Soffid XACML Editor

Soffid XACML Editor

- XACML Editor
- Policy set
- Policy
- Policy reference
- Policy set reference
- Target
- Rules
- Variables
- Obligations
- Conditions
- Expressions

XACML Editor

Description

> Soffid Console provides a graphical interface, with a hierarchy structure, that allows the management of Policy Decision Points in a easy way. You can create new policy sets, policies, policy set references and policy references.

To start you only need to click the button with the add symbol (+) and start to configure the policy set.

Once you have created the root policy set, you can add new policy sets, polices, policy set references and policy references as your company need. You only need to click on the proper button and fulfill the data. You can add more than one root policy set.

Also, you can import a PolicySet into the system. You need click the import option on the hamburger icon and pick up the file to import, that file must be a well-formed XML.

Screen overview

https://www.youtube.com/embed/C3LMc4rrEQI?ref=0

Related objects

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

Actions

Add new	Allows you to add a new policy set. You can choose that option on the hamburger menu or click the add button (+). Second, you need to fulfill the mandatory fields, also the target, and the obligations, and apply changes.
Import	Allows you to import an XML file to add a new policy set. You can choose that option on the hamburger menu. Then you can pick up a .XML file and Soffid will import the file. If you cancel that operation, Soffil will not upload and save the file.
New policy set	Allows you to add a new policy set as a child of another policy set. You can choose that option under the proper policy set, and then fulfill the form.
New policy	Allows you to add a new policy as a child of another policy set. You can choose that option under the proper policy set, and then fulfill the form.
New policy reference	Allows you to add a new policy reference as a child of another policy set. You can choose that option under the proper policy set, and then fulfill the form.
New policy set reference	Allows you to add a new policy set reference as a child of another policy set. You can choose that option under the proper policy set, and then fulfill the form.

Policy set

Description

> A **PolicySet** is a container that can hold other Policies or PolicySets, as well as references to policies found in remote locations.
>
> - Policy Combining Algorithm
> - Target
> - Obligations

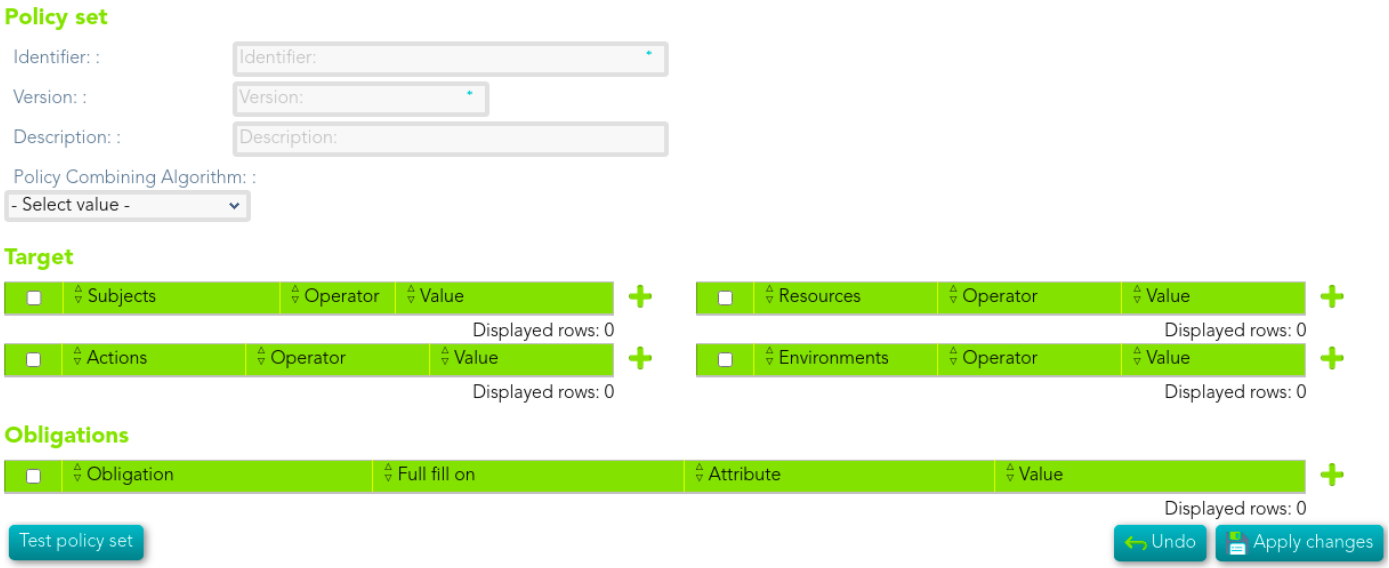
Every PolicySet contains a target and obligations, both can be empty.

