

**Kofax SmartHub Connector**

**Document Forensics with KTA**

March 2021  
Version 1.0

Table of Contents

[What is Kofax Forgery Detection? 2](#_Toc67394625)

[Why Kofax Smart Hub? 3](#_Toc67394626)

[How do I download the Forgery Detection project from SmartHub? 3](#_Toc67394627)

[How do I Know if the document is trusted? 3](#_Toc67394628)

[Architecture of the connector 4](#_Toc67394629)

[KTA import Settings 4](#_Toc67394630)

[Frequently Asked Questions? 5](#_Toc67394631)

What is Kofax Forgery Detection?

Forgery Detection system protects business processes and automated workflows from forgery-based frauds. The solution inspects financial documents, bank statements, and other documents submitted to our customers for signs of manipulation and raises an alert when a modification, file corruption, inconsistency with past behavior, or other anomaly is found by the AI-based system.

The KTA connector built with Resistant AI provides straight-through processing of documents and images via the Resistant REST APIs.

Why Kofax Smart Hub?

Kofax SmartHub is a digital showcase of assets connecting customers with pre-built, integrated components and solutions to extend their digital workforce. The Forgery Detection solution will be easily available on SmartHub, built on top of Kofax’s Intelligent Automation platform. It accelerates customer automation journeys and reduces the need for custom development work. SmartHub also allows partners to expose their value-added solution to new prospects and customers.

How do I download the Forgery Detection project from SmartHub?

The solution is available at <https://smarthub.kofax.com/> and downloadable from [Github](https://github.com/Syed-Ahmed-Kofax/Document_Forensics_KTA_Resistant). It comes with a detailed readme file which describes how to set up the solution in KTA.

How do I Know if the document is trusted?

The Resistant AI system receives documents or images via a secure REST API, via email or file placed in their drives. It processes the files and returns an estimate that categorizes the document into one of the 4 levels of trust:

Trusted (the best):

Trusted files contain significant evidence that they are authentic (issued by a known and trusted organization) and unmodified since their issuance. Such files are safe for fully automated processing. To be rated as trusted, the files typically need to come from a known issuer through a fully digital process. Electronic signature is helpful, but neither necessary nor sufficient.

Normal:

Files don't show any sign of integrity tampering, but their origin and authenticity can not be ascertained based on the available evidence.

Warning:

The files with this verdict show evidence of modifications or tampering, but the intent of the tampering does not unambiguously indicate a fraudulent intent. This verdict is typical for detections on unstructured or unknown documents, scanned documents or lower-quality documents. The low-quality documents that are blurry, out-of-focus or show flash reflection can be highlighted with Warning as well.

High-Risk (the worst):

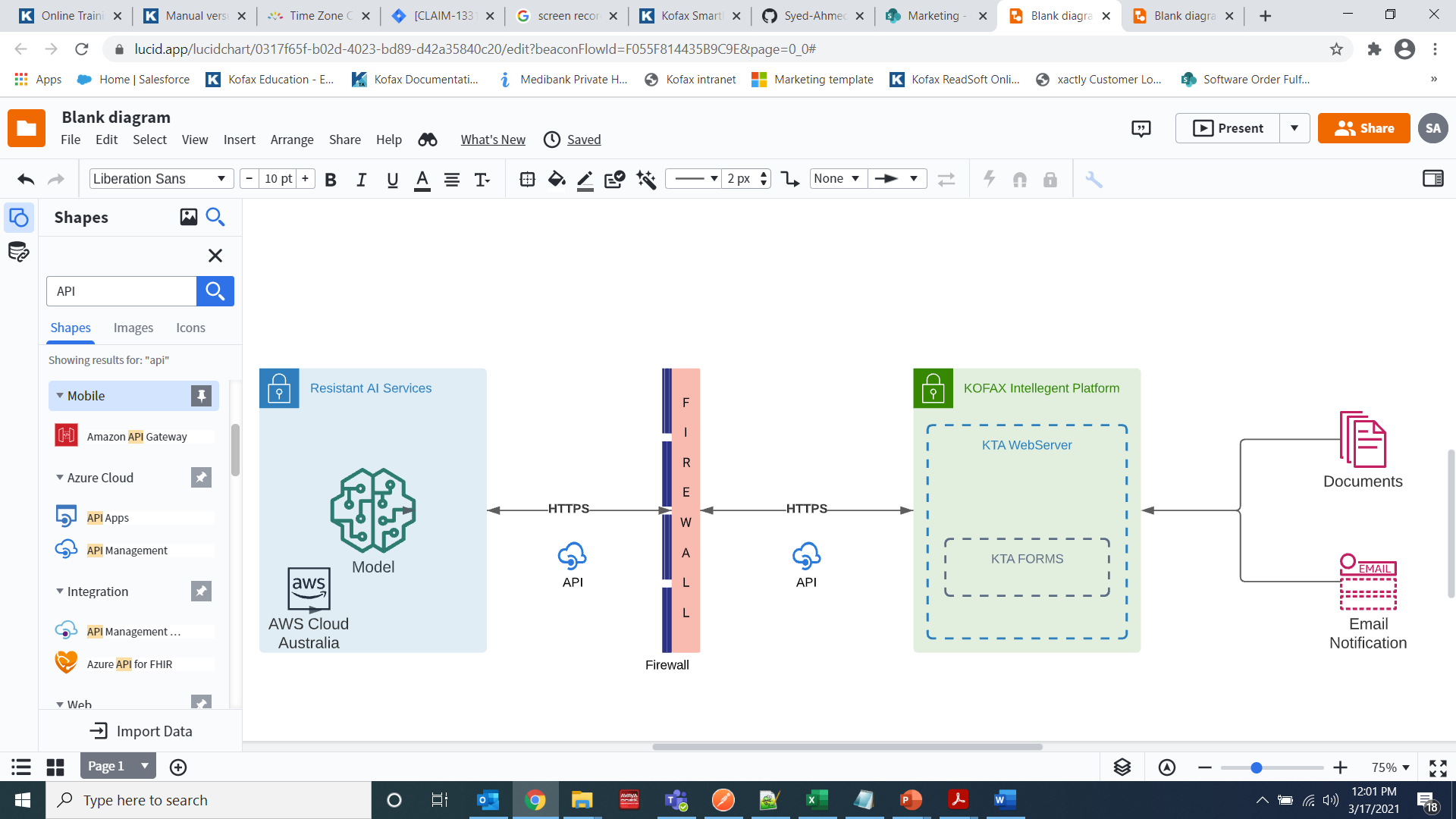
High-Risk documents contain such signs of tampering that the intentional fraud is the most likely explanation.

