2016

SAFAX

User Manual

TU/e Security Group

Table of Contents

Chapter 1

Introduction

1.1 Purpose

Cloud storage services have become increasingly popular in recent years. Users are often registered to multiple cloud storage services that suit different needs. However, the ad-hoc manner in which data sharing between users is implemented leads to issues for these users. For instance, users are required to define different access control policies for each cloud service they use and are responsible for synchronizing their policies across different cloud providers. Users do not have access to a uniform and expressive method to deal with authorization. Current authorization solutions cannot be applied *as-is*, since they cannot cope with challenges specific to cloud environments.

In order to address these challenges we have developed SAFAX [1], an extensible authorization framework offered as a service. SAFAX provides a novel XACML-based architectural framework tailored to the development of extensible authorization services for clouds. The key design principle underlying SAFAX is that all components are loosely coupled services, thus providing the flexibility, extensibility and scalability needed to manage authorizations in cloud environments. SAFAX's architecture allows users to: *a)* deploy their access control policies in a standard format; *b)* in a single location; and *c)* augment policy evaluation with information from user selectable external trust services.

In order to ease the management of policies and configuration of policies, SAFAX provides users with a Graphical User Interface (referred as SAFAX GUI) that communicates with the SAFAX services.

This document presents the functionalities for users provided by the SAFAX GUI.

1.2 List of Acronyms and Definitions

1.2.1 List of Acronyms

CH: Context Handler

GUI: Graphical User Interface

PAP: Policy Administration Point

PEP: Policy Enforcement Point

PIP: Policy Information Point

SAFAX: eXtensible Authorization Framework As a Service

UDF: User Defined Function

XACML: eXtensible Access Control Markup Language

1.2.2 List of Definitions

Guest user: A user that does not provide login details but still uses SAFAX application.

SAFAX: An extensible authorization framework offered as a service.

User: The user of SAFAX

1.3 Overview

SAFAX provides a graphical user interface (GUI) that allows users to create new projects (Section 2.6), configure (Section 2.7) or remove (Section 2.8) existing projects. Users can create new demos contained in existing projects (Section 2.9), remove existing demos (Section 2.17). After creating projects and demos, users can upload access requests (Section 2.12) and policies (Section 2.10). Users can evaluate an access request against authorization policies and review access decisions (Section 2.15). After evaluating policies, users can view detailed logs of their current and past sessions (Section 2.18). If users have any problem while using SAFAX, they can report to administrators (Section 2.20). To support the evaluation of access requests in distributed and collaborative environments, components in the XACML reference architecture [7] are implemented as loosely coupled web services in SAFAX (Section 2.17). Therefore, each SAFAX component is self-contained and does not depend on the contexts or states of other components. This allows users to choose different web services (Section 2.16) from different third-party vendors who register their services with SAFAX. This also allows advanced features (Chapter 3) to be added to SAFAX while core functionalities are still maintained (Chapter 2). Detailed example demos that contain access requests, authorization policies, and necessary demo and component configurations can be found in Examples project (Chapter 4).

Chapter 2

Basic Functionalities

2.1 Welcome Screen

2.1.1 Functional Description

The users land here when they are not logged in and want to use the application.

2.1.2 Caution and Warning

Not applicable.

2.1.3 Formal Description

The Welcome screen is shown in Figure 2.1. The user can choose to create a new account, continue using the application with an existing account, or use the guest account.

2.1.4 Related

- The *Login* button gives the Login screen (Section 2.2).
- The *Sign Up* button gives the Register screen (Section 2.3).
- The Login as Guest button gives the Continue without registering to SAFAX (Section 2.4)

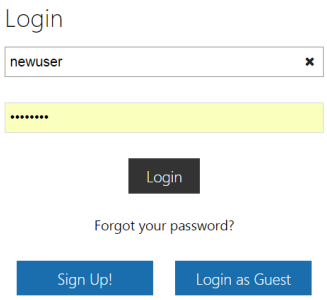


Figure 2.1 Welcome screen

2.2 Login Screen

2.2.1 Functional Description

The user can login using a previously created account.

2.2.2 Caution and Warning

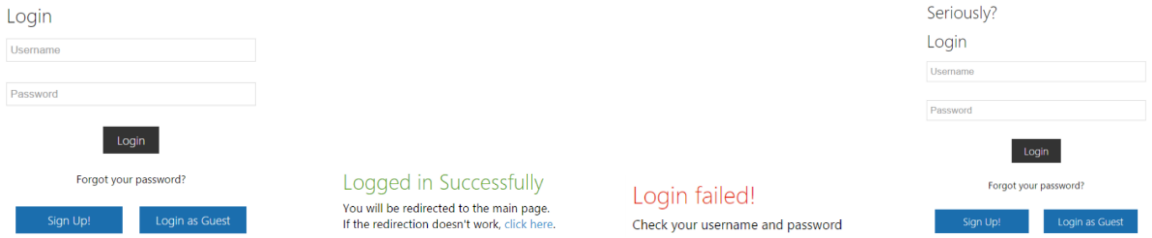
- When the user does not fill in the email field, the screen in Figure 2.2(d) is shown.
- When the user does not fill in the password field, the screen in Figure 2.2(d) is shown.
- When the user enters the wrong password, the user cannot be authenticated and the screen in Figure 2.2(c) is shown.

2.2.3 Formal Description

The user enters username and password.

2.2.4 Related

- When successfully logged in the user is redirected to the Home screen (Section 2.5).



a. Login screen b. Login success c. Login failure d. Login error

Figure 2.2 Login screen

2.3 Register Screen

2.3.1 Functional Description

The user can request an account by clicking *Register* in the menu. After this, the system administrator should activate the account.

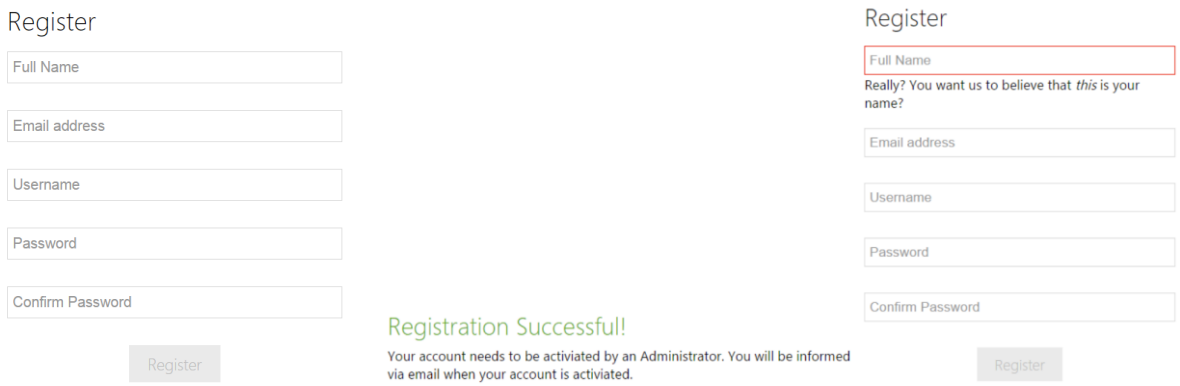
2.3.2 Caution and Warning

- When the user does not fill in the necessary information, the screen in Figure 2.3.1(c) is shown.

2.3.3 Formal Description

In the registration form (Figure 2.3.1(a)), the user should fill in the following information:

- Full name
- Email address
- Username,
- Password
- Confirm password



a. Registration form b. Registration success c. Registration error

Figure 2.3.1 Registration Screen

2.3.4 Related

- Upon completion of the registration process, a notification is sent to the system's administrator for approval. The user will be notified when the account has been approved by system's administrator (Figure 2.3.2)

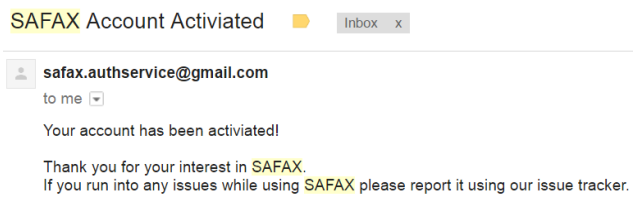


Figure 2.3.2 SAFAX Account Activated Notification

2.4 Continue Without Account Screen

2.4.1 Functional Description

The user can login without using an account.

2.4.2 Caution and Warning

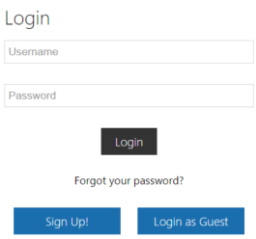
Not applicable.

2.4.3 Formal Description

The user can continue using the application without an existing account.

2.4.4 Related

- When successfully logged in by using a guest account, the user is redirected to the Home screen (Section).



a. Login screen

b. Login success

Figure 2.4 Login screen

2.5 Home Screen

2.5.1 Functional Description

The user can access SAFAX functionalities.

2.5.2 Caution and Warning

Not applicable.

2.5.3 Formal Description

The Home screen is shown in Figure 2.5. From here the user can see a list of projects. User can also use the main navigation menu to access SAFAX functionalities.

2.5.4 Related

- The *Home* button gives the Home screen (Section 2.5).
- The plus icon near *Projects* heading gives the Create Project screen (Section 2.6)
- The *Policy Evaluation* button gives the Policy Evaluation screen (Section 2.7).

- The *Service Registry* button gives the Service Registry screen (Section 2.18).
- The *Account Activity* button gives the Report Issues screen (Section 2.19).
- The *Issue Tracker* button gives the Report Issues screen (Section 2.20).
- The *About* button gives the About screen (Section 2.21).
- The *Help* button gives the Help screen (Section 2.22).
- The *Settings* button gives the Setting screen (Section 2.23).
- The *Log out* button gives the Logout screen (Section 2.24).

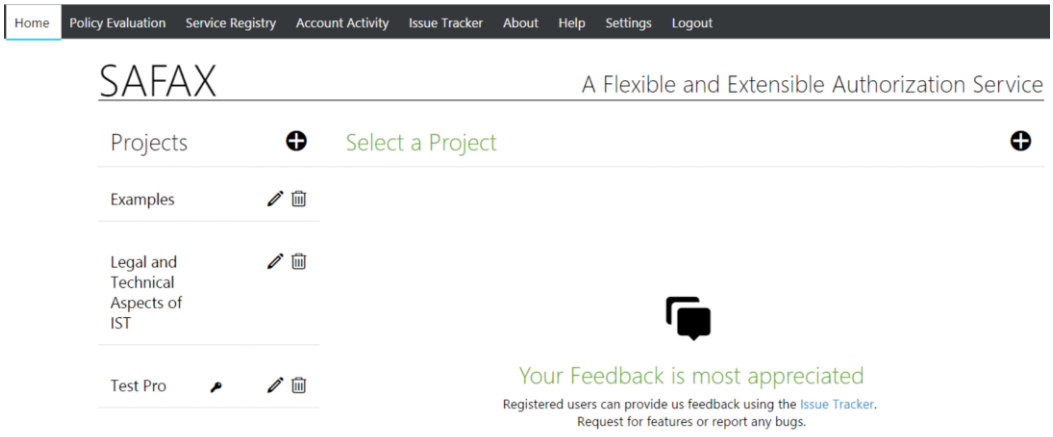


Figure 2.5 Welcome screen

2.6 Create Project Screen

2.6.1 Functional Description

Users can add new projects.

