

Why choose SDS Manager

How to set up Single Sign-On (SSO) with Microsoft Azure?

1. On the Microsoft Azure Dashboard, select **Enterprise applications**.

Welcome to Azure!

Don't have a subscription? Check out the following options.



Start with an Azure free trial

Get \$200 free credit toward Azure products and services, plus 12 months of popular [free services](#).

[Start](#)



Manage Microsoft Entra ID

Manage access, set smart policies, and enhance security with Microsoft Entra ID.

[View](#)

[Learn more](#)



Azure for Students

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

[Start](#)

Azure services



[Create a resource](#)



Enterprise applications



Quickstart Center



Azure AI Foundry



Kubernetes services



Virtual machines



App Services



Storage accounts



SQL databases



[More services](#)

Resources

[Recent](#)

[Favorite](#)

Name

Type

Last Viewed



No resources have been viewed recently

2. On this page, create your own application by selecting "**Integrate any other application you don't find in the gallery (Non-gallery)**", then enter the name of your application and click **Create**.

Why choose SDS Manager

The screenshot shows the Microsoft Azure portal interface. At the top, the 'Microsoft Azure' header is visible. Below it, the 'Browse Microsoft Entra Gallery' section is active. A red box highlights the '+ Create your own application' link, with a red arrow and the number '1' pointing to it. Below this, there are filters for 'Single Sign-on: All', 'User Account Management: All', and 'Categories: All'. The 'Cloud platforms' section displays logos for Amazon Web Services (AWS), Google Cloud Platform, Oracle, and SAP. A red arrow and the number '2' point to the SAP logo. Below this, the 'On-premises applications' section contains three cards: 'Add an on-premises application', 'Learn about Application Proxy', and 'On-premises application provisioning'. The 'Featured applications' section at the bottom shows logos for Adobe Identity Management (SAML), Atlassian Cloud, AWS Single-Account Access, and Box. On the right side, the 'Create your own application' sidebar is open. It contains a 'Got feedback?' link, a description of the application creation process, and a section titled 'What's the name of your app?' with a dropdown menu showing 'SDS Manager'. Below this, there are radio buttons for 'Configure Application Proxy for secure remote access to an on-premises application', 'Register an application to integrate with Microsoft Entra ID (App you're developing)', and 'Integrate any other application you don't find in the gallery (Non-gallery)'. The 'Integrate any other application you don't find in the gallery (Non-gallery)' option is selected. Below this, there is a section titled 'We found the following applications that may match your entry' with a list of recommended applications: IDID Manager, NetCloud Manager, ProNovos Ops Manager, E Sales Manager Remix, and SPSJProduction Manager. At the bottom of the sidebar, there is a blue 'Create' button, with a red arrow and the number '3' pointing to it.

3. For the Single Sign-On settings, choose **SAML**.

Why choose SDS Manager

Microsoft Azure

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery >

SDS Manager | Overview

Enterprise Application

Overview

- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs
 - Provisioning logs
 - Access reviews
- Troubleshooting + Support

Properties

SM

Name: SDS Manager

Application ID: 7c90373d-e370-429b-93c6-...

Object ID: 3652958a-f476-4d32-8c8d-0...

Getting Started

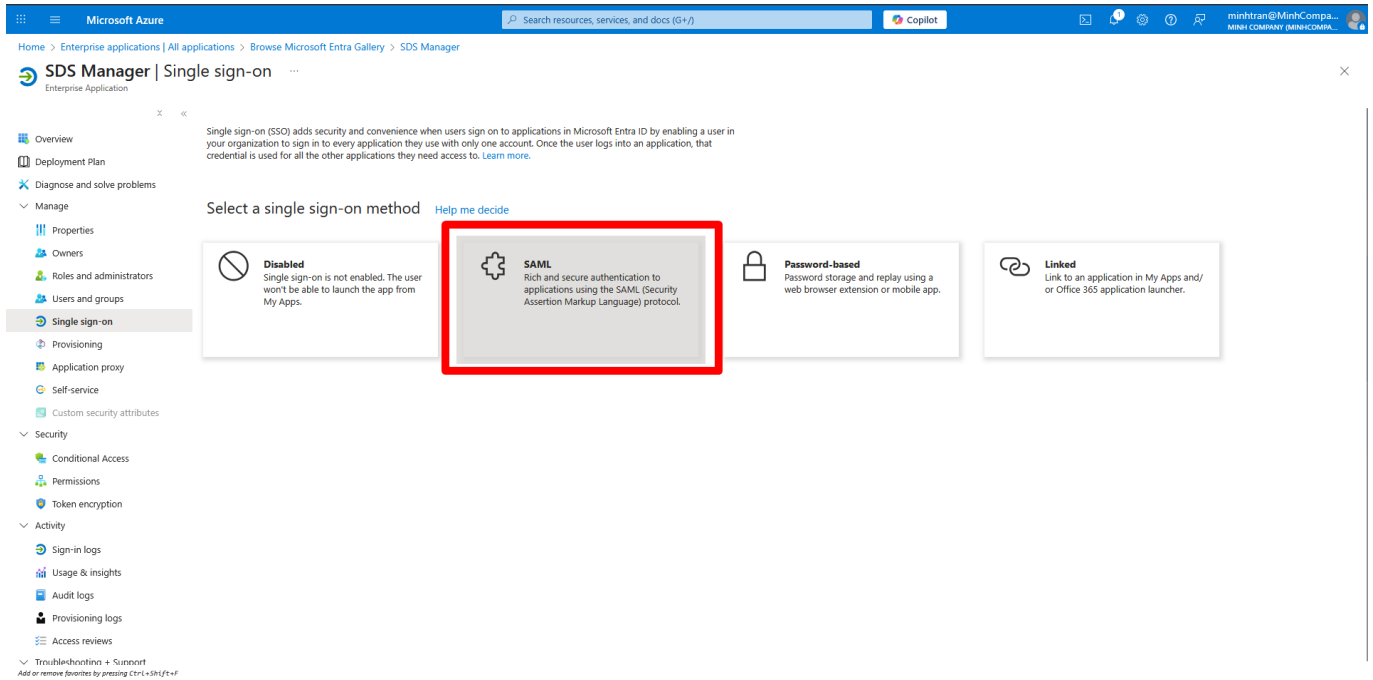
- 1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)
- 2. Set up single sign on**
Enable users to sign into their application using their Microsoft Entra credentials
[Get started](#)
- 5. Self service**
Enable users to request access to the application using their Microsoft Entra credentials
[Get started](#)

