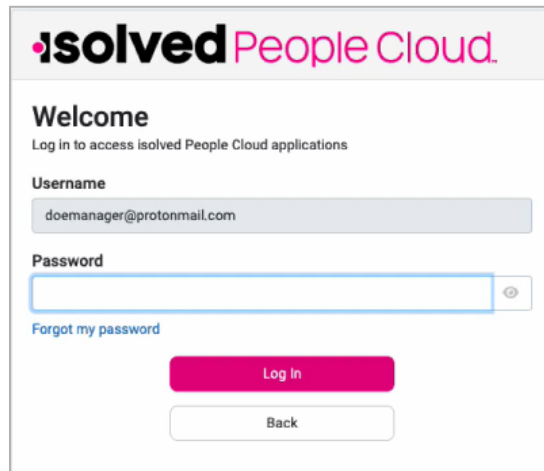


Overview

isolved is committed to protecting your data. All users are required to use Multi-Factor Authentication (MFA) with every login to isolved. This article discusses what to expect the first time you log in after the update.

Logging in

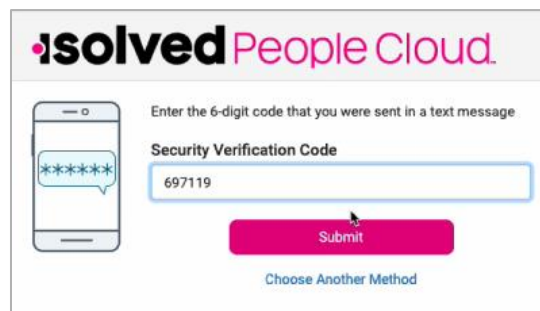
1. Key in your **Username** and **Password** as usual and select **Log In**.



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

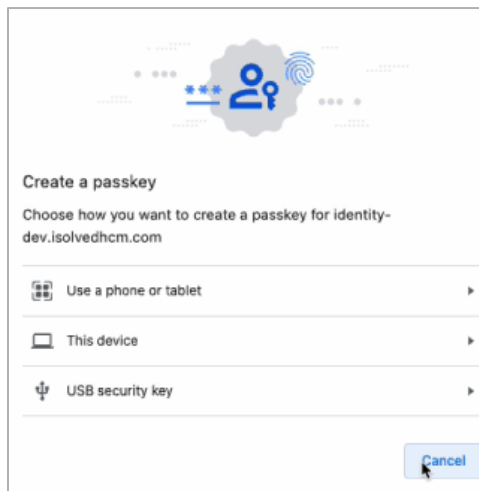
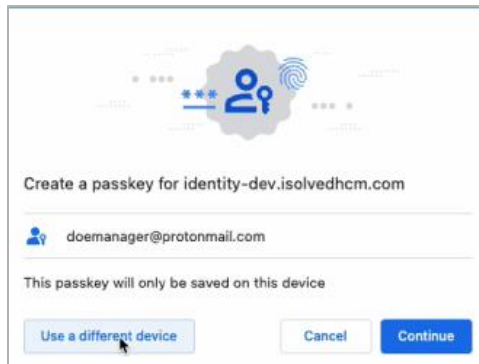


3. Enter the code you receive into the **Security Verification Code** field, or you can select **Choose Another Method** to receive the code to the other verification option. Click on the **Submit** icon.



Help Docs

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.



Help Docs

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](#).

Commonly Asked Questions

Q: What if I don't remember my password?

A: Use the "Forgot Password" option.

Q: What are the key features and functionality?

A: We now offer MFA options outside of email and text messaging. WFA 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 will still need to do some kind Internal FAQs: Identity Server of WFA regardless. This could be different from what they are used to today depending on the system settings per client.

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

No.