RECFACES

ID-LOGON

TECHNICAL DESCRIPTION

IDLG.TI.DOC.990

CONTENTS

1 INTRODUCTION (PURPOSE)

The Id-Logon system (hereinafter referred to as the “System”) is developed to ensure biometric access control in operating and information systems.

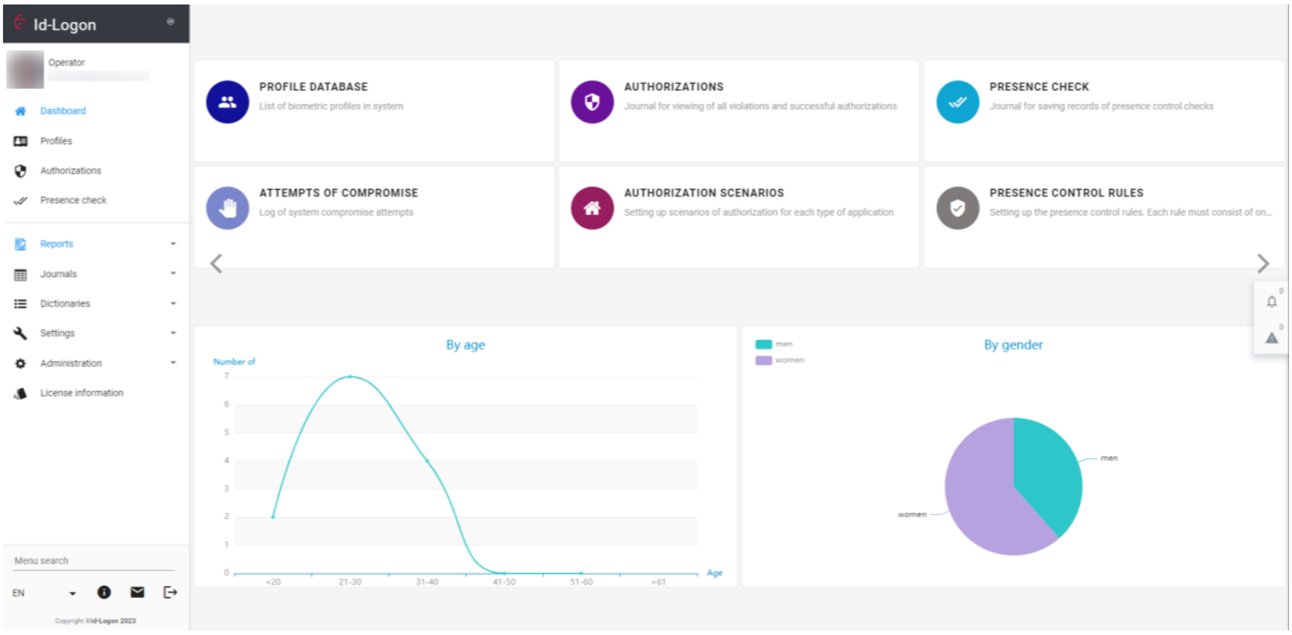
The System is intended to check access rights when logging into systems with the help of biometric identification and verification and ensures that the data on a person in front of a computer is reliable. Granting access to operating and informational systems by biometric authentication eliminates the risk of spoofing user data.

A person is identified via web cameras or scanners connected to a computer by capturing biometric data of a person. Then, Id-Logon checks if the obtained biometric samples correspond to the data in the profile database. As a result, a person is either granted access to the system, or the access is denied.

Access verification is provided with biometrics and password input.

The System is designed for:

- 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 a 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.



PROFILE DATABASE
List of biometric profiles in system

AUTHORIZATIONS
Journal for viewing of all violations and successful authorizations

PRESENCE CHECK
Journal for saving records of presence control checks

ATTEMPTS OF COMPROMISE
Log of system compromise attempts

AUTHORIZATION SCENARIOS
Setting up scenarios of authorization for each type of application

PRESENCE CONTROL RULES
Setting up the presence control rules. Each rule must consist of on...

