DTP 5.4.0

DTP

The following DTP features, fixes, and updates were added in this release:

Development Testing Platform is Now Officially DTP

We've retired the product name "Development Testing Platform" in favor of the shorter and more memorable "DTP."

Updated LDAP Integration

We've simplified the configuration interface for connecting DTP to your user directories. The streamlined interface is not only easier to configure, it also supports syncing multiple LDAP servers. See Configuring LDAP for additional information.

Upgrade Notes

If you are upgrading to 5.4 from a previously installed version of DTP, note that the values that define filter attributes in the PSTSecConfig.xml configuration file will be migrated to a new JSON file for compatibility with the 5.4 LDAP integration implementation. The experience should be seamless, but we recommend verifying that your user and group import settings function as expected. The following functionalities related to user directory configuration have been removed in DTP 5.4:

- **Accept JNDI environment properties**. This allowed users to specify a different authentication scheme than basic username/password pairs.
- **Ignore Communication Errors**. This was enabled DTP to ignore referral-related errors from Active Directory servers.
- **Built-in automatic import**. This feature was a built-in cron job scheduler.
- Default attributes for Active Directory when creating a new configuration.

In previous versions, importing user attribute changes made on the LDAP server required new DTP directories. In 5.4, user attributes are updated in the existing DTP directory when importing users from the LDAP server.

Suppress Violations from the Violations Explorer

You need the ability to control the potentially large flow of static analysis violations reported throughout the development lifecycle. Manually managing static analysis results is labor-intensive, inefficient, and unsustainable because it may involve spending resources on less important issues, while missing issues that have a greater impact to the business.
You can now mark violations in the Violations Explorer that are suppressed in the next code analysis run and persist in developers' IDEs. See Violations Explorer.

Upgrade Notes

The recommended workflow for simulating suppressions in previous versions of DTP was to mark violations with the Do Not Show priority. This priority hides violations in DTP interfaces, but does not programmatically suppress violations. If you were using this approach as a means of suppressing violations, you can convert the hidden violations into true suppressions:

1. Duplicate your filter and rename the copy (e.g., "My Filter with do not show").
2. Edit the duplicate filter and enable the **Do not show** option in the Included Priorities section (see Setting Priorities in Filters).
3. Return to your dashboard and add a violations widget configured to use the new filter (see Static Analysis Widgets).
4. Click on the widget to drill down to the Violations Explorer and search for violations prioritized as Do Not Show (see Searching for Violations).
5. Select all violations in the search results table and enable the **Suppress the selected violations in subsequent analysis runs** option in the Prioritization tab. Include your rationale in the text area.
6. Click **Apply**. During the next static analysis run, the analyzer will mark these violations as suppressions. This will be reflected in XML/HTML reports generated by the analyzer as well as in DTP widgets, reports, and Violations Explorer.
7. After the next static analysis run, enable the **Do not show** option for the original filter. You will now be able to see all violations and all suppressions, even suppressions that have Do Not Show priority.
8. (Optional) Delete the duplicate filter.

End of life for Do Not Show priority

The Do Not Show priority will no longer be treated as suppressions in C/C++test, dotTEST, and Jtest 10.4.0 and later. The Do Not Show priority has also been deprecated and will no longer be included in future versions of DTP.

If you are upgrading your Parasoft code analysis tools from 9.x or older to 10.4.0, you will need to migrate suppression data to the current implementation. Contact Parasoft to access our dedicated tool, which migrates suppression data stored in Team Server (TCM) to DTP. See Migrating Team Server Suppression Data to DTP for details.

All Built-in Reporting Interfaces Use the Latest Static Analysis REST API

The static analysis REST API is a key component of the analytics DTP delivers. In this release, we've updated all built-in reports, widgets, and explorers to use the latest version of the API, which enables you to view build-to-build trend data in all interfaces. See REST API.

Upgrade Notes

The /v1/staticAnalysisViolations API is deprecated in this release. Use v1.2 or newer.

Build Retention Configuration

You can configure the amount of unit testing, coverage, resource coverage, and metrics data that DTP stores. Amounts of data are specified in number of builds, e.g., you can configure DTP to store 10 builds worth of metrics data. See Configuring Data Retention Settings for details.

Upgrade Notes

The DTP Database Updater 224 process may take several minutes to complete (7 minutes for 1 million rows). The actual time depends on the memory allocated to the database, as well as the number of rows in the UNBRANCHED_CANONICAL_RESOURCES table.

The DTP Database Updater 227 process may take several minutes to complete. The actual time depends on the memory allocated to the database, as well as the number of rows in the COVERAGE table. A COVERAGE table with 50 million rows requires approximately 1.5 hours.

Widget Updates

The following widgets were added in this release:

- Resource Groups - Top 10 Tree Map: This widget shows up to 10 resource groups with the highest values for the selected metric.
- Resource Groups - Top 5 Table: This widget shows the five resource groups with the highest aggregate values for the selected metric.
- Quality Status: This widget shows the overall code quality status for the target build.
- Portfolio - Quality Status: This widget shows the overall quality status for all projects you're assigned to.
- Tests - Changed - Status: This widget shows how many test cases changed status from the Baseline build to the Target build.

In addition, coverage-related widgets were moved from the Test Widgets category to a dedicated Coverage Widgets category. See Coverage Widgets.

Updates to the Violations Explorer

We've improved the interface for suppressing violations, as well as merged the timeline tab into the violation history tab in the Violations Explorer actions panel. See Violations Explorer for details.

Updates to the Coverage Explorer

We've updated the underlying API endpoints for the Coverage Explorer, as a result, we were able make the following updates:

- Search for files using Ant patterns
- Browse method-level nodes
- Specify coverage thresholds in the search results
- General UI improvements

Metrics Dashboard Template

DTP now ships with a built-in metrics dashboard template to help you quickly start reviewing metrics data. See Built-in Dashboard Templates.

Combined DTP and Enterprise Pack Installer

The DTP installer now includes DTP Enterprise Pack, which simplifies the usability and deployment of Parasoft's advanced analytics and reporting architecture. Review the Installation Guide for installation and upgrade information.

Additional DTP Updates

- DTP no longer ships with built-in test configurations. You can create test configurations or upload test configurations shipped with your code analysis and test execution tool using the DTP test configurations interface.
- Improved ability to correlate same violations in different branches
- Improved ability to correlate same file, regardless of source control settings
- Improved Data Collector performance related to processing static analysis and coverage reports
- Added the ability to delete builds of any age.
- Added the ability to customize HTML/PDF report from the Build Audit Report
- The following built-in custom processors were removed:
    - qualityDebt
    - riskAnalysis
    - tasksCreation
    - violationsGroupTrend
    - violationsDiff
    - violationsSunburst
- New coverage by resource group endpoints have been added to the API.
- Project Center has been deprecated.
- We created a patch to help Concerto users with Oracle databases update to DTP. Contact your Parasoft representative for additional information.
- The default dashboard has been updated. See Built-in Dashboard Templates.
- Data Collector has been updated to verify project membership for users publishing code and analysis data to DTP. See Adding Teams to Projects.
- The OWASP Top 10 dashboard template and OWASP Top 10 widget have been updated for the OWASP Top 10 2017 guideline. These assets have also been removed from the DTP installer and are available in the Security Compliance Pack for DTP 5.4.1 (contact your Parasoft representative). See Built-in Dashboard Templates and Compliance Widgets for additional information.
- DTP now ships with Java 8 update 172.
- DTP now ships with Apache Tomcat 8.5.30. See DTP Server Settings for relevant information.
- General user interface improvements.

DTP Enterprise Pack

The following DTP Enterprise Pack features, fixes, and updates were added in this release:

CERT C Compliance

The CERT C Compliance extension is a suite of assets that enable you readily monitor compliance with CERT C guidelines, as well as demonstrate compliance for auditing purposes. The CERT C Compliance Pack ships with the Security Compliance Pack for DTP 5.4.1, which is available as a separate download (contact your Parasoft representative).

See for details CERT C Compliance for additional information.

Updated Violations Event Flow

The Violations Event flow is a common utility used to build extensions with Extension Designer. The flow leverages the DTP static analysis REST API, which was updated in DTP 5.4.0. This change enables you to view build-to-build trend data instead of the time-based method of showing trend data in previous releases.

As a result of the update, any custom artifacts you may have built using the Violation Events flow or that leverage the static analysis API directly will need to be updated to use the new version. New versions of the following pre-built artifacts are now available:

- Policy Center Practice - Static Analysis
- Policy Center Practice - Defects for JIRA
- Static Analysis Violation Reporter for Atlassian JIRA

See Using the Built-in Common Flows for additional information.

Updated Test Stability Report

The Test Stability Report has been updated. The artifact ships with a new statistics widget and includes additional UI improvments.

Additional DTP Enterprise Pack Updates

- The Security Impact profile was removed from the Key Performance Indicator extension. The profile ships with the CWE Compliance.

Resolved Issues

The following PRs and FRs were addressed in this release:

ID	Description

DTP-5020	unable to start data collector backup, Data Collector Backup Privileges Error
DTP-5295	Improve performance of parsing static analysis reports
DTP-5396	Improve performance of deleting builds - modify /v1/violations API
DTP-5816	Group Synchronization does not sync the emails field