Tutorial: Azure Active Directory single sign-on (SSO) integration with KnowledgeOwl

Article • 11/10/2021 • 7 minutes to read • 16 contributors

In this article

In this tutorial, you'll learn how to integrate KnowledgeOwl with Azure Active Directory (Azure AD). When you integrate KnowledgeOwl with Azure AD, you can:

- Control in Azure AD who has access to KnowledgeOwl.
- Enable your users to be automatically signed-in to KnowledgeOwl with their Azure AD accounts.
- Manage your accounts in one central location - the Azure portal.

Prerequisites

To get started, you need the following items:

- An Azure AD subscription. If you don't have a subscription, you can get a free account .
- KnowledgeOwl single sign-on (SSO) enabled subscription.

Scenario description

In this tutorial, you configure and test Azure AD SSO in a test environment.

- KnowledgeOwl supports **SP and IDP** initiated SSO.
- KnowledgeOwl supports **Just In Time** user provisioning.

Add KnowledgeOwl from the gallery

To configure the integration of KnowledgeOwl into Azure AD, you need to add KnowledgeOwl from the gallery to your list of managed SaaS apps.

1. Sign in to the Azure portal using either a work or school account, or a personal Microsoft account.
2. On the left navigation pane, select the **Azure Active Directory** service.
3. Navigate to **Enterprise Applications** and then select **All Applications**.
4. To add new application, select **New application**.
5. In the **Add from the gallery** section, type **KnowledgeOwl** in the search box.
6. Select **KnowledgeOwl** from results panel and then add the app. Wait a few seconds while the app is added to your tenant.

Configure and test Azure AD SSO for KnowledgeOwl

Configure and test Azure AD SSO with KnowledgeOwl using a test user called **B.Simon**. For SSO to work, you need to establish a link relationship between an Azure AD user and the related user in KnowledgeOwl.

To configure and test Azure AD SSO with KnowledgeOwl, perform the following steps:

1. **Configure Azure AD SSO** - to enable your users to use this feature.
   a. **Create an Azure AD test user** - to test Azure AD single sign-on with B.Simon.
   b. **Assign the Azure AD test user** - to enable B.Simon to use Azure AD single sign-on.
2. **Configure KnowledgeOwl SSO** - to configure the single sign-on settings on application side.
   a. **Create KnowledgeOwl test user** - to have a counterpart of B.Simon in KnowledgeOwl that is linked to the Azure AD representation of user.
3. **Test SSO** - to verify whether the configuration works.

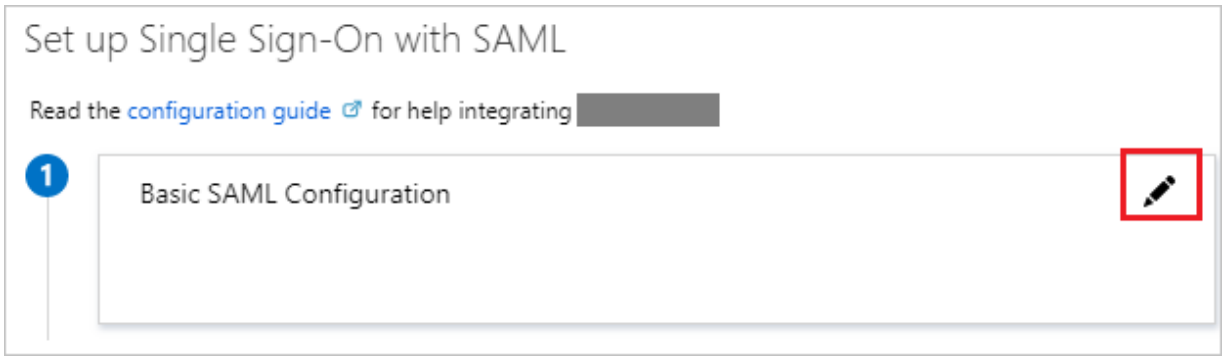
Configure Azure AD SSO

Follow these steps to enable Azure AD SSO in the Azure portal.

1. In the Azure portal, on the **KnowledgeOwl** application integration page, find the **Manage** section and select **single sign-on**.