The target contains the subjects, resources, actions and environments where the policy set will be applied. A target can contain more than one subject, environment, resource or action or none of them.

Policy Set can be exported to an XML file by clicking on Export button. The file will contain the Policy Set Target and all the elements included in it, like other PolicySets, Policies or References.

It is possible to create a new version for a PolicySet by clicking on 'Add new version'. That will copy all PolicySet elements on the tree with the following version number.

Screen overview



Related objects

- **Policy**
- **Policy set reference**
- **Policy reference**
- **Target**
- **Obligations**

Standard attributes

- **Identifier**: identify the policy set.
- **Version**: version of the policy set.
- **Description**: brief description of the policy set.
- **Policy Combining Algorithm:** determines how the different Policies in the PolicySet will be applied. You can visit the XACML Rule combining algorithm page for more information.
- **Target:** The policy result will be MATCHES if it all the target elements defined match.
  - Subjects
  - Resources
  - Actions
  - Environments
- **Obligations**

Actions

Apply changes	Allows you to save the data of a new policy set or to update the data of a specific policy set. To save the data it will be mandatory to fill in the required fields
Undo	Allows you to quit without applying any changes.
Delete	Allows you to delete a policy set. You can choose that option on the trash icon. To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Export	Allows you to export a XML file that contain the policy set.
Add new version	Allows you to add a new versión of the policy set.
Test policy set	Allows you to test the policy set creating the XML file necessary with the defined policies and rules.

---

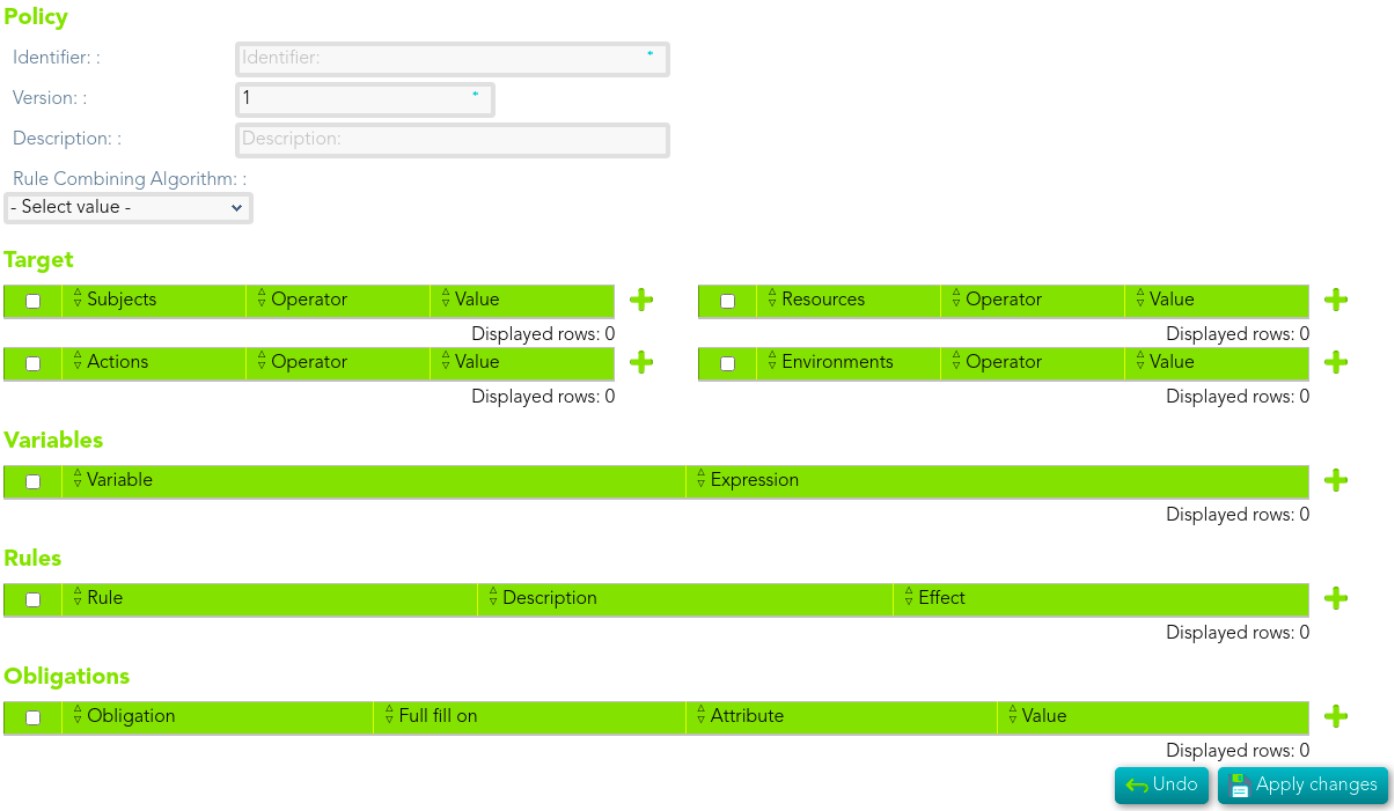
https://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html

