Troubleshoot SAML-based single sign-on

Article • 11/16/2021 • 4 minutes to read • 4 contributors

In this article

If you encounter a problem when configuring an application. Verify you have followed all the steps in the tutorial for the application. In the application’s configuration, you have inline documentation on how to configure the application. Also, you can access the List of tutorials on how to integrate SaaS apps with Azure Active Directory for a detail step-by-step guidance.

Can’t add another instance of the application

To add a second instance of an application, you need to be able to:

- Configure a unique identifier for the second instance. You won’t be able to configure the same identifier used for the first instance.
- Configure a different certificate than the one used for the first instance.

If the application doesn’t support any of the above. Then, you won’t be able to configure a second instance.

Can’t add the Identifier or the Reply URL

If you’re not able to configure the Identifier or the Reply URL, confirm the Identifier and Reply URL values match the patterns pre-configured for the application.

To know the patterns pre-configured for the application:

1. Open the Azure portal and sign in as a **Global Administrator** or **Co-admin.** Go to step 7. If you are already in the application configuration blade on Azure AD.
2. Open the **Azure Active Directory Extension** by clicking **All services** at the top of the main left-hand navigation menu.
3. Type in "**Azure Active Directory**" in the filter search box and select the **Azure Active Directory** item.
4. click **Enterprise Applications** from the Azure Active Directory left-hand navigation menu.
5. click **All Applications** to view a list of all your applications.

    - If you do not see the application you want show up here, use the **Filter** control at the top of the -**All Applications List** and set the **Show** option to **All Applications.**

6. Select the application you want to configure single sign-on.
7. Once the application loads, click the **Single sign-on** from the application's left-hand navigation menu.
8. Select **SAML-based Sign-on** from the **Mode** dropdown.
9. Go to the **Identifier** or **Reply URL** textbox, under the **Domain and URLs section.**
10. There are three ways to know the supported patterns for the application:

    - In the textbox, you see the supported pattern(s) as a placeholder *Example:* https://contoso.com .
    - if the pattern is not supported, you see a red exclamation mark when you try to enter the value in the textbox. If you hover your mouse over the red exclamation mark, you see the supported patterns.
    - In the tutorial for the application, you can also get information about the supported patterns. Under the **Configure Azure AD single sign-on** section. Go to the step for configured the values under the **Domain and URLs** section.

If the values don't match with the patterns pre-configured on Azure AD. You can:

- Work with the application vendor to get values that match the pattern pre-configured on Azure AD
- Or, you can contact Azure AD team at aadapprequest@microsoft.com or leave a comment in the tutorial to request the update of the supported patterns for the application

Where do I set the EntityID (User Identifier) format

You won't be able to select the EntityID (User Identifier) format that Azure AD sends to the application in the response after user authentication.

Azure AD select the format for the NameID attribute (User Identifier) based on the value selected or the format requested by the application in the SAML AuthRequest. For more information visit the article Single Sign-On SAML protocol under the section NameIDPolicy,

Can't find the Azure AD metadata to complete the configuration with the application

To download the application metadata or certificate from Azure AD, follow these steps:

1. Open the **Azure portal** and sign in as a **Global Administrator** or **Co-admin.**
2. Open the **Azure Active Directory Extension** by clicking **All services** at the top of the main left-hand navigation menu.
3. Type in "**Azure Active Directory**" in the filter search box and select the **Azure Active Directory** item.
4. Select **Enterprise Applications** from the Azure Active Directory left-hand navigation menu.
5. Select **All Applications** to view a list of all your applications.

    - If you do not see the application you want show up here, use the **Filter** control at the top of the **All Applications List** and set the **Show** option to **All Applications.**

6. Select the application you have configured single sign-on.
7. Once the application loads, click the **Single sign-on** from the application's left-hand navigation menu.
8. Go to **SAML Signing Certificate** section, then click **Download** column value. Depending on what the application requires configuring single sign-on, you see either the option to download the Metadata XML or the Certificate.

Azure AD doesn't provide a URL to get the metadata. The metadata can only be retrieved as a XML file.

Customize SAML claims sent to an application

To learn how to customize the SAML attribute claims sent to your application, see Claims mapping in Azure Active Directory for more information.

Next steps

- Quickstart Series on Application Management

Recommended content

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.

Debug SAML-based single sign-on - Azure AD

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

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 Single Sign On SAML Protocol - Microsoft identity platform

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

SAML authentication with Azure Active Directory

Architectural guidance on achieving SAML authentication with 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.

Quickstart: Enable single sign-on for an enterprise application - Azure AD

Enable single sign-on for an enterprise application in Azure Active Directory.

How the Microsoft identity platform uses the SAML protocol

This article provides an overview of the single sign-on and Single Sign-Out SAML profiles in Azure Active Directory.

Show more