

[Docs](#) / [Power Platform](#) / [Power Apps](#) / [Portals](#) / [Portal authentication](#) /

Configure a SAML 2.0 provider for portals with Azure AD

Article • 02/15/2022 • 2 minutes to read • [3 contributors](#)



In this article, you'll learn about configuring a SAML 2.0 provider for portals with Azure Active Directory (Azure AD).


ⓘ Note


- Portals can be configured with identity providers that conform to the Security Assertion Markup Language (SAML) 2.0 standard. In this article, you'll learn about using Azure AD as an example of identity providers that use SAML 2.0. Changes to the authentication settings **might take a few minutes** to be reflected on the portal. Restart the portal by using **portal actions** if you want the changes to be reflected immediately.

To configure Azure AD as the SAML 2.0 provider

1. Select [Add provider](#) for your portal.
2. For **Login provider**, select **Other**.
3. For **Protocol**, select **SAML 2.0**.
4. Enter a provider name.

Configure identity provider

 Select provider

 Configure SAML 2.0 provider

Select a provider
Select the identity provider to use with your portal.

Select login provider

Other

Protocol

SAML 2.0


Provider name *


Contoso SAML 2.0

5. Select **Next**.

6. In this step, you create the application and configure the settings with your identity provider.

Configure identity provider


 Select provider

 Configure SAML 2.0 provider

1. Create and configure SAML 2.0 provider settings
To use a SAML 2.0 based identity provider, you'll need to create an application and configure settings with your identity provider. [Learn more](#)
Add the following Reply URL while creating the application.

Reply URL ⓘ

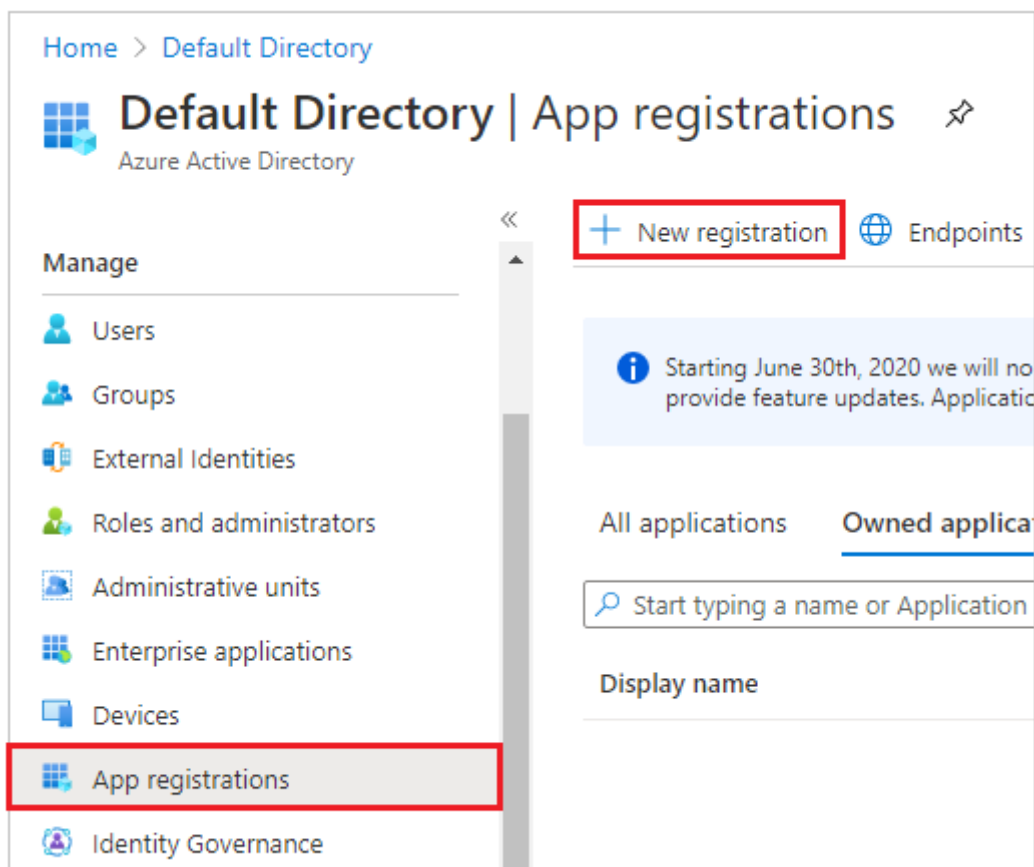
https://contoso-portal.powerappsportals.com/signin-saml_1

 Copy

ⓘ Note

- The Reply URL is used by the app to redirect users to the portal after the authentication succeeds. If your portal uses a custom domain name, you might have a different URL than the one provided here.
- More details about creating the app registration on the Azure portal are available in [Quickstart: Register an application with the Microsoft identity platform](#).

