



# Single Sign On (SSO) for Maptek Account

---

Overview and Rollout Instructions  
June 2024


## What is Single Sign On (SSO)?

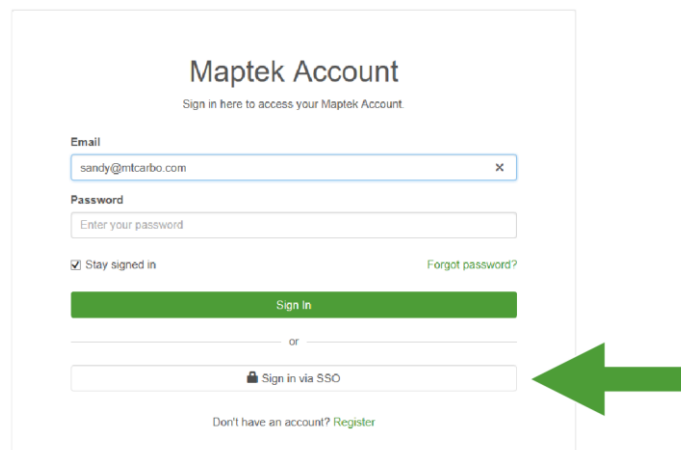
Single Sign On (SSO) is an authentication process that allows users to access multiple services with a single set of login credentials. When implemented in your organisation's Maptek Account, SSO allows users to sign in to their Maptek Account using their standard login credentials for your organisation.

The main benefits of enabling SSO are:

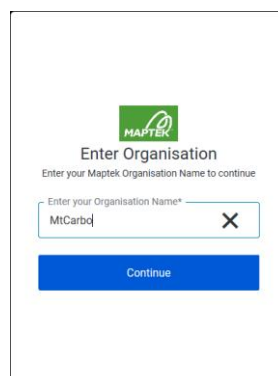
- **Improved user experience.** From the user's perspective, SSO provides a login method consistent with other systems in your organisation. SSO eliminates the need for users to manage a different set of credentials for Maptek Account.
- **Enhanced security.** SSO enables a single source of security by linking users' access to Maptek Account to their security credentials in your organisation.
- **Streamlined access management.** Because SSO links a user's Maptek Account login to their organisation login, Administrators can efficiently provision and deprovision user access to Maptek Account.

## What will the user see?

After rolling out SSO, when the user signs in to Maptek Account in Maptek Workbench, they will see a button labelled  **Sign in via SSO**.



After clicking this button, the user will be prompted to enter your *Maptek Organisation Name*:



When the user clicks **Continue**, they will then be prompted to log in using your organisation's Identity Provider. Once authenticated, the user will be signed in to their Maptek Account.

## Requirements

- To roll out SSO, your organisation's Identity Provider (IdP) must be compatible with SAML.
- SSO must be enabled by Maptek in your Maptek Account configuration before it can be rolled out by your organisation. The next section describes the procedure.

## Enabling SSO

Before SSO can be configured and rolled out, Maptek needs to enable it in your organisation's Maptek Account.

The process for this is as follows:

1. Decide on your *Maptek Organisation Name*. This is the name that users will need to enter each time they sign in to Maptek Account using SSO. The Maptek Organisation Name must:
  - Only contain letters, numbers, dashes (-) and underscores (\_)
  - Start with a letter or number
  - Be between 3-50 characters in length

**i Note:** Your chosen Maptek Organisation Name can include a combination of uppercase and lowercase letters, but when the user enters the name, case is ignored.

2. Contact Maptek and request that SSO be enabled for your organisation. You will need to provide the following information:
  - **Maptek Organisation Name.**
  - **Root admin.** Please provide the contact details of the person in your organisation who will be responsible for configuring SSO in your organisation's Maptek Account.

Maptek will enable SSO in your Maptek Account configuration and provide the root admin with the required privileges to configure SSO.

3. When Maptek confirms that SSO has been enabled, the special admin contact will be able to configure and roll out SSO for your organisation, as described in the next section.

## Configuring and rolling out SSO

**i Note:** Only the designated root admin as discussed in the previous section can configure SSO.

To configure and roll out SSO follow these steps:

1. In your IdP, configure groups and assign members to them according to your organisation's requirements.

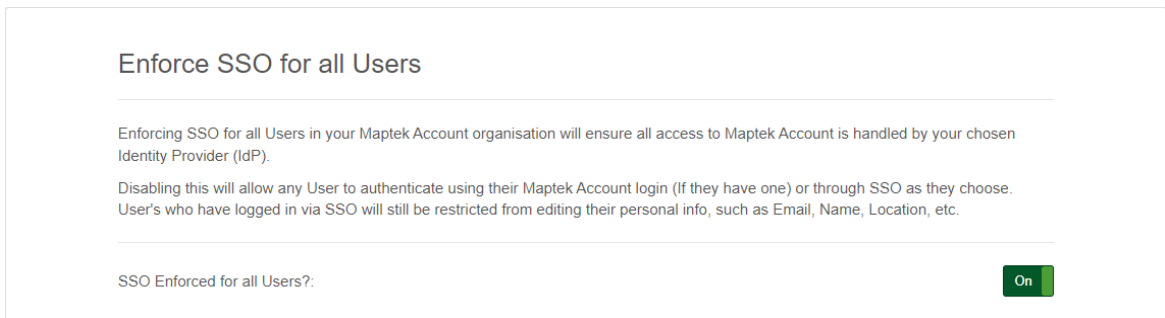
**i Note:** When using SSO, users' group memberships are handled by the IdP and cannot be managed in Maptek Account. Any existing group memberships in Maptek Account that do not match with those configured in the IdP will be removed for users using SSO.

