

AuthzServer

<http://<host IP authzserver>:9000/authzserver/>

As a requirement to create a Security Policy is necessary to previously provision:

- Security domain
- Organization
 - Users
- Source of identification

This guide will provision the different values associated to be used in the Pilot1

- Security domain = assist_pilot1
- Organization = transport_org
- Organization users
 - user1 / demo_truck1 (oauth2)
 - user2 / demo_truck2 (oauth2)
- Source of identification = mobileapp

AuthzServer Configuration

- Security Domain

Create a Security Domain

The screenshot shows the AuthzServer configuration interface. At the top, there is a navigation bar with five tabs: Home, Organizations, Security Domains, Data, and Security Policy. The 'Security Domains' tab is selected. Below the navigation bar, there is a sidebar with three options: Security Domains, Identification types, and Sources of identification. The 'Security Domains' option is selected. In the main content area, there is a text input field containing the text 'assist_pilot1'. To the right of the input field is an 'Add' button.

- Organization

Create organization

The screenshot shows the AuthzServer configuration interface. At the top, there is a navigation bar with five tabs: Home, Organizations, Security Domains, Data, and Security Policy. The 'Organizations' tab is selected. Below the navigation bar, there is a sidebar with two options: Organizations and Users. The 'Organizations' option is selected. The main content area is currently empty.

Add Organization

Name
Add

Later we will create/provision the users associated to this organization

- **Security Domain**

Associate the organization to the Security domain

Home
Organizations
Security Domains
Data
Security Policy

Security Domains
Identification types
Sources of identification

assist_pilot1

Organization

Role

transport_org
owner
Add

This step will link an Organization with a Security Domain

assist_pilot1

Organization

Role

transport_org
owner
Del

- **Identification types**

Different type of data for identification can be used. If not created, we can provide new types.

Home

Organizations

Security Domains

Data

Security Policy

Security Domains

Identification types

Sources of identification

Identification types

	carplatereader	Del
	qrreader	Del
	rfidreader	Del
	presencesensor	Del
	robotid	Del
	adminid	Del
	tokenid	Del
	oauth2	Del
		Add

- **Sources of identification**

We can create sources of identification for client app to use oauth as Identification type.

It is mandatory to select the Security Domain to be used.

Domain

assist_pilot1

Identifier	Identification type	
	oauth2	Add

Identifier must be associated with the name that will be used later in the client app for the resource (**idresource**).

In the example we will use as Identifier= **mobileapp**

assist_pilot1

Identifier	Identification type	
mobileapp	oauth2	Del

- **Organization/users**

Create users for organization transport_org

- user1

- user2

Create user1 for transport_org

transport_org

Username: user1 Add

A user in an organization can have different ways to be identified

user1 Del

Value	Identification type	
demo_truck1	oauth2	Add

Additional values for identification can be added. For example

- tokenid

transport_org

user1

Value	Identification type	
demo_truck1	oauth2	Del
1234567890xyz	tokenid	Del

Add

Create user2 for transport_org

transport_org

user1

user2

Value	Identification type	
demo_truck1	oauth2	Del
1234567890xyz	tokenid	Del

Value	Identification type	
demo_truck2	oauth2	Del
1234567890abc	tokenid	Del

Authserver will validate requests from user1 and user2 using the provisioned Identification types.

It will be necessary that the same value for user1 will be provisioned on the IdM.

The configuration guide to provision mobileapp and users is described here in IdM Keycloak clientapp configuration.

Federated Provider



Create a Federated Provider

Provider name = geolocation

Value set key name = userid



Value set key name should be the key name of the field used as reference for the value set.

Configure a Federated Provider

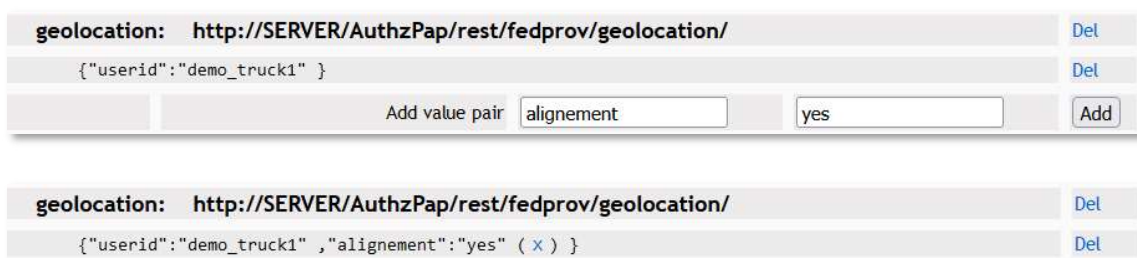
These values will feed an endpoint PIP to be checked when evaluate the policy.

- demo_truck1 / alignment / yes
- demo_truck2 /alignment / no

Assing a value-set for the value-set name created for the Federated Provider



Assign the values that the Federated provider will provide to later match with a Security Policy



To assign a new values that will be used to evaluate in security policy, repeat the process.

This is the result of the process for provisioning values to be consumed in the Data Provider

Data Provider



After configuration of a Data Provider. This will add an endpoint to be consumed by the AuthzServer and these data will be used to be evaluated in the Security Policy

<http://192.168.15.178:9000/authzserver/rest/fedprov/geolocation>

```
[{"userid":"demo_truck1","alignement":"yes"}, {"userid":"demo_truck2","alignement":"no"}]
```

Configure a Data Provider

Data provider values should be linked with the Provider name associated in the Federated Provider i.e., **geolocation** to be consumed as a URL in the PIP

- Name = geolocation_provider
- Domain = assist_pilot1_transport
- PIP URL
http://192.168.15.178:9000/authzserver/rest/fedprov/geolocation/<in_value>
- Input value = **object-id** (*)

Add Data provider				
PIP URL	/<in-value>			
Name	geolocation_provider	Domain	assist_pilot1_transport ▾	Add
Rest Method	GET ▾	Input value		

Complete the URL with the PIP using provider name and select the Domain

Add Data provider				
PIP URL	http://192.168.15.178:9000/authzserver/rest/fedprov/geolocation/<in-val			
Name	geolocation_provider	Domain	assist_pilot1_transport ▾	Add
Rest Method	GET ▾	Input value	object-id	

(*) In this case **object-id** due to the value will be associated to the type of identification for a user

user1 Del

Value	Identification type	
demo_truck1	oauth2	Del
123456789		

Username to identify the user in Authzserver. To use this username as Input Value in Data Providers, must use 'object-id'

This is the result after provisioning the PIP for the geolocation provider

assist_pilot1_transport_org

geolocation_provider	PIP URL: http://192.168.15.178:9000/authzserver/rest/fedprov/geolocation/<in-value>	Up Down Del
Method: GET	Input value: object-id	
Add Output values		
Out value		
Category	access-subject	Data type string
XACML url	urn:oasis:names:tc:xacml:1.0:subject:changeMe	Add

As a last step is necessary assign and change XACML URL to evaluate parameter i.e., we will give the name **alignementstatus** which will be the output to the variable set **alignement** configured for the value pair (alignment = yes, or alignment= no) assigned for the Provider name, in the Federated Provider section.

- Out value = alignement
- urn:oasis:names:tc:xacml:1.0:subject:alignementstatus

assist_pilot1_transport_org

geolocation_provider	PIP URL: http://192.168.15.178:9000/authzserver/rest/fedprov/geolocation/<in-value>	Up Down Del
Method: GET	Input value: object-id	
Add Output values		
Out value	alignement	
Category	access-subject	Data type string
XACML url	urn:oasis:names:tc:xacml:1.0:subject:alignementstatus	Add

Data provider created

assist_pilot1_transport_org

geolocation_provider	PIP URL: http://192.168.15.178:9000/authzserver/rest/fedprov/geolocation/<in-value>	Up Down Del
Method: GET	Input value: object-id	
alignement	access-subject	string Del
urn:oasis:names:tc:xacml:1.0:subject:alignementstatus		
Add Output values		
Out value		
Category	access-subject	Data type string
XACML url	urn:oasis:names:tc:xacml:1.0:subject:changeMe	Add

Security Policy

Create a security policy for the Security domain and Organization

Select a Security domain

Security domain

assist_pilot1

As previously linked Security domain will present the Organization associated with this security domain.

Security domain	Management policy	Status	Last deploy time			
assist_pilot1						
	Domain assist_pilot1_transport_org	Not initialized	Never	Edit	Clean	Export

Return

Create a Security Policy

Edit

Rules

Add Rule:

Permit

Add

Add Obligation:

Permit

area1-inalert

Add

Return

Add a Rule and Edit

Rules

Rule: 11	Effect: Permit	Edit	Delete
----------	----------------	------	--------

Add Rule:

Permit

Add

Edit

Rule: 11

Effect: Permit

Condition ID	Description (All must be met)				
Add Condition:		string	string-equal	access-subject	Add

An example for the Security Policy will evaluate

- Authenticated user input from an application consuming oauth2
- Alignment status between the truck and the crane simulated by the geolocation provider

```
[{"userid":"demo_truck1","alignement":"yes"}  
[{"userid":"demo_truck2","alignement":"no"}]
```

Security Policy is formed by rules. We can add Condition or Evaluations to a Rule.

