

Use guide

v1.4



This guide describes how to interpret the information generated by Alice at the end of an onboarding process.

Find the user

Once Alice’s onboarding process is complete, the result becomes immediately available and can therefore be consulted from the Dashboard. Specifically, simply navigate to the user list section (<https://dashboard.alicebiometrics.com/#/users>) and quickly filter using the email that was used during the registration stage.

Alice

alice-demo

Go to user with ID...

Users

Resources

ADMINISTRATION

Team

Credentials

Audit Log

Duplicates

Filters

Please, select one

Search

Type to search

From

Choose a date

Until

Choose a date

Users

UUID	Email	First name	Last name	State	Selfie	Documents	Created at	Agent
63a983ff-b735-41f2-876d-58076fb04911	iPhone_rqDe0@alice-demo.com			In progress	Yes	0	2023-01-19 16:20:08	onboarding-ios 1.10.6
89ca09ba-e577-41f8-8fde-4fa591d9d3e3	test11@wizink.com			To review	Yes	0	2023-01-18 10:47:39	onboarding-ios 1.10.6
0016fc2c-976e-4f69-a3de-463e28272b26	test10@wizink.com			In progress	Yes	1	2023-01-18 10:41:23	onboarding-ios 1.10.6
363ac8c6-5eb7-43e5-abbe-711ff57b660a	fnyr2q78_test@host.es			In progress	No	0	2023-01-18 10:13:43	onboarding-web 6.3.4
fd7820a6-cebe-4c95-801b-85a2e9df5601	test2@binbin.com			In progress	No	0	2023-01-17 13:22:53	onboarding-ios 1.10.6
2771098d-b1e2-40f2-9d1a-bb61ac01efb2	test@binbin.com			To review	Yes	2	2023-01-17 13:16:31	onboarding-ios 1.10.6
685ca61a-9d2b-4760-9951-0886a068b3b1	2x6a1mkc_test@host.es			Not started	Yes	1	2023-01-17 10:59:33	onboarding-web 6.3.4
d0360ecd-077c-4040-ab82-1fab91e532d6	testing@mcmcj.com			Not started	Yes	1	2023-01-17 10:58:37	onboarding-ios 1.10.6
95f662c4-76fd-40d5-a801-ea795ce263bc	mKzNaNhLVs@alice-demo.com			Accepted	Yes	1	2023-01-16 21:37:54	onboarding-android 1.14.0
817209ba-615d-4808-8de0-677f037db875	jdhdh@skdbdh.com			To review	Yes	1	2023-01-16 18:16:35	onboarding-ios 1.10.6
d7cc8ce6-30ab-4684-bf7c-7bd71604a995	B0sbBqlssuj@alice-demo.com			To review	Yes	1	2023-01-16 09:02:48	onboarding-android 1.13.4
23a9a1de-e6af-4f4a-bb99-17cac49129f8	B0sbBqlsuj@alice-demo.com			To review	Yes	1	2023-01-16 09:01:54	onboarding-android 1.13.4
fc6fc488-0a6a-442a-bafe-4f49f46455c9	KVKaARVChToR@alice-demo.com			In progress	Yes	0	2023-01-13 07:49:01	onboarding-android 1.13.4
d52e1f0d-32ba-4555-ab5c-7a9d5d74f586	qdMsnXmWZh0@alice-demo.com			In progress	Yes	0	2023-01-13 07:48:22	onboarding-android 1.13.4
4a15a88a-13ce-4906-aa6a-07ff84f6ca6c	DoBasEGHfSdR@alice-demo.com			In progress	Yes	0	2023-01-13 07:47:18	onboarding-android 1.13.4
40727278-7056-427d-aa63-db843e4299f6	WmUaasgzvIKO@alice-demo.com			In progress	Yes	0	2023-01-13 07:45:49	onboarding-android 1.13.4
97c4a25d-105d-46df-ac45-a03161cf6442	QRVIYiIiZa@alice-demo.com			In progress	Yes	0	2023-01-13 07:44:43	onboarding-android 1.13.4

User profile

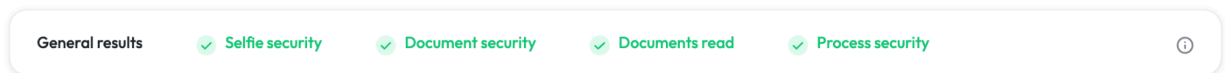
The user profile is the section of the Dashboard from which you can see the result of the onboarding process carried out. Although Alice's SDKs capture the different pieces of evidence sequentially, and are therefore already available as they are uploaded, the final result should not be interpreted until the minimum pieces of evidence are complete (a selfie and an identity document).