2.6.2 Caution and Warning

- When the user creates more than the allowed number of projects, the error in Figure 2.6(b) is shown.

2.6.3 Formal Description

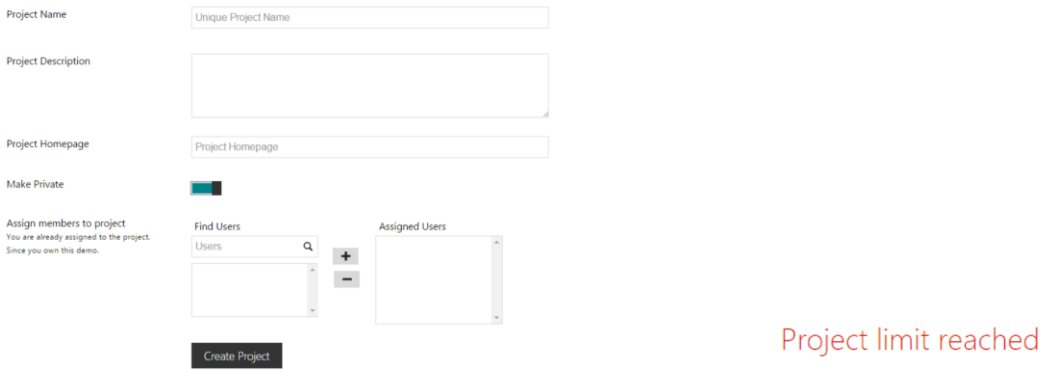
On the home page of SAFAX, click on the plus icon near *Projects* heading. The screen in Figure 2.6(a) will be displayed. The user can fill in the following information:

- Project name
- Project description
- Project homepage
- Project visibility (public or private)
- Project member

After clicking the *Create Project* button, the project is created.

2.6.4 Related

Not applicable.



a. Create project form a. Create project error

Figure 2.6 Create Project screen

2.7 Configure Existing Project Screen

2.7.1 Functional Description

Users can modify existing project information.

2.7.2 Caution and Warning

- When the user does not have the rights to remove existing projects, an error in Figure 3.7(c) is shown

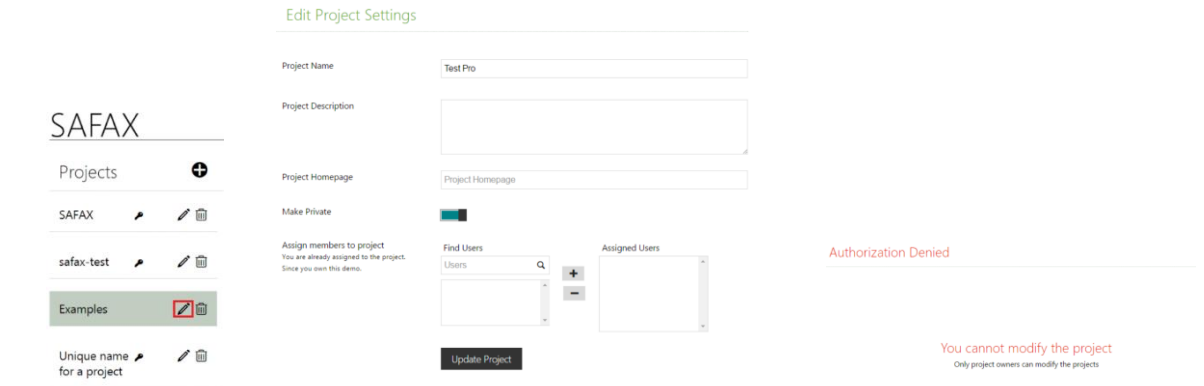
2.7.3 Formal Description

On the home page of SAFAX, below *Projects* heading, there is a list of existing projects. In the list, click the pencil icon near an existing project to navigate to the project configuration interface of that project (Figure 2.7(a)). The configuration form, as shown in Figure 2.7(b) will show up. Users can change project information such as name, description, and website. Users can also share project with a number of users or all users by making the project public.

Finally, click *Update Project* button to save the changes.

2.7.4 Related

Not applicable.



a. Modify project button b. Edit project setting form c. Edit project error

Figure 2.7 Configure existing project screen

2.8 Remove Existing Project Screen

2.8.1 Functional Description

Users can remove existing projects.

2.8.2 Caution and Warning

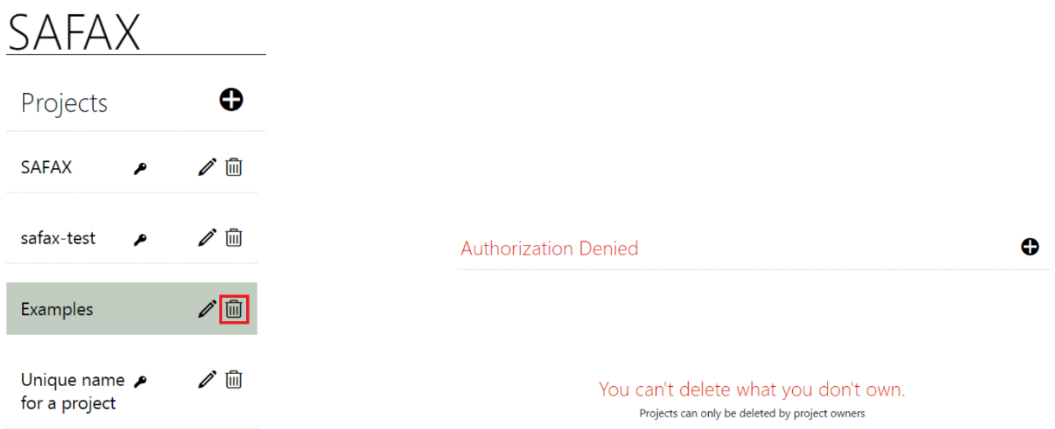
- When the user does not have the rights to remove existing projects, an error in Figure 2.8(b) is shown

2.8.3 Formal Description

On the home page of SAFAX, below *Projects* heading, there is a list of existing projects. In the list, click the trash icon near an existing project to remove that project (Figure 2.8(a)).

2.8.4 Related

Not applicable.



a. Remove project button b. Remove project error

Figure 2.8 Remove existing project screen

2.9 Create Demo Screen

2.9.1 Functional Description

Users can add new demos.

2.9.2 Caution and Warning

Not applicable.

2.9.3 Formal Description

On the home page of SAFAX, click on an existing project. A list of demos of that project is displayed on the screen (Figure 2.9.1). Click the plus icon near *Demos configured for this project* heading. The screen, as shown in Figure 2.9.2 will show up. Now fill in the following information:

- Demo name
- Demo description

Finally, click *Create Demo* button.

2.9.4 Related

- After successfully creating a demo, users can upload authorization policies to this demo (Section 2.10)
- After successfully creating a demo, users can upload access requests to this demo (Section 2.12)
- Demo information can be changed later by users (Section 2.14)

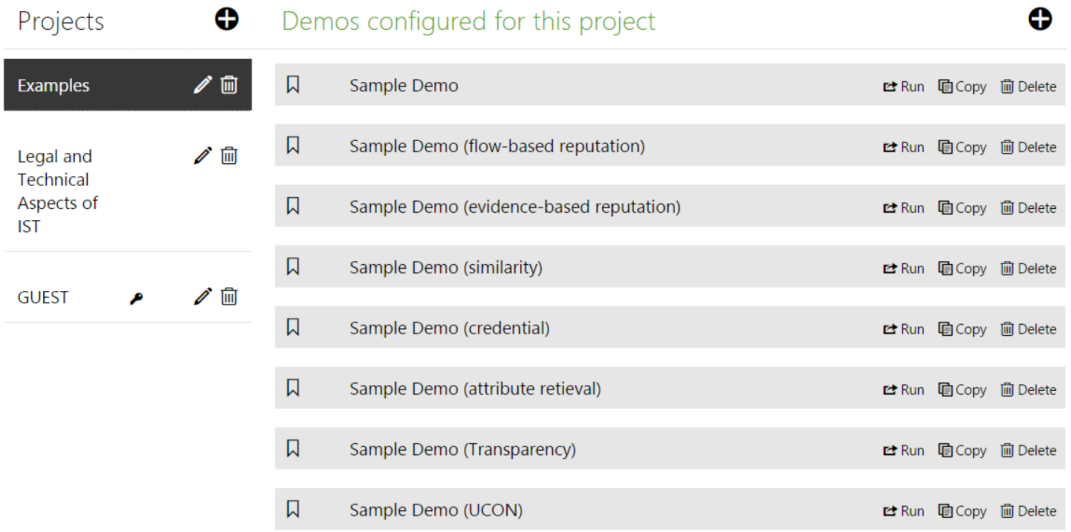


Figure 2.9.1 Demo list

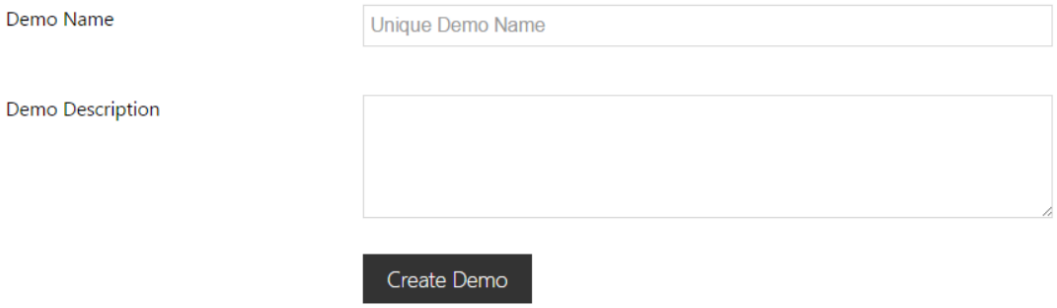


Figure 2.9.2 Create demo form

2.10 Upload Policy Screen

2.10.1 Functional Description

Users can upload authorization policies to existing demos.

2.10.2 Caution and Warning

- When the user does not have the rights to upload policies to an existing demo, the XACML settings are shown in grey (Figure 2.10.2).

2.10.3 Formal Description

On the home page of SAFAX, click on an existing project. A list of demos of that project is displayed on the screen (Figure 2.9.1). Click to choose an existing demo. The screen in Figure 2.10.1 will be displayed. Now use the upload icon below *XACML* headings to upload a policy to this demo.

2.10.4 Related

Not applicable.