What's New

Sign in charts have moved!
The new Insights view shows sign in info along with other useful application data. [View insights](#)

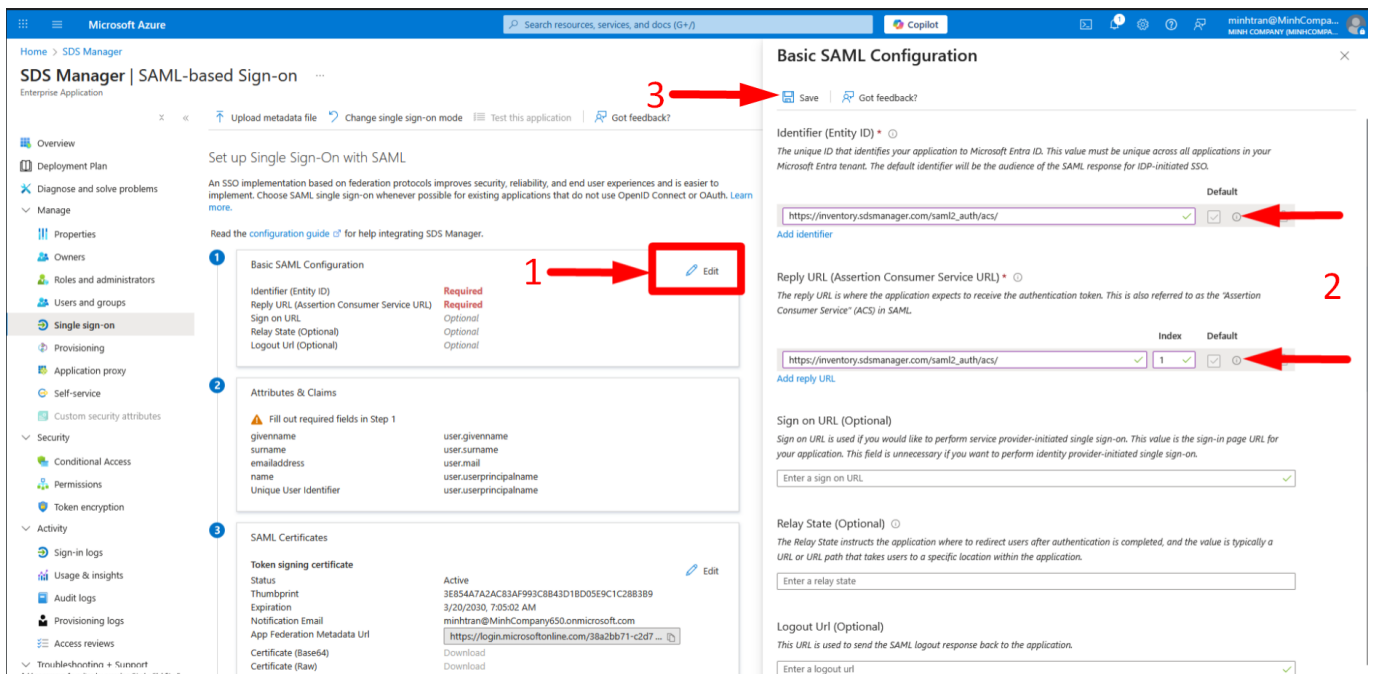
Delete Application has moved to Properties
You can now delete your application from the Properties page. [View properties](#)

Why choose SDS Manager



4. Edit the Basic SAML configuration by entering:

- **Identifier (Entity ID):** https://inventory.sdsmanager.com/saml2_auth/acs/
- **Reply URL (Assertion Consumer Service URL):** https://inventory.sdsmanager.com/saml2_auth/acs/



5. Finally, please provide the SDS Manager Team with the **App Federation Metadata URL** and **Application ID**, so we can complete the setup for you.

