

Introduction

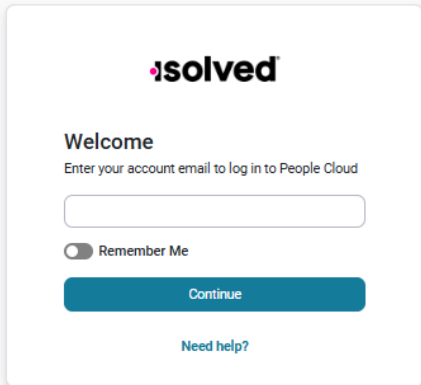
The purpose of this article is to explain the process of logging into Employee Self-Service (ESS), Updating Multi-Factor Authentication (MFA) settings and to provide some tips and tricks.

Logging In

In order to log into isolved, enter your Employee Self-Service email address, and the password you created when you authenticated your account. Please ensure that passwords are a minimum of 12 characters, at least one lower-case alpha (a-z), one upper-case alpha (A-Z), one numeric (0-9), and one special character. Spaces are allowed to support the use of easier to remember passphrases. Going forward, your password will not expire. Passwords may also not duplicate any of your previous ten passwords.

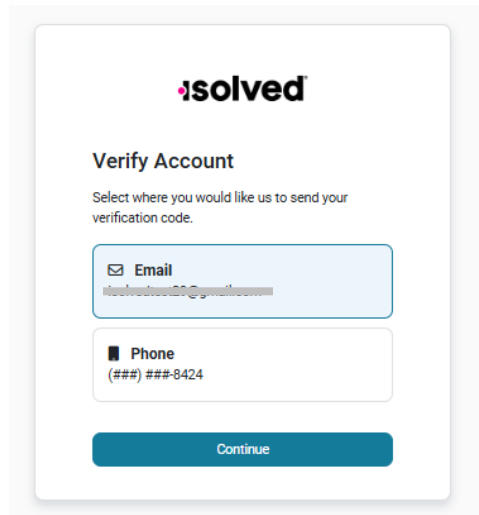
If you enter an incorrect password five times, the system locks you out. You receive a message after each attempt, indicating the number of attempts remaining. After the fifth incorrect attempt, you are locked out for ten minutes. After ten minutes, use the **Did you forget your password** link to change your password. If you need access to the system sooner, contact your company's administrator to unlock your account.

1. Key in your **Username** select **Next**.

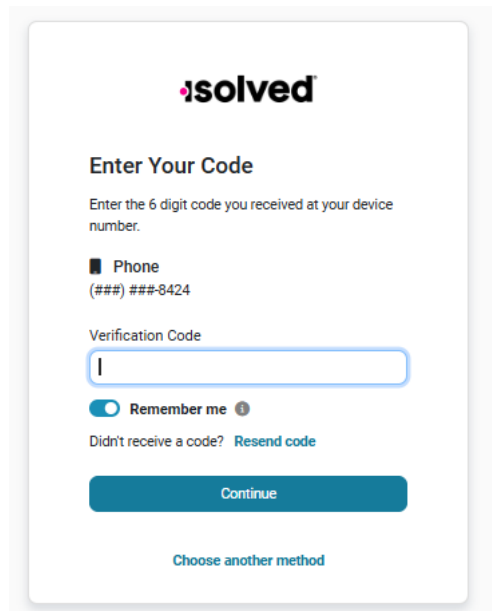


2. Key in **Password** and select **Log In**.
3. Select a verification option, then select **Request Security Code**.

Note: The “Text” option appears only if you entered your cell phone number during authentication. If you have not verified your phone number in over a year, the system prompts the user to confirm or update their phone number.



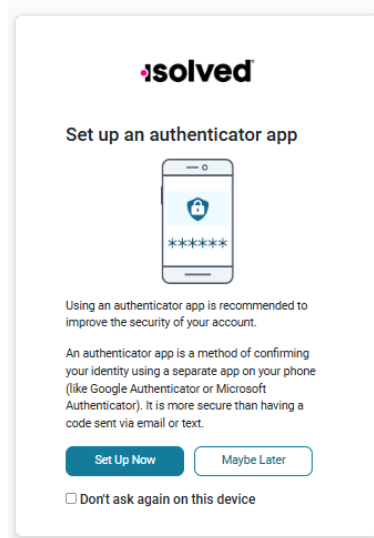
4. Enter the code you receive into the **Security Verification Code** field, or you can select **Choose Another Method** to receive the code to the other verification option. Click on the **Submit** icon. On this screen, you can select the “Remember me on this device” (note: this is selected by default on initial login). If this option is checked, then your security verification is valid for 12 hours. If the box is not checked, you’ll be asked to authenticate at any subsequent login, regardless of the amount of time that has passed. Whatever you elect to do with checking or unchecking the box will stay as the default until either a different selection is made, or 30 days has passed with no change, at which time the box will revert to being checked.




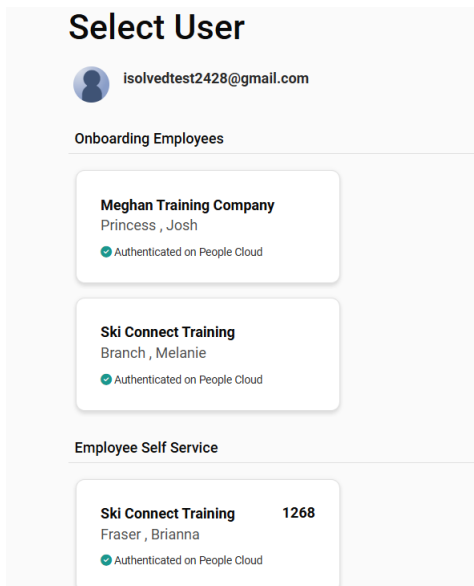
5. You are then given several options to set up a Passwordless Login
 - a. **Set Up Now** icon to set up your passwordless option.
Note: You are able to make changes to this at any time when logged in by selecting **My Account (Profile)** in Adaptive Employee Experience). Once this is set up, future logins use what you have added for your options. You may be able to use FaceID, Thumbprint, Passcode, or PIN.
 - b. The **Maybe Later** option allows you to set up the passwordless criteria later. This does not allow you to bypass the authentication process. If the **Maybe Later** option is selected, you’re presented the

opportunity to set up an authenticator app for subsequent logins. This, too, you can choose to Set Up Now, or you may set it up at a later juncture. Choosing **Set Up Now** leads you through the steps to set up your authenticator app.

- c. 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 authentication process.



- 6. Going forward, you can log in to your account by either of these methods:
 - a. Entering your password (this option requires entering a code sent to your email or phone).
 - b. If you've elected to utilize a passwordless option (authenticator app or passkey), you'll have the option to select passkey  when you log in to isolved which allows you to use the passkey you enabled for that device or the authenticator app that you set up. Even if you've opted to set up passwordless login, you can still enter a password.
- 7. When logging with **Adaptive Employee Experience (AEE) or Mobile App** if user is attached to multiple sites, you will have a tile for each site to select.



Account Lock

isolved automatically locks an account after 5 unsuccessful login attempts. As the user attempts fail, a message counts down the remaining attempts before the account is locked.

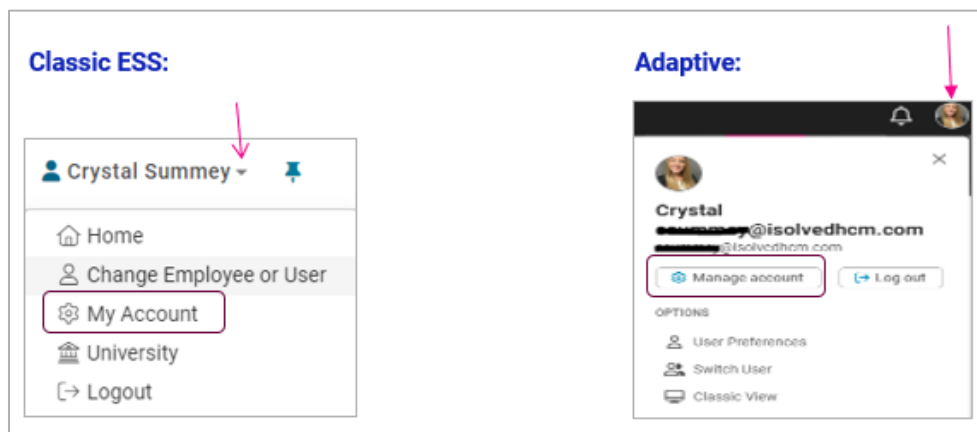
If an account is locked, it is denoted by a check mark in the “Self Service Account Locked” box on the Employee **General** screen. To unlock a locked account, click on the check box to remove the mark, then click **Save**. If no action is taken by the Client User to unlock, the account will automatically unlock after 10 minutes. It is recommended to use the “Forgot Password” function after the account is locked to reset the password.

Screen Activity Timeout

isolved will close after 20 minutes of inactivity. This timeout is set at the server-level and cannot be changed. This is a security measure to keep information safe.

Managing Multi-Factor Authentication (MFA)

To make changes, when you are logged in, select **My Account** if you are in the **Classic ESS** view or **Manage account** if you are in the **Adaptive Employee Experience (AEE)**.



You are directed to your **My Account** page to make changes. Depending on the security levels setup by your organization, the user is asked to authenticate before updating any information on the **My Account** Screen.

Security Features

To enhance employee security with People Cloud, we have added a **Breached Password Protection** feature, along with new **Unrecognized Device Email Notifications**.

Breached Password Protection

Automatic Detection:

Our system continuously monitors usage of breached passwords using a comprehensive 3rd party database of known breaches commonly found on the dark web.

If a user's password is found to be compromised, the system will automatically flag it.

Mandatory Password Change:

Users with breached passwords are required to change their password immediately after a successful login. They are also asked to setup new authentication methods such as a new authenticator app or passwordless authentication.

The system will guide users through a secure password reset process to ensure their account remains protected.

isolved People Cloud

Change Password

▲ Password Update Required ×

You're accessing isolved with a password found on a breached list. For your security, We are requiring a password reset on your account. This reset will remove any authenticator apps and passwordless authentication methods (passkeys).

After changing your password, you can setup a new authenticator app or add a new passwordless method (passkey) to enhance your login experience.

Create New Password (required)

Your new password must contain:

- Password strength
- Minimum length of 12 characters
- At least on uppercase character (AZ)
- At least one special character (#*!\$)
- At least one digit (0-9)

Re-enter Password (required)

Confirm Password and Login

If a user tries to change the password to a breached password or if they try to register an account with a breached password, they would receive the following error:

isolved People Cloud

Change Password

× Password Security ×

This password was detected on a breached list, and was rejected to maintain your security. Please enter a new password.

Create New Password (required)

● Password security not met

Your new password must contain:

- Password strength
- Minimum length of 12 characters
- At least on uppercase character (AZ)
- At least one special character (#*!\$)
- At least one digit (0-9)

Re-enter Password (required)

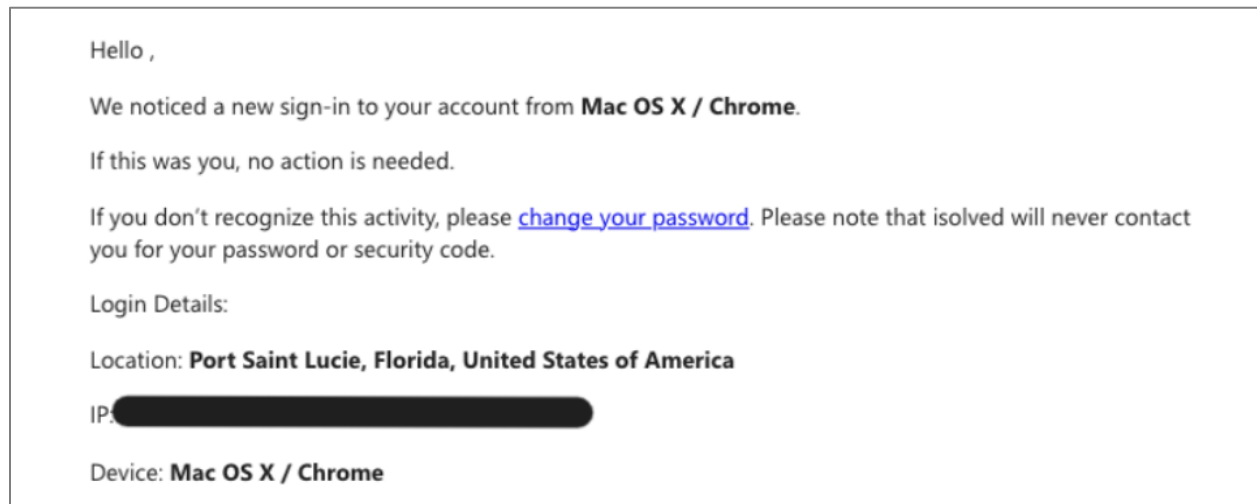
Confirm Password and Login

Profile Email Notifications

Unrecognized Device Usage:

Users will receive an email notification when their account is accessed from an unrecognized device. This will enhance account security by informing users of potential unauthorized access, allowing them to take immediate action if necessary.

It will only be sent to the user experiencing the issue and is sent from noreply@isolvedhcm.com.



This will be detected based off the IP address and browser. Currently it utilizes 90 days of previous IP/Browser history for comparison. More factors will be added so that we can more accurately depict suspicious activity.

Currently, the Identity admin will be able to see if a user was forced to reset their password on the logs. With an upcoming release, a flag will be visible if the user is found to have a bad password.

UserChangePasswordAfterLogin

Please note the user is not locked out. The system is alerting the user that they need to either reset (breached password) or be aware about the login location.

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 type of MFA, regardless. This could be different from what they are accustomed to depending on the system settings per client.

Q: Can we opt-out of the multifactor authentication?

No.

Q: Is the timeout in AEE changing? Right now, they can stay logged in for up to 30 days.

A: Yes,

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 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: How does SAML function in combination with MFA?

A: SAML is something clients can configure to use their own login mechanisms instead of our Identity Server. An example of SAML is OneLogin or MicrosoftApps/Authenticator. Internally, we log into that and then have access via SSO to all our "isolved apps." Some clients may have this set up for their business already.