MindManager

MindManager Cloud Services
Google GSuite Single Sign-on Configuration Instructions

Presented by MindManager Product Management, Engineering, & Operations

January 10, 2023

Table of Contents

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).

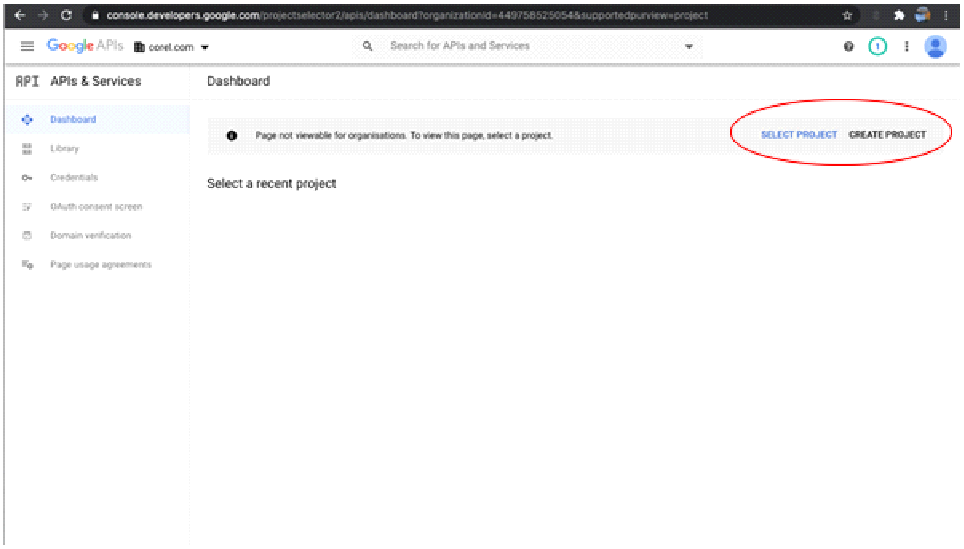
Single Sign-on works with the following MindManager products and services:

- 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 License Administration Portal
- Zapier

Google GSuite SSO configuration

Set up a new External OAuth consent screen by completing the following steps.

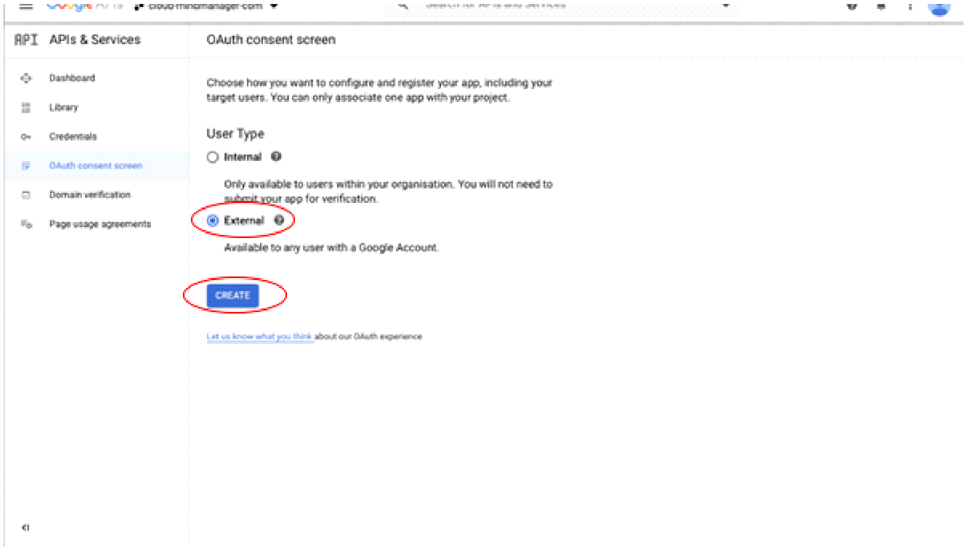
1. Go to https://console.developers.google.com/
2. In the Google Developers Console, click **Select Project** or **Create Project**.



Page not viewable for organisations. To view this page, select a project.

Select a recent project

3. If a new project is created, on the OAuth consent screen enable the **External** option and click **Create**.



cloud-mindmanager-com

APIs & Services

Dashboard

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

User Type

○ Internal

Only available to users within your organisation. You will not need to submit your app for verification.

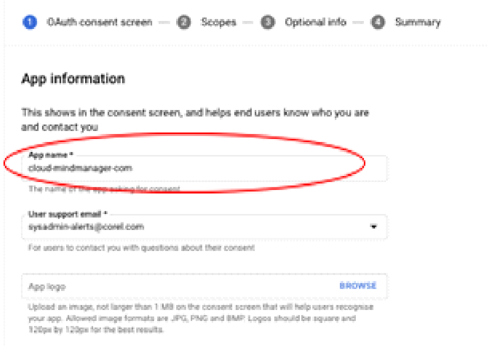
● External

Available to any user with a Google Account.

CREATE

Let us know what you think about our OAuth experience

4. In the App information area, enter **cloud-mindmanager.com**.



1 OAuth consent screen — 2 Scopes — 3 Optional info — 4 Summary

App information

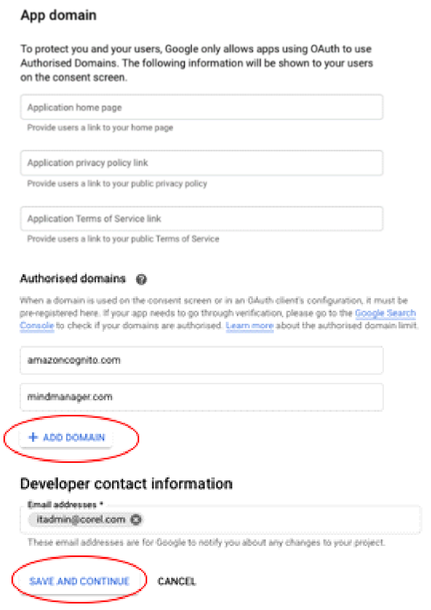
This shows in the consent screen, and helps end users know who you are and contact you

App name *
cloud-mindmanager-com
The name of the app asking for consent

User support email *
sysadmin-alerts@corel.com
For users to contact you with questions about their consent

App logo BROWSE
Upload an image, not larger than 1 MB on the consent screen that will help users recognise your app. Allowed image formats are JPG, PNG and BMP. Logos should be square and 120px by 120px for the best results.

5. In the Authorized domains area, click **Add Domain**.
6. Enter *amazoncognito.com* and click **Add Domain**.
7. Enter *mindmanager.com*.



App domain

To protect you and your users, Google only allows apps using OAuth to use Authorised Domains. The following information will be shown to your users on the consent screen.

Application home page
Provide users a link to your home page

Application privacy policy link
Provide users a link to your public privacy policy

Application Terms of Service link
Provide users a link to your public Terms of Service

Authorised domains

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the Google Search Console to check if your domains are authorised. Learn more about the authorised domain limit.