2. On the **Select a single sign-on method** page, select **SAML**.

3. On the **Set up single sign-on with SAML** page, click the pencil icon for **Basic SAML Configuration** to edit the settings.



4. On the **Basic SAML Configuration** section, if you wish to configure the application in **IDP** initiated mode, enter the values for the following fields:

   a. In the **Identifier** text box, type the URL using one of the following patterns:

```
HTTP
https://app.knowledgeowl.com/sp
https://app.knowledgeowl.com/sp/id/<unique ID>
```

   b. In the **Reply URL** text box, type the URL using one of the following patterns:

```
HTTP
https://subdomain.knowledgeowl.com/help/saml-login
https://subdomain.knowledgeowl.com/docs/saml-login
https://subdomain.knowledgeowl.com/home/saml-login
https://privatedomain.com/help/saml-login
https://privatedomain.com/docs/saml-login
https://privatedomain.com/home/saml-login
```

5. Click **Set additional URLs** and perform the following step if you wish to configure the application in **SP** initiated mode:

   In the **Sign-on URL** text box, type the URL using one of the following patterns:

```
HTTP
https://subdomain.knowledgeowl.com/help/saml-login
https://subdomain.knowledgeowl.com/docs/saml-login
https://subdomain.knowledgeowl.com/home/saml-login
https://privatedomain.com/help/saml-login
https://privatedomain.com/docs/saml-login
https://privatedomain.com/home/saml-login
```

> **Note**
>
> These values are not real. You'll need to update these value from actual Identifier, Reply URL, and Sign-On URL which is explained later in the tutorial.

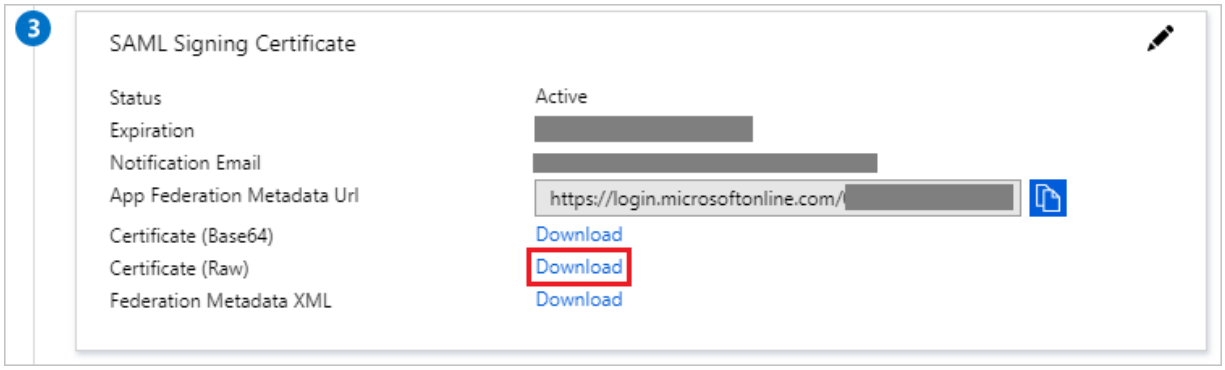
6. KnowledgeOwl application expects the SAML assertions in a specific format, which requires you to add custom attribute mappings to your SAML token attributes configuration. The following screenshot shows the list of default attributes.

7. In addition to above, KnowledgeOwl application expects few more attributes to be passed back in SAML response which are shown below. These attributes are also pre populated but you can review them as per your requirements.

