Creating Custom Test Configurations

In this section:

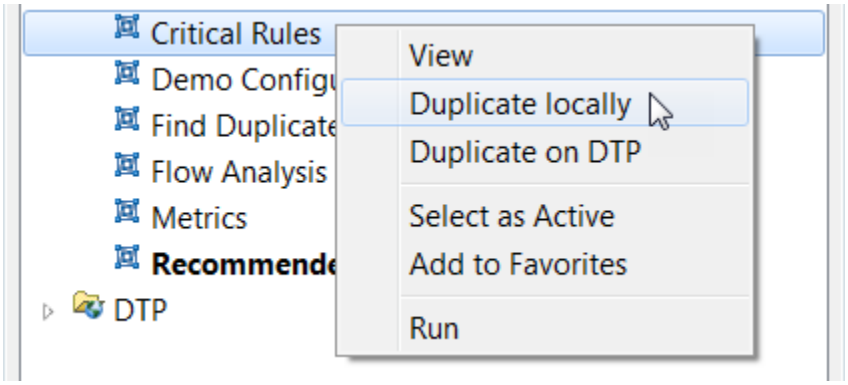
To create a custom test configuration, you need to:

1. Duplicate an existing test configuration locally or on DTP.
2. Modify the duplicated configuration to meet your organization's development policy.

Creating and Customizing Test Configurations Locally

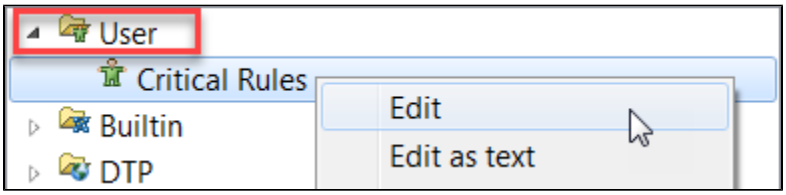
To create a custom configuration locally, you need to copy a selected built-in configuration to the User directory, and then customize the duplicated configuration.

1. Click **Parasoft** in the menu bar and choose **Options** (Visual Studio) or **Preferences** (Eclipse). Then select **Configuration**.
2. Right-click the test configuration you want to duplicate, then choose **Duplicate Locally**.



   The configuration will be added to the **User** directory and nested in a parent directory matching the source.
3. Right-click the duplicate configuration and choose **Edit** to open the Test Configuration Editor in you browser.

   NOTE: The Test Configuration Editor is handled by a separate web server process and may be blocked if a strict firewall is installed on your machine. In such case, allow the process to run when prompted.

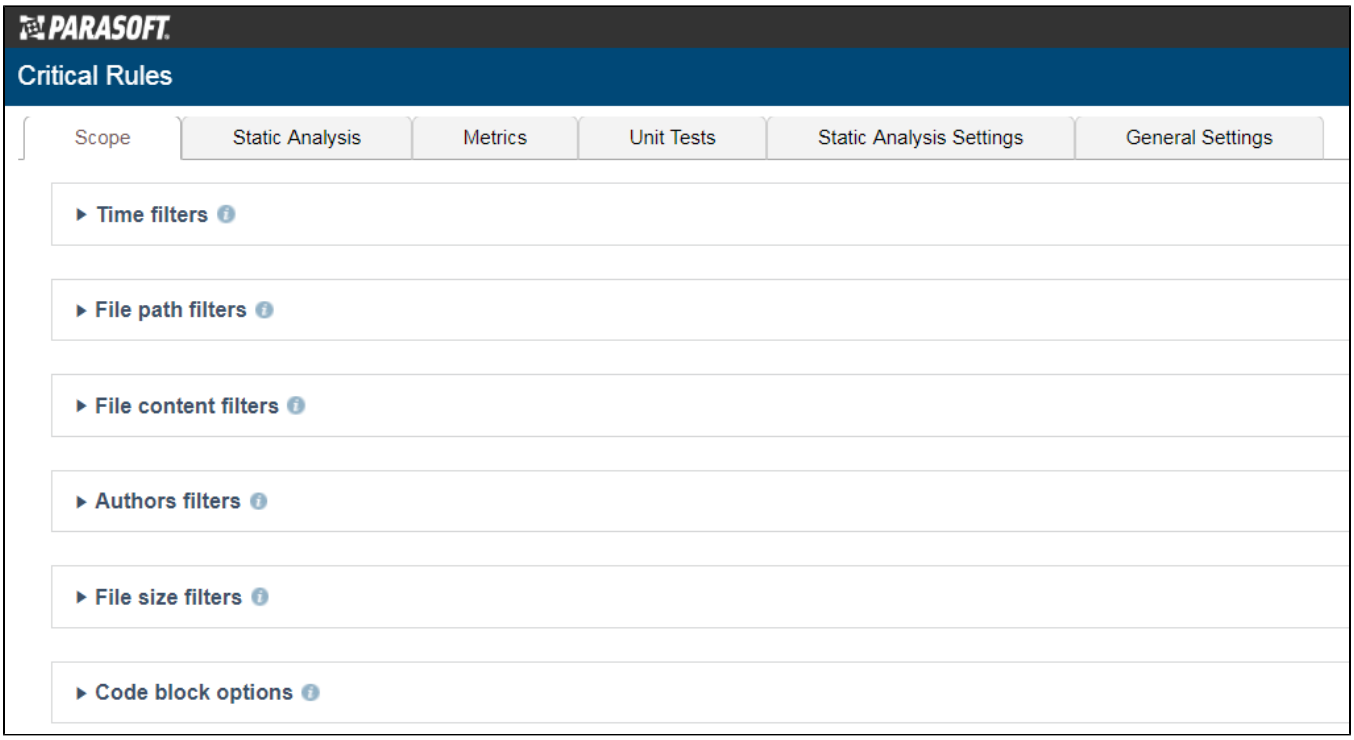


   Choosing **Edit as text** opens a textual representation of the configuration in a simple configuration editor (deprecated).

