SDSS - user's manual

version 0.2.0 - 13 December 2013

PoSecCo

http://www.posecco.eu

Contents

1 Introduction

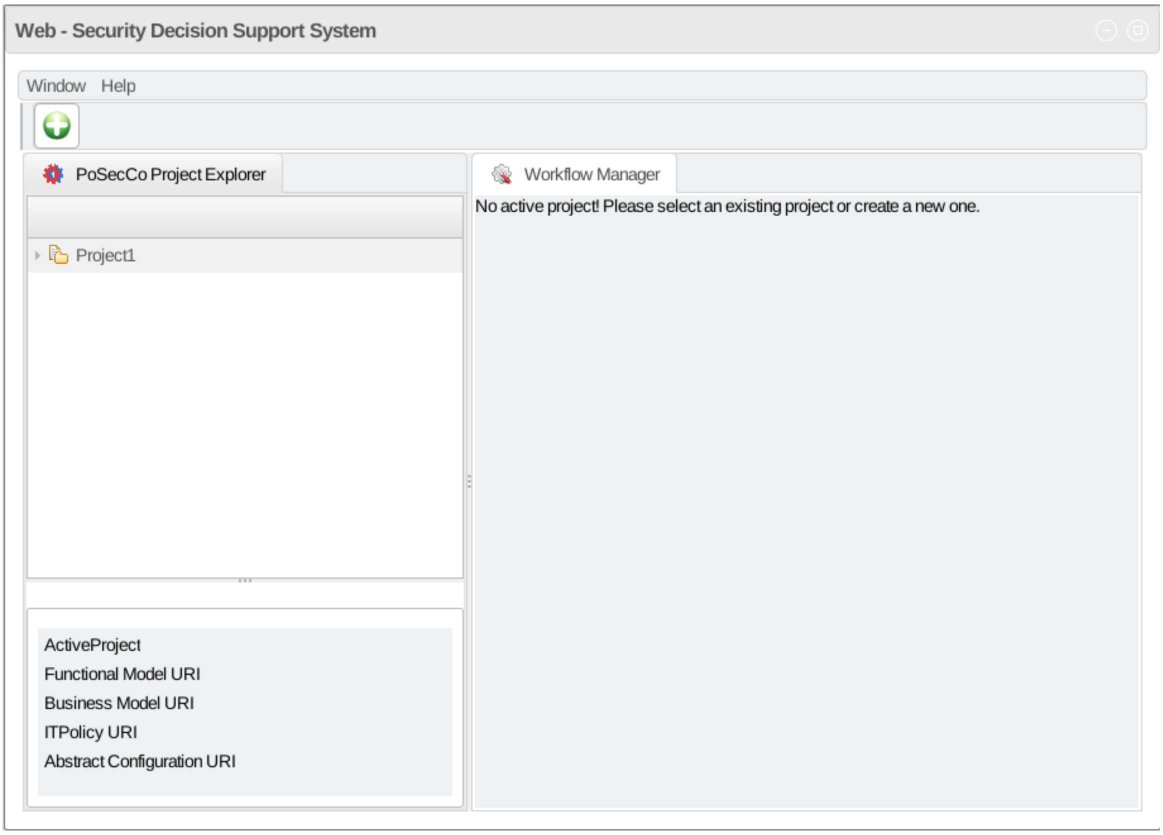
The role of this document is to introduce the PoSecCo Security Decision Support System, the framework intended to perform the refinement of IT Policies into abstract configurations, the harmonization of IT Policies, and the analysis Logical associations and Abstract configurations. After having provided the necessary information to install the PoSecCo Security Decision Support System, this document presents a brief description of the components, the list of used plug-ins and the external third party components needed for a correct functioning.

2 How to get the SDSS

The SDSS is available as a web application developed using Eclipse RAP technology. The SDSS is released under EPL license. It can be downloaded from:
`http://security.polito.it/posecco/sdss`
To run the SDSS, you must:

- install a web container (e.g., Apache Tomcat)
- deploy the SDSS .war into you web container
- open your browser and go to the portal initial web page whose URL is
  `web_container_URL/sdss_full/projectmanager`
  For the default Tomcat web container on the local host, the URL would be:
  `localhost:8080/sdss_full/projectmanager`

If the installation is correct, you should be able to see the SDSS Main perspective shown below:



Web - Security Decision Support System

No active project! Please select an existing project or create a new one.