Figure 1. System dashboard

2 SOFTWARE DESCRIPTION

2.1 SYSTEM COMPONENTS

For the correct functioning of the System, the following minimal set of equipment is required:

- Server for the System Core
- Server(-s) for video preprocessing (if necessary)
- Client PC
- Cameras
- Network switches to provide data transmission between the System components

The detailed description of the equipment recommended characteristics is indicated below.

2.2 ARCHITECTURE

The System consists of the following components:

- **Id-Logon Core** — the server part of the System, consisting of separate services, including the System settings interface, recognition algorithms, database and reports.
- **Id-Logon Tracker** — video preprocessing server.
- **WinLogon** — a client application for Windows providing biometric authentication for access to the Windows operating system.
- **AppLogon** — a client application for Windows providing biometric authentication for access to applications and information systems.
- **UserControl** — a client application for Windows providing biometric control of presence and other rules of being at a PC.

The System can be integrated with:

- **Active Directory (LDAP)**, using the adapter that is supplied along with the System

2.3 SOLUTION ORGANIZATION SCHEME

2.3.1 GENERAL SCHEME

The System provides authentication in an operating system or a corporate application with local or domain credentials and a local webcam. It also ensures each employee presence in front of a computer with a webcam or controls presence of a group of employees with an IP-camera (**Figure 2**).

