



We are happy to provide you with a wide range of communication means to get in contact with us:

www.recfaces.com

+971 4 8368339

sales@recfaces.com

ID-LOGON USE CASES

Id-Logon is a software product for facial biometric authentication of users in information systems

Id-Logon allows performing secure and convenient password-free facial biometric authentication of users to grant access to various corporate information systems. The solution also provides periodical status checking of the user in front of the client device at the moment, in order to determine possible scenarios of limiting access and informing the responsible information security office about violations.

WHAT DOES THE USER GET?

- Secure biometric authentication of users in various corporate information systems
- Convenient password-free authentication using the users' biometric data
- Additional two-factor authentication mode: biometric data and PIN code / password
- Periodical presence checks of the user in front of the client device
- Performing various scenarios of access restriction and notifying information security office in case of the user status mismatch
- Prompt notification of information security service if more than one person works with the client device
- Timely processing of requests from corporate information systems and DLP systems on the user's biometric verification in case of performing significant operations or suspicion of a possible data breach
- Ready-made integration with Microsoft Active Directory, and possible integrations with other LDAP catalogs, such as Oracle Internet Directory, IBM Tivoli Directory Server



INSTALLATION TAKES 20 MINUTES

IN JUST 20 MINUTES YOU GET A READY-TO-USE PRODUCT WITH ALL THE NECESSARY FUNCTIONAL POSSIBILITIES

The Id-Logon solution is installed on the customer's computing infrastructure, while applications for authentication are installed on the client corporate devices. Corporate client devices of users are equipped with biometric data sensors: standard web cameras or specialized web cameras for increased system compromise control and obtaining biometric data in low-light conditions. The solution has an independent modern graphical interface.

Simple passwords and password-free authentication

One of the key problems faced by corporate information system security is weak or common passwords, the great majority of which has already been compromised. The penetration tests and account compromise by password guessing attacks are the most simple and fast attacks to hack the corporate system or get administrative privileges. The success rate of such attacks makes up to 85% of cases, including large corporations. Id-Logon password-free biometric authentication allows you to perform the procedure in the most secure and convenient way possible.

Password-free authentication and user convenience

Many employees fail to memorize frequently updated passwords set by strict password policies for corporate accounts, because of the requirements for the length of passwords and the presence of special characters in them (lowercase and uppercase letters, numbers, characters). As a result, employees do not find anything better than just to write down a new password and leave it next to their workplace. Thus, the strictest corporate password policy fails due to simple human inattention and negligence. Id-Logon provides password-free user authentication using individual biometric data. The solution uses built-in methods to effectively prevent compromise attempts made with photo or video materials. This ensures high level of protection from hacking attacks and timely informing the information security specialists about them. Thus, Id-Logon provides an increased level of authentication accuracy with simple and user-friendly procedure.

Two-factor authentication

Id-Logon additional security ensures that only you can access your account, even if someone else got your password. In addition to passwords or PIN codes, the system provides biometric verification of the user, which eliminates the possibility of using corporate information by a third party.

User presence check

After authorization, the user may leave the workplace for a while. Id-Logon is running in the background and repeatedly checks the status of the user who is in front of the client device screen after successful authorization. If Id-Logon does not detect the user in front of the client device, it increases the frequency of background biometric verification, and automatically blocks access after the specified period of time, if the user is absent.

If after successful authorization of a user, another employee or a third party starts working with the client device, the system informs the information security staff about the incident and can automatically block access to corporate information resources.

One workplace for one employee

Id-Logon allows you to restrict access rights to third parties while using client devices. Specifically, several employees cannot simultaneously be at the same client device. The solution running in the background automatically identifies it as a violation and blocks access to corporate information resources. Access rights are defined by the system administrator, and for this purpose Id-Logon has flexible settings that allow using a role model. Employees are registered in the biometric profile database and then linked to specific client devices.