- a. Sign in to the [Azure portal](#).
- b. Search for and select **Azure Active Directory**.
- c. Under **Manage**, select **App registrations**.
- d. Select **New registration**.



- e. Enter a name.
- f. If necessary, select a different **Supported account type**. More information: [Supported account types](#)
- g. Under **Redirect URI**, select **Web** (if it isn't already selected).
- h. Enter the **Reply URL** for your portal in the **Redirect URI** text box.
Example: `https://contoso-portal.powerappsportals.com/signin-saml_1`

ⓘ Note

If you're using the default portal URL, copy and paste the **Reply URL** as shown in the **Create and configure SAML 2.0 provider settings** section on the

Configure identity provider screen (step 6 above). If you're using a custom domain name for the portal, enter the custom URL. Be sure to use this value when you configure the **Assertion consumer service URL** in your portal settings while configuring the SAML 2.0 provider.

For example, if you enter the **Redirect URI** in Azure portal as `https://contoso-portal.powerappsportals.com/signin-saml_1`, you must use it as-is for the SAML 2.0 configuration in portals.

Home > App registrations >

Register an application

* Name

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

Contoso SAML 2.0 ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Default Directory 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)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

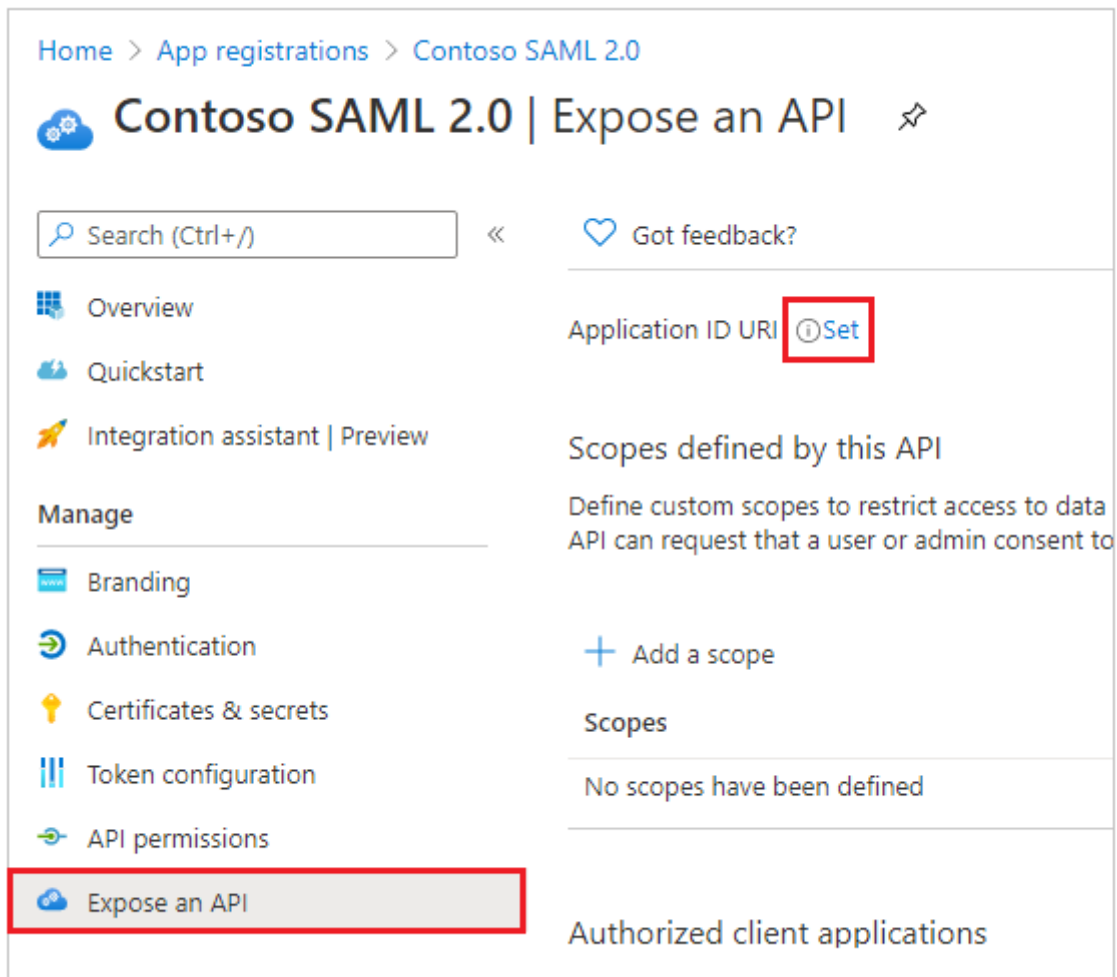
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ✓ `https://contoso-portal.powerappsportals.com/signin-saml_1` ✓

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

Register

- i. Select **Register**.
- j. Select **Expose an API**.
- k. For **Application ID URI**, select **Set**.



l. Enter the portal URL as the **App ID URI**.

