



Microsoft Single Sign-on Instructions

Presented by MindManager Product Management, Engineering, & Operations

September 19, 2024

Table of Content

<i>Table of Contents</i>	1
<i>About MindManager SSO</i>	3
<i>SAML Configuration Instructions</i>	4
Creating and Configuring Your Enterprise Application	4
Submit Your Setup Details In the MindManager Admin Portal	10
Step 1 - SSO Setup Information	10
Step 2- Domain Name Verification	11
Step 3 - Ready for Testing	12
Step 4 - Ready to Activate	13
Step 5 - Activated	13
<i>OpenID Configuration Instructions</i>	14
Creating and Configuring Your Enterprise Application	14
Submit Your Setup Details In the MindManager Admin Portal	22
Step 1 - SSO Setup Information	22
Step 2 - Domain Name Verification	22
Step 3 - Ready for Testing	24
Step 4 - Ready to Activate	24
Step 5 - Activated	25

About MindManager SSO

Single Sign-on allows your organization to bypass MindManager account creation and instead use your existing single sign on provider to sign into MindManager software. This is accomplished by establishing trust between your OpenID Connect or SAML Provider and MindManager's Authentication System (Amazon Web Services (AWS) Cognito).

Single Sign-on works with the following MindManager products and services:

- MindManager Windows 21 or greater
- MindManager Mac 13.2 or greater
- MindManager Snap (desktop, mobile, & app extensions)
- Co-editing
- Publishing
- MindManager for Microsoft Teams
- MindManager Web
- MindManager Chromebook
- MindManager License Administration Portal
- Zapier

SAML Configuration Instructions

ATTENTION: Screenshot examples in this document from are shown for reference only, you should perform these changes in your own Microsoft Azure portal.

Creating and Configuring Your Enterprise Application

1. Go to <https://portal.azure.com/>
2. Navigate to **Azure Active Directory**

Welcome to Azure!

Don't have a subscription? Check out the following options.



Start with an Azure free trial

Get \$200 free credit toward Azure products and services, plus 12 months of popular [free services](#).

[Start](#) [Learn more](#)



Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

[View](#) [Learn more](#)



Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

[Explore](#) [Learn more](#)

Azure services



[Create a resource](#)



[All resources](#)



[Azure Active Directory](#)



[Quickstart Center](#)



[Virtual machines](#)



[App Services](#)



[Storage accounts](#)



[SQL databases](#)




















[Azure Cosmos DB](#)



[More services](#)

3. In the manage area of the Azure Active Directory admin center, click **Enterprise Applications**

-  Overview
-  Preview features
-  Diagnose and solve problems
- Manage**

-  Users
-  Groups
-  External Identities
-  Roles and administrators
-  Administrative units
-  Enterprise applications
-  Devices
-  App registrations
-  Identity Governance
-  Application proxy
-  Custom security attributes (Preview)
-  Licenses
-  Azure AD Connect
-  Custom domain names

4. Click **New Application**, then click **Create your own application**

Microsoft / Azure / Enterprise applications / Browse Azure AD Gallery

[+ Create your own application](#) | [Request new gallery app](#) | [Got feedback?](#)


+ You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from apps. Browse or create your own application here.


Single Sign-on : **All** | User Account Management : **All** | Categories : **All**

Cloud platforms


Amazon Web Services (AWS)



Google Cloud Platform



Oracle



Create your own application

[Got feedback?](#)

If you are developing your own application, using Application Proxy, or want to application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

☐ Configure Application Proxy for secure remote access to an on-premises ap

☐ Register an application to integrate with Azure AD (App you're developing)

☒ Integrate any other application you don't find in the gallery (Non-gallery)

5. Type a name for the app (EG “MindManager SSO”), and choose **Integrate any other application you don't find in the gallery (Non-gallery)**, then click **Create**
6. In the manage area, click **Single sign-on**, then click **SAML**



Overview



Deployment Plan

Manage



Properties



Owners



Roles and administrators (Preview)



Users and groups



Single sign-on



Provisioning



Application proxy



Self-service



Custom security attributes
(preview)

Security



Conditional Access



Permissions



Token encryption

Activity

7. In the **Basic SAML Configuration** area, click **Edit**
8. In the **Identifier (Entity ID)** section enter: `urn:amazon:cognito:sp:eu-central-1_Yl6Ea8Vvt`

