** > **Notification Templates**, in the configurations editor listing area, either:

   a. Expand an existing template rule that you would like to edit.

or

b. Click **Add Rule** to add a new template rule, and expand the newly created node.

2. In **Rule**, select the notification rule to which you want this template to apply.
3. Expand the **Template Sections** node.
4. Either:

a. Expand an existing section node to edit a previously added section.

or

b. Click **Add Section** to add a new section, and expand the newly created node.

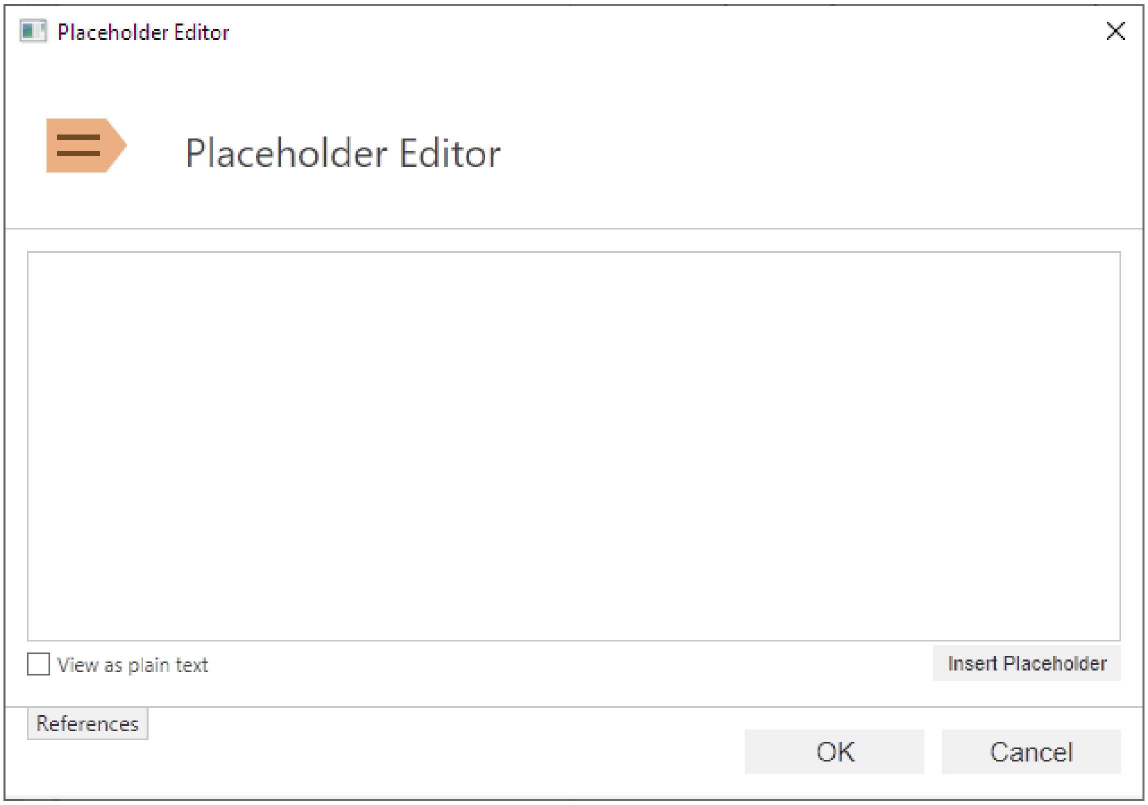
For any sections that your template does not include, the M-Files server uses the corresponding sections of the special `Default` template. If the `Default` template cannot be found, M-Files server uses the corresponding sections of a fallback template located in the installation directory.

5. In **Template Section**, select the section that you would like to modify.

Tip: Hovering the mouse cursor on top of the section names in the drop-down menu displays a short description for each section.

6. Click the cogwheel icon (⚙) in the value field of the Template Entry setting.

☑ The **Placeholder Editor** dialog is opened.



7. To the text box, enter the content of the section.

Use the **Insert Placeholder** button to add a dynamically updated reference in your content. Clicking the button adds a set of curly brackets in the text box. You can either start typing the name of the placeholder or press the down arrow key to bring up a list of available placeholders, such as the title or class of the object that triggered the notification. Some placeholders, however, only work with specific sections.

8. Once you are done editing the template content, click **OK** to close the **Placeholder Editor** dialog.

9. Optional: Repeat the steps from 4 to 8 to edit or add as many sections as needed.

10. Once you are done with your changes, click **Save**.

Placeholders for Notification Templates

In addition to the object properties, such as the title or the class of the object, you can use a set of special placeholders in your notifications. These placeholders are described in the table below.

Placeholder	**Description**
All referred objects()	All the referred objects in the properties of the object.
ApproveLink()	A link for an assignment approval in the notification email. If you have specified the URL for M-Files Web or for the Classic M-Files Web in the vault properties, the link is an HTTP-formatted hyperlink. If no URL has been set, an M-Files link is used.
Caused by()	The name of the user who caused the event.
Caused by account()	The account name for the user who caused the event.
`EventID()`	The ID of the event.
FileName()	The name of the file.
ID()	The (external) ID of the object.
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.
NameAndLinks()	A plain text formatted text fragment containing URLs to the object for M-Files Desktop, M-Files Web, and M-Files Mobile.
NameAndLinksHtml()	An HTML-formatted hyperlink containing URLs to the object for M-Files Desktop, M-Files Web, and M-Files Mobile.
`NameWithHtmlLink()`	An M-Files link that opens a web page where the user can select the client in which to open the target of the link.
`NameAndSeparateLink()`	The same placeholder as `NameWithHtmlLink()` but the name and the URL are shown as separate plain-text fragments.
Notification rule name()	The name of the notification rule that caused the event.
ObjTitle()	The name or title of the object.
ObjType()	The type of the object.

Placeholder	Description
OldProperty(Undefined)	The old value of the specified property of the object. *Undefined* is replaced with the property the old value of which you want this placeholder to display in the notification. After selecting this placeholder, open the **References** tab and select the desired value via drop-down menu in the **Item** column.
RejectLink()	A link for an assignment rejection in the notification email. If you have specified the URL for M-Files Web or for the Classic M-Files Web in the vault properties, the link is an HTTP-formatted hyperlink. If no URL has been set, an M-Files link is used.
Rolled back to version()	The version that the object was rolled back to.
Timestamp()	The time when the event occurred.
URL()	A URL that shows the latest version of the object in M-Files Desktop.
UrlToLatestClassicWeb()	A URL that shows the latest version of the object in the classic M-Files Web.
UrlToLatestMobile()	A URL that shows the latest version of the object in M-Files Mobile.
UrlToLatestWeb()	A URL that shows the latest version of the object in M-Files Web.
UrlToVersion()	A URL that shows the specific version of the object in M-Files Desktop.
UrlToVersionClassicWeb()	A URL that shows the specific version of the object in the classic M-Files Web.
UrlToVersionMobile()	A URL that shows the specific version of the object in M-Files Mobile.
UrlToVersionWeb()	A URL that shows the specific version of the object in M-Files Web.
UserCausedState(Undefined)	The user who moved the object into a specific state. *Undefined* is replaced with the target state. After selecting this placeholder, open the **References** tab and select the desired value via drop-down menu in the **Item** column.
VaultGuid()	The unique identifier (GUID) of the vault.
VaultName()	The name of the document vault.
Version()	The version of the object.

Setting Up Push Notifications for the M-Files Mobile Apps

Push notifications allow sending notifications from M-Files Server to iOS and Android devices that have the M-Files mobile app installed. Push notifications are sent for the same events as email notifications except for digest messages. Once they are enabled, you will receive a push notification, for instance, when a new assignment is created for you. You can also create personalized notification rules with the classic M-Files Desktop (see Editing Notification Settings in the Classic M-Files Desktop).

To enable push notifications

- in an on-premises environment or in your own cloud environment, follow the instructions provided in the sections Creating a notification hub in Azure, Setting up an Azure notification hub for push notifications, and finally Enabling push notifications in M-Files vaults.
- in M-Files Cloud, simply follow the steps from 9 to 16 under Enabling push notifications in M-Files vaults. No other changes are needed.
- Vault users should enable push notifications on their iOS or Android devices. They will receive push notifications when they are logged in to a vault that has push notifications enabled. Note that vault users do not have to keep the M-Files application running to receive push notifications from a vault, as long as they are logged in to the vault ensures that they can receive push notifications.

Before you begin, note that notifications need to be enabled on the M-Files server (see Editing Notification Settings in M-Files Admin).

Creating a notification hub in Azure

M-Files push notifications use Azure notification hubs for delivering the notifications (see Microsoft Azure Notification Hubs). You therefore need to have a valid Microsoft Azure subscription before moving forward. Visit https://azure.microsoft.com to create a subscription if you do not yet have one.

Do the following steps to create a new notification hub in Azure:

1. Sign in to Azure Portal.
2. Select **Create a resource** > **Mobile** > **Notification Hub**.
3. In the **Notification Hub** field, enter a unique name.
4. In the **Create a new namespace** field, enter a namespace name.

   If you do not yet have a service bus namespace, you can use the default one. It is automatically created based on the hub name, provided that the namespace name is available.

   If you already have a namespace that you want to create the hub in, click the **Select existing** link and then select **Create**.
5. Select your **Location**, **Resource Group**, and **Subscription**.
6. Select a suitable price tier (for details, see Notification Hubs pricing).

Setting up an Azure notification hub for push notifications

After you have created an Azure notification hub, it needs to be configured for different mobile platforms. You can find the settings for the available notification services by doing these steps:

1. Sign in to Azure Portal.
2. Select **All services**.
3. Under **Mobile**, select **Notification Hubs**.
4. From the list of notification hubs, select the hub that was created according to the instructions in Creating a notification hub in Azure.
5. Under **Notifications Settings**, do one of the following, or both:

   a. Enter the iOS configuration under **Apple (APNS)**. You can request the configuration settings from our customer support in M-Files Support Portal or your M-Files reseller.

or

b. Enter the Android configuration under **Google (GCM)**. You can request the configuration settings from our customer support in M-Files Support Portal or your M-Files reseller

Enabling push notifications in M-Files vaults

After you have created a notification hub and set it up for push notifications, you need to enable push notifications for the M-Files vaults in which you want them to be used, as well as to set up the connection between M-Files and the Azure notification hub. You can store the connection settings to the Windows registry of the M-Files server computer or set them separately for each vault in M-Files Admin, or both. The server-level settings are not used in any vaults for which the connection settings have been specified with M-Files Admin.

First, you need to locate the connection details in your notification hub settings:

1. Sign in to Azure Portal.
2. Select **All services**.
3. Under **Mobile**, select **Notification Hubs**.
4. From the list of notification hubs, select the hub that was created according to the instructions in Creating a notification hub in Azure.

If you want to store the connection details to the Windows registry of the server computer, do the following steps:

5. Optional: Under the notification hub settings, select **Properties**.
6. Optional: Copy the value of the **Name** field and enter it as the value of the following Windows registry key on the M-Files server computer:

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\`*`<version>`*`\Server\MFServer`**
Value name	`AzureNotificationHubName`
Value type	`REG_SZ`
Description	The name of the Azure notification hub to use for delivering the notifications.
Value	`<the notification hub name>`

7. Optional: Under the notification hub settings, select **Access Policies**.
8. Optional: Copy the value of the **DefaultFullSharedAccessSignature** field and enter it as the value of the following Windows registry key on the M-Files server computer:

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\`*`<version>`*`\Server\MFServer`**
Value name	`AzureNotificationHubConnectionString`
Value type	`REG_SZ`
Description	The connection string for the Azure notification hub.

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer**
Value	`<the connection string for the notification hub>`

To enable push notifications in a vault:

9. Open M-Files Admin.

10. In the left-side tree view, expand a connection to M-Files server.

11. Expand **Document Vaults**.

12. Expand a vault.

13. Select **Configurations**.

14. In the task area, select **Advanced Vault Settings**.

15. Expand **Notifications** and select **Push Notifications**.

16. Set the value of the **Enabled** setting to **Yes**.

If the connection details have not been stored to the Windows registry of the server computer, or if you want to vault-specifically override the server-level settings, do the following:

17. Optional: Enter the notification hub name and the connection string as the values of the **Notification Hub Name** and **Connection String** settings, respectively.

   ⓘ To get the value for **Notification Hub Name**, open your notification hub settings (see steps from 1 to 4), select **Properties** and enter the **Name** value to your configuration.

   To get the value for **Connection String**, open your notification hub settings (see steps from 1 to 4), select **Access Policies** and enter the **DefaultFullSharedAccessSignature** value to your configuration.

18. Click **Save** to save your changes once you are done.

Finalize the process by doing either step 19 or steps 20 and 21, depending on where the connection settings are stored. Note that restarting the vault or the server should always be done in a controlled manner and users should be notified beforehand so that no work is lost.

19. If you saved the connection details to the vault (see step 17), restart the vault.

   ⓘ In this case, you can skip steps 20 and 21.

20. If the connection settings are stored on the server computer (see steps from 5 to 8), restart the **MFServer** service as instructed in step 21.

21. Use Windows Task Manager to restart the **MFServer** service:

   a) Right-click the taskbar and select **Task Manager**.

      ✓ The **Task Manager** window is opened.

   b) Open the **Services** tab.
   c) Right-click the **MFServer** service and select **Restart**.

Your vault is now set up to send push notifications to vault users. Repeat the process for as many vaults as needed.

3.2.8. Setting Up Web and Mobile Access to M-Files

This section tells you how to set up both versions of M-Files Web, Microsoft Office for the web services for M-Files Web, M-Files Mobile, and the M-Files REST API.

In M-Files Cloud, all the clients and services are normally enabled out of the box. However, you can use Advanced Vault Settings (AVS) to change the default client and set classic M-Files Web links to always be redirected to M-Files Web. The settings in AVS are in the section **Configuration** > **Client** > **Web**.

These are the available configurations:

	M-Files Web	MS Office for M-Files Web	Classic M-Files Web	REST API	M-Files Mobile
Both web clients and M-Files Mobile	✓	✓ *	✓	✓	✓
M-Files Web	✓	✓ *	#	#	#**
Classic M-Files Web and M-Files Mobile	#	#	✓	✓	✓

*) If you do not use M-Files Cloud, you must set up Microsoft Office for the web separately. See Setting up Microsoft Office for the web.

**) If you do not want to set up the classic M-Files Web for the mobile apps, you can set M-Files Mobile to use gRPC. Refer to Setting Up M-Files to Use gRPC.

Important information

- If M-Files Web was previously set up on the server with the instructions in Setting Up the Backend for M-Files Web and Web-Based Add-Ins (September '22 Update and Earlier): We recommend that you remove the old configuration before you set up M-Files Web with the instructions given here.
  - Alternatively, you can continue to use the old setup. It enables the core functionality but it can be that features added to the product after the release of the setup wizard are not available.
- Components in the section Enabling Internet Information Services (IIS) Components must be enabled on the M-Files Web server.
- If you get an error during the setup, exit the wizard, fix the issue in IIS Manager, and start the wizard again. The error can be, for example, that a newly created website cannot start because the port number is already in use.
- You must set up the IIS binding for the website that users access. This is mandatory for HTTPS connections.
  - The use of self-signed certificates with IIS site bindings can break the classic M-Files Web and the REST API, especially in proxy setups.
- When both web clients are set up, there is outgoing HTTP(S) traffic from the M-Files application server to the site binding address given during the setup. Make sure that custom HTTP headers are not stripped or removed between the servers and that traffic is allowed between them.
- When M-Files Web is set up, there is HTTP traffic between the IIS site and the M-Files server. The M-Files Web traffic uses the port 7767 and the Office for the web services use the port 7768.
- When the settings are saved in M-Files Admin, they are moved, not copied, to the Internet Information Services settings of the server.

- After the setup, make sure that you do not have old `vnext` or `wopi` websites or applications in IIS from older installations and setups.
- You can use Advanced Vault Settings to disable the classic M-Files Web and set classic M-Files Web links to be automatically redirected to M-Files Web. The setting is **Configuration** > **Client** > **Web** > **Disable Classic M-Files Web and Redirect Links to M-Files Web**.
  - The setting does not apply to reset password links and URLs created with the **Share Public Link** feature.
- M-Files Mobile users can use a QR code for easy access to the vault.
  - Alternatively, admins can create login links for M-Files Mobile users. After the user logs in, the vault connection information is saved to the device. For details and examples, refer to M-Files URL Properties.
- To enable push notifications for M-Files Mobile, see Setting Up Push Notifications for the M-Files Mobile Apps.

Troubleshooting

If you have set up the classic M-Files Web and M-Files Web, and the classic M-Files Web reports 404 errors, refer to this article.

In this chapter

- Enabling Internet Information Services (IIS) Components
- Using the Set Up Web and Mobile Use Dialog
- Using Proxy Setup with M-Files Web

Enabling Internet Information Services (IIS) Components

The Internet Information Services (IIS) components listed on this page must be enabled on the M-Files Web server before web and mobile access can be set up.

Note: If you use M-Files Web (instead of the classic M-Files Web), you must also have the URL Rewrite and Application Request Routing IIS modules installed on the IIS server.

Here are the steps to enable the features with Microsoft Windows Server 2019. Refer to Microsoft Windows instructions for other operating system versions.

1. Open **Server Manager**.
2. In the **Dashboard** view, click **Add roles and features**.
3. In **Before You Begin**, click **Next**.
4. In **Installation type**, select **Role-based or feature-based installation** and click **Next**.
5. In **Server Selection**, select your server and click **Next**.
6. In **Server Roles**, enable the roles listed here.

Path	Role name
Web Server (IIS) > **Web Server** > **Common HTTP Features**	**Default Document**
	Directory Browsing
	HTTP Errors

Path	Role name
	Static Content
	HTTP Redirection
Web Server (IIS) > **Web Server** > **Performance**	All roles
Web Server (IIS) > **Web Server** > **Security**	**Request Filtering**
	Basic Authentication
	Windows Authentication
Web Server (IIS) > **Web Server** > **Application Development**	All roles
Web Server (IIS) > **Management Tools**	All roles

7. In **Features**, enable the features listed here.

    - **.NET Framework 4.7 Features** > **.NET Framework 4.7**
    - **.NET Framework 4.7 Features** > **ASP.NET 4.7**
    - **IIS Hostable Web Core**

8. Click **Next**.

9. Click **Install**.

10. When the installation is complete, click **Close**.

You now have the neccesary IIS components installed. Next, you can enable web and mobile access on the selected server computer.

Using the Set Up Web and Mobile Use Dialog

This section tells you how to set up the web and mobile clients and the REST API with the **Set Up Web and Mobile Use** dialog.

In this chapter

Setting Up M-Files Web

The steps given here tell you how to enable these clients and services:

- M-Files Web
- Microsoft Office for the web services for M-Files Web

The classic M-Files Web, M-Files REST API, and M-Files Mobile are not enabled. If you do not want to set up the classic M-Files Web for the mobile apps, you can set M-Files Mobile to use gRPC. Refer to Setting Up M-Files to Use gRPC.

Make sure that these requirements are completed:

- The server uses M-Files October '22 Update or later.
  - If the server uses an older version, we recommend that you upgrade to a more recent version. Alternatively, refer to Setting Up the Backend for M-Files Web and Web-Based Add-Ins (September '22 Update and Earlier).
- The server uses IIS (Internet Information Services) and Microsoft .NET Framework (not .NET) 4.7.2, 4.8.x, or later.
- You are an M-Files system administrator on the server.
- The IIS modules URL Rewrite and Application Request Routing are installed on the IIS server.
- You have set up IIS binding for the website that users access with a DNS name, such as `https://myvault.mycompany.com`.
  - If you want to create a new website for M-Files Web, do the binding setup after you have saved your changes in M-Files Admin.

Important remarks:

- If M-Files Web was previously set up on the server with the instructions in Setting Up the Backend for M-Files Web and Web-Based Add-Ins (September '22 Update and Earlier): We recommend that you remove the old configuration before you set up M-Files Web with the instructions given here.
- If you get an error during the setup, exit the wizard, fix the issue in IIS Manager, and start the wizard again. The error can be, for example, that a newly created website cannot start because the port number is already in use.

Do these steps:

1. Open M-Files Admin on the server.

   ⓘ ❗ **Important:** If IIS and M-Files are on separate servers, see Using Proxy Setup with M-Files Web instead of the instructions given here.

2. In the left-side tree view, select a server connection.
3. Click **Set Up Web and Mobile Use** > **Set up M-Files Web** > **Next**.
4. Select one of these options:

Option	Result and instructions
Use an existing website	Use an existing Internet Information Services site for M-Files Web. In the drop-down menu, select one of the available sites.
Create a new website	Create a new Internet Information Services website for M-Files Web. Enter the name and TCP port for the site. Make sure that the given port number is not already in use. **Note:** You can use this option only with a server operating system.

Option	Result and instructions
Create a new virtual directory	Add a new virtual directory to the selected Internet Information Services website and use the directory for M-Files Web. Select an available site and enter a name for the virtual directory. **Note:** You can use this option only with a server operating system.

5. Select **Save**.
6. Open the Document Vault Advanced Properties dialog and add the M-Files Web URL (or URLs) according to the IIS bindings.
7. After 20 to 30 seconds, enter your website address in a browser and make sure that the client opens (or clients open) correctly.

Setting Up Classic M-Files Web and M-Files Mobile

The steps given here tell you how to enable these clients and services:

- Classic M-Files Web
- M-Files REST API
- M-Files Mobile
    - The default connection protocol is HTTPS. To set M-Files Mobile to use gRPC, refer to Setting Up M-Files to Use gRPC.

M-Files Web and Microsoft Office for the web services for M-Files Web are not enabled.

Make sure that these requirements are completed:

- The server uses IIS (Internet Information Services) and Microsoft .NET Framework (not .NET) 4.7.2, 4.8.x, or later.
- You are an M-Files system administrator on the server.
- You have set up IIS binding for the website that users access with a DNS name, such as `https://myvault.mycompany.com`.
    - If you want to create a new website for M-Files Web, do the binding setup after you have saved your changes in M-Files Admin.

Important remarks:

- If you get an error during the setup, exit the wizard, fix the issue in IIS Manager, and start the wizard again. The error can be, for example, that a newly created website cannot start because the port number is already in use.

Do these steps:

1. Open M-Files Admin on the server.

    Important: If IIS and M-Files are on separate servers, refer to Configuring the Classic M-Files Web on a Separate Server Computer instead of the instructions given here.

2. In the left-side tree view, select a server connection.
3. Click **Set Up Web and Mobile Use** > **Set up classic M-Files Web (and REST) and M-Files Mobile** > **Next**.
4. Select one of these options:

Option	Result and instructions
Use an existing website	Use an existing Internet Information Services site for M-Files Web. In the drop-down menu, select one of the available sites.
Create a new website	Create a new Internet Information Services website for M-Files Web. Enter the name and TCP port for the site. Make sure that the given port number is not already in use. **Note:** You can use this option only with a server operating system.
Create a new virtual directory	Add a new virtual directory to the selected Internet Information Services website and use the directory for M-Files Web. Select an available site and enter a name for the virtual directory. **Note:** You can use this option only with a server operating system.

5. Select **Save**.
6. Open the Document Vault Advanced Properties dialog and add the M-Files Web URL (or URLs) according to the IIS bindings.
7. After 20 to 30 seconds, enter your website address in a browser and make sure that the client opens (or clients open) correctly.

Setting Up Both Web Clients and M-Files Mobile

The steps given here tell you how to enable these clients and services:

- M-Files Web
- Microsoft Office for the web services for M-Files Web
- Classic M-Files Web
- M-Files REST API
- M-Files Mobile
    - The default connection protocol is HTTPS. To set M-Files Mobile to use gRPC, refer to Setting Up M-Files to Use gRPC.

Make sure that these requirements are completed:

- The server uses M-Files October '22 Update or later.

- If the server uses an older version, we recommend that you upgrade to a more recent version. Alternatively, refer to Setting Up the Backend for M-Files Web and Web-Based Add-Ins (September '22 Update and Earlier). Refer to the M-Files 2018 user guide for setup instructions for the classic M-Files Web.

- The server uses IIS (Internet Information Services) and Microsoft .NET Framework (not .NET) 4.7.2, 4.8.x, or later.
- You are an M-Files system administrator on the server.
- The IIS modules URL Rewrite and Application Request Routing are installed on the IIS server.
- You have set up IIS binding for the website that users access with a DNS name, such as `https://myvault.mycompany.com`.

    - If you want to create a new website for M-Files Web, do the binding setup after you have saved your changes in M-Files Admin.

Important remarks:

- If M-Files Web was previously set up on the server with the instructions in Setting Up the Backend for M-Files Web and Web-Based Add-Ins (September '22 Update and Earlier): We recommend that you remove the old configuration before you set up M-Files Web with the instructions given here.
- If you get an error during the setup, exit the wizard, fix the issue in IIS Manager, and start the wizard again. The error can be, for example, that a newly created website cannot start because the port number is already in use.

Do these steps:

1. Open M-Files Admin on the server.

    ! **Important:** If IIS and M-Files are on separate servers, see Using Proxy Setup with M-Files Web instead of the instructions given here.

2. In the left-side tree view, select a server connection.

3. Select **Set Up Web and Mobile Use**.

4. Select one of these options:

Option	Description
Set up M-Files Web, classic M-Files Web (enabled), M-Files REST API, and M-Files Mobile	This option sets up all the listed clients.
Set up M-Files Web, classic M-Files Web (disabled), M-Files REST API, and M-Files Mobile	This option sets up all the listed clients but sets the classic M-Files Web to be disabled. All links that refer to the classic M-Files Web are automatically redirected to M-Files Web.

    You can enable or disable the classic M-Files Web after it is set up. See Enabling or Disabling the Classic M-Files Web.

5. Select **Next**.

6. Select one of these options:

Option	Result and instructions
Use an existing website	Use an existing Internet Information Services site for M-Files Web.

Option	Result and instructions
	In the drop-down menu, select one of the available sites.
Create a new website	Create a new Internet Information Services website for M-Files Web. Enter the name and TCP port for the site. Make sure that the given port number is not already in use. **Note:** You can use this option only with a server operating system.
Create a new virtual directory	Add a new virtual directory to the selected Internet Information Services website and use the directory for M-Files Web. Select an available site and enter a name for the virtual directory. **Note:** You can use this option only with a server operating system.

7. In **Site Binding Address**, enter a site binding that the M-Files application server can use to reach the IIS proxy server computer.

   It is not necessary to use HTTPS or the port 443. You can also use HTTP and any other port or binding available on the IIS server. For example, if the IIS proxy uses a self-signed certificate for the website binding, you must use HTTP because M-Files does not support self-signed certificates in this context.

   If you have many vaults or many DNS names for the IIS sites, we recommend that you use the IP address of the IIS server as the site binding address. It can be necessary to create an appropriate binding on the IIS site for this purpose. For example, the binding `http://127.0.0.1:8088` normally allows any incoming traffic for the IIS server IP.

   For a virtual directory, include also the directory name. Refer to the table and this article for examples and more information.

Example	Site binding address	Port	Directory name
`http://127.0.0.1:80`	`http://127.0.0.1`	`80`	-
`http://127.0.0.1:8800/M-Files`	`http://127.0.0.1`	`8800`	`M-Files`

8. Optional: If IIS and the M-Files server are on separate servers, enable **Use proxy server setup** and enter the app server address to use a proxy environment.

   For instructions on how to set up the proxy server and the site binding address, see Using Proxy Setup with M-Files Web.

9. Select **Next** or **Save**.

   The available option changes according to your selection in step 4. Additionally, you can skip steps 10 and 11 if you selected to disable the classic M-Files Web.

10. Optional: Enable **Use M-Files Web as default web client on this server**.

    Before you continue, read the information on the page carefully.

    If this setting is not enabled, the classic M-Files Web is used as the default client. This also lets you control the default web client vault-specifically. See Changing the default web client vault-specifically.

    If you use OAuth-based authentication in the vault, the default web client setting can have an effect on the endpoint settings of your configuration. For more information, refer to Setting Up OAuth 2.0 for the New M-Files Web and Web-Based Add-Ins.

11. Select **Save**.

12. Open the Document Vault Advanced Properties dialog and add the M-Files Web URL (or URLs) according to the IIS bindings.

13. After 20 to 30 seconds, enter your website address in a browser and make sure that the client opens (or clients open) correctly.

The users can now open the web clients with the addresses given here.

M-Files Web set as the default client:

Client	**Address**	**Example**
M-Files Web	*<server address>*	`https://cloudvault.mycompany.com`
Classic M-Files Web	*<server address>*`/login.aspx`	`https://cloudvault.mycompany.com/login.aspx`
REST API endpoint	*<server address>*`/REST`	`https://cloudvault.mycompany.com/REST`

Classic M-Files Web set as the default client:

Client	**Address**	**Example**
M-Files Web	*<server address>*`/vnext`	`https://cloudvault.mycompany.com/vnext`
Classic M-Files Web	*<server address>*	`https://cloudvault.mycompany.com`
REST API endpoint	*<server address>*`/REST`	`https://cloudvault.mycompany.com/REST`

Changing the Default Web Client

In environments where you use both versions of M-Files Web, you can select the default web client for all vaults on the server, or for each vault.

Note: If you use OAuth-based authentication in the vault, the default web client setting can have an effect on the endpoint settings of your configuration. For more information, refer to Setting Up OAuth 2.0 for the New M-Files Web and Web-Based Add-Ins.

Changing the default web client server-specifically

With these steps, you can change the default web client settings collectively for all vaults on the server. You must have the M-Files system administrator permissions on the server to access these settings.

1. Open M-Files Admin.
2. In the left-side tree view, select a server connection.

   If you use an IIS (Internet Information Services) proxy setup, connect to the M-Files server on the proxy computer instead of the M-Files application server.
3. Select **Set Up Web and Mobile Use** > **Change the default web client on this server** > **Next**.
4. Enable or disable **Use M-Files Web as default web client on this server**.

   Before you continue, read the information on the page carefully.
5. Select **Save**.
6. Open the Document Vault Advanced Properties dialog and add the M-Files Web URL (or URLs) according to the IIS bindings.

   See this table for additional information.
7. After 20 to 30 seconds, enter your website address in a browser and make sure that the client opens (or clients open) correctly.

If you use many websites to access M-Files Web, and if they run on the same IIS server, the sites have the same default client. If you have many IIS servers as proxies on computers separate from the M-Files application server, each server can have their own default client.
Changing the default web client vault-specifically

Before you start, make sure that these prerequisites are completed:

- The new M-Files Web is not set as the default client on the server.
  - See Checking information about the current web setup for instructions on how to see information about the default client.
- If you have an on-premises setup where you have access to server settings, configure mappings between incoming connections and vaults.
  - If you use M-Files Cloud, it is not necessary to configure the mappings.
  - Without vault-specific DNS names (all vaults are accessed with the same address), you cannot change the default client for each vault.

To change the default web client settings separately for a vault:

1. In the **Advanced Vault Settings** section of M-Files Admin, go to **Client** > **Web**.

   The **Manage Client Settings Centrally** setting must be set to **Yes**. Before you set it to **Yes**, read the setting description on the **Info** tab.
2. Select a value for **Use as Default Web Client**.

   Use the value **Yes** for M-Files Web and the value **No** for the classic M-Files Web.

3. Click **Save**.
4. Open the Document Vault Advanced Properties dialog and add the M-Files Web URL (or URLs) according to the IIS bindings.
5. After 20 to 30 seconds, enter your vault address in a browser and make sure that the selected client opens correctly.

The users can now open the web clients with the addresses given here.

M-Files Web set as the default client:

Client	Address	Example
M-Files Web	*<server address>*	`https://cloudvault.mycompany.com`
Classic M-Files Web	*<server address>*`/login.aspx`	`https://cloudvault.mycompany.com/login.aspx`
REST API endpoint	*<server address>*`/REST`	`https://cloudvault.mycompany.com/REST`

Classic M-Files Web set as the default client:

Client	Address	Example
M-Files Web	*<server address>*`/vnext`	`https://cloudvault.mycompany.com/vnext`
Classic M-Files Web	*<server address>*	`https://cloudvault.mycompany.com`
REST API endpoint	*<server address>*`/REST`	`https://cloudvault.mycompany.com/REST`

Checking information about the current web setup

You can use the **Set Up Web and Mobile Use** dialog to see information about your current setup. When you are done, click **Cancel** so that you do not save any unwanted changes.

Information about the current setup available in the dialog:

Section	Information available
"Select what you want to do" section	If the option to change the default client is available, both web clients are enabled.
M-Files Web connection details	• Site binding address • Enabled or disabled state of the proxy setup • App server address
Default web client selection	• Enabled or disabled status of the **Use M-Files Web as default web client on this server** setting • If the setting is disabled, the classic M-Files Web is the default client on the server level.

Section	Information available
	• If the setting is enabled, you cannot change the default client on the vault level. • This step is only available if you have previously enabled both web clients. • To see information about the default client setting, select the option **Set up M-Files Web, classic M-Files Web (and REST) and M-Files Mobile** or **Change the default web client on this server**.

Information about the current setup not available in the dialog:

Section	Information not available
"Select what you want to do" section	Enabled or disabled status of the services when both web clients are not enabled. You can find this information in IIS.
M-Files Web connection details	Website used to set up access to M-Files Web. You can find this information in IIS.

Enabling or Disabling the Classic M-Files Web

This page tells you how to enable or disable the classic M-Files Web client. When it is disabled, all classic M-Files Web links are automatically redirected to M-Files Web.

M-Files Cloud

If you use M-Files Cloud, use the Advanced Vault Settings (AVS) option **Configuration** > **Client** > **Web** > **Disable Classic M-Files Web and Redirect Links to M-Files Web**. The AVS option changes the default client for the vault, not the server.

On-premises servers

To enable or disable the classic M-Files Web on an on-premises server:

1. Open M-Files Admin.
2. In the left-side tree view, select a server connection.
3. Select **Set Up Web and Mobile Use**.
4. Select **Enable or disable classic M-Files Web on this server**.

   This option is not available if the classic M-Files Web has not been set up.
5. Enable or disable **Use the classic M-Files Web on this server**.
6. Select **Save**.

Using Proxy Setup with M-Files Web

These instructions tell you how to set up an environment with a reverse proxy and an application server. In this setup, there is a separate proxy server for IIS (Internet Information Services) and another server for the M-Files application.

Configuring the application server

If you do not use separate DNS names for your vaults (all vaults are accessed with the same address), you can skip this section.

To configure the server where M-Files is installed:

1. Use Registry Editor to add this registry setting:

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\Common`**
Value name	`VaultDNSConfig`
Value type	`REG_MULTI_SZ`
Value	`https://<proxy server address>={<GUID of the vault to use>}` For example: `https://proxyserver.mycompany.com={F565EDFE-939E-4507-B078-D06902888C98}`
Description	Adds a mapping between the vault and the proxy server.

2. Add this registry key to let each vault control the default web client:

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\Common`**
Value name	`NewWebAsDefault`
Value type	`REG_SZ`
Value	`False`
Description	New web is not the default client for this server. Each vault can control the default web client.

3. Restart the M-Files Server service.
4. Optional: Set M-Files Web as the default client for the vault (see Changing the default web client vault-specifically).
5. Restart the M-Files Server service on the proxy server.

Configuring the proxy server

Note: If you want to set up only the classic M-Files Web, only the first step is necessary.

