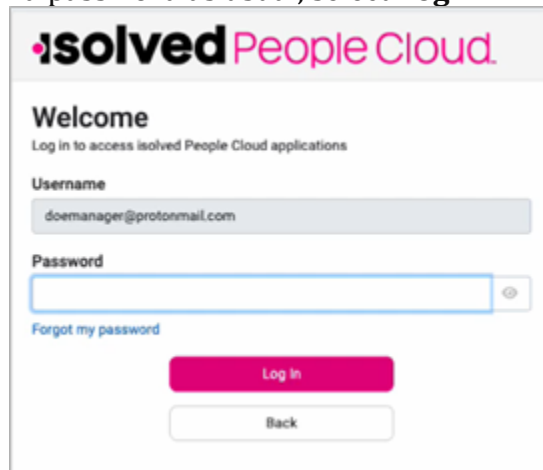


**ATTENTION!** On November 17, 2023, Isolved will require users to use a Multi-Factor Authentication (MFA) every time they log in to Isolved. This is to provide employees with a more secure platform. Please read the important information below about this new requirement. Most users authenticate their account through email and text.

## Logging in

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



The screenshot shows the login page for Isolved People Cloud. At the top, the logo reads "isolved People Cloud". Below the logo, it says "Welcome" and "Log in to access isolved People Cloud applications". There are two input fields: "Username" with the value "doemanager@protonmail.com" and "Password" which is currently empty. A link "Forgot my password" is located below the password field. At the bottom, there are two buttons: a pink "Log In" button and a white "Back" button.

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



The screenshot shows the verification page for Isolved People Cloud. At the top, the logo reads "isolved People Cloud". Below the logo, it says "Please verify your account by selecting one of the methods below:". There are two radio button options: "Email: doemanager@protonmail.com" and "Text Message: (###) ###-4508". The "Text Message" option is selected. At the bottom, there are two buttons: a pink "Request Security Code" button and a white "Cancel" button.

3. Use the code you receive, or you can select **Choose Another Method** to receive the code to the other verification option. 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

**isolved** People Cloud

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

Security Verification Code

Submit

[Choose Another Method](#)

Remember this device?

4. Click on the **Set Up Now** icon to set up your passwordless option.  
**Note:** You are able to make changes to this at any time when logged in by selecting **My Account (Profile)** in Adaptive Employee Experience). Once this is set up, future logins use what you have added for your options. You may be able to use FaceID, Thumbprint, Passcode, or PIN.

**isolved** People Cloud

### Log in without a password

You can use your device's unlock mechanism (PIN, Touch ID, etc) as an easier and more secure alternative to a password.

Note: Anyone who is able to unlock this device can log in without your password.

[Set Up Now](#) [Maybe Later](#)

Don't ask again on this device

Create a passkey for identity-dev.isolvedhcm.com

doemanager@protonmail.com

This passkey will only be saved on this device

[Use a different device](#) [Cancel](#) [Continue](#)

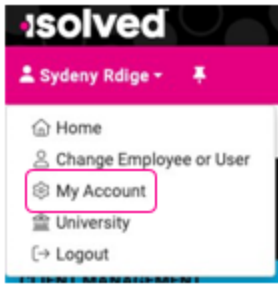


5. Clicking on the **Maybe Later** icon allows you to set up the passwordless criteria later. This does not allow you to bypass the multifactor authentication process.
6. Select **Don't ask again on this device** if you don't want this message to show up again. This does not allow you to bypass the multifactor authentication process.
7. After setting up your passkey, when you log into isolved in the future, you are presented with the option to either use your password or use the passkey.
8. Click here for a [Full Flowchart of Login Steps](#).

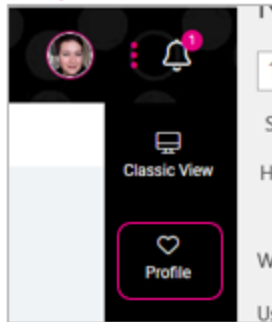
## Managing MFA

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.

## Classic ESS:



## Adaptive:



Name	Created	Last used	
optional	Yesterday	Yesterday	

## Commonly Asked Questions

### Q: What are the key features and functionality?

A: We now offer MFA options outside of email and text messaging. 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 of Internal MFA: Identity Server of MFA regardless. This could be different than what they are used to today depending on the system settings per client.

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

**A:** No.

**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: 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.

**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: Why is isolved requiring MFA?**

**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.

**Q: When does this go into effect?**

**A:** The requirement for MFA goes into effect for all isolved users on November 3, 2023.

**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 long are user sessions?**

**A:** If a user is using text, email or a 3rd party authenticator app 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.

**NOTE:** The 12-hour bypass will be the default option, and this does not impact users who set up passwordless MFA as they are not prompted to enter a code. If the bypass is unchecked, then the system will require MFA after 15 minutes of inactivity .

**Q: Can users have password-less 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 password-less options can be used on multiple devices.

**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 authentication options can be used?**

**A:**

- **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.  
**Note:** Each user needs 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's nothing to install and no codes to enter. Security keys are a great solution if mobile devices aren't an option for users. Keys are available from manufacturers like YubiKey.

**Q: Will this affect SAML?**

**A:** No, SAML is not affected.