ActiveProject
Functional Model URI
Business Model URI
ITPolicy URI
Abstract Configuration URI

Figure 1: The PoSecCo Project Explorer View

3 Getting started

The SDSS relies on a MoVE repository that is used to store the SDSS Projects. An SDSS project contains the following information (meta-models):

- the *target landscape*, that is, the system to configure, represented as an instantiation of the PoSecCo functional system meta-model. The landscape description cannot be instantiated using the SDSS and must be linked when a new project is created;
- the *business requirements*, optional, represented as an instantiation of the PoSecCo business policy meta-model. Business requirements cannot be instantiated using the SDSS and must be linked when a new project is created;
- the *IT policy*, represented as an instantiation of the PoSecCo IT policy meta-model. The IT policy can be specified with the SDSS therefore an empty instantiation is created if it is not selected during project creation. If business requirements are specified, the specified IT policy instances will be associated to business requirement instances. It is intended that the IT policy will be the (manual) refinement of associated business requirement instances;
- the *abstract configurations*, represented as an instantiation of the PoSecCo Configuration meta-model. Configurations can be specified with the SDSS therefore an empty instantiation is created if it is not selected during project creation. Additionally, configurations can be derived from the IT Policy using the SDSS by performing automatic or assisted refinement;
- the *workflow type*, that captures one “correct” way to use the SDSS by determining the allowed operations and their correct sequence. According to the selected workflow some of the policy models above can be optional or mandatory;
- the *formal ontology*, represented in OWL, that connects and enriches all the previous meta-model instantiations with additional data used for inference and refinement purposes. In particular, the ontology stores the Logical Associations, an intermediate policy representation used to generate of configurations of infrastructure security controls (e.g., border firewalls, VPN gateways). The ontology is automatically created and maintained by the SDSS from the selected landscape, policies, and workflow and it does not need to be created or explicitly managed by the user.

Workflow types

There are several operations that can be performed using the SDSS, they are named here Workflow phases and listed below:

- Edit IT Policy, allows the specification of IT policies and the association of IT policies to business requirements. This phase is performed by the IT Policy tool (see [5]);
- Harmonize IT policy, verifies the coherence of the specified IT policies and suggests remediations. This phase is performed by the IT Policy tool (see [5]);
- Refine IT policy, uses the IT policy to derive the abstract configurations for access control devices (e.g., authentication and authorization at the endpoints). This phase is performed by the IT Policy tool (see [5]);
- Generate logical associations, interprets the IT policy and refine it into a set of logical associations, a less abstract but still topology-independent policy representation. This phase serves as an intermediate task to configure infrastructure security controls. This phase is performed by the LA Generator Service (see [6]);
- Analyze Logical Associations, shows possible inconsistencies or ambiguity in the interpretation of the logical associations and helps the user to resolve them. This phase is performed by the Analysis Service, Logical association section (see [1]);

- Refine Logical associations (also said Generate optimized configurations), uses the logical associations to derive optimized abstract configurations. This phase is performed by the Infrastructure Configuration Service (see [4]);
- Edit configurations, allows users to specify logical associations or to edit previously generated abstract configurations. This phase is performed by the Configuration Editor (see [3]);
- Analyze configurations, shows possible inconsistencies or ambiguity in the data protection and filtering configurations and helps the user to resolve them. This phase is performed by the Analysis Service, Configuration section (see [2]);

Based on these phases, several workflow types are allowed by the SDSS. They are listed below.

General SDSS workflow

The SDSS General workflow is the most general SDSS workflow. It contains all the phases with all their dependencies. All other workflows are subcases of this one. It requires the availability of a previously instantiated landscape description and optionally, of business requirements. Moreover, all other policy meta-models can be optionally linked. This workflow is shown in Figure 2.