9. In the **Reply URL (Assertion Consumer Service URL)** section, you now need to add **2 Reply URLs**
 - a. MindManager Reply URLs vary depending on the currently available user pool.
 - b. To get the URLs for the currently available user pool, please visit the **current user pool page** at: <https://cloud.mindmanager.com/api/v1/current-userpool-domains>
There should be 2 different URLs displayed at the top of the page.
 - c. Copy the first URL from the **current user pool page**.
 - d. In the Reply URL area, paste the **first URL** into the first field.
 - i. After pasting the URL, insert **https://** at the beginning of the URL, and change the text **oauth2** to **saml2**
 - ii. For example, if the current user pool page shows:
user-pool/oauth2/idpresponse
it should be changed to:
https://user-pool/saml2/idpresponse
 - e. Copy the second URL from the **current user pool page**.
 - f. In the Reply URL area, paste the **second URL** into the second field
 - i. Once again, after pasting the URL, insert **https://** at the beginning of the URL and change the text **oauth2** to **saml2**
 - g. Click Save
 - h. Example below. *Entity ID and URI shown are for illustrative purposes only; be sure to use the entity ID from step 8 above and get the latest URIs from the current user pool page.*

If you are updating an older MindManager SSO setup, please use the entity ID from your current configuration.

Basic SAML Configuration

 Save |  Got feedback?

Identifier (Entity ID) * ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

☒ ⓘ

Reply URL (Assertion Consumer Service URL) * ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

☒ ⓘ

10. In the Attributes & Claims area, Click **Edit**

11. Then click **Add New Claim**


12. **Enter the following information**


Name: **Email**

Namespace: **http://schemas.xmlsoap.org/ws/2005/05/identity/claims**

Source: **Attribute**




Source attribute: **(Use field which includes your member email address)**

 **Microsoft Azure**


 Search resources, services, and docs (G+)

[Home](#) > [Parallels Inc - PREPROD LAB](#) > [Enterprise applications](#) > [mind](#) > [SAML-based Sign-on](#) > [Attributes & Claims](#)

Manage claim ...

 Save  Discard changes |  Got feedback?

Name *	<input type="text" value="Email"/>
Namespace	<input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"/>
Source *	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation
Source attribute *	<input type="text" value="user.userprincipalname"/>

 Claim conditions

13. Copy the **App Federation Metadata URL** in the SAML Signing Certificate area

Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Email	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML Signing Certificate

Edit

Status	Active
Thumbprint	
Expiration	11/11/2024, 6:49:12 AM
Notification Email	
App Federation Metadata Url	<div>https://login.microsoftonline.com/ <div></div></div>
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Submit Your Setup Details in the MindManager Admin Portal

Please visit the MindManager Admin portal at <https://cloud.mindmanager.com/admin>.

After signing in, click the “Setup SSO” button to begin.

Step 1 - SSO Setup Information

Input the required information into the fields, then click submit.

- **App Federation Metadata URL**
 - Found in the SAML Signing Certificate area, you copied this in step 13.
- **List of domains**
 - The list of domains that you want to be redirected to use your Organization’s Active Directory to Sign In.
 - This is usually the company domain, for example at Corel it is **corel.com** but you can include additional domains that may fall under the same active directory, for example we also include **mindmanager.com**. This means that anyone with an **@corel.com** or **@mindmanager.com** email address will be redirected to Corel’s Azure AD for sign in.

Step 2- Domain Name Verification

MindManager requires domain name verification. This process ensures your organization is the rightful owner of the domains you are requesting us to redirect to your SSO provider. Domain verification also enables your administrator to delete MindManager cloud data for users with email addresses that match your verified domains.

Verify your domain using one of the methods below (you do **NOT** need to do both):

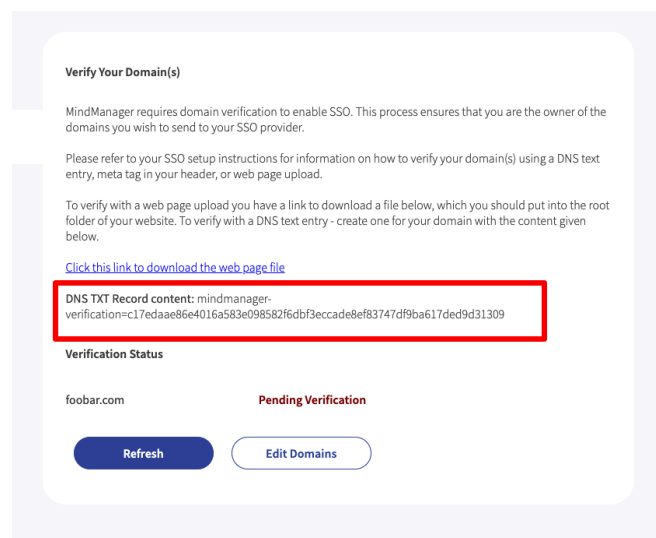
1. Add a DNS TXT entry to your DNS record to confirm that you own the domain.

