BIZDATA

eZintegrations™

Oracle Time and Labor Cloud integration with Biometric Systems

Oracle Time and Labor (part of Oracle Cloud HCM) is a wide-ranging, user-friendly, regulated time recording and management solution that provides you with full visibility and control over your most important resource, your workers. Time and Labor allow for quick time and absence recording using a daily, weekly, or monthly calendar. As a simple and quick way to enter time into the system, full drag and drop capabilities are offered, as well as the option to enter time or absence for a range of dates.

A biometric device is based on technology that can identify a person based on their unique facial traits, fingerprints, signatures, DNA, or iris pattern. Biometric security systems employ automated procedures in which human interaction is minimized to recognize and then validate an individual's identification based on distinguishing physiological or behavioral attributes such as fingerprints, face photos, iris recognition, and voice recognition.

Data Integration problem with Biometric Systems

• Data Quality Issue

Biometric data is frequently acquired in an unstandardized way, which can lead to data discrepancies. Data quality concerns might make it difficult to correctly integrate and analyze data, resulting in erroneous identification and authentication findings.

• Data Standard Issue

Biometric data is frequently kept in diverse forms, making it difficult to combine data from various sources. A lack of data standards can make comparing data and ensuring data accuracy and consistency across multiple systems challenging.

• Data Security Issue

Biometric information can be sensitive and must be protected at all costs to avoid being hacked or abused. Integrating biometric data with various applications raises the danger of data breaches, making it critical to implement strong security measures.

• System Complexity

Biometric systems may be complicated, necessitating specialized knowledge to successfully integrate and handle data. Integrating information across different databases can increase the system's complexity, making it difficult to confirm that the system is running properly.

• Data Privacy Issue

Biometric data is subject to privacy restrictions, and organizations must verify that they comply with applicable laws and regulations. Integrating biometric data with other systems increases the possibility of data privacy infractions, making it critical to set explicit data privacy rules and procedures.

Understanding eZintegrations™ solution through use case

A well-known software corporation has just hired contract workers for a new project in Chicago and Los Angeles. Both permanent and contract staff are paid and billed separately. They have implanted biometrics everywhere to track the regularly of their employees, however they have recently been experiencing issues with employee tracking as well as payment and billing for employees.

Challenges

Managing a workforce of both contract and permanent personnel is a demanding task for a software development business. Each working day counts towards the ultimate deadline when a company has a time-sensitive project. Furthermore, managing these employees' attendance and hourly billing becomes a challenge for the company.

Calculating the compensation of hybrid staff members, where permanent employees are paid a fixed wage and are expected to work a particular number of hours per week and contract-based employees are paid by hourly rates and their attendance is flexible, is another difficulty.

Given that the employees are in two distinct locations, calculating pay becomes increasingly challenging. To track each worker's biometrics for all gates, compute their hours of employment, and decide their remuneration.

Managing time worked and absences is a difficult and time-consuming procedure that is presenting a number of issues for the company. One of the most serious concerns is the lack of a centralized system for managing all forms of time worked and absences, which leads to inefficiencies and a lack of visibility. This is making monitoring employee hours and absences difficult, resulting in payroll and time off balance mistakes and inconsistencies.

Organization is also failing to comply with labor rules and collective bargaining agreements resulting in penalties and reputational harm. Furthermore, managing time worked and absences across multiple systems is difficult and time-consuming, necessitating manual data entry and verification, increasing the risk of errors and inaccuracies.

The lack of a centralised system is also leading to employee unhappiness, especially when there are errors or inconsistencies in payroll or time off balances, resulting in low morale and attrition.
Another concern with biometrics is data quality. Biometric data is frequently acquired in an unstandardized way, which might lead to discrepancies in the data. Another aspect to consider is data privacy and security. Biometric data is very sensitive, and any breach or unauthorized access to it can have devastating ramifications for individuals.

Scaling up biometric systems to handle more users or bigger amounts of data may be difficult, especially for a bigger corporation. This is due to the considerable computational needs for processing biometric data, and as the number of users or data points rises, so does the amount of technology necessary to analyse the data.

Integrating biometric systems with other systems can be problematic, especially if they use distinct biometric data types or formats. This can cause problems when attempting to communicate or interchange biometric data between multiple organisations or systems, making it difficult to develop a unified and standardised strategy to biometric data management. Implementing a biometric system can be costly, especially if the organisation is attempting to combine several biometric data types or working with a big volume of data.

Furthermore, the company lacks experts who can assist in the integration and management of data from multiple sources. Another problem is that they must invest in the appropriate technological resources and staff to successfully manage and integrate biometric data. Also, cost related to integrating and managing data from multiple sources is high.

The company collects biometric data in numerous ways, such as fingerprints, face recognition, and iris scans, amid others. Each biometric data type has distinct properties, and combining data from disparate sources can be difficult. Distinct biometric data types may necessitate unique algorithms, processing approaches, and storage formats, making a standardized strategy to data integration challenging to develop.

Solution

The necessity of collecting data from numerous data sources in order to gain better insights and implement effective solutions is becoming a new requirement for every organization. Organizations nowadays demand an integration solution that is cost-effective, less complex, and can complete integration in a shorter duration.

eZintegrations™ is a cloud-based iPaaS platform that provides a cost-effective and efficient solution for data integration across several platforms. The platform's no-code or low-code approach allows businesses to accomplish integrations with minimum IT assistance, reducing the strain on IT staff while saving time and resources. Its intuitive layout and simple navigation make it accessible to anyone with minimal technological knowledge. It also features an improved functionality that allows users to self-register, own, and add other users to the platform in a matter of minutes.

The platform is intended to connect to over 5000 different SaaS apps and APIs, giving businesses flexibility and adaptability when integrating data across platforms. The capacity of the platform to convert, wrangle, and orchestrate data across two systems aids in the integration process. One of the most significant advantages of eZintegrations™ is its low cost. The platform considerably decreases the additional investment expenditures that organisations experience in order to create their own iPaaS platform, making it an inexpensive choice for small and medium-sized firms.

Business Benefits

- ### Improved Business Processes

Biometric data integration can enhance corporate operations by lowering the time and resources necessary for identification and authentication processes, allowing staff to focus on other vital duties.

- **Better Data Management**

Integrating biometric data can help enhance data management by delivering more accurate and consistent data, lowering the chance of oversights and data duplication.

- **Increased Efficiency**

Integrating biometric data may boost productivity by automating identification and authentication procedures, which reduces the need for manual input and verification.

- **Real-Time Monitoring**

Biometric data integration allows for real-time monitoring of activities, with quick notifications in the event of unauthorised access attempts or questionable activity.

- **Cost Savings**

By decreasing the need for manual entry and verification, optimising processes, and enhancing data accuracy, biometric data integration can contribute to cost savings.

BIZDATA

CONTACT US

For more information about Bizdata Appliance,
visit www.bizdata360.com or
call +1-650-283-1644 to speak to an Bizdata representative.