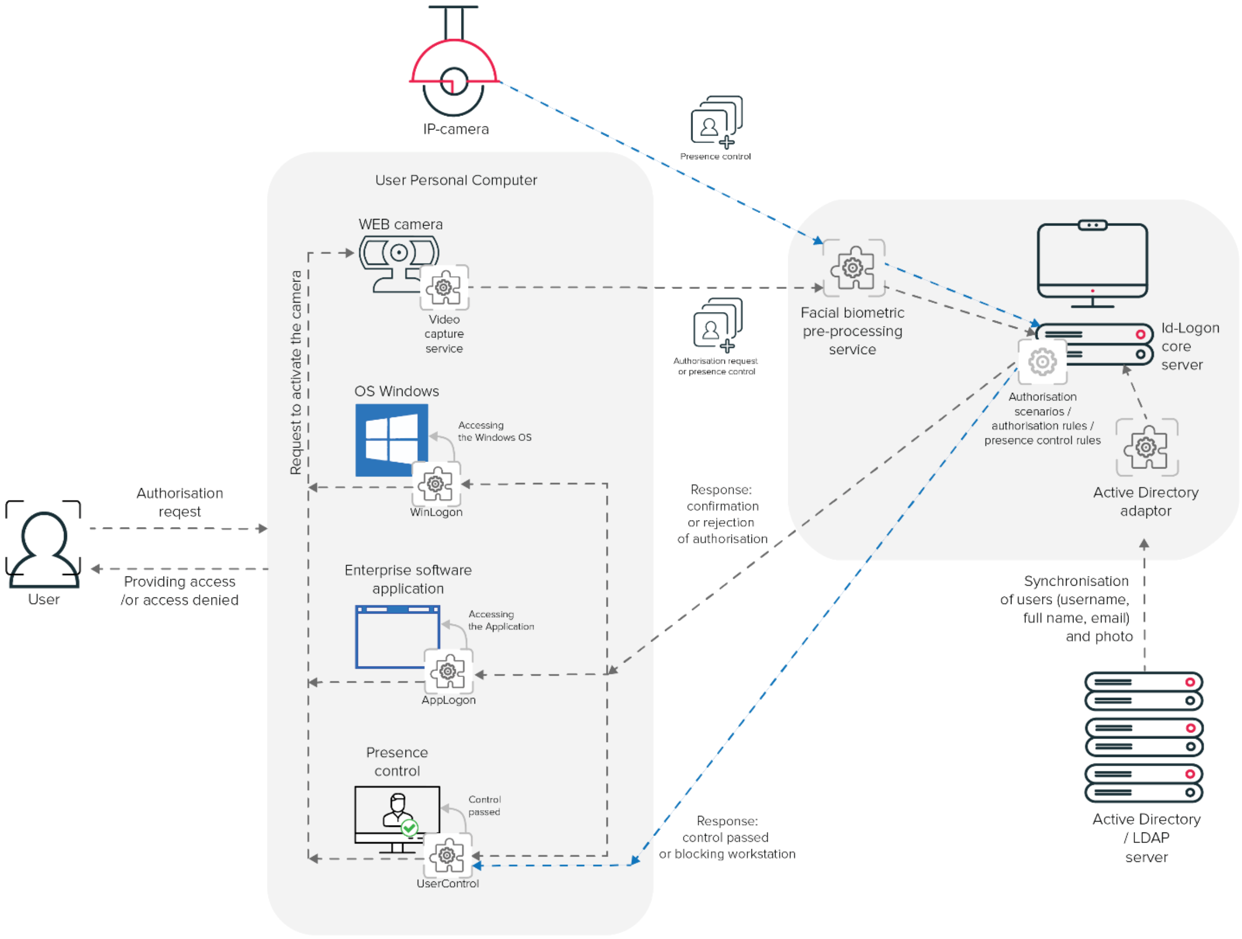


Figure 2. General scheme of Id-Logon system deployment

To enable the corresponding functionalities, the following applications supplied along with Id-Logon should be installed on the client local PC:

- **WinLogon** — an application for authentication in Windows OS.
- **AppLogon** — an application for authentication in corporate information system and specialized applications.
- **UserControl** — an application that ensures presence control and other rules of being at PC. UserControl can automatically block PC in any rule violation occurs.

2.3.2 SOLUTION FOR USER AUTHENTICATION IN WINDOWS VIA WINLOGON

The WinLogon client application provides biometric authentication to access Windows OS.

The Solution deployment scheme is the following (**Figure 3**):

- In accordance with its settings, the WinLogon app initiates a request to activate a webcam.
- Data from the camera video stream is captured (depending on the settings) by the video capture service and transmitted to the video preprocessing service, where it is preprocessed using the processor power of the client PC.
- The processed photos and biometric templates are sent to the Id-Logon Core server, where identification and/or verification of the user is performed.
- On the basis of the identification result and configured authorization scripts, the System grants or denies access and returns a response to the client PC.
- Based on the received response, the service grants access or denies user request to log in to Windows.

With a special adapter, the Core server can be integrated with Active Directory (LDAP), which becomes the primary source of information about users, their access rights, access lists and photos. On the basis of this information, Id-Logon fills both the profile database and the various directories that determine access to the systems.

