



ID-LOGON



BIOMETRIC SOFTWARE PRODUCT FOR AUTHENTICATION IN OPERATING
AND INFORMATION SYSTEMS. EMPLOYEE ATTENDANCE TRACKING

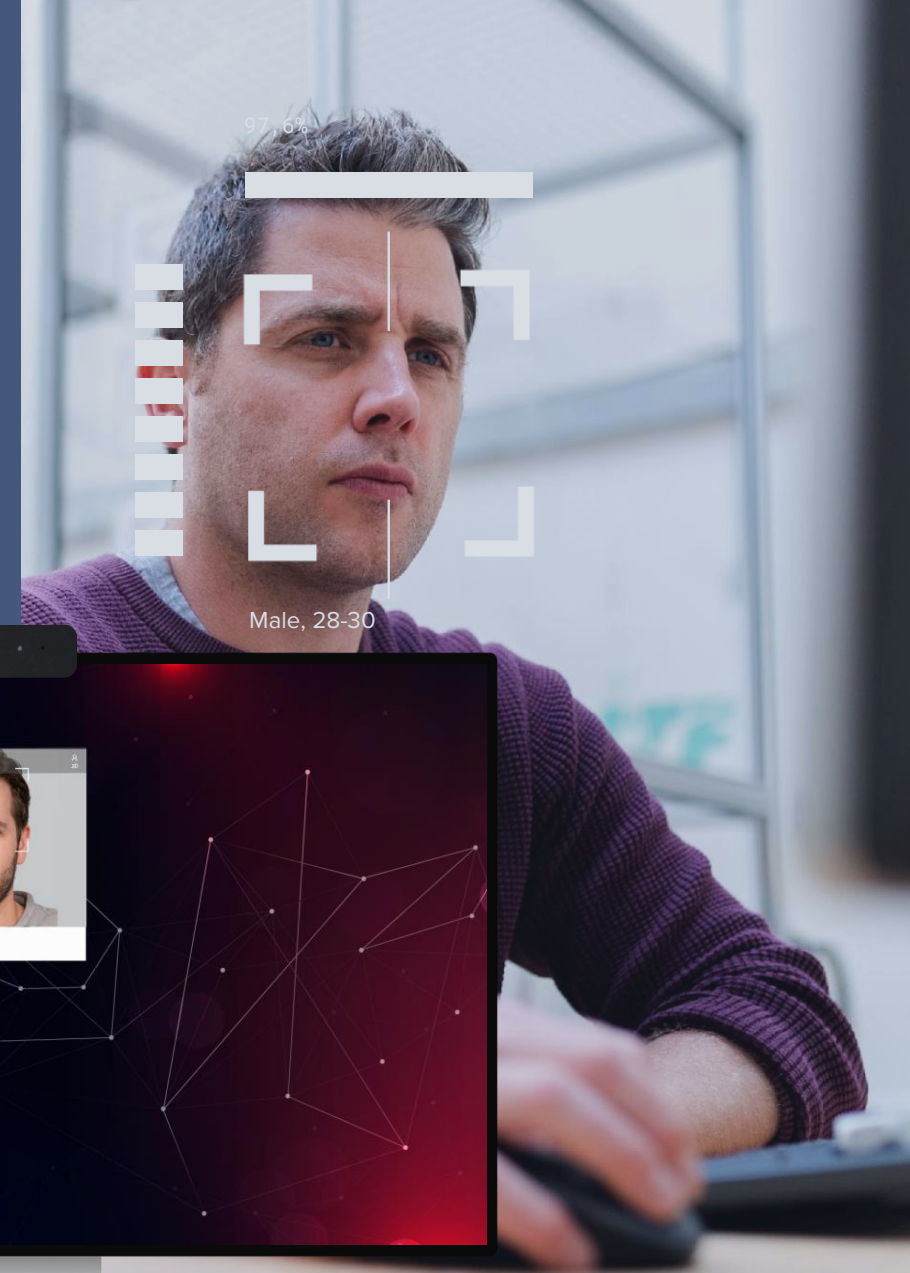


Id-Logon

The solution ensures easy and secure authentication in operational systems and enterprise applications as well as reliable tracking of authorized employees' presence at their workplace.

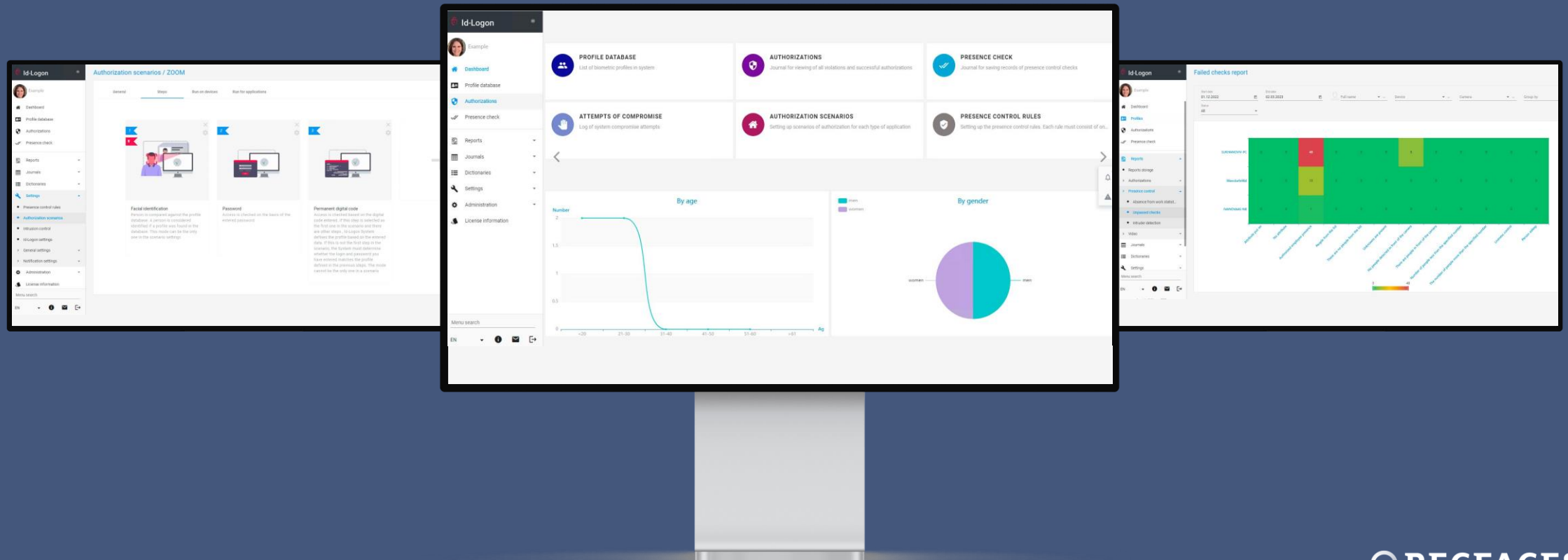
Id-Logon checks for the user's access rights to a PC or an information system by face and can serve as the main or additional verification factor in the following scenarios:

- Windows OS authentication;
- Two-factor authentication;
- Access to various applications;
- Employee presence control at PC;
- Blocking unauthenticated PC users.



