Security Compliance Pack

The Parasoft Security Compliance Pack is a set of artifacts for your DTP infrastructure that help you implement your software security compliance initiatives. It includes configurations that re-orient static analysis data to report violations according to security compliance standards. It also includes widgets for viewing your security compliance status and custom compliance DTP dashboards for monitoring the progress toward your overall security compliance goals. The Security Compliance Pack supports the following standards by default:

- CERT C
- CERT C++
- CWE List Version 4.0
- CWE Top 25
- CWE Top 25 + On the Cusp
- UL 2900
- OWASP Top 10
- PCI DSS 3.2

Contact your Parasoft representative for download and licensing information.

Requirements

- DTP and DTP Enterprise Pack 2020.1 or later with Enterprise license.
- A Parasoft code analysis tool with the Flow Analysis license feature enabled. See the documentation for individual artifacts for specific requirements.

Terminology

Parasoft's security compliance solution includes the assets installed and deployed to DTP using DTP Enterprise Pack, as well as the collection of test configurations executed in Parasoft tools that check code against specific standards. The term Security Compliance Pack refers to the complete security compliance solution, but in some contexts we mean the set of test configurations in the tool UI or the collection of DTP assets.

Compatibility

New versions of DTP compliance packs are available each new version DTP and DTP Enterprise Pack. Newer versions usually include updated test configurations, widgets, reports, and other enhancements. We strongly recommend upgrading your code analysis tool, DTP, and the compliance pack to the latest version to ensure full compatibility.

The following table describes the optimized deployment:

Compliance Pack	DTP / DTP Enterprise Pack	Tool	Supported test configurations
2020.1	2020.1	2020.1	• CERT C • CERT C++ • CWE List Version 4.0 • CWE Top 25 + On the Cusp • CWE Top 25 • OWASP Top 10 • PCI DSS 3.2 • UL 2900
5.4.3	5.4.3	10.4.3.	• CERT C • CERT C++ • CWE List Version 3.4 • CWE Top 25 + On the Cusp • CWE Top 25 • OWASP Top 10 • PCI DSS 3.2 • UL 2900
5.4.2	5.4.2	10.4.2	• CERT C • CERT C++ • CWE List Version 3.2 • CWE Top 25 + On the Cusp • CWE Top 25 • OWASP Top 10

5.4.1	5.4.1	10.4.1	• CERT C • CERT C++ • CWE List Version 3.1 • CWE Top 25 + On the Cusp • CWE Top 25 • OWASP Top 10
5.4.0	5.4.0	10.4.0	• CERT C • CWE List Version 2.11 • CWE Top 25 + On the Cusp • CWE Top 25 • OWASP Top 10

Parasoft Security Compliance Pack Artifacts

The Security Compliance Pack includes the following artifacts:

- CERT C Compliance
- CERT C++ Compliance
- CWE Compliance
- Key Performance Indicator
- OWASP Compliance
- PCI DSS Compliance

See the documentation for these artifacts for usage details.

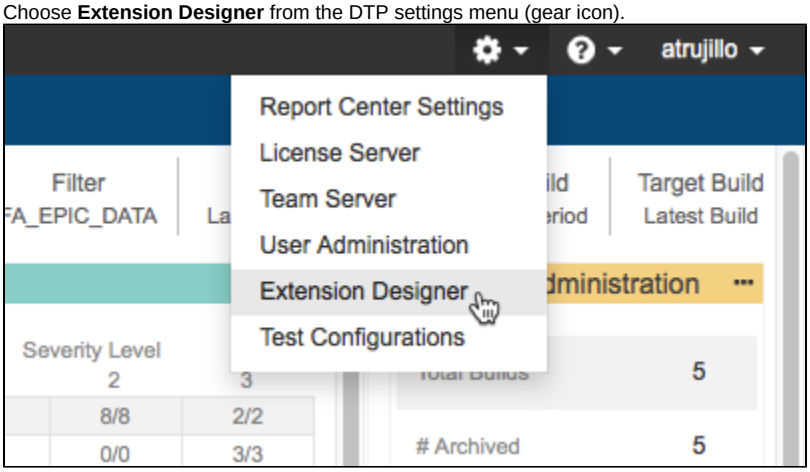
Process Overview

1. Download and install the Security Compliance Pack (security-compliance-<version>.zip) into your DTP environment. Installing the package adds several files that configure DTP to report code analysis violations according the supported security standards.
2. Use DTP Extension Designer to deploy the compliance artifact(s) you want to analyze code against.
3. Connect an instance of your tool to DTP and analyze the project using a Security Compliance Pack test configuration. Test configurations ship with the Parasoft tools and with the Security Compliance Pack. The configurations are automatically uploaded to your DTP test configurations when you deploy the compliance pack. You can run code analysis using either instance of the test configuration. See the documentation for your tool for static analysis execution instructions.
4. Add the security compliance dashboard(s) and widgets to DTP and configure them to view the data according to your security standard.
5. Interact with the widgets and reports to identify code that needs to be fixed, as well as print out the reports for auditing purposes.

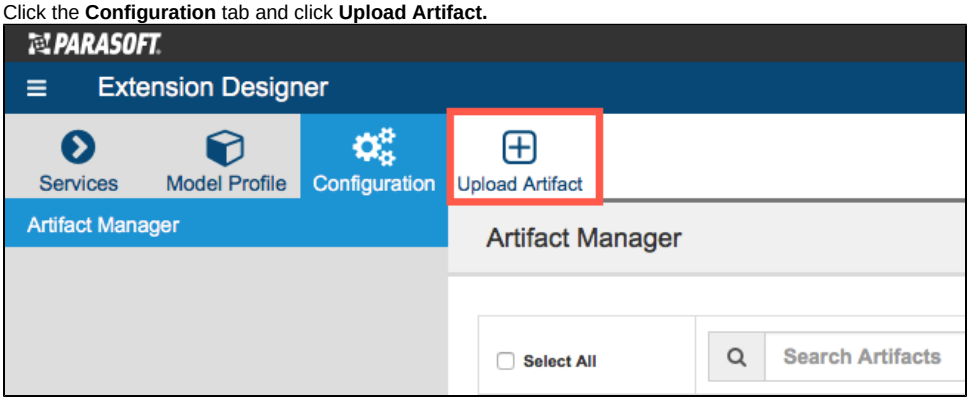
Installation

Parasoft provides the compliance pack as a compressed folder (.zip). Extension Designer will expand the .zip file and move the contents to the appropriate location when uploaded. The following process is also described in the Downloading and Installing Artifacts section:

1. Choose **Extension Designer** from the DTP settings menu (gear icon).



2. Click the **Configuration** tab and click **Upload Artifact.**



3. Browse for the .zip file when prompted and click **Install**.

After the compliance pack files have been installed, the next step is to deploy the artifacts for the compliance standard(s) you want to measure your code against. See the following documentation for instructions:

- CERT C Compliance
- CERT C++ Compliance
- CWE Compliance
- Key Performance Indicator
- OWASP Compliance
- PCI DSS Compliance

Upgrading

Although Parasoft extensions are designed to be forward compatible, they are not guaranteed to work in newer versions of DTP or Extension Designer. We strongly recommend installing the latest version of the artifact and removing the previous version.

1. Make a backup of the model/profiles associated with your security compliance artifacts. See Working with Model Profiles for instructions on how to export copies of your models and profiles.
2. Delete the existing models/profiles and install the newer artifact as described in Installation.
3. Un-deploy older artifact from Extension Designer by deleting its nodes and clicking **Deploy**.
4. Deploy the newer version.
5. New models and profiles are installed as part of the upgrade. Refer to your backed up models/profiles and apply any modifications you may have implemented in the previous version to the newly installed models/profiles.