Security settings

- Authorizations
- Authentication
- Password policies
- Configure PAM session servers
- PAM Rules
- PAM Policies
- Password recovery configuration
- OTP settings
- XACML Policy Management
- XACML PEP configuration
- Digital certificates
- Recertification policies
- Issue policies
- Break-glass recovery configuration

Authorizations

Definition

> Soffid console provides a granular access control system. That granular control system allows the administrator user to assign granular permissions to roles. Be in mind that some permissions may inherit some other permissions.

You cannot assign permissions directly to users. Instead, permissions are assigned to roles and roles are assign to users, either directly or through grant inheritance.

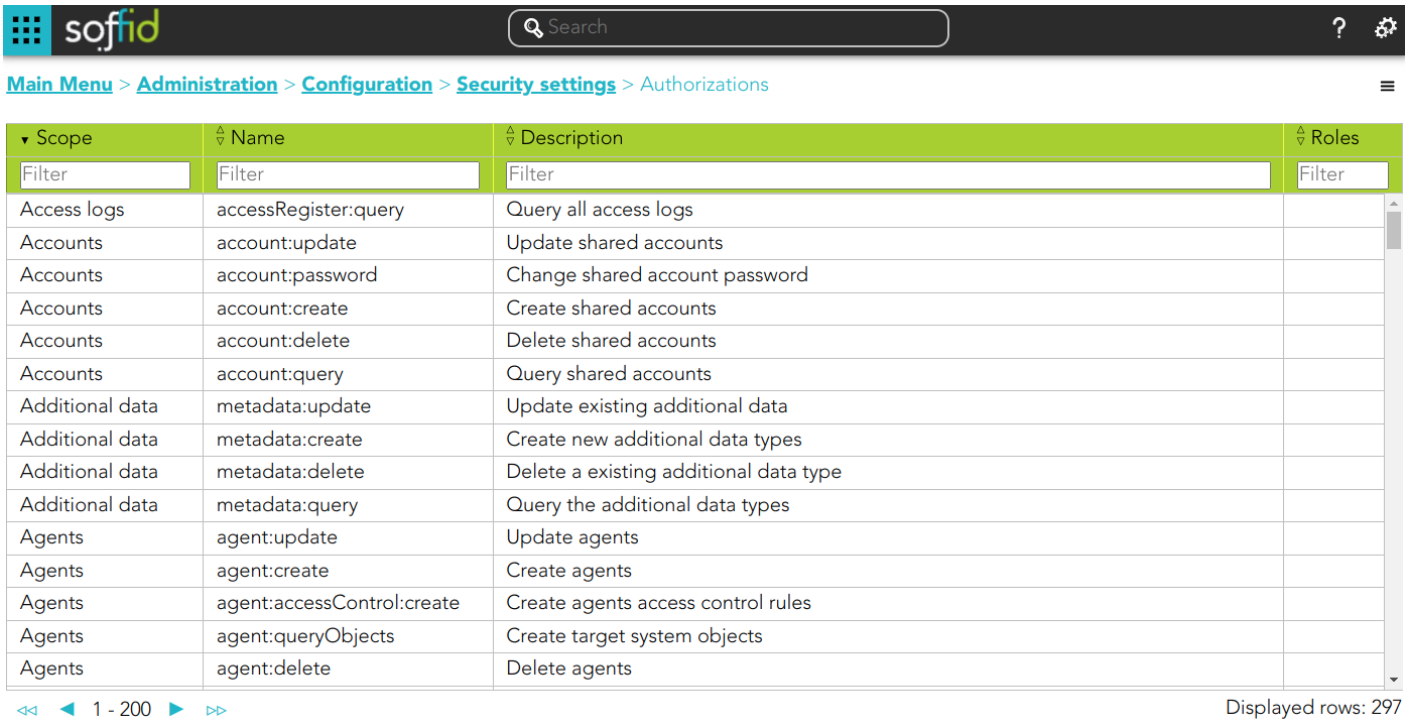
The roles may be created into Soffid application system, but could also be included in any other application system.

Permissions are grouped into permission scopes. Most scopes are Soffid object types, but there are one special scope named Soffid, that applies to Soffid console web pages.

Addons can create their own authorizations that automatically will appear at this screen. When a new addon has been installed and applied, the first thing to do use to be assign permissions for this new addon. In fact, administrators won't be able to manage the addon unless the log out and log in to get the newly created permissions.

The permissions given to roles and the roles given to users are cached by Soffid. In order to reapply permissions, the user should close its session and log-in again

Screen overview



Related objects

1. **Roles**
2. **Information system**

Standard attributes

- **Scope**: scope of application.
- **Name**: name of the granular permission.
- **Description**: brief description of the granular permission.
- **Roles**: role list assigned to that granular permission.
- **Description**: role description
- **Information system**: asset or application, from a functional point of view.
- **Target system**: target system name.
- **Domain**: the role is limited to that scope.

Actions

Authorization query action

Import	Allows you to upload a CSV file with the authorization data to add or to update the granular control system. If they exist, the values of the CSV file will prevail. First, you need to pick up a CSV file, that CSV has to contain a specific configuration. Then you need to check the contents. And finally, you need to select the mappings for each column of the CSV file to import the data correctly and to click the Import button.
Download CSV file	Allows you to download a CSV file with the authorization data.

Authorization detail actions

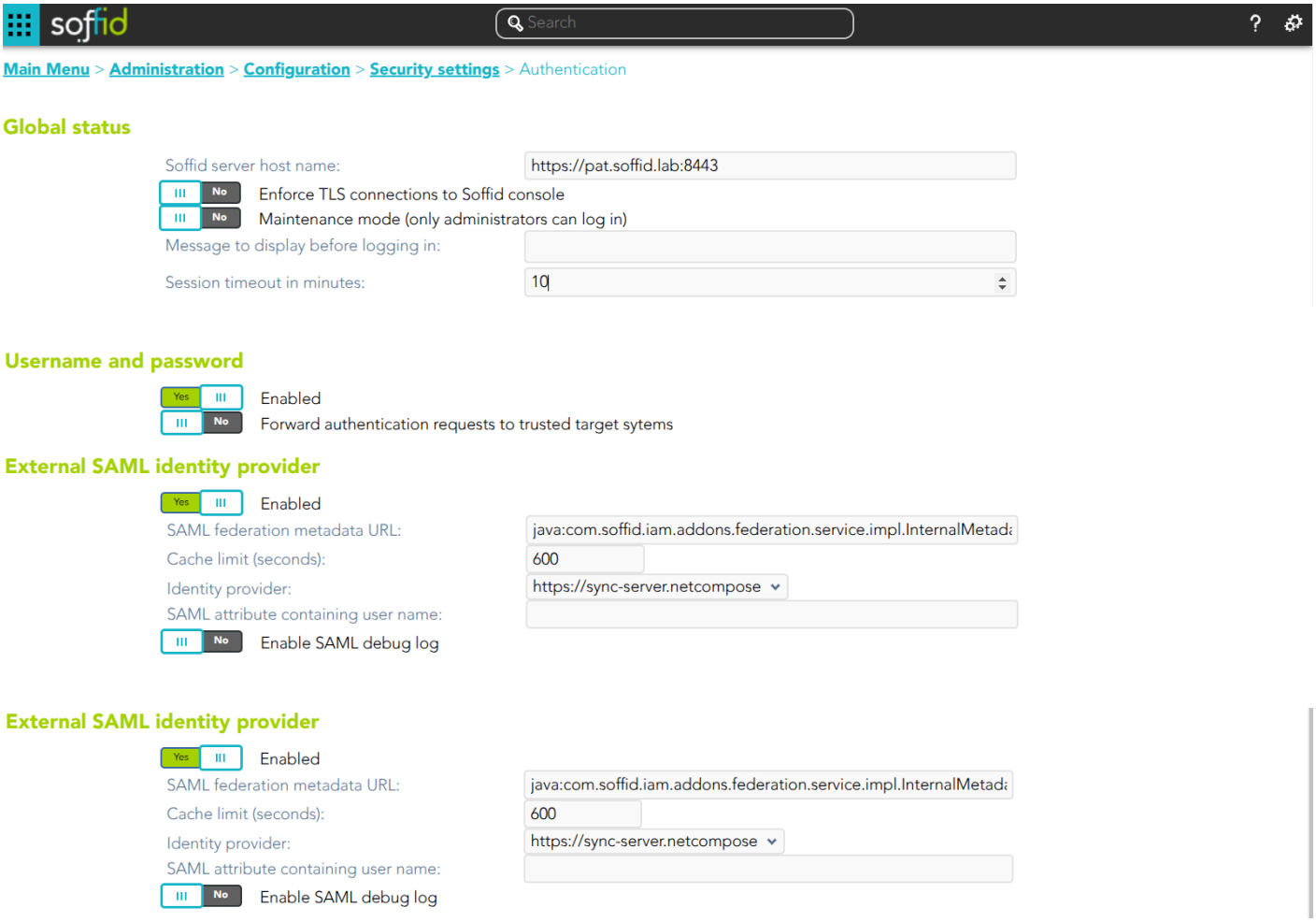
Add new	Allows you to add a new role to the authorization. You can choose that option clicking the add button (+). First, you need to search a role writing the role name on the field, and Soffid will show the values related. Second, you can select one or more roles and accept. And finally, you need to apply changes to save the roles added. If you cancel that action, no role will be assigned.
Delete	Allows you to delete one or more roles from an authorization. To delete one role, you need to click the subtraction symbol (-), located at the end of the row, of the role which you want to delete and then apply changes. To delete more than one role, you can select the roles which you want to delete and there click the subtraction symbol (-) and then apply changes. It is mandatory apply changes to save the roles deleted. Soffid will ask you for confirmation to perform that action, you could confirm or cancel the operation.
Apply changes	Allows you to update the changes made on the authorization.
Undo	Allows you to quit without applying any changes.

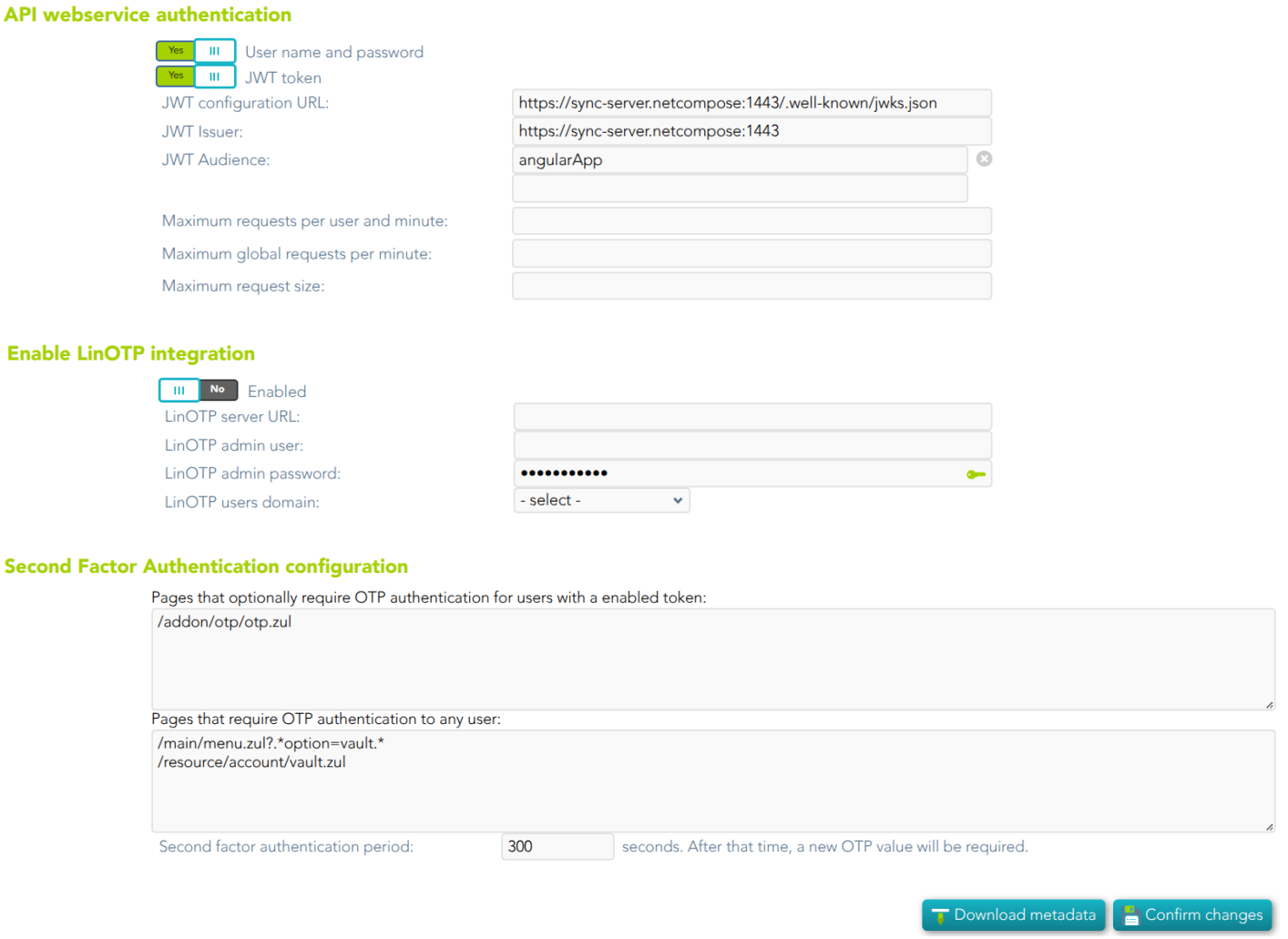
Authentication

Definition

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

Screen overview





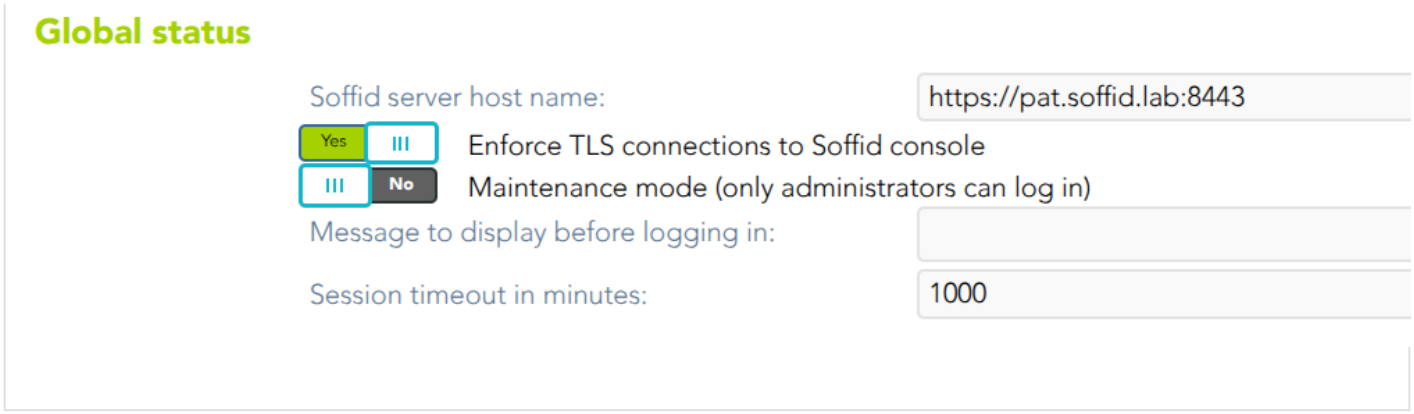
Standard attributes

Global status

- **Soffid server host name**
- **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.

Image



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

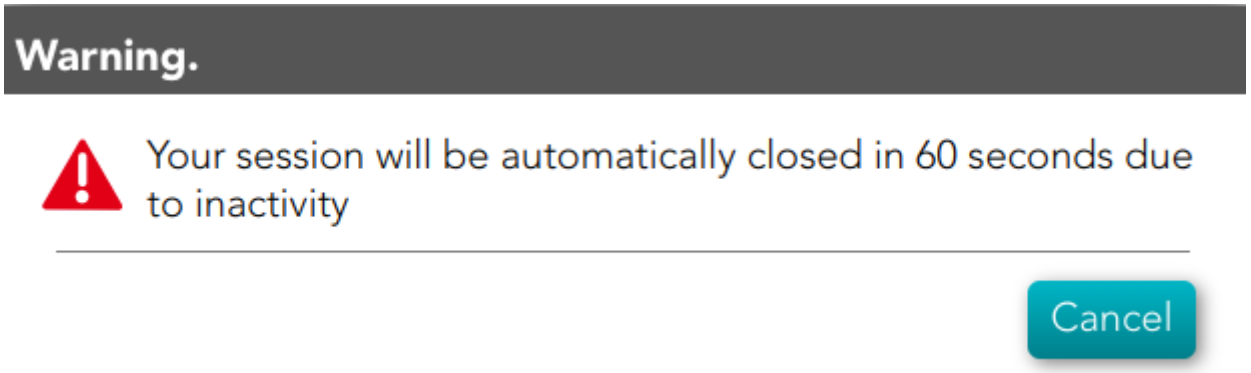
Image

- **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 seconds 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. (Available since console version 3.5.26)

Image



Username and password

Internal

- **Enabled**: the only one 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.

External

- **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.

> Not all the external systems are included, only the ones that have marked the check "Trust password" on the agent. For more information about agents please visit the Agents page.

Once an agent is configured, Soffid will still use its internal tables to authenticate usernames and passwords.

If the password entered by the user does not match, the Soffid core will issue a "ValidatePassword" task for each trusted target system. If any of the trusted target systems accepts the password, it will be hashed and stored in Soffid tables and login will be accepted.

