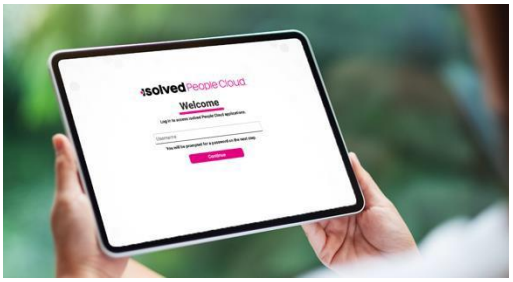
Your isolved People Cloud Login Update is Here!

The security of customers' data is a top priority for isolved. We continue to analyze the safeguards in place to maintain confidentiality, integrity and secure accessibility for your business and employees.



In our ongoing commitment to ensure optimal security, we will be implementing measures like multi-factor authentication (MFA). Effective **February 23, 2024**, all users will be required to utilize MFA as a mandatory security measure.

The first time you log in after the release, you will be given the option to set up an additional method of authentication, such as an authenticator app, FaceID/touch ID, or security key. You can utilize one of the additional methods we have added for enhanced security, or you may proceed with using email or text message as your authentication method. Going forward, you will be required to use multi-factor authentication at least every 12 hours as you log in to isolved People Cloud.

FAQ

Q1: What is multi-factor 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.

Q2: 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.

Q3: Is isolved requiring customers to enable MFA?

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

Q4: Why is isolved requiring MFA?

A: There is 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.

Q5: What is the advantage of MFA to me?

A: Clients will have a greater ability to protect their company's and employee's data utilizing additional options to authenticate seamlessly with a more intuitive user interface.

Q6: When does this go into effect?

A: The requirement for MFA will go into effect for all isolved users on February 23, 2024.

Q7: 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 will ensure they can authenticate regardless of using the new options we have added.

Q8: What impact will this have on users?

A: Users will now be asked to authenticate once every 12-hour period, as opposed to once every 30 days or when a new IP address is identified.

Q9: How long are user sessions?

A: This has not changed in classic isolved; if a user is inactive for approximately 20 minutes, a popup will appear with a warning that the session will close. The session can be interacting with the site in some way such as moving to another screen. The inactivity timeout for Adaptive Employee Experience, including the mobile app, is now 15 minutes.

Q10: Can users have password-less access on multiple devices?

A: Yes, each device will allow and recognize what was set up on that device and use that as a default. Some password-less options can be used on multiple devices.

Q11: 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 at least every 12 hours as they log in to isolved. Users can remove the default 12-hour option and authenticate every login if needed.

Q12: What authentication options can be used?

- Authorization Codes: Users can receive authorization codes as they have before.
- Platform Authenticators: Easy MFA verification using a desktop or mobile device's built-in authenticator service, such as Windows Hello, Touch ID, or Face ID.
    - Each user will need to enable these native options on their device of choice to use them. If someone does not have Face ID enabled on their device, then they will not be prompted to use this frictionless option.
- Third-Party Authenticator Apps: Authenticate with apps that generate temporary codes based on the OATH time-based one-time password (TOTP) algorithm. There are many apps available, including Google Authenticator, Microsoft Authenticator, and Authy.
- FIDO2 Password-less Authentication Security Keys: These small physical devices are easy to use because there is nothing to install and no codes to enter. Security keys are a great solution if mobile devices are not an option for users. Keys are available from manufacturers like YubiKey.

Q13: Where can I go to learn more?

There are resources available in the University with the tag "multi-factor authentication", including Identity Server - Multi Factor Login Instructions.