M-FILES CORPORATION

SETTING UP AND USING M-FILES FOR GOOGLE WORKSPACE ADD-ON

LAST UPDATED 2 OCTOBER 2024

VERSION 3.5

Contents

1. Introduction

The M-Files for Google Workspace add-on lets you save your Google Drive and Gmail content to your M-Files vault directly from Google Chrome. You can use Google Workspace also in Multi-Server Mode. This document explains how to set up and use the add-on.

For instructions on setting up and using the M-Files Google Drive connector, which provides access to content residing in Google Drive accounts via the M-Files user interface, refer to Installing, Configuring, and Using M-Files Google Drive Connector.

The information in this document applies to the add-on version 6.0.4 and later.

1.1 Prerequisites

Please make sure your environment meets these requirements:

PRODUCT	REQUIRED VERSION
M-Files Desktop	M-Files Online
M-Files Server	M-Files Online
Google Chrome	75.0.3770 or later

Before you set up the M-Files for Google Workspace add-on, make sure that:

- You have a license for M-Files for Google Workspace. To get the license, write to licensing@m-files.com.
- M-Files server is enabled with web access and HTTPS connection protocol.

Note: Only M-Files single sign-on (SSO) login is supported with Google Workspace accounts.

2. Setting Up Your M-Files Vault

If your vault is in M-Files Cloud, you can skip section 2.1.

2.1 Web Access and HTTPS Connection

To use M-Files with Google Workspace, web access and HTTPS connections are mandatory in the server setup process. If you use M-Files Cloud, you can skip these steps and continue to section 2.2.

To set up web access, Internet Information Services (IIS) Manager needs to be configured correctly at the server level. In addition, HTTPS connection needs to be enabled for web access.

For more information on setting up web access and enabling IIS components, refer to Enabling the Necessary Internet Information Services (IIS) Components. For more information on enabling HTTPS connection, refer to HTTPS Connections to M-Files Server.

2.1.1 Restricting the Add-on Web Access

By default, the web access of the M-Files for Google Workspace add-on is not limited to any specific domains. However, you can allow access only for the needed sites using Chrome policies.

To limit the site access of the add-on:

1. Log in to https://admin.google.com/ with your Google Workspace account.
2. Click **Devices** to access the *Device management* page.
3. Under *Device settings*, select **Chrome Management**.
4. Select **Apps and extensions**. Click the cogwheel icon to access the *Additional application settings* page.
5. **Optional**: In the left-side menu, select the desired Google Workspace organization.
6. Scroll down to the section *Block extensions by permissions* to define the allowed and blocked sites.

   Note that the selection does not affect forced installed extensions.
7. To *Runtime blocked hosts,* enter `*://*` to block all URLs.
8. To *Runtime allowed hosts,* enter these mandatory URLs:

   ```
   https://mail.google.com
   https://drive.google.com
   https://docs.google.com
   https://goomfiext.appspot.com
   https://www.googleapis.com
   https://storage.googleapis.com
   ```
9. Still in *Runtime allowed hosts*, add the vault URLs that you want to access with the add-on. You can define complete URLs (for example, `https://my-vault.my-domain.com`) or sets of URLs with an asterisk (*) (for example, `https://*.my-second-domain.com`).

   > **Note:** You cannot use path components in the URL (for example, https://my-vault.my-domain.com/REST/*).

10. Click **SAVE**.

    The changes are propagated to the Google Workspace customer level.

Before you continue, wait a few seconds to make sure that the changes have been applied. Then, do these steps to check that the settings are correct:

11. Open the Chrome browser and log in to it with a Google Workspace account that the policies apply to.
12. Go to the Policies page `chrome://policy`.
13. Find the **ExtensionSettings** policy setting in the list and check that:
    a. Source is **Cloud**.
    b. Status is **OK**.
    c. On **Policy value**, allowed URLs are listed in **runtime_allowed_hosts**, and **runtime_blocked_hosts** has the value `*://*`.

For more information, refer to these Google instructions.

Note: Local device or Windows Group Policies and Linux policies take precedence over Chrome policies. For more information on Chrome policy management, refer to these Google instructions.

2.2 M-Files Single Sign-On with Google Workspace Accounts

M-Files SSO with Google Workspace accounts provides the login process with Google identities. The setup also enables users to use M-Files for Google Workspace without a separate login.

2.2.1 Setting Up User Login Accounts

To use a Google Workspace account to log in to M-Files, the M-Files user account must match the Google Workspace account.

If you use M-Files Cloud and you do not have the necessary Windows login accounts set up, contact support@m-files.com to help you with the setup.

To set up user login accounts that match the respective Google Workspace email addresses:

1. Open M-Files Admin.
2. Expand a server connection and select **Login Accounts**.
3. Click **New Login Account** on the task area.

   The *New Login Account* dialog opens.
4. In *Username*, enter the username part of the Google Workspace email address.

   For example, if the user's email address is `bob@example.fi`, the value is `bob`.
5. Under *Authentication*, select **Windows authentication**.
6. In *Domain or computer*, enter the Google Workspace domain, such as `example.fi`.

   The *Windows account* field gets automatically filled with `<Google Workspace domain>\<username>`. For example, if the user's email address is `bob@example.fi`, the is `example.fi\bob`.
7. Fill in other information according to the instruction in the M-Files user guide.
8. Click **OK**.
9. **Optional:** Do the steps from 3 to 8 to add more login accounts.
10. Add the accounts as vault users.

    For instructions, refer to Creating a User in the M-Files user guide.

2.2.2 Configuring OpenID Connect or OAuth 2.0 authentication for M-Files Server

To configure M-Files Server, use the configurations editor in M-Files Admin. In on-premises environment, you can alternatively apply registry key settings on the server computer.

Using the configurations editor in M-Files Admin to configure M-Files Server

Please make a note that the settings are vault specific, and they will only work in M-Files Web when it is accessed using a DNS name that is mapped to a specific vault.

