Mitratech Document Vault™
powered by M-Files®

Installation Guide
for eCounsel

Version 3.2.0
6/16/2020

June 2020

Table of Contents

Overview

The information in this installation guide can be used to install and configure the components of Mitratech Document Vault, a Document Management System (DMS) integration between Bridgeway Suite and M-Files.

Components

Mitratech Document Vault includes the following components:

- **Mitratech Document Vault Server:** Powered by M-Files Server, this server manages the storage of all documents and associations between matters and documents.
- **Mitratech Document Vault Desktop Client:** Available for Microsoft Windows, this locally-installed interface allows users to view and associate documents with matters. The Client should be installed on all computers for users who frequently add and review documents for matters. Typically, the users who have the Client on their desktop are named users.
- **Mitratech Document Vault Web:** This browser-based interface allows users to view documents attached to matters. This interface can be configured for access through a tab or widget in eCounsel. The Web interface has functionality similar to the desktop client, but is intended for Read-Only and concurrent users.

Some features are available in the Desktop Client but **not** in the Web interface:

- The ability to create and edit views
- The ability to view security rights on documents
- The **Most Recently Accessed** panel (however, the Web interface does include a similar link in the left pane)
- Integration with Microsoft Outlook and Microsoft Office (Microsoft Word, Microsoft PowerPoint, Microsoft Excel) using a plugin
- Access to the virtual **M:** drive
- Check-in reminders when closing Microsoft Office documents
- Offline availability
- Annotations
- The ability to **Save As** or **Convert to PDF**
- Highlighted search results

System Requirements

See the *Mitratech Document Vault Technical Overview* for a complete list of Mitratech Document Vault server requirements.

Before You Begin

This guide is intended for Information Technology (IT) professional who will be installing the M-Files Server portion of Mitratech Document Vault and configuring it for use with the M-Files Client. The steps to complete an integration include:

1. Install the M-Files Server. You must have administrative rights on the server machine to install. If you are enabling the M-Files Web Client, see the *M-Files User Guide* for instructions on configuring access.
2. Enter a license key for the M-Files Server. Mitratech provides a license key for each integration.
3. Restore the vault provided by Mitratech.
4. Optionally, migrate the vault to Microsoft SQL Server if your site is not using the default Firebird Embedded database.
5. Import users into M-Files from your Active Directory (AD).
6. Create a document vault connection. This step tests that clients can connect to the M-Files Server.
7. Connect M-Files to eCounsel.
8. If you are implementing access to the M-Files Web Client through eCounsel, see the *Bridgeway Suite Web Page Container Widget Guide* for information on deploying the widget. See Configuring M-Files Web Access for information on the settings to use when configuring the widget.
9. After the synchronization between eCounsel and M-Files is complete, configure user accounts for M-Files access if needed.
10. Install M-Files Clients on all computers for users who will be storing and viewing documents frequently. After installation, create a document vault connection on each user computer.

Mitratech Support

E-mail Mitratech Support at ecounselsupport@mitratech.com for all technical inquiries.

Installing the Mitratech Document Vault Server

Installing the M-Files Server

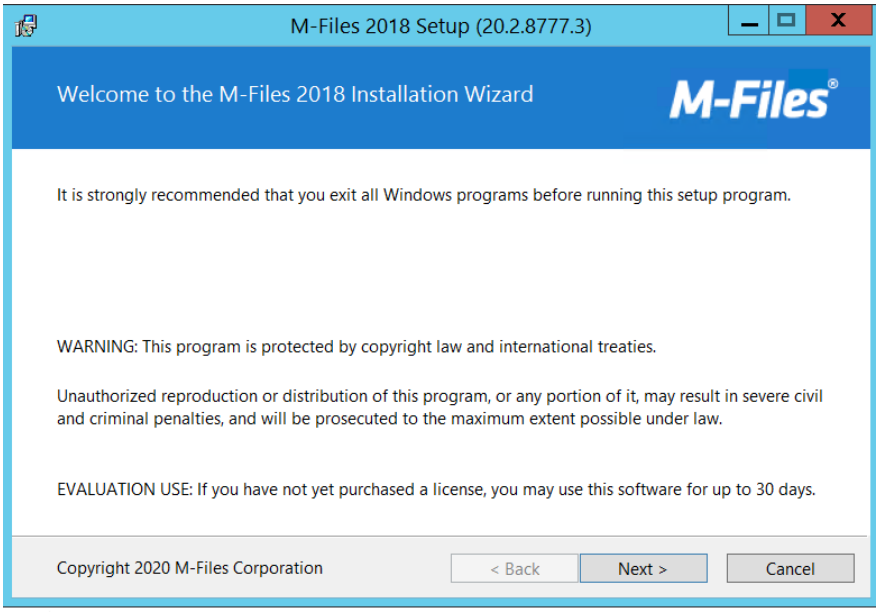
Powered by M-Files Server, Mitratech Document Vault manages the storage of all documents and associations between matters and documents. Installing Mitratech Document Vault includes installation of the M-Files Server. After installing the M-Files Server, you must enter a license key, restore the vault, which has been customized to work with eCounsel, and import users.

If you want to allow M-Files Web Client access, install .NET Framework version 4.0 (or higher) and Internet Information Services (IIS) on the server machine prior to installing M-Files Server (see Configuring M-Files Web Access for more information).

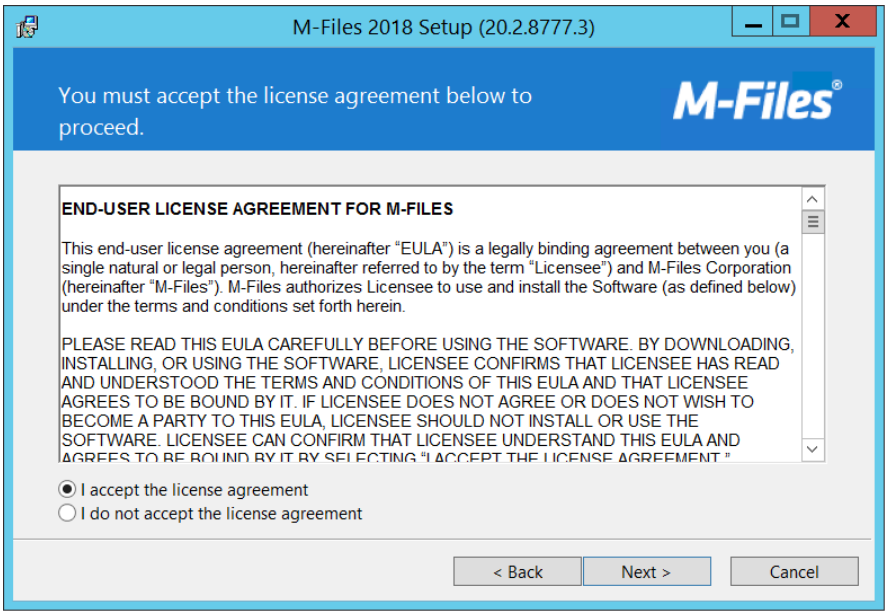
Firewall settings should be configured according to the specifications outlined in the *Mitratech Document Vault Technical Overview*.

To upgrade the M-Files Server to M-Files 2018:

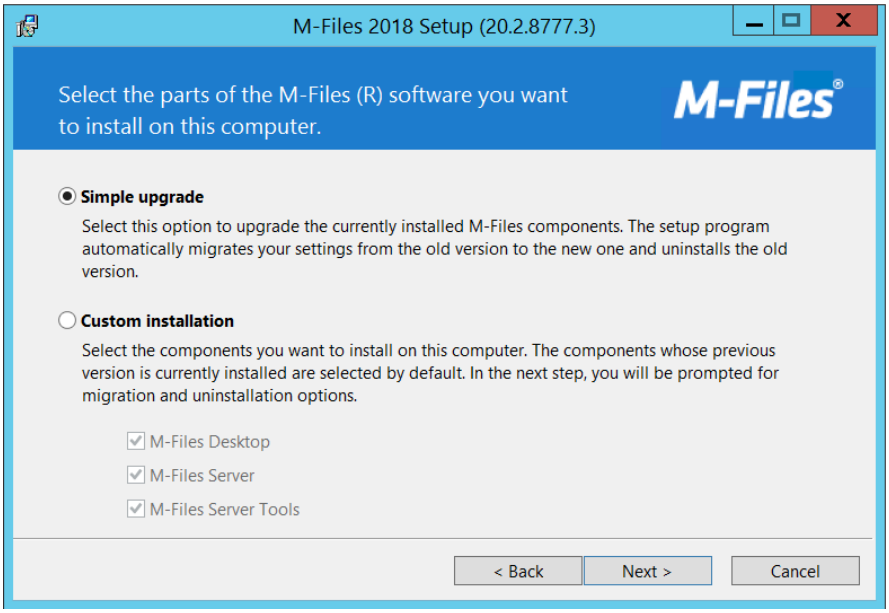
1. Double-click on the M-Files Mitratech installation file provided by Mitratech to start the installation process.
2. On the **Welcome to the M-Files 2018 Installation Wizard**, click **Next**.



3. On the **License Agreement** screen, review the license agreement, click *I accept the license agreement* to continue, and click **Next**.

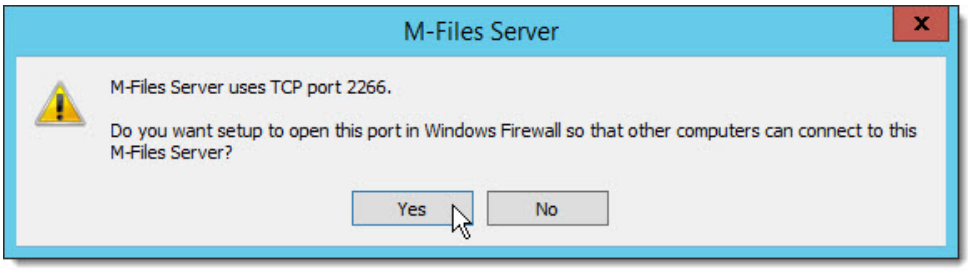


4. On the **Installation Type** screen, select the *Simple upgrade*. Click **Next**. Note that if you are installing M-Files for the first time, select a *Custom installation* and select all three checkboxes. (You will need to specify a destination folder prior to installing the files.)



5. On the **Ready to Install the Application** screen, click **Next**.

6. If port 2266 is not open on the server computer, click **Yes**.



7. If Microsoft SQL Server 2012 Native Client is not installed on the server computer, it will be installed.
8. M-Files will install the files in a default location. Click **Finish** when the installation has completed.

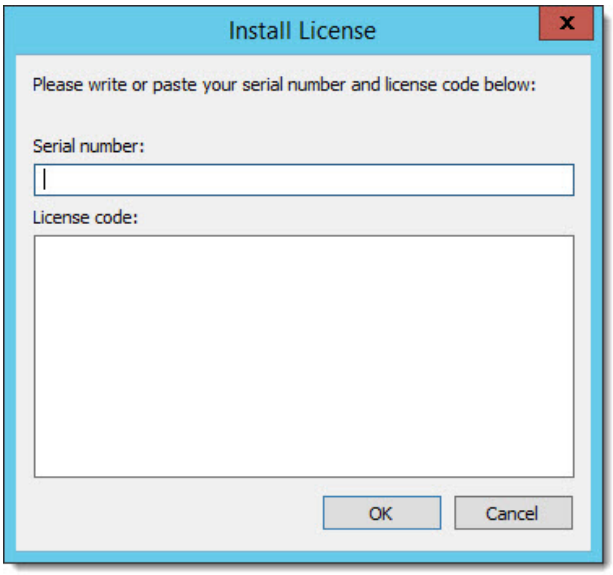
Although the **M-Files Desktop Settings** dialog box opens to create a document vault connection, you must first enter a license key, create an administrative login account, and restore the Mitratech Document Vault if this is a new installation.

Entering a License Key

Upon initial installation of the M-Files server, you must enter a license key to activate the deployment. Locate the serial number and license code provided to you by Mitratech prior to executing the steps below.

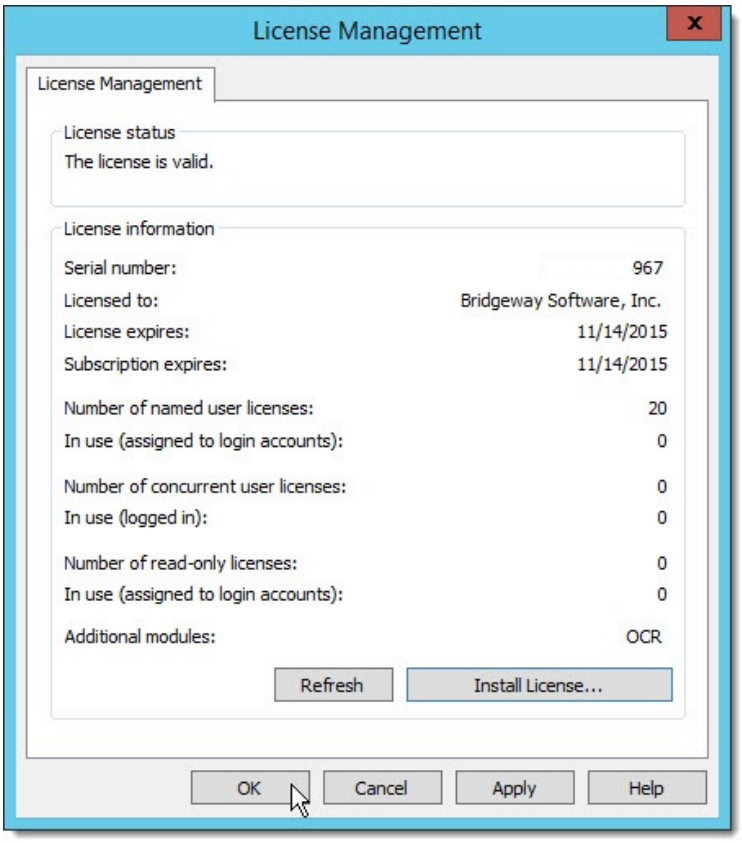
To enter a license key:

1. Open the M-Files Admin tool.
2. On the **M-Files Admin** window, click the **Local Computer** node in the right treeview.
3. In the *Server Management* area, click **License Management**. Alternatively, you can right-click the **Local Computer** node and select **License Management**.
4. On the **License Management** dialog box, click on the **Install License** button.
5. On the **Install License** dialog box, type the serial number provided to you by Mitratech.



6. Copy-and-paste the license code in the text box.
7. Click **OK**.

8. On the **License Management** dialog box, confirm the details of the license and click **OK**.



Restoring the Vault

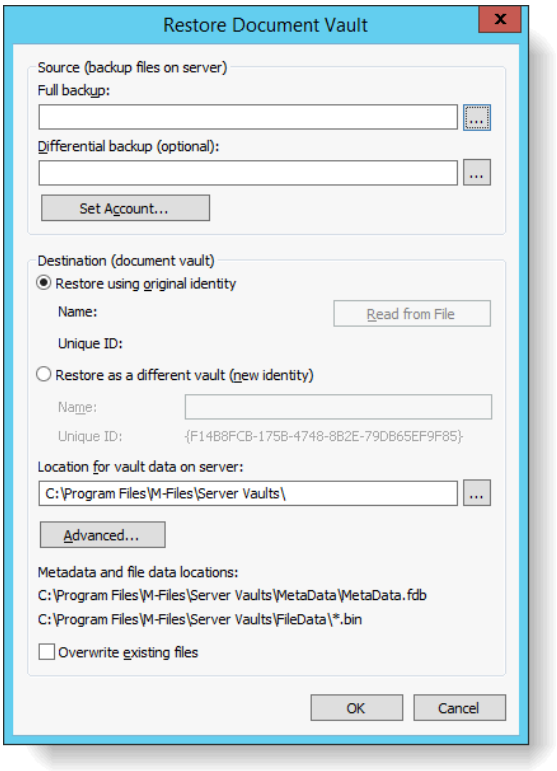
Next, you must restore the vault using the file provided by Mitratech and the M-Files Admin tool. Microsoft Windows Registry settings that point to the Mitratech Document Vault are installed with the M-Files client. Most of these settings specify the vault name.

Restoring vaults, creating new vaults, or copying vaults should be performed with caution.

To restore the Mitratech Document Vault:

1. Open the M-Files Admin tool.
2. On the **M-Files Admin** window, click the **Local Computer** node in the right treeview.
3. Click the **Document Vaults** node under **Local Computer**.
4. In the *Document Vaults* area, click **Restore Document Vault.** Alternatively, you can right-click the **Local Computer** node and select **Restore Document Vault**.

5. On the **Restore Document Vault** dialog box, click the **...** button next to the Full backup text box and select the **.mfb** file provided by Mitratech.



6. In the *Destination (document vault)* area, if the values do not appear for the vault, click the **Read from File** button to populate the Name and Unique ID fields.
7. Click **OK**.
8. On the message box that appears, click the **Leave Unchanged** button.
9. When the restore compile is complete, click **OK**.

To change the File Data location:

1. On the **M-Files Admin** window, right-click on the new vault, select *Operations* and select *Take Offline*.
2. Navigate to the folder where the file data is located (typically **C:\Program Files\M-Files\ServerVaults**<*Vault_Name*>).
3. Copy the **FileData** folder from the current location to the new folder location.
4. On the **M-Files Admin** window, right-click on the vault, and select *Properties*.
5. On the **Document Vault Properties** dialog box, select the **Advanced** tab.
6. Select the **Define** button, and then select the **Advanced** button.
7. Select the *Separate location for file data* option.
8. For the path, select the new location of the folder where you pasted the **FileData** folder.
9. Select **OK**, select **OK** again, select **Apply**, and then select **OK** again.
10. On the **M-Files Admin** window, right-click on the vault, select operations and select *Bring Online*.

Migrating the Vault to Microsoft SQL Server

By default, restoring the Mitratech Document Vault installs the vault to the Firebird Embedded database. If you want to use Microsoft SQL Server as the database, you must convert the vault so that data can be stored on an existing Microsoft SQL Server.

Using Microsoft SQL Server

Mitratech recommends using Microsoft SQL Server with large document vaults that containing over 100,000 documents and objects. Using Microsoft SQL Server offers a number of benefits over Firebird:

- More efficient use of the database server memory
- Improved backup storage of large data vaults
- A readily-available mirrored database server in case of outage or errors
- Greater overall efficiency with large document vaults

Microsoft SQL Server can be located on the same machine as the M-Files Server, or it can be installed on another server. If installed on separate servers, the M-Files Server and the Microsoft SQL Server must be linked with a fast network connection.

Before you begin

Using Microsoft SQL Server requires:

- An administrator familiar with the Microsoft SQL Server management
- A separately-purchased license (Microsoft SQL Server licenses are not included with the M-Files licenses)
- A Microsoft SQL Server machine with a sufficient amount of memory, a sufficient number of processors of appropriate speed, and sufficient hard drives. Instructions for ensuring the efficient operation of Microsoft SQL Server can be found in the Microsoft SQL Server documentation.

Migrating the Database

You can easily migrate to Microsoft SQL Server from Firebird with the **Migrate to Microsoft SQL Server...** function. You can only migrate the document vault database engine from Firebird to Microsoft SQL Server; migrating from Microsoft SQL Server to Firebird is not supported.

Before migrating the database, you will need to create two database accounts and create the shell database into which the Firebird Embedded database will be migrated.

Creating Database Accounts

Users can log in using SQL Server Authenticated logins or Windows Authenticated accounts. If you are using SQL Server Authenticated logins, create two accounts:

- An administrator who is the owner of the database and creates objects in the database.
- A basic user account who only has the rights necessary to operate M-Files; the application will use this account when connecting to the database.

The user names can follow your company's standard naming conventions.