Mobility

Id-Logon allows identification and verification of users when using mobile devices such as smartphones or tablet computers. This is particularly important for companies whose employees work remotely with no fixed workplace. Id-Logon provides authentication of a mobile device to be authenticated, grants or denies access to the device or to a specific corporate application. At the same time, the information security service receives information about the authenticated user of the mobile device, thus providing a higher level of the corporate data security.

Analytics and reporting

Id-Logon can create reports on results of the user authentication to corporate information resources and violations committed when working with them. For instance, you can view the number and statistics of violations by a set of client devices of interest, as well as get detailed information on the authentication violations parameters or the use of corporate resources for a specific violation. The filters provided in the system allow you to promptly and conveniently generate a report on a set of parameters of interest.

User verification by DLP request

The joint work of DLP systems and Id-Logon allows you to perform background user verification at the request of the DLP system in case of suspicious actions, as well as while performing a specified list of operations in corporate information systems. In case of a request from a corporate information system or DLP systems, Id-Logon verifies the authorized user, and also informs about the presence of other employees or unauthorized persons.

Identity verification prior to significant transactions

Id-Logon launches active verification (verification window) of the user to confirm the identity prior to the operation for a given set of significant actions in corporate information systems. This mode allows you to make sure that an authorized employee is performing the action, as well as save a verification log for such actions.

Open API

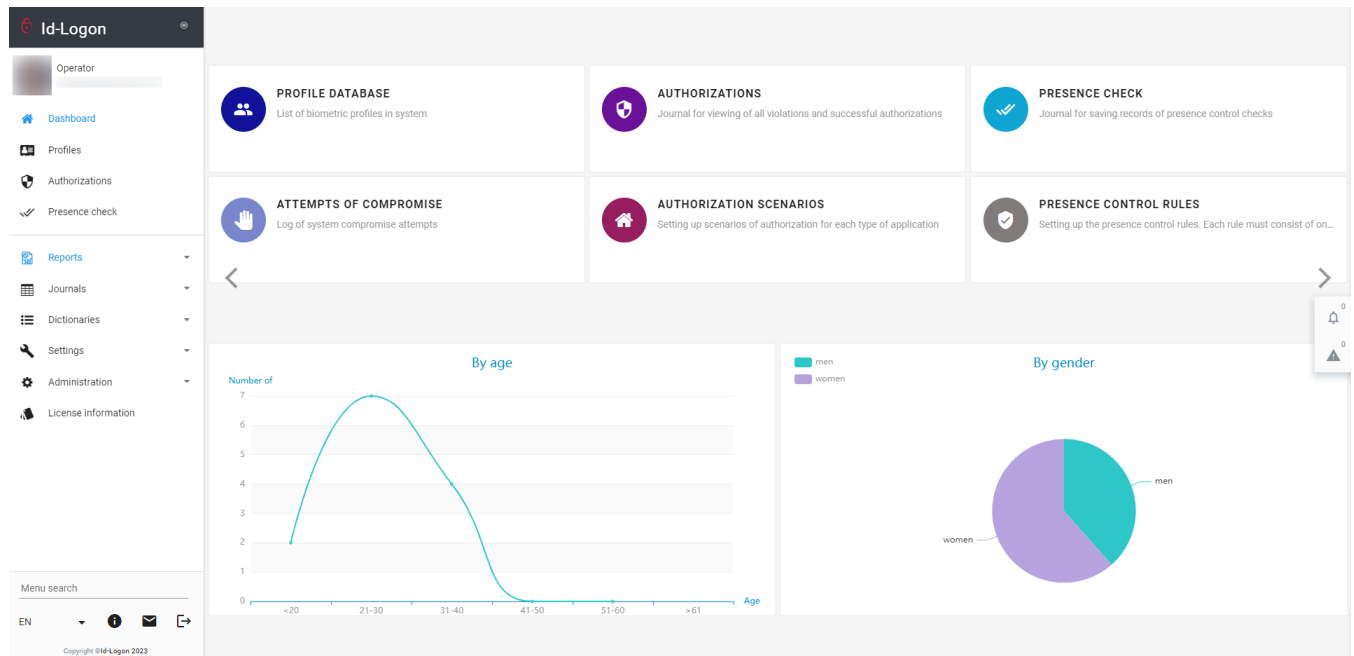
Id-Logon can be easily integrated with various external information systems using an open API.