External SAML identity provider

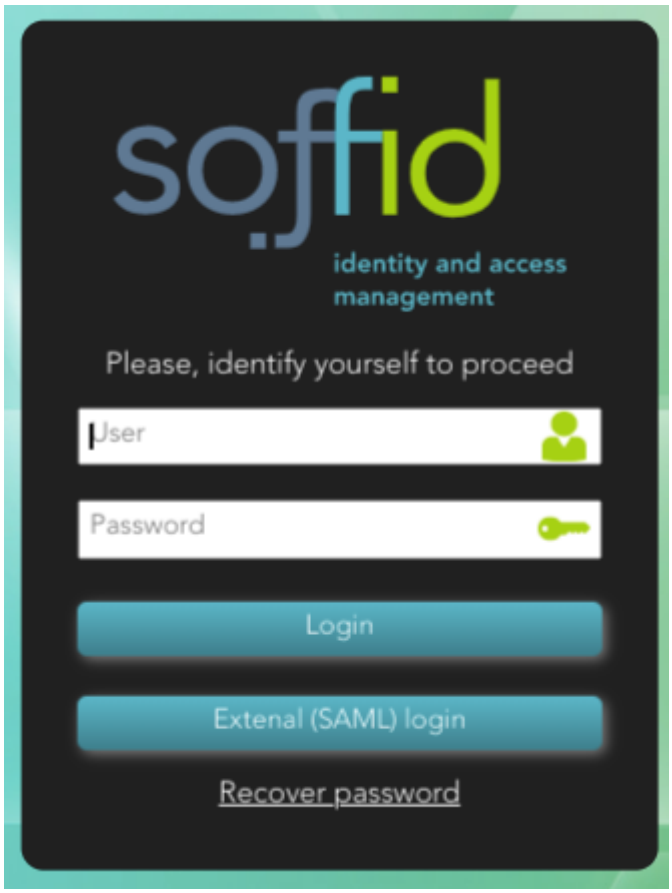
It should be noted this feature does not depend on the federation addon. That is a feature included by default in the Soffid smart engine to allow you to include in the authentication flow a mechanism to use a third-party SAML system.

- **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**: 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.

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

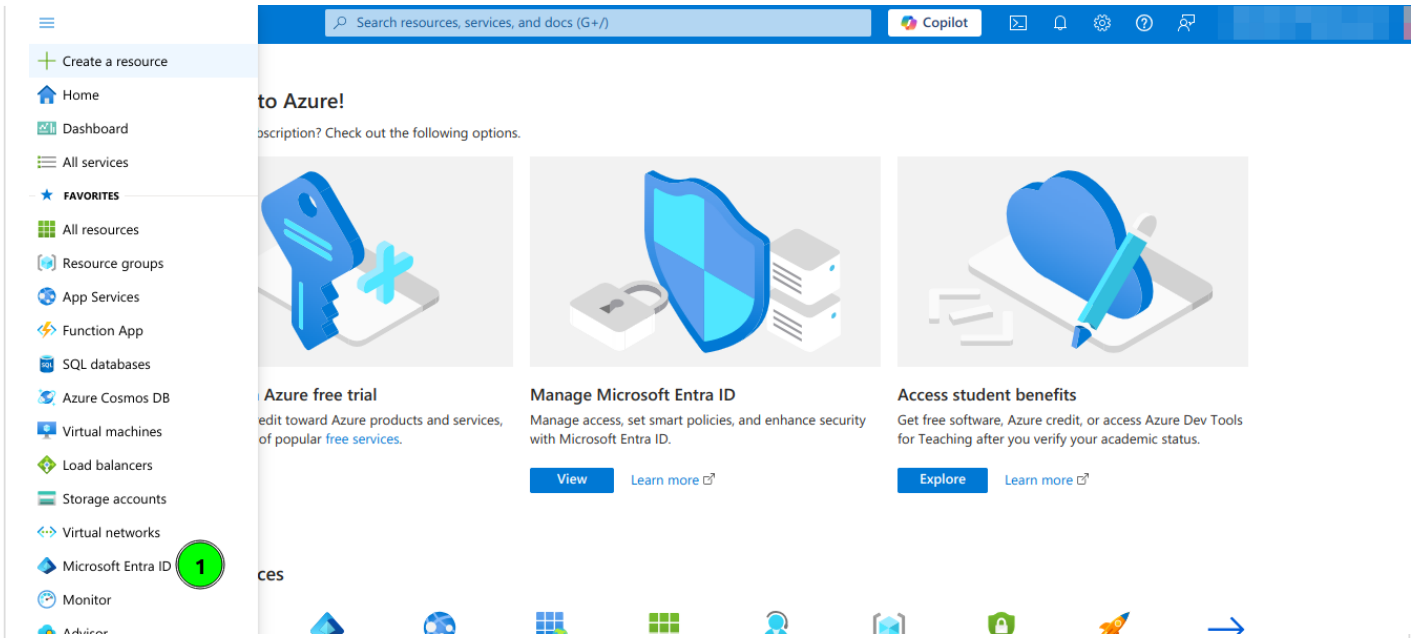
Introduction

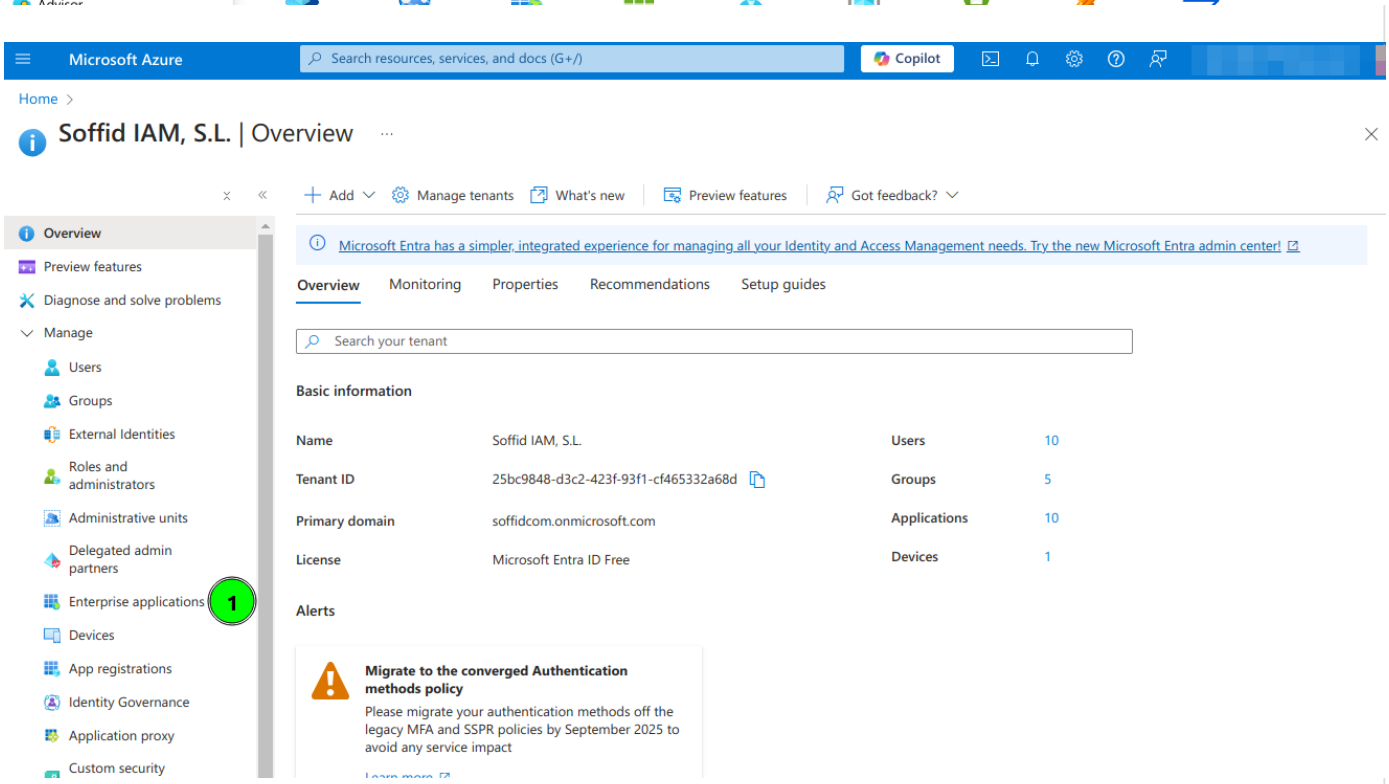
Steps to configure Office 365 as External SAML identity provider.

Step-by-Step

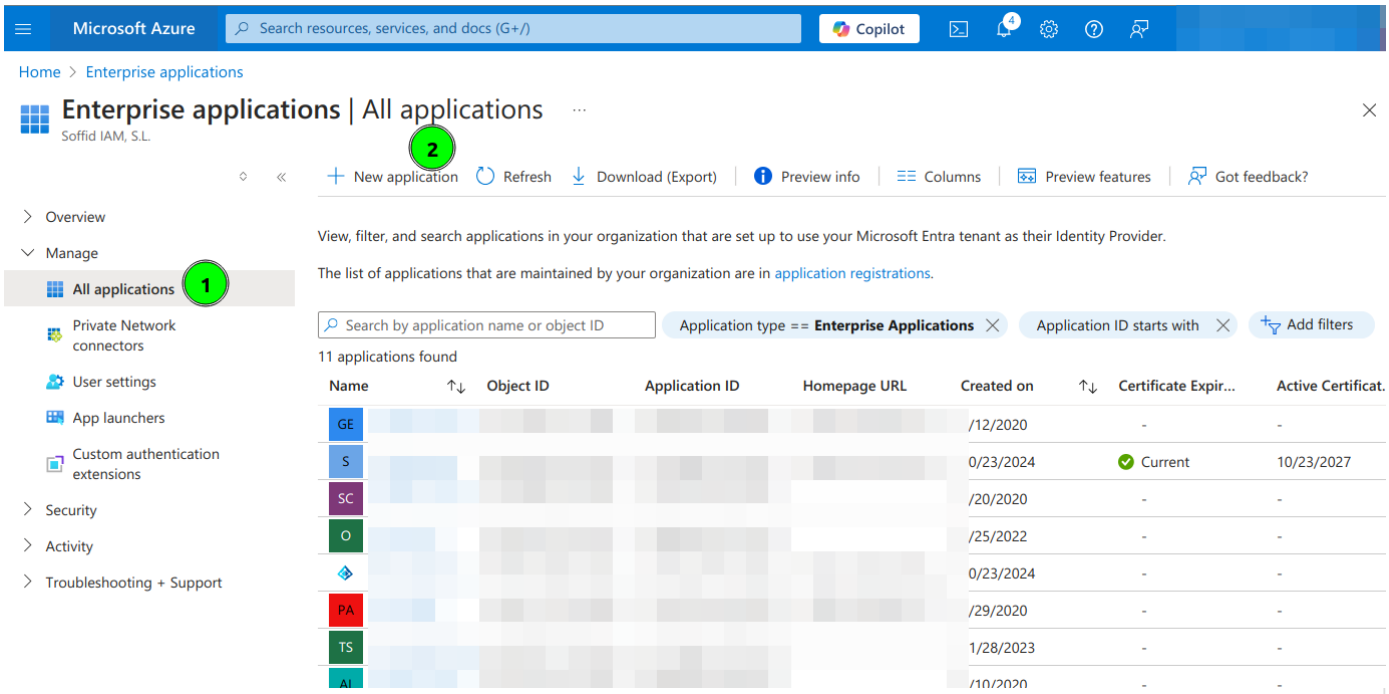
1. Open a https://portal.azure.com

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

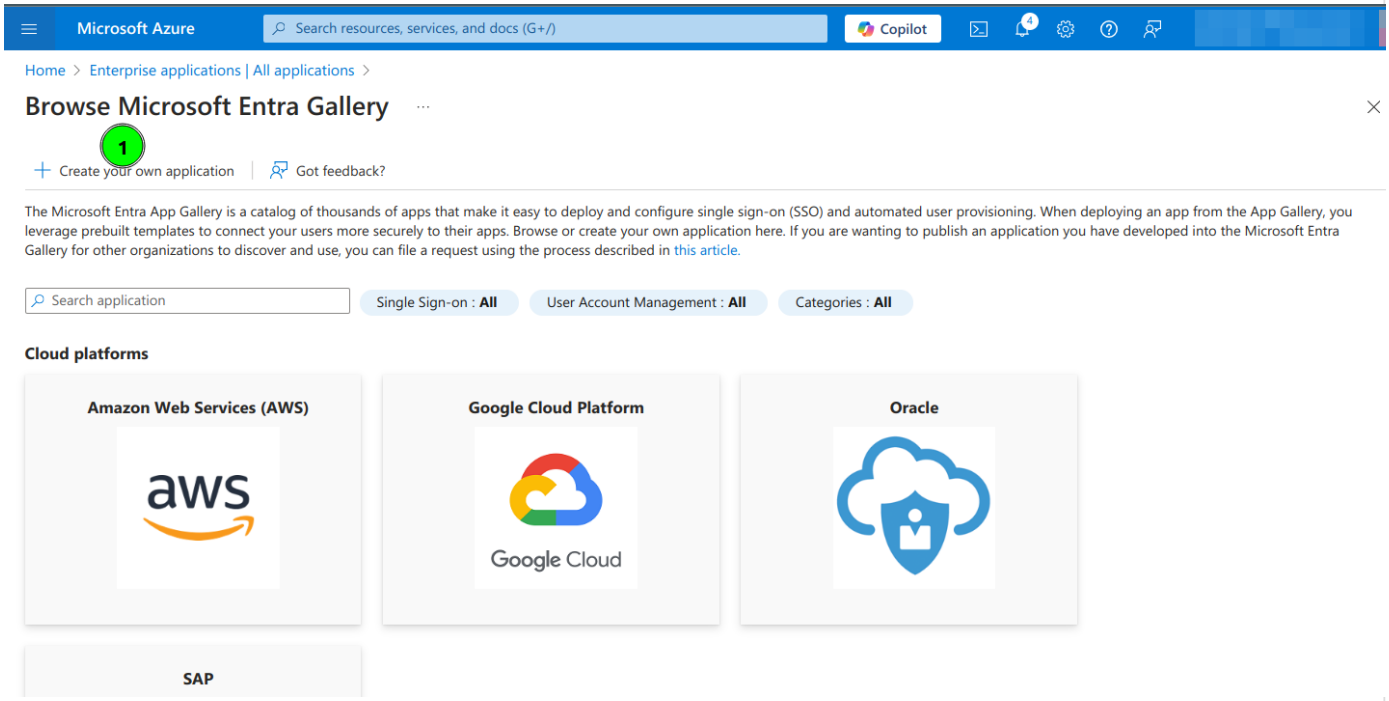




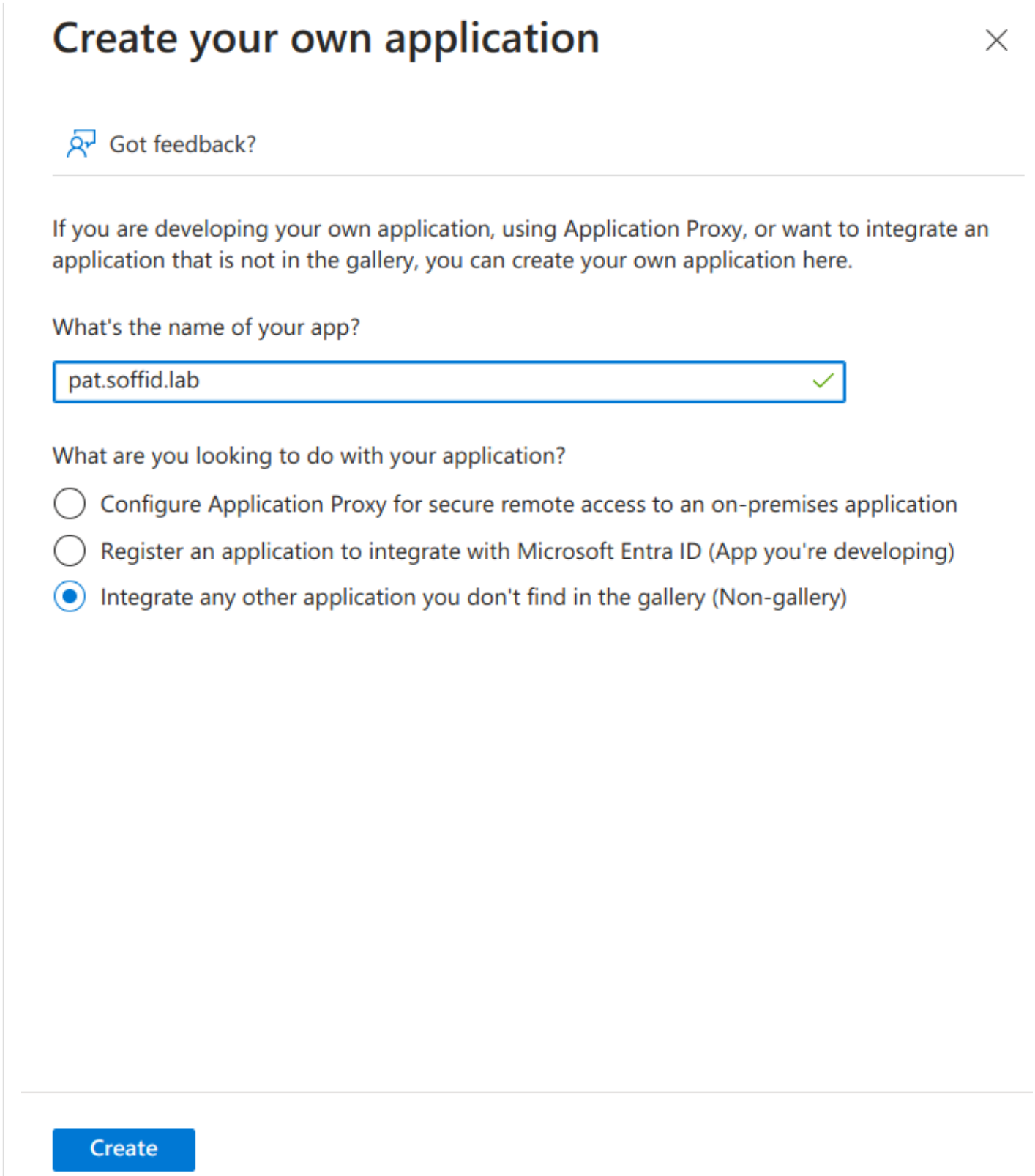
3. Select **All applications** and click **New Application**