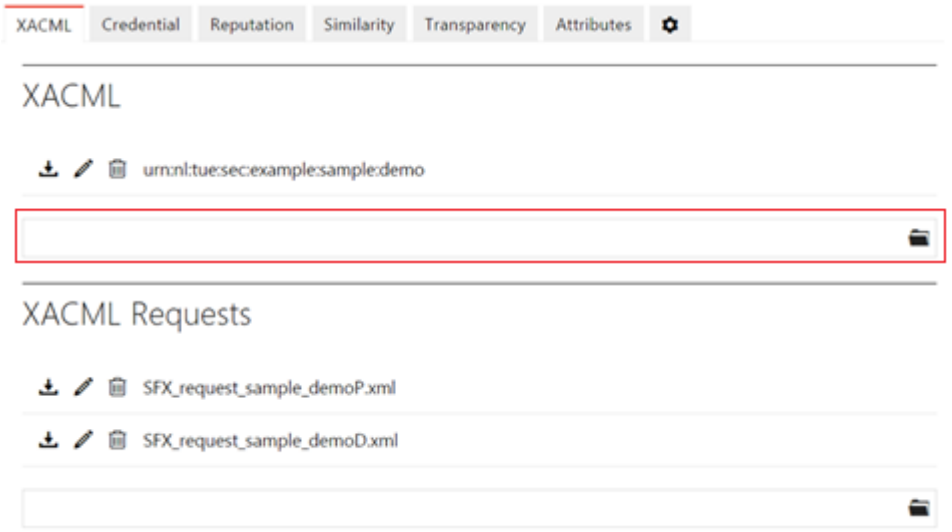


Figure 2.10.1 Upload policy screen

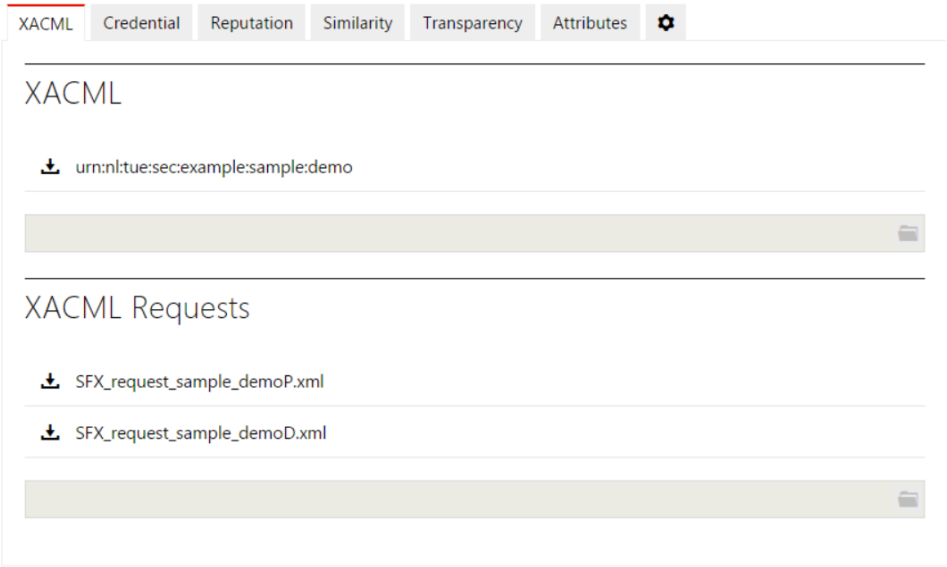


Figure 2.10.2 Upload policy error

2.11 Remove Existing Policy Screen

2.11.1 Functional Description

Users can remove existing authorization policies of an existing demo.

2.11.2 Caution and Warning

- When the user does not have the rights to remove policies from an existing demo, the XACML settings are shown in grey (Figure 2.11.2).

2.11.3 Formal Description

On the home page of SAFAX, click on an existing project. A list of demos of that project is displayed on the screen (Figure 2.9.1). Click to choose an existing demo. The screen, as shown in Figure 2.11.1 will show up. Now use the trash icon to remove a policy from this demo.

2.11.4 Related

Not applicable.

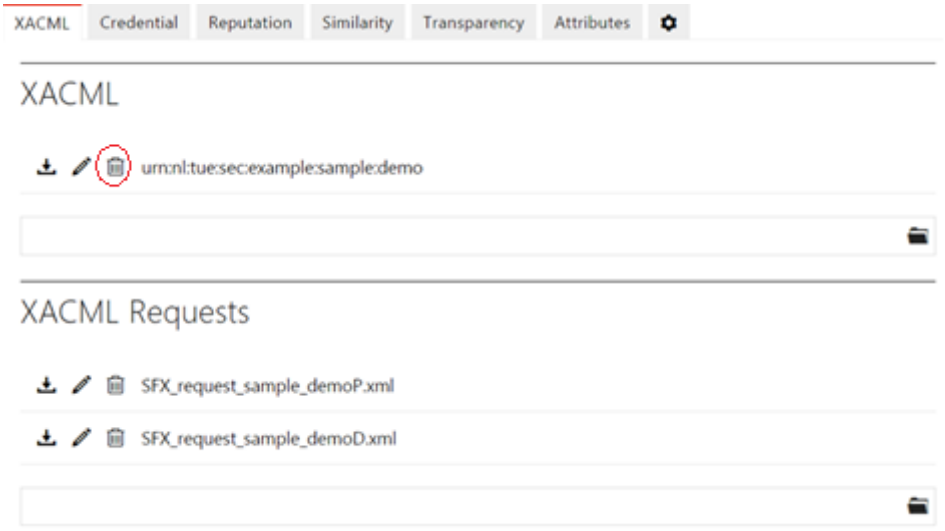


Figure 2.11.1 Remove policy screen

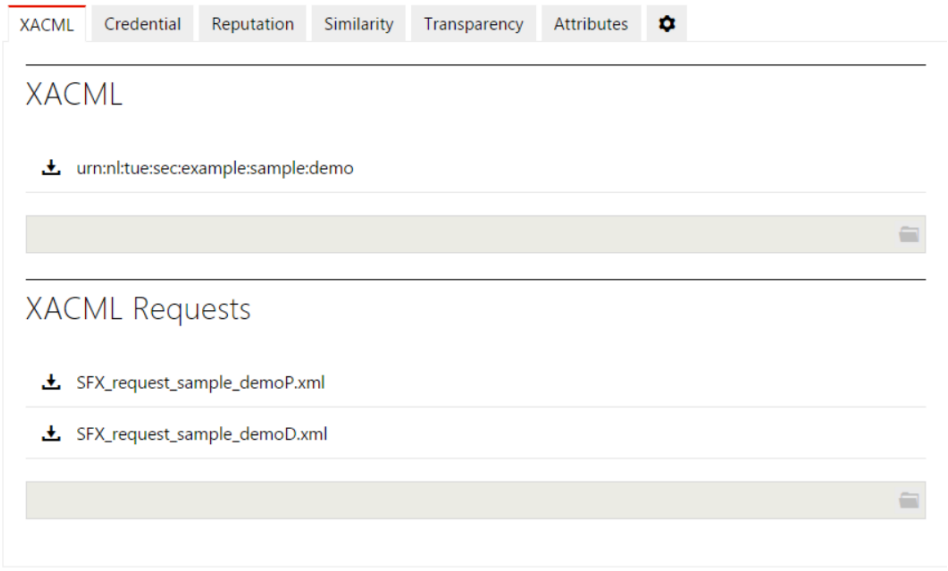


Figure 2.10.2 Remove policy error

2.12 Upload Request Screen

2.12.1 Functional Description

Users can upload access requests to existing demos.

2.12.2 Caution and Warning

- When the user does not have the rights to upload access requests to an existing demo, the XACML settings are shown in grey (Figure 2.12.2).

2.12.3 Formal Description

On the home page of SAFAX, click on an existing project. A list of demos of that project is displayed on the screen (Figure 2.9.1). Click to choose an existing demo. The screen in Figure 2.12.1 will show up. Now use the upload icon below *XACML Requests* heading to upload a policy to this demo.

2.12.4 Related

Not applicable.

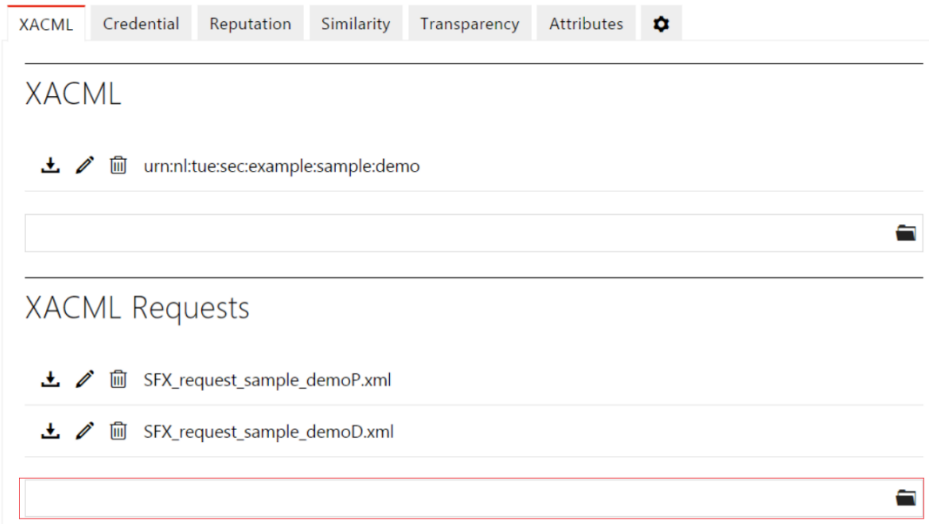


Figure 2.12.1 Upload request screen

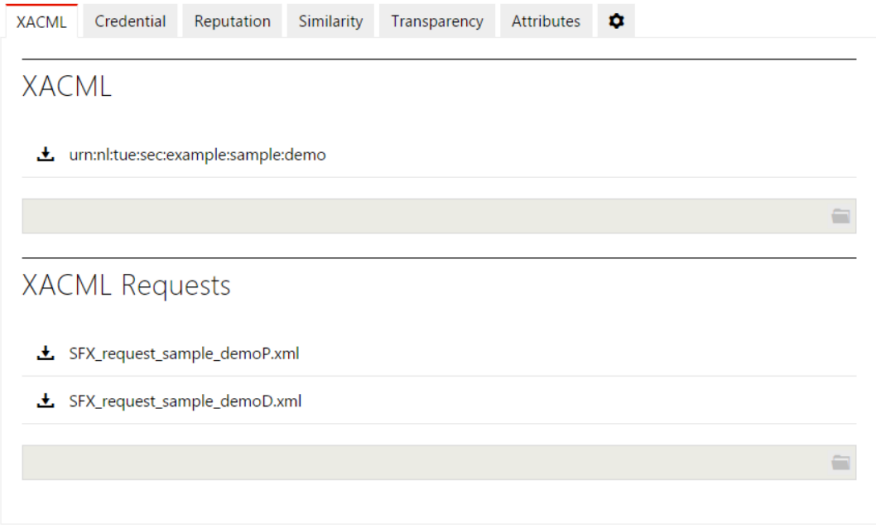


Figure 2.12.2 Upload request error

2.13 Remove Existing Access Request Screen

2.13.1 Functional Description

Users can remove existing access requests of an existing demo.

2.13.2 Caution and Warning

- When the user does not have the rights to remove access request from an existing demo, the XACML settings are shown in grey (Figure 2.11.2).

2.13.3 Formal Description

On the home page of SAFAX, click on an existing project. A list of demos of that project is displayed on the screen (Figure 2.9.1). Select an existing demo. The screen in Figure 2.13.1 will be displayed. Now use the trash icon to remove a request from the demo.

2.13.4 Related

Not applicable.

