HUMMINGBIRDS AI

Security & Privacy Considerations of GuacamoleID

HUMMINGBIRDS AI

Disclaimer

This document describes the security features of GuacamoleID software as planned for production release. Beta and pilot releases might have variances that will be specified at delivery time.

What Personally Identifiable Information (PII) and/or sensitive data does the software handle?

The software collects facial biometric information in the form of visual telemetry. **No picture or video is recorded/stored.** The only information stored is a series of numbers that describe certain non-descript elements of facial characteristics. The image or video of the person can NOT be reconstructed using the collected information.

How does the software store sensitive information?

All sensitive data is encrypted in storage. The software encodes the information using secure symmetric encryption (AES-256 or stronger). The key is a secure, unique, and randomly generated symmetrical key that is stored in the device's operating system secure credential repository.

Can the collected information about a person be used to authenticate through other authentication/identification services?

No. Generally, the data collected and stored **is not sufficient** to create a picture or video of the person to identify the person further. Essentially, the data is **useful only** to the Guacamole software.

Does the software record any images or videos?

No. The software processes the video received in **real-time**, and after analyzing the telemetry data, the actual images are **discarded**.

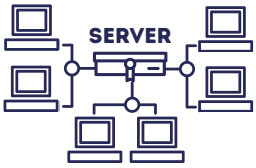
Will My Sensitive Data Go to The Internet/Cloud?

No. For security and privacy reasons, the software is designed to work **without using any cloud-based services**. Generally, the software has two modes of operation that the clients can choose from:

1. <u>Standalone Application</u>:

In this mode, all biometric data stay in the device and they are **never transmitted** over any network. The downside is that every person needs to be registered on every device that they use for the first time they log into that device.

This mode is suited for settings where employees typically have a designated workstation.



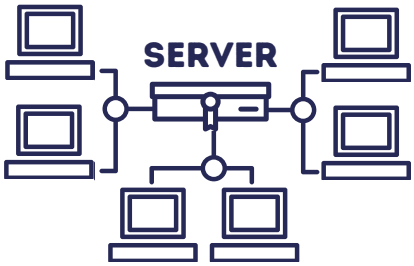
2. <u>Connected Application</u>:

In this mode, a **private server** is deployed in the local network that connects a group of workstations together.

Registrations (biometric telemetry required for identification) are **securely transmitted** inside the local network to the server and distributed to other devices in the same local group. This setup is optimized for settings where employees frequently use a pool of available workstations.

What are the security considerations of the Connected Application mode for GuacamoleID?

In the Connected Application:



- All sensitive information is **encrypted** during registration and transmission using industry-accepted encryption standards (TLS 1.3 or stronger)
- All nodes authenticate the local group's server by validating a **pinned certificate.**
- The server authenticates all registered nodes using a **secure ID** used for license management and device authentication.
- Nodes have individual permissions that can be **managed on the server** to submit new registrations to the server. Nodes can be removed or their access to adding **new registrations** can be revoked from the server.

What happens if for some reason my face changes and the software doesn't recognize me anymore?

Within the first few minutes (first 5 minutes by default) after logging in, the software will prompt you to register your face either if there is no registration (e.g. first time after roll-out), or if the face doesn't match. This ensures that the person that authenticated is the same person performing the registration and prevents session hijacking during an active session.

If for any reason, the software fails to recognize you, the easiest way is to log out and log back in so that the face can be registered anew.

Does the software require internet connectivity?

At this time, the only internet connectivity used is for **license validation**. Upon request, the software can be **deployed in air-tight networks** by deploying a local license activation server.

What if I have a legitimate reason to give access to my device to a trusted person?

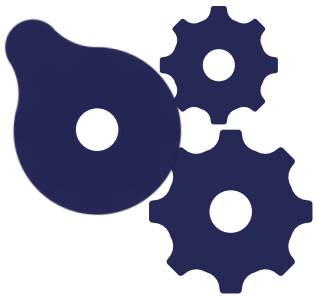
There are three ways of achieving this:

- You can **pause continuous facial authentication temporarily** (anywhere from 5 minutes to up to 4 hours). Please note that we might need to either authenticate your face or re-authenticate you (ask for your password) if there is some **time passed** from your login to ensure that you are the person pausing it and this **mechanism can not be abused**.

- In certain settings where the admin has enabled a trusted local group if the face is recognized, the software may provide a **soft notification** but will not block access for a **certain period of time**.

- If the settings are enabled to allow you to do this, you can **allow a third-party face** to become trusted by registering that face.

Please note that these behaviors are configurable by the organization's administration and the permitted behavior may differ depending on the deployment.



Every Computer Has Chips,
It's Time For Guacamole!

For further information and questions, please contact hello@hummingbirds.ai or your sales point of contact.

HUMMINGBIRDS AI

AI With The Speed of Hummingbirds

hummingbirds.ai | hello@hummingbirds.ai