

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

Microsoft Azure

Home > Enterprise applications | All applications >

Browse Microsoft Entra Gallery

+ Create your own application

Search application

Single Sign-on: All User Account Management: All Categories: All

Cloud platforms

- Amazon Web Services (AWS)
- Google Cloud Platform
- Oracle
- SAP

On-premises applications

- Add an on-premises application
- Learn about Application Proxy
- On-premises application provisioning

Featured applications

- Adobe Identity Management (SAML)
- Atlassian Cloud
- AWS Single-Account Access
- Box

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?
SDS Manager

What are you looking to do with your application?

- 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)
- Integrate any other application you don't find in the gallery (Non-gallery)

We found the following applications that may match your entry
We recommend using gallery applications when possible.

- IDID Manager
- NetCloud Manager
- ProNovos Ops Manager
- E Sales Manager Remix
- SPS SPSJProduction Manager

Create

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

Why choose SDS Manager

portal.azure.com/#view/Microsoft_AAD_IAM/ManagedAppMenuBlade/~./Overview/appld/7c90373d-e370-4

Microsoft Azure Search resources, services, and docs (G+)

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](#)

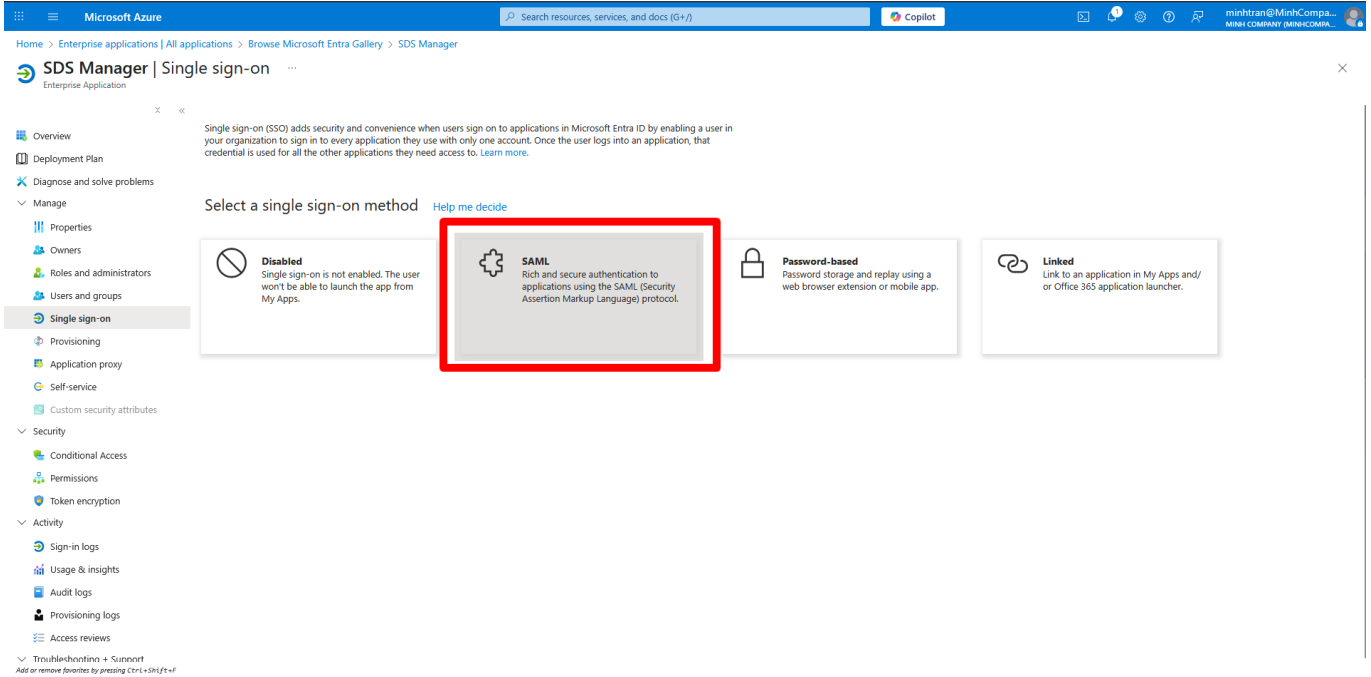
What's New

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](#)