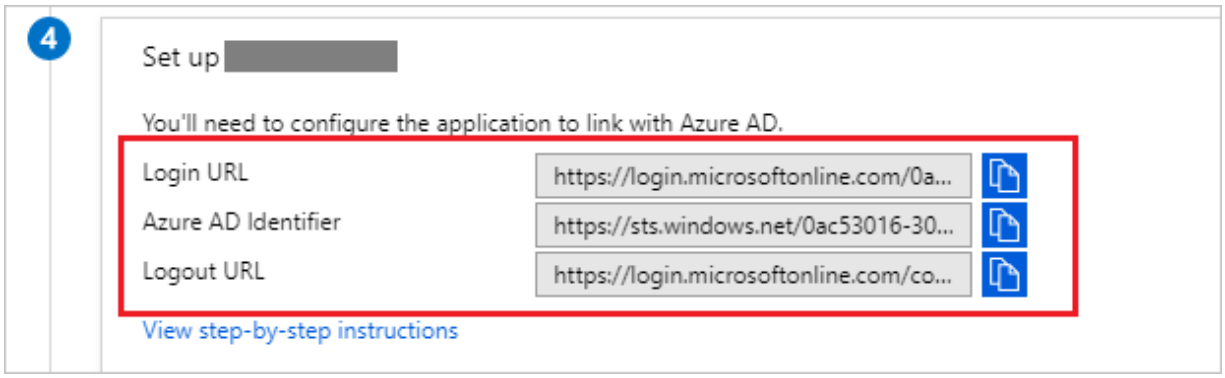
Name	Source Attribute	Namespace
ssoid	user.mail	`http://schemas.xmlsoap.org/ws/2005/05/identity/claims`

8. On the **Set up single sign-on with SAML** page, in the **SAML Signing Certificate** section, find **Certificate (Raw)** and select **Download** to download the certificate and

save it on your computer.



9. On the **Set up KnowledgeOwl** section, copy the appropriate URL(s) based on your requirement.



Create an Azure AD test user

In this section, you'll create a test user in the Azure portal called B.Simon.

1. From the left pane in the Azure portal, select **Azure Active Directory**, select **Users**, and then select **All users**.
2. Select **New user** at the top of the screen.
3. In the **User** properties, follow these steps:
   a. In the **Name** field, enter `B.Simon`.
   b. In the **User name** field, enter the username@companydomain.extension. For example, `B.Simon@contoso.com`.
   c. Select the **Show password** check box, and then write down the value that's displayed in the **Password** box.
   d. Click **Create**.

Assign the Azure AD test user

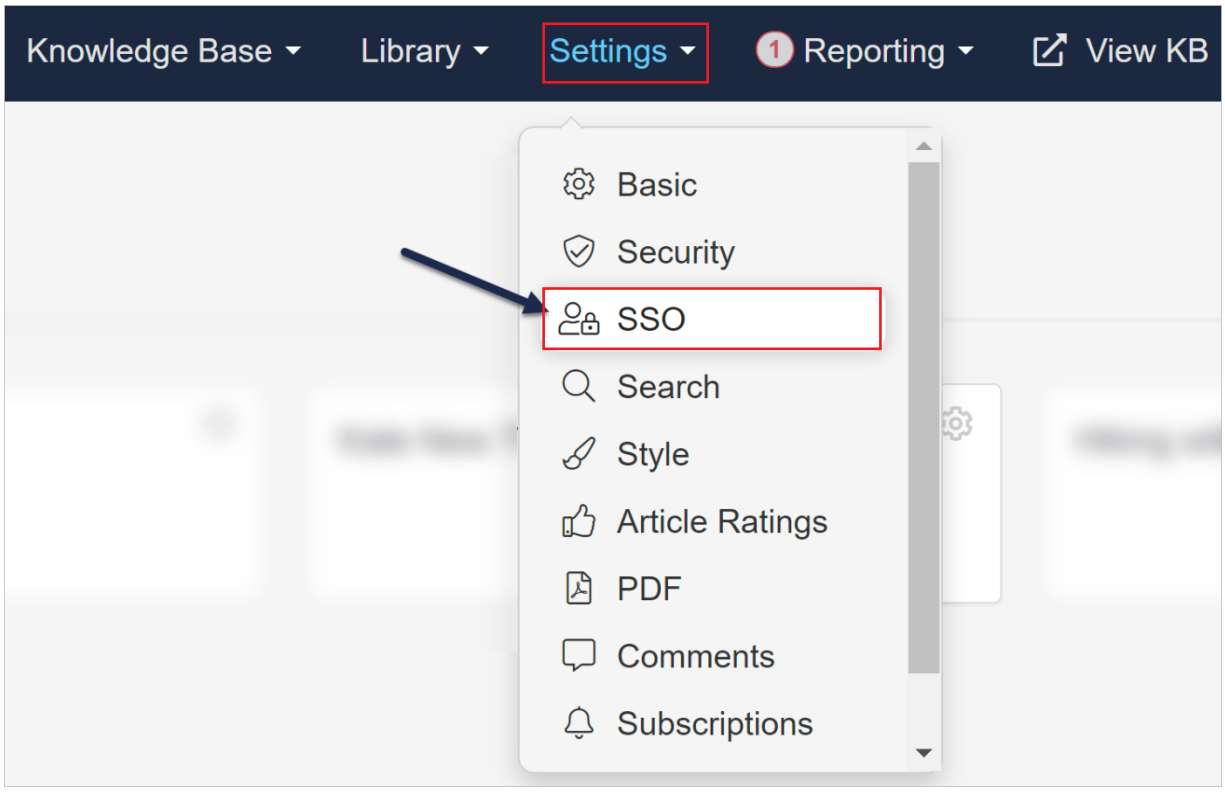
In this section, you'll enable B.Simon to use Azure single sign-on by granting access to KnowledgeOwl.

