



Kofax Mobile ID Capture Best Practices Guide

Version: 2.7.0

Date: 2023-08-10

KOFAX

© 2023 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

Table of Contents

Preface	4
Chapter 1: Overview	5
Security recommendations.....	5
Licensing.....	5
Real-Time Transformation Interface.....	5
TotalAgility.....	6
Chapter 2: Input images	7
Image source.....	7
General image requirements.....	7
Chapter 3: Image processing	8
Server-side processing.....	8
Chapter 4: Scaling and performance	9
TotalAgility optimization recommendations.....	9
TotalAgility and Real-Time Transformation Interface scaling and performance.....	9
Chapter 5: Extraction, verification, and facial recognition	10
Risk profile.....	10
Expected use case.....	11
Controlling image capture.....	11
Image quality.....	11
User instructions.....	11
Tuning results.....	12
Valid document tuning.....	12
Invalid document tuning.....	12
Combining results.....	12
Future tuning.....	13
Chapter 6: Troubleshooting	14
Installation troubleshooting.....	14
Kofax Mobile ID Capture installation.....	14
Error responses.....	14
Frequently asked questions.....	15

Preface

This guide provides best practices, suggestions, and background conceptual information to help developers use the Kofax Mobile ID Capture to create their own applications.

Chapter 1

Overview

Kofax Mobile ID Capture can be deployed in two fashions, on-device extraction and server-side extraction. The workflow for both extraction processes is largely the same. The user will capture the image on their mobile device. The image must then be processed for extraction. The background of the surface the identity document was captured on will be cropped so that only the identity document is present. Processing may also correct skew, keystone distortions, or warn the user that the image they have captured is unsatisfactory for extraction. After extraction is completed, the extracted data is returned to the user.

Security recommendations

It is recommended that you have a valid SSL certificate.

Licensing

Kofax Mobile ID Capture requires the appropriate licenses to use different features. These are listed in the following tables. For both of these tables use the following symbols to indicate the type of license:

- 1/doc: The volume license is decremented per document. Sending both front and back images is considered one document.
- 1/pg: The volume license is decremented per page. Sending both front and back images is considered two pages.

License error exceptions are written in `ErrorDetails` field.


Real-Time Transformation Interface

License ID	License Type	License Name	Mobile ID Extraction	ID Verification	ID - Facial Recognition
210	Volume	Kofax Transformation Unlimited Fields Extraction	1/doc	1/doc	1/doc
110	Volume	Kofax Mobile ID Capture Server and Device Extraction	1/doc		

License ID	License Type	License Name	Mobile ID Extraction	ID Verification	ID - Facial Recognition
111	Volume	Kofax Mobile ID Capture ID Verification		1/doc	
112	Volume	Kofax Mobile ID Capture Facial Recognition			1/doc

TotalAgility

License ID	License Type	License Name	Mobile ID Extraction	ID Verification	ID - Facial Recognition
106	Volume	TotalAgility Unlimited Fields Extraction	1/pg	1/pg	1/pg
110	Volume	Kofax Mobile ID Capture Server and Device Extraction	1/doc		
111	Volume	Kofax Mobile ID Capture ID Verification		1/doc	
112	Volume	Kofax Mobile ID Capture Facial Recognition			1/doc

 The observed licensing behavior only applies when `StoreFolderAndDocuments` is set to `True` in the request.

Chapter 2

Input images

Image source

Images can come from the following sources.

- Mobile device: The Kofax Mobile Capture SDK has specific capture experiences for capturing image of identity documents. If you are using the Kofax Mobile Capture SDK, please see the *Kofax Mobile Capture SDK Best Practice Guide* for details. If you are using the native capture experience on a mobile device, please see the General Image Requirements section below.
- Scanner: If the source of your input image is a flatbed scanner or a multi function printer, you must make sure it is set to scan in color and have the DPI set to at least 500 dpi.

General image requirements

For the best data extraction results, your image should meet these requirements:

- At least 5 megapixels. Larger sizes are better.
- The identity document should be on an uncluttered and untextured background.
- Having contrast between the color of the document and the background will improve cropping accuracy.
- The image should be in focus. Any blurriness will impact data extraction.
- Free of glare.
- Free of shadows.

Chapter 3

Image processing

Server-side processing

For server-side processing, follow these recommendations.