To configure the server used as the reverse proxy:

1. Set up the proxy server with the instructions given in Configuring the Classic M-Files Web on a Separate Server Computer.

   ⓘ During the setup, make note of this information:

- M-Files Server must be the same version as the one installed on the application server.
- No vaults can be attached to the M-Files Server installation on the proxy server.
- If you have many vaults with separate DNS names, the IIS (Internet Information Services) site on the proxy server must respond to all of them publicly. In other words, the IIS site must have the necessary bindings.

2. Open M-Files Admin.

3. Connect to the M-Files Server instance of the proxy computer.

In most situations, M-Files Admin and M-Files Server are installed on the same proxy computer. This means that you can use M-Files Admin to connect to M-Files Server locally.

IIS must run on the same proxy computer as the M-Files Server instance to which you are connected.

4. Configure M-Files Web with the instructions in Setting Up M-Files Web or Setting Up Both Web Clients and M-Files Mobile.

During the configuration, make note of these substeps:

a) Make sure that the address of the site specified in the **Set Up Web and Mobile Use** dialog is the same as the one used in step 1 of Configuring the application server.

This is also the address with which the users connect to the M-Files Web client.

b) Enable **Use proxy server setup**.

c) In **Site Binding Address**, enter a site binding that the M-Files application server can use to reach the IIS proxy server computer.

It is not necessary to use HTTPS or the port 443. You can also use HTTP and any other port or binding available on the IIS server. For example, if the IIS proxy uses a self-signed certificate for the website binding, you must use HTTP because M-Files does not support self-signed certificates in this context.

If you have many vaults or many DNS names for the IIS sites, we recommend that you use the IP address of the IIS server as the site binding address. It can be necessary to create an appropriate binding on the IIS site for this purpose.

Example: The IIS server's private IP is `10.0.0.1`. You have bound the port `8080` to it and have not limited the binding to a specific IP. Set `http://10.0.0.1:8080` as the site binding address.

d) In **App server address**, enter the server address of the server where M-Files is installed.

For example: `http://appserver.mycompany.com:7767` or `http://192.168.1.2:7767`, where you can replace the IP address with the actual IP address of the M-Files server computer. Always use the HTTP protocol for this connection. If you have changed the gRPC web port for the M-Files server, use that port here instead. For more information about gRPC in M-Files, refer to Setting Up M-Files to Use gRPC.

5. Use M-Files Admin to connect to M-Files Server on the application server.

6. Open the Document Vault Advanced Properties dialog and add the M-Files Web URL (or URLs) according to the IIS bindings.

7. After 20 to 30 seconds, enter your proxy website address (in this example, `https://proxyserver.mycompany.com`) in a browser and make sure that M-Files Web opens correctly.

3.2.9. Publishing Vault Content with Classic M-Files Web

Normally, you must have a username and a password to use a vault with M-Files Web. However, you can also use M-Files Web to publish documents to people that do not use M-Files. Users can access this type of vault without user credentials and they have read access to the content. You can, for example, share on your website a price list that is saved to M-Files and is always up to date.

If you use the classic M-Files Web, do the steps given in the subsections. Before you start, make sure that M-Files Web is correctly configured and that you have the External Connector license.

New M-Files Web and M-Files Mobile

If you use the new M-Files Web or M-Files Mobile, enable the Anonymous authentication feature. The rest of the steps in this section are not necessary.

In this chapter

Creating a Login Account for Publishing

Note: These instructions are only for the classic M-Files Web.

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 used for publishing.
2. In the left-side tree view, expand a connection to M-Files server.
3. Click **Login Accounts**.
4. In the task area, click **New Login Account**.

   ✓ The **New Login Account** dialog is opened.
5. In **Username**, enter a username.

   ⓘ For example, `Publishing`.
6. In **Authentication**, select **M-Files authentication**
7. In **Password**, enter a password.
8. In **Confirm password**, enter the same password.
9. In **License type**, select a license.

   ⓘ For information about the license types, see License type.

10. Click **OK**.

The created login account is added to the **Login Accounts** list.

For information on the next step, see Adding the Login Account as a User to the Publishing Vault.

Adding the Login Account as a User to the Publishing Vault

Note: These instructions are only for the classic M-Files Web.

Second, add the created login account as a user to the publishing vault:

1. Open M-Files Admin on the M-Files server used for publishing.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click **Users**.
6. Click **New User** on the task area.

   ✓ The **New User** dialog is opened.
7. In **Login account**, select the login account that you created.
8. Enable **External user**.
9. Optional: Enable **User cannot create documents or other objects**.
10. Optional: Enable **User cannot create or modify traditional folders**.
11. Optional: Enable **User cannot create or modify private views or notification rules**.
12. Click **OK**.

The user is added to the **Users** list.

For information on the next step, see Giving Read Permissions to the Publishing Vault User.

Giving Read Permissions to the Publishing Vault User

Note: These instructions are only for the classic M-Files Web.

Third, give the user read permissions to published documents:

1. Open M-Files Admin on the M-Files server used for publishing.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Click **Named Access Control Lists**.

6. Do one of these steps:

   a. Click **New Named Access Control List** to create a named access control list for the user.

      or

   b. Double-click an existing named access control list on the **Named Access Control Lists** list to edit the permissions of the user.

7. If you started to create a named access control list, in **Name**, enter a name for the list.

8. Click **Add**.

9. In **Users or user groups**, select the user.

10. Click **Add**.

11. Select the user and specify these permissions:

Permission	**Allow / Deny**
Change Permissions	Deny
Delete	Deny
Edit	Deny
Read	Allow

12. Optional: Do this step if your named access control list has all permissions set to **Allow** for the **All internal users** user group. Otherwise, skip this step.

   a) Click **Add**.
   b) Select **All internal users** and click **Add**.
   c) In the **Users and user groups** list, select **All internal users**.
   d) In the **Permissions** section, set the **All** permission to **Allow**.

13. Click **OK**.

14. Set the named access control list to all documents that you want to be accessed without credentials.

For information on the next step, see Enabling the Login Account to Log In Automatically.

Enabling the Login Account to Log In Automatically

Note: These instructions are only for the classic M-Files Web.

Finally, set M-Files to log in to the classic M-Files Web automatically:

1. On the M-Files server, use Registry Editor to create this registry key, where *<version>* is the M-Files version number (for example `11.1.4310.92`) and *<website ID>* is a unique ID given to the M-Files Web site by Internet Information Services (IIS):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFWA\Sites
\<website ID>\
```

- If there is only one website, the site ID is usually `1`.
- If the M-Files Web site runs in the virtual directory of the website, add a colon and the name of the virtual directory after the site ID. For example, if the application is in the M-Files Web virtual directory of this single website, the website ID is `1:MFWA`.

- The IIS server software in Windows 2003 shows the ID as one column.

2. Specify the registry key values to be used for automatic login. This table contains the values available for specification:

Value	Type	Description
Domain	REG_SZ	If the authentication method in use is Windows authentication, specify the domain in this value.
Password	REG_SZ	The login password.
UserName	REG_SZ	The login account name.
Vault	REG_SZ	The document vault ID. The value can be for example `{A8DCB561-913F-4318-A276-E7E171EAFBE6}`. The value can be found in the **Document Vault Properties** window of a vault in M-Files Admin.
WindowsUser	REG_DWORD	Specifies the authentication method. `False` is for M-Files authentication, and `True` is for Microsoft Windows authentication.

3. Close Registry Editor.

4. Use Windows Task Manager to restart the **MFServer** service:
   a) Right-click the taskbar and select **Task Manager**.

   ✓ The **Task Manager** window is opened.

   b) Open the **Services** tab.
   c) Right-click the **MFServer** service and select **Restart**.

The selected login account can now automatically log in to the classic M-Files Web, and the account can access published documents without user credentials.

Creating Direct Web Links

Note: These instructions are only for the classic M-Files Web.

When automatic login is enabled, you can create direct weblinks between, for example, the company website and documents. You can give the opening page, `openfile.aspx`, these parameters:

Parameter	Description
`objtype`	The object type ID of the document that contains the file to be opened. This parameter is required. To see the list of object type IDs, do the first four steps of the Creating a New Object Type task.
`docid`	The ID of the document that contains the file to be opened. This parameter is required.
`docver`	The version of the document that contains the file to be opened. If this parameter is not set, the link always refers to the latest version of the document.
`fileid`	The ID of the file to be opened. This parameter is only required when the document that contains the file is a multi-file document.
`filever`	The version number of the file.

Parameter	Description
`showopendialog`	Specifies whether the browser shows an opening dialog. By default, the value is `1` and the dialog is shown. If the value is set to `0`, the dialog is not shown.

Here are some examples:

- `https://<server>/openfile.aspx?objtype=0&docid=71`
- `https://<server>/openfile.aspx?objtype=0&docid=71&docver=7`
- `https://<server>/openfile.aspx?objtype=0&docid=71&docver=7&fileid=71`
- `https://<server>/openfile.aspx?objtype=0&docid=71&showopendialog=0`

Replace *`<server>`* with the web address of your own server.

Optional: Changing Publication Settings

Note: These instructions are only for the classic M-Files Web.

When documents are published online, it is usually a good idea to hide some of the object properties. For example, if the user has read-only access, it is not necessary to show the functions for editing. With the publication settings, the users can be given suitable and sufficient functions that facilitate and simplify accessing and processing of the published information.

Opening publication settings

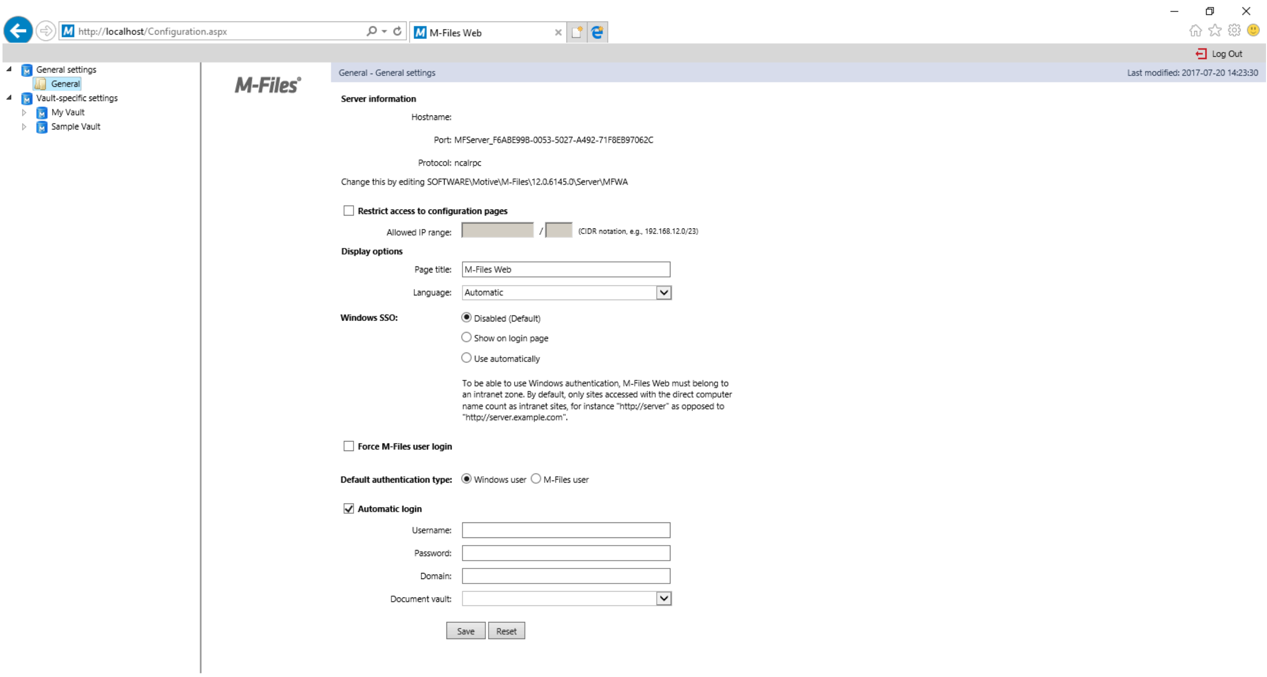
You can specify different publication settings with a separate configuration site.

Log in to the configuration page with `<your organization's M-Files Web URL>/configuration.aspx`. For example, `http://www.publications.company.com/configuration.aspx`.

Note: You must be a system administrator to edit the publication settings.

General settings

In the general settings, you can make selections that are used for the configuration site and all vaults of the site.



General - General settings

Last modified: 2017-07-20 14:23:30

Server information

Hostname:

Port: MFServer_F6ABE99B-0053-5027-A492-71F8EB97062C

Protocol: ncalrpc

Change this by editing SOFTWARE\Motive\M-Files\12.0.6145.0\Server\MFWA

□ **Restict access to configuration pages**

Allowed IP range: / (CIDR notation, e.g., 192.168.12.0/23)

Display options

Page title: M-Files Web

Language: Automatic

Windows SSO:

● Disabled (Default)

○ Show on login page

○ Use automatically

To be able to use Windows authentication, M-Files Web must belong to an intranet zone. By default, only sites accessed with the direct computer name count as intranet sites, for instance "http://server" as opposed to "http://server.example.com".

□ **Force M-Files user login**

Default authentication type: ● Windows user ○ M-Files user

☑ **Automatic login**

Username:

Password:

Domain:

Document vault:

Figure 65: 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 website 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 classic 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 classic 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 classic 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 classic 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.
- The vault language has been set for the vault user.
- 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, the classic 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 the classic M-Files Web.

Note: For security reasons, federated authentication is recommended. For more information, see User authentication.

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 the classic 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

In the vault-specific settings you can specify, for example, these things:

- Whether the vault is to be available for use with the classic 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 with the classic 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 select the layout elements to be displayed in the vault. For example, you can hide the task area or display the listing area only.

Microsoft Office for the web editor

To set up the Microsoft Office for the web editor, refer to Enabling Microsoft Office for the Web Services for M-Files.

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 the classic 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 let you control which functions are available for the users of the vault.

- *Save view settings*. If many 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 classic 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 area.

> **Note:** If you hide the **New** commands, users cannot create new objects. If the **View and Modify** commands are hidden, they are not available in the context menu either.

In this chapter

Example: Changing the Appearance of the Classic 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. In 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. Click a folder in the selected vault to select the category that you want to edit:

   a. Select the **Controls** folder to show or hide M-Files Web user interface controls.

      or

   b. Select the **Task area** folder to show or hide elements in the M-Files Web task area.

4. Select the **Show** or **Allow** radio button for the elements that you want to enable.

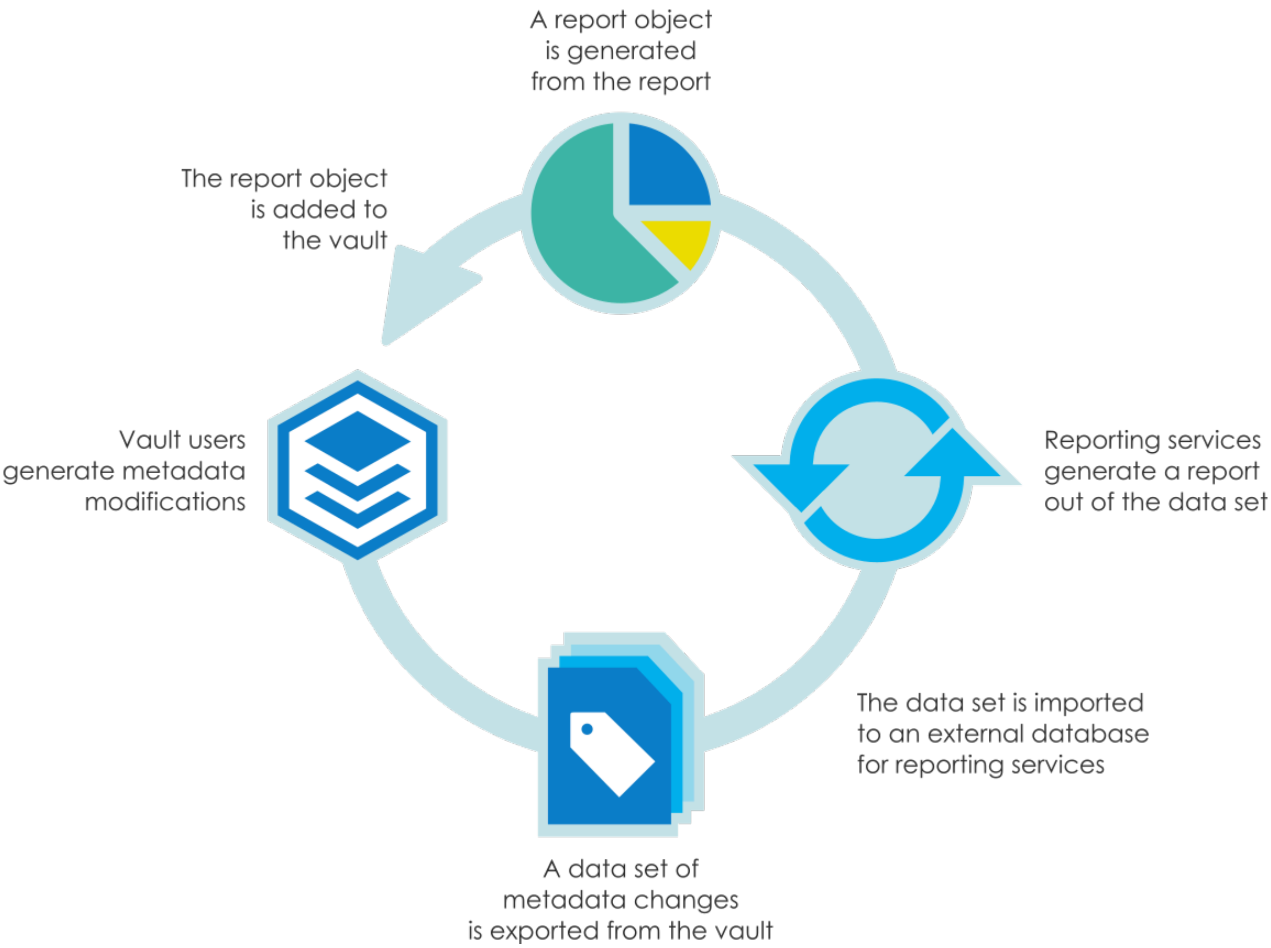
   If you want to show the **Log Out** button in the task area, go to the **Task area** settings, and select **Show** for the **Log Out** option.

5. Select the **Hide** or **Disallow** radio button for the elements that you want to disable.

3.2.10. 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.


A report object is generated from the report
The report object is added to the vault
Vault users generate metadata modifications
Reporting services generate a report out of the data set
The data set is imported to an external database for reporting services
A data set of metadata changes is exported from the vault

Activation

The reporting module enables data export from M-Files to create reports and display them in the M-Files user interface. The module is available for a separate fee.

In most environments, the module is automatically activated if your subscription includes it. If licenses are managed manually on your on-premises M-Files server, refer to Managing Server Licenses.

To find out how M-Files can support your business with M-Files reports, please contact us at sales@m-files.com.

Reporting database

The reporting data is exported from the vault to an external reporting database. In M-Files Cloud, the reporting database is available for a separate fee.

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.

In this chapter

- Creating a Data Set

- Specifying the Report Access Identity
- Creation of Reports and the Required Software
- Creating a Report Object for a Report
- Exporting a Report

Creating a Data Set

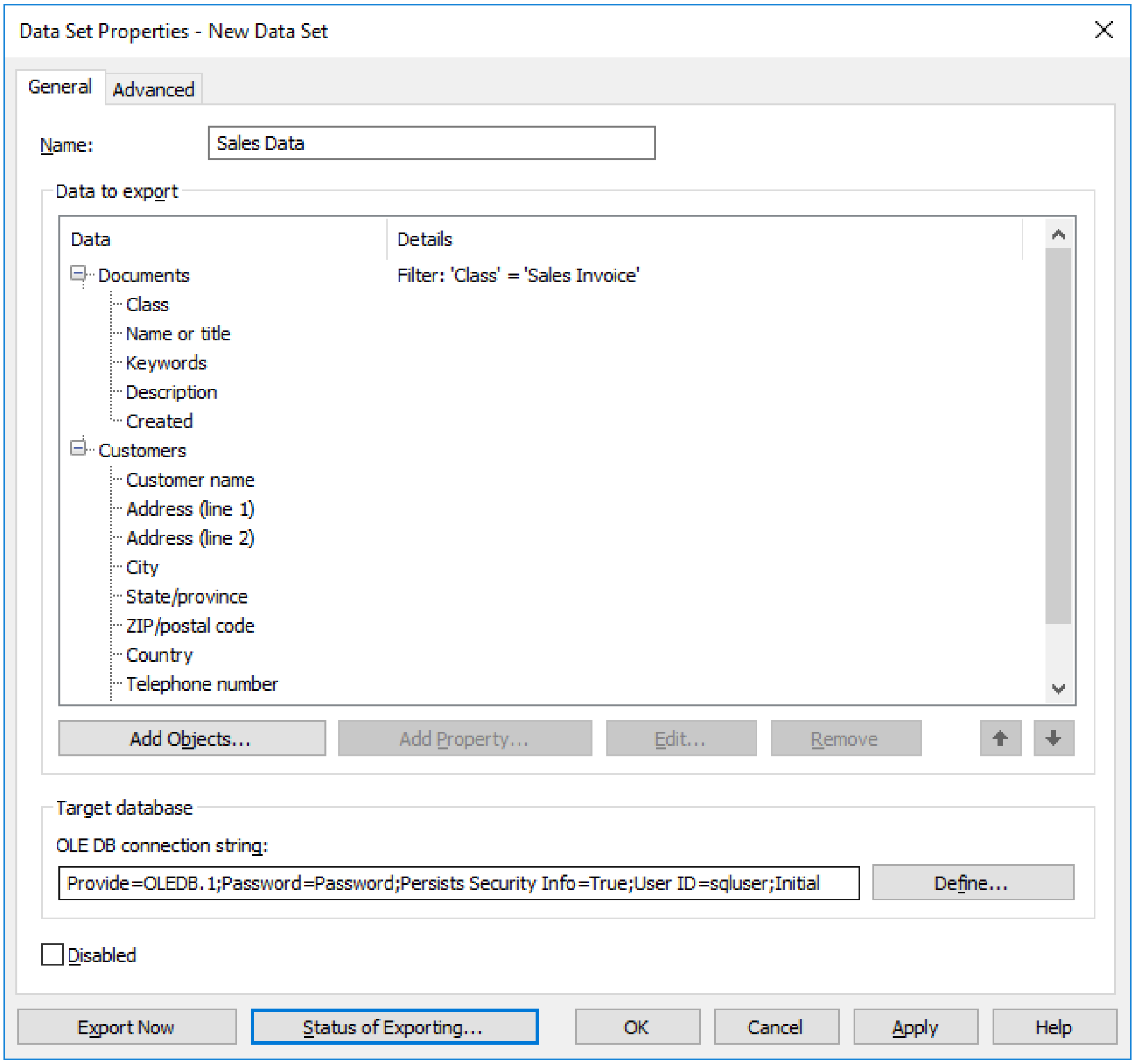
With *M-Files Reporting Data Services*, you can export data from M-Files to external databases (SQL Server). You can select which data is exported, set scheduled data exports, and generate reports of the exported data set. *M-Files Reporting Data Services* is installed when you install M-Files Server.

Before you create a data set, we recommend that you create a new target database to which the new data set is exported.

To create a data set:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Reporting and Data Export** and then click **New Data Set** on the task area.

   ☑ The **Data Set Properties** dialog opens.



Data Set Properties - New Data Set

Name: Sales Data

Data to export

Data	Details
Documents	Filter: 'Class' = 'Sales Invoice'
Class	
Name or title	
Keywords	
Description	
Created	
Customers	
Customer name	
Address (line 1)	
Address (line 2)	
City	
State/province	
ZIP/postal code	
Country	
Telephone number	

Target database

OLE DB connection string:

Provide=OLEDB.1;Password=Password;Persists Security Info=True;User ID=sqluser;Initial

□ Disabled

6. In the **Name** field, enter a name for the new data set.

7. 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.

8. 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 Property-Based Conditions.

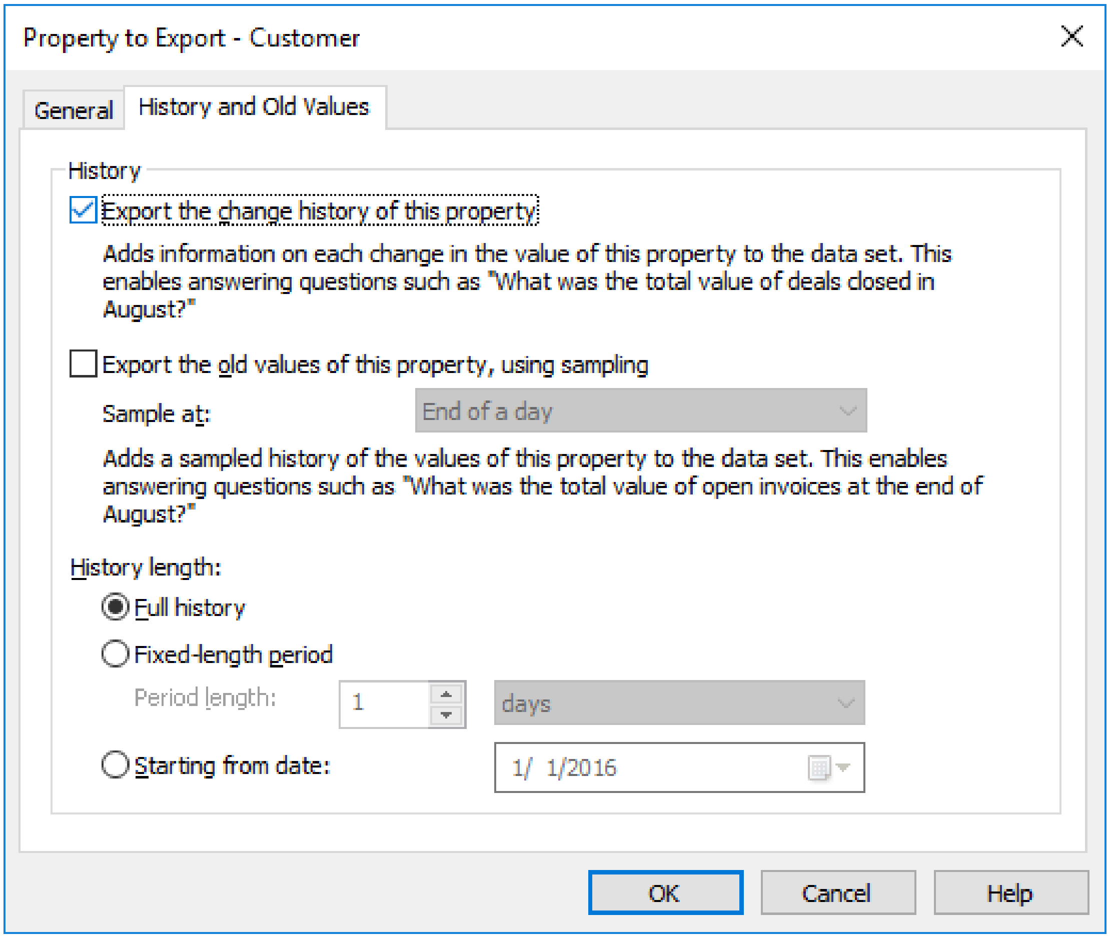
9. Optional: Select the object that you just added to the **Data to export** section and click **Add Property...** to add for the selected object type a property that you want to be exported.

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.



Property to Export - Customer

General | History and Old Values

History

☑ Export the change history of this property

Adds information on each change in the value of this property to the data set. This enables answering questions such as "What was the total value of deals closed in August?"

□ Export the old values of this property, using sampling

Sample at: End of a day

Adds a sampled history of the values of this property to the data set. This enables answering questions such as "What was the total value of open invoices at the end of August?"

History length:

● Full history

○ Fixed-length period

Period length: 1 days

○ Starting from date: 1/ 1/2016

c) Check the **Export the change history of this property** 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** 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 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.

10. 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.

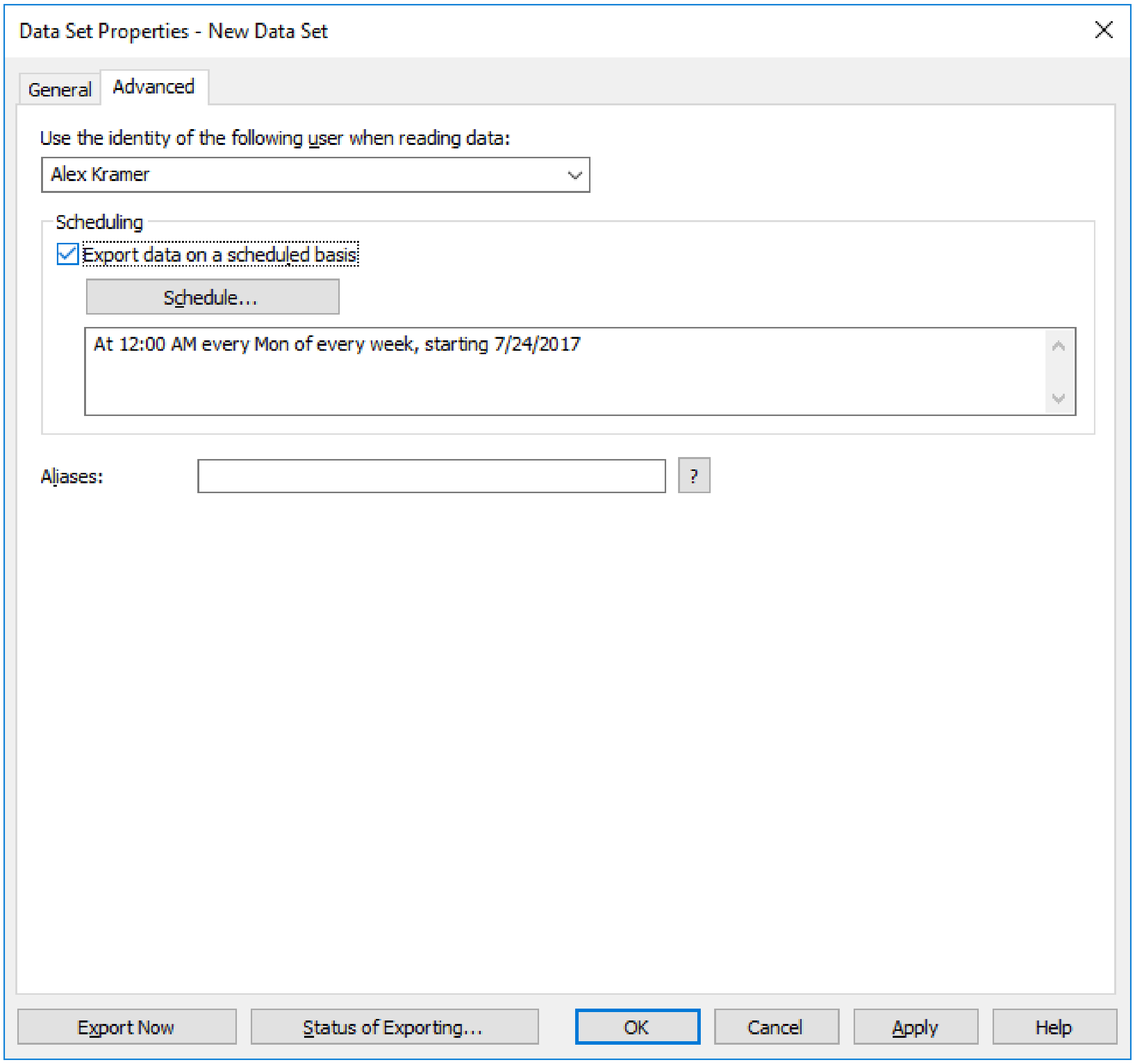
Note: We recommend that you use a separate target database for every new data set.

If you use Microsoft SQL Server as the target database, it is advised to use Microsoft OLE DB Driver for SQL Server (`MSOLEDBSQL`) as the data provider, and to use either **Simple** or **Bulk-logged** as the **Recovery model** setting in the target database. This will significantly improve the speed and performance of exporting data sets.

For more information on database connection strings, see Connections to External Databases for Object Types.

11. Go to the **Advanced** tab.

☑ The **Advanced** tab is opened.



Data Set Properties - New Data Set

Use the identity of the following user when reading data: Alex Kramer

Scheduling

☑ Export data on a scheduled basis

At 12:00 AM every Mon of every week, starting 7/24/2017

Aliases:

12. In the **Use the identity of the following user when reading data** drop-down menu, 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.

If the metadata structure of the vault is translated into multiple languages, the metadata language of the exported data set depends on the vault language settings of the user whose identity is used for reading data.

If you have the Electronic Signatures and Advanced Logging module in use, you must select **(M-Files Server)** as the user.

13. 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, contact our customer support in M-Files Support Portal or your M-Files reseller.

14. Optional: On the **Advanced** tab, define an alias for the data set.

    Use semicolons (;) to separate many aliases.

    When automatic aliases are in use and you write a name on the **General** tab, the **Aliases** field on the **Advanced** tab is automatically filled in. The alias has the format <*predefined prefix*>.<*name*>. Configure automatic aliases for your vault in Advanced Vault Settings.

15. 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.

16. 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) and then create a report object in M-Files to read the report (see Creating a Report Object for a Report).

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 and for reading them.

To specify the report access identity:

1. Open M-Files Admin.

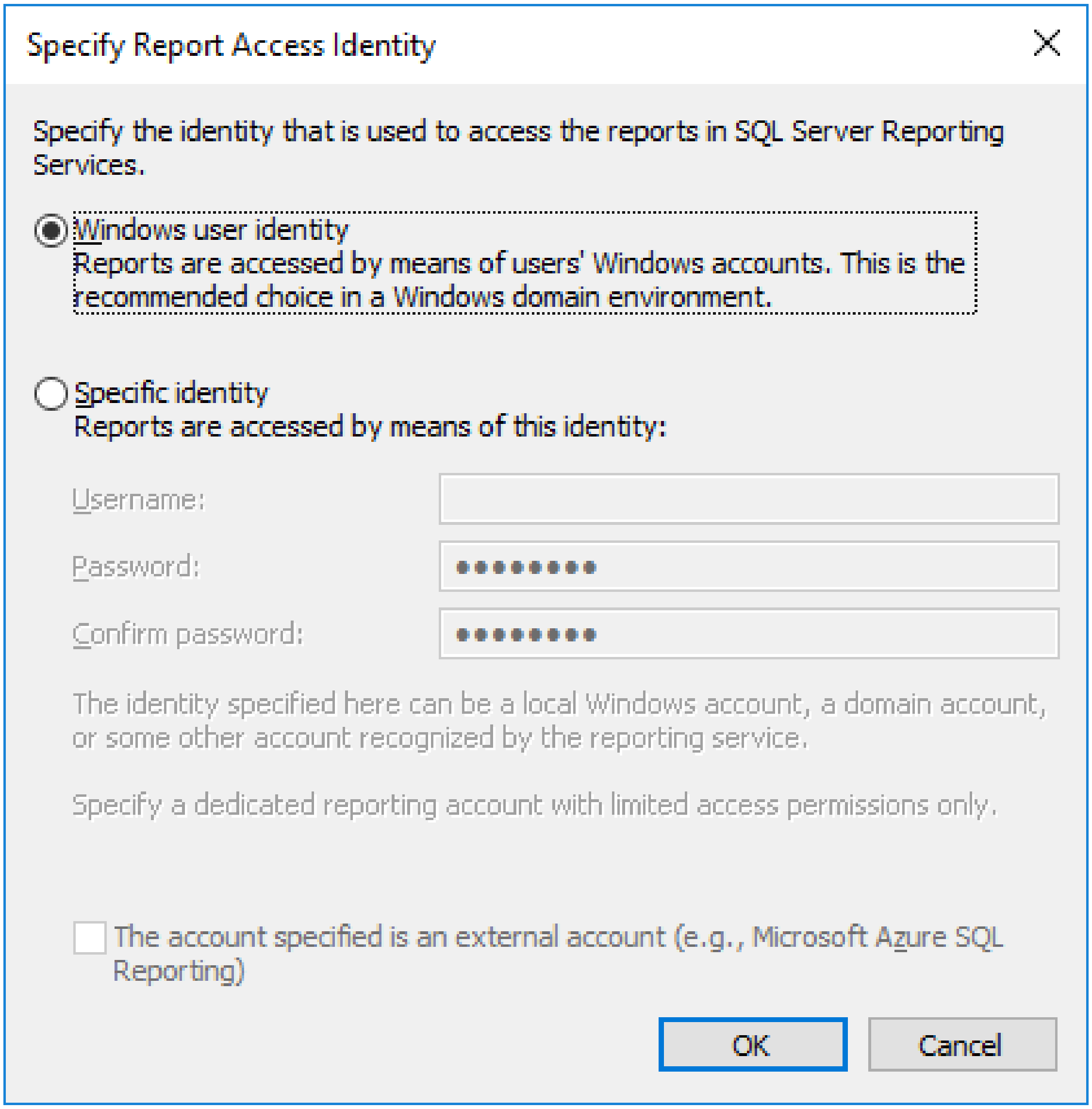
2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Select **Reporting and Data Export** and then click **Specify Report Access Identity** in the task area.

    ✓ The **Specify Report Access Identity** dialog is opened.



Specify Report Access Identity

Specify the identity that is used to access the reports in SQL Server Reporting Services.

● Windows user identity
Reports are accessed by means of users' Windows accounts. This is the recommended choice in a Windows domain environment.

○ Specific identity
Reports are accessed by means of this identity:

Username:

Password: ●●●●●●●●

Confirm password: ●●●●●●●●

The identity specified here can be a local Windows account, a domain account, or some other account recognized by the reporting service.

Specify a dedicated reporting account with limited access permissions only.

□ The account specified is an external account (e.g., Microsoft Azure SQL Reporting)

6. Select either:

   a. **Windows user identity**: Select this option to access reports with 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)** check box if the specified account is an external account.

7. 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 and for reading them.

Creation of Reports and the Required Software

Reports from M-Files to an external database use the Microsoft SQL Server Reporting Services infrastructure, which must be set up correctly.

When reports are created for M-Files, the SQL Server Reporting Services system contacts the exporting database to generate reports when the classic M-Files Desktop requires it.

Microsoft SQL Server Reporting Services can be installed with the SQL Server package (Microsoft SQL Server 2012 or later).

Free SQL Server Express versions can also be used for reporting. To use SQL Server Express, you must use the SQL Server Express with Advanced Services edition. The edition contains the necessary reporting services module. Download it from Microsoft's website at https://www.microsoft.com/en-us/sql-server/sql-server-editions-express.

For more information, refer to http://msdn.microsoft.com/en-us/library/ms159106.aspx (SQL Server Books Online).

In planning reports, you must use **Business Intelligence Development Studio** or the simpler **Report Builder** tool. The person responsible for the planning must have experience and skills in creating reports. Contact our consulting services personnel for help with report planning (sales@m-files.com).

For installation instructions of Microsoft's reporting services, visit Microsoft's webpages or contact our customer support in M-Files Support Portal or your M-Files reseller.

Note: Instructions on planning and creating reports and using third-party software are available from the M-Files consulting services for a 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), it can be retrieved for use in the classic M-Files Desktop.

For displaying reports, Microsoft .NET Framework (not .NET) 4.7.2, 4.8.x, or later (or the most recent available *Client Profile* version) is required. If the client computer does not have an appropriate .NET Framework installed, the report is not shown and the user is prompted to install the framework. You can download the most recent .NET Framework version from Microsoft Download Center.

Follow these steps to create a report object:

1. In M-Files, right-click on the listing area and select **Create** > **Report...** from the context menu.

   ✓ The **New Report** dialog is opened.

2. In the **Name or title** field, enter a name describing the report.

   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`.

   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, contact our customer support in M-Files Support Portal or your M-Files reseller.

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.

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** 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). 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 with the classic M-Files Desktop whenever necessary. For more information, contact our customer support in M-Files Support Portal or your M-Files reseller.

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.

3.2.11. Event Handlers and Scripts

This section describes how to create new event handlers and how to use scripts in M-Files. You might also want to see the FAQ article How do I write VBScript code for M-Files purposes?.

Note: When you develop new extensions or edit existing ones, we recommend that you replace VBScript content with Vault Application Framework (VAF) compatible code for future compatibility. For more information on the benefits of VAF development over VBScript, refer to The Vault Application Framework in M-Files Developer Portal.

Note: In a shared M-Files Cloud environment, you can only install custom code that M-Files has validated.

In this chapter

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. The operations are specified using variables, generic features of VBScript, and M-Files API.

Examples of event handler use:

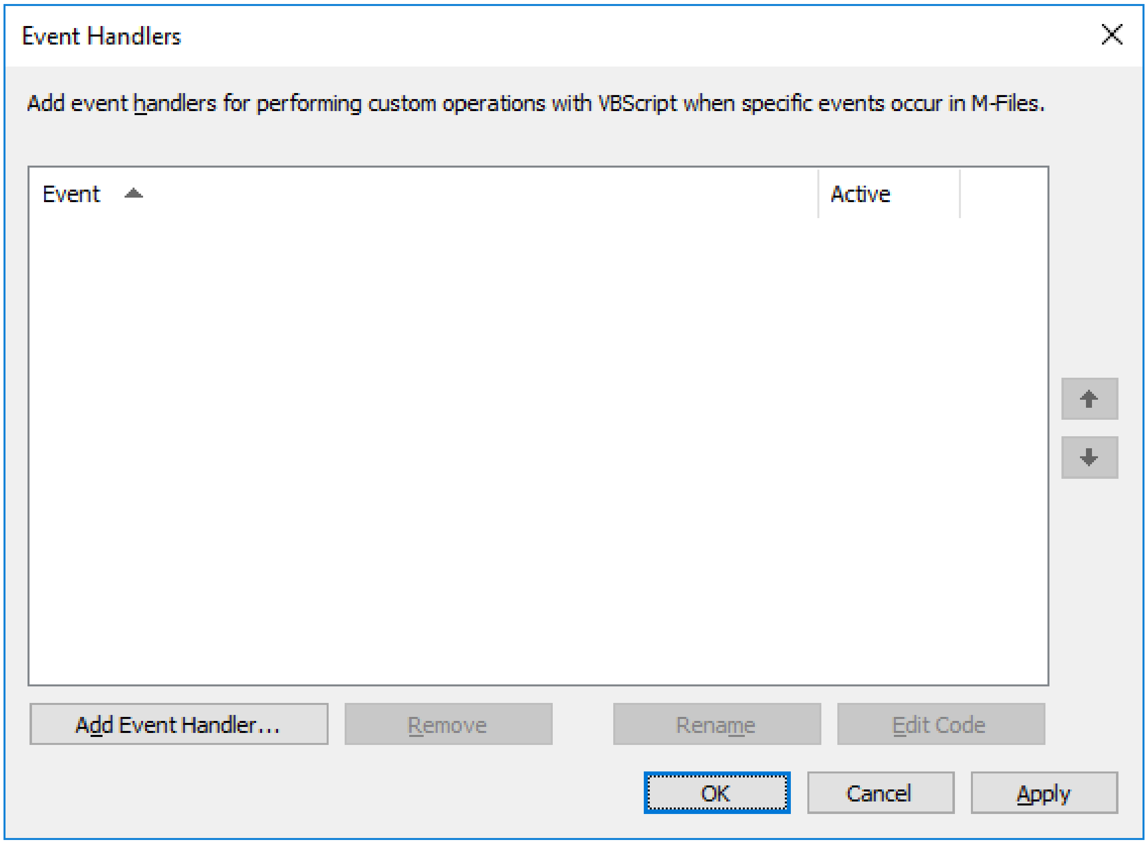
- Object permissions can be set to change automatically when the object properties are changed.
- Certain basic documents can be added to every new project through a pre-defined project model.
- Specified Word documents can always be saved as PDFs, so that when a Word file is checked in, it is saved 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 M-Files API documentation is available online: M-Files API.

Do the following steps to create a new event handler:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Right-click a vault.
4. Click **Event Handlers**.

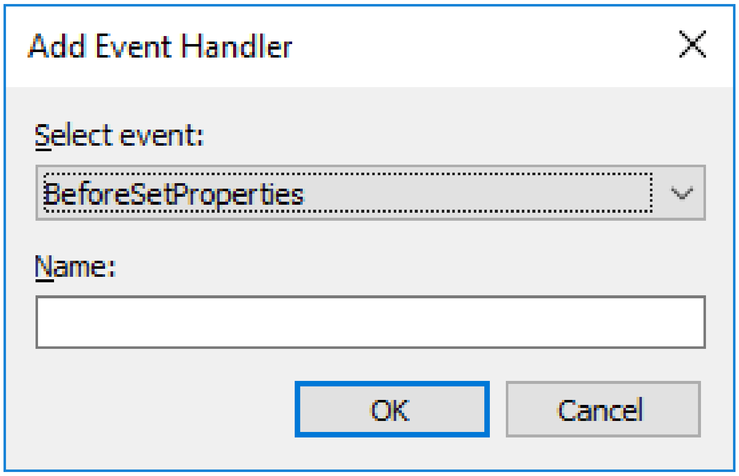
✓ The **Event Handlers** dialog is opened.



Add event handlers for performing custom operations with VBScript when specific events occur in M-Files.

5. Click the **Add Event Handler...** button.

✓ The **Add Event Handler** dialog is opened.



6. Use the **Select event** drop-down menu to select the event for which you want to create an event handler.

   If you want to create an event handler that is invoked whenever a new object is about to be created, select the **BeforeCreateNewObjectFinalize** event.

   For the list of available events and their descriptions, see Available Event Handlers

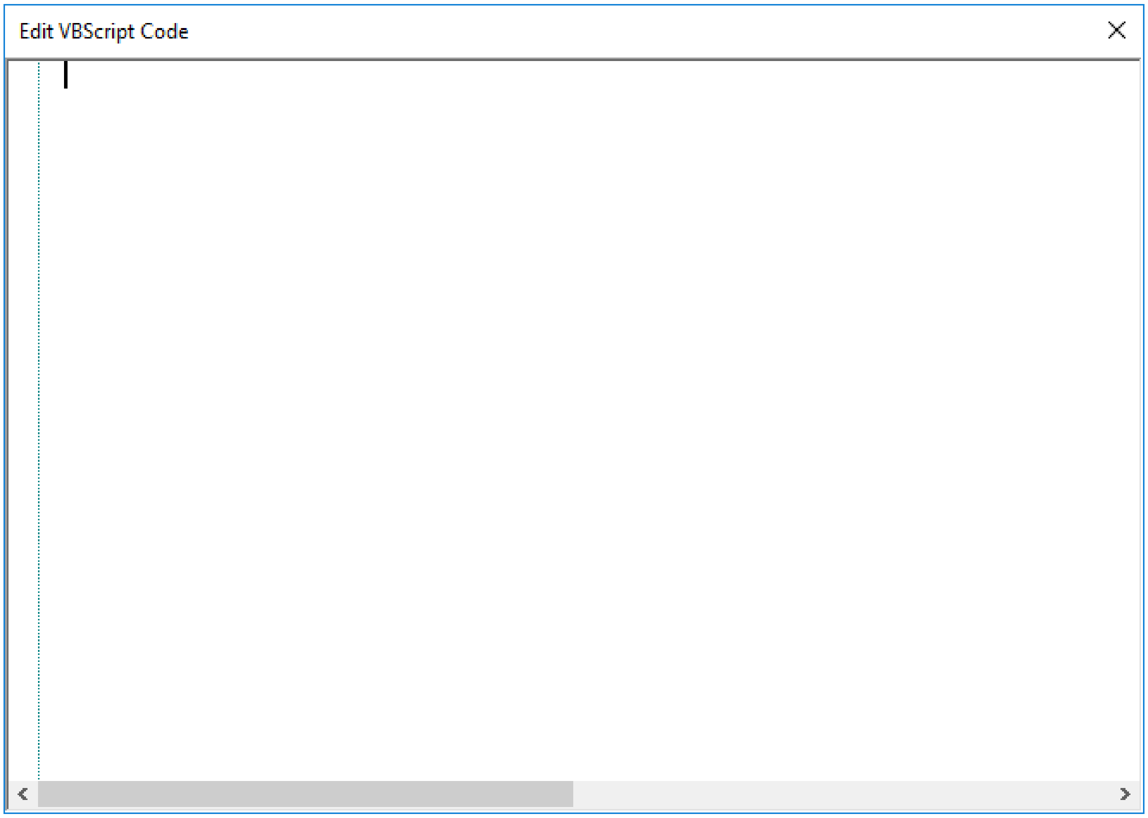
7. In the **Name** field, enter a descriptive name for the new event handler and click **OK** to close the **Add Event Handler** dialog.

   `Check for duplicate titles.`

   If you have more than one event handler of the same type, you may change their execution order by selecting the event handler in the **Event Handlers** dialog and clicking either the up or down arrow button along the right corner of the dialog.

8. Back in the **Event Handler** dialog, click **Edit Code**.

   ✓ The **Edit VBScript Code** window is opened.



9. Enter the code to be executed when the event handler is invoked, and then close the **Edit VBScript** window.

   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:

```
' 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
```

10. 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.

In this chapter

- Available Event Handlers

Available Event Handlers

Below you can find the available event handlers, with their variables and explanations. For more information about variables, see Available VBScript Variables.

Vault-level event handlers

The event handlers listed in this section are triggered by operations on the vault level.

Note: An exception in an event handler prevents the triggering operation from being executed.

Event handler	Variables	Execution
BeforeSetProperties AfterSetProperties	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • PropertyValues • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	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 AfterCreateNewObjectFinalize	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • PropertyValues • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	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 AfterCancelCreateObject	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	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.

Event handler	Variables	Execution
BeforeCheckInChanges AfterCheckInChanges	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	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 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 AfterCancelCheckOut	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	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.

Event handler	Variables	Execution
AfterCancelCheckoutFinalize	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	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 AfterCheckOut	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	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 AfterDeleteObject	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	The event handlers are executed when an object is marked as deleted.

Event handler	Variables	Execution
BeforeDestroyObject AfterDestroyObject	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	The event handlers are executed when an object is destroyed from the document vault.
BeforeDestroyObjectVersion AfterDestroyObjectVersion	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	The event handlers are executed when an individual version of the object is destroyed from the document vault.
BeforeSetObjectPermissions AfterSetObjectPermissions	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • ObjectAccessControlList	The event handlers are executed when the object permissions are changed.

Event handler	Variables	Execution
BeforeFileUpload	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • FileTransferSessionID	The event handler is executed when the user starts a file transfer to M-Files Server.
AfterFileUpload	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • FileTransferSessionID • FileVer	The event handler is executed when the file transfer to the server is completed.
BeforeFileDownload AfterFileDownload	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • FileTransferSessionID • ObjID • FileVer	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.

Event handler	Variables	Execution
BeforeCreateNewValueListItem AfterCreateNewValueListItem	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • ValueListItem	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	• Vault • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • LoginAccount	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	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • LoginAccount	The event handler is executed when the user has successfully logged in to the document vault.

Event handler	Variables	Execution
BeforeLogoutFromVault	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	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	• Vault • VaultSharedVariables • SavepointVariables • TransactionCache • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • LoggedOutUserID	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	• Vault • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • RestoredVersions • ObjVer	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.

Event handler	Variables	Execution
Replication: AfterCreateNewObjectFinalize	• Vault • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • RestoredVersions • ObjVer	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	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • Input • Output	The event handler is invoked explicitly by the client (the so-called vault extension method). The developer of the vault extension method must make sure that the user can be allowed to execute the method. In other words, the method should check the identity of the calling user and terminate if they do not have the required administrative rights in the vault.
BeforeCreateLoginAccount AfterCreateLoginAccount	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • LoginAccount	BeforeCreateLoginAccount: The event is triggered before a vault-level login account is created in the vault database. AfterCreateLoginAccount: The event is triggered after a vault-level login account is created in the vault database.

Event handler	Variables	Execution
BeforeModifyLoginAccount AfterModifyLoginAccount	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • LoginAccount	BeforeModifyLoginAccount: The event is triggered before a vault-level login account is modified in the vault database. AfterModifyLoginAccount: The event is triggered after a vault-level login account is modified in the vault database.
BeforeRemoveLoginAccount AfterRemoveLoginAccount	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • LoginAccount	BeforeRemoveLoginAccount: The event is triggered before a vault-level login account is removed from the vault database. AfterRemoveLoginAccount: The event is triggered after a vault-level login account is removed from the vault database.
BeforeCreateUserAccount AfterCreateUserAccount	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • UserAccount	BeforeCreateUserAccount: The event is triggered before a user account is created in the vault database. AfterCreateUserAccount: The event is triggered after a user account is created in the vault database.

Event handler	Variables	Execution
BeforeModifyUserAccount AfterModifyUserAccount	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • UserAccount	BeforeModifyUserAccount: The event is triggered before a user account is modified in the vault database. AfterModifyUserAccount: The event is triggered after a user account is modified in the vault database.
BeforeRemoveUserAccount AfterRemoveUserAccount	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • UserAccount	BeforeRemoveUserAccount: The event is triggered before a user account is removed from the vault database. AfterRemoveUserAccount: The event is triggered after a user account is removed from the vault database.
BeforeCreateUserGroup AfterCreateUserGroup	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • UserGroupAdmin	BeforeCreateUserGroup: The event is triggered before a user group is created in the vault database. AfterCreateUserGroup: The event is triggered after a user group is created in the vault database.

Event handler	Variables	Execution
BeforeModifyUserGroup AfterModifyUserGroup	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • UserGroupAdmin	BeforeModifyUserGroup: The event is triggered before a user group is modified in the vault database. AfterModifyUserGroup: The event is triggered after a user group is modified in the vault database. **Note:** The AfterModifyUserGroup event handler is not executed when the *All internal users* group is modified.
BeforeRemoveUserGroup AfterRemoveUserGroup	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • UserGroupAdmin	BeforeRemoveUserGroup: The event is triggered before a user group is removed from the vault database. AfterRemoveUserGroup: The event is triggered after a user group is removed from the vault database.
AfterBringOnline BeforeTakeOffline	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	AfterBringOnline: The event is triggered after the vault is brought online. BeforeTakeOffline: The event is executed before the vault is taken offline. An exception in any of the two event handlers does not prevent the online/offline transition.

Event handler	Variables	Execution
AfterCheckInChangesFinalize	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	The event is triggered when the check-in operation and all the operations after the check-in are complete. The event is also triggered when an object is immediately checked in after it has been created. If the object check-in starts a series of automatic state transitions, AfterCheckInChangesFinalize is triggered after the first transition.
BeforeCreateView AfterCreateView	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • View	BeforeCreateView: The event is triggered before a new view is created in a vault. AfterCreateView: The event is triggered after a new view has been created in a vault.
BeforeModifyView AfterModifyView	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • View	BeforeModifyView: The event is triggered before changes made to a view become effective. AfterModifyView: The event is triggered after changes made to a view have become effective.

Event handler	Variables	Execution
BeforeDeleteView AfterDeleteView	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • View	BeforeDeleteView: The event is triggered before a view that is set to be deleted is actually deleted. AfterDeleteView: The event is triggered after a view has been deleted.
BeforeReturnView	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • View	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 AfterUndeleteObject	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	BeforeUndeleteObject: The event handler is triggered before an object is undeleted. AfterUndeleteObject: The 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.

Event handler	Variables	Execution
AfterUndeleteObjectFinalize	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	This event is triggered after the object undelete operation is complete and you are able to work with the undeleted object.
BeforeModifyMFilesCredentials AfterModifyMFilesCredentials	• Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID • ActivityID	BeforeModifyMFilesCredentials: The event handler is triggered before the password of the M-Files login account is changed. AfterModifyMFilesCredentials: The event handler is triggered after the password of the M-Files login account is changed.
BeforeCheckinChangesFinalize	• ObjVer • DisplayID • Vault • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	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.

Event handler	Variables	Execution
BeforeAddUserGroupMember AfterAddUserGroupMember	- ObjVer - DisplayID - Vault - CurrentUserID - CurrentUserSessionInfo - VaultSharedVariables - SavepointVariables - TransactionCache - MFScriptCancel - GetExtensionObject - MasterTransactionID - CurrentTransactionID - ParentTransactionID - MemberID - GroupID	BeforeAddUserGroupMember: The event is triggered before the API call AddMemberToUserGroup. AfterAddUserGroupMember: The event is triggered after the API call AddMemberToUserGroup.
BeforeRemoveUserGroupMember AfterRemoveUserGroupMember	- ObjVer - DisplayID - Vault - CurrentUserID - CurrentUserSessionInfo - VaultSharedVariables - SavepointVariables - TransactionCache - MFScriptCancel - GetExtensionObject - MasterTransactionID - CurrentTransactionID - ParentTransactionID - MemberID - GroupID	BeforeRemoveUserGroupMember: The event is triggered before the API call RemoveMemberFromUserGroup. AfterRemoveUserGroupMember: The event is triggered after the API call RemoveMemberFromUserGroup.

Server-level event handlers

This section lists event handlers that are triggered by server-level operations. These operations also cause a corresponding event to be executed in all online vaults of the server.

Note: An exception in a server-level event handler prevents the triggering operation from being executed, but any vault-level event handler exceptions do not affect server-level operations.

Event handler	Variables	Execution
BeforeRunScheduledJob AfterRunScheduledJob	• CurrentUserID • CurrentUserSessionInfo • GetExtensionObject • MFScriptCancel • ScheduledJob • ScheduledJobOutputInfo	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 AfterCreateLoginAccount	• LoginAccount • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	BeforeCreateLoginAccount: The event is triggered for all online vaults before a login account is created on the server. AfterCreateLoginAccount: The event is triggered for all online vaults after a login account is created on the server.
BeforeModifyLoginAccount AfterModifyLoginAccount	• LoginAccount • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	BeforeModifyLoginAccount: The event is triggered for all online vaults before a login account is modified on the server. AfterModifyLoginAccount: The event is triggered for all online vaults after a login account is modified on the server.

Event handler	Variables	Execution
BeforeRemoveLoginAccount AfterRemoveLoginAccount	• LoginAccount • CurrentUserID • CurrentUserSessionInfo • VaultSharedVariables • SavepointVariables • TransactionCache • MFScriptCancel • GetExtensionObject • MasterTransactionID • CurrentTransactionID • ParentTransactionID	BeforeRemoveLoginAccount: The event is triggered for all online vaults before a login account is removed from the server. AfterRemoveLoginAccount: The event is triggered for all online vaults after a login account is removed from the server.
BeforeModifyMFilesCredentials AfterModifyMFilesCredentials	• CurrentUserID • CurrentUserSessionInfo • GetExtensionObject	BeforeModifyMFilesCredentials: The event handler is triggered for all online vaults before the password of an M-Files login account is changed. AfterModifyMFilesCredentials: The event handler is triggered for all online vaults after the password of an M-Files login account is changed.

Available VBScript Variables

VBScript code is edited in the **Edit VBScript code** window available in the following dialogs:

- Property Definition Automatic Values
- Automatically Validating Property Values
- Trigger
- Workflow State Actions
- Workflow State Conditions
- Event Handlers

The available variables are described in the table below.

Note: When you develop new extensions or edit existing ones, we recommend that you replace VBScript content with Vault Application Framework (VAF) compatible code for future compatibility. For more information on the benefits of VAF development over VBScript, refer to The Vault Application Framework in M-Files Developer Portal.

Note: The M-Files API documentation is available online: M-Files API.

Variable	Data type	Mode	Use
ActivityID	MFilesAPI.TypedValue	In	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	Boolean	Out	Can be used to allow or deny automatic state transition when running the automatic state transition script.
CurrentTransactionID	MFilesAPI.TypedValue	In	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	MFilesAPI.Number	In	Contains the ID of the user who performed the action that triggered the script.
CurrentUserSessionInfo	MFilesAPI.SessionInfo	In	Contains information about the login session of the user who caused the operation.
DisplayID	MFilesAPI.TypedValue	In	Contains the object's unique ID. This ID is shown on the object's metadata card 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	MFilesAPI.Number	In	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	MFilesAPI.FileVer	In	Contains the complete unique ID of the target file, consisting of the file ID and file version.

Variable	Data type	Mode	Use
GetExtensionObject	(method)	N/A	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.
GroupID	MFilesAPI.Number	In	The ID of the target user group.
Input	MFilesAPI.TypedValue	In	A client-defined parameter for the `VaultExtensionMethod` event handler.
IsCancellable	MFilesAPI.BooleanValue	In	Normally, scripts can cancel a server operation and revert the associated transaction by raising an error in the script. The `IsCancellable` variable specifies whether the script is allowed do this. If the value of the variable is `false`, M-Files Server will ignore any errors raised in the script. If the script raises an error while the value of the variable is `false`, however, an error is written to the Windows event log and all the changes made through the script are reverted. The server operation then proceeds to completion.

Variable	Data type	Mode	Use
LastUsed	MFilesAPI.TypedValue	In	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	MFilesAPI.Number	In	Contains the logged out user ID after logout.
LoginAccount	MFilesAPI.LoginAccount	In	Contains the user account data in the login.
MasterTransactionID	MFilesAPI.TypedValue	In	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.
MemberID	MFilesAPI.Number	In	The ID of the member who is added to or removed from a user group. The value is negative if the member is a user group.
MFScriptCancel	MFilesAPI.Number	In	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	MFilesAPI.Number	Out	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, 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	MFilesAPI.ObjectAccessControlList	In	Contains the current permissions of the viewed object.

Variable	Data type	Mode	Use
ObjID	MFilesAPI.ObjID	In	The ID of the object being processed.
ObjVer	MFilesAPI.ObjVer	In	Contains the complete unique ID of the target version, consisting of the object type ID, object internal ID, and object version.
Output	MFilesAPI.TypedValue	Out	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 data type 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	MFilesAPI.TypedValue	In	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	MFilesAPI.PropertyDef	In	Contains the information about the property value being calculated, such as the property value definition ID, name, and data type.
PropertyValue	MFilesAPI.PropertyValue	In	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.

Variable	Data type	Mode	Use
PropertyValues	MFilesAPI.PropertyValues	In	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. **Note:** Some property definitions are not shown when using the `PropertyValues` variable in scripts (see Property definitions not shown for scripts).
RestoredVersions	MFilesAPI.IDs	In	Contains object versions of the exported object that were imported from the content package.
SavepointVariables	MFilesAPI.NamedValues	In/ Out	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	MFilesAPI.ScheduledJob	In	Contains a description of the scheduled job which is being performed.
ScheduledJobOutputInfo	MFilesAPI.ScheduledJobOutputInfo	In	Contains information of the scheduled job result after the job has been performed.
StateID	MFilesAPI.Number	In	Contains the workflow state identifier which can be used to recognize the process state in scripts related to the workflows.
StateTransitionID	MFilesAPI.Number	In	The ID of the state transition.
TransactionCache	MFilesAPI.NamedValues	In/ Out	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	MFilesAPI.UserAccount	In	Vault user information.
UserGroupAdmin	MFilesAPI.UserGroupAdmin	In	Vault user group information.
ValueListItem	MFilesAPI.ValueListItem	In	Contains the value list value which is being processed in the event handler.

Variable	Data type	Mode	Use
Vault	MFilesAPI.Vault	In	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. 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	MFilesAPI.NamedValues	In/ Out	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" )`

View	MFilesAPI.View	In	Contains the view which is being processed in the event handler.

Property definitions not shown for scripts

The property definitions listed in the following table are not shown by using the `PropertyValues` variable in scripts:

ID	Name
24	Status changed
22	Single file
27	Deleted

ID	Name
28	Deleted by
33	Comment
29	Version label
30	Size on server (this version)
31	Size on server (all versions)
32	Marked for archiving
46	Collection members (documents)
47	Collection members (document collections)
101	Class groups
41	Assignment description
42	Deadline
43	Monitored by
44	Assigned to
45	Marked as complete by
97	Marked as rejected by
79	Workflow Assignment
81	Accessed by me
82	Favorite view
89	Object changed
90	Permissions changed
91	Version label changed
92	Version comment changed
93	Deletion status changed
96	Conflict resolved
105	Object changed for export
106	Object version changed for export

For example, the following piece of script results in a "not found" error:

```
Dim DeadlineValue
DeadlineValue = PropertyValues.SearchForProperty(42).TypedValue.DisplayValue
```

Tip: You can use the GetProperties method to get all the properties of a specific object.

Execution Order of Scripts

User-specified scripts in M-Files are executed in a specific order and the point in which they are executed depends on the event for which the script is written. See the lists below for the order in which events are by default executed when a user does a certain action in a vault. Note that the exact order and number of events that are triggered after a specific user action depend on the vault structure and the types of scripts used in the vault.

Execution order examples

The user creates an object and immediately checks it in:

1. Property value validation
2. Calculating automatic property values
3. The BeforeCreateNewObjectFinalize event
4. Workflow state preconditions
5. Workflow state actions
6. The BeforeCheckInChangesFinalize event
7. The AfterCreateNewObjectFinalize event
8. The AfterCheckInChangesFinalize event

The user creates an object, edits its property values, and checks in the object:

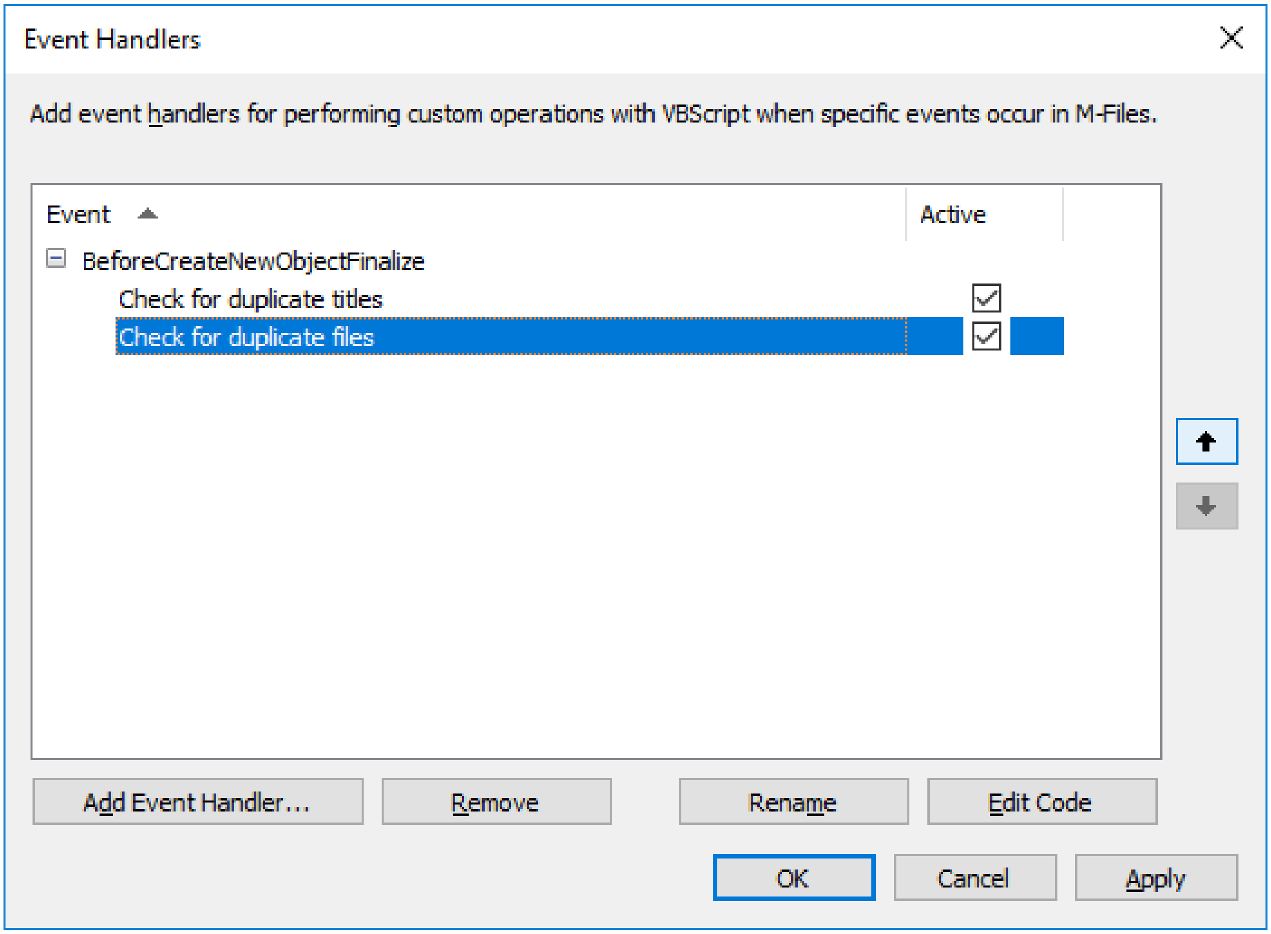
1. Property value validation
2. Calculating automatic property values
3. The BeforeCreateNewObjectFinalize event
4. The AfterCreateNewObjectFinalize event
5. The BeforeSetProperties event
6. Property value validation
7. Calculating automatic property values
8. The AfterSetProperties event
9. The BeforeFileUpload event
10. The AfterFileUpload event
11. The BeforeSetProperties event
12. Calculating automatic property values
13. The AfterSetProperties event
14. The BeforeCheckInChanges event
15. Workflow state preconditions
16. Workflow state actions
17. The BeforeCheckinChangesFinalize event
18. The AfterCheckInChanges event
19. The AfterCheckInChangesFinalize event

The user edits the property values and changes the workflow state of an object:

1. The BeforeCheckOut event
2. The AfterCheckOut event
3. The BeforeSetProperties event
4. Property value validation
5. Calculating automatic property values
6. The AfterSetProperties event
7. The BeforeCheckInChanges event
8. Previous workflow state postconditions
9. New workflow state preconditions
10. Workflow state actions
11. The BeforeCheckinChangesFinalize event

12. The AfterCheckInChanges event
13. The AfterCheckInChangesFinalize event
14. The BeforeReturnView event

If you have more than one event handler of the same type, you can change their execution order by selecting the event handler in the **Event Handlers** dialog and clicking either the up or down arrow button along the right side of the dialog:



Add event handlers for performing custom operations with VBScript when specific events occur in M-Files.

Event	Active
⊟ BeforeCreateNewObjectFinalize	
Check for duplicate titles	☑
Check for duplicate files	☑

Execution order for external object types

Operations in an external database are done as the second last action. For example, here is the execution order for when the user creates an external database object and checks it in:

1. Property value validation
2. Calculating automatic property values
3. The BeforeCreateNewObjectFinalize event
4. Workflow state preconditions
5. Workflow state actions
6. The BeforeCheckInChangesFinalize event
7. The AfterCreateNewObjectFinalize event
8. `INSERT` action to the external database
9. The AfterCheckInChangesFinalize event

3.2.12. Intelligent Metadata Layer

Intelligent Metadata Layer, abbreviated as IML, is a repository-neutral approach to intelligent information management that unifies information across different sources based on context, not on the system or folder in which the information is stored.

IML allows an M-Files user to connect to multiple different external repositories in addition to the traditional M-Files document vaults. By means of special vault applications known as connectors, the user can browse and edit content residing in external sources within the M-Files user interface.

IML provides automatic classification and metadata to your documents with the aid of so-called intelligence services that add a layer of artificial intelligence to M-Files. Intelligence services are vault applications that classify documents for you by determining the class of the document and suggesting metadata values by analyzing file content semantically and visually.

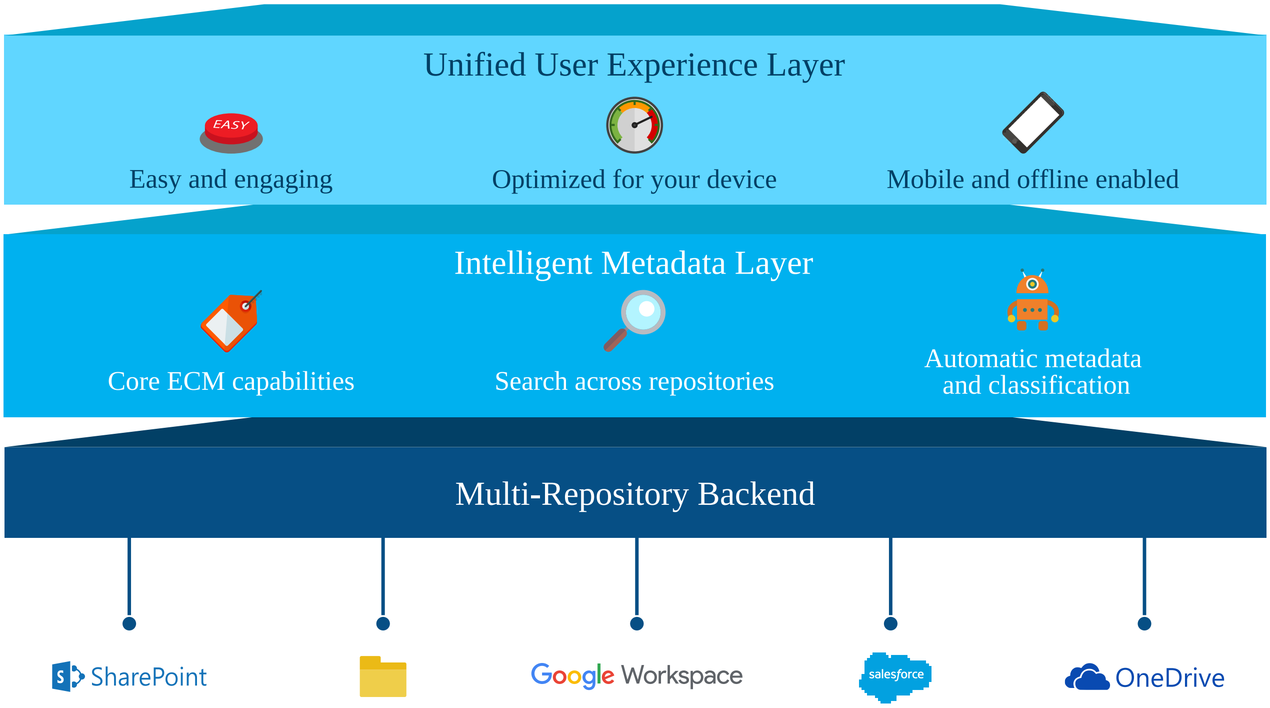
For a more thorough overview of IML, see the document Intelligent Metadata Layer.

Note: To use IML features, you need an appropriate Intelligent Metadata Layer license and Microsoft .NET Framework (not .NET) 4.7.2, 4.8.x, or later installed on the M-Files server computer.

Note: Some M-Files applications that were released before M-Files 2018 may not be compatible with external repository content. Before taking IML into use, ensure that all your business-critical M-Files applications are compatible with content stored in external repositories.

Architecture of IML

The architecture of IML can be divided into three separate layers: the unified user experience layer on the top, the intelligent metadata layer in the middle, and the multi-repository backend at the bottom.


Unified User Experience Layer
EASY
Easy and engaging
Optimized for your device
Mobile and offline enabled
Intelligent Metadata Layer
Core ECM capabilities
Search across repositories
Automatic metadata and classification
Multi-Repository Backend
SharePoint
Google Workspace
salesforce
OneDrive

The top layer, the **unified user experience layer**, serves to offer a unified user experience regardless of the repository in use. It lets information be viewed and edited with the familiar M-Files Desktop, M-Files Web and M-Files Mobile user interfaces, no matter where the information resides.

The middle layer, also known as **Intelligent Metadata Layer**, is the central component in the IML architecture. It consists of all the essential enterprise content management capabilities, such as a versatile search interface, workflows, version history, checking out documents for editing, and a multi-repository search. The M-Files approach of classifying documents with metadata and categorizing content into metadata-based views allows documents to be found on the basis of what they are about instead of where they reside. The multi-repository search is the M-Files version of an enterprise search, allowing documents to be searched for across repositories.

The middle layer also adds artificial intelligence into the M-Files system. The so-called intelligence services offer means for automatic metadata suggestions and document classification by performing text and image analytics on content that is added to M-Files, and by applying machine learning on vault user behavior patterns. Intelligence services are vault applications that, when installed, can shoulder the burden of specifying metadata and classifying documents. Additionally, the IML application programming interface allows intelligence services to be developed by third parties so that they can be tailor-made to suit specific needs and environments of diverse organizations and businesses.

For more information on intelligence services, see Intelligence Services.

The bottom layer, the **multi-repository backend**, acts as an interface between M-Files and external repositories. By means of vault applications known as connectors, M-Files users are able to view and modify content in external repositories by using the M-Files user interface. Connectors establish connections between M-Files and external repositories and allow the user to view and edit content from various different external sources as though the user was operating within a single document vault.

For more information on connectors, see Connectors.

In this chapter

Intelligence Services

Intelligence services are vault applications that are designed to analyze and classify documents and offer metadata suggestions based on file contents, existing metadata, and even user behavior. Intelligence services make use of technologies such as text analytics and machine learning to define and maintain document metadata for the user.

Refer to M-Files Catalog to see the available intelligence services.

Intelligence services can operate in many ways and come into play in different situations. They can be tailor-made for M-Files, they can take advantage of a third-party component or an API, or connect to a third-party service to perform content analysis for M-Files.

Tip: Developers can build and customize their own intelligence services. For more information, refer to Visual Studio Template for Building Intelligence Services.

Intelligence services are at work in the background, for example, when the user drags and drops a new document to M-Files or modifies a specific property value on the metadata card. In such instances, intelligence services analyze the contents of new documents and metadata modifications and offer metadata suggestions based on the analyses that they conduct.

If you for instance add a contract to M-Files, the intelligence service may automatically suggest contract to be used as the document class and propose values for customer and contact details, among other metadata fields, by deducing the information from the file contents. Users may then add suggested values as they see fit. This type of automation can significantly speed up the process of adding metadata for M-Files objects.

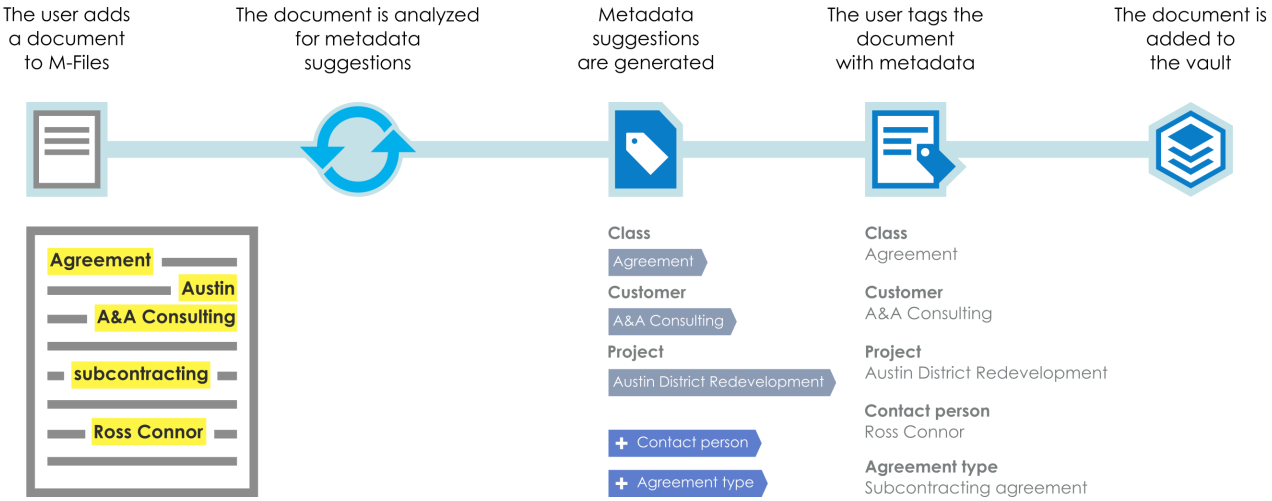

The user adds a document to M-Files
The document is analyzed for metadata suggestions
Metadata suggestions are generated
The user tags the document with metadata
The document is added to the vault
Agreement
Austin
A&A Consulting
subcontracting
Ross Connor
Class
Agreement
Customer
A&A Consulting
Project
Austin District Redevelopment
+ Contact person
+ Agreement type
Class
Agreement
Customer
A&A Consulting
Project
Austin District Redevelopment
Contact person
Ross Connor
Agreement type
Subcontracting agreement

Figure 66: Intelligence services aid you in tagging documents with metadata.

As another example, when an image is added to M-Files, an intelligence service can conduct a visual analysis on the new image before the user fills in the metadata. The analysis identifies individual objects, concepts and human faces as well as facial features in the image and generates a textual description and subject labels of the image contents. The description and labels are in turn offered as metadata suggestions for the description and keywords fields on the metadata card. The user can then add any suggestions that she deems appropriate as metadata values and optionally edit the added values to further specify the metadata.

Note: Metadata suggestions are not shown for users with a read-only license.

In this chapter

- Adding an Intelligence Service
- Configuring an Intelligence Service
- M-Files Aino Metadata

Adding an Intelligence Service

Complete the following steps to add an intelligence service to a vault on the M-Files Server computer:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Right-click a vault.
5. Click **Applications**.

   ✓ The **Applications** window is opened.
6. Click the **Install** button.
7. Locate the application package stored on your computer and click **Open**.

You are prompted to restart the document vault.

8. Click **Yes** at the prompt.

9. If you have any open sessions in the selected vault, you are prompted to close any open sessions. Click **Yes**.

The selected intelligence service is installed and should be listed in the **Applications** window. After the intelligence service has been successfully installed, it should be configured. For instructions on configuring an intelligence service, see Configuring an Intelligence Service.

Configuring an Intelligence Service

Intelligence services are configured in the M-Files Admin configurations editor. For instructions on using the editor, see Using the Configurations Editor.

Complete the following steps to configure an intelligence service:

1. Open M-Files Admin.

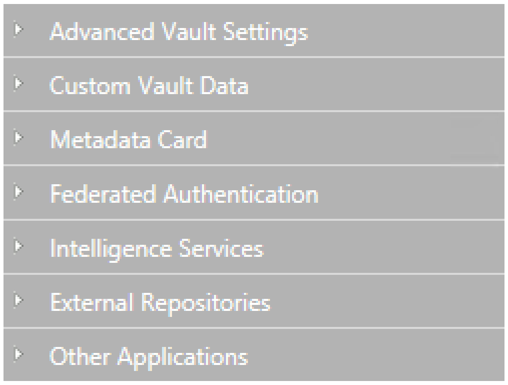
2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Document Vaults**.

4. Expand a vault.

5. Select **Configurations**.

6. In the gray navigation area, expand **Intelligence Services** and then select the intelligence service that you want to configure.



7. Open the **Configuration** tab, and then expand the **General Settings** section and edit the configuration as applicable:

Setting	Description
Enabled	Specifies whether the intelligence service is enabled or not.
Suggestions	These settings are used for mapping metadata suggestions with M-Files properties.
Maximum Processing Time in Seconds	The maximum amount of time in seconds that the intelligence service waits for the suggestions to be processed and generated before canceling the operation.

8. Expand the **Service-Specific Settings** section and edit the configuration as applicable.

   The settings under **Service-Specific Settings** vary across intelligence services. See service-specific instructions for more information.

9. Click **Save** to save your configuration.

10. Restart the vault.

Your configurations should now be effective and the intelligence service should be ready for use.

M-Files Aino Metadata

M-Files Aino Metadata is a vault application and an intelligence service that uses Large Language Models (LLMs). The service processes document contents to create and give metadata suggestions to users in the new M-Files Desktop and in M-Files Web.

Note: M-Files Aino Metadata is automatically installed and updated but its use requires a separate license.

Administrators can configure which properties are suggested and add detailed descriptions that guide the LLM to find relevant values from document content. Administrators can also further fine-tune the property suggestions process so that certain properties are only suggested for certain types of documents. If the document class is not yet known, M-Files Smart Classifier will automatically help with that if it is enabled in the vault.

When the LLM uses value list items to make property suggestions, it tries to convert plain text suggestions into resolved M-Files value list items. If the LLM cannot find an exact match, it will still suggest new possible value list items.

Admin aid

Refer to these documents for more technical information:

- M-Files Aino - Getting started
- M-Files Aino - Administrator Guide
- M-Files Aino - FAQ
- M-Files Aino - Security and Data Protection Features
- M-Files Smart Classifier - FAQ
- Installing and Configuring M-Files Smart Classifier

Connectors

Connectors establish a connection between M-Files and external repositories. They bring external data into the M-Files user interface and allow it to be viewed and modified in the same fashion as information is commonly processed in M-Files. In other words, files in an external repository, such as a network folder, are displayed in M-Files like any other M-Files objects and they can be edited and enriched with metadata in the same manner as any other information residing in an M-Files document vault.

Refer to M-Files Catalog to see the available connectors.

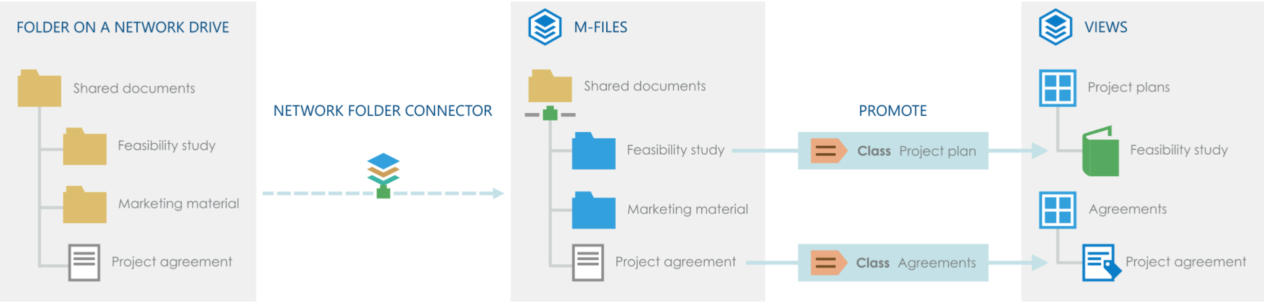


Figure 67: Connectors let you integrate M-Files with external repositories so that you can view and modify external repository content in M-Files. By adding metadata, you can promote files and folders in external repositories to M-Files objects so that they can be, for example, organized into metadata-driven views.

Objects in external repositories are by default unmanaged, but they can be promoted to managed objects. For more information, see Unmanaged and Managed Objects and Promoting Unmanaged Objects.

In this chapter

Adding a Connector

Complete the following steps to add a connector to a vault on the M-Files Server computer:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Right-click a vault.
5. Click **Applications**.

   ☑ The **Applications** window is opened.
6. Click the **Install** button.
7. Locate the application package stored on your computer and click **Open**.

   ☑ You are prompted to restart the document vault.
8. Click **Yes** at the prompt.
9. If you have any open sessions in the selected vault, you are prompted to close any open sessions. Click **Yes**.

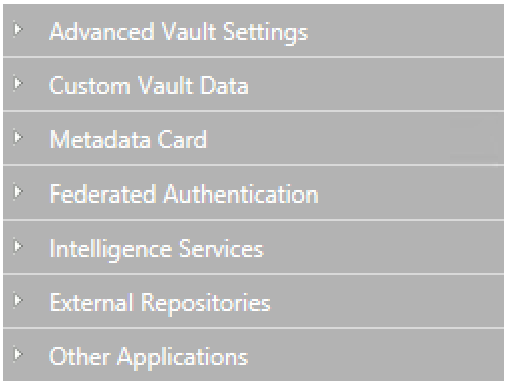
The selected connector is installed and should be listed in the **Applications** window. After the connector has been successfully installed, it should be configured. For instructions on configuring a connector, see Configuring a Connector.

Configuring a Connector

Connectors are configured in the M-Files Admin configurations editor. For instructions on using the editor, see Using the Configurations Editor.

Complete the following steps to configure a connector:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Configurations**.
6. In the gray navigation area, expand **External Repositories** and then select the connector that you want to configure.



7. In the **Dashboard** tab, either:

   a. Click **Add Connection** to add a new connection.

      Note: You cannot add more connections than specified in the external repositories configuration. To increase the limit, see Increasing the Number of Allowed External Repository Connections.

   or

   b. Select an existing connection and click **Configure**.

8. Expand **General Settings** and edit the configuration as applicable:

Setting	Description
Enabled	Specifies whether the connection is enabled or not.
Display Name	The display name for the connection, shown in the listing area under **External Views**.

Setting	**Description**
Authentication	Specifies the authentication type used for connecting to the external repository. The available options are: • `Personal` • `Common` • `Anonymous` See External Repository Authentication for further information.
Permissions	These options allow you to use a default M-Files NACL for the objects in the external repository.
Automatic Association	These options allow you to automatically associate M-Files users with external users and user groups. This section consists of the following options: • `Association Methods`: Allows you to specify association methods if common authentication is used. Supported values: • `username`: Forms an association if an external username matches an M-Files username. • `User Association during Login`: Lets the M-Files user to be associated with the external repository user when the user logs in to the repository with M-Files. This setting can be used if personal authentication is enabled. • `User Association with User Groups during Login`: Allows external repository group memberships to be synchronized in M-Files when the user logs in to the repository using personal authentication. • `Replicate All User Groups`: If enabled, all available user groups and the group hierarchy of the external repository is replicated to M-Files.

Setting	Description
Mapping	These options are used for mapping objects in the external repository with M-Files objects, and external metadata with M-Files properties. You can enter the value `*` in the **External Type** field of an object type mapping to use the same object type for all the external objects available through this connection. **Note:** External files should be mapped to an M-Files object type that has the option **Objects of this type can have files** enabled. For more information on object type properties, see Creating a New Object Type. You can use the file extension based filtering settings under object type mappings to specify which external repository objects should be listed in M-Files. The file extensions should be entered without a preceding period (for instance: `bmp`), and only a single one should be specified per value field. Excluded external objects are not indexed, either.
Search Indexing	These options affect the way content in the external repository is indexed for searching.

9. Expand the **Connector-Specific Settings** section and edit the configuration as applicable.

   The settings under **Connector-Specific Settings** vary across connectors. See connector-specific instructions for details.

10. Optional: In the gray navigation area, right-click the connection and select **Authenticate Common User** from the context menu to add the common user credentials for accessing the repository.

11. Optional: In the gray navigation area, right-click the connection and select **Authenticate Indexer User** from the context menu to add the credentials that are used for indexing the contents of the repository.

12. Optional: In the gray navigation area, right-click the connection and select **Authenticate Permissions Retriever** from the context menu to add the credentials for fetching the external repository object permissions.

    The option is displayed in the connector context menu only if the connector requires a permissions retriever to be assigned. Otherwise, only the options for authenticating a common user and an indexer user are shown.

13. Click **Save** to save your configuration.

14. Restart the vault.

Your configuration should now be effective. You can inspect the **Dashboard** tab to see the status of the external repository connection.

After you have enabled an external repository connection, the connector must usually do many operations to get the content in the external repository fully accessible from M-Files. If there is a large amount of content that must be indexed, this can take a long time.

In this chapter

External Repository Authentication

Administrators must specify the type of authentication to be used for each external repository connection in M-Files Admin. The **Authentication** setting specifies the credentials that are used for accessing the external repository. Administrators can specify that *anonymous*, *common*, or *personal* authentication is used.

See also External Repository Users and External Repository User Groups for instructions on associating external repository users and user groups with M-Files users and user groups.

Anonymous Authentication

You must set the **Authentication** setting to **Anonymous** for repositories that do not need to authenticate users at all.

Common Authentication

The administrator specifies credentials that are stored in the M-Files vault database in encrypted format. These credentials are used for every M-Files user when they access the external repository via M-Files.

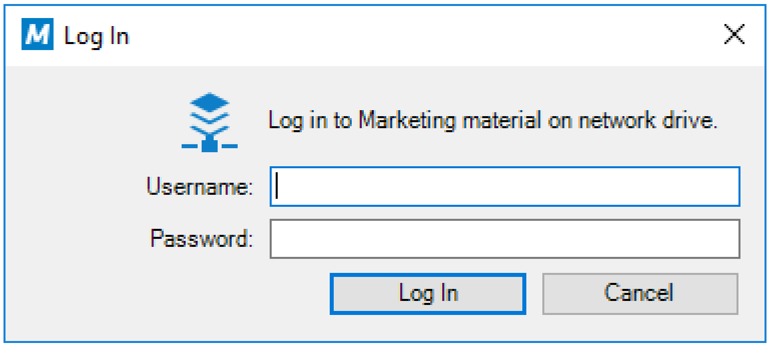
Common is the recommended authentication type in two scenarios:

- The external repository contains data that can be accessed by every M-Files vault user or a certain subset of vault users. Using this authentication type saves users from having to log in to the repository manually.
- The external repository must be made accessible for users that do not have credentials to the external repository. This might be the case, for example, when an organization wants to grant external subcontractors access to a network folder with M-Files that they would otherwise not have access to.

  - Using common authentication for this purpose can also require that the external users are granted access to the content through a named access control list, as the common authentication only allows the users to access the repository, not the actual content. Alternatively, the vault users that should be able to access the external content can be associated with the common external user.

Personal Authentication

When the type of authentication is set to **Personal**, the user is prompted to provide their credentials in the M-Files client when they access the external repository:



Logging out from Or Logging in to an External Repository

To log out from or to log back in to an external repository that uses user-specific authentication:

1. Click the initials in the top-right corner of the user interface.
2. Select **External Repositories**.
3. Select the external repository connection and then one of these options:

   a. Click **Log In** to log in to the repository to which you are no longer connected.

      or

   b. Click **Log Out** to log out of the repository to which you are currently connected.
4. Click **Close**.

Increasing the Number of Allowed External Repository Connections

If you use M-Files Cloud, request our customer support (M-Files Support Portal) or your M-Files reseller to increase the maximum number of connections if necessary.

To change the **Maximum Number of Connections** setting, you need to have the system administrator permissions.

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.
2. Expand **External Repositories**.
3. In **Maximum Number of Connections**, speficy the number of allowed external repository connections.
4. Click **Save**.

Unmanaged and Managed Objects

External files that do not have M-Files metadata are unmanaged objects in M-Files terminology. You can view and edit them in M-Files, but the changes are saved only to the external repository, and M-Files Server does not keep a version history for these objects.

When you add metadata properties for an unmanaged object, it is promoted to a managed object in M-Files. Managed objects can be edited in the external system or in M-Files, but M-Files keeps a version history only of the changes made in M-Files. Because the external repository does not necessarily support version history, M-Files Server saves all object versions in M-Files and only the latest version in the external system.

Note: Unmanaged objects that are checked out cannot be promoted. Before you promote an object, make sure that the object is not checked out to you or someone else. For more information, see these instructions.

Reasons to promote objects to managed objects

You can use these essential M-Files features with managed objects:

- Version history
- Object relationships
- Document collections
- Workflows
- Assignment features
- Check out and check in
- Co-authoring
- Converting single-file document to multi-file documents
- Object comments
- Scanning and text recognition
- Annotations
- Sharing objects with the **Copy Link** option
- Offline availability

Unmanaged objects are also not part of replication packages.

Creating objects with metadata

You can use the features given here to create M-Files objects with metadata. Make sure that you use only one of them. If you use more than one feature, the same content is migrated to the vault more than once.

- Promote unmanaged objects
- Create a connection to an external source
- Save folders to M-Files
- M-Files Smart Migration
- M-Files Importer

Promoting Unmanaged Objects

To convert an unmanaged object to a managed object:

1. In M-Files Desktop or M-Files Web, find and select an unmanaged object.
2. Make sure that the object is not checked out for editing.

    a. If the object is checked out to you, you can right-click the object and select **Check In** or **Undo Checkout** from the context menu.

    or

    b. If the object is checked out to someone else, see the metadata card of the object to identify the user who has checked out the object, and then ask them to check it in.
3. Use the **Class** drop-down menu to change the class of the object.
4. When you have changed the class, you can enrich the object with metadata as you see fit.

The class that you select sets the default metadata properties of the object.

5. Click **Save** to save your changes.

The selected object in the external repository has now been promoted into a managed object.

Connection to On-Premises Data with M-Files Ground Link

With M-Files Ground Link, you can get access to on-premises data or business applications. M-Files Ground Link lets you establish a safe connection to external repositories in private networks. Thus, a direct network path or content migration is not necessary.

With the Ground Link feature, you can get access to on-premises repositories from a cloud vault in the same way as in on-premises environment. You can also use Ground Link to connect an on-premises vault to external data or business applications. To do one of these two, connect a Ground Link proxy on M-Files Server to the vault.

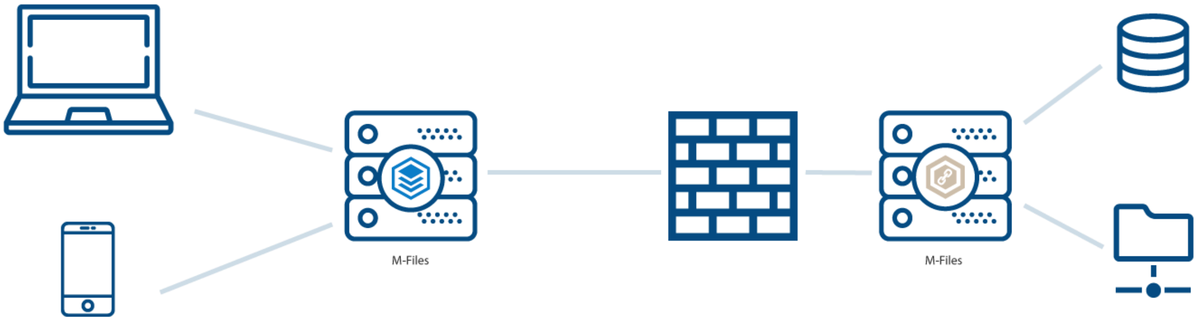


Figure 68: A Ground Link proxy lets a vault connect to private repositories, such as network folders, without a direct network path.

In this chapter

Setting up M-Files Ground Link

Before you set up the Ground Link feature, make sure that these prerequisites are completed:

- gRPC connections are permitted on the on-premises server on which the Ground Link proxy will be configured. This server is later in this instruction called Ground Link proxy server.

If you connect the Ground Link proxy to an on-premises vault, also make sure that these prerequisites are completed:

- gRPC connections are permitted on the M-Files server.
- The M-Files server has a valid TLS certificate for the encryption of the gRPC connections.

For more information, refer to the knowledge base document Setting Up M-Files to Use gRPC.

To set up the Ground Link feature, you first install external repository connectors to a Ground Link proxy. Then, you set up repository connections in the vault. After that, you can see and edit the on-premises data directly from the vault.

Enabling Ground Link Connection

Complete these steps to enable the channel connection for Ground Link in a vault:

1. Open M-Files Admin and go to a vault.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
2. Click **Configurations**.
3. In the navigation area, expand **Advanced Vault Settings** > **Configuration**.
4. Click **Ground Link**.
5. On the **Configuration** tab, set **Enabled** to **Yes**.
6. Click **Save**.
7. Restart the vault for the settings to take effect.

   Note: Taking a vault offline should always be done in a controlled manner and the vault users should be notified beforehand.

8. In the gray navigation area, expand **External Repositories** > **Ground Link** and select **Configuration**.
9. On the **Configuration** tab, specify these settings:

Setting name		**Description**	**Example value**
Enabled		This setting specifies whether Ground Link is enabled or not.	**Yes**
Remoting Service	**Shared Secrets**	A shared secret lets a Ground Link proxy authenticate the vault. Make sure that the shared secret is complex and long enough. You can specify one or more shared secrets. You must enter the shared secret when you configure the Ground Link proxy.	

Setting name		**Description**	**Example value**
	Timeouts	The timeout values specify in seconds how long remote calls wait for a response. Use the default values. **Note:** These settings are not available for M-Files Cloud vaults.	
Keep Alive Interval		This setting specifies in seconds how frequently the vault makes sure that the Ground Link services are connected.	`60` (default value)

10. Optional: Specify the other settings.

For more information, select a setting and see the **Info** tab.

11. Click **Save**.

Now that the vault uses Ground Link, you can configure the Ground Link proxy.
Configuring a Ground Link Proxy

Before you start, make sure that these prerequisites are completed:

- Your Ground Link proxy server has sufficient hardware resources. See the recommended hardware setup.
- You have M-Files Server and M-Files Admin installed on the Ground Link proxy server. However, a separate license for M-Files Server is not necessary.
- You are logged in to M-Files Server with a login account that has the System administrator server role. To create a login account, see Creating a Login Account.
- Your Ground Link proxy server can connect to the on-premises resources (for example, a network folder or an external database) that you want to make available in the vault.

To configure a Ground Link proxy on the Ground Link proxy server:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Click **Ground Link Proxies**.
4. On the right-side pane, click **New Ground Link Proxy**.

   ✓ The **New Ground Link Proxy** dialog is opened.

5. Enter a name for the Ground Link proxy.
6. Select the database engine for storing Ground Link proxy data.

   a. To use Firebird, select **Use Firebird**.

   or

b. To use Microsoft SQL Server, select **Use Microsoft SQL Server**.

For more information, see Database engine and data storage.

7. Click **Define**.

The settings dialog for the search engine is opened.

8. Complete one of these options:

Option	Description
On the Ground Link Proxy - Firebird dialog	**a.** Click the **...** button and select the file location for the Ground Link proxy data. **b.** Click **OK** to close the dialog.
On the Ground Link Proxy - Microsoft SQL Server dialog	Do the steps from 6 to 10 in Migrating the Ground Link Proxy Database to Microsoft SQL Server.

9. Click **OK** to close the **New Ground Link Proxy** dialog.

10. Install those external repository connectors that your vault will use to the newly created Ground Link proxy.

Note: If a valid vault application license is necessary for a connector, the license will be for the vault and for the server that contains the vault.

For more information, see Installing and Managing Vault Applications.

To get access to on-premises network folders from M-Files Cloud, install M-Files Network Folder Connector.

The Ground Link proxy is now ready for configuration.

11. In the left-side tree view, under **Ground Link Proxies**, select the newly created Ground Link proxy.

12. On the **Configuration** tab, specify these settings:

Setting name		Description	Example value
Enabled		This setting specifies whether Ground Link is enabled or not.	**Yes**
Password		Enter a password that you will use when you apply a configuration for a Ground Link service in the vault.	
Channel	**Network Address**	Enter the network location of the server to connect to. If you connect the Ground Link proxy to an M-Files Cloud, enter the DNS name of the vault.	`aa-consulting.cloudvault.m-files.com`

Setting name		**Description**	**Example value**
	Port number	Enter the port that the server listens. If you connect the Ground Link proxy to an M-Files Cloud vault, the correct port number is `443`. If you use the gRPC protocol, use the same port number that your M-Files client uses to connect to the server. For more information, see Adding a Vault Connection. Make sure that the necessary ports are open in the firewall.	`443` or `7766`
	Secure	This setting specifies whether a secure (SSL encrypted) channel connection is used. In production environments, insecure connections are not recommended.	**Yes**
	Vault GUID	Enter the GUID of your vault. To see the vault GUID, right-click the vault and select **Properties**. The GUID is shown in the **Unique ID** field in the **Document Vault Properties** dialog.	`{990827D8-8AF2-4A4EB121-4C1A8AD8ECD0}`
	Shared Secret	Copy the shared secret from the vault configuration. The channel connection cannot be established if the shared secret does not match one of the shared secrets specified for Ground Link.	
	Reconnect Interval	This value specifies in seconds how frequently the Ground Link proxy tries to connect when the vault is disconnected.	`60` (default value)
	Keep Alive Interval	This value specifies in seconds how frequently the Ground Link proxy makes sure that the connection to the vault operates correctly.	`60` (default value)
	Timeouts	The timeout values specify in seconds how long remote calls wait for a response. Use the default values.	

Setting name		Description	Example value
Multi-Server Compatibility	**Check Compatibility**	This setting specifies whether the multi-server mode compatibility is checked. If you connect the Ground Link proxy to an M-Files Cloud, this setting must be set to **Yes**.	**Yes** (default value)

13. Optional: Specify the other settings.

ⓘ For more information, select a setting and see the **Info** tab.

14. Click **Save**.

The connection between the vault and the Ground Link proxy is established. Next, you can set up the Ground Link services in the vault.

You can see the status of the vault connection on the **Dashboard** tab.

Configuring External Object Types over Ground Link

This example tells you how to configure M-Files OLE DB External Object Type Connector in a vault as a Ground Link service to update object types to and from an external database. You can also use the external object type (EOT) connector for value lists. For instructions on how to configure other available M-Files EOT connectors, refer to Installing and Configuring M-Files Connector for Salesforce and Installing and Configuring M-Files Connector for Microsoft Dynamics 365 in M-Files Support Portal.

On the Ground Link proxy server, make sure that the M-Files OLE DB External Object Type Connector application is enabled:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Ground Link Proxies**.
4. Right-click a Ground Link proxy and select **Applications**.

   ☑ The **Applications** dialog is opened.

5. In the list of applications, find **M-Files OLE DB External Object Type Connector** and make sure that its status is **Enabled**. By default, the application is disabled.

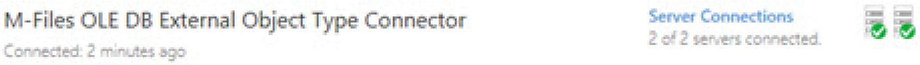
   ⓘ To enable the application:

   a) Select **M-Files OLE DB External Object Type Connector**.
   b) Click **Enable**.
   c) In the dialog that is opened, click **Yes** to restart the Ground Link proxy.

6. Click **Close** to close the **Applications** dialog.
7. On the Ground Link proxy dashboard, make sure that the vault and the EOT connector are connected:

- **Cloud Vault Connection** shows a green circle (●).
- In **Installed Connectors**, **M-Files OLE DB External Object Type Connector** shows that one or more servers are connected.

  For example:



M-Files OLE DB External Object Type Connector
Connected: 2 minutes ago

Server Connections
2 of 2 servers connected.

  Note: After the application is enabled, it can take a few minutes to create the server connection for the EOT connector. If necessary, click **Refresh** to update the view.

Next, create an object type, that uses the EOT connector, to the vault:

8. Open M-Files Admin and go to a vault for which you have enabled the Ground Link connection.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
9. Expand **Metadata Structure (Flat View)**.
10. Click **Object Types**.
11. In the task area, click **New Object Type**.

    The **Object Type Properties** dialog is opened.
12. Specify the information on the **General**, **Advanced**, and **Permissions** tabs. For instructions, see Creating a New Object Type.

Finally, configure the connection to the external database:

13. In the **Object Type Properties** dialog, go to the **Connection to External Database** tab and enable the option **Use a connection to an external database to import and modify objects that reside in the external database**.
14. Select **Application connection**.
15. In **Service**, select `M-Files OLE DB from Ground Link proxy` *`<name of the Ground Link proxy>`*.
16. Click **Configure**.
17. If M-Files asks whether you want to create the object type, select **Yes**.
18. In the **External Object Type Connector** dialog that is opened, configure the connection to the external database. For instructions, see Connections to External Databases for Object Types.
19. After you have saved the configuration, do these operations to make sure that the connection operates without erros:
    a) Click **Test Select** in the top-right corner of the dialog to test the SELECT statement. If the test is successful, M-Files shows you a summary of the property mappings. If the test fails, errors are shown instead. In this case, edit the configuration and try again.

b) Make sure that there are no errors on the **Local** and **Server** tabs in the lower-left corner of the dialog. If there are errors, use the given information to solve them.

20. Click **Close** to close the **External Object Type Connector** dialog.

21. In the **Object Type Properties** dialog, click **OK**.

The object type is now updated to and from the external database.

Configuring Connectors over Ground Link

This example tells you how to configure M-Files Network Folder Connector in a vault as a Ground Link service. For information on support for other connectors, contact our customer support in M-Files Support Portal or your M-Files reseller.

Before you begin, make sure that M-Files Network Folder Connector is installed to the Ground Link proxy that is connected to your vault.

To configure a connection to a Ground Link proxy:

1. Open M-Files Admin and go to a vault for which you have enabled the Ground Link connection.

   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.

2. Click **Configurations**.

3. In the navigation area, expand **External Repositories**.

4. Click **Ground Link**.

   On the **Dashboard** tab, you see the connected Ground Link proxies with the available Ground Link services. Make sure that the service that you want to configure, in this case **Network Folder**, is online.

5. In the gray navigation area, expand first the **Ground Link** node and then the Ground Link proxy whose service you want to use.

6. In the gray navigation area, select the Ground Link service, in this case **Network Folder**.

7. On the **Dashboard** tab, select **Add Connection**.

8. In the confirmation dialog that is opened, click **OK**.

9. On the **Dashboard** tab, click **Configure** to configure the new connection.

   For more information, refer to Installing and Configuring M-Files Network Folder Connector.

10. Click **Save**.

11. Click **Apply**.

   The **Enter Password** dialog is opened.

12. Enter the password that is defined in the Ground Link proxy configuration.

13. Optional: Authenticate background users. After you have given the credentials, save and apply the settings again.

    ℹ For more information, refer to Installing and Configuring M-Files Network Folder Connector.

14. Click **Save**.

15. Optional: Repeat the steps from 5 to 12 to add more connections.

Now you have access to the on-premises network folders from the vault. The objects in the network folders are shown in M-Files. You can edit them and give them metadata in the same way as objects that are stored in the vault.

Backing Up and Restoring a Ground Link Proxy

We recommend that you back up the Ground Link proxy always after you have made changes to the Ground Link proxy or to the connections over Ground Link. If a Ground Link proxy is destroyed or the data gets corrupted, you can restore the Ground Link proxy from a backup file. The backup file includes the Ground Link configuration and the connector configurations.

This section tells you how to back up and restore a Ground Link proxy.

For information on how to change the location of Ground Link proxies and Ground Link proxy services with the backup and restore operations, see Changing the Location of Ground Link Proxy Services.

Backing Up a Ground Link Proxy

To back up a Ground Link proxy:

1. Open M-Files Admin.

2. In the left-side tree view, expand a connection to M-Files server.

3. Expand **Ground Link Proxies**.

4. Right-click a Ground Link proxy.

5. Click **Operations** > **Back Up**.

    ☑ The **Back Up Ground Link Proxy** dialog is opened.

6. Click the **...** button to select the file location for the M-Files backup file (MFP).

7. Optional: Click **Set Account...** to run the task with another account than the Local System account. If the file location is on a network drive that the Local System account cannot get access to, you must set another account. On the **Set Account** dialog:

    a) Select **This account**.
    b) In **This account**, enter the name of the user account.
    c) In **Password** and **Confirm password**, enter the password of the user account.
    d) Click **OK** to close the **Set Account** dialog.

8. Optional: Select the **Overwrite existing files** check box if you want to overwrite the existing file in the file location.

9. Click **OK** to close the dialog and start the backup.

Restoring a Ground Link Proxy

To restore a Ground Link proxy from a backup file:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Right-click **Ground Link Proxies**.
4. Click **Restore Ground Link Proxy**.

   ✓ The **Restore Ground Link Proxy** dialog is opened.
5. In **Full backup**, specify the location of the backup file from which you want to restore the Ground Link proxy.
6. Select either:

   a. **Restore using original identity**: Select this option to to restore the Ground Link proxy with the existing ID. The existing Ground Link proxy services and the connections to them will be automatically enabled.

      or

   b. **Restore as a different Ground Link proxy (new identity)**: Select this option to restore the Ground Link proxy with a new ID. In **Name**, enter a name for the Ground Link proxy.

      To enable the connections to the Ground Link proxy services, you must remove the existing connections to the original Ground Link proxy services. For more instructions on managing the connections, refer to the connector instructions, such as Installing and Configuring M-Files Network Folder Connector.
7. In **Location for Ground Link proxy data on server**, specify the location for the Ground Link proxy data.
8. Optional: Select the **Overwrite existing files** check box if you want to overwrite the existing file in the file location.
9. Optional: If you do not want to temporarily disable the vault applications, unselect the **Disable vault applications** check box.

   ⓘ For data security reasons, we recommend to enable the vault applications separately after the Ground Link has been restored.
10. Click **OK**.

    ✓ The Ground Link proxy is restored from the backup file.
11. Optional: Enable the vault applications. For instructions, see Installing and Managing Vault Applications.

Migrating the Ground Link Proxy Database to Microsoft SQL Server

Before you begin, make sure that

- your Ground Link proxy uses the Firebird database engine.
- you have a Microsoft SQL Server connection.

- you have backed up the Ground Link proxy.

You can migrate your Ground Link proxy database from Firebird to Microsoft SQL Server with M-Files Admin.

To migrate the Ground Link proxy database to Microsoft SQL Server:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Ground Link Proxies**.
4. Right-click a Ground Link proxy.
5. Click **Operations** > **Migrate to Microsoft SQL Server**.

   ✓ The **Ground Link Proxy - Microsoft SQL Server** dialog is opened.
6. In **Server name**, enter the connection address to your Microsoft SQL Server, such as `mysqlserver.mydomain.local`.
7. In **Database name**, enter a name for the Ground Link proxy database.

   ℹ We recommend to use the same name as the Ground Link proxy has on M-Files Server.
8. In the **Administrator credentials** and **Basic user credentials** sections, enter the credentials. For instructions, refer to this table.
9. Optional: Click **Test Connection** to test the connection to your Microsoft SQL Server.
10. Click **OK**.

    ✓ A warning dialog is opened to tell you that the operation cannot be undone.
11. Click **Yes** to close the warning dialog and start the migration.

Your Ground Link proxy now uses the Microsoft SQL Server database engine. The database of your Ground Link proxy is on the specified Microsoft SQL Server.

Disabling the Ground Link Connection

If you want to disable the Ground Link feature in a vault, follow the instructions below.

1. Open M-Files Admin and go to a vault.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
2. Select **Configurations** and expand **Advanced Vault Settings**.
3. Expand the **Configuration** node and select **Ground Link**.
4. On the **Configuration** tab, set the **Enabled** value to **No**.
5. Click **Save**.

6. Restart the vault for the settings to take effect.

   Note: Taking a vault offline should always be done in a controlled manner and the vault users should be notified beforehand.

Changing the Location of a Repository Connection

You can move a repository connection to a connected Ground Link proxy or to another vault. This lets you preserve the repository's index and the metadata of promoted objects.

To do this:

1. Open M-Files Admin and go to a vault for which you have enabled the Ground Link connection.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
2. Click **Configurations**.
3. In the navigation area, expand **External Repositories**.
4. Click **Ground Link**.

   ✓ The Ground Link dashboard is opened.
5. In the **Manage Connections** section of the dashboard, click **Migrate Connection**.
6. In the **Connection** section of the **Migrate Connection** dialog, select the connection that you want to move.

   ✓ The **Connection ID**, **Service**, and **Location** fields are automatically filled.

   Note: The service listed in the dialog must be available in the new location.
7. Optional: If a password is necessary for the connection, enter it.
8. In the **New location** section, select the location to which the connection is moved.
9. Optional: If you selected to move the connection to a Ground Link proxy, enter the password that is specified in the Ground Link proxy configuration.
10. Click **Migrate**.

The repository connection is moved to the selected location.

In the **Manage Connections** section, it is also possible to give a repository connection a new ID. This can be helpful, for example, to access promoted objects after you have deleted and recretead a connection.

Changing the Location of Ground Link Proxy Services

You can back up and restore a Ground Link proxy to:

- Move a Ground Link proxy to another server.
- Move Ground Link proxy services to a new Ground Link proxy.

This section tells you how to complete these operations.

Note: Other use cases can have unwanted effects.

Moving a Ground Link Proxy to Another Server

Before you restore the Ground Link proxy on the new server, make sure that the Ground Link proxy is offline.

To move a Ground Link proxy to another server:

1. In M-Files Admin, back up a Ground Link proxy.
2. In the left-side tree view, right-click the Ground Link proxy.
3. Click **Take Offline**.
4. Restore the Ground Link proxy on the new server.
5. Optional: To destroy the original Ground Link proxy, right-click the Ground Link proxy on the old server and select **Operations** > **Destroy** from the context menu.
   a) In the warning dialog that is opened, click **Yes** to close the dialog and destroy the Ground Link proxy.

Moving Ground Link Proxy Services to a New Ground Link Proxy

Before you enable the restored Ground Link proxy, uninstall the unnecessary applications from the two Ground Link proxies.

To move some Ground Link proxy services with all their connections to a new Ground Link proxy:

1. In M-Files Admin, disable a Ground Link proxy.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Ground Link Proxies** and select a Ground Link proxy.
   d) Open the **Configuration** tab.
   e) Set **Enabled** to **No**.
   f) Click **Save**.
2. Back up the Ground Link proxy.
3. Enable the Ground Link proxy.
   a) In the left-side tree view, select the Ground Link proxy.
   b) Open the **Configuration** tab.
   c) Set **Enabled** to **Yes**.
   d) Click **Save**.
4. Restore the Ground Link proxy as a different Ground Link proxy (new identity).
5. Uninstall those applications from the original Ground Link proxy that you want to move to the restored Ground Link proxy.

   For more information, see Installing and Managing Vault Applications.

6. Uninstall those applications from the restored Ground Link proxy that you do not want to move to the restored Ground Link proxy.

   For more information, see Installing and Managing Vault Applications.

7. Enable the restored Ground Link proxy.
   a) In the left-side tree view, select the Ground Link proxy.
   b) Open the **Configuration** tab.
   c) Set **Enabled** to **Yes**.
   d) Click **Save**.

3.2.13. Customizing Server and Vault Behavior

This section collects Microsoft Windows registry settings, M-Files named value settings, and advanced vault settings that you can apply on the M-Files server computer to customize the behavior of M-Files Server and the vaults.

Note: You need M-Files Named Value Manager for distributing named value settings. For downloading the application as well as for instructions on using it, see the document Distributing Vault-Specific Registry Settings from M-Files Server.

In this chapter

Enabling Co-Authoring for Microsoft Office Documents

When co-authoring is enabled, many people can edit Office documents together. There are two versions of the co-authoring feature: desktop co-authoring and web co-authoring.

With desktop co-authoring, users can edit documents together with Microsoft 365 desktop applications in M-Files Web and the new M-Files Desktop. Desktop co-authoring is available for M-Files Cloud customers in selected M-Files platform editions. When this feature is enabled, it is the default edit operation for documents that can be co-authored.

With web co-authoring, users can edit documents together with Microsoft Office for the web. Web co-authoring is available in M-Files Web, the new M-Files Desktop, and the classic M-Files Desktop.

Note: You can only enable one type of co-authoring in one vault.

In this chapter

- Enabling Desktop Co-Authoring
- Enabling Web Co-Authoring

Enabling Desktop Co-Authoring

To enable desktop co-authoring in a vault, you must first complete provisioning for the feature. For instructions, refer to Provisioning for Desktop Co-Authoring in the M-Files knowledge base.

Desktop co-authoring requires M-Files March '25 Update or later.

Desktop co-authoring is available for M-Files Cloud customers in selected M-Files platform editions. When this feature is enabled, it is the default edit operation for documents that can be co-authored.

Note:

After desktop co-authoring is enabled, it cannot be disabled.

Note:

This feature is in development for M-Files Web and the new M-Files Desktop. More functionalities will be available soon.

For a full list of functionalities and limitations, refer to Desktop Co-Authoring FAQ in the M-Files knowledge base.

1. Open M-Files Admin.
2. In the left-side tree view, right-click a vault and select **Properties**.

   ✓ The **Document Vault Properties** dialog opens.
3. In the **Desktop co-authoring** section of the **General** tab, enable **Enabled**.

   ✓ A confirmation dialog opens.
4. Click **Yes** to close the confirmation dialog.
5. In **Tenant ID**, enter your organization's Microsoft 365 tenant ID.

ⓘ Make sure that you use the same tenant where you provisioned this feature. For information on where to find the ID, refer to How to find your tenant ID in Microsoft documentation.

6. In **SharePoint URL**, enter your organization's Microsoft SharePoint root URL.

   https://{organization}.sharepoint.com

7. Click **OK**.

Enabling Web Co-Authoring

Prerequisites

Before you enable web co-authoring, make sure that:

- M-Files Web is set up. If you use M-Files Cloud, M-Files Web is already set up. Otherwise, set up M-Files Web in M-Files Admin.
- You have the latest Microsoft security updates in your environment. For information on the available updates, refer to Microsoft Update Catalog.

Setting up Microsoft Office for the web

To use web co-authoring, you must enable Microsoft Office for the web tools in your vaults.

Deployment	Instructions
M-Files Cloud	You must have a valid Microsoft 365 subscription to use the Microsoft Office for the web services. Request our customer support (M-Files Support Portal) or your M-Files reseller to enable these features.
On-premises server	Refer to Enabling Microsoft Office for the Web Services for M-Files to deploy Office Online Server and set M-Files to use Microsoft Office for the web services.
Self-managed cloud environment	Your organization must be a part of Office Cloud Storage Partner Program to enable these features. Refer to Enabling Microsoft Office for the Web Services for M-Files to deploy Office Online Server and set M-Files to use Microsoft Office for the web services.

Setting the Initial State of the Task Area

By default, the task area is collapsed and it can be expanded by the user. Add this registry key on the client computer to specify whether task area is visible or hidden when the user opens the classic M-Files Desktop. This setting must be added before the user has logged in to the vault for the first time.

Key	**`HKEY_CURRENT_USER\SOFTWARE\Motive\M-Files\<version>\Client\MFShell<vault name>`**
Value name	`TaskPaneInitialState`

Key	**HKEY_CURRENT_USER\SOFTWARE\Motive\M-Files\<version>\Client\MFShell<vault name>**	
Value type	REG_DWORD	
Description	Specifies whether the task area is hidden, visible, or completely disabled when the user opens the classic M-Files Desktop.	
Default value	1	The task area is hidden.
Valid values	0	The task area is disabled and cannot be opened by the user.
	1	The task area is hidden but can be expanded by the user.
	2	The task area is visible but can be hidden by the user.

Hiding Properties in the Classic M-Files Desktop

Use the settings in this section to make the classic M-Files Desktop show only a selected set of properties in these places:

- the **Insert Column** list for the listing area
- the list of properties after you click **Add property** on the metadata card
- the list of properties available in the search options

Selecting properties to be shown in the Insert Column list

To select which properties are shown in the **Insert Column** list:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **Columns** > **Insertable Columns**.

3. Set **Hide Default Insertable Columns** to **Yes**.

4. Expand **Visible Insertable Columns**.

5. Click **Add Column**.

6. As the value of the **Column** setting, select a property that you want to add to the list.

7. Repeat steps 5 and 6 for as many properties as necessary.

8. Click **Save**.

Selecting properties to be shown in the Add property list

To select which properties are shown in the **Add property** list:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **Properties** > **Visible Properties**.

3. Set **Hide All Default Properties** to **Yes**.

4. Expand **Property Definitions**.

5. Click **Add Property definition**.

6. As the value of the **Property definition** setting, select a property that you want to add to the list.

7. Repeat steps 5 and 6 for as many properties as necessary.

8. Click **Save**.

Selecting properties to be shown for search options

To select which properties are shown for search options:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **Search** > **Advanced Search Properties**.

3. Set **Hide All Default Properties** to **Yes**.

4. Expand **Property Definitions**.

5. Click **Add Property Definition**.

6. As the value of the **Property Definition** setting, select a property that you want to add to the list.

7. Repeat steps 5 and 6 for as many properties as needed.

8. Click **Add Value List**.

9. As the value of the **Value List** setting, select a value list that you want to add to the list.

10. Repeat steps 8 and 9 for as many value lists as necessary.

11. Optional: Change the value of the **Checked out / Checked out to** setting if you want to hide the properties **Checked out**, **Checked out to**, or both from the list.

12. Click **Save**.

Disabling the Comment Dialog for Assignments

When you mark an assignment complete, the classic M-Files Desktop shows the comment dialog. You can change this behavior with the instructions given here.

Disabling the comment dialog for assignments in Advanced Vault Settings

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **Client** > **Desktop** > **Assignments**.

   ⓘ The **Manage Client Settings Centrally** setting must be set to **Yes**. Before you set it to **Yes**, read the setting description on the **Info** tab.

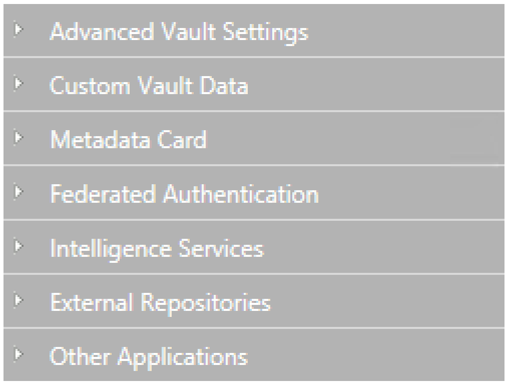
3. Change the behavior with the **Show Mark Complete Dialog** setting.

   ⓘ For information about the options, see the setting description on the **Info** tab.

Disabling the comment dialog for assignments with Custom Vault Data

Note: You cannot use this method if Manage Client Settings Centrally is set to **Yes**.

1. In M-Files Admin, access the custom vault data section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, expand **Custom Vault Data**.



2. Select **Namespace Registry** > **Configuration**.
3. Expand the **Namespaces** node, click **Add Namespace**, and expand the newly added namespace node.
4. In the **Group** field, type a suitable group name, such as `Assignments`.
5. Use the **Storage Type** drop-down menu to select the **MFConfigurationValue** storage.
6. In the **Namespace** field, enter the following value: `M-Files.Core.Client.Settings`
7. In the **Namespace Label** field, type a suitable label, such as `Assignments`.
8. In the **Namespace Description** field, enter for example `Settings related to assignments`.
9. Click **Save** to save the namespace settings.
10. In the gray navigation area, expand **Named Values**.
11. Expand the namespace group you just created, then select the namespace node, and finally the **Configuration** node.
12. Click **Add Named Value**, and expand the newly created named value node.
13. In the **Name** field, enter the value `ShowMarkCompleteUI`.
14. In the **Value** field, enter a configuration similar to the example below.