Policy

Description

> A Policy represents a single access control policy, expressed through a set of Rules.
>
> - Policy Combining Algorithm
> - Target
> - Variables
> - Rules
> - Obligations

Screen overview



Related objects

- **Policy set**
- **Target**
- **Variables**
- **Rules**
- **Obligations**

Standard attributes

Policy set

- **Identifier**: identify the policy.
- **Version**: version of the policy.
- **Description**: brief description of the policy.
- **Policy Combining Algorithm:** determines how the different rules will be applied. You can visit the XACML Rule combining algorithm page for more information.

Target

The policy result will be MATCHES if it all the target elements defined match.

- Subjects
- Resources
- Actions
- Environments

Variables

- Variables

Rules

- Rules

Obligations

- Obligations

Actions

Apply changes	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
Undo	Allows you to quit without applying any changes.
Delete	Allows you to delete a policy. You can choose that option on the trash icon.To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Export	Allows you to export a XML file that contain the policy.
Add new version	Allows you to add a new versión of the policy.

---

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

Policy reference

Description

The policy reference is used to reference a policy element. The reference is made by id of the policy. However, the mechanism for resolving a policy set reference to the corresponding policy is outside the scope of this specification.

Related objects

- **Policy**

Standard attributes

- **Identifier**: policy set identifier.
- **Version**:
  - **Specific version**: specifies a matching expression for the version of the policy referenced
  - **Version range**: specifies a range of version
  - **Any version**

Actions

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

Export	Allows you to export a XML file that contain the policy reference.
Add new version	Allows you to add a new versión of the policy reference

---

http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

Policy set reference

Description

The policy set reference is used to reference a policy set element. The reference is made by id of the policy set. However, the mechanism for resolving a policy set reference to the corresponding policy set is outside the scope of this specification.

Related objects

- **Policy set**

Standard attributes

- **Identifier**: policy set identifier.
- **Version**:
  - **Specific version**: specifies a matching expression for the version of the policy set referenced
  - **Version range**: specifies a range of version
  - **Any version**

Actions

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

Export	Allows you to export a XML file that contain the policy set reference.
Add new version	Allows you to add a new versión of the policy set reference

---

http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

Target

Description

Defines to which access requests a policy or rule applies. In XACML all the attributes are categorized into four main categories:

- **Subjects**
- **Resources**
- **Actions**
- **Environments**

A target can contains more than one subject, environment, resource or action or none of them. The target is the way to define the scope of an autorization policy. The result will be MATCHES if it all the target elements defined match.

- **Attribute Designator**: lets the policy specify an attribute with a given name and type, and optionally an issuer as well.
- **Attribute Value**: contains a literal attribute value.

Screen



Related objects

- **Policy set**
- **Policy**
- **Rules**

Categories

Subjects

> An actor whose attributes may be referenced by a predicate.