- Processing in Kofax Mobile ID Capture: It is recommended to use the processing engine within the Kofax Mobile ID Capture product. This engine will always be the most up to date. To specify this engine, use the `xcropImage` parameter.
- Processing with Real-Time Transformation Interface: Though it is recommended that processing be performed in the Kofax Mobile ID Capture product, you are still able to process raw image with Real-Time Transformation Interface by setting the `processImage` parameter to true.
- Processing with a mobile device using the Kofax Mobile Capture SDK: If you are capturing an image with the Kofax Mobile Capture SDK, you can process the image on the device. Use the recommended processing string that can be found in the *Kofax Mobile Capture SDK Best Practices Guide*.
- Image quality analysis: This feature is available when using an Real-Time Transformation Interface server. It will review the submitted raw image and determine if it is suitable for extraction. See the *Real-Time Transformation Interface Administrator's Guide* for more information.

Chapter 4

Scaling and performance

TotalAgility optimization recommendations

To ensure optimum performance, we recommend that the following features are incorporated into your TotalAgility environment:

- Capture Groups to Preload. This optimizes extraction time by preloading the classification and extraction groups of a TotalAgility project into memory.
- PrecompileSyncProcesses. This compiles the process map of the TotalAgility project before execution.

See the TotalAgility documentation for more information on both of these features.

TotalAgility and Real-Time Transformation Interface scaling and performance

Kofax Mobile ID Capture is capable of scaling linearly while processing documents submitted via Real-Time Transformation Interface to Kofax Transformation Services or via RTTS to TotalAgility. Throughput for processed front images can reach 8 transactions per second with 95% of the response times being below 3 seconds.

Kofax Mobile ID Capture processing requires about 50% less hardware when image processing takes place on the device than when image processing takes place in the server.

Chapter 5

Extraction, verification, and facial recognition

Kofax Mobile ID Verification is a solution that is capable of ID data extraction, classification and validation. The validation process evaluates a driver's license, passport or other form of identification to verify if it is real, valid and has not been tampered with. An additional layer of protection can be used to then capture a picture of the user and compare it to the picture on the ID to ensure the person in possession of the ID is the person pictured on the ID.

When working with the Kofax Mobile ID Verification solution, there are several factors that should be considered in order to get the best results possible. These factors vary from conceptual understanding of your organization to the technical implementation of the solution and include the following:

- Understanding your risk profile.
- Understanding your expected use case for the solution.
- Controlling how the images are captures.
- Image quality.
- Providing proper user instructions.

Risk profile

The risk profile of an organization varies based on their expected use case for their solution and what results they expect from it. To set a risk profile, organization must first understand that ID validation will not always flag valid IDs as valid and fraudulent IDs as fraudulent. The solution is tuned to capture more fraudulent IDs, which will result in more false positives, or allow more valid IDs which will allow some fraudulent documents to pass. The organization must understand the impact this will have on the solution they are putting in place and decide how to best tune their solution to meet their needs and expectations.

Here are a few examples of different risk profiles:

- When security is crucial, such as entry points into secure buildings and loan applications for new customers, you may opt for a stricter risk profile that rejects more valid IDs than accepts invalid ones. In this case, it is worth having customers with valid IDs be inconvenienced by providing additional verification than to let those with fraudulent IDs get through.
- When user experience is more important than security, such as opening accounts for existing customers, you may opt for a more relaxed risk profile that accepts more valid IDs, even if some invalid IDs are accepted as well. Your organization may use such a relaxed risk profile with a known group of customers or when other safeguards offer protection against fraudulent IDs.

Expected use case

The use case of the overall solution must be well understood to help develop both the risk profile and to understand the technology used to capture the images. When evaluating the use case, understand the overall organization goals, regulatory requirements of the solution and the speed at which the solution works.

Controlling image capture

To achieve the best results for the solution, consider how the image of the ID and Selfie will be captured into the solution. Limiting these pathways improves results and reduces risks to the solution. For example, capturing from a mobile application only is an ideal way to capture IDs and Facial images. Other capture methods include specific types and models of ID scanners that are used in controlled environments (a teller at a bank, for instance).

Do not to give the user opportunity to send manipulated images to the solution, just as submitting an image from their desktop or gallery of their mobile device.

Image quality

Having a quality captured image is extremely important to getting accurate results from the solution. Not only is the resolution and focus of the image important, but other factors like lighting, alignment, glare and crop are all items that should be considered while capturing both ID images and facial images. The Kofax Mobile Capture SDK has many tools built into the solution that will help users capture a quality image and will help analyze the image before it is sent to the server for extraction and validation. See the Kofax Mobile Capture SDK documentation for details on how to capture quality images, functions in the Kofax Mobile Capture SDK to capture a good image, and how to analyze the captured image to ensure it will work with the solution. These features include the following:

- Quick Analyzer
- Guides and overlays to help align the image
- Auto Capture to help automatically take the image

User instructions

In developing your solution, include clear and concise instructions. The capture screen should include on-screen guides and prompts that indicate how to orient the image and warn of conditions that will prevent a clean capture (such as focus or glare). For capturing ID documents, instructions should show the user how to align the document to the camera. For Selfie capture, users should be instructed to remove their glasses and be mindful of the lighting for best results.

