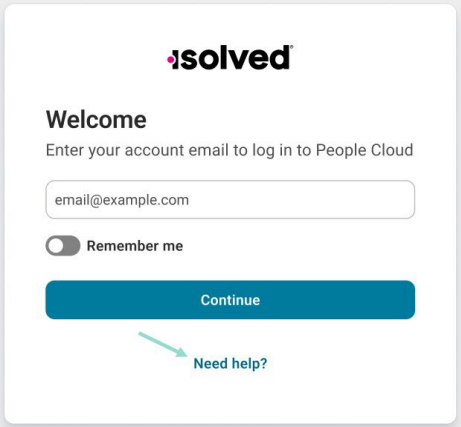
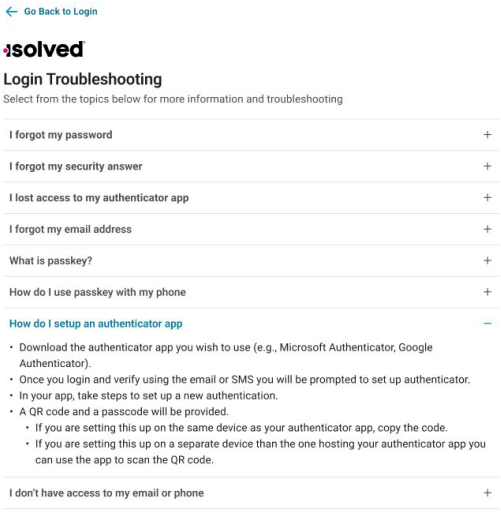
PAYSERV
PAYROLL SOLUTIONS

Multi-Factor Authentication (MFA) Updates

To enhance the security of your account, we will be updating our Multi-Factor Authentication (**MFA**) process by November 1, 2025.

Instead of receiving codes via email or text message for verification, **you will be required to use either a Passkey or an Authenticator App, such as *Microsoft Authenticator* or *Google Authenticator* for MFA.**





You will be required to authenticate using one of our secure methods:

Passkeys or Authenticator App

Passkeys are cryptographic credentials stored on your device and can used with biometrics such as Face ID, a fingerprint or can be a device PIN. (Much like how we log into our phones or computers).

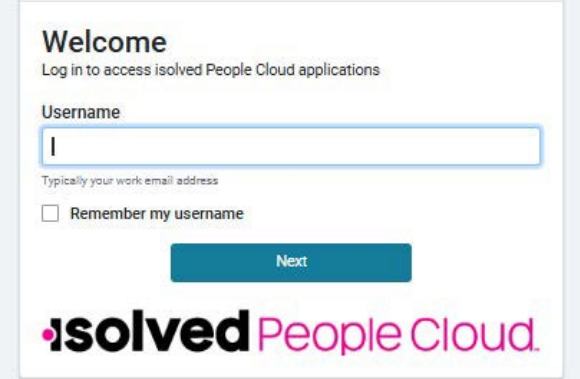
- **Passkey** = Biometric (Face ID, Touch ID, etc.), Windows Hello, or security key

Authenticator apps generate time-based one-time pass codes (TOTP) that are more secure than text or email codes.

- **Authenticator app** = Microsoft Authenticator, Google Authenticator, etc.

You will be prompted to set up your passkey or authenticator app through the system.

