

## Contents

Introduction	1
Configuring an Enterprise Application for SAML SSO	1
Service Provider Configuration	8
SP-Initiated SSO	8
IdP-Initiated SSO	10
SAML Logout	11
Multitenant Support	12
Troubleshooting	13

## Introduction

This document describes integration with Microsoft Entra ID (previously known as Azure Active Directory) as the identity provider.

For information on configuring Microsoft Entra ID for SAML SSO, refer to the following article.

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-applicationportal-setup-sso

## Configuring an Enterprise Application for SAML SSO

Login to Microsoft Entra as an administrator.

https://entra.microsoft.com

It's also possible to access the configuration through Azure.

#### https://portal.azure.com

Navigate to enterprise applications for Microsoft Entra.



Add a non-gallery application. The application name is for display purposes only.

<ul> <li>Contraction application - 11 S +</li> <li>C S poted appreciately/black/Material</li> </ul>	nih AAD 10M StarffoordApplication/Merchlade/AlAppl/merch/	* 0 0 C D # 0
= Microsoft Azure P Inischando	crim, services, and does (Dv))	D G 0 0 7 G gaangtonponentipet.
Control of the second sec	ann I gallwy agu 🛛 🛇 Got feedlaad. Hens Chit leer la satisficiant to the legary tare galwy regenerates. + (Single Sign-ont: All) (Sine Account Management: All (Easignine: All)	Create your own application     White the intervel of your applit     Compare Application (     Compare Application (     Compare Application (     Page intervel)     Page intervel     Pa
Amazon Web Services (AWS)	Geogle Cloud Plattom	Orack
On-premises applications		
Add an on-promises application Onlyget Apple Ad Autocold Prog. Is created access	Learn about Application Proxy Dearther to as Application Proxy to provide access while acc to your or primer application.	
Contegen Active AC Againcades Proce to metters Moni-	autat entole barrine tradi Appliatori Pole to provide autar vende auta te yeer en presiet applicatore.	

### Assign users access to the application.

A banglebeneghtstade Man	* +			- 0 =
← = ○ ■ potelance	carry/Hala/Microsoft, AAD_000/MenugedAppMicroBla	n/Usim/applit/24020091 the 4285-atta5 salit1215att65sApen	0/07/0001dd4-456-629/3/06d5ac. 👲 🛛	0 0 G D A 🚺 I
= Microsoft Azure	P learn mourie, where and the file)		E & 🖉 Ø 7 G	gavat@componentipec.
Herei I componentquar 3.E	nterprise spyktations 1. Diserplicitary/veProvider			
ExampleServic Enterior formation	eProvider   Users and groups			×
Conview	<ul> <li>Add overgroup: p<sup>2</sup> bit:    herear</li> <li>The application will access to external access</li> </ul>	P. Lipsker Controller:   → Column:   ♥, 641 Healback?     Address: See Solida Support: I to an acception to accept the		
Capiciyeant Plan	and the second statement of the second se			
Marage	Fort 50 shows to shares at ones it proops, we	int a shajibiy darme		
III. Properties	Display Marva	Object Type	Role accipted	
28 Ownets	🗋 🙆 Jak Dae	Lite-	User .	
🌲 Rober and administration (Pre-	TRM)			
3 Units and groups				
Singh sign on				
Introvisionerg				
<ul> <li>Applement provy</li> </ul>				
C fait envior				
Security				
Southtonal Actes				
A Accesso				
Q Toter encyption				
Activity				
3 Syrin				
a Unige & regets				
Audit logs				
🛓 Proxisioning keps (Preview)				
21. Actual indexe				

Select SAML as the single sign-on method.

