

Access Control

Biometric access control solution enabling a multi-factor identification of company's employees and visitors

Biometrics for access control is gaining popularity each day for its profitability, security and user-friendliness. Covering a vast number of market needs, biometrics is an obvious choice of enterprises globally.

BioTime is a biometric access control system allowing for reliable, secure and privacy-protected identification of the company's employees by their fingerprints, proximity cards and/or PIN codes and passwords.

Embedding BioLink's patented matching technology, BioTime is a tool of choice for the following enterprise units:

- Corporate security department;
- HR department;
- IT department;
- Secretariat.

The key identifier used in BioTime is the fingerprint, a human's unique biometric feature. Biometrics employed for controlling access guarantees that the protected areas and facilities can only be accessed by the authorized personnel. Employees cannot lose, forget or share their biometric identifiers; fingerprints are unchanged and can be produced for identification an unlimited number of times.

BioTime is a hardware-and-software solution. Apart from the software packages providing convenient enrollment and administration capabilities, the system includes fingerprint scanners combined with controllers of the following mechanisms: electromechanical and electromagnetic door-locks, turnstiles, gateways, etc.

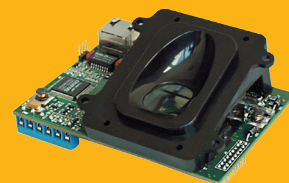
The fingerprint scanner and controller are embedded into an Ethernet terminal equipped with a keypad and display. The display shows the basic information about the registered event (check-in/check-out), while the keypad is used to type a PIN code that can be either an alternative identifier or a parameter complementary to biometric identification to optimize the employee access time.

To target a wider audience, the terminal is compatible with contactless card readers. In this case BioTime allows comparing the produced fingerprint with its digital template stored on the proximity card, making it a "portable biometric database".



BioTime Advantages

- Diversity of supported identifiers: biometrics, proximity cards, PIN codes, passwords;
- Wide range of available access control devices;
- Fault-tolerance through support of the local, network and combined operation modes;
- Scalability and centralized management;
- Ability to build several embedded security contours within an organization;
- Thorough integration with the biometric time and attendance system.



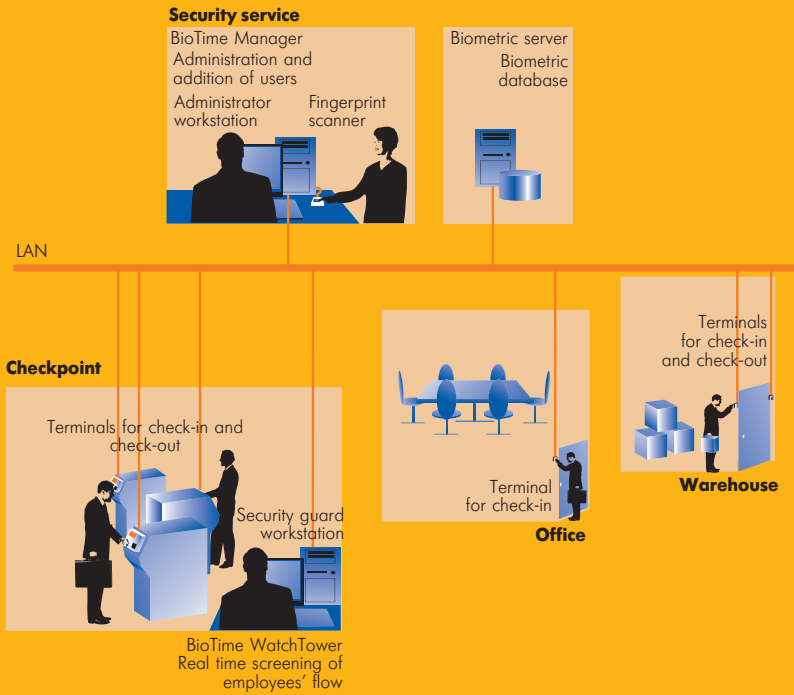
BioLink U-Match BI Ethernet, fingerprint scanner with controller, embedded version



BioLink FingerPass IC allows identifying users by fingerprints, contactless cards and PIN codes



BIO-METRICA, LLC



All terminals can operate in local, network and combined modes thus providing a system fault-tolerance, which means that in the event of LAN failures and/or temporary unavailability of BioTime Server BioTime system continue functioning.

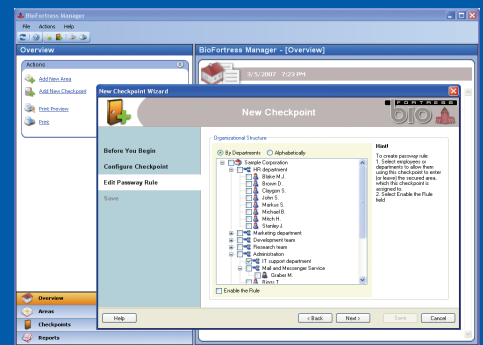
BioTime allows the management of user rights to access the most sensitive areas, such as top management offices, server rooms, inventory stock, etc. For example, an ordinary employee can only be granted the right to go through the central entrance, while the system administrator, apart from the central entrance, will also be authorized to access the server room. A higher protection level is achieved through building several security contours, meaning that a person who managed to get unauthorized access into one security contour will be denied access to another security contour. Access to protected areas and facilities is granted according to the time schedule defined by the enterprise security service.

BioTime generates comprehensive reports such as

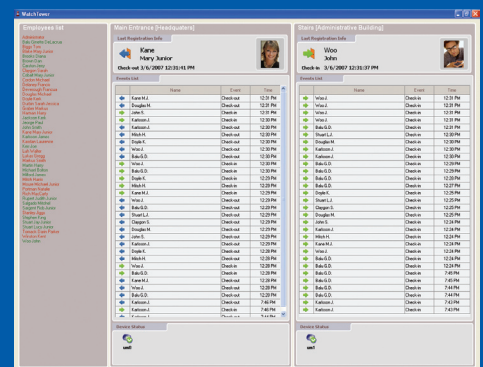
- Time of access of the protected areas and facilities and leaving them;
- Events of going through the security contours;
- Following the schedules of staying in office, including unplanned early arrivals and late departures;
- Attempts made by employees to access the protected areas outside the working schedule;
- Duration of staying beyond the protected territories, such as smoke breaks.

To manage the system, the following software modules are used

- BioFortress Manager – administrator workstation: allows creation of a list of areas and facilities requiring access control, defining access rights of the company employees, building security contours and generating various reports;
- Watch Tower – security guard workstation: provides on-line information on the events such as going through access control points including detailed employee data (full name, photo) and displays information related to several access control points.



BioFortress Manager – administrator workstation



Security guard's workstation



Bio-Metrica LLC
email: info@bio-metrica.com
Phone: +1-407-209-3373
WEB: www.bio-metrica.com
HQ: Orlando Florida USA