Using several biometric solutions for security boost

The RecFaces portfolio includes Id-Gate, a specialized solution for access control and management systems that receives and stores personalized information about the employee's arrival to the company or departure. The joint use of Id-Logon and Id-Gate solutions allows you to control the authentication of employees in information systems, as well as to notify security about authentication attempts of the user who is not in the base of access control and management system.

EXAMPLE OF THE ID-LOGON INTERFACE

Id-Logon dashboard



Id-Logon profile database

The Id-Logon profile database interface allows for searching and filtering profiles. The top section includes search and filter options:

- Profile search**: Select a list (All)
- Portraits in profile**: All
- Profile activity**: Profile activity
- Creation date and time, from**: Creation date and time, to

Below these options is a table of profiles, filtered by photo. The table has the following columns: Full name, Gender, Age, Phone number, and Email. The table displays 12 profiles, with the first 10 visible in the screenshot. The bottom of the table shows a total of 12 profiles and a pagination control.

Full name	Gender	Age	Phone number	Email
[Profile 1]	F	22		
[Profile 2]	F	27		
[Profile 3]	F	20		
[Profile 4]	F	25		
[Profile 5]	F	26		
[Profile 6]	F	21		
[Profile 7]	M	37		
[Profile 8]	M	27		
[Profile 9]	M	37		
[Profile 10]				
[Profile 11]				
[Profile 12]				

Total: 12

“Intruder detection” report

Id-Logon

Operator

Dashboard

Profiles

Authorizations

Presence check

Reports

Reports storage

Authorizations

Presence control

Absence from work statist...

Unpassed checks

Intruder detection

Video

Journals

Dictionaries

Settings

Menu search

EN

Intruder detection

From date and time To date and time Full name Camera Device Type of violation Department

List

Camera photo	Profile photo	Full name	Date and time	Department	In lists	Device	Camera	Type of violation
			02.05.2023 18:34:08			DEPLOYM-VAHLNOG	DEPLOYM-VAHLNOG	No unknown people
			02.05.2023 18:29:22	Biometry department		DEPLOYM-VAHLNOG	DEPLOYM-VAHLNOG	No unknown people
			02.05.2023 18:18:29	Biometry department		DEPLOYM-VAHLNOG	DEPLOYM-VAHLNOG	No unknown people
			02.05.2023 18:11:50			DEPLOYM-VAHLNOG	DEPLOYM-VAHLNOG	No unknown people
			02.05.2023 18:08:00	Biometry department		DEPLOYM-VAHLNOG	DEPLOYM-VAHLNOG	No unknown people
			02.05.2023 18:06:52	Biometry department		DEPLOYM-VAHLNOG	DEPLOYM-VAHLNOG	No unknown people
			02.05.2023 18:05:34	Biometry department		DEPLOYM-VAHLNOG	DEPLOYM-VAHLNOG	No unknown people
			02.05.2023 17:47:49	Biometry department		DEPLOYM-VAHLNOG	DEPLOYM-VAHLNOG	No unknown people
			02.05.2023 17:47:33	Biometry department		DEPLOYM-VAHLNOG	DEPLOYM-VAHLNOG	No unknown people

