Overview

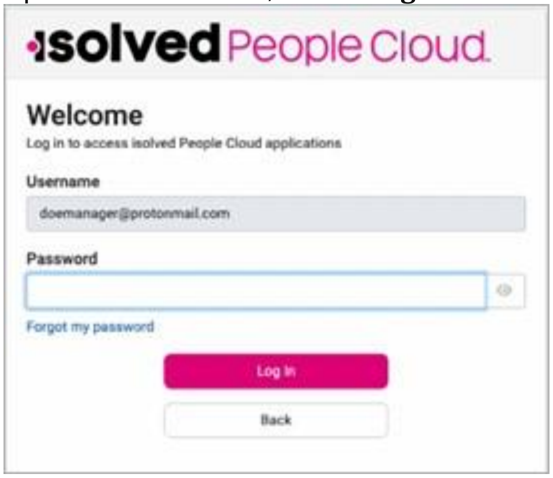
isolved is committed to protecting your data. All users will be required to use Multi-Factor Authentication (MFA) every time they login to isolved. HCM software is a gateway to extremely sensitive personally identifiable information, along with sensitive business and payroll related information. It is imperative that we protect that information and data at all costs. As cyberattacks grow more common, passwords no longer provide sufficient safeguards against authorized account access. It's our commitment to our customers to stay up to date on industry standards for security.

How Can Users Authenticate and what Options are There?

- Email
- Text (Work cell phones and personal phones are required for this option. Desk phones and extensions are prohibited.)

Logging in

1. Key in your username and password as usual, select **Log In**.



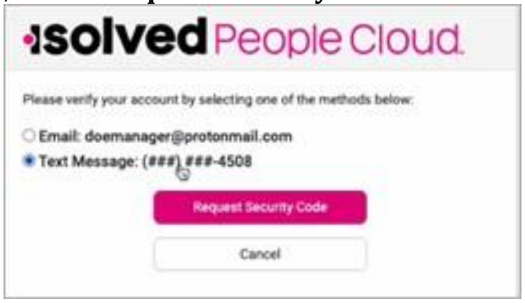
Welcome

Log in to access isolved People Cloud applications

Username: doemanager@protonmail.com

Password:

2. Select a verification option, select **Request Security Code.**



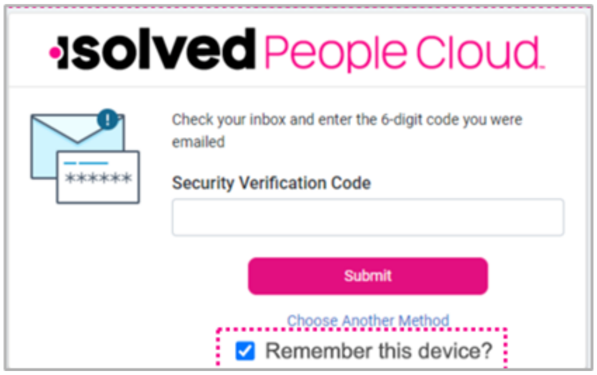
Please verify your account by selecting one of the methods below:

○ Email: doemanager@protonmail.com

● Text Message: (###) ###-4508

3. Use the code you receive. Select **Submit**.

   a. This will default to have **Remember this device** checked, by having this checked, the system will not require MFA for 12 hours; if this is unchecked, MFA will be required for each login.

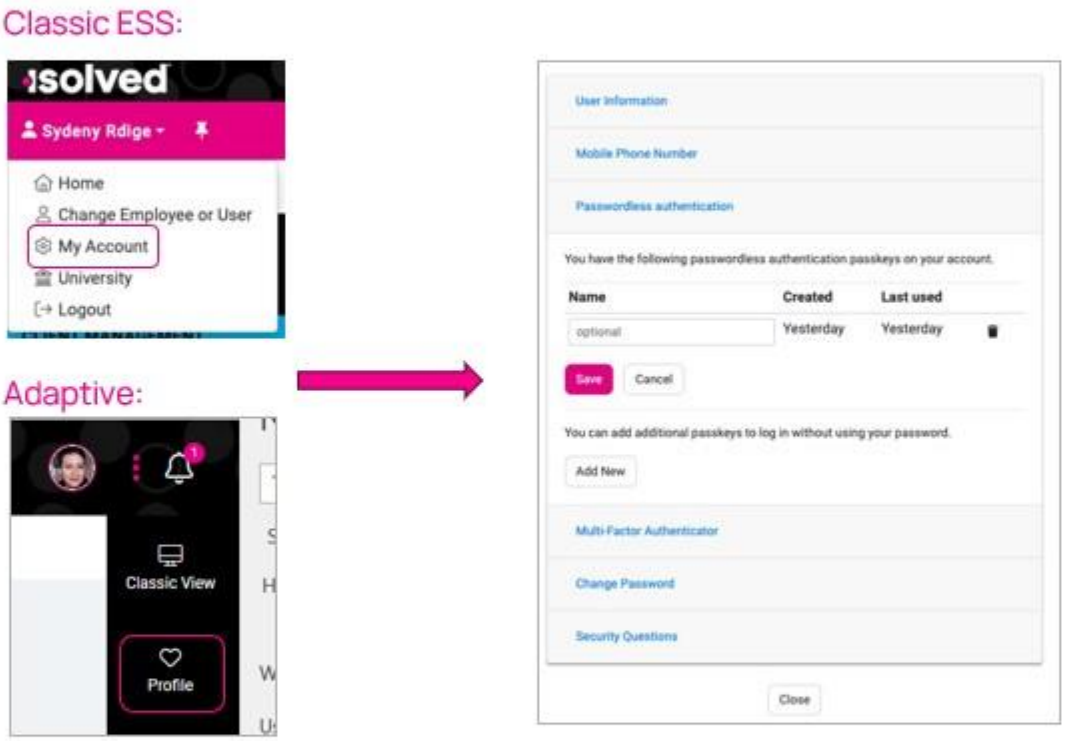


Check your inbox and enter the 6-digit code you were emailed

Security Verification Code

Managing MFA

To make changes, when you are logged in, select **My Account** if you are in the Classic ESS view or **Profile** if you are in the Adaptive Employee Experience.



You have the following passwordless authentication passkeys on your account.

Name	Created	Last used
optional	Yesterday	Yesterday

You can add additional passkeys to log in without using your password.

Commonly Asked Questions

Q: 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.

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: When does this go into effect?
A: The requirement for MFA goes into effect for all isolved users on November 3, 2023.

Q: Why is isolved 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: Can we opt-out of the multi-factor authentication?
A: No.

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 long are user sessions?
A: If a user is using text or email for MFA, upon each initial login, they will have the ability to "Remember this device," or bypass MFA, for twelve (12) hours. This eliminates the need for MFA upon each login for that 12-hour period.