```
{
"MFShell":{
     "ShowMarkCompleteUI":<X>
     }
}
```

Change the value of <*X*> according to how you want the user interface to behave:

Value of <*X*>	Description
0	The comment dialog is not shown.
1	The comment dialog is shown. This is the default behavior.
2	The comment dialog is shown for assignments when they are marked complete in the task area.

Value of *<X>*	Description
`3`	The comment dialog is shown for assignments when they are marked complete with the metadata card.

15. Click **Save** to save the configuration.

The new behavior is enabled for users as soon as they have logged out from and logged back in to the vault. To log out all vault users, restart the vault. However, taking a vault offline must always be done in a controlled manner and the vault users must be notified beforehand.

Setting a Primary File Type for Multi-File Documents

You can set a file type of your choice to act as the primary file type for multi-file documents in the vault. This has these effects:

- The icon of the specified file type is shown as the icon of the multi-file document.
- The Document Preview shows the preview of the primary file when the multi-file document is selected.
- Double-clicking the object does the default action of the primary file type.

Note: This feature is supported in the classic M-Files Desktop only. The common Windows dialogs, such as **Open** or **Save As**, are not affected by the primary file type settings.

To specify a primary file type to be used in a vault, do these steps on the M-Files server computer:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **Multi-File Documents** and select **Primary Files**.

3. Click **Add Document Class**.

4. Expand the newly created node and select a class value for the **Document Class** setting.

   This value specifies the object class to which the setting applies.

5. Expand **File Name Filters** and click **Add Filter**.

   These filtering settings specify the primary file type for the selected class.

6. Expand the newly created node and specify a value for the **Filter** setting.

   The value can include wildcard characters, for example: `order-?.txt` or `*.pdf`.

Enter only a single value for each setting node. You can, however, add as many setting nodes with the **Add Filter** command as you need.

The filtering values are evaluated from top to bottom. You can move a setting up or down by right-clicking it (the node level under **File Name Filters**) and selecting **Move Up** or **Move Down** in the context menu.

7. Click **Save** once you are done with your changes.
8. Restart the vault for the settings to take effect.

Note: Taking a vault offline should always be done in a controlled manner and the vault users should be notified beforehand.

Multi-file documents of the selected class stored in this vault and any connected external repositories now use the specified file type as their primary file and behave as described at the top of this section. If the document contains more than one file matching the filtering conditions, the file that has been added first is used as the primary file.

Setting Character Limit for Inserted Properties

You can set a limit for the maximum number of characters that a property value added to Microsoft Word documents can contain. Add this Microsoft Windows registry setting to the client computer:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Client\MFOfficeAddin**	
Value name	`LongValueInMultilineTextPropertyInWordAllowed`	
Value type	`REG_DWORD`	
Description	Specifies whether users can add property values of over 255 characters to Microsoft Word documents with the M-Files **Insert Property** feature.	
Default value	`1`	Long values can be added.
Valid values	`0`	When a long property value is added to a Microsoft Word document, only the first 255 characters are shown.
	`1`	It is possible to add long values. The number of characters added can be higher than 255 characters.

Enabling Automatic Updates for Metadata Fields

You can add metadata properties to Microsoft Word, Microsoft Excel, and Microsoft PowerPoint documents with the M-Files for Microsoft Office plugin. The Microsoft Office plugin is included in the M-Files Desktop installation package. For more information on this feature, see Add M-Files Property.

With M-Files Desktop, the Microsoft Office plugin updates the property values when the document is opened in the Microsoft Office application. In addition, you can set the metadata fields to be updated on the server when the document is checked in. This can be especially helpful for M-Files Web and M-Files Mobile users.

Note: In some environments, automatic metadata field updates can decrease performance.

To enable automatic metadata field updates during document check-in:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **File Operations** > **Extension Filter for Embedded Metadata Update on Check-In**.

3. Click **Add Extension**.

4. In **Extension**, enter the file extension.

   These are the valid values:

   - `DOC` and `DOCX`
   - `XLS` and `XLSX`
   - `PPT`, `PPTX`, and `ODP`
   - `ALL`

   Use `ALL` to set the metadata of all valid file types to be updated. When you use this value, do not add other extensions.

5. Repeat the steps 3 and 4 for each file extension.

6. Click **Save**.

Configuring Public Links

Note: The classic M-Files Desktop in M-Files January '24 Update and later no longer refer to public links. Instead, these links have the name visitor link for anyone. This means that user interface uses the new name "visitor link for anyone", but the links still use the configuration of public links. The classic M-Files Web still uses the term "public link".

Important information

A public link created by a user will work as long as these requirements are met:

- The user's account is enabled.
- The user has at least read permissions to the document.

For security reasons, the link will stop working if either requirement is not met. To share documents with a large number of people without access to M-Files, consider these alternative sharing methods:

- M-Files Hubshare offers more control and security.
- Anonymous vault access lets users access a vault without credentials.

Before you start to configure public links, make sure that these prerequisites are completed:

- The classic M-Files Web has been set up.
- The home page for the classic M-Files Web has been specified in **Document Vault Properties**.

To enable or disable public links for all vaults on an M-Files Server, see Configuring public links for M-Files Server. When you have configured public links for M-Files Server, you can configure vault-specific public link settings.

To configure visitor links for anyone for the classic M-Files Desktop and public links for the classic M-Files Web, see Configuring visitor links for anyone for the classic M-Files Desktop and public links for the classic M-Files Web. To only configure public links for the classic M-Files Web, see Configuring public links for the classic M-Files Web.

Configuring public links for M-Files Server

To configure public links for M-Files Server:

1. Add or edit this registry setting on the M-Files Server computer:

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer`**	
Value name	`EnableSharedPublicLinks`	
Value type	`REG_DWORD`	
Description	Enables or disables the public link feature on the server. When disabled, visitor links for anyone and public links cannot be created with clients or APIs, and previously shared visitor links for anyone and public links no longer operate. If you disable this feature, make sure that you also specify the same settings for the necessary clients. For instructions, see Configuring visitor links for anyone for the classic M-Files Desktop and public links for the classic M-Files Web or Configuring public links for the classic M-Files Web.	
Default value	`1`	
Valid values	`1`	The **Create Visitor Link for Anyone** option is enabled.
	`0`	The **Create Visitor Link for Anyone** option is disabled.

2. Use Windows Task Manager to restart the **MFServer** service:
   a) Right-click the taskbar and select **Task Manager**.

      ✓ The **Task Manager** window is opened.

   b) Open the **Services** tab.
   c) Right-click the **MFServer** service and select **Restart**.

Configuring visitor links for anyone for the classic M-Files Desktop and public links for the classic M-Files Web

Before you start, make sure that notifications are enabled on the server and in the vault. Otherwise, passcodes to open M-Files links cannot be sent.

To configure visitor links for anyone for the classic M-Files Desktop and public links for the classic M-Files Web:

1. Expand the **Custom Vault Data** section in **Configurations**.

2. Expand **Namespace Registry** > **Configuration**.

3. Click **Add Namespace** and expand the new namespace node.

4. In **Storage Type**, select **MFConfigurationValue**.

5. In **Namespace**, enter this value: `M-Files.Core.Sharing.PublicLinks.Settings`

6. Enter values for **Group**, **Namespace Label**, and **Namespace Description**.

7. In the navigation area, expand **Named Values** > **<namespace group name>** > **<namespace label>** and click **Configuration**.

   The namespace group name and label are the ones that you set in step 6. For example, **Named Values** > **Sharing Settings** > **Public Link Sharing Settings**.

To disable or enable the **Visitor Link for Anyone** feature in the classic M-Files Desktop and the **Share Public Link** feature in the classic M-Files Web:

8. Click **Add Named Value** and expand the new named value node.

9. In **Name**, enter `Enabled`.

10. Do one of these steps:

    a. To disable the features, in **Value**, enter this value:

    ```
    false
    ```

    Note: If you disable the features, make sure that you also add the corresponding registry setting for M-Files Server. For instructions, see Configuring public links for M-Files Server.

    or

    b. To enable the features, in **Value**, enter this value:

    ```
    true
    ```

    Note: The features are enabled by default.

To specify whether the visitor links for anyone and public links can point to the latest version of the shared files or only to the specific, shared version:

11. Click **Add Named Value** and expand the new named value node.

12. In **Name**, enter this value: `AllowSharingLatestVersion`

13. Do one of these steps:

    a. To allow links to point to the latest version of the shared file, in **Value**, enter this value:

    ```
    true
    ```

    or

b. To set links to always point to the specific, shared file version, in **Value**, enter this value:

```
false
```

Note: Visitor links for anyone and public links normally always point to the specific version that the user has shared.

To specify the default expiration time for public links in the classic M-Files Web:

14. Do the steps from 1 to 7, but use this value in **Namespace**: `M-Files.Core.Client.Settings`

15. Click **Add Named Value** and expand the new named value node.

16. In **Name**, enter this value: `DefaultExpireInDays`

17. In **Value**, enter the expiration time in days. For example:

```
10
```

In the example, the expiration time for public links is 10 days if the user does not change it in the **Share Public Link** dialog.

After you have configured the features, restart the vault so that the changes are taken into use:

18. Restart the vault.

Configuring public links for the classic M-Files Web

To configure public links for the classic M-Files Web in the **Advanced Vault Settings** section in M-Files Admin:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. In the navigation area, expand **Client** > **Classic Web** > **Sharing**.

3. Do the necessary changes.

   Note: If you set **Enable Sharing** to **No**, make sure that you also add the related registry setting for M-Files Server. For instructions, see Configuring public links for M-Files Server.

4. Click **Save**.

Configuration Options for the "Send and Save to M-Files" Button

Using M-Files Named Value Manager, you may add the **Send and Save to M-Files** button to the Microsoft Outlook composer window on all client computers, or disable the **Send and Save to M-Files** button altogether. For more information on the **Send and Save to M-Files** function, see Functions in Microsoft Outlook.

Note: You need M-Files Named Value Manager for distributing the settings. For downloading the tool as well as for instructions on using it, see the document Distributing Vault-Specific Registry Settings from M-Files Server.

Complete the following steps to configure the **Send and Save to M-Files** button for all client computers:

1. Open M-Files Named Value Manager.
2. Use the **Server** drop-down menu to select the M-Files server and then the **Vault** drop-down menu to select the document vault.
3. Use the **Storage Type** drop-down menu to select the `MFConfigurationValue` storage.
4. In the **Namespace** field, enter the following value: `M-Files.Core.Client.Settings`
5. Click **Add** to add a new key.
6. In the left-side pane, double-click **New Named Value Key** and enter the following value: `MSOutlookRibbon`
7. Select the newly added key, and then either:

   a. If you want to display the **Send and Save to M-Files** button in the Microsoft Outlook composer window on all client computers, add the following value to the right-side pane:

   ```
   {
     "Common": {
       "MSOutlookRibbon": {
         "ShowSendAndSaveInBuiltInTab": 1
       }
     }
   }
   ```

   or

   b. If you want to disable the **Send and Save to M-Files** button on all client computers, add the following value to the right-side pane:

   ```
   {
     "Common": {
       "MSOutlookRibbon": {
         "ShowSendAndSaveInMFilesTab": 0
       }
     }
   }
   ```

8. Click **Save** and then close M-Files Named Value Manager if you no longer need it.

The **Send and Save to M-Files** button settings you have specified affect all vault users in the selected vault.

Disabling the Reference Direction Setting for Grouping Levels

When you are creating or editing a grouping level for a view, the **Define Grouping Level** dialog normally shows the **Reference direction** setting that allows you to select the metadata reference direction between the object type of the grouping level and the objects in the view. You can use a Windows registry setting to disable this option and therefore only allow the **To <selected object type>** reference direction to be used.

Do the following to disable the **Reference direction** setting in the **Define Grouping Level** dialog:

1. Add the following setting to the Windows registry of the server computer:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Server\MFServer\VaultOptions\{*<vault GUID>*}**	
Value name	EnableReverseGroupingLevelsForViews	
Value type	REG_DWORD	
Description	Specifies whether the **Reference direction** setting is in use in the **Define Grouping Level** dialog in this vault.	
Default value	The default value is 1, meaning that the setting is enabled.	
Valid values	1	The setting is in use.
	0	The setting is not in use. The reference direction is always **To <selected object type>**.

2. Repeat step 1 for as many vaults as needed.
3. Use Windows Task Manager to restart the **MFServer** service:
   a) Right-click the taskbar and select **Task Manager**.

      ✓ The **Task Manager** window is opened.

   b) Open the **Services** tab.
   c) Right-click the **MFServer** service and select **Restart**.

Enabling Phonic and Fuzzy Searches

Phonic and fuzzy searches are disabled by default in a vault and you can enable them in M-Files Admin.

> **Note:** To use this feature, your search engine must be dtSearch.

To enable phonic searches, fuzzy searches, or both:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

      ✓ The advanced vault settings are shown.

2. Expand **Search** > **Full-Text Search**.

3. Set **Enable Fuzzy Searching** to **Yes**.

4. Set **Enable Phonic Searching** to **Yes**.

5. Click **Save**.

6. Use Windows Task Manager to restart the **MFServer** service:
   a) Right-click the taskbar and select **Task Manager**.

      ✓ The **Task Manager** window is opened.

   b) Open the **Services** tab.
   c) Right-click the **MFServer** service and select **Restart**.

Setting Up Synonym Search

You must set up the synonym search and create a custom thesaurus so that the vault users can find documents using synonyms in the search query. If your thesaurus is large, the synonym search can have a negative effect on the performance of the search.

Note: To use this feature, your search engine must be dtSearch.

To set up the synonym search:

1. Use a text editor to create your own custom thesaurus file that is similar to this:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<dtSearchUserThesaurus>
 <Item>
  <Name>Synonyms for announcement</Name>
  <Synonyms>announcement notice bulletin statement publication</Synonyms>
 </Item>
 <Item>
  <Name>Synonyms for contract</Name>
  <Synonyms>contract agreement deal arrangement</Synonyms>
 </Item>
</dtSearchUserThesaurus>
```

   Each `Item` contains a synonym group. The `Name` element contains a description for the synonym group and it has no effect on search. The `Synonyms` element contains a single synonym group. Separate the synonyms with a space.

2. Save the file with the name `thesaur.xml` here:

```
C:\Program Files\M-Files\<version>\Server\<language code of the search language>
```

3. Open M-Files Admin and go to a vault.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.

4. Click **Configurations**.
5. In the navigation area, expand **Advanced Vault Settings** > **Configuration** > **Search**.
6. Click **Full-Text Search**.
7. In **Thesaurus**, enter `thesaur.xml`.
8. Click **Save**.
9. Close M-Files Admin.
10. Use Windows Task Manager to restart the **MFServer** service:
    a) Right-click the taskbar and select **Task Manager**.

       The **Task Manager** window is opened.

    b) Open the **Services** tab.
    c) Right-click the **MFServer** service and select **Restart**.

Now when users search for `announcement`, the search results list documents that contain the words `announcement`, `notice`, `bulletin`, `statement`, or `publication`. Synonyms are identified in document contents and metadata.