Fully-featured interface

Intuitive interface allows users to get quick and convenient access to all functions and features of the solution, from operating mode to fine-tuning, ensuring the efficiency of advanced biometric opportunities



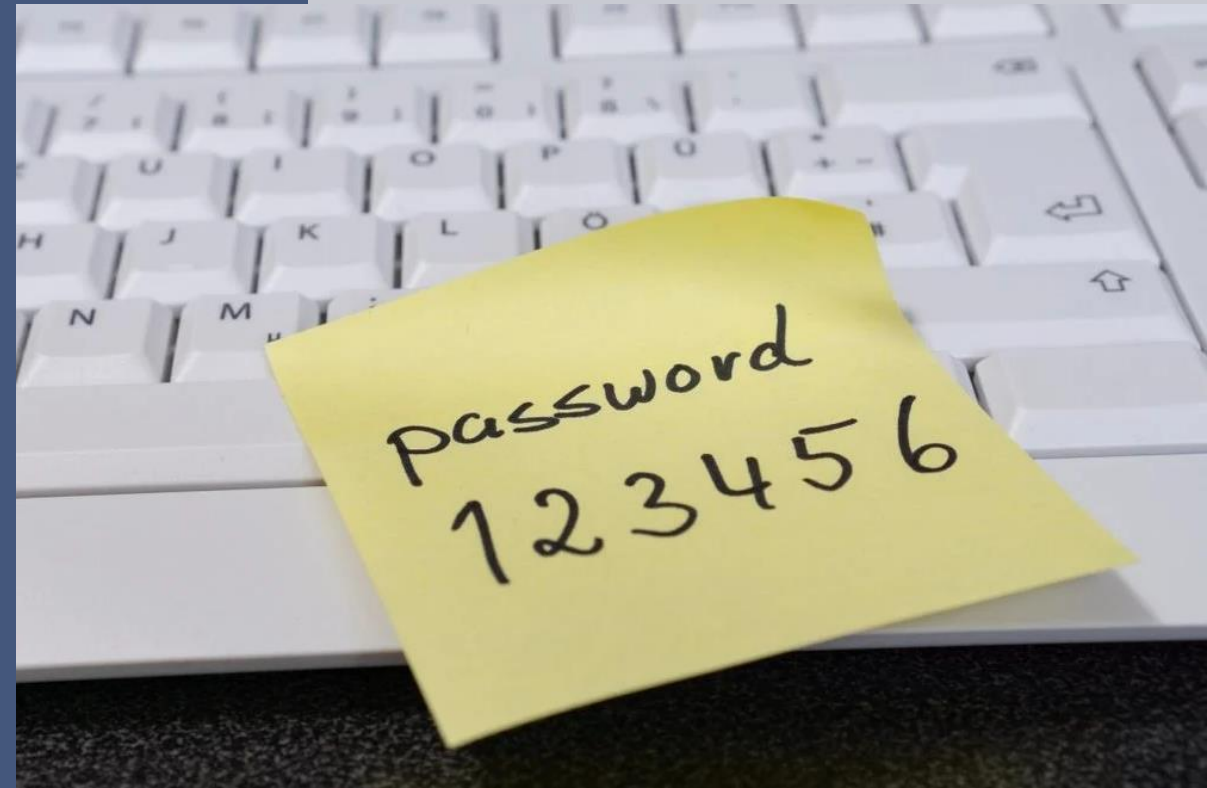
Our customers' challenges

Shortcomings of classic methods of authentication by login and password

- 1 The employee can share information with someone else or write it down on paper. Account credentials can be stolen by malware

Solution

Authentication by face allows to prevent unauthorized access attempts with someone else's account credentials



Our customer's challenges

Numerous points of failure

2 Multi-factor authentication requires additional technical capacity, which will increase the number of points of failure and reduce the system availability.

Solution

Face biometrics is used on the client side and is not liable to distortions arising in external channels.



Our customers' challenges

Impossibility to verify who is working at the computer

3 If authentication has been passed, and the access to the system has been granted, but the employee has left for a while, a malicious user can easily gain access to the system

Solution

The solution recognizes an "intruder" by face and automatically blocks their access to the system



Our customers' challenges

Centralized password change policies are ignored by employees

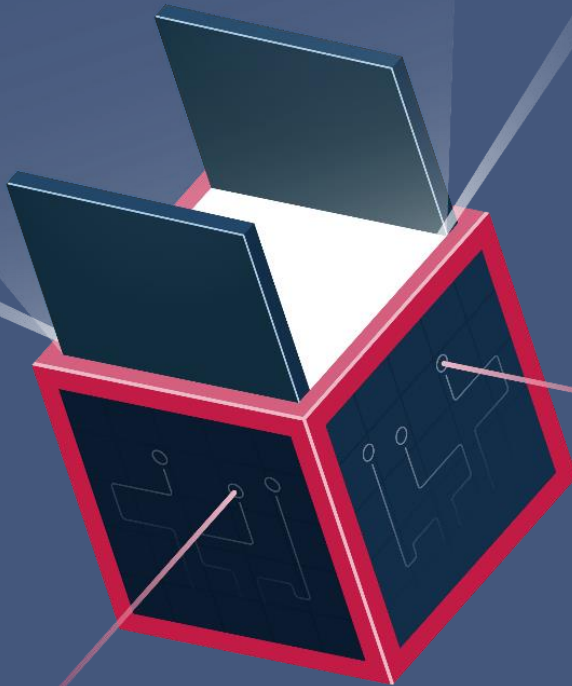
4 Passwords may differ by 1 character from the previous one, or get simplified over time. It certainly increases the workload of administrative staff

Solution

Due to face authentication, there is no need to use passwords, which will add to users' convenience but won't jeopardize security



Id-Logon key benefits



01

Id-Logon **INSTALLATION** takes only **20 MIN**

02

EMPLOYEE ATTENDANCE TRACKING using PC or CCTV cameras

03

CENTRALIZED CONFIGURATION of authentication scenarios in OS and IS

04

Ready-made **INTEGRATION ADAPTER** with **Active Directory/LDAP** for a quick start

