

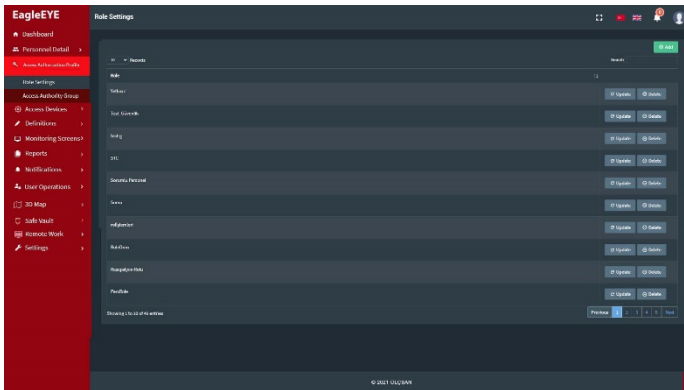
EagleEYE

Identity and Access Management

Identity and Access Management

Identity Management

Identity Management (IdM) is to ensure that the right users have access to the right resources at the right time, for the right purposes, in order to ensure computer and network traffic security. Fulfills the need for access to appropriate resources and compliance requirements. EagleEYE Identity Management module closes the user authentication vulnerability, which is one of the most important vulnerabilities in cyber security.

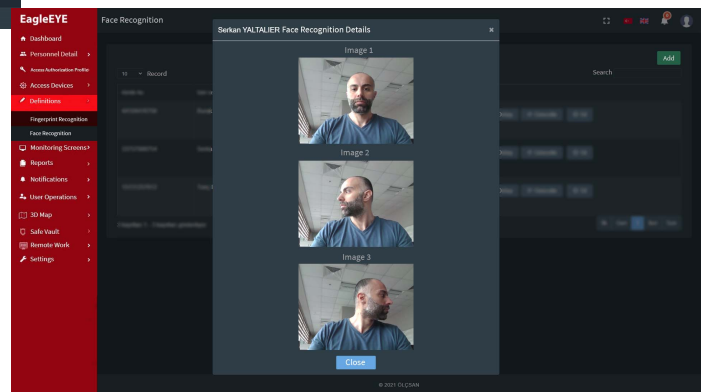


Access Tracking

Access tracking; It is the monitoring screen that shows the servers, clients and applications accessed by staff and all users in real time. The transactions made on the basis of the selected user are followed and examined. It checks for policy violations.

Strong Validation

Access to the computer is by face recognition. High security vitality verification is provided by finger biometrics and iris. All operations performed on the screen and the applications used are recorded. EagleEYE automatically closes the application or session when the screen is left unattended or an unauthorized person looks at the screen. Face recognition is done with face recognition software we have developed and any 3rd party camera (standard camera on a portable computer).



Features

- Identity access management with password, smart card and biometric data
- 2FA (2 factors), MFA (multi-factor) authentication
- Strong Authentication
- Windows login and Application Login with Biometrics
- LDAP Support (Open LDAP, MS Active Directory)
- Standard report and dynamic reporting, Multilingual Interface
- Identity and Card Management
- Biometric Device Registration and Management
- Security Policy Server, logging
- End-to-end secure communication (AES 256bit SSL)
- Real Time User Control (The screen turns off when the user leaves the PC)
- End-to-end secure messaging, file encryption, authentication and terminal authentication
- Real-time analysis and fraud detection

Advantages

- Ultimate Computer Security
- Wide range of hardware support
- User-friendly WEB-based Graphics Interface, Modern Design
- Online and offline work
- Certificate management
- Human resources integration
- Compliant with PDPA Circular
- Quick installation and use with ready-made profiles.
- Fast and efficient training program
- Cloud support
- Easy integration of 3rd party products
- Mobile device and tablet support

Technical support/ticket system

Sub Modules: Automation - Monitoring - Compliance - Recording - Workflow Validation - Role and Policy Management - Reports and Analysis.

Password Management

EagleEYE Password Management module is a secure vault application that securely stores and manages sensitive information such as passwords, documents and digital identities of employees' employees.

Password Management is a fast and secure solution for users to reset their passwords and/or open blocked accounts without assistance from the service desk in institutions. It supports multiple authentication methods and service desk integration, reducing the workload of IT teams and increasing security.



High Security

Users and system security is enhanced by Strong Authentication.

Transactions such as resetting passwords and opening blocked accounts are monitored and reported in real time. Automatically problem records are opened, updated and closed in the ticket system. All these processes are easily monitored and controlled with a browser-based interface.

No to Weak Password!

The majority of users have many different passwords. These passwords are written on a note paper on the computer or on the desk and/or stored in a file inside the computer. In applications that are constantly asked to change the password, it becomes very difficult to change the password after a while, the passwords are forgotten / confused and the need for support arises. It is a laborious process for both the user and the support team and causes a waste of time. A secure password cannot be created every time.



Features

- LDAP (Open LDAP, MSActive Directory), Soft Token, Okta, JWT, OIDC, RADIUS, GitHub Support
- 2FA (2 factors), MFA (multi factors) and Strong Authentication
- Standard report and dynamic reporting, Multilingual Interface
- Password synchronization.
- It reduces the passwords to the minimum number.
- Forces you to choose stronger passwords.
- Mobile device & biometrics usage (fingerprint, face, iris etc...)
- Desktop and Mobile Device support
- Security Policy Server, logging
- Microsoft CA and other certificate authority's support.
- End-to-end secure communication (AES 256bit SSL)

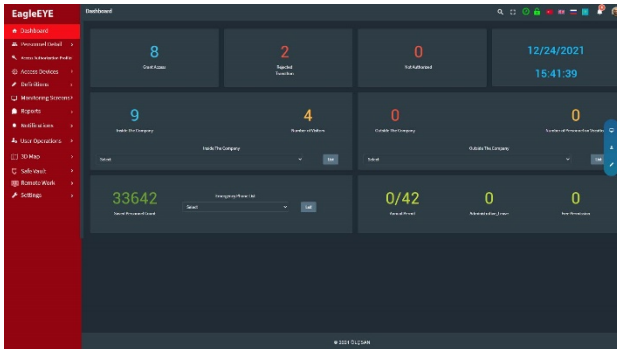
Advantages

- User-friendly WEB-based Graphics Interface, Modern Design
- Mobile phone and tablet support
- VPN integration
- Vitality check
- Online and offline work
- Fast and efficient training program
- Cloud support
- Easy integration of 3rd party products
- Technical support/ticket system
- Compliant with PDPA Circular

Sub Modules: Full and semi-automatic service – Monitoring – Integrated 2FA, MFA – Strong Authentication – Integrated Access

Privileged Access Management

EagleEYE Privileged Access module is one of the important digital workflow problems of institutions; accounts with high privileges that are shared among many people, static passwords that create security problems, passwords that are known by many people and who's responsible is not described, provide solutions to the problems caused by people who have left the institution and still have access. Eliminates password fatigue and security flaws by providing a secure, centralized vault for password storage and access. Increases IT efficiency by automating the frequent password changes required in critical systems. Provides preventive and detective security controls through approved workflows and real-time alerts for password access. Provides security controls and regulatory compliance.



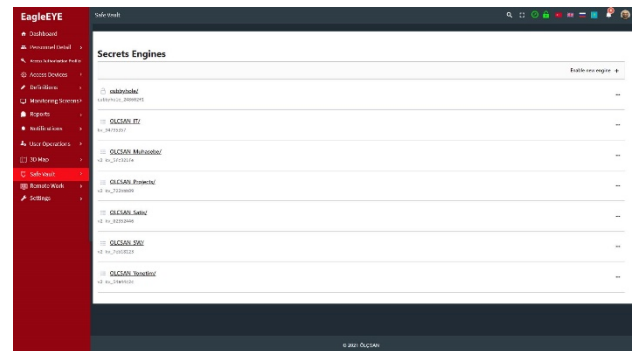
Safe Vault

It organizes all your privileged identities by storing them in a centralized vault. It allows you to securely share your passwords with members of your team on a need-based basis. It automatically resets the passwords of servers, databases, network devices and other resources.

Controls access to IT resources and applications based on roles and job responsibilities. Initiates direct connections to remote IT resources, websites and applications. Makes video recording and auditing of all privileged accounts, has a complete record of all actions.

Monitoring Screens

It is monitored / managed / controlled that which accounts the personnel use instantly, what changes are made, whether there is an abnormality in access, compliance with rules and policies, and whether security is in danger.



Features

- Easy and secure user identification.
- Strong, multi-factor authentication.
- Access authorization profiles for system administrators and other users.
- Access and session registration controls.
- LDAP Support (Open LDAP, MSActive Directory)
- Standard report and dynamic reporting, Multilingual Interface
- Mobile device & biometrics usage (fingerprint, face, iris etc...)
- Device and Application Management
- Security Policy Server, logging
- End-to-end secure communication (AES 256bit SSL)
- Real-time data replication, Geographical distribution.
- Active - active architecture.

Advantages

- Wide range of hardware support
- User-friendly WEB-based Graphics Interface, Modern Design
- VPN integration
- High security and redundant safe
- Mobile phone and tablet support
- Online and offline work
- Fast and efficient training program
- Cloud support
- Easy integration of 3rd party products
- Technical support/ticket system
- Compliant with PDPA Circulars.

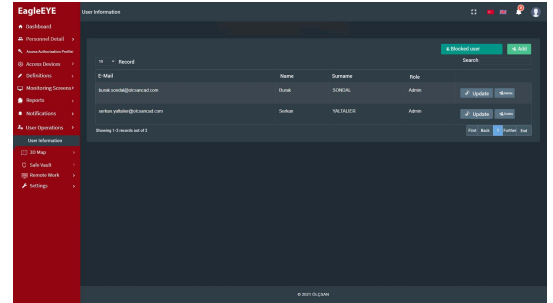
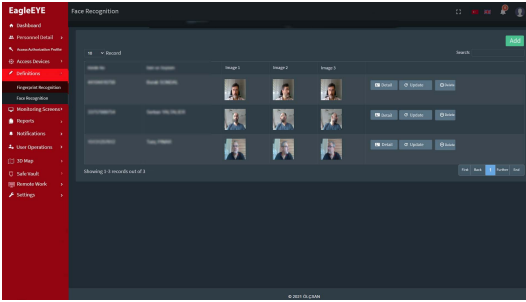
Sub modules: Password vault - Monitoring - Random and Automatic Password - Role and Policy Management - Strong authentication

Other Modules

EagleEYE provides the use and management of different processes from a single WEB-based panel.

Lifecycle

It is the module that performs the processes of authorization of personnel, cards, biometrics and applications, design, printing and personalization of cards, as well as certificate management of cards and applications.

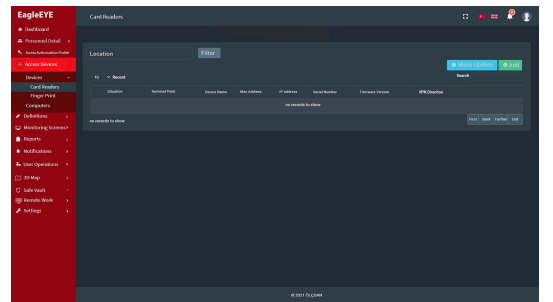
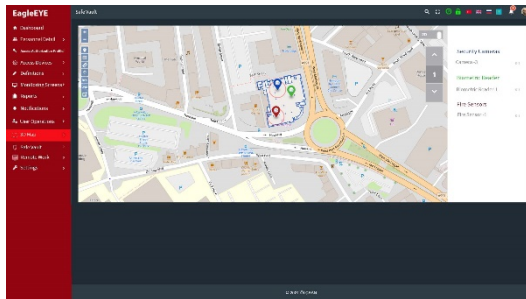


Remote work module

It is the module that provides general and one-time authorization of employees to work remotely, monitoring and approval of application and / or device usage times, and managing all these processes.

Terminal Management

It is the module that provides instant data tracking of the connected devices, whether they are operational, remote authorization of the devices, making their controls and managing the data going to the devices.

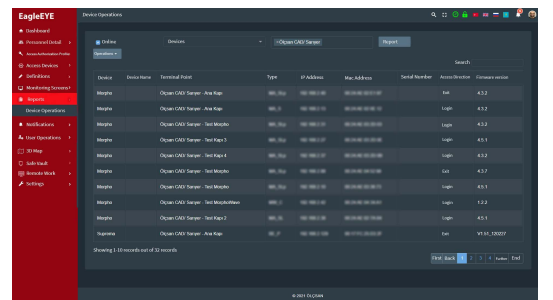
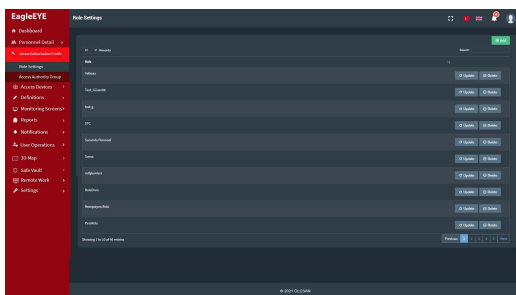


Map and Plan

It is the module where the campus where the institution is geographically located, the access points on the floor plans and the devices are displayed on a single screen.

Reports / Notifications

It is the module in which all detailed information in the system is reported together with the relevant breakdowns. The Notifications module manages the risky situations and reports that generate alarms to reach the relevant persons, and the sending of warning messages by e-mail.



Authorization Profile

It is the module that defines user authorizations on the system, determines and manages personnel and access authorizations. Unauthorized and unauthorized access is prevented through the module.

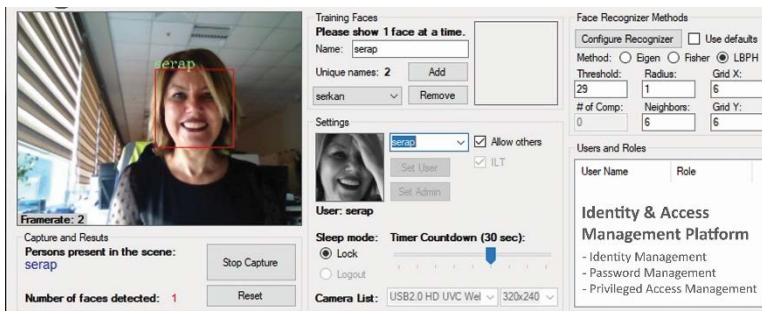
Powerful Biometric Verification

EagleEYE reflects its long years of security and biometrics experience to authentication modules. Weak passwords are vulnerable to vulnerabilities. User authentication and management, reinforced with biometric security, prevents the use of stolen user information, which is observed in 81% attack type, and the cracking of weak passwords.

As a member of the EAB European Biometrics Union, we follow all standards and apply them to our innovative products.

Few applications support multi-factor access (MFA). It is necessary to encourage/enforce strong authentication before automatic password reset.

1. All users are directed to use MFA and even required users to use SA (Strong Authentication). 2. Send PIN from phone / email. 3. With the smartphone application, both login via smartphones (using a factor we carry / own) are supported, and the smartphone is used as a biometric verification device (without using an additional device with our mobile biometric verification application). 4. Existing OTP systems can be integrated. 5. Fingerprint, contactless fingerprint, finger vein print, palm vein print, face and iris technologies are supported to eliminate 2FA security problems. 6. Strong validation (SA) is done by viability check.


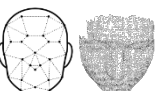






Face Tracking App

Authentication of people with a standard fingerprint scanner and/or WEB camera has weak points.

Standard fingerprint scanners and cameras do not have fake finger/photo detection capabilities.

EagleEYE biometric authentication components; It consists of facial recognition and tracking and other biometric comparison software, finger biometrics or iris scanners capable of fake finger and vitality detection, and a WEB camera.

 <p>Finger print</p>	<p>Fake fingerprint and liveness detection, encrypted template support, 19794-2/4 and custom templates...</p>	 <p>Face Recognition</p>	<p>2 and 3 dimensional face recognition algorithms. Vitality and fever measurement support, mask control.</p>	 <p>Iris Recognition</p>	<p>Live iris template support, iris and face fusion combined support.</p>
 <p>Contactless Fingerprint</p>	<p>Contactless 3D fingerprint. 4 fingers together and very fast...</p>	 <p>Finger Vein Print</p>	<p>Finger vein pattern, vitality recognition and fake finger detection. 10% FAR...</p>	 <p>Palm Vein Print</p>	<p>High sensitivity and non-contact pass support with palm vein patterns...</p>



There is a wide range of device support and open API and WEB service support to add new devices and services.

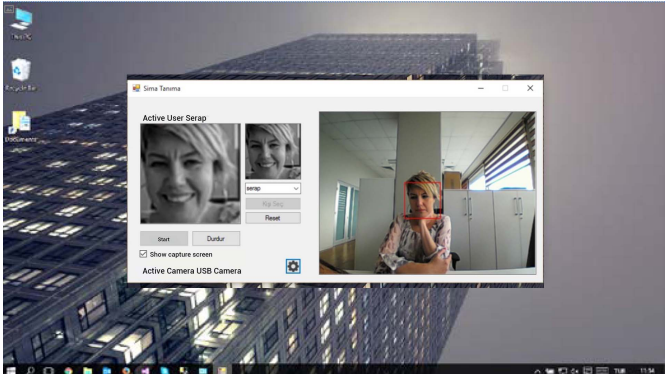
Screen Security

Starting from accessing the computer, it checks in real time that the person who is authorized to access all applications is at the screen, and prevents unauthorized people from viewing the information on the screen.

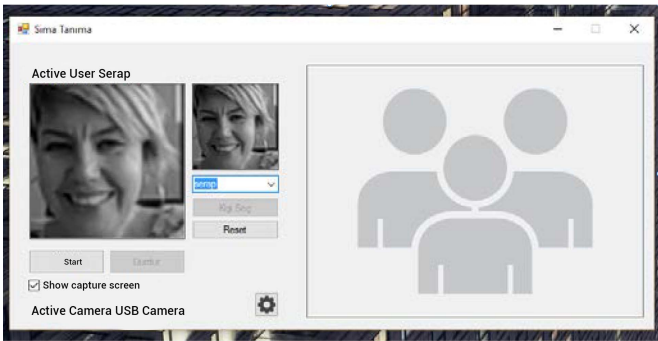
Advanced Face Recognition

Access to the computer is by face recognition.

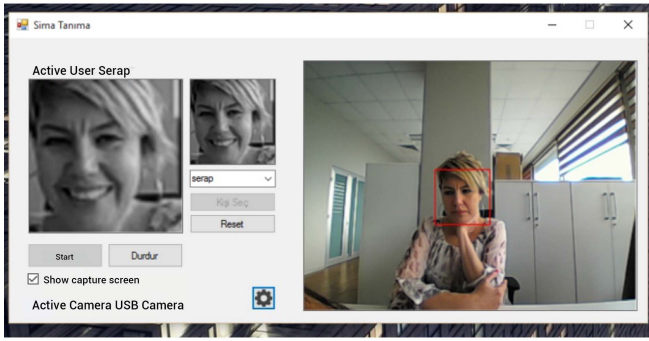
For liveness verification; Finger biometrics and iris are used. All operations and applications used at the beginning of the screen are logged. EagleEYE automatically logs out/locks the screen from the application or when the user gets up from the screen or looks at the screen without permission.




- Windows logon and application login with Biometrics - Real Time User Control - (The screen turns off when the user leaves the screen) - Reporting, Policy Server support, LDAP integration



Registration Screen

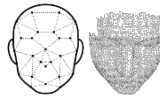


Registration Verification Screen




Record

Full screen, application window, UI metadata, Metadata manipulation, Keyboard, memory copy, Webcam




Face recognition

2 and 3 dimensional face recognition algorithms. Vitality, access permission and screen security



Search

Metadata (who, when, from, where, duration...). Session content (keywords).



Recording monitoring

DB data, recorded video, MPEG4 video, PNG webcam images, XML metadata



Security

Right to search. Playback right. Powers. Workflow approval.

EagleEYE Licensing

With EagleEYE, we offer our customers the licensing packages they need with different options.

EagleEYE Modules	Lite	Basic	Professional	Enterprise
Monitoring	✓	✓	✓ ✓	✓ ✓ ✓
Reports	✓	✓	✓ ✓	✓ ✓ ✓
Personnel Operations	✓	✓	✓	✓
Definitions	✓	✓	✓	✓
Access Authorization Profile	✓	✓	✓	✓
User operations	✓	✓	✓	✓
Terminal Management	-	✓	✓	✓
Safe Vault Transactions	-	-	✓	✓
Notifications E-Mail	-	-	✓	✓
Remote Work	-	-	✓	✓
Data Transfer (SQL, Excel)	-	-	✓	✓
Screen Protection	option	option	✓	✓
2FA / MFA	option	option	✓	✓
Powerful Biometric Verification	option	option	option	✓
Map	-	-	option	✓
Plan	-	-	option	✓
LOG	-	-	✓	✓
Card Life Cycle	-	-	option	✓
Add-ons				
Web User Interface	✓	✓	✓	✓
Multiple Monitor Support	option	-	✓	✓
Mobile Application	-	option	option	✓
Reader License Support	-	selective	selective	selective

Optional: Selected by the customer

Selective: The customer should choose according to their number of readers the appropriate reader license package

Supported Hardware and Software List:

