# || Parallels<sup>®</sup>

# Using Microsoft Entra ID / Azure as an external Identity Provider (IdP) for Parallels Secure Workspace

• Parallels Secure Workspace

# Resolution

To successfully use Microsoft Azure as an external Identity Provider (IdP) for Parallels Secure Workspace, it's important that the **username claim** returns the **user principal name (UPN)** in the LDAP environment, which is most commonly an Active Directory (AD).

## **Configuring Parallels Secure Workspace: host headers**

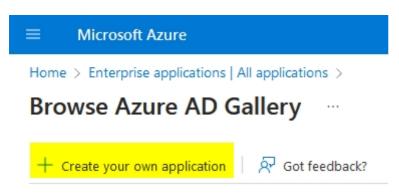
This needs to be configured per Workspace domain.

First, go to **System Settings > Global > Domains**. Select the Workspace domain for which this authentication flow will be configured. Validate what is specified for **host headers**. It should contain the host header that will be used to access the Parallels Secure Workspace environment. In this guide, this will be workspace.somedomain.org .

Microsoft Azure will only allow URLs using https; so make sure there is an SSL certificate configured in Parallels Secure Workspace for this Workspace domain.

# **Creating Azure Enterprise Application**

Log in to <u>portal.azure.com</u> and locate **Enterprise Applications**. Click [ + Create your own application ].



Give the application a name of your choice. Leave the radio button set to "Integrate any other application you don't find in the gallery (Non-gallery)".

# 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?

Awingu-Guide-Custom-Username-Claim

What are you looking to do with your application?

- O Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

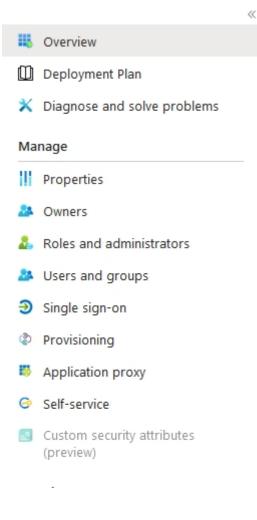
Confirm by pressing [Create].

After a bit, the properties of the Enterprise Application should be shown. In the left navigation menu, choose **Single sign-on**.

Home > Enterprise applications | All applications > Browse Azure AD Gallery >

# Guide-Custom-Username-Claim | Overview

Enterprise Application



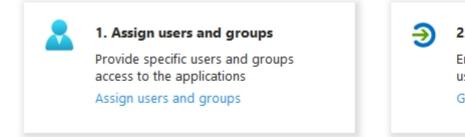
Choose SAML:

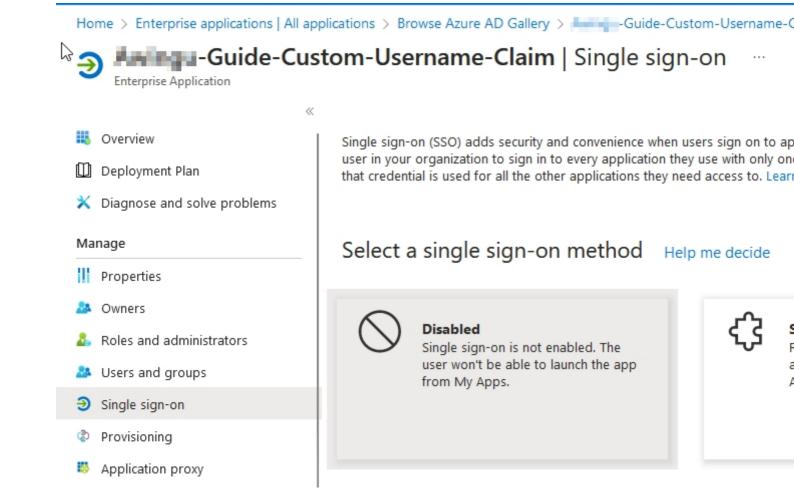
## Properties

AW

/	Name (i)
	-Guide-Custom-Use 🗈
	Application ID (i)
	Alainin alaini alaini alaini 🖉
	Object ID