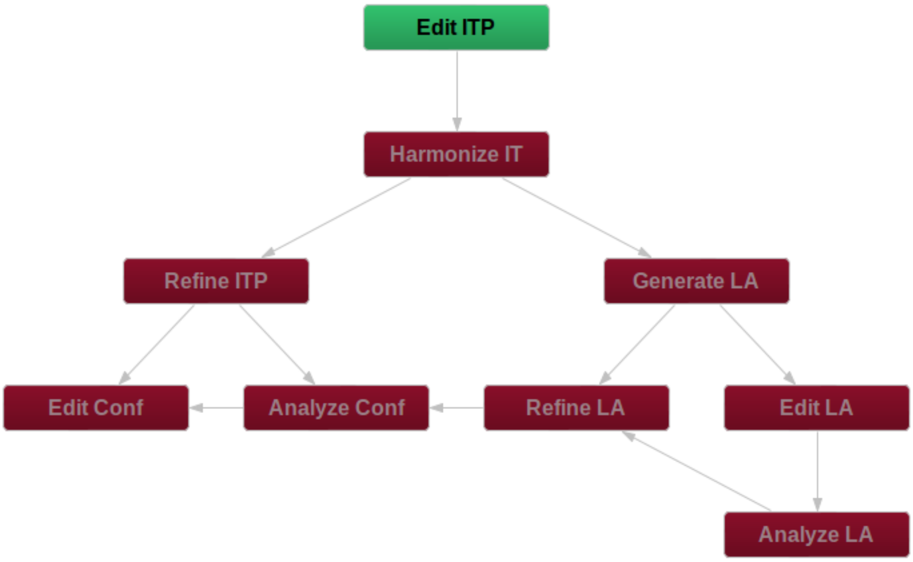


Figure 2: The General SDSS workflow graph.

Edit and Harmonize ITP workflow

This workflow is used to specify an IT policy, connect it to the business requirements, and to verify its coherence. It requires the availability of a previously instantiated landscape description and optionally, of business requirements. Moreover, an existing IT policy can be optionally linked. It is suggested for security architects whose objective is to generate a coherent set of high-level policies, the IT policy, without the need for actual deployment of configurations. This workflow is shown in Figure 3.

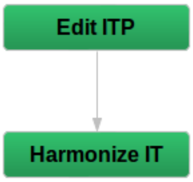


Figure 3: Edit and Harmonize ITP workflow graph.

Configure endpoint security control workflow

This workflow is used to refine an IT policy into access control configurations for endpoint security controls (e.g., operating systems, databases), to edit the generated configurations[1]. and to verify their coherence[2]. It requires the availability of a previously instantiated landscape description and of an IT policy, and optionally, of business requirements. It is suggested for security administrators whose objective is to generate a coherent set of configurations for the existing access control mechanisms. This workflow is shown in Figure 4.

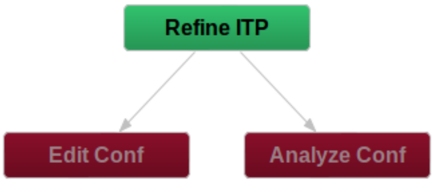


Figure 4: Configure endpoint security control workflow graph.

Configure infrastructure security control workflow

This workflow is used to refine an IT policy into configurations for filtering (e.g., firewalls) and data protection (channel and message protection systems) security controls (also including infrastructure security controls). It also allow users to specify and edit the generated logical associations and configurations, and to verify the coherence of both logical associations and configurations. It requires the availability of a previously instantiated landscape and optionally, of business requirements. Moreover, other policy meta-models can be optionally linked. It is suggested for security administrators whose objective is to generate a coherent and optimized set of configurations for the existing security mechanisms also including infrastructure elements like firewalls and VPNs. This workflow is shown in Figure 5.

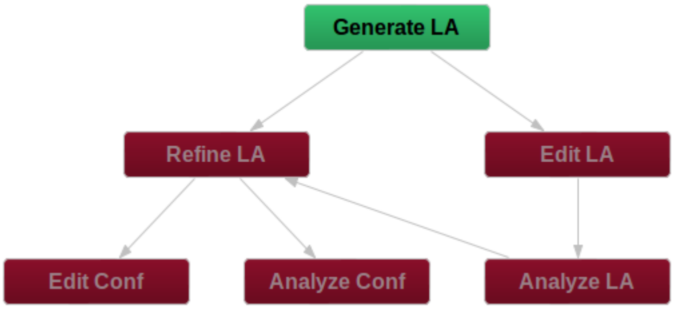


Figure 5: Configure infrastructure security control workflow graph.

Edit and analyze Logical Associations workflow

This workflow is used to specify and edit logical associations, and to verify their coherence. It requires the availability of a previously instantiated landscape. Moreover, an instantiation of the ontology (where the logical associations are or will be stored) can be optionally linked. It is suggested for security administrators whose objective is to generate a coherent set of end-to-end security requirements, for instance, the allowed communications and channels to protect. This workflow is shown in Figure 6.