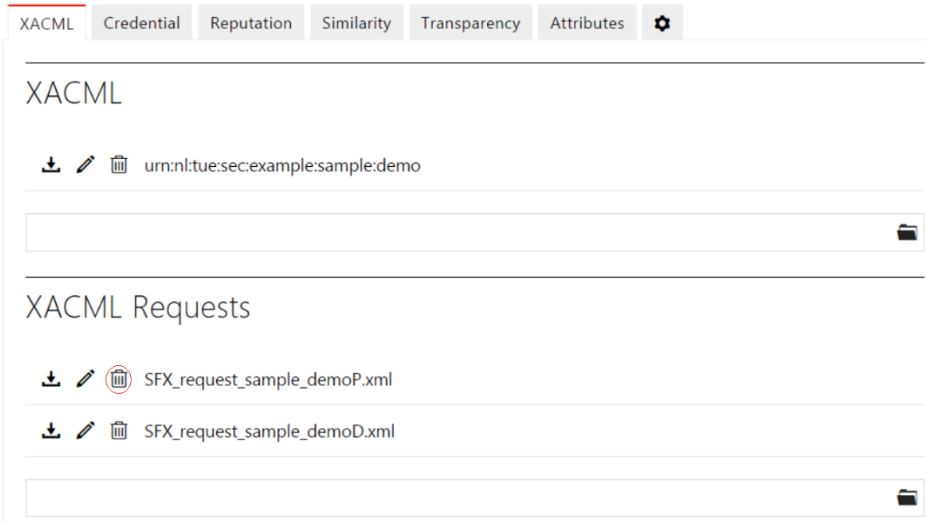


Figure 2.13.1 Remove access screen

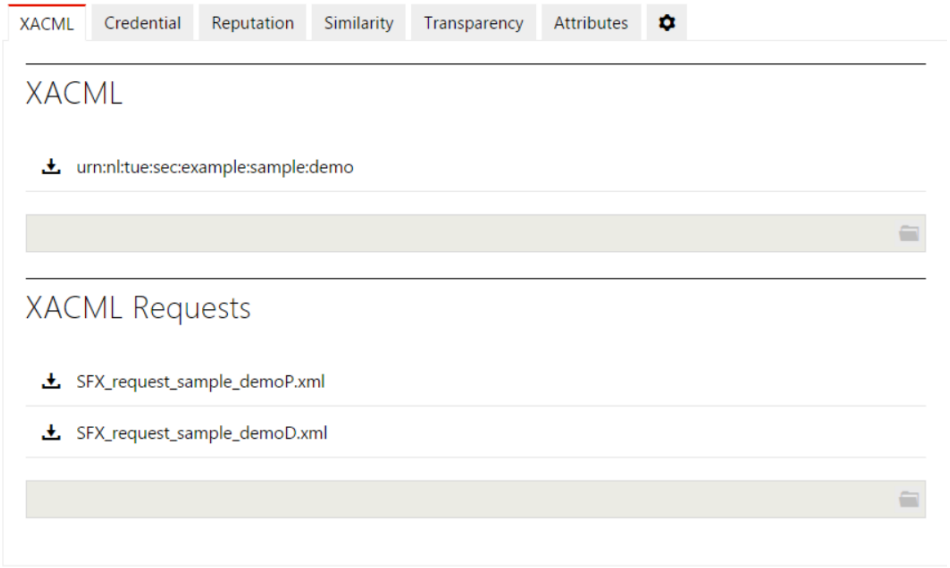


Figure 2.13.2 Remove access error

2.14 Change Demo Setting Screen

2.14.1 Functional Description

Users can change demo settings.

2.14.2 Caution and Warning

- When the user does not have the rights to change demo settings, the input fields are shown in grey (Figure 2.14.3).

2.14.3 Formal Description

On the home page of SAFAX, click on an existing project. A list of demos of that project is displayed on the screen (Figure 2.9.1). Click to choose an existing demo. Click to choose the setting icon (Figure 2.14.1). The screen in Figure 2.14.2 will be displayed. Now uses can change the following information:

- Demo name
- Demo description
- Demo location

After modifying these attribute, click *Save Settings* button to save the changes.

2.14.4 Related

Not applicable.

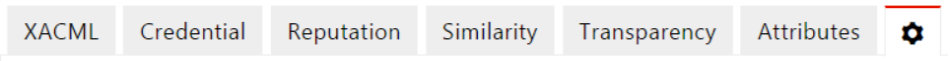


Figure 2.14.1 Setting icon

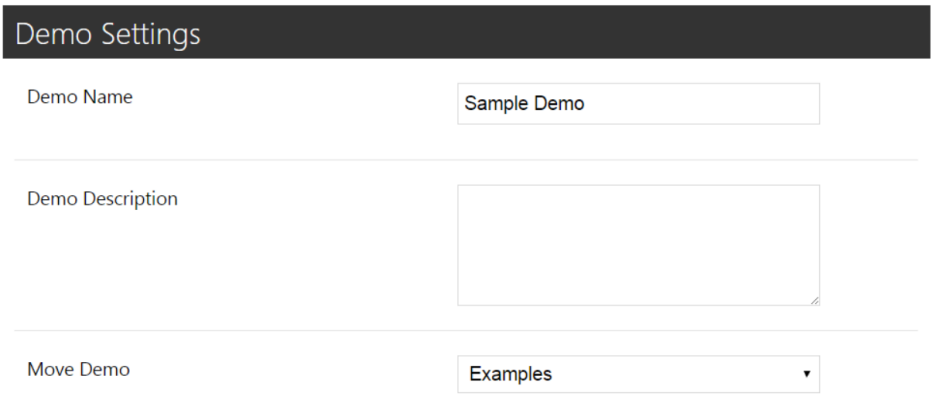


Figure 2.14.2 Change demo setting screen

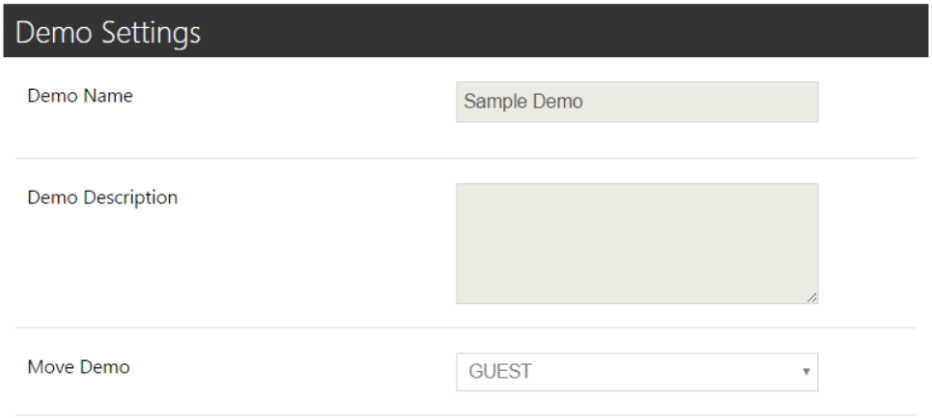


Figure 2.14.3 Change demo setting error

2.15 Policy Evaluation Screen

2.15.1 Functional Description

Users can evaluate access requests against authorization policies.

2.15.2 Caution and Warning

Not applicable.

2.15.3 Formal Description

There are two options to access the Policy Evaluation screen.

- On the home page of SAFAX, click *Policy Evaluation* menu. A list of demos is displayed on the screen (Figure 2.15.1). Click to choose an existing demo. The policy evaluation screen is displayed (Figure 2.15.3).
- On the home page of SAFAX, click an existing project. A list of demos of that project is displayed on the screen (Figure 2.9.1). Click to choose an existing demo. Click the *Run* button as shown in Figure 2.15.2. The policy evaluation screen is displayed (Figure 2.15.3).

A list of access requests in displayed under Available Requests heading (Figure 3.15.2). Click to choose an existing request. Click the Run button (Figure 3.15.2). The result is displayed on the screen (Figure 3.15.3).

2.15.4 Related

- Upon completion of the evaluation, users can see detailed evaluation log by clicking *Analyse Trace* button (Section 2.18).
- Users can also upload a new request to be evaluated by clicking the upload icon in Figure 2.15.3.

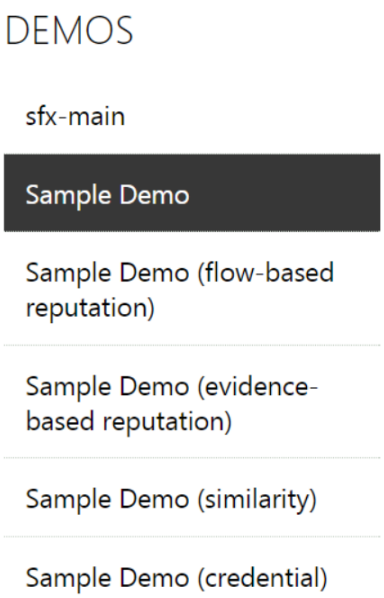


Figure 2.15.1 Demo list

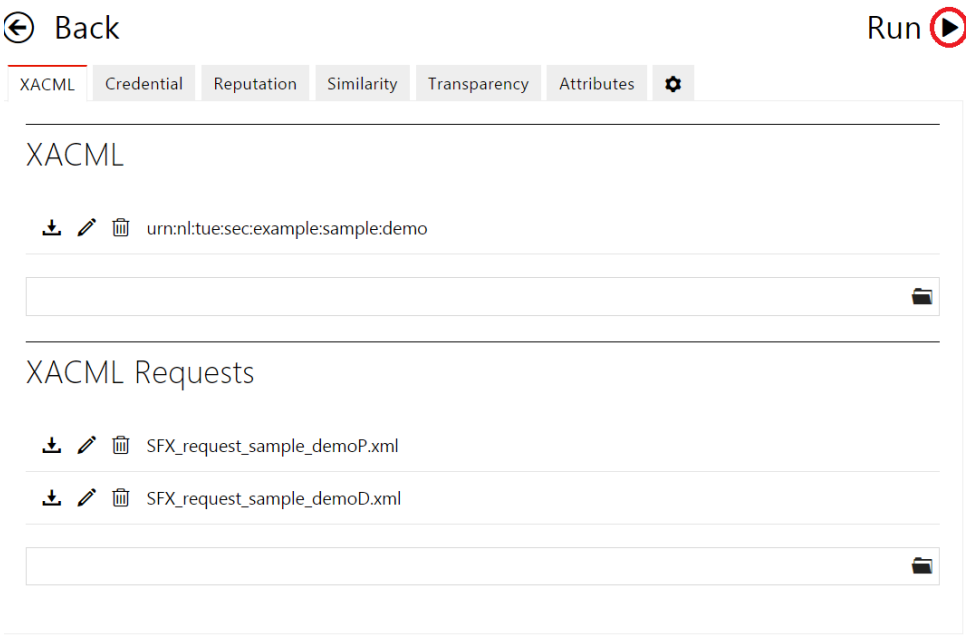


Figure 2.15.2 Evaluation run button

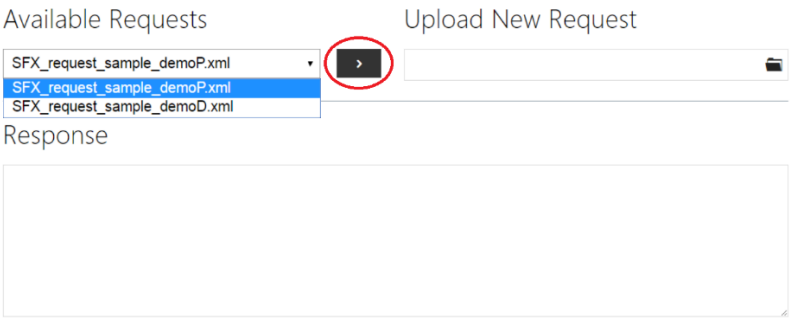


Figure 2.15.3 Policy evaluation screen

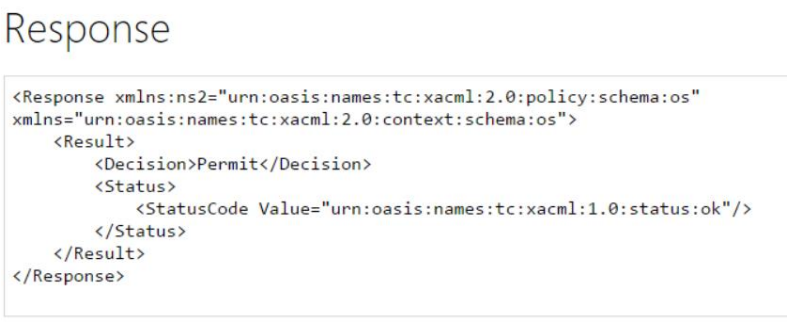


Figure 2.15.4 Policy evaluation result

2.16 XACML Component Setting Screen

2.16.1 Functional Description

Users can change the XACML components of an existing demo.

