



MindManager Cloud Services

## Okta Single Sign-on Configuration Instructions

Presented by MindManager Product Management, Engineering, & Operations

September 19, 2023

# Table of Contents

<i>Table of Contents</i>	2
<i>About MindManager SSO</i>	3
<b>Configure your SAML connection using the Okta admin dashboard</b>	4
<b>Submit Your Setup Details In the MindManager Admin Portal</b>	17
<b>Domain Name Verification</b>	17
<b>Security Review</b>	19
<b>Ready for Testing</b>	19

# 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

# Okta Single Sign-on Configuration Instructions (SAML)

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

Configuration of SSO with Okta requires **that you have access to your Okta admin dashboard**.

Configure your SAML connection using the Okta admin dashboard

## 1. Log into your Okta account.

### Optional shortcut (advanced):

Once you are logged in, it may be possible to go directly to the page for creating your custom MindManager app integration with the correct URL and skip to step 6.

The URL will have a special prefix for your account; let's use "prefix-123" as an example. Your logged-in URL might look like this:

```
🔒 prefix-123.okta.com/app/UserHome?session_hint=AUTHENTICATED
```

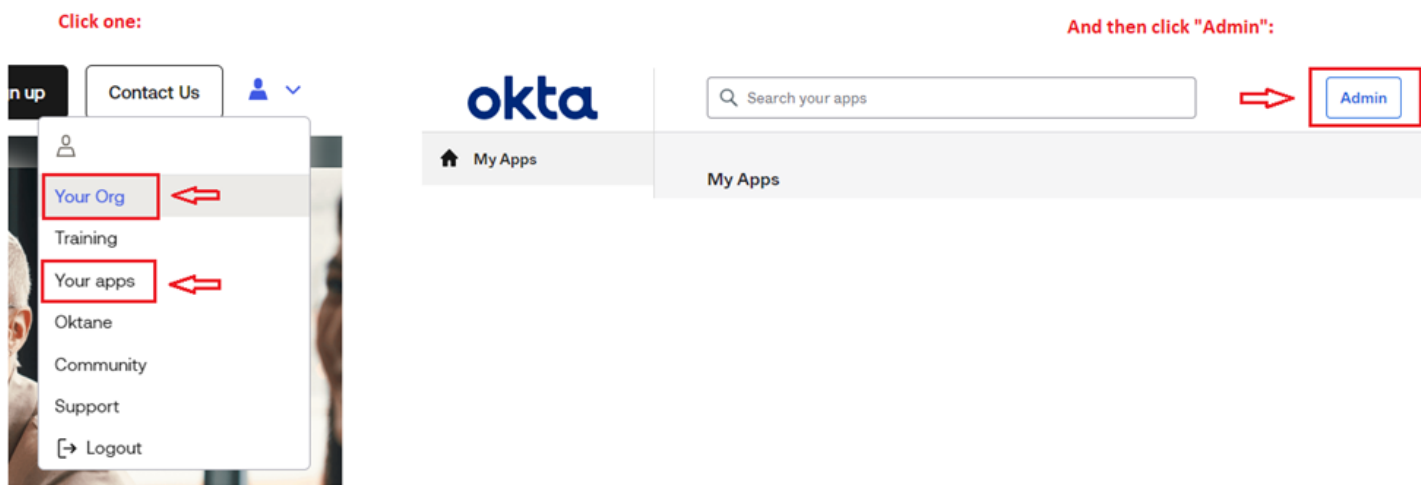
You can go directly to the page to create a new app integration by adding **-admin** to your prefix and **/admin/apps/saml-wizard/create** after "okta.com," like so:

```
🔒 https:// prefix-123 -admin.okta.com/admin/apps/saml-wizard/create
```