Edit and analyze configurations workflow

This workflow is used to specify and edit configurations, and to verify their coherence. It requires the availability of a previously instantiated landscape description. Moreover, an instantiation of the configurations can

[1] an access control configuration editor is not yet available in this version of the SDSS
[2] an access control configuration editor is not yet available in this version of the SDSS

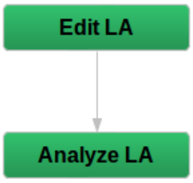


Figure 6: Edit and analyze Logical Associations workflow graph.

be optionally linked. It is suggested for security administrators whose objective is to perform fast and simple changes into the configurations, e.g., to cope with emergencies or attacks with the support of an anomaly analysis tools. Additionally, it can be used to directly write the configurations, but its use is not suggested as it invalidates all the main advantages of the policy-based refinement approach PoSecCo is proposing. This workflow is shown in Figure 7.

Analyze Conf
Edit Conf

Figure 7: Edit and analyze configurations workflow graph.

Optimize infrastructure security controls configurations workflow

This workflow is used to refine logical associations into a set of optimized configurations for filtering (e.g., firewalls) and data protection (channel and message protection systems) security controls (also including infrastructure security controls). It also allow users to specify and edit the generated logical associations and configurations, and to verify the coherence of both logical associations and configurations. It requires the availability of a previously instantiated landscape and optionally, of business requirements. Moreover, other policy meta-models can be optionally linked. It is suggested for security administrators whose objective is to generate a coherent and optimized set of configurations for the existing security mechanisms also including infrastructure elements like firewalls and VPNs but starting from a less abstract policy representation. This workflow is shown in Figure 8.

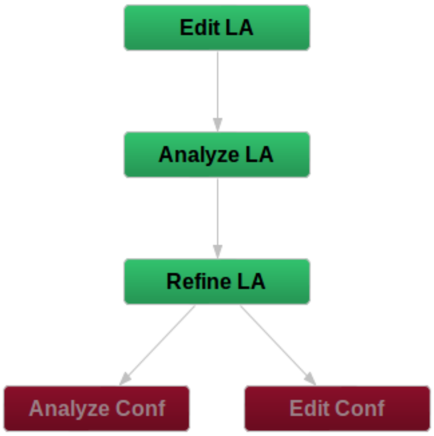


Figure 8: Optimize infrastructure security controls configurations workflow graph.

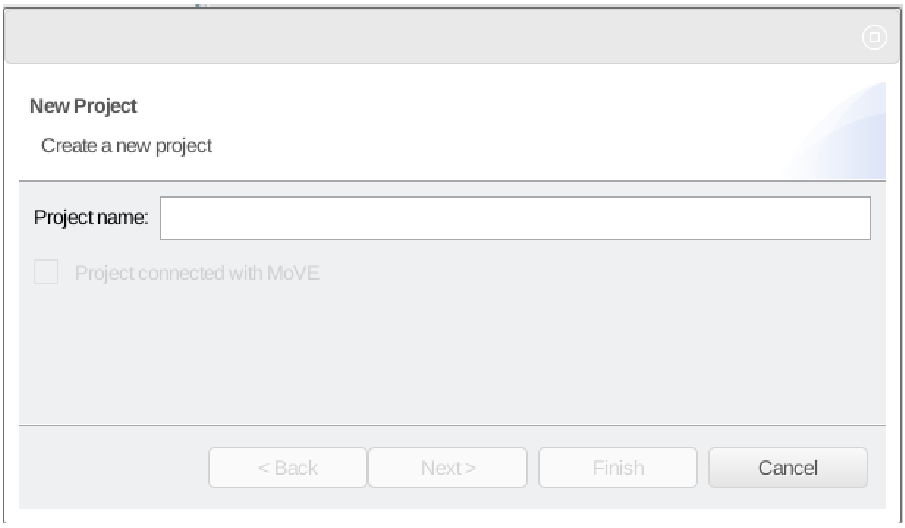
4 The project Manager

The first operation needed to use the SDSS is to select the active project, otherwise, no operations/phases are available. These task is performed by using the SDSS Project Manager that automatically starts when the SDSS is executed.

