

Unauthorized access to critical third party software like SCADA systems, CAM Software, Planning Software, Administration management tools etc. can cost you millions in damages !

- Setup in minutes
- Add on to any third party software
- Easy to administer
- Quick Reports
- Strong Encryption

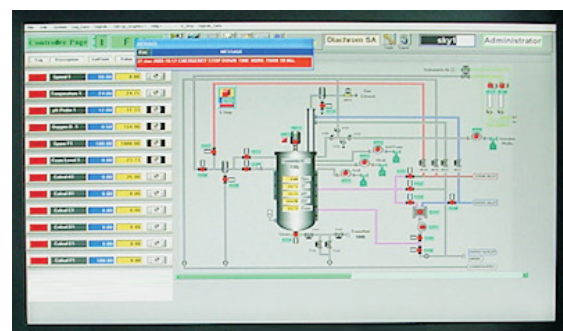


Traditional software login process relies on passwords. Passwords can be shared, are forgotten, misplaced, need frequent changes and so on. You can instantly plug-in the Streme Biometric system into your existing third party software. With each vendor, you need a separate registration process. Using Streme Biometric, you now combine authentication process into a single suite.

## Applications

### Scada Software

Auto login to scada systems with biometric authentication. This ensures that the scada software does not login at all without biometric authentication. In environments, where control of factory processes has to be monitored and controlled, this is a must have add-on.

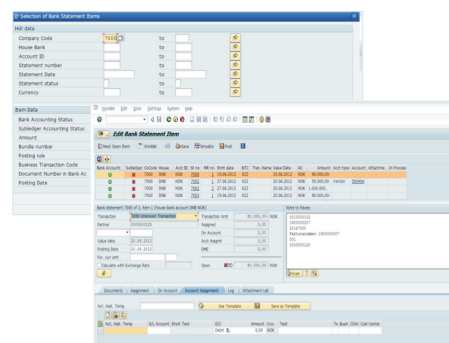


### Corporate Control room systems

In control rooms, it is vital to restrict access only to certain authorized employees and contractors. Control rooms are central to managing and controlling business and industrial processes. Cameras, safety equipment, machines on the network etc. are all monitored in this room. Robust authentication provided by Streme Biometric is an established requirement.

### Administration systems

Managing master data for administration systems is critical. Authentic login by authorized personnel is mandatory. The access to master data is vital for smooth functioning of inter related systems. The Streme Biometric authentication add-on ensures that only select users get access to the machines.



# Streme Biometric

A complete range of biometric access Add on solutions

**STREME**<sup>®</sup>  
Framework • Products • Solutions

## Streme Biometric A complete range of biometric access Add on solutions

A range of devices that connect using industry standard protocols like serial, usb, poe etc. are available for integration. Depending on the operating requirement, environment conditions and interface, the correct model and hardware OEM is chosen.

### STHB1 Finger print

With devices capable of storing hundreds to tens of thousands of finger prints, the finger print devices are fast, reliable and rated to work in commercial or industrial environments.

### STHB2 Iris Scanning

Iris scanning devices for very high security applications are integrated with the authentication engine. These are usually used in addition to other authentication add-ons like finger print, voice etc.

### STHB3 Voice recognition

Voice recognition devices for additional layer of authentication. This compares the voice sample of the person with the recorded sample and grants access. Usually it is coupled with some other authentication module.

### STHB4 Face recognition

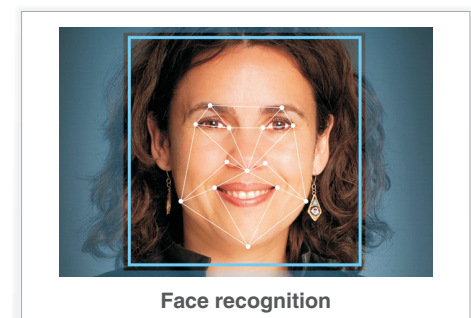
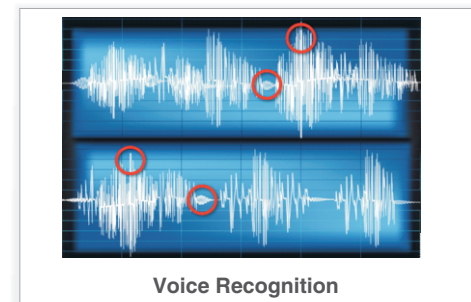
Face recognition and algorithms integrated for pattern matching to automatically authenticate the users. This can use high end cameras or a simple web camera focused on the user. Images can be captured for comparison or just for reference. Optionally, videos can be stored and tagged to the user login in the video management server for seamless information access.

### STHBSP Access Engine

Access engine is configured to work with almost any third party software like scada, cctv control system etc. Integrating seamlessly with login modules, the engine grants access to the third party software only when the biometric system is successful. A range of devices and technologies like finger print device, face recognition etc. are supported. Designed to be resilient to attempts to be cloned, bypassed or shut down, the engine logs its activities in encrypted format and sends alerts and status to a central enterprise server.

### STHB SM Management Suite

Management suite registers the biometric information and maps the same to access passwords. All information is stored in encrypted format to prevent unauthorized access. A central management suite allows centralization of data and link to active directory to enterprise wide biometric management. Self registration or centralized registration of biometric information is provided for large deployments.



To know more visit: [www.streme.tv](http://www.streme.tv)

Call us on: **+91-9167397102**  
**+91-9930264735**

**Disclaimer:** The system is designed to protect access to your data by additional biometric authentication. The system works only with correct installation, regular monitoring and acting on reports generated by the system. The system depends on continuous power, network connectivity etc. to function properly. Any direct, indirect or consequential damages caused by this system shall be limited to the purchase price of the system.