## **Getting Started**

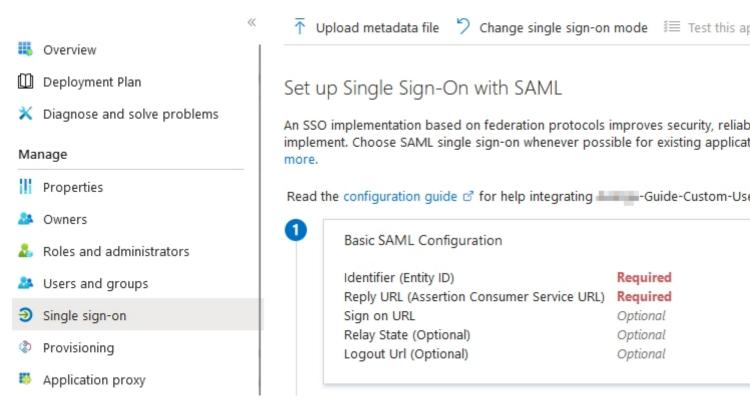




This will need to be completed step by step. In the **Basic SAML Configuration**, click on **Edit**.

# -Guide-Custom-Username-Claim | SAML-based Sign-on

Enterprise Application



## **Basic SAML Configuration**

- Identifier (Entity ID): This identifier can be any value. It will need to be the same in Parallels Secure Workspace later on. In this example, it is Workspace-Guide-Custom-Username-Claim
- Reply URL (Assertion Consumer Service URL): This will need to match the ACS URL in the Parallels Secure Workspace. In this example, it would be https://workspace.somedomain.org/api/saml/
- Sign on URL (Optional): No need to configure.
- Relay state (Optional): No need to configure.
- Logout Url (Optional): Recommended. This will need to match the log out URL in Parallels Secure Workspace In this example, it would be https://workspace.somedomain.org/api/slo/

# **Basic SAML Configuration**

🔚 Save | 🔗 Got feedback?

3

#### Identifier (Entity ID) \* 🕕

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

	Default	
-Guide-Custom-Username-Claim	V ()	Î
Add identifier		

#### Reply URL (Assertion Consumer Service URL) \* ①

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:///api/saml/	<u>~</u>		v (	) 🗊

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.

https://

 $\sim$ 

# Attributes & claims

Mind that the user principal name (UPN) is used as the link between the Azure user and the LDAP user. If the user happens to have a different UPN on Microsoft Azure, the username claim will need to be adjusted as below.

#### Click Edit next to Attributes & claims.

Atti	ributes & Claims		🖉 Edi
give	enname	user.givenname	
surr	name	user.surname	
ema	ailaddress	user.mail	
nam	ne	user.userprincipalname	
Uni	que User Identifier	user.userprincipalname	

In most configurations, the claim http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name is used [...]. By default, this returns the user principal name of the Azure user.

Microsoft Azure	۶	Search resources, service
Home > Enterprise applications   All applications > Browse Azure	AD Gallery >	uide-Custom-Username-(
Attributes & Claims		
+ Add new claim + Add a group claim ≡≡ Columns   🕺	Got feedback?	
Required claim		
Claim name	Туре	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname
Additional claims		
Claim name	Туре	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

Advanced settings

When this does not match the UPN of the LDAP user, there are two options:

- 1. Click the claim name and change the **source attribute** to something else, for example: **user.extensionattribute1**
- 2. Click [ + Add new claim ] to add an entirely custom claim.
  - ◆ **Name:** Can be anything. For example: customatt
  - Namespace: Can be left blank.
  - Name format: Don't change, leave to default.

...

• Source: Depends on the use case. Most commonly: point to an Attribute and set Source attribute to the attribute (on the Azure AD) in which the user principal name of the local Active Directory will be stored. Do not forget to make sure this field is populated with the local UPN for the users who will be using Parallels Secure Workspace.

# Manage claim

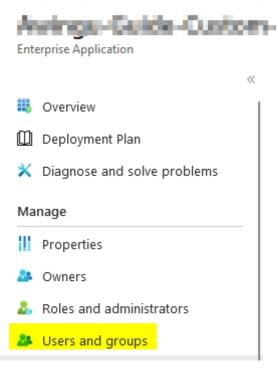
🔚 Save 🗙 Discard changes 🛛 🖗 Got feedback?			
Name *	customatt		
Namespace	Enter a namespace URI		
∧ Choose name format			
Name format	Omitted (default)		
Source *	Attribute      Transformation      Directory schema extension (Preview)		
Source attribute *	user.extensionattribute1		
✓ Claim conditions			
$\sim$ Advanced SAML claims options			

Click Save.

## Configuring users and groups

Click Users and groups. Select all the users and groups who should have access to the Workspace.