OR

2. Upload an HTML file provided to you in the "Domain verification" section to your root web directory.

Verify your domain with a DNS TXT record

The "Domain verification" section provides the TXT information you will need to add to your DNS record.



1. Navigate to the DNS record section of your domain host.
2. Add the TXT entry to your DNS record.
3. Add @ to the Host field (if it is required by your domain host).

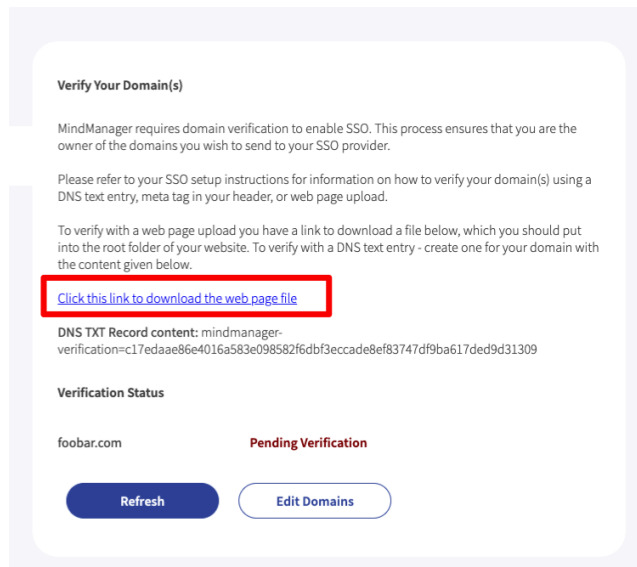
4. Once the changes have propagated across your domain's web servers, click the Refresh button at the bottom of the “Domain verification” section.

Note: Typically, this change takes only minutes to occur, however there are cases where it may take up to 72 hours to complete.

Note: The precise steps you need to perform to add a DNS TXT entry to your DNS record may vary by domain host.

Verify your domain by uploading an HTML file to your root web directory

The “Domain verification” section provides the HTML verification file you need to upload to your website.



1. Download the HTML verification file.
2. Upload the file to the root directory of your website.
3. Once it is done, click the Refresh button at the bottom of the “Domain verification” section.

Step 3 - Ready for Testing

After you have successfully completed domain verification, the status in the admin portal will show as “Ready for Testing.” Please follow the instructions in the admin portal to test SSO.

Step 4 - Ready to Activate

After you have successfully tested signing in to MindManager using your identity provider, the status in the admin portal will show as “Ready to Activate.” Please follow the instructions in the admin portal to activate SSO.

Step 5 - Activated

After you have activated SSO, the status in the admin portal will show as “Activated.” Users under your domain will now be redirected to your identity provider when signing in to MindManager.

You’re done!

You can also edit or delete your SSO setup from this screen.

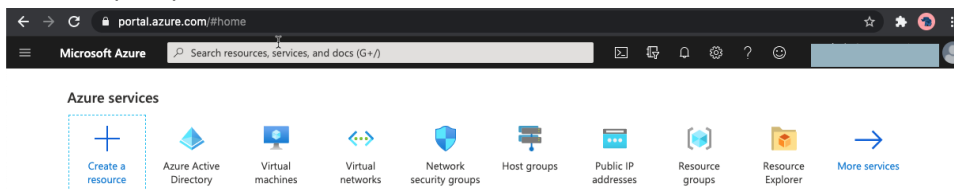
OpenID Configuration Instructions

ATTENTION: Screenshot examples in this document from Corel Corp are shown for reference only, you should perform these changes in your own Microsoft Azure portal.