4. Click a tab to access a group of related test configuration settings. For additional information about test configuration settings, mouse over an information icon ("i") next to a configuration setting. The following tabs are available:
   - Scope Tab
   - Static Analysis Tab
   - Metrics Tab
   - Unit Tests Tab
   - Static Analysis Settings Tab
   - General Settings Tab

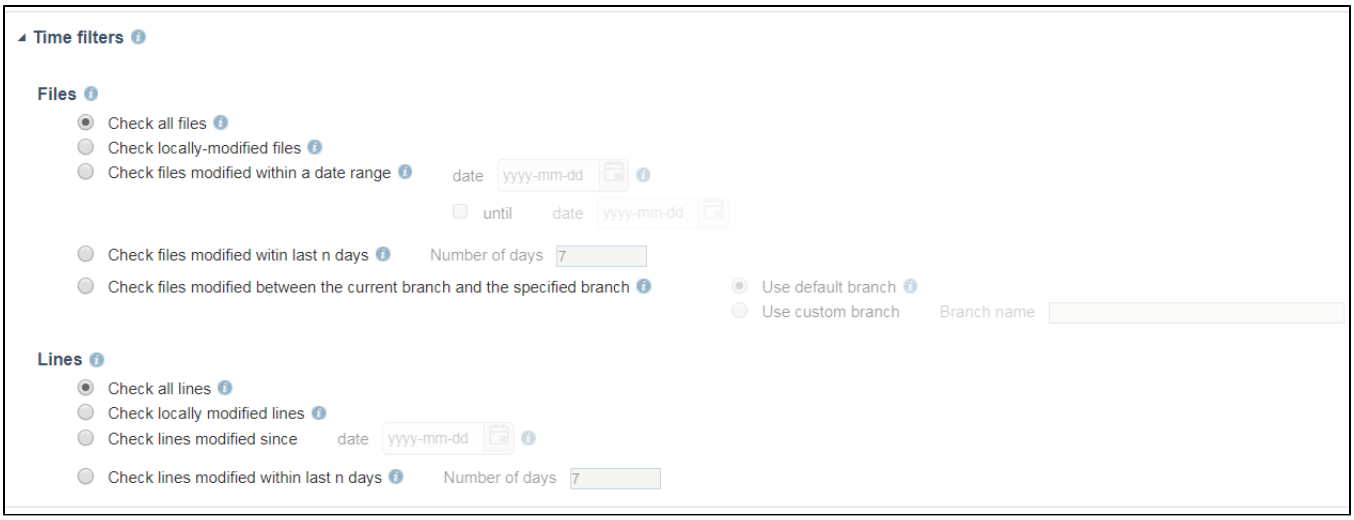
Scope Tab

The **Scope** tab contains a set of filters that you can configure to define the parts of the code that the test configuration should cover. You must connect the C/C++test to source control in order to collect scope information. Click **Save** to preserve any changes you make on this tab.



Time Filters

Expand the **Time filters** settings to set time-based filters at the file or line level. The time filters enable you to restrict the scope of analysis to a specific date range or period. If the `scope.scontrol` setting is set to `true` and the source control settings for C/C++test are configured, the modification time is set from the source control history. If `scope.local` is set to `true`, then the modification time is set form the file system of the machine running analysis.



You can configure the following settings:

File-level settings

Check all files	Default. Enable this option to include all files in the scope of the analysis the user has access to.
Check locally-modified files	Enable this option to check only locally-modified files. Files in the source control system will be excluded. The following setting must be configured for this option to take effect: `scope.scontrol=true`
Check files modified within a date range	Enable this option and specify a date range to include in the scope. Files that were modified or added within the specified range will be checked.

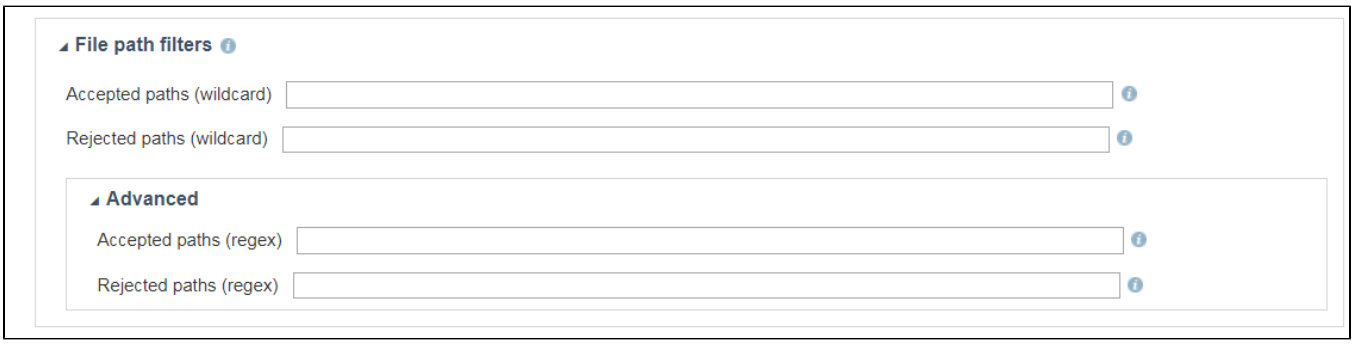
Check files modified witin last n days	Enable this option and specify the number of days to include in the scope. Files that were modified or added within the specified number of days will be checked.
Check files modified between the current branch and the specified branch	Enable this option to specify a range of branches to include in the scope. Files that were modified from the user's current branch to the specified branch will be checked. Files that did not change between branches are excluded. You can enable the following options: • Enable the **Use default branch** option to compare the current branch to the branch that the SCM considers default. • Enable the **Use custom branch** and specify a branch to compare with the current branch.

Line-level Settings

Check all lines	Default. Enable this option to include all lines of code in the scope of the analysis the user has access to.
Check locally-modified lines	Enable this option to check only locally-modified lines of code. Lines of code in the source control system will be excluded. The following setting must be configured for this option to take effect: `scope.scontrol=true`
Check lines modified since	Enable this option and specify a cut-off date to include in the scope. Lines of code that were modified or added within the specified range will be checked.
Check lines modified witin last n days	Enable this option and specify the number of days to include in the scope. Lines of code that were modified or added within the specified number of days will be checked.

File Path Filters

Expand the **File path filters** section to specify file path patterns to include and/or exclude from analysis. Relative paths within a workspace/solution.



The following settings are available:

Accepted paths (wildcard)	Specify a comma-separated list of files to include. Wildcards are supported (e.g., *.cpp, *.java, *.cs).
Rejected paths (wildcard)	Specify a comma-separated list of files to exclude. Wildcards are supported (e.g., *.cpp, *.java, *.cs).

Expand the **Advanced** discloser triangle to use regular expressions to set the file path filters. The following settings are available:

Accepted paths (regex)	Specify a regular expression. Files that match the pattern will be included in the analysis.
Rejected paths (regex)	Specify a regular expression. Files that match the pattern will be excluded in the analysis.