Tuning results

After the Kofax Mobile ID solution is established and installed, take time to tune the solution. Kofax Professional Services should be engaged for this task to ensure proper guidance and expectation setting.

Tuning the solution helps solidify the risk profile. The tuning process consists of two general steps:

1. Run valid documents through the workflow with the goal of allowing all documents to pass.
2. Run invalid documents through the solution. These documents should be fraudulent documents that have been confiscated, or are creative representations of fraudulent documents that might be used against the solution based on the established use case.

In both cases, use the same capture method that end users will use to capture the documents for tuning.

Valid document tuning

Running valid documents through the solution with valid selfies does a few things:

- Establishes that the capture workflow is working as expected and provides quality images to the solution.
- Allows for base thresholds to be set for the different algorithms used in the solution.

It is expected that most valid documents of good quality should pass through the solution.

Invalid document tuning

This step involves sending invalid document to the solution. These are documents that one would expect to fail the validation test. It is important that, especially with the spoof testing, that the proper capture workflow is used. Spoof images should not be sent to the solution directly or in a way that doesn't represent a real world entry point because it may lead to unexpected results.

It is important to expect that not all fraudulent documents will be caught on the first run through of the solution with invalid documents. The purpose of the first try of invalid tuning is to review the different thresholds of the known fraudulent documents as they pass through the solution. The solution can then be tuned to capture more invalid documents.

Combining results

When you have completed both valid and invalid tuning, review the results of both and—with the original risk profile in mind—update threshold settings on the solution to allow the valid documents to pass and fraudulent documents to be caught based on the desired risk profile.

Some organizations may choose to capture as many fraudulent documents as possible that pass through the system, which may result in more valid documents being stopped as well. Other organizations may choose to ensure valid customers are allowed to pass, which may let more fraudulent documents through the solution.

Reviewing the tuning and updating the thresholds and settings of the solution will help set the baseline. At this point, the solution is ready to go into production.

Future tuning

Tuning should not just happen once, but should be done on a regular basis. Once production data can be run through the system, thresholds should be reviewed and adjusted based on the larger quantity of production data. This can lead to greater accuracy, better results, and an even greater return on investment.

Chapter 6

Troubleshooting

Installation troubleshooting

Mobile ID performs the following types of installation and troubleshooting.

Kofax Mobile ID Capture installation

The Real-Time Transformation Interface and Kofax Mobile ID Capture installer is a simple one that checks prerequisites, copies files, and modifies the configuration .xml file. Use the default MSI installer logging tools if something is wrong.

For TotalAgility, no installation is performed.

Error responses

Error response indicate issues that can be resolved as follows. For more details, please refer to *Kofax Mobile ID Capture Administrator's Guide*.

Kofax Mobile ID Capture

If extraction was not successful, a generic error message is provided with a 200 OK (in case of TotalAgility or Real-Time Transformation Interface with enabled Enhanced Error Reporting feature) or 500 Internal Server Error status message.

For further clarification, user can set `ErrorAnalysis` parameter to true. This causes the JSON response to populate the `ErrorDetails` field.

For more technical analysis, such as cropping issues or issues with bar code parsing, use the `EnableLogging` and `LogFolder` parameters.

Kofax Mobile ID Verification and Kofax Mobile ID Facial Recognition

If an unexpected result occurs, the values returned from the fields `VerificationTransactionId` and `FRTransactionId` contain transaction IDs that can be searched on the Verification Application site and reviewed.

Error messages related to Kofax Mobile ID Verification are returned in the `VerificationErrorInfo` field, and error messages related to Kofax Mobile ID Facial Recognition are returned in the `FRErrorInfo` field. Further investigation can be done by checking the verification environment logs.

Frequently asked questions

The first request often times out.

The Mobile ID loads and initializes all models up-front. The more variants there are for a region, the longer it takes to load and initialize. A warmup image can be used to mitigate initial load time. See the *Real-Time Transformation Interface Administrator's Guide* for instructions.

All images return classification failures.

Check the following:

- Make sure all images have been processed. Unprocessed images often fail to classify.
- Make sure processed images are not processed twice. Over-processing results in unusable images.
- Make sure you are setting the correct `Region` and `IDType` for the document you are using.
- When taking pictures of images, minimize glare and avoid overexposure and underexposure. These can affect classification.

Classification is successful, but the extraction results are not good.

Make sure that the image is an acceptable resolution. A resolution of 500 dpi is recommended.

The resolution is correct, but the extraction results are not good.

Review the raw image and make sure the original image is set to a high resolution. If you are using the Mobile SDK, set `videoMode=false`.