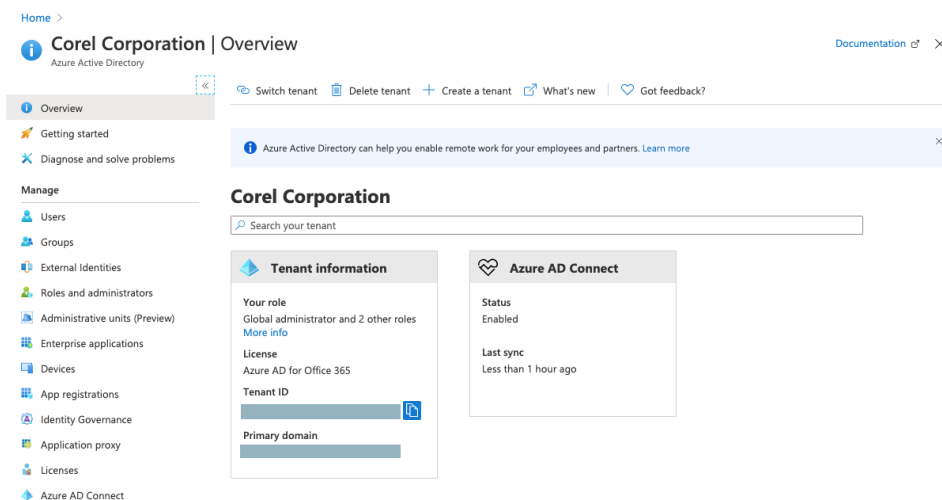
Creating and Configuring Your Enterprise Application

Register a new application using the Azure Active portal by completing the following steps.

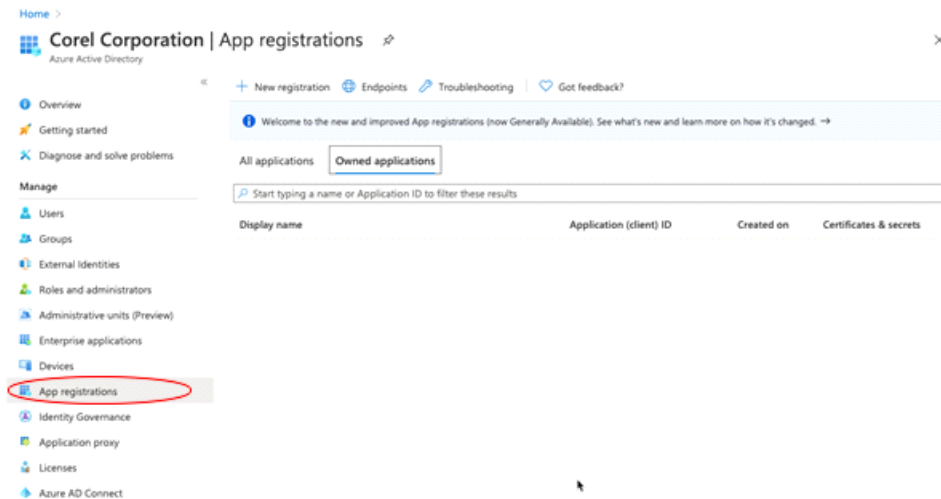
1. Go to <https://portal.azure.com/>



2. Navigate to Azure Active Directory.



3. In the Manage area of the Azure Active Directory admin center, click **App registrations**.



4. Click **New registration**.
5. On the Register an application page, type the name that the user will see for this application in the **Name** box.
6. In the Supported account types area, enable the **Accounts in this organizational directory only** option.
7. Next, enter the redirect URI into the **Redirect URI** box.
 - a. MindManager Redirect URIs vary depending on the currently available user pool.
 - b. To get the URIs for the currently available user pool, please visit the **current user pool page** at: <https://cloud.mindmanager.com/api/v1/current-userpool-domains>
There should be 2 different URIs displayed at the top of the page.
 - c. Copy the **first URI** from the **current user pool page**
 - d. Paste the **first URI** into **Redirect URI** box.
 - i. After pasting the URL, insert **https://** at the beginning of the URL
 - ii. For example, if the current user pool page shows:
user-pool/oauth2/idpresponse
it should be changed to:
https://user-pool/oauth2/idpresponse
8. Click **Register**.

Home > Corel Corporation | App registrations >

Register an application

Name

The user-facing display name for this application (this can be changed later).

cloud-mindmanager-com ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Corel Corporation only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web https://login.mindmanager.com/oauth2/iddresponse ✓

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

9. In the Manage area, click **Authentication**.

Home > Corel Corporation | App registrations >

cloud-mindmanager-com | Authentication

Search (Cmd+/) Save Discard Got feedback?