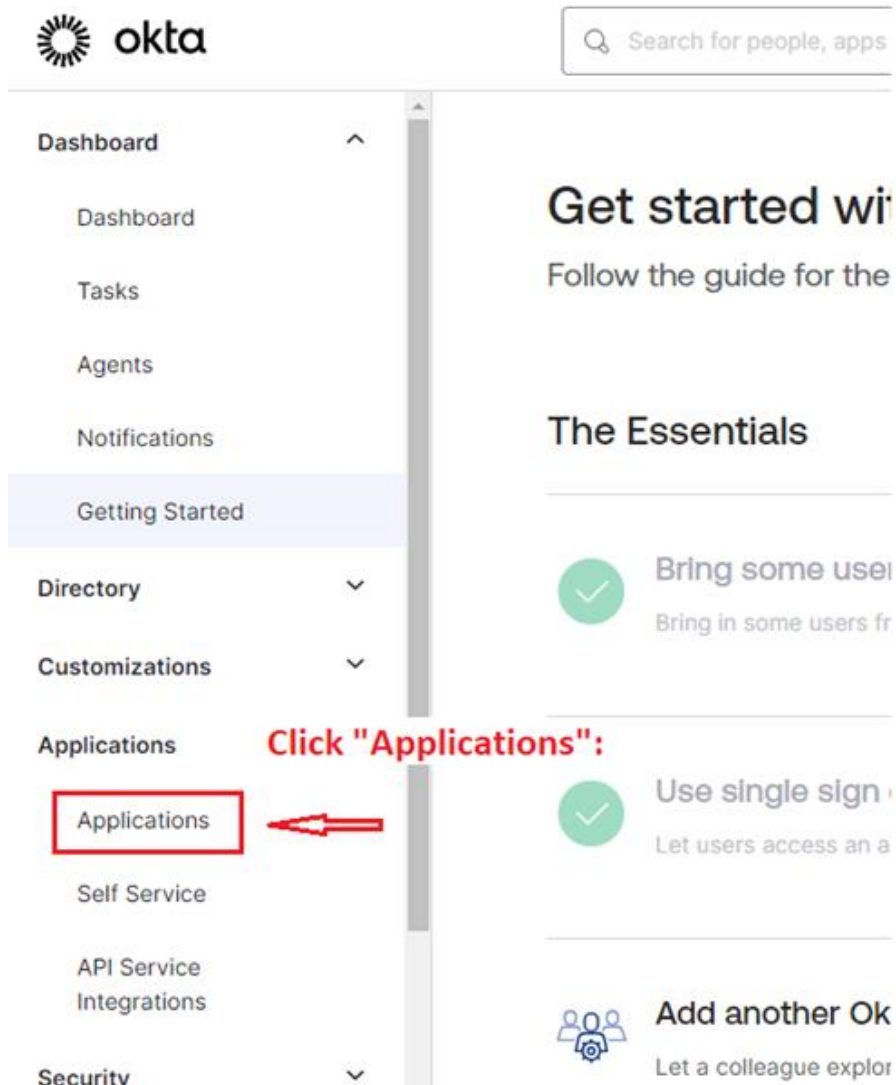
Alternatively, move on to step 2 for the click-through process.

## 2. Go to the admin dashboard.

If you signed in via <https://www.okta.com>, you can reach the admin dashboard by clicking **Your Org** or **Your apps** on the dropdown box below your profile icon and then clicking the **admin** button at the top of the next page, left of your user name:



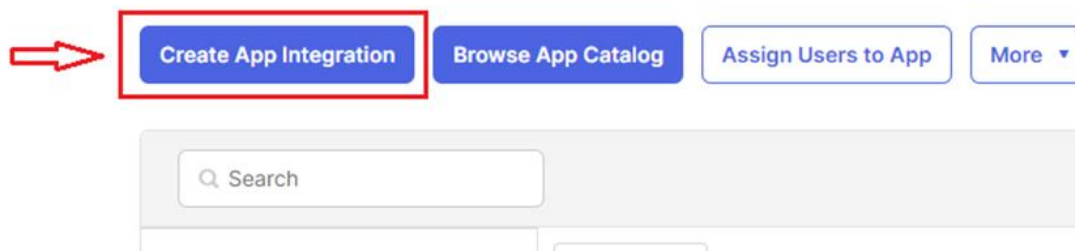
## 3. On the next page, click “Applications” under the “Applications” tab.



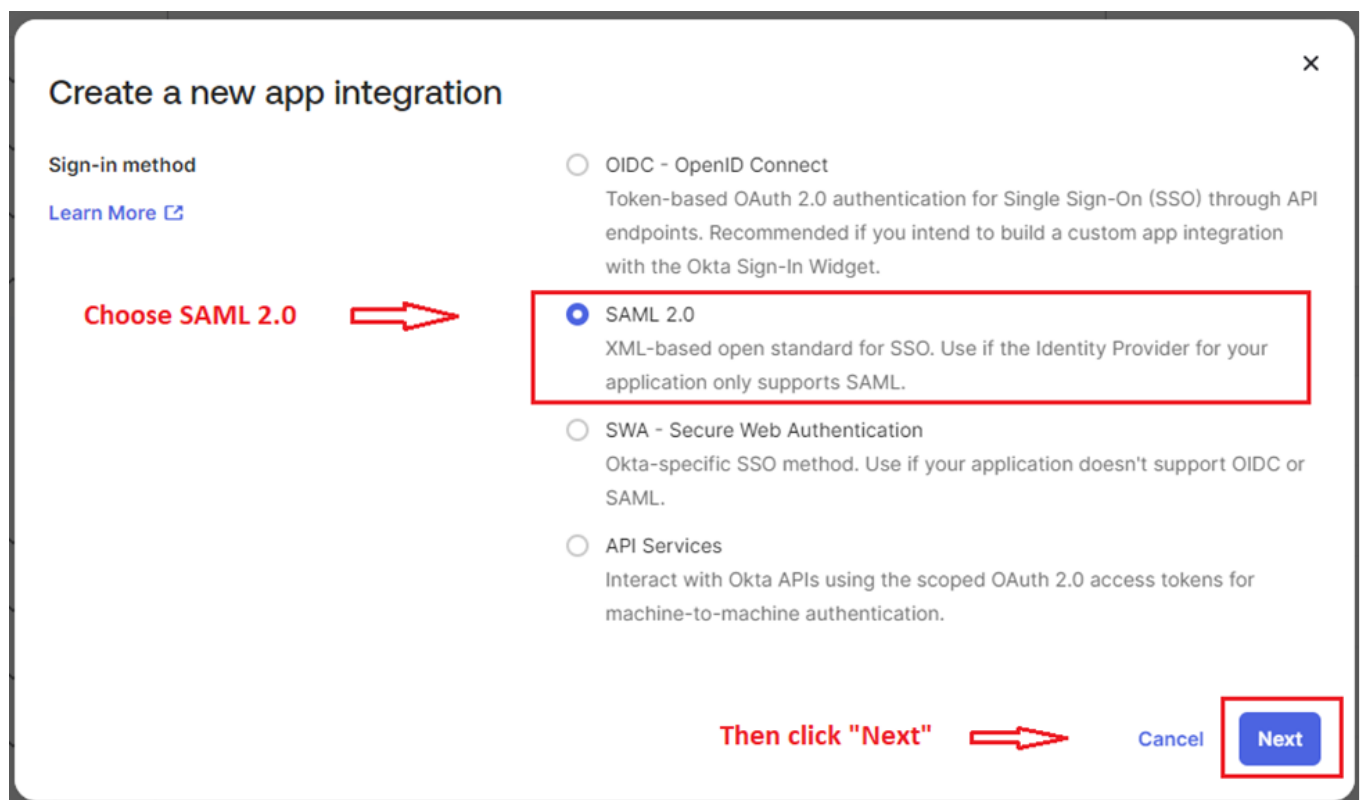
**4. On the next page, click “Create App Integration”:**

Click "Create App Integration":

## Applications



5. On the popup, choose SAML 2.0 and click "Next."








6. On the "Create SAML Integration" page, give the app a name, and click "next."

Calling the app “MindManager” is just a suggestion!

It technically isn’t necessary to add a logo or adjust any other configuration, so the rest on this page is your preference.

## Create SAML Integration

1 General Settings	2 Configure SAML
<div><div>1 General Settings</div><div><p><b>Give the app a name:</b></p><p>App name  <input type="text" value="MindManager"/></p><p>App logo (optional)  </p><div></div><p>App visibility <input type="checkbox"/> Do not display application icon to users</p><p><a href="#">Cancel</a> <b>Then click "next":</b>  <input type="button" value="Next"/></p></div></div>	

### 7. On the “Configure SAML” step, enter the following information:

1. In the **Single Sign-on URL** field, you now need to enter a **URL**
  - a. MindManager Single Sign-on 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. Paste the **first URL** into the **Single Sign-on URL** 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>
2. In the **Audience URI (SP Entity ID)** field enter: **urn:amazon:cognito:sp:eu-central-1\_Yl6Ea8Vvt**
3. In the **Name ID Format** dropdown menu select **EmailAddress**
4. In the **Application Username** dropdown menu select **Email**

**NOTE: If you are making an update to your existing SSO configuration, please use the Single sign-on URL and Audience URI from your previous configuration.**

Information shown below is for illustrative purposes only, be sure to follow the instructions above to input the correct information.

## Create SAML Integration

1 General Settings	2 Configure SAML
--------------------	------------------

A SAML Settings

General

Single sign-on URL ⓘ

https://mindmanagerdev.com/saml2/idpresponse

☒ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ⓘ

urn:amazon:cognito:sp:eu-central-1\_TaRERIfZ1

Default RelayState ⓘ

If no value is set, a blank RelayState is sent

Name ID format ⓘ

EmailAddress ▼

Application username ⓘ

Email ▼

Update application username on

Create and update ▼

Show Advanced Settings

**8. Under “Attribute Statements (optional),” enter the following:**

- For the “Name” field:  
<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>
- For the “Name format” field, choose **URI Reference**
- For the “Value” field: **user.email**

Your “Attribute Statements” area should look like this:

Attribute Statements (optional)[LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="http://schemas.xml:"/>	<input type="text" value="URI Reference"/>	<input type="text" value="user.email"/>

Add Another

**9. Click “Next” at the bottom of the page.**

[Add Another](#)

---

**Group Attribute Statements (optional)**

Name	Name format (optional)	Filter
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/> <input type="text"/>

[Add Another](#)

**B** Preview the SAML assertion generated from the information above

[<> Preview the SAML Assertion](#)

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

[Previous](#)
[Cancel](#)
Click "Next"
➔
[Next](#)


## 10. Fill out the “Feedback” form.

As a suggestion, click the “I’m an Okta customer adding an internal app” option, fill out the rest as you prefer, and click “Finish” at the bottom.

3 Help Okta Support understand how you configured this application


**Suggestion:**


Are you a customer or partner?

☒ I'm an Okta customer adding an internal app 

☐ I'm a software vendor. I'd like to integrate my app with Okta

---

 The optional questions below assist Okta Support in understanding your app integration.

App type 

☐ This is an internal app that we have created

Contact app vendor

☐ It's required to contact the vendor to enable SAML

---

Which app pages did you consult to configure SAML?

Enter links, describe where the pages are, or anything else you think is helpful

---

Did you find SAML docs for this app?


Enter any links here

---

Any tips or additional comments?

Placeholder text

---

[Previous](#) Click "Finish":  [Finish](#)

## 11. Add people to the app by user account or by group.

In our example, we had named the app "MindManager."

← Back to Applications

The screenshot shows the MindManager application interface. At the top, there is a navigation bar with a gear icon, the text "MindManager", and buttons for "Active", "View Logs", and "Monitor Imports". Below this is a tabbed interface with "General", "Sign On", "Import", and "Assignments". The "Assignments" tab is selected and highlighted with a red box. A red arrow points to this tab with the text "Click 'Assignments' tab". Below the tabs, there is a section with "Assign" and "Convert assignments" buttons, a search bar, and a "People" dropdown. A dropdown menu is open under "Assign", showing "Assign to People" and "Assign to Groups". A red arrow points to "Assign to People" with the text "Assign to users". Below this, there is a table with columns "Type" and "Groups". The table contains several rows of binary code (0s and 1s) and a magnifying glass icon.

Clicking “Assign to People” or “Assign to Groups” should open a popup.