1. In the Azure portal, select **Enterprise Applications**, and then select **All applications**.
2. In the applications list, select **KnowledgeOwl**.
3. In the app's overview page, find the **Manage** section and select **Users and groups**.
4. Select **Add user**, then select **Users and groups** in the **Add Assignment** dialog.
5. In the **Users and groups** dialog, select **B.Simon** from the Users list, then click the **Select** button at the bottom of the screen.
6. If you are expecting a role to be assigned to the users, you can select it from the **Select a role** dropdown. If no role has been set up for this app, you see "Default Access" role selected.
7. In the **Add Assignment** dialog, click the **Assign** button.

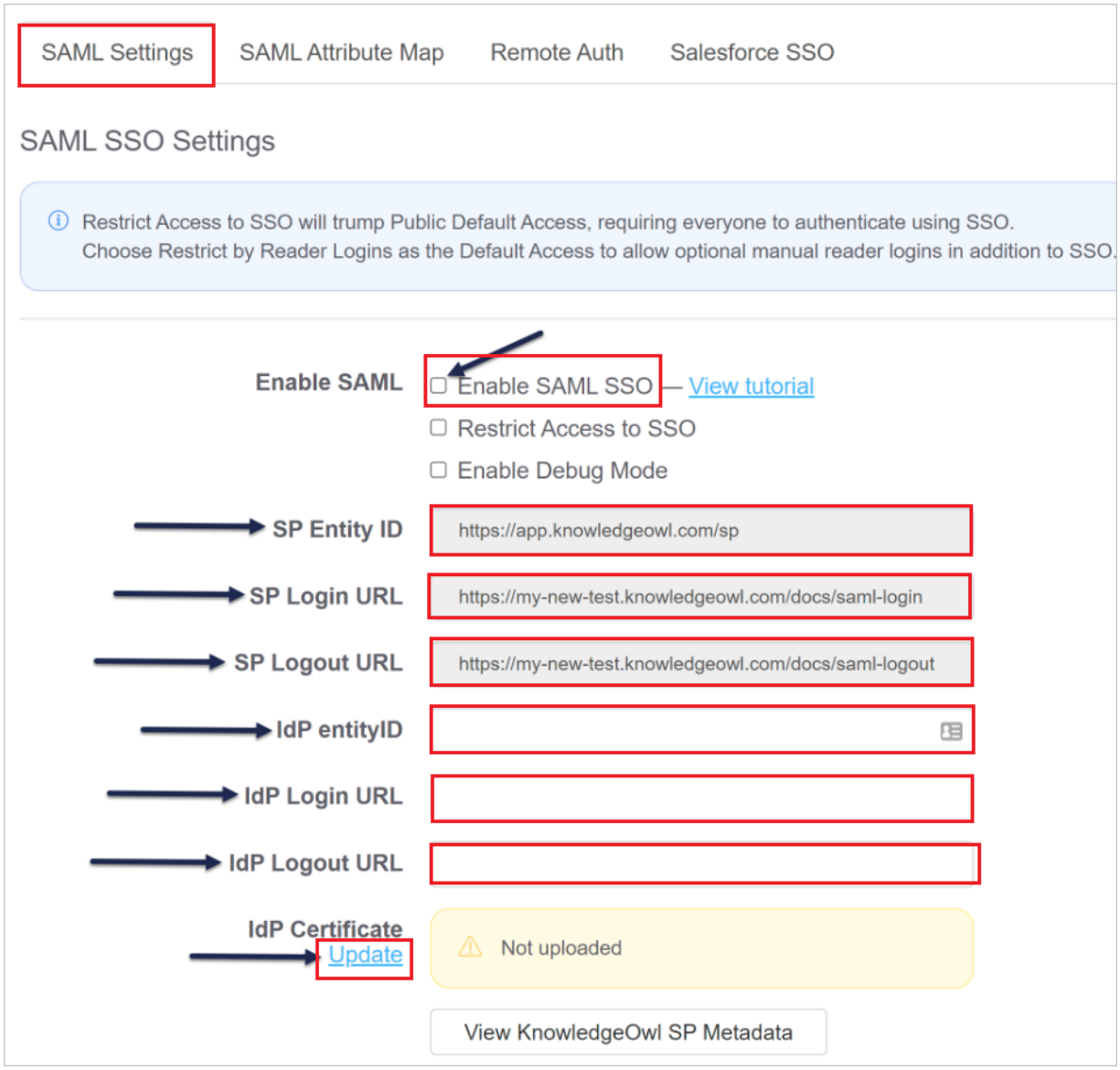