amazoncognito.com

mindmanager.com

+ ADD DOMAIN

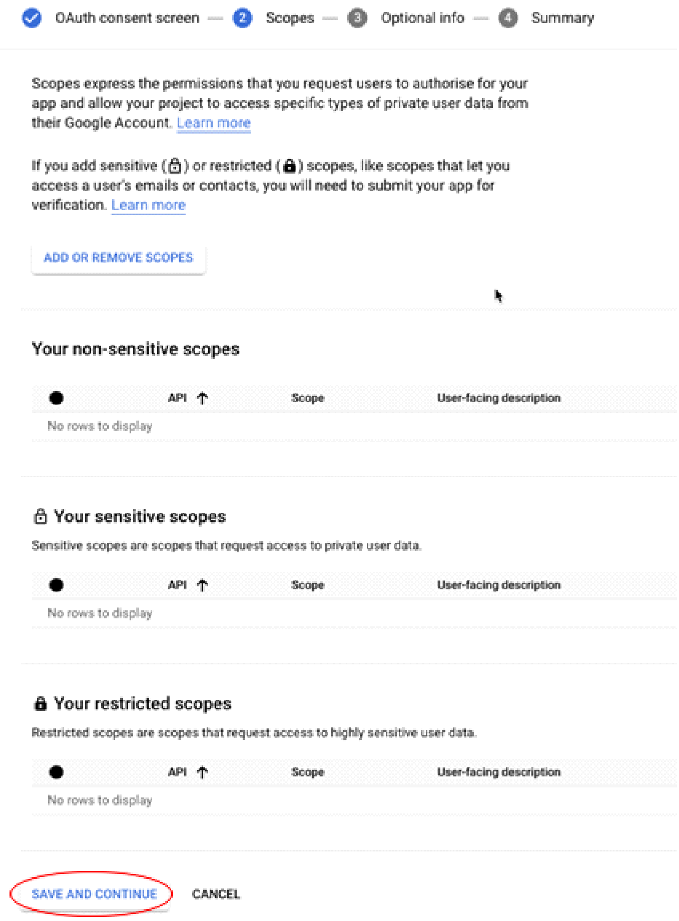
Developer contact information

Email addresses *
itadmin@corel.com
These email addresses are for Google to notify you about any changes to your project.

SAVE AND CONTINUE CANCEL

8. Click **Save and Continue**.

9. On the Scopes page, click **Save and Continue**.



✓ OAuth consent screen — 2 Scopes — 3 Optional info — 4 Summary

Scopes express the permissions that you request users to authorise for your app and allow your project to access specific types of private user data from their Google Account. Learn more

If you add sensitive (🔓) or restricted (🔒) scopes, like scopes that let you access a user's emails or contacts, you will need to submit your app for verification. Learn more

Your non-sensitive scopes

●	API ↑	Scope	User-facing description
No rows to display			

🔓 Your sensitive scopes

Sensitive scopes are scopes that request access to private user data.

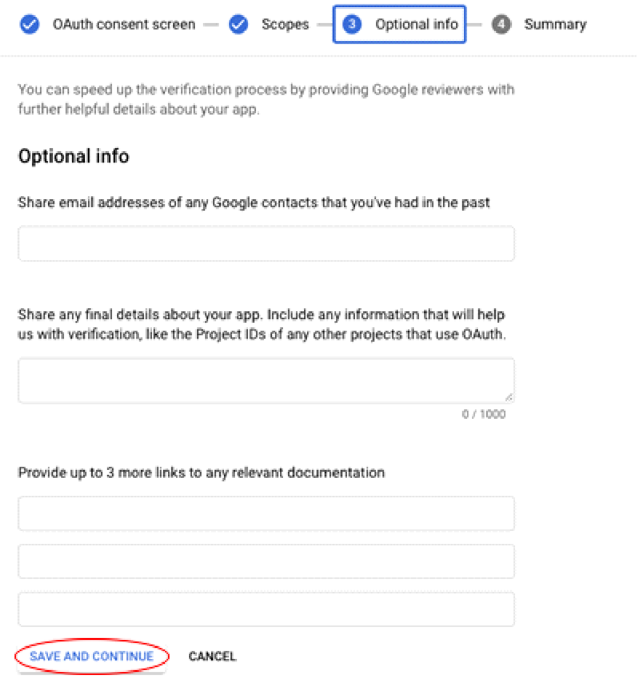
●	API ↑	Scope	User-facing description
No rows to display			

🔒 Your restricted scopes

Restricted scopes are scopes that request access to highly sensitive user data.

●	API ↑	Scope	User-facing description
No rows to display			

10. On the Optional info page, click **Save and Continue**.



✓ OAuth consent screen — ✓ Scopes — 3 Optional info — 4 Summary

You can speed up the verification process by providing Google reviewers with further helpful details about your app.