05

INTEGRATION with personnel control or data leakage protection systems

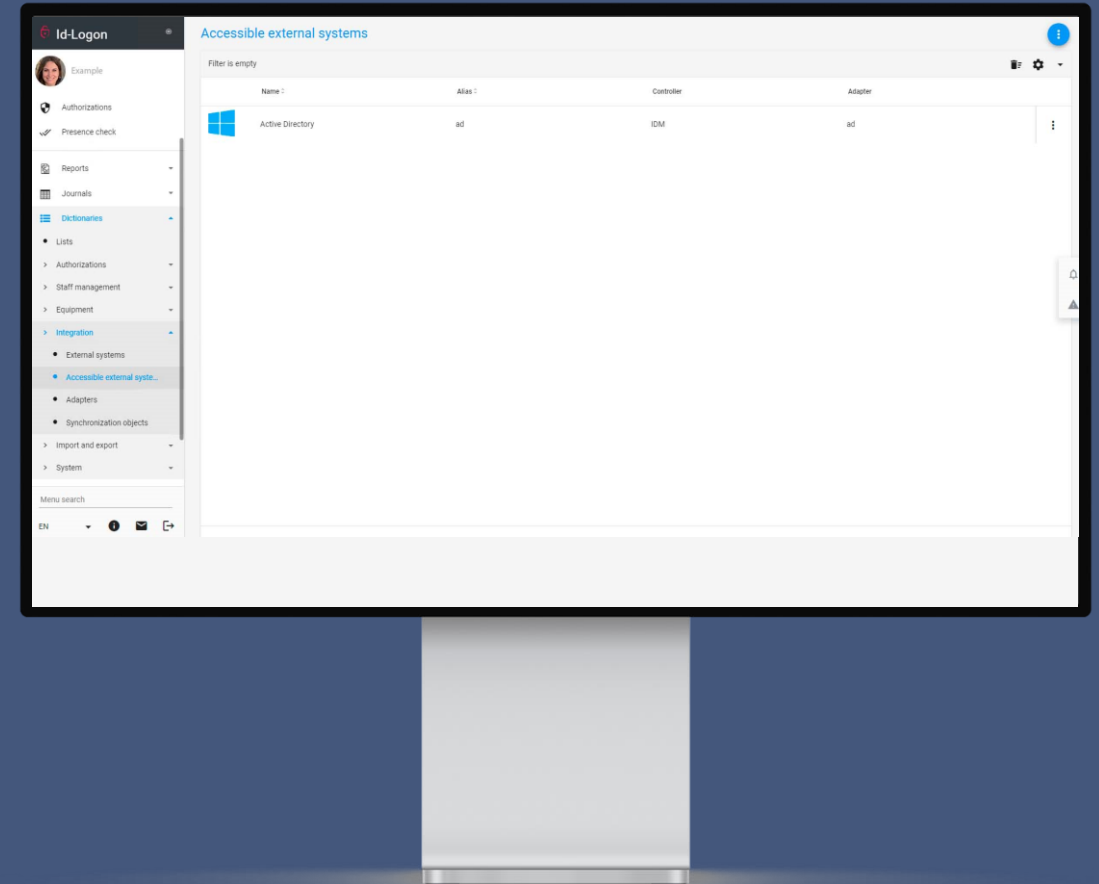
06

WELL-MANAGED release **POLICY** and support system

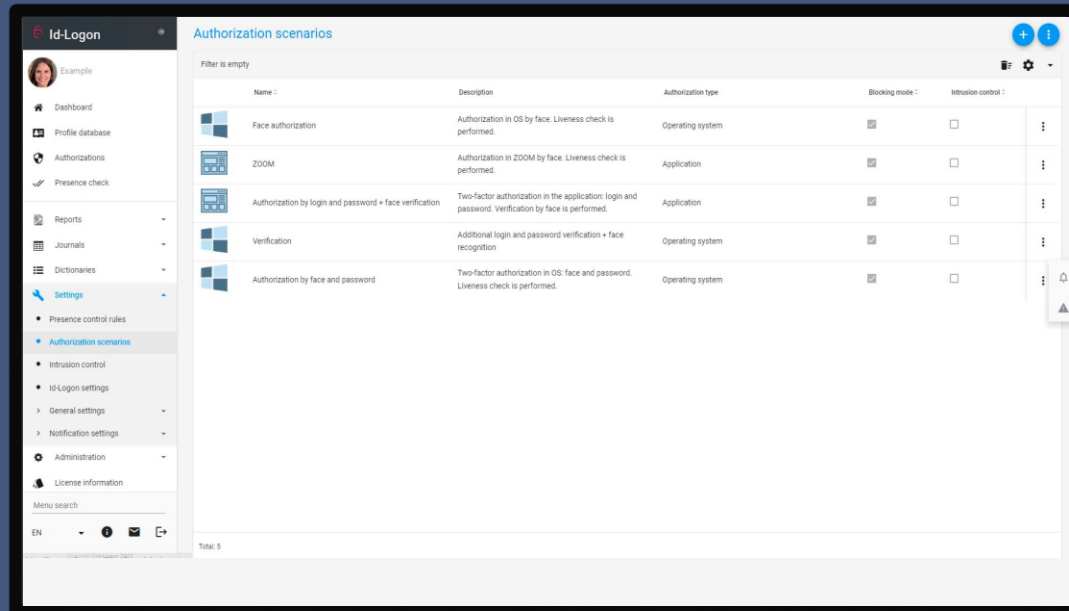
Id-Logon benefits

- **INCREASING THE SECURITY LEVEL OF ACCESS TO THE IT-INFRASTRUCTURE**

The solution provides easy and reliable authentication by face in **Microsoft Windows OS**, as well as in enterprise applications using a webcam, increasing critical infrastructure security. Facial biometrics can be used as a single authentication factor, as well as a primary or a secondary factor in a multi-factor authentication scenario