= Microsoft Azure 💷	methomologies, while an and data (Gay)		🔲 🖸 🗗 🖉 🎯 🤉 🕲 davageoutop
ExampleServicePro     Extended AppleServicePro     Extended AppleService	vider   Single sign-on = Select a single sign-on method we	is me decide	
Cosplayment Plan     Munage     Monopellies     Adverant     Redve and adversariation (Preview)	Shabled Bright sign for the cost or stablest. The user work has able to isometrities app from My Appro	SAML Birth and musick and heritration to supplications using the SAM (Security Assertion Markop Language) permitted	Parmanet isospe and replay unity a met browne estimates to recible equ.
Contrart groups     Single segment     Providence     Application prove     Suff service	Link to an application in My dags, angler Office 368 application taxestee		
Cookierent Anzen  Annen   Permanen  Teler encyclor  Activity  Sign on  Activity  Appl Congres  Appl Ogn  Appl Ogn  Percenter			

Configure single sign-on.

The identifier is the SAML entity ID. This name must match with the local service provider name. For example, if the LocalServiceProviderConfiguration's Name is https://ExampleServiceProvider, then the identifier must be set to the same value.

The reply URL is the assertion consumer service URL (e.g. https://localhost:44360/SAML/AssertionConsumerService).

The logout URL is the logout service URL (e.g. https://localhost:44360/SAML/SingleLogoutService).

The optional Sign On URL isn't used. It's for those scenarios where the service provider doesn't support IdP-initiated SSO. Microsoft Entra will redirect to this URL and then expect the SP to initiate SSO back to Microsoft Entra (i.e. SP-initiated SSO). It's not part of the actual SSO flow or SAML specification but rather a workaround for when IdP-initiated SSO isn't supported.

The optional relay state isn't used.

<ul> <li>A basi SWI Configuration Mar. 2</li> <li>← → C ■ pottel appreciate///</li> </ul>	+ hhite	nnih AAD WAAMmigrid-EpitAinalhain Gig	-Deviet	nicoscolas via 400 eno solucitado especialmente site em sou centra 🖇		G D A O I
= Microsoft Azure 🔑	learn and	ution, larvision, and chics (Div))		E E Ø Ø ?	G genni	Componentipet
ExampleServiceProvid	er   SA	ML-based Sign-on		Basic SAML Configuration		×
Overview     Copicyment Pan     Manaze	Secu	e Single Sign-On with SAML		indentifies (Entity (D) * (i)). The styles of the SOR sequence for DF-robust SO The styles $10^{40}$ -robust SO	Default	
If Properties Ja Corrent A Corrent A Corrent D Corrent and prope D Single sign ont D Single sign ont D Single sign ont D Single sign ont	0	Recently a data gade of the sets of equilating to Bases (AML Configuration Mapping IRL Valancian Concurrent Service URL) Sign on URL Solay States Loggist URL	Rage Rage Option Option Option	Prepay, Unsumpled environment     Prepay, URL, IAssertion Consumer Service URL) *      The default rapid URL will be the destination in the SAPK regions for XPP-Indianal 500	Ortan	
Application provy     Aufinewide Security     Costitional Access     Aneneouses	0	Maer Attributes & Claims givername warnere erzabadiwen ratem Unigan Maer Handike	orang orang urang urang urang urang	Tetapi //scathari 24390/52240_20asetionConsumediterrian		
View encyclan	0	SAMAL Exporting Certificate Datus Thumbarine Thumbarine Notification Invest App Federation Metadata Uni Certificate Statistics Certificate Statistics Certificate Statistics Texter Statist Statist	Active BCDA S22A S221 S221 S221 Down Down Down Down	Relay State		Di 2

Alternatively, rather than entering these values manually, the service provider SAML metadata file may be uploaded.

