

# BioUptime® Technical Specifications

## General Functions

- **Creating and keeping detailed records of biometrics installations** (e.g. address, contact list for each organization, installation type and location, time zone, unit/element names and types, serial numbers, comments) and easy drill-down navigation to an individual unit/element view (the lowest level of hierarchy) from an bird's eye view of all sites and installations
- **Collecting, consolidating, and logging events** generated from all units/elements in a biometric system (e.g. capture device, biometric algorithm, algorithm licensing expiration date, server, hard drive, operating system, database, network, user interface, any end-to-end service/business process)
- **Processing/sorting/organizing/filtering** collected events
- **Detecting, diagnosing, and presenting/notifying critical events** (alerts) and root-causes to biometrics operations personnel
- **Generating reports** on operational reliability, availability, maintainability, and performance metrics (e.g. goals and parameters defined in a Service Level Agreement)
- **Performing** corrective actions

## Features

- **Event logging/consolidation/grouping:** organizes events based on units/elements, sites/installations, business processes/units, departments/organizations/geographic regions, global (bird's eye view)
- **Event/alert analytics:** detects and diagnoses critical events (alerts) and root-causes
- **Event/alert user interface (UI):** presents events and instant notifications via web-based UI and email
- **Reporting:** generates email reports on SLA metrics (e.g. downtime) and details for supporting troubleshooting
- **Inventory/record of installations:** keeps lists of geographically spread sites and installations with detailed information about them for reasons such as archiving or remote troubleshooting (detail record such as address, contact list for each organization, installation type and location, time zone, unit/element name, type, serial number, comments, etc.)
- **Drill-down navigation:** capable of drilling-down to an individual unit/element view (the lowest level of hierarchy) from the bird's eye view of all sites and installations
- **Corrective actions:** capable of setting/changing a parameter or triggering an action in the monitored unit/element

## Configuration/customization

- **User-defined events:** capable to define, add, and modify new type of events
- **User-defined alerts:** capable to define, add, and modify new type of alert rules and logic
- **Event update frequency:** capable of setting/changing how often units/elements report their events (e.g. every five minutes)
- **User Interface:** supports developing the UI for different Eco-systems and platforms (e.g. iOS, Android, etc.)
- **Site administration:** adaptable to requirements such as creating and adding: new organizations, installations, and units, new type of installations and units

## Flexibility and compatibility

- **Biometric modality/type:** Biometric agnostic/independent, works with all types of biometrics
- **Biometric sample acquisition sensor type:** Sensor-agnostic/independent, works with all types of capture devices
- **Unit/element type:** ability to monitor any user defined unit/element
- **Vendor independent:** vendor agnostic/independent, capable of working with hardware and software from any vendor

# BioUptime® Technical Specifications

## Scalability and Performance

- **Multi-unit/element management:** capable of monitoring thousands of units/elements with acceptable performance (dependent on server hardware configuration)
- **Multi-site management:** supports unlimited (theoretically) number of user-defined sites/installations, business processes/ units, departments/ organizations/geographic regions
- **Users:** supports unlimited (theoretically) number of users

## User management

Supports three level of user roles and access rights:

- **Super Admin:** has the highest access rights and can perform all BioUptime functions.
- **General Manager:** manager level account that can create new users of same level and create organizations and installations
- **Operator:** has the lowest access rights and suited for day to day management and maintenance. Operator is able to input data and receive alerts

## Security

- **Data encryption:** encrypted data transfer (e.g. SSL) for every event transmission between a monitored unit/element (or its agent) and the BioUptime Server
- **Agent-BioUptime server authentication:** authentication for every event transmission between a monitored unit/element (or its agent) and the BioUptime Server

## Technical requirement for BioUptime Server

- **Minimum HW requirements:** any modern Intel/AMD based machine with 10 gigabyte of available disk space, 2 GB RAM, and network interface
- **Supported OS:** Linux, Mac OS X

## Technical requirement for BioUptime User Interface (UI)

Internet connection, web browser (e.g. Firefox, IE, Safari, Chrome, etc.)

## Integration support

- **Agent/client interface/mechanism:** has its own agent description/method
- **API technology:** open API for developing customized agents. Based on Service Oriented Architecture (SOA), Web services-based platform (WSDL interface), rapid and easy to integrate with
- API documentation and sample code

## User/customer support

- **Guideline and tutorials:** UI manual, installation manual, troubleshooting help, white papers, presentations
- **Online support** (web portal)
- Telephone and Skype support