Configure KnowledgeOwl SSO

1. In a different web browser window, sign in to your KnowledgeOwl company site as an administrator.

2. Click on **Settings** and then select **SSO**.



3. In the Scroll to **SAML Settings** tab, perform the following steps:



a. Select **Enable SAML SSO**.

b. Copy the **SP Entity ID** value and paste it into the **Identifier (Entity ID)** in the **Basic SAML Configuration** section on the Azure portal.

c. Copy the **SP Login URL** value and paste it into the **Sign-on URL and Reply URL** textboxes in the **Basic SAML Configuration** section on the Azure portal.

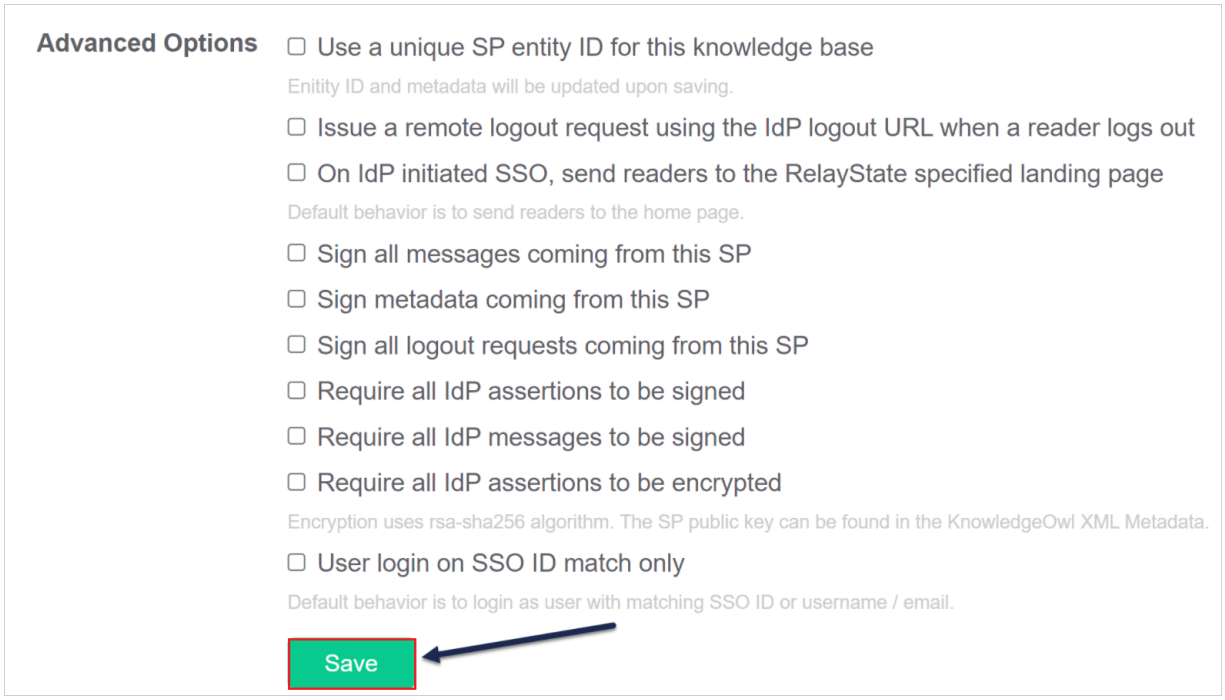
d. In the **IdP entityID** textbox, paste the **Azure AD Identifier** value, which you have copied from the Azure portal.