Disabling the Search for Inflected Forms

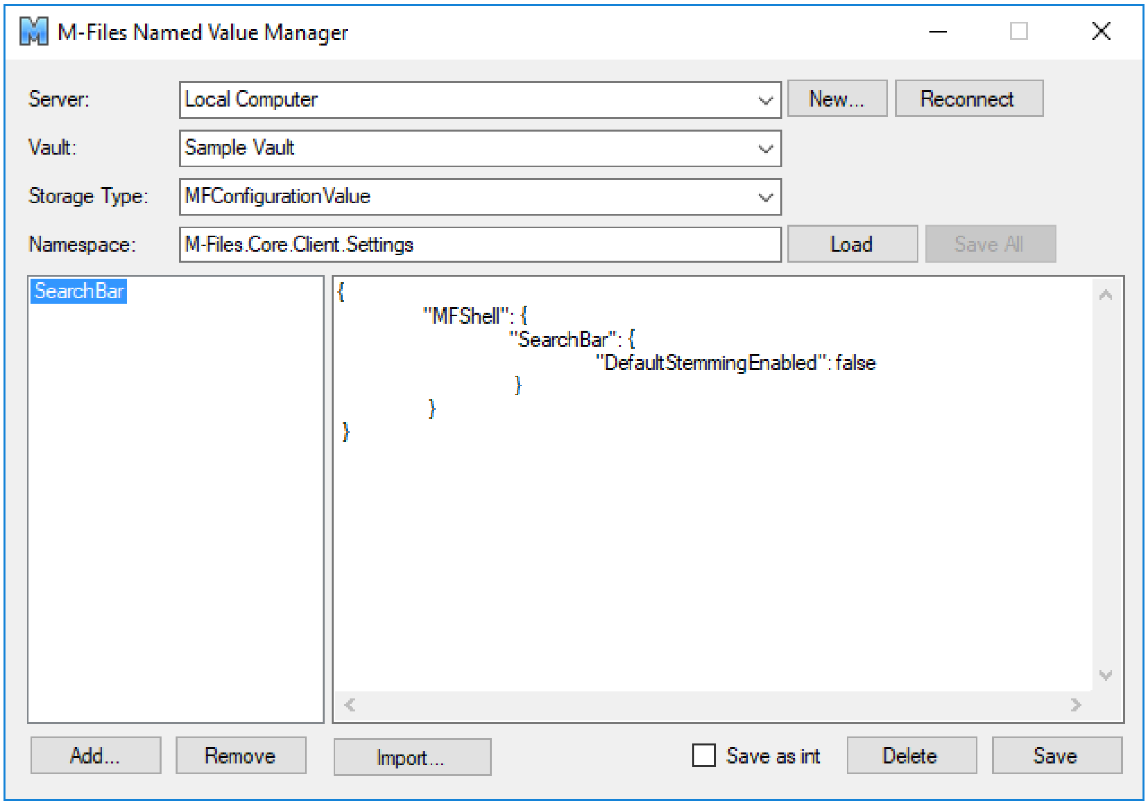
By default, M-Files searches for inflected forms of your search term (see Quick Search for more information). This feature can be disabled by unchecking the option **Look for different inflected forms of the words in Quick Search** in the **Additional Conditions** dialog. If you want this feature to be disabled by default for all vault users, complete the steps below on the M-Files server computer.

> **Note:** You need M-Files Named Value Manager for distributing these settings. For downloading the application as well as for instructions on using it, see the document Distributing Vault-Specific Registry Settings from M-Files Server.

1. Open M-Files Named Value Manager.
2. Use the **Server** drop-down menu to select the M-Files server and then the **Vault** drop-down menu to select the document vault.
3. Use the **Storage Type** drop-down menu to select the `MFConfigurationValue` storage.
4. In the **Namespace** field, enter the following value: `M-Files.Core.Client.Settings`
5. Click **Add...** to add a new key.
6. In the left-side pane, double-click **New Named Value Key** and enter the following value: `SearchBar`
7. Select the newly added key, and in the right-side pane, enter the following value:

```
{
    "MFShell": {
        "SearchBar": {
            "DefaultStemmingEnabled": false
        }
    }
}
```

Your configuration in M-Files Named Value Manager should now be similar to the example shown below.



Server: Local Computer

Vault: Sample Vault

Storage Type: MFConfigurationValue

Namespace: M-Files.Core.Client.Settings

SearchBar

```
{
        "MFShell": {
                "SearchBar": {
                        "DefaultStemmingEnabled": false
                }
        }
}
```

☐ Save as int

8. Click **Save** and then close M-Files Named Value Manager if you no longer need it.

The search for inflected forms is now disabled by default in the selected vault for all vault users.

Disabling the Sorting of Search Results by Their Relevance

By default, M-Files sorts search results by their relevance. For more information on how document relevance in relation to the search term is determined, see Search result sorting.

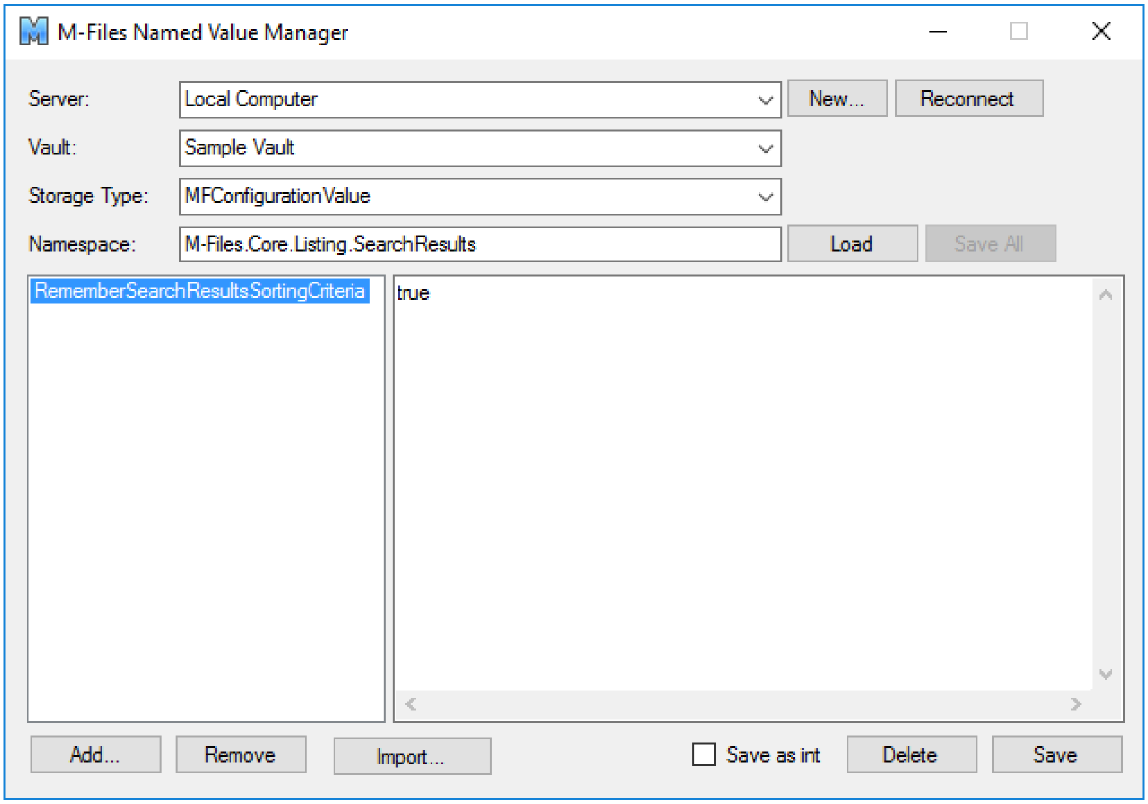
Note: You need M-Files Named Value Manager for distributing some of the settings. For downloading the application as well as for instructions on using it, see the document Distributing Vault-Specific Registry Settings from M-Files Server.

This behavior can be prevented so that search results are sorted by user preference instead. Make the following changes on the M-Files Server computer to prevent search results to be automatically sorted by their relevance:

1. Open M-Files Named Value Manager.
2. Use the **Server** drop-down menu to select the M-Files server and then the **Vault** drop-down menu to select the document vault.
3. Use the **Storage Type** drop-down menu to select the `MFConfigurationValue` storage.
4. In the **Namespace** field, enter the following value: `M-Files.Core.Listing.SearchResults`
5. Click **Add...** to add a new key.

6. In the left-side pane, double-click **New Named Value Key** and enter the following value: `RememberSearchResultsSortingCriteria`
7. Select the newly added key, and in the right-side pane, enter the following value: `true`

   Your configuration in M-Files Named Value Manager should now be similar to the example shown below.



Server: Local Computer

Vault: Sample Vault

Storage Type: MFConfigurationValue

Namespace: M-Files.Core.Listing.SearchResults

RememberSearchResultsSortingCriteria

true

□ Save as int

8. Click **Save** and then close M-Files Named Value Manager if you no longer need it.
9. Optional: If you use the classic M-Files Web, make the following registry change on the M-Files server computer:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Server\MFWA\Sites\1\Vaults\*<vault GUID>*\Configurations**	
Value name	`DefaultSearchSortPropertyID`	
Value type	`REG_SZ`	
Description	The ID of the property by which search results are sorted.	
Value	*<no value>*	Empty the value to disable the sorting of search results by their relevance in M-Files Web.

10. Use Windows Task Manager to restart the **MFServer** service:
    a) Right-click the taskbar and select **Task Manager**.

       The **Task Manager** window is opened.

    b) Open the **Services** tab.
    c) Right-click the **MFServer** service and select **Restart**.

M-Files no longer forces search results to be sorted by their relevance, and therefore users can change the column by which search results are sorted and the user preference is retained in subsequent searches.

Configuring Search Facets

Search facets are filters that let users get more focused search results. These filters include, for example, customer, file type, class, and date. Facets and faceted search are available in vaults that use Micro Focus IDOL or Smart Search as the search engine. Only system admins and users with the **Full control of vault** rights can change these settings. For more information about the configuration, refer to the document Configuring Faceted Search.

When the setup is saved, M-Files Desktop and M-Files Web show search facets after the user does as search. After you have specified the settings, vault restart is not necessary.

To add a search facet:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ☑ The advanced vault settings are shown.

2. Expand **Search** > **Facets**.
3. Click **Add Facet**.
4. Expand the created facet.
5. In **Type**, select a facet that the users will see in as a filter.

   ⓘ For more information about the configuration, refer to the document Configuring Faceted Search.

6. Select values for the remaining type settings.
7. Optional: Set **Show More Link** to **Yes** if you want the users to see the link when there are more than five facet values.
8. Optional: In **Display Order**, write an integer that sets the order of the filters in the user interface.

   ⓘ A facet with the value `1` is put before a facet with the value `2`, and so on.

9. Click **Save**.

Configuring Automatic Updates with Registry Settings

In addition to using the **Automatic Updates** dialog, you can configure automatic updates on the server computer and client computers with Microsoft Windows registry settings. For the changes to take effect, you must restart the M-Files Server service. For more information on automatic updates, see Updating M-Files.

Note: If automatic updates are disabled, you must have local administrative permissions on your computer to install an available update.

Tip: In Microsoft Windows, you can use Group Policy Objects to distribute registry settings to multiple computers.

Disabling or enabling automatic updates

Add or edit the following Windows registry setting to disable or enable the automatic updates. To make sure that your M-Files software is always up to date, do not disable automatic updates.

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\Common\Updates`**	
Value name	`Enabled`	
Value type	`REG_DWORD`	
Description	If the value is set to `0`, automatic updates are disabled on the target computer, including manual update checks with the **Automatic Updates** dialog. You can update the software by downloading and running the installation package by hand.	
Default value	The default value is `1`.	
Valid values	`1`	Updates are enabled on the computer.
	`0`	Updates are disabled on the computer.

Disabling or enabling automatic update features

Add or edit the Windows registry settings in this section to disable or enable specific features of automatic updates.

Disabling or enabling the setting for automatic update installation

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Common\MFAUClient`**	
Value name	`AllowToUseAutoInstallationFeature`	
Value type	`REG_DWORD`	
Description	If the value is set to `0`, installing automatic updates is disabled and only the **Download updates automatically** option is visible on the **Settings** tab in the **Automatic Updates** dialog. You can still install updates in the **Installation** tab of the **Automatic Updates** dialog.	
Default value	The default value is `1`.	
Valid values	`1`	The setting **Install updates automatically** is shown on the **Settings** tab.
	`0`	The setting **Install updates automatically** is not shown and updates are not automatically installed.

Disabling or enabling automatic update installation

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Common\MFAUClient`**
Value name	`EnableAutoInstallation`

Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Common\MFAUClient`	
Value type	`REG_DWORD`	
Description	With this setting, you can specify whether automatic updates are automatically installed. If the setting `AllowToUseAutoInstallationFeature` is set to `0`, this setting has no effect.	
Default value	The default value is `0`.	
Valid values	`0`	Automatic updates are not automatically installed. The **Install updates automatically** option is disabled on the **Settings** tab of the **Automatic Updates** dialog.
	`1`	Automatic updates are automatically installed. The **Install updates automatically** option is enabled on the **Settings** tab of the **Automatic Updates** dialog.

Disabling or enabling automatic update downloads

Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Common\MFAUClient`	
Value name	`EnableUpdates`	
Value type	`REG_DWORD`	
Description	If the value is set to `0`, M-Files no longer downloads updates automatically, but you can run the update check manually in the **Installation** tab of the **Automatic Updates** dialog.	
Default value	The default value is `1`.	
Valid values	`1`	M-Files automatically checks for updates and downloads a new version if one is available.
	`0`	M-Files does not check for new versions automatically.

Disabling or enabling automatic update options in the user interface

Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Common\MFAUClient`	
Value name	`CanConfigureAutoInstallingViaUi`	
Value type	`REG_DWORD`	
Description	If the value is set to `0`, the settings shown on the **Settings** tab in the **Automatic Updates** dialog cannot be changed.	
Default value	The default value is `1` for Microsoft Windows Server operating systems and `0` for other operating systems.	
Valid values	`1`	Settings shown on the **Settings** tab in the **Automatic Updates** dialog can be changed.
	`0`	Settings shown on the **Settings** tab in the **Automatic Updates** dialog cannot be changed.

Controlling the installation deadline

If necessary, you can adjust the installation deadline and the amount of time by which users can delay the installation. Add the following registry settings on the target computer to adjust the installation deadline:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common \MFAUClient**	
Value name	PostponeDurationInHours	
Value type	REG_DWORD	
Description	Users can delay the installation process once before it is started. Edit this value to change the number of hours by which users can delay the installation process by selecting **Update Later** in the options dialog.	
Default value	10	The default value for the additional delay is 10 hours.
Valid values	Any number of hours.	

Defining the installation schedule

You can select the preferred days and time of installing M-Files updates. It is recommended that you select a date and time that is outside working hours so that installing updates does not interrupt daily M-Files tasks in the organization.

Note that the computer must be running and not in sleep or hibernate mode when the update is scheduled to be installed. If the computer is not running when the scheduled installation time occurs, the update is attempted to be installed or scheduled the next time the computer is started.

Add the following registry settings on the target computer to define an installation schedule:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common \MFAUClient**	
Value name	AutoInstallDays	
Value type	REG_SZ	
Description	One or more days when automatic updates are attempted to be installed. Separate multiple values with a semicolon.	
Default value	mon;tue;wed;thu;fri;sat;sun	By default, automatic updates are attempted to be installed every day of the week.
Valid values	mon	Monday
	tue	Tuesday
	wed	Wednesday
	thu	Thursday
	fri	Friday
	sat	Saturday
	sun	Sunday

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common \MFAUClient**	
Value name	AutoInstallTimeOfDay	
Value type	REG_SZ	
Description	The time of day in 24-hour format when automatic updates are attempted to be installed.	
Default value	02:00	By default, automatic updates are attempted to be installed at 02:00.
Valid values	Any valid time of day.	

Defining the maximum random added delay before the update

You can add random delay to the beginning of the automatic updates by adding the following registry setting on the target computer:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\*<version>*\Common \MFAUClient**	
Value name	AdditionalMaxRandomSleepingPeriod	
Value type	REG_DWORD	
Description	The maximum value for the random delay (in other words sleeping) added to the main sleeping period (default: one hour) at the beginning of the automatic updates poll-download-install cycle. The randomness establishes a crude form of load balancing in a network. When defining the value, take into consideration that too large values may impact polling frequency and that also several other registry settings affect the sleeping period and installation. Their combined effect can result in unwanted consequences, such as preventing a user from postponing the installation during office hours or delaying the download to occur only after a weekly installation day. With the default settings, the poll-download-install cycle restarts every 1-2 hours with a mean value of 1.5 hours.	
Default value	3600	The default maximum added delay value is one hour (3600 seconds).
Valid values	0	No random added delay.
	<1-86400>	Maximum random added delay in seconds.

Specifying PDF Conversion Limitations for Indexing and File Preview

You can use these settings to specify file size and conversion time limits for PDF conversions done in the context of indexing and file previews.

The limits are not used in these contexts:

- PDF Processor module of M-Files Compliance Kit
- PDF conversion caused by a workflow state
- PDF conversion done in an M-Files client

These are the default settings for the maximum size of the source file by file type.

- Email file: 10 MB
- Microsoft Excel file: 10 MB
- Image file: 100 MB

- PDF file: 10 MB
- Microsoft PowerPoint file: 10 MB
- Microsoft Visio file: 10 MB
- Microsoft Word file: 25 MB

The maximum processing time is 120 seconds.

To change these values, do the steps given here on the M-Files server computer as a system administrator.

To change a file size limit:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **PDF Conversion**.

3. Expand a file format.

4. In **Maximum Source File Size**, enter the size limit in bytes.

5. Optional: Specify the other settings for the selected file format.

   ⓘ For more information, select a setting and see the **Info** tab.

6. Click **Save**.

To change the conversion time limit:

7. In the **Advanced Vault Settings** section, expand **File Previews** > **Viewer Files** and change the value of **PDF Conversion Timeout**.

To apply the changes:

8. Use Windows Task Manager to restart the **MFServer** service:
   a) Right-click the taskbar and select **Task Manager**.

   ✓ The **Task Manager** window is opened.

   b) Open the **Services** tab.
   c) Right-click the **MFServer** service and select **Restart**.

Defining File Types for Indexing

M-Files Server tries to index the contents of the most general file types when a new file version is checked in to M-Files Server. Indexing enables users to search documents and objects from M-Files using the words that can be found in the file content. This topic lists the files whose contents are indexed by default and tells how to add file types to be indexed and how to exclude file types from indexing.

Note: Metadata is always indexed regardless of whether the file extension is in the list of file types to be indexed or in the blacklist of file types not to be indexed.

The following table lists the extensions of files whose contents are indexed by default when dtSearch or Micro Focus IDOL search engine is in use.

Table 1: Extensions of File Types Indexed by Default

File Extension	Information on File Extension
123	Lotus
CSV	Comma separated values file
DOC	Microsoft Word
DOCM	Microsoft Word Open XML, macro-enabled document
DOCX	Microsoft Word
DOT	Microsoft Word template
DOTM	Microsoft Word macro-enabled template
EML	Email message
HTM	Hypertext Markup Language file
HTML	Hypertext Markup Language file
ICS	Universal calendar file
KEY	Apple
MSG	Microsoft Outlook email message
NUMBERS	Apple
ODF	OpenDocument
ODG	OpenDocument
ODP	OpenDocument
ODS	OpenDocument
ODT	OpenDocument
ONE	OneNote
OTG	OpenDocument
OTP	OpenDocument
OTS	OpenDocument
OTT	OpenDocument
PAGES	Apple
PDF	Portable Document Format file created by Adobe Acrobat or another PDF application
POT	Microsoft PowerPoint template

File Extension	Information on File Extension
POTX	Microsoft PowerPoint template
PPT	Microsoft PowerPoint
PPTM	Microsoft PowerPoint, macro-enabled
PPTX	Microsoft PowerPoint
PTM	Microsoft PowerPoint, macro-enabled template
QPW	Corel Quattro Pro
RTF	Rich Text Format file
STC	StarOffice
STI	StarOffice
STW	StarOffice
SXC	StarOffice
SXD	StarOffice
SXG	OpenOffice
SXI	StarOffice
SXW	StarOffice
TXT	Standard text document
WB1	Corel Quattro Pro
WB2	Corel Quattro Pro
WB3	Corel Quattro Pro
VDX	Microsoft Visio
WKS	Lotus
WPD	WordPerfect
WPF	WordPerfect
WRI	Microsoft Write
VSD	Microsoft Visio
VSDX	Microsoft Visio
XLS	Microsoft Excel
XLSB	Microsoft Excel, binary format
XLSM	Microsoft Excel, macro-enabled
XLSX	Microsoft Excel
XLT	Microsoft Excel template
XLTM	Microsoft Excel, macro-enabled template
XLTX	Microsoft Excel template
XML	Extensible Markup Language data file

File Extension	Information on File Extension
XPS	Microsoft page layout
XSL	XML style sheet

Using Blacklist in Indexing

If you do not want to use the default list of file types to be indexed, you can use the built-in blacklist instead. The blacklist contains a predefined set of file extensions specifying the file types that are not indexed.

Complete the following steps to set the built-in blacklist to be used in indexing:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **Search** > **Full-Text Search**.

3. Set **Use File Extension Blacklist Instead of Whitelist in Indexing** to **Yes**.

4. Click **Save**.

Defining Additional File Types for Indexing

In addition to either the list of file types to be indexed or the list of file types not to be indexed, you can define other file types to be indexed. Also, you can define some file types you do not want to be included in indexing. For example, you have the list of file types to be indexed, but you would like to exclude one of the file types from indexing. To exclude the file contents from indexing, you must define the file extension according to the following instructions.

To define file types to be indexed or not to be indexed:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **Search** > **Full-Text Search** > **File Extensions To Index** or **File Extensions To Not Index**.

3. Click **Add Extension**.
4. In the **Extension** field, enter the file extension, for instance `dwg`.
5. Repeat the steps 3 and 4 for each file extension.
6. Click **Save** to save your configuration.

Configuring Mappings Between Incoming Connections and Vaults

Note: Before you configure the mappings, make sure that you have registered the vault-specific DNS (Domain Name System) names to DNS.

To specify mappings between incoming connections and M-Files vaults, add this registry configuration on the M-Files server computer.

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\`*`<version>`*`\Server\Common`**
Value name	`VaultDNSConfig`
Value type	`Multi-String Value`
Description	The value specifies mappings between incoming connections and vaults.

Value	`https://`*`<DNS name for the vault 1>`*`={`*`<vault GUID for the vault 1>`*`}`
	`https://`*`<DNS name for the vault 2>`*`={`*`<vault GUID for the vault 2>`*`}`
	For example:
	`https://vault1.company.com={990827D8-8AF2-4A4E-B121-4C1A8AD8ECD0}`
	`https://vault2.company.com={F565EDFE-939E-4507-B078-D06902888C98}`

You can write one entry per row. To map many DNS names to a single vault, write each connection on a separate row. However, you cannot map the same DNS name to many vaults. If the list contains the same DNS name many times, only the topmost entry in the list is effective. For the changes to take effect, you must restart the M-Files Server service.

Specifying Vault-Specific Locale Settings

In most cases, M-Files clients show date and time values in the format specified in the regional settings of the client computer. However, in some M-Files Server operations, number and date values are formatted with the locale settings of the M-Files server computer. In M-Files Cloud, the server uses US locale.

If you cannot change the server computer's locale, you can specify locale settings for the vault to override the server locale. This can be useful, for example, if you use M-Files Cloud.

Specifying vault-specific locale settings for server-side PDF conversions

When the M-Files server converts Microsoft Word documents that contain dynamic metadata fields to PDF, M-Files refreshes the metadata fields before the conversion process. Number and date values are formatted with the locale settings of the M-Files server computer.

To specify the locale setting for a vault:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **PDF Conversion** > **Word Files**.

3. In **Formatting Locale**, enter the language culture name.

   Enter the value as a Microsoft Windows language code identifier (LCID). For example, `fi-FI`, `en-US`, or `sv-SE`.

4. Click **Save** to save your configuration.

Number and date metadata fields in PDF conversions now use the new locale setting.

Specifying vault-specific date and time format for automatic values and notifications

You can specify a custom date and time format for automatic values (for example, properties that use simple concatenation of properties) and notifications.

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

To specify a custom date and time format for automatic values:

2. Expand **Properties** > **Format for Calculated Dates and Times**.

3. Use the **Date Format** and **Time Format** settings to specify the date and time format. For instructions and examples, select one of the settings and see the **Info** tab.

   Important: You must specify both settings. Otherwise, M-Files uses the locale settings of the server.

4. Click **Save**.

5. Optional: Use the **Recalculate** option to update the existing automatic values of a property.

To specify a custom date and time format for notifications:

6. In the advanced vault settings, expand **Notifications**.

7. Make sure that **Enable Vault Notifications** is set to **Yes**.
8. Use the **Custom Date Format** and **Custom Time Format** settings to specify the date and time format. For instructions and examples, select one of the settings and see the **Info** tab.

   Important: You must specify both settings. Otherwise, M-Files uses the locale settings of the server.
9. Click **Save**.

Preventing Linked Documents from Being Removed

If the user groups *All internal users* or *All internal and external users* do not have edit permissions on a linked document from an external file source, the document is removed from the external file source when it is added to M-Files.

This behavior can be prevented by making the following changes on the M-Files Server computer:

1. Add the following registry key and value:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer**
Value name	`IgnoreACLsForExternalLinks`
Value type	`REG_DWORD`
Description	Prevents linked documents from being removed from the external file source if document vault users do not have edit permissions to them.
Value	`1`

2. Use Windows Task Manager to restart the **MFServer** service:
   a) Right-click the taskbar and select **Task Manager**.

      ✓ The **Task Manager** window is opened.
   b) Open the **Services** tab.
   c) Right-click the **MFServer** service and select **Restart**.

Linked documents are now not removed from the external source even if document vault users do not have edit permissions to the linked documents.

To restore the default behavior, set the `IgnoreACLsForExternalLinks` value to `0`, and restart the M-Files Server service with Windows Task Manager.

Registry Setting for Extending Firebird Usability

Make the following changes on the M-Files server computer to extend Firebird usability in 64-bit installations:

1. Add the following registry entry:

Key	**HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer\Vaults\<vault GUID>**	
Value name	DBPageSize	
Value type	REG_DWORD	
Description	Changes the usable memory of the Firebird vault.	
Value	00004000	Sets the page file size at 16,384 bytes, which is the Firebird maximum. This increases the database memory allocation and use to two gigabytes.

2. Use Windows Task Manager to restart the **MFServer** service:
   a) Right-click the taskbar and select **Task Manager**.

      ✓ The **Task Manager** window is opened.

   b) Open the **Services** tab.
   c) Right-click the **MFServer** service and select **Restart**.

3. Run the **Optimize Database (Thorough)** operation for the vault (see Vault Maintenance for more information).

Settings for Vault Performance Measurement

The vault performance tests (see Measuring Vault Performance for further information) have predefined threshold times. The test results indicate if a test takes longer than the time specified by the threshold value. See below for instructions on modifying the threshold values for vault performance tests.

Defining the threshold time for the database insert speed test

The default threshold time for the database insert speed test is 6,000 milliseconds. You may modify the threshold time by completing the following steps on the M-Files server computer:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

      ✓ The advanced vault settings are shown.

2. Expand **Performance** > **Server Tests** > **Database Insert Speed**.

3. In the **Threshold** field, enter the threshold time for the database insert speed test in milliseconds.

4. Click **Save** to save your configuration.

Defining the threshold time for the network round-trip test

The default threshold time for the network round-trip test is 1,500 microseconds. You may modify the threshold time by completing the following steps on the M-Files server computer:

1. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

   ✓ The advanced vault settings are shown.

2. Expand **Performance** > **Server Tests** > **Network Round Trip**.

3. In the **Threshold** field, enter the threshold time for the network round-trip test in microseconds.

4. Click **Save** to save your configuration.

Setting M-Files Services to Use a Managed Service Account

You can set M-Files Server services to use a managed service account (MSA) or a group managed service account (gMSA). The account must have local administrator permissions on the server.

> **Important:** M-Files services normally use the **Local System account** for login. Use a different account only when you have a reason to do so. The **MFSetup** service must use the **Local System account**.

Do these changes before you install M-Files. If you have already installed M-Files, you can do the changes before you update M-Files to the latest version. If M-Files is already updated to the latest version, you must uninstall M-Files, do the changes, and install M-Files again.

To set the M-Files Server services to use a service account:

1. Open Registry Editor.

2. Refer to this table and add the required registry values:

Keys	• `HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\Common\Server\MFServer` • `HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\Common\Server\MFServerAux` • `HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\Common\Server\MFDataExport` • `HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\Common\Server\MFIndexingManager`
Value	• Name: `ServiceAccountName` • Type: `REG_SZ` • Content: `<domain>\<service account name>`

	- Example content: `testdomain\myMSA$`

Note: All the services in the table must use the same service account.

3. Install M-Files.
4. Use Windows Task Manager to restart the **MFServer** service:
   a) Right-click the taskbar and select **Task Manager**.

      ✓ The **Task Manager** window is opened.

   b) Open the **Services** tab.
   c) Right-click the **MFServer** service and select **Restart**.

These services now use the service account:

- M-Files Server
- M-Files Server Auxiliary Services
- M-Files Reporting Data Services
- M-Files Indexing Services

Enabling Cross-Origin Resource Sharing (CORS)

Web browsers cannot normally request resources from outside the domain where the resources are hosted. These Cross-Origin Resource Sharing (CORS) settings can be necessary if, for example, you have an application that uses the M-Files REST API to communicate with the vault.

Important: The use of CORS is a security relaxation. Before you continue, make sure that the risk is acceptable.

In M-Files Cloud, use Advanced Vault Settings to enable CORS. In an on-premises environment, you can use Advanced Vault Settings or Windows registry settings. With M-Files April '24 Update and later, it is recommended to use Advanced Vault Settings.

Enabling CORS with Advanced Vault Settings

Open Advanced Vault Settings and go to **Configuration** > **Client** > **Rest Api** > **Security And CORS**. Click the information icon (ⓘ) of each setting for details. Remember to enable CORS for all the necessary vaults.

To use this method in on-premises environments, incoming connections and vaults must be mapped. See Configuring Mappings Between Incoming Connections and Vaults.

Enabling CORS with registry settings

In an on-premises environment, you can enable CORS with Windows registry settings. To do this, add the keys and values given here to the Windows registry of the M-Files Web server:

Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFWA\Sites\<site name or ID in Internet Information Services>`
Value name	`EnableCrossOriginAccess`

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\`*`<version>`*`\Server\MFWA\Sites\`*`<site name or ID in Internet Information Services>`***
Value type	`REG_MULTI_SZ`

Value	A list of mappings that specify which origins have access to which vaults. On each row, specify the host name (DNS name) on the left side of the equals character. After the equals character, add the allowed origins separated with semi-colons. It is not recommended to use an asterisk (`*`) because it gives cross-origin access from all sites.
	Setting format for two vaults, hostnames separated by a line break:
	`<hostname 1>=<allowed origins separated with semicolons>`
	`<hostname 2>=<allowed origins separated with semicolons>`
	You can normally check the URL of the origin domains with your browser. For example, for SharePoint web apps, the format of the URL is `https://`*<domain identifier>–<instance identifier>*`.sharepoint.com`.

Example value	`https://sample-vault.cloudvault.m-files.com=https://mfiles-123asd.sharepoint.com;https://mfiles-098xcv.sharepoint.com`
	`https://aa-consulting.cloudvault.m-files.com=https://aa-consulting-123asd.sharepoint.com;https://aa-consulting-098xcv.sharepoint.com`
	`https://vaultXXX.cloudvault.m-files.com=https://mfiles-123asd.sharepoint.com`

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\`*`<version>`*`\Server\MFWA\Sites\`*`<site name or ID in Internet Information Services>`***
Value name	`AllowedCrossOriginHeaders`
Value type	`REG_SZ`
Description	The headers to be allowed in the response.
Value	`Origin,Content-Type,Accept,Access-Control-Allow-Origin,Cache-Control,X-Authentication,X-Requested-With,X-Vault,M-Files-Vault,m-files-session,m-files-extensions`

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\`*`<version>`*`\Server\MFWA\Sites\`*`<site name or ID in Internet Information Services>`***
Value name	`AllowedCrossOriginMethods`
Value type	`REG_SZ`
Description	The methods to be allowed in the response headers.
Value	`PUT,POST,GET,OPTIONS`

Microsoft Authentication Library (MSAL) with M-Files Mobile

You can use Microsoft Authentication Library (MSAL) with M-Files Mobile for authenticating to M-Files vaults. When MSAL is enabled, the M-Files Mobile applications use the library for authenticating to the vaults.

Note: You can use MSAL only with Microsoft Entra ID.

To enable MSAL:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Click **Federated Authentication**.
5. In the **Configuration** tab, expand **Scopes** > ***:Windows** > **Configurations** > **Configuration** > **Settings** > **Client**.

   Make a note that the name of the **Configuration** setting can come from automatic configuration and have a different name. For example, `AAD.MFGenerated`.
6. In **Show advanced options**, select **Yes**.
7. In **UseMicrosoftAuthenticationLibraryInMobile**, select **True**.

   For information about the setting, see the **Info** tab.
8. Click **Save**.

MSAL can now be used for authenticating to M-Files vaults in M-Files Mobile.

4. Frequently Asked Questions

This section deals with some of the most common questions related to the use of M-Files.

This section deals with some of the most common questions related to the use of M-Files. The questions have been divided into the categories below.

Daily use of M-Files

- Can I do the same stuff with M-Files Mobile as with M-Files Desktop and M-Files Web?
- How can I add a new item to a value list?
- How can I add a new property to a class?
- How can I create a document that is only visible to me?
- How can I create a new view in which the objects are displayed by customer?
- How can I find the documents I have created myself?
- How do I change the name of my computer without interfering with M-Files functionality?
- Why can't I edit a document that has been checked out?

Administration of M-Files

- How can I add a new item to a value list?
- How can I add a new user to a vault?
- How can I add a new property to a class?
- How do I change the login account of a user?
- How do I format the date in M-Files?
- How do I import e-mail messages from a specific IMAP folder?
- Why are there objects with the same ID in the vault?
- What is the difference between a user and a login account?
- Why does the intelligence service not extract metadata from some of the files?

Maintenance of M-Files

- How do I maintain the M-Files server machine?
- Why is my M-Files not as fast as it used to be?
- How do I migrate my document vaults to a new server?
- How do the automatic updates work?
- How much disk space do encrypting file data and taking backups require?
- How often should I make backups?
- How often should I reboot the M-Files server machine?
- What is not included in the backups?
- What kind of operations can I schedule to be run at specific intervals in M-Files?
- How do I check the full version number of M-Files Desktop and M-Files Server?
- How do I save a copy of M-Files errors in the Windows Application event log

Common problems for document vault users

- Why can't I access the document vault?
- Why can't I convert a document to PDF format or annotate a document?
- Why can't I find the Checked Out to Me view?
- Why can't I save an email message as an Outlook message to M-Files?
- Why did a file with a grayed-out icon appear on the M-Files drive when I saved a new document in Microsoft Word?
- Why do document timestamps have the wrong time?

General questions

- Where can I find more information when I need it?
- What are the hardware requirements and recommendations?
- What's new in this M-Files version?
- How do the automatic updates work?
- Can I use M-Files programmatically?
- How do I write VBScript code for M-Files purposes?
- What is the difference between a named access control list (NACL) and a user group?

In this chapter

4.1. Daily Use of M-Files

This section contains frequently asked questions related to the daily use of M-Files.

