

FAQ

What Is Continuous Authentication for Agents?

Continuous Authentication (CA) makes work from anywhere possible. It is a remote worker enrollment and authentication platform. It takes the place of brick and mortar monitoring and security maintenance. And the whole thing runs in a browser in the background.

It makes working from home a long-term reality for many contact center agents. Supervisors and administrators protect and maintain agents and sensitive material in the new distributed work world.

How do I enroll?

To enroll, complete the face scan and upload a photo of your ID (optional).

Is it safe to have my face scanned?

Yes, it is safe. See [Why a Facial Scan is Your Friend](#) for details.

3D Face Map	You'll receive an email asking you to enroll. Access the welcome email on your phone with either safari (on iOS) or Chrome (on Android). Once in the correct browser on your device, scan your face with the CA 3D face scan. CA walks you through how to complete the scan with onscreen instructions for an accurate map.
Photo & Upload (optional)	Then take a photo of your driver's license or ID document front and back. The picture on the license or ID is compared to the face scan to verify they match. Journey can also verify that the ID is authentic.

What happens after I enroll?

Once enrolled, you have access to an authentication page. There you log in with your user ID and authenticate actively with your facial biometric.

What do I do when my shift starts?

To begin work, enter your user ID and perform an active authentication. After authenticating with that scan, Continuous Authentication runs passive authentication regularly. You are not interrupted unless the scan isn't captured. CA runs in a background browser tab until there is an anomaly.

An anomaly is:

- multiple faces detected
- a span of time without a successful passive authentication

In those circumstances, an alert prompts you to look into the camera for a quick authentication. You may be required to perform an active authentication if a set of passive authentications fail.

What Are the Authentication Types?

There is active and passive authentication.

Active	Active authentication is a deliberate act of looking at the camera where Continuous Authentication takes a picture of your face. This image uploads to the server for comparison to your original biometric face map.
Passive	CA takes photos until there is a match to the original. This happens automatically without any action from you. Failed photos are discarded and not saved.

How is my privacy protected?

- Blurring is provided to obscure backgrounds.
- Images are need-to-know only and viewable only by authorized personnel.
- The biometric face map is not an actual photo, instead it is a set of meta data and not a picture.
- Databases are all encrypted and Journey does not store any data on our network.