Total: 59

Authorization journal

Id-Logon

Operator

Dashboard

Profiles

Authorizations

Presence check

Reports

Journals

My notifications

Duplicate profiles

Authorizations

Intrusion attempts

Locked devices

Presence control

Video

Photo import

Menu search

EN

Authorization journal / Authorization of 07.07.2023 14:03:53

General information

Start date and time
07.07.2023 14:03:00

Full name

Position

Subdivision
Biometry department

Date and time of the end of the check
07.07.2023 14:04:00

Login
user

Camera
Demo-Pc

Result

Account type
Group

Login
user

Authorization type
Operating system

Current step
Facial verification

Failed steps
0

List
Employees

Device
Demo-Pc

Steps passed
2

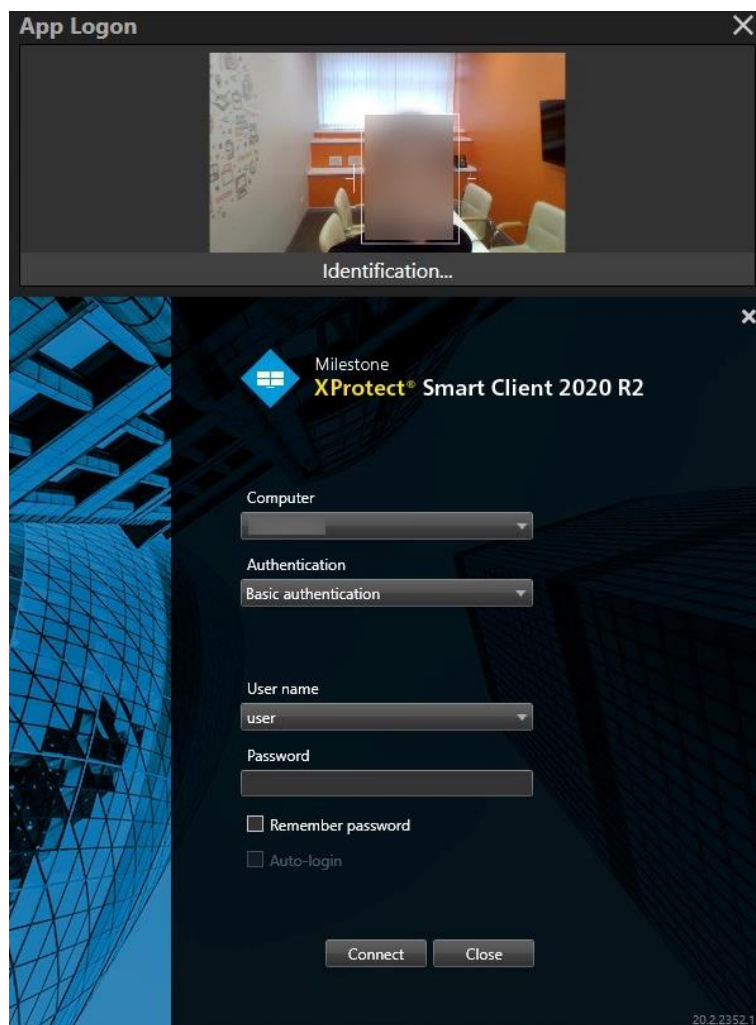
Status
Completed

Authorization photo

Profile photo

[Go to profile](#)

Id-Logon integrated in the Milestone XProtect interface





BANKS AND FINANCIAL INSTITUTIONS

USE CASE:

The development of cyberattack methods and the importance and sensitivity of the information circulating in the banking sector require banks to introduce new and improve existing information security systems.

Continuous expansion and improvement of legislation standards in banking information security are connected to the fact that banks carry out various actions and operate in different areas that require appropriate information security tools.

With the help of biometric technologies, the Id-Logon system ensures secure and convenient biometric authentication of bank employees in corporate information systems, controls the presence of bank employees at their workplaces, restricts access to information resources in the absence of employees at their workplaces, and provides biometric confirmation of significant transactions.