You can add everyone (**recommended**), specific groups (if available),

The screenshot shows a popup window with a blue circular icon on the left. To the right of the icon, the text "Everyone" is displayed in blue, followed by "All users in your organization" in black. On the far right, there is a blue button labeled "Assign".

Or by individual username / email (the same username / email used to log into Okta).

The screenshot shows a popup window with a search bar at the top containing the text "Search...". Below the search bar, there are two input fields: "Your name" and "Your okta username", both in red text. On the right side, there is a blue button labeled "Assign".

When you click “Assign,” you will see another popup. Clicking “Save and Go Back” will allow you to add more users or groups.

## Assign MindManager to People



User Name

you@company.com

Click here...



Save and Go Back

Cancel

When you're finished, just click "Done":

## Assign MindManager to People



Q Search...

Your name

yourname@company.com

Assigned

Another name

anothername@company.com

Assign

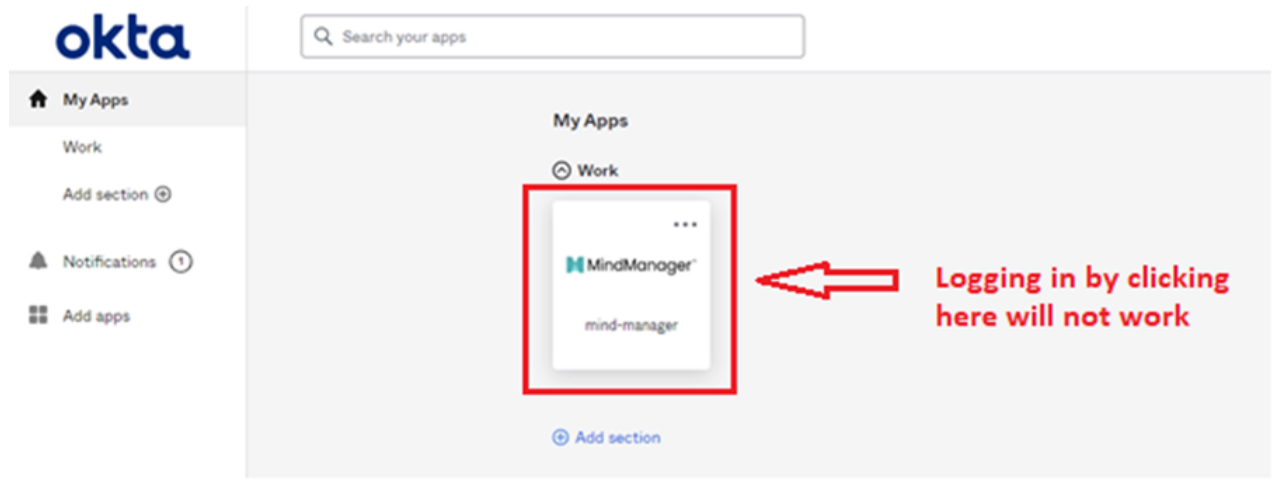
And you're done!



Done

### Important:

If you look at your non-admin Applications page (that you reach without clicking through to reach the admin dashboard), there will be an icon for your created MindManager app. If you click on the icon, **the login will not work.**



## 12. Copy the Metadata URL

Click **Applications** in the side menu.

Select the **MindManager** app you configured.

Click the **Sign On** tab.

Click **Copy**.

The screenshot shows the Okta Admin Console interface. On the left is a sidebar menu with options: Dashboard, Directory, Customizations, Applications (expanded), Self Service, API Service Integrations, Security, Workflow, Reports, and Settings. The main content area is titled 'mindmanager' and has tabs for General, Sign On (selected), Import, and Assignments. Under the 'Sign On' tab, there's a 'Settings' section with an 'Edit' link. The 'Sign on methods' section explains that the sign-on method determines how a user signs into and manages their credentials. Below this, the 'SAML 2.0' method is selected. A box labeled 'Metadata details' contains the 'Metadata URL' and a 'Copy' button. A red arrow points from the 'Copy' button to the 'Copy' text in the instructions. Below the 'Metadata details' box is a 'More details' link. At the bottom, the 'Credentials Details' section shows 'Application username format' as 'Email', 'Update application username on' as 'Create and update' (with an 'Update Now' button), and 'Password reveal' as 'Allow users to securely see their password (Recommended)'.

