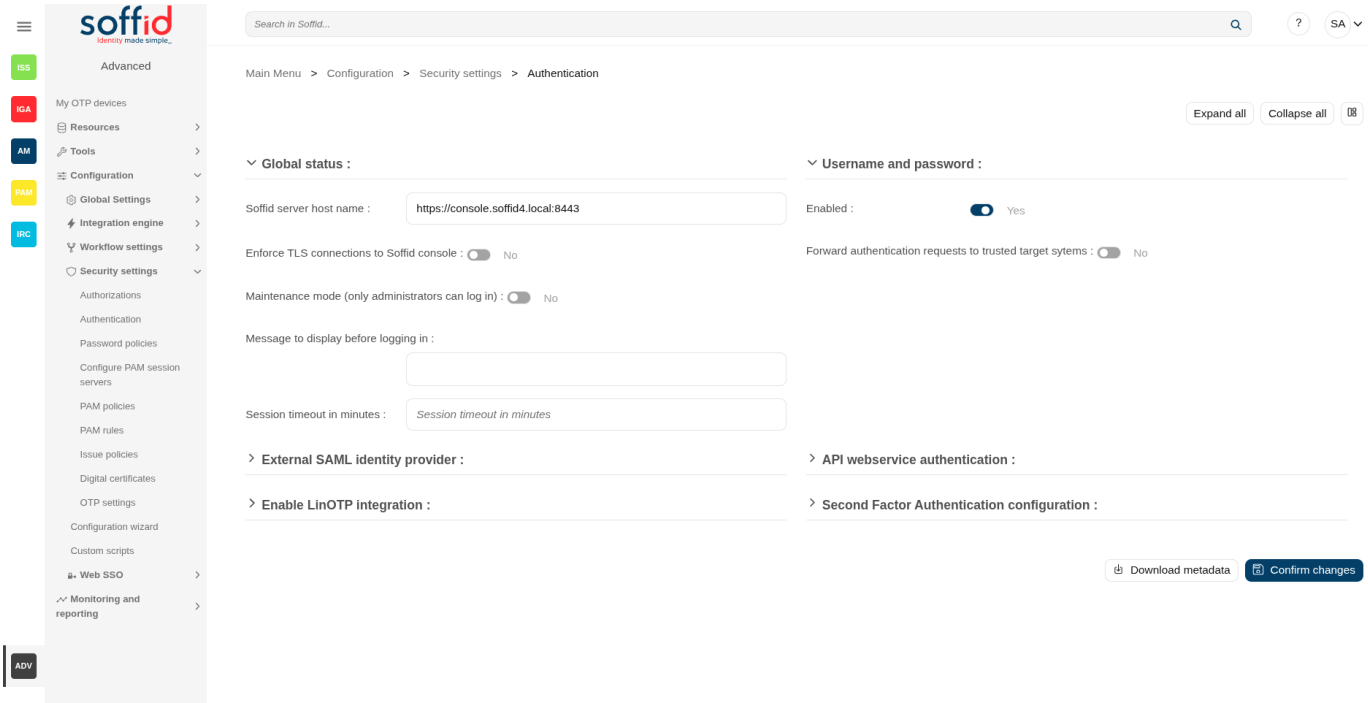
Authentication

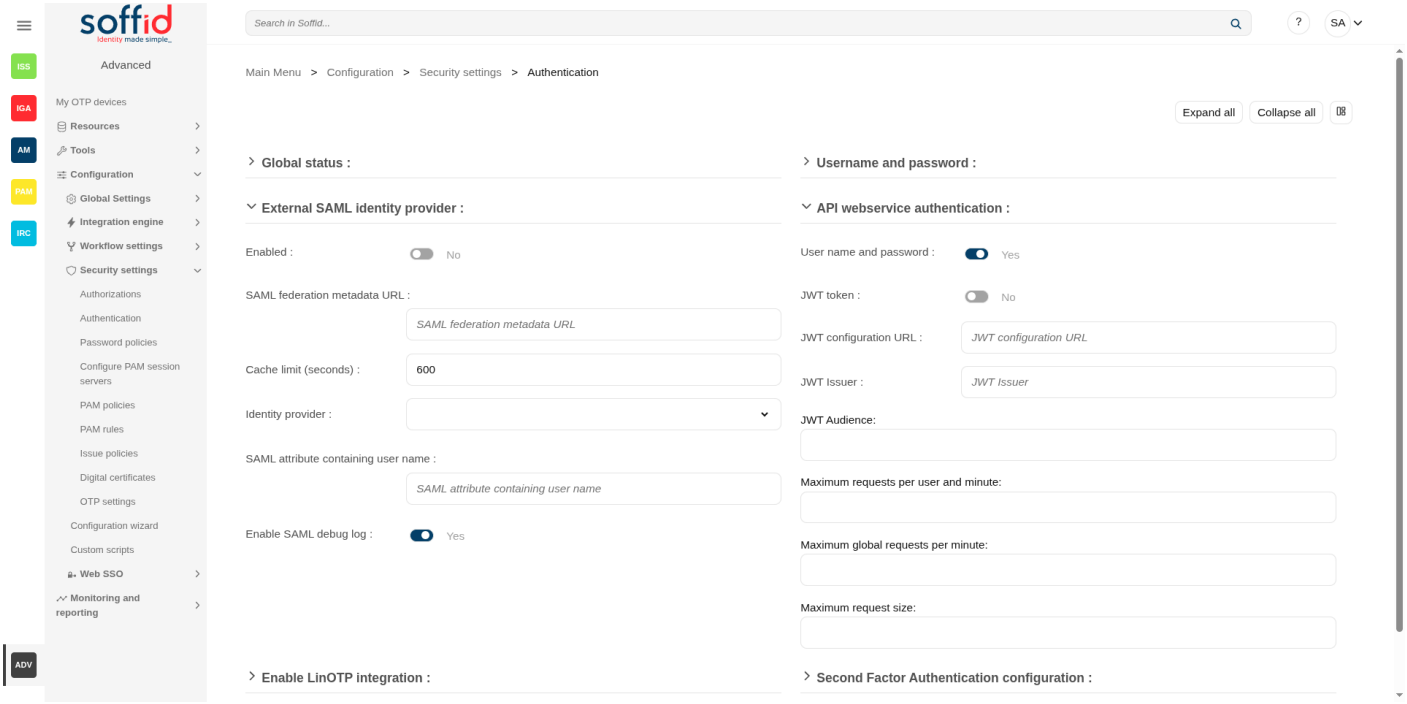
Definition

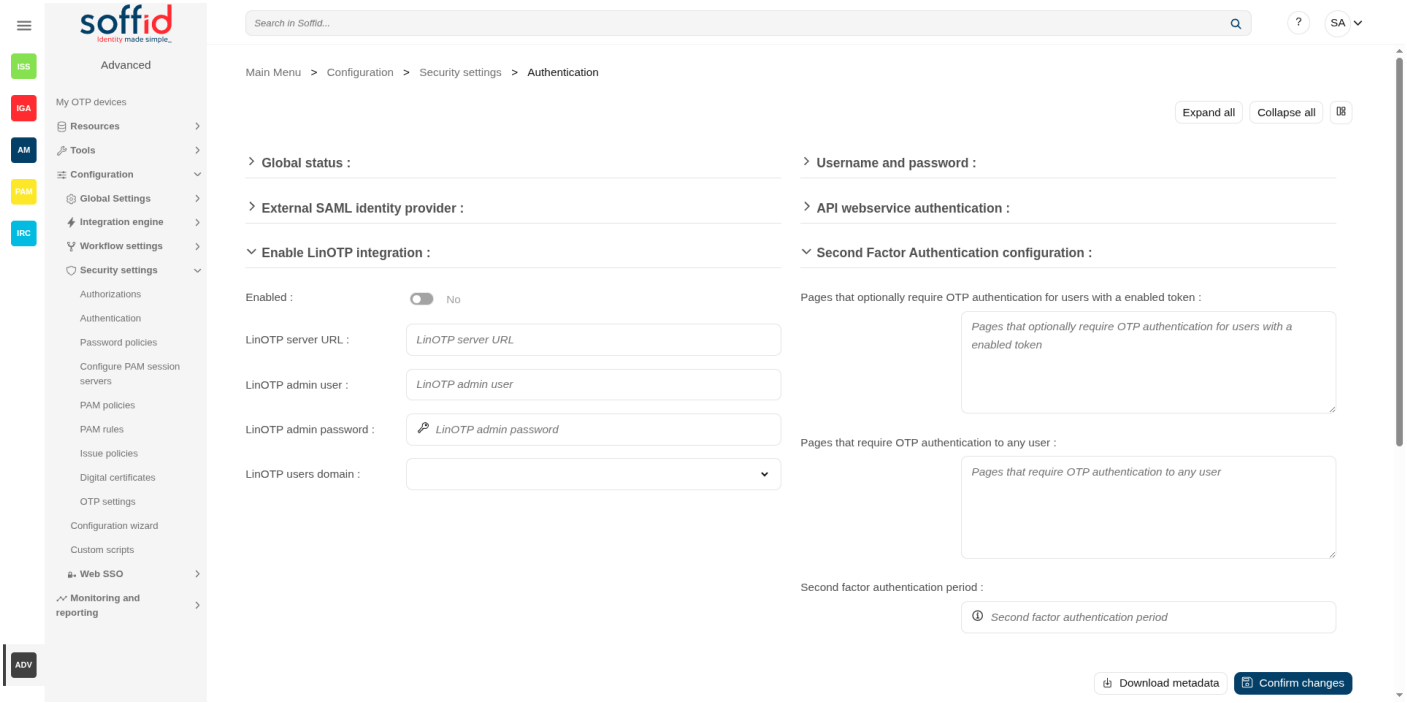
> This page gathers different types of settings that may affect user authentication in the Soffid Console.