sighterestion was a	+				- 0 ×
C # portelabrecom	(9934ada/Mcc	mork_AAD_000/MenugedAppManaBl	en/SignOvropenU24d0045 Viai-400-eN/0 SSU(1)16d5U/oSpecial-00	minista salas entre actili definida 🛛 🕸	U Q C D A 💮 :
Microsoft Azure	0 Jeschimo	ories, whiles, and data (Dv))		🛾 🖬 🖉 🖉 🖉 🤤	gavan@compenientspac.
· F componentiques > Entery	prise spipkcari	ion 1 DampietarykeProvider (*			
mpleServiceProvi	ider   SA	ML-based Sign-on			×
	* Ť.V	ipload restadato file 🍏 Change singh	oge en mode 🛛 lied the application 👘 🗢 fait herdlank?		
and the second second second	Uplo	ad metadata file.			
10	Values Examp	For the fields below are provided by E ActionsicsProvider.	rangleServiceProvider. You may either enter those values manually, or up	tood a pre-configured SAML metadota Ne	a provided by
operses	500	t willing			
harmelt:		M Nesser			
dae and administration (Preview)		Contraction of the second seco			
encod groups		Signari UR:	Optional		
ngla sign an		Logovi Uri	Optimiz		
ro-islaneng					
pplcation pravy	0	Unor Attributes & Chima	1 Mar.		
e#-service		(Description)	2 10		
ay.		iumane.	presidente.		
additional Activity		ratman Takman	new mechanism preparate new const		
Accession of the local data and the		Unigon User Herdifier	user user providelineme		
den encyption -	0	TAMI Dropper Carribule	1		
9	142	must reduced relevants	Ø ne		
ign im		DArus Thumbprint	Active 9CIATIONEACESCITYEADISI20885782510019CA8C48		
lage & raghts		Experiences Not Excitory investig	12/21/2025 ± 90.17 AM		
udit logs		App Federation Metadata-Uni	inter Avenue account of a supplication of the state		
routstanding logs (Prenimul)		Certificate (Searf-E) Certificate (Search	Down Assail		
jamai undered		Pederation Metadata XML	Descrimant		
innaang iken wergeline b genes sege 8: regelin ofd logs ondaateg logs (Presewe canadateg logs (Presewe canadateg	0	Unique Une Herbite SAML Eigenry Constraine Dense Teorhysies Sagendon Age Teorison Metabara Uni Confliction Innel Conflicted Service Teorison Metabara Uni Conflicted Service Teorison Metabara Uni	san uanprengalagea Active Acti		

User attributes and claims may be edited. These map user properties in Microsoft Entra to the SAML subject name identifier (Name ID) and SAML attributes sent in the SAML assertion as required by the service provider.

