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

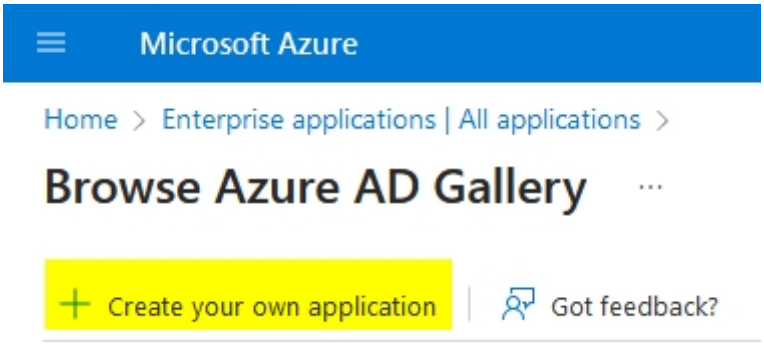
This needs to be configured per Workspace domain.

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 .

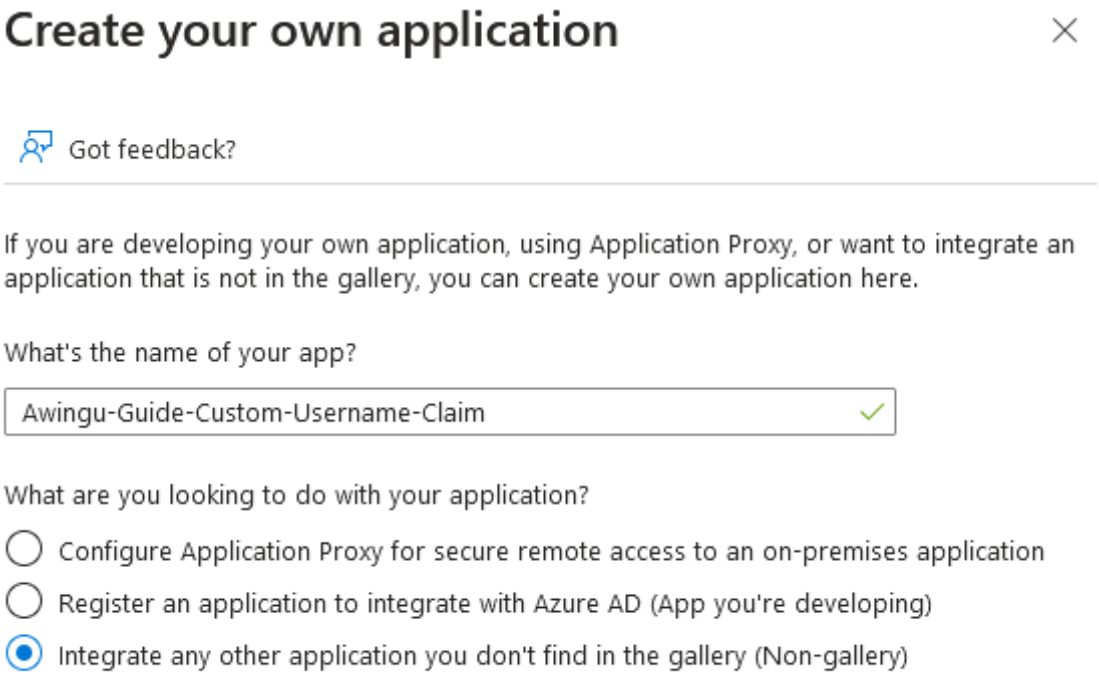
Microsoft Azure will only allow URLs using https; so make sure there is an SSL certificate configured in Parallels Secure Workspace for this Workspace domain.

Creating Azure Enterprise Application

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

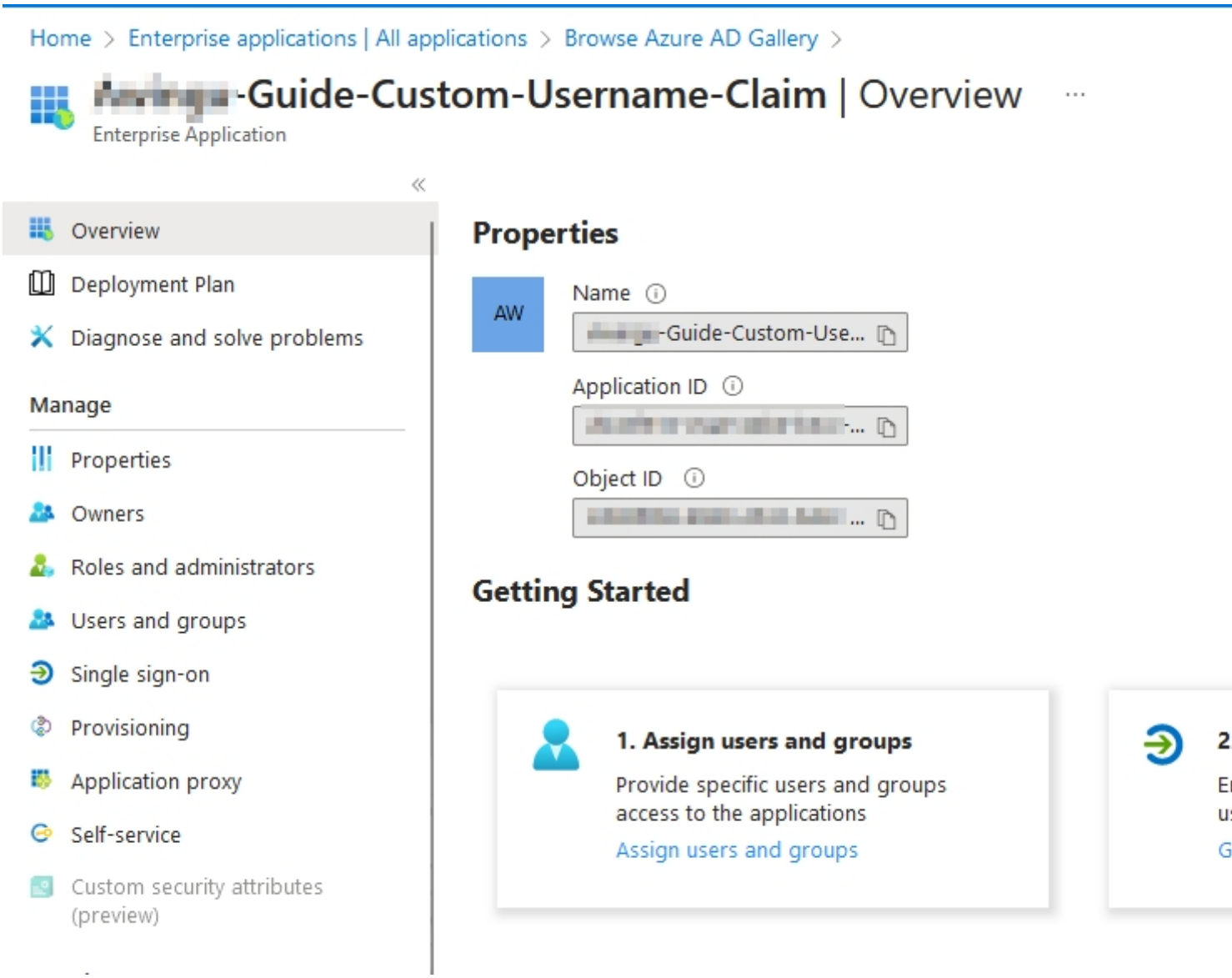


Give the application a name of your choice. Leave the radio button set to "Integrate any other application you don't find in the gallery (Non-gallery)".