For instructions, refer to Configuring OpenID Connect and OAuth 2.0 for M-Files Authentication and use these values:

SETTING LOCATION	SETTING NAME	VALUE
Scope > **Configurations** > **Configuration**	Name	Google (for example)
	Authentication protocol	OpenID Connect or OAuth 2.0
Scope > **Configurations** > **Configuration** > **Settings** > **Server**	OpenID Provider metadata URI	https://accounts.google.com/.well-known/openid-configuration
	AccountClaim	email
	Audience	The same value as in **Scope** > **Configurations** > **Configuration** > **Settings** > **Client** > **ClientID**.
	Show advanced options	Yes
	EnableLogging	true
	AccessTokenType	Opaque token
	Keep AccessTokenType value	Yes
	UserInfoEndpoint	https://www.googleapis.com/oauth2/v2/userinfo
	Keep UseIdTokenAsAccessToken value	true
Scope > **Configurations** > **Configuration** > **Settings** > **Client**	DisplayName	Google
	ClientID	Refer to Obtain OAuth 2.0 credentials.
	Show advanced options	Yes
	ClientSecret	Refer to Obtain OAuth 2.0 credentials.
	AuthorizationEndpoint	https://accounts.google.com/o/oauth2/v2/auth
	TokenEndpoint	https://oauth2.googleapis.com/token
	Scope	openid profile email
	UseIdTokenAsAccessToken	false
	UseAccessTokenInWeb	true

Using registry key settings to configure M-Files Server

To set up M-Files SSO with Google Workspace accounts, add the following registry key settings on the server computer:

Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer\Authentication\Scopes\Host:<M-Files Web DNS>:Windows\Plugins\MFiles.AuthenticationProviders.OAuth`

Value name	`Configuration`
Value type	REG_SZ

Description	The value refers to the symbolic name of the configuration that is specific to this authentication scope.
Value	`GoogleSSO` (for example)

Value name	`IsDefault`
Value type	REG_DWORD
Description	The value specifies whether this plugin is the default plugin for the specified authentication scope.
Value	`1` (true)

Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer\Authentication\Configurations\<Configuration>`

Value name	`ForceDownLevelAccountName`
Value type	REG_SZ
Description	The UPN-style account names are, by default, converted into down-level style accounts. For instance, `myUsermane@myDomain.com` → `myDomain.com\myUsername`. By setting ForceDownLevelAccountName to "true", the user accounts must be created in M-Files as Windows accounts. For instance, if the original user account name is `MyUsername@myDomain.com` and the `ForceDownLevelAccountName` is "true", create a Windows account in M-Files with the name `myDomain.com\myUsername`.
Value	true

Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer\Authentication\Configurations\<Configuration>\ClientSpecific`

Value name	`Protocol`
Value type	REG_SZ
Description	Defines the protocol for the plugin and configuration.
Value	`OAuth 2.0`

Value name	`Enablelogging`
Value type	REG_SZ
Description	If true, M-Files writes more detailed information about the authentication flow to the Windows application log, including the messages with the information entry type.
Value	`true`

Value name	Scope
Value type	REG_SZ
Description	Scope (authorization scope) defines an access to a particular resource. With scope, you can define to what kind of resources the requested access token has access on the resource server. For example, if the authorization code is requested with an "email" scope, the access token exchanged from the authorization code will have access to user-related data that has the same "email" scope defined.
Value	`https://www.googleapis.com/auth/userinfo.email`

Value name	AuthorizationEndpoint
Value type	REG_SZ
Description	AuthorizationEndPoint is the endpoint where M-Files sends the request for an authorization token. The authorization token is exchanged into an access token in the next phase. When the resource owner receives the request, it identifies the requesting application (M-Files) and the user by asking for an authorization from M-Files to use the user's identity, and then sends the authorization token back to M-Files.
Value	`https://accounts.google.com/o/oauth2/auth`

Value name	Tokenendpoint
Value type	REG_SZ
Description	TokenEndpoint is the endpoint where M-Files sends the authorization token to and receives the access token from. After receiving the authorization token from AuthorizationEndpoint, M-Files exchanges the authorization token to an access token by sending a request to TokenEndpoint. The authorization server validates the authorization token and returns an access token back to M-Files.
Value	`https://accounts.google.com/o/oauth2/token`

Value name	Clientid
Value type	REG_SZ
Description	Web Application Credentials Client ID from Google Developer Console. ClientID identifies the requesting application (M-Files) to the authorization server. Stands for the client_id parameter in the OAuth 2.0 specification. For more information on creating a Client ID, see the previous section.
Value	`fe19542e-d352-4499-bd9c-24cd6b2183ca` (for example)

Value name	Clientsecret
Value type	REG_SZ
Description	Web Application Credential Client Secret, which is linked to Client ID. The value of ClientSecret is visible to the clients, so it is not considered to be a secret in this context. For more information, see the previous section.
Value	Ywv14txfGNajhsd7Vues48H0R (for example)

Value name	RedirectURI
Value type	REG_SZ
Description	RedirectURI is affects M-Files Desktop, M-Files Admin, M-Files Desktop Settings, and M-Files Web. The redirect URI is added into the HTTP request as the redirect_uri parameter value when requesting for authorization code or access token from the authorization server. The authorization server returns the code or access token to the given URI if it matches the one configured on authorization server. The same redirect URI must usually be configured as trusted also in the authorization server.
Value	https://**<M-Files Web DNS>/**authentication/<configuration name>/read

Value name	RedirectURIForNative
Value type	REG_SZ
Description	RedirectURIForNative only affects M-Files Desktop, M-Files Admin and M-Files Desktop Settings. The redirect URI is added into the HTTP request as the redirect_uri parameter value when requesting for authorization code or access token from the authorization server. Authorization server returns the code or access token to the given URI if it matches the one configured on the authorization.
Value	https://**<M-Files Web DNS>**

Value name	RedirectURIForWeb
Value type	REG_SZ
Description	RedirectURIForWeb only affects M-Files Web. The redirect URI is added into the HTTP request as the redirect_uri parameter value when requesting for authorization code or access token from the authorization server. Authorization server returns the code or access token to the given URI if it matches the one configured on the authorization server. The same redirect URI must usually be configured as trusted also in the authorization server.
Value	https://**<M-Files Web DNS>**/authentication/<configuration name>/read

Value name	`RedirectURIForMobile`
Value type	REG_SZ
Description	RedirectURIForMobile only affects M-Files Mobile. If this value is set, the login page is opened in the default browser of the mobile device. Otherwise, the application uses either the RedirectURI or the RedirectURIForNative value, and the login page is displayed in an embedded browser in the application. Note that using the embedded login page option may be deprecated for certain identity providers (such as Google). **Note**: Supported in M-Files mobile apps for iOS and Android. Requires M-Files 11.3.4330.196 or later. The redirect URI is added into the HTTP request as the redirect_uri parameter value when requesting for authorization code or access token from the authorization server. Authorization server returns the code or access token to the given URI if it matches the one configured on the authorization server. The same redirect URI must usually be configured as trusted also in the authorization server. Use the following format to form RedirectURIForMobile: https://<M-Files Mobile DNS>/authentication/<configuration name>/mobile
Default value	`https://<M-Files Mobile DNS>/authentication/<configuration name>/mobile`