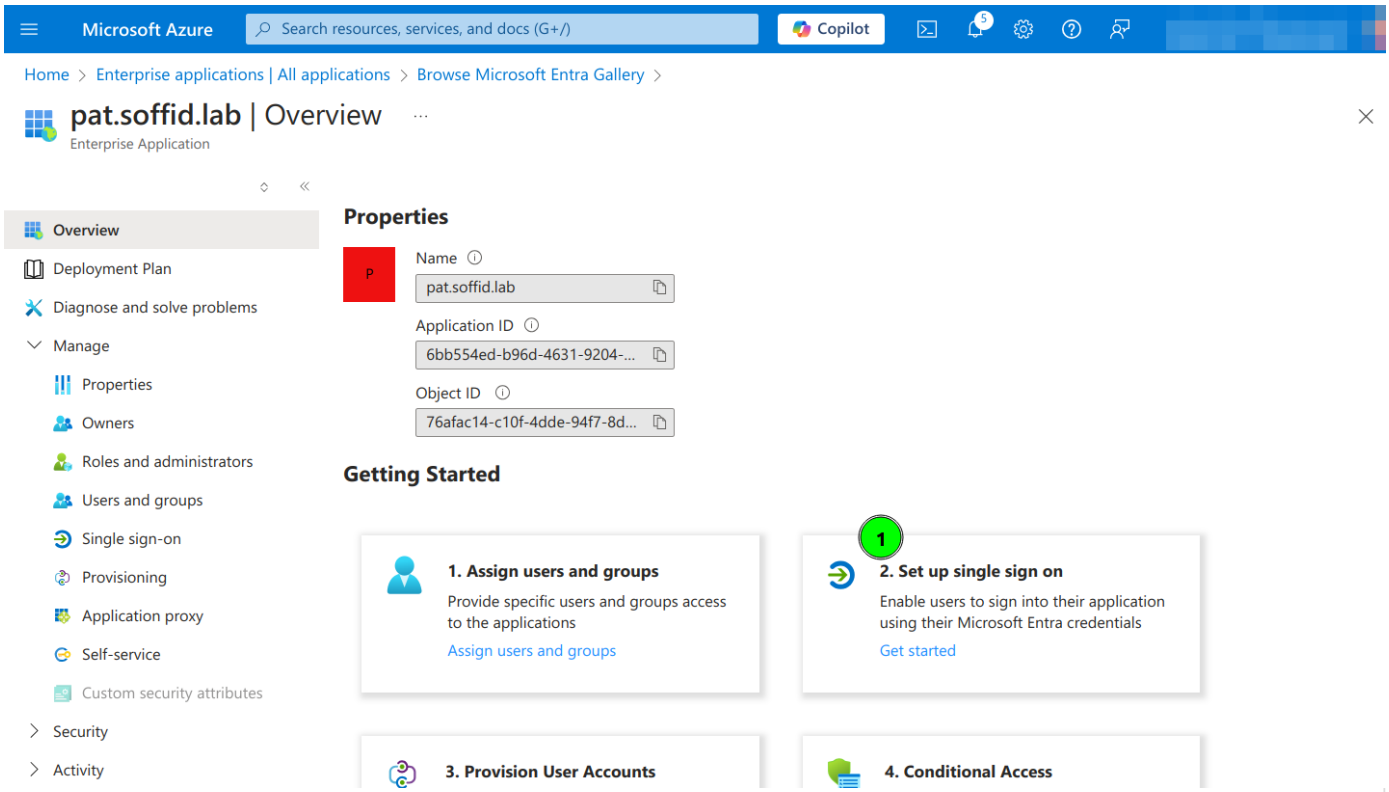
4. Select Create your own application



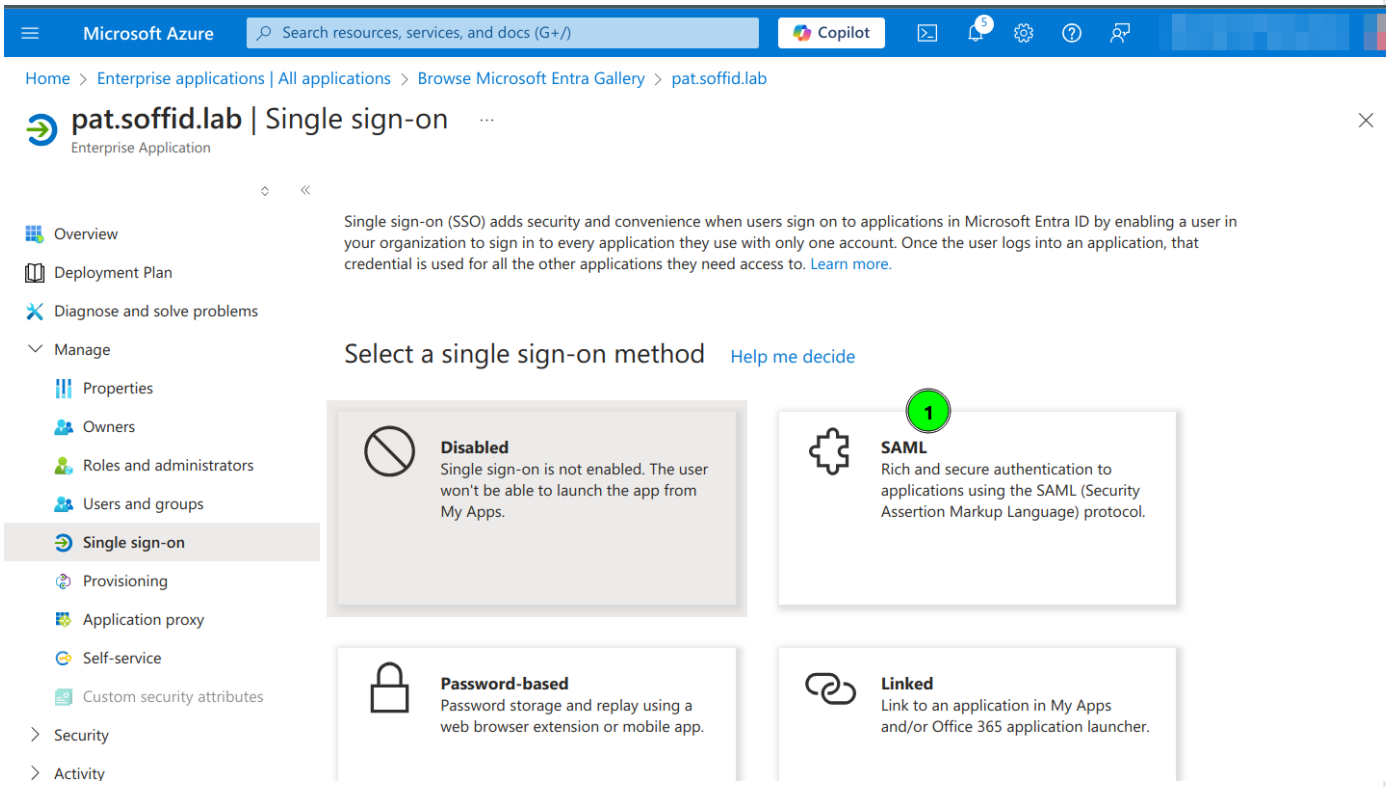
5. Type the name of your app and select the "Integrate any other application you don't find in the gallery (Non-gallery)" option



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

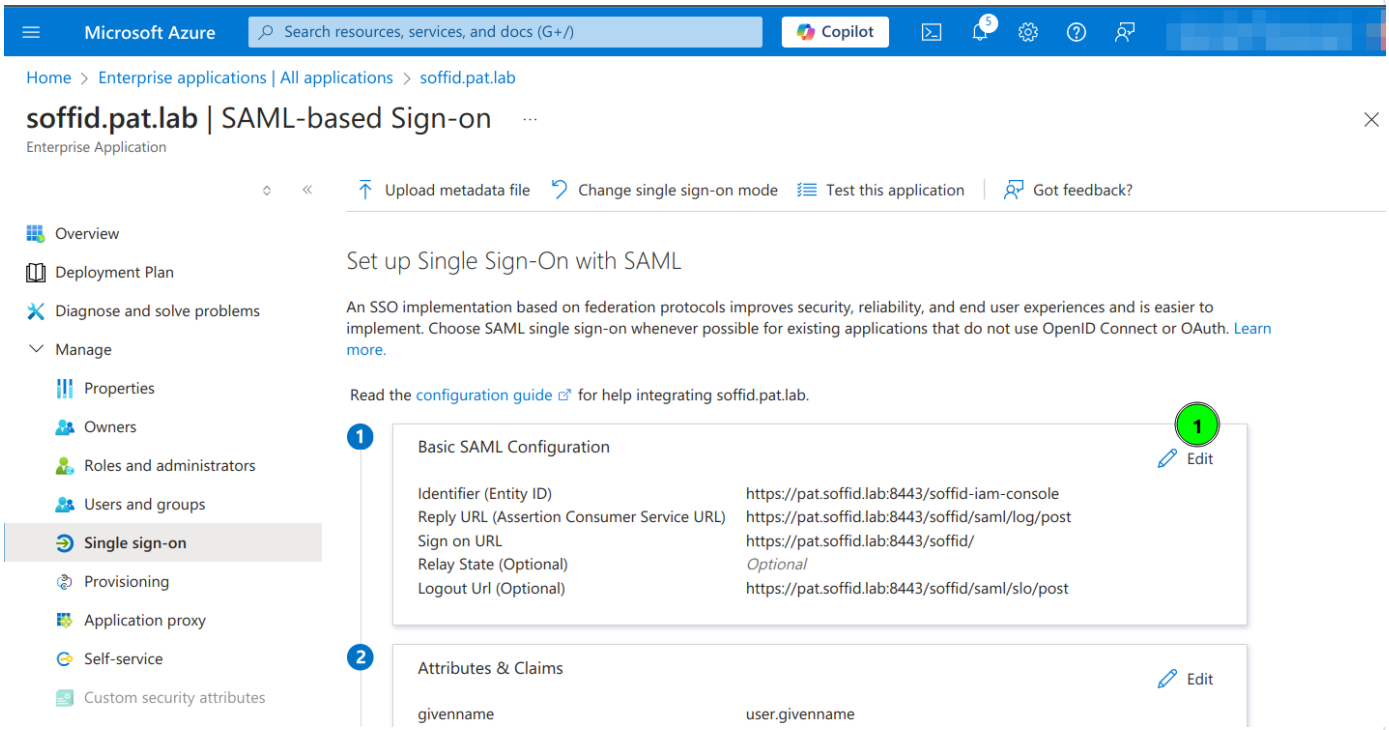


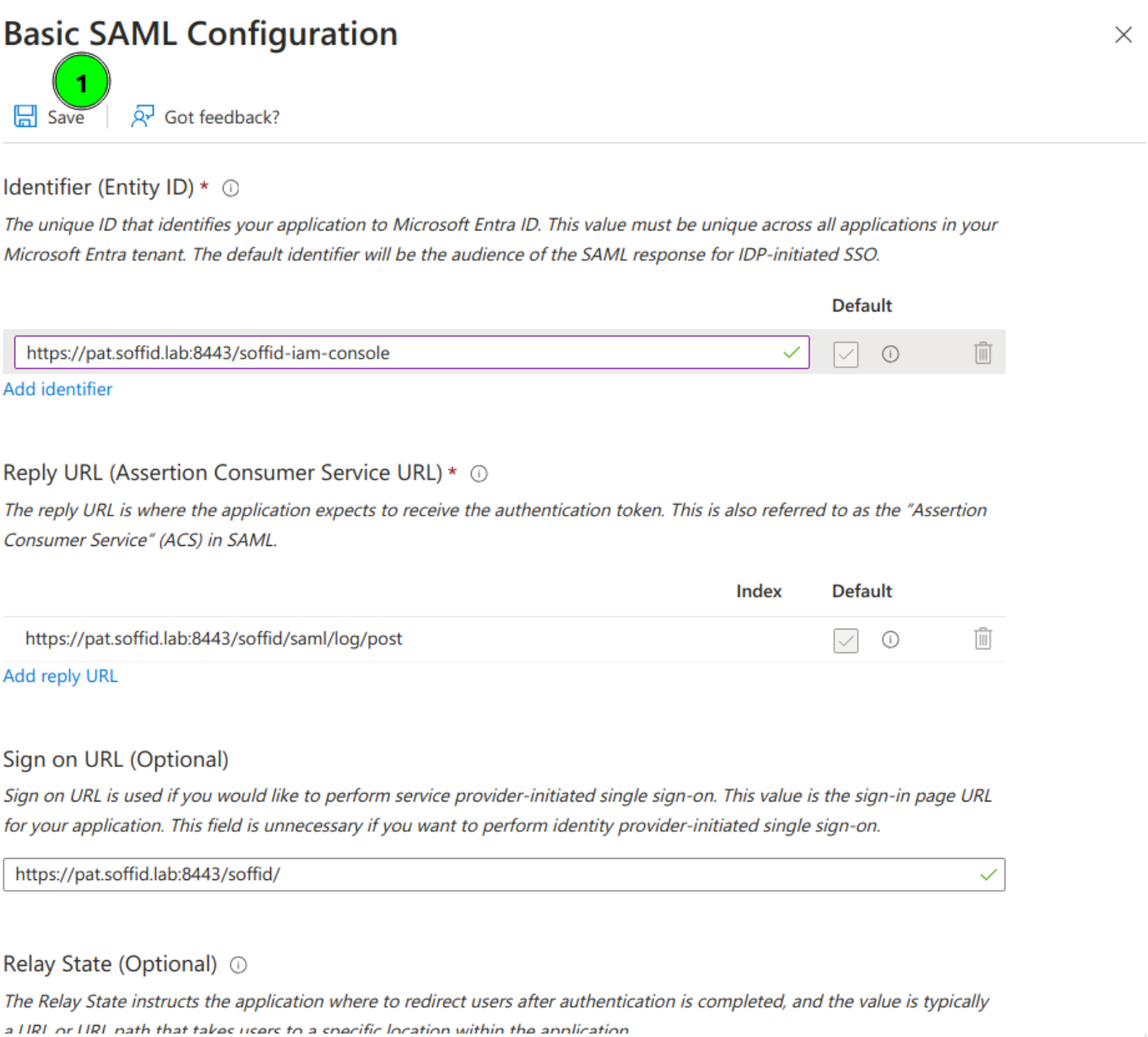
7. Click the **SAML** option



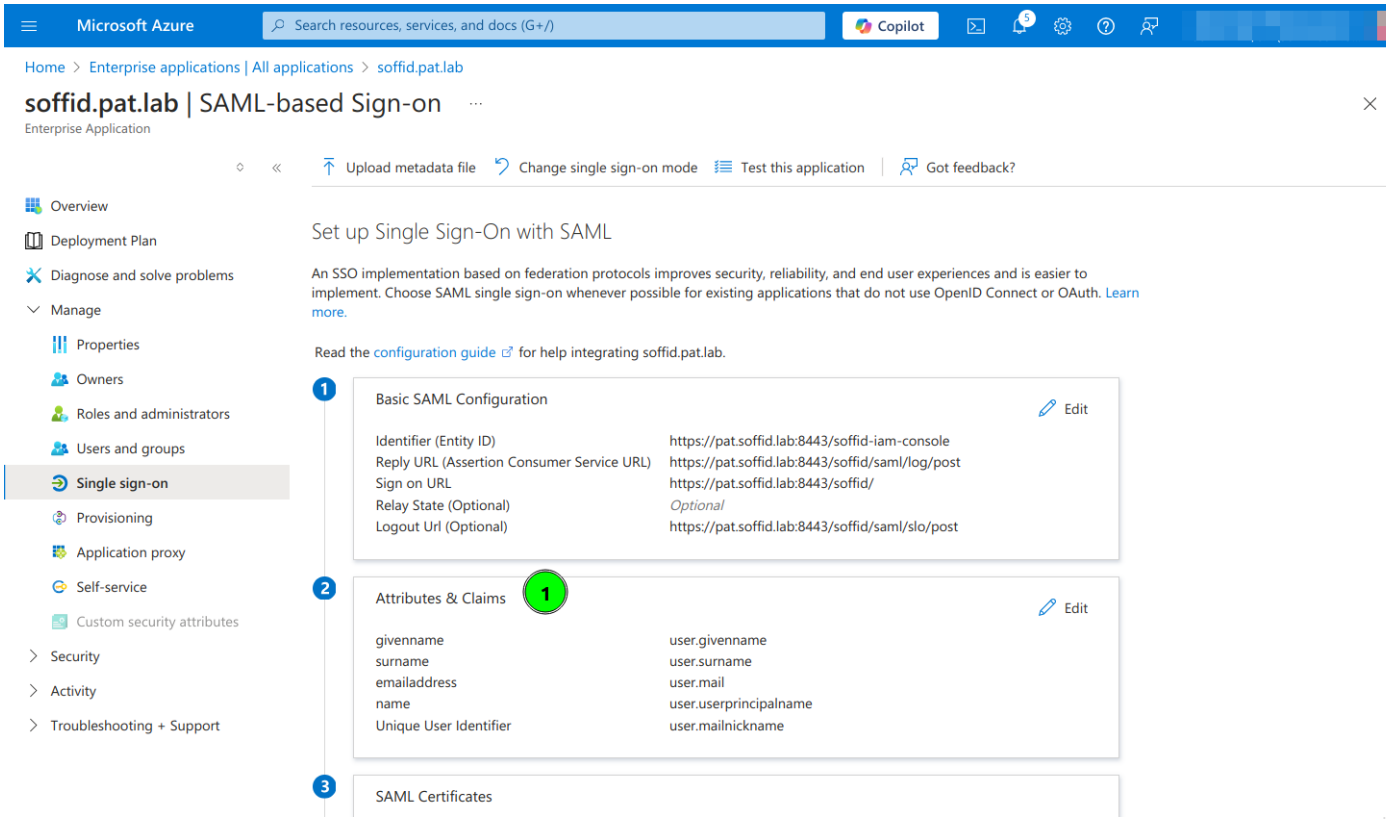
8. Enter the **Basic SAML Configuration** and Save:

- **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

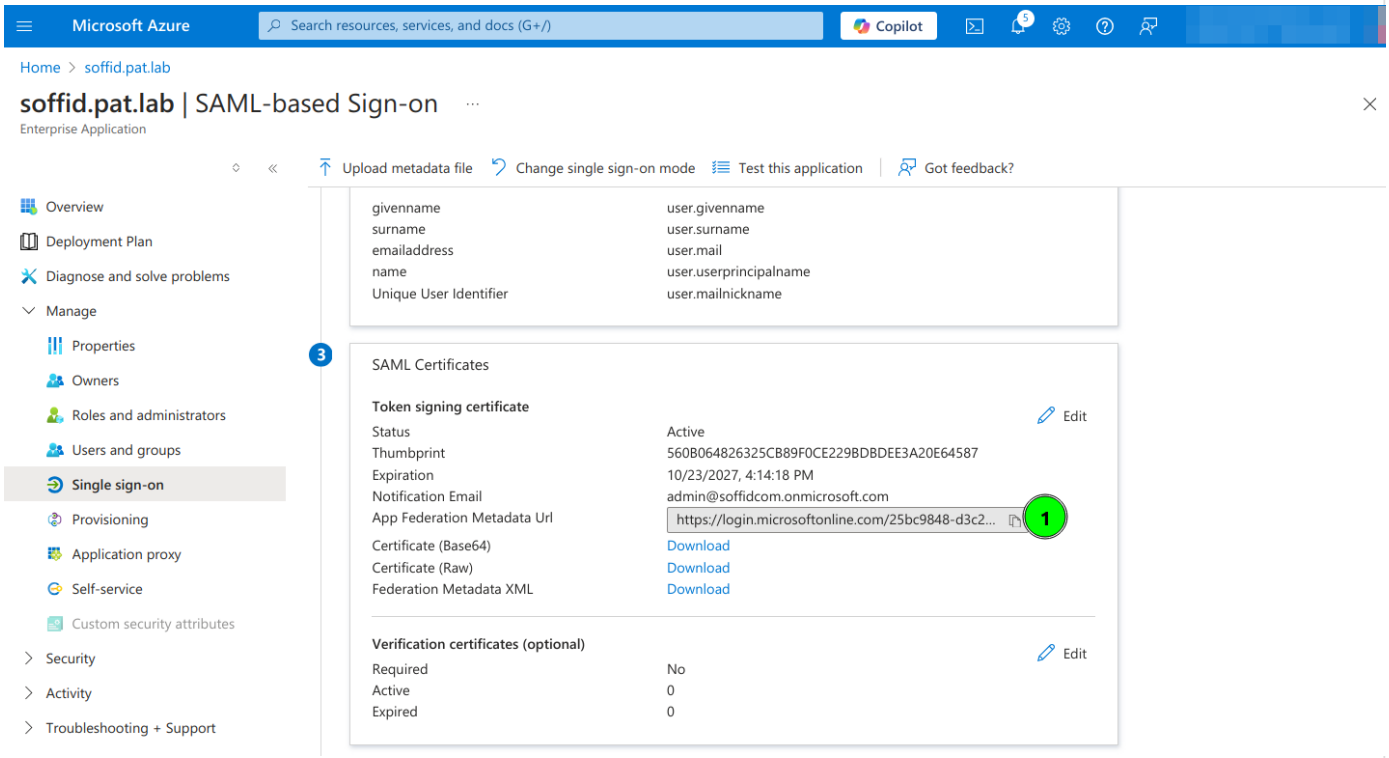
Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	1 user.mailnickname [nam...

Additional claims

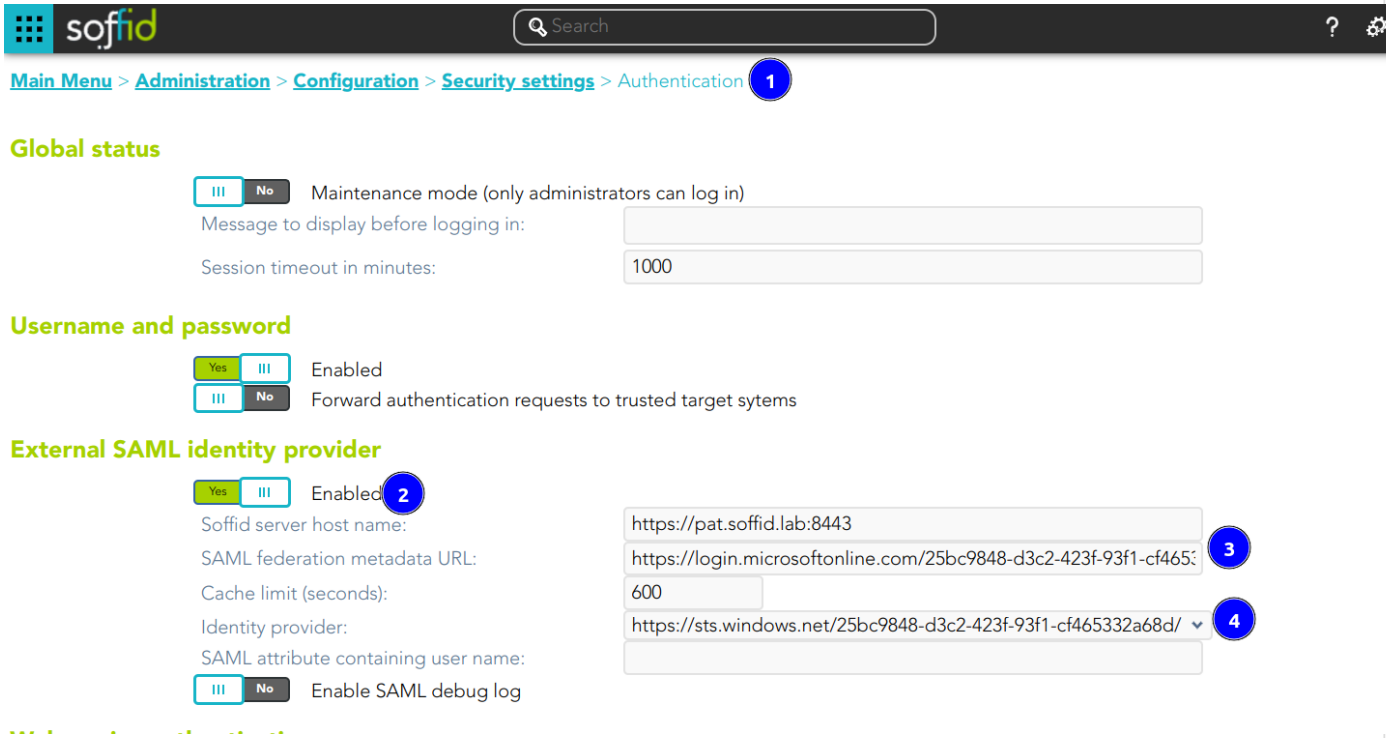
Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname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

Advanced settings

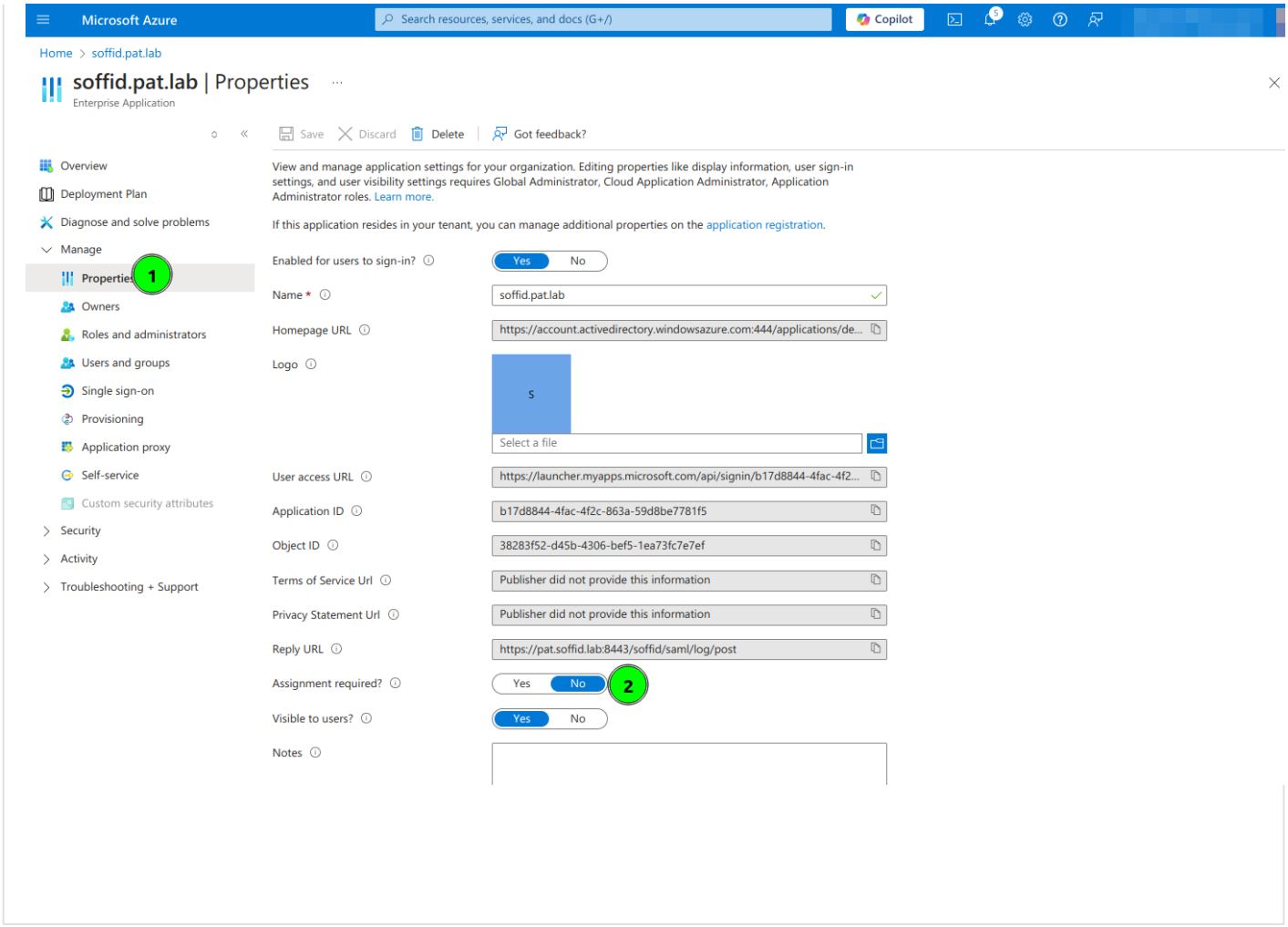
10. Copy the App Federation Metadata Url



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



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



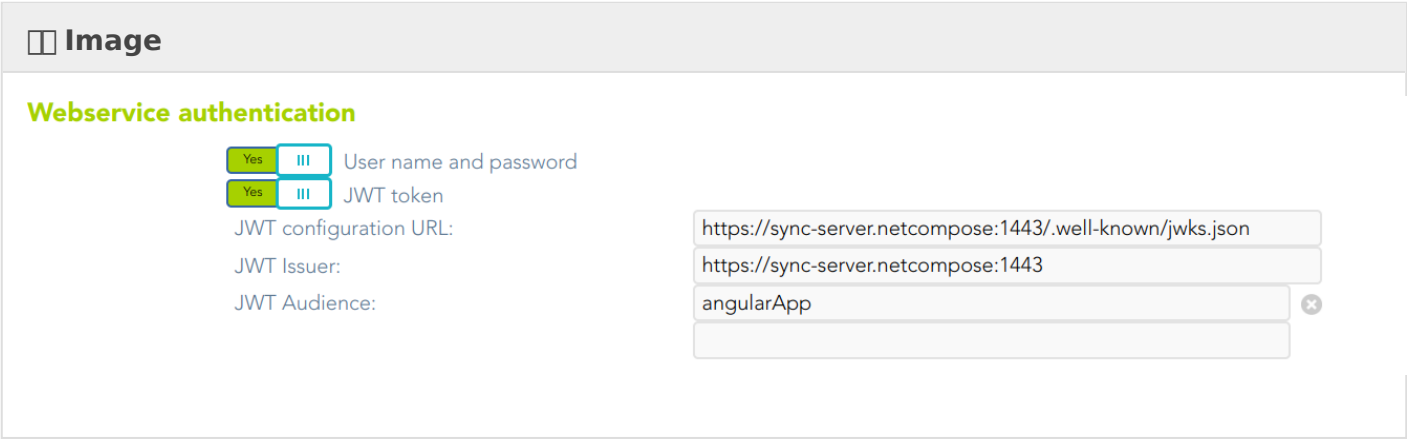
Webservice authentication

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

- **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.

> 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

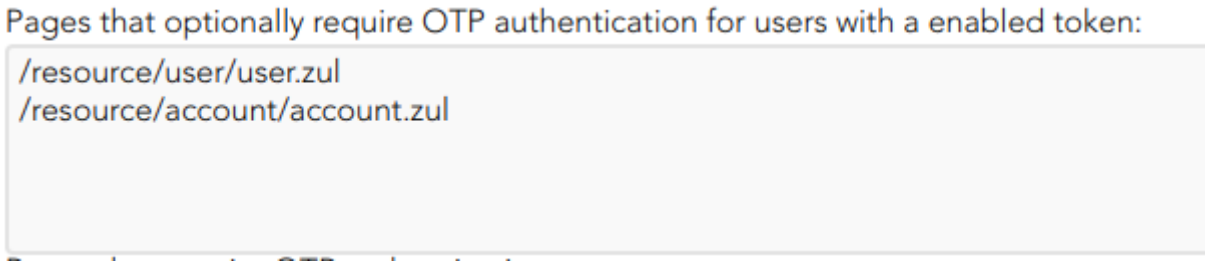
> If you want to configure the **Soffid OTP** you could visit Two factor authentication (2FA) chapter.

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

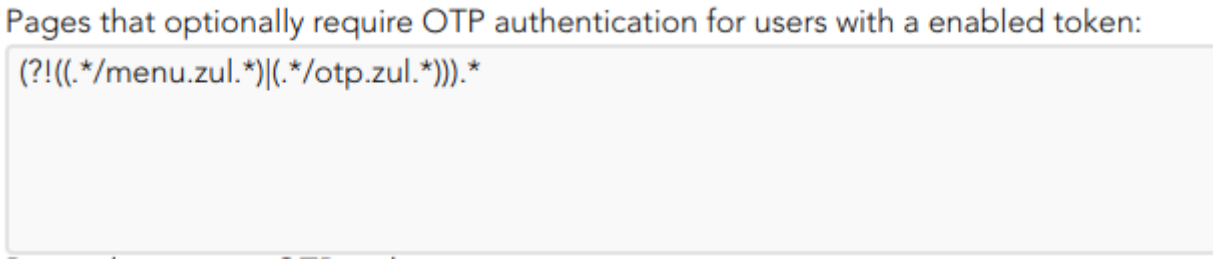
Request only the OTP for these pages:



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

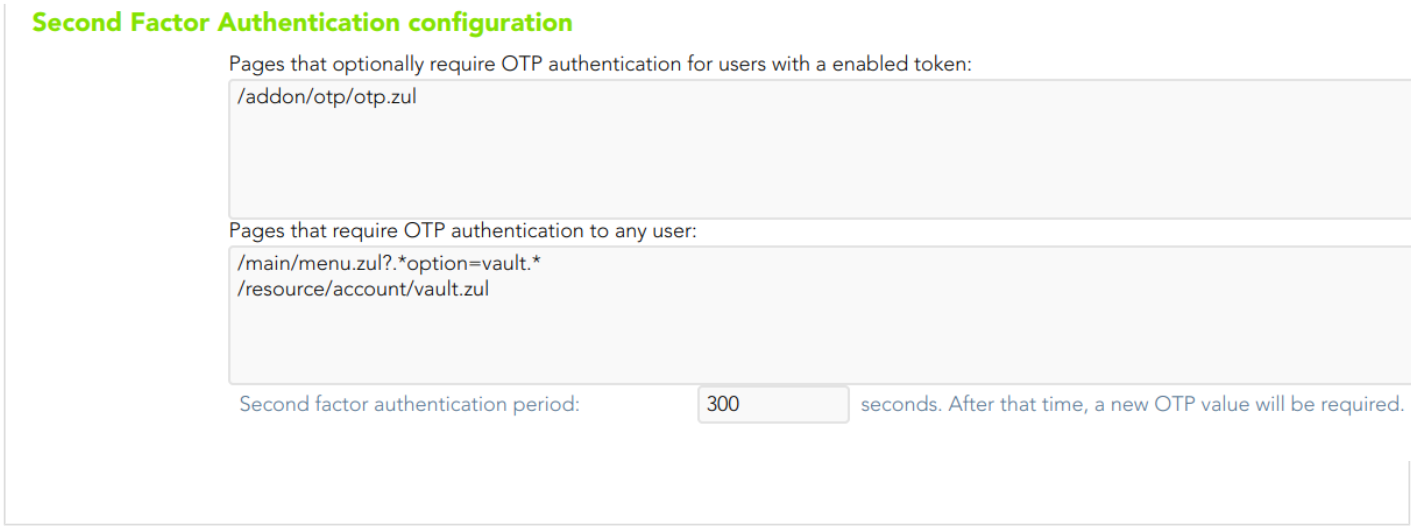
◫ Example

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

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.

Password policies

Definition

Password domain

Is a logical way of grouping managed systems that are sharing the same password for each account. If the administrator chooses to have the same password for every system, only one password domain should exist. If the administrator chooses to assign a different password for each system, then a password domain should be created for each managed system.