The first thing we see as soon as we enter the user profile are the views of the status of the process and its overall result.

Regarding the status of the process, we only consider that a user is ready to review when it equals "To Review" (as seen in the image). This indicates that the user has uploaded all the evidence and therefore finished their process.



On the other hand, the view of the result of the process consists of four main checks: selfie security, document security, document reading and process security.



- Selfie security → Indicates if the selfie belongs to a real person and also matches the identity shown in the document.
- Document security → Indicates if the document displayed is legitimate or contains fraudulent features.
- Document read → Indicates if the document has been read correctly.
- Process security → Indicates if the process has been carried out correctly or if, on the other hand, it shows any indication or fraudulent features such as change of IP, change of device, carrying out the process in several sequential acts, etc.

These four parameters make it possible to make a global decision on the video identification process. For a user to be accepted, they must obtain a positive result in all four (green check).

These parameters are obtained from multiple analyses, of which the details are offered for consultation or additional clarification in the form of different checks that are displayed on the same dashboard page, which have a normalized value between 0 and 100 and are considered accepted values above 50 (if any are below 50, it will result in a negative value in one or several of the four global parameters).


Below are detailed for informational purposes which are all those low-level checks that the tool also has.

Selfie

In this section, apart from generic information such as timestamps or identifiers, four indicators are shown that allow us to better understand the process of capturing the selfie.

Selfie

Active



Show video

InvalidateDelete

Selfie Metadata

Selfie UUID
d5720ec6-6b12-4caf-a506-82f6e01a067b

Created at
February 19 2024 10:33:45

✓ Selfie security

✓ Liveness

✓ Only one face

✓ Uncompromised

✓ Captured with a legitimate device

99 / 100

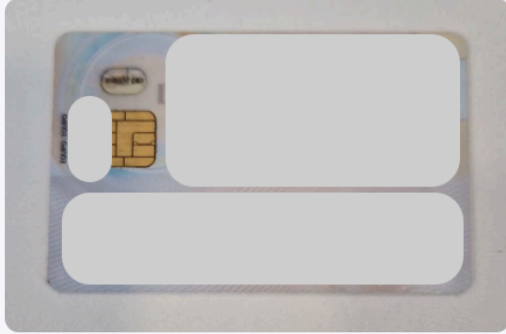

- Liveness → Indicates if the selfie corresponds to a legitimate access, without indications of any type of identity fraud (photos, videos, masks, etc.).
- Only one face → Indicates if there is only one person or face present in the selfie.
- Uncompromised → Indicates if the face is included in an internal database managed by Alice where reported fraudsters are continuously added.
- Captured with a legitimate device → Indicates if the selfie was taken using the Alice SDKs or not.

Documents

In this section, apart from the generic information such as timestamps or identifiers, a series of indicators are shown that allow us to better understand the document capture process.

Documents

ID card



☐ Whole image

[NFC info](#)


[Invalidate](#)

[Delete](#)

Document Metadata

Selected issuing country

Selected document type

ESP 

ID card

Document UUID

9ed20377-f9a7-4f08-9b61-f9651bc08460 [🔗](#)

Created at

February 19 2024 10:34:06

✔ Document security

✔ Matches expected document

✔ Face in front side

✔ Face matching

✔ Uncompromised

✔ Not forged

✔ Not printed

✔ Not shown on screen

95 / 100

100 / 100

99 / 100

74 / 100

79 / 100

Not a synthetic document

N/A

✔ Checked MRZ

Authentic NFC chip

✔ Front and back of the same document

✔ Coherent dates with each other

✔ Unexpired document

✔ Age matches estimated age

✔ Captured with a legitimate device

100 / 100

- Selected issuing country and document type → Indicates the issuing country and the document type selected by the user when uploading the document in question.
- Matches expected document → Indicates if the document uploaded is the same as the one expected by the customer/system.
- Face in front side → Indicates if the document has a face in the front side.
- Face matching → Indicates if there is a correspondence between the person present in the selfie and the person present in the photograph of the document.