e. In the **IdP Login URL** textbox, paste the **Login URL** value, which you have copied from the Azure portal.

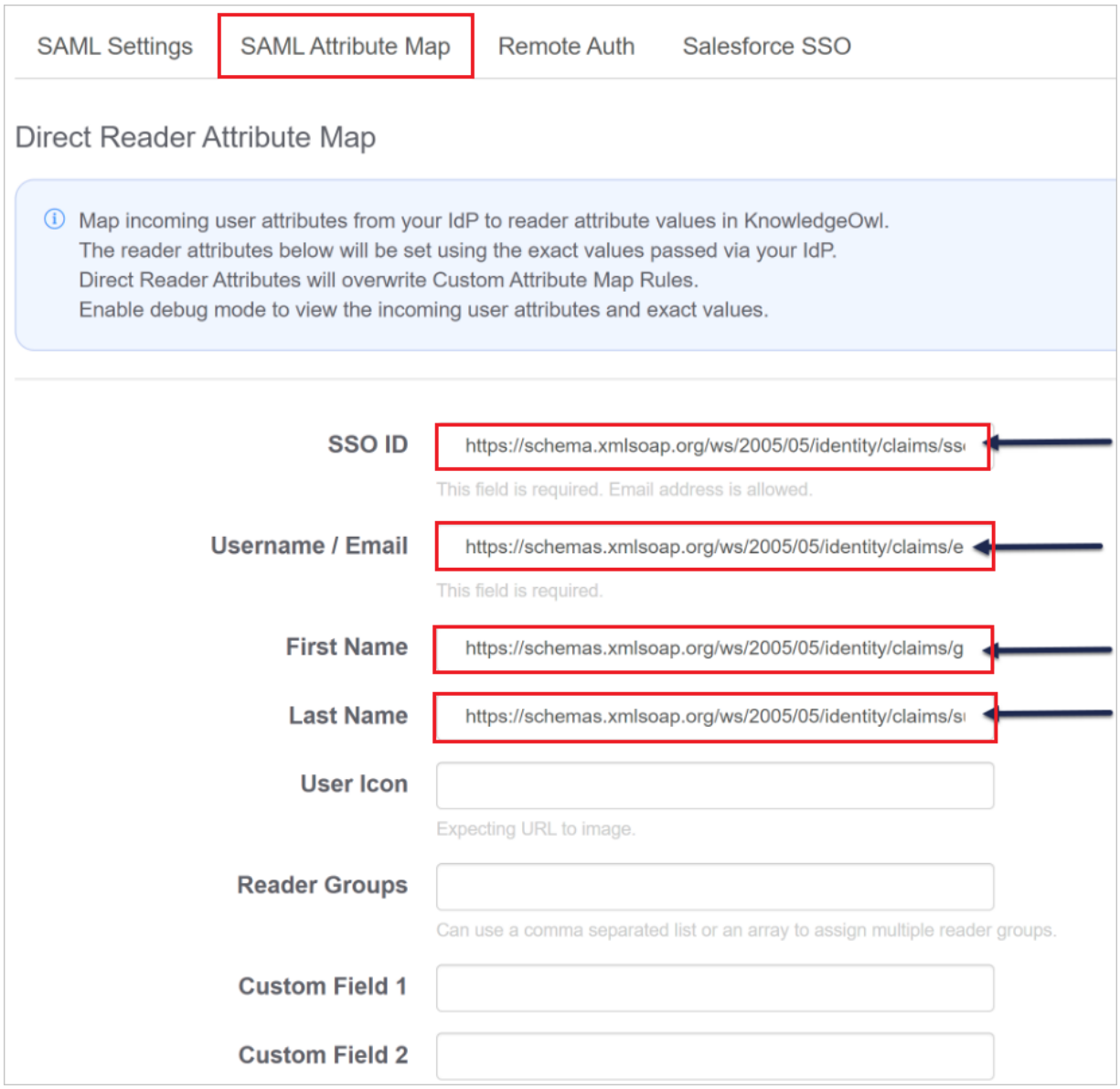
f. In the **IdP Logout URL** textbox, paste the **Logout URL** value, which you have copied from the Azure portal.