Password policies

Password policies allow you to define custom rules that passwords must comply with to enhance system security. For each password domain, Soffid allows you to create different password policies related to user type. It is only possible to define a single password policy for one password domain and one user type.

There are two kinds of password policies.

- The first one is for user selected passwords. That is the default behavior.
- The second one is system generated passwords. These policies are useful for shared accounts when using Enterprise Single Sign-on.

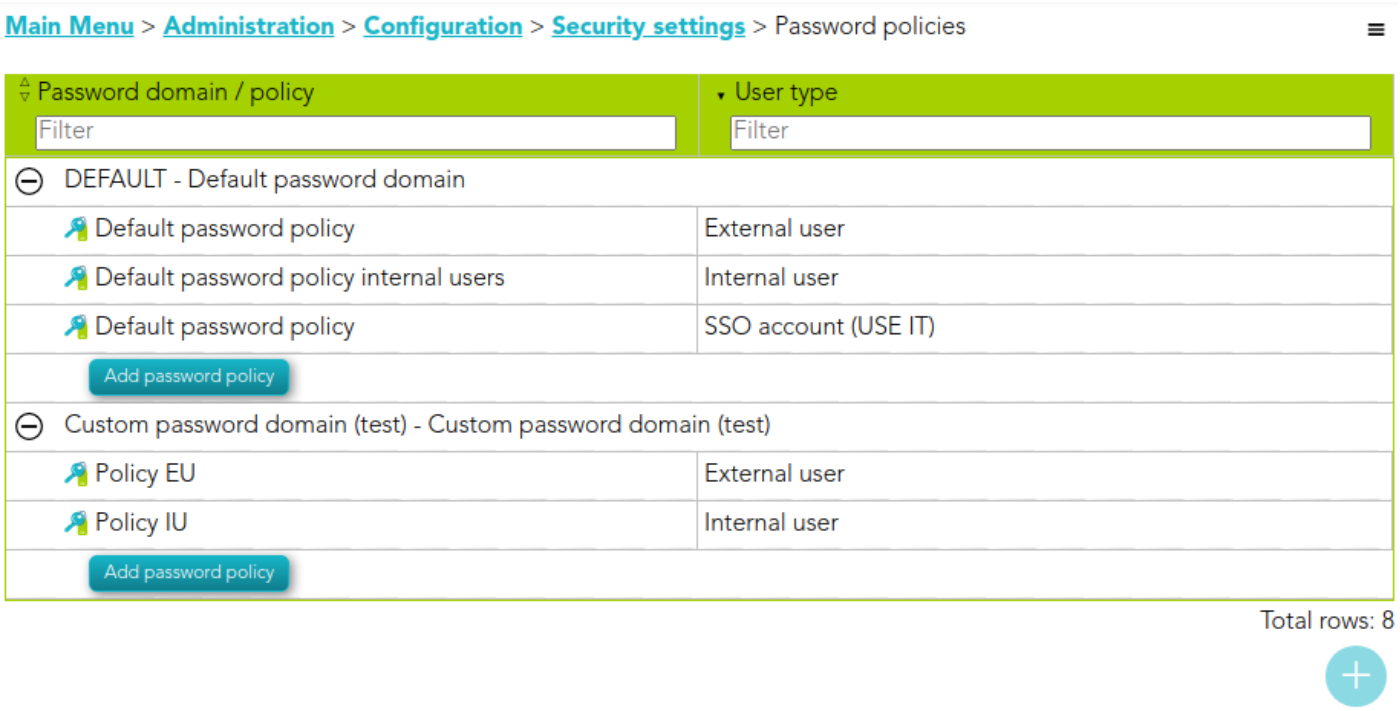
A password policy will also define how often the password needs to be changed and how many days are allowed to change it.

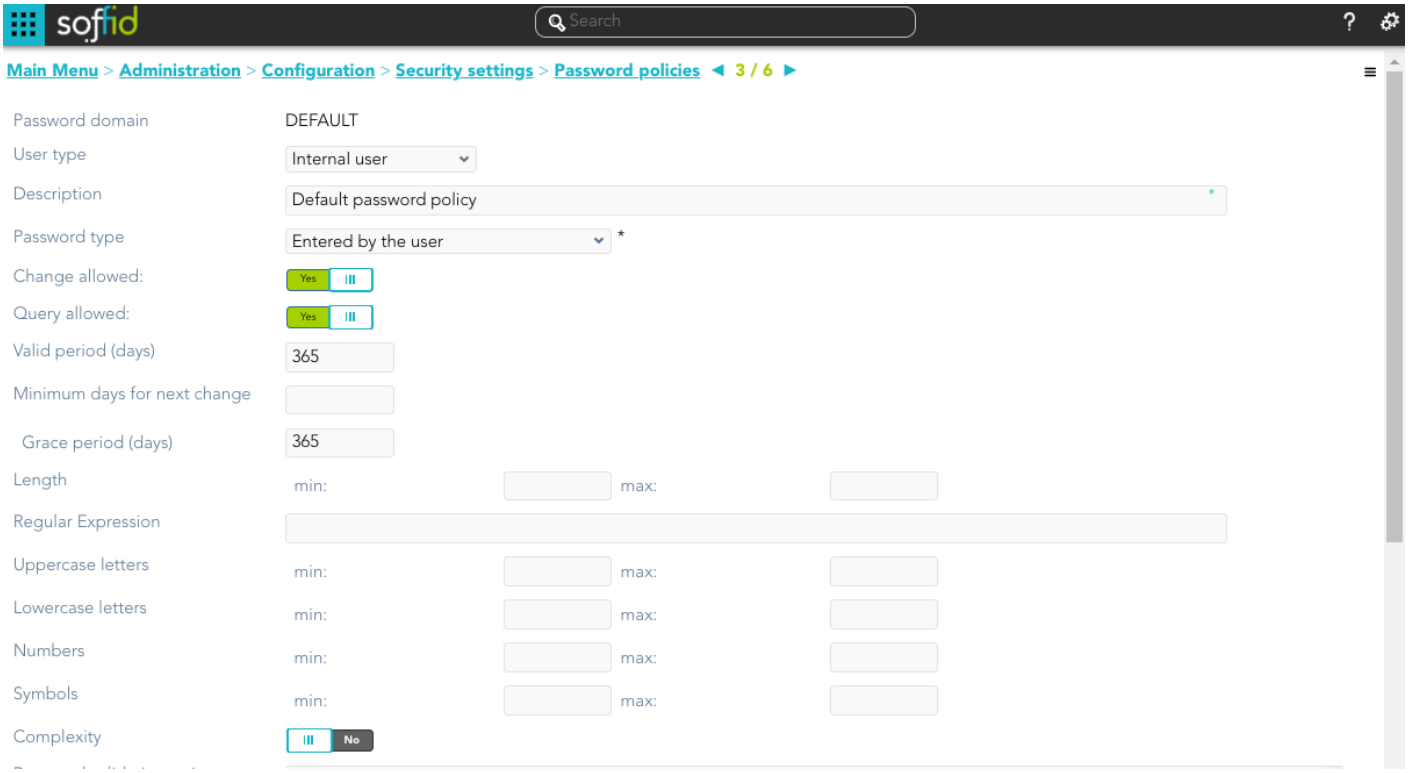
Regarding password complexity, you can specify the minimum and the maximum number of lowercase letters, uppercase letters, numbers, and symbols, as well as password length.

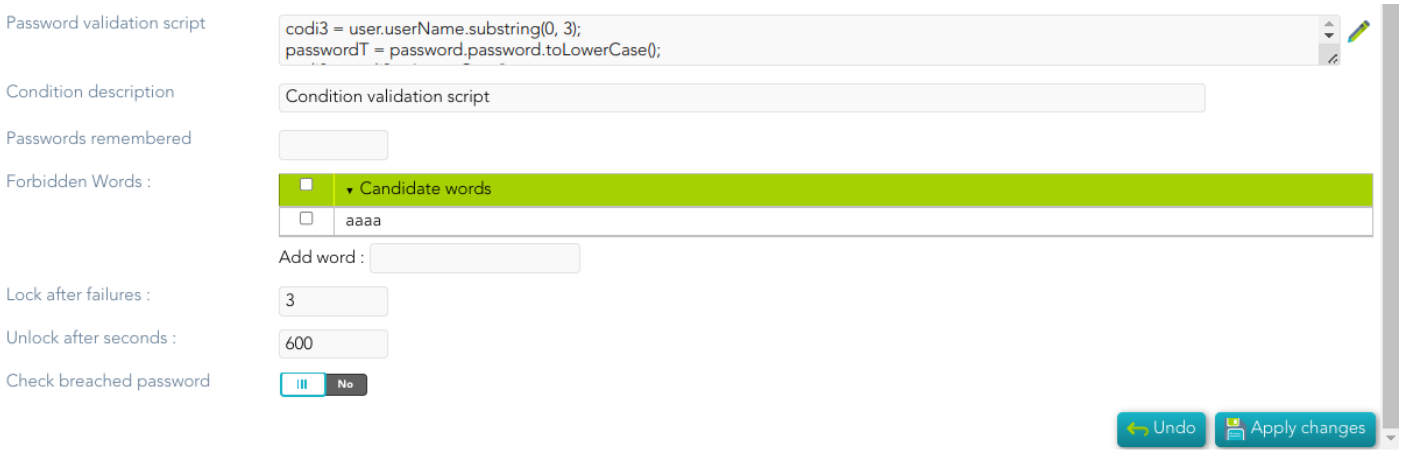
The administrator users can define a regular expression that must match each password. This can be used, for instance, to ensure that the first password is not numeric.

It is allowed to create a list of forbidden words that cannot be used as passwords.

Screen overview







Related objects

1. **Password domain**
2. **User Type**

Standard attributes

Password Domain

- **Code**: password domain identifier code.
- **Description**: a brief description of the password domain.

Password policies

- **Password domain**: the password policy belongs to that password domain.
- **User type**: specific user type for which the password policy is created.
- **Description**: a brief description of the password policy.
- **Password type**: the king of policies password:
  - **Entered by the user**: that is the default behavior.
  - **Automatically generated**: these policies are useful for shared accounts when using Enterprise Single Sign-on.
- **Change allowed**: if it is checked, the user could change automatically generated passwords.
- **Query allowed**: if is checked, the user can view the current password.
- **Valid period (days)**: the change of the password will be asked in that number of days. That option is available when you select the "Entered by the user" option.
- **Minimum days for next change**
- **Grace period (days)**: additional days allowed to the valid period, for changing the password. That option is available when you select the "Entered by the user" option.

- **Renewal Time**: added number of days to change the password. That option is available when you select the "Automatically generated" option.
- **Length (min & max)**: added the number of days to change the password.
- **Regular expression**: the password must comply with that regular expression.
- **Uppercase letters (min & max)**: min and max number of uppercase letters that be included on the password.
- **Lowercase letters (min & max)**: min and max number of lowercase letters that be included on the password.
- **Numbers (min & max)**: min and max number of numbers that be included on the password.
- **Symbols (min & max)**: min and max number of symbols that are included on the password.
- **Complexity**: Similar operation to the same option in Active Directory. It is mandatory to use three different types of characters (uppercase, lowercase, numbers, and symbols), it is not allowed to use the user code, name, or surname.
- **Password validation script**: script to validate additional password conditions. The result must be true or false.
- **Condition description**: description of the validation script. This condition will be displayed in the Password policy field when the user try to change the password from My Profile.
- **Passwords remembered**: the number of passwords the system will remember.
- **Forbidden words**: list of forbidden words that may not be used to create a password if they are selected. It will be case insensitive. For instance, there will be no distinction between "Soffid", "SOFFID", or "soffid".
- **Lock after failures**: the number of login attempts before blocking an account.
- **Unlock after seconds**: the number of seconds an account is blocked.
- **Check breached password**

Password validation script example:

```
codi3 = user.userName.substring(0, 3);
codi3 = codi3.toLowerCase();
if (passwordT != null)
 if(codi3.equals(passwordT.substring(0,3)))
   return false;
return true;
```

Actions

Password policies query actions

Add new domain	Allows you to create a new **password domain**. You can choose that option on the hamburger menu or click the add button (+).To add a new password domain it will be mandatory to fill in the required fields
Add new password policy	Allows you to create a new **password policy** on a specific password domain. Below the father password domain, you can find the button to perform that action. To add a new password policy it will be mandatory to fill in the required fields.

Password domain detail actions

Apply changes	Allows you to save a new password domain or to update the password domain changes. To save the data it will be mandatory to fill in the required fields.
Delete	Allows you to delete a password domain. To delete a password domain you can click on the hamburger icon and then click the delete button (trash icon). Soffid will ask you for confirmation to perform that action, you could confirm or cancel the operation.
Undo	Allows you to quit without applying any changes.

Password policies detail actions

Apply changes	Allows you to create a new password policy or to update password policy changes. To save the data it will be mandatory to fill in the required fields.
Delete	Allows you to delete a password policy. To delete a password policy you can click on the hamburger icon and then click the delete button (trash icon). Soffid will ask you for confirmation to perform that action, you could confirm or cancel the operation.
Undo	Allows you to quit without applying any changes.
Add word	Allows you to create a new forbidden word. Those forbidden words may not be used to create a password if they are selected.

Configure PAM session servers

Definition

Soffid provides the functionality that allows you to configure the Jump servers. That option is located on

`Main Menu > Administration > Configure Soffid > Security settings > Configure PAM session servers`

To configure that functionality is mandatory to install PAM following the instructions of the PAM installation page.

> A Jump server is the control point that forces users to log into that system first, then, they could traverse to other servers without having to log in again. The purpose of a jump server is to be the only gateway for access to your infrastructure reducing the size of any potential attack surface.

Screen overview

https://www.youtube.com/embed/iABzqU40Pws?rel=0

Related objects

- **soffid-pam-store**: storage server container
- **soffid-pam-launcher**: launcher container

Standard attributes

- **Group name**: name to identify the configuration.
- **Description**: a brief description.
- **User name**: user name given at installation of PAM
- **Password**: password given at installation of PAM.
- **URL**: of the storage. The default port is 8081.
- **Jump servers**: list of jump servers. A URL of each jump server. The default port is 8082.

Actions

Add new	Allows you to add a new configuration of PAM. You can choose that option by clicking the add button (+). You must fill in all the attributes to save a new configuration.
Delete	Allows you to delete one or more configuration PAM registers, you must select one or more records from the list and click the button with the subtraction symbol (-). To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Apply chanages	Allows you to create a new configuration PAM or to update an existing one. To save the data it will be mandatory to fill in the required fields. Also, the password and user name should be correct to connect.
Undo	Allows you to quit without applying any changes made.

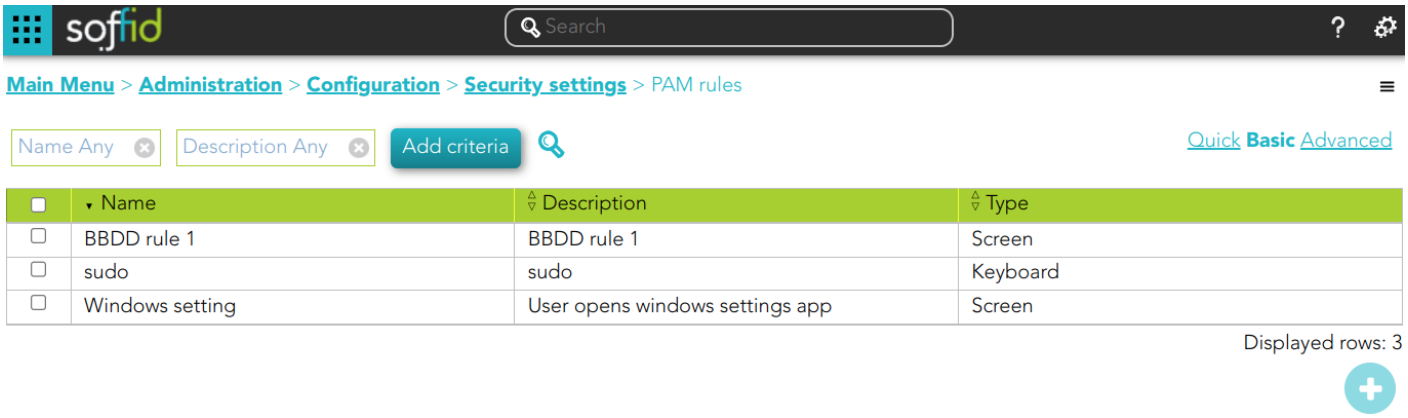
PAM Rules

Definition

> Soffid allows you to define rules to detect commands executed on a server. When a user launches a command defined on a rule, Soffid will detect it.

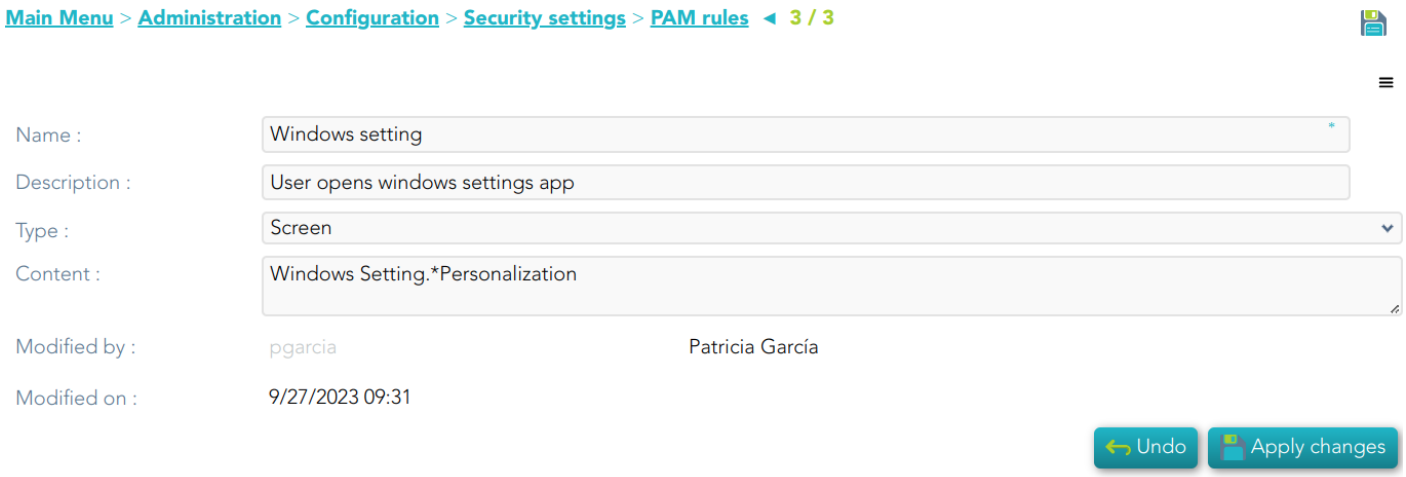
To use those rules you need to define the PAM policies. For more information, you can visit the PAM policies page.