Id-Logon benefits



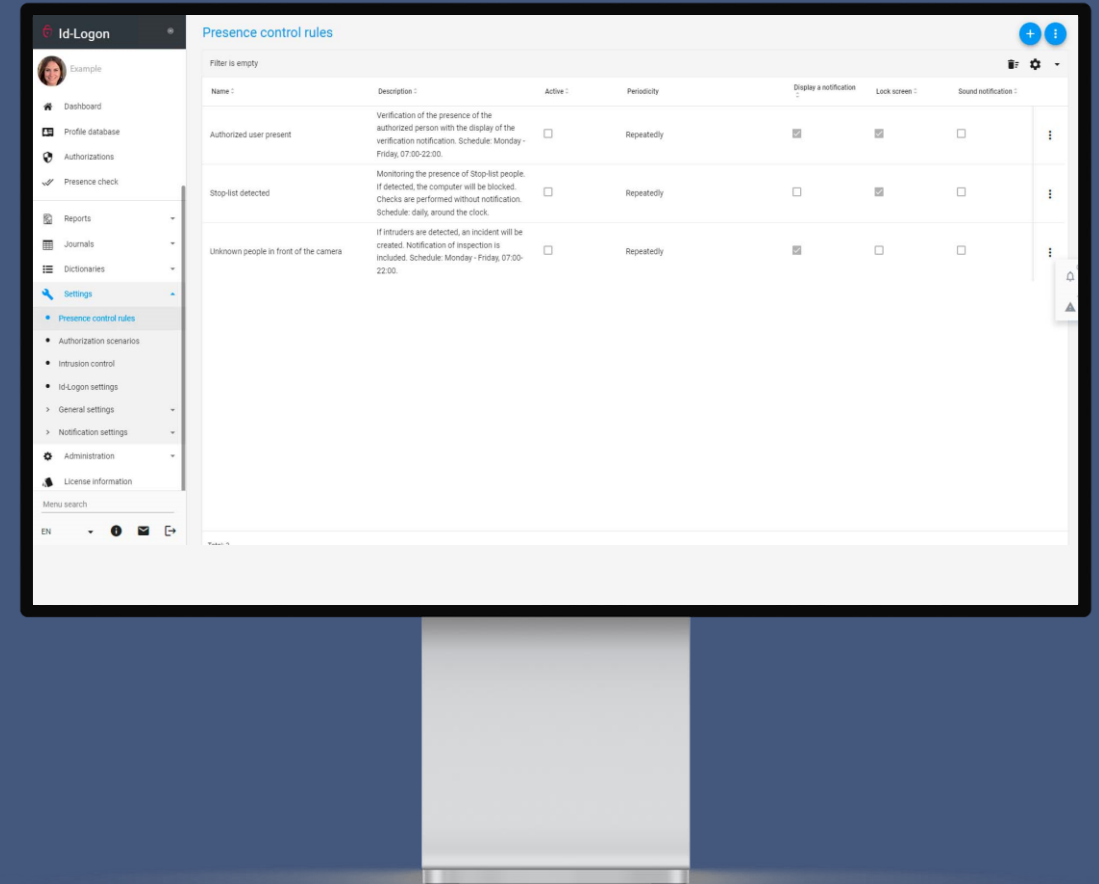
- AUTHENTICATION IN VARIOUS APPLICATIONS AND ENTERPRISE SYSTEMS WITHOUT PASSWORD**

The solution ensures password-free authentication based on a user's facial biometrics in corporate systems and applications. This solution reduces the time and complexity of authentication, increasing users' convenience without jeopardizing security

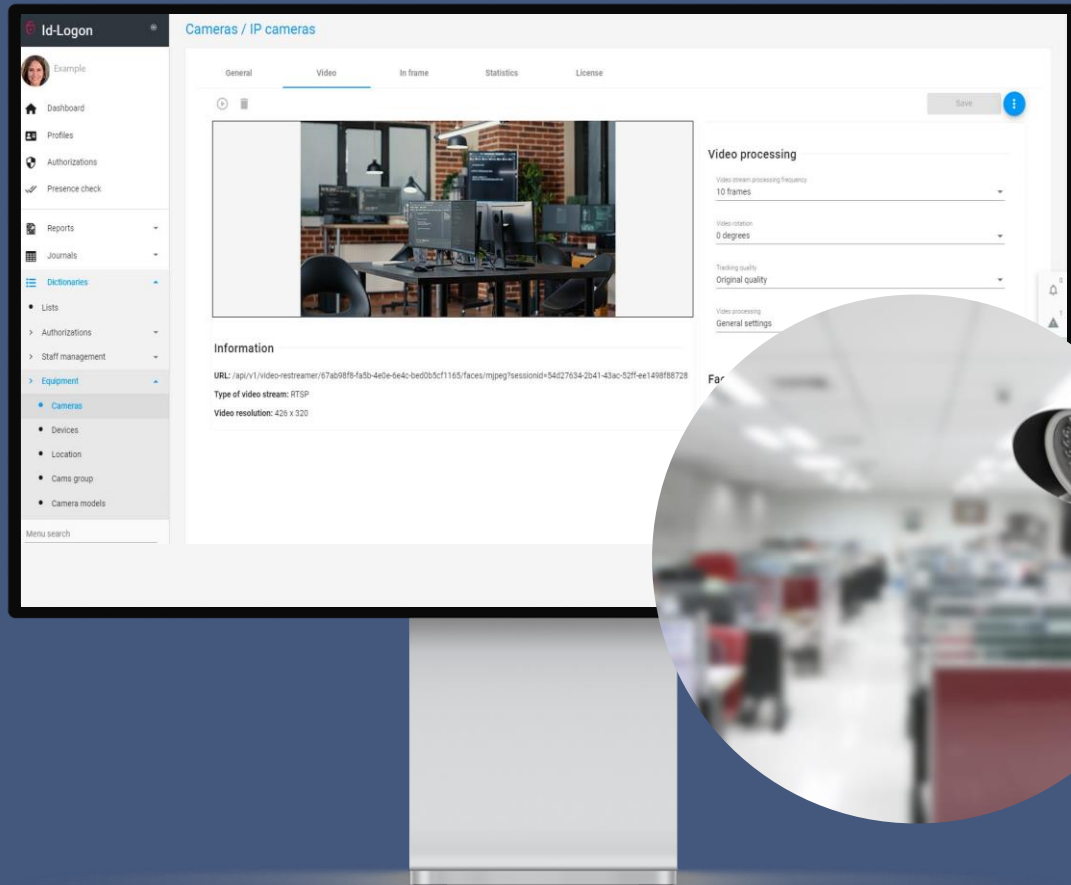
Id-Logon benefits

- **EMPLOYEE WORK ATTENDANCE TRACKING (FROM PC)**

The Solution can check at specified intervals through the camera whether an employee is present at the workplace. If the employee is absent, the Solution will record the detected fact and, depending on the settings, can block the workplace or notify the security service.