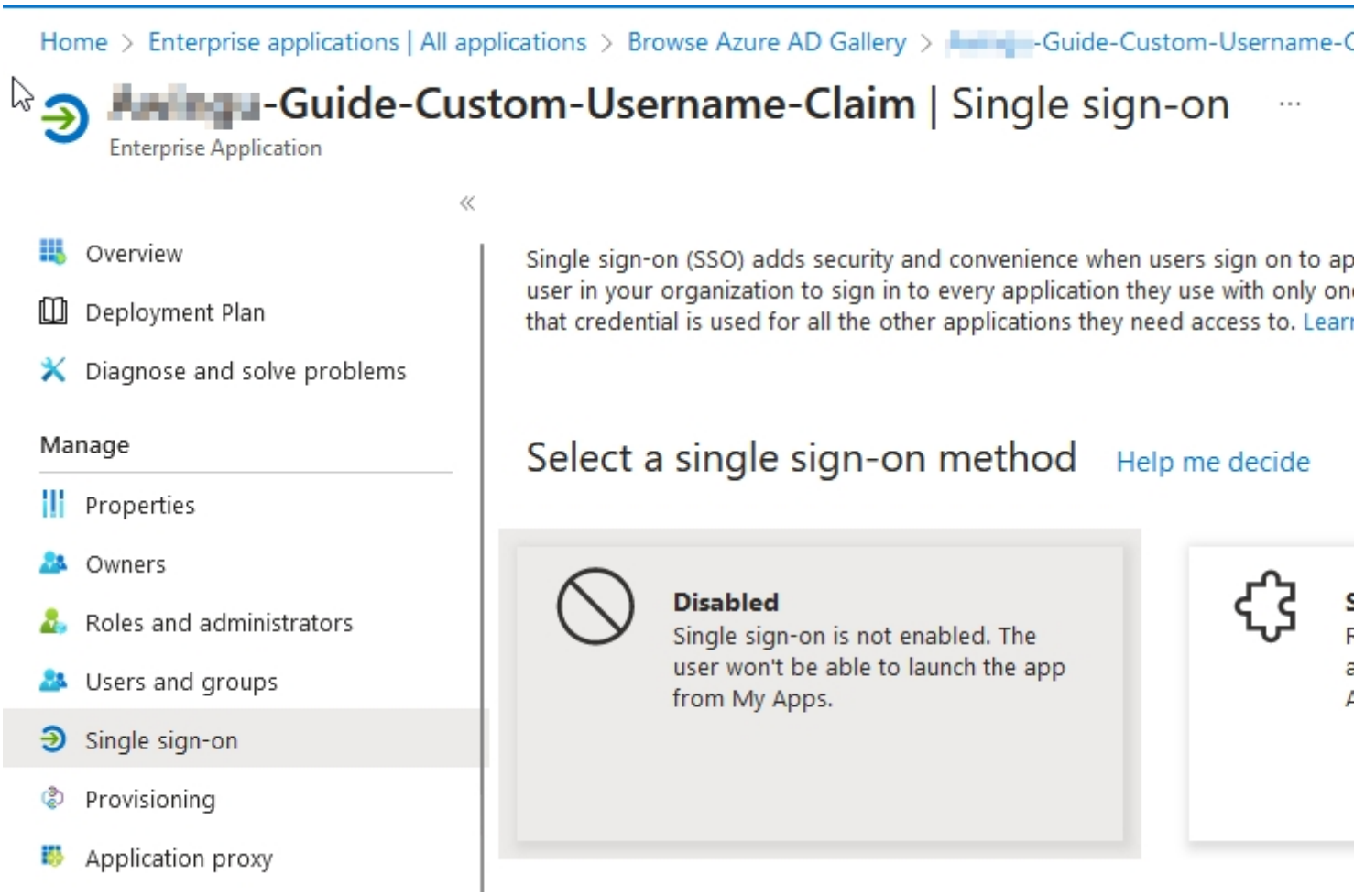


Confirm by pressing **[Create]**.

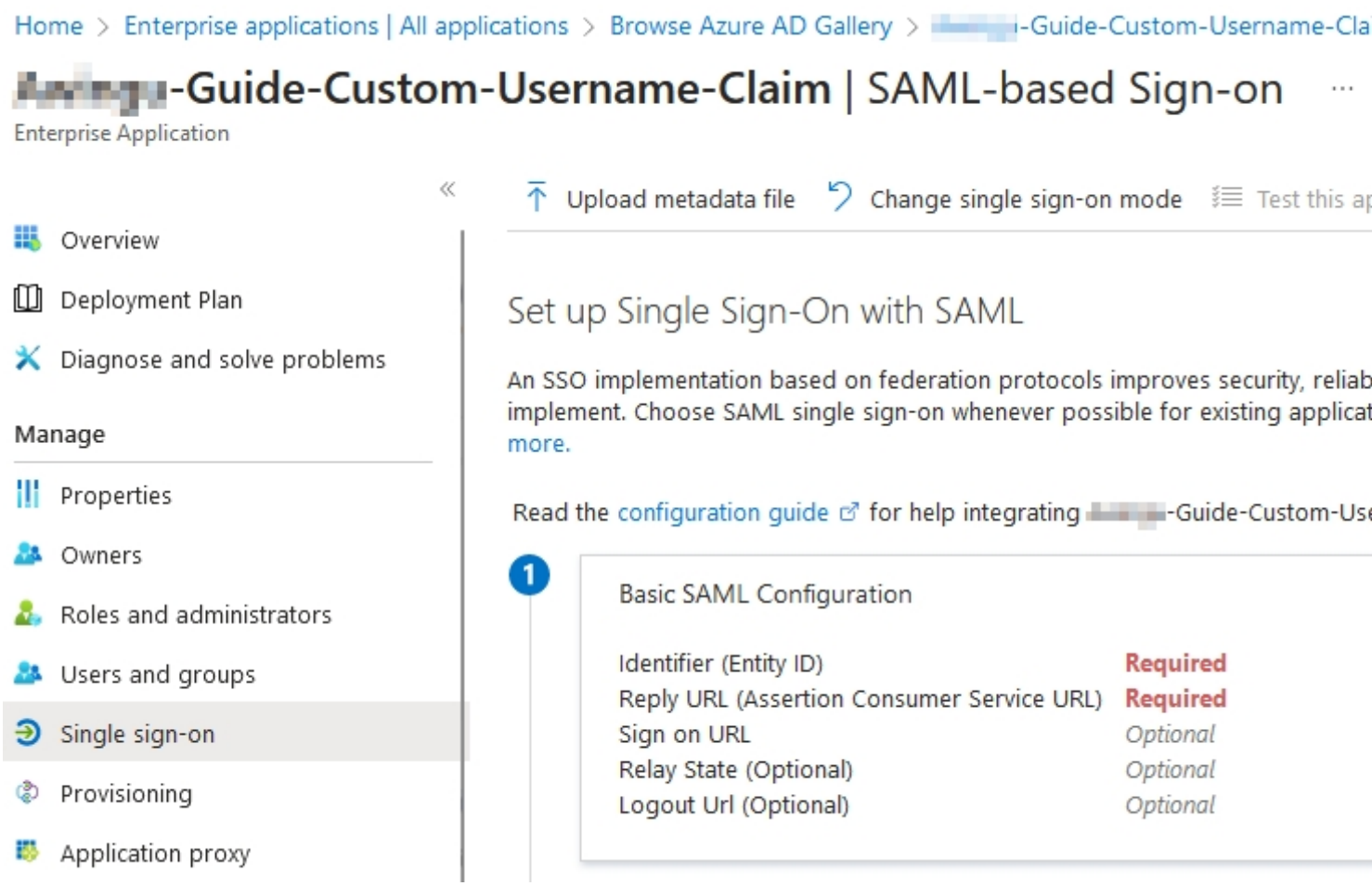
After a bit, the properties of the Enterprise Application should be shown.
In the left navigation menu, choose **Single sign-on**.


Home > Enterprise applications | All applications > Browse Azure AD Gallery >
-Guide-Custom-Username-Claim | Overview
Enterprise Application
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 (preview)
Properties
AW
Name
-Guide-Custom-Use...
Application ID
Object ID
Getting Started
1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

Choose **SAML**:



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



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?

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
[redacted]-Guide-Custom-Username-Claim	✓

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.

	Index	Default
https://[redacted]/api/saml/		✓

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.

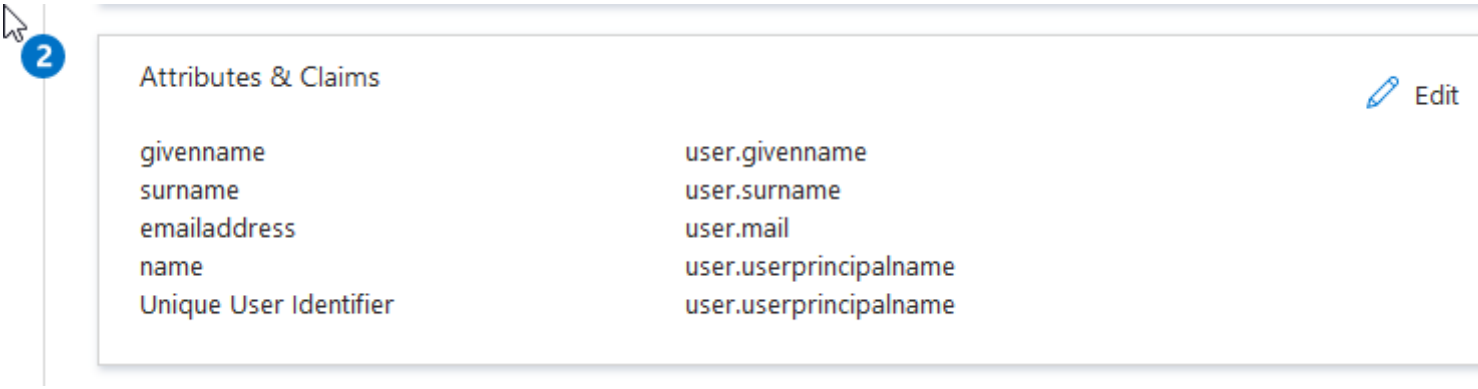
https://[redacted]/api/slo/

Click **[Save]**.

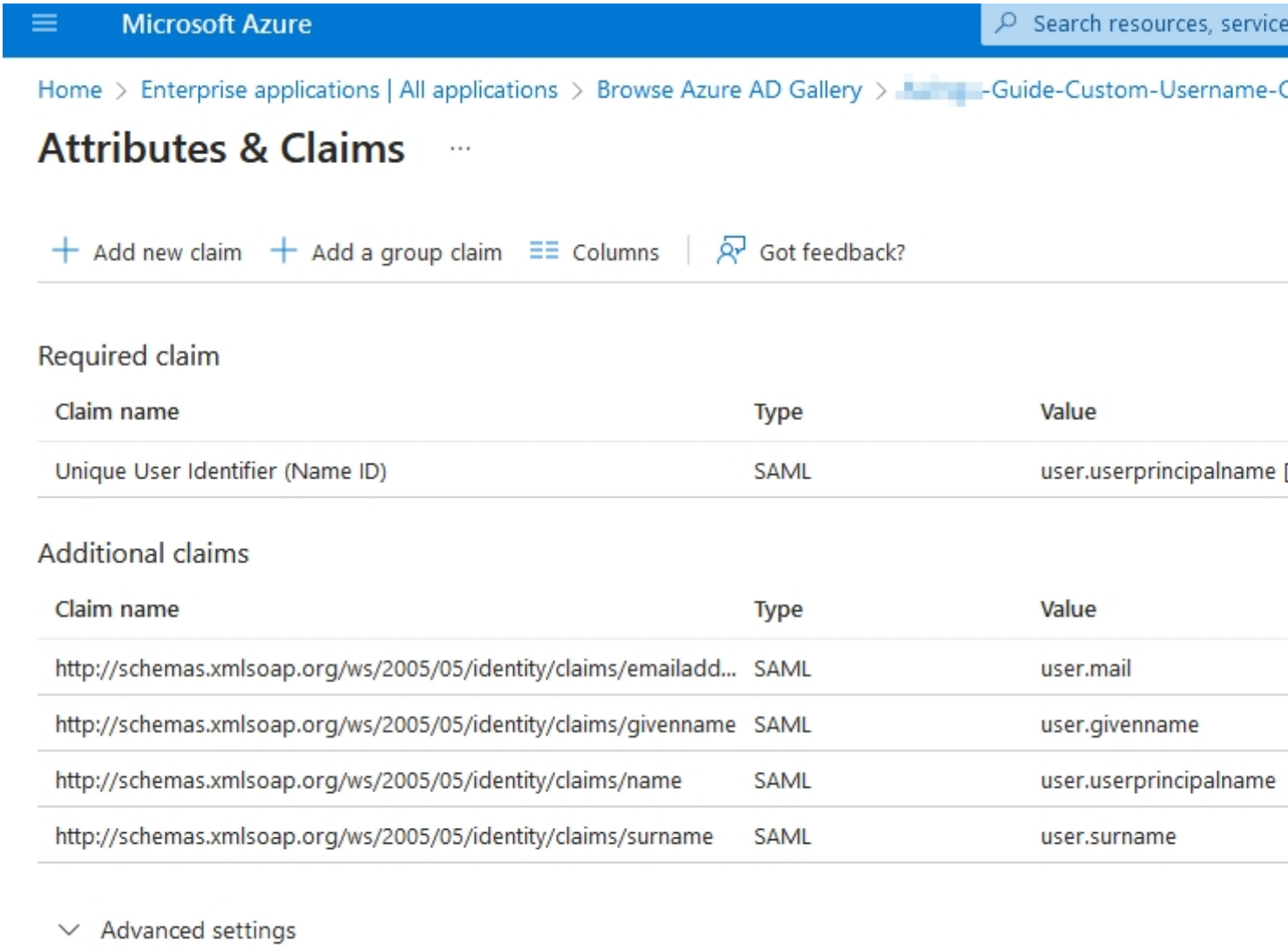
Attributes & claims

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.**

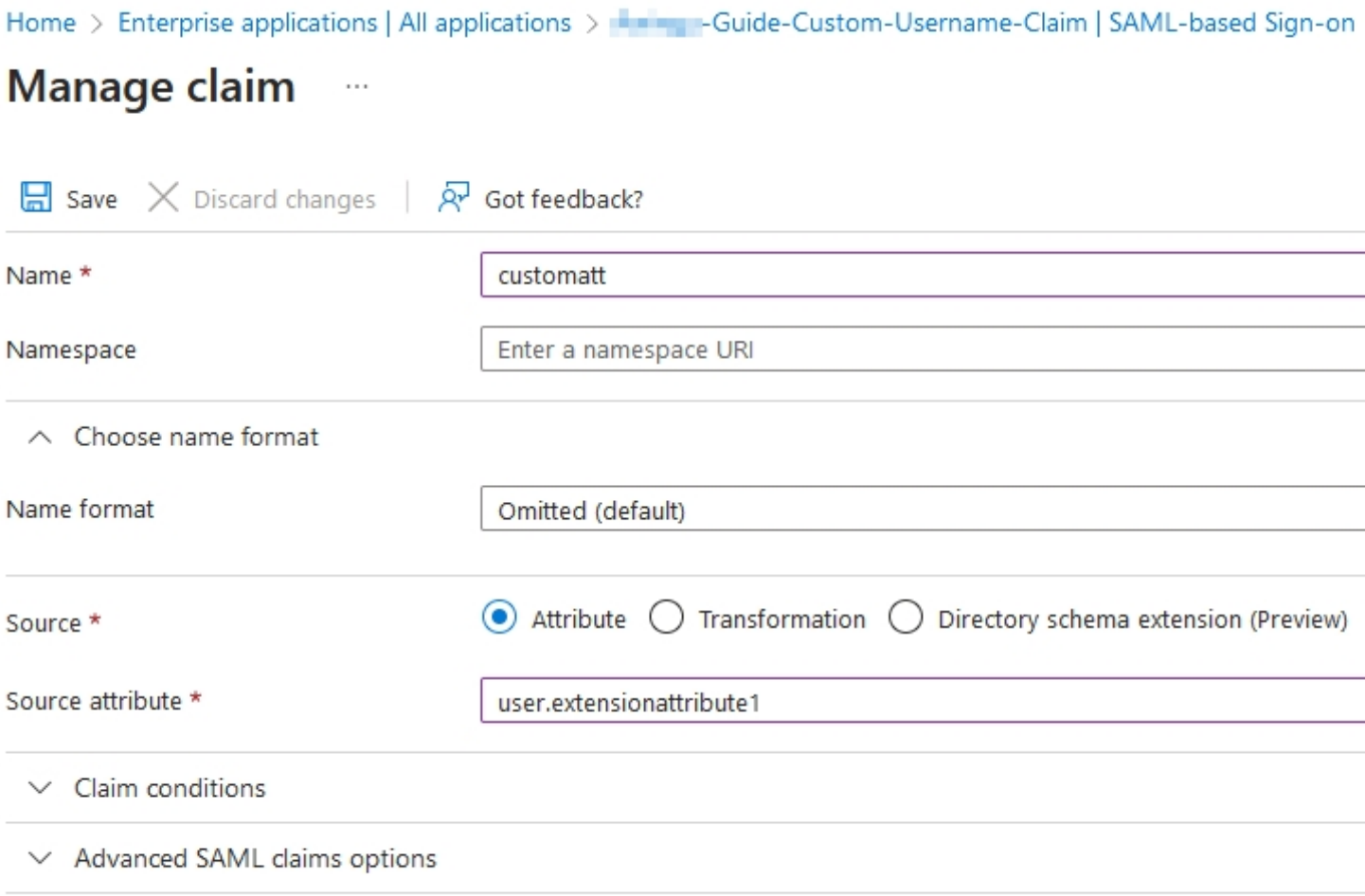


In most configurations, the claim **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name** is used **[...]**. By default, this returns the user principal name of the Azure user.



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

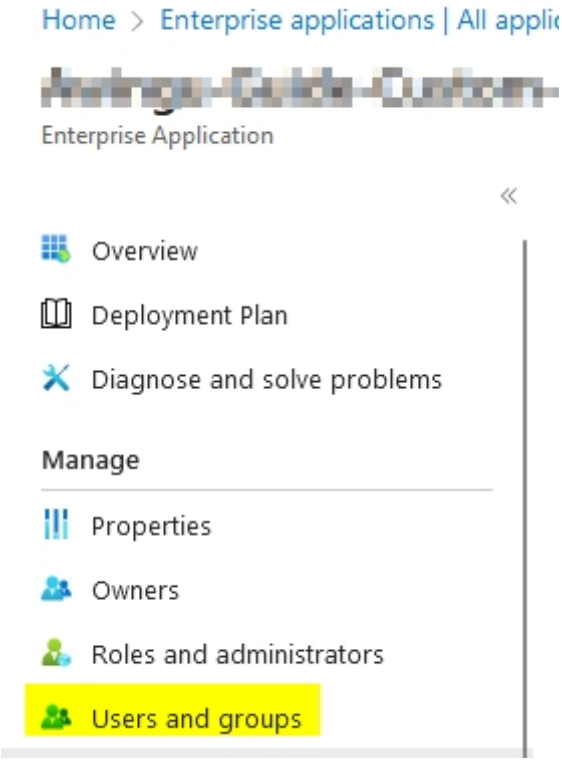
1. Click the claim name and change the **source attribute** to something else, for example: **user.extensionattribute1**
2. Click [+ Add new claim] to add an entirely custom claim.
    - **Name:** Can be anything. For example: customatt
    - **Namespace:** Can be left blank.
    - **Name format:** Don't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



Click **Save**.

Configuring users and groups

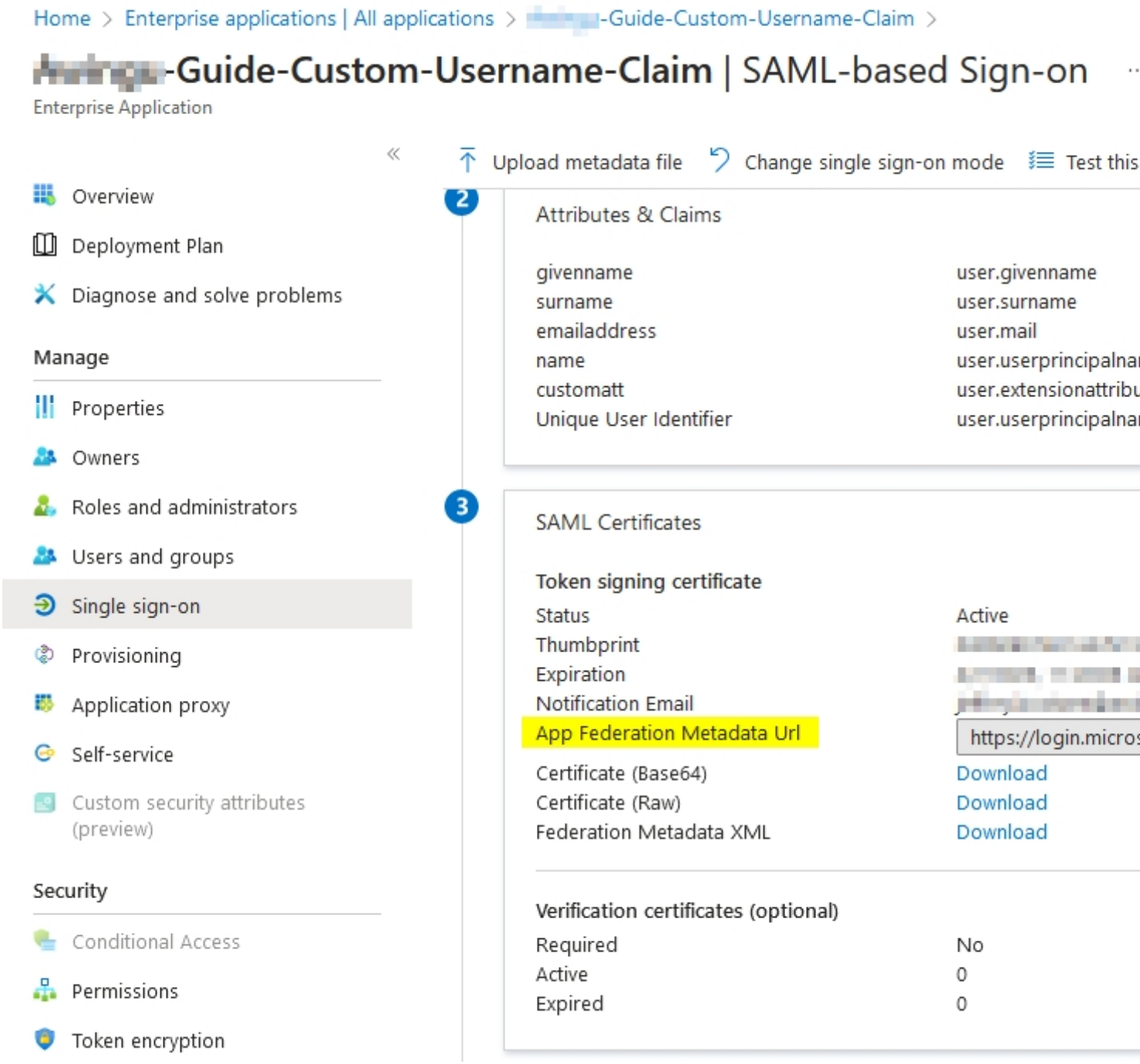
Click **Users and groups**. Select all the users and groups who should have access to the Workspace.



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.



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.**
    - ◊ Default: 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://[redacted]/api/saml/

The URL the SAML IdP will call after authentication.

Entity Id [redacted]-Guide-Custom-Username-Claim

Unique identifier of the SAML IDP

Metadata Type

- (●) URL
- ( ) XML

The type of metadata configured

Metadata URL https://login.microsoftonline.com/[redacted]

The metadata URL eg.: "https://login.microsoftonline.com/<tenant-id>/federationme

Single Logout

- (●) Enabled
- ( ) Disabled

Also logs the user out of the IdP if he logs out of this workspace. The Workspace S

Workspace Single Logout URL https://[redacted]/api/slo/

The URL that will be redirected to after the IdP finishes the Single Logout process. T

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

The SAML claim of the display name e.g. http://schemas.xmlsoap.org/ws/2005/05/

Workspace URL https://[redacted]

The Workspace base URL used to construct the redirect URL (for OpenID) or the A

Click **Apply**.

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.