Soffid could use different kinds of external authentication sources. These mechanisms could be selectively enabled or disabled.

Screen overview







Related objects

- Users : users must have a enabled Soffid account.
- Identity provider : users could log in with the Soffid idp or another external idp.
- Console log : to check the console logs
- Account naming rules : to configure the LinOTP service

Standard attributes

Global status

- **Soffid server host name**: URL generated in the installation configuration.
- **Enforce TLS connections to Soffid console:** If you check this option, it will be is mandatory to restart the Soffid Console.

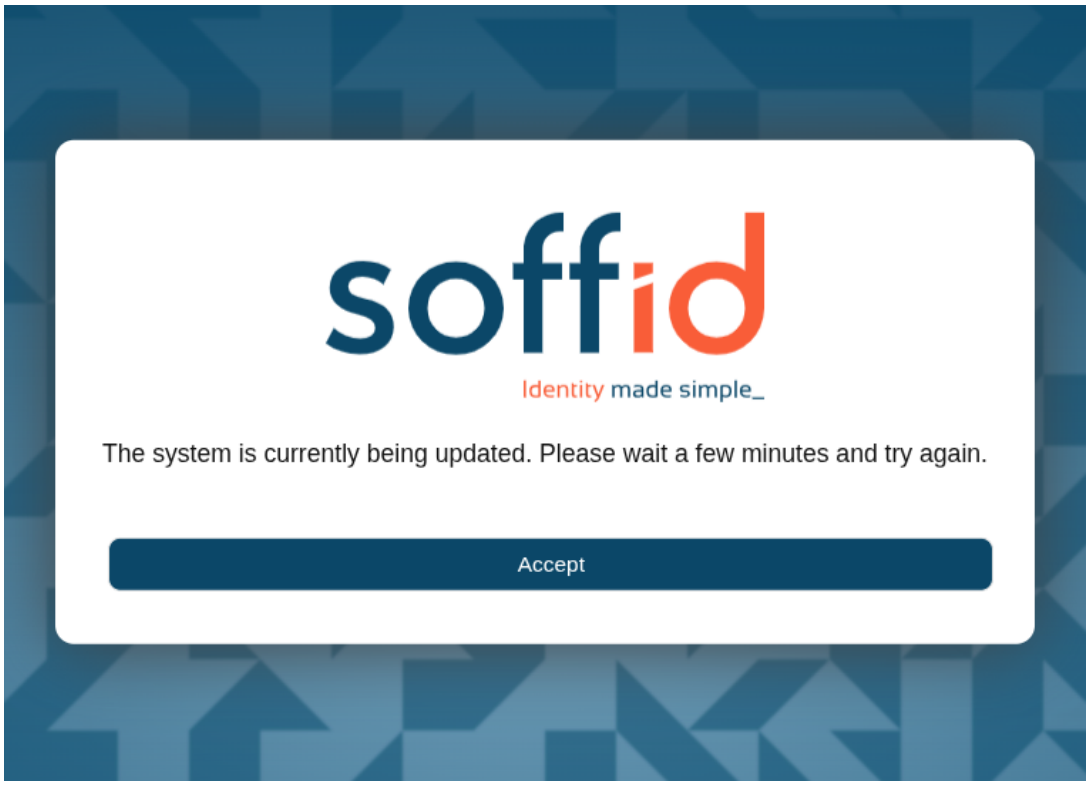
> Once you check the **Enforce TLS connections to Soffid Console** option, there are no easy way to come back. You should use this option only en Production environments.

- **Maintenance mode (only administrators can log in)**: if this option is checked (value is Yes), only the administrators could connect to Soffid Console.

Image

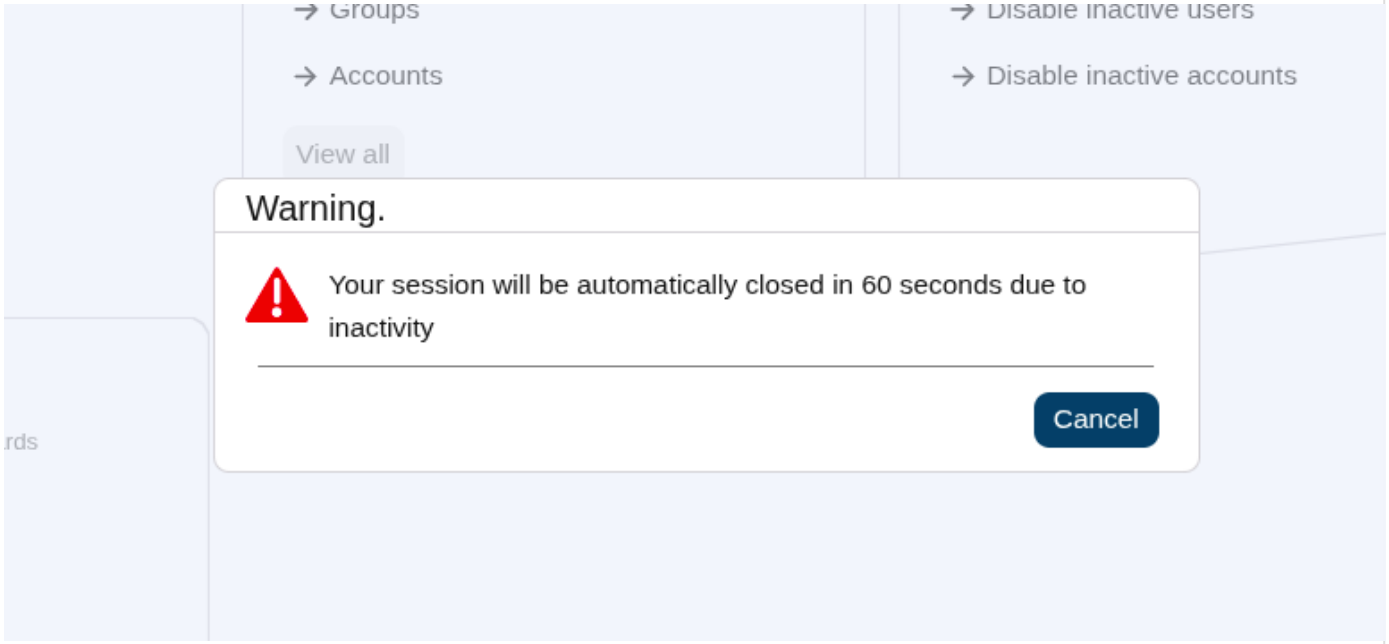
- **Message to display before logging in**: administrators can configure a banner that will be displayed before the user logging in. This banner will display security advice.

Image



- **Session timeout in minutes**: time in minutes it takes for the console to display the message indicating that the session is being closed. If nothing is indicated, the session does not expire.

Image



Username and password

- **Enabled**: the only attribute enabled by default in the installation of Soffid. It is the internal username and password authentication mechanism. Therefore, the authentication is made with the username and password of the soffid account.
- **Forward authentication requests to trusted target systems**: to use external username and password sources. Therefore, the authentication is made with the username and password of an account of an external system.

> This authentication is applies only to agents that have checked "Trust password" in the agent. For more information about agents please visit the Agents page.

> If the password entered by the user does not match with the Soffid account (if the attribute "Enabled" is checked), the Soffid core will issue a "ValidatePassword" task for each trusted target system (with checked "Trust password"). If any of the trusted target systems accepts the password, it will be hashed and stored in Soffid tables and login will be accepted.

> Be aware that this password change in Soffid will affect all systems that share the same password domain (defined in the password policies).

External SAML identity provider

It should be noted this feature does not depend on the federation addon. That is a feature included by default in the Soffid smart engine to allow you to include in the authentication flow a mechanism to use a third-party SAML system.

Soffid's own identity provider can also be used.

- **Enable**: check it (select value Yes) to use an external SAML Identity Provider.
- **Soffid Server host name**: the URL that will be used by external IdP. This URL will be resolved by end user's browser in order to send the SAML assertion.
- **SAML federation metadata URL**: the URL where federation information can be found. If the Soffid console can fetch federation metadata, the Identity provider drop-down will be filled in with any identity provider found in the federation metadata URL.
- **Cache limit (seconds)**: how often the federation information will be refreshed. By default, 10 minutes will be taken.
- **Identity provider**: Identity Provider to use for authentication.
- **Enable SAML debug log**: it displays more trace in the Console log files

Finally, download the Soffid Console and load it into your SAML Identity Provider federation.

If SAML Identity Provider is enabled, as well as username and password, the user will have the chance to select the preferred authentication method. Otherwise, if only SAML is enabled, the user will be automatically redirected to SAML Identity Provider.