#### Home > Enterprise applications | All applic



## Grabbing federation metadata URL

#### Click Single sign on.

Under step 3, locate the **App Federation Metadata URL**. Copy this value, it's needed in the Parallels Secure Workspace configuration.

# -Guide-Custom-Username-Claim | SAML-based Sign-on

**Enterprise Application** 

Overview	2 Attributes & Claims	
] Deployment Plan		
Contraction Diagnose and solve problems	givenname surname	user.givenname user.surname
	emailaddress	user.mail
lanage	name	user.userprincipalna
	customatt	user.extensionattrib
Properties	Unique User Identifier	user.userprincipalna
Owners		
Roles and administrators	3 SAML Certificates	
Users and groups		
Sinale sign-on	Token signing certificate	
Single sign-on	Status	Active
Provisioning	Thumbprint	
Application prove	Expiration Notification Email	physical section.
Application proxy	App Federation Metadata Url	https://login.micro
Self-service	Certificate (Base64)	Download
Custom security attributes	Certificate (Base64) Certificate (Raw)	Download
(preview)	Federation Metadata XML	Download
ecurity	Verification certificates (optional)	
Conditional Access	Required	No
	Active	0
Permissions	Expired	0
Token encryption		

### **Configuring Parallels Secure Workspace: Federated Authentication**

In System Settings, after making sure the relevant domain is selected in the top left:

Navigate to **System Settings > Configure > User Connector.** 

- 1. Under **Reverse Proxy**, verify the **default login host header** is set to the host header which end users will use to access this Workspace domain (e.g. workspace.somedomain.org ).
- 2. Under Federated Authentication:
  - 1. Set the **Type** to **Pre-Authentication.** (Note: This article is limited to the instructions to set up Pre-Authentication, but these steps are the same when setting up Single Sign-On (SSO). SSO requires additional steps though.)
  - 2. Set the **Protocol** to **SAML.** 
    - ◊ Entity ID: Can be anything, for example: Workspace-Guide-Custom-Username-Claim
  - 3. Set the **Metadata Type** to **URL**. Paste the URL found in the Enterprise Application's Single Sign On Settings. It should look like

this: https://login.microsoftonline.com/<unique\_id>/federationmetadata/2007-06/federationmetadata.xml?app

- 4. It's recommended to enable **Single Logout**.
- 5. Change the Username claim.
  - Obfault: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
  - ♦ When using a custom claim: use the claim name, for example: customatt
- 6. Display Name Claim: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
- 7. Workspace URL: This will be used to construct the ACS URL for the Authentication Provider. In most scenarios, this is the host header that end users will use to access this Workspace domain. For example: https://workspace.somedomain.org
- 8. Click [Apply].

Note: the URLs will update each time the "Workspace URL" value has been saved.

ACS URL	https://
	The URL the SAML IdP will call after authentication.
Entity Id	-Guide-Custom-Username-Claim
	Unique identifier of the SAML IDP
Metadata Type	O URL
	O XML
	The type of metadata configured
Metadata URL	https://login.microsoftonline.com/
	The metadata URL eg.: "https://login.microsoftonline.com/ <tenant-id>/federationme</tenant-id>
Single Logout	<ul> <li>Enabled</li> </ul>
	O Disabled
	Also logs the user out of the IdP if he logs out of this workspace. The Workspace S
Workspace Single Logout	https://
URL	The URL that will be redirected to after the IdP finishes the Single Logout process.
Username Claim	customatt
	The SAML claim of the username e.g. http://schemas.xmlsoap.org/ws/2005/05/ider UPN.
Display Name Claim	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
bispidy nume oralli	The SAML claim of the display name e.g. http://schemas.xmlsoap.org/ws/2005/05/
	e e. the stant of the alopicy funde e.g. http://onefinde.xfilloodp.org/#3/2003/03/
Workspace URL	https://
	The Workspace base URL used to construct the redirect URL (for OpenID) or the A

# **Additional hints**

If **Azure AD Connect** (**AADConnect**) is being used to synchronize users from local Active Directory to Azure AD:

Set up a custom rule as described here:

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

- **inbound**: local AD (user principal name) -> metaverse
- **outbound**: metaverse -> extension1 (or any of the other ones available).

There's also a technical video available.

© 2024 Parallels International GmbH. All rights reserved. Parallels, the Parallels logo and Parallels Desktop are registered trademarks of Parallels International GmbH. All other product and company names and logos are the trademarks or registered trademarks of their respective owners.