Id-Logon benefits

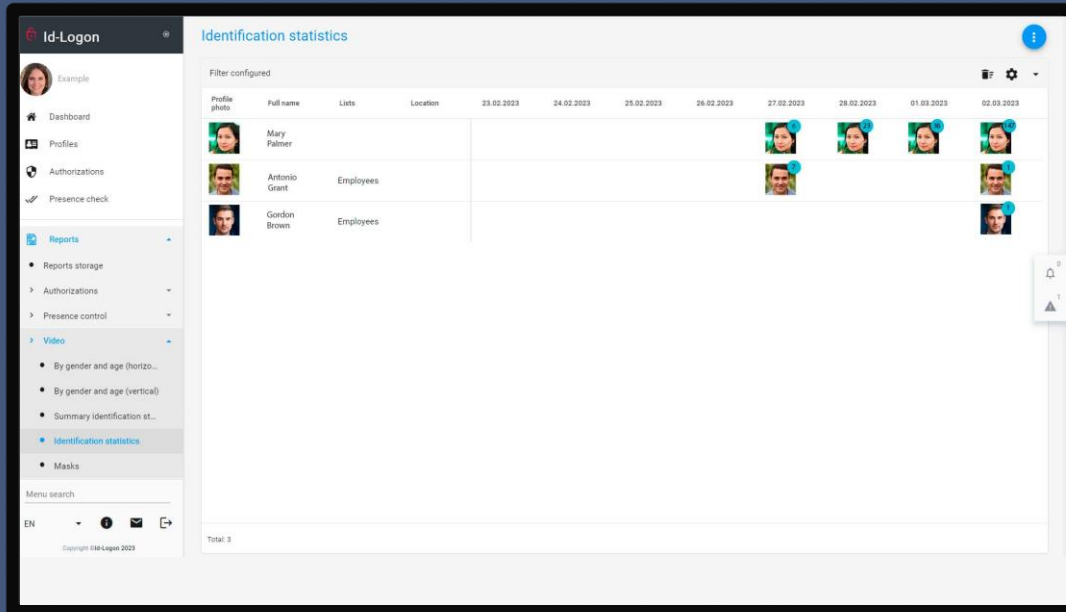


- **EMPLOYEE PRESENCE CONTROL (WHEN THERE IS NO PC)**

For presence control of an employee, whose work doesn't require the use of a PC, the Solution allows you to record absence time in the working area through an IP camera and promptly notify the appropriate services

For example, it goes for video surveillance operators, nuclear power plant operators, machinists, drivers, etc.

Id-Logon benefits



- **PROMPT NOTIFICATIONS ON SECURITY BREACH ATTEMPTS**

The solution instantly identifies a person who is currently using the information system and sends a notification to the security service or other customer's IS to form a rapid response to the event

- **CONVENIENT TOOLS FOR INVESTIGATING SECURITY INCIDENTS**

The solution provides convenient tools for system audits and statistical reporting, and reduces the time spent on investigating security incidents

Reports

- **USERS' AUTHORIZATION**

The operator can generate a report in a few clicks in a given date range on successful and unsuccessful authentication attempts by devices or applications

- **ABSENTEEISM STATISTICS**

The solution allows you to build a statistical report on the facts of employees' absence from the operator's workplace during periodic inspections. The report can be built both for specific employees and for devices

- **REPORT ON CHECKS THAT HAVE NOT BEEN PASSED**

The solution allows you to display as a diagram, download as a table or send by email a report on unsuccessful checks, including up to 12 criteria that can be considered a violation. For example, "unknown persons present", "missing people from the list", "the limit of the maximum number of people exceeded" and many other types of reports

- **VIOLATORS DETECTED**

The operator can build a report on detected violators in a given date range with selection on the basis of the following criteria: by device, lists, departments, name or type of violation

- **REPORT ON COMPROMISE ATTEMPTS**

The solution automatically detects attempts to compromise the system by presenting a paper photo or video on a smartphone screen. Depending on the task, the Solution can automatically block both the device on which the breach is detected and the user whose data is used to compromise the system, as well as notify the security service and record information about the event in the log. Based on this data, the Solution makes a compromise report available to security personnel

- **BLOCKED DEVICES**

In case of multiple violations of the same type, the Solution allows you to automatically block the device. Operators have a log of blocked devices and the right to unblock the device after investigating the causes of blocking and eliminating the source of violations.

Advantages of the solution when using API

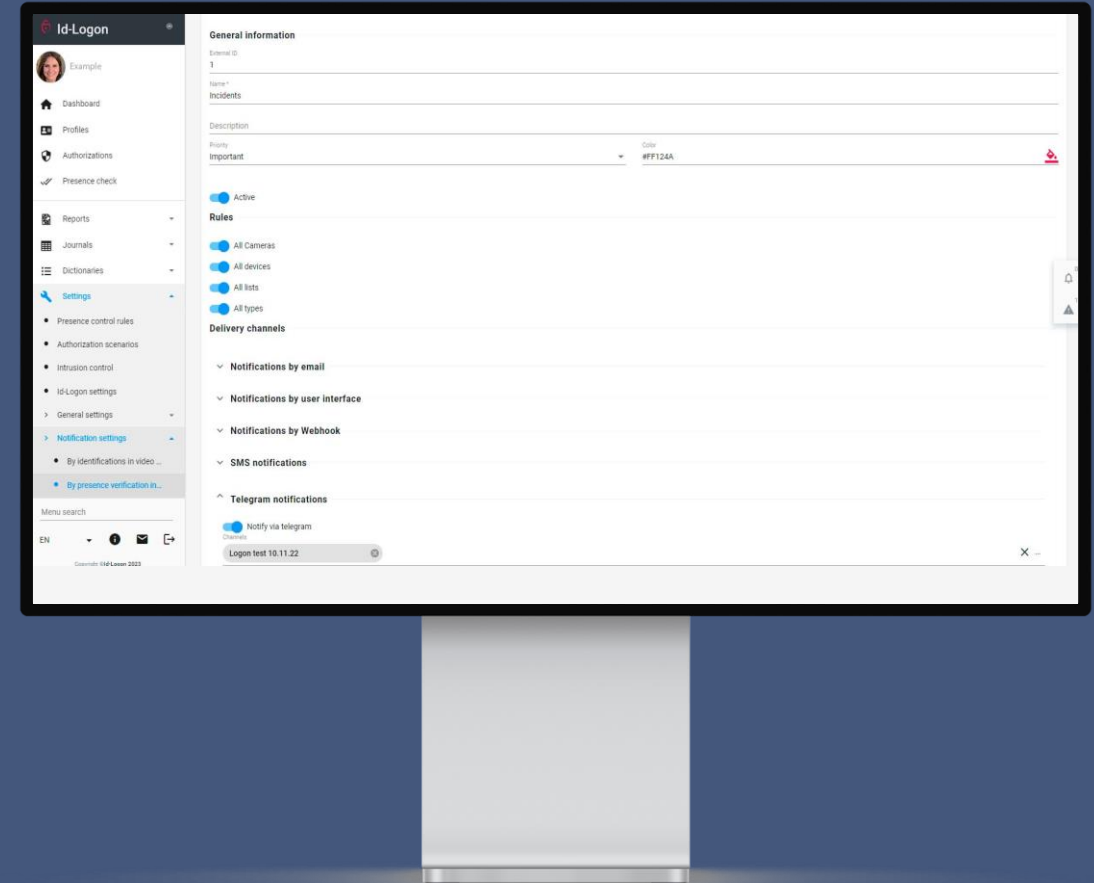
- **ENRICHING EMPLOYEE CONTROL SYSTEMS**

The Solution allows you to increase the reliability of employee control in recording systems by biometrically identifying personnel who are at PCs equipped with webcams. If deviations are detected, the solution will automatically send notifications to security personnel

- **ENRICHING INFORMATION LEAKAGE CONTROL SYSTEMS WITH FACIAL BIOMETRICS CAPABILITIES**

The Solution expands the capabilities of DLP (Data Leakage Protection) systems through biometric personalization of each user's work session.