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Owners

Roles and administrators (Preview)

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

Add a platform

Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

https://login.mindmanager.com/oauth2/iddresponse

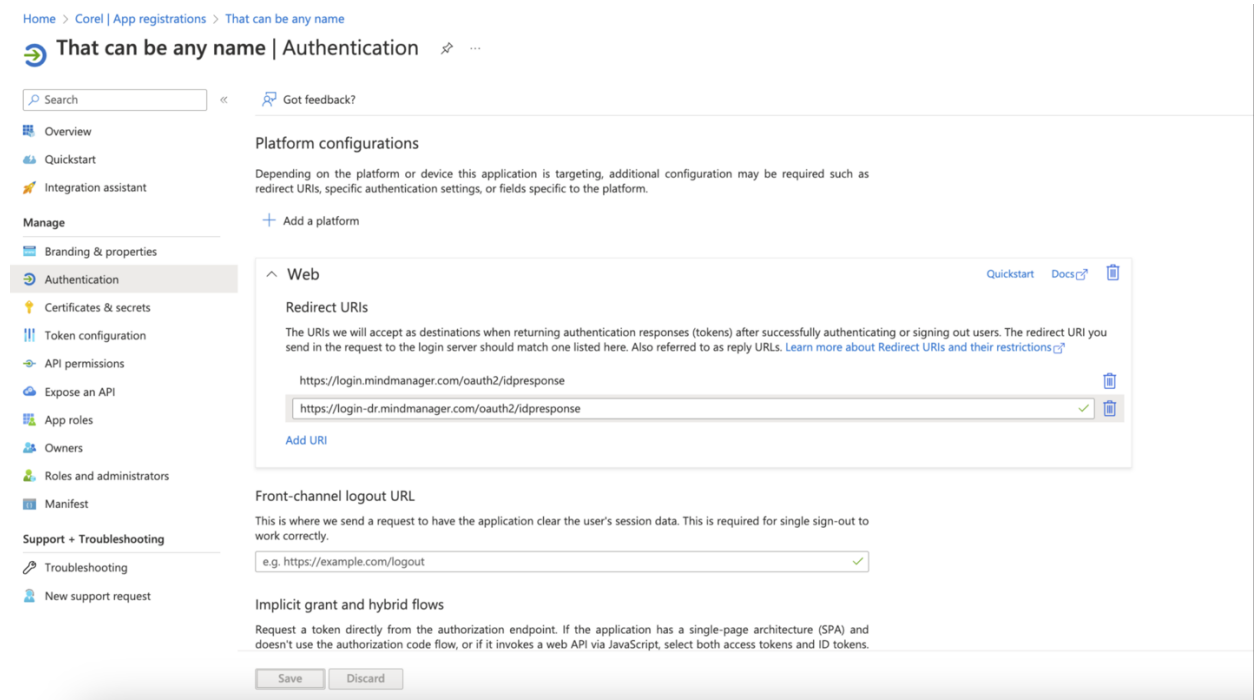
Add URI

Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://myapp.com/logout ✓

10. In the Platform Configurations area, you now need to add a second **Redirect URI**
 - a. MindManager Redirect URIs vary depending on the currently available user pool.
 - b. To get the URIs for the currently available user pool, please visit the **current user pool page** at: <https://cloud.mindmanager.com/api/v1/current-userpool-domains>
There should be 2 different URIs displayed at the top of the page.
 - c. Copy the **second URI** from the **current user pool page**
 - d. In the **Web** section, click **Add URI**, then paste the **second URI** into the field.
 - i. After pasting the URL, insert **https://** at the beginning of the URL
 - ii. For example, if the current user pool page shows:
user-pool/oauth2/idpresponse
it should be changed to:
https://user-pool/oauth2/idpresponse
 - e. You should have 2 **different** URIs listed. Example with added URIs shown below. *URIs shown are for illustrative purposes only, be sure to get the latest URIs from the current user pool page.*



11. On the Platform Configurations page, click **Save**.
12. In the Manage area, click **Certificates & secrets**.

13. On the Certificates & secrets page, click **New client secret**.

Home > Corel Corporation | App registrations >

cloud-mindmanager-com | Certificates & secrets

Search (Cmd+J)

Overview

Quickstart

Integration assistant (preview)

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Owners

Roles and administrators (Preview)

Manifest

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires
No certificates have been added for this application.		

