

Clareity Password-less FAQ

Frequently Asked Questions and Key Information (2026-02-026)

What is Password-less?

Password-less is a modern authentication framework that utilizes Passkeys as the primary method, eliminating the need for users to enter a password. It offers direct, highly secure multi-factor authentication (MFA) with minimal friction for users. This approach represents the future of logins, as traditional passwords are quickly becoming obsolete.

Who Enables Password-less?

Password-less is enabled at the organization or MLS level. Until it is activated, users will not see any changes and advanced functions will not be available. Once enabled, the main login screen will display the Password-less login button, indicating that the feature is active.

Do I Need My Username?

Yes, entering your username is required as it personalizes your login process. Multiple options are available to save your username at the device level—the easiest is selecting the checkbox on the login screen.

Can I Still Log In With a Password?

Yes, the login screen allows users to choose either Password-less or traditional password login. Password login may be useful if you experience issues with a passkey or are logging in from a new or public device. Password logins are evaluated using the same Assure risk criteria and may prompt an MFA challenge as needed.

Will I Experience Additional MFA Challenges?

No—Passkey is itself a form of MFA authentication. During regular logins, you will not be challenged for additional MFA. However, MFA may be required for special operations, such as adding a Passkey to your profile.

What Is Logged?

Assure evaluates every login and maintains a complete log of risk criteria, consistent with current reporting. Enhanced reporting features are planned for the near future.

Can I Have More Than One Passkey?

Yes, if Password-less is enabled, you can activate up to three Passkeys with your Clarity profile. A new management page allows you to add, delete, and rename your keys.

Can I Use My Passkey Across Devices?

Yes, there are multiple ways to use your Passkey on different devices.

Browser-Based Passkeys: The easiest way to use the same Passkey on multiple devices. You must be logged into the relevant browser or mobile device from the same ecosystem with the account that stores the Passkey. See below for details:

- **Apple iCloud Keychain:** Stores and syncs Passkeys across Apple devices signed into the same Apple Account, with iCloud Keychain enabled.
- **Google Password Manager:** Stores and syncs Passkeys across Android devices (and Chrome) signed into the same Google Account.
- **Microsoft Password Manager (in Microsoft Edge):** Stores Passkeys in Edge and can sync them across devices where you're signed into Edge with the same Microsoft account (availability and behavior may vary by platform and rollout).

Password Manager Applications: Applications like:

- Keeper
- 1Password
- Bitwarden
- Proton Pass

can also be used to store Passkeys and work across devices. These are best for users comfortable managing their own password manager setup. We do not recommend a specific provider—please research carefully before choosing an app.

Do You Support Cross-Device Passkey Sign-In?

Yes, you can use your phone as a universal Passkey. This setup is highly secure but can be technical and varies by device. We recommend this only for tech-savvy users already familiar with the process. Clarity follows FIDO2 standards, including device proximity, for secure authentication.

Are There Other Ways to Log In?

Stay tuned—over the coming months, we will announce additional innovations to make Password-less login even more secure and easier to use.