Image

Office 365 as External SAML identity provider

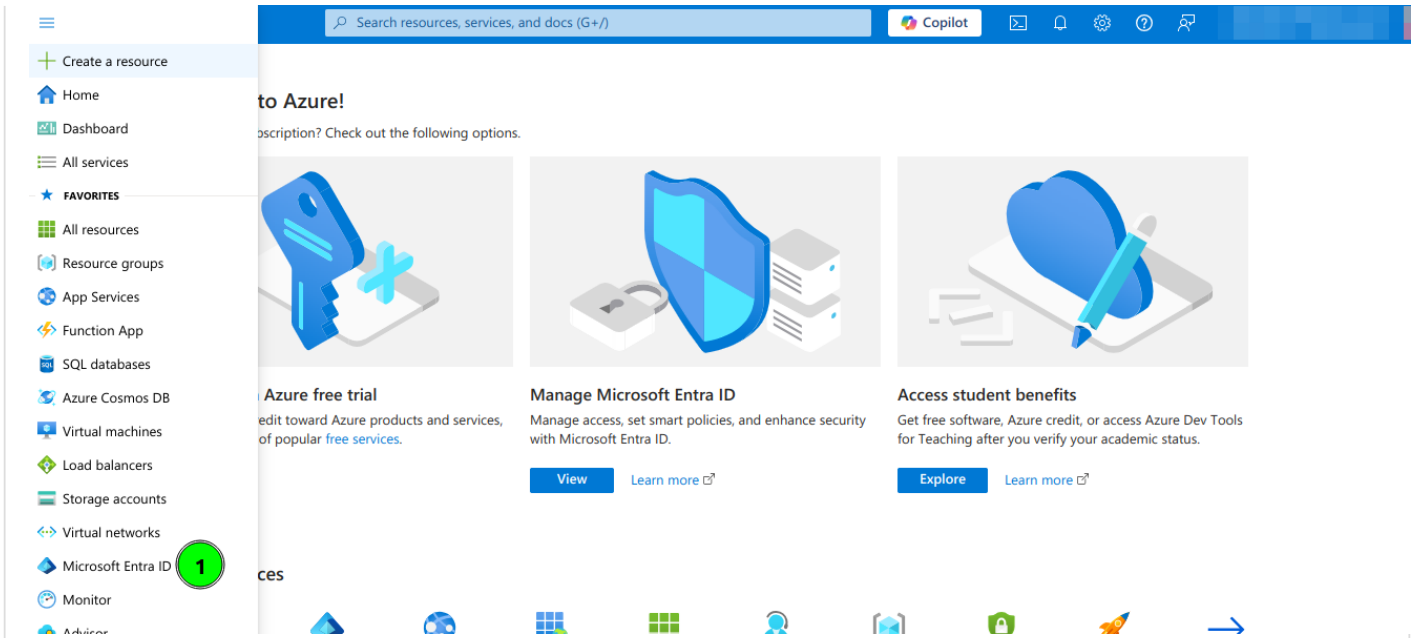
Introduction

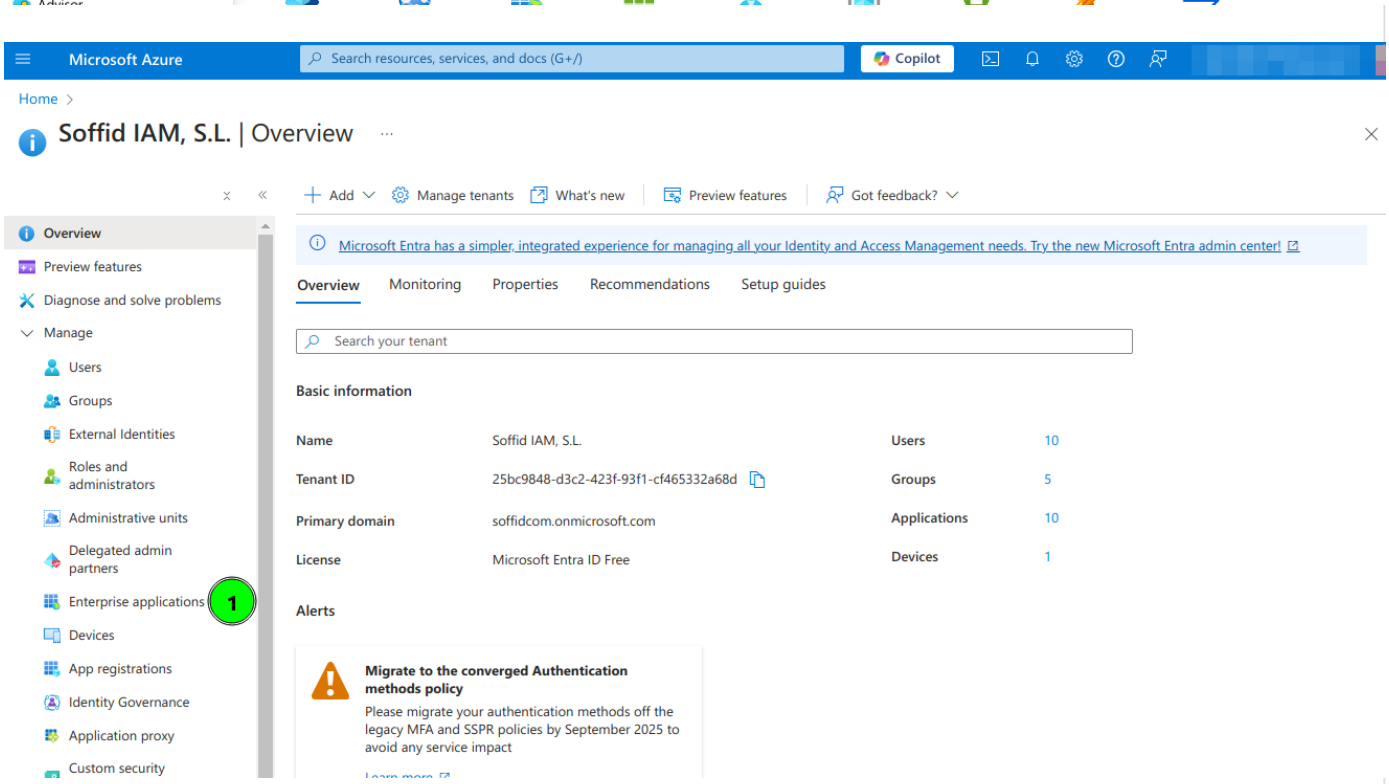
Steps to configure Office 365 as External SAML identity provider.