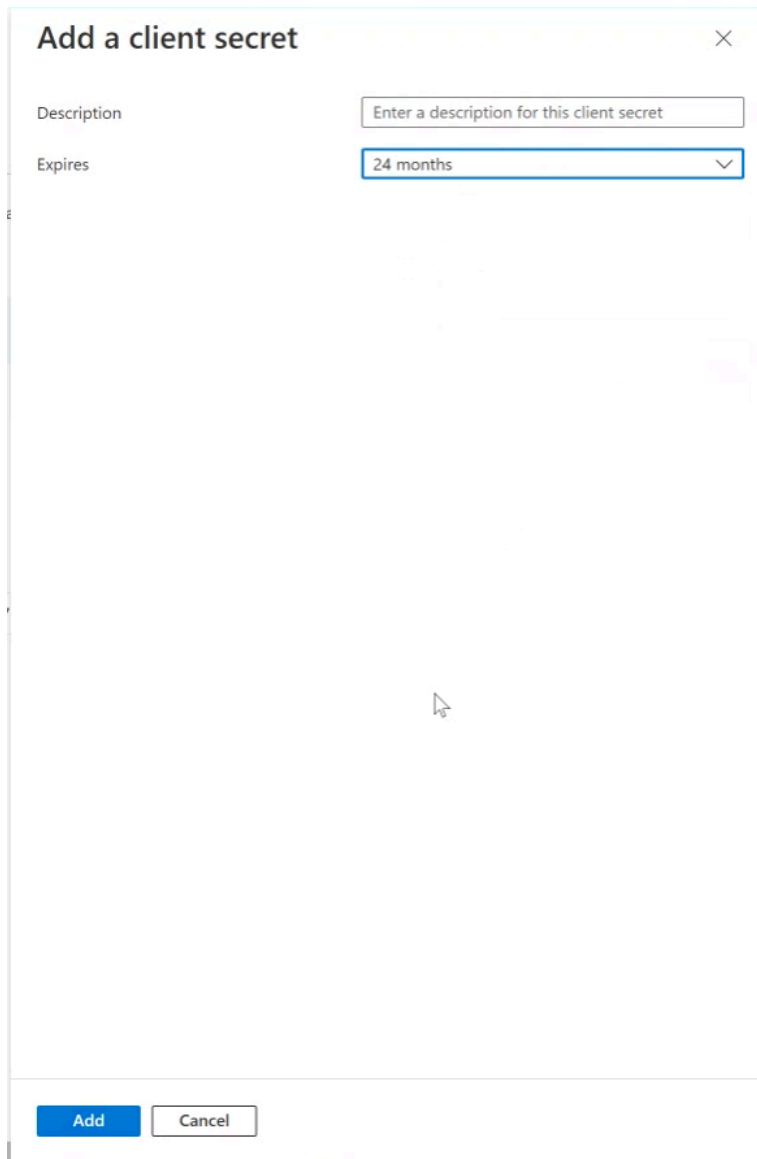
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value
No client secrets have been created for this application.		

14. In the Add a client secret window, type a descriptive name for the secret (optional) and select an expiry option.



The screenshot shows a dialog box titled "Add a client secret". It has a close button (X) in the top right corner. Below the title, there are two fields: "Description" with a text input field containing the placeholder "Enter a description for this client secret", and "Expires" with a dropdown menu currently showing "24 months". At the bottom of the dialog are two buttons: "Add" (in blue) and "Cancel" (in white).

- a. Due to requirements of the Microsoft Azure system, the SSO connection with MindManager requires a secret token that has an expiration date. MindManager requires choosing an expiration date of 24 months or greater to minimize the frequency of updating your secret token with our team. If your secret token expires before you provide a new one to the MindManager team, **NONE OF YOUR USERS OR ADMINS WILL BE ABLE TO ACCESS THE MINDMANAGER ADMIN PORTAL OR MINDMANAGER PRODUCTS.** To avoid this scenario, your organization must do the following:
- i. Add a new client secret token to your existing app in Azure that you are using for MindManager SSO.

- ii. **Submit the new secret token through the SSO setup process in the MindManager Admin portal at least 4 weeks prior to your previous secret token's expiration date to allow time for our team to update without service interruption.**

15. Click **Add**.

16. In the Client secrets area, click the **Copy to clipboard** button in the **Value** column for the secret that you created. This information must be provided in the MindManager Admin portal SSO setup form.

Description	Expires	Value	Secret ID
Demo Cert	5/4/2022	VH17Q~_ymm1w8gyx32SAtlmrNkh1dw...	5179a12d-0035-4170-a475-3e8614c177b2

17. In the Manage area, click **API permissions**.

Home > Corel Corporation | App registrations > cloud-mindmanager-com | API permissions

Search (Cmd+J) Refresh

Overview Quickstart Integration assistant (preview)

Manage

Branding Authentication Certificates & secrets **API permissions** Expose an API Owners Roles and administrators (Preview) Manifest

Support + Troubleshooting Troubleshooting New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Corel Corporation

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
User Read	Delegated	Sign in and read user profile	-	...