In this chapter

4.1.1. Can I do the same stuff with M-Files Mobile as with M-Files Desktop and M-Files Web?

Refer to the document M-Files Client Feature Comparison for a comprehensive list of features available in each M-Files client.

4.1.2. How can I add a new item to a value list?

You can use the **Add Value** button in the toolbar when you work with the metadata card. This function is available only if it has been specified in the value list properties that end 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**. Click **Contents** > **New Item**. If you do not have administrator rights, check with the system administrator that **Allow users to add new values to this list** is enabled in the properties of the value list.

If the value list is based on an object type, new values are added to the list when new objects of that type are created in the M-Files clients.

4.1.3. 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 click **Add property** on 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 are an M-Files system administrator and 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).

4.1.4. 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.

4.1.5. How can I create a new view in which the objects are displayed by customer?

1. In the classic M-Files Desktop, click the **All** tab.
2. Click the **Create** (⊕) button.
3. Select **View**.
4. In **Name**, enter a descriptive name for the view. For example, `Customers`.
5. Click **Add**.

   ☑ The **Define Grouping Level** dialog is opened.
6. Use the **Property** drop-down menu to select the **Customer** property.
7. Click **OK** to close the **Define Grouping Level** dialog.
8. Click **OK** to close the **Define View** dialog.

Your new view is now listed in the **My Views** section.

For more information about views, see Using Views.

4.1.6. How can I find the documents I have created myself?

You can search for documents based on certain specifications with the **Additional Conditions** dialog.

1. Click the **Search options** button (☰) and then click the **Additional Conditions...** button.
2. Open the **Properties** tab.
3. Click the **Add Condition** button.
4. Specify **Created by** as the property, select the equals sign (=) as the operator, and your login account as the value.
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. For more information, see Property-Based Conditions and Creating a View.

4.1.7. How do I change the name of my 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.

4.1.8. 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.

Sending a check-in request

You can also send a check-in request to the user who has checked out a document: Right-click the document and select **Send Check-in Request**. The user gets an email message about the request. The message also contains a link to the document. The check-in request is sent to the email address associated with the user's login account.

4.1.9. How does the duplicate detection feature work?

If you try to save a file that is already in the vault, M-Files lets you know. M-Files shows you the duplicate documents to which you have permissions.

M-Files compares only the file content of the documents. Thus, their metadata can be different. For example, the duplicate documents can have a different name, version history, permissions, and workflow.

The feature does the comparison on a binary level with MD5 checksums. M-Files shows duplicate file content for documents that have the same MD5 value.

Note: In some cases, the MD5 value can be different even when the file content of the compared documents is the same. This happens because some files formats store additional metadata in the file which changes the MD5 value.

4.2. Administration of M-Files

This section contains frequently asked questions related to the administration of M-Files.

In this chapter

4.2.1. How can I add a new item to a value list?

You can use the **Add Value** button in the toolbar when you work with the metadata card. This function is available only if it has been specified in the value list properties that end 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**. Click **Contents** > **New Item**. If you do not have administrator rights, check with the system administrator that **Allow users to add new values to this list** is enabled in the properties of the value list.

If the value list is based on an object type, new values are added to the list when new objects of that type are created in the M-Files clients.

4.2.2. How can I add a new user to a vault?

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Users**.
6. Click **New User** on the task area.

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

7. Use the **Login account** drop-down menu to select a login account for the new user.

   The *Login account* drop-down menu lists all login accounts that have not been added to the document vault. If you want to create an entirely new login account, see Login Accounts.

8. Specify the permissions for the user and then click **OK**.

The new user is added to the document vault.

Note: For further instructions, see Creating a User.

4.2.3. 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 click **Add property** on 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 are an M-Files system administrator and 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).

4.2.4. How do I change the login account of a user?

Sometimes it can be necessary to change the login account for a user. For example, when a user's last name has changed or when login accounts are moved between domains. To keep the user history and the user's personal settings in the vault, do not delete the vault user. Instead, change its login account where necessary. For the differences of these two, see the descriptions of login account and user.

In the M-Files June '24 Update and later, the events that are related to users also include a user account ID. The user account ID stays the same even when the account name is changed.

Important: Changing login accounts when users are synchronized from Microsoft Entra ID

If new login accounts are synchronized from Entra ID, M-Files automatically creates new users for the new login accounts. To associate the new login account with the correct existing user, you must first delete the new, automatically created user. Before you do this, make sure that the user has not used the automatically created user account. Otherwise, user settings and history are lost.

Before you begin, make sure that the new login account has been created in M-Files. To change a login account of a user:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Users**.

   ✓ The **Users** list is opened in the right-side pane.
6. Right-click the user whose login account you want to change and select **Properties**.
7. In the **User Properties** dialog, use the **Login account** drop-down menu to select a new login account for the user.
8. Click **OK**.

The new login account is now associated with the existing user. When the user logs in with the new user credentials, their previous user history and personal settings in the vault are available.

4.2.5. How do I format the date in M-Files?

The **Date** data type of a property is used to show a date and time as a property value. To change the format, change the date and time format settings of the client computer's operating system.

Note: These instructions are for Windows 10, but the procedure is highly similar for other Windows versions.

Do these steps on the M-Files client computer to change the date format:

1. Right-click the Windows Start button and select **Settings**.
2. Select **Time & language** > **Region** > **Additional date, time, & regional settings**.

   ✓ The **Clock and Region** window is opened.
3. In **Region**, click **Change date, time, or number formats**.

   ✓ The **Region** dialog is opened.
4. On the **Formats** tab, click **Additional settings**.

   ✓ The **Customize Format** dialog is opened.
5. Open the **Time** tab and enter a format to **Short time**.

6. Open the **Date** tab and enter a format to **Short date**.
7. Click **OK** to close the **Customize Format** dialog.
8. Click **OK** to close the **Region** dialog.

All the properties that use the Date data type now use the format that you have specified here.

How do I format the date on the M-Files server computer?

Many M-Files Server operations use date and time information. For example, script executions and PDF conversions. The date and time settings of the M-Files server computer's system account specify how dates and times are formatted in such operations.

> **Tip:** If you cannot change the locale settings of the server computer, you can use these instructions to override the server's locale settings: Specifying vault-specific date and time format for automatic values and notifications. This can be useful, for example, when you use M-Files Cloud.

Do these steps on the M-Files server computer to change the date and time format:

1. Right-click the Windows Start button and select **Settings**.
2. Select **Time & language** > **Region** > **Additional date, time, & regional settings**.

   ✓ The **Clock and Region** window is opened.
3. In **Region**, click **Change date, time, or number formats**.

   ✓ The **Region** dialog is opened.
4. On the **Formats** tab, click **Additional settings**.

   ✓ The **Customize Format** dialog is opened.
5. Open the **Time** tab and enter a format to **Short time**.
6. Open the **Date** tab and enter a format to **Short date**.
7. Click **OK** to close the **Customize Format** dialog.
8. Open the **Administrative** tab.
9. Click **Copy Settings**.
10. Enable **Welcome screen and system accounts**.
11. Click **OK** to close the dialog.
12. Click **OK** to close the **Region** dialog.

All dates and times generated by the M-Files server computer now use the format that you have specified in the steps here.

4.2.6. How do I import e-mail messages from a specific IMAP folder?

M-Files allows you to automatically import email messages from a specific email folder on an IMAP server to a vault. To do this, use the Connections to External Sources function in M-Files Admin and specify a new connection to a mail source.

For instructions on specifying a connection to an IMAP email server, see Mail Sources.

4.2.7. What is the difference between a user and a login account?

The concepts of a user and a login account are both integral parts of M-Files, but there is an important difference between them:

- Users are vault-level objects that store user-specific settings and user history as well as permissions for performing certain operations in a vault. A user object is always linked to one and only one 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.

Example

A&A Consulting hires a new engineer, Amanda Reade, and she naturally needs to have access to the M-Files vaults of the company.

1. The M-Files administrator of the company creates the login account *AmandaR* in M-Files Admin.

    - Amanda can now be authenticated to M-Files Server.
2. The administrator creates the vault user *AmandaR* to all the appropriate vaults.

    - Amanda now has access to the vaults specified by the administrator.

As a result, the login account *AmandaR* is linked to all the newly created users, and the vault user *AmandaR* in all the appropriate vaults is linked to the said login account. The new engineer now also has access to all the required M-Files vaults.

4.2.8. Why are there objects with the same ID in the vault?

Object IDs are object type specific. This is why it is relatively common for many objects in the vault to have the same ID. For example, it is normal for a **Project** object and **Employee** object to have the same ID.

Sometimes, however, even two objects of the same type can seem to have the same ID. This can occur because the display ID shown on the metadata card can get its value from different types of identifiers used in M-Files. This page tells you about these identifiers and how they are used as the object's display ID.

The M-Files vault identifies an object with – and uses as the object's display ID – one of these identifiers:

Identifier type	Description
Internal ID	Each object in the vault has an internal ID. Internal ID is unique to each object per object type in a vault. When you refer to an object in a vault, for example in a script, you must refer to it with its internal ID.
Original ID	An original ID is used when an object is replicated from another vault. The original ID contains the internal ID that the object has in the vault in which it was created. In addition to the original ID, the replicated object gets a new internal ID in the target vault.
External ID	Objects imported from an external database have an external ID. The object is identified with this identifier in the external database. In addition to the external ID, the object has an internal ID in the vault.

The display ID gets its value from one of these IDs in this order of priority:

1. External ID
2. Original ID
3. Internal ID

In other words:

- If an object has an external ID, it is shown as the object's ID on the metadata card.
- If an object has an original ID but no external ID, the original ID is shown as the object's ID on the metadata card.
- If an object has no external or original ID, the internal ID is shown as the object's ID on the metadata card.

Note: You can use the `%INTERNALID%` placeholder for a property of the **Text** data type to add the internal ID to the object metadata as an automatic property value. For instructions, see Specifying an Automatic Value for a Property and Simple concatenation of properties.

4.2.9. Why does the intelligence service not extract metadata from some of the files?

In some situations, intelligence services such as M-Files Information Extractor are unable to produce metadata suggestions based on the content of certain files. The issue may be caused by the simple fact that M-Files Server is not able to read the file content, and therefore not able to provide the content to the intelligence service for analysis.

You may come across this kind of issue, for example, if your organization uses password-protected PDF files. If opening the PDF file without a password or copying content from it is restricted in the security settings of the PDF file, M-Files will not be able to access the file content. For more information about password-protected PDF files, see this Adobe article.

4.3. Maintenance of M-Files

This section contains frequently asked questions pertaining to the maintenance of M-Files.

In this chapter

4.3.1. How do I maintain the M-Files server machine?

The information on this page applies to an on-premises installation. The M-Files system administrator must do these maintenance tasks on the M-Files server machine to maintain its operational efficiency.

Frequency	Task
Daily	Checking Windows Event Logs
Weekly	Clearing Replication Conflicts
Monthly	Verifying Resource Usage
Quarterly	Verifying the integrity of master database backups and vault backups. See Maintenance recommendations for on-premises vaults.
Biannual	Manual Optimization Using Verify and Repair
Annual	Archiving M-Files Event Logs Cleaning the vaults

Follow the links for further instructions on carrying out a specific task.

In this chapter

- Using Verify and Repair
- Archiving M-Files Event Logs

Checking Windows Event Logs

Check events related to M-Files in the Windows event log on a regular basis for any issues, especially ones pertaining to backups. You might want to also consider using a PowerShell script or a third-party application for sending e-mail notifications when aforementioned events occur.

1. Press ⊞ Win + R on the M-Files server computer.

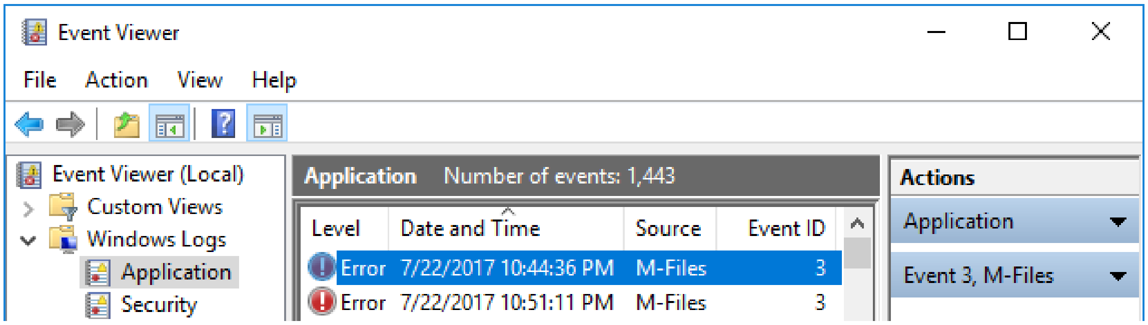
   ✓ The **Run** dialog is opened.

2. In the **Open** text field, type in `eventvwr` and click **OK**.

   ✓ Event Viewer is opened.

3. Expand the **Windows Logs** node.
4. Select the **Application** node.

   ✓ The application log is displayed:



Level	Date and Time	Source	Event ID
Error	7/22/2017 10:44:36 PM	M-Files	3
Error	7/22/2017 10:51:11 PM	M-Files	3

5. Click **Filter Current Log...** on the **Actions** pane in the **Application** section to list only the entries that are related to M-Files.

   ✓ The **Filter Current Log** dialog is opened.

6. In the **Event sources** drop-down menu, select all the applications related to M-Files, such as **M-Files**, **M-Files Compliance Kit**, and **MFClient**.
7. Click **OK** to close the **Filter Current Log** dialog.

The application event log should now list only the entries that are related to M-Files.

> **Note:** If the disk space on the server computer allows, we recommend expanding the maximum log size of the **Application** log to, for instance, 200,000 KB to cover more events. In some error cases, a large number of events may be recorded to the log, thus filling the default log size of about 20 MB very quickly. This may make it impossible to track down the origin of the issue. You can change the log size by right-clicking the **Application** node in the left-side tree view and then selecting **Properties** from the context menu. Expanding the log size of the client computers is rarely needed, but may be of use in some cases.

Verifying Resource Usage

It is important to keep track of how much resources are needed to run the M-Files system. If the resource consumption reaches certain thresholds, it might be time to consider upgrading your system. See also System Requirements and Technical Details for the hardware and system operating requirements.

Monitor at least the following resource components:

- vault metadata and file data size

  Note: You can check the location of the metadata file and the file data folder in the **Document Vault Properties** dialog in M-Files Admin. See Checking the Size of a Firebird Metadata File for detailed instructions.
- memory
- disk space and health
- backup size and duration (should not overlap with optimization)

Clearing Replication Conflicts

Regularly verify that all your scheduled replication tasks produce the expected results and that there are no replication conflicts in any of the vaults. For instructions on how to find and resolve replication conflicts, see Conflicts and their resolution.

Clear replication conflicts at least once a week, but it is a good idea to appoint a user to check the conflicts every day.

Manual Optimization

If your organization uses Microsoft SQL Server as the database engine and you store the file data in a file system folder (instead of the vault database), manually run the **Optimize Database (Thorough)** operation from one to four times a year. This is the only way to remove any destroyed files from the file data server in this type of setup. Run the operation also after an exceptionally large number of files have been destroyed at once, for example after files are archived to another vault.

Note: Make sure that the optimization is not done between file data and metadata backups.

Note: It is possible that Firebird and Microsoft SQL Server vaults are taken offline for the duration of the operation. Before you run the operation for Firebird vaults, make sure that the server has at least three times the amount of hard disk space required by the metadata file of the vault. For instructions on how to check the size of the vault metadata file, see Checking the Size of a Firebird Metadata File.

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Right-click a vault.
5. Click **Maintenance** > **Optimize Database (Thorough)**.
6. Enable **Delete the files of destroyed objects**.

   This option is available only when the files are in the file system and the vault uses Microsoft SQL Server.

Note: If this option is enabled and the vault uses dtSearch, the vault will be taken offline.

7. Click **Yes** at the prompt.

The database of the selected vault is optimized.

Note: Depending on the size of the vault, the operation can take an extensive amount of time to complete.

Using Verify and Repair

Verify and Repair does these checks:

- Makes sure that the database is intact.
- Makes sure that all the data has been saved correctly to M-Files.
- Makes sure that the file sizes and the file checksums of the physical files in the vault file data location match those reported by the metadata database.

Verify and Repair (Quick) checks for metadata inconsistency issues and makes sure that the files for the objects are present with the correct size and status.

Verify and Repair (Thorough) does also file integrity checks for the file data. More specifically, the operation calculates checksums and makes sure that delta files can be reconstituted. See important information for details.

Recommendations

Do the **Verify and Repair (Quick)** operation in these situations:

- Two or three times a year.
- Before you migrate a vault from Firebird to Microsoft SQL Server.
- Before you migrate a vault to M-Files Cloud.
- Before a server upgrade when you do not use automatic updates.
- Before you do large changes to the environment.

  - For example, changes to server hardware or upgrades of the server operating system.
- When the vault does not operate normally.

Important information

Before you start, read the information in this section carefully.

In most cases, use the **Verify and Repair (Quick)** operation.

- Use the thorough operation only if you have a reason to suspect that the contents of the data files are corrupt. This can be, for example, because your antivirus software has changed the data.
- The thorough operation takes considerably longer than the quick operation.
- Before you start a thorough check, it can be useful to temporarily disable the weekly **Optimize Database (Thorough)** operation in scheduled jobs. The optimization job can take the vault offline and interrupt the verify and repair operation.

Reported errors

In the **Verify Document Vault** report dialog, if you see errors that cannot be repaired automatically:

- Create a support case in M-Files Support Portal or contact your M-Files reseller immediately. Please provide the full contents of the report dialog and the full version number of your M-Files Server software.
- Do not try to repair the errors yourself.
- Do not click **Yes** in the dialog to let M-Files try to repair the errors.

Errors that cannot be repaired automatically are explicitly marked in the list of errors. When M-Files support has fixed the errors, start the verify and repair operation again.

Errors in automatic repair process

In the **Verify Document Vault** report dialog, if there are only issues that M-Files can fix automatically, click **Yes**. If the process ends with an error, create a support case in M-Files Support Portal or contact your M-Files reseller immediately.

Do the steps given here only if M-Files support tells you to do so:

a) Open Advanced Vault Settings.
b) Go to **Database** > **Verification**.
c) Set **Take the Vault Offline** to **Yes**.

It can be useful to set this to **No** after the process.

d) Start the **Verify and Repair (Quick)** operation again.

Operation duration and interruptions

- The vault can be used when the operation searches for issues.
- If the vault is taken offline, the operation is interrupted. For example, the weekly thorough optimization or other maintenance breaks (such as installation of vault applications) can cause this.
- The operation can be long. The length of the operation is mainly dependent on these factors:
  - Size of the file data database
  - Number of files in the vault
  - Number of object versions in the vault
  - Performance of the server machine
- In very large vaults, the operation can time out. For more information, see this article: Verify and Repair Times Out Due to Communication Failure.

Starting the Verify and Repair operation

To start the operation:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Right-click a vault.
5. Select **Maintenance** > **Verify and Repair (Quick)**.

   It is rarely necessary to do the thorough operation. See this information.

M-Files checks the vault for errors. See this information for instructions on how to repair errors.

Archiving M-Files Event Logs

If your organization uses unlimited event logs (see The Electronic Signatures and Advanced Logging module), it is a good idea to archive M-Files event logs once or twice per year. If you also have M-Files Compliance Kit installed, you can do this automatically with the Log Exporter module. For more information, refer to Compliance Kit - Log Exporter - Functional Description.

If The Electronic Signatures and Advanced Logging module and Advanced Event Log features are not in use, M-Files Server removes the oldest events when the number of events is close to the specified maximum.

To export all the events in the event log manually:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Select **Event Log**.
6. In the task area, click **Export**.
7. Click **Export All Events**.

   ✓ The **Browse For Folder** dialog is opened.
8. Select the folder to which you want to export the events and click **OK**.

   ✓ The **Confirm Delete** dialog is opened.
9. Click **Delete** to delete the exported events from the event log.

The events from the M-Files event log are archived in the selected location as an XML file.

4.3.2. Why is my M-Files not as fast as it used to be?

If M-Files users are experiencing noticeable performance issues in their day-to-day use of M-Files, carry out the procedures outlined below to pinpoint the potential source or sources of the problem. System slowness may be caused by various factors, such as hardware or infrastructure issues, vault structure or periodic maintenance operations, or issues related to opening views or files, and so on.

When you contact our support about performance issues, it is best to attach these details to your request:

- Windows application event log copy for M-Files events (see How do I save a copy of M-Files errors in the Windows Application event log for instructions)
- An export of Server Activity Monitor data in M-Files Admin
- Screenshot of the Windows Task Manager tab displaying CPU and RAM usage
- Page file information
- Hardware specifications of the servers

Performance issues caused by factors related to hardware or infrastructure

Performance issues may be caused by hardware or infrastructure related problems. Inspect the following performance counters on the M-Files Server computer as well as the Microsoft SQL Server computer (if they are separate servers):

- The page file usage: Use Performance Monitor to check the current and peak page file usage. Note that Windows always uses the page file no matter how much RAM you have, but if the page file peak usage is higher than around 10 percent, it may indicate that the system is at least periodically low on RAM or that RAM usage is excessive. See Inspecting Page File Usage in Performance Monitor for instructions on checking page file usage.
- Current RAM usage in Windows Task Manager.
- The CPU load in Windows Task Manager: If the load spikes close to 100 percent, the system may be under-resourced or some of the processes may be hoarding excessive amounts of resources.
- The network connectivity between the server computers if M-Files Server and Microsoft SQL Server are running on separate servers. Network latency between the servers may cause noticeable slowness for the end users. We recommend M-Files Server and Microsoft SQL Server to be used in the same subnetwork to reduce latency.
- Make sure the Microsoft SQL Server instance has been assigned a memory limit. It should be set high enough to provide as much RAM for the SQL Server as possible but low enough to prevent the system from swapping. In general, leave from 3 to 4 GB for the host operating system and its services, and if M-Files Server runs on the same system, allocate from 2 to 3 GB for it and other processes. See Changing the Memory Limit for a Microsoft SQL Server Instance for instructions on setting the memory limit for the Microsoft SQL Server instance.

  Note: These values are approximates and depend on multiple factors, such as the number of vaults, the use of server side vault applications, and so on.

Performance issues caused by vault structure or periodic maintenance operations

System slowness may also be caused by issues in the vault structure, and periodic maintenance operations may be perceived as performance issues by the end user.

The following factors related to vault structure or maintenance operations can cause (temporary) system slowness:

- The metadata of the vault may not be optimal. There should not, for instance, be value lists with tens of thousands of entries or classes with hundreds of obligatory properties.
- Modifying named access control lists causes the permissions of every affected document to be updated and may thus induce temporary system slowness.
- Running background jobs like optimizations and backups may cause temporary slowness. These operations should not be run during high usage hours.
- A large number of export and import jobs running at short intervals can cause performance issues.
- A large number of connections to external sources that synchronize at short intervals can cause performance issues.
- The event log in M-Files Admin may be used to reveal instances of exceptional vault use, such as excessive number of file downloads.
- For Firebird vaults, the metadata file size should be no larger than 2 GB per vault. See Registry Setting for Extending Firebird Usability for instructions on defining the maximum metadata file size and Checking the Size of a Firebird Metadata File for instructions on checking the metadata file size.

Performance issues in opening views or performing searches

Do these checks to verify if system slowness occurs in conjunction with opening views or performing searches:

1. Use M-Files Desktop on the M-Files server computer and use *Local Procedure Call* as the protocol for connecting to the vault to rule out potential network-related issues. See Adding a Vault Connection for instructions on defining the vault connection and using *Local Procedure Call* as the protocol.
2. Log in to the vault as a normal user, not as administrator, so that permission checks are not bypassed when using the vault and thus you can verify whether or not the issue is related to permission checks.
3. Try to change the properties of a view, and then press ⇧ Shift + F5 to fully refresh the view. Try to modify different properties of views, such as filters or grouping levels, to see if the problem is related to views.

   Note: You can create a copy of an existing view so that you do not need to change the properties of the original view. Right-click a view of your choice and select **Copy** from the context menu, then right-click on an empty space in the listing area and select **Paste** from the context menu.

In this chapter

How do I save a copy of M-Files errors in the Windows Application event log

Note: These instructions are for Windows 10, but the procedure is highly similar for other Windows versions.

If every M-Files user in your organization is experiencing the same issue, it is recommended to save a copy of the application event log on the M-Files server computer. If the issue is an isolated one, on the other hand, you should only save a copy of the log on the computer where the issue occurs. Complete the steps below on the appropriate computer.

1. Right-click the **Start** icon and select **Event Viewer** from the context menu.

   ✓ The **Event Viewer** window is opened.

2. Expand **Windows Logs**.

3. Click **Application**.

4. Click **Filter Current Log** on the **Actions** pane.

   ✓ The **Filter Current Log** dialog is opened.

5. Open the **Event sources** drop-down menu and select *M-Files* and any other applications related to M-Files, such as *M-Files Compliance Kit* or *MFClient*.

6. Click **OK** to close the **Filter Current Log** dialog.

7. Click **Save Filtered Log File As** on the **Actions** pane.

8. Specify a location and a file name, and then click **Save**.

A copy of the filtered application event log is saved to the location that you have specified. The copy contains only the errors that are related to M-Files.

Inspecting Page File Usage in Performance Monitor

Do the following steps to inspect page file usage in Performance Monitor:

1. In the Windows start menu, open **Administrative Tools**
2. Open **Performance Monitor**.
3. Expand **Monitoring Tools**.
4. Click **Performance Monitor**.
5. Right-click on the graph and select **Add Counters...** from the context menu.

   ✓ The **Add Counters** dialog is opened.
6. From the **Available counters** list, select *Paging File*.
7. Click on the down-arrow icon to the right of *Paging File*.
8. Select **% Usage** under *Paging File* and then click the **Add** button to add the counter on the **Added counters** list.
9. Click **OK** to close the **Add Counters** dialog.

Changing the Memory Limit for a Microsoft SQL Server Instance

To change the memory use of a Microsoft SQL Server instance:

1. Open Microsoft SQL Server Management Studio.
2. Log in to your server.
3. In Object Explorer, right-click a server and select **Properties**.

   ✓ The **Server Properties** dialog is opened.
4. Click the **Memory** node.
5. In **Server memory options**, enter values to the **Minimum server memory** and **Maximum server memory** fields.
6. Click **OK** to close the **Server Properties** dialog.

Guidelines for Microsoft SQL Server Memory Limit

If Microsoft SQL Server memory consumption is not limited, Microsoft SQL Server can use a large amount of memory and the server can after some time start to use virtual memory. This can cause performance issues and other problems.

The best practice is to set the Microsoft SQL Server memory limit so that the operating system does not use the paging file in normal operation. It is usually better to set the memory limit too low than too high. In most environments, you must keep at least 2 GB memory free for the operating system. In systems with more available memory, leave more capacity for the operating system.

There are many things that have an effect on the applicable memory limit. You can, for example, monitor the system behavior to find the correct memory limit.

Examples

If Microsoft SQL Server is used on a dedicated server and the server machine has 8 GB of memory, set the Microsoft SQL Server memory limit to 5 or 6 GB.

If Microsoft SQL Server is used on a server that does also other tasks, make sure that there is enough free memory for other applications. If M-Files Server is used on the same server, decrease the memory limit 1 to 2 GB more. For example, if the server machine has 8 GB of memory and M-Files Server is not in heavy use, the applicable Microsoft SQL Server memory limit is 3 or 4 GB.

Checking the Size of a Firebird Metadata File

The metadata file of a Firebird vault is by default stored under the following location on the server computer:

```
C:\Program Files\M-Files\Server Vaults\<vault name>\MetaData
```

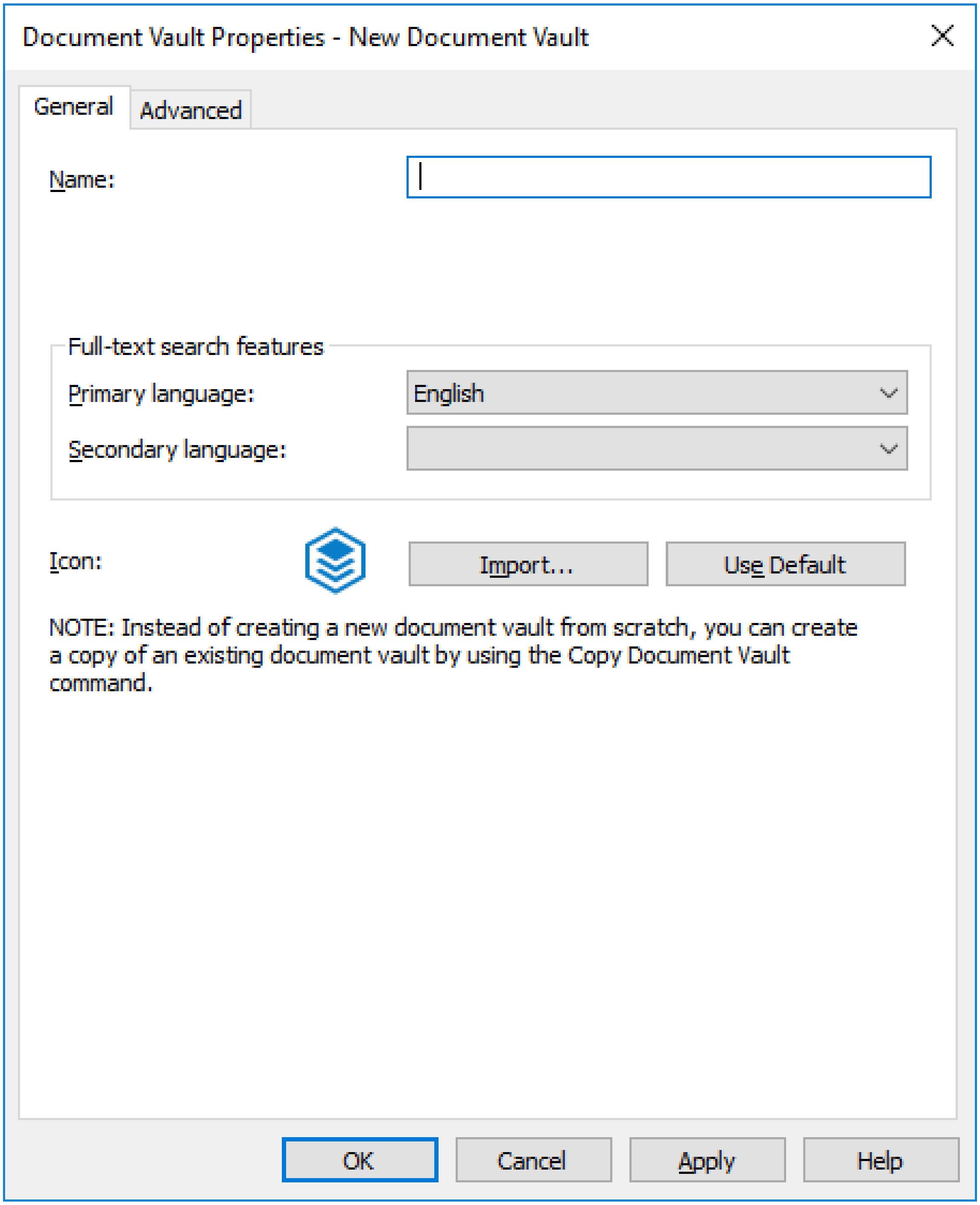
We recommend that you start to plan migration to Microsoft SQL Server when the size of the metadata file for a vault is close to 1 GB.

Tip: You can change the amount of usable memory of a Firebird vault to two gigabytes. See Registry Setting for Extending Firebird Usability.

Do the following steps to check the size of the metadata file:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Right-click a vault.
4. Click **Properties**.

   ✓ The **Document Vault Properties** dialog is opened.



Document Vault Properties - New Document Vault

Name:

Full-text search features

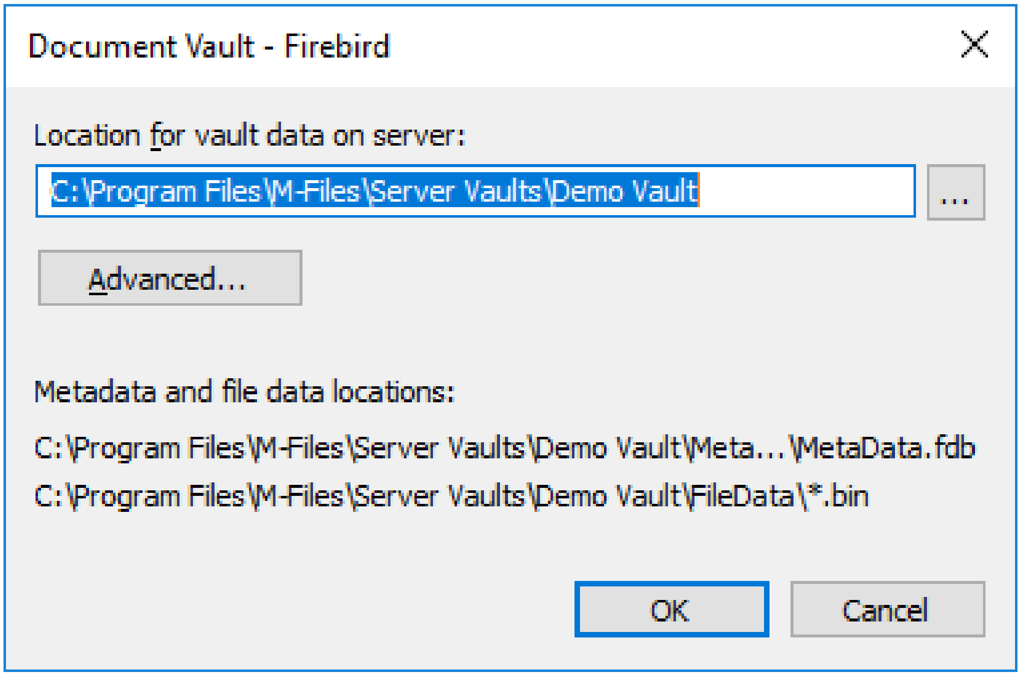
Primary language: English

Secondary language:

NOTE: Instead of creating a new document vault from scratch, you can create a copy of an existing document vault by using the Copy Document Vault command.

5. Open the **Advanced** tab.
6. Under the **Use Firebird** option, click the **Define...** button.

   ✓ The metadata file location along with the file data location is shown at the bottom of the dialog.



Document Vault - Firebird

Location for vault data on server:

C:\Program Files\M-Files\Server Vaults\Demo Vault

Metadata and file data locations:

C:\Program Files\M-Files\Server Vaults\Demo Vault\Meta...\MetaData.fdb
C:\Program Files\M-Files\Server Vaults\Demo Vault\FileData\*.bin

7. Open the metadata file folder you have located in the previous step and select the metadata file.
8. Check the file size in the status bar.

4.3.3. How do I migrate my document vaults to a new server?

When migrating document vaults to a new server, use the same version of M-Files on both the old and the new server. If you need to upgrade M-Files in conjunction with the migration, upgrade M-Files on the new server only after the migration is complete and you have verified that the document vaults are functional on the new server.

Migrating document vaults to a new server when using Firebird as the database engine

If your document vaults use Firebird, complete the following steps to migrate the vaults to a new server:

1. Make sure there are no documents checked out on any workstation.

   You may create a view that contains all the documents that are currently checked out in the vault by using the **Checked out** status filter for a view.

