

Installation (via Dockerfile) To build and run from source code, check out the User Manual.

1 Requirements

System

- OS Ubuntu 22.04
- CPU > 4 cores
- Memory > 16GB
- Free Space > 10GB

Software

- Docker

2 Build

- 1 Launch Docker Desktop
- 2 Download & unzip `setup-aiverify.zip`
- 3 Open a terminal and change directory.
`cd aiverify-user`
- 4 Execute the following command.

```
bash docker-build.sh
```

In Docker Desktop, open 'Images' tab.
You should see `ai-verify` running.

3 Run

- 1 Run the start script.

```
bash docker-start.sh
```

- 2 Open <http://localhost:3000>

To start with a clean state,

```
bash docker-start.sh --reset
```



Upon initial start-up of the toolkit, pages might take some time to load.

Prepare Input Files

The AI Verify Toolkit supports technical tests for these models & datasets:

Binary Classification

Scikit-Learn 1.2.2

- Logistic Regression
- Decision Tree
- Gradient Boosting Classifier
- Random Forest
- Bagging Classifier
- Perceptron

Tensorflow 2.12.0

- Keras Sequential

XGBoost 1.7.5

- XGB Classifier
- XGB Booster

LightGBM 3.3.5

- LGBM Classifier

Multiclass Classification

Scikit-Learn 1.2.2

- Logistic Regression
- Decision Tree
- Gradient Boosting Classifier
- Random Forest
- Bagging Classifier
- Perceptron

Tensorflow 2.12.0

- Keras Sequential

XGBoost 1.7.5

- XGB Classifier

Regression

Scikit-Learn 1.2.2

- Linear Regression
- Extra Tree Regressor
- Gradient Boosting Regressor
- Random Forest Regression

Tensorflow 2.12.0

- Keras Sequential

XGBoost 1.7.5

- XGB Regressor

Dataset Formats Supported

Tabular: Pandas, Delimiter-separated Values (comma, tab, semicolon, pipe, space, colon)
Image: .jpeg, .jpg, .png

You will need the following files:

AI Model or Pipeline

The prediction model to be tested.
You can include any data pre-processing as part of a pipeline. (only Scikit-Learn pipelines are supported)

Testing Dataset

Any dataset to be used for testing

Ground Truth Dataset*

A dataset that contains the ground truth.
For image datasets, this is the annotated ground truth file and should contain the image file names and ground truth.

Background Dataset*

A dataset that is representative of the dataset's population.

**The Testing Dataset can be used if it fulfils the requirements.*

All input files should be <4GB and **serialized*** by pickle or joblib.
**except for image datasets and Tensorflow models*

1 Upload Required Datasets

- 1 From the Home Page, click on 'Models & Data'
- 2 Click on 'New Dataset +'
- 3 Upload the **Testing, Ground Truth, and Background Datasets.**
- 4 Click on
- 5 Once validation is completed, click on

2 Upload AI Model to be Tested

- 1 From the Home Page, click on 'Models & Data'
- 2 Click on 'New AI Model +'
- 3 Select AI Model OR Pipeline and click
- 4 Upload the **AI Model** to be tested.
- 5 Indicate its **Model Type.**
- 6 Click on
- 7 Once model validation is completed, click on
- 8 Provide a brief description of your model.
- 9 Click
- 10 Click on

Using the AI Verify Report Template

1 Create New Project

- 1 Click 'Create New Project'.
- 2 Provide the general information.
- 3 Click **Next >** to proceed.

2 Select Report Template

- 1 Select '**AI Verify Summary Report Template for Classification Models**'.
- 2 Click **Next >** to proceed.

3 Design the Report

- 1 Click
- 2 Click on **X** to remove modelName.
- 3 Enter 'modelName' as the **Name** and the descriptive name of the AI model as the **Value**.
- 4 Click on **+**
- 5 Click on **X** to remove modelPurpose.
- 6 Enter 'modelPurpose' as the **Name** and a short description of the AI model as the **Value**.
- 7 Click on **+**
- 8 Click on the cover page widget.
- 9 Click on
- 10 Select 'modelName' as the variable for **ReportSubtitle1**.
- 11 Select 'company' as the variable for **ReportSubtitle2**.
- 12 Click **Next >** to proceed.

4 Select Datasets

Testing Dataset

- 1 Click on
- 2 Click on the testing dataset to be used, then

Ground Truth Dataset

- 3 Click on
- 4 Click on the ground truth dataset to be used, then
- 5 Click on the dropdown to select the ground truth column.

5 Select AI Model

- 1 Click on
- 2 Click on the AI model to be tested, then

6 Provide Test Arguments

Fairness Metrics Toolbox for Classification

- 1 Click on
- 2 Provide the test arguments:

Sensitive Feature Names

Column name of the sensitive feature in the testing dataset.
Click + to add more than one.

- 3 Click

Robustness Toolbox

- 4 Click on
- 5 Provide the test arguments:

Annotated Ground Truth Path

Path to the ground truth dataset.
For Image: Path to the annotated ground truth file.

Name of column containing image file names

Column name in the annotated ground truth file for image datasets that contains the image file names.

- 6 Click

SHAP Toolbox

- 7 Click on
- 8 Provide the test arguments.

Type of Explainability

Type of explainability test to be run.

Path of the Background

Path to the background dataset to be used to create permutations.

Size of the Background*

The number of data points from the background dataset to be sampled.

Size of the Test Dataset*

The number of data points from the test dataset to be sampled.

**Enter 0 to skip sampling and use the entire dataset.*

- 9 Click

7 Complete Process Checklists

- 1 For the 11 process checklists,
- 2 Click on
- 3 Complete each process check by indicating its completion status.

Yes No Not Applicable

- 4 Provide the relevant **elaboration**.
- 5 At the end of each checklist, provide a **summary justification**.
- 6 Click on once checks are complete.

8 Select Fairness Metrics using Fairness Tree

- 1 Click on to open the Tree.
- 2 Provide the following definitions:

Sensitive Feature Name(s)

The sensitive feature(s) previously selected in [Step 6](#), separated by commas.

Favourable Allocated Resource / Opportunity

Column name in the annotated ground truth file for image datasets that contains the image file names.

Qualified Group

Name of the group that is supposed to receive the resource / opportunity.

Unqualified Group

Name of the group that is NOT supposed to receive the resource / opportunity.

- 3 Click once all fields are filled.
- 4 Select the desired outcomes.
- 5 For each desired outcome selected, document the reasons.
- 6 Click once completed.
- 7 Select the relevant options and document the reasons.
- 8 Click

9 Run Test & Generate Report

- 1 Once verified that all test arguments and process checks are completed, click on **Next >**
- 2 Click
- 3 Once the tests completed running, view PDF report generated by clicking on