|  |
| --- |
| HUSACCT |
| Manual HUSACCT |
| Validate component |

**Introduction**

The validate component of the HUSACCT application is responsible for validating the defined rules against the analysed dependencies. This manual will describe the features that the users can use of the GUI that the validate part of the application provides for the user.

The precondition before this part of the application can be used are:

* The source code is analysed
* Logical modules are defined
* The classes or packages of the source code are mapped to the defined logical modules
* The logical defined architecture must contain rules

Table of contents

[1. Terminology 2](#_Toc327619491)

[2. Supported rules 3](#_Toc327619492)

[3. Browse Violations 5](#_Toc327619493)

[3.1 Filter dialog 7](#_Toc327619494)

[4. Exporting a report 10](#_Toc327619495)

[5. Configuration 11](#_Toc327619496)

[5.1 Configure severities 11](#_Toc327619497)

[5.2 Configure severities per rule type and per violation type 12](#_Toc327619498)

[5.3 Configure active violation types 13](#_Toc327619499)

# Terminology

Not all use cases will be covered in this document, but sometimes some terms will be used to make some things clear. Therefore most used terminology will be explained in this paragraph.

History points  
When HUSACCT periodically is used, there might be the need of an overview of violations in the past. One point of the past is a history point.

Rule types and violation types  
A rule is of specific type (rule type). A rule that can be applied on ore more modules (depending on the rule type).   
A violation type is the type of the violation that can occur during the validation process. It is possible to filter on violation types in the define process (see for more information the documentation of the define component).

Exception rules  
Some rule types can have exception exception rules are mostly counterparts of the rule type. For example the exception rule of rule type ‘Is Not Allowed To Use’ is Is Allowed To Use’.

Violation

When a rule is exceeded during validation process, a violation is occurred.

Severity

Each rule and violation type have their own severity. If a rule has a lower severity than a violation type (or vice versa), always the highest severity will be taken as the severity.

# Supported rules

The following rules are provided in the HUSACCT applications and can be validated and which exception are possible on the specific/explained rule. Every rule has violation types, the possible violation types will be given for each rule.

Interface convention

A specified module must implement an interface or one interface of another specified component, package or class.

The exception that is possible on this rule is that there is a possibility to exclude classes/packages from this rule.

Subclass convention

A specified module must extend a class or one interface of another specified component, package or class.

The possible exception is that there is a possibility to exclude classes/packages from this rule.

Naming convention

All the classes and/or packages in the specified module must meet to the specified regex (see table 1).

The possible exceptions are:

* a possibility to exclude classes/packages
* add another naming convention for classes/packages that were specified in the main rule.

|  |  |  |
| --- | --- | --- |
| Regex | Validates |  |
| \*Friends\* | domain.locationbased.foursquare.History  domain.locationbased.latitude.Friends  infrastructure.socialmedia.locationbased.foursquare.FriendsDAO  infrastructure.socialmedia.locationbased.foursquare.MyFriendsDAO | false  true  true  true |
| \*Account | domain.locationbased.foursquare.MyAccount  domain.locationbased.latitude.Map  infrastructure.socialmedia.locationbased.foursquare.AccountDAO | true  false  false |
| DAO \* | infrastructure.socialmedia.locationbased.foursquare.DAOFourSquare  infrastructure.socialmedia.locationbased.foursquare.IMap  domain.locationbased.foursquare.History | true  false  false |

Table 1

The first regex of table 1 enforces that a class/packages must contain the word ‘Friends’ (case-sensitive).

The second regex enforces that a class/package must end with the word ‘Account’ (case-sensitive). The third regex enforces that all the classes and/or packages must start with the word ‘DAO’ (case-sensitive).

Visibility convention

All the classes and/or packages in the specified module must have to specified visibility.

The possible exceptions are:

* a possibility to exclude classes/packages
* add another visibility convention for classes/packages that were specified in the main rule

Is allowed to use

This rule can only be defined as exception rule. All the classes/packages between two logical modules are allowed to have a dependency.

Is not allowed to use

All the classes/packages between two logical modules are not allowed to have a dependency with each other.

The possible exception is to define a ‘is allowed to use’ rule.

Is only allowed to use

One defined logical module is only allowed to have dependencies with another defined logical module.

The possible exception is to define a ‘is allowed to use’ rule.

Is only module allowed to use

Of all defined logical modules may only one logical module have dependencies with another specified logical module.

There are no possible exception rules.

Must use

At least one class/package between two logical modules must have a dependency with each other.

The possible exception is to define a ‘is allowed to use’ rule.

Is not allowed to make back-call

This rule can only be applied on modules of type layer (see for more information the manual of the define component). A layer may not have dependency with layers that are defined with a higher hierarchal level then the layer on which the rule is applied to.

The possible exception is to define a ‘is allowed to use’ rule.

Is not allowed to make skip-call

This rule can only be applied on modules of type layer (see for more information the manual of the define component). A layer may not have dependency with layers that are defined with a lower hierarchal level then the layer on which the rule is applied to, except for the layer that is directly under the layer on which the rule is applied to.

The possible exception is to define a ‘is allowed to use’ rule.