In case of suspicious activity, the DLP system can perform an unscheduled check by face of who exactly is using the information system. Due to a wide range of the Solution's capabilities, security services can develop and implement their own checks in accordance with the changing threat model



Technological advantages



EASY INSTALLATION
of the solution



Automatic **LIVENESS**
CONTROL



PROFILES
AUTOUPDATE



EASY data **IMPORT**
and **EXPORT TOOLS**



Additional authentication factors
and **CONFIGURABLE SCENARIOS**



Role-based **POLICY**
OF RIGHTS



READY-MADE INTEGRATION
with Active Directory /LDAP



Flexibly configurable **NOTIFICATION**
SYSTEM



API for integration



INTEGRATION with external
systems via CSV file



Duplicated **PROFILES CONTROL**

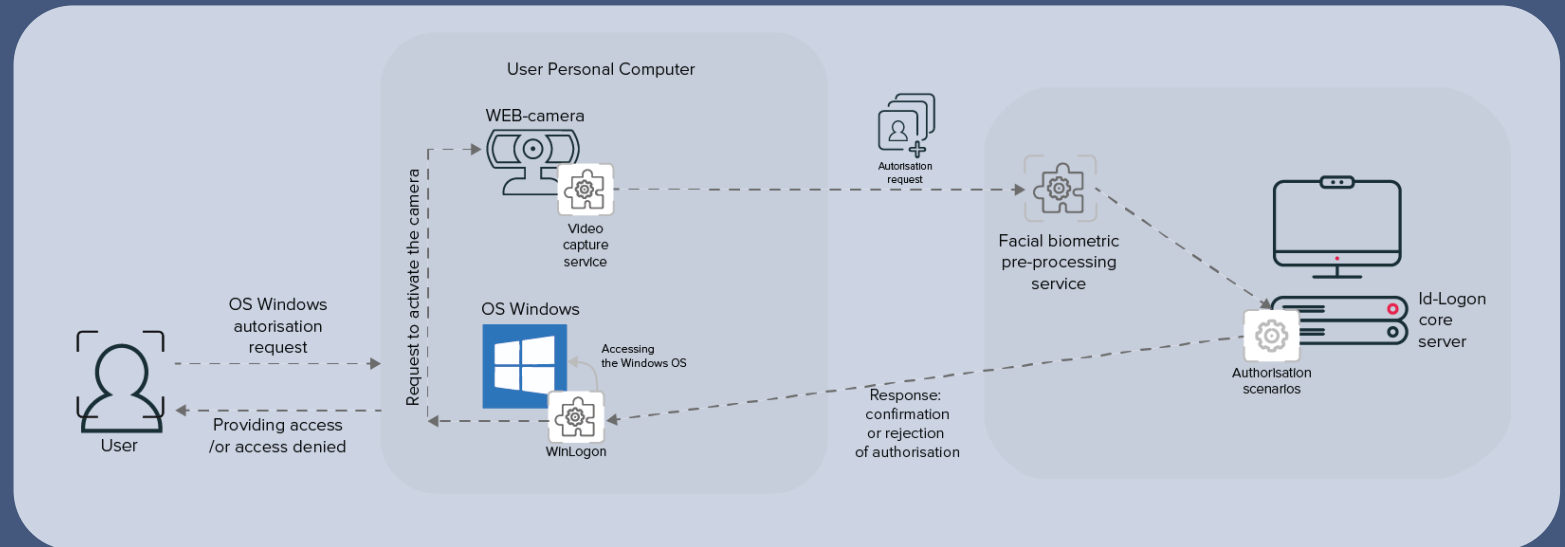


High level of
INFORMATION
SECURITY

User authentication in Windows via the WinLogon client application

The WinLogon client application provides biometric authentication for access to the Windows operating system

The Solution deployment diagram contains the following steps:



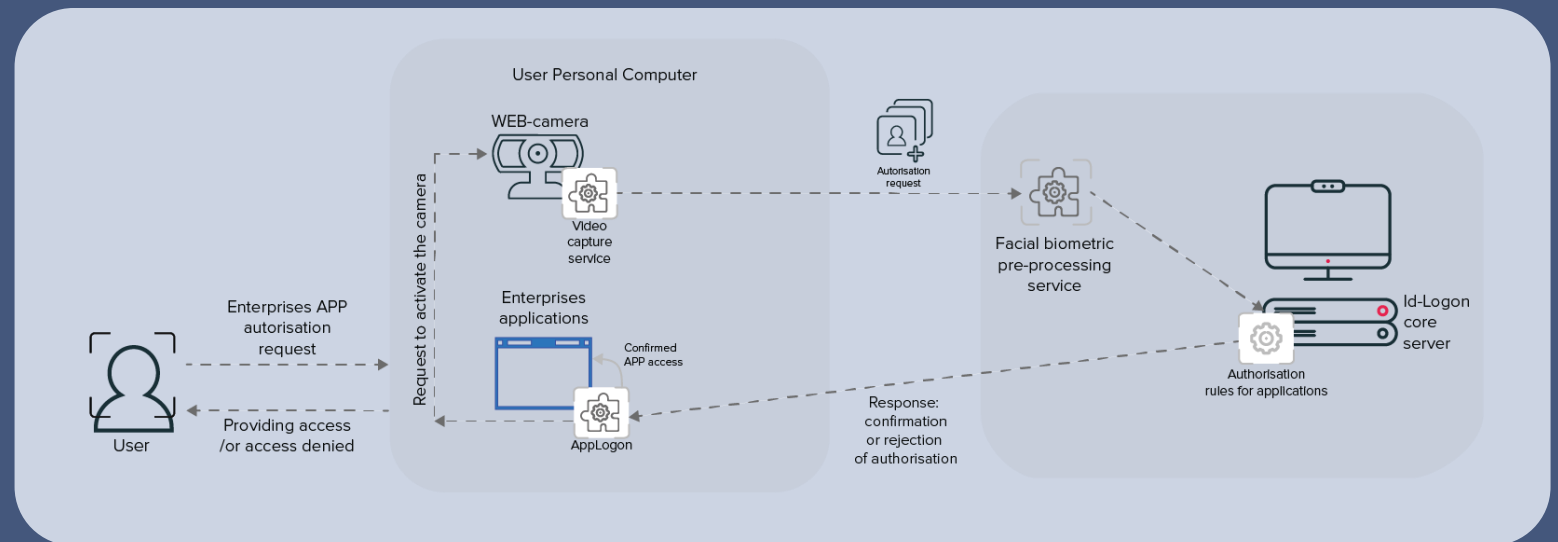
- The WinLogon application, in compliance with its settings, initiates a request to turn on the WEB camera.
- The data is captured from the camera video stream (depending on the settings) by the Video Capture Service and transmitted to the Video Preprocessing Service and pre-processed using the CPU power of the client's PC.