Creating the Shell SQL Server Database and Set the Database Owner

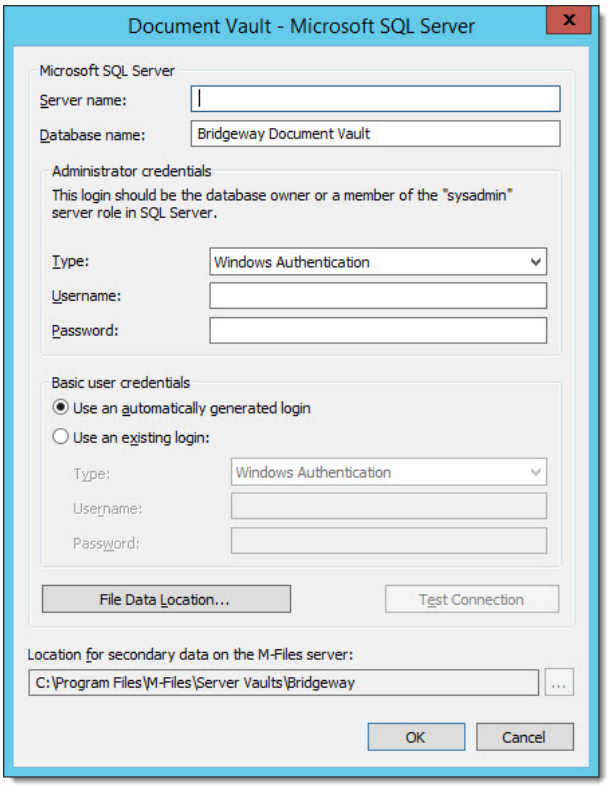
The shell database is an empty database to which M-Files will connect and build everything it needs to be the M-Files SQL Server database. The database name can follow your company's standard naming conventions. A DBA will need to connect to the SQL Server with DBA rights and run the following script to create the database and make the Administrator account the owner of the database:

```
USE master
GO
CREATE DATABASE <DatabaseName> COLLATE Latin1_General_CI_AS
GO
USE <DatabaseName>
GO
EXEC sp_changedbowner '<AdminLogin>'
GO
```

where <*DatabaseName*> is the name of the database and <*AdminLogin*> is the login of the administrator database account that you created for this step.

To migrate the Mitratech Document Vault to Microsoft SQL Server:

1. Open the M-Files Admin tool.
2. On the **M-Files Admin** window, click the **Local Computer** node in the right treeview.
3. Expand the **Document Vaults** node under **Local Computer**.
4. Right-click the **Document Vault**, select *Operations*, and select *Migrate to Microsoft SQL Server*.
5. In the Server name field in the **Document Vault** dialog box, type the fully qualified name and port of the Microsoft SQL Server in the form of <*ServerName*>,<*Port*>.
6. Type the name of the Microsoft SQL Server database in the Database name field.



7. In the *Administrator Credentials* area, select the type of credentials being supplied, and enter a name and credentials for the database owner. These credentials belong to the administrator account that you created earlier.
8. In the *Basic User Credentials* area, select to automatically generate logins or enter the credentials of the account that you created earlier. This account is used for reading and writing to the database.
9. Click the **Test Connection** button. Click **OK** on the message box that the test connection succeeded.

10. On the **Document Vault** dialog box, click **OK**.
11. Click **Yes** to proceed to convert the database to Microsoft SQL Server.
12. Click **OK** on the message box that the conversion succeeded.

To change the File Data location:

If you want to store files on a file server instead of in a database, follow these steps:

1. On the **M-Files Admin** window, right-click on the new vault, select *Operations* and select *Take Offline*.
2. Navigate to the folder where the file data is located (typically **C:\Program Files\M-Files\ServerVaults**<*Vault_Name*>).
3. Copy the **FileData** folder from the current location to the new folder location.
4. On the **M-Files Admin** window, right-click on the vault, and select *Properties*.
5. On the **Document Vault Properties** dialog box, select the **Advanced** tab.
6. Select the **Define** button, and then select the **Advanced** button.
7. Select the *Separate location for file data* option.
8. For the path, select the new location of the folder where you pasted the **FileData** folder.
9. Select **OK**, select **OK** again, select **Apply**, and then select **OK** again.
10. On the **M-Files Admin** window, right-click on the vault, select operations and select *Bring Online*.

Adding or Importing Users into Document Vault

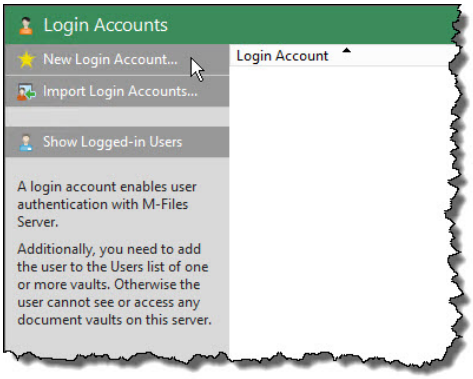
Prior to adding a document vault connection to test the M-Files Client installation on the server machine, you can create new user login accounts manually, or you can import user accounts from your Active Directory (AD) to use Mitratech Document Vault.

Creating a Login Account

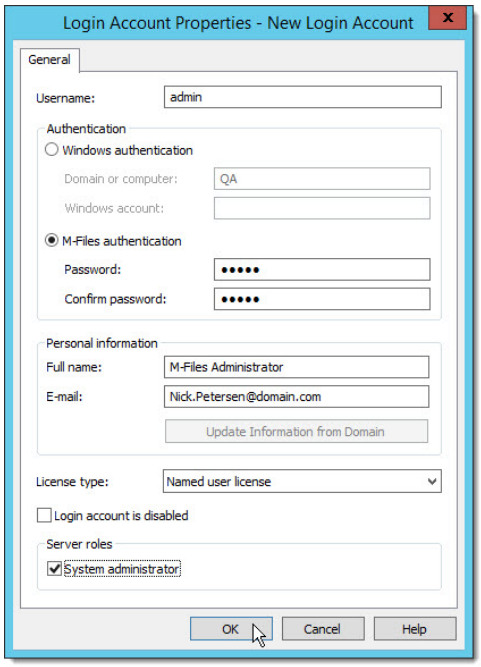
Only a user with full Administrator rights can create new accounts or modify existing login accounts.

To create a login account:

1. Open the M-Files Admin tool.
2. On the **M-Files Admin** window, expand the **Local Computer** node in the navigation pane and click the **Login Accounts** node.
3. In the *Login Accounts* area, click **New Login Account**.



4. On the **Login Account Properties** dialog box, enter the user name. For hosted installations in the Mitratech Cloud, the user name will be the user's email address.

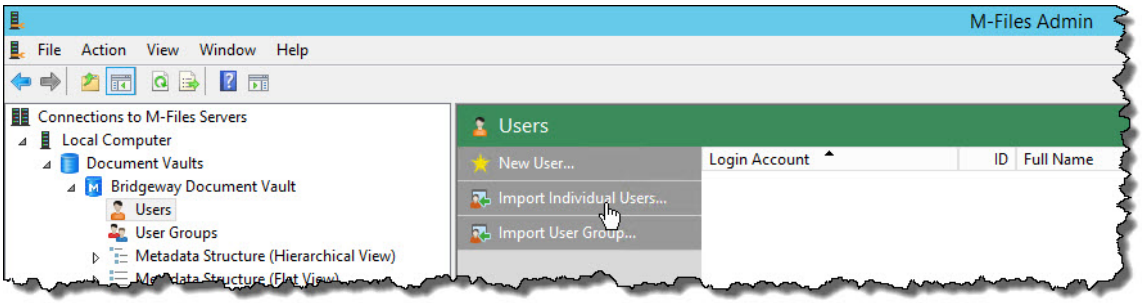


5. Select M-Files authentication and type a password. The password can be no longer than 14 characters and can support special characters.
6. Select the license type.
7. If the user is to be granted full Administrator rights, select *System administrator*. Business-user admins can be made **Vault Admins** when they are given rights to their vault.
8. Click **OK**.

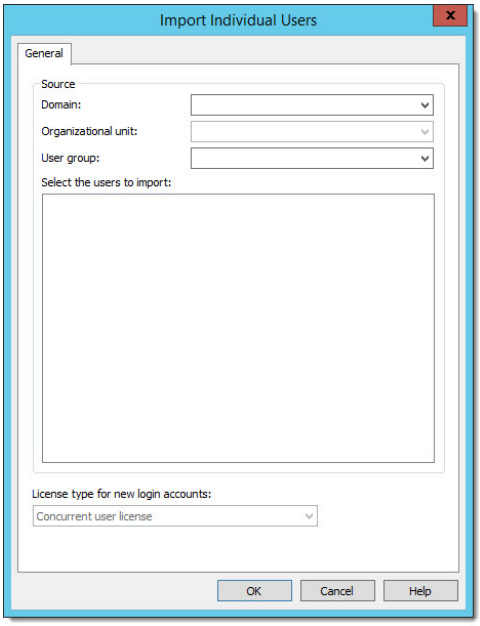
Importing Login Accounts into Mitratech Document Vault

To import login accounts into Mitratech Document Vault:

1. Open the M-Files Admin tool.
2. On the **M-Files Admin** window, expand the **Local Computer** node in the navigation pane.
3. Expand the **Document Vaults** node under **Local Computer**.
4. Expand the **Document Vault** under Document Vaults.
5. Click the **Users** node.
6. In the *Users* area, click **Import Individual Users.**



7. On the **Import Individual Users** dialog box, select the domain that contains the AD.



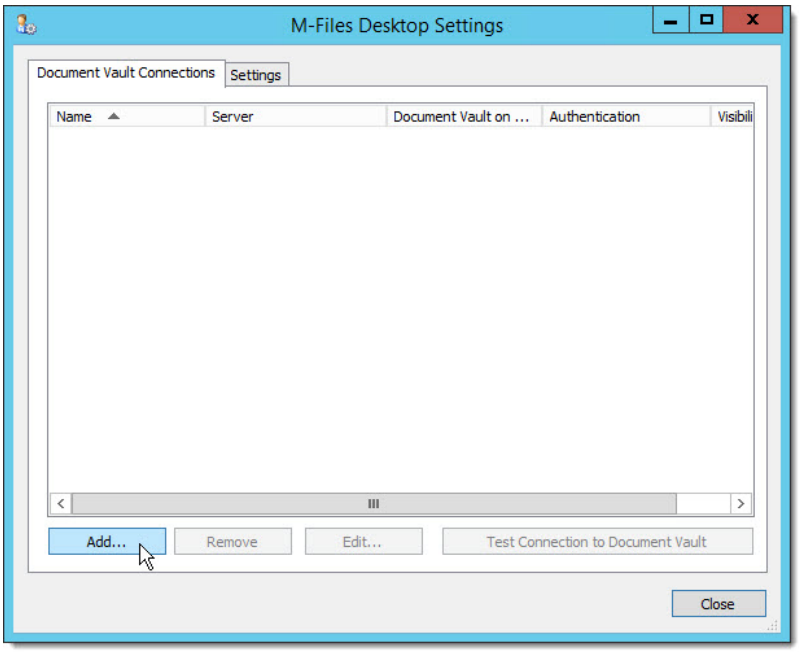
8. Select an organization unit or select (any) to import all AD user accounts.
9. Select a user group.
10. Select individual accounts by clicking on a user account and pressing the <Ctrl> key to select multiple user accounts.
11. Select the type of license for the user accounts. Change the license type to *Named user license* to avoid conflicts if you have existing users in the system.
12. Click **OK**.
13. When the import is complete, click **OK**.