Screen overview



Keyboard example

Screen example



Keyboard example

Standard attributes

- **Name**: name to identify the rule.
- **Description**: a brief description of the rule.
- **Type**: rule type.
  - **Keyboard**: Indicate the command typed in the terminal that you want to control.
  - **Screen**: Indicate the text displayed in the screen that you want to control.
- **Content**: the content of the rule that Soffid will detect. Be in mind, that Soffid will consider blanks, returns, and all characters you type.
- **Modified by**: user who modified that rule.
- **Modified on**: the date and time of the update.

Actions

PAM rules query

Query	Allows you to query PAM rules through different search systems, Quick, Basic and Advanced.
Add or remove columns	Allows you to show and hide columns in the table.
Add new	Allows you to create a new PAM rule. You can choose that option on the hamburger menu or click the add button (+). To add a new PAM rule it will be mandatory to fill in the required fields.
Delete	Allows you to remove one or more PAM rules by selecting one or more records and next clicking the button with the subtraction symbol (-). To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Import	Allows you to upload a CSV file with the PAM rules list to add or update PAM rules to Soffid. First, you need to pick up a CSV file, that CSV has to contain a specific configuration. Then you need to check the content to be loaded, it is allowed to choose if you want or not to load a specific attribute. And finally, you need to select the mappings for each column of the CSV file to import the data correctly and click the Import button.
Download CSV file	Allows you to download a CSV file with the PAM rules information.

PAM rules detail

Apply changes	Allows you to create a new configuration PAM rule or to update an existing one. To save the data it will be mandatory to fill in the required fields.
Undo	Allows you to quit without applying any changes made.
Delete	Allows you to delete a PAM rule. To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.

PAM Policies

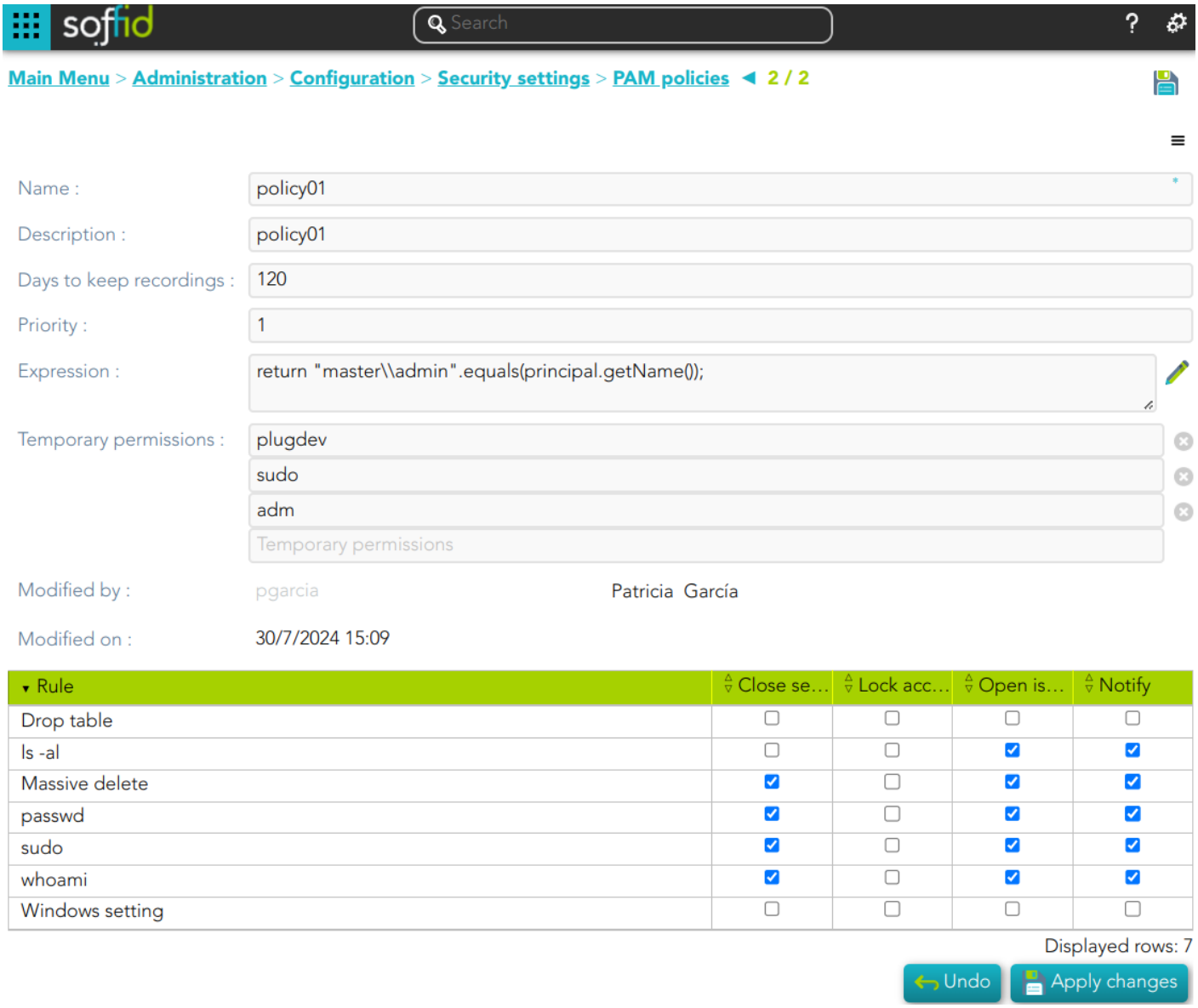
Definition

Privileged Access Management (PAM) policies are a set of guidelines and controls that dictate how privileged access is granted, managed, and audited within an organization.

Soffid allows you to define policies, those policies can be made up of several rules. For each rule, you could select the action to perform when Soffid detects that rule is accomplished.

To use those policies you need to define how policies will be used by each folder in the password vault. For more information, you can visit the Password Vault page.

Screen overview



Standard attributes

- **Name**: name to identify the policy.
- **Description**: a brief description of the policy.
- **Days to keep recordings**: number of days that recordings will be kept.
- **Priority**: allows you to set the priority between the different PAM policies configured. When there are several policies, the policy to be applied is evaluated according to priority and expression.
- **Expression**: this expression is evaluated to determine the priority of the policy to be applied. When there are several policies, the policy to be applied is evaluated according to priority and expression.
- **Temporary permissions**: these permissions will be assigned to the user's account on the target system. The permissions will be maintained for the duration of the session. Once the session is over, the permissions will be revoked. The account must be a managed account.

- **Modified by**: user who modified that rule.
- **Modified on**: the date and time of the update.

When you save the standard attributes of a PAM policy and edit the policy again, the rule list will be shown. Here you can customize the policy depending on the existing rules.

- **Rule list**: show a list of the PAM rules defined. You can check/uncheck the available options. You can choose zero, one, or several:
  - **Close session**: when the rule is met, Soffid will close the session.
  - **Lock account**: when the rule is met, Soffid will lock the account.
  - **Open issue**: when the rule is met, Soffid will open a new issue (*).
  - **Notify**: when the rule is met, Soffid will send a notification about the action.

> (*) You can visit the following page for more information about the issues: https://bookstack.soffid.com/books/soffid-3-reference-guide/page/issue-policies and https://bookstack.soffid.com/link/1153#bkmrk-pam-violation

> The PAM policies configuration is sent to the user-console.policies to the Store container. You can find this file at /opt/soffid/tomee/data/ips

Image

Actions

PAM rules query

Query	Allows you to query PAM policies through different search systems, Quick, Basic and Advanced.
Add or remove columns	Allows you to show and hide columns in the table.
Add new	Allows you to create a new PAM policy. You can choose that option on the hamburger menu or click the add button (+). To add a new PAM policy it will be mandatory to fill in the required fields.
Delete	Allows you to remove one or more PAM policies by selecting one or more records and next clicking the button with the subtraction symbol (-). To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Import	Allows you to upload a CSV file with the PAM policies list to add or update PAM policies to Soffid. First, you need to pick up a CSV file, that CSV has to contain a specific configuration. Then you need to check the content to be loaded, it is allowed to choose if you want or not to load a specific attribute. Finally, you need to select the mappings for each column of the CSV file to import the data correctly and click the Import button.
Download CSV file	Allows you to download a CSV file with the PAM policies information.

PAM rules detail

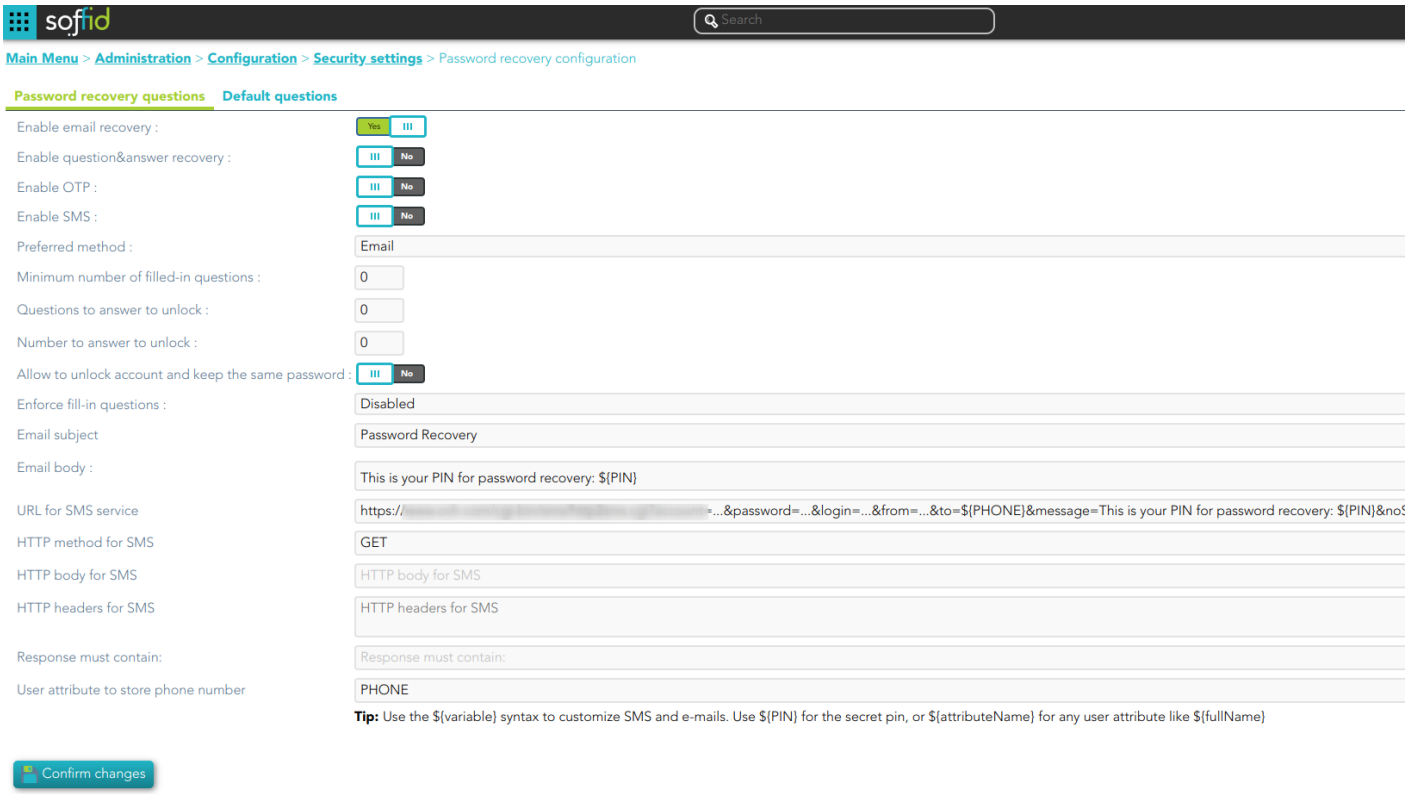
Apply changes	Allows you to create a new configuration PAM policy or to update an existing one. To save the data it will be mandatory to fill in the required fields.
Undo	Allows you to quit without applying any changes made.
Delete	Allows you to delete a PAM policy. To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.

Password recovery configuration

Description

Soffid provides you the functionality that allows to the users recover their passwords. To do that, the admin user, o a user with the proper roles, must config the the password recovery parameters.

Screen Overview



Custom attributes

- **Enable email recovery**: if Yes is selected, it will allow password recovery through an e-mail sent to an authorized mailbox.
- **Enable question&answer recovery**: if Yes is selected, a question and control response will be requested.
- **Enable OTP**: if Yes is selected, an OTP will be required to recover the password. That OTP depends on the OTP settings configured into the Soffid Console and the OTP devices configured for the end-user.
- **Enable SMS**: if Yes is selected, an SMS will be send to recover the password.
- **Preferred method**: in case you select two or more previous options, this drop-drown will allow you to priorize one option over the others.
- **Minimum number of filled-in questions**: indicates the minimum number of user questions that must be have answered in the end-user's profile to can use this recover password method.
- **Questions to answer to unlock**: indicates the number of questions that must be formulated to the end-user to reset his password.
- **Numer to answer to unlock**: indicates the number of answers that must be answered by the end-user to reset his password.
- **Allow to unlock account and keep the same password**: allows to administrator user to unlock an end-user's account and keep the same password.
- **Enforce fill-in questions:** allow on each access Soffid to check if the questions are answered. In case the questions have not been not answered, Soffid will display a window with the questions to answer or to config to the end-user depending on that value.
  - **Disabled**: allows you to disable that functionality.
  - **Required**: if this option is selected, the system will check if the user questions are answered correctly.
    If the user have not a required number of questions defined or he have not answered all his questions, the system will show the retrieve password questions page.
  - **Optional**: when this option is selected, the system will check the user questions but it will not show the retrieve password questions page if the user questions does not meet the configuration parameters.
- **Email subject**
- **Email body**
- **URL for SMS service**
- **HTTP method for SMS**
- **HTTP body for SMS**
- **HTTP headers for SMS**
- **Response must contain**
- **User attribute to store phone number:** user object attribute defined on the Metadata page to save the phone number.

Actions

Confirm changes	Allows you to save the data of password recovery configuration. To save the data it will be mandatory to fill in the required fields.

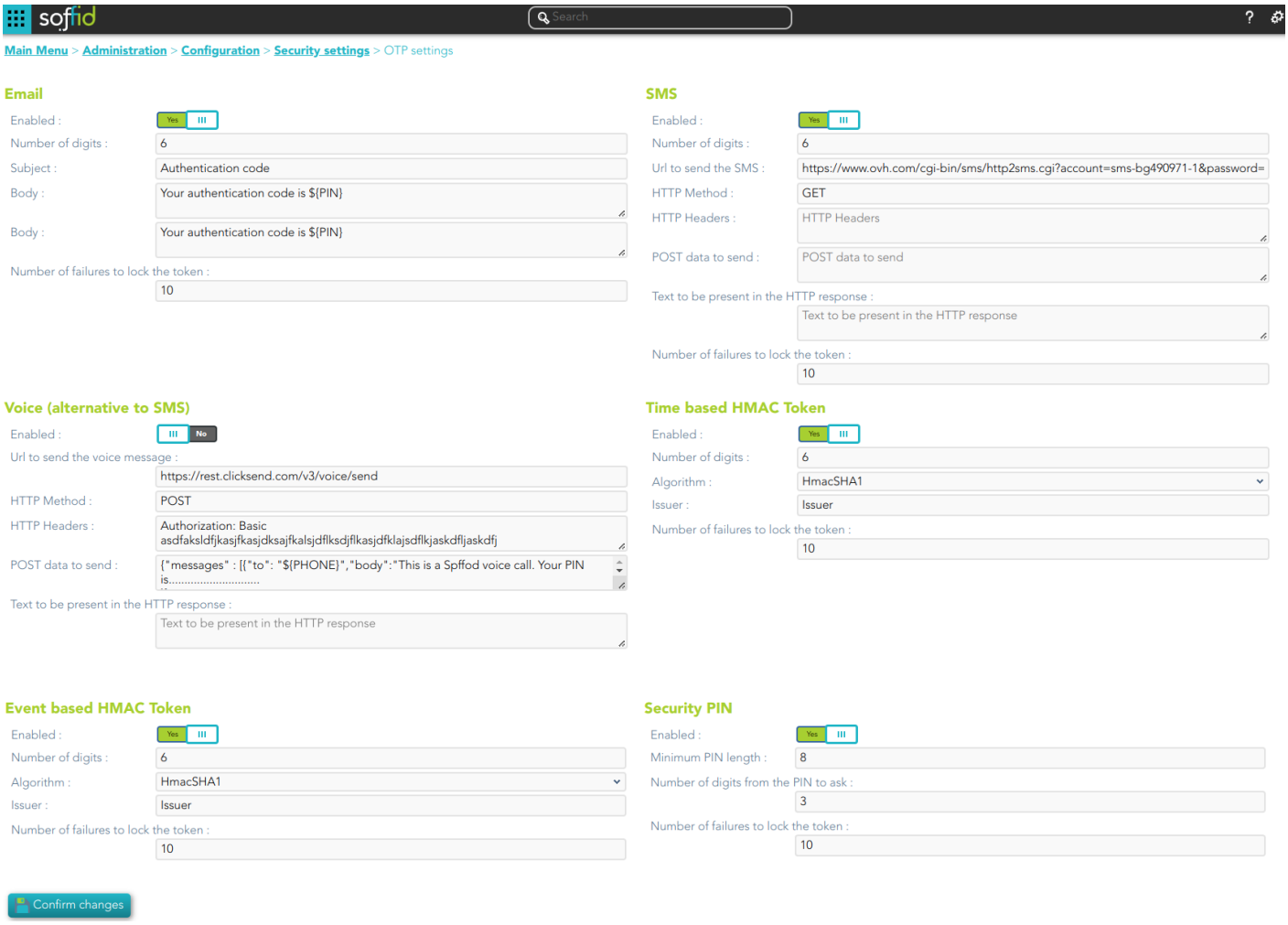
OTP settings

Definition

The OTP settings allow the administrator users to configure the available OPT options. Soffid provides four different OTP implementations.