# Browse Violations

After defining the logical architecture, mapping scanned source code to the logical architecture and defining rules in the logical architecture the possibility is available to check if the defined architecture has violations.

This can be done in the *browse violations screen* (figure 1). The goal of this screen is to validate the project and to see if any violations have occurred. Additional features are:

* sorting
* filtering
* creating a history point.

The screen can be opened through “menu -> Validate -> Validate now” or by pressing the “validate now” icon (C:\git\Nieuw\HUSACCT-1\src\husacct\common\resources\control\icon-validate.png) in the quick menu. The screen will be available after classes are mapped to a logical architecture.

**Note: When storing the workspace the violations won’t be stored. The violation history points are experimental and unwanted behavior can occur.**

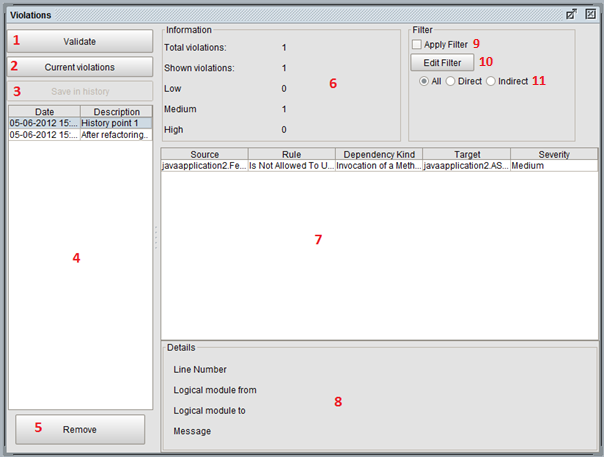


Figure 1 *Browse Violations screen*

Explanation of components of figure 1:

1. When this button is pressed, the system will check if there are violations on the defined rules.
2. When this button is pressed, the last known violations will be shown to the user. The violations will be shown in area 7.
3. When this button is pressed, the system creates a history point of the last known violations. When the violations are saved the system will disable the button. For saving the violations you need to add a description of the violations.
4. This table contains all the created/available history points. After clicking on a row, the system will show the violations that are saved in that point. The violations will be shown in area 7.
5. When this button is pressed, the system will remove the selected history point. Selected in area 4.
6. This panel shows information about the amount of violations. It shows the total violations, the violations shown this moment and the amount of violations per severity.
7. This table shows all the violations. The violations can be sorted by clicking on the headers, e.g. ‘Source’. If you want more information about a violation select the row of the specific violation. The information will be shown in area 8.

* Source: the ‘from’ path from which the dependency/violation starts. Contains the physical path of the source file were the violations occurs.
* Rule: the name of the defined rule.
* Dependency kind: the type of dependency/violation that occurs in this violation.
* Target: the ‘to path from which the dependency/violation ends. Contains the physical path of the source file were the violations occurs.
* The severity of the violation.

1. This panel shows information about the selected of the selection violation in area 7.

* Line number: the line number in the source code where this violations occurs.
* Logical module from: the name of the logical module where the physical class of the ‘Source’ column of area 7 is mapped into.
* Logical module to: the name of the logical module where the physical class of the ‘Target’ column of area 7 is mapped into.
* Message: a textual description of the defined rule.

1. With this checkbox you can turn the filter on or off.
2. When this button is pressed it will open the Filter dialog, (part 2).
3. This is an on screen filter to switch between all kinds of dependencies, only direct dependencies or only indirect dependencies. These only work when the checkbox of area 9 is selected.

## Filter dialog

The violations table can also be filtered. This screen provides an easy to use way to filter the violations. During filtering can be chosen to show or hide the selected values. There are two tabs in this screen. In the first tab only the rule types and violation types are shown. In the second tab there is a possibility to filter on the source path of the violations.

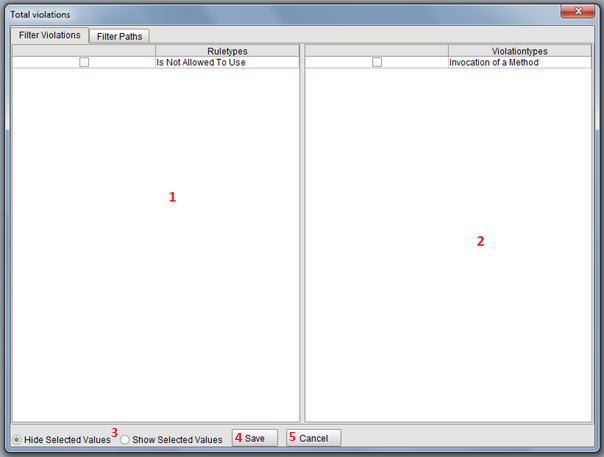


Figure 2 *Filter Dialog tab for filtering rule- and/or violation types*

1. In this table the rule types that will be filtered can be selected.
2. In this table the violation types that will be filtered can be selected.
3. The option to choose if the filtered values must be shown or must be hidden.
4. When this button is pressed, the violations will be filtered.
5. When this button is pressed, the screen will be closed.