Key	`HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer\Authentication\Configurations\<Configuration>\ServerSpecific`

Value name	`Accountclaim`
Value type	REG_SZ
Description	The name of the main claim representing the user's account name, expected response from authorization server when exchanging the access token to user account information or a JWT token.
Value	`email`

Value name	`AccessTokenType`
Value type	REG_SZ
Description	The type of token to use. When the token is used for authentication only, it is usually `JWT`. If you use other Google services, such as Google Workspace or Gmail integration, set it to `opaque`. If you set the token type to `opaque`, also add the `PreserveServerSpecificSetting_AccessTokenType` registry key.
Value	`opaque or JWT`

Value name	`PreserveServerSpecificSetting_AccessTokenType`

Value type	REG_SZ
Description	If you set `AccessTokenType` to `opaque`, you must add this registry key with the value `true` so that the automatic metadata update does not override the `AccessTokenType` setting. Otherwise, the default value JWT is used.
Value	`true`

Value name	`UserInfoEndpoint`
Value type	REG_SZ
Description	The endpoint where M-Files sends the access token within an HTTP authorization header. For instance, `Bearer va.x7khd789as8d7asd`. The identity provider verifies the access token, and if this succeeds, the IdP returns the user claims as JSON.
Value	`https://www.googleapis.com/oauth2/v2/userinfo`

The following example registry template and the attached *Example SSO registry settings.txt* file help you add the registry key settings.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer\Authentication]
[HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer\Authentication\Configurations]
[HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-
Files\<version>\Server\MFServer\Authentication\Configurations\<Configuration>]
"ForceDownLevelAccountName"="true"

[HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-
Files\<version>\Server\MFServer\Authentication\Configurations\<Configuration>\ClientSpecific]
"Protocol"="OAuth 2.0"
"Enablelogging"="true"
"Tokenendpoint"="https://accounts.google.com/o/oauth2/token"
"Scope"="https://www.googleapis.com/auth/userinfo.email"
"AuthorizationEndpoint"="https://accounts.google.com/o/oauth2/auth"
"Clientid"="<Clientid>"
"Clientsecret"="<Clientsecret>"
"RedirectURI"="https://<M-Files Web DNS>/authentication/<Configuration>/read"
"RedirectURIForNative"="https://<M-Files Web DNS>"
"RedirectURIForWeb"="https://<M-Files Web DNS>/authentication/<Configuration>/read"
"RedirectURIForMobile"="https://<M-Files Mobile DNS>/authentication/<Configuration>/mobile"

[HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-
Files\<version>\Server\MFServer\Authentication\Configurations\<Configuration>\ServerSpecific]
"Accountclaim"="email"
"AccessTokenType"="opaque"
"PreserveServerSpecificSetting_AccessTokenType"="true"
"UserInfoEndpoint"="https://www.googleapis.com/oauth2/v2/userinfo"

[HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer\Authentication\Scopes]
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer\Authentication\Scopes\Host:<M-Files Web DNS>:Windows]

[HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer\Authentication\Scopes\Host:<M-Files Web DNS>:Windows\Plugins]

[HKEY_LOCAL_MACHINE\SOFTWARE\Motive\M-Files\<version>\Server\MFServer\Authentication\Scopes\Host:<M-Files Web DNS>:Windows\Plugins\MFiles.AuthenticationProviders.OAuth]
"Configuration"="<Configuration>"
"IsDefault"=dword:00000001
```

For more information on the keys and key settings, refer to Configuring OpenID Connect and OAuth 2.0 for M-Files Authentication.

2.2.3 Setting up OAuth Client ID

This section tells you how to set up a client ID using GCP (Google Cloud Platform). You can create a client ID also in other environments.

1. Log in to https://console.cloud.google.com with your Google Workspace account.
2. Create a new project. For instructions on creating a project, refer to these Google instructions.
3. Select the newly created project from the drop-down menu.
4. In the left-side menu, select *APIs & Services* > *Credentials*.
5. In the left-side menu, select **OAuth consent screen**.
6. Under *User type*, select **Internal**.
7. In *Application name,* enter the name for the application.
8. Click **Save**.
9. Go back to the Credentials page and select Create credentials > OAuth client ID.
10. In *Application type*, select **Web application**.
11. In *Authorized redirect URIs*, enter the URI `https://<M-Files Web DNS>/authentication/<configuration name>/read`. Make sure the redirect URI ends with `/authentication/<configuration name>/read`.

    Take the `configuration name` from the **Federated Authentication** settings of your vault:

    a. In M-Files Admin, go to the vault and select **Configurations > Federated Authentication**.
    b. On the **Configuration** tab, expand a scope. For example, `*` or `*Windows`.
    c. In **Scope**, expand **Configurations**.
    d. Under the configuration, copy the **Name** value. Avoid special characters in its value.

    If you have not yet done the configuration, see Adding Federated Authentication Configurations.
12. Click **Create**.

After a successful setup, the *OAuth client* dialog that shows your client ID and secret is shown. You need these values when you apply the registry key settings for the M-Files server (see the next section).

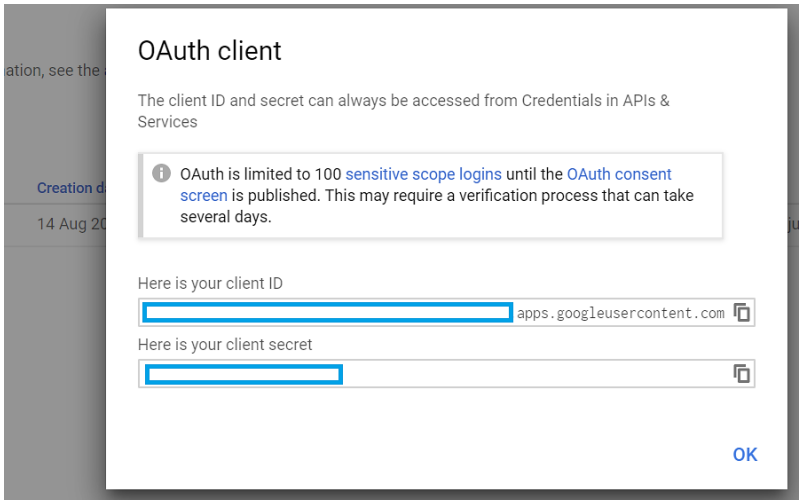


Image 2.2.2: *The OAuth client* dialog.

3. Google Admin Console

The add-on application must be marked as trusted so that it can access your Google Workspace data. M-Files for Google Workspace Admin (Admin Site) must also be marked as trusted to allow the use of Google Signin to access vault management. Refer to these Google instructions on how Google Workspace administrators can control application access.

Mark the apps with these IDs as trusted:

- **Beta**: 1073826182848-dc6odo2b5m6tsj71poaepo310q4tom2u.apps.googleusercontent.com
- **Production**: 1073826182848-ra668v5gkjl8b560ednucspp5kigpf4h.apps.googleusercontent.com
- **Admin Site**: 487249060432-7ct0lcrs2sis8qr11no3grvkj2um69sf.apps.googleusercontent.com

If your company uses a cloud access security broker (CASB), such as Cloudlock, make sure that the add-on is whitelisted for the CASB as well.

4. Admin Site

M-Files for Google Workspace Admin is the Admin Site tool for customers to configure their M-Files for Google Workspace usage. Log in to Admin Site as Super Admin to add admin users and organizational units. Additionally, you can set up servers and edit server and vault settings. This section tells you how to use Admin Site.

4.1 Accessing Admin Site

Before you access Admin Site, make sure that you have logged in to the Chrome browser with the Google Workspace account which has been given access to Admin Site. Also, turn sync on in Chrome.

Admin Site can be accessed from https://admin.workspace.m-files.com/. If your account does not have access to Admin Site, you will automatically be redirected to the Super Admin login page (see next section). If your account has the "Super Admin" role, enter your credentials again to log in to Admin Site.

4.1.1 Super Admin Login

When you have purchased M-Files for Google Workspace, you must have a Google Workspace account with the "Super Admin" role to get access to Admin Site. When you are logged in, you can use the tool to add new admin users (see section 4.3).

To log in as Super Admin:

1. Go to https://admin.workspace.m-files.com/super-admin-login.
2. Log in with a "Super Admin" Google Workspace account.

   Result: Admin Site asks for additional permissions to: *See info about users on your domain*. These permissions are used to verify that your account has the "Super Admin" role.
3. Click **Allow**.

4.2 Administrator Roles

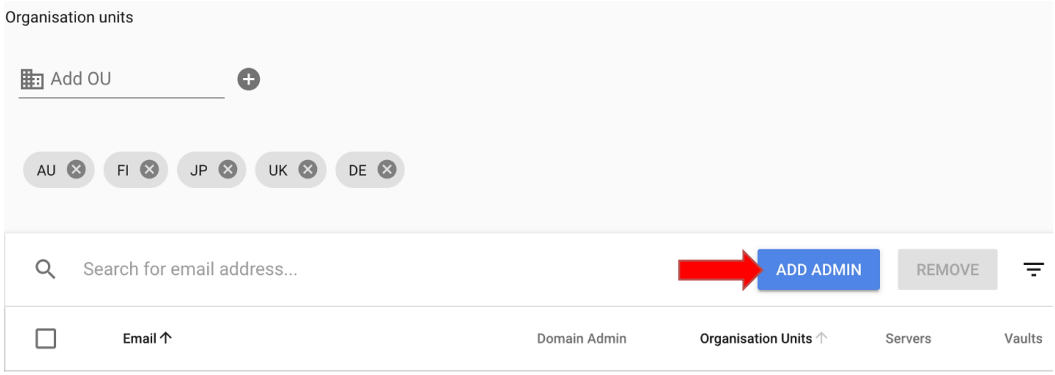
The solution is built with two administrative roles: *Super Admins* and *Domain Admins*.

Both roles can create, update, and delete organizational units; add domain admin users; and configure servers and vaults. Super admins can additionally log in with Super Admin Login.

4.3 Adding Admin Users

To add admin users:

1. Log in to Admin Site at https://admin.workspace.m-files.com.
2. On the **Domain settings** tab, click **ADD ADMIN**.



The *Add a new admin user* dialog is opened.

3. In **Email address**, enter the email address of the admin user.
4. Enable **Domain admin**.

   If no roles are checked and the user is not a super admin, they cannot access the admin tool.
5. Click **ADD**.

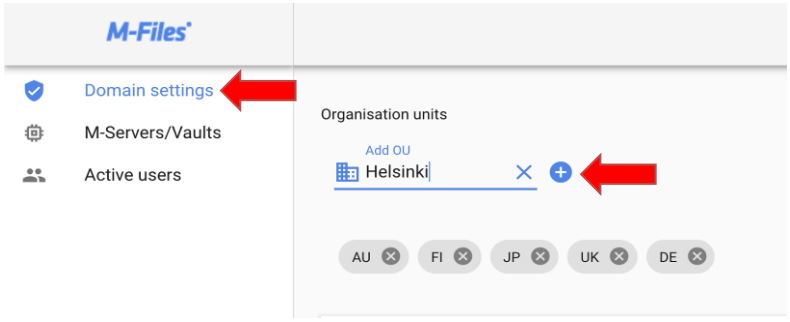
Result: The admin user is added to the admin list.

4.4 Adding Organizational Units

Organizational units are used to separate vault connections inside the same domain. For example, Human Resource department might want to have their own organizational unit called HR. HR is then used to tag the vaults that the Human Resource department uses.

To add an organizational unit:

1. Log in to Admin Site at https://admin.workspace.m-files.com.
2. Go to **Domain settings**.
3. In **Add OU**, enter a name for the unit.
4. Click the plus icon next to the text field.



Result: The organizational unit is added to the domain.

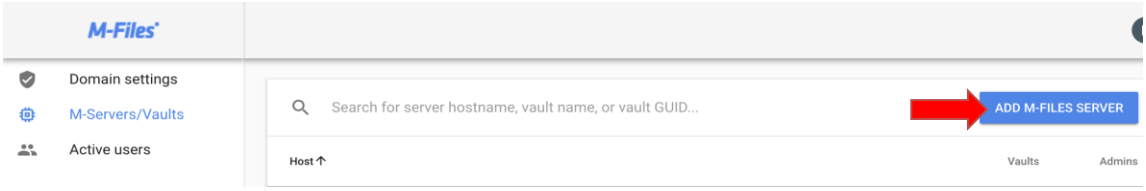
4.5 Setting Up Servers

On the *M-Servers/Vaults* tab, domain-level admin users can set up servers and vaults.

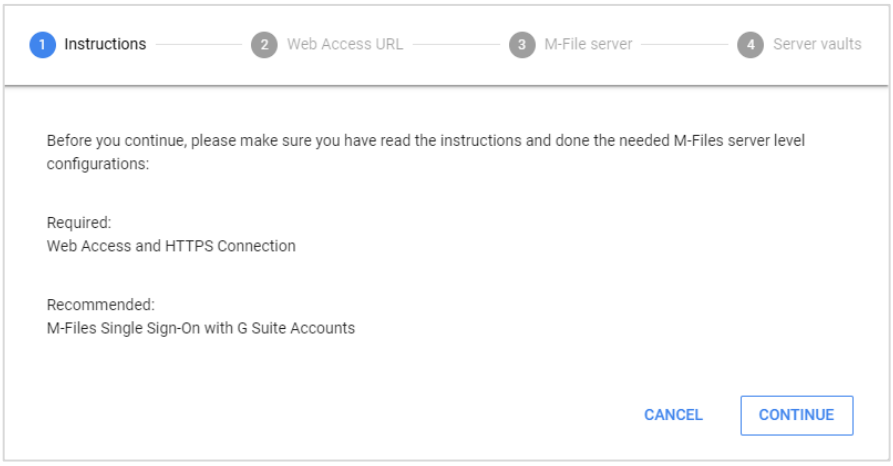
To set up servers:

1. Log in to Admin Site at https://admin.workspace.m-files.com.

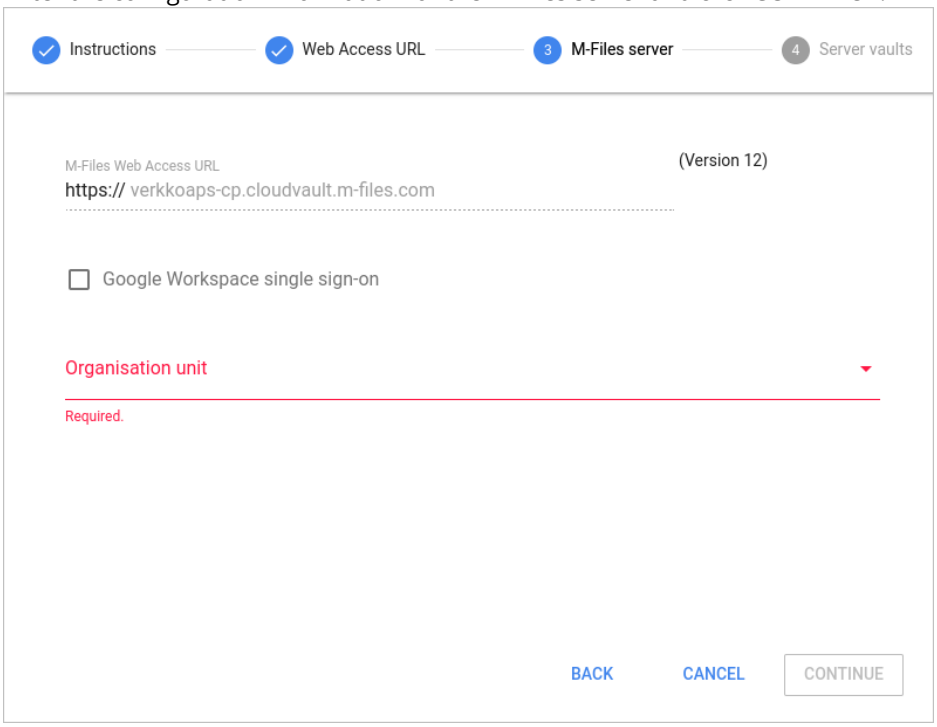
2. On the *M-Servers/Vaults* tab, click **ADD M-FILES SERVER**.



The **Adding server** start dialog is opened.

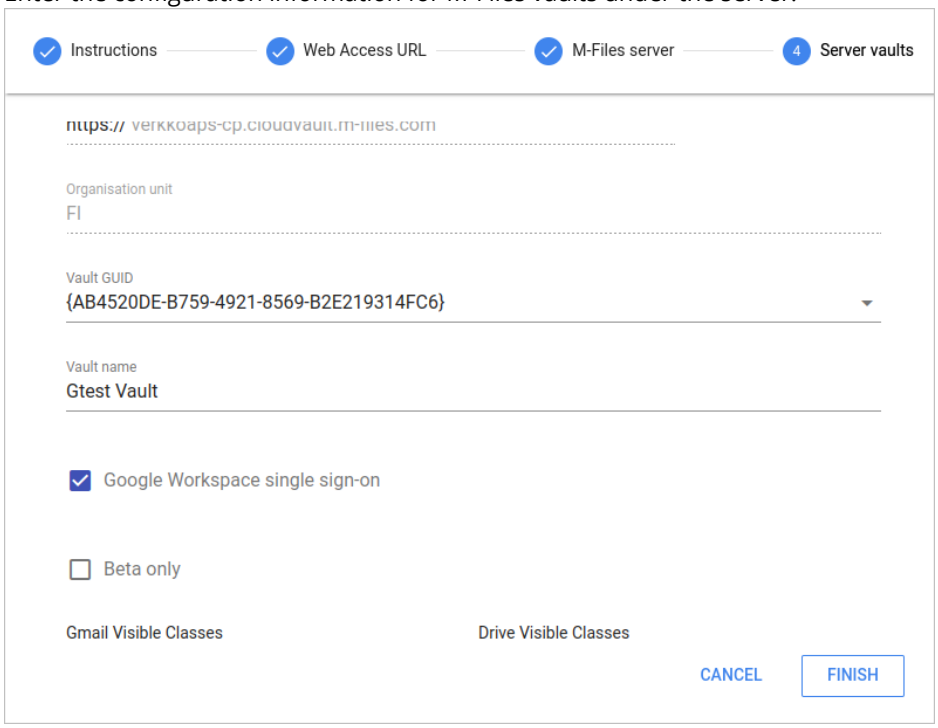


3. Make sure that web access and HTTPS connection are enabled on the M-Files server and click **CONTINUE**.
4. To the text field, enter the M-Files Web URL.
5. **Optional:** If your M-Files server is configured with Google Workspace SSO login, click **CONNECT** to test the connection.
6. Click **CONTINUE**.
7. Enter the configuration information for the M-Files server and click **CONTINUE**.



Note: Do not **select Google Workspace single sign-on** if your M-Files server has not been configured to use Google Workspace accounts.

8. Enter the configuration information for M-Files vaults under the server.



Note: If your server is not enabled with Google Workspace SSO, manual input of GUID is required.

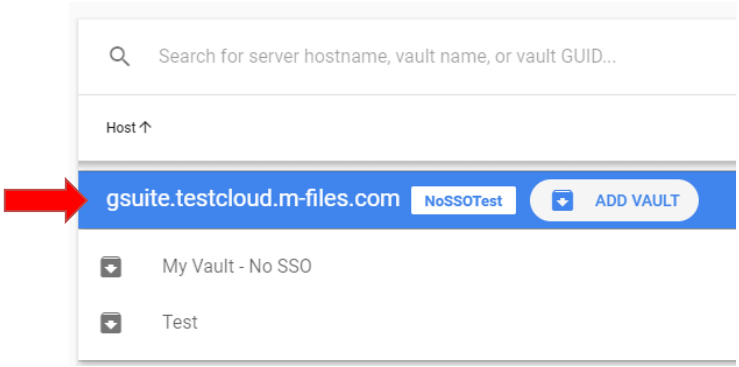
9. Click **FINISH**.

4.6 Editing Servers and Vaults

4.6.1 Editing Server Settings

To edit server settings:

1. Log in to Admin Site at https://admin.workspace.m-files.com.
2. Click on the blue bar to edit (or delete) an M-Files server connection.



3. Edit the information as necessary.

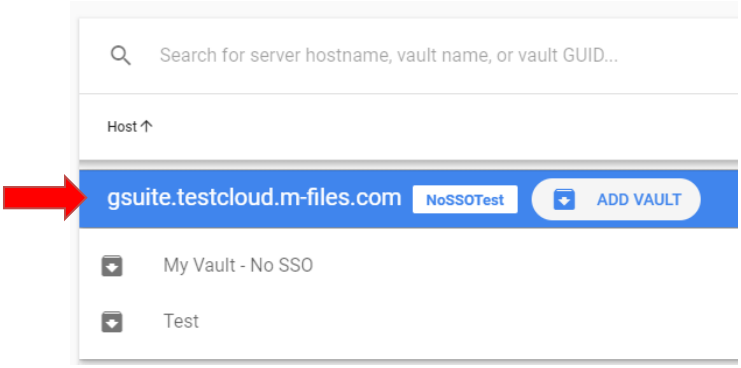
SETTING	DESCRIPTION
Single sign-on	Indicates whether the server has been configured with Google Workspace SSO. Enabling this setting helps in getting the vault GUIDs during the setup process. Please note that the setting does not have a direct impact on the vaults.
Server organisation unit	If you have defined organizational units (section 4.4), this setting allows you to select the correct organizational unit that will use these server settings.
Preshared Key	If you have defined M-Files server to use a pre-shared key, you must enter the key to this field.

4. Click **SAVE**.

4.6.2 Editing Vault Settings

To edit vault settings:

1. Click on a vault to edit (or delete) the M-Files vault connection.



2. Edit the information as necessary.

SETTING	DESCRIPTION
Vault GUID	Allows you to select or enter the vault GUID.
Vault label	The name of the vault.
Google Workspace single sign-on	Indicates whether Google Workspace SSO is used with this vault.
Drive sync enabled	Indicates whether synchronization is enabled for Drive.
Beta only	Enabling this setting makes the vault visible only in the beta version of the M-Files extension.
Gmail Visible Classes	Allows you to manage class names that are visible in Gmail. If this is not configured, all classes are visible.
Drive Visible Classes	Allows you to manage class names that are visible in Drive. If this is not configured, all classes are visible.
Gmail hidden property definitions	Allows you to manage property IDs that are hidden in Gmail.

4.7 Active Users

Information on active users is available in Admin Site at https://admin.workspace.m-files.com on the *Active users* tab.

5. Using the Add-On

The M-Files for Google Workspace add-on allows you to save your Google Drive and Gmail content to your M-Files vault directly from Google Chrome. This section tells you how to use the add-on.

5.1 Prerequisites

Before you use the add-on, make sure that you have logged in to the Chrome browser with your work Google Workspace account. Also, turn sync on in Chrome.

Log in to the browser with the same Google Workspace account that is used to log in to the add-on in Gmail or Google Drive. To add a new Chrome user to a Google Workspace account, refer to these Google instructions.

5.2 Getting Started

To open the M-Files extension, open Gmail or Google Drive, Docs, Sheets, or Slides and, on the side panel, click the icon for the M-Files for Google Workspace add-on. If you are not logged in to an M-Files vault, the login tab is opened. To log in to a vault, see the instructions in section 5.2.1.

Before you save emails or files, check your general and vault settings. For more information, see sections 5.2.1 and 5.2.2.

Click the three-dot menu in the upper right corner of the extension to open one of these tabs: **Recent**, **General Settings**, **Vault Settings**, or **Save to M-Files**. For more information, see the subsections.

5.2.1 General Settings

To edit the general settings:

1. Click the three-dot menu in the upper right corner of the extension and select **General settings**.