The available projects are listed in the PoSecCo Project Explorer View (see Figure 1). By clicking on one of the listed projects, the active project is automatically defined.

To create a new project, the SDSS Project Manager provides a wizard. By clicking on the "create new project button" (the big +), the user is required to:

- (Step 1) enter the name of the new project (see Figure 9);
- (Step 2) select the workflow type to use (see Figure 10);
- (Step 3) select the meta-model instantiations he wants to include (see Figure 11). A further check is performed to understand which meta-models can be included.



New Project

Create a new project

Project name:

□ Project connected with MoVE

Figure 9: Create new project wizard: name the project.

References

[1] The PoSecCo project. Analysis Service LA User Manual. http://security.polito.it/posecco/sdss/um-LAAnalysisService.pdf.

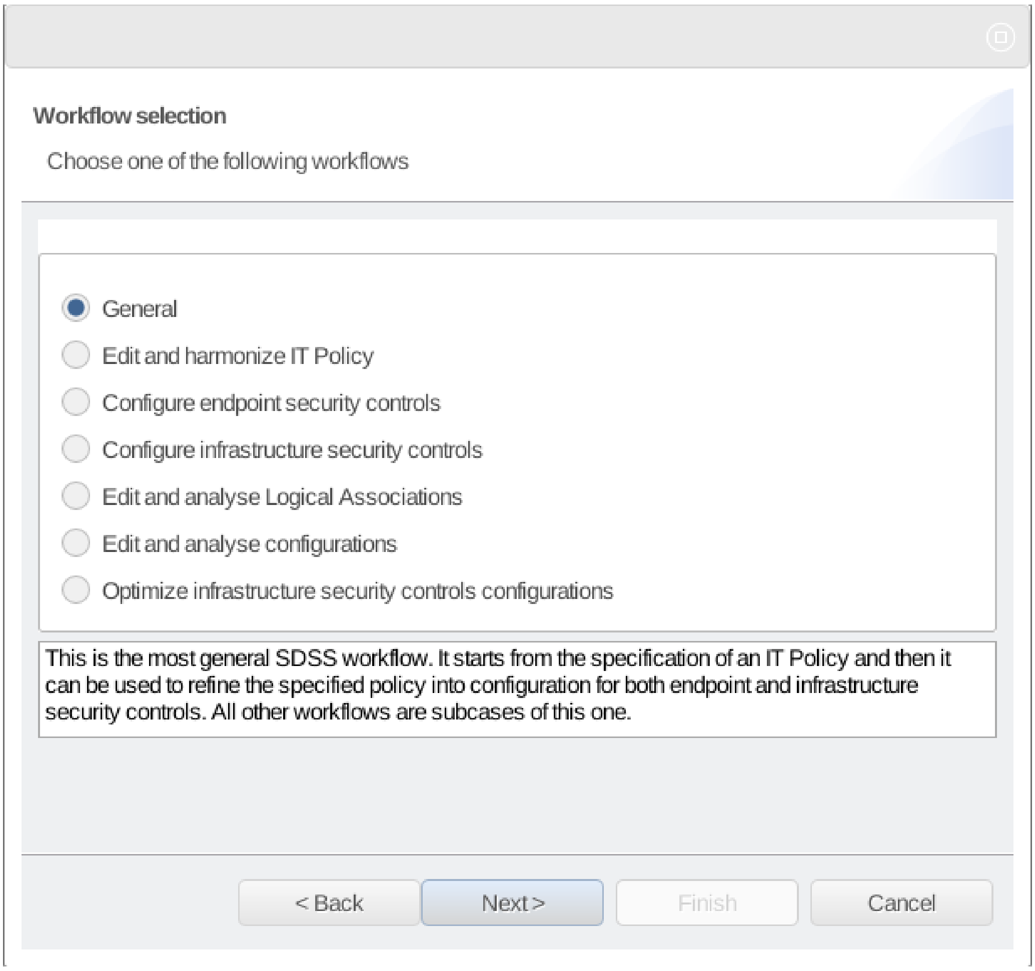
[2] The PoSecCo project. Analysis Service User Manual. http://security.polito.it/posecco/sdss/um-AnalysisService.pdf.

[3] The PoSecCo project. Configuration Editor User Manual. http://security.polito.it/posecco/sdss/um-ConfigurationEditor.pdf.