g. Upload the downloaded certificate form the Azure portal by clicking the **Upload** link beneath **IdP Certificate**.

h. Click **Save** at the bottom of the page.

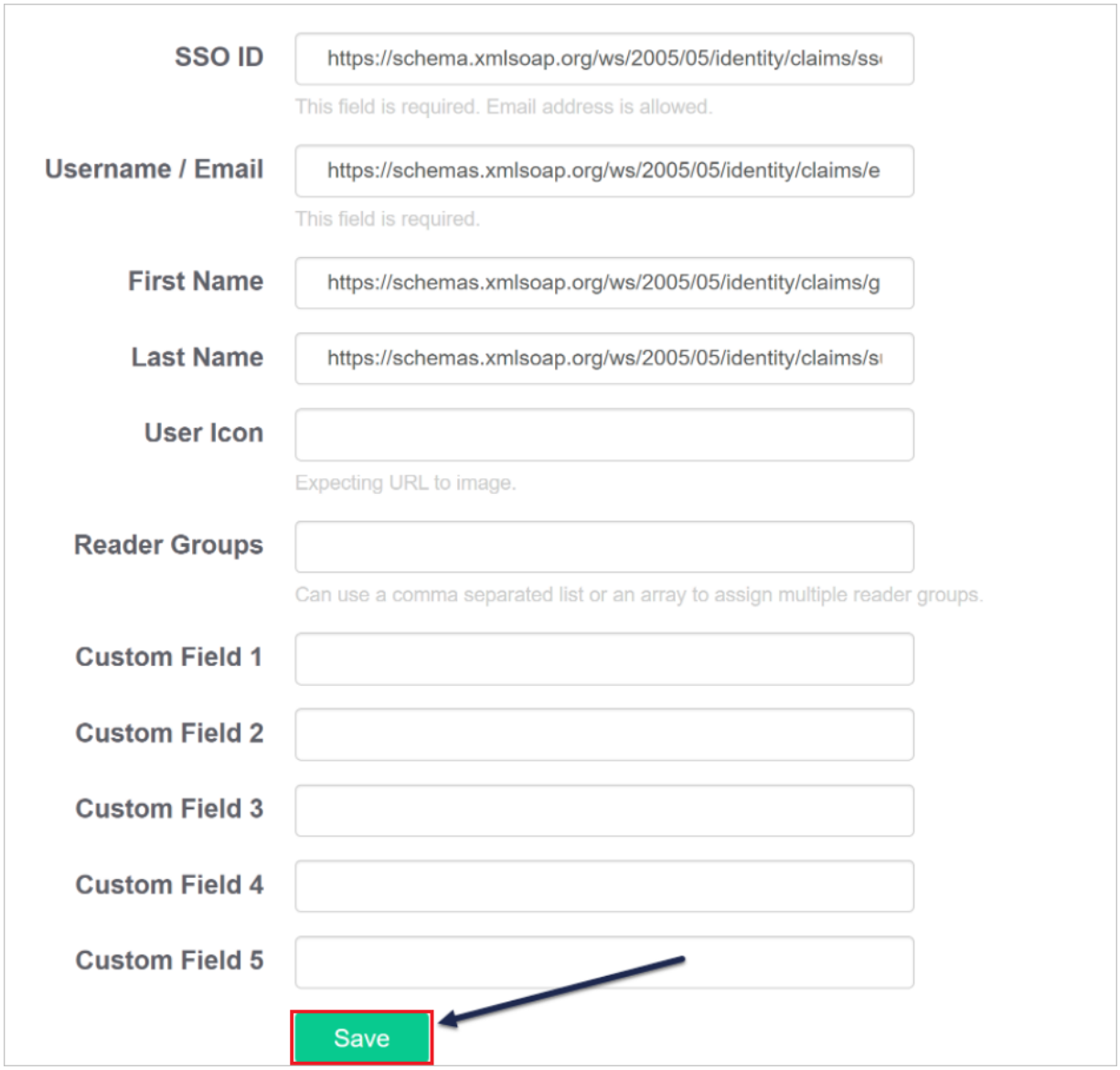


i. Open the **SAML Attribute Map** tab to map attributes and perform the following steps:



- Enter `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ssoid` into the **SSO ID** textbox.
- Enter `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress` into the **Username/Email** textbox.
- Enter `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname` into the **First Name** textbox.
- Enter `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname` into the **Last Name** textbox.

j. Click **Save** at the bottom of the page.



Create KnowledgeOwl test user

In this section, a user called B.Simon is created in KnowledgeOwl. KnowledgeOwl supports just-in-time user provisioning, which is enabled by default. There is no action item for you in this section. If a user doesn't already exist in KnowledgeOwl, a new one is created after authentication.

> ⓘ **Note**
>
> If you need to create a user manually, contact **KnowledgeOwl support team**.

Test SSO

In this section, you test your Azure AD single sign-on configuration with following options.

SP initiated

- Click on **Test this application** in Azure portal. This will redirect to KnowledgeOwl Sign on URL where you can initiate the login flow.
- Go to the KnowledgeOwl sign-on URL directly and initiate the login flow from there.

IDP initiated

- Click on **Test this application** in the Azure portal and you should be automatically signed in to the KnowledgeOwl application for which you set up the SSO.

You can also use the Microsoft My Apps portal to test the application in any mode. When you click the KnowledgeOwl tile in the My Apps portal, if configured in SP mode you would be redirected to the application sign on page for initiating the login flow and if configured in IDP mode, you should be automatically signed in to the KnowledgeOwl application for which you set up the SSO. For more information about the My Apps portal, see Introduction to My Apps .