C • postal anex care/Vitabil/Momenty/Add/UMM/munghd-postal-sides diap/Dr/paped/24420004/164-400-4601/36000000464/3684-406-4201/200400. *********************************	A the Attributes & Classer Water & 🕈				- 0 ×
Microsoft Adam         Discontinuous environmentation (Liver Control (Live Control (Live Control (Liver Control (Live Control (Liver Contro	← → O a portal apreciary/Hilds/Mcmuth.240_00MMenup	dAppManallanis/SignOn/opp10/24d20045	Viei 420-eND 55011116-5	Minigensi comulati sala Ane acti comuni 👲 🛛	0 0 C b # 📵 i
Intervel       Composition of poly billing in a good billing i	= Microsoft Abuse P Institutions and an and the s	R-vit		E 6 0 7 6	gavin@componentspac
User Attributes & Claims - ///////////////////////////////////	Home I componentquase ) Entergence applications ( DeeppleCarvivePo	router > SAML based Sign-ret > .		25	
+ bill a group dam, == Colorers         Required dam         Cains new       Wale         Voige Unit der Merriller Name Di       wan sergenreipationer (varient fire, ***         Additional dams       ***         Cars neine       Wale         Improve frams zerinder op weg 196/2005/00/ der Hyrd armsmaladowa       wan mail         Improve frams zerinder op weg 196/2005/00/ identify damsmaladowa       wan mail         Improve frams zerinder op weg 196/2005/00/ identify damsmaladowa       wan mail         Improve frams zerinder op weg 196/2005/00/ identify damsmaladowa       wan mail         Improve frams zerinder op weg 196/2005/00/ identify damsmaladowa       wan zerinder mail	User Attributes & Claims -				×
P All res claim + All sprop claim + Column         Required claim         Claim name       Wake         Unique User Merriller IName (D)       can surgemorphatisere (name) (name)         Claim name       Wake         Commande       wake         Required claims       can surgemorphatisere (name) (name)         Commande       wate mail         Required claims       can mail         Requ					
Nagainal dam       Olars new     Male       Unique Uner Kerner Dit     une surgrenzipationen (narinal fer.)       Additional damm.     ***       Additional damm.     ***       Ener new     Male       Intra // Othernal.com/org/ny/2005/00/Interty/clains/semalables     une mail	+ sequencies + engalishingen en Contain				
Oaks new     Make       Unique Uner Starten ED     Lawin seergrinzejabliseer (navisal fer, 1+4)       Additional claims     Make       Ener nem     Make       Intra / Octomatic sering on grav/2005/SU/Linetity (name dia line)     1+4       Intra / Octomatic sering on grav/2005/SU/Linetity (name dia line)     1+4       Intra / Octomatic sering on grav/2005/SU/Linetity (name dia line)     1+4	Required claim				
Livigue Uner Henr Bit Lann Lann Lann Lann Lann Lann Lann Lan	Claim name	Value			
Additional claims Class state Note http://tchanal.unitog.org/w/2005/0/likenity/claims/gvemante claim.greensate end http://tchanal.unitog.org/w/2005/0/likenity/claims/gvemante end http://tchanal.unitog.org/w/2005/0/likenity	Unique User Ident (Cer Thanse (C)	uan unryrinclashame barraid for.			
Clear name         Wake           http://clearac.unit/op.org/w0/2005/00/ldenthy/damo/pomental         user.mal         ***           http://clearac.unit/op.org/w0/2005/00/ldenthy/damo/pomental         user.mal         ***           http://clearac.unit/op.org/w0/2005/00/ldenthy/damo/pomental         user.genergan/gatemet         ***	Additional claims				
http://chanal.unito.go.org/ww/2005/00/labelty/damo/manalables     uwer.mail     ***       intg://uhamal.unito.go.org/ww/2005/00/labelty/damo/govername     user_gregoration     ***       http://uhamal.unito.go.org/ww/2005/00/labelty/damo/govername     user_gregoration     ***	Claim name	Vabae			
Intgr/whenal.militag.org/w/2011/01/Wenhyldens/givemane (and givemane *** http://whenal.militag.org/w/2011/01/Wenhyldens/wane /***	http://ctienar.amb/op.org/wc2005/06/denthy/diams/enaladdiese	upst mail	- +++		
http://demai.amitoap.org/wo/3653R/dentsyvtaine/mane ase-aregimicgalitane ***	intpl//whenel.enlicep.org/w/2003/05/illentity/clanic/givernane	Lost give marke	444		
	http://schemal.amiloap.org/wo2005416/identity/daine/name	uar unrgrocquitane			
Hetps/schemaumisospotg/wv2505/00/demby/size-schemamen user sumares ***	Http://schemas.vellulap.org/wv/2005/05/identity/slams/scuments	Unit Jurname	101		

The SAML signing certificate is used by Microsoft Entra to sign SAML messages. If required, this certificate and the signature options may be changed.