18. On the API permissions page, click **Add a permission**.

19. In the Request API permissions pane, click **Microsoft Graph**.

Request API permissions

Select an API

Microsoft APIs APis my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

20. Click **Delegated permissions**.

Request API permissions

All APIs

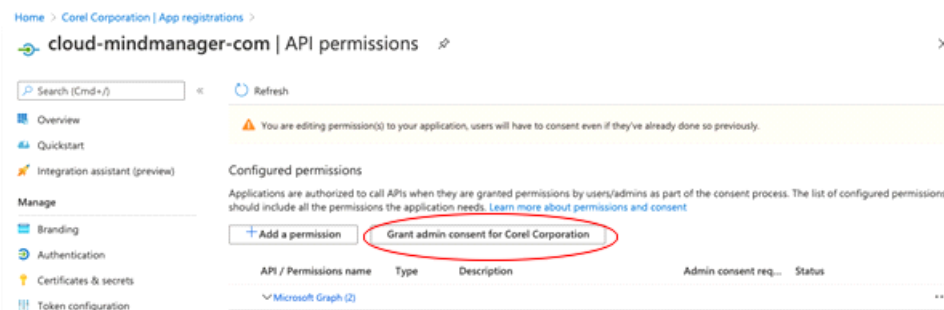
Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

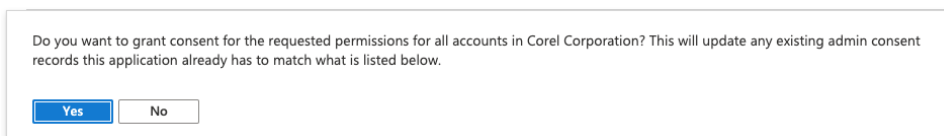
Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

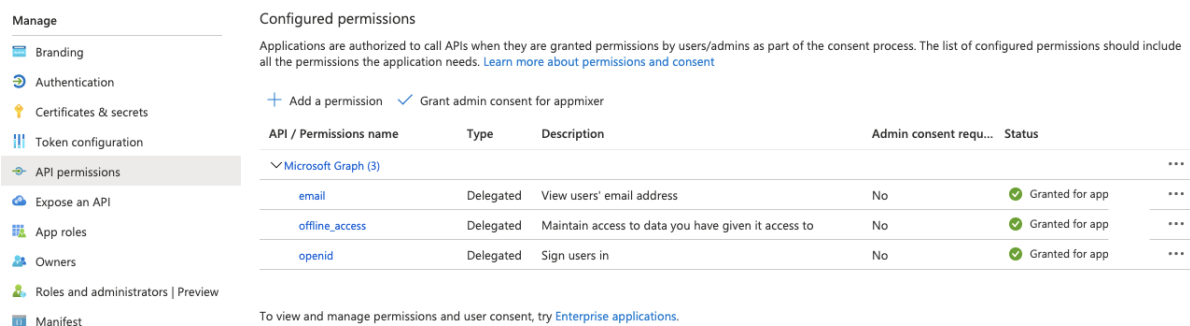
21. In the Openid permissions area, enable the **email**, **offline_access**, **openid**, and **profile** check boxes.
22. Click **Add permissions**.
23. On the API permissions page, click **Grant admin consent**.



24. Click **Yes** to confirm.



25. Configuration Complete (see next section)
26. The **minimum** permissions required for SSO to work with MindManager are shown in the following example, please ensure you have granted permission for the following:



- a. Email
- b. Offline_access
- c. openid

Submit Your Setup Details in the MindManager Admin Portal

Please visit the MindManager Admin portal at <https://cloud.mindmanager.com/admin>.

After signing in, click the “Setup SSO” button to begin.

Step 1 - SSO Setup Information

Input the required information into the fields, then click submit.

- **Application Client ID**
 - Found on the Overview Page in Microsoft Azure
- **Client Secret Value**
 - Found on the Certificates & Secrets page in the **Value** column in Microsoft Azure — the information copied in step 16.
- **Secret Token Expiration Date**
 - Found on the Certificates & Secrets page in the **Expires** column in Microsoft Azure — enter a date based on the expiration you entered in step 14.
 - The MindManager system will send you reminder emails leading up to your token expiration so that you can renew the token without service interruption.
- **Directory (tenant) ID**
 - Found on the Overview Page in Microsoft Azure
- **List of domains**
 - The list of domains that you want to be redirected to use your Organization’s Active Directory to Sign In.
 - This is usually the company domain, for example at Corel it is **corel.com** but you can include additional domains that may fall under the same active directory, for example we also include **mindmanager.com**. This means that anyone with an **@corel.com** or **@mindmanager.com** email address will be redirected to Corel’s Azure AD for sign in.

