State of Alaska EVV
Therap Aggregator and
Login Platform Modernization

Business Requirements Document
Version 1.0
9/25/2023

Version History

Version	Date	Modifications
1.0	9/25/2023	Initial Draft

Table of Contents

Abbreviation Definitions

Abbreviation	Definition
OTP	One Time Passcode
2FA	Two factor Authentication
QR Code	Quick Response Code

Overview

Therap will be ending the use of the Okta login tool and transitioning to a login platform completely hosted by Therap. This will increase efficiency and allow Therap to offer more User controls for themselves in the Aggregator. In addition, Admin Users for each agency will be able to have more controls over their staff users' access as well.

First Time Login

First Time Login (Post Release)

After the release and change to the Therap login platform, when Aggregator users log in for the first time, they will be required to follow the steps to set up their new password and set up their required Two factor Authentication.

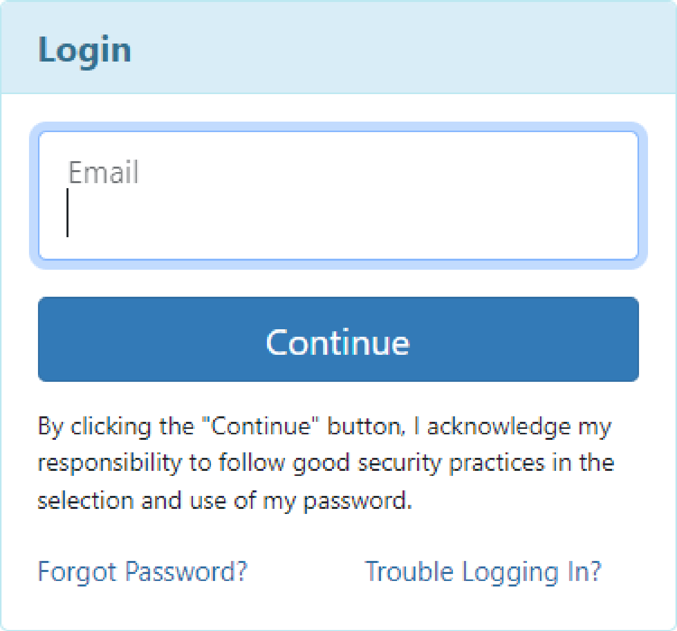
Contact AKsupport@therapservices.net if there are any problems with your first-time login.

Saved Temporary Transition Password

After the release, users will be able to log into their current account using their existing email addresses. Users will find the **New** login page for the Aggregator here:

https://secure.therapevv.net/auth/login

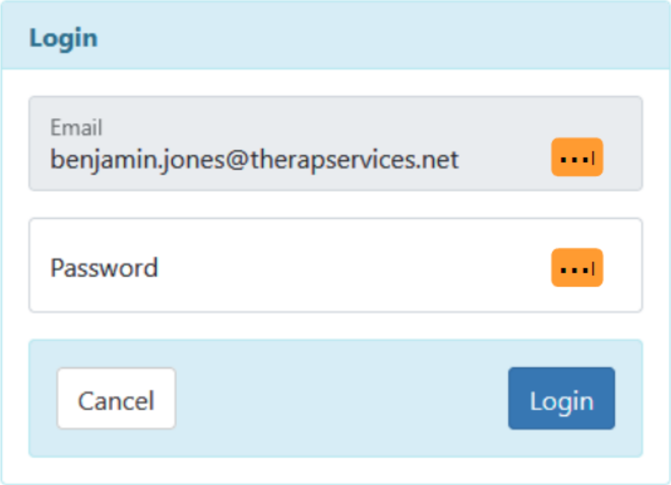
On the next screen, users will need to enter the email address and click continue. This will be the same email address they used for the Okta login platform previously.



By clicking the "Continue" button, I acknowledge my responsibility to follow good security practices in the selection and use of my password.

On the next screen, users will have the option to put their password in their password field.

IMPORTANT: For the first-time login, users must use the temporary transition password they created and previously saved to log in.



Login

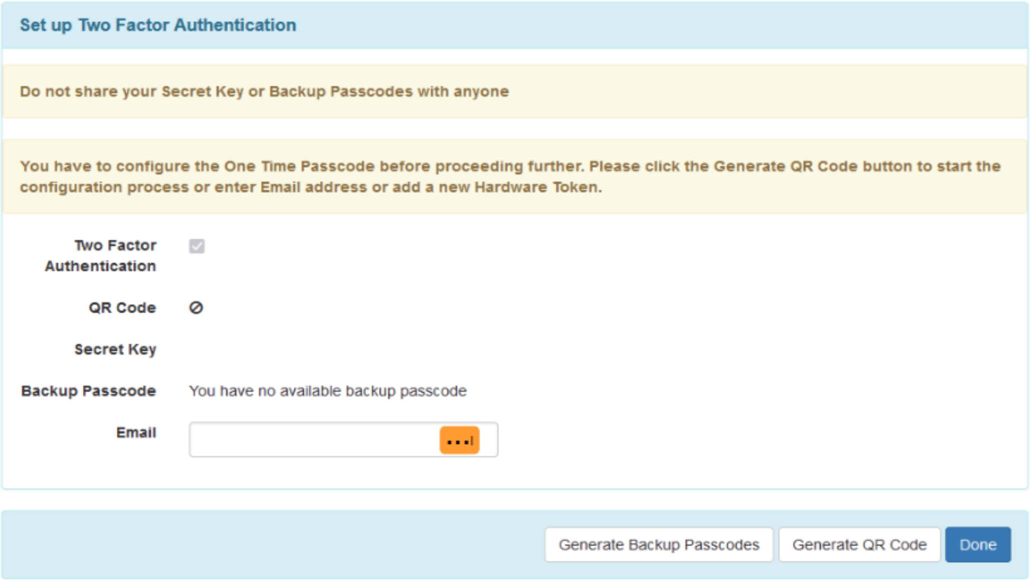
Email
benjamin.jones@therapservices.net

Password

Two-Factor Authentication

All users are still required to use a Two Factor Authentication to access the Therap Aggregator. Users will be required to set up their Two Factor Authentication in order to complete login setup as part of the initial login to the new platform and to successfully log in subsequently. Users will not be able to take any further actions until this setup is completed.

Users have the option to use an Authenticator (QR Code), their email, generate Backup Passcodes, and/or a Secret Key provided as their Second Factor. On the next screen, users will be required to set up at least one 2FA (second factor) option.