   For instructions on specifying a view, see Creating a View.

2. Take the vaults offline.

   For instructions, see Taking a Vault Offline.

3. Back up the master database and copy the backup file to the new server computer.

   For instructions, see Backing Up the Master Database.

4. Take full backups of your document vaults and copy the backup files to the new server computer.

The backup files contain file data regardless of whether the file data is stored in the default location, or in a separately specified location, so there is no need to copy the file data separately.

For instructions, see Backing Up a Vault.

5. Install M-Files to the new server computer:
   a) In the M-Files Setup wizard, click **Next**, select **I accept the license agreement**, and then click **Next** again.
   b) Select the **Evaluation installation** option.

      By selecting the **Evaluation installation** option, you do not have to install a license on the new server because the existing license is taken into use when you restore the master database.
   c) Complete the installation.
6. Open M-Files Admin on the new server computer.
7. Restore the master database.

   For instructions, see Restoring the Master Database.
8. Restore the document vaults from the backups using the option **Restore using original identity**.

   Pay attention to file data locations when restoring the vaults. If in doubt, check the settings on the old M-Files server.

   For instructions, see Restoring a Vault.
9. Copy the search indexes from the old server computer to the new one:
   a) In M-Files Admin, in the left-side tree view, right-click a vault and select **Properties**.
   b) Open the **Advanced** tab, and then click **Define**.

      By default, the `Indexes` folder can be found under the location specified in the **Location for vault data on server** field.

      In larger vaults, the search indexes might be placed in an alternate location. Check the index location according to the instructions in How do I check the location of the active search indexes?.
   c) Copy the `Indexes` folder to the new server for each vault that you want to migrate.
10. Optional: Specify notification settings if you wish to enable notifications.

    For instructions, see Editing Notification Settings in M-Files Admin.
11. Specify backup jobs and update the backup file locations if necessary.

    For instructions, see Scheduled Backup Jobs.
12. Stop and disable the M-Files Server service on the old server computer to make sure no users accidentally connect to it in the future.
13. Either:

a. If you are using a DNS alias for your M-Files Server, update the alias to point to the new server computer. This way you do not have to distribute new vault connection settings to client computers.

   or

b. Edit the document vault connection settings on the client computers so that they connect to the new server address. For instructions, see Adding a Vault Connection.

14. Make sure that any external systems that point towards M-Files use either the DNS alias, or the DNS name or IP address of the new M-Files server.

15. Disconnect the old server computer.

Migrating document vaults to a new server when using Microsoft SQL Server as the database engine

The instructions assume that Microsoft SQL Server is not changed during the migration. If Microsoft SQL Server is installed on the same computer as M-Files Server and therefore also requires migration, see Migrating the Vault Database from One Microsoft SQL Server to Another for further instructions. It does not matter whether you migrate M-Files Server before migrating the document vaults or the other way around.

If your document vaults use Microsoft SQL Server, complete the following steps to migrate the vaults to a new server:

1. Make sure there are no documents checked out on any workstation.

   ⓘ You may create a view that contains all the documents that are currently checked out in the vault by using the **Checked out** status filter for a view.

   For instructions on specifying a view, see Creating a View.

2. Take the vaults offline.

   ⓘ For instructions, see Taking a Vault Offline.

3. Back up the master database and copy the backup file to the new server computer.

   ⓘ For instructions, see Backing Up the Master Database.

4. In Microsoft SQL Server Management Studio, take full backups of your document vaults as a precaution.

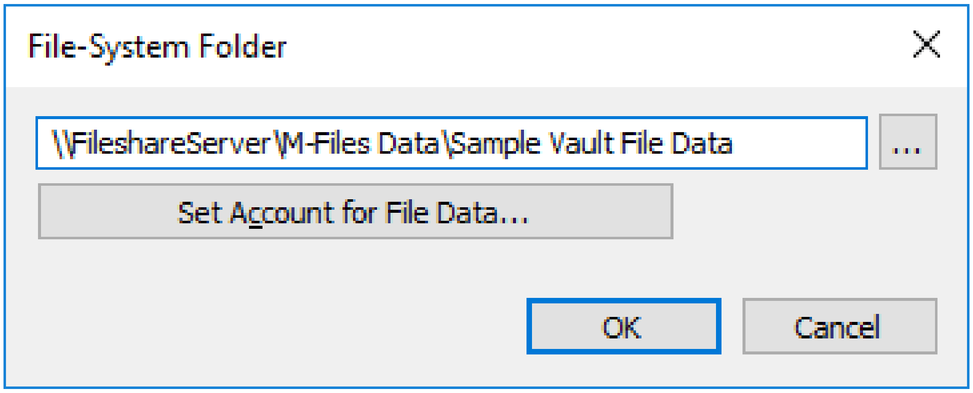
5. If the file data is stored on the file system, complete the following steps:

   a) In M-Files Admin, in the left-side tree view, right-click a vault and select **Properties**.
   b) Open the **Advanced** tab and click **Define**.
   c) Click **File Data Location**.

      ☑ The **File Data Location** dialog is opened.

   d) Click **Define**.

      ☑ The **File-System Folder** dialog is opened.



File-System Folder

\\FileshareServer\M-Files Data\Sample Vault File Data

e) Using File Explorer or any other file managing application, copy the file data folders from the location shown in the **File-System Folder** dialog to the new server computer or network share.

6. Attach the document vaults to the new server in M-Files Admin using the original identities of the vaults.

   If the file data is stored on the file system, make sure to specify the correct file data location when attaching the vaults.

   For instructions, see Attaching a Vault and Changing the Location of the Vault File Data for Microsoft SQL Server.

7. Copy the search indexes from the old server computer to the new one:

   a) In M-Files Admin, in the left-side tree view, right-click a vault and select **Properties**.

   b) Open the **Advanced** tab and click **Define**.

      By default, the `Indexes` folder can be found under the location specified in the **Location for secondary data on the M-Files server** field.

      In larger vaults, the search indexes might be placed in an alternate location. Check the index location according to the instructions in How do I check the location of the active search indexes?.

   c) Copy the `Indexes` folder to the new server for each vault that you want to migrate.

8. Optional: Specify notification settings if you wish to enable notifications.

   For instructions, see Editing Notification Settings in M-Files Admin.

9. Specify backup jobs and update the backup file locations if necessary.

   For instructions, see Scheduled Backup Jobs.

10. Stop and disable the M-Files Server service on the old server computer to make sure no users accidentally connect to it in the future.

11. Either:

    a. If you are using a DNS alias for your M-Files Server, update the alias to point to the new server computer. This way you do not have to distribute new vault connection settings to client computers.

       or

    b. Edit the document vault connection settings on the client computers so that they connect to the new server address. For instructions, see Adding a Vault Connection.

12. Make sure that any external systems that point towards M-Files use either the DNS alias, or the DNS name or IP address of the new M-Files server.

13. Disconnect the old server computer.

Additional configuration required for the classic M-Files Web

If M-Files Web is installed on the M-Files application server, you need to install Internet Information Services and M-Files Web on the new server computer after installing M-Files Server on the new server computer.

If M-Files Web is installed on a separate proxy server instead, the following steps must be completed.

1. If you upgrade M-Files Server after migrating to a new server computer, upgrade the M-Files Web proxy server to the same M-Files version as the one you installed on the new application server.
2. In the Microsoft Windows registry of the M-Files Web proxy computer, update the following setting to point to the new M-Files application server:

Key	**`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFWA`**
Value name	`Server`
Value type	`REG_SZ`
Value	The DNS name of the M-Files application server.

Additional configuration required if you use RPC over HTTPS

On the RPC proxy computer, update the HOSTS file so that the server hostname (the one that clients use for connecting to the M-Files server) points to the IP address of the new M-Files application server.

For further information, see the document Enabling RPC over HTTPS Connections to M-Files Server.

4.3.4. How do the automatic updates work?

M-Files automatically checks for software updates. When an M-Files update becomes available, the update is downloaded to your computer and installed automatically. You can delay the update for a limited time if you are working on something important while an update becomes available.

The feature gets the latest update information from the update server using HTTPS on TCP port 443. This means that normally it is not necessary for you to change any firewall settings.

Note: For the automatic updates to run, local administrative permissions on your computer are not necessary.

See also Updating M-Files.

4.3.5. How much disk space do encrypting file data and taking backups require?

If you enable encrypting file data at rest or backups on the M-Files server computer, it is essential that you ensure that there is enough disk space on the server computer at all times to accommodate encrypted file data and backup data.

Disk space needed for encrypting file data at rest

Encrypting file data at rest makes an encrypted copy of your file data while leaving the unenrypted file data temporarily in place, which essentially doubles the space needed for vault file data on the disk. Thus enabling encryption requires at least double the amount of disk space that your vault file data takes. You can specify the location of the vault file data with the database engine settings in the advanced properties of your vault.

After you have enabled encryption and ensured that your vault content is accessible, you must manually run the **Optimize Database (Thorough)** operation to remove the unencrypted file data of the vault. If the option **Delete the files of destroyed objects** is available, select it.

Note: Make sure that the optimization is not done between file data and metadata backups.

Note: The scheduled automatic optimization does not remove the unencrypted file data.

Disk space needed for backups
As a general rule of thumb, the server machine should always have at least an equal amount of free disk space as the overall disk space required for 1) the file data and metadata of your document vaults and 2) the server-specific data of the M-Files Server instance. However, it is highly recommended that you keep several backups of the vault and server data to give yourself several chances to recover data in the event of system failure or data loss. Therefore the recommended disk space needed for backups is dependent on the backup policy used in your organization.

For more comprehensive backup instructions, please see the M-Files knowledge base article M-Files Backup Policy.

Important: Do not back up an active M-Files system with a snapshot of the file system where its data is stored. This can create a damaged or unusable backup because write operations to files (most importantly, the database engine files) can be ongoing and, thus, incomplete. If you use full virtual machine (VM) snapshots for backups, make sure that the VM software fully supports creation of snapshots of an active system. This means that the software can restore the system to exactly the same state, including the memory and CPU states.

4.3.6. 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 with the scheduled jobs in M-Files Admin. 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.

Important: Do not back up an active M-Files system with a snapshot of the file system where its data is stored. This can create a damaged or unusable backup because write operations to files (most importantly, the database engine files) can be ongoing and, thus, incomplete. If you use full virtual machine (VM) snapshots for backups, make sure that the VM software fully supports creation of snapshots of an active system. This means that the software can restore the system to exactly the same state, including the memory and CPU states.

4.3.7. How often should I reboot the M-Files server machine?

M-Files Server itself does not necessarily require the M-Files server machine to be rebooted, but you should schedule periodic reboots of the server machine because of the added benefit and security of installing Microsoft Windows updates. Keeping a server online without periodic updates and restarts leads to potential vulnerabilities and even failures due to pending operating system updates.

For best practices on scheduling periodic reboots, the article Best Practices with Microsoft Windows Server Update Services provides examples on better control on restarting the server after installing Microsoft Windows updates when avoiding a reboot is not an option.

4.3.8. What is *not* included in the backups?

The vault backup operation can be used to store your vault file data and metadata so that in the event of data loss, your document vault can be recovered from a backup. See Backing Up a Vault for instructions on backing up a document vault.

Data that is collected or generated by someone or something else than vault users and administrators is considered secondary data, and such data is not included in the backups as it is generally not needed for succesfully restoring a document vault.

Below is a categorization of secondary data that is not included in the vault backup files. Note that you generally do not need to worry about this type of data when considering backups as this data is always automatically generated by the M-Files system whenever needed. Below information is therefore mainly for your reference only.

Search indexes

M-Files generates and maintains indexes of your vault document contents and metadata by periodically going through the contents of the document vault. These indexes are used for locating objects when the M-Files search function is used.

Index data may be stored in the following locations on the M-Files server computer:

`C:\Program Files\M-Files\Server Vaults\Indexes`

`C:\Program Files\M-Files\Server Vaults\<vault>\Indexes\`

Usually, this type of data need not be preserved for backups or when migrating document vaults to a new server computer. However, in large vaults, where the index recreation can take a large amount of time, it is recommended to back up the index as well. For more information, refer to M-Files Backup Policy.

Image thumbnails

Image thumbnail files are generated by M-Files when the thumbnail view is used in M-Files Desktop. For more information on different view modes, see Customizing the User Interface of the classic M-Files Desktop.

Thumbnail data may be stored in the following locations on the M-Files server computer:

`C:\Program Files\M-Files\Server Vaults\Thumbnails`

`C:\Program Files\M-Files\Server Vaults\<vault>\Thumbnails`

This type of data need not be preserved for backups or when migrating document vaults to a new server computer.

Document preview files

Document preview data is generated by M-Files when documents are previewed in the **Preview** tab in the M-Files client.

Document preview data may be stored in the following folders on the M-Files server computer:

`C:\Program Files\M-Files\Server Vaults\ViewerFiles`

`C:\Program Files\M-Files\Server Vaults\<vault>\ViewerFiles`

This type of data need not be preserved for backups or when migrating document vaults to a new server computer.

Logs

M-Files creates log files in various locations on the M-Files server computer after certain processes are run. The log files generally have either the `LOG` or the `TXT` file extension. Log files are often used for troubleshooting purposes and may be requested by our customer support for further analysis of an issue.

This type of data need not be preserved for backups or when migrating document vaults to a new server computer.

4.3.9. What kind of operations can I schedule to be run at specific intervals in M-Files?

The following operations can be scheduled and run by M-Files Server as background processes:

- updating object workflow states
- sending notifications
- updating external object types
- updating external value lists
- making a backup of a vault
- optimizing vault database
- exporting content
- importing content
- backing up master database

See the links above for instructions on how you can specify a schedule to determine when each operation is run.

4.3.10. How do I check the location of the active search indexes?

By default, the `Indexes` folder can be found under the location specified in the properties of the vault. Check the index location:

1. In M-Files Admin, in the left-side tree view, right-click a vault.

2. Click **Properties**.

3. Open the **Advanced** tab, and then click **Define**.

   By default, the `Indexes` folder can be found under the location specified in the **Location for secondary data on the M-Files server** field.

In larger vaults, the search indexes might be placed in an alternate location. Check the alternate index location:

4. In M-Files Admin, go to the **Advanced Vault Settings** section.
   a) Open M-Files Admin.
   b) In the left-side tree view, expand an M-Files server connection.
   c) Expand **Document Vaults**.
   d) Expand a vault.
   e) Click **Configurations**.
   f) In the navigation area, click **Advanced Vault Settings**.
   g) Open the **Configuration** tab.

      ✓ The advanced vault settings are shown.

5. Expand **Search** > **Indexes**.

6. Check the active indexes from **Active Metadata Index** and **Active Filedata Index** or **Active Combined Index**.

7. Check the path to the indexes from the **Path** field of the index.

4.3.11. How do I check the full version number of M-Files Desktop and M-Files Server?

Note: These instructions are for Windows 10, but the procedure is highly similar for other Windows versions.

With the steps given here, you can see the full version number of M-Files Desktop and M-Files Server.

1. Right-click the Windows taskbar and select **Task Manager**.

2. Open the **Services** tab.

3. Find the **MFClient** (M-Files Desktop) and **MFServer** (M-Files Server) services in the list.

4. Take note of the full version number of each service.

   For example, `24.8.13981.4`.

4.3.12. How do I save a copy of M-Files errors in the Windows Application event log

Note: These instructions are for Windows 10, but the procedure is highly similar for other Windows versions.

If every M-Files user in your organization is experiencing the same issue, it is recommended to save a copy of the application event log on the M-Files server computer. If the issue is an isolated one, on the other hand, you should only save a copy of the log on the computer where the issue occurs. Complete the steps below on the appropriate computer.

1. Right-click the **Start** icon and select **Event Viewer** from the context menu.

✓ The **Event Viewer** window is opened.

2. Expand **Windows Logs**.
3. Click **Application**.
4. Click **Filter Current Log** on the **Actions** pane.

   ✓ The **Filter Current Log** dialog is opened.

5. Open the **Event sources** drop-down menu and select *M-Files* and any other applications related to M-Files, such as *M-Files Compliance Kit* or *MFClient*.
6. Click **OK** to close the **Filter Current Log** dialog.
7. Click **Save Filtered Log File As** on the **Actions** pane.
8. Specify a location and a file name, and then click **Save**.

A copy of the filtered application event log is saved to the location that you have specified. The copy contains only the errors that are related to M-Files.

4.4. Common Problems for Document Vault Users

This section contains frequently asked questions related to common issues that document vault users may encounter.

In this chapter

4.4.1. 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) and that a *user* (refer to Users) 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.

4.4.2. Why can't I convert a document to PDF format or annotate a document?

This topic gives guidance if you have issues with one of these situations in the classic M-Files Desktop:

- You right-click a document and select **Save as PDF** > **Save as PDF**.
- You right-click a document and select **Save as PDF** and then **Convert to PDF (replaces original file)** or **Convert to PDF (adds separate file)**.
- You right-click a document and select **Scanning and Text Recognition (OCR)** > **Convert to Searchable PDF**.
- You right-click a document and select **Create** > **Annotation**.

Issues surrounding PDF conversions and annotations may be related to the same root cause since annotating a document requires that it is first converted to PDF format. See below for common solutions to these issues.

Reinstall the PDF converter

You may need to reinstall the PDF converter used by M-Files if you receive one of the following error messages after attempting to convert a document to PDF or after attempting to add annotations to a document:

- `The M-Files PDF printer driver is not properly installed. Class not registered.`
- `Unspecified error.`

First you must uninstall PDF-XChange from your computer:

1. On the Windows Start menu, select **Settings**.
2. Select **System** > **Apps & features**.
3. Select PDF-XChange and click **Uninstall**.

Next, reinstall PDF-XChange:

1. Open the file `C:\Program Files\M-Files\<version>\Client\PDFX6SA_sm.exe`.
2. Follow the installer instructions to complete the installation.

Make sure that your computer has an application for opening the original document

To be able to convert a document to PDF format in M-Files, you need to have an application for opening the document installed on your computer. So for instance, if you wish to convert a Microsoft Word document to PDF, you need to have Microsoft Word installed on your computer. And similarly, if you want to convert a Microsoft Excel workbook to PDF, you must have Microsoft Excel installed on your computer.

Make sure that the document is not checked out

Ensure that the document you are trying to convert is not checked out by another user. You need to able to check out the document to convert it to PDF format.

Make sure that the document is not protected by password

Ensure that the document that you are trying to convert is not password-protected. If the document is protected by a password, M-Files is unable to open it and in such cases you are unable to convert the document to PDF format or to add annotations to it.

Make sure that the document is not too large

If you attempt to add annotations to your document but the annotation toolbar is not shown, the file size of the document may be too large.

Similarly, your document may be too large if you try to convert it to PDF format but the conversion fails and an error message similar to the following is displayed:

```
Conversion of the file "Document.docx" to PDF format failed.
The size of the file, [11437522] bytes, exceeds the maximum size 10485760
 bytes specified for Word conversions.
```

By default, the maximum file size for PDF conversions is 10 MB for these file formats:

- Email messages
- Microsoft Excel documents
- Images
- PDF documents
- Microsoft PowerPoint documents
- Visio documents
- Microsoft Word documents

Another limitation of converting large documents to PDF is time. If your PDF conversion takes more than 120 seconds to complete, the conversion fails with an error message similar to the following:

```
Conversion of the file "Document.docx" to PDF format failed.
The maximum execution time of 120 seconds was exceeded.
```

These limitations can be increased by modifying advanced vault settings on the M-Files server computer. For instructions, see Specifying PDF Conversion Limitations for Indexing and File Preview.

Enable the extended language support

If there are problems with non-English content, you can try to enable the Advanced Vault Settings option **PDF Conversion** > **Word Files** > **Extended Language Support**.

4.4.3. 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.

Note: You can hide views by clicking the view and selecting **Hide View** from the **View** menu.

Do the following steps to display hidden views:

1. In the listing area, right-click on an empty area and select **Unhide Views...** from the context menu.

   ✓ The **Unhide Views** dialog is opened.

2. Select the hidden view from the list and click **Unhide**.

3. Click **Close** to close the **Unhide Views** dialog.

4.4.4. Why can't I save an email message as an Outlook message to M-Files?

If you are an M-Files system administrator, you must enable saving attachments in Outlook format and install Microsoft Exchange Server or a 32-bit MAPI client on the M-Files server computer that hosts the vault. For more information, see Mail Sources.

If you are a vault user, inform your M-Files system administrator about this issue and refer the administrator to this page.

4.4.5. Why did a file with a grayed-out icon appear on the M-Files drive when I saved a new document in Microsoft Word?

The file became a temporary local file in the document vault. You can convert the *temporary local file to a document*. For instructions, see Converting a temporary local file to a document.

4.4.6. Why do document timestamps have the wrong time?

If you create a document in M-Files, the **Created** timestamp shows the time when the document is created in the vault. If you drag and drop a file to create a document in M-Files, the **Created** timestamp shows when the document is added to M-Files. In other words, it is not the original creation time of the file. As a result, the **Last modified** timestamp can be earlier than the **Created** timestamp.

For imported files, the **Created** timestamp shows the original creation time and not the time that the file was imported to your M-Files vault.

When a document is added to M-Files, M-Files Server stores the **Created** timestamp in the UTC-0 format and the M-Files client then adjusts the displayed timestamp according to the time zone settings of your operating system.

4.5. General Questions

This section contains general questions about M-Files.

In this chapter

4.5.1. Where can I find more information when I need it?

In addition to this guide, you can look for help in Getting Started with M-Files or consult your organization's M-Files system administrator.

Customer Support

The M-Files upgrade agreement covers customer support (see also Contacting Support).

Please note that customer support does not provide instructions on using the software.

More Information

For more information, you may consult the following sources:

- M-Files knowledge base
- M-Files Community

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

4.5.2. What are the hardware requirements and recommendations?

For technical specifications, refer to System Requirements and Technical Details.

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.

4.5.3. What's new in this M-Files version?

For more information about new, version-specific M-Files features, refer to the M-Files website page https://community.m-files.com/product-resources.

4.5.4. How do the automatic updates work?

M-Files automatically checks for software updates. When an M-Files update becomes available, the update is downloaded to your computer and installed automatically. You can delay the update for a limited time if you are working on something important while an update becomes available.

The feature gets the latest update information from the update server using HTTPS on TCP port 443. This means that normally it is not necessary for you to change any firewall settings.

Note: For the automatic updates to run, local administrative permissions on your computer are not necessary.

See also Updating M-Files.

4.5.5. 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).

4.5.6. How do I write VBScript code for M-Files purposes?

Note: When you develop new extensions or edit existing ones, we recommend that you replace VBScript content with Vault Application Framework (VAF) compatible code for future compatibility. For more information on the benefits of VAF development over VBScript, refer to The Vault Application Framework in M-Files Developer Portal.

You can use VBScript (Microsoft Visual Basic Scripting Edition) code in M-Files for the following functions:

- calculating automatic property values
- validating property values automatically
- triggering state transitions
- executing custom actions in a workflow state
- specifying custom conditions for workflow states for objects to be moved into or out of the said state
- defining customized events that are executed when specific events occur

See the links above for instructions on adding VBScript code in each instance.

You can access and manage objects contained in the document vault by means of M-Files API and VBScript in the above-mentioned circumstances.

VBScript basics

Below are some elementary basics of VBScript to get you started. Note that we are just scratching the surface here. See Useful resources for further instructions. If you are new to scripting and unfamiliar with concepts such as variables and functions, it might be helpful to first read a beginner's guide to scripting, such as Learn Beginning Scripting.

Statements

In VBScript, a line break ends a statement and thus there is no separate termination character for ending statements. The example below contains two statements:

```
Dim szPropertyName
szPropertyName = PropertyDef.Name
```

If you want to divide a statement into separate lines, you may use the underscore character (_) to indicate that a statement is continued on the next line:

```
Err.Raise MFScriptCancel, _
    "The document vault already contains an object with the same title.
 Please choose another title."
```

Commenting

Always comment what you are doing in your code so that others reading your code understand what is going on. You can add a comment in your code using the `'` character:

```
' Get the title of the object.
Dim szCurrentTitle
szCurrentTitle = oCurrentTitleProp.GetValueAsUnlocalizedText
```

It is a good approach to add a comment above any line of code that you may think is not immediately obvious to the reader.

Variables

Variables are declared using the `Dim` keyword:

```
Dim szCurrentTitleProp
```

Values are assigned to variables using the equals (`=`) sign. You should always declare you variables before assigning them new values:

```
Dim szCurrentTitleProp
szCurrentTitleProp =
 PropertyValues.SearchForProperty( iTitleProperty ).GetValueAsUnlocalizedText
```

You may use the `Option Explicit` statement to force explicit declaration of all variables. If you attempt to use an undeclared variable when `Option Explicit` is enabled in your script, your script will not work. For instance, the following script would not work since the variable `szValue` has not been declared before it is assigned a value:

```
Option Explicit
szValue = PropertyValue.GetValueAsUnlocalizedText
```

When you are scripting in M-Files, you have a number of predefined variables at your disposal. The variable `PropertyValue`, for example, can be used for fetching the value of a property. See Available VBScript Variables for the complete list of predefined variables.

Note: We recommend you to use the so-called Hungarian notation when naming variables. This way you, or whoever reading your code, has a clear understanding of the data type of the value stored in the the variable. You can use, for instance, the following notation:

- "sz" for strings
- "o" for objects
- "i" for integers
- "b" for Booleans
- "f" for floating-point numbers
- "d" for dates

Constants

You can use constants for storing values that must remain constant throughout the script:

```
Const iMaxNumberOfItems = 50
```

Note that you must assign a literal value to a constant. You cannot use a variable, another constant or a function to initialize a constant.

Objects

Objects are assigned to variables using the `Set` statement. You may create a new instance of an M-Files API object and assign it to a variable in the following fashion:

```
Dim oTitleSearch
Set oTitleSearch = CreateObject( "MFilesAPI.SearchCondition" )
```

Objects are components that have their own properties and methods. Methods are functions that belong to a specific object and that can be used in the context of the object. Properties, on the other hand, are used to view or set values of an object. You access the properties and methods of an object using dot notation:

```
oTitleSearch.Set oTitleExpression, MFConditionTypeEqual, oTitleTypedValue
```

Method arguments, such as `oTitleExpression`, `MFConditionTypeEqual`, and `oTitleTypedValue` in the above example, are listed after the method and separated by a comma. Parameters are passed either by value or by reference. If a method takes a parameter by value, the method copies the value passed as the argument and thus the original value is unchanged. If, on the other hand, a method takes a parameter by reference, any changes the method may cause to the argument also impact the original reference. The value `Nothing` should be used if the default value of the parameter is to be used.

When scripting in M-Files, you will take advantage of the objects available in VBScript, and more importantly, the objects available in M-Files API. Refer to the M-Files API documentation for complete details.

Concatenating strings

You may concatenate two or more strings into one using the `&` operator:

```
' 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
```

In the above example, the proposal title, stored in the variable `szName`, is the result of the concatenation of the following strings:

- string literal `Proposal #`
- the proposal number, stored in the `szNumber` variable
- another string literal `/`
- the customer name, stored in the `szCustomer` variable

The resulting proposal title could thus be, for example, `Proposal #5577 / ESTT`.

You can add a line break to your string by concatenating the `VbCrLF` constant with your strings:

```
Err.Raise MFScriptCancel, _
    "The document vault already contains an object with the same title." &
 VbCrLF & "Please choose another title."
```

Raising errors

If you need to, say, validate a property value with VBScript, it is necessary to display an error message to the user if the value the user entered is invalid. You can raise an error in VBScript using the `Raise` method of the `Err` object:

```
Err.Raise MFScriptCancel, "The property """ & szPropertyName & """ must have
 a value of at least 10 characters."
```

The method takes the error number and description as parameters. For M-Files scripting purposes, the `MFScriptCancel` variable is used as it stores the M-Files error number.

If statements

`If` statements are used for executing a group of statements if the condition specified in the `If` statement evaluates to true:

```
If Len( szValue ) < 10 Then

    Err.Raise MFScriptCancel, "The property """ & szPropertyName & """ must
 have a value of at least 10 characters."

End If
```

The if block must end with an `End If` statement. All the statements between `If` and `End If` are executed if the condition specified between `If` and `Then` evaluates to true. You can use the `And` operator to specify multiple conditions that must all be true for the if block to be executed, or the `Or` operator to specify multiple operators, one of which must be true for the if block to be executed. You can use the following comparison operators for specifying the condition:

- `==` checks if the value of two operands are equal or not, if yes, then the condition is true.
- `<>` checks if the value of two operands are equal or not, if not, then the condition is true.
- `>` checks if the value of the left operand is greater than the value of the right operand, if yes, then the condition is true.
- `<` checks if the value of the left operand is less than the value of the right operand, if yes, then the condition is true.
- `>=` checks if the value of the left operand is greater than or equal to the value of the right operand, if yes, then the condition is true
- `<=` checks if the value of the left operand is less than or equal to the value of the right operand, if yes, then the condition is true

You can also nest an `If` statement inside another `If` or, say, an `Else` statement or use the `ElseIf` statement to create a deeper branching logic in your script.

Functions and subroutines

You can use a subroutine to define a section of code to be used multiple times by reference in your code:

```
Sub CloseFile()
    oMyFile.Close
    Set oMyFile = Nothing
End Sub
```

Or, you can define a function to use multiple times a section of code that returns a value of some kind:

```
Function IsOdd( iValue )
    If iValue MOD 2 = 0 Then ' Even value.
        IsOdd = False
    Else ' Odd value.
        IsOdd = True
    End If
End Function
```

To call a subroutine or function in your script, just refer to it by name:

```
Closefile()
IsOdd( 5 )
```

Useful resources

Your most valuable sources of information on scripting within M-Files are the following:

- M-Files API documentation
- Available VBScript Variables

The M-Files API documentation is an exhaustive reference to the M-Files API objects, methods, interfaces, properties, and enumerations that you can take advantage of within VBScript code. The latter resource, on the other hand, lists and explains all the variables with preassigned values that you can readily utilize in your VBScript code.

In addition to the two aforementioned resources, you may find the following external websites useful:

- VBScript User's Guide
- VBScript Functions
- Learn Beginning Scripting

Example

The example below is a script that can be used for validating a property when the user attempts to save metadata changes on the metadata card. The script ensures that the entered property value must be at least 10 characters in length. Let us take a closer look at the script:

```
Option Explicit

Dim szPropertyName, szValue

szPropertyName = PropertyDef.Name

szValue = PropertyValue.GetValueAsUnlocalizedText
```

```
If Len( szValue ) < 10 Then

    Err.Raise MFScriptCancel, "The property """ & szPropertyName & """ must
 have a value of at least 10 characters."

End If
```

First, the variables `szPropertyName` and `szValue` are declared, after which the name of the property and its value we are validating are stored in the variables we have just declared. We use the `GetValueAsUnlocalizedText` method (refer to the M-Files API documentation for more information) to obtain the property value as unlocalized text.

Our condition for validating the property value is that the value must have at least 10 characters. We evaluate that condition in an `If` statement. We have defined in the condition of the `If` statement that the length of the property must be less than 10 characters for the statement inside the `If` statement to be executed. If the property value is 10 characters or more, the `If` code block is not executed and the script execution is finished.

In the if block, we send an error message to the user where we state that the property value that the user entered must have at least 10 characters, thus instructing the user to add a longer value. After the error message is displayed, the metadata card is displayed again, allowing the user to modify the invalid property value.

For complete instructions on validating property values with VBScript, see Automatically Validating Property Values.

4.5.7. What is the difference between a named access control list (NACL) and a user group?

M-Files allows you to use named access control lists and user groups to manage information related to a group of individuals, but they essentially serve a very different purpose.

With **user groups**, administrators can arrange individuals into separate groups based on common features, such as their position in the organization (for example "HR" and "Managers"), their physical location (for instance "Vermont office" and "Chicago office"), or their expertise (such as "Legal matters" and "Translation"). User groups can be managed with M-Files Admin (see User Groups).

Named access control lists, on the other hand, can be used for specifying various access rights to objects in a vault. They contain a list of subjects (individual users, user groups or pseudo-users) coupled with a list of permissions, essentially controlling rights for reading, editing and deleting objects as well as for changing their permissions. Named access control lists can also be managed with M-Files Admin (see Named Access Control Lists).

Example: Employment agreements to be visible to the HR department only

The vault contains a large number employment agreements that are currently visible to all vault users. The HR manager wants them to be visible to the HR team only.

The first thing she needs to do is create a user group for all the users that belong to the HR team. Now, as she cannot use the user group to directly control any access rights, she also needs to create a named access control list for associating the newly created user group with the access rights of her choice.

Note: Users whose login account has the **System administrator** system role, and users who have either the **See and read all vault content** or **Full control of vault** rights are able to see all vault content.

Finally, the HR manager must associate the newly created named access control list with the employment agreements. She can do this with the properties of the employment agreement class.

Opening the properties dialog for a class:

1. Open M-Files Admin.
2. In the left-side tree view, expand a connection to M-Files server.
3. Expand **Document Vaults**.
4. Expand a vault.
5. Expand **Metadata Structure (Flat View)**.
6. Click **Classes**.
7. In the listing area, select the class representing the employment agreements.

   ⓘ If there is no class for employment agreements, you can create a new class for this purpose.

8. From the task bar on the left side of the listing area, select **Properties**.

Setting the class to use the named access control list:

9. Open the **Automatic Permissions** tab.
10. Check the **Restrict the permissions of objects that refer to this class** check box.
11. Check the **Use named access control list** check box.
12. Select the newly created named access control list in the menu below the check box.
13. Click **OK** to close the **Class Properties** dialog.
14. Optional: If an information dialog about disabled automatic permissions for certain property definitions is displayed, note down the property definitions mentioned in the **Property definitions currently disabled** list and click **OK**.

    ⓘ To make sure that the permission settings are activated when the class for an employment agreement is selected as the value of any of the properties mentioned in the list, you need to explicitly allow automatic permissions to be used for these property definitions.

15. In the dialog changed automatic permissions, select either:

    a. **Change Objects' Permissions** to apply the new access rights to all the objects that will be created from this moment forward.

       Note: Object permissions are updated as an asynchronous background task. Object permissions may be updated when, for example, a named access control list, a user, a user group, or the value of a pseudo-user (such as a project manager) is modified. You may monitor the progress of the task in M-Files Admin in the **Background Tasks** section. For more information, see Monitoring Background Tasks.

       or

    b. **Change and Activate Objects' Permissions** to apply the new access rights to all the existing objects as well as to all the objects that will be created from this moment forward.

or

c. **Cancel** to return to the **Class Properties** dialog.

Enabling automatic permissions to be used through related properties:

16. Optional: In the left-side tree view, under **Metadata Structure (Flat View)**, select **Property Definitions**.
17. Optional: Double-click one of the property definitions that you noted down in step 14.
18. Optional: Select the **Enable automatic permissions via this property** check box and click **OK**.
19. Optional: Select either **Change Objects' Permissions** or **Change and Activate Objects' Permissions** (see step 15).
20. Optional: Repeat the steps from 17 to 19 for all the property definitions noted down in step 14.
21. Close M-Files Admin.

Depending on what you selected in step 15, either a) only new objects or b) both new and existing objects whose class represents the employment agreements are now visible only to the user group whose members are part of the HR department. As explained in this note, this does not, however, apply to system administrators and vault users with rights to see and read all vault content.

Index