AI VERIFY

AI GOVERNANCE TESTING FRAMEWORK AND TOOLKIT

Quick Start Guide

VERSION 0.3.0-BETA

Installation

1 System Requirements

- ☐ OS > Ubuntu 18.04 or > Windows 10 (64-bit)
- ☐ CPU* > 4 cores
- ☐ Memory > 16 GB
- ☐ Free Space > 6 GB

* Mac computers with Apple silicon M1 and M2 chips are currently not supported

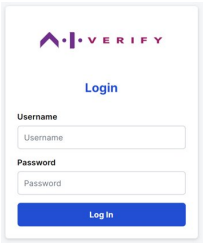
2 Run Docker Image

1. Install Docker on Windows or Linux
2. Unzip the ai-verify-latest-beta.zip file & copy the folder location
3. Open a terminal & change directory to the folder location (e.g. C:\Users\John\Documents\)
   > cd C:\Users\John\Documents\ai-verify-latest-beta
4. > Linux
   sudo docker load < ai-verify-image-v0.3.0-beta.tar
   > Windows
   docker load -i .\ai-verify-image-v0.3.0-beta.tar
5. > docker run -d -p 4200:4200 --sysctl net.ipv4.tcp_fin_timeout=30 --sysctl net.ipv4.ip_local_port_range="15000 65000" --sysctl net.ipv4.tcp_tw_reuse=1 ai-verify-image

Key this in as a single line of command

3 Web Portal Login

1. Open https://localhost:4200/



2. Username: **test** | Password: **test**

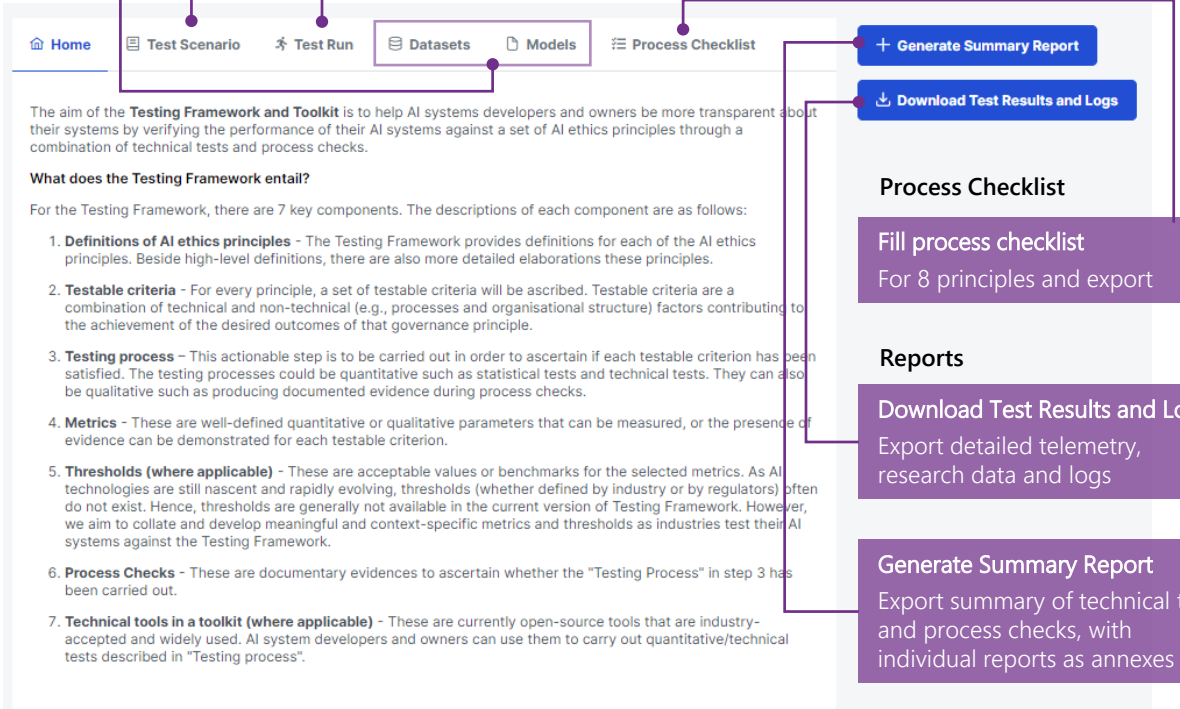
Overview

Technical Tests

Upload datasets & model
Used for fairness, robustness & explainability tests

Create test scenario
Add the test cases for the principle(s)

Run test scenario
Execute the test scenario and view/export results



Process Checklist

Fill process checklist
For 8 principles and export

Reports

Download Test Results and Logs
Export detailed telemetry, research data and logs

Generate Summary Report
Export summary of technical tests and process checks, with individual reports as annexes

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Technical Tests Principles: Fairness (F), Robustness (R), and Explainability (E)

4 Create Test Scenario

1 Click the Test Scenario tab
2 Click +
3 Select mode of accessing the AI model based on supported models and/or configurations