[4] The PoSecCo project. Infrastructure Configuration Service User Manual. http://security.polito.it/posecco/sdss/um-InfrastructureConfigurationService.pdf.

[5] The PoSecCo project. IT Policy Tool User Manual. http://security.polito.it/posecco/sdss/um-ITPolicyTool.pdf.

[6] The PoSecCo project. LA Generation Service User Manual. http://security.polito.it/posecco/sdss/um-LAGenerator.pdf.



Workflow selection

Choose one of the following workflows

● General

○ Edit and harmonize IT Policy

○ Configure endpoint security controls

○ Configure infrastructure security controls

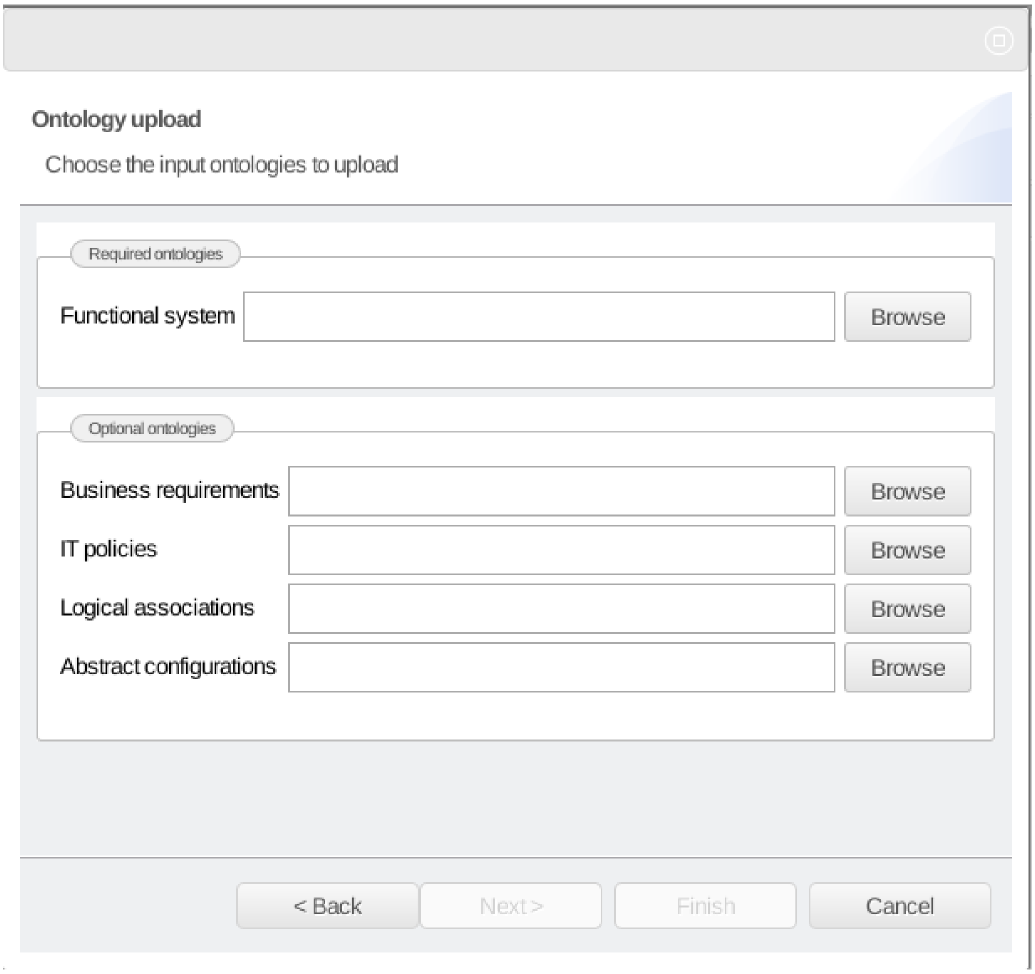
○ Edit and analyse Logical Associations

○ Edit and analyse configurations

○ Optimize infrastructure security controls configurations

This is the most general SDSS workflow. It starts from the specification of an IT Policy and then it can be used to refine the specified policy into configuration for both endpoint and infrastructure security controls. All other workflows are subcases of this one.

Figure 10: Create new project wizard: choose the workflow.



Ontology upload

Choose the input ontologies to upload

Figure 11: Create new project wizard: choose meta-models.