Step-by-Step

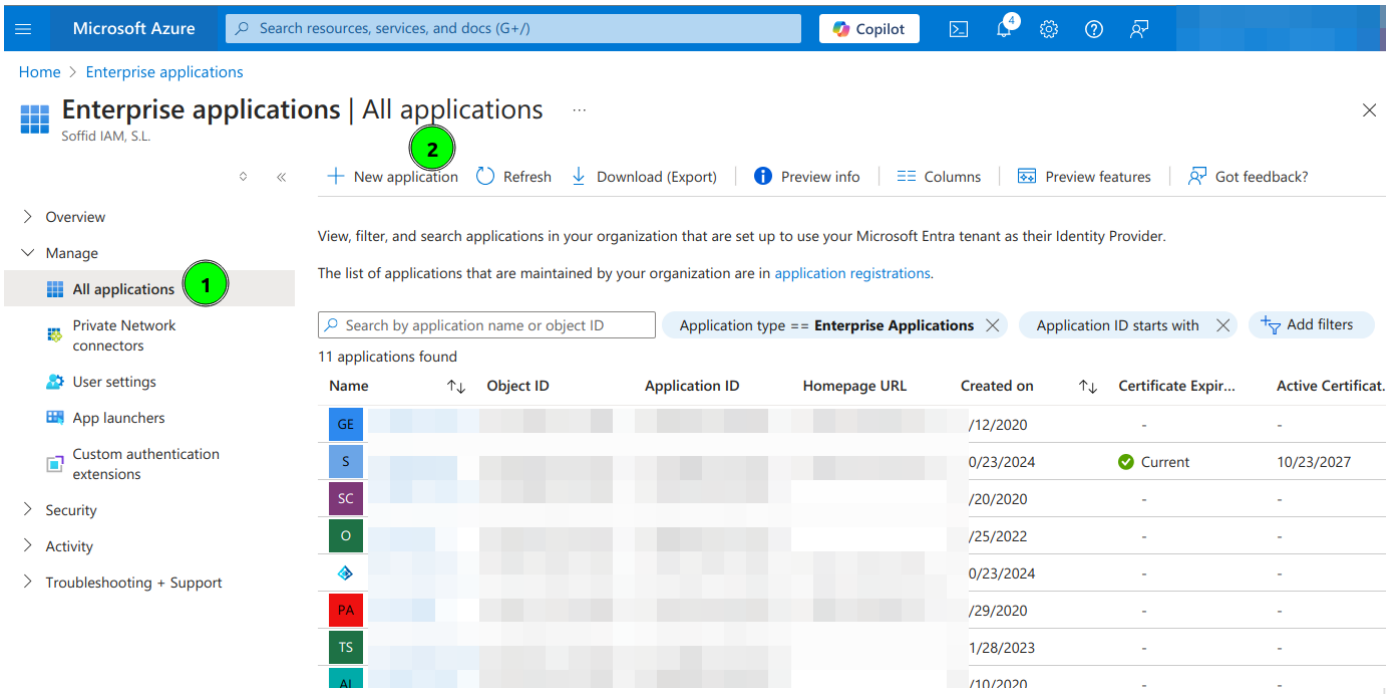
1. Open a https://portal.azure.com

2. Open **Microsoft Entra ID** and then select **Enterprise applications** option

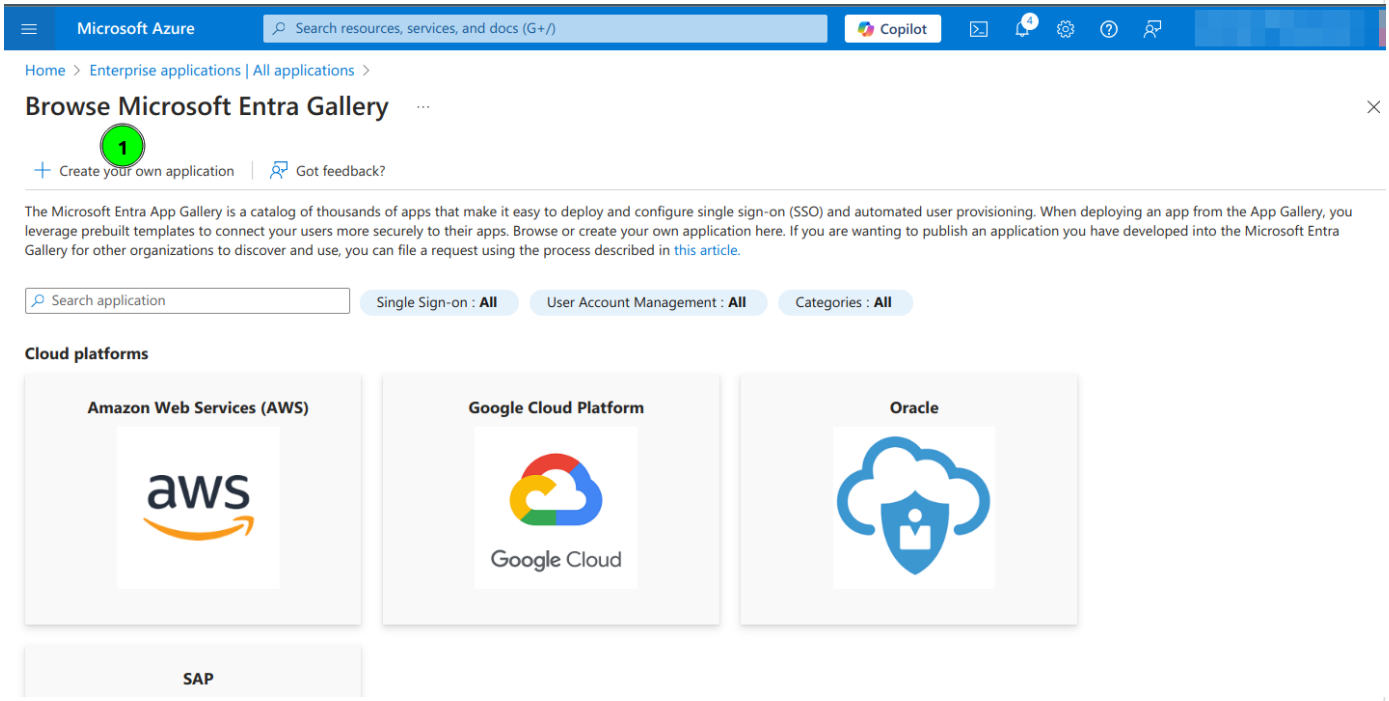




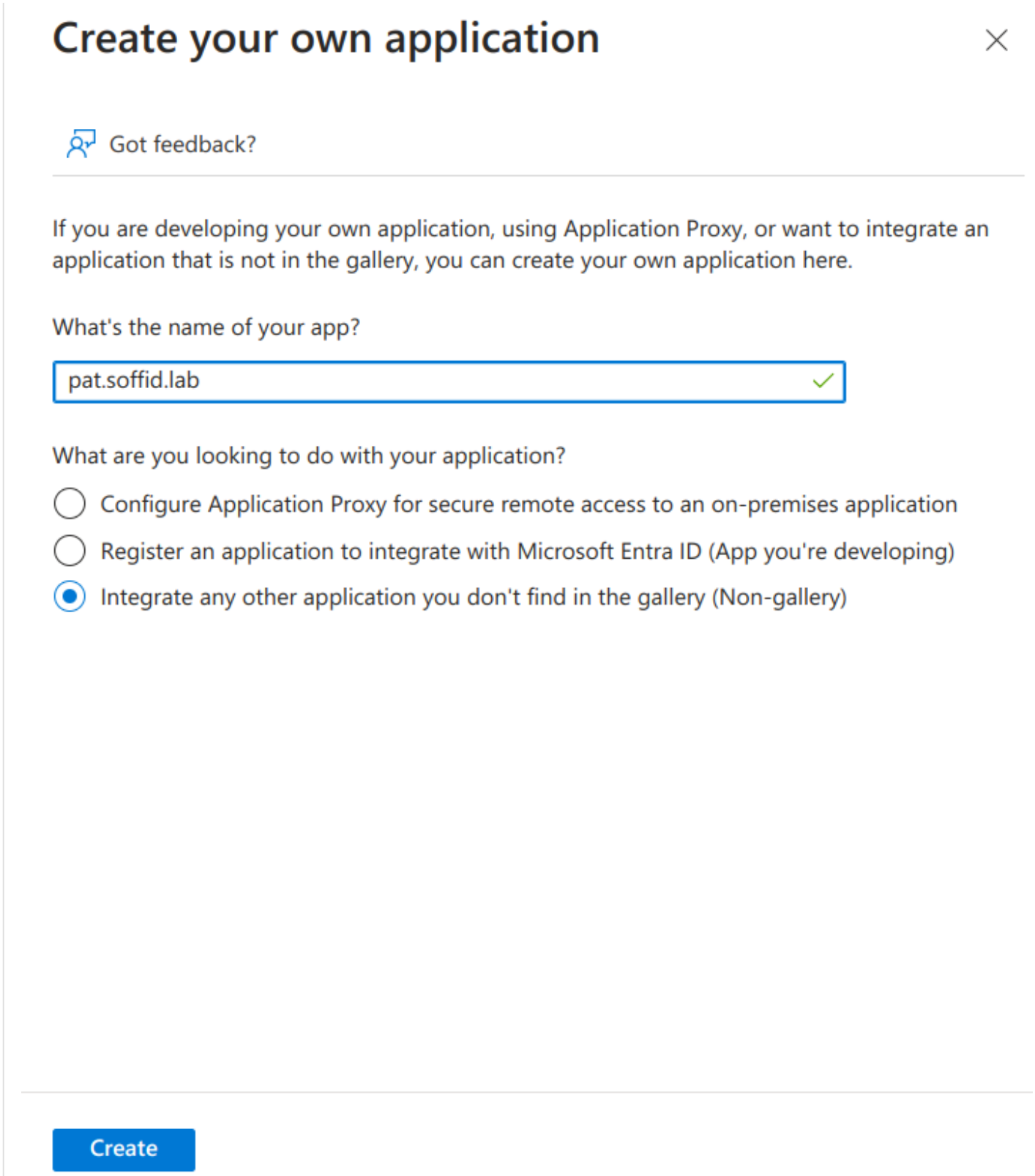
3. Select **All applications** and click **New Application**