Main Menu > Administration > Configuration > Security settings > OTP settings

Screen overview



Standard attributes

Email

- **Enabled**: allows you to enable or disable the OTP implementation.
- **Number of digits**: number of digits of the PIN code that will be generated.
- **Subject**
- **Body**
- **Number of failures to lock the token**

> To send an email, will be mandatory to fill in the value of the **mail.from** parameter. You can visit the mail server parameters.

SMS

- **Enabled**: allows you to enable or disable the OTP implementation.
- **Number of digits**: number of digits of the PIN code that will be generated.
- **URL to send the SMS**: enter the URL of your SMS provider rest service

```
https://www.xxxxxxx.com/cgi-bin/sms/http2sms.cgi?account=sms-bg490971-1&password=XXXXXXt&login=user&from=SOFFID&to=${PHONE}&message=This is your access PIN: ${PIN}&noStop&contentType=application/json&class=0
```

- **HTTP Method**: enter POST or GET depending on your provider documentation
- **HTTP Header**: optionally, you can add any HTTY header, including Basic or Bearer authentication tokens. The header must include the header name and header value. For instance:
  `Authorization: Basic dXNlcjpwYXNzd29yZA==`
- **POST data to send** Enter the body of the HTTP request
- **Text to be present in the HTTP response**: Soffid will check the response from your SMS Provider contains this text

```
"status":100
```

- **Number of failures to lock the token**

The URL and POST data to be sent, the administrator can use some tags that will be replaced by some target user attributes:

- ${PHONE}: The target phone number
- ${PIN}: The one-time password to be entered by the user
- ${userAttribute}: Any of the standard or custom user attributes, like ${fullName} or ${userName}

Voice (alternative to SMS)

- **Enabled**: allows you to enable or disable the OTP implementation.
- **URL to send the SMS**: enter the URL of your voice call provider rest service
- **HTTP Method**: enter POST or GET depending on your provider's documentation
- **HTTP Header**: optionally, you can add any HTTY header, including Basic or Bearer authentication tokens. The header must include the header name and header value. For instance:

  ```
  Authorization: Basic xxxxxxxxxxxxxxOUVCRS1DMzE0LTI3MzAtQkY0Qy05RDgwRTMyQUQ4OUY=
  Content-Type: application/json
  Accept: application/json
  ```

- **POST data to send** Enter the body of the HTTP request.

  ```
  Text to be present in the HTTP response: Soffid will check the response from your SMS Provider contains this text
  ```

  The POST data to be sent, the administrator can use some tags that will be replaced by some target user attributes:

- ○ ${PHONE}: The target phone number
  ○ ${PIN}: The one-time password to be entered by the user
- **Number of failures to lock the token**

Time based HMAC Token

- **Enabled**: allows you to enable or disable the OTP implementation.
- **Number of digits**: number of digits of the PIN code that will be generated.
- **Algorithm**: allows you to select an HMAC algorithm.
- **Issuer**
- **Number of failures to lock the token**

Event based HMAC Token

- **Enabled**: allows you to enable or disable the OTP implementation.

- **Number of digits**: number of digits of the PIN code that will be generated.
- **Algorithm**: allows you to select an HMAC algorithm.
- **Issuer**
- **Number of failures to lock the token**

Security PIN

- **Enabled**: allows you to enable or disable the Security PIN implementation.
- **Minimum PIN length**: minimum number of digits that the PIN has to have.
- **Number of digits from the PIN to ask**: number of digits that Soffil will ask to verify the identity.
- **Number of failures to lock the token**

Actions

Confirm changes	Allows you to save the updates and quit the page.

XACML Policy Management

Definition

The **PDP, Policy Decision Point**, is in charge of evaluating the defined rules. The Policy Decision Point is essentially a policy compiler. The PDP must verify that the specified rules are within the scope of the rule authors authority. The PDP **provides the authorization** to the PEP.

XACML Policy Management

The policy language is used to describe general access control requirements, and has standard extension points for defining new functions, data types, combining logic, etc. The request/response language lets you form a query to ask whether or not a given action should be allowed, and interpret the result.

`Main Menu > Administration > Configuration > Security settings > XACML Policy Management`

It is possible to import an existing PolicySet into Soffid. The file to import must be a well-formed XML.

> To know more about XACML, read XACML 2.0 Standard Specification

Related objects

- Policy set
- Policy
- Policy set reference
- Policy reference

---

https://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html

XACML PEP configuration

Description

The **PEP, Policy enforcement point**, is a component of policy-based management, **where enforce the policies**. It is the component that serves as the gatekeeper to access a digital resource. The PEP gives the PDP, Policy Decision Point, the job of deciding whether or not to authorize the user based on the description of the user's attributes.

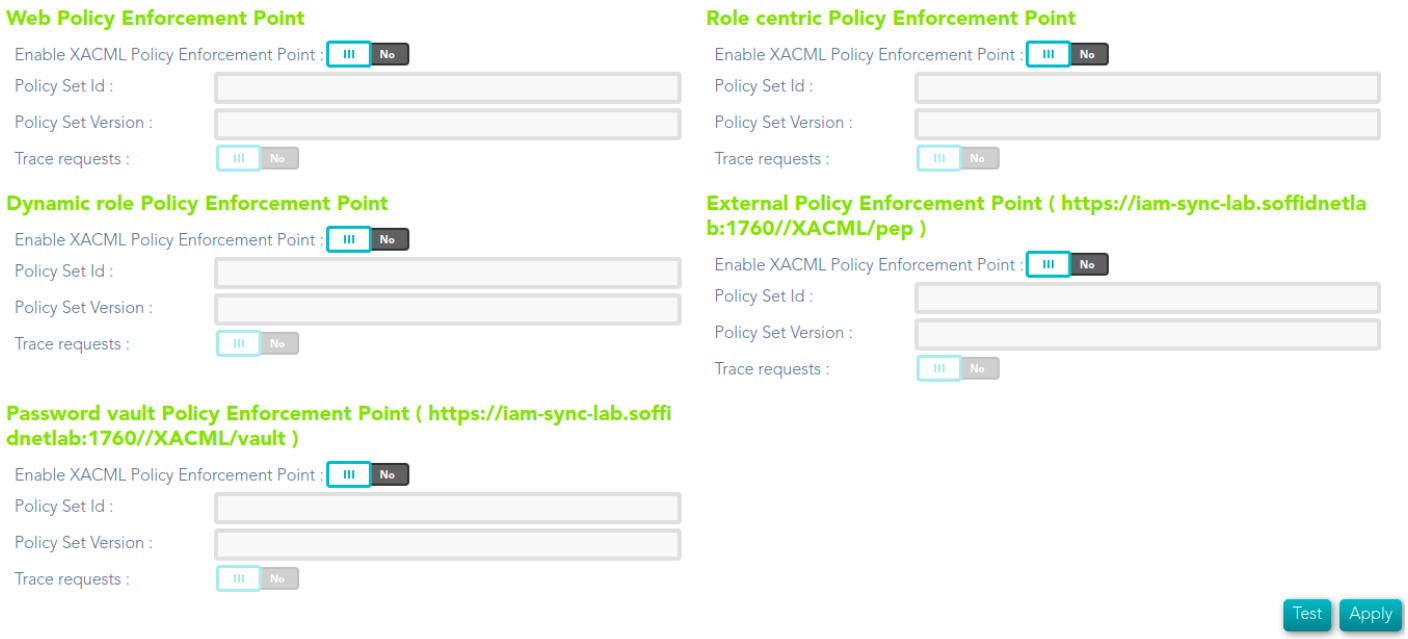
XACML PEP configuration

Soffid allows you to configure different policies enforcement points, each of then can use a different policy set.

`Main Menu > Administration > Configuration > Security settings > XACML PEP configuration`

- Web Policy Enforcement Point
- Role centric Policy Enforcement Point
- Dynamic role Policy Enforcement Point
- External Policy Enforcement Point
- Password vault Policy Enforcement Point

Screen



Common attributes

Common attributes for each PEP:

- **Enable XACML Policy Enforcement Point**: select the Yes option to enable the PEP.
- **Policy Set Id**: policy set identifier.
- **Policy Set Version**: version of the policy set to enforce.
- **Trace requests**: select the Yes option to enable the trace.

Policies enforcement points

Web Policy Enforcement Point

The policy will be enforced when the user open a new Soffid page. Using this PEP you can define the rules to access to Soffid pages.

SUBJECTS	RESOURCES	ACTIONS	ENVIRONMENTS

User User attributes Account System Role Group Primary Gorup IP Address	Server URL	Get Put Post	Current Time Current Date Current DateTime

Role centric Policy Enforcement Point

The policy will be enforced when the user login into Soffid. It will calculate the user authorizations as of the permissions that the user has assigned.

SUBJECTS	RESOURCES	ACTIONS	ENVIRONMENTS
User User attributes Account System Role Group Primary Gorup IP Address	Soffid object Attributes	create update delete query	Current Time Current Date Current DateTime

Dynamic role Policy Enforcement Point

The policy will be enforced when the user performs an action to evaluate if the user has or not authorization. The user must have the proper role and comply with the XACML rule.

You can use that PEP to split the permissions, for instance, a support group can update the permission of a specific group of user, and another support group can update the permissions of another group of users.

SUBJECTS	RESOURCES	ACTIONS	ENVIRONMENTS
User User attributes Account System Role Group Primary Gorup IP Address	Soffid object Attributes (*)	create update delete query	Current Time Current Date Current DateTime

(*) It is allowed to use "Attribute Selector" to configure Dynamic role policy.

External Policy Enforcement Point (https://iam-sync-lab.soffidnetlab:1760//XACML/pep)

PEP of general purpose. Calling the web service, the clients can made validations and figure out if the users have access.

SUBJECTS	RESOURCES	ACTIONS	ENVIRONMENTS
User User attributes Account System Role Group Primary Gorup IP Address	Token Method Soffid object	Get Put	Current Time Current Date Current DateTime

Password vault Policy Enforcement Point (https://iam-sync-lab.soffidnetlab:1760//XACML/vault)

The policy will be enforced when the password vault is used.

SUBJECTS	RESOURCES	ACTIONS	ENVIRONMENTS
User User attributes Account System Role Group Primary Gorup IP Address	Access level Account System Login Vault Folder Server URL	setPassword queryPassword queryPasswordBypassPolicy launch	Current Time Current Date Current DateTime

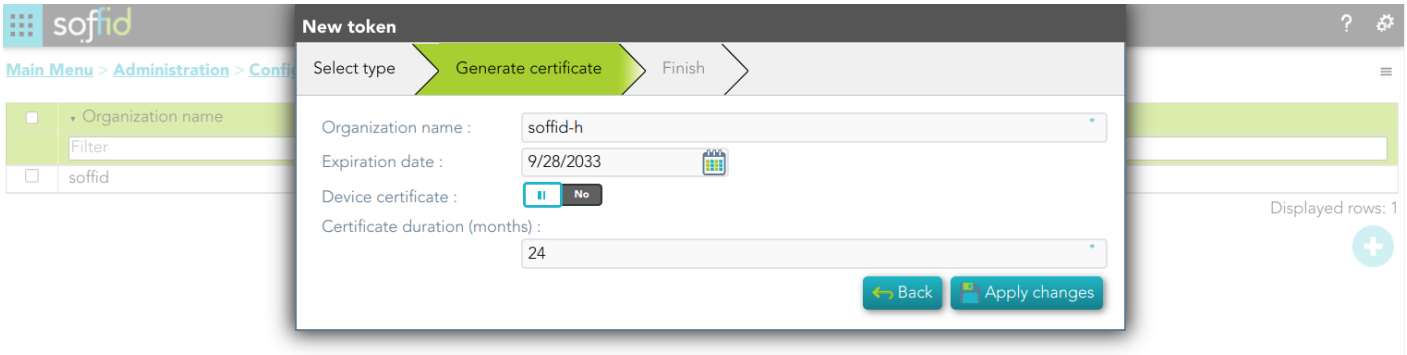
Digital certificates

Definition

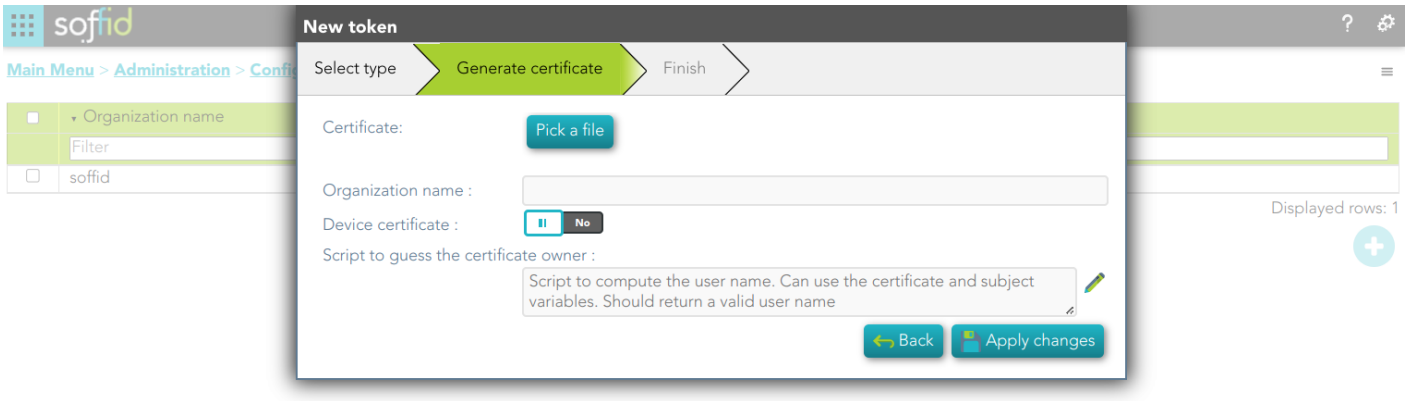
Soffid includes Digital certificate functionality as a security enhancement. You could add new Digital certificates, internal or external. If you select the external certificate, you could add a valid certificate to Soffid; If you select the internal certificate, Soffidl will generate a valid certificate.

Screen Overview

Internal



External



Standard attributes

Internal

- **Organization name**
- **Expiration date**: referring to the root certificate.
- **Device certificate**: Indicates if the certificate is for a device
- **Certificate duration (months)**: Referring to users' certificates.

External

- **Certificate:** root of the certification authority.
- **Organization name**
- **Device certificate: Indicates if the certificate is for a device**
- **Script to guess the certificate owner**: script to compute the user name. Can use the certificate and subject variables. Should return a valid user name.

Actions

Digital certificates query

Add new	Allows you to add a new certificate. You can choose that option on the hamburger menu or click the add button (+). To add a new certificate it will be mandatory to fill in the required fields.
Delete	Allows you to remove one or more certificates by selecting one or more records and next clicking the button with the subtraction symbol (-). To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Download CSV file	Allows you to download a CSV file with the digital certificates data.

New token

Next	Allows you to browse the wizard to create a new certificate.
Apply changes	Allows you to save the data of a new certificate or to update the data of a specific certificate. To save the data it will be mandatory to fill in the required fields
Undo	Allows you to quit without applying any changes.

Recertification policies

Description

> Soffid allows you to establish some policies to define the scope of the recertification process.

Menu option

Main Menu > Administration > Configuration > Security settings > Recertification policies

Screen overview

Custom attributes

- **Name**: name to identify the policy
- **Type**: list of available recertification types.
  - **User entitlements**: the recertification process will be conducted to review user access rights.
  - **Role definitions**: the recertification process will be conducted to review the relationship between roles.

    - **Share account entitlements**: the recertification process will be conducted to review access rights to shared accounts.
- **Filter**: this allows you to define a script to identify the grant list to which to apply the recertification process. The **grant object** *(*1)* is always available. You can use the Enumeration SoDRisk to compare:
    - **SOD_LOW**
    - **SOD_HIGH**
    - **SOD_FORBIDDEN**
    - **SOD_NA**
- **Step 1 expression**: this allows you to define a script to determine who is or are in charge to approve or deny the recertification process in the first level.
- **Step 2 expression**: this allows you to define a script to determine who is or are in charge to approve or deny the recertification process after the first level of approval.
- **Step 3 expression:** this allows you to define a script to determine who is or are in charge to approve or deny the recertification process after the second level of approval.
- **Step 4 expression**: this allows you to define a script to determine who is or are in charge to approve or deny the recertification process after the third level of approval.
- **Mail Template**: this allows you to define a template to send an email to the people in charge to approve or deny. Be in mind, that to work fine, the review process link must be `${url}`

> *(*1)* **grant object** is a com.soffid.iam.api.RoleAccount object.