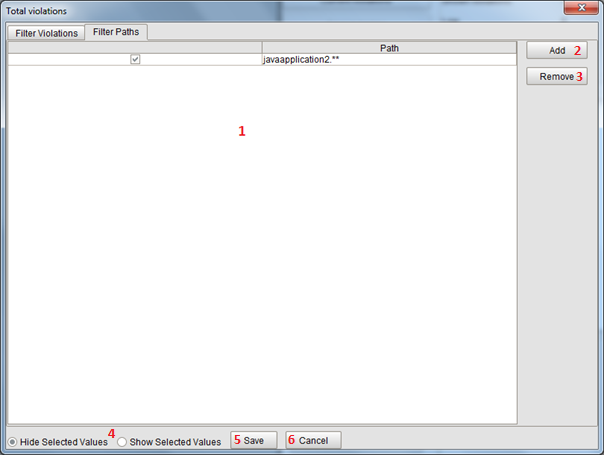


Figure 3 *Filter dialog tab for filtering classpaths*

1. This table shows all the paths are added to filter. The physical paths can be filtered with a regex, the possibilities will be explained in table 2.
2. When this button is pressed, the system will add an empty field to area 1.
3. When this button is pressed, the system will remove the selected row from area 1.
4. The option to choose if the filtered values must be shown or must be hidden.
5. When this button is pressed, the violations will be filtered.
6. When this button is pressed, the screen will be closed.

|  |  |  |
| --- | --- | --- |
| Your Input Example | Path Input Example | Output Example |
| java.St\* | java.String  java.StringBuffer  java.String.Fake  com.class.String | java.String  java.StringBuffer |
| java.St\*\* | java.String  java.StringBuffer  java.String.Fake  com.class.String | java.String  java.StringBuffer  java.String.Fake |
| \*.String | java.String  java.StringBuffer  java.String.Fake  com.class.String | java.String |
| \*\*.String | java.String  java.StringBuffer  java.String.Fake  com.class.String | java.String  com.class.String |
| \*\*Stri\*\* | java.String  java.StringBuffer  java.String.Fake  com.class.String | java.String  java.StringBuffer  java.String.Fake  com.class.String |

Table 2 *overview of possible regexes for filtering*

# Exporting a report

There also is the possibility to export the violations. Currently the violations can be exported to the following file types:

* XML
* HTML
* PDF

You can open this screen at “menu -> Validate -> Violation Report”.



Figure 4 *Export report browse dialog*

1. When this button is pressed, it opens an export dialog. (see figure 5)
2. When this button is pressed, the report will be exported.



Figure 5 *Export Report file dialog*

1. Select the file name and directory where the file must be saved.
2. Select the type of the file.
3. When this button is pressed, the path will be set in figure 4.
4. When this button is pressed, the screen will be closed.

# Configuration

The validate component provides also the possibility to configure the following:

* Severities; adding new severities and change existing severities.
* Severity per rule type; change the severity for a rule.
* Severity per violation type; change the severity for a violation type.
* Active violation types; which violation types should be enabled by default in the filter when adding new rules in the define component. (For more information about filtering in rule types see the manual of the define component.)

The changes that are made are not directly reflected in the GUI. For example when severities are changed in the configuration, there must be revalidated to reflect the changes that are made in the configuration.

The screen is available once a workspace has been created. The configuration screen is available through “menu -> Validate -> Configuration”.

## Configure severities

There are two or more tabs on the screen. The first is to create and edit severities. For every supported programming language a tab will be shown. Inside each of ‘programming language’ tab will contain three other tabs. The first two tabs are for setting the severity per rule/ violation types. The last tab is to set the active violation types.



Figure 6 *Configuration tab for changing and/or adding severities*

1. This table lists all the severities. It is possible to change the name and/or color of a severity. The color can be changed by clicking on the color bar and a color picker dialog will pop up. The severities are in order from lowest to highest.
2. When this button is pressed, an empty severity will be added on the lowest place.
3. When this button is pressed, the selected severity will be moved up in the list.
4. When this button is pressed, the selected severity will be moved down in the list.
5. When this button is pressed, all the severities will be restored to the default severities.
6. When this button is pressed, all the changes in this tab will be saved.
7. When this button is pressed, the screen close without saving

## Configure severities per rule type and per violation type



Figure 7 *Configuration tab for assigning severities to a rule-/violation type*

This screen applies for the first two tabs.

1. List of categories.
2. Table with rule types or violation types. Changed by selecting a different category in area 1. You can change the severity by clicking on the severity name.
3. When this button is pressed, the selected rule type will be restored to its default severity level.
4. When this button is pressed, all the rule/ violation types will be restored to their default value.
5. When this button is pressed, all the changes in this tab will be saved.
6. When this button is pressed, the screen close without saving.

## Configure active violation types



Figuur 8 Configuration tab for setting the active violationtypes per rule type

1. List of categories.
2. List of rule types. Changes when you select another category in area 1
3. Table of active violation types. Changes when you select another rule type in area 2.
4. When this button is pressed, selects all the active violation types.
5. When this button is pressed, deselect all the active violation types
6. When this button is pressed, all the changes in this tab will be saved.
7. When this button is pressed, the screen close without saving