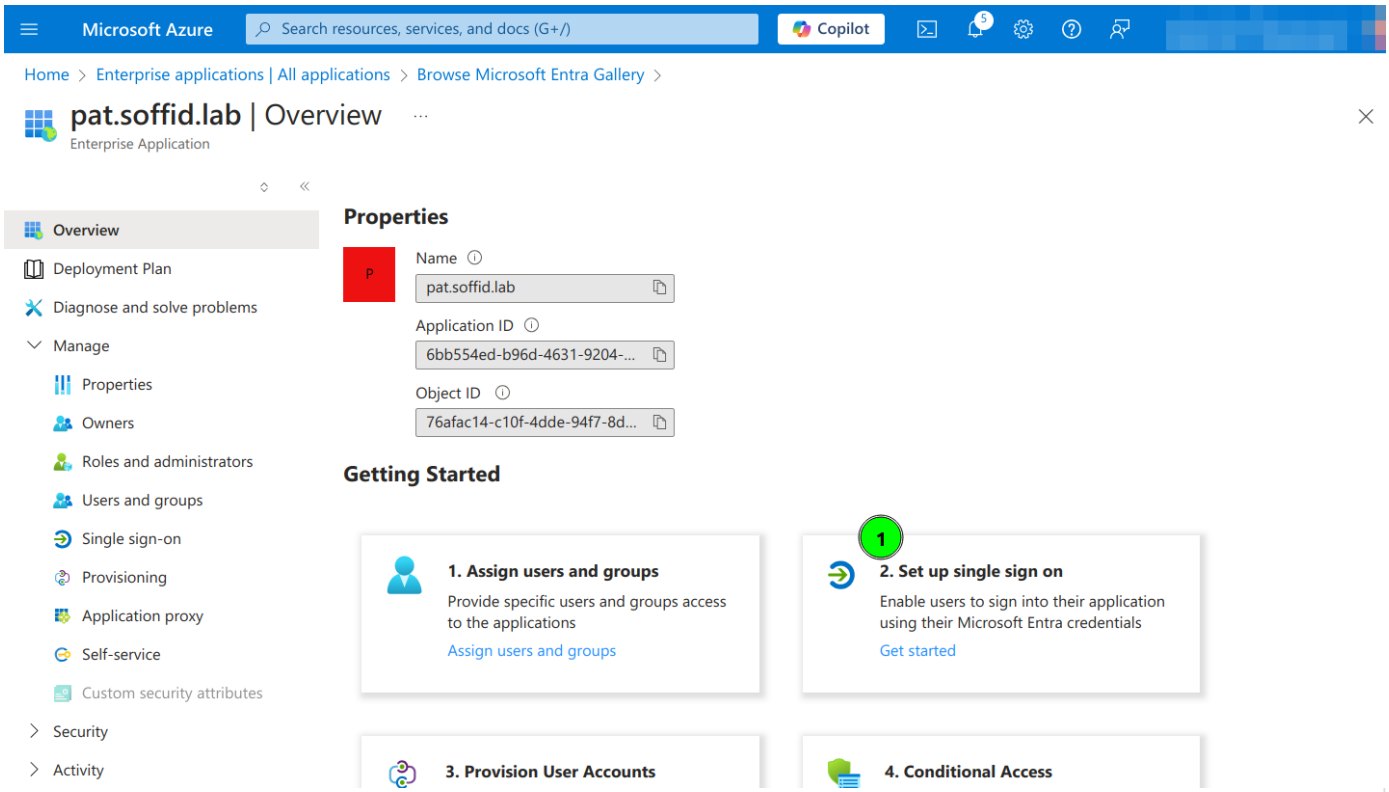
4. Select Create your own application



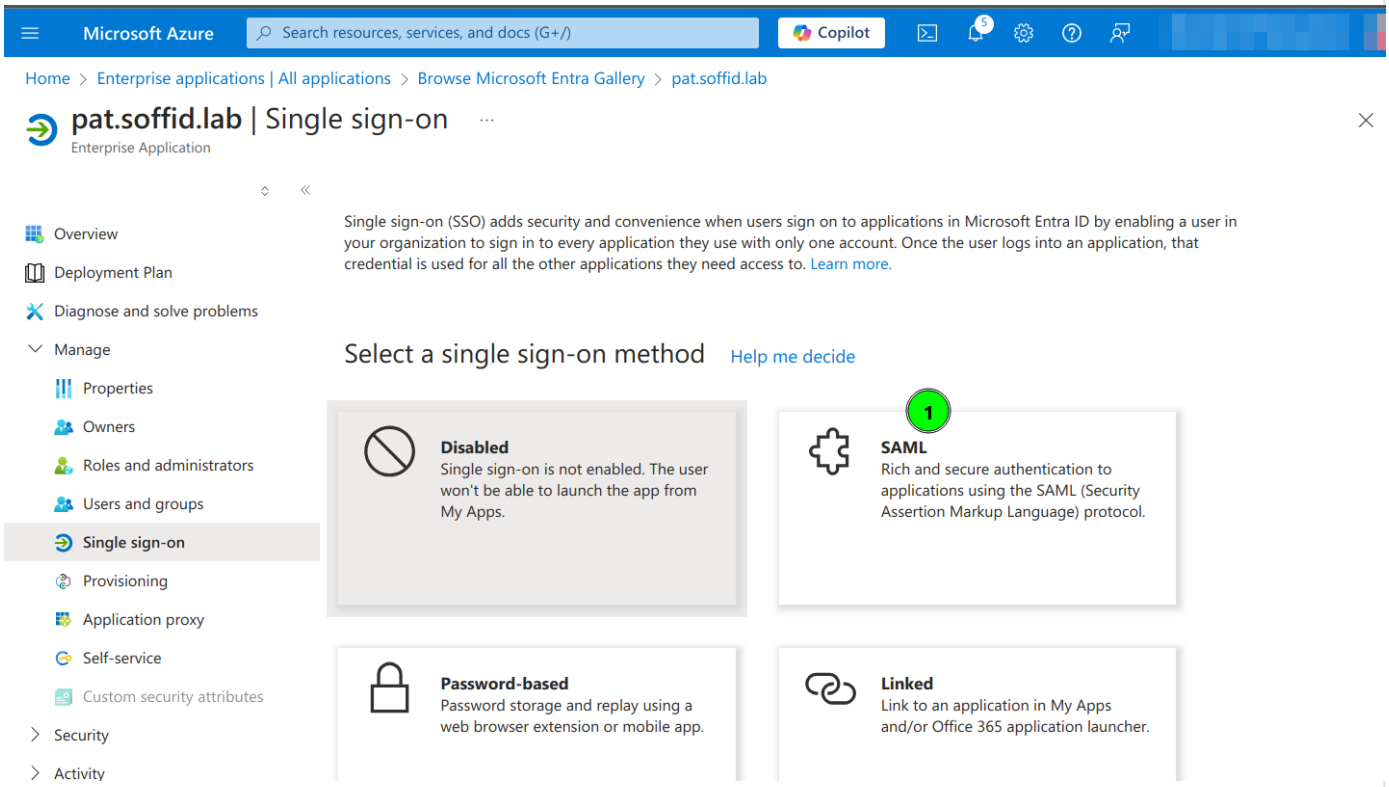
5. Type the name of your app and select the "Integrate any other application you don't find in the gallery (Non-gallery)" option