2.16.2 Caution and Warning

- When the user does not have the rights to change XACML components, the input fields are shown in grey (Figure 2.16.3).

2.16.3 Formal Description

On the home page of SAFAX, click an existing project. A list of demos is displayed on the screen (Figure 2.15.1). Click to choose an existing demo. Click to choose the setting icon (Figure 2.16.1). The screen, as shown in Figure 2.16.2 will show up. Now uses can change the following components:

- PDP
- PEP
- CH
- PIP
- PAP
- Root combining algorithm

Finally, click on *Save Settings* button.

2.16.4 Related

- Users can see a list of services registered in SAFAX (Section 2.17).

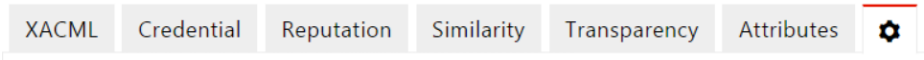


Figure 2.16.1 Setting icon

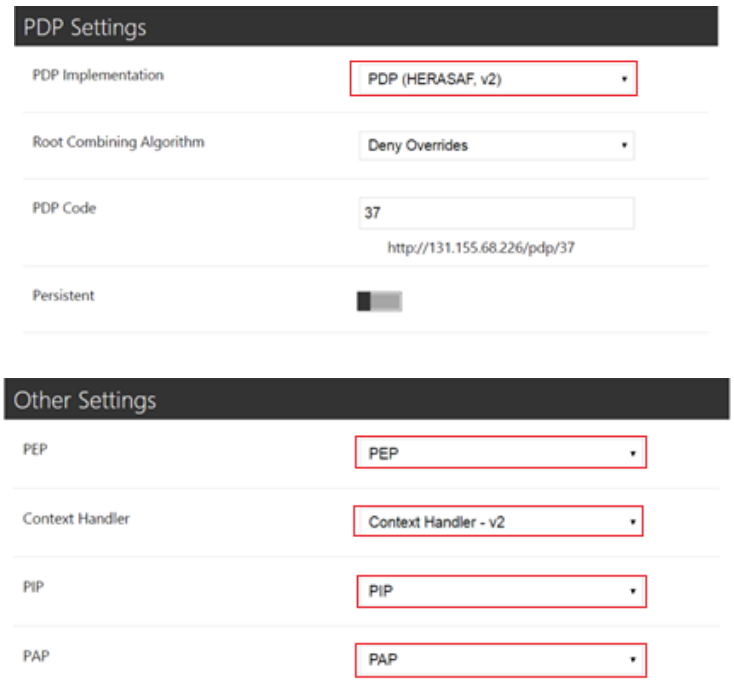


Figure 2.16.2 XACM component setting screen

2.17 Remove Existing Demo Screen

2.17.1 Functional Description

Users can remove existing demos.

2.17.2 Caution and Warning

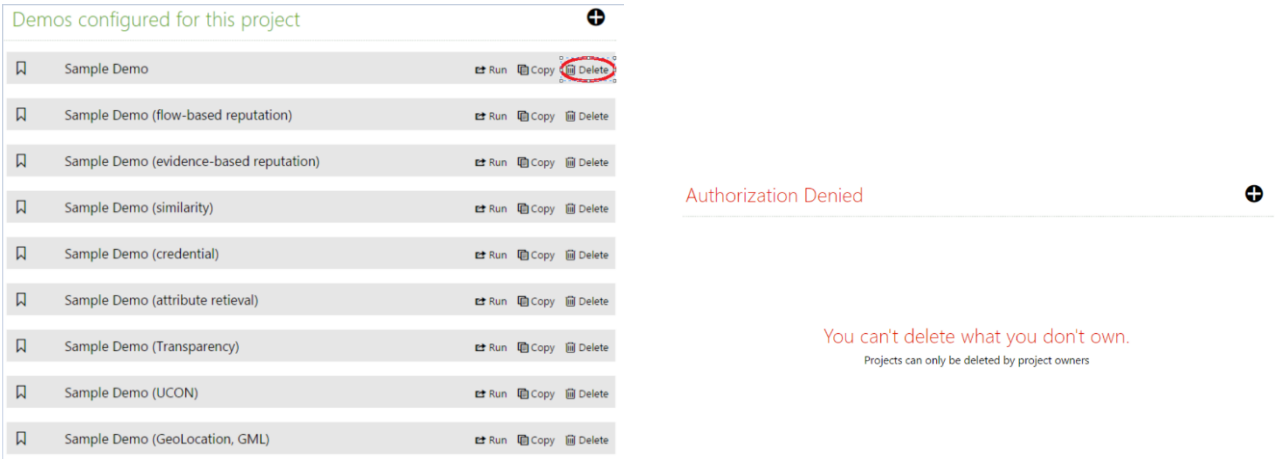
- When the user does not have the rights to remove existing demos, an error in Figure 2.17(b) is shown

2.17.3 Formal Description

On the home page of SAFAX, click an existing project. A list of demos is displayed on the screen (Figure 2.9.1). Click the trash icon near an existing demo to remove that demo. (Figure 2.17(a)).

2.17.4 Related

Not applicable.



a. Remove demo button b. Remove demo error

Figure 2.17 Remove existing demo screen

2.18 Service Registry View Screen

2.18.1 Functional Description

Users can view a list of services registered in SAFAX.

2.18.2 Caution and Warning

Not applicable.

2.18.3 Formal Description

On the home page of SAFAX, click Service Registry menu (Figure 2.18.1). A list of services is displayed on the screen (Figure 2.18.2).

2.18.4 Related

Not applicable.

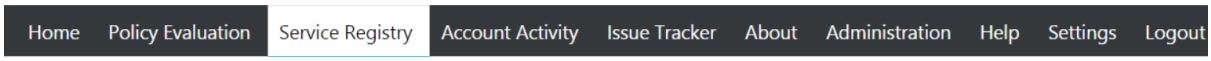


Figure 2.18.1 Service registry menu

SAFAX A Flexible and Extensible Authorization Service

Category	Service	Service ID	Provider	URL
ch	Context Handler - v2	nl:tue:sec:ch:evaluate	TUE	http://localhost/ch/evaluate
ch	Context Handler - v2	nl:tue:sec:ch:get:attributes	TUE	http://localhost/ch/get/attributes
ch	Context Handler - v2	nl:tue:sec:ch:get:ucon:attributes	TUE	http://localhost/ch/get/ucon/attributes
ch	Context Handler - v2	nl:tue:sec:ch:re-evaluate	TUE	http://localhost/ch/evaluate/ucon
ch	Safax Context Handler - v2	nl:tue:sec:safax:ch:evaluate	TUE	http://localhost/safax_ch/evaluate
ch	Safax Context Handler - v2	nl:tue:sec:safax:ch:get:attributes	TUE	http://localhost/safax_ch/get/attributes
ch	Well known text Context Handler - v2	nl:tue:sec:wkt:ch:evaluate	TUE	http://localhost/wkt_ch/evaluate
ch	Well known text Context Handler - v2	nl:tue:sec:wkt:ch:get:attribute	TUE	http://localhost/wkt_ch/get/attribute
other	UCON Obligation Service	nl:tue:sec:ucon:os:handle	TUE	http://localhost/os-ucon/handle/obligation
other	UCON Obligation Service	nl:tue:sec:ucon:os:stop	TUE	http://localhost/os-ucon/stop/ucon
pap	PAP	nl:tue:sec:safax:pap:get:pdp:policies	TUE	http://localhost/pap/get/pdp/policies
pdp	Duc PDP Service	lmd:nl:tue:sec:safax:ch:evaluate	TUE	http://131.155.69.231/herasaf/pdp/evaluate

Figure 2.18.2 Service registry view screen

2.19 Account Activity Screen

2.19.1 Functional Description

Users can see all evaluation activities happened in the past.

2.19.2 Caution and Warning

Not applicable.

3.19.3 Formal Description

On the home page of SAFAX, click *Account Activity* menu (Figure 2.19.1). A list of transactions is displayed and grouped into:

- *Current Session Transactions*
- *Past 20 Transactions*
- *Restore Deleted Items*

Click a transaction to view its detailed log (Figure 2.19.2). A detailed log is then displayed (Figure 2.19.3).

2.19.4 Related

Not applicable.

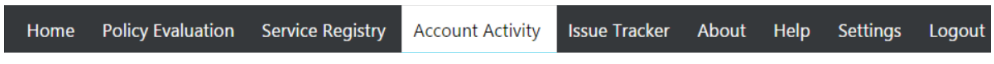


Figure 2.19.1 Account Activity Menu

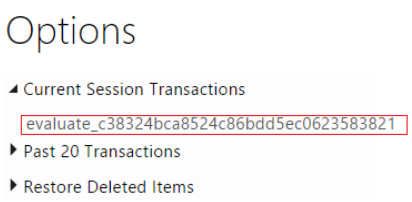


Figure 2.19.21 Current Session Transactions View

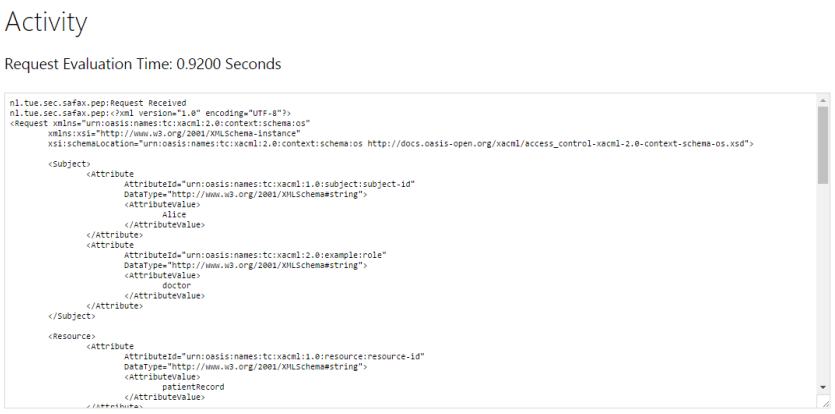


Figure 2.19.32 Detailed Log View

2.20 Report Issue Screen

2.20.1 Functional Description

Users can report an issue to SAFAX administrators.