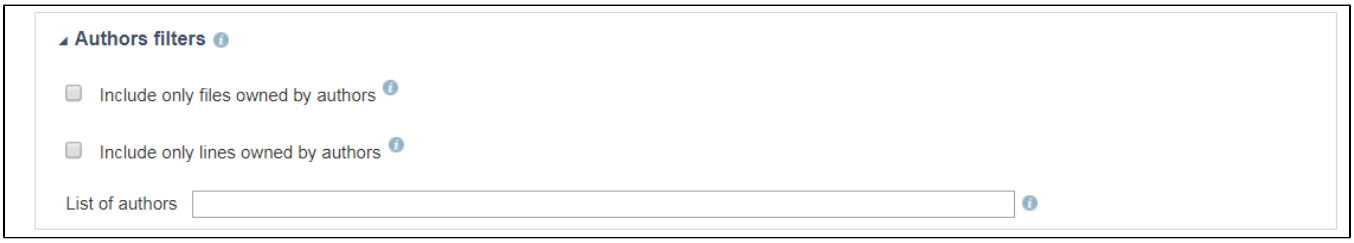
File Content Filters

Expand the **File content filters** section to specify regular expressions that exclude specific types of files based on content, e.g., auto-generated files.

> **File filtering takes priority over code block filtering**
>
> A potential conflict may occur if you use both filter types at the same time.

Author Filters

Expand the **Author filters** section to limit the scope of analysis to specific authors. If the `scope.scontrol` setting is set to `true` and the source control settings are configured, then file authorship is taken from the source control system. If the `scope.xmlmap` is set to `true` and the XML map settings are configured, then files authorship is taken from the map.

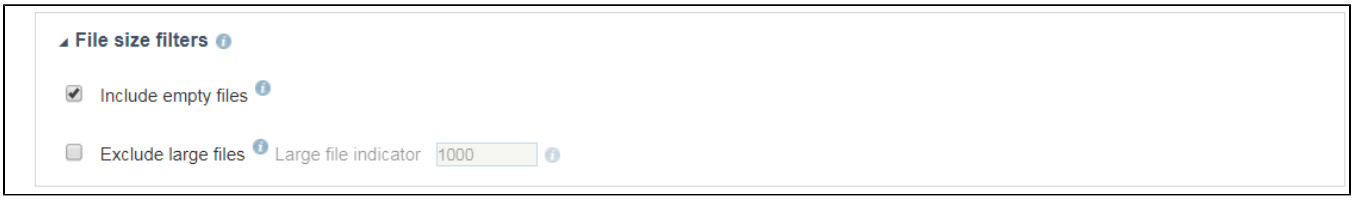


The following options are available:

Include only files owned by authors	Enable this option to only include files owned by the authors specified in the List of authors field.
Include only lines owned by authors	Enable this option to only include lines of code owned by the authors specified in the List of authors field.
List of authors	Specify a comma-separated list of authors whose code should be analyzed.

File Size Filters

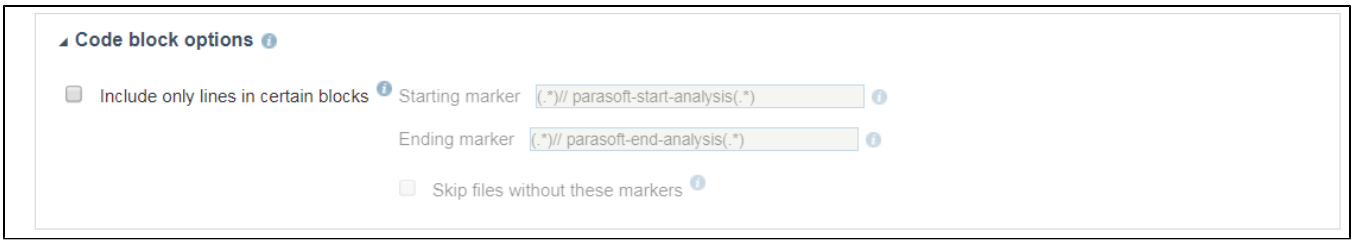
Expand the **File size filters** section to limit the scope of analysis based on file size.



Code Block Options

Expand the **Code block** options section to define specific blocks of code to include or exclude from the analysis.

> **File filtering takes priority over code block filtering**
>
> A potential conflict may occur if you use both filter types at the same time.

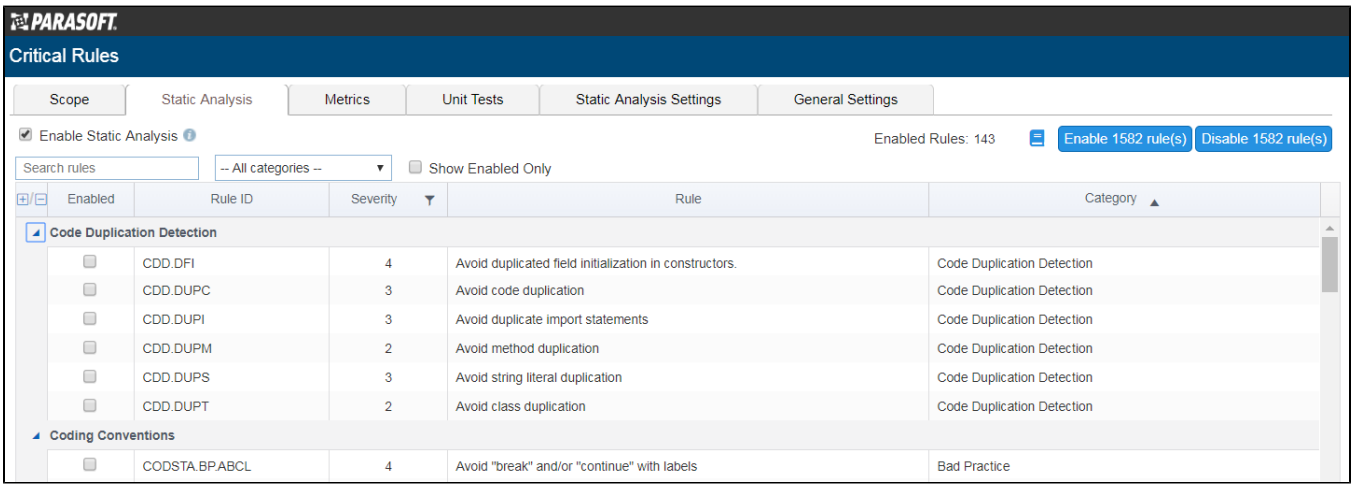


Include only lines in certain blocks	Enable this option to include only the code defined by the Starting and Ending marker fields in the analysis.
Starting marker	Specify a regular expression to mark the start of the code block that should be analyzed.
Ending marker	Specify a regular expression to mark the beginning of the code block that should be analyzed.

Skip files without these markers	Enable this option skip files that do not include patterns that match the Starting and Ending marker fields.

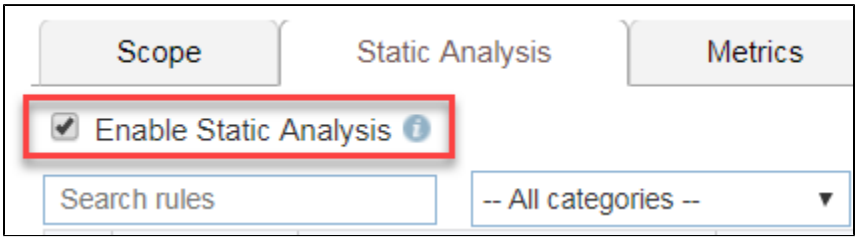
Static Analysis Tab

Click the **Static Analysis** tab to enable/disable the static analysis rules the configuration uses. This page shows all the supported rules. Click **Save** to preserve any changes you make on this tab.



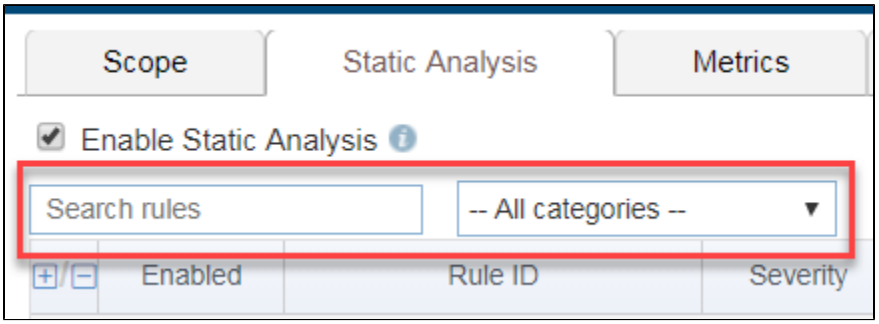
Enabling Static Analysis

Enable or disable the **Enable static analysis** checkbox to enable/disable static and flow analysis.

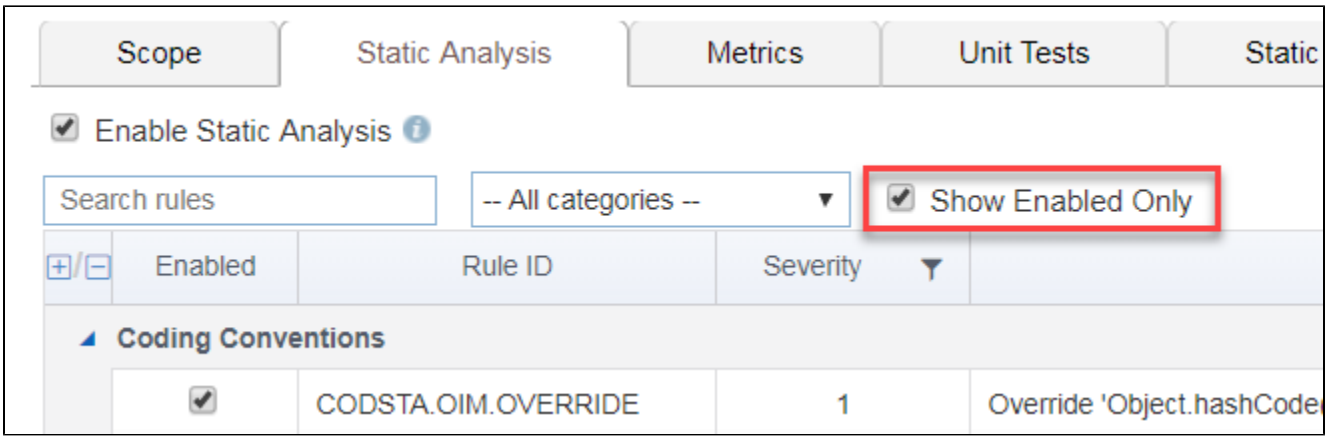


Finding Rules

You can use the search bar to find a specific rule or rule category. You can also use the drop-down menu to filter by category and browse for a rule.

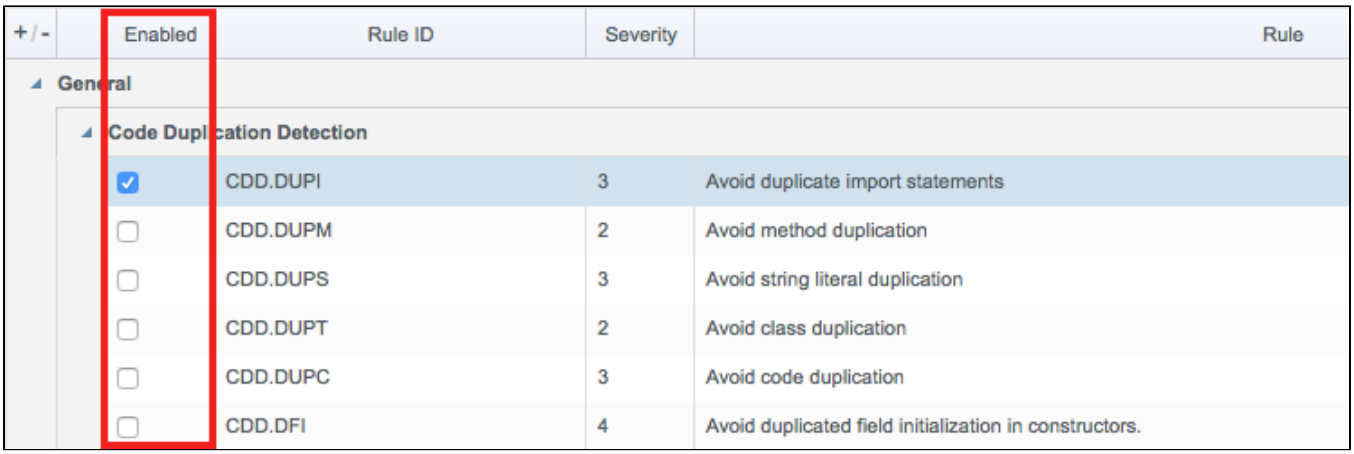


Enable the **Show Enabled Only** option to only show the enabled rules.

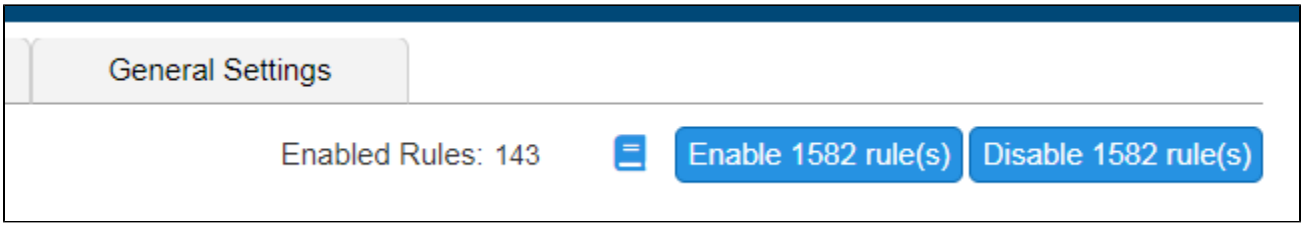


Enabling and Disabling Rules

Rules are grouped by category. Expand a category and enable the rule to use it in the test configuration.

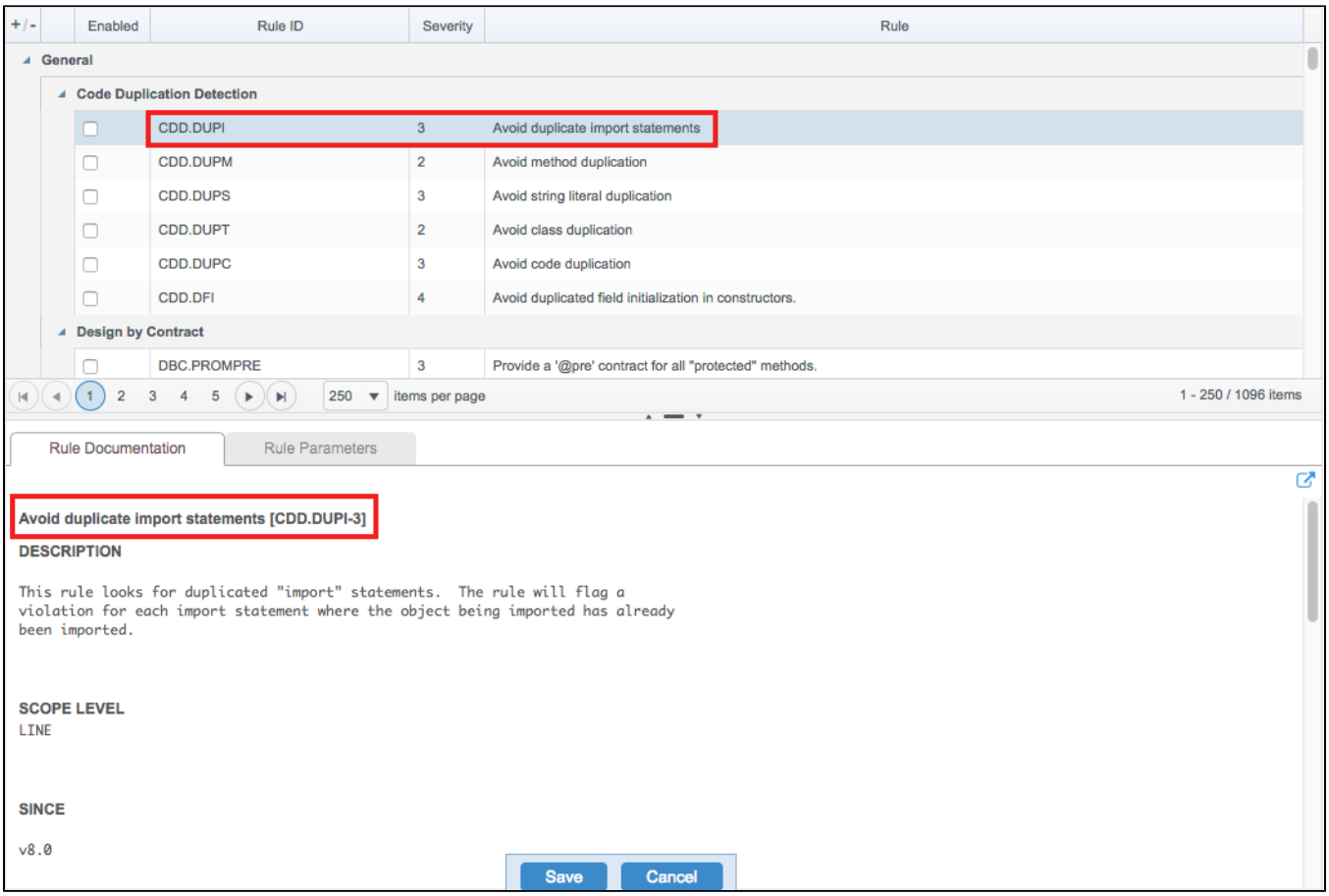


Click the **Enable [number] of rule(s)** or **Disable [number] of rule(s)** button to quickly enable or disable all rules in the configuration.

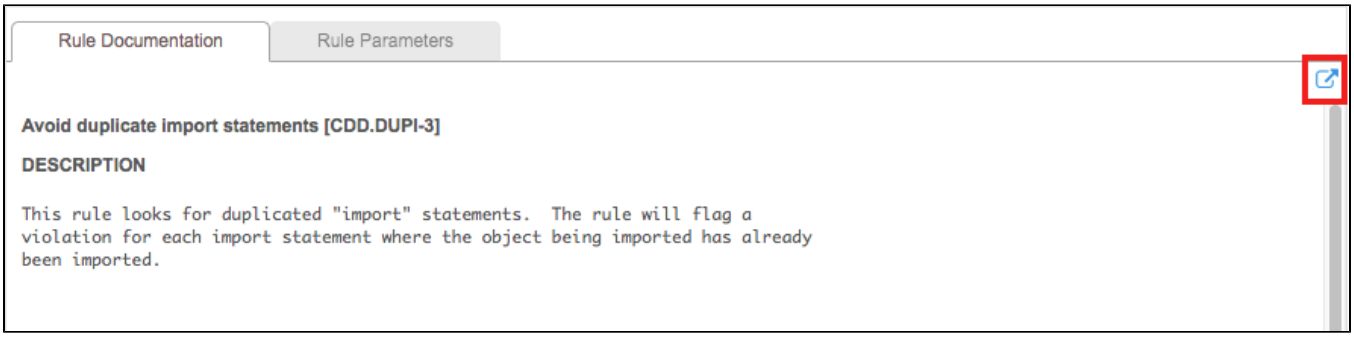


Viewing Rule Documentation

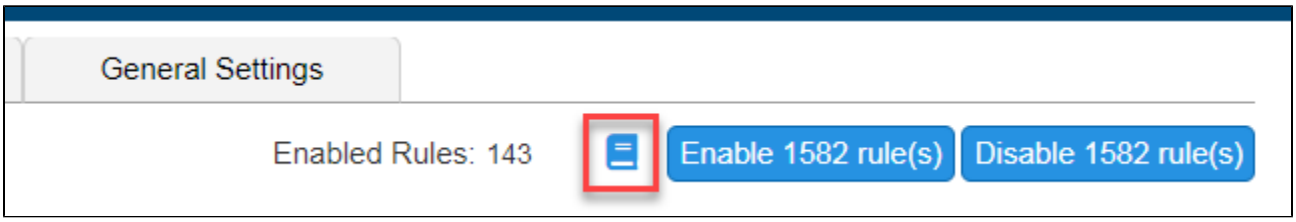
Click on a rule to open the documentation panel.



You can also open the rule documentation in new browser tab.

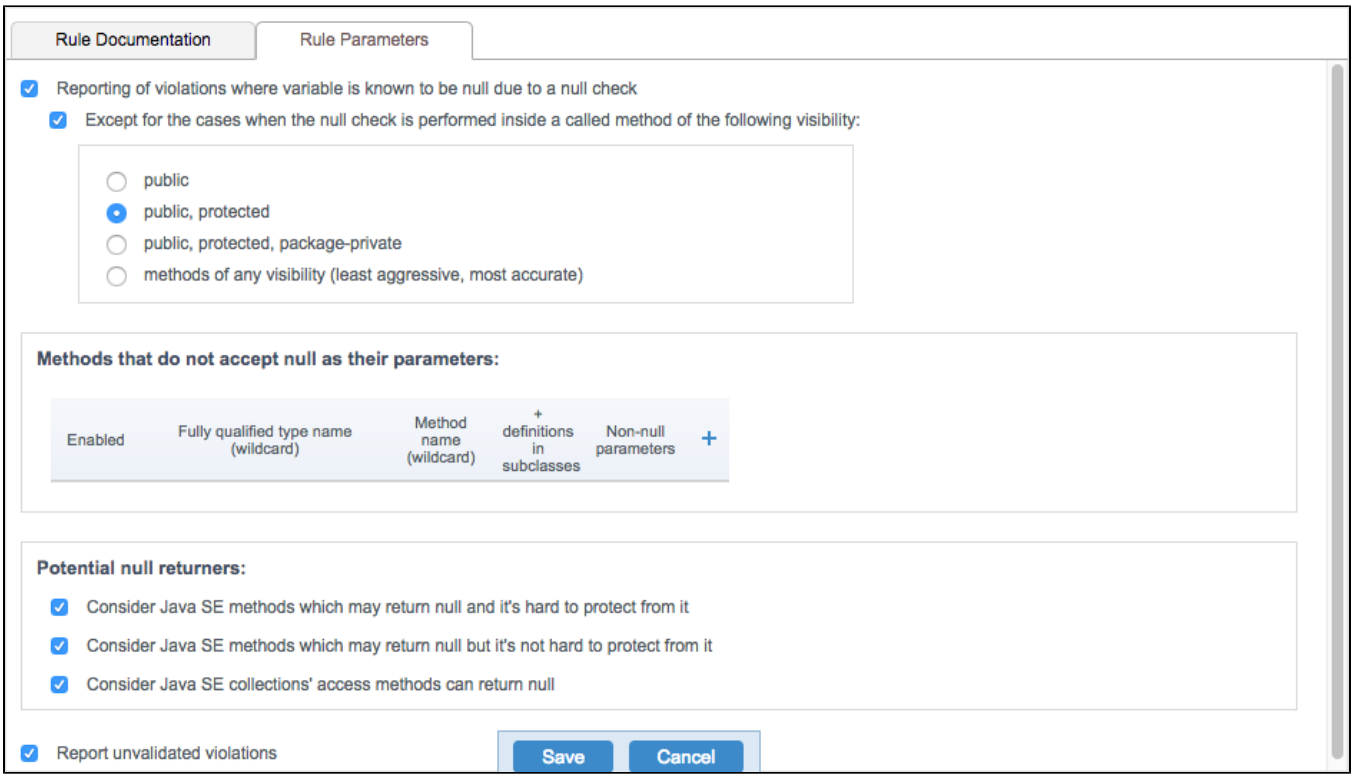


Click on the documentation icon to open all documentation for the enabled rules in a new browser tab.



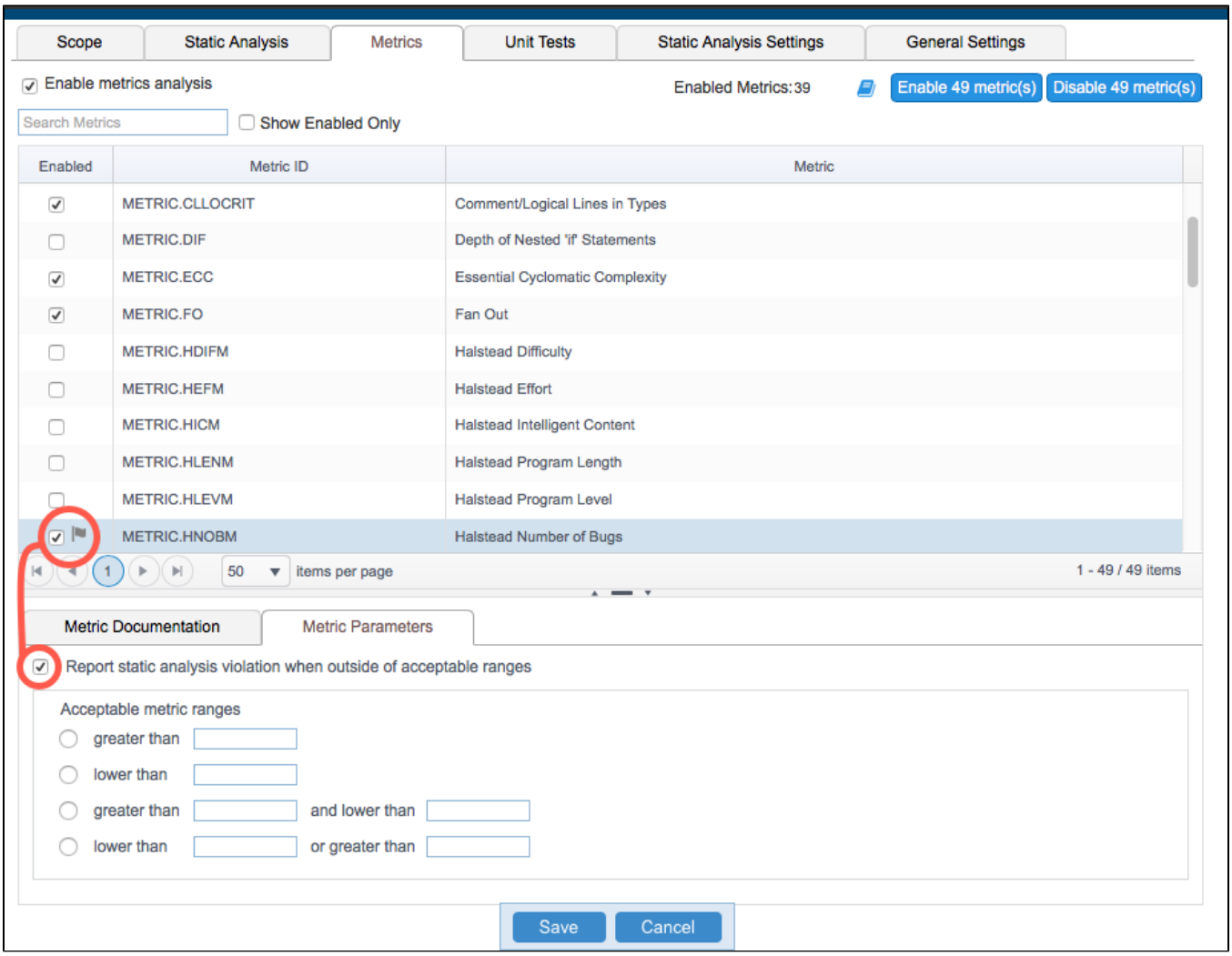
Parameterizing Rules

If the rule can be configured, parameters can be set in the rule options panel. Click on a rule and click the Rule Parameters tab to configure the rule. The options available are specific to each rule.



Metrics Tab

Click the **Metrics** tab to enable/disable the metrics collected and calculated during analysis. Click **Save** to preserve any changes you make on this tab.

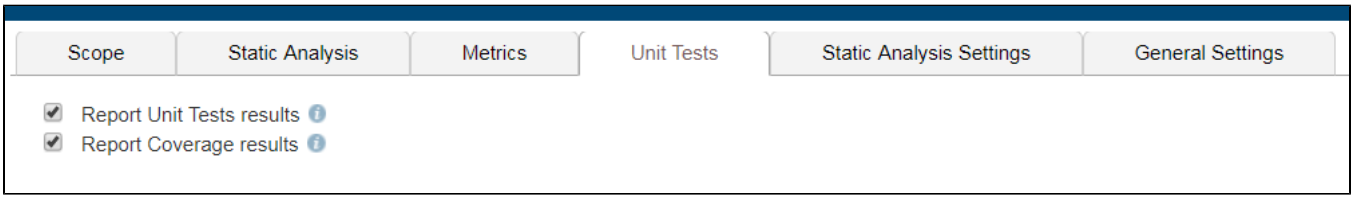


You can perform the following actions:

- Enter a metric ID in the search field to locate a specific metric.
- Enable the **Show Enabled Only** option to filter by enabled metrics.
- Click **Enable [n] metric(s)** or **Disable [n] metric(s)** to enable or disable all metrics in the test configuration.
- Enable/disable individual metrics.
- Enable the **Report static analysis violation when outside of acceptable ranges** option to configure an upper and lower threshold for the metric. A flag icon will appear in the Enabled column if this option is enabled.
- Click on a metric to view the documentation.

Unit Tests Tab

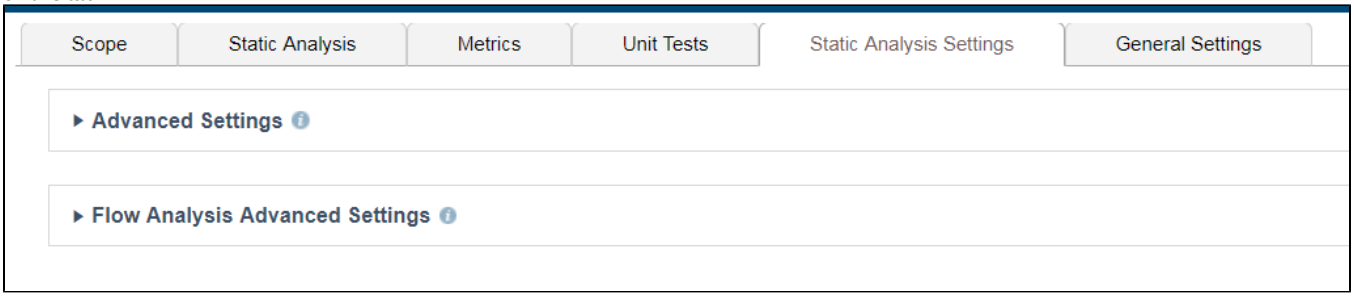
Click the **Unit Tests** tab to access controls for unit test execution and coverage data collection.



You can enable/disable the collection of unit test results and coverage analysis.

Static Analysis Settings Tab

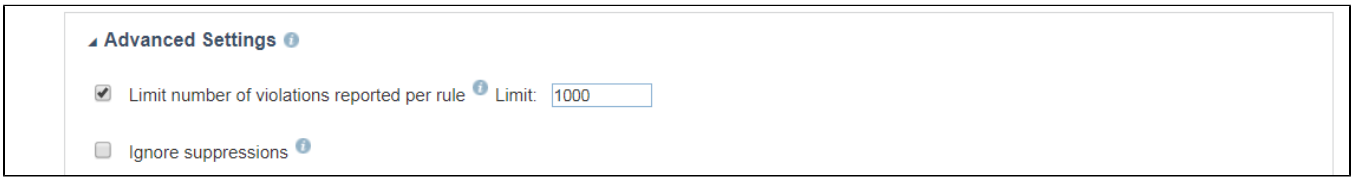
Click the **Static Settings Analysis** tab allows you to configure your static analysis and flow-based analysis. Click **Save** to preserve any changes you make on this tab.



Advanced Settings

Expand the **Advanced Settings** section to enable the following options:

- Set an upper limit on the number of violations that can be reported for each rule.
- Enable/disable suppressions configured on the Engine host.



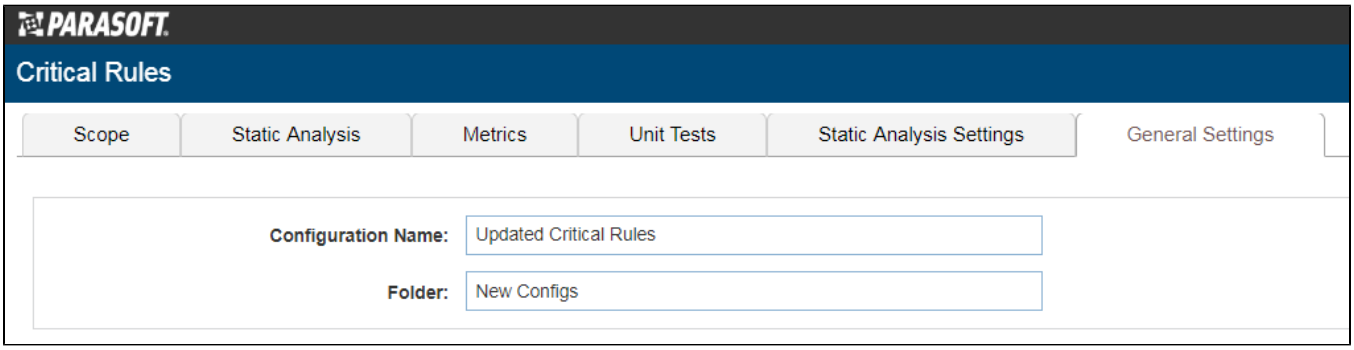
Flow Analysis Advanced Settings

Expand the Flow Analysis Advanced Settings section to configure settings related to performance, reporting verbosity, null-checking method parameterization, and resources checked.

See Configuring Flow Analysis for details.

General Settings Tab

Click on the **General Settings** tab to view and edit the name and location of the test configuration. Click **Save** to preserve any changes you make on this tab.

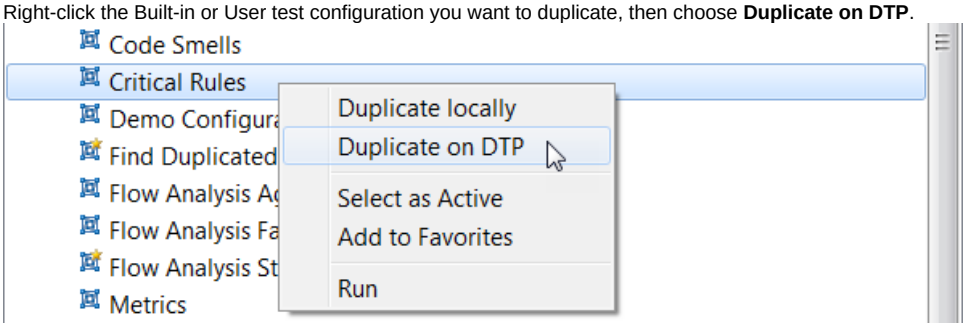


Enter a name in the **Folder** field to change the location of the test configuration. Entering the name of an existing folder moves the test configuration to that location in the test configuration tree. If the name you specify doesn't exist, a new folder will be created and the test configuration moved into it. You can also nest folders by placing a forward slash (/) between folder names.

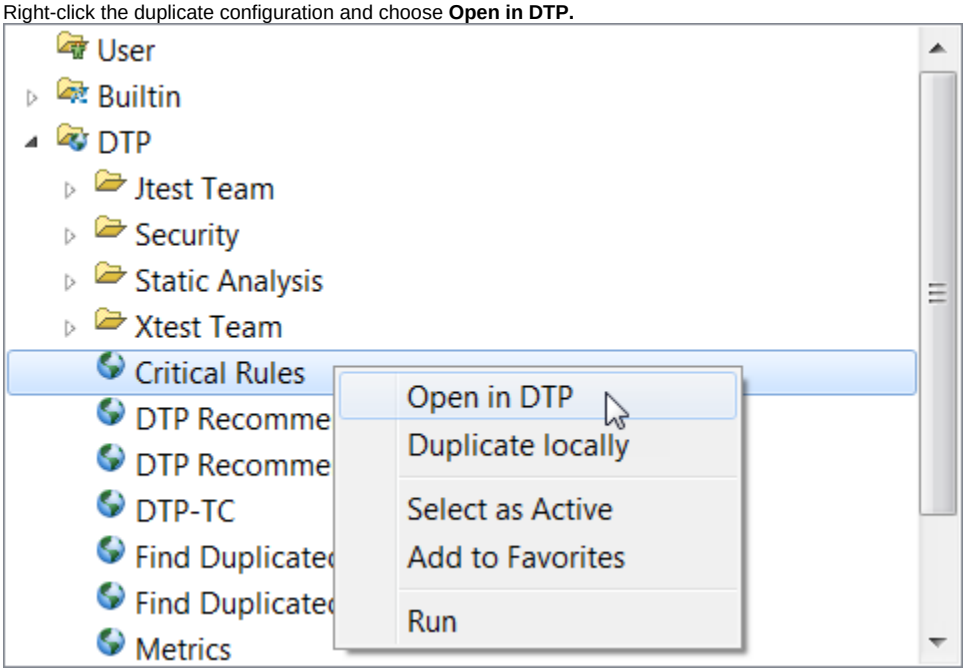
Creating and Customizing Test Configurations on DTP

1. Click **Parasoft** in the menu bar and choose **Options** (Visual Studio) or **Preferences** (Eclipse).

   Then select **Configuration**.
2. Right-click the Built-in or User test configuration you want to duplicate, then choose **Duplicate on DTP**.

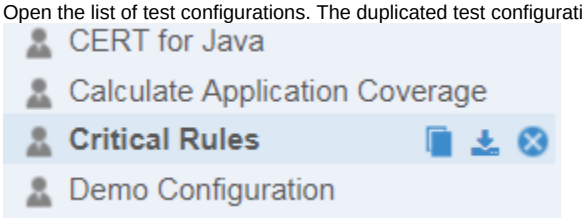


   The configuration will be added to the **DTP** directory and uploaded to the DTP server (see Connecting to DTP)
3. Right-click the duplicate configuration and choose **Open in DTP.**



   If you are not logged in DTP, the DTP login page will open in a browser. Provide your credentials to log in. The **Test Configuration** page in DTP will open.

4. Open the list of test configurations. The duplicated test configuration will be available in the configurations lists.



5. Click the duplicated test configuration to open the configuration interface. See the DTP documentation for details about how to customize test configurations on DTP.