bioconnect.

Insights for BioConnect Enterprise 4.7
A Proactive Approach to Security

How A Hybrid Architecture Helps You Securely Get The Most Out Of Your Biometric System

BioConnect is committed to providing you with the highest level of security and data privacy while continuing to innovate and provide value for the enterprise. With the release of BioConnect Enterprise 4.7 we will begin to make use of a hybrid architecture. This means that you will continue to rely on the privacy and security of on-premise applications while benefiting from the flexibility of cloud-based features.

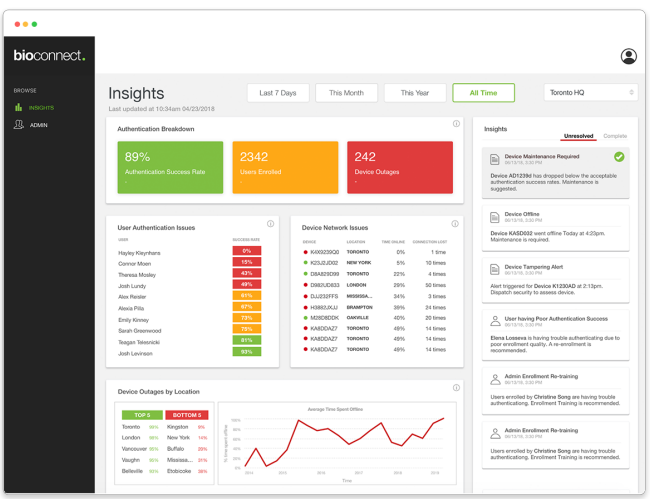
Benefits

Insights is a new cloud-based application feature that can be enabled in BioConnect Enterprise 4.7. This tool can provide your team with rich data and analytics along with alerts and notifications that help you resolve some of the most common issues encountered with biometric systems. The insights feature helps identify the following:

- Which users are having difficulty authenticating?
- Which devices are experiencing network or hardware issues?
- Which locations are experiencing network issues?
- Which users need to be re-enrolled?
- Which admins need to be re-trained on proper enrollment capturing techniques?

Having access to insights will help your security team be proactive instead of reactive. You will be able to identify and address issues before they become problems. You will be able to see the performance of your system improve over time as your team can focus on optimizing and improving your enterprises' overall security.

The design of this hybrid architecture is focused on combining leading practices in security and data privacy. Below we will outline how this architecture works to provide value while keeping your data secure. Our insights feature is the first to make use of this hybrid architecture.



bioconnect.

Architecture

Your BioConnect system will now push data to the BioConnect Cloud at regular intervals. Before this data leaves your network, it passes through our data anonymization service. This service removes all personally identifiable information (PII) from the data. This is done to comply with standards and regulations such as General Data Protection Regulation (GDPR) and Privacy by Design. All data is stored within AWS' secure cloud infrastructure. None of the data can be traced back to a specific individual.

Names and card numbers are entirely removed from the data set. Biometric templates are not sent to the cloud. When you access the insights application from your own local computer, BioConnect combines on-premise data (user names, device names, location names) with cloud-based data (alerts, notifications, performance history) and displays it in your web-browser. This tool provides you with important alerts and system information that will allow your team to make better decisions.

What Is Pushed To The BioConnect Cloud?

System Activity Data

- Access Events
  Successful/failed authentication attempts
- Network-Related Issues
  Device connection/disconnect events

Standard Account Data

- Software Version
- Device Count
- User Count

What Data Does Not Get Pushed To The BioConnect Cloud?

Biometric Templates

- Biometric templates are not sent to the cloud

Personal User Data

- User names are removed before data is sent to the cloud
- User card numbers are removed before data is sent to the cloud
- Admin login credentials are not sent to the cloud

Device Data

- Device names are removed before data is sent to the cloud
- Device locations are removed before data is sent to the cloud

Opting Out

If you do not wish even your anonymized data to be sent through to the BioConnect Cloud, you can contact our customer support team to disable the feature.