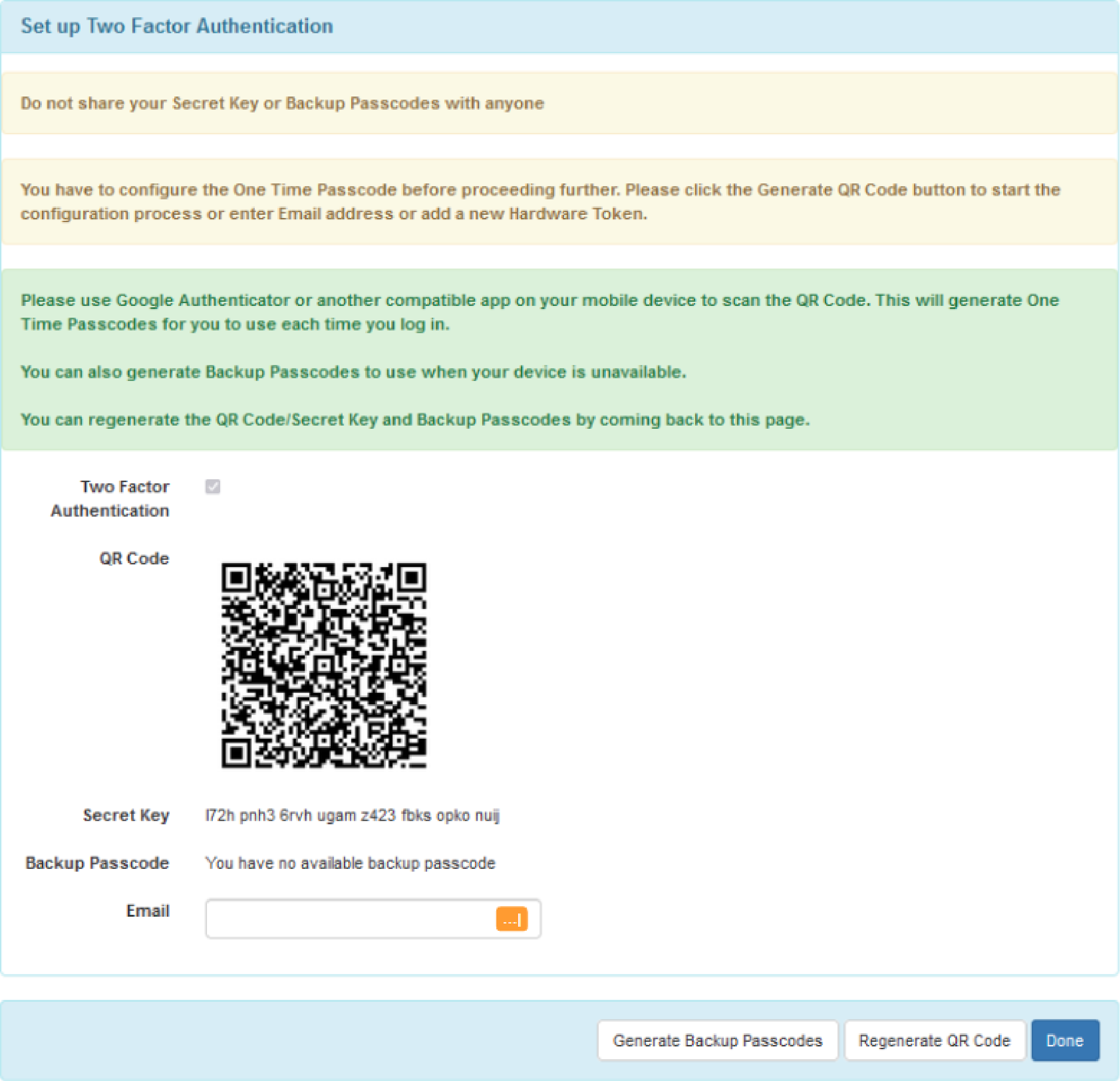
Set up Two Factor Authentication

Do not share your Secret Key or Backup Passcodes with anyone

You have to configure the One Time Passcode before proceeding further. Please click the Generate QR Code button to start the configuration process or enter Email address or add a new Hardware Token.

Two Factor Authentication	☑
QR Code	⊘
Secret Key	
Backup Passcode	You have no available backup passcode
Email	

To set up an Authenticator to use as your 2FA, click “Generate QR Code” and open your Authenticator app to scan this code. Please use Google Authenticator or another compatible app on your mobile device to scan the QR Code. This will generate a One Time Passcode for you to use each time you log in.



Set up Two Factor Authentication

Do not share your Secret Key or Backup Passcodes with anyone

You have to configure the One Time Passcode before proceeding further. Please click the Generate QR Code button to start the configuration process or enter Email address or add a new Hardware Token.

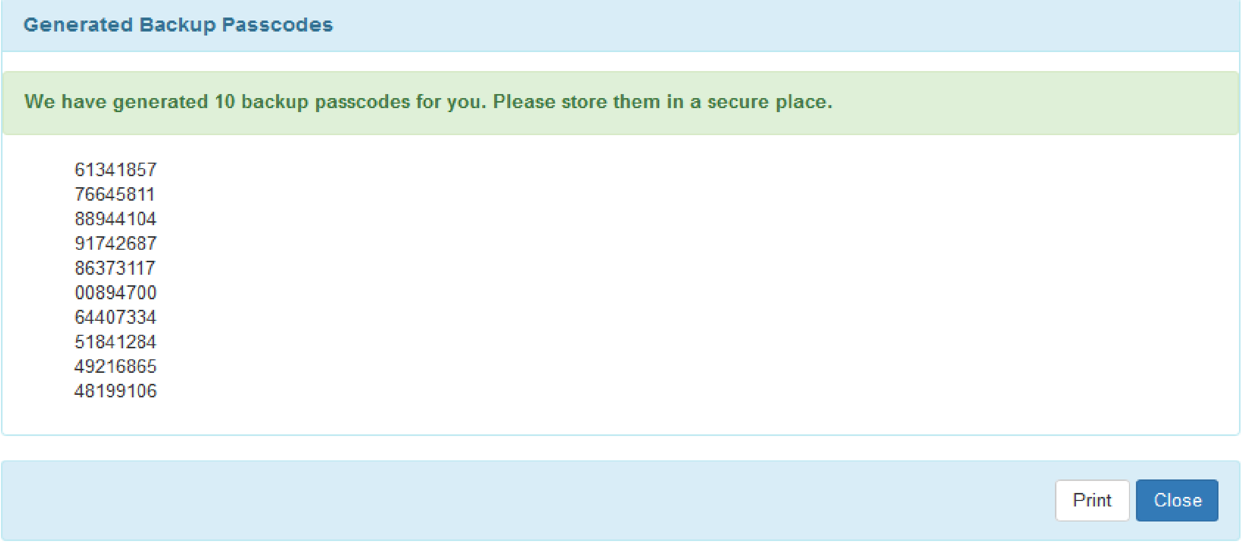
Please use Google Authenticator or another compatible app on your mobile device to scan the QR Code. This will generate One Time Passcodes for you to use each time you log in.

You can also generate Backup Passcodes to use when your device is unavailable.

You can regenerate the QR Code/Secret Key and Backup Passcodes by coming back to this page.

Two Factor Authentication	☑
QR Code	
Secret Key	l72h pnh3 6rvh ugam z423 fbks opko nuij
Backup Passcode	You have no available backup passcode
Email	

To generate backup codes to use one time each as your 2FA, click "Generate Backup Passcodes" and save these codes securely. This will generate 10 backup codes that can be used one time to log in.