A SAVE Signing Cartillater - Maxima	+		110000000000000000000000000000000000000			-	0 ×
Microsoft Apure	marth and	nort, AAO, WAN, Vanaged App Marsallatis, Sign Divis accom, annois, and data (Gv)	gril/2422893-1181-	00-410 SSUU	Ind/Milesperiol/10	E G O O 7 C dweigenzeur	ntapat
ExampleServiceProvid	er   S/	ann I Dampiclanskafnorder I MML-based Sign-on	SAML Signing Certificate Warage the certificate was the lase to lase the lase at the same age			and to your date	×
Constant Pan		eranlachtete sam rame ann Unige Uan throthe sam	Actue	4/5/2014	11.42.42 AM	8980448982910404290429113379473019047310	100
Marage III: Ropedie; 30: Ourse: 41: Robe and administration (Period) 42: Units and groups 43: Single services	0	SAML Eigening Certificate Datus Aday Thandigene BCA Exploration Work Antification (Ipeal Antification (Ipeal Angi Federation Metadate Liff Itt	Signing Cation Signing Algorithm Notification Dro geomitication	ell Ackdommen entrype a strete consel	Tign SAMLand SHA-258	4f2m	× ×
Application provy     Security     Conditional Access     Anonexame	0	Cetholis Souri-S Dive Cetholis Sovi Dive Hubridson Mendalo (M. Dive Set up Example Service/Provider Yea/II ward to certigere the application to link with A Login (IR. International Cetholis Section 1997) Accessed Divertifier Inter					
Q     Internet system       Activity     Internet system       Internet system     Internet system       Internet system     Internet system       Internet system     Internet system	0	Legan LIPE. In Wee cap by any numerican. Test single sign on with Example ServicitYovicer Test to see if segin upp are in our leng. Open all real					
Processing says investor     Access investor							

Information is displayed that's required for configuring the service provider application.

The login URL is the PartnerIdentityProviderConfiguration's SingleSignOnServiceUrl.

The Microsoft Entra identifier is the PartnerldentityProviderConfiguration's Name.

The logout URL is the PartnerIdentityProviderConfiguration's SingleLogoutServiceUrl.

Alternatively, the Microsoft Entra federation metadata XML may be downloaded and imported into the service provider's SAML configuration.



Once the Microsoft Entra configuration and the service provider's SAML configuration are complete, SSO may be tested.

Microsoft Azure	eixth ins	second reactions, and check (D-v))	-	D 0 0 1 0 annacontourbe
normi il complementiquice il Erengenia	n nçişiki at	tone   DeempletterviceProvider		Test single sign-on with ExampleServiceProvider
ExampleServiceProvide	±r \$/	ML-based Sign-on		
. U Overview	Ť	aload netadata file 🈏 Orange angie sign on mod zmaładzbetz	*	Minimut incomments including the by Ages Secure Tape to laterate the accounts were capture and residues galaxies. Make survivor allow Hild party contains if you have extended it fair this remains will done up.
Capitywert Plan		nater and Unique Une StericTer alle	-	n Meann main nan yns haan soedigannel Laaropelsen (arfiniske betoe betoe betoe
C hoordes	0	SAML Report Certificate		Eign in an connect case
Owners		tuna Adv	244	Sign in an our leave also detailes frontes estention
Rober and administration (Preview)		Thankarint IKS Exploration IKS	14	
Cent and groups		Notification Enall gas	in i	executing errors If you exclusive an error to be sign or page, please patter theiran. If you still we the same time, please wait his maple of minutes and
Sign sign of		DetFute Sami-C		why and a second s
fro-isoreng		Destificate Revit Down Twiteradow Menudatis XML Durye	N/I	and day be with a solution of
Appleation prov		Set up Example ServiceProvider	1	Report in Wind St Private and Constitution Constances in Section 401 and and a sector research in
<ul> <li>Set environ</li> </ul>	0		5 Set up ExampleServiceProvider	
Conditional Activity		Yeal II reard to configure the application to low with	to be with A	fair multiple publics
Parentare		Again AD Ment Tar	1.0	
Tolumencyption		Lingsont LPEL THE	é.	
away.		some unit på med konsergente		
Sgrim	-			
Usage & regits	0	Test single sign on with ExampleServiceProvider	θ.	
Audit logs		This to all if sight sign on it norting. Users all re-		
Provisioning keps (Preview)		Test		

## Service Provider Configuration

The following partner identity provider configuration is included in the example service provider's SAML configuration.

```
{
    "Name": "https://sts.windows.net/f2f933ec-d7c9-433f-8926-d3a0732a7dcf/",
    "Description": "Entra ID (Azure AD)",
    "SingleSignOnServiceUrl": "https://login.microsoftonline.com/f2f933ec-d7c9-433f-8926-d3a0732a7dcf/saml2",
    "SingleLogoutServiceUrl": "https://login.microsoftonline.com/f2f933ec-d7c9-433f-8926-d3a0732a7dcf/saml2",
    "PartnerCertificates": [
    {
        "FileName": "certificates/azure.cer"
     }
    ]
}
```

This information is available as part of the enterprise application single sign-on configuration in Microsoft Entra.