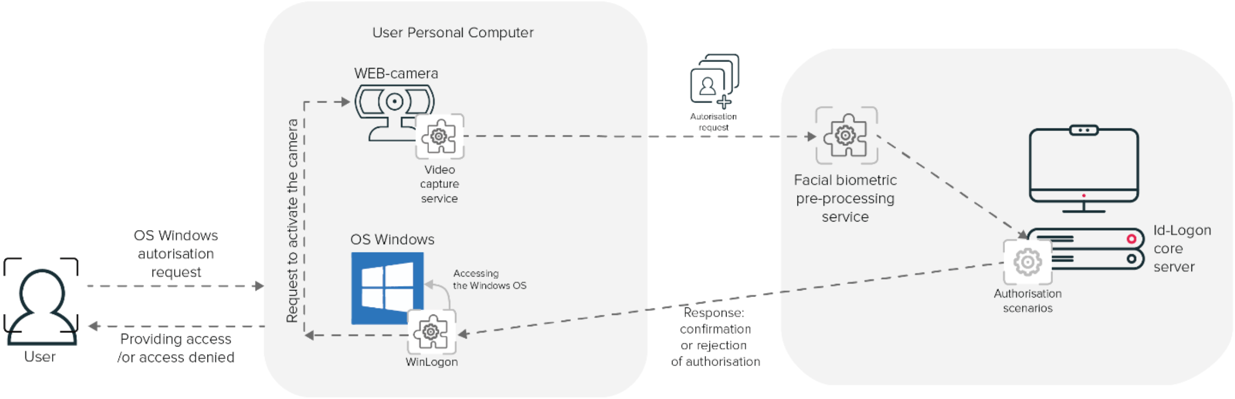

User Personal Computer
WEB-camera
Request to activate the camera
Video capture service
Autorisation request
Facial biometric pre-processing service
Id-Logon core server
Authorisation scenarios
OS Windows
Accessing the Windows OS
WinLogon
Response: confirmation or rejection of authorisation
OS Windows autorisation request
Providing access /or access denied
User

Figure 3. Solution deployment scheme for user authentication in Windows OS

2.3.3 SOLUTION FOR USER AUTHENTICATION IN CORPORATE APP VIA APPLOGON

The AppLogon client application provides biometric authentication in one or several apps specified in the system settings.

In this case, the deployment scheme of the Solution is almost identical to the above-mentioned scheme of user authentication with the WinLogon application (**Figure 4**):

- In accordance with its settings, the AppLogon app initiates a request to activate a webcam.
- Data from the camera video stream is captured (depending on the settings) by the video capture service and transmitted to the video preprocessing service, where it is preprocessed using the processor power of the client PC.
- The processed photos and biometric templates are sent to the Id-Logon Core server, where identification and/or verification of the user is performed.
- On the basis of the identification result and configured authorization scripts, the System grants or denies access and returns a response to the client PC.
- Based on the received response, the service grants access or denies user request to log in to corporate app.

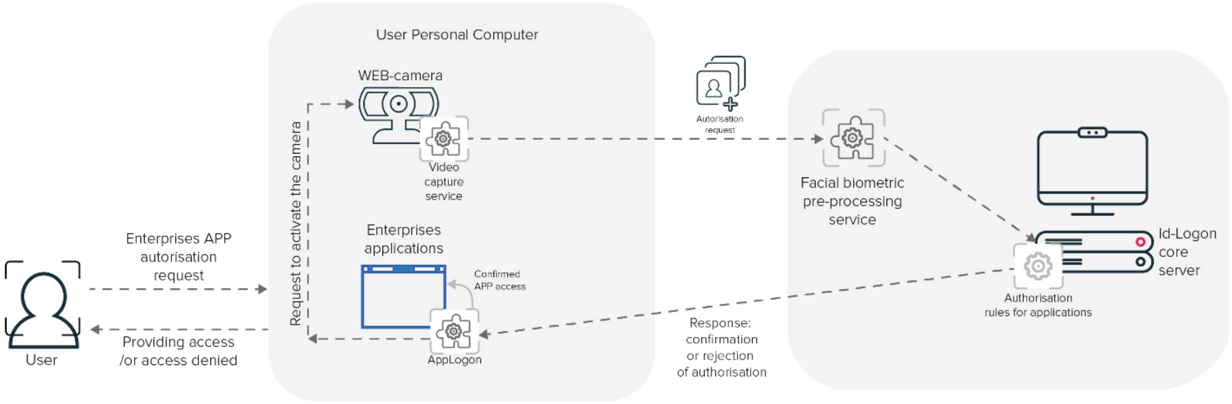

User Personal Computer
WEB-camera
Video capture service
Request to activate the camera
Enterprises applications
Confirmed APP access
AppLogon
Enterprises APP autorisation request
Providing access /or access denied
User
Autorisation request
Facial biometric pre-processing service
Id-Logon core server
Authorisation rules for applications
Response: confirmation or rejection of authorisation

Figure 4. Solution deployment scheme for user authentication in a chosen app

2.3.4 SOLUTION FOR PRESENCE CONTROL VIA USERCONTROL

The UserControl client application provides biometric control of presence/absence of an employee at the workplace, as well as presence of unauthorized persons in front of the computer (**Figure 5**).

The operation scheme of the solution with UserControl is the following:

- In accordance with its settings, the UserControl app initiates a request to activate a webcam.
- Data from the camera video stream is captured (depending on the settings) by the video capture service and transmitted to the video preprocessing service, where it is preprocessed using the processor power of the client PC.
- The processed photos and biometric templates are sent to the Id-Logon Core server, where identification and/or verification of the user is performed.
- On the basis of the identification result and configured authorization scripts, the System returns a response to the client PC.
- Based on the received response, the service records a passed check in the presence check log or blocks access in case of violation of control rules.

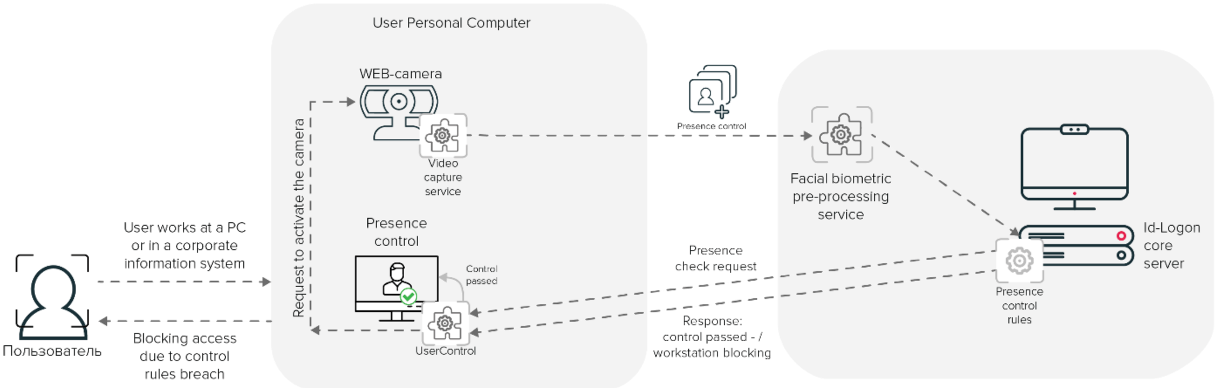

User Personal Computer
WEB-camera
Video capture service
Request to activate the camera
Presence control
Control passed
UserControl
User works at a PC or in a corporate information system
Пользователь
Blocking access due to control rules breach
Presence control
Facial biometric pre-processing service
Presence check request
Response: control passed - / workstation blocking
Id-Logon core server
Presence control rules

Figure 5. Solution deployment scheme for presence control via UserControl

2.3.5 SOLUTION FOR PRESENCE CONTROL WITH IP CAMERA

If the employee workplaces are not equipped with web cameras, it is possible to install one IP camera to control presence of a group of persons. In this case, the UserControl service must be installed on each computer (**Figure 6**).

The operation scheme of such a solution is the following:

- In accordance with its settings, the UserControl app initiates a request for an IP camera to capture data.
- Data from the camera video stream is transmitted to the video preprocessing service, where it is preprocessed using the processor power of the client PC.
- The processed photos and biometric templates are sent to the Id-Logon Core server, where identification and/or verification of the user is performed.
- On the basis of the identification result and configured authorization scripts, the System returns a response to the client PC.
- Based on the received response, the service records a passed check in the presence check log or blocks access in case of violation of control rules.

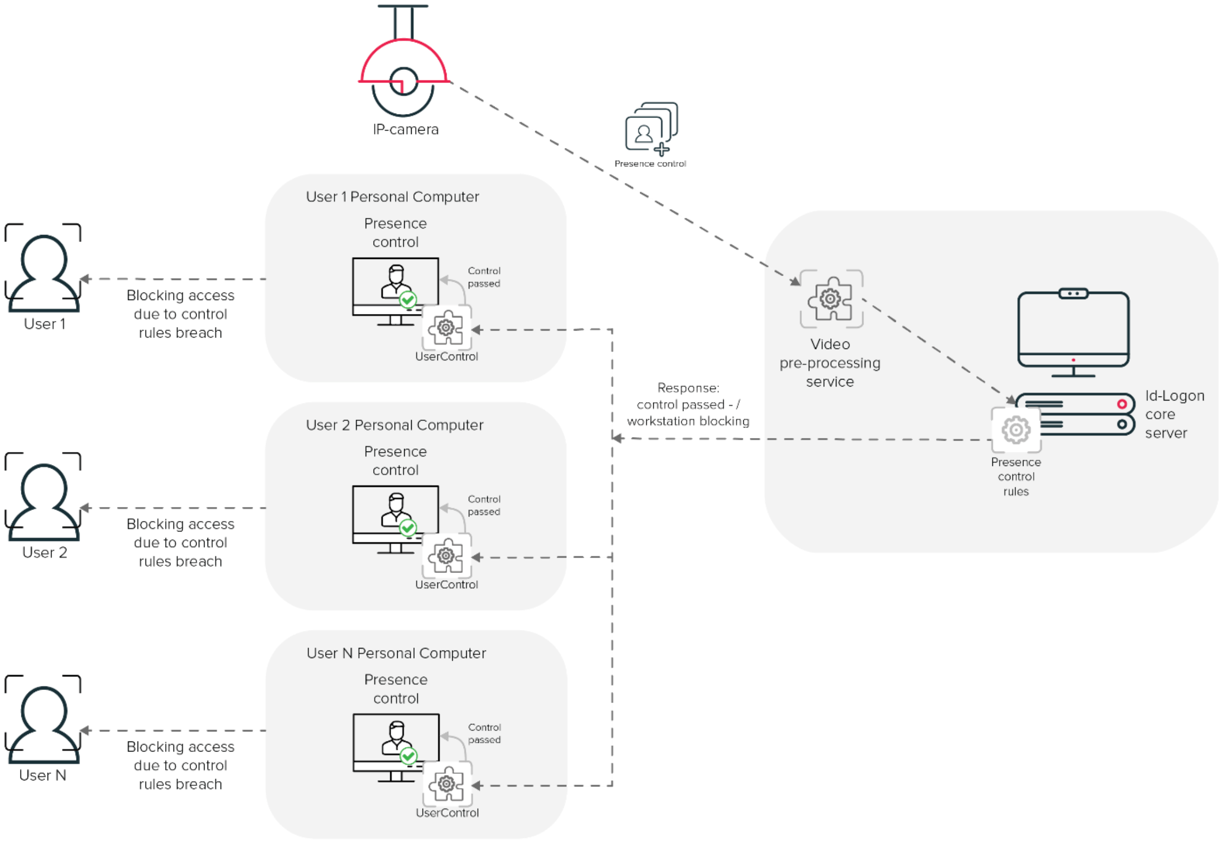


Figure 6. Solution deployment scheme for presence control with IP camera

2.4 TECHNOLOGIES

The system is developed with the use of the following programming languages:

- Golang
- C#
- AngularJS
- RabbitMQ
- Nginx
- PostgreSQL
- Redis

2.5 LIST OF ID-LOGON CORE SERVICES

Id-Logon Core includes the following services:

Table 1. Id-Logon Core services description

Service	Description	Port
mauth-win-logon	Client application for Windows authentication	None
mauth-client-app-config	Service for client settings	None
Nginx	A web server and mail proxy server	80, 443, 23231
PostgreSQL	Free and open-source relational database management system (RDBMS)	5432
RabbitMQ	Service providing work with data queues	5672, 15672
Redis	Open-source software for managing NoSQL databases	6379
mkvz-tracker	Service for preprocessing video stream (tracker)	8001
mkvz-launcher	Service for managing client applications	8876
mkv-server-report	Service for generating reports: includes reports by gender, age, visits, etc.	11084
mu-server-api	Notification service	11090
support-server-api	Service for system maintenance	11091
mkv-server-url-shortener	URL shortening service	11092
mas-server-api	Management service, which provides API for processing data about devices, applications, cameras	11101
mas-server-settings	Service for storing configuration settings and sending them to the modules	11102
mauth-server-api	Service for managing authentications in Windows and applications	11200
mauth-server-report	Service for generating reports on user biometric authentication	11201
user-control-server-api	Service for controlling of the user presence at their workplace	11202
user-control-server-report	Service for generating reports on user presence control	11203
mpdn-secret-vault-api	Service for storing personal data	11204
mfs-server-api	Service for storing and working with images	11300
mfs-server-thumbnail	Service for working with thumbnails of the file storage	11301
fs-server-api	File storage service	11302

mi-sender-email	Service for sending e-mail notifications	11400
mi-sender-http	Service for sending notifications by http (push)	11401
mi-sender-smsmodem	Service for sending SMS with a USB gsm modem	11402
mi-server-api	Service for implementing API functions to work with services	11403
mi-sender-telegram	Service for sending SMS to Telegram	11404
mi-controller-acs	Service for integration with external systems and request routing between them	11406
mi-controller-idm	Service for integration with external IDM systems and sending requests to corresponding adapters	11407
mi-adapter-idm-ad	Service of integration adapter with Active Directory	11431
mkv-server-admin	User interface for the System administration module	11500
mkv-server-api	The service contains API methods to work with the main functionality of the System	11501
mkv-server-auth	Service for authorization in the System by entering a username and password	11502
mkv-server-ws	Application back-end for working with the client via WebSocket	11503
backup-client-server-api	System data backup service	11506
logging-server-api	Service is used to get logs from services	11509
event-configuration-api	Service for simplifying working with event storage, so that a single request creates a pool of necessary entries in the dictionaries for event processing	11510
event-storage-server-api	Service for processing System events and performing various actions depending on the type of event	11511
mkv-client-profiles-import	Service for importing profiles into the System	11514
mas-meta-server-api	Meta information service	11515
monitoring-server-api	Services for monitoring statuses of the running services	11517
statistics-server-api	Service for recording statistics on the System operation	11518
audit-server-api	Auditing and logging service	11521
mkv-server-auth-ldap	Service for authorization in the System via LDAP/AD	11522
mkvz-onvif-cameras	Service for searching and connecting cameras supporting ONVIF protocol	11550
mas-server-report	Report service for MAS	11553
mie-export-api	Service for exporting customized data sets from CSV	11555
mie-import-api	Service for importing customized data sets to CSV	11556
logging-server-siem	Service for SIEM logging	11557
mmpd	Service for managing detecting processes	11600
compromise-server-api	Service for compromise control	11605
modi-image-worker	Service for processing photos (crop, resize, etc.)	11700
modi-server-api	Service for processing discrete images	11701
modi-ubda-tevian-[01-04]	Service for processing photos: searching faces and creating biometric templates	11710 y [01], 11711 y [02], 11712 y [03], 11713 y [04]

mrp-server-api	Service that provides API for processing data during working with the streaming video	11800
mrp-server-ubt-broker	Service for UBT proxying to other systems	11801
mrp-matching-tevian-go	Matching service for the Tevian engine	11806
mrp-server-broker	Service managing a request queue to the matching algorithms	11821
mrp-server-image-broker	Service for image distribution among trackers	11822
ms-server-filecache	Service providing file caching	11900
mkv-scheduler-api	Service that implements working with scheduled tasks	11910
video-restreamer-server	Server for video restreaming	40000, 40001

One of the server requirements for installing the Id-Logon Core software package is the absence on the server of the software specified in the table above and the presence of free ports indicated in the table.

3 REQUIREMENTS FOR CORRECT WORK

3.1 ID-LOGON SERVER

It is recommended to install the Id-Logon Core on the server. Server characteristics directly depend on the number of cameras processed by the System. An approximate calculation for the most common values is presented in the table below.

Table 2. Server requirements

Number of cameras	CPU (Core)	RAM (GB)	HDD (GB)	SSD (GB)
1	5	16	600	240
2	6	16	700	240
3	8	16	700	240
5	10	32	800	240
7	14	32	900	240
10	18	64	1000	240

Operating System: Windows 10 Pro (2004 and later, according to the end date of the operating system support), Windows Server 2016/2019 and later. If you have the “Windows 10 Pro N” OS edition installed, you have to additionally install the “Media Feature Pack” component. The account (login/password) (including for a remote user) must remain unchanged throughout the installation. The account (login/password) must allow upgrading privileges to Administrator if necessary.