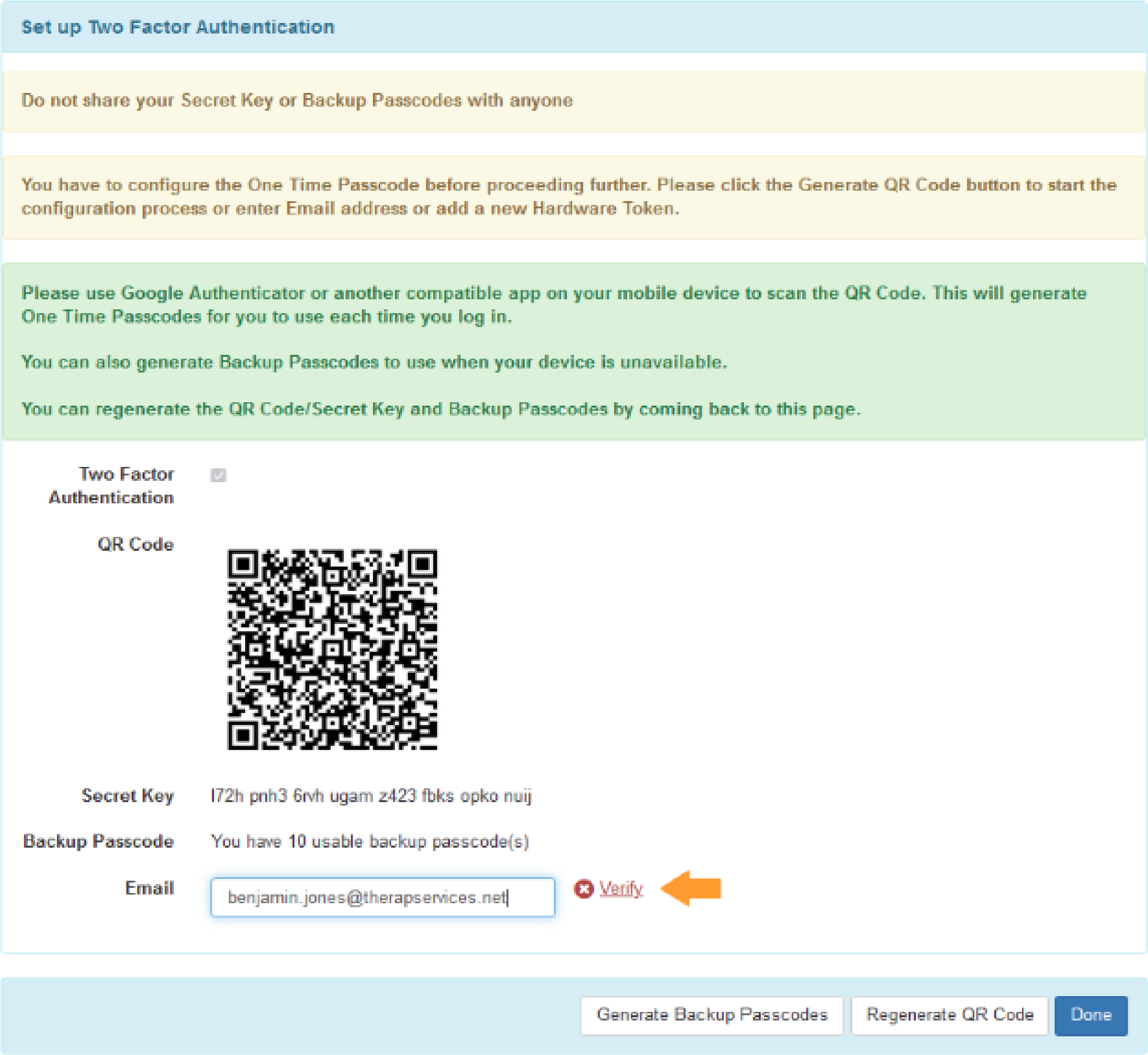


Generated Backup Passcodes

We have generated 10 backup passcodes for you. Please store them in a secure place.

```
61341857
76645811
88944104
91742687
86373117
00894700
64407334
51841284
49216865
48199106
```

To use your email as your 2FA, enter your email and verify it by clicking the “link to Verify and entering the token you receive in that email account.



Set up Two Factor Authentication

Do not share your Secret Key or Backup Passcodes with anyone

You have to configure the One Time Passcode before proceeding further. Please click the Generate QR Code button to start the configuration process or enter Email address or add a new Hardware Token.

Please use Google Authenticator or another compatible app on your mobile device to scan the QR Code. This will generate One Time Passcodes for you to use each time you log in.

You can also generate Backup Passcodes to use when your device is unavailable.

You can regenerate the QR Code/Secret Key and Backup Passcodes by coming back to this page.

Two Factor Authentication ☑

QR Code

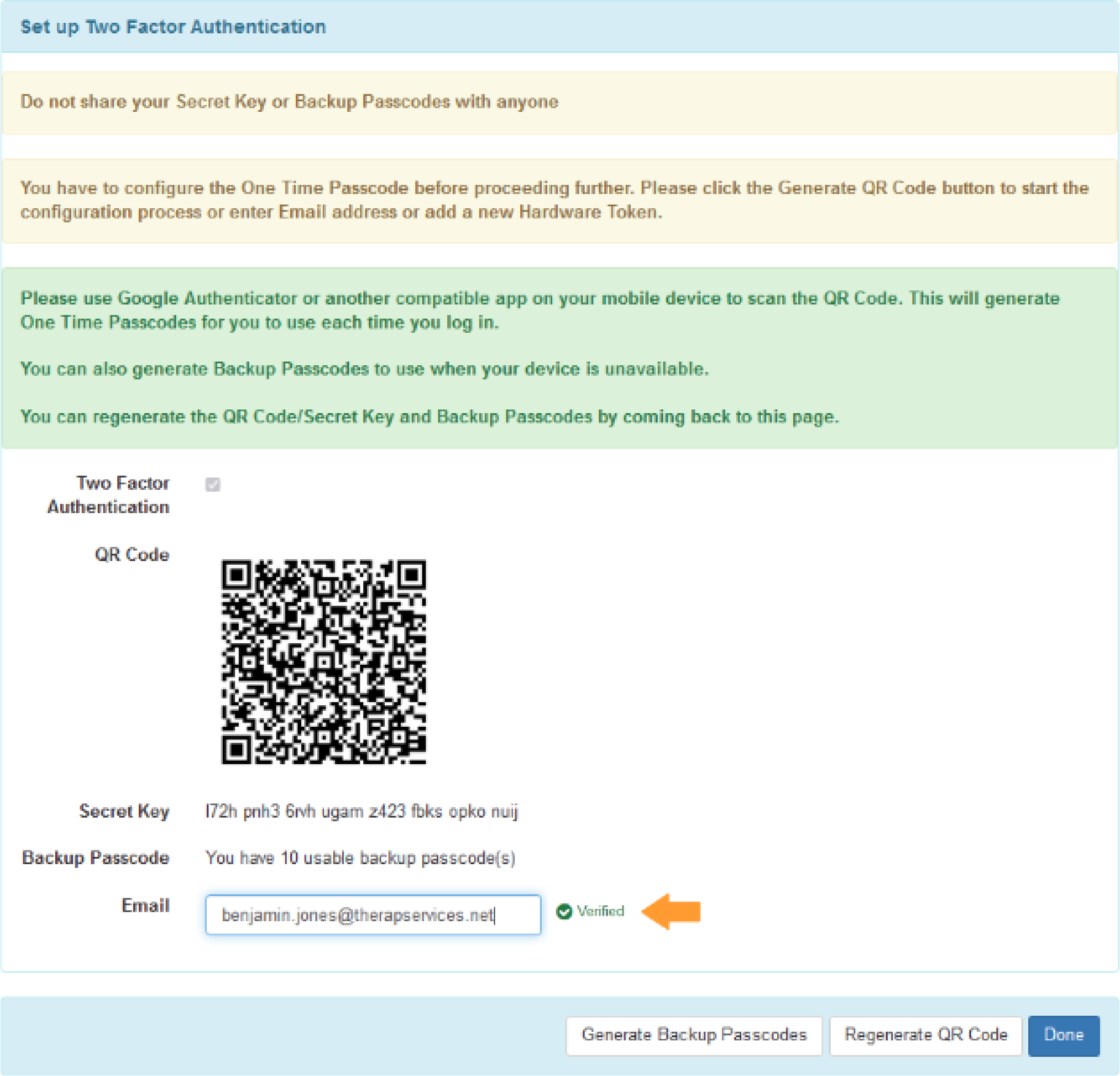
Secret Key l72h pnh3 6rvh ugam z423 fbks opko nuij

Backup Passcode You have 10 usable backup passcode(s)

Email benjamin.jones@therapservices.net

Please note the following:

- Some users have reported the Therap email housed in their spam folder or quarantined accounts.
  - Please ensure you can accept an email from Therap
- The token received is time-sensitive.