The image shows a 'Set the App ID URI' dialog box. It has a title bar at the top. Below the title, there is a label 'Application ID URI' and a text input field containing the URL 'https://contoso-portal.powerappsportals.com'. At the bottom of the dialog, there are two buttons: 'Save' (highlighted in blue) and 'Discard'.

Note

The portal URL might be different if you're using a custom domain name.

m. Select **Save**.

Application ID URI	<input type="text" value="https://contoso-portal.powerappsportals.com"/>	  
--------------------	--	---

n. Keep the Azure portal open, and switch to the SAML 2.0 configuration for Power Apps portals for the next steps.

7. In this step, enter the site settings for the portal configuration.

2. Configure site settings

After creating and configuring the settings for the provider, you must configure the following site settings in your portal to federate with the SAML 2.0 based identity provider. [Learn more](#)

Metadata address * ⓘ

Authentication type * ⓘ

Service provider realm * ⓘ

Assertion consumer service URL * ⓘ

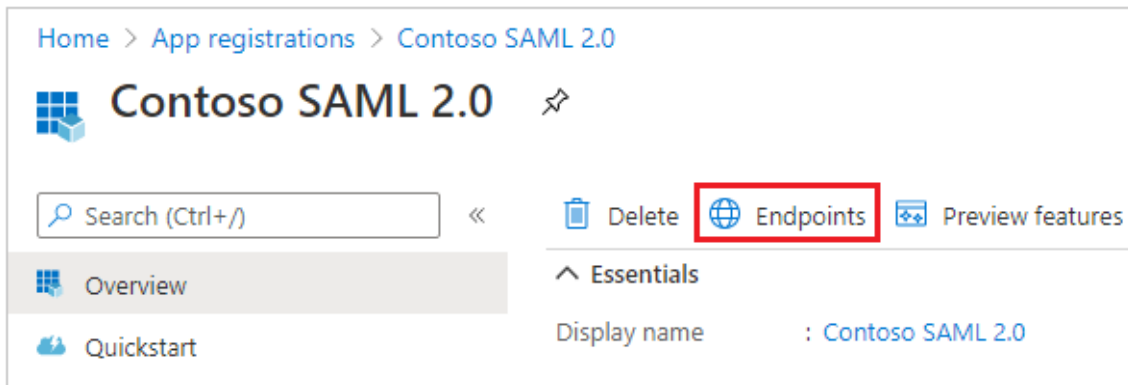
Tip

If you closed the browser window after configuring the app registration in the earlier step, sign in to the Azure portal again and go to the app that you registered.

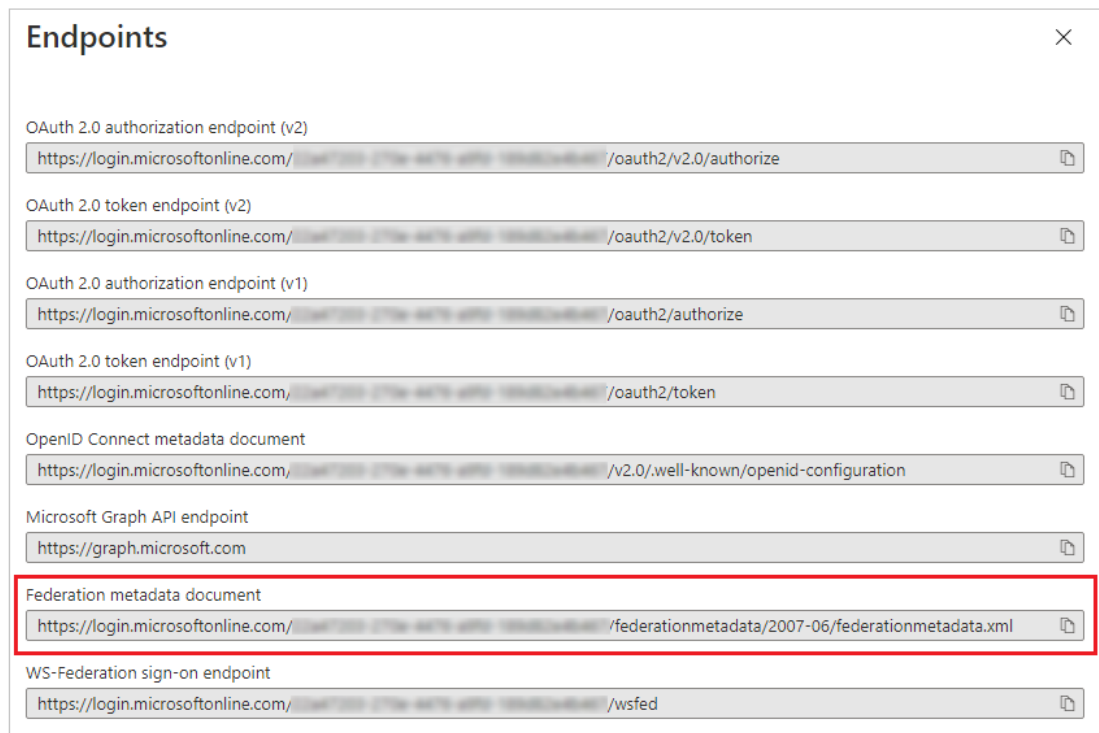
a. **Metadata address:** To configure the metadata address, do the following:

i. Select **Overview** in the Azure portal.

ii. Select **Endpoints**.



i. Copy the URL for **Federation metadata document**.

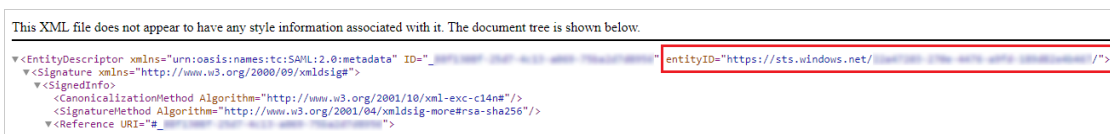


ii. Paste the copied document URL as the **Metadata address** for portals.

b. **Authentication type**: To configure the authentication type, do the following::

i. Copy and paste the **Metadata address** configured earlier in a new browser window.

ii. Copy the value of the **entityID** tag from the URL document.



iii. Paste the copied value of `entityID` as the **Authentication type**.

Example: `https://sts.windows.net/7e6ea6c7-a751-4b0d-bbb0-8cf17fe85dbb/`

c. **Service provider realm:** Enter the portal URL as the service provider realm.

Example: `https://contoso-portal.powerappsportals.com`

ⓘ Note

The portal URL might be different if you're using a custom domain name.

d. **Assertion consumer service URL:** Enter the **Reply URL** for your portal in the **Assertion consumer service URL** text box.

Example: `https://contoso-portal.powerappsportals.com/signin-saml_1`

The screenshot shows the 'Web' configuration page in the Azure portal. Under the 'Redirect URIs' section, there is a text box containing the URL `https://contoso-portal.powerappsportals.com/signin-saml_1`, which is highlighted with a red rectangle. Below this, a red arrow points down to another text box labeled 'Assertion consumer service URL *'. This second text box also contains the same URL `https://contoso-portal.powerappsportals.com/signin-saml_1` and is highlighted with a red rectangle. The interface includes links for 'Quickstart', 'Docs', and 'Add URI'.

ⓘ Note

If you're using the default portal URL, you can copy and paste the **Reply URL** as shown in the **Create and configure SAML 2.0 provider settings** step. If you're using a custom domain name, enter the URL manually. Be sure that the value you enter here is exactly the same as the value you entered as the **Redirect URI** in the Azure portal earlier.

8. Select **Confirm**.

Configure identity provider

✓ Select provider

✓ Configure SAML 2.0 provider

✓ SAML has been successfully configured

Your SAML provider has been successfully configured

Provider name
Contoso SAML 2.0

Site settings
Metadata address
`https://login.microsoftonline.com/[redacted]/federationmetadata/2007-06/federationmetadata.xml`

Authentication type
`https://sts.windows.net/[redacted]/`

Service provider realm
`https://contoso-portal.powerappsportals.com`

Assertion consumer service URL
`https://contoso-portal.powerappsportals.com/signin-saml_1`

> Additional settings

Close

9. Select **Close**.

See also

[Configure a SAML 2.0 provider for portals with AD FS](#)

[FAQ for using SAML 2.0 in portals](#)

[Configure a SAML 2.0 provider for portals](#)

Recommended content

[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.

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.

Azure Single Sign On SAML Protocol - Microsoft identity platform

This article describes the Single Sign-On (SSO) SAML protocol in Azure Active Directory

Debug SAML-based single sign-on - Azure AD

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

Tutorial: Azure AD SSO integration with Azure AD SAML Toolkit

Learn how to configure single sign-on between Azure Active Directory and Azure AD SAML Toolkit.

SAML authentication with Azure Active Directory

Architectural guidance on achieving SAML authentication with Azure Active Directory

Advanced certificate signing options in a SAML token - Azure AD

Learn how to use advanced certificate signing options in the SAML token for pre-integrated apps in Azure Active Directory

Customize app SAML token claims - Microsoft identity platform

Learn how to customize the claims issued by Microsoft identity platform in the SAML token for enterprise applications.

Show more ▾