The partner certificate is the SAML signing certificate downloaded from Microsoft Entra. We recommend downloading the base-64 encoded certificate.

Ensure the PartnerName specifies the correct partner identity provider.

```
"PartnerName": "https://sts.windows.net/f2f933ec-d7c9-433f-8926-d3a0732a7dcf/"
```

## **SP-Initiated SSO**

Browse to the example service provider.



Click the button to SSO to the identity provider.

Login to Microsoft Entra as a user assigned to the application.

Superior to allow account 8 +		- 0 ×
<ul> <li>September answer</li> <li>C Aussian Sector</li> <li>C Aussian Sector</li></ul>	Ald Carrier (1974) And Carrier	- 0 K
	Next           Q <sub>2</sub> Sign-in options	are Phone & Locotter

The user is automatically logged in at the service provider.



## **IdP-Initiated SSO**

Browse to https://myapps.microsoft.com and login.

Alternatively, browse to the URL specified in the application properties for direct access to the application.

Select the ExampleServiceProvider application.



The user is automatically logged in at the service provider.



## SAML Logout

Microsoft Entra supports both SP-initiated and IdP-initiated SAML logout.

## **Multitenant Support**

The previous sections describe SAML SSO to Entra ID in a single tenant deployment.

Entra ID also supports SSO from any Microsoft Entra tenant by converting a single tenant application to multitenant. For more information, refer to:

https://learn.microsoft.com/en-us/entra/identity-platform/howto-convert-app-to-be-multitenant

Entra ID publishes both tenant specific and tenant independent SAML metadata.

https://learn.microsoft.com/en-us/entra/identity-platform/federation-metadata

The following partner identity provider configuration is included in the example service provider's SAML configuration.

The name is a regular expression that matches any Entra tenant. This is required as Entra ID sets the issuer field to that of the tenant where the user is authenticated and this isn't necessarily known at configuration time.

The first certificate is from the single tenant's SAML metadata. The other certificates are from the tenant independent SAML metadata. SAML messages originating from the tenant where the application is deployed will be signed with a tenant specific certificate. SAML messages from any other tenant will be signed with a tenant independent certificate.

```
"Name": "https://sts.windows.net/",
"Description": "Entra ID (Azure AD) multitenant",
"SingleSignOnServiceUrl": "https://login.microsoftonline.com/common/saml2",
"SingleLogoutServiceUrl": "https://login.microsoftonline.com/common/saml2",
"PartnerCertificates": [
 {
  "FileName": "certificates/azure.cer"
 },
 {
  "FileName": "certificates/azure-common-1.cer"
 },
 {
  "FileName": "certificates/azure-common-2.cer"
 },
 {
  "FileName": "certificates/azure-common-3.cer"
 },
 {
  "FileName": "certificates/azure-common-4.cer"
 }
]
}
```

To support matching SAML message issuer fields against the PartnerIdentityProviderConfiguration.Name pattern, regular expression support must be enabled. This should be done at application start-up.

using ComponentSpace.Saml2.Configuration.Resolver;

// Support matching SAML message issuer fields against regular expression patterns. builder.Services.AddTransient<ISamlConfigurationNameResolver, RegexSamlConfigurationNameResolver>();

## Troubleshooting

Most issues result from configuration mismatches. Ensure that the Microsoft Entra configuration and the service provider configuration are consistent with each other.