2. Log in to Maptek Account.

3. In Maptek Account, create groups corresponding to those configured in your IdP. The group names must match those defined in your IdP exactly.
4. Decide whether you want to enforce SSO for all users after rollout.

By default, SSO will be enforced for all users, meaning they will not be able to log in with their previous Maptek Account credentials once SSO is rolled out.

If you want to give users the choice between using their existing credentials or SSO to sign in, change the setting located under **Administration > More > Organisation Settings > Manage SSO Enforcement**.



**Enforce SSO for all Users**

Enforcing SSO for all Users in your Maptek Account organisation will ensure all access to Maptek Account is handled by your chosen Identity Provider (IdP).

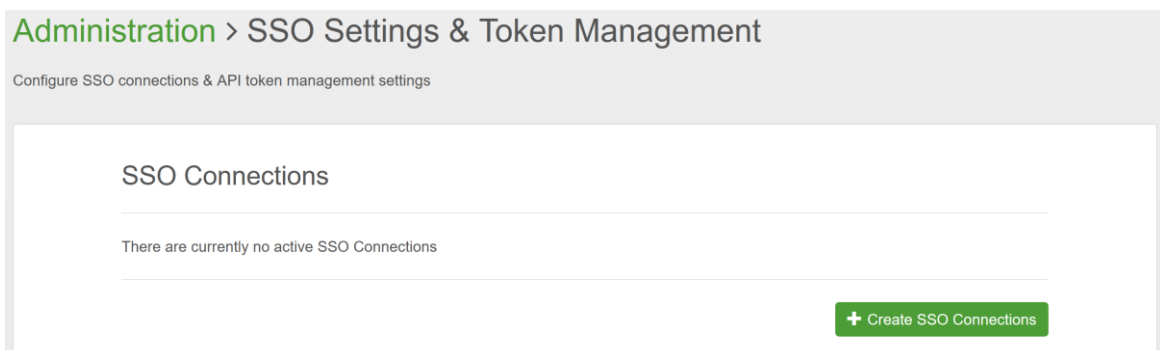
Disabling this will allow any User to authenticate using their Maptek Account login (if they have one) or through SSO as they choose. User's who have logged in via SSO will still be restricted from editing their personal info, such as Email, Name, Location, etc.

SSO Enforced for all Users?:  On

You can choose to turn this option off before rollout to ensure continuity for users who are logged in. The setting can be changed any time after rollout.

**Note:** The root admin retains the ability to sign in without SSO, regardless of this setting. Additionally, individual users can be configured to ignore SSO enforcement, allowing them to sign in with separate credentials.

5. Navigate to **Administration > More > Organisation Settings > Manage SSO Settings** and click **Manage** to open the **SSO Settings & Token Management** page.
6. Under **SSO Connections**, click **Create SSO Connections**.



**Administration > SSO Settings & Token Management**

Configure SSO connections & API token management settings

**SSO Connections**

There are currently no active SSO Connections

[+ Create SSO Connections](#)

7. Follow the instructions on the page under **Step 1: Service Provider Metadata** to establish a trust relationship in your IdP with Maptek Account as a service provider.

## Step 1: Service Provider Metadata

First, you'll need to create an Application in your IdP and select SAML as the connection type.

The following information is what's required to establish a trust relationship with Maptek Account as a Service Provider. You can copy and paste this information or download the Maptek Account metadata file and upload it to your IdP.

[Download Metafile](#)

Single Sign On URL:

[Copy](#)

Entity ID:

[Copy](#)

- Follow the instructions on the page under **Step 2: Identity Provider Metadata** to configure Maptek Account with your IdP sign-in URL and signing certificate.

## Step 2: Identity Provider Metadata

Second, once the App has been created in the IdP, Maptek Account requires Sign In URL and Signing Cert provided by your IdP.

Connection Description

IdP Provided Sign in URL\*

Signing Certificate (Only upload if you wish to change the cert)

[Choose file](#) No file chosen

Only accept PEM or CER or CERT certificate

### Instructions for Adding Attribute Statements in Your IdP Configuration

The following claims/properties are required for Maptek Account SSO to function. Failing to set these up will result in SSO not working.

- firstName
- lastName
- email
- maGroups (Group Attribute Claim): A list of groups to link up with the Maptek Account equivalent. This is done through exact name matching.

Optional claims/properties to enhance your Identity Provider (IdP) configuration

- jobTitle (optional): Improve support and user experience by providing user's job title and site name from your IdP
- siteName (optional)
- location (optional): If not provided, your organization's users will be prompted to select a location, and the value should be in the country code format. (e.g. "AU" or "US")

Important Note:

When configuring the "maGroups" attribute in your Identity Provider (IdP), please be aware that we currently enforce a maximum limit of 20 groups per user.

Some IdPs offer the ability to use group filtering, which we recommend utilizing.

If you wish, you can prefix these groups in the IdP with "MaptekAccount-", the application will align the groups sent from your IdP with Maptek Account groups by name, excluding the specified prefix. (e.g. IdP Group "MaptekAccount-Vulcan Users" will match to Maptek Account group "Vulcan Users")

Without the prefix, exact name matching will occur.

(e.g. IdP Group "Vulcan Users" will match to Maptek Account group "Vulcan Users")

The attribute keys are case-sensitive and must match exactly as listed. Any variation may result in an inability to recognize the provided values.

[Confirm and Save](#)

- Click **Confirm and Save**. SSO will now be enabled.