okta

Search for people, apps and groups

devmnr  
okta-d

← Back to Applications

mindmanager

Active View Logs Monitor Imports

Since you have a working SAML integration, submit it for Okta review to publish in the OAN. [Submit your app for review](#)

General Sign On Import Assignments

Settings Edit

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3<sup>rd</sup> party application. Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

Metadata details

Metadata URL <https://dev-20236632.okta.com/app/exka6xt0oivDX3SQA5d7/sso/saml/metadata> [Copy](#)

More details

Credentials Details

Application username format Email

Update application username on Create and update [Update Now](#)

Password reveal ☐ Allow users to securely see their password (Recommended)

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3<sup>rd</sup> party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP. [View SAML setup instructions](#)



## Submit Your Setup Details In the MindManager Admin Portal

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

- **App Federation Metadata URL**
  - Found under your application's **Sign On** tab, you copied this in step 12.
- **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](mailto: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):

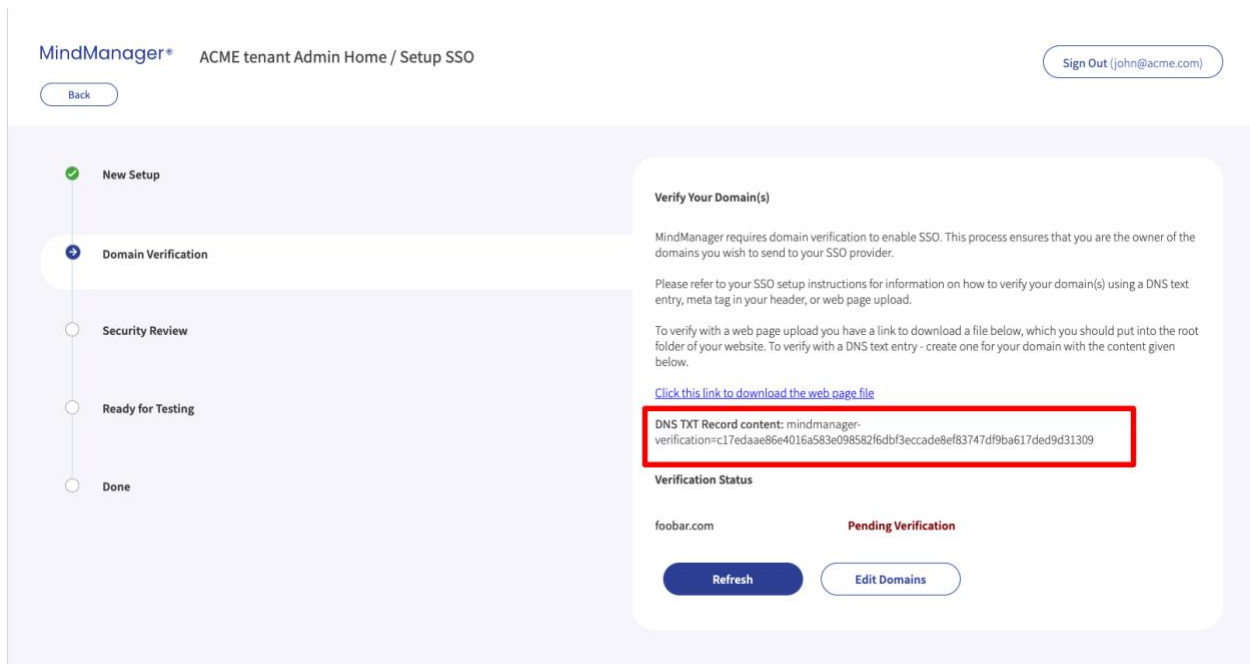
1. Add a DNS TXT entry to your DNS record to confirm that you own the domain.

**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.



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.

[Back](#)

✓ New Setup

+ Domain Verification

○ Security Review

○ Ready for Testing

○ Done

**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**[Refresh](#)[Edit Domains](#)

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.