2. **Optional**: Click **Language** and select a language.
3. Click **Organizational unit** and select an organizational unit.
   Result: The available vaults are listed under **Vault access**.

To log in to a vault, complete one of these steps:

- If the vault is enabled with Google Workspace account login, click the vault. You are automatically logged in.
- If the vault is enabled with username and password login, enter your user credentials.

The connected vaults are indicated with the open lock icon (🔓). The emails and files are saved to the vault that is shown in the top area of the extension.

5.2.2 Vault Settings

To open the vault-specific settings, click the three-dot menu in the top right corner of the extension and select **Vault settings**.

In vault settings, you can set prefilled metadata for emails and files that are saved to M-Files:

OPTION	DESCRIPTION
Default metadata	Select this option to use a predetermined set of metadata.
From latest saved email OR **From latest saved file**	Select this option to use the metadata of the latest, previously saved email or file.
None	If you select this option, no metadata is prefilled. This is the default option.

Table 1: Options for **Prefilled metadata**.

If you selected **Default metadata**, do these steps to define the default metadata:

1. Under **Metadata in use**, click **Edit**.
2. Select a class.
3. **Optional:** Enter other metadata.
   - Click a property to edit a property value.
   - Click **Add property** at the end of the property list to add properties.
4. When you are ready, click **Save**.

The text field under **Metadata in use** shows the selected set of prefilled metadata.

Gmail-specific settings

In Gmail's vault settings, you can also:

- In the **Save emails in a conversation** section, change how emails that belong to the same conversation are saved:

OPTION	DESCRIPTION
To the same multi-file document	Select this option to save emails that belong to the same conversation to the same multi-file document in M-Files.
As separate documents	Select this option to save emails that belong to the same conversation as separate documents in M-Files.

Table 2: Options for **Save emails in a conversation**.

- In the **Saving** section, select the default file format. The options are EML (default), HTML, or both.
- In the **Automatic saving** section, change the settings for automatic saving. For more information, see section 5.3.4.

In addition to the extension's email conversation setting, the Gmail's **Conversation view** setting has an effect on how email conversations are saved to M-Files. For example, when you save a reply to an email and the conversation view is enabled, both emails are saved. However, if the conversation view is disabled, only the reply is saved.

5.2.3 Recent

When you open the M-Files extension and you are logged in to a vault, the **Recent** tab is shown. It shows you the M-Files documents that you have recently accessed.

In **Recent**, you can:

- Click a file to preview it.
- Use the three-dot menu of a document to open it in M-Files Web or M-Files Desktop.
- Click the magnifying glass in the top area of the extension to search for documents.

5.2.4 Save to M-Files

Select an email or file to save it to M-Files. For more information, see sections 5.3 and 5.4.

5.3 Using the Gmail Integration

In Gmail, you can use the M-Files extension to save and update emails to M-Files. This includes:

- Saving an existing email.
- Saving many emails at once.
- Sending an email and saving it to M-Files at the same time.
- Updating the properties of previously saved emails.
- Setting the extension to automatically save emails that you want.

This section tells you how to do these operations.

5.3.1 Saving Existing Emails to M-Files

To save existing emails to M-Files:

1. To select the email that you want to save, complete one of these steps:
   a. Select the check box of the email that you want to save. Use this option if you want to save many emails at once.
   b. Open an email.

   Result: The metadata tab is loaded.
2. **Optional**: In **Save as type**, change the file format.
   - **Email (EML)**: The attachments are embedded in the email file. By default, this option is selected.
   - **HTML**: The attachments are saved as separate files to the same multi-file document as the email. If there are no attachments, the HTML file is saved as a single-file document.
   - **Email (EML) and HTML**: The email is saved in both formats.

   Tip: Use Google Docs, Slides, or Sheets to save only one attachment.
3. Select a class.
4. **Optional:** Enter other metadata. Specify at least the mandatory properties that show an asterisk (*).
   - Click a property to edit a property value.
   - Click **Add property** at the end of the property list to add properties.
5. Click **Save**.

Result: The email is saved to the vault that is shown in the top area of the extension. If you selected many emails, new emails are saved with the selected settings and the metadata of the previously saved emails is updated.

5.3.2 Saving a New Email to M-Files

To send an email and save it to M-Files at the same time:

1. Compose a new message or reply to an email conversation.
2. Select **Save sent email to M-Files**.

   Result: The metadata tab is loaded.