6. Click on **Set up single sign on**

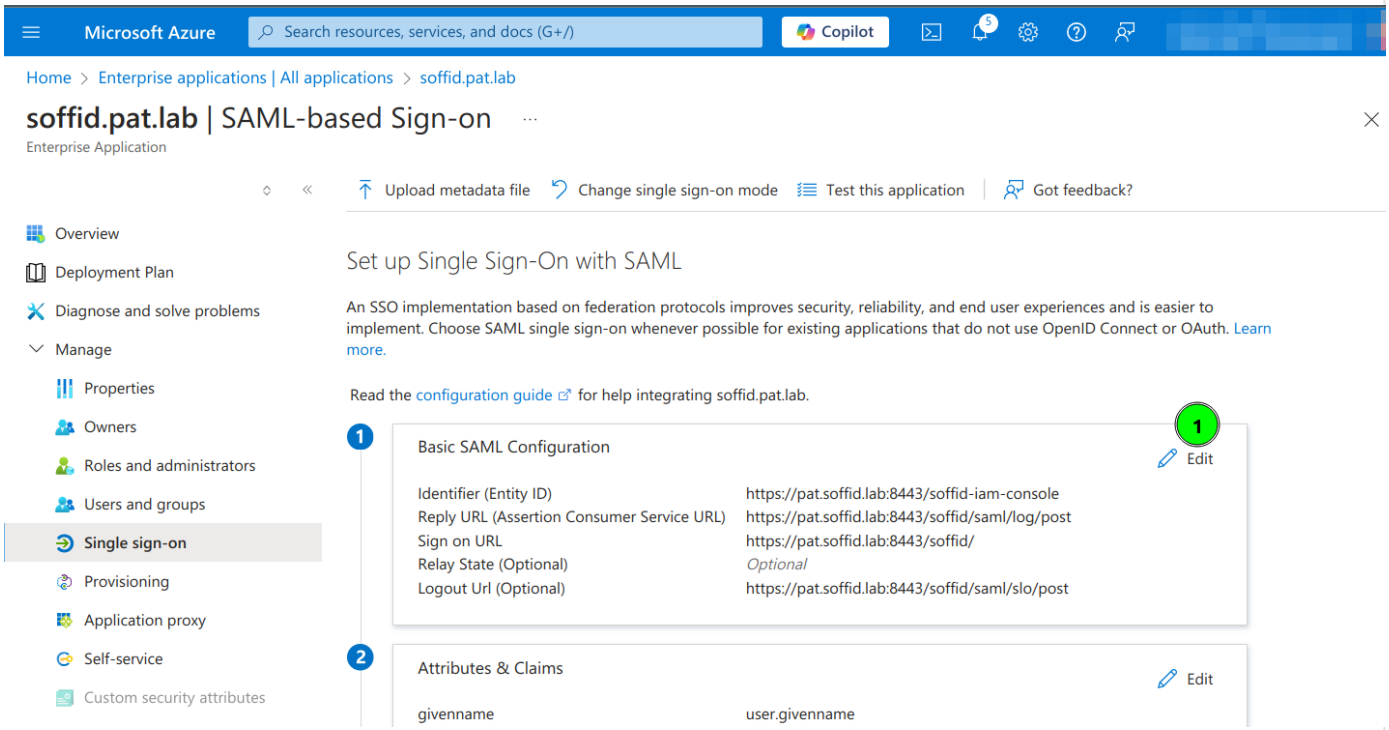


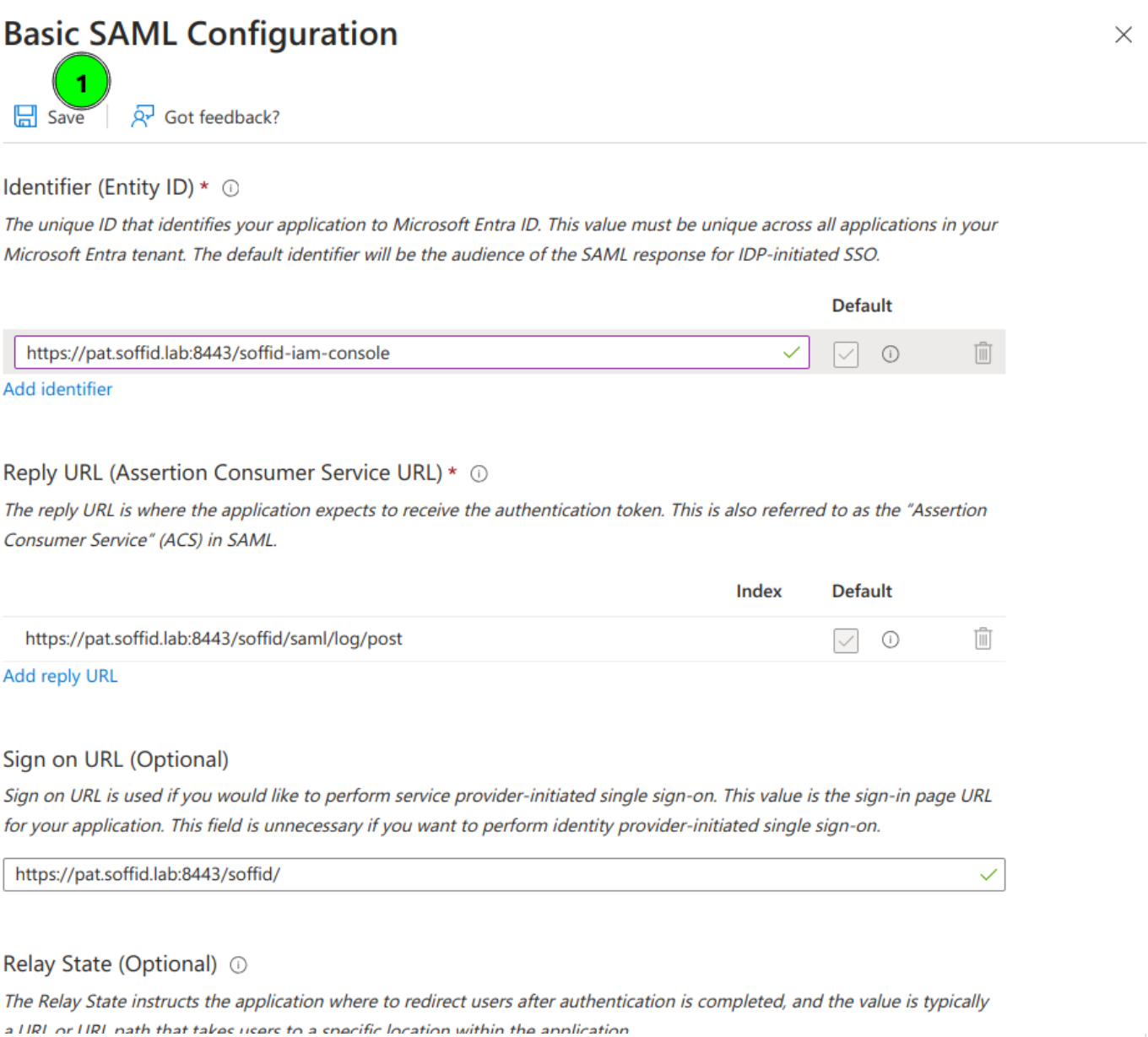
7. Click the **SAML** option



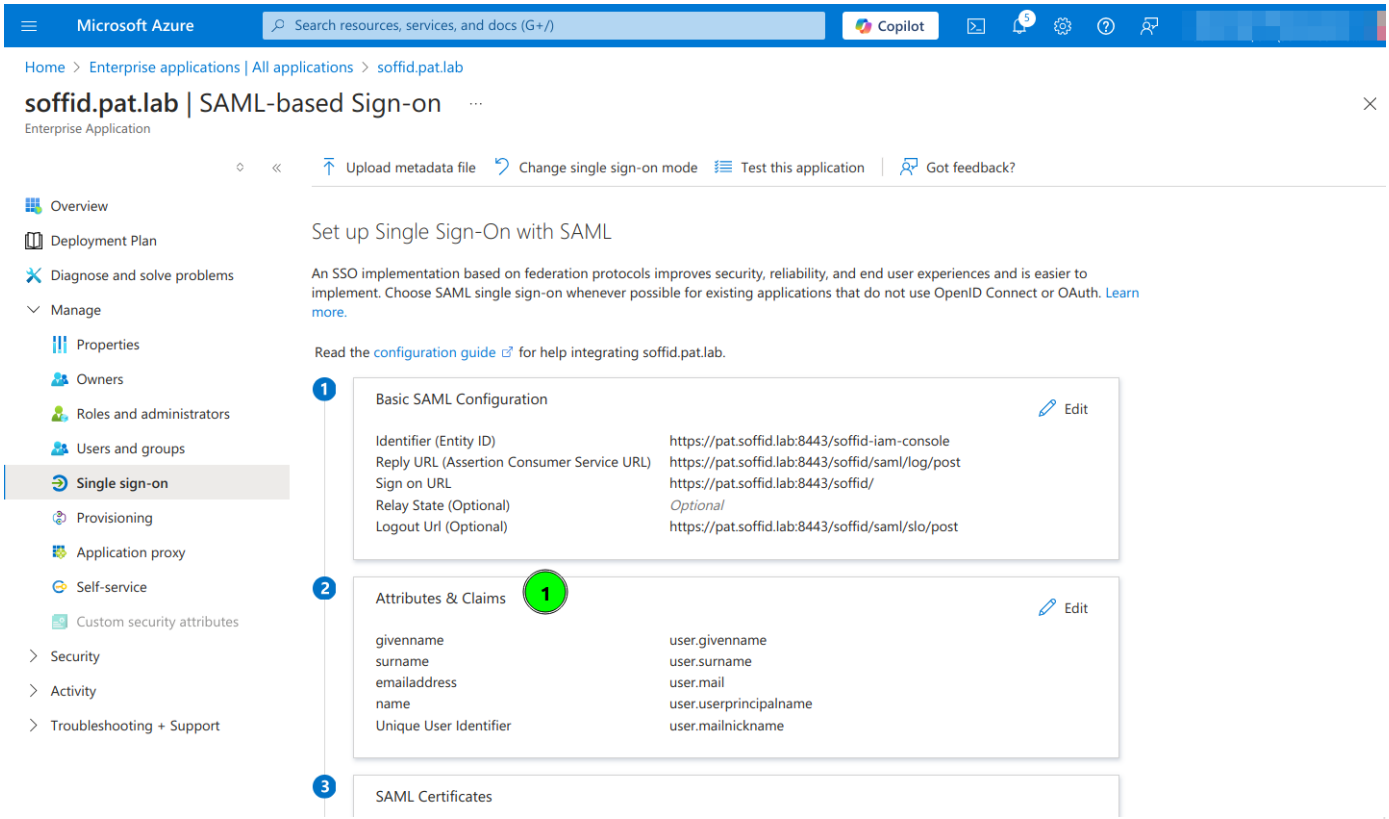
8. Enter the **Basic SAML Configuration** and Save:

- **Identifier**: https://<YOUR-SERVER>/soffid-iam-console
- **Reply URL**: https://<YOUR-SERVER>/soffid/saml/log/post
- **Sign on URL**: https://<YOUR-SERVER>/soffid/
- **Logout URL**: https://<YOUR-SERVER>/soffid/saml/slo/post





9. Configure **Attributes & Claims** and change the attributes and claims to send the mailnickname as the user identifier (nameid)



Attributes & Claims

Add new claim | Add a group claim | Columns | Got feedback?

Required claim

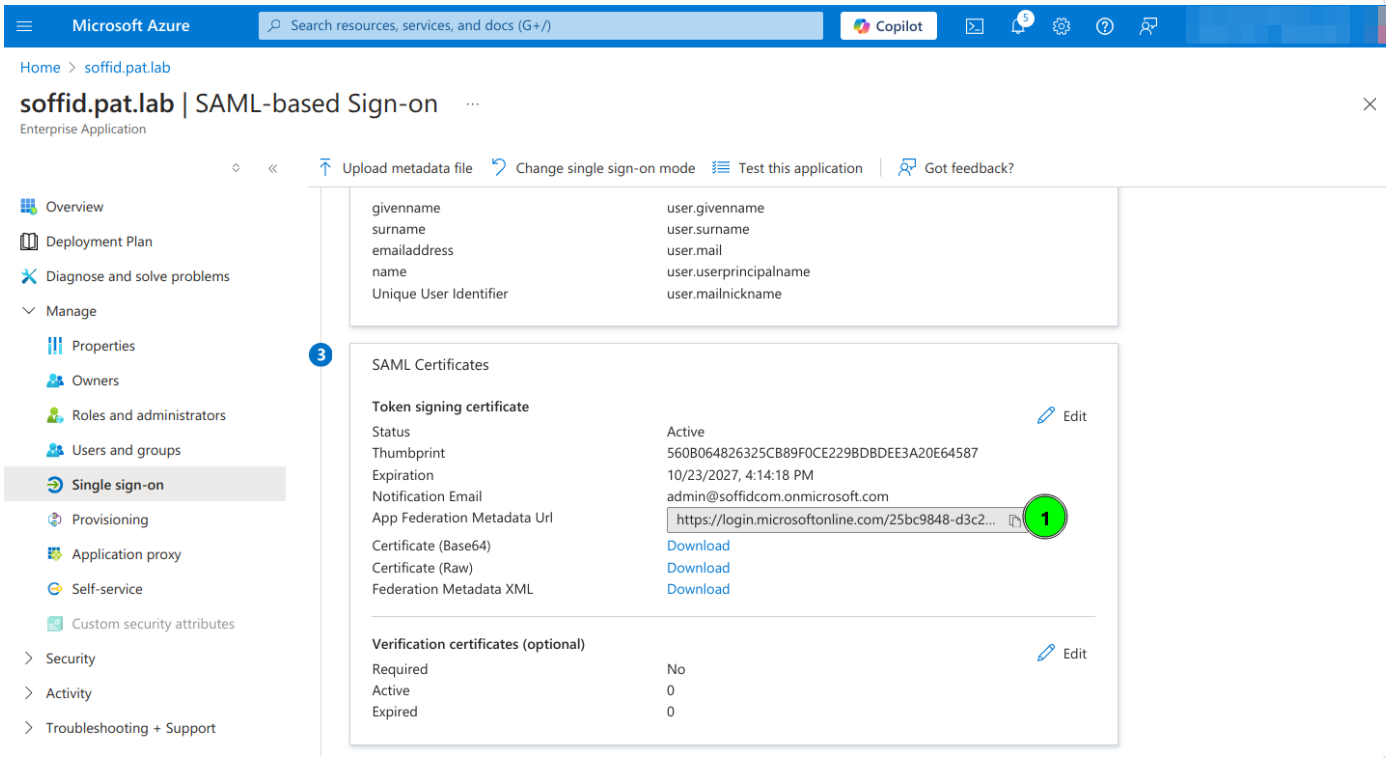
Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	1 user.mailnickname [nam...

Additional claims

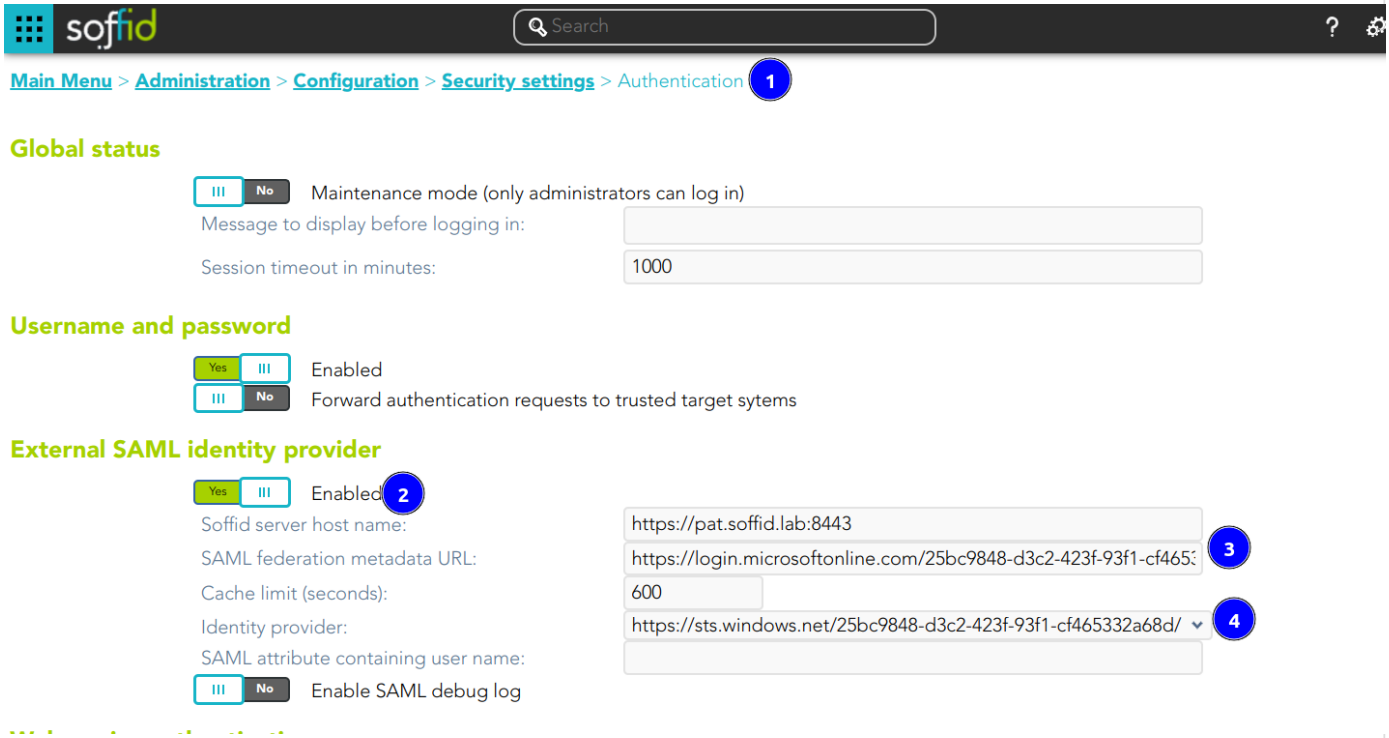
Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

Advanced settings

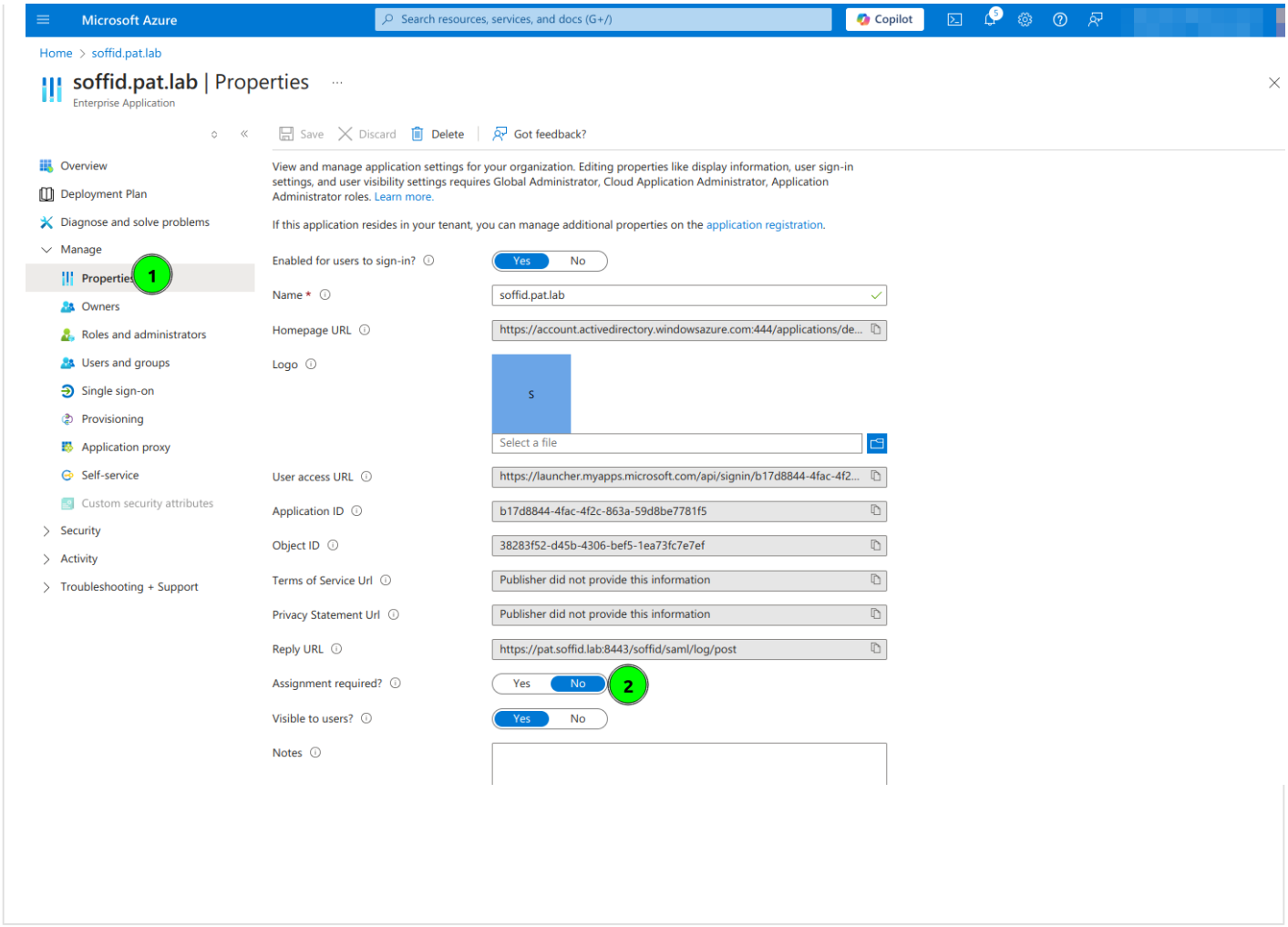
10. Copy the App Federation Metadata Url



11. Configure the **External SAML identity Provider** in the Soffid Console Authentication page



12. Optional, **enable any user to login**



API webservice authentication

Soffid allows you to configure the way to verify the identity of a user or system accesing to the Soffid Web Service, to ensure that only authorized entities can interact with the service.

> This webservice is included in the addon SCIM, it must be installed previously.

- **User name and password**: allows you to use user and password to access to the Soffid Web Service.
- **JWT token**: allows you to use JWT token to access to the Soffid Web Service.
- **JWT configuration URL**: URL where the jwks.json are available to download.
- **JWT issuer**: identifies the principal that issued the JWT.
- **JWT audience**: identifies the recipients that the JWT is intended for.
- **Maximum requests per user and minute**: maximum requests per user and minute.
- **Maximum global requests per minute**: maximum global requests per minute.
- **Maximum request size**: maximum request size.

> Bear in mind that the Identity Provider needs to have enabled the OpenID profile.

> Also, the Identity Provider cert must be in the Console cacerts.

Enable LinOTP integration

Soffid allows you to use an external OTP, LinOTP in this case. If you decide to use LinOTP, Soffid could be configured to request the user to authenticate using a second factor authentication to perform certain actions. In another case, you can use the Soffid OTP.