Why choose SDS Manager

Microsoft Azure

Home > Enterprise applications | All applications > SDS Manager

SDS Manager | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Troubleshooting + Support

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

https://inventory.sdsmanager.com/saml2_auth/acs/

Add identifier

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

https://inventory.sdsmanager.com/saml2_auth/acs/

Index 1

Add reply URL

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

Logout URL (Optional)

This URL is used to send the SAML logout response back to the application.

Enter a logout url

Attributes & Claims

givenname user.givenname

surname user.surname

emailaddress user.email

name user.name

Unique User Identifier user.principalname

SAML Certificates

Token signing certificate

Status Active

Thumbprint Missing

Expiration 3/20/2030, 7:05:02 AM

Notification Email

App Federation Metadata Url https://login.microsoftonline.com/38a2bb71-c2d7-42ab-be2...

Certificate (Base64) Download

Certificate (Raw) Download

Federation Metadata XML Download

Verification certificates (optional)

Required No

Active 0

Expired 0

Set up SDS Manager

You'll need to configure the application to link with Microsoft Entra ID.

Login URL https://login.microsoftonline.com/38a2bb71-c2d7-42ab-be2...

Microsoft Entra Identifier https://login.microsoftonline.com/38a2bb71-c2d7-42ab-be2...

Logout URL https://login.microsoftonline.com/38a2bb71-c2d7-42ab-be2...

Microsoft Azure

Home > Enterprise applications | All applications > SDS Manager

SDS Manager | Properties

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Troubleshooting + Support

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

If this application resides in your tenant, you can manage additional properties on the [application registration](#).

Enabled for users to sign-in? Yes No

Name * SDS Manager

Homepage URL https://account.activedirectory.windowsazure.com:444/applications/de...

Logo SM

Select a file

User access URL https://launcher.myapps.microsoft.com/api/signin/dc680d0d-e12a-45...

Application ID dc680d0d-e12a-453c-8344-11bb8359e9f4

Object ID 7e08057f-aefa-4459-80d7-f6475b650985

Terms of Service Url Publisher did not provide this information

Privacy Statement Url Publisher did not provide this information

Reply URL https://inventory.sdsmanager.com/saml2_auth/acs/

Assignment required? Yes No

Visible to users? Yes No

Notes

6. After you provide us with the **App Federation Metadata URL** and **Application ID**, SDS Manager will give you a quick-access link to add in this field below. After that, you can log in with a single click whenever you want.

Why choose SDS Manager

Home > Minh Company > Enterprise applications > Enterprise applications | All applications > SDS Manager

SDS Manager | SAML-based Sign-on

Enterprise Application

Overview | Deployment Plan | Diagnose and solve problems | Manage | Properties | Owners | Roles and administrators | Users and groups | **Single sign-on** | Provisioning | Application proxy | Self-service | Custom security attributes | Security | Conditional Access | Permissions | Token encryption | Activity | Sign-in logs | Usage & insights | Audit logs | Provisioning logs | Access reviews | Troubleshoot and support

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Read the [configuration guide](#) for help integrating SDS Manager.

1 Basic SAML Configuration

Identifier (Entity ID) [https://inventory.sdsmanager.com/saml2_auth/acs/](#) [Edit](#)

Reply URL (Assertion Consumer Service URL) [https://inventory.sdsmanager.com/saml2_auth/acs/](#)

Sign on URL (Optional) [Optional](#)

Relay State (Optional) [Optional](#)

Logout URL (Optional) [Optional](#)

2 Attributes & Claims

Attribute	Claim
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate	Status	Active
Thumbprint	FC464524669356F8C5272922A41F84771F2EBDA	
Expiration	8/28/2028, 2:24:23 PM	
Notification email	Missing	
App Federation Metadata URL	https://login.microsoftonline.com/38a2bb71-c2d7-...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Verification certificates (optional)

Required	Active	Expired
No	0	0

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) * [Add identifier](#)

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

[https://inventory.sdsmanager.com/saml2_auth/acs/](#) ☒ [Add identifier](#)

Reply URL (Assertion Consumer Service URL) * [Add reply URL](#)

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://inventory.sdsmanager.com/saml2_auth/acs/	1	<input checked="" type="checkbox"/>

[Add reply URL](#)

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

☒

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout URL (Optional)

This URL is used to send the SAML logout response back to the application.

☒

Then you can access it via <https://myapps.microsoft.com>.

Unique solution ID: #4846

Author: n/a

Last update: 2025-08-29 05:56