

# Control iD iDFace Face Reconginition Access Controller



## Control iD iDFace Face Reconginition Access Controller Owner's Manual

[Home](#) » [Control iD](#) » Control iD iDFace Face Reconginition Access Controller Owner's Manual 

### Contents

- [1 Control iD iDFace Face Reconginition Access Controller](#)
- [2 Specifications](#)
- [3 FAQs](#)
- [4 OVERVIEW](#)
- [5 PRODUCT USING INSTRUCTIONS](#)
- [6 Documents / Resources](#)
  - [6.1 References](#)
- [7 Related Posts](#)

# Control iD

Control iD iDFace Face Reconginition Access Controller



## Specifications

- **Product Name:** midface
- **Manufacturer:** Control iD (a company of the ASSA ABLOY Group)
- **Identification Methods:** Facial validation, Mifare RFID cards, QR codes, PINs/passwords

## FAQs

- **Q: What type of Personal Identifiable Information (PII) is stored by iDface?**
  - **A:** The PII stored by iDface can include default information, biometric templates, or templates stored on cards.

## OVERVIEW

### What is iDface?

- iDface is an access controller capable of identifying users through facial validation, Mifare RFID cards, QR codes or PINs/passwords. The product is fully manufactured by Control iD, a company of the ASSA ABLOY Group.

## PRODUCT USING INSTRUCTIONS

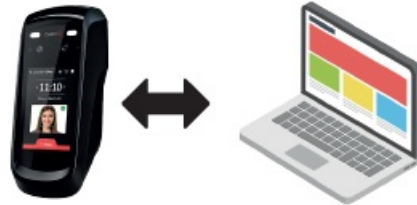
### In what configurations can iDface be used?

- midface supports 5 different modes of operations, described below:

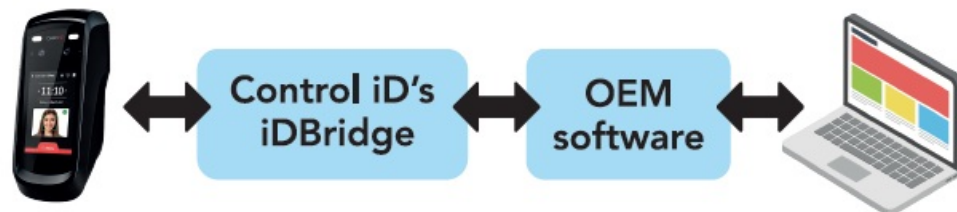
- **Standalone**



- **Embedded web server**



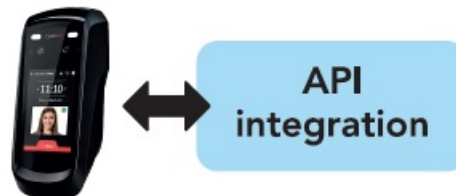
- **OEM integration**



- **insecure Cloud**



- **API Integration**



## **Standalone**

- In the standalone configuration, iDFace does not need to be connected to a network, and all configurations are performed on the device's Graphical User Interface (GUI).
- Data can be imported or exported by using a standard USB flash drive.

## **Embedded Web Server**

- For small-scale deployments (i.e. just a few devices), users may opt to use the embedded web interface available on iDFace to manage users and logs (i.e. export/import data). The only requirement for this operation mode is to connect an Ethernet cable to the iDFace.

## **OEM integration**

- Control iD products integrate with major access control software providers. In this mode, all iDFaces must be connected to the network and Control iD's iDBridge integration software package must be installed.

## **iD Secure Cloud**

- iDFace natively integrates with iD Secure Cloud. No on-premises software components are necessary for a true plug-and-play experience. iD Secure Cloud also comes with a mobile app for iOS and Android. In this mode, all iDFaces must have internet connection.
- iD Secure Cloud ([www.idsecure.com.br](http://www.idsecure.com.br)) is an access control software developed by Control iD and hosted on Amazon AWS. The software can be accessed over the internet and enables the management of users, devices, access rules, schedules and many other configuration options.

## **API integration**

- iDFace offers an open API allowing customers to connect directly to the device and manage all access control functions (e.g. users, logs, rules etc.). Although this option requires some development, it offers maximum flexibility.

## **What type of Personal Identifiable Information (PII) is stored by iDFace?**

- As a minimum, iDFace requires an identification number (ID) per user.
- Optionally, the user's name and the user's RFID card number may also be stored in iDFace.
- For facial identification, the user may choose from 3 different scenarios:

### **Default**

- By default, iDFace stores a picture of the user and his/her corresponding biometric template.

### **Template only**

- In this mode, iDFace receives the picture of the user for enrollment (i.e. template extraction), but the device only saves the corresponding biometric template (i.e. the picture is never saved in non-volatile memory).

### **Template on card**

- In this mode, iDFace saves the biometric template of the user in an RFID card and no biometric data is stored in the device.
- For validation, the user will have to present his/her card to the face, and the device will confirm that whoever is in front of the terminal matches the template stored in the card (no biometric data will be saved in the device's non-volatile memory and the credential holder is also the sole owner of the biometric data).

## **What is a biometric template?**

- Each template consists of a selection of significant features of a facial scan (for example, the distance between facial elements). In that sense, a biometric template is a binary representation of a person's face but contains

much less information than a picture. Control iD's facial template is about 1kB in size where a typical cell phone picture is usually 4000KB or more.

- A biometric template, on its own, is useless outside this system. The user data points cannot be reconstituted to create an entire facial scan. Also, companies cannot cross-reference users' biometric templates with national registries or any other external databases.
- In short, the secured template serves one sole purpose: to identify the user onsite and grant access.

#### **Does iDFace support encryption for data in transit?**

- Yes, iDFace supports HTTPS and TLS 1.3.

#### **What methods are used to authenticate users accessing iDFace?**

- iDFace implements username/password authentication over HTTPS for granting access to the API.

#### **What type of logs does iDFace offer?**

- iDFace provides an audit log (system modifications etc.), an access log and an alarms log (tamper, door forced etc.).

#### **Is there video recording when authentications take place?**

- No, iDFace doesn't record any video internally during authentication or otherwise.
- iDFace supports the ONVIF (Open Network Video Interface Forum) protocol and optionally allows NVRs (Network Video Recorders) to record videos in real-time from the device.

#### **What is the fallback if a user cannot/does not want to use facial identification?**

- iDFace supports Mifare RFID cards, QR codes, and PINs/passwords for users who can't or don't want to use facial identification.


#### **How does the system work when exposed to the elements such as direct sunlight?**

- As with any facial identification solution, direct sunlight is not ideal but Control iD's iDFace implements an HDR (High Dynamic Range) camera that enables the product to perform well in adverse scenarios (direct sunlight or low light at night). Testing and environmental deployment examples have proven competitive advantages versus comparable facial identification models in the market.

#### **Is facial identification for access control legal in the US?**

- Facial identification for access control is legal in the US in most cases if customers and users comply with applicable federal, state, and municipal laws and regulations, which may include compliance obligations such as providing notice, obtaining consent, etc.
- Each deployment is unique and we advise you to consult your company's Legal team.

## Documents / Resources

 <p>Control iD</p> <p>iDFace Facial Identification Features and Benefits</p>	<p><a href="#">Control iD iDFace Face Reconginition Access Controller</a> [pdf] Owner's Manual</p> <p>iDFace Face Reconginition Access Controller, iDFace, Face Reconginition Access Controller, R econginition Access Controller, Access Controller, Controller</p>
---	--

## References

- [iD Control iD | iDSecure](#)
- [User Manual](#)

### Manuals+ Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.