Set up Two Factor Authentication

Do not share your Secret Key or Backup Passcodes with anyone

You have to configure the One Time Passcode before proceeding further. Please click the Generate QR Code button to start the configuration process or enter Email address or add a new Hardware Token.

Please use Google Authenticator or another compatible app on your mobile device to scan the QR Code. This will generate One Time Passcodes for you to use each time you log in.

You can also generate Backup Passcodes to use when your device is unavailable.

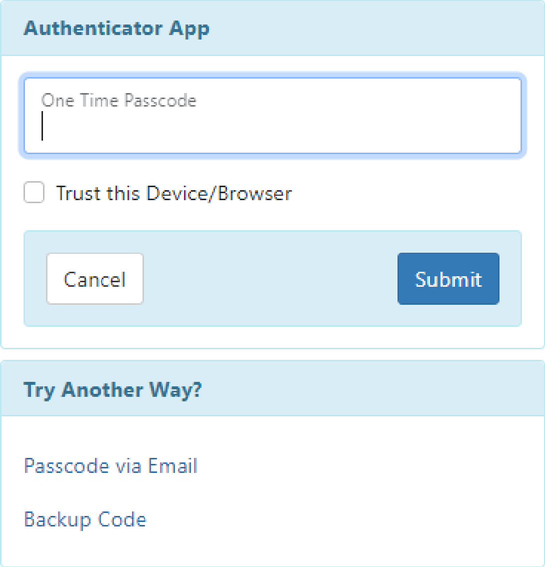
You can regenerate the QR Code/Secret Key and Backup Passcodes by coming back to this page.

Two Factor Authentication	☑
QR Code	
Secret Key	l72h pnh3 6rvh ugam z423 fbks opko nuij
Backup Passcode	You have 10 usable backup passcode(s)
Email	benjamin.jones@therapservices.net ✓ Verified

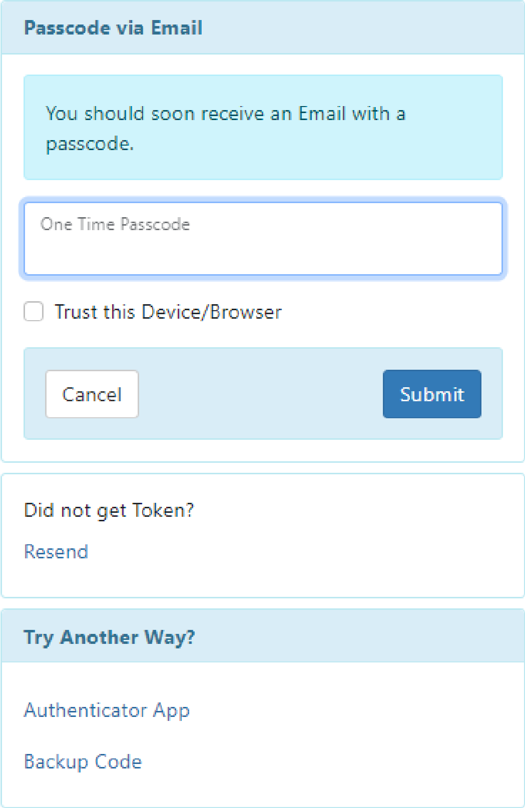
Users can update and manage this directly after logging in successfully. The details are described in the Two Factor Authentication section.

The next time you log in, you will be asked to enter your 2FA based on the 2FA options you have set up. If you have set up more than one method, you will see options to switch and try using a different 2FA to log in.

Authenticator App 2FA

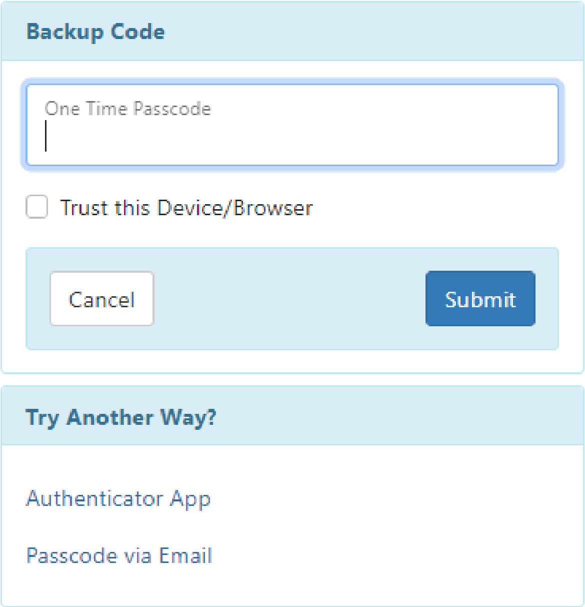


Email 2FA



You should soon receive an Email with a passcode.

Backup Code 2FA



Backup Code

One Time Passcode

☐ Trust this Device/Browser

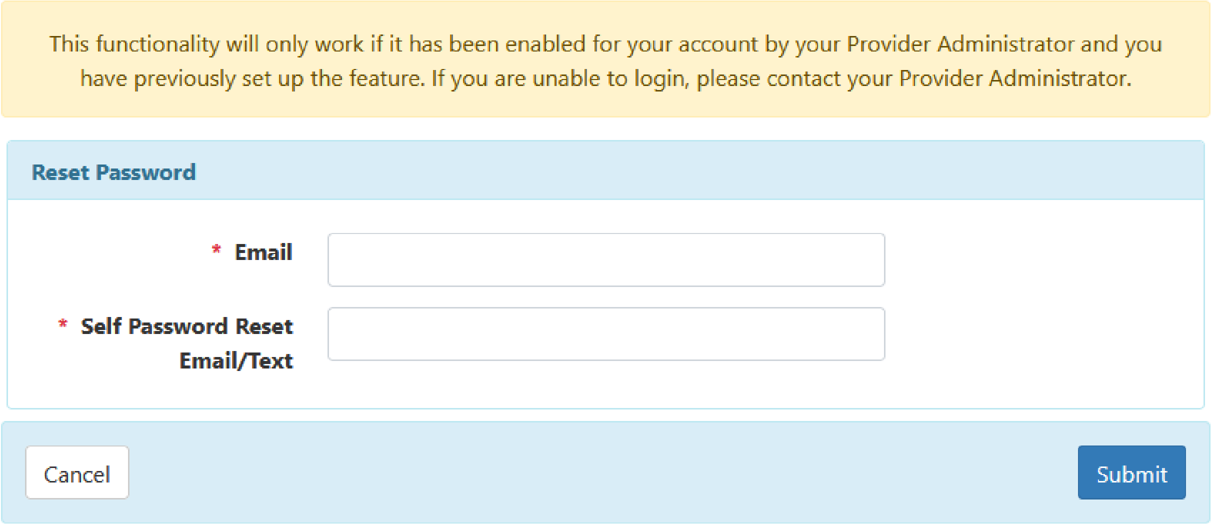
Try Another Way?