You will receive an email confirmation from noreply@mindmanager.com that we have successfully received your setup request (be sure to check your spam/junkmail folders).

Step 2 - Domain Name Verification

MindManager requires domain name verification. This process ensures your organization is the rightful owner of the domains you are requesting us to redirect to your SSO provider. Domain verification also enables your administrator to delete MindManager cloud data for users with email addresses that match your verified domains.

Verify your domain using one of the methods below (you do **NOT** need to do both):

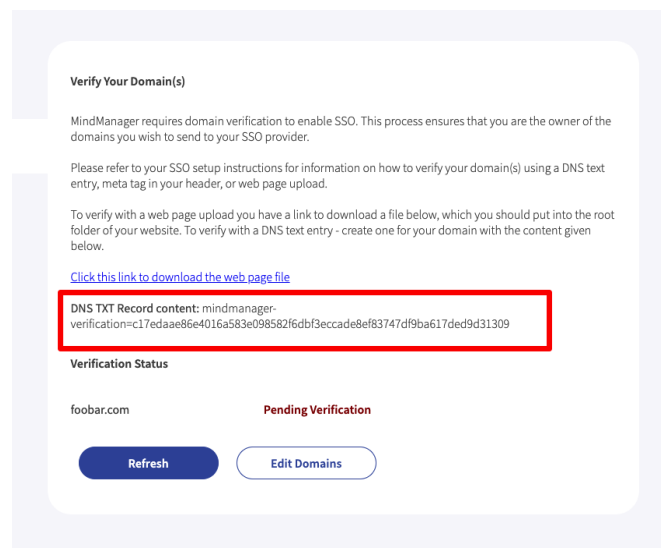
3. Add a DNS TXT entry to your DNS record to confirm that you own the domain.

OR

4. Upload an HTML file provided to you in the "Domain verification" section to your root web directory.

Verify your domain with a DNS TXT record

The "Domain verification" section provides the TXT information you will need to add to your DNS record.



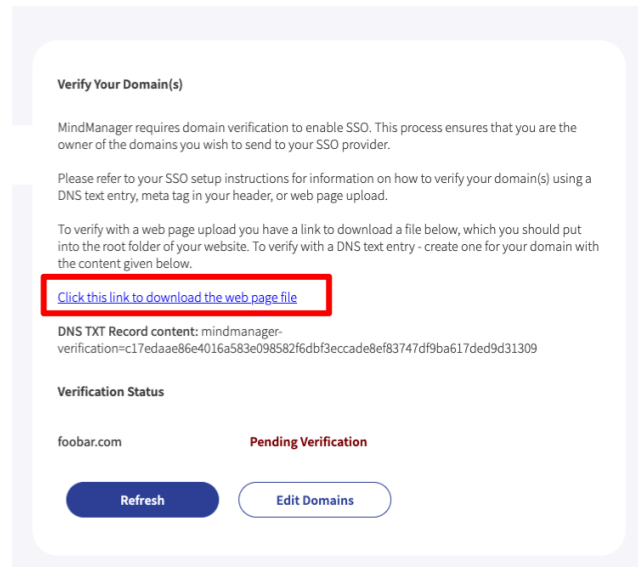
5. Navigate to the DNS record section of your domain host.
6. Add the TXT entry to your DNS record.
7. Add @ to the Host field (if it is required by your domain host).
8. Once the changes have propagated across your domain's web servers, click the Refresh button at the bottom of the "Domain verification" section.

Note: Typically, this change takes only minutes to occur, however there are cases where it may take up to 72 hours to complete.

Note: The precise steps you need to perform to add a DNS TXT entry to your DNS record may vary by domain host.

Verify your domain by uploading an HTML file to your root web directory

The “Domain verification” section provides the HTML verification file you need to upload to your website.



4. Download the HTML verification file.
5. Upload the file to the root directory of your website.
6. Once it is done, click the Refresh button at the bottom of the “Domain verification” section.

Step 3 - Ready for Testing

After you have successfully completed domain verification, the status in the admin portal will show as “Ready for Testing.” Please follow the instructions in the admin portal to test SSO.

Step 4 - Ready to Activate

After you have successfully tested signing in to MindManager using your identity provider, the status in the admin portal will show as “Ready to Activate.” Please follow the instructions in the admin portal to activate SSO.

Step 5 - Activated

After you have activated SSO, the status in the admin portal will show as “Activated.” Users under your domain will now be redirected to your identity provider when signing in to MindManager.

You’re done!

You can also edit or delete your SSO setup from this screen.