Examples

Some sample scripts for the filters and approval steps are shown below

Filter

Return all grants with risk.

```
return grant.sodRisk != null
&& grant.sodRisk != es.caib.seycon.ng.comu.SoDRisk.SOD_NA;
```

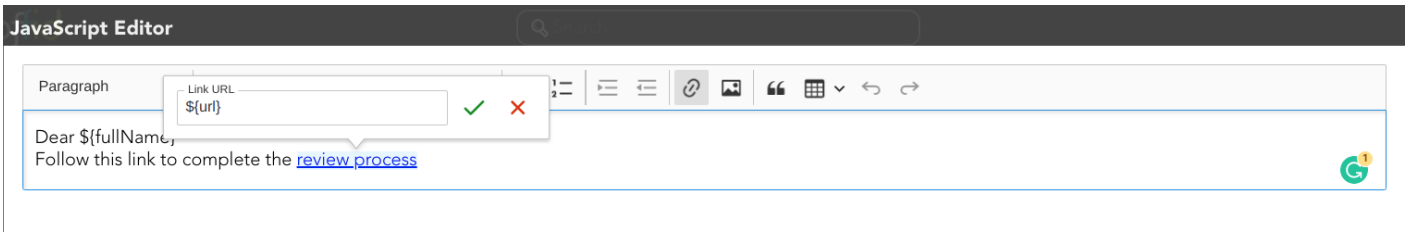
Steps

```
account = serviceLocator.getAccountService().findAccountById(grant.accountId);
StringBuffer sb =  new StringBuffer();
```

```
for (owner : account.ownerUsers) {
  if (sb.length() > 0)
    sb.append(" ");

  sb.append(owner);
}
if (sb.length() > 0)
  return sb.toString();
else
  return "admin";
```

```
com.soffid.iam.api.Role role =
serviceLocator.getApplicationService().findRoleByNameAndSystem(grant.roleName, grant.system);
StringBuffer sb =  new StringBuffer();
List owners = role.getAttributes().get("owner");
if (owners != null) {
for (owner : account.ownerUsers) {
    if (sb.length() > 0)
    sb.append(" ");

        sb.append(owner);
}
}

if (sb.length() == 0)
return "admin";
else
return sb.toString();
```

Mail template



Actions

Recertification policies query

Add new	Allows you to add a new Recertification policy. You can choose that option on the hamburger menu or click the add button (+). To add a new it is necessary to fill in the required fields.
Delete	Allows you to remove one or moreRecertification policies by selecting one or more records and next clicking the button with the subtraction symbol (-). To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Import	Allows you to upload a CSV file with the Recertification policies to add or update the attribute definition to Soffid. First, you need to pick up a CSV file, that CSV has to contain a specific configuration. Then you need to check the content to be loaded, it is allowed to choose if you want or not to load a specific attribute. And finally, you need to select the mappings for each column of the CSV file to import the data correctly and click the Import button.
Download CSV file	Allows you to download a CSV file with the basic information of all Recertification policies.
Add or remove columns	Allows you to show and hide columns in the table. You can also set the order in which the columns will be displayed. The selected columns and order will be saved for the next time Soffid displays the page to the user.

Recertification policies details

Apply changes	Allows you to **save** the data of a new policy or to update the data of a specific policy **and quit**. To save the data it will be mandatory to fill in the required fields.
Save	Allows you to **save** the data of a new policy or to update the data of a specific policy. To save the data it will be mandatory to fill in the required fields.
Delete	Allows you to remove a specific policy. You can choose that option on the hamburger icon. To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Undo	Allows you to quit without applying any changes.

https://download.soffid.com/doc/console/latest/uml/es/caib/seycon/ng/comu/SoDRisk.html

Issue policies

Definition

Soffid has defined automatic events by default. For each of these events, it is possible to define the tasks to be performed and configure them.

You can find this functionality in the following path:

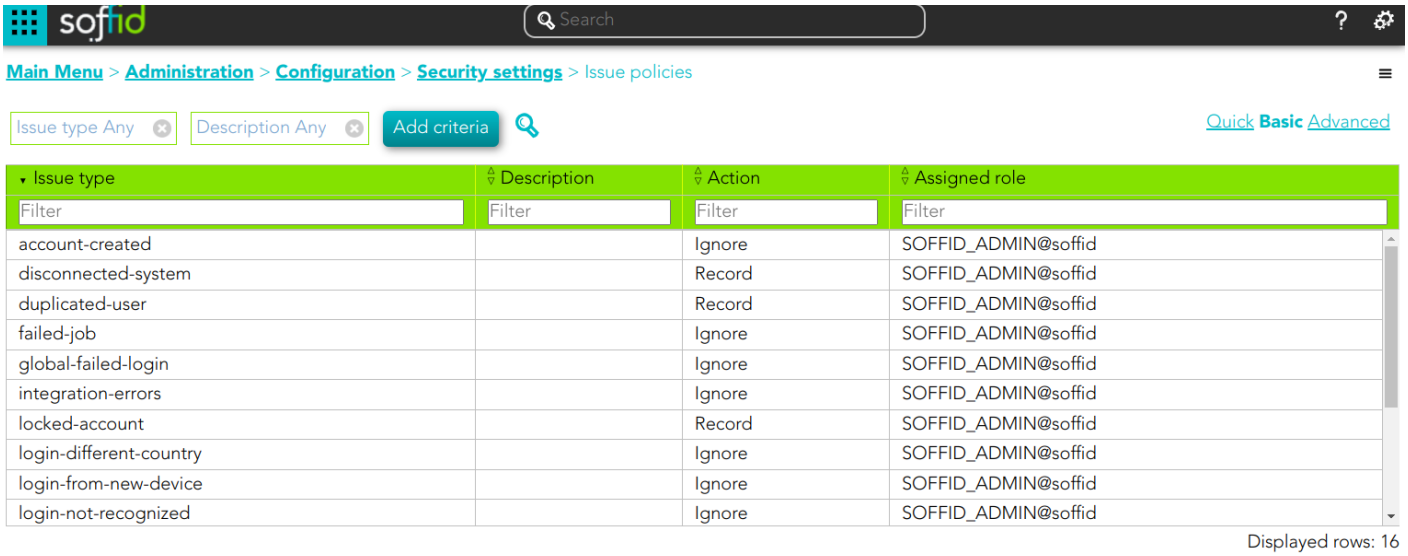
`Main Menu > Administration > Configuration > Security settings > Issue policies`

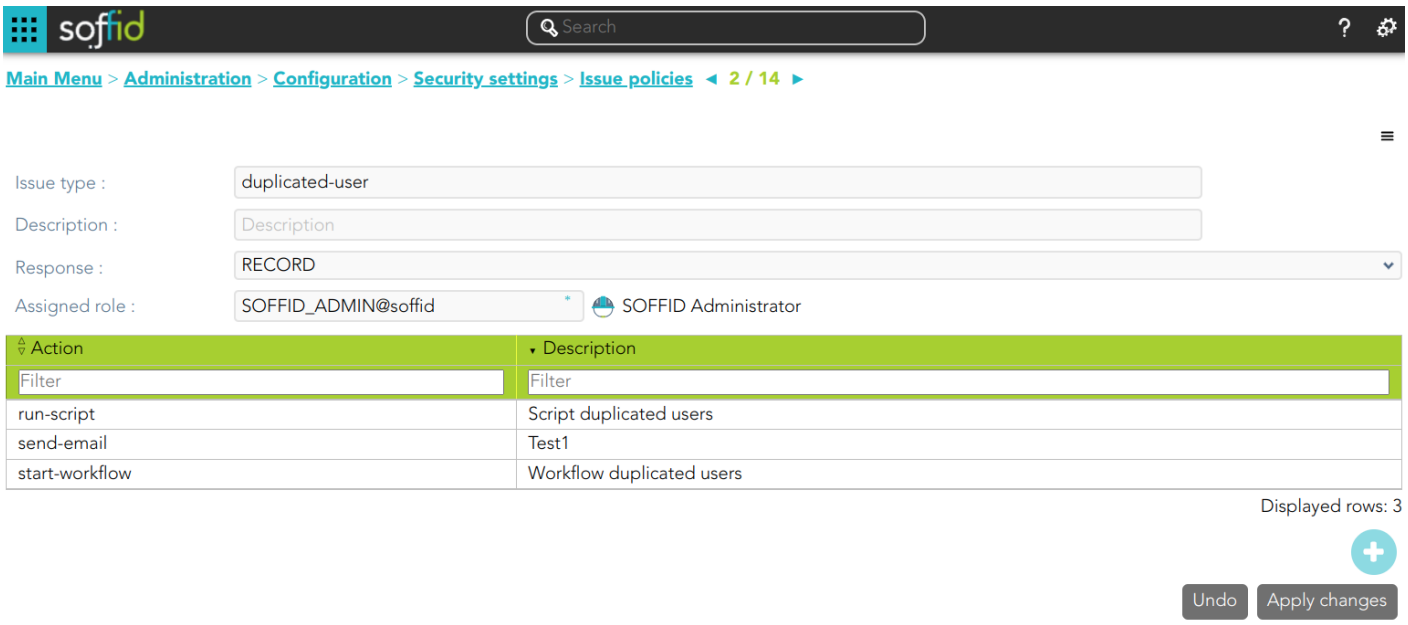
The default events are the following;

Issue Type	Description
account-created	This issue is created when the Sync Server detects when a new account is created. This may occur after the Reconciliation process has been executed.
disconnected-system	This issue is created when the Sync Server detects that some target system is offline.
discovered-host	This issue is created when the Sync Server detects a new host in the network. This only occurs after the Network Discovery process has been executed.
discovered-system	This issue is created when the Sync Server detects a new system in a host. This only occurs after the Network Discovery process has been executed.
duplicated-user	This issue is created the system detects that there are duplicate users, or when the task is generated manually from the user management.
enabled-account-on-disabled-user	This issue is created when an enabled account is detected on a disabled user. This may occur after the reconciliation process has been executed.
failed-job	This issue is created when the system detects job failures. This may occur by running any scheduled task.
global-failed-login	This issue is created when the number of session start failures exceeds the threshold of 0.8.

integration-errors	This issue is created when the Sync Server detects an integration error between Soffid and an end system. You can check the task in the Monitoring & Reporting.
locked-account	This issue is created when an account has been blocked for exceeding the maximum number of login attempts. You can configure the property *Lock after failures* in the Password policies settings. Even if it is temporarily locked, the incident will be generated.
login-different-country	This issue is created when Soffid detects a new login from a different country. It only works with the Identity Provider and it is necessary to have the geolocation database updated.
login-from-new-device	This issue is created when Soffid detects a new login from a new device. It only works with the Identity Provider.
login-not-recognized	This issue is created when Soffid detects a login not recognized (disabled user or user does not exist) in the Soffid Console or in Soffid as an Identity Provider.
otp-failures	This issue is created when an OTP is blocked for exceeding the number of attempts. Currently blocked with 10 unsuccessful attempts.
pam-violation	This issue is created when any of the rules of the PAM are violated. You can define the PAM rules and the PAM policies. Be in mind, that you must check the "Open issue" option in the PAM policies you wish to control.
password-changed	This issue is created when a Password change is detected. These changes come from the end system (Active Directory or Soffid OpenLDAP) and Soffid has been notified. The issue is not created if it is the operator or a script that changes the password in Soffid.
permissions-granted	This issue is created when it is detected that permissions have been given to a user on the end system. This may occur after the reconciliation process has been executed.
risk-increase	This issue is created when it is detected the risk level of a user is increased. You can configure the risks in the Segregation of Duties option.
robot-login	This issue is created when it is detected is detected that someone who has not passed the CAPTCHA is trying to log in to the Identity Provider.
security-exception	This issue is created when unauthorized access to the console via WebService or admin console occurs.

Screen Overview





Related Objects

1. **Roles**

Standard attributes

- **Issue type**: by default, some issues type are defined in Soffid Console.
- **Description**: a brief description of the issue.
- **Action**:
  - **Ignore**: the action will be ignored, and no additional actions will be run.
  - **Record**: the action will be recorded and an issue with the status Acknowledged will be created. The actions configured for the Acknowledged status will be run.

    - **Manage**: a new issue will be created in the New status and the action configured for this status will be run.
- **Assigned role**: the role who will be the owner of the created issues.
- **Actions list**: list of actions to be taken when this issue occurs. You can choose one or more actions from the list and configure them:
    - **Issue status**: it is used to determine the point when the action will be launched.
        - New.
        - Acknowledged.
        - Solved.
        - Solved - Not a duplicate.
    - **Actions**:
        - **Notify affected user**: this allows you to configure an email that will be sent to the affected users.
        - **Send custom email:** this allows you to configure a custom email that will be sent to specific users.
        - **Run script**: allows you to type a script that will be performed
        - **Look affected accounts**: allows you to configure an email that will be sent to the owner user.
        - **Look affected host**.
        - **Notify issue owner by email**.
        - **Acknowledge**.
        - **Start new process**.: allows you to configure the workflow that will be run.
    - **Description**: a brief description of the action you are defining.

> Note that it will be necessary to restart the Sync Server when changing the action of an issue.

Actions

Issue policies query action

Download CSV file	Allows you to download a CSV file with the issue policies data.

Issue policy detail

Add new	Allows you to add a new action to the issue policy. You can choose the action from the action list. Depending on the selected action, you must fill in different information. Once the information will be filled in, you need to close the window and Apply the changes.

Delete	Allows you to delete one or more actions from the actions list.
Apply changes	Allows you to update the changes made to the issue policy.
Undo	Allows you to quit without applying any changes.

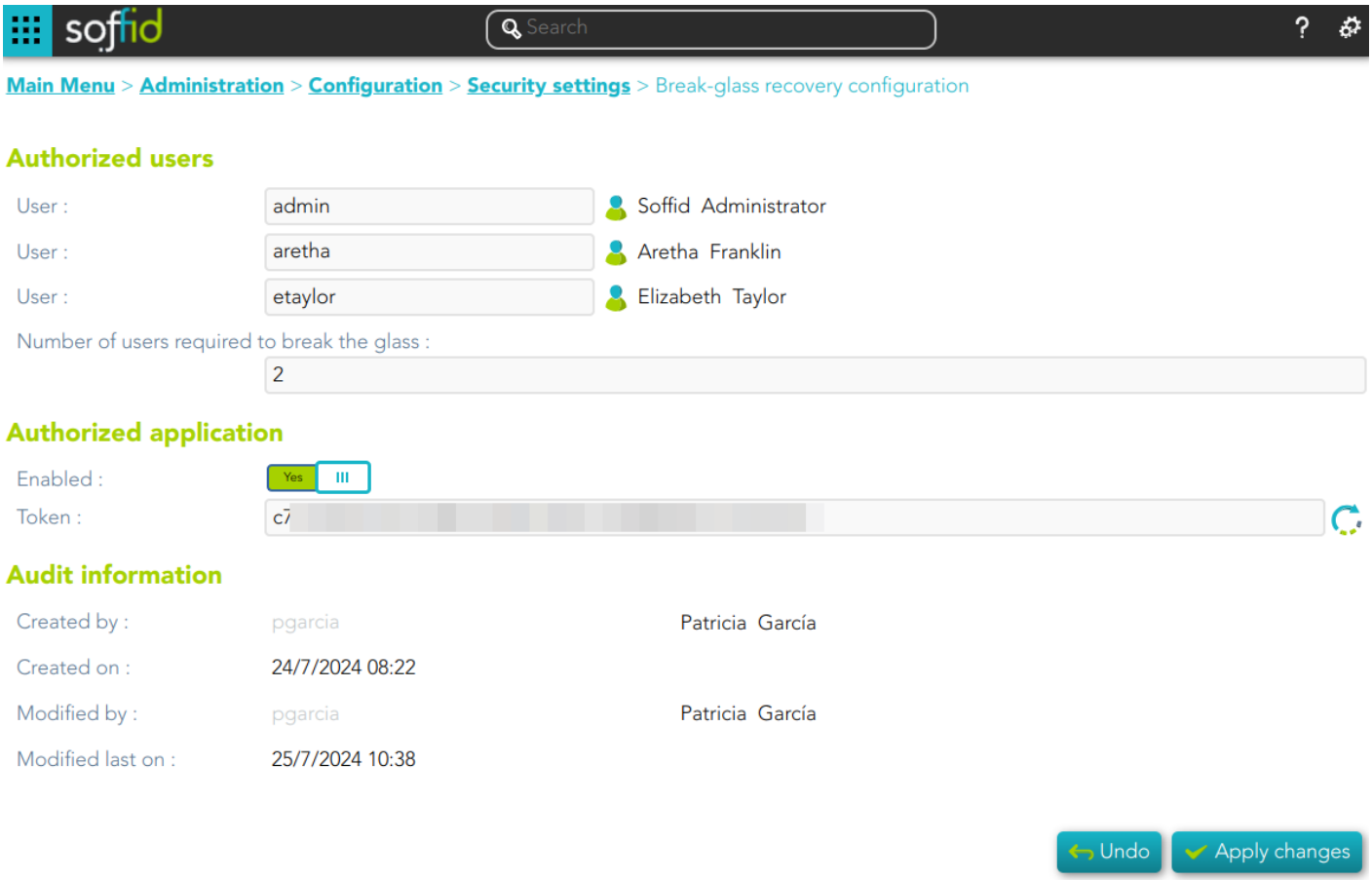
Break-glass recovery configuration

Definition

Break glass is the mechanism that allows users to gain emergency access to critical systems or information under exceptional circumstances when normal access procedures are not viable.

> For more information you can visit the Break Glass book.

Screen overview



Related objects

1. **User**

Standard attributes

Authorized users

Allows you to configure from one to three users to break glass

- **User**: allows you to choose the first users to break the glass.
- **User**: allows you to choose the second users to break the glass.
- **User**: allows you to choose the third users to break the glass.
- **Number of users required to break the glass**: this number allows you to configure the number of users required to break the glass

Authorized application

- **Enabled**: allows you to enable or disable the the break-glass recovery.
- **Token**: allows you to generate a new token by clicking the refresh icon.

Audit information

- **Created by**
- **Created on**
- **Modified by**
- **Modified last on**

Actions

Generate Token	Allows you to generate a new Token by clicking the refresh icon 
Apply changes	Allows you to update the changes made on the break glass recovery configuration.
Undo	Allows you to quit without applying any changes.