- The processed photos and biometric templates are sent to the Id-Logon core server, where user identification and/or verification is performed.
- Based on the identification result and configured authentication scenarios, the Solution grants or denies access and returns a response to the client's PC.
- Based on the received answer, the service grants access or denies the user's request to log in to Windows.

Customer authentication in the enterprise application via the AppLogon service

AppLogon service provides biometric authentication in one or more application(s) specified in the System settings

The Solution deployment diagram in this case is almost identical to the user authentication scheme through the WinLogon application mentioned above:

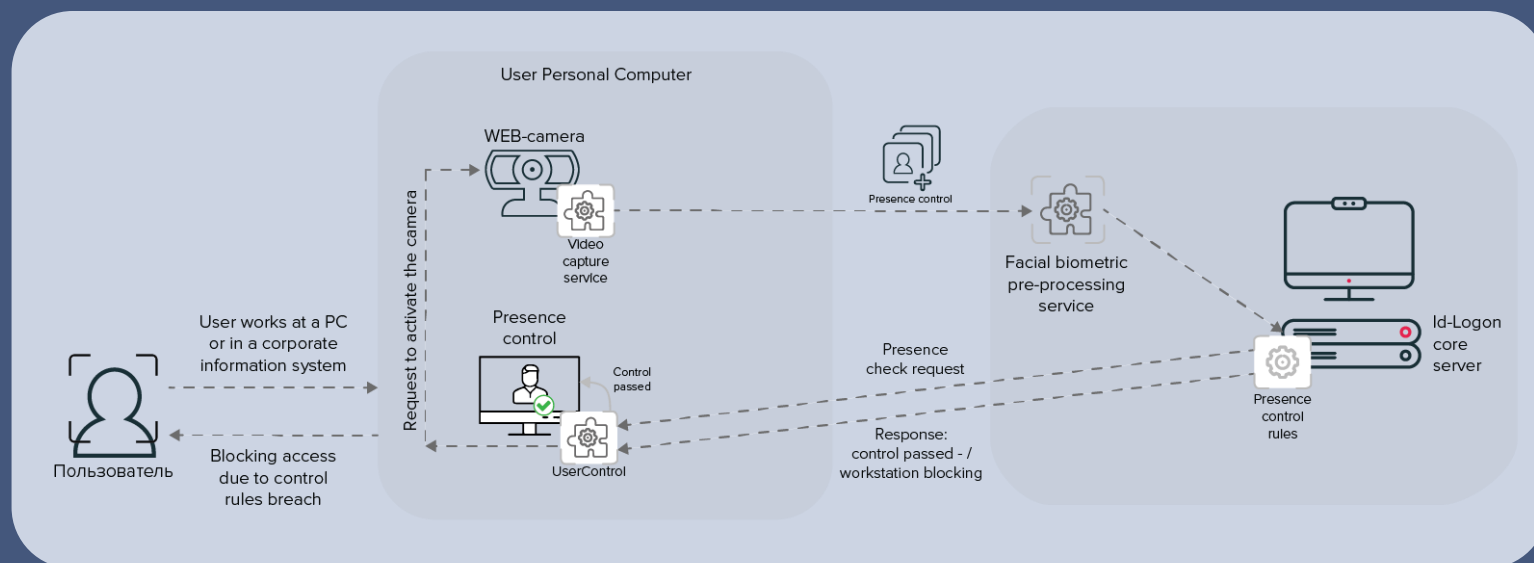


- The AppLogon application, in compliance with its settings, initiates a request to turn on the WEB camera.
- The data is captured from the camera video stream (depending on the settings) by the Video Capture Service and transmitted to the Video Preprocessing Service and pre-processed using the CPU power of the client's PC.
- The processed photos and biometric templates are sent to the Id-Logon core server, where user identification and (or) verification is performed.

- Based on the identification result and configured authentication scenarios, the Solution grants or denies access and returns a response to the client's PC.
- Based on the received answer, the service grants access or denies the user's request to log in to the enterprise application.

User attendance control via the UserControl service

The UserControl service is used for biometric user work attendance tracking, as well as for detecting unauthorized employees using the PC



Steps of the Solution deployment:

- The UserControl Service according to its settings initiates a request to turn on the WEB-camera.
- The data is captured from the camera video stream (depending on the settings) by the Video Capture Service and transmitted to the Video Preprocessing Service and pre-processed using the CPU power of the client's PC.
- The processed photos and biometric templates are sent to the Id-Logon core server, where user identification and (or) verification, as well as verification for compliance with the Presence Control Rules are performed.

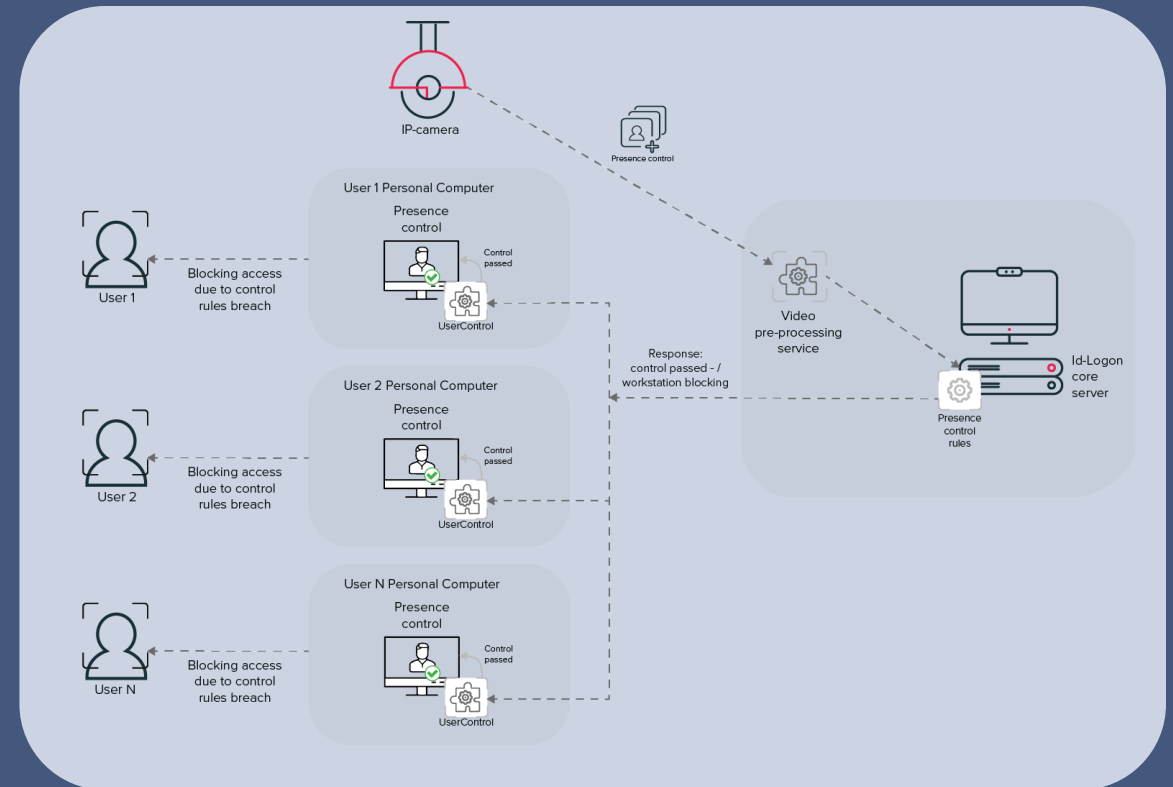
- Based on the identification result and configured authentication scenarios, the Solution returns a response to the client's PC.
- Based on the response received, the service records a successfully passed check in the presence check log or blocks access for violation of control rules.