1. Key in your Username and Password as usual, and select Log In.

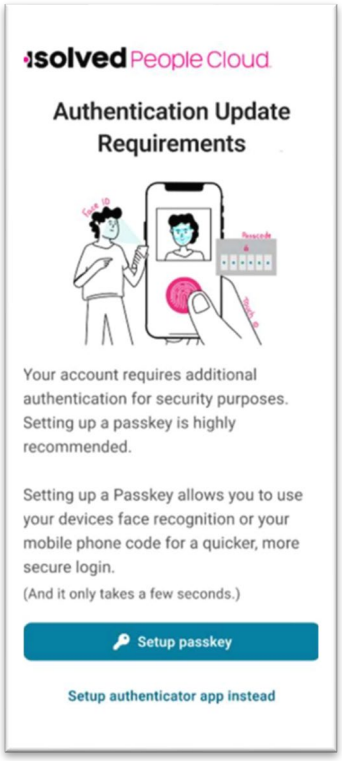


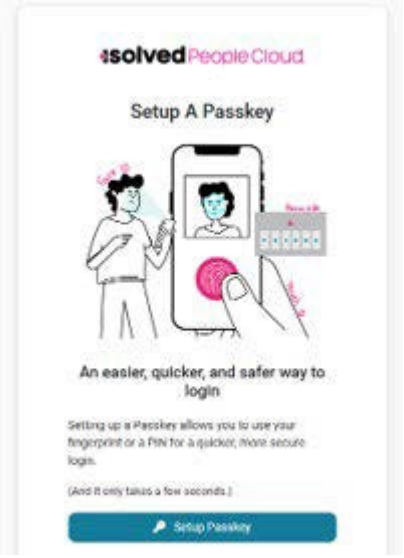
2. Select your Authentication option.
3. You are then taken to the Application Portal upon login.

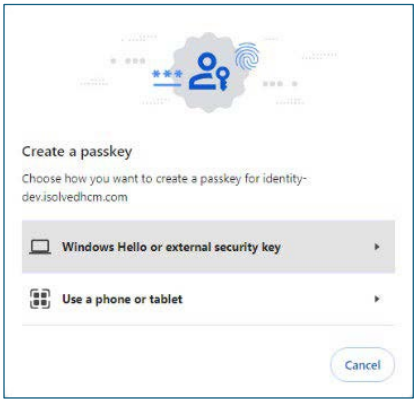
   Note: If you have not yet configured your Passkey or Authenticator App, you will have the option to verify via SMS/Email before being taken through the Authenticator configured.

Passkey Setup

The Setup Passkey allows you to set up your passwordless option. You can make changes to this at any time when logged in by selecting your avatar/initials in the upper right corner of the screen, then Manage Account. Once this is set up, future logins use what you have added for your options. You may be able to use FaceID, Thumbprint, Passcode, PIN, or other options present on your device.