Mode 1: Upload AI Model (Supported Models)

Binary Classification (F, R, E)

Scikit-Learn
- Logistic Regression Classifier
- SVM Classifier
- Decision Tree Classifier
- Gradient Boosting Classifier
- Random Forest Classifier
- AdaBoost Classifier
- Bagging Classifier
- Linear Perceptron Classifier

XGBoost
- XGBClassifier
- XGBBooster

LightGBM
- LGBMClassifier

Binary Classification (F, E)

Tensorflow
- Keras Sequential with binary classification as loss

Regression (F, E)

Scikit-Learn
- Linear Regressor
- Gradient Boosting Regressor

XGBoost
- XGBRegressor

Mode 2: API-based Testing (Experimental)

Binary Classification (F, R, E)
- Any algorithm type

Regression (F, E)
- Any algorithm type

Supported API Configurations

HTTP Method
- GET
- POST

Request Body Content Type
- Multipart/form-data
- Application/x-www-form-urlencoded
- None

Authentication
- No Auth
- Bearer Token
- Basic Auth

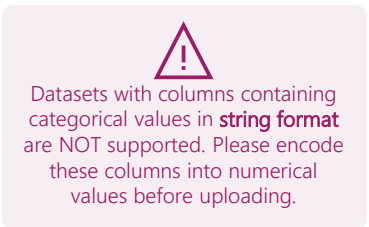
Response Content Type
- Text/plain
- Application/json

**Prediction output should be an integer*

4 Prepare the relevant input files for the principles to be tested

Input	F	R	E	Contains	Library Version	Serialized by
Background Dataset			✓	Features, Ground Truth	Pandas 1.3.5	Pickle or Joblib
Test Dataset	✓	✓	✓			
AI Model (if using Mode 1)	✓	✓	✓	NA	NA	

5 Enter details for General and click Next
6 Upload Test Data and select test dataset file
7 Choose **Ground Truth** column name and click Next
8 Mode 1: Select AI Model file, select **Model Type** and **Algorithm Type**, and click Next
Mode 2: Configure model server parameters for API Config and click Next
Review the configurations and click Next
9 Click + Create New Test to create Tests cases and Save



5 Create Test Cases

1 Select **Fairness/Robustness/Explainability** as Test Principle and click Next
2 Enter Test Description and click Next
3 Enter Arguments and click Next
> **Fairness -** If model is binary classification type, go to →
> **Robustness –** Choose **data type**
> **Global Explainability –** Choose **global** for **Explainability Type**
> **Local Explainability –** Choose **local** for **Explainability Type**
4 Review information and click Add Test

Fairness Tree
- Enter definitions to contextualise the fairness tree to the use case and click ›
- Check generated fairness tree for coherence and edit the inputs provided in 3 and a if required
- **1st level** Choose up to 3 desired outcomes by clicking on the text and document reasoning
- Rank the selected desired outcomes by dragging ☰ if > 1 option is selected and click ›
- **2nd & 3rd level** Choose 1 option, document reasoning and click ›
- **End** Review inputs, click ⎘ and Next

6 Run Test Scenario

1. Click the Test Scenario tab
2. At the scenario row, click
3. Skip execution of a test case (optional) by checking Skip
4. Click Run Tests
5. Status is found in Test Run tab

7 View Results in Portal

1. Click the Test Run tab
2. At the scenario row, click
3. Results of the technical tests appear with details in the tabs

8 Export Results as PDF

1. Click the Test Run tab
2. At the scenario row, click
3. Configure the PDF in the pop-up that appears
4. Click to start export

Process Checklist

Principles: All

9 Create Checklist

1. Click the Process Checklist tab
2. Click
3. Enter the **Name** of the process checklist
4. Toggle between the tabs for the 8 principles
5. For each testable criteria and process, select **Completed** status, enter **Elaboration** and **Industry Feedback** for it.
6. Click Save regularly, as there is no auto-save function for the checklist

10 Export Checklist as PDF

1. Click Export PDF within the 'Create/ Update Process Checklist' page, or
   Click under the Process Checklist tab to export to PDF
2. Configure the PDF in the pop-up that appears
3. Under report type, select ***Internal + Feedback***
4. Click to start export

Summary Report

11 Export Report as PDF

1. Click + Generate Summary Report
2. Choose the correct scenario(s) when Selecting Technical Tests on the left, by clicking and for the test scenario(s). The chosen demo scenario will appear on the right under Selected Technical Tests
3. Click Next
4. Select Process Checklist & click Next
5. Click Export PDF to generate report

Test Results & Logs

12 Export Test Results and Logs

1. Click Download Test Results and Logs
2. Set password
3. Click Download and a .zip file will be exported

For Windows 10 users, the built-in extractor in File Explorer will not be able to extract the files. Please download and use other file extractors (e.g., 7-zip)

After completing the technical tests and process checklist, kindly send the *Process Checklist Report (Internal + Feedback)*, *Summary Report* as well as *Test Report and Logs* to IMDA/PDPC