Optional info

Share email addresses of any Google contacts that you've had in the past

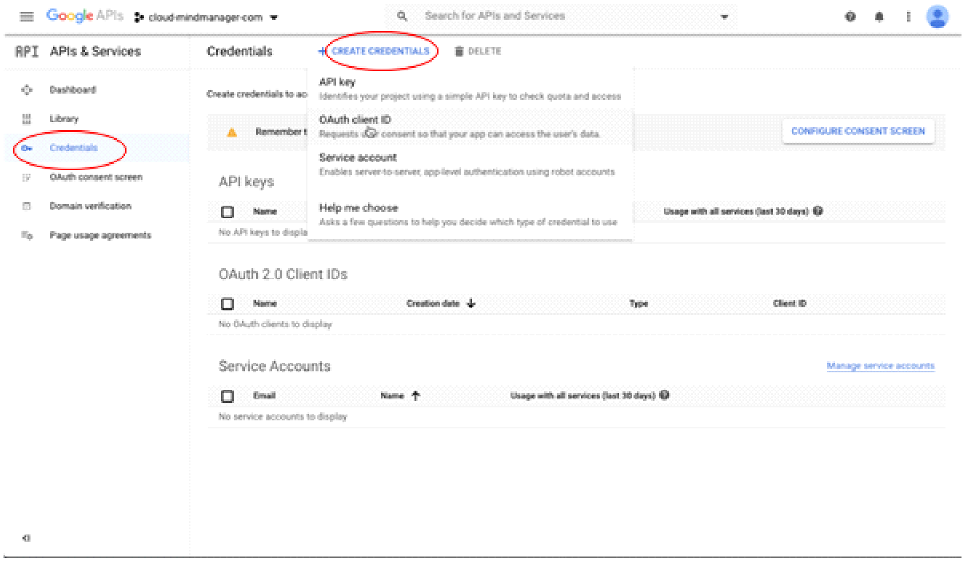
Share any final details about your app. Include any information that will help us with verification, like the Project IDs of any other projects that use OAuth.

0 / 1000

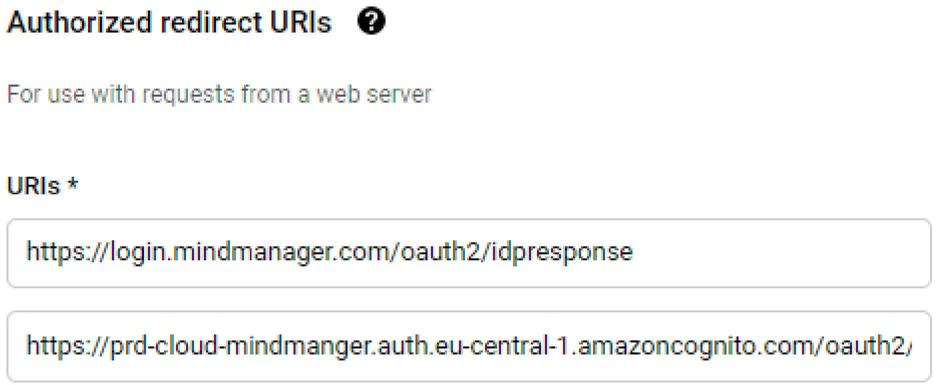
Provide up to 3 more links to any relevant documentation

11. In the APIs & Services area, click **Credentials**.

12. Click **Create Credentials**, and select **OAuth client ID**.


Google APIs
cloud-mindmanager-com
Search for APIs and Services
API APIs & Services
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
Credentials
CREATE CREDENTIALS
DELETE
Create credentials to ac
Remember t
CONFIGURE CONSENT SCREEN
API key
Identifies your project using a simple API key to check quota and access
OAuth client ID
Requests user consent so that your app can access the user's data.
Service account
Enables server-to-server, app-level authentication using robot accounts
Help me choose
Asks a few questions to help you decide which type of credential to use
API keys
Name
Usage with all services (last 30 days)
No API keys to displa
OAuth 2.0 Client IDs
Name
Creation date
Type
Client ID
No OAuth clients to display
Service Accounts
Manage service accounts
Email
Name
Usage with all services (last 30 days)
No service accounts to display

13. On the **OAuth client ID page**, you now need to add **2 Redirect URIs**
    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. In the Authorized redirect URIs area, Click **Add URI** if more fields are needed, then paste the **first URI** into the field.
    e. Copy the second URI from the **current user pool page**.
    f. Click **Add URI** again if needed, then paste the **second URI** into the field.
    g. Example with added URIs below. *URIs shown are for illustrative purposes only, be sure to get the latest URIs from the current user pool page.*