2.20.2 Caution and Warning

Not applicable.

2.20.3 Formal Description

On the home page of SAFAX, click *Issue Tracker* menu (Figure 2.20.1). A list of reported issues and resolved issues is shown on the right of the screen Figure (2.20.2).

To report a new issue, fill in the following information in the report issue form on the left of the screen (Figure 2.20.2):

- Title
- Issue description

2.20.4 Related

Not applicable.

Figure 2.20.1 Issue Tracker Menu

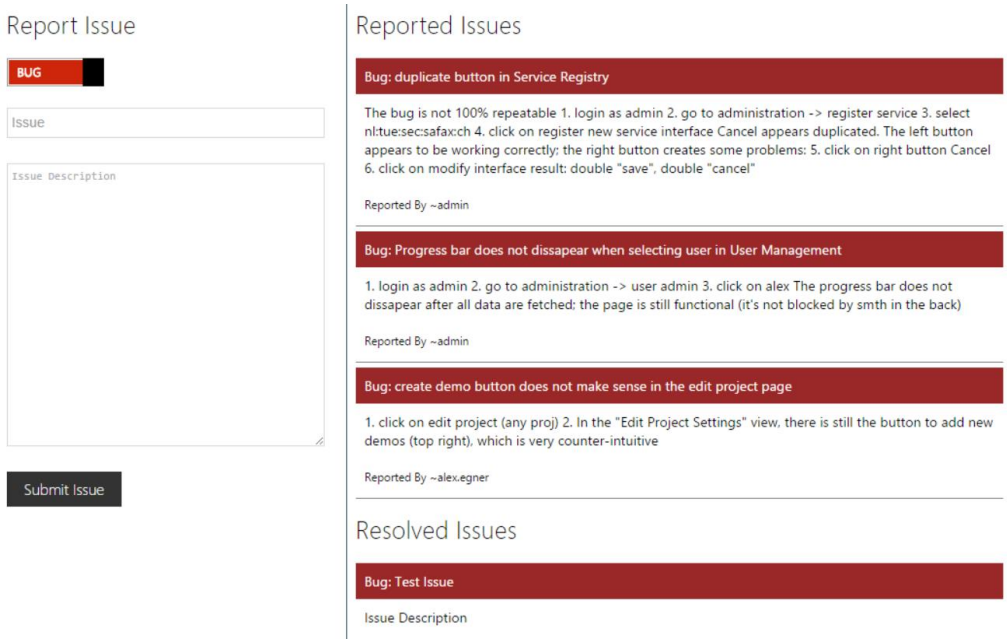


Figure 2.20.23 Report issue screen

2.21 About Screen

2.21.1 Functional Description

Users can view overview information of SAFAX and a list of SAFAX versions.

2.21.2 Caution and Warning

Not applicable.

2.21.3 Formal Description

On the home page of SAFAX, click *About* menu (Figure 2.21.1). The About screen is displayed (Figure 2.21.2).

2.21.4 Related

Not applicable.

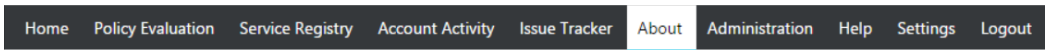


Figure 2.21.1 About Menu

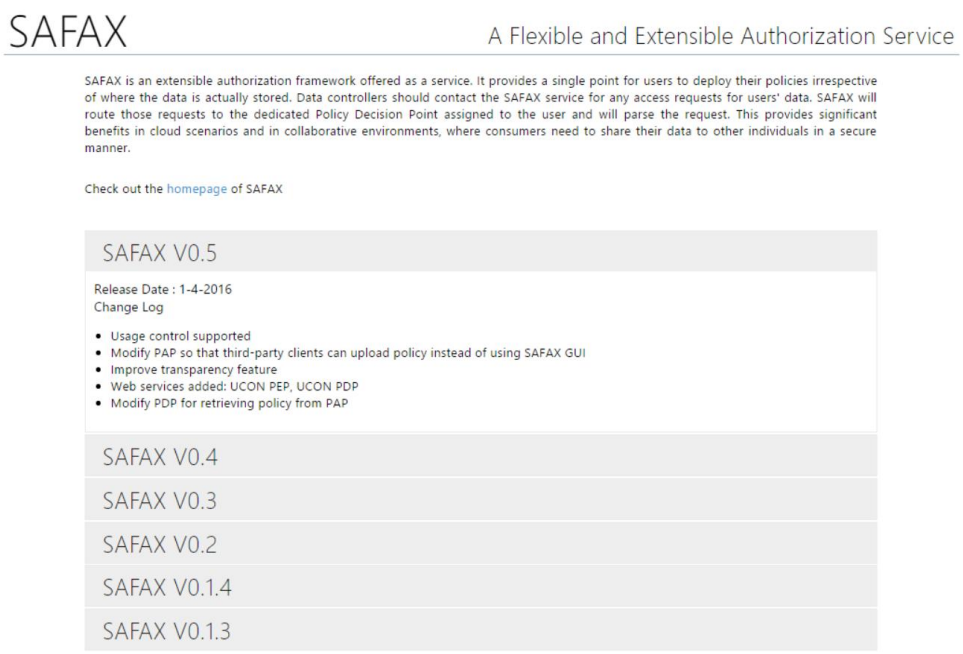


Figure 2.21.24 About screen

2.22 Help Screen

2.22.1 Functional Description

Users can view help information of SAFAX and a list of UDFs.

2.22.2 Caution and Warning

Not applicable.

2.22.3 Formal Description

On the home page of SAFAX, click *Help* menu (Figure 2.2.1). Help screen is displayed (Figure 2.22.2).

2.22.4 Related

Not applicable.

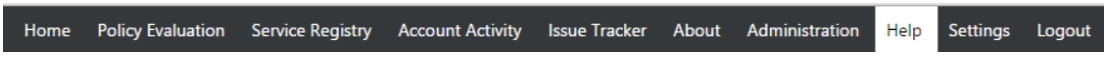


Figure 2.22.1 Help Menu

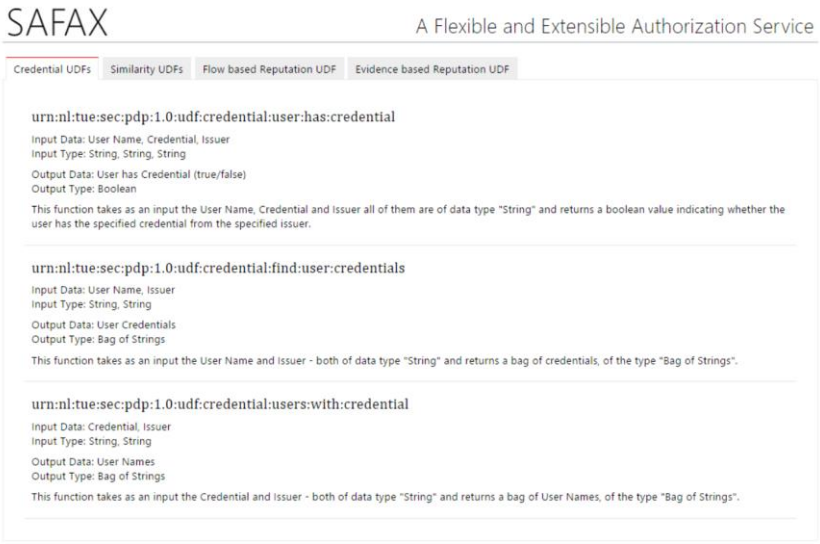


Figure 2.22.25 Help screen

2.23 Settings Screen

2.23.1 Functional Description

Users can change account settings.

2.23.2 Caution and Warning

Not applicable.

2.23.3 Formal Description

On the home page of SAFAX, click *Settings* menu (Figure 2.23.1). Help screen is displayed (Figure 2.23.2). User can change the following information:

- Username
- Full name
- Password

Finally, click *Update Account* button to save the changes.

2.23.4 Related

Not applicable.

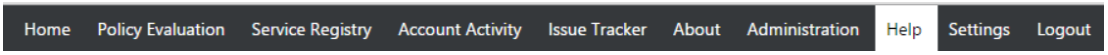


Figure 2.23.1 Settings menu

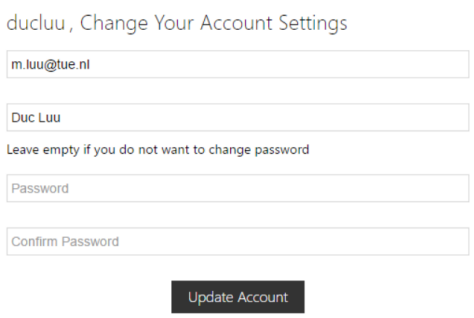


Figure 2.23.26 Settings screen

2.24 Logout Screen

2.24.1 Functional Description

From here, users can log out.

2.24.2 Caution and Warning

Not applicable.

2.24.3 Formal Description

On the home page of SAFAX, click *Logout* menu (Figure 2.24.1). User is logged out and welcome screen is displayed (Section 2.1).

2.24.4 Related

Not applicable.

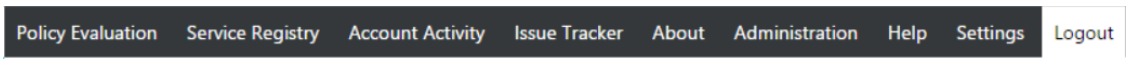


Figure 2.24.1 Logout menu

Chapter 3

Advanced Functionalities

3.1 Credential-based Trust Management Service

3.1.1 Functional Description

Credential-based trust management is an approach to access control in distributed systems where access decisions are based on policy statements issued by multiple principals and stored in a distributed manner. In trust management, the policy statements of a principal can refer to other principals' statements; thus, the process of evaluating an access request consists of finding a "chain" of policy statements that allows the access to the requested resource. SAFAX supports credential-based trust management as an external service. In particular, SAFAX uses a credential-based trust management service based on GEM [8], a distributed goal evaluation algorithm for trust management systems.

3.1.2 Caution and Warning

Not applicable.

3.1.3 Formal Description

On the home page of SAFAX, click an existing project. A list of demos is displayed on the screen (Figure 2.9.1). Click to choose an existing demo. Click the *Credential* tab (Figure 3.1). Users can upload a trust policy for a new issuer by clicking the folder upload icon. Users can also view or modify the content of the issuer files.

3.1.4 Related

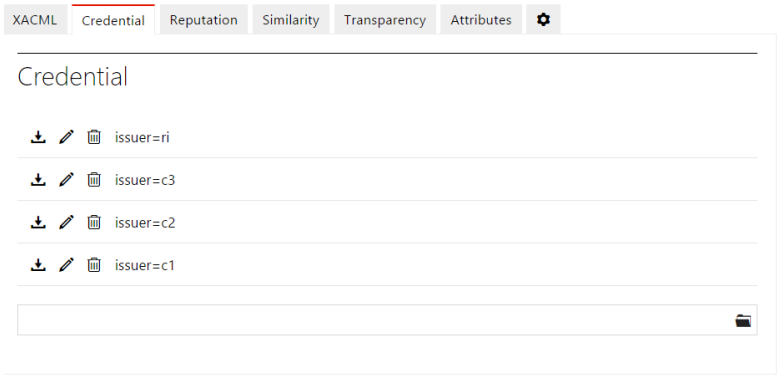


Figure 3.1 Credential-based trust management service screen

3.2 Reputation-based Trust Management Service

3.2.1 Functional Description

SAFAX supports two types of reputation: flow based reputation [6] and evidence based reputation [5].