- **Enabled:** check it (select value Yes) to use an external SAML Identity Provider.
- **LinOTP server URL**: URL of your LINOTP service.
- **LinOTP admin username:** username of the admin account used by Soffid.
- **LinOTP admin password**: password of the admin account used by Soffid.
- **LinOTP users domain**: the user's domain for LinOTP authentication. The selected user domain will guess the LinOTP username for any Soffid identity. It is extremely important when LinOTP users do not match Soffid usernames. Please visit the Account naming rules page for more information

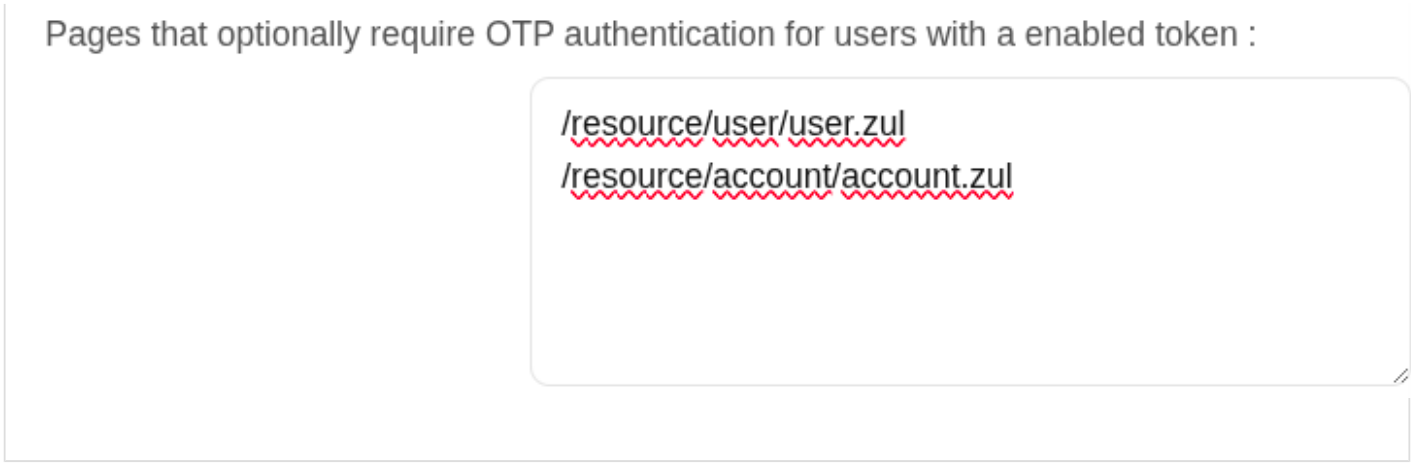
> If you want to configure the **Soffid OTP** you could visit Two factor authentication (2FA) chapter.

Second Factor Authentication configuration

- **Pages that optionally require OTP authentication for users with an enabled token**: (Optional) If a URL optionally requires OTP authentication, and the user does not have any OTP token, access will be granted. Otherwise, if the user has an OTP token, the OTP value will be required, and no access will be allowed until the user provides the right token value.
  - You can include the list of pages to include the two factors only for the users with the token.

Example

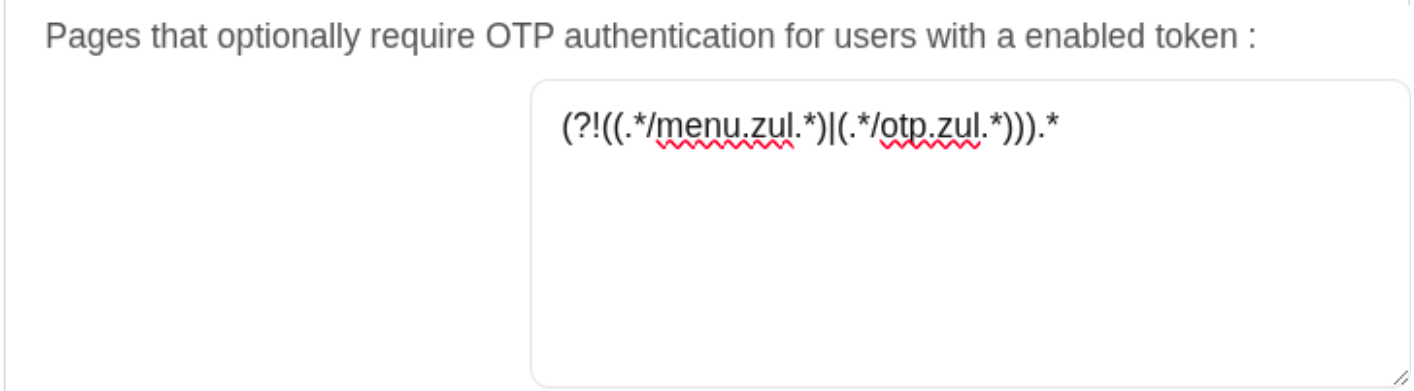
Request only the OTP for these pages:



- You can add a regular expression to determine the list of pages to always include the second factor to the users with the token

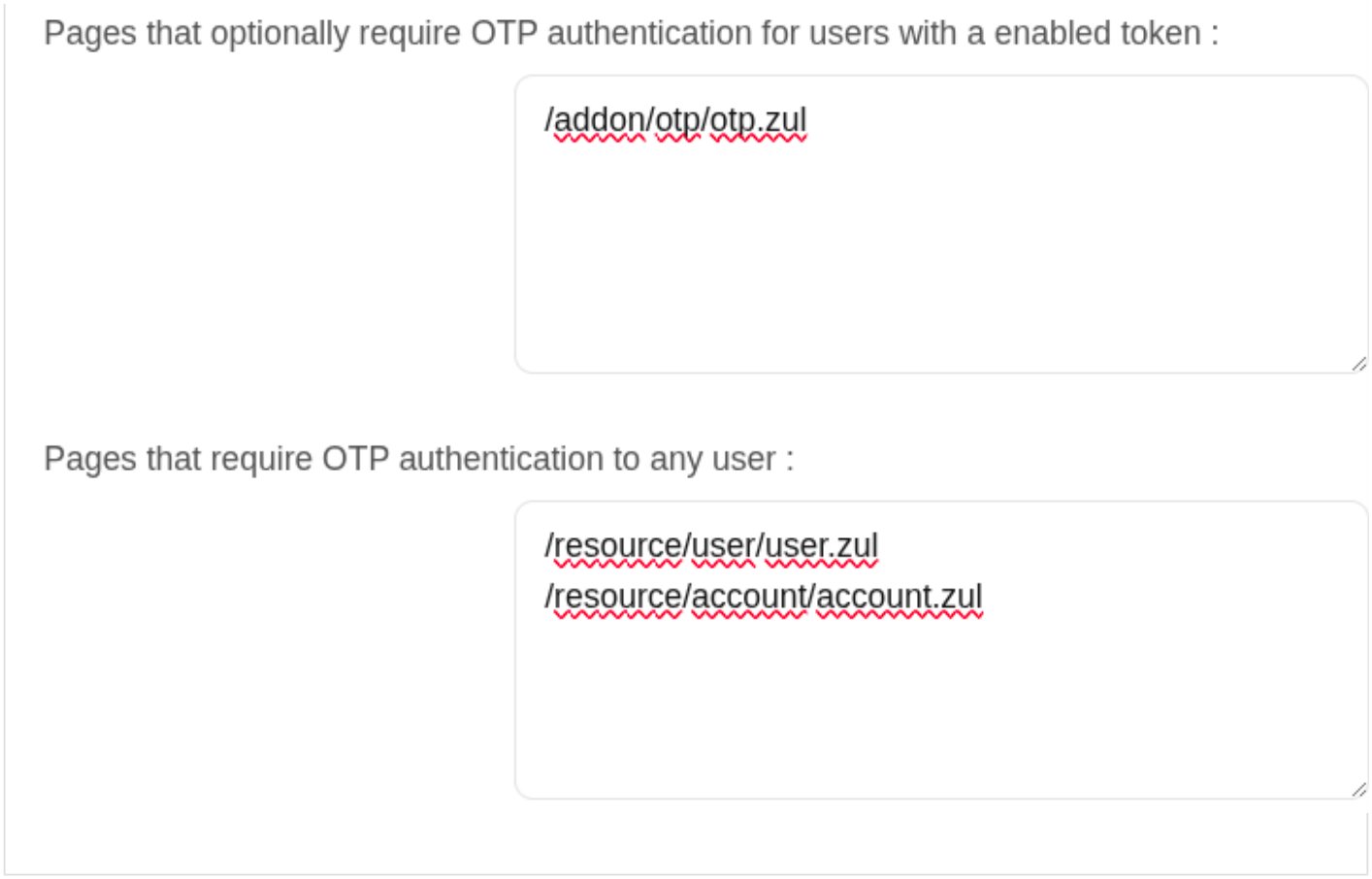
Example

Request OTP for all pages except those containing menu.zul or otp.zul:



- **Pages that require OTP authentication to any user**: (Mandatory) You should include the list of pages to always include the second factor to the users with the token. Therefore, if a URL strictly requires OTP authentication, users with no token won't be allowed to use them.

Example



- **Second factor authentication period**: number of seconds after that, a new OTP value will be required.

In both configurations, if OTP is required by the user, a popup requesting the token value is raised to write the OTP value.

Actions

Expand all	Displays all the attributes of the different blocks.
Collapse all	Hide all attributes of the different blocks.
"Types of views"	Change the view type: Classic view, Modern view, Compact design.
Download metada	Allows you to download an XML file with metadata to load it into your SAML Identity Provider federation when you use an External SAML identity provider
Confirm changes	Allows you to save the changes made in the Authentication setup.

Revision #10
Created 19 July 2025 12:08:14 by Sion Vives

Updated 22 September 2025 13:01:06 by Sion Vives