AF64

Privacy Overview

Overview

The AF64 Access Station Pro is designed to deliver smart, secure, and seamless entry — while prioritizing and protecting user privacy. This guide explains how Verkada protects user data, supports various user enrollment pathways, and provides tools for Verkada Command administrators to manage Face Unlock responsibly

While the AF64 and Face Unlock features are designed with privacy in mind, it is the responsibility of the customer deploying the system to comply with laws and regulations that apply to them.

Enrollment

- **Enrollment:** Face Unlock offers configurable enrollment pathways to support organizations' compliance needs when enabling Face Unlock. User consent can be collected directly from users through the self-enrollment process or centrally managed by a Verkada Command administrator in accordance with the organization's internal policies.
- **User Data Control:** Users can opt-out of using Face Unlock for their access credential at any time by contacting a Verkada Command administrator for their organization. Once the Command administrator disables Face Unlock for the user, the user's Face Unlock credential is deleted.

Protecting User Data by Design

- **Face credentials:** When a user or Command administrator uploads a photo during Face Unlock enrollment, facial recognition technology is used to convert the image of the user's face into a face vector, which is a numerical representation that serves as the user's face credential for future authentication attempts. This face credential depicts the user as a series of numbers instead of an image. The face credential cannot be used to reverse-engineer the original image.
- **Data Storage:** Face credentials created from Face Unlock enrollment photos are stored both on device and in the cloud to support centralized management and multi-device functionality. Face credentials are encrypted at-rest on the AF64 and in-transit with Command.
- **Edge-Based Processing:** When a visitor presents their face to the AF64 reader, the facial authentication and credential matching is performed locally on the device.
- **Cloud-Based Processing (if Verkada's People Analytics camera features are enabled on AF64):** The AF64's camera can be connected to Command's People Analytics camera features, where available. If People Analytics features that use facial recognition technology (such as Face Detection or Person of Interest) are enabled, a copy of the face scan and face vector may also be sent securely to the cloud to support those features.
- **Data Minimization:** The face credential is linked to the user's profile within the Verkada Command Access Control backend, ensuring it enables authentication without exposing the underlying credential data to Command administrators.
- **Retention:** The face credential derived from a user's profile photo is retained on the cloud and on device until the profile is no longer registered for Face Unlock. Face vectors from images captured by the AF64 reader for Face Unlock authentication are deleted from the device once credential matching is complete.

Administrative Safeguards and Accountability

- **Role-Based Access Controls:** Only authorized Command administrators can manage users' Face Unlock credentials. Strict role-based permissions in Verkada Command help limit access to those with appropriate privileges, helping protect user data and maintain accountability.
- **Audit Logging:** All administrative actions related to Face Unlock credential management are logged to allow organizations to audit activity, support accountability, and demonstrate compliance.