3.2.2 Caution and Warning

Not applicable.

3.2.3 Formal Description

On the home page of SAFAX, click an existing project. A list of demos is displayed on the screen (Figure 2.9.1). Click to choose an existing demo. Click the *Reputation* tab (Figure 4.2).

3.2.4 Related

Not applicable.

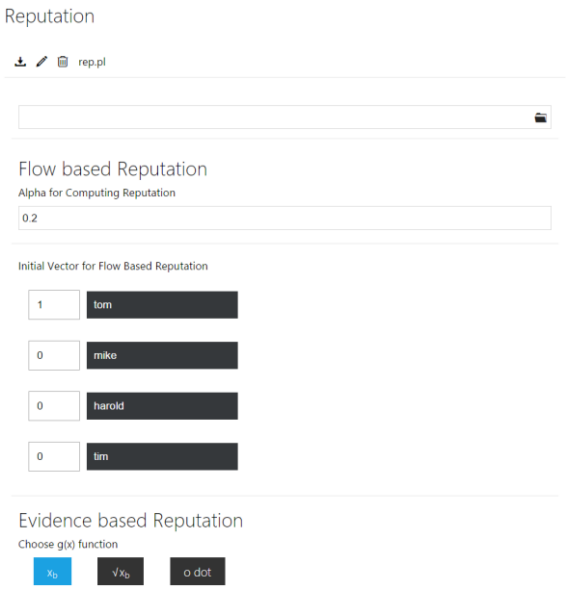


Figure 3.2 Reputation-based trust management service screen

3.3 Policy Alignment Service

3.3.1 Functional Description

Policy alignment service in SAFAX is an external trust service that aims to address the problem of ontology alignment.

3.3.2 Caution and Warning

Not applicable.

3.3.3 Formal Description

On the home page of SAFAX, click an existing project. A list of demos is displayed on the screen (Figure 2.9.1). Click to choose an existing demo. Click the *Similarity* tab (Figure 3.3).

3.3.4 Related

Not applicable.

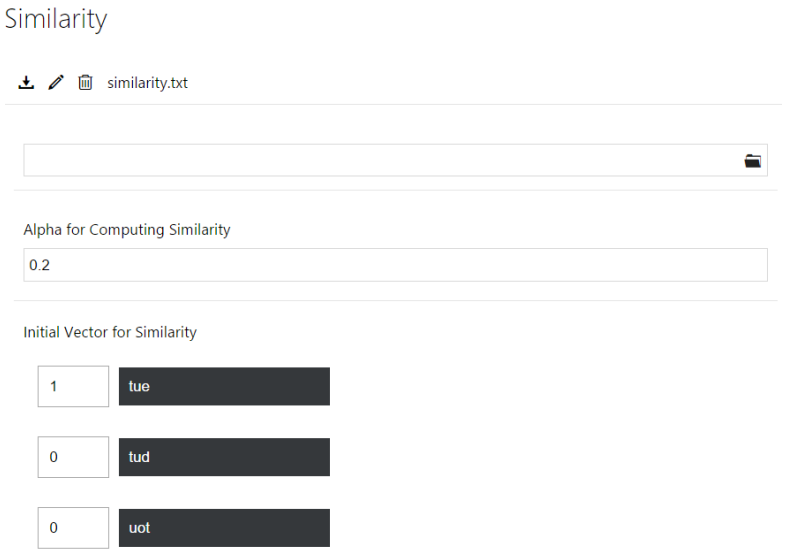


Figure 3.3 Policy alignment service screen

3.4 Geolocation Service

3.4.1 Functional Description

SAFAX supports GeoXACML [9] with Geography Markup Language (GML) 2.0 definition [3].

3.4.2 Caution and Warning

Not applicable.

3.4.3 Formal Description

On the home page of SAFAX, click an existing project. A list of demos is displayed on the screen (Figure 2.9.1). Click to choose an existing demo. Click the Settings button (Figure 3.4.1).

Under *PDP Settings* section, choose the PDP (HERASAF_GEOLOCATION, v2) (Figure 3.4.2).

SAFAX also provides a CH that supports well-known text format (WKT) [4] in access requests. An example of such request is shown in Figure 3.4.3.

To use this CH, click the *Other Settings* tab and in the CH implementation choose *Well known text Context Handler* – v2 (Figure 3.4.4).

3.4.4 Related

Not applicable.

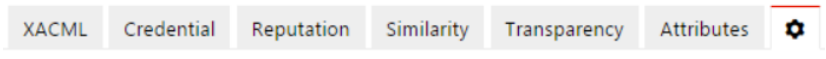


Figure 3.4.1 Setting button

Figure 3.4.2 PDP settings for geolocation

```
<Subject>
        <Attribute
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                DataType="http://www.w3.org/2001/XMLSchema#string">
                <AttributeValue>
                        mike
                </AttributeValue>
        </Attribute>
        <Attribute
                AttributeId="urn:nl:tue:sec:example:geolocation:location"
                DataType="urn:ogc:def:dataType:wkt">
                <AttributeValue>
                     POINT (20 21)
                </AttributeValue>
        </Attribute>
</Subject>
```

Figure 3.4.3 WKT Example

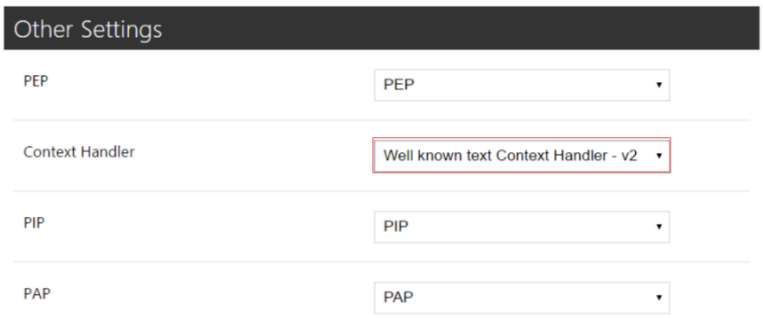


Figure 3.4.4 CH Settings for Geolocation with WKT Requests and Policies

3.5 Attribute Retrieval Service

3.5.1 Functional Description

During policy evaluation, the PDP might require additional attributes. The PDP request the PIP through the Context Handler to provide these attributes. SAFAX provides an attribute retrieval service that allows users to upload additional attributes to the PIP.

3.5.2 Caution and Warning

Not applicable.

3.5.3 Formal Description

On the home page of SAFAX, click an existing project. A list of demos is displayed on the screen (Figure 2.9.1). Select the desired demo. Click the *Attributes* tab (Figure 3.5.1).

The attributes must be in a CSV file. The file contains the following elements:

- AttributeID
- AttributeValue
- DataType
- ReferenceAttributeID
- ReferenceAttributeValue

For example, the following content of a CSV file describes that John's credit is 50:

- urn:oasis:names:tc:xacml:1.0:subject:subject-id,john,string,null,null
- credit,50,integer,urn:oasis:names:tc:xacml:1.0:subject:subject-id,john

Users can use the folder icon to upload the CSV file to the PIP (Figure 3.5.2).

3.5.4 Related

Not applicable.

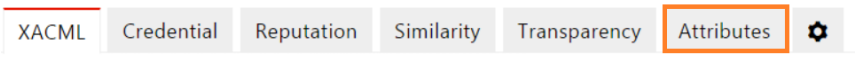


Figure 3.5.1 Attributes Tab

Figure 3.5.2 Attributes upload screen

3.6 Transparency Service

3.6.1 Functional Description

Transparency in SAFAX aims to detect mismatches between the decision enforced by the authorization system and the user policies [2].

3.6.2 Caution and Warning

Not applicable.

3.6.3 Formal Description

On the home page of SAFAX, click an existing project. A list of demos is displayed on the screen (Figure 2.9.1). Click to choose an existing demo. Click the *Transparency* tab (Figure 3.6.1).

In SAFAX, the transparency feature is deployed as a PEP or as a PDP. To use the Transparent PDP click PDP Settings tab and change the PDP Implementation to Transparent PDP (Figure 3.6.2).

To use the Transparent PEP click Other Settings tab and choose Transparent PEP as the PEP component (Figure 3.6.3). Click *Save Settings* to save changes and click *Run* to evaluate a request. When a mismatch occurs, SAFAX displays it on the screen (Figure 3.6.3).

3.6.4 Related

Not applicable.