Architecture of the connector

KTA connects with the Resistant.AI services through number of API’s within the KTA workflow to automate the customer experience without any hassle of setting up or configuring document parameters, settings or preferences.

The below diagram shows

* The documents received via multi-channel are ingested by KTA
* KTA calls the Resistant AI API’s to send the JSON payload over a secured channel
* The result is received in a form of JSON
* A KTA Form displays the document along with its indicators



KTA import

The documents are ingested by KTA through document pooling on the watched folder. The import configuration of files enables the function to ingest the documents in the KTA system.

Frequently Asked Questions?

Below is the list of possible questions gathered to answer the basic questions about storage and detection

Storage

Is data stored in the cloud? And how long its stored?

Yes. To ensure maximum system performance and support flexibility, the Resistant AI service is offered primarily via the cloud. It is completely up to the customer to choose the document retention period. By default, our recommendation is at least 90 days

How do you secure the transfer of the data? and what happens after the document is uploaded to the server?

Data transfer is handled via secure TLS connection. Each user is authenticated using an API key in the https header. Upon submitting a file to the server, a unique ephemeral environment is deployed to process the file. As soon as the analysis is complete, the environment is destroyed, and the result of the analysis is returned to the caller.

How many documents can the system process simultaneously?

The solution is designed to process documents in parallel and independently from one another. The maximum allowed time in the test to process the 1,000 documents simultaneously is 60 second.

Detection

What type of files do you support?

The Resutant AI solution supports the following type of files: PDF, JPEG, PNG, TIFF and HEIC.

How long does it take to analyze a document?

When it comes to analyzing digital PDF documents, the p95 speed is around 15 seconds. Processing images is a bit more demanding, taking anywhere up to 35s.

What languages do you support?

Forgery detection works for any writing system.

Are there any limits when it comes to the size of the document?

AWS S3 limits file sizes of up to 5GB. The only technical limitation for the document processing is the associated 15-minute timeout. Any processing that takes longer than this will not succeed.

**Who do I need to contact to get the Resistant AI private keys & the user credentials?**

The Private Authorization key & account can be requested on the email provided below along with the reference of Kofax SmartHub.

[sales@resistant.ai](mailto:sales@resistant.ai)

Once the package is downloaded and imported in KTA, the private key can be replaced in the server variables section as described below:

|  |  |
| --- | --- |
| **Key** | **Value** |
| Authorization Key | Private authorization key for API calls to happen. |
| File Upload Directory(On-Prim deployment only) | Computer directory through which KTA will ingest the files, check import settings in KTA for watched folder name |
| Do not change below, unless consulted or advised | |
| Document Viewer URL | Internal to Resistant – URL on which the document viewer is built |
| Get File Upload URL | Internal to Resistant – S3 File upload URL |
| Get Analysis URL | Internal to Resistant – Analysis URL for getting the results |