   > **Note:** To change the tab on the M-Files extension, unselect the checkbox or send the email.

3. Enter the necessary information as in steps from 2 to 4 in Saving Existing Emails to M-Files.
4. Click **Send**.

Result: The message is sent and saved to the vault that is shown in the top area of the extension.

5.3.3 Updating the Properties of Saved Emails

To update the properties of an email that has already been saved to M-Files, select the email and edit the fields of the metadata tab. When you are ready, click **Update**.

5.3.4 Saving Emails Automatically

You can set the add-on to automatically save emails to the vault based on the conversation that they belong to, the labels that the emails are tagged with, or both.

To edit the settings for automatic saving:

1. Click the three-dot menu in the top right corner of the extension and select **Vault settings**.
2. Under **Automatic saving**, in **Default file format**, select the file format. The options are EML (default), HTML, or both. For more information, see step 2 in Saving Existing Emails to M-Files.
3. In **Automatically save**, select or unselect the options that you want:

OPTION	DESCRIPTION
Replies to a saved email	Select this option to automatically save replies and forwards to an email that you have saved to M-Files. When the extension saves the replies, it uses the **Save emails in a conversation** vault setting to select how the emails are saved to M-Files. Even if the email messages are saved as separate documents, all email messages that belong to the same conversation have the same **Message ID** property.
Emails that match a label rule	Select this option to use labels to automatically save emails with predefined set of metadata to M-Files. To add a label rule, see the instructions later in this section. Because the Gmail's **Conversation view** setting has an effect on labeling, it also has an effect on how the labeled emails are saved to M-Files. For more information, refer to Create labels to organise Gmail.

Table 3: Options for **Automatically save**.

> **Note**: Synchronization between Gmail and M-Files is run with one hour intervals. In other words, it may take a maximum of one hour for the emails to be automatically saved to the vault.

To add a label rule:

1. Under **Label rules**, click **New**.

   Result: The **New label rule** tab is opened.
2. In **Name**, enter a name for your rule.
3. Under **Select labels**, select the Gmail labels that you want to trigger automatic saving.

   The emails must have all the labels listed in the right-side text box for the rule to be triggered.
4. Under **Define metadata**, select a class for the emails.
5. **Optional:** Enter other metadata. Specify at least the mandatory properties that show an asterisk (*).
   - Click a property to edit a property value.
   - Click **Add property** at the end of the property list to add properties.
6. Click **Save**.

To edit a label rule, open the vault settings, select a label rule and click **Edit**. Make your changes and click **Save**.

5.4 Using the Google Drive Integration

In Google Drive, you can use the M-Files extension to save and update files to M-Files. This includes:

- Saving an existing file as a new M-Files document.
- Adding an existing file to an M-Files document.
- Saving many files at once.
- Saving a new file.
- Updating previously saved files.
- Setting the extension to synchronize documents between Drive and M-Files.

This section tells you how to do these operations.

The files that have been saved to M-Files show the M-Files icon next to the file name.

5.4.1 Saving Files to M-Files as New Documents

To save existing files to M-Files as new documents:

1. To select a file that you want to save, complete one of these steps:
   a. Select a file and, on the M-Files extension, select **Save to M-Files**
   b. Right-click a file and select **Save to M-Files** > **Save to M-Files**.

   To save many files at once, press and hold the Ctrl key and select the files.

   Result: The metadata tab is loaded.
2. **Optional**: In **Save as type**, change the file format. All file formats do not let you change it.
3. **Optional:** Select **Enable automatic synchronization** to keep the document synchronized between Google Drive and M-Files based on the detection of version difference.
4. Select a class.
5. **Optional:** Enter other metadata. Specify at least the mandatory properties that show an asterisk (*).
   - Click a property to edit a property value.
   - Click **Add property** at the end of the property list to add properties.

6. **Optional:** If you selected many files, in **Save files**, select one of these options:

OPTION	DESCRIPTION
To the same multi-file document	Select this option to save the files to the same multi-file document in M-Files. Once selected, a preview of the multi-file document is shown. Use the **Name or title** property to enter a name for the multi-file document. Note that the files that have already been saved to M-Files are not included in the document.
As separate documents	Select this option to save the files as separate documents in M-Files.

7. Click **Save**.

Result: The files are saved to the vault that is shown in the top area of the extension.

5.4.2 Adding Files to M-Files Documents

To add a file to an M-Files document:

1. To select a file that you want to save, complete one of these steps:
   a. Select a file and, on the M-Files extension, select **Add to existing document**.
   b. Right-click a file and select **Save to M-Files** > **Add to existing document**.

   Result: A list of recent documents is shown.
2. Select the document to which you want to add the selected file. If the file is a single-file document, it will be converted to multi-file document.
3. Click **Next**.
4. **Optional**: Edit the metadata.

   Note: All files in the multi-file document will have the selected properties.
5. Click **Save**.

Result: The file is added to the selected document. If the document was a single-file document, it is converted to multi-file document.

5.4.3 Saving a New File to M-Files

To create a new file and save it to M-Files:

1. Click **New**.
2. Select one of these options:
   - Google Docs
   - Google Sheets
   - Google Slides
3. Edit the document.
4. Fill in the fields on the metadata card. For instructions, see section 5.4.1.
5. Click **Save**.

5.4.4 Updating Files to M-Files

To update a file to M-Files, select the file. Edit the fields of the metadata tab where necessary.

> **Note:** You cannot change the file format of files that have already been saved to M-Files as single-file documents.

When you are ready, click **Update**.

5.5 Using the Docs, Sheets, and Slides Integrations

When you open a file in Google Docs, Sheets, or Slides, the metadata tab is loaded. To save or update the file to M-Files, fill in the fields of the metadata tab and click **Save** or **Update**.

> **Note:** You can only save files as single-file documents.

To use multi-file documents, save the files in Google Drive.

6. Known Limitations

If you save an email or document with settings that do not give you permissions to see the document in M-Files, the file is saved but the add-on can't show any information about it. For example, classes and workflow states can set automatic permissions.

7. Change History

The table below describes the essential changes by document version.

VERSION	DATE	ESSENTIAL CHANGES
1.0	2019/09/18	Initial version.
1.1	2019/09/19	Small changes to the section 2.2. Example registry template added to the section 2.2.3.
1.2	2019/09/26	Reference to example registry template file attached to the instruction added to the section 2.2.3.
1.3	2019/10/04	RedirectURIForMobile added to the section 2.2.3.
1.4	2019/11/28	Updated section 3. Added the description for *Drive Visible Classes* to section 4.6.2. Multiple other sections and screenshots updated throughout the document.
1.5	2019/12/11	Added a note about the synchronization time to section 5.3.4.
1.6	2020/05/05	Changes throughout the document.
1.7	2020/05/18	Added section 4.1. Additionally, added to sections 5.1 and 6.1 that sync needs to be on in Chrome.
1.8	2020/07/09	Updated sections 5.4 and 5.7 and 5.3.4 with the new way of saving email conversations.
1.9	2020/08/05	Changes to sections 5.4 and 5.7 related to the new way of saving email conversations. Obsolete information removed.
2.0	2020/10/13	Added sections 6.2 and 6.7.11

2.1	2020/11/09	Screenshot updated and instructions on how to open the M-Files extension added under sections 5.1 and 6.1.
2.2	2021/03/04	Changed Google G Suite to Google Workspace. Added to section 1.1 the license requirement. Minor changes throughout the document.
2.3	2021/03/19	Section 3 updated. Formatting fixes done.
2.4	2021/03/30	Missing allowed hosts added to section 2.1.1.
2.5	2021/04/07	Links in sections 4.1 and 4.3–4.7 updated.
2.6	2021/04/26	Added section 5.3 and modified one step in instructions on (sending and) saving emails.
2.7	2021/05/10	Changed the sequence of sections 3 and 4. Added Admin Site to section 3. Added instructions on the Super Admin login to section 4.1.
2.8	2022/02/22	Totally renewed and combined the sections related to using the add-on (section 5). Section 6 added.
2.9	2022/05/19	Updated section 2.2.2 with configuration name in the redirect URI. Added default file format setting to section 5.2.2. Added registry key settings AccessTokenType and PreserveServerSpecificSetting_AccessTokenType to section 2.2.2. Other minor modifications.
3.0	2022/12/13	Added a mention that Multi-Server Mode is supported. Also added a table of the necessary values for OAuth configuration in section 2.2.2.
3.1	2023/03/21	Added a table to section 2.2.2. Also changed the ID of trusted Admin Site in section 3.
3.2	2023/08/07	Changes throughout the document.
3.3	2023/10/10	Moved the Keep UseIdTokenAsAccessToken value setting to the new location in the table in section 2.2.2.
3.4	2024/05/28	Updated sections 4.2, 4.3, 4.5, and 4.6 to reflect the removal of “Server admin” and “Vault admin” roles.
3.5	2024/10/02	Corrected the value of TokenEndPoint in section 2.2.2.

8. Reference Documents

- Installing, Configuring, and Using M-Files Google Drive Connector
- Prevent Chrome extensions from altering webpages
- Understand Chrome policy management
- OAuth2 Authentication
- Configuring OpenID Connect and OAuth 2.0 for M-Files Authentication
- Turn sync on and off in Chrome
- Control which third-party & internal apps access Google Workspace data
- Share Chrome with others