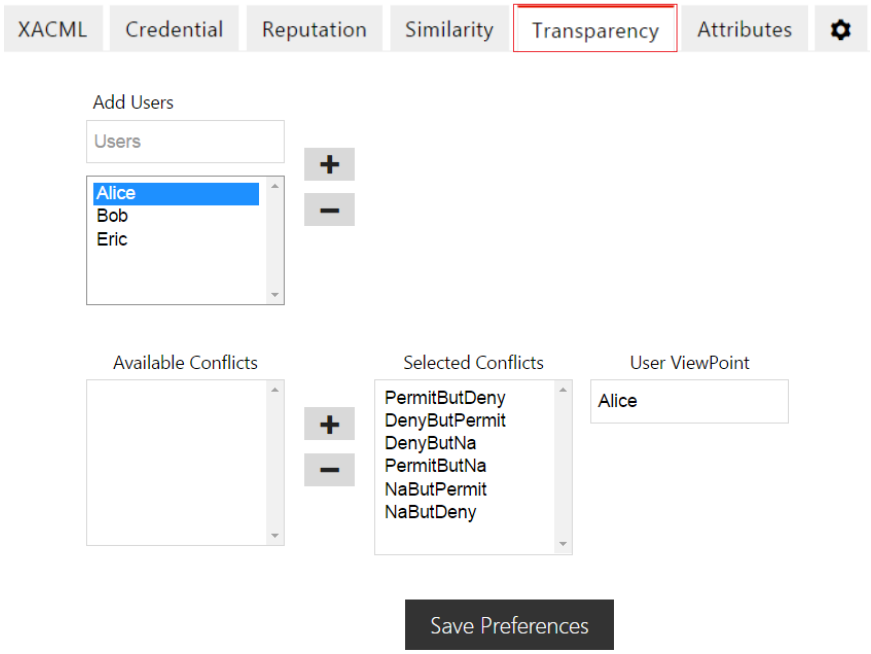


Figure 3.6.1 Transparency configuration screen

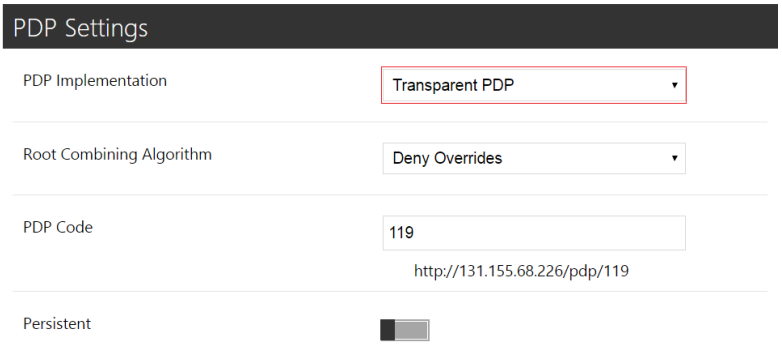


Figure 3.6.27 Transparent PDP

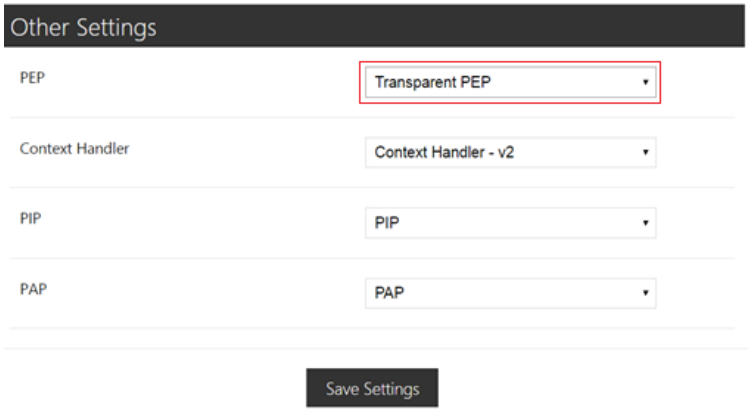


Figure 8 Transparent PEP

Figure 3.6.4 Transparency Notification

3.7 UCON Service

3.7.1 Functional Description

The UCON service allows control over a resource during the entire lifetime of its usage. It is based on two distinctive characteristics: attribute mutability and access decision continuity.

3.7.2 Caution and Warning

Not applicable.

3.7.3 Formal Description

On the home page of SAFAX, click an existing project. A list of demos is displayed on the screen (Figure 2.9.1). Click to choose an existing demo. Click the *Settings* button (Figure 3.7.1).

In SAFAX, the UCON feature is implemented as a PEP component. Under *Other Settings* section, in the PEP configuration change to UCON PEP (Figure 3.7.2). Click *Save Settings* to make changes and click *Run* to evaluate a request.

The response interface shows the entire usage of a resource during real time (Figure 3.7.3).

3.7.4 Related

Not applicable.

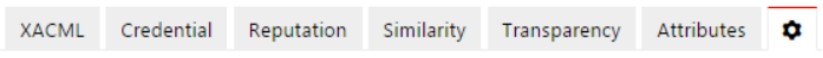


Figure 3.7.1 Setting button

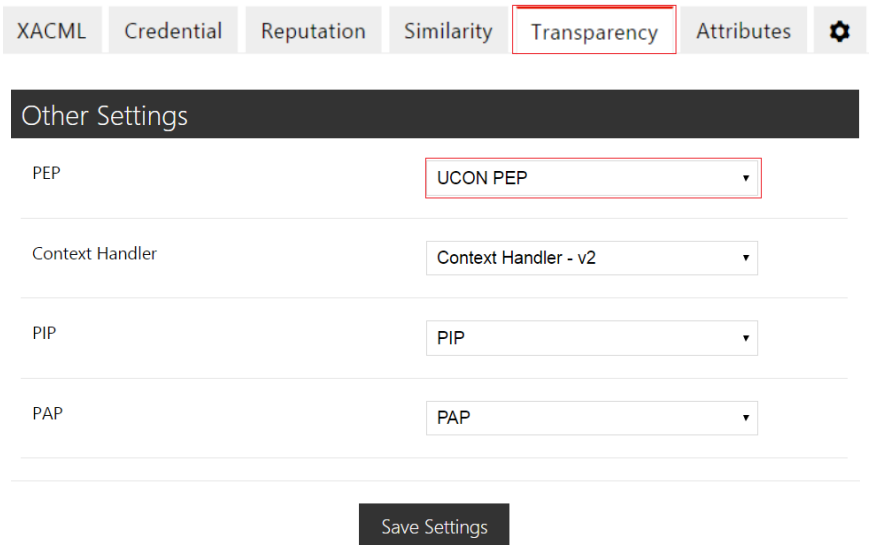


Figure 3.7.2 UCON Settings

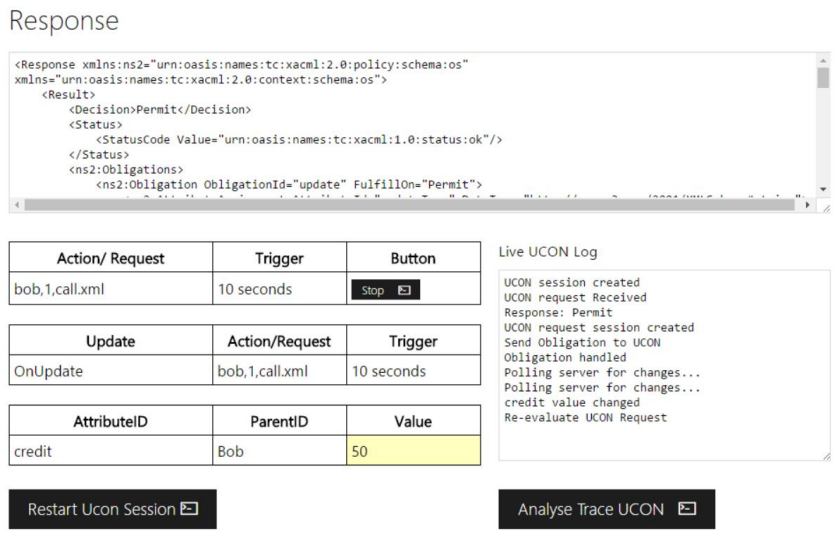


Figure 3.7.3 UCON Response

Chapter 4

Examples

4.1 Example Demo Screen

4.1.1 Functional Description

The *Examples* project contains detailed examples of normal, transparency, UCON, geolocation policies and requests.

4.1.2 Caution and Warning

Not applicable.

4.1.3 Formal Description

On the home page of SAFAX, click *Examples* project. A list of demos is displayed on the screen (Figure 4.1). Click a demo to view its policies, requests, and demo and component configurations (Figure 4.2)

4.1.4 Related

Not applicable.

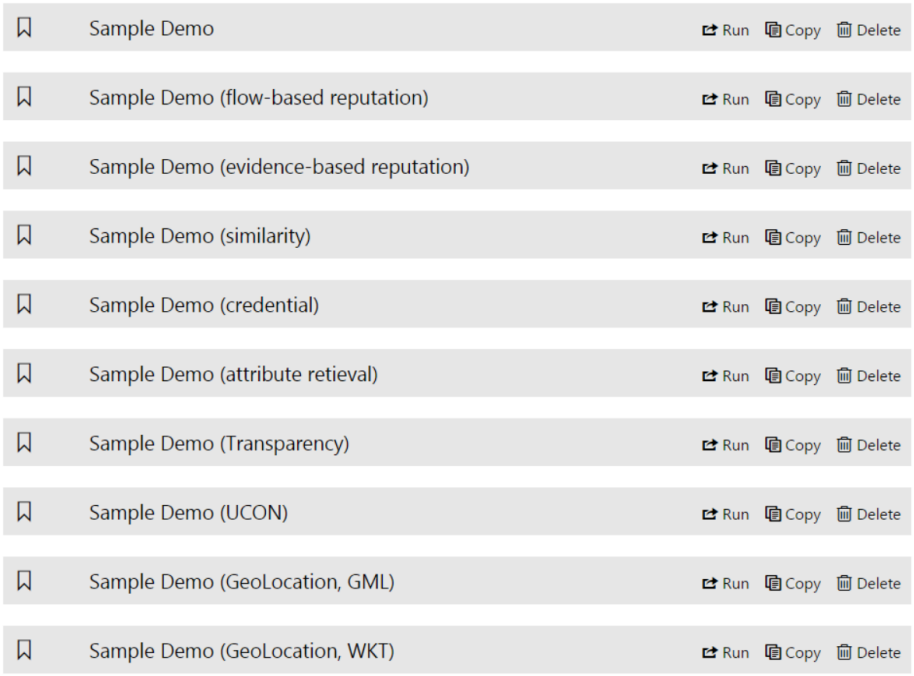


Figure 4.1 Example demos

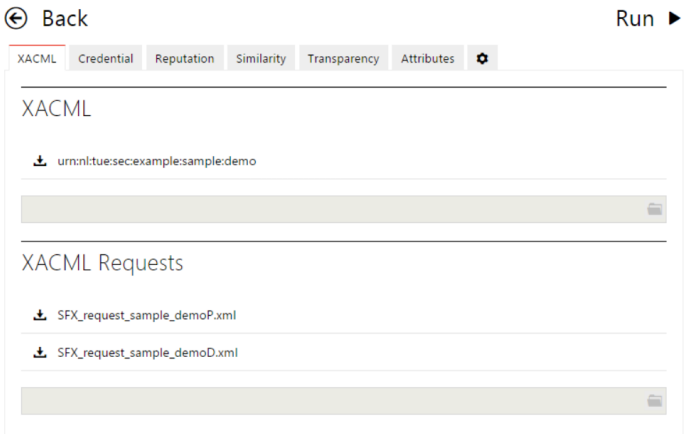


Figure 4.2 Detailed example demo screen

References

[1] S. P. Kaluvuri, A. I. Egner, J. den Hartog, and N. Zannone. SAFAX -- an extensible authorization service for cloud environments. Frontiers in ICT 2(9), 2015.

[2] R. Mahmudlu, J. den Hartog, and N. Zannone. Data Governance & Transparency for Collaborative Systems. In Proceedings of the 28th Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec 2016), 2016. Springer.

[3] Open Geospatial Consortium Inc. Geospatial eXentsible Access Control Markup Language (GeoXACML) Extension A – GML2 Encoding [Internet]. 2007 Nov [cited 2016 May 20]. Available from http://www.opengeospatial.org/standards/geoxacml.

[4] Open Geospatial Consortium Inc. OpenGIS Implementation Standard for Geographic information – Simple feature access – Part 1: Common architecture [Internet]. 2011 May [cited 2016 May 20]. Available from http://www.opengeospatial.org/standards/sfa.

[5] B. Skoric, S. de Hoogh, and N. Zannone. Flow-based Reputation with Uncertainty: Evidence-Based Subjective Logic. International Journal of Information Security, 2015.

[6] A. Simone, B. Skoric, and N. Zannone. Flow-based reputation: more than just ranking. International Journal of Information Technology & Decision Making, 11(3):551-578, 2012.

[7] OASIS. eXtensible Access Control Markup Language (XACML) Version 2.0 [Internet]. 2005 Feb [cited 2016 May 20]. Available from https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.

[8] D. Trivellato, N. Zannone, and S. Etalle. GEM: a Distributed Goal Evaluation Algorithm for Trust Management. Theory and Practice of Logic Programming, 2014

[9] Open Geospatial Consortium Inc. Geospatial eXentsible Access Control Markup Language (GeoXACML) version 1 corrigendum [Internet]. 2007 Nov [cited 2016 May 20]. Available from http://www.opengeospatial.org/standards/geoxacml.