Employee attendance control via IP-cameras

If users' PCs are not equipped with WEB-cameras, it is possible to install one IP-camera to control employee work attendance. In this case, the UserControl service must be installed on each computer.

Steps of the Solution deployment:

- The UserControl service initiates a request to read data from the IP camera.
- The data is transmitted from the camera video stream to the Video Preprocessing Service and pre-processed using the CPU power of the client's PC.
- The processed photos and biometric templates are sent to the Id-Logon core server, where user identification and (or) verification, as well as verification for compliance with the Presence Control Rules are performed.
- Based on the identification result and configured authentication scenarios, the Solution returns a response to the client's PC.
- Based on the response received, the service records a successfully passed check in the presence check log or blocks access for violation of control rules.



Cycle of a successful project



20 minutes
Id-Logon installation process

Demo license



Free access



**Automated Working
Stations (3)**

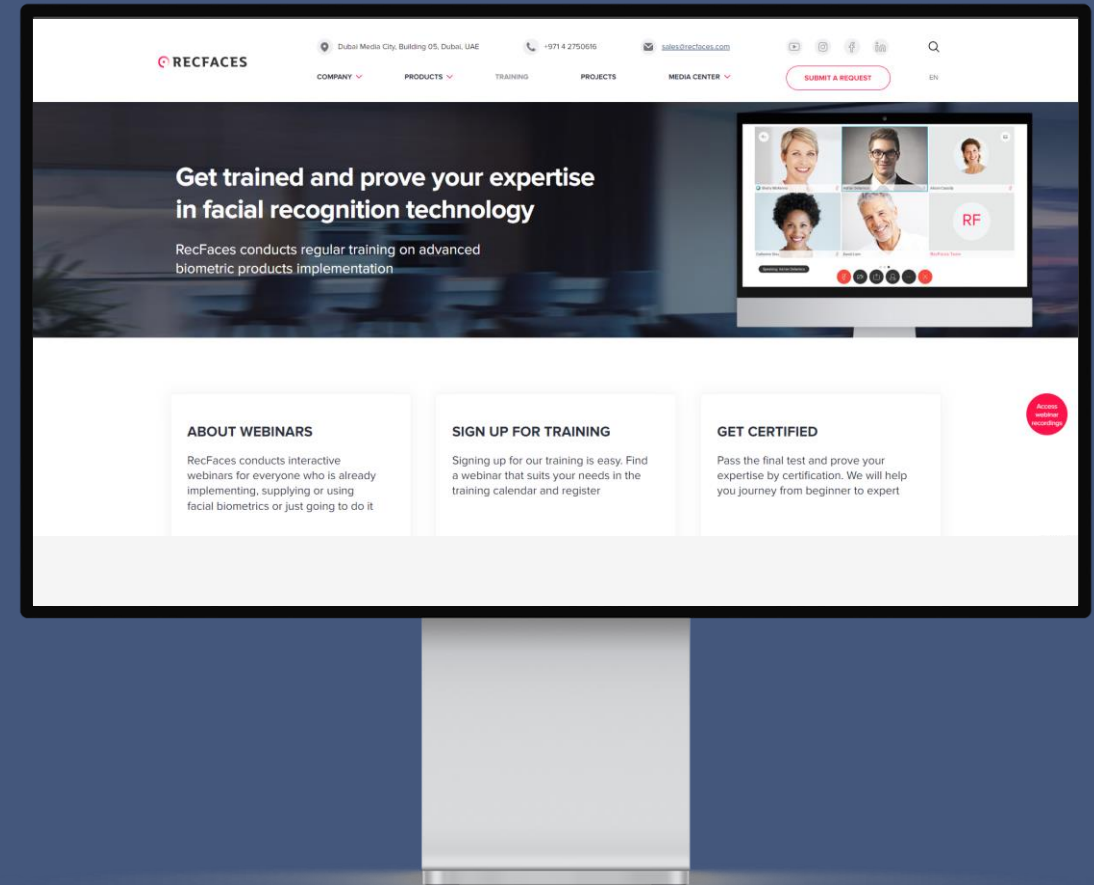


**Time period
3 months**

Sharing experience on biometrics implementation

Why our webinars are worth attending:

- **Free participation** and feedback
- **Certificate** of course completion
- **Live broadcast** and products' demonstration in real-time
- **Access to all supplementary materials:** recorded webinars, presentations, tests
- **Demo license**



Course structure

Lecture 1. Sales. Introduction to biometrics

Introductory webinar. General information on biometrics, face recognition and RecFaces' solutions. Our experts explain how biometric products function and how they can be implemented

Lecture 2. Pre-sales. Product overview

The second part of our product course. This webinar gives a deeper understanding of the product and its benefits as well as allows partners to evaluate the convenience of our product's interface

Lecture 3. Technical information. Administration and fine-tuning

Technical information, administration and fine-tuning. After our product webinars the user will be able to install the solution and provide its smooth performance without involving any IT specialists

Licensing policy



Number of AWS

User workstation licence



Technical support

The support certificate includes software updates and technical support

About RecFaces

Pool

Of ready-made
biometric products

Among the first

To develop biometric software
products in the world

More than 200

Installations around
the world



International projects

The airport in Kenya, Shopping centers in
Brazil and Peru, Stadium in Australia, Metro
in Thailand, and many others

Team of experts




Developers, technical engineers and
analysts with more than 15 years of
experience in IT

Integration with leading vendors

 **RECFACES**



 Dubai Internet City Building 3,
Dubai, UAE

 www.recfaces.com
 sales@recfaces.com
 +971 4 8368339