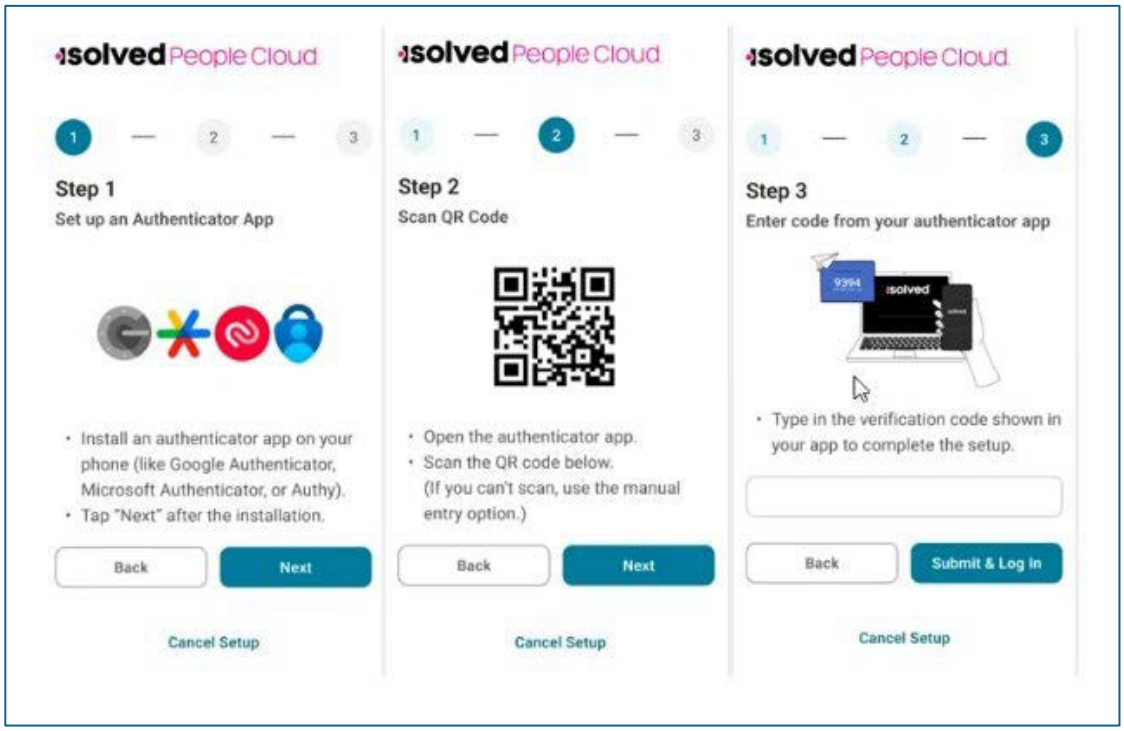






Authenticator App

Choosing Set Up Authenticator App instead leads you through the steps to set up your authenticator app.



How do I set up and use an authenticator app?

- Download the authenticator app you wish to use (e.g., Microsoft Authenticator, Google Authenticator).
- Once you login and verify using email or SMS you will be prompted to set up authenticator.
- In your app, take steps to set up a new authenticator.
- A QR code and a passcode will be provided.
    - If you are setting this up on the same device as your authenticator app, copy the code.
    - If you are setting this up on a separate device than the one hosting your authenticator app you can use the app to scan the QR code.

Frequently Asked Questions

Q: What is multifactor authentication (MFA)?

A: MFA is an effective way to increase protection for user accounts against common threats like phishing attacks, credential stuffing, and account takeovers.

Q: Can we opt-out of the multi-factor authentication?

A: No.

Q: How does MFA work?

A: MFA adds another layer of security to your login process by requiring users to enter two or more pieces of evidence - or factors - to prove they are who they say they are. One factor is something the user knows, such as their username and password combination. Other factors are verification methods that the user has in their possession, such as an authenticator app or security key.

Q: What are the key features and functionality?

A: MFA requires a user to validate their identity with two or more forms of evidence or factors when they log in. We are enforcing a minimum of two. One factor is something the user knows, such as their username and password combination. Other factors are verification methods that the user has in their possession.

Q: Can a user have passwordless access on multiple devices?

A: Yes, each device allows and recognizes what was set up on that device and uses that as a default. Some passwordless options can be used on multiple devices.

Q: What might a user expect this to do that it does not?

A: The user may expect to not do this every login if they are on the same device, a registered IP address, or have logged in within the same day – however, they still need to do some kind Internal FAQs: Identity Server of MFA regardless. This could be different than what they are used to today depending on the system settings per client.

Q: Is PayServ requiring clients to enable MFA?

A: MFA will automatically be enabled for you. This will be a requirement for all users accessing our software, isolved People Cloud.

Q: Why is PayServ requiring MFA?

A: There’s nothing more important than the trust and success of our customers. We understand that the confidentiality, integrity, and availability of each customer’s data is vital to their business, and we take the protection of that data very seriously. As the global threat landscape evolves, implementing these security measures is essential for the safety and well-being of your business and employees.

Q: Is there anything I can do to prepare my employees?

A: Yes! While employees already have the option to authenticate using their email, you should encourage ALL employees to ensure they also have a phone number registered to their account. This ensures they can authenticate regardless of using the new options we've added.

Q: What impact will this have on users?

A: Users will now be asked to authenticate each time they login, as opposed to once every 30 days or when a new IP address is identified.

Q: How frequently must users provide a verification method when logging in directly?

A: As part of this update, users will need to provide a verification method every time they log in to isolved.

Q: What happens if we have high security set up for our client users or ESS users and someone loses their phone with the authenticator application?

A: Please contact Support for assistance if the employee loses access to their authenticator.

If you have any questions, we can help.

Please contact your specialist directly.