Authorized redirect URIs

For use with requests from a web server

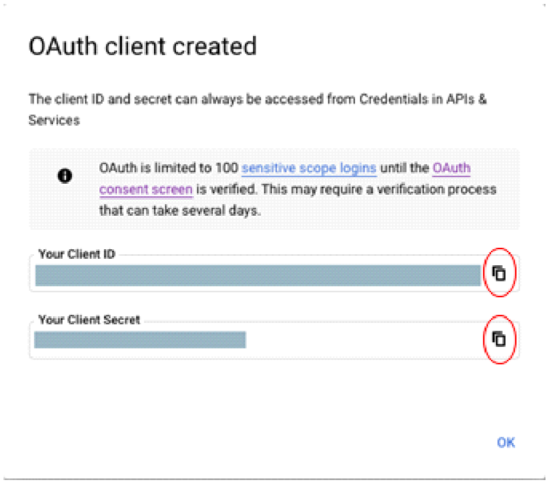
URIs *

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

https://prd-cloud-mindmanger.auth.eu-central-1.amazoncognito.com/oauth2/

14. Click **Create**.

15. **Copy** the **Client ID** and **Client Secret** from the OAuth client created screen and paste it into the MindManager admin portal.



OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

OAuth is limited to 100 sensitive scope logins until the OAuth consent screen is verified. This may require a verification process that can take several days.

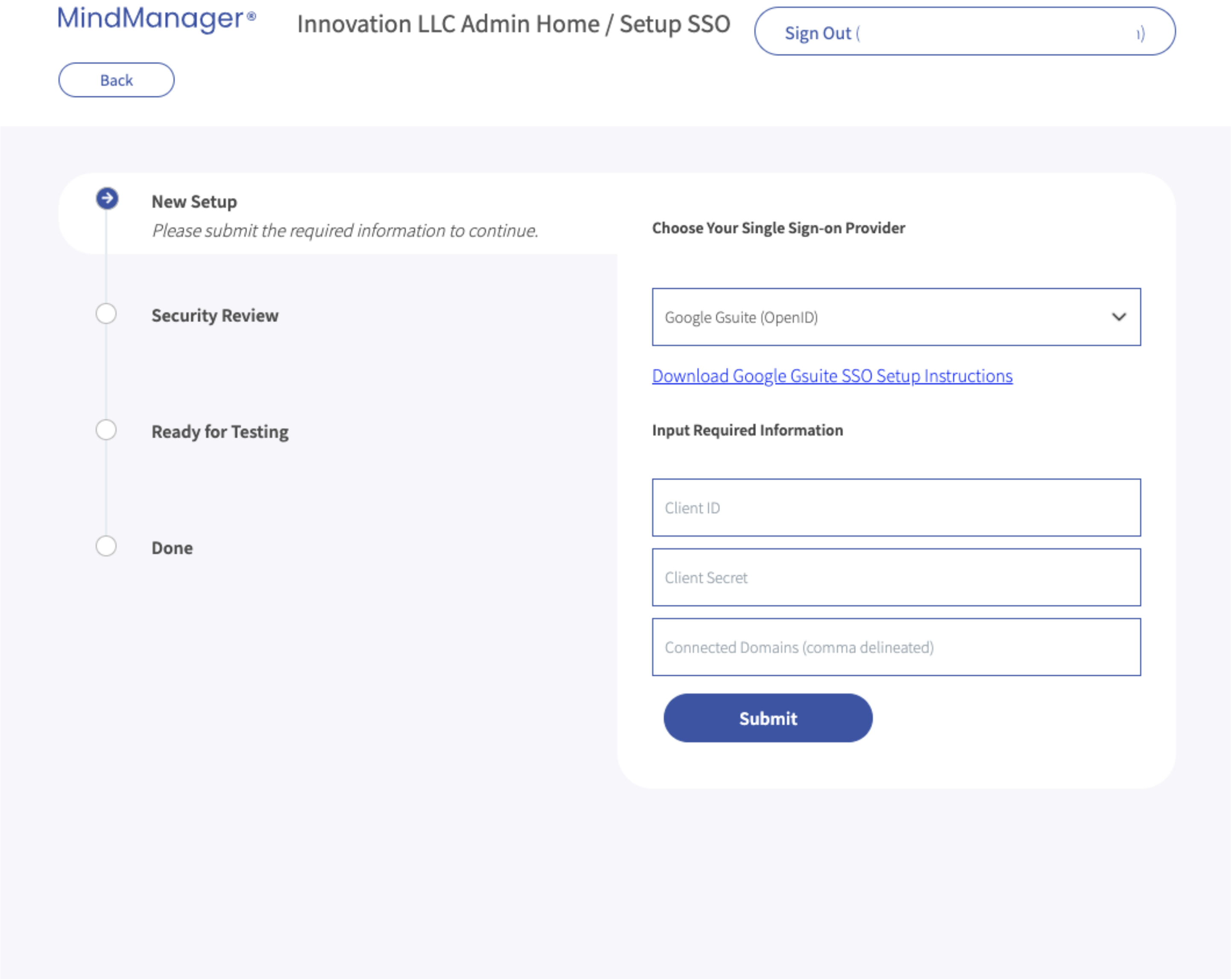
Your Client ID

[redacted]

Your Client Secret

[redacted]

Submit Your Setup Details In the MindManager Admin Portal



New Setup

Please submit the required information to continue.