Authenticator App

Passcode via Email

Self Password Reset

Users can now use Self Password Reset by clicking on Forgot Password? Or Trouble Logging In? And use their Email to reset their passwords themselves. By default, users will find their Login Email already set as Email for Self Password Reset Configuration.



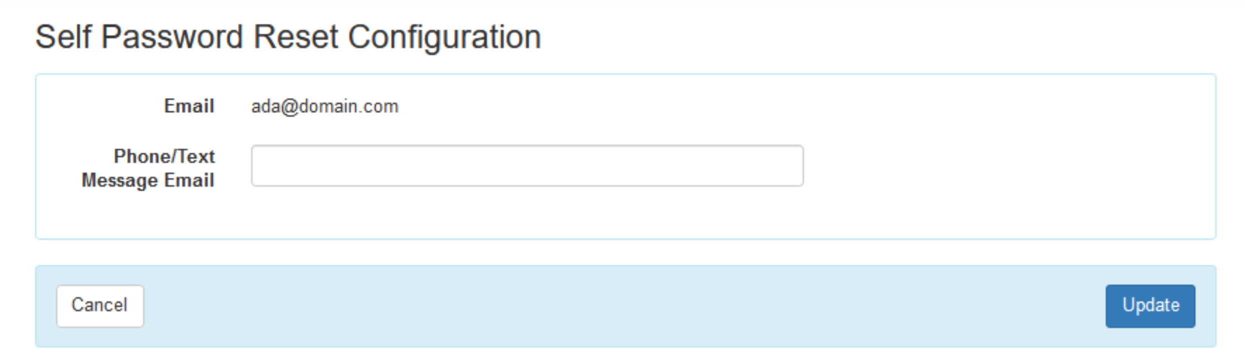
This functionality will only work if it has been enabled for your account by your Provider Administrator and you have previously set up the feature. If you are unable to login, please contact your Provider Administrator.

Reset Password

* Email

* Self Password Reset Email/Text

Users must have previously configured their Self Password Reset in order to use this option of logging in.



Self Password Reset Configuration

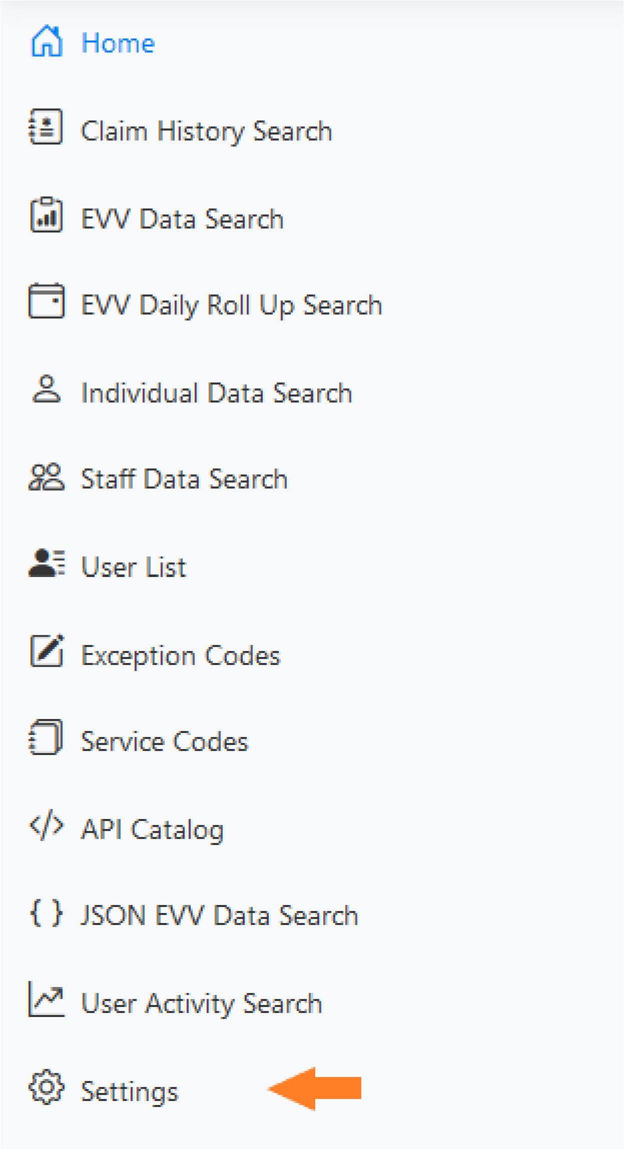
Email	ada@domain.com
Phone/Text Message Email	

Contact AKsupport@therapservices.net if there are any problems with your first-time login.

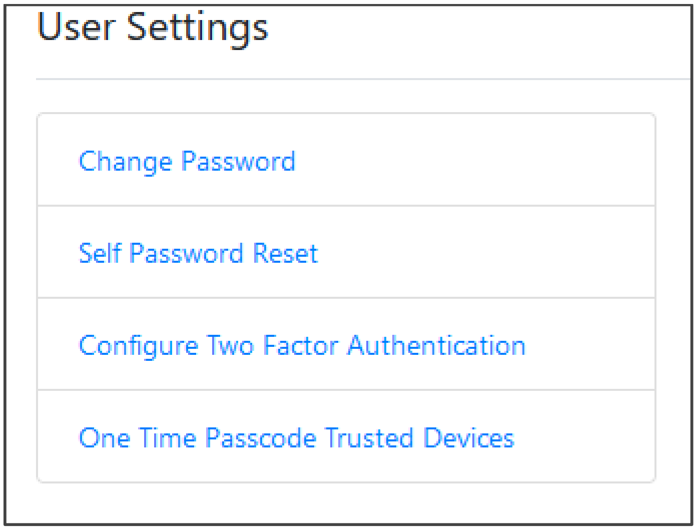
New Settings Features

After the release and the login platform change, Users will have a new Settings option from which they will be able to change their password, Configure Self Password Reset, Configure Two Factor Authentication, and One Time Passcode (OTP) Trusted Devices in the User Settings section.

Additionally, Provider Super Admin Users will have the ability to view their Password Policy and set Provider Preference.



Regular users will have the following options:


User Settings

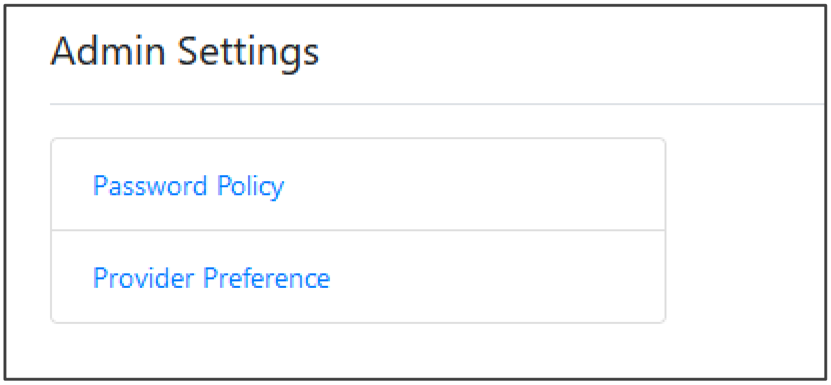
Change Password

Self Password Reset

Configure Two Factor Authentication

One Time Passcode Trusted Devices

Admin User will find additional options to set provider password policy and Provider Preference.

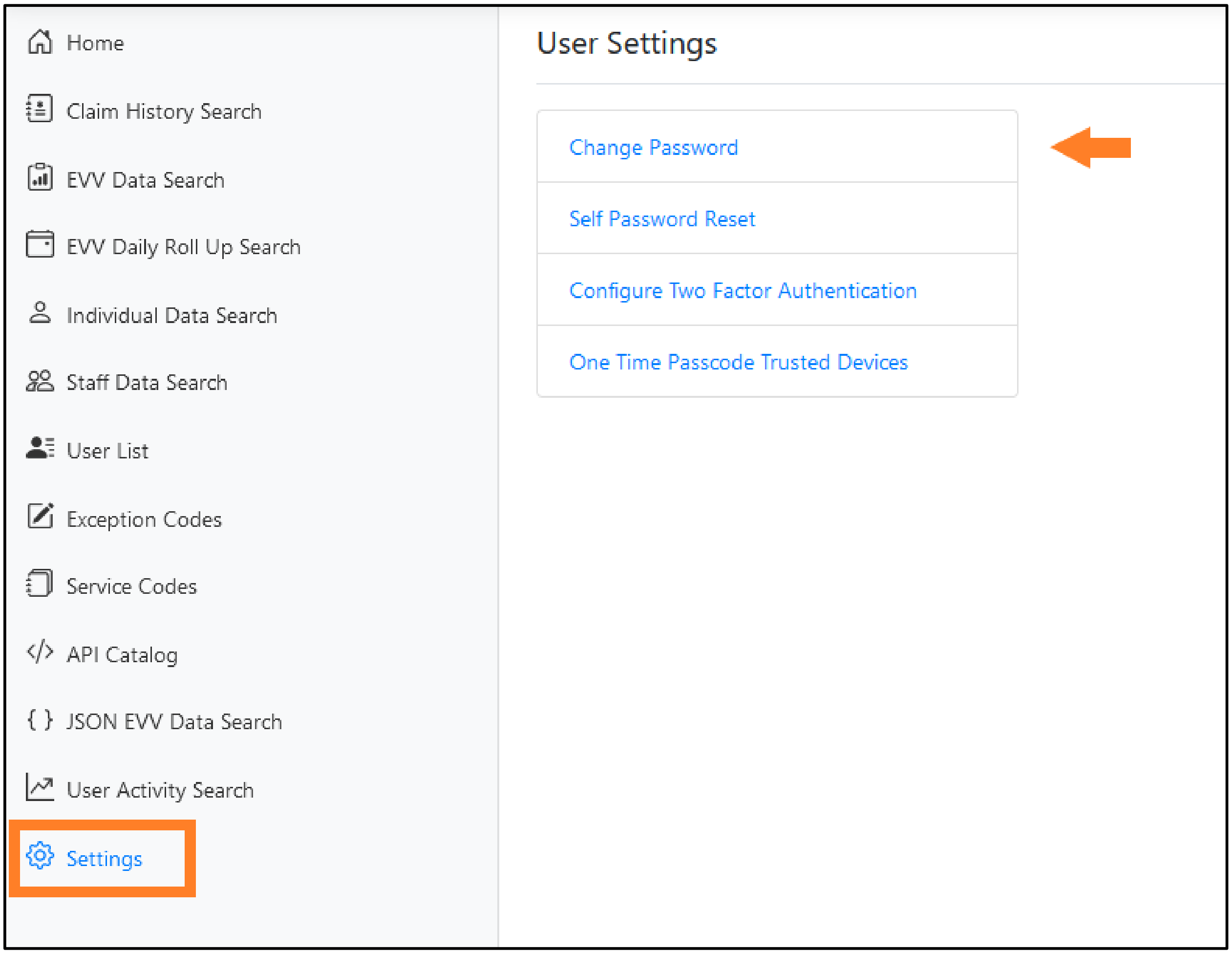

Admin Settings

Password Policy

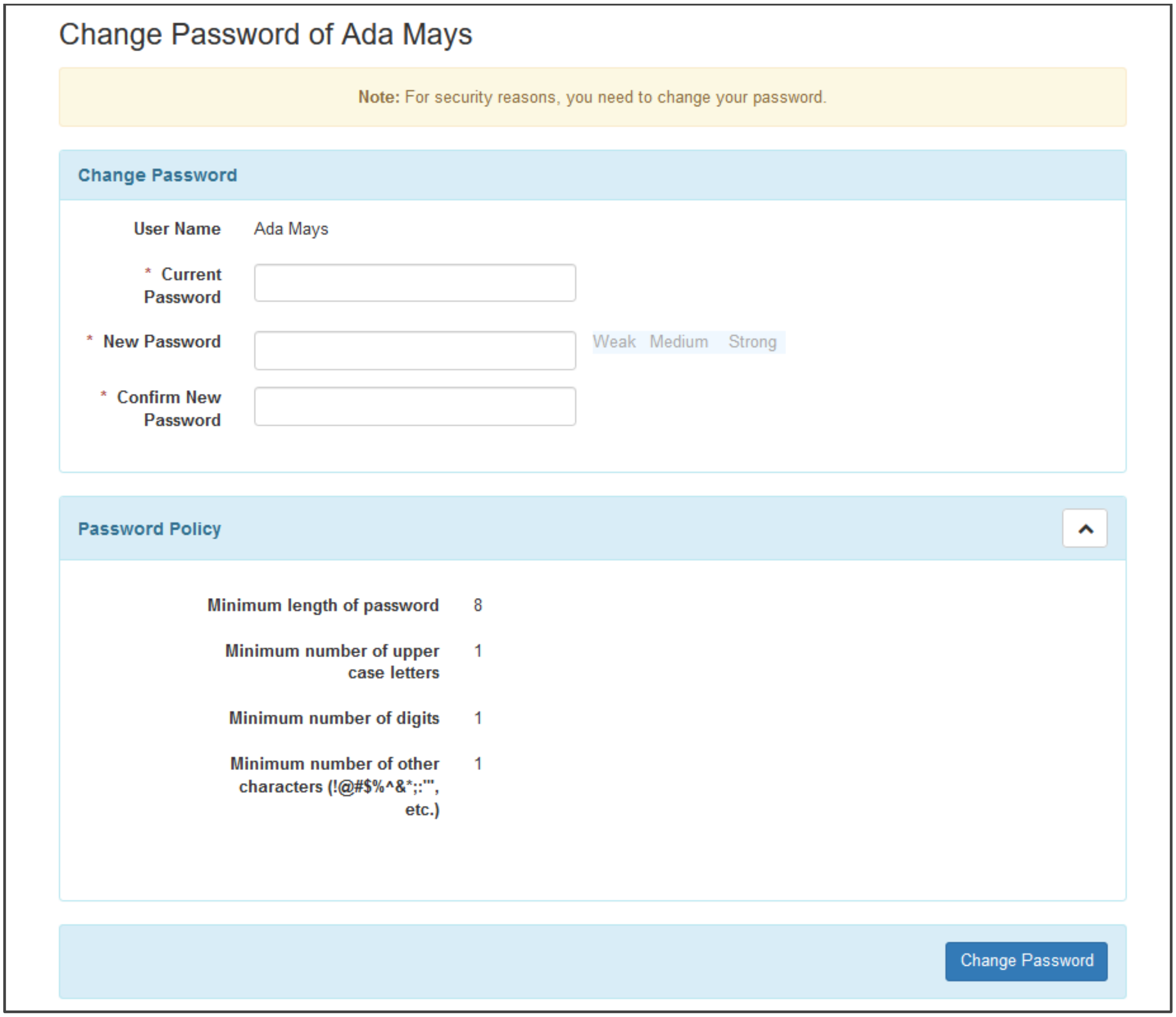
Provider Preference

Change Password

Users can change their password themselves at any time by clicking on Settings and selecting Change Password.



Upon clicking “Change Password,” they will be able to view the Change Password page. To complete the password change, they will need to put in their old password to confirm the new password. Users will also be able to see the password policy while setting up their new password.



Change Password of Ada Mays

Note: For security reasons, you need to change your password.

Change Password

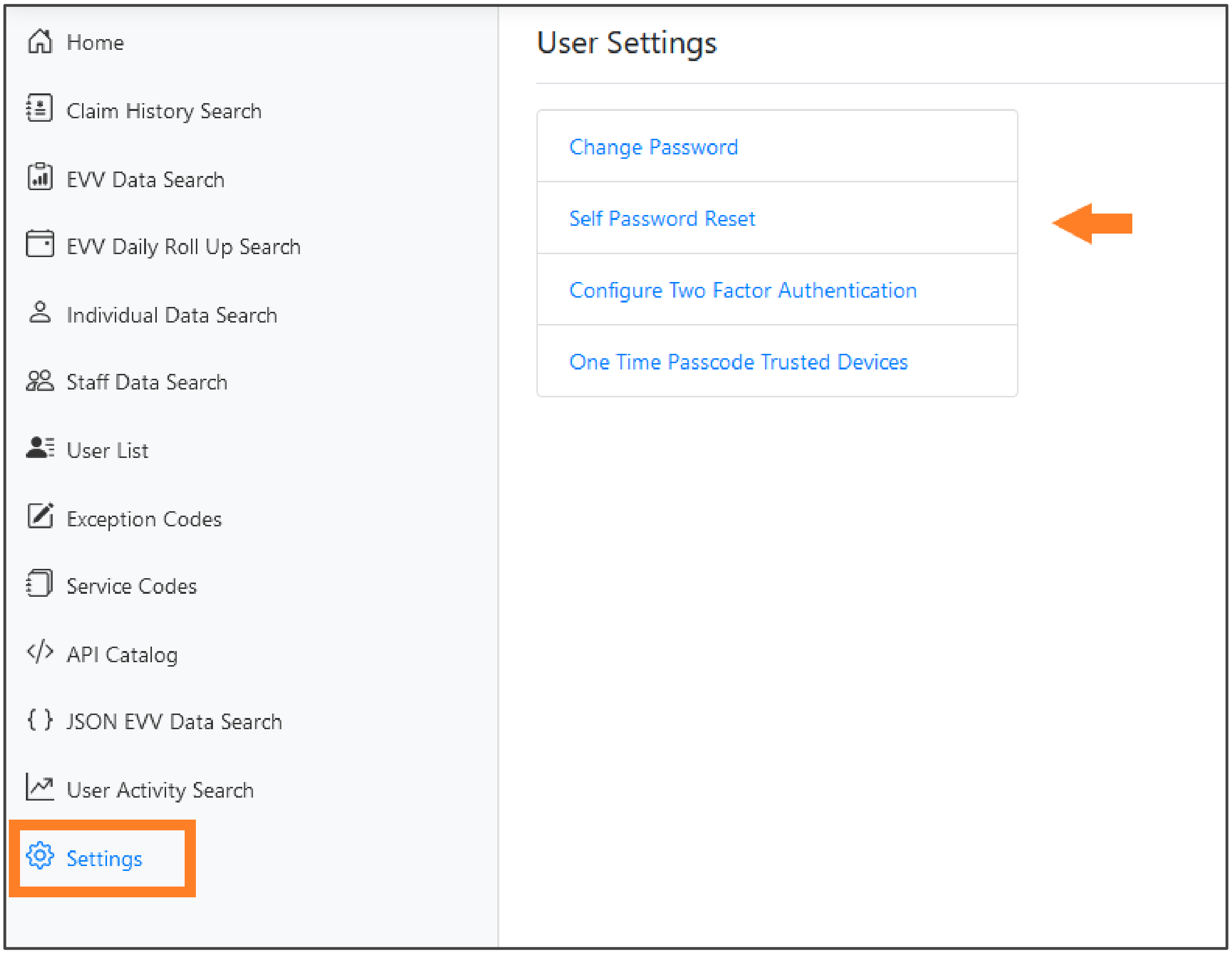
User Name	Ada Mays
* Current Password	
* New Password	Weak Medium Strong
* Confirm New Password	

Password Policy

Minimum length of password	8
Minimum number of upper case letters	1
Minimum number of digits	1
Minimum number of other characters (!@#$%^&*;:'", etc.)	1

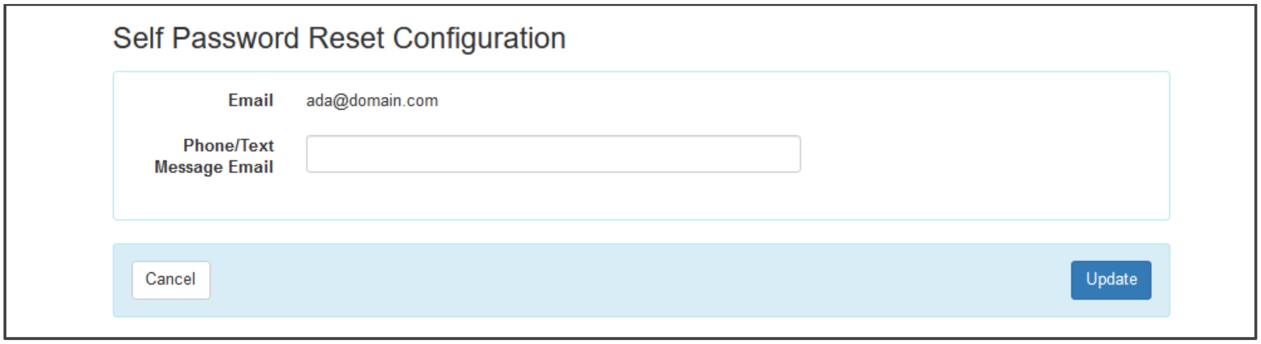
Self Password Reset

Users will find the option to configure their Self Password Reset from the following link.



Users can use their login Email to reset their password by themselves. If they want to configure their Phone/Text Message Email, they have to provide the correct email address for their cell phone provider in the corresponding fields.

To configure Self Password Reset for a mobile device please see the following Self Password Reset Tokens via Mobile SMS Text.

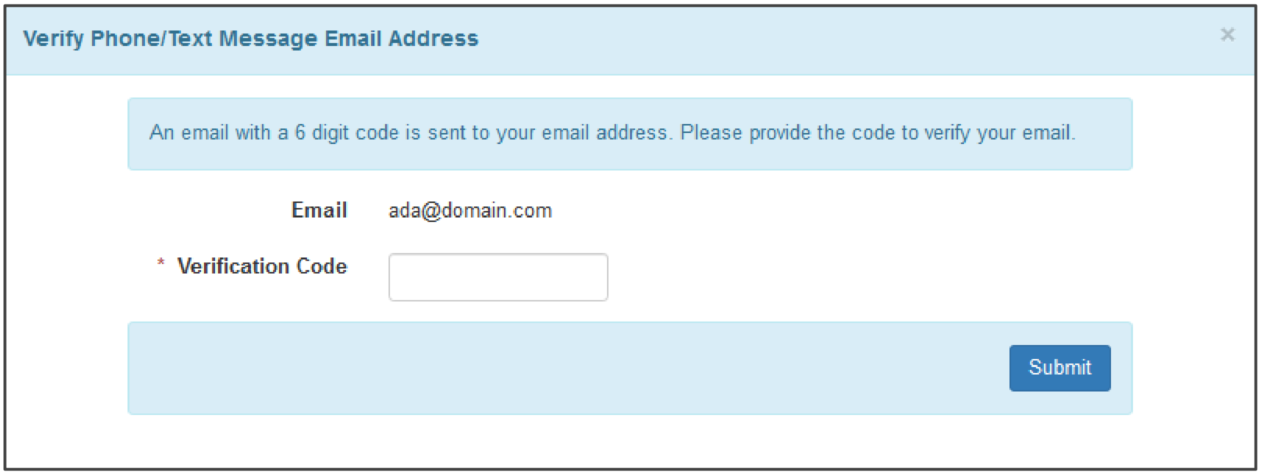


Self Password Reset Configuration

Email ada@domain.com

Phone/Text Message Email

To complete setting up their Phone/Text Message Email, users will need to verify their email address by entering the verification code sent to their provided Email address.

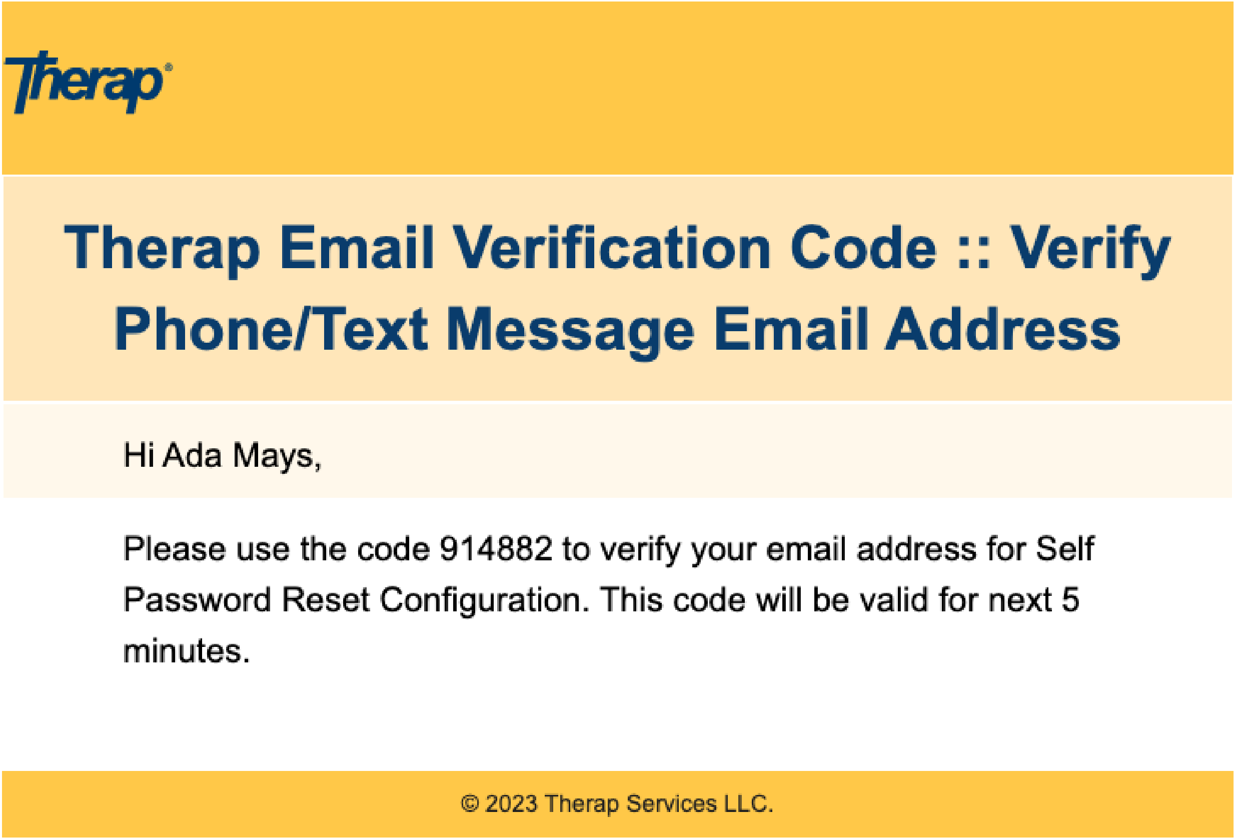


Verify Phone/Text Message Email Address

An email with a 6 digit code is sent to your email address. Please provide the code to verify your email.

Email ada@domain.com

* Verification Code



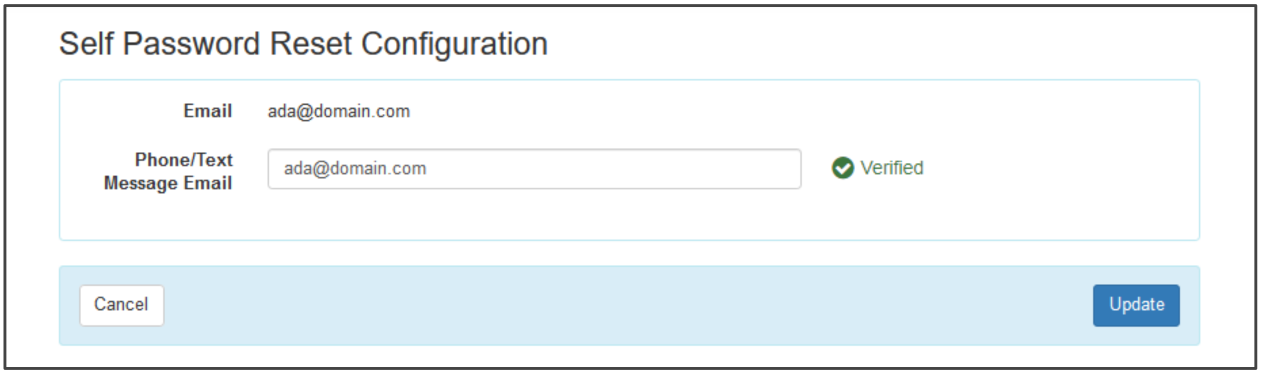
Therap Email Verification Code :: Verify Phone/Text Message Email Address

Hi Ada Mays,

Please use the code 914882 to verify your email address for Self Password Reset Configuration. This code will be valid for next 5 minutes.

© 2023 Therap Services LLC.