- Secure biometric authentication of bank employees in various corporate information systems
- Convenient password-free authentication using the users' biometric data
- Additional two-factor authentication mode: biometric data and PIN code / password
- Periodical presence checks of the user in front of the client device
- Performing various scenarios of access restriction to bank's corporate information and notifying information security office in case of the user status mismatch
- Prompt notification of information security service if more than one person works with the client device
- Timely processing of requests from corporate information systems and DLP systems on the user's biometric verification in case of performing significant operations or suspicion of a possible data breach
- Ready-made integration with Microsoft Active Directory, and possible integrations with other LDAP catalogs, such as Oracle Internet Directory, IBM Tivoli Directory Server
- Additional check of the employee's arrival time to the company while performing authentication in informational systems. It may be implemented by Id-Logon interaction with Id-Gate, a software product that enriches access control systems with biometric functionality.

ENERGY SECTOR

USE CASE:

The energy sector belongs to those strategic industries where the availability of special measures for ensuring information security is essential. While for administrative departments it is enough to have standard information security tools, technological areas of energy generation and delivery to end-users require an increased level of protection.

The importance of information security in the energy sector is determined by the possible cyberattack impact. Not only does it result in the significant material damage and reputational costs, but also in the harm to the population health, disruption of the city or region infrastructure. Insufficient attention to user authentication issues in corporate and technological systems of energy enterprises provides additional risks of cyber threats.

The absence of a control room specialist can also result in a full-fledged accident in the event of an emergency. The Id-Logon system uses biometric technologies to provide secure and convenient biometric authentication of fuel-energy complex enterprise employees in corporate information systems, track the presence of an employee at the workplace, inform about their absence for a long time, and restrict access to information resources of the enterprise if the employee is not at the workplace.

- Secure biometric authentication of users in various corporate information systems
- Convenient password-free authentication using the users' biometric data
- Additional two-factor authentication mode: biometric data and PIN code / password
- Periodical presence checks of the user in front of the client device
- Performing various scenarios of access restriction and notifying information security office in case of the user status mismatch
- Prompt notification of information security service if more than one person works with the client device
- Timely processing of requests from corporate information systems and DLP systems on the user's biometric verification in case of performing significant operations or suspicion of a possible data breach
- Ready-made integration with Microsoft Active Directory, and possible integrations with other LDAP catalogs, such as Oracle Internet Directory, IBM Tivoli Directory Server
- Additional check of the employee's arrival time to the company while performing authentication in informational systems. It may be implemented by Id-Logon interaction with Id-Gate, a software product that enriches access control systems with biometric functionality.

INDUSTRIAL FACILITIES

USE CASE:

The security of industrial enterprises is one of the pillars of national security. It is crucial to control the presence of employees at the workplace of industrial enterprises (central technological points, control rooms, security posts).

The absence of an operator or security officer at such facilities as nuclear power plants, thermal and hydroelectric power plants, and industrial plants can lead to a disaster.

Therefore, it is extremely important to track the employee's presence at the workplace.

With the help of biometric technologies, the Id-Logon system provides presence control of an employee at the workplace, and also restricts unauthorized persons.

- Secure biometric authentication of users in various corporate information systems
- Convenient password-free authentication using the users' biometric data
- Additional two-factor authentication mode: biometric data and PIN code / password
- Periodical presence checks of the user in front of the client device
- Performing various scenarios of access restriction and notifying information security office in case of the user status mismatch
- Prompt notification of information security service if more than one person works with the client device
- Timely processing of requests from corporate information systems and DLP systems about the user's biometric verification in case of performing significant operations or suspicion of a possible data breach
- Ready-made integration with Microsoft Active Directory, and possible integrations with other LDAP catalogs, such as Oracle Internet Directory, IBM Tivoli Directory Server
- Additional check of the employee's arrival time to the company while performing authentication in informational systems. It may be implemented by Id-Logon interaction with Id-Gate, a software product that enriches access control systems with biometric functionality.

LICENSING POLICY

The **Id-Logon** system is a complete software product and is distributed by transferring electronic license keys. Such keys are required for the core element of the Id-Logon system, as well as for a number of connected user workplaces.

User workplace license



License for the Id-Logon system core element and user workplaces

Technical support



1. Dealing with emergencies during the Id-Logon system operation
2. Providing Id-Logon updates and documentation
3. Consultations while setting up and configuring the solution