The following components **must not** be pre-installed on the server:

- PostgreSQL
- RabbitMQ
- Redis
- Web server that uses ports 80 and 443

3.2 RECOMMENDATIONS ON CAMERAS

3.2.1 CAMERA SELECTION

Cameras must have the following characteristics:

- image resolution: 720p and higher
- video stream frame rate: 25 fps and higher
- viewing angle: at least 65 degrees; 75 degrees and higher is recommended
- IR illumination (optional)
- focus: fixed/autofocus
- **without** fisheye effect
- 16:9 aspect ratio

To ensure natural skin color capturing, the color temperature of lighting must be between 4,800 and 6,500 and be uniform, i.e. illuminate an entire area at the same level. The required color temperature is provided by fluorescent or LED lights.

The light sources in the facial area must create illumination of:

- at least 300 lux for cameras without automatic illumination correction
- at least 100 lux for cameras with automatic illumination correction

3.2.2 CAMERA INSTALLATION

For receiving accurate facial biometric data, you should fulfill the following conditions (**Figure 7**):

- The camera is placed at eye level.
- The employee looks directly into the camera, with face and shoulders squared to the camera.
- The face is evenly illuminated so that there are no shadows, glare, or areas of over illumination in the image.
- Only one face is present in the photo.
- The expression of the face is neutral (without smile), both eyes are normally open (not too wide) and clearly distinguishable (hair not covering eyes, mouth closed).
- There is no bright backlight, side light and shadows.
- The distance between pupils in the image is at least 120 pixels.

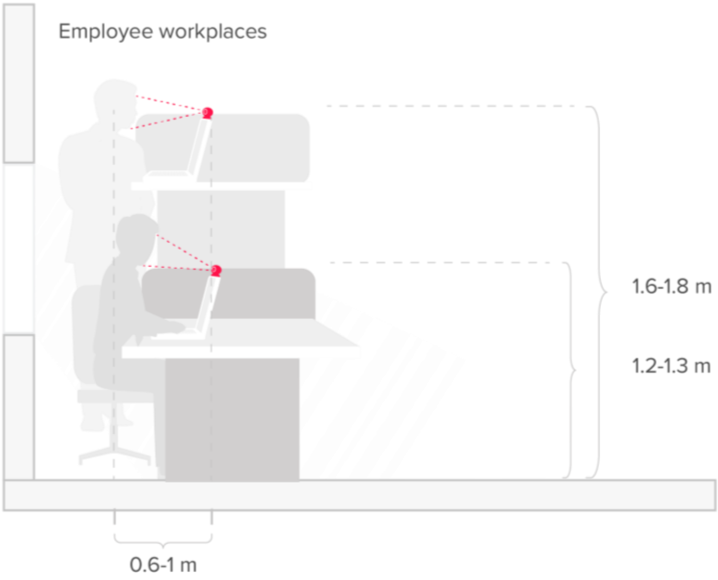


Figure 7. Recommendations on camera placement

4 LANGUAGE SUPPORT

The Id-Logon software is a multilingual solution that allows you to choose from the following language options:

- English (by default)
- Spanish

The list of available languages can be expanded upon request.

5 DOCUMENTATION LIST

- Id-Logon Administrator's Guide
- Id-Logon Operator's Guide
- WinLogon Application Installation and Configuration Guide
- AppLogon Application Installation and Configuration Guide
- UserControl Application Installation and Configuration Guide

6 SOFTWARE MANUFACTURER

RecFaces FZ-LLC

Address: Dubai Internet City Building 3, Dubai, UAE

Telephone: +971 4 8368339

E-mail:

- General questions: in@recfaces.com
- License and partner policy: sales@recfaces.com
- Technical support: id-logon@recfaces.com