Creating a Document Vault Connection

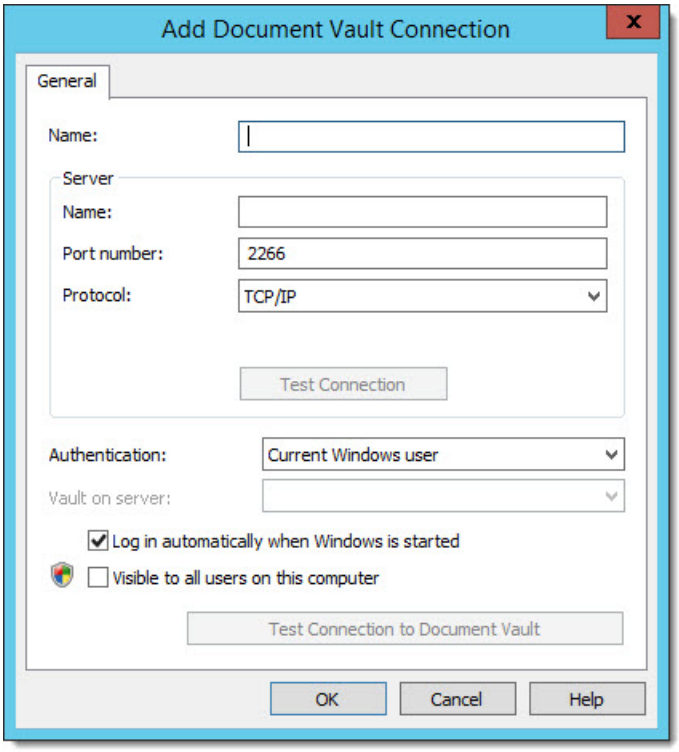
Once the M-Files Server is installed, you can create a connection to the vault provided by Mitratech for the integration with eCounsel. This connection allows users to access the vault from the M-Files Client. The instructions below can be used to test the vault connection on the server and after installing the M-Files Client on user machines.

To create a connection:

1. If the **M-Files Desktop Settings** dialog box is not open, open the M-Files Desktop Settings tool.
2. On the **M-Files Desktop Settings** dialog box, click the **Add** button.

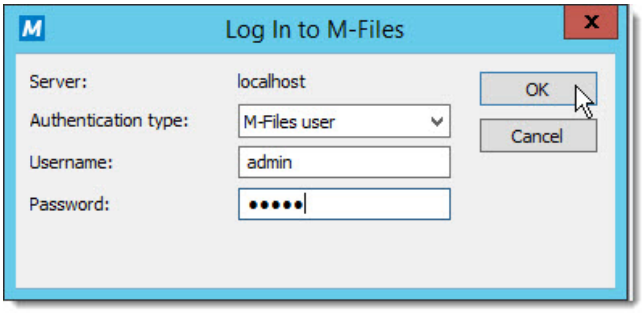


3. On **Add Document Vault Connection** dialog box, type "Document Vault" as the name of the vault. The name must be typed exactly as shown for the integration to work properly.



4. Type "localhost" for the server name if you are connecting a client on the M-Files Server machine. Otherwise, type the fully qualified name of the M-Files Server.
5. Select *M-Files user* for the authentication type.
6. Click the drop-down for the Vault on server field.

7. On the **Log In to M-Files** dialog box, type the user name of a valid login account and the corresponding password, and click **OK**.



8. Select the Mitratech provided vault for the vault on server.
9. Click in the checkbox to enable M-Files to log in automatically when Microsoft Windows is started.
10. Click the **Test Connection to Document Vault** button. Click **OK** on the message box that the test connection succeeded.
11. On the **Add Document Vault Connection** dialog box, click **OK**.
12. On the **M-Files Desktop Settings** dialog box, click **Close**.

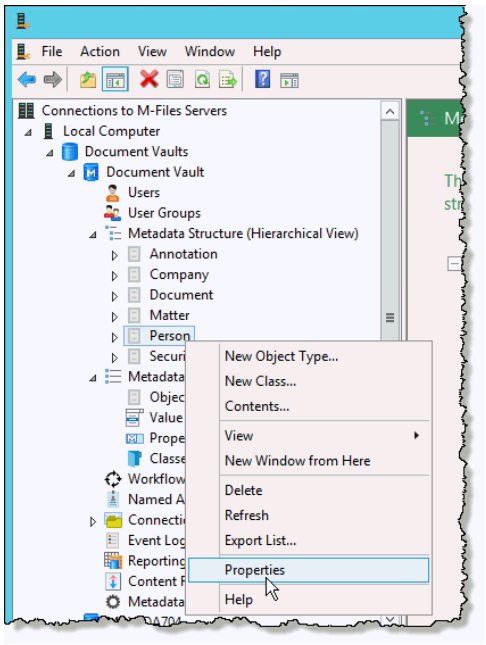
Connecting M-Files to eCounsel

Mitratech Document Vault uses a SQL connector as the data migration tool to pull data from eCounsel to M-Files so that users can attach documents to eCounsel matters. To connect M-Files to eCounsel, configure the Person properties in the Metadata Structure of the M-Files Admin, associate the Vault users to staff records, and then configure the Security Group, Company, and Matter properties.

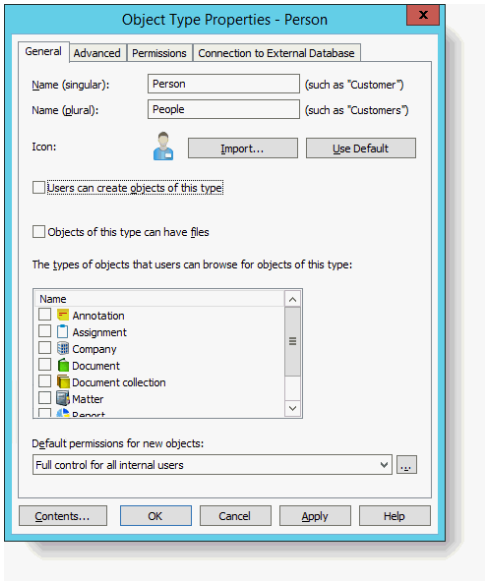
Configuring Person Properties

To configure the Person properties:

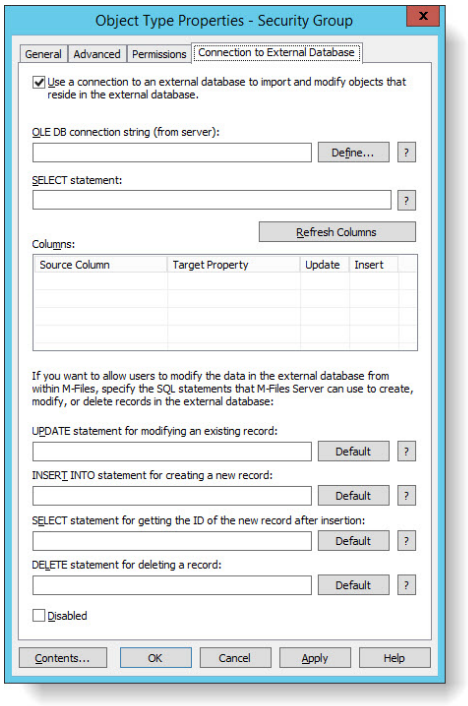
1. Open the M-Files Admin tool.
2. In the navigation tree, expand the desired vault and the **Metadata Structure (Hierarchical View)**.
3. Right-click **Person** and select **Properties**.



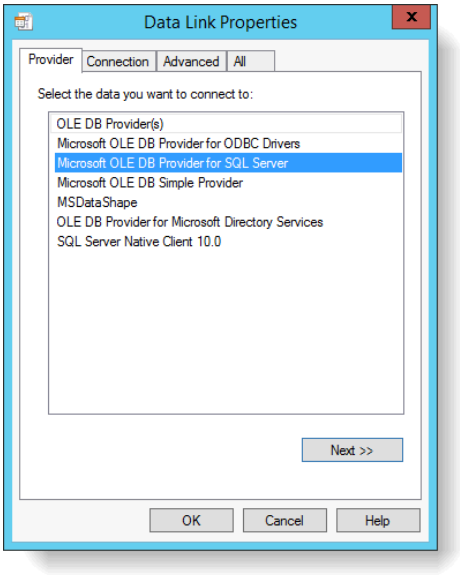
4. On the **General** tab, clear the *Users can create objects of this type* checkbox.



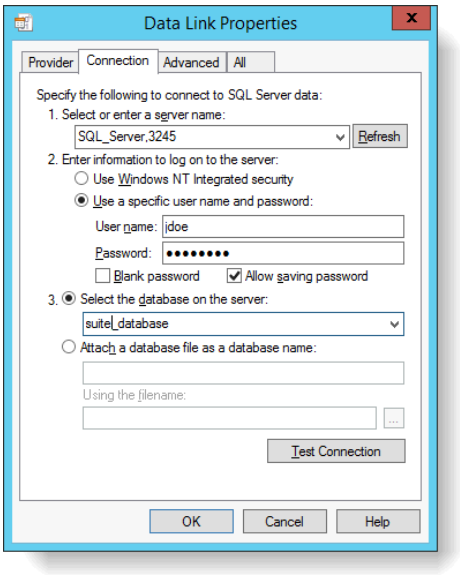
5. On the **Connection to External Database** tab, select **Use a connection to an external database to import and modify objects that reside in the external database.**



6. Click the **Define** button for the OLE DB connection string. In the dialog box that appears, your entries will depend on the database you are using.
7. If using a SQL Server source database:
    - Chose **Microsoft OLE DB Provider for SQL Server**, then click **Next.**



    - On the **Connection** tab, enter the server name and port in the form of <*ServerName*>,<*Port*> and connection credentials. Select **Allow saving password** and select the correct source database from the dropdown list.



- Click **Test Connection** and if the test is successful, click **OK**.

8. If using an ORACLE source database:
   - Chose **Oracle Provider for OLE DB**, then click **Next**.
   - On the Connection tab, enter the Data Source (TNS Alias) and connection credentials and select **Allow saving password**.
   - Click **Test Connection** and if the test is successful, click **OK**.
9. On the **Connection to External Database** tab, for SQL configurations, enter **select * from DV_Staff** as the SELECT statement. For ORACLE configurations, enter the same statement but add the schema qualifier before the view name. For example, **select * from SchemaOwner.DV_Staff**.
10. Click the **Refresh Columns** button.
11. Associate the ten source columns that appear with the following target properties:

ObjectID	Object ID
TypeClass	Type (Class)
Name	Name
FirstName	First Name
MiddleName	Middle Name
LastName	Last Name
Suffix	Suffix
Status	Status
Email	Email
Person_ID	Person_ID

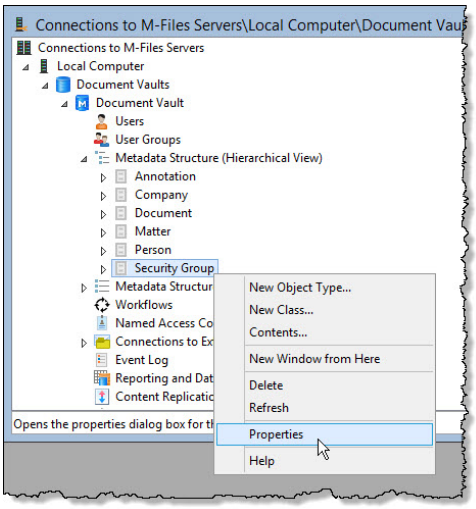
12. Click **Apply** to synchronize data from eCounsel into the Document Vault**.** A full refresh of this object type initially populates the values in the list. Click the **Contents…** button and check that data has been imported.
13. If no data appears in the **Contents** screen, click the **Refreshing Status…** button to view the current status of the refresh process or the last successful execution date and time.

The Document Vault synchronizes security rights so that documents inherit the security from their associated matters. In order to properly translate these security rights, the Document Vault users must be mapped to their corresponding "Staff" record from eCounsel.

Configuring Security Group Properties

To configure the Security Group properties:

1. In the M-Files Admin tool navigation tree, expand the desired vault and the **Metadata Structure (Hierarchical View)**.
2. Right-click **Security Group** and select **Properties**.



3. On the **General** tab, clear the *Users can create objects of this type* checkbox.
4. Configure the **General** tab and the **Connection to External Database** tab in the same way as you configured the Person properties, except for SQL configurations, enter **select * from DV_SecGroup** as the SELECT statement. For ORACLE configurations, enter the same statement but add the schema qualifier before the view name. For example, **select * from SchemaOwner.DV_SecGroup**.
5. Click the **Refresh Columns** button.
6. Associate the three source columns that appear with the following target properties:

ObjectID	Object ID
Name	Name
RelatedPeople	Related People

7. Click **Apply** to synchronize data from eCounsel into the Document Vault**.** A full refresh of this object type initially populates the values in the list. Click the **Contents…** button and check that data has been imported.

Associating Users to Staff Records

The final step of adding a new login account as a user on your vault requires mapping that login to the equivalent "Staff" (Person) record inside the vault. This step links the matter-level security to documents based on the user's logical group, private matter, and limited access rights.

To associate a Vault User to the Staff records:

1. Login to the M-Files client using an Administrator or Vault Admin account.
2. Navigate to the **Staff** folder and locate the Staff record of the new user. (Note: the records synchronize from eCounsel; if you do not see the person listed, the synchronization may not yet have occurred.)
3. On the **Metadata** card, click the Vault User field and select the correlating login account.
4. Click **Save**. This step applies the user's security across all existing documents. Depending on the size of the database, this step can take a while to complete.

Configuring Company Properties

To configure the Company properties:

1. In the M-Files Admin tool navigation tree, expand the desired vault and the **Metadata Structure (Hierarchical View)**.
2. Right-click Company and select **Properties**.
3. Configure the **General** tab and the **Connection to External Database** tab in the same way as you configured the Person properties, except for SQL configurations, enter **select * from DV_Company** as the SELECT statement. For ORACLE configurations, enter the same statement but add the schema qualifier before the view name. For example, **select * from SchemaOwner.DV_Company**.
4. Click the **Refresh Columns** button.
5. Associate the seven source columns that appear with the following target properties:

TypeClass	Type (Class)
ObjectID	Object ID
Name	Name
CompanyClassification	Company Classification
Status	Status
WebSite	Web Site
Company_ID	Company_ID

6. Click **Apply** to synchronize data from eCounsel into the Document Vault**.** A full refresh of this object type initially populates the values in the list. Click the **Contents…** button and check that data has been imported.
7. If no data appears in the **Contents** screen, click the **Refreshing Status…** button to view the current status of the refresh process or the last successful execution date and time.

Configuring Matter Properties

To configure the Matter properties:

1. In the M-Files Admin tool navigation tree, expand the desired vault and the **Metadata Structure (Hierarchical View)**.
2. Right-click Matter and select **Properties**.
3. Configure the **General** tab and the **Connection to External Database** tab in the same way as you configured the Security Group properties, except for SQL configurations, enter **select * from DV_Matters** as the SELECT statement. For ORACLE configurations, enter the same statement but add the schema qualifier before the view name. For example, **select * from SchemaOwner.DV_Matters**.
4. Click the **Refresh Columns** button.
5. Associate the 20 source columns that appear with the following target properties:

ObjectID	Object ID
TypeClass	Type (Class)
MatterNumberName	Matter Name (Number)
MatterName	Matter Name
LogicalGroup	Logical Group
MatterType	Matter Type
MatterStatus	Matter Status
OpenDate	Open Date
CloseDate	Close Date
Region	Region
State	State
Country	Country
LegalSection	Legal Section
LawArea	LawArea
LawSubArea	Law Subarea
FileNumber	File Number
ReadWriteAccess	Read Write Access
ReadOnlyAccess	Read Only Access
Matter_ID	MatterID
MatterNumber	Matter Number

6. Click **Apply** to synchronize data from eCounsel into the Document Vault**.** A full refresh of this object type initially populates the values in the list. Click the **Contents…** button and check that data has been imported.
7. If no data appears in the **Contents** screen, click the **Refreshing Status…** button to view the current status of the refresh process or the last successful execution date and time.

Configuring M-Files Web Access

M-Files Web access requires .NET Framework version 4.0 (or higher) and Internet Information Services (IIS) on the server machine.

M-Files Web can be accessed through a **Matter** tab in eCounsel by deploying the *Web Page Container* widget. The number of results displayed inside the *Web Page Container* widget is limited to 500.

To enable web access to M-Files:

1. Open the  M-Files Admin tool.
2. On the **M-Files Admin** window, click the **Help** menu and select *Help on M-Files Admin*.
3. Search for the "Enabling Web and Mobile Access" topic in the M-Files User Guide Help.
4. Follow the instructions to enable the M-Files Web Client.

To enable the Java applet for M-Files Web:

1. Open a browser and navigate to http(s)://<*Your M-Files Web domain*>/Configuration.aspx.
2. Login with system administrator credentials.
3. In the navigation pane, expand **Vault-specific settings**.
4. Select the appropriate vault and set the *Java applet* option to **Enable**.

To configure the Web Page Container widget in eCounsel:

1. Open Suite Manager.
2. On the **Suite Manager** control panel, click the **Widgets** component in the *System Configuration* area.
3. On the **Widgets** window, click **Import**.
4. On the **Select the XML or Script File for Import** dialog box, select the *XML Files* type, navigate to the **WebPageContainerWidget.xml** file provided by Mitratech, and click the **Open** button.
5. On the **Widget Information** dialog box, enter the following information:
    - The Uniform Resource Locator (URL) to access the M-Files Web page in the form:

      http://<*MFilesServer*>/Default.aspx?Searchpane=false&Taskpane=false#<*VaultGUID*>/views/_tempsearch?limit=500&0_o=0&00_p1027=$matterNumber.val$

      where:

      <*MFilesServer*> is the fully qualified name of the server machine on which the M-Files Web Client is installed

      <*VaultGUID*> is the Mitratech Document Vault identifier (such as 4E369F48-228E-4923-A662-103C4C31437F); to identify the vault GIUD, right-click the name of the vault in the M-Files Admin tool and select *Properties*

      Note: With this configuration, the number of results that are display in eCounsel is limited to 500 files.

- The number of pixels used to determine the height of the Web page for optimal display.
- Click the *Display as popup* checkbox to create a blank page to display the Web page (as opposed to displaying the contents of the Web page on the tab).
- If encryption is used, the type of encryption and key to be used to encrypt information passed between Bridgeway Suite and the Web page. Currently, Mitratech supports the com.bridgeway.utilities.BSICrypt3DesSpec encryption provider (an encryption algorithm using the Cryptix engine).

6. On the **Widget Information** dialog box, click **Save and Close**.
7. See the *Web Page Container Widget Guide* for information on configuring access to the widget in eCounsel.

Configuring Email Integration

If you are not using the Microsoft Outlook plug-in and want to drag-and-drop emails onto the Web client, you can configure how metadata properties are automatically populated. **Since most users will be using the plug-in to drag-and-drop e-mails, this section is optional.**

To configure email client integration properties:

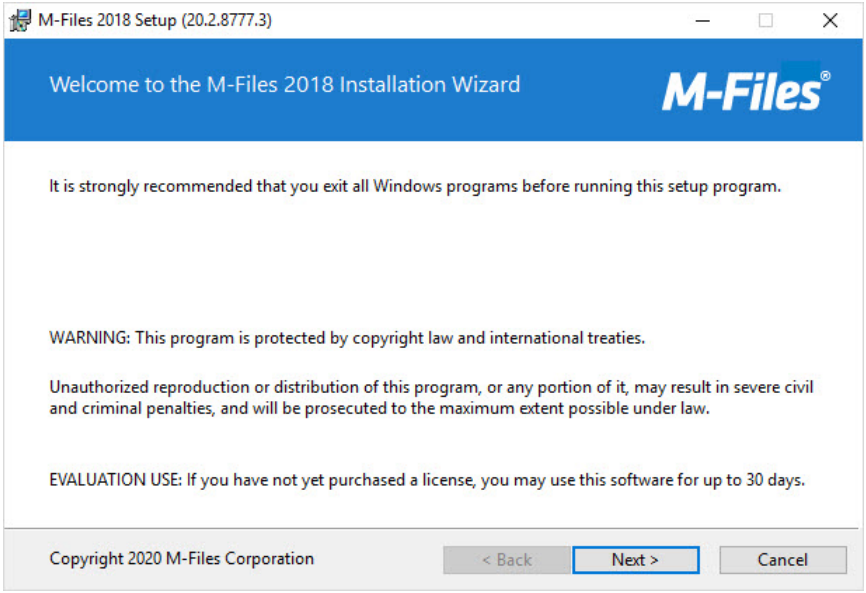
1. Open the  M-Files Admin tool.
2. Expand the **Local Computer** node and the **Document Vaults** node in the treeview.
3. Right-click on the Document Vault and select **E-mail Client Integration Settings**.
4. Select the **Advanced** tab.
5. For each of the fields, select the header field values from which you want M-Files to pull the metadata.
6. Click **OK**.

Installing the Mitratech Document Vault Client

Once Mitratech Document Vault has been installed, configured, and synchronized with eCounsel, named users can install the M-Files Client on their desktop.

To Install the M-Files Client:

1. Double-click on the M-Files Client installation file provided by Mitratech to start the installation process.
2. On the **Welcome to M-Files 2018 Installation Wizard**, click **Next**.



3. On the **License Agreement** screen, review the license agreement, click *I accept the license agreement* to continue, and click **Next**.

4. M-Files will install the files in a default location. Click **Finish** when the installation has completed.
5. Create a document vault connection.

Upgrading Mitratech Document Vault

You can only upgrade to Mitratech Document Vault 3.2 from Mitratech Document Vault 2.1. If you have an earlier version, you must upgrade to Mitratech Document Vault 2.1 first.

To upgrade Mitratech Document Vault:

1. Upgrade the M-Files server and clients.
2. Update the Vault Structure.
3. Verify and enable the event handlers.

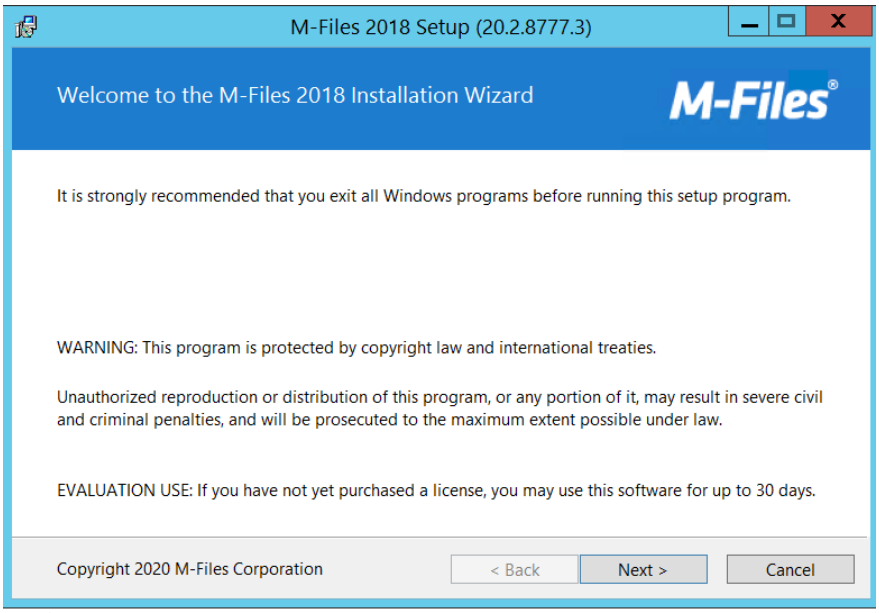
Upgrading M-Files

In order to upgrade to a new version of the M-Files Server and M-Files Client, use the steps below.

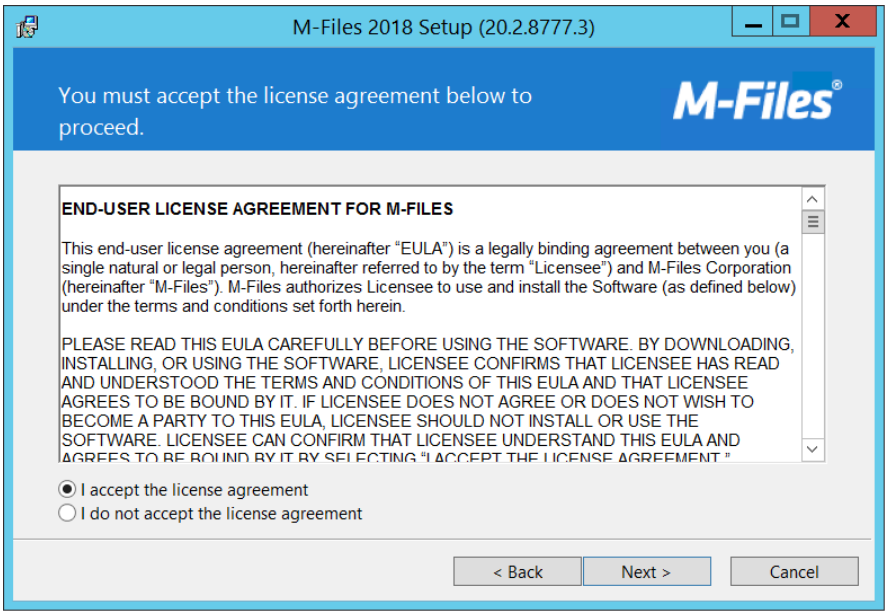
Upgrading M-Files Server

To upgrade the M-Files Server:

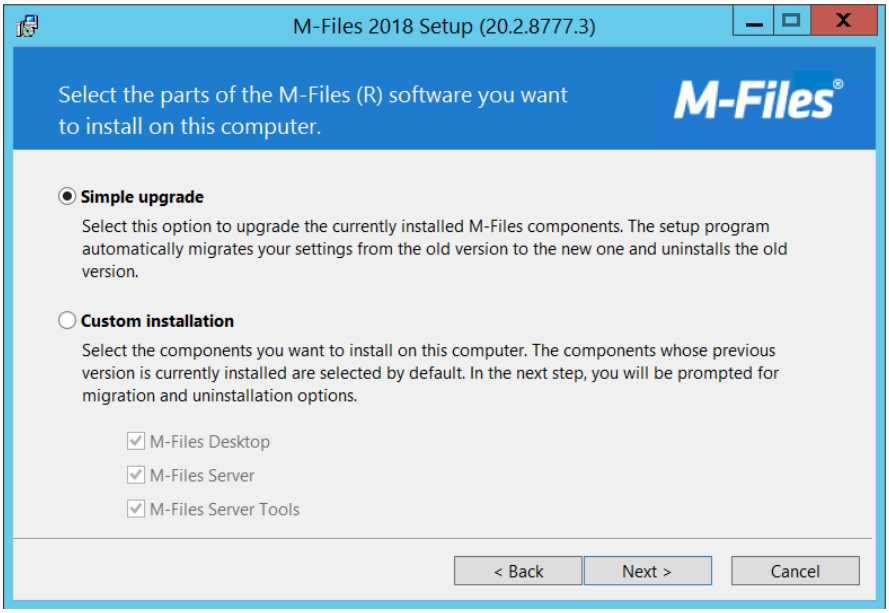
1. Double-click on the M-Files Mitratech installation file provided by Mitratech to start the installation process.
2. On the **Welcome to the M-Files 2018 Installation Wizard**, click **Next**.



3. On the **License Agreement** screen, review the license agreement, click *I accept the license agreement* to continue, and click **Next**.



4. On the **Installation Type** screen, select *Simple upgrade*. Click **Next**.

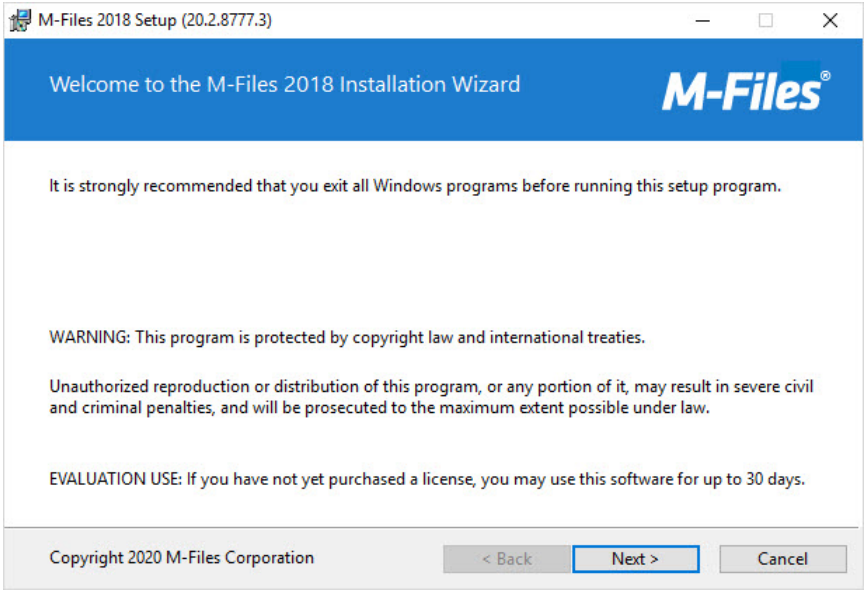


5. On the **Ready to Install** screen, click **Next**.
6. M-Files will overwrite the files in the location. Click **Finish** when the installation has completed.

Upgrading M-Files Clients

To Upgrade the M-Files Client:

1. Double-click on the M-Files Mitratech installation file provided by Mitratech to start the installation process.
2. On the **Welcome to the M-Files 2018 Installation Wizard**, click **Next**.



3. On the **License Agreement** screen, review the license agreement, click *I accept the license agreement* to continue, and click **Next**.

4. M-Files will install the files in the installation location used for the previous installation. Click **Finish** when the installation has completed.

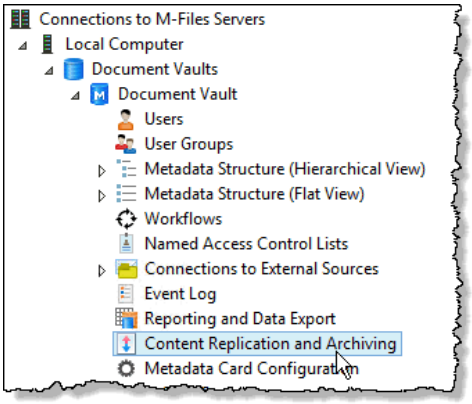
Updating the Vault Structure

Before you begin:

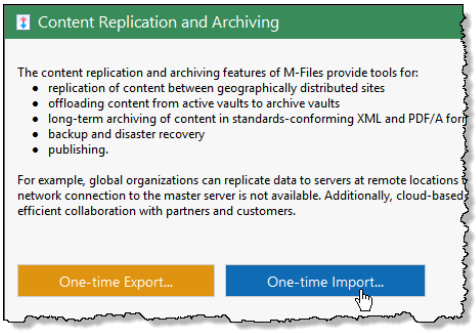
- Create a backup copy of the vault.
- Save the contents of the **Document Vault** folder in the installation media to a convenient location on your machine.
- Extract the contents of the **vault 29 to 30 patch import file.zip** file (provided with Document Vault 3.1). If you are upgrading from Document Vault 2.1, you will need to first use the **vault 25 to 28 patch import file.zi**p file; if you are upgrading from Document Vault 3.0, you will need to use the **vault 28 to 29 patch import file.zip** file also.

The following actions are required for **each** document vault that is being updated **before** the Document Vault update is installed:

1. Open the M-Files Admin Tool.
2. In the navigation pane on the left, expand **Local Computer** and then **Document Vaults**. Expand the document vault that you want to update and click **Content Replication and Archiving**.

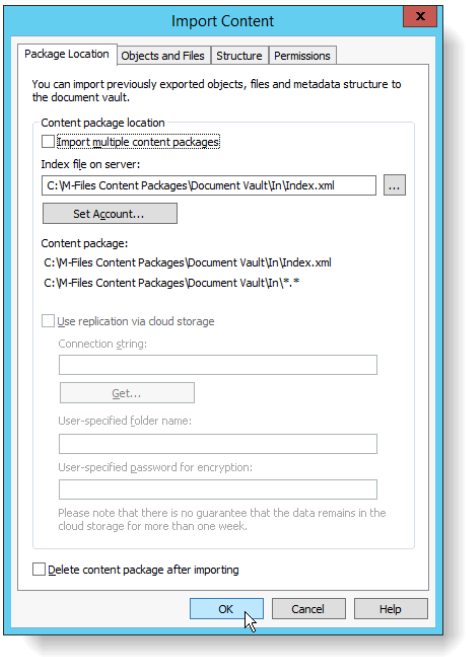


3. In the *Content Replication and Archiving* pane, click the **One-time Import...** button.



.

4. In the **Import Content** dialog box, browse to the **index.xml** file in the patch folder and click **OK**.



5. A summary of the content to be imported appears and prompts "Do you want to proceed with importing of the content above?" Click **Yes**.
6. The content is imported. Click **OK** on the confirmation dialog box.

Verifying and Enabling the Event Handlers

Verify and enable the Event Handlers

1. In the navigation pane, right-click the vault and choose **Event Handlers** from the context menu.
2. Make sure all 15 event handlers are present and each checkbox is selected.

SAML Authentication

SAML (Security Assertion Markup Language) is an XML-based protocol for controlling authentication between Identity Provider (IdP) and the service provider. This integration allows IdP, using LDAP (Lightweight Directory Access Protocol), to be configured to use Microsoft Windows Active Directory (AD) or OpenLDAP as a username and password directory. This integration needs to be configured to specify the IdP service to use in order to authenticate user logins.

For information on configuring SAML in M-Files, refer to the M-Files document *Configuring SAML 2.0 for M-Files Authentication*.

For information on configuring SAML in Suite Manager, refer to the *Bridgeway Suite Login Authentication Guide*.

Troubleshooting

Why is a user who is inactive in eCounsel still active in Mitratech Document Vault?

Inactivating a user in eCounsel does not inactivate the user in Mitratech Document Vault. The vault administrator must deactivate the account using the Administrator Tool in M-Files. In addition, if the associated person in eCounsel is inactive or has been deleted, the vault administrator must perform the same action in M-Files.

Why is my eCounsel user not created in M-Files?

If a person in eCounsel is associated with multiple users in Suite Manager, the integration is not able to create the correct user/person association in M-Files. Contact your eCounsel administrator to make sure that only one user in Suite Manager is associated with a single person in eCounsel.

Why can't I login to Mitratech Document Vault?

Make sure you have a valid eCounsel account, and the account is not locked. Also, contact your eCounsel administrator to make sure the eCounsel security attribute is set to *Allow* for Mitratech Document Vault (at group or user level).

Why is a deleted matter still appearing in M-Files?

Although you can delete a matter in eCounsel, the matter still appears in M-Files for data integrity reasons. Once any record has been synchronized with M-Files, it will not be removed from M-Files. Status updates to the record will still occur.

Why am I getting an unspecified error (too many lookups)?

Make sure the document is not already saved to a different matter. You can only save a document to a single matter.

Why can't I change the matter name?

You cannot change the metadata such as matter name. You will get an error and must discard the changes.

Why can't I modify matters/people/entities?

eCounsel is the "system of record" for all data being synchronized with Mitratech Document Vault. Any changes to the specific data (such as name, matter type, etc) should be made in eCounsel. Use the link to eCounsel to open the record to make data changes.

Why isn't my new matter appearing in Mitratech Document Vault?

When you add a matter to eCounsel or edit an existing record, data synchronization may have a short lag time. Data is automatically refreshed with a default sync time of 15 minutes for new matters and 24 hours for any other updates. However, data can manually be refreshed at any time. For example, a user may want to add a document to the Document Vault immediately after adding a new matter to eCounsel. To refresh the data"

1. Click the **Refresh** icon on the document Metadata card.
2. Select the type of refresh:
    - A **Quick** refresh updates the system with only new matters and new objects.
    - A **Full** refresh is required if security updates have been made to existing records.

Why am I getting a warning that Java is not updated in the Chrome browser?

- Make sure that the version of Java is up-to-date.
- Enter "chrome://flags/#enable-npapi" in the Chrome browser address bar. Click the **Enable** link for the Enable NPAPI configuration option. Click the **Relaunch** button that now appears at the bottom of the configuration page.
- Restore the Java security prompts settings to their default values. In the Microsoft Windows Control Panel, double-click **Java**. On the **Security** tab, click the **Restore Security Prompts** button.
- Add an exception for your website. On the **Security** tab of the Java Control Panel, click the **Edit Site List** button and add the web site with the https:// or http:// prefix.
- Remove all downloaded mffta.jar resources from the Java cache. On the **General** tab of the Java Control Panel, click the **View** button for the Temporary Internet Files. Select **Resources** from the **Show** dropdown list and then delete all resources named like "mffta.jar".
- Restart the browser application.

Why am I having connectivity issues with the M-Files Server?

If your company uses computer security software such as Websense, contact your vault administrator to add the M-Files Server to your company's list of acceptable sites. Also, make sure you log out of the Mitratech Document Vault Web client prior to closing the browser. Closing the browser without logging out may cause a delay in being able to log in again.

Why aren't I seeing the Document Vault folder in Microsoft Outlook?

Verify that the M-Files Office Add-in has not been disabled in Microsoft Outlook.

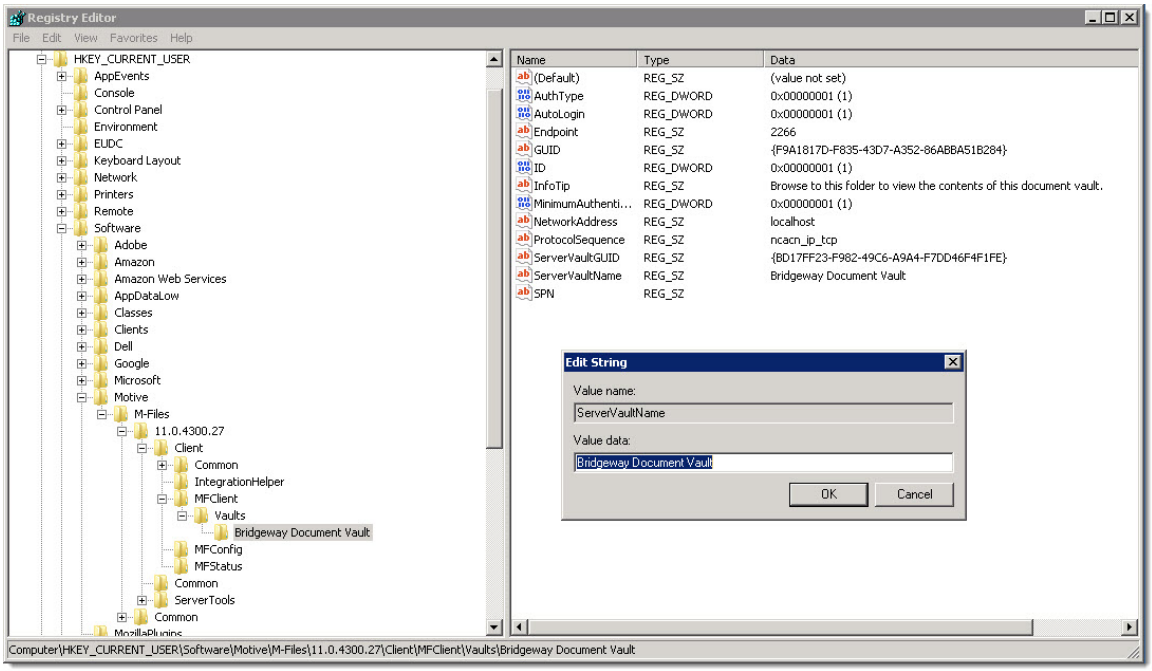
Appendix

M-Files Microsoft Windows Registry Settings

Windows Registry settings are installed on the M-Files Server machine and on each machine where the M-Files client is installed. If a vault is restored or imported with a name other than "Document Vault", you must edit the setting on each user's computer to match the vault name.

To change the vault name in the Registry on the M-Files Server machine:

1. Open the Registry Editor on the M-Files Server machine.
2. Navigate to the **Computer / HKEY_CURRENT_USER / Software / Motive / M-Files / 20.2.8777.3 / Client / MFClient / Vaults / Document Vault** folder.
3. Double-click on the ServerVaultName key.
4. On the **Edit String** dialog box, type the value for the vault name and click **OK**.

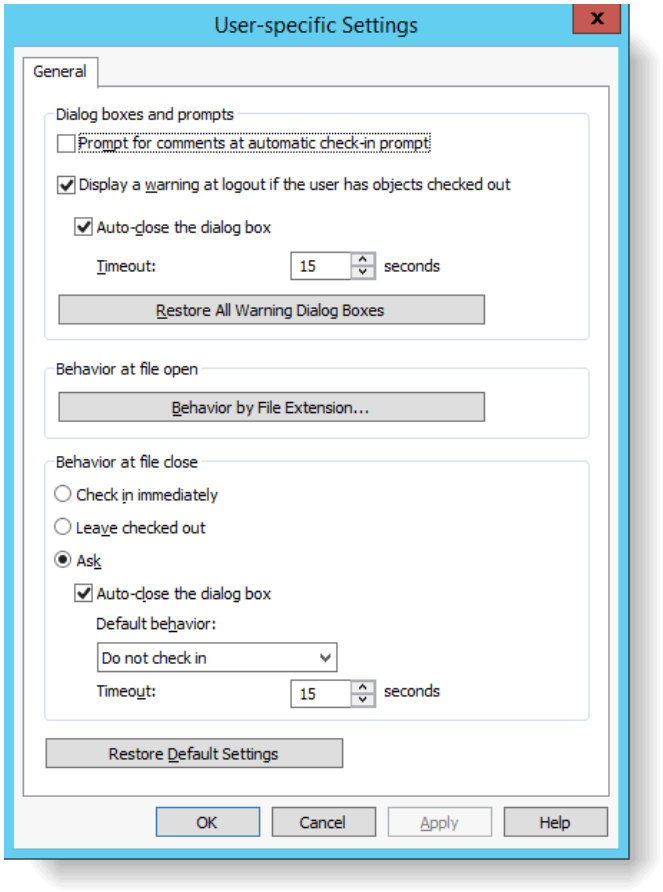


5. Search for "Document Vault" throughout the Registry and change all to be consistent with the vault name.

User- and Computer-Specific Settings

User-specific Settings

To access user-specific settings, open the M-Files Desktop Settings and click the **User-specific Settings** button on the **Settings** tab.



Dialog boxes and prompts

If **Prompt for comments at automatic check-in prompt** is selected, the user is prompted for comments when a document is checked in. Note: if the *Check in immediately* option has been selected in the *Behavior at file close* area, the user will not be prompted for comments.

By default, **Display a warning at logout if the user has objects checked out** and **Auto-close the dialog box** are selected.

Behavior at file open

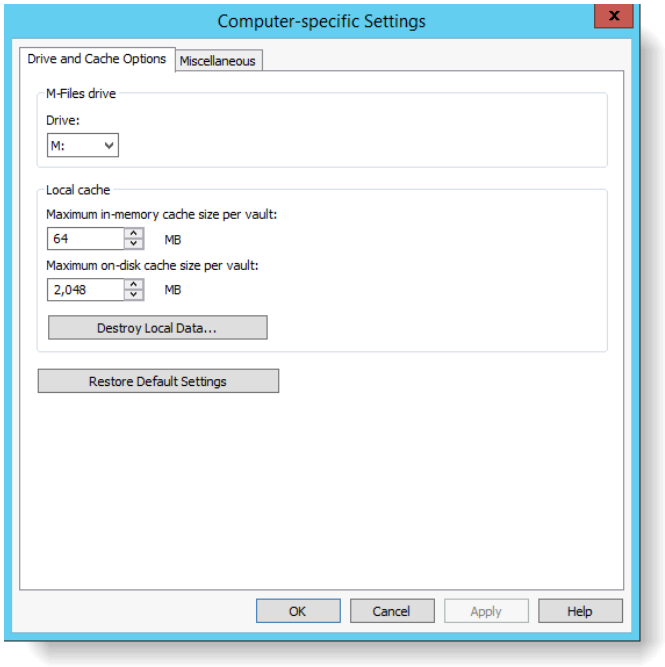
In this area, you can define whether a particular file format is always opened in a state of *Check Out* or *Open as read-only*, or if you want the user to specify the state in which a file of a certain format is opened.

Behavior at file close

The definitions specified here define which actions are performed when a file is closed and apply to all file formats. By default, the user is prompted for action when a file is closed. If the user does not change the default procedure (Do not check in), the dialog box automatically closes after a designated time and the document remains checked out.

Computer-Specific Drive and Cache Settings

To access the computer-specific drive and cache settings, open the M-Files Desktop Settings and click the **Computer-specific Settings** button on the **Settings** tab.



M-Files Drive

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

Local cache

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

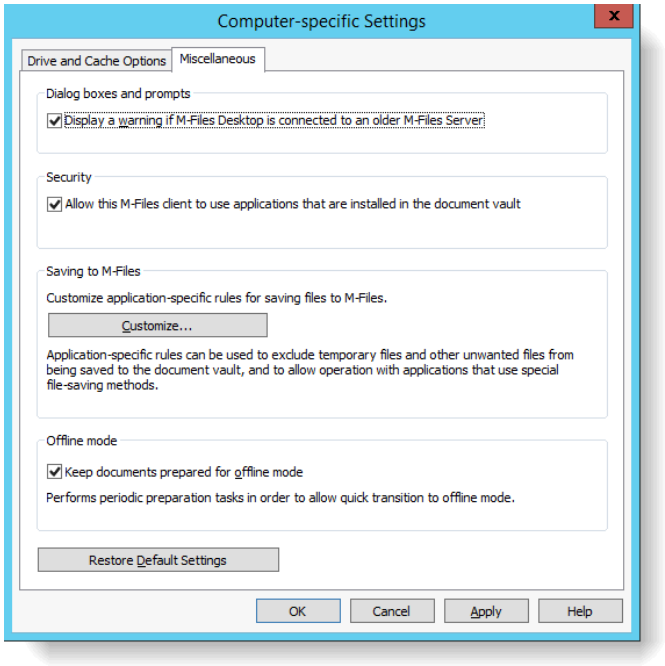
- **Maximum in-memory cache size per vault** - the maximum amount of the computer's main memory that the document cache is allowed.
- **Maximum on-disk cache size per vault** - the maximum amount of the computer's disk space that the document cache is allowed.

Destroy Local Data

M-Files saves information about the documents locally in the computer's cache. The data remains on the server, but the cache makes M-Files faster to use. If this local cache needs to be destroyed, click **Destroy Local Data**. Local cache information about the documents by user and by document vault will be destroyed.

Miscellaneous Computer-specific Settings

To access the computer-specific drive and cache settings, open the M-Files Desktop Settings, click the **Computer-specific Settings** button on the **Settings** tab, and select the **Miscellaneous** tab on the **Computer-specific Settings** dialog box.



Dialog boxes and prompts, Security

The default settings in this area are:

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

Saving to M-Files

You can customize application-specific rules for saving files to M-Files. For example, application-specific rules can exclude temporary files and other unwanted files from being saved to the document vault. Rules can also allow operation with applications that use special file saving methods. For example, a rule can guarantee that a metadata card of new files is displayed if automatic identification is not functioning.

To add a new behavior, click the **Customize** button and then click the **Add...** button.

On the **General** tab, you can change the **Detect file save operations from standard file dialog boxes** setting. You can also specify which file formats are always accepted or always excluded from being saved in M-Files.

On the **Advanced** tab, you can change the **Detect file closing and apply user-specific check-in behavior** setting. You can also define process-specific file formats that will be immediately checked-in when the new file with the appropriate extension has been saved and the metadata card has been completed.

Offline mode

By default, the documents are kept ready for the offline mode. You can deselect this option if the workstation is never used offline or if the offline state seems to cause additional load for the machine.

Export Vault Connections and Settings

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

By sharing and enabling the exported registry file on other computers, you can use common M-Files configuration data on several computers. The export options are on the **Settings** tab of the M-Files Desktop Settings component.

Index