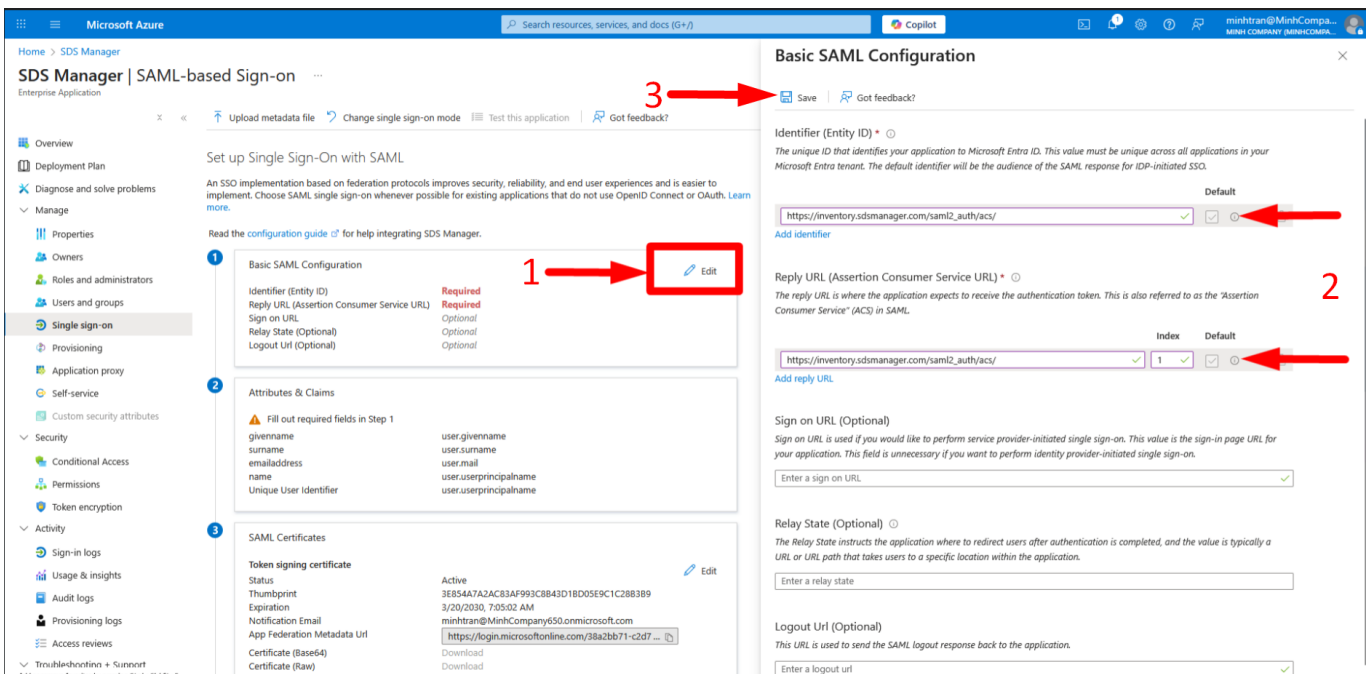
portal.azure.com/#view/Microsoft_AAD_IAM/ManagedAppMenuBlade/~./SignOn/appld/7c90373d-e370-429b-93c6-956dc3f1bfe2/objectId/3652958a-f476-4d32-8c8d-0219e3cf92bb

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 | Search resources, services, and docs (G+)

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

Identifier (Entity ID) *

Reply URL (Assertion Consumer Service URL) *

Sign on URL (Optional)

Relay State (Optional)

Logout URL (Optional)

Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	
name	
Unique User Identifier	user.userprincipalname

SAML Certificates

Token signing certificate	Status	Expiration	Thumbprint
Microsoft	Active	3/20/2030, 7:05:02 AM	Microsoft

Verification certificates (optional)

Required	Active	Expired
No	0	0

Set up SDS Manager

Login URL:

Microsoft Entra Identifier:

Logout URL:

Microsoft Azure | Search resources, services, and docs (G+)

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 *

Homepage URL

Logo

User access URL

Application ID

Object ID

Terms of Service URL

Privacy Statement URL

Reply URL

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

Single Sign-On (SSO)

Single Sign-on Configuration for SDS Manager

Help

Federation metadata document*

Application (client) ID*

Email attribute mapping*

name

SSO attribute name that maps to the user email (e.g., "emailAddress", "email", etc.)

SSO Login URL

Enable for users

Save Configuration

Test

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 sign-in + Support

Add or remove favorites by pressing Ctrl+1+Sh+1-F+7

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		Edit
Identifier (Entity ID)	https://inventory.sdsmanager.com/saml2_auth/acs/	
Reply URL (Assertion Consumer Service URL)	https://inventory.sdsmanager.com/saml2_auth/acs/	
Sign on URL	Optional	
Relay State (Optional)	Optional	
Logout URL (Optional)	Optional	

2 Attributes & Claims		Edit
givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	

3 SAML Certificates		Edit
Token signing certificate		
Status	Active	
Thumbprint	FC464524669356F8C527292A41F84771F2EBDA	
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)		Edit
Required	No	
Active	0	
Expired	0	

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/

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/

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

7. Define the roles (App registrations, not Enterprise Applications)

Azure Portal → Azure Active Directory → App registrations → SDS Manager → App roles

Go to **App registrations** and create the custom roles:

1. **Azure Portal → Azure Active Directory → App registrations**
2. Search for and select **SDS Manager**
3. In the left menu → **App roles**

Why choose SDS Manager

4. Click **Create app role** and add roles matching your SDS Manager roles, for example:

- Display name: Admin | Value: Admin
- Display name: Staff | Value: Staff
- Display name: Read Only | Value: ReadOnly
- Display name: Admin Light | Value: AdminLight
- (The **Value** field is what gets sent in the SAML assertion — it must match the role names in SDS Manager exactly, case-insensitive)

5. Save each role

Microsoft Azure portal screenshot showing the 'App roles' configuration page. The page displays a table of app roles with columns for Display name, Description, Allowed member types, Value, ID, and State. The roles listed are:

Display name	Description	Allowed member types	Value	ID	State
AdminLight	AdminLight	Users/Groups	AdminLight	89d0c472-ad1d-4b25-...	Enabled
User	User	Users/Groups		18d14569-c3bd-439b-...	Enabled
msiam_access	msiam_access	Users/Groups		b9632174-c057-4f7e-...	Enabled
Admin	Admin	Users/Groups	Admin	7afb82d2-5970-4c7c-a...	Enabled

8. Assign users to those roles

Enterprise Applications → SDS Manager → Users and groups

After roles are defined in App registrations, go back to Enterprise Applications → Users and groups → assign individual users or groups to the appropriate app role.

Why choose SDS Manager

Home > Enterprise applications | All applications > SDS Manager | Users and groups

Add Assignment ...

Minh Company

 Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

1 user selected.

Select a role *

AdminLight

Assign

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

Why choose SDS Manager

Unique solution ID: #4846

Last update: 2026-06-18 11:09