Next steps

Once you configure KnowledgeOwl, you can enforce session control, which protects exfiltration and infiltration of your organization's sensitive data in real time. Session control extends from Conditional Access. Learn how to enforce session control with Microsoft Defender for Cloud Apps.

Recommended content

Debug SAML-based single sign-on - Azure AD

Debug SAML-based single sign-on to applications in Azure Active Directory.

Azure AD Connect: Use a SAML 2.0 Identity Provider for Single Sign On - Azure

This document describes using a SAML 2.0 compliant Idp for single sign on.

Error message appears on app page after you sign in - Azure AD

How to resolve issues with Azure AD sign in when the app returns an error message.

Tutorial: Azure Active Directory integration with SAML SSO for Confluence by resolution GmbH

Learn how to configure single sign-on between Azure Active Directory and SAML SSO for Confluence by resolution GmbH.

Configure a SAML 2.0 provider for portals with Azure AD - Power Apps

Learn how to configure SAML 2.0 for portals with Azure Active Directory.

Error AADSTS750054 - SAMLRequest or SAMLResponse must be present as query string parameters in HTTP request for SAML Redirect binding. - Active Directory

Describes a problem in which you receive an error message when signing in to SAML-based single sign-on configured app that has been configured to use Azure Active Directory as an Identity Provider (IdP). The error you receive is Error AADSTS750054 - SAMLRequest or...

Problems signing in to SAML-based single sign-on configured apps - Active Directory

Guidance for the specific errors when signing into an application you have configured for SAML-based federated single sign-on with Azure Active Directory.

Troubleshoot SAML-based single sign-on - Azure AD

Troubleshoot issues with an Azure AD app that's configured for SAML-based single sign-on.

Show more