Security Review

Ready for Testing

Done

Choose Your Single Sign-on Provider

Google Gsuite (OpenID)

Download Google Gsuite SSO Setup Instructions

Input Required Information

Client ID

Client Secret

Connected Domains (comma delineated)

Input the required information as described below into the fields in your Admin portal (https://cloud.mindmanager.com/admin) via the **Setup SSO** button.

- **Application Client ID**
  - Found on the App Registrations Overview Page
- **Client Secret**
  - Found on the App Registrations Certificates & Secrets page — the information copied to a text file in step 20.
- **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).

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):

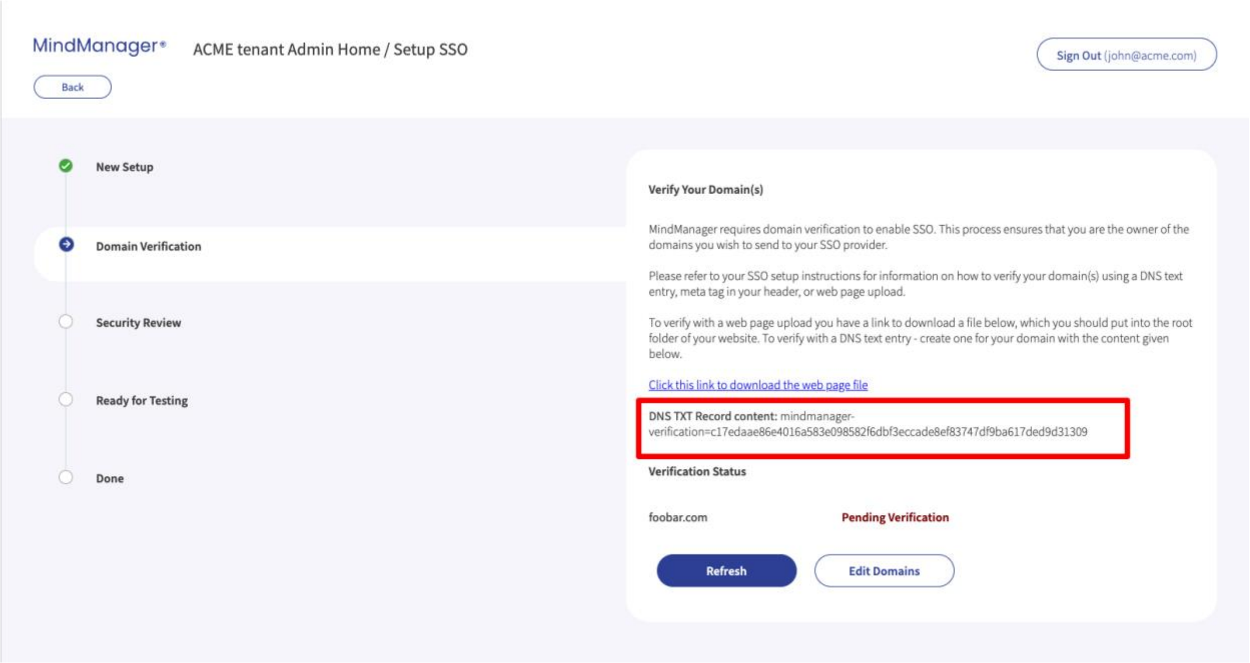
1. Add a DNS TXT entry to your DNS record to confirm that you own the domain.

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.



Verify Your Domain(s)

MindManager requires domain verification to enable SSO. This process ensures that you are the owner of the domains you wish to send to your SSO provider.

Please refer to your SSO setup instructions for information on how to verify your domain(s) using a DNS text entry, meta tag in your header, or web page upload.