- Uncompromised → Indicates if the document is included in an internal database managed by Alice where false public documents are continuously included in the network.
- Not forged → Indicates if the data included in the document is legitimate or not.
- Not printed → Indicates if the shown document is printed or it is the original.
- Not shown on screen → Indicates if the pictures were taken to the original document or through a screen.
- Not a synthetic document → Indicates if the uploaded document is a digitally generated image. It only applies in case of using a version of the product with file upload.
- Checked MRZ → Indicates if the MRZ (or any other code such as PDF417, QR, etc.) present in the document is verified (it respects the expected format for this type of code).
- Authentic NFC chip → Indicates, if it is a document that has an NFC chip, NFC reading has been enabled and the device used has an NFC reader; if the information available on the document chip has been correctly extracted and read.
- Front and back of the same document → Indicates if the information present on both sides of the document is consistent with each other.
- Coherent dates with each other → Indicates whether the different dates present in the document are consistent with each other.
- Unexpired document → Indicates if the document is expired.
- Captured with a legitimate device → Indicates if the document was taken using the Alice SDKs or not.

Apart from all these indicators, this section of the user profile shows all the data that has been extracted and read from the document on all sides of the document. Also including for most of them certain alerts that corroborate their correct reading, integrity and coherence.

✔ Document reading

✔ Matches expected document

✔ Read MRZ

✔ Checked MRZ

Summary Front Back

Given name

✔ Consistent field

Surname

✔ Consistent field

First surname

✔ Consistent field

Second surname

✔ Consistent field

Birth date

✔ Checked field
✔ Valid date format
✔ Valid date range
✔ Over 18
✔ Consistent field

Birth place

Nationality

✔ Checked field
✔ Consistent field

Sex

✔ Checked field
✔ Consistent field

ID number

✔ Checked field
✔ Consistent field

Document number

✔ Checked field
✔ Consistent field

Issue date

✔ Checked field
✔ Valid date format
✔ Valid date range
✔ Consistent field

Expiration date

✔ Checked field
✔ Valid date format
✔ Valid date range
✔ Unexpired date
✔ Consistent field

Document type

✔ Checked field

Document country

✔ Checked field

Address

Address line 1

City

Province

Optional data

✔ Checked field

MRZ

✔ Checked field
✔ Completed MRZ name

CAN

Parent's names

Process

This section shows information about how the onboarding process was done.

- Unique device → Indicates if the process was completely done using the same device.
- Unique IP → Indicates if the process was completely done using the same IP address.
- Total sessions → Indicates how many times the user opens the onboarding process.
- Sessions to complete onboarding → Indicates how many times the user opens the onboarding until the process was completed.

✓ Process security

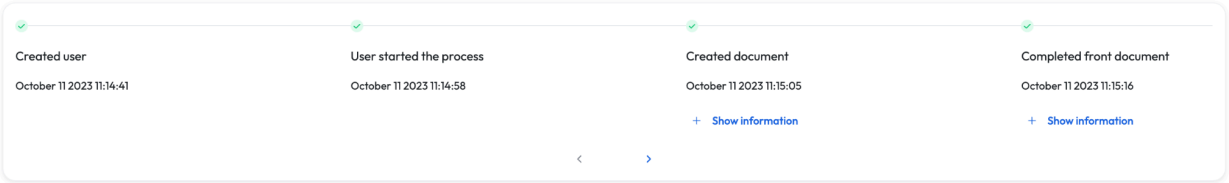
Unique device	✓
Unique IP	✓
Total sessions	1
Sessions to complete onboarding	1

Timeline

This section shows the time sequence of the different milestones that a user has gone through during their onboarding process.

Each of these events is accompanied by a timestamp indicating when it occurred. Likewise, if the element in question is shown, new additional information is displayed regarding said action, such as the device and the IP address from which it was carried out, the version of the product, or the country and type of document used.

Timeline





Alice

www.alicebiometrics.com