

Creating Custom Test Configurations

In this section:

- [Creating and Customizing Test Configurations Locally](#)
- [Creating and Customizing Test Configurations on DTP](#)

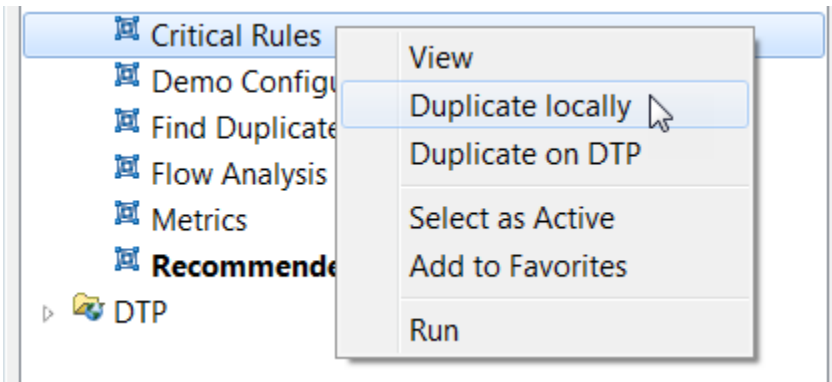
To create a custom test configuration, you need to:

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.

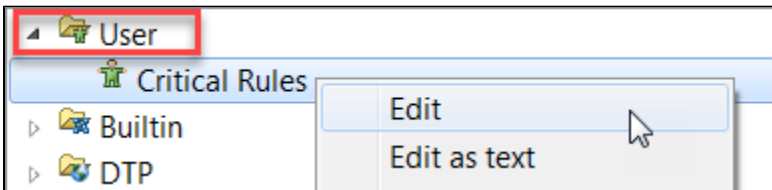
1. Click **Parasoft** in the menu bar and choose **Options** (Visual Studio) or **Preferences** (Eclipse). Then select **Configuration**.
2. Right-click the test configuration you want to duplicate, then choose **Duplicate Locally**.



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 your 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.

Critical Rules

Scope Static Analysis Metrics Unit Tests Static Analysis Settings General Settings

▶ Time filters ⓘ

▶ File path filters ⓘ

▶ File content filters ⓘ

▶ Authors filters ⓘ

▶ File size filters ⓘ

▶ Code block options ⓘ

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 from the file system of the machine running analysis.

Time filters ⓘ

Files ⓘ

- Check all files ⓘ
- Check locally-modified files ⓘ
- Check files modified within a date range ⓘ
 - date ⓘ
 - until date ⓘ
- Check files modified within last n days ⓘ Number of days
- Check files modified between the current branch and the specified branch ⓘ
 - Use default branch ⓘ
 - Use custom branch Branch name

Lines ⓘ

- Check all lines ⓘ
- Check locally modified lines ⓘ
- Check lines modified since date ⓘ
- Check lines modified within last n days ⓘ Number of days

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: <code>scope.scontrol=true</code>
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 within 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: <ul style="list-style-type: none"> • 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: <code>scope.scontrol=true</code>
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 within 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.

File path filters ⓘ

Accepted paths (wildcard) ⓘ

Rejected paths (wildcard) ⓘ

Advanced

Accepted paths (regex) ⓘ

Rejected paths (regex) ⓘ

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.

File content filters ⓘ

Exclude auto-generated files ⓘ Patterns ⓘ

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.

Authors filters ⓘ

Include only files owned by authors ⓘ

Include only lines owned by authors ⓘ

List of authors ⓘ

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.


File size filters ⓘ

Include empty files ⓘ

Exclude large files ⓘ Large file indicator ⓘ

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.

Code block options ⓘ

Include only lines in certain blocks ⓘ Starting marker ⓘ
 Ending marker ⓘ

Skip files without these markers ⓘ

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.

The screenshot shows the Parasoft Critical Rules configuration page. The 'Static Analysis' tab is selected. The 'Enable Static Analysis' checkbox is checked. The 'Enabled Rules: 143' indicator is visible, along with 'Enable 1582 rule(s)' and 'Disable 1582 rule(s)' buttons. A search bar and a category dropdown menu are present. The table below lists the rules:

Enabled	Rule ID	Severity	Rule	Category
<input checked="" type="checkbox"/>	Code Duplication Detection			
<input type="checkbox"/>	CDD.DFI	4	Avoid duplicated field initialization in constructors.	Code Duplication Detection
<input type="checkbox"/>	CDD.DUPC	3	Avoid code duplication	Code Duplication Detection
<input type="checkbox"/>	CDD.DUPI	3	Avoid duplicate import statements	Code Duplication Detection
<input type="checkbox"/>	CDD.DUPM	2	Avoid method duplication	Code Duplication Detection
<input type="checkbox"/>	CDD.DUPS	3	Avoid string literal duplication	Code Duplication Detection
<input type="checkbox"/>	CDD.DUPT	2	Avoid class duplication	Code Duplication Detection
<input checked="" type="checkbox"/>	Coding Conventions			
<input type="checkbox"/>	CODSTA.BPABCL	4	Avoid "break" and/or "continue" with labels	Bad Practice

Enabling Static Analysis

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

This close-up shows the 'Static Analysis' tab selected. The 'Enable Static Analysis' checkbox is checked and highlighted with a red box. Below it are the search rules input field and the category dropdown menu.

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.

This close-up shows the search bar and category dropdown menu highlighted with a red box. The search bar contains the text 'Search rules' and the dropdown menu is set to '-- All categories --'. Below the search bar, the table headers 'Enabled', 'Rule ID', and 'Severity' are visible.

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

Scope Static Analysis Metrics Unit Tests Static

Enable Static Analysis ⓘ

Search rules -- All categories -- Show Enabled Only

+/-	Enabled	Rule ID	Severity	
▲ Coding Conventions				
	<input checked="" type="checkbox"/>	CODSTA.OIM.OVERRIDE	1	Override 'Object.hashCode


Enabling and Disabling Rules

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

+/-	Enabled	Rule ID	Severity	Rule
▲ General				
▲ Code Duplication Detection				
	<input checked="" type="checkbox"/>	CDD.DUPI	3	Avoid duplicate import statements
	<input type="checkbox"/>	CDD.DUPM	2	Avoid method duplication
	<input type="checkbox"/>	CDD.DUPS	3	Avoid string literal duplication
	<input type="checkbox"/>	CDD.DUPT	2	Avoid class duplication
	<input type="checkbox"/>	CDD.DUPC	3	Avoid code duplication
	<input type="checkbox"/>	CDD.DFI	4	Avoid duplicated field initialization in constructors.

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

General Settings

Enabled Rules: 143  **Enable 1582 rule(s)** **Disable 1582 rule(s)**

Viewing Rule Documentation

Click on a rule to open the documentation panel.

+ / -	Enabled	Rule ID	Severity	Rule
General				
Code Duplication Detection				
<input type="checkbox"/>		CDD.DUPI	3	Avoid duplicate import statements
<input type="checkbox"/>		CDD.DUPM	2	Avoid method duplication
<input type="checkbox"/>		CDD.DUPS	3	Avoid string literal duplication
<input type="checkbox"/>		CDD.DUPT	2	Avoid class duplication
<input type="checkbox"/>		CDD.DUPC	3	Avoid code duplication
<input type="checkbox"/>		CDD.DFI	4	Avoid duplicated field initialization in constructors.
Design by Contract				
<input type="checkbox"/>		DBC.PROMPRE	3	Provide a '@pre' contract for all "protected" methods.

1 - 250 / 1096 items

Rule Documentation | Rule Parameters

Avoid duplicate import statements [CDD.DUPI-3]

DESCRIPTION

This rule looks for duplicated "import" statements. The rule will flag a violation for each import statement where the object being imported has already been imported.

SCOPE LEVEL

LINE

SINCE

v8.0

Save Cancel

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

Rule Documentation | Rule Parameters

Avoid duplicate import statements [CDD.DUPI-3]


DESCRIPTION

This rule looks for duplicated "import" statements. The rule will flag a violation for each import statement where the object being imported has already been imported.



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

General Settings

Enabled Rules: 143  Enable 1582 rule(s) Disable 1582 rule(s)

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.

Rule Documentation

Rule Parameters

Reporting of violations where variable is known to be null due to a null check

Except for the cases when the null check is performed inside a called method of the following visibility:

public

public, protected

public, protected, package-private

methods of any visibility (least aggressive, most accurate)

Methods that do not accept null as their parameters:

Enabled	Fully qualified type name (wildcard)	Method name (wildcard)	+ definitions in subclasses	Non-null parameters	
					+

Potential null returners:

Consider Java SE methods which may return null and it's hard to protect from it

Consider Java SE methods which may return null but it's not hard to protect from it

Consider Java SE collections' access methods can return null

Report unvalidated violations

Save

Cancel

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.

Scope Static Analysis Metrics Unit Tests Static Analysis Settings General Settings

Enable metrics analysis Enabled Metrics: 39 [Enable 49 metric\(s\)](#) [Disable 49 metric\(s\)](#)

Search Metrics Show Enabled Only

Enabled	Metric ID	Metric
<input checked="" type="checkbox"/>	METRIC.CLLOCRT	Comment/Logical Lines in Types
<input type="checkbox"/>	METRIC.DIF	Depth of Nested 'if' Statements
<input checked="" type="checkbox"/>	METRIC.ECC	Essential Cyclomatic Complexity
<input checked="" type="checkbox"/>	METRIC.FO	Fan Out
<input type="checkbox"/>	METRIC.HDIFM	Halstead Difficulty
<input type="checkbox"/>	METRIC.HEFM	Halstead Effort
<input type="checkbox"/>	METRIC.HICM	Halstead Intelligent Content
<input type="checkbox"/>	METRIC.HLENM	Halstead Program Length
<input type="checkbox"/>	METRIC.HLEVM	Halstead Program Level
<input checked="" type="checkbox"/>	METRIC.HNOBM	Halstead Number of Bugs

1 50 items per page 1 - 49 / 49 items

Metric Documentation Metric Parameters

Report static analysis violation when outside of acceptable ranges

Acceptable metric ranges

greater than

lower than

greater than and lower than

lower than or greater than

[Save](#) [Cancel](#)

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.

Scope Static Analysis Metrics Unit Tests Static Analysis Settings General Settings

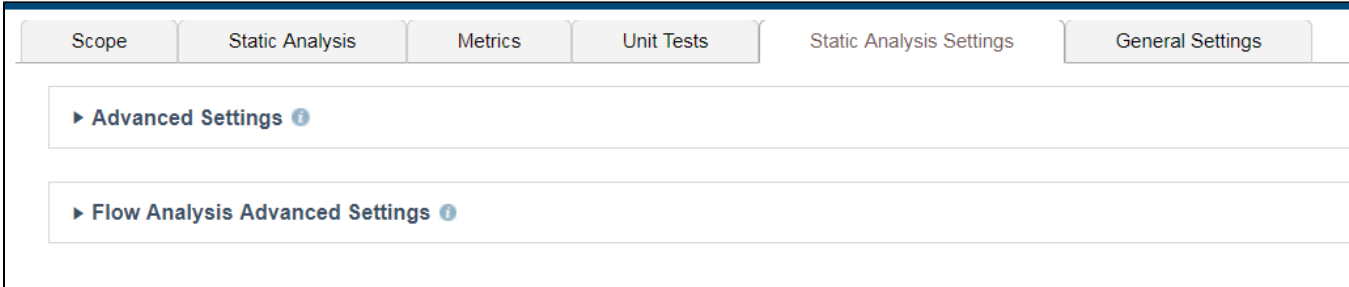
Report Unit Tests results ⓘ

Report Coverage results ⓘ

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

Static Analysis Settings Tab

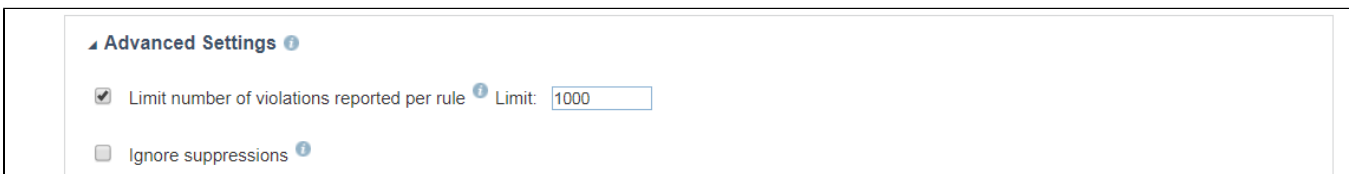
Click the **Static Settings Analysis** tab allows you to configure your static analysis and flow-based analysis. Click **Save** to preserve any changes you make on this tab.



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.



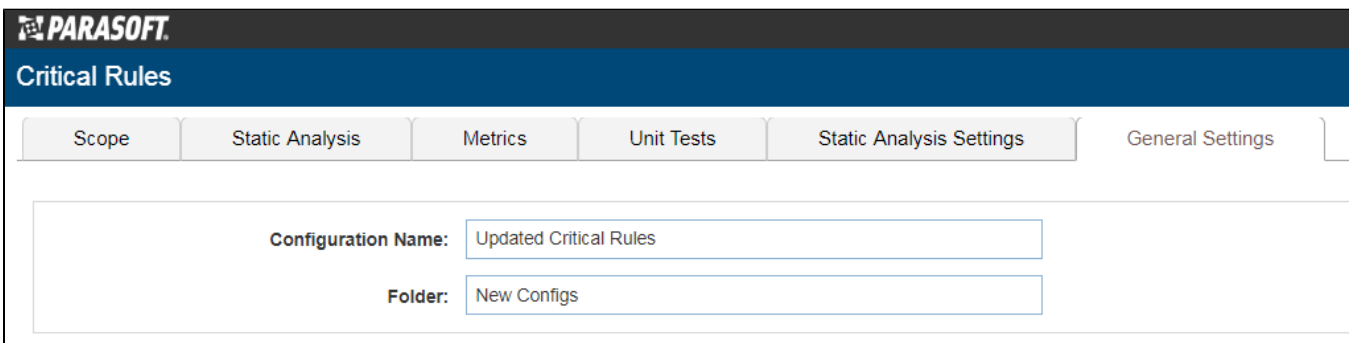
Flow Analysis Advanced Settings

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

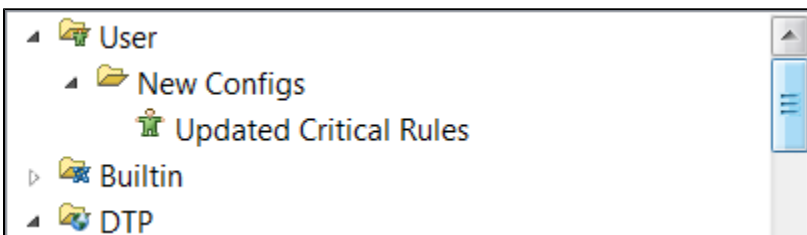
See [Configuring Flow Analysis](#) for details.

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.



i 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.

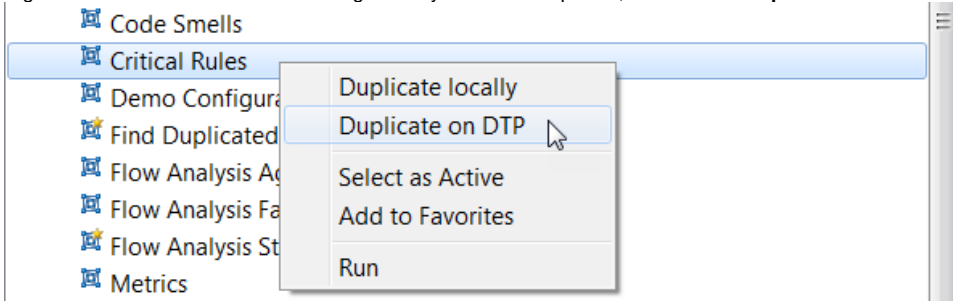


Creating and Customizing Test Configurations on DTP

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

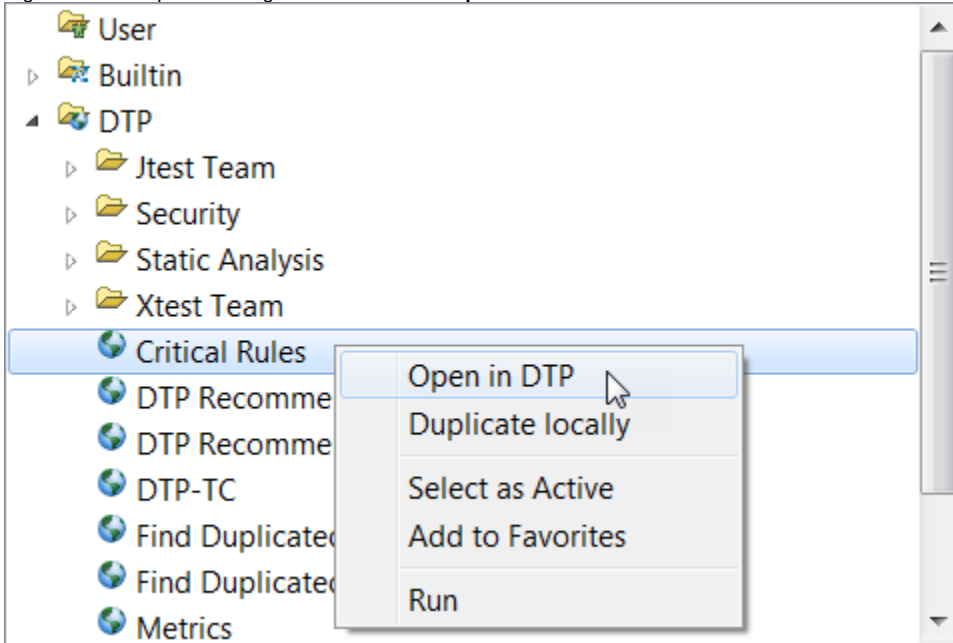
Then select **Configuration**.

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.

The screenshot shows a web-based configuration interface for a test configuration named "Critical Rules (1)". The interface has a top navigation bar with tabs for "Scope", "Static Analysis", "Metrics", "Unit Tests", "Static Analysis Settings", and "General Settings". The "Static Analysis Settings" tab is currently active. The configuration details are as follows:

- Configuration Name:** Critical Rules (1)
- Folder:** (empty text input field)
- Access:** Private (indicated by a blue button with a checkmark)
- Tags:** Add a tag (text input field)
- Configuration URL:** ".dtp://Critical Rules (1)"
- Last Modified:** 2019-04-19 6:31:09 AM
- Author:** (empty text input field)
- Approved by:** (empty text input field)
- Description:** (empty text area)

At the bottom of the configuration form, there are two buttons: "Save" and "Cancel". The footer of the interface reads "Powered by Parasoft DTP. Copyright © 1996-2019."