To verify with a web page upload you have a link to download a file below, which you should put into the root folder of your website. To verify with a DNS text entry - create one for your domain with the content given below.

Click this link to download the web page file

DNS TXT Record content: mindmanager-verification=c17edaae86e4016a583e098582f6dbf3eccade8ef83747df9ba617ded9d31309

Verification Status

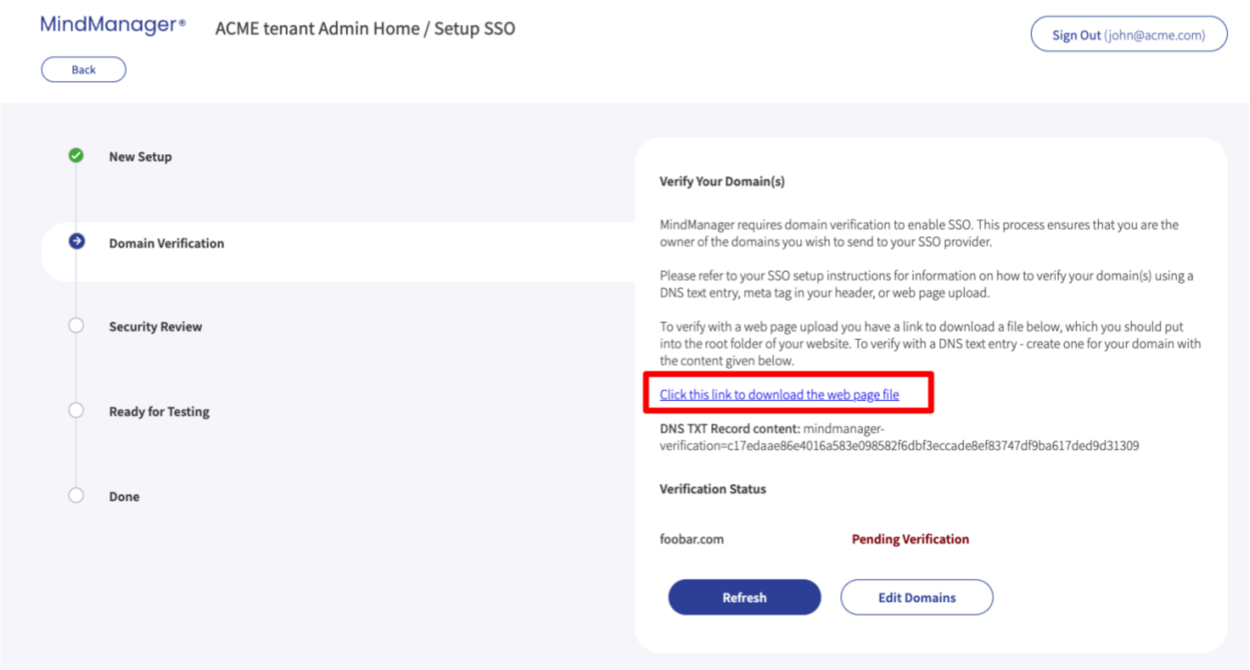
foobar.com **Pending Verification**

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.



Verify Your Domain(s)

MindManager requires domain verification to enable SSO. This process ensures that you are the owner of the domains you wish to send to your SSO provider.

Please refer to your SSO setup instructions for information on how to verify your domain(s) using a DNS text entry, meta tag in your header, or web page upload.

To verify with a web page upload you have a link to download a file below, which you should put into the root folder of your website. To verify with a DNS text entry - create one for your domain with the content given below.

Click this link to download the web page file

DNS TXT Record content: mindmanager-verification=c17edaae86e4016a583e098582f6dbf3eccade8ef83747df9ba617ded9d31309

Verification Status

foobar.com	**Pending Verification**

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.

Security Review

After you have successfully completed Domain verification, your SSO setup will move to the Security Review stage, during this stage, our team will review and add the configurations necessary to enable SSO. The security review usually takes 3-5 business days.

Ready for Testing

After our team reviews your submission and completes our configuration, you will get another email notification that your setup is ready for testing. The status in the admin portal will also show as “Ready for Testing.” Please follow the instructions in the admin portal to test your setup. If everything is working as intended, you’re done!

If you encounter issues with your setup please use the admin portal to submit a support ticket.