Add Evaluation:	<input type="text"/>	string	string-equal	access-subject	Add
Add Condition:	<input type="text"/>	string	string-equal	access-subject	Add

We will create a security policy that will check

- Input data on action for a client app authenticated user
- Alignment status yes / no

Add new condition

- urn:oasis:names:tc:xacml:1.0:action:action-id

Add Condition:	<input type="text"/>	string	string-equal	action	Add
----------------	----------------------	--------	--------------	--------	-----

In the condition setting is mandatory to select **action**

The condition to be checked is action = start_unload_truck

In the condition setting is necessary to select **Value**

Cond: 32	Evaluations: (At least one must be met) (action) => urn:oasis:names:tc:xacml:1.0:action:action-id ----- string-equal ----- start_unload_truck(x) (Value)	<input type="text"/>	Add	Del	Delete Condition
----------	---	----------------------	-----	-----	------------------

Add a new condition in the rule

- urn: oasis:names:tc:xacml:1.0:subject:alignementstatus

Add Condition:	<input type="text"/>	string	string-equal	access-subject	Add
----------------	----------------------	--------	--------------	----------------	-----

In the condition setting is mandatory to select **access-subject**

The condition to be checked is alignementstatus = yes or alignementstatus = no

In the condition setting is necessary to select **value** (that will be replaced by yes or no)

Cond: 41	Evaluations: (At least one must be met) (access-subject) => urn:oasis:names:tc:xacml:1.0:subject:alignementstatus <input type="text"/> <input type="button" value="Add"/> Del ----- string-equal ----- yes(x) (Value)	<input type="button" value="Delete Condition"/>
----------	--	---

Rule 11 is formed with

- Cond: 32
- Cond: 41

Rule:11	Effect: Permit		
Condition ID	Description (All must be met)		
Cond: 32	Evaluations: (At least one must be met) (action) => urn:oasis:names:tc:xacml:1.0:action:action-id ----- <input type="text"/> <input type="button" value="Add"/> Del string-equal ----- start_unload_truck(x) (Value)	<input type="button" value="Delete Condition"/>	
Add Evaluation:	<input type="text"/> <input type="button" value="string"/> <input type="button" value="string-equal"/> <input type="button" value="access-subject"/> <input type="button" value="Add"/>		
Cond: 41	Evaluations: (At least one must be met) (access-subject) => urn:oasis:names:tc:xacml:1.0:subject:alignementstatus <input type="text"/> <input type="button" value="Add"/> Del ----- string-equal ----- yes(x) (Value)	<input type="button" value="Delete Condition"/>	

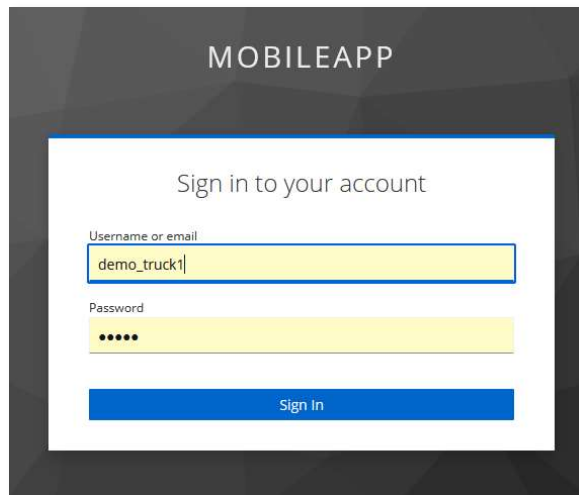
Once that the Security Policy is created it should be exported

Management domain policy exported						
Security domain	Management policy	Status	Last deploy time			
assist_pilot1						
Domain	assist_pilot1_transport_org	Exported	2022/10/06/12:42:47	<input type="button" value="Edit"/>	<input type="button" value="Clean"/>	<input type="button" value="Export"/>

Note: Authenticated user on an external application

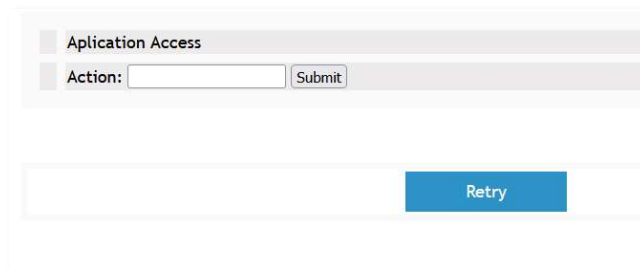
<http://192.168.15.178:8000/clientApp/mobileapp.jsp>

Redirection to IdM to authenticate the client application authentication against the IdM

A screenshot of a web application titled "MOBILEAPP". It features a "Sign in to your account" section with two input fields: "Username or email" containing the text "demo_truck1" and "Password" containing six dots. Below the fields is a blue "Sign in" button.

After user authentication the client application will accept input values to be evaluated in the Security Policy.

<http://192.168.15.178:8000/clientApp/mobileapp.jsp>

A screenshot of a web form titled "Application Access". It contains an "Action:" label followed by a text input field and a "Submit" button. Below this is a large empty text area and a blue "Retry" button.

Security policy rule will be created to evaluate application input on Action

start_unload_truck

Aplication Access

Action:

Retry