Represents the entity making a request for access to a resource.

Allows you to add one or more subjects as a target where the policy will be applied.

To configure a subject, first of all you need to select an attribute. You can select a value for an attribute designator list, or write the attribute selector value and select the data type.

Then, you need to select the operator, it will be used to compare or compute attributes.

And finally, you need to set a value, with which the attribute will be computed or compared. The value data type depends on the attribute data type.

Resources

> Data, service or system component.

Allows you to add one or more resources as a target where the policy will be applied.

To configure a resource, first of all you need to select an attribute. You can select a value for a attribute designator list, or write the attribute selector value and select the data type.

Then, you need to select the operator, it will be used to compare or compute attributes.

And finally, you need to set a value, with which the attribute will be computed or compared. The value data type depends on the attribute data type.

Actions

> An operation on a resource.

Allows you to add one or more actionss as a target where the policy will be applied.

To configure an action, first of all you need to select an attribute. You can select a value for a attribute designator list, or write the attribute selector value and select the data type.

Then, you need to select the operator, it will be used to compare or compute attributes.

And finally, you need to set a value, with which the attribute will be computed or compared. The value data type depends on the attribute data type.

Environments

> The set of attributes that are relevant to an authorization decision and are independent of a particular subject, resource or action.

Allows you to add one or more environments as a target where the policy will be applied.

To configure an environment, first of all you need to select an attribute. You can select a value for a attribute designator list, or write the attribute selector value and select the data type. The

Then, you need to select the operator, it will be used to compare or compute attributes.

And finally, you need to set a value, with which the attribute will be computed or compared. The value data type depends on the attribute data type.

Actions

The behavior of the actions is the same in each category, subjects, actions, resources and environments.

Add new	Allows you to add a new element to the list. To add a new element you need to click the add button, located at the end of the header and fulfill the form and save the data.
Delete	Allows you to delete an element to the variable list. To delete the element, you need to click the element you want to delete, and click the button with the subtraction symbol (-) at the end of the record. To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Close	Allows you to save the data of a new element or to update the data of a specific element. To save the data it will be mandatory to fill in the required fields

Undo	Allows you to quit without applying any changes.

---

https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

Rules

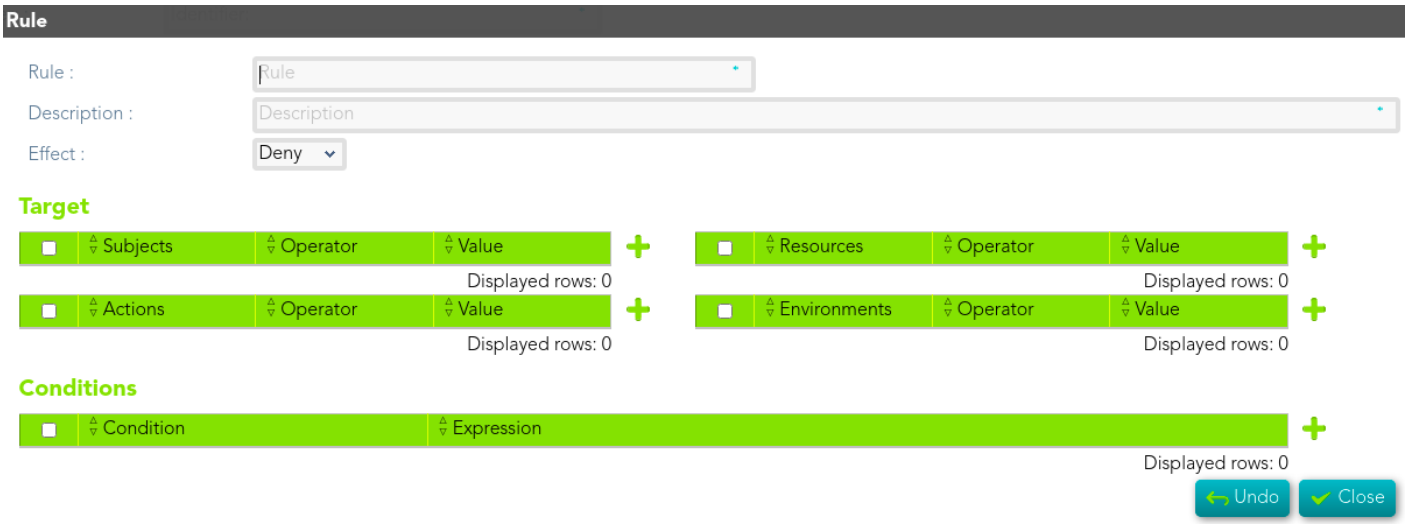
Description

> A rule is the most elementary unit of policy. It may exist in isolation only within one of the major actors of the XACML domain. In order to exchange rules between major actors, they must be encapsulated in a policy. A rule can be evaluated on the basis of its contents.

Each rule sets a specific condition for allowing or denying access to a resource.

A rule is composed by a target, an effect and a condition. It is able to add more than one rule to the policy.

Screen overview



Related objects

- **Policy**

- **Target**
- **Conditions**

Standard attributes

- **Rule**: rule name.
- **Description**: brief description of the rule.
- **Effect**: "Rule effect declaration. When a rule evaluates to ‘True’ it emits the value of the Effect attribute. This value is then combined with the Effect values of other rules according to the rule combining algorithm."Two values are allowed:
  - Permit.
  - Deny.
- **Target**
- **Conditions**

Actions

Add new	Allows you to add a new rule to the rules list. To add a new rule you need to click the add button, located at the end of the header and fulfill the form and save the data.
Delete	Allows you to delete a rule to the rules list. To delete the rule, you need to click the rule you want to delete, and click the button with the subtraction symbol (-) at the end of the record. To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Close	Allows you to save the data of a new rule or to update the data of a specific variable. To save the data it will be mandatory to fill in the required fields
Undo	Allows you to quit without applying any changes.

---

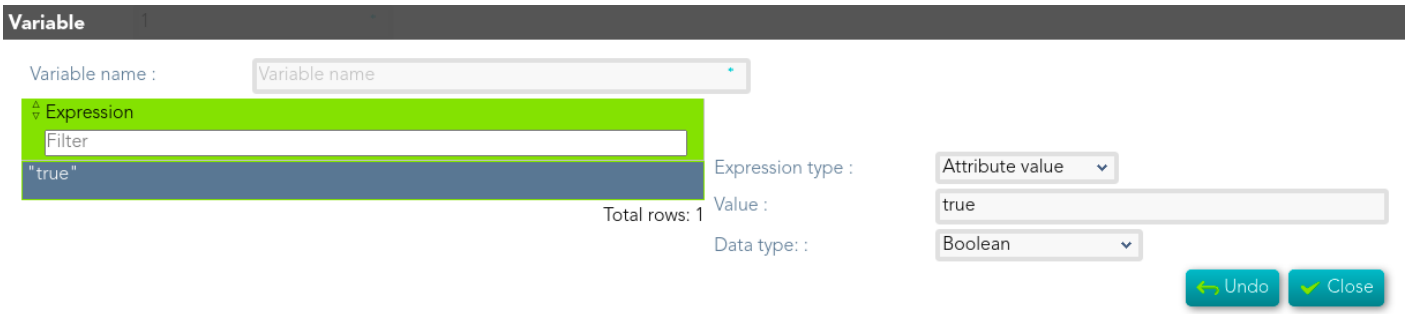
https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

Variables

Description

> Variables are the elements to define functions that may be used througthout the policy.

Screen overview



Related objects

- **Policy**
- **Expressions**

Standard attributes

- **Variable name**: Name to identify the variable.
- **Expressions**: Any element of ExpressionType complex type.

Actions

Add new	Allows you to add a new variable to the variables list. To add a new variable you need to click the add button, located at the end of the header and fulfill the form and save the data.
Delete	Allows you to delete a variable to the variable list. To delete the variable, you need to click the variable you want to delete, and click the button with the subtraction symbol (-) at the end of the record. To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Close	Allows you to save the data of a new variable or to update the data of a specific variable. To save the data it will be mandatory to fill in the required fields
Undo	Allows you to quit without applying any changes.

---

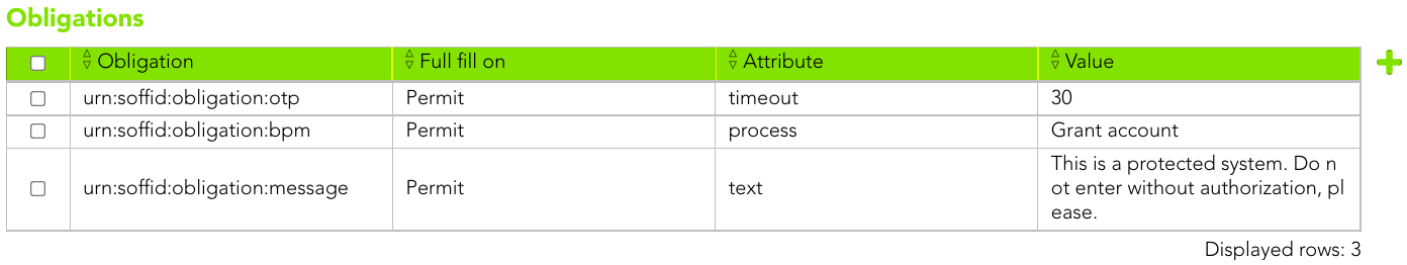
https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

Obligations

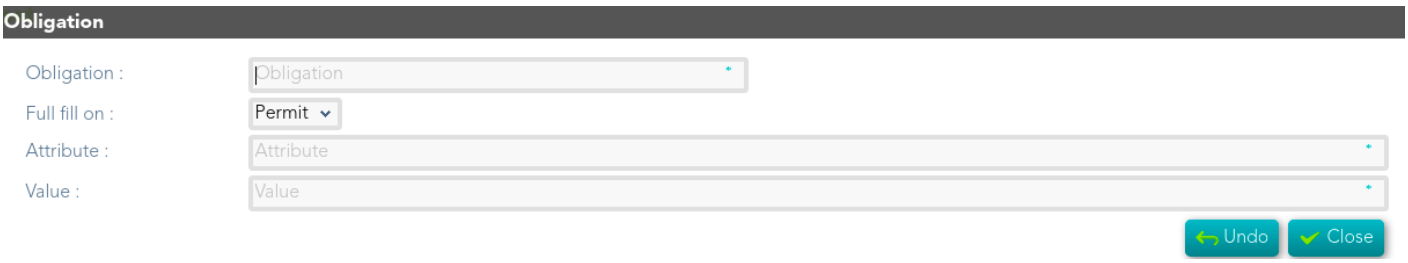
Description

> XACML defines obligations as actions that have to be returned to the PEP with the PDP response XACML .
>
> If the PDP's evaluation is viewed as a tree of rules, policy sets and policies, each of which returns "Permit" or "Deny", then the set of obligations returned by the PDP to the PEP will include only the obligations associated with those paths where the effect at each level of evaluation is the same as the effect being returned by the PDP.

Screen Overview



Add Obligation



Related objects

- **Policy set**
- **Policy**

Standard attributes

- **Obligation**:
  - urn:soffid:obligation:otp
  - urn:soffid:obligation:message
  - urn:soffid:obligation:bpm
  - urn:soffid:obligation:session-recording
  - urn:soffid:obligation:notify-owner
- **Full fill on**:
  - Permit
  - Deny
- **Attribute**:
  - **text**: message that will be showed.
  - **process**: process that will be launched.
  - **timeout**: period of time the otp code will be valid for.
- **Value**: the value of the attribute.

OBLIGATION	ATTRIBUTE
urn:soffid:obligation:otp	timeout
urn:soffid:obligation:message	text
urn:soffid:obligation:bpm	process

Actions

Add new	Allows you to add a new obligation to the obligations list. To add a new obligation you need to click the add button, located at the end of the header and fulfill the form and save the data.

Delete	Allows you to delete an obligation to the obligations list. To delete the obligation, you need to click the obligation you want to delete and click the button with the subtraction symbol (-) at the end of the record. To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Close	Allows you to save the data of a new variable or to update the data of a specific variable. To save the data it will be mandatory to fill in the required fields
Undo	Allows you to quit without applying any changes.

---

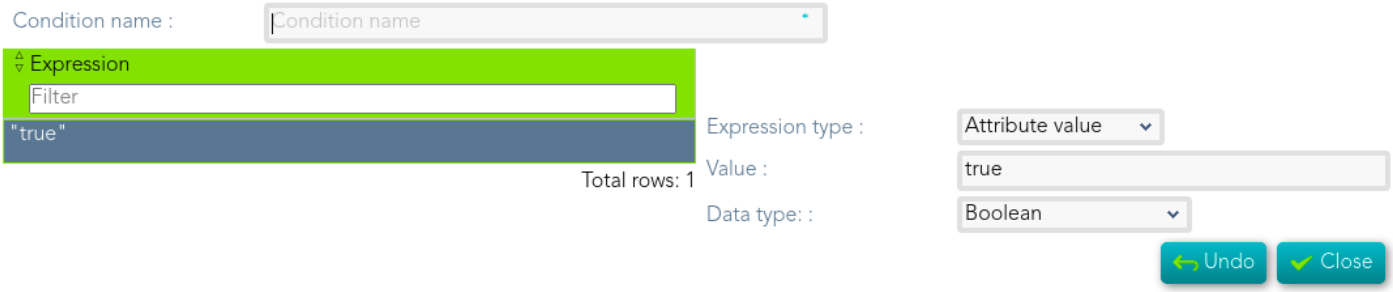
http://www.oasis-open.org/committees/xacml/

Conditions

Description

> Condition represents a Boolean expression that refines the applicability of the rule beyond the predicates implied by its target. Therefore, it may be absent.

Screen overview



Related objects

- **Policy**
- **Expressions**

Standard attributes

- **Condition name**: Name to identify the condition.
- **Expressions**: any element of ExpressionType complex type that return true or false.

Actions

Add new	Allows you to add a new condition to the conditions list. To add a new condition you need to click the add button, located at the end of the header and fulfill the form and save the data.
Delete	Allows you to delete a condition to the variable list. To delete the condition, you need to click the condition you want to delete, and click the button with the subtraction symbol (-) at the end of the record. To perform that action, Soffid will ask you for confirmation, you could confirm or cancel the operation.
Close	Allows you to save the data of a new condition or to update the data of a specific condition. To save the data it will be mandatory to fill in the required fields
Undo	Allows you to quit without applying any changes.

---

https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

Expressions

Description

> The Expression signifies that an element that extends the ExpressionType and is a member of the Expression substitution group shall appear in its place. The Expression is not used directly in a policy.

Expressions are elements that allow to evaluate conditions within rules and policies to make access decisions.

Related objects

- **Variables**
- **Conditions**

Standard attributes

The attributes depend on the Expression type selected.

EXPRESSION TYPE	OTHER FIELDS	DATA TYPE
Attribute value	**Value**: alfanumeric field	Available data types.
Resource	**Attribute designator** • URL • Soffid object • Account name • System name • Login name • Vault folder • Access level	Available data types.

EXPRESSION TYPE	OTHER FIELDS	DATA TYPE
Subject	**Attribute designator** • User • User attributes • Account • System • Role • Group • Primary Group • IP Address	Available data types.
Action	**Attribute designator**: • method	Available data types.
Environment	**Attribute designator**: • Country • Current Time • Current Date • Current DateTime	Available data types.
Attribute selector	**Attribute selector**: alphanumeric field	Available data types.
Variable	**Variable**: alfanumeric field	--
Function	**Function type**: • Comparison • Arithmetic • Conversions • Date conversions • Boolean Operators • String Functions • Set Functions • Bag Functions • HigherOrderBagFunctions • XPath	Available data types.

EXPRESSION TYPE	OTHER FIELDS	DATA TYPE
Function name	**Function type**: • Comparison • Arithmetic • Conversions • Date conversions • Boolean Operators • String Functions • Set Functions • Bag Functions • HigherOrderBagFunctions • XPath **Function**: the value depends on the function type selected.	Available data types.

Data Type

Available data types

- String:
- Boolean
- Integer
- Double
- Date and time
- Date
- Time
- HEX-encoded binary
- URI
- Year-month duration
- Day-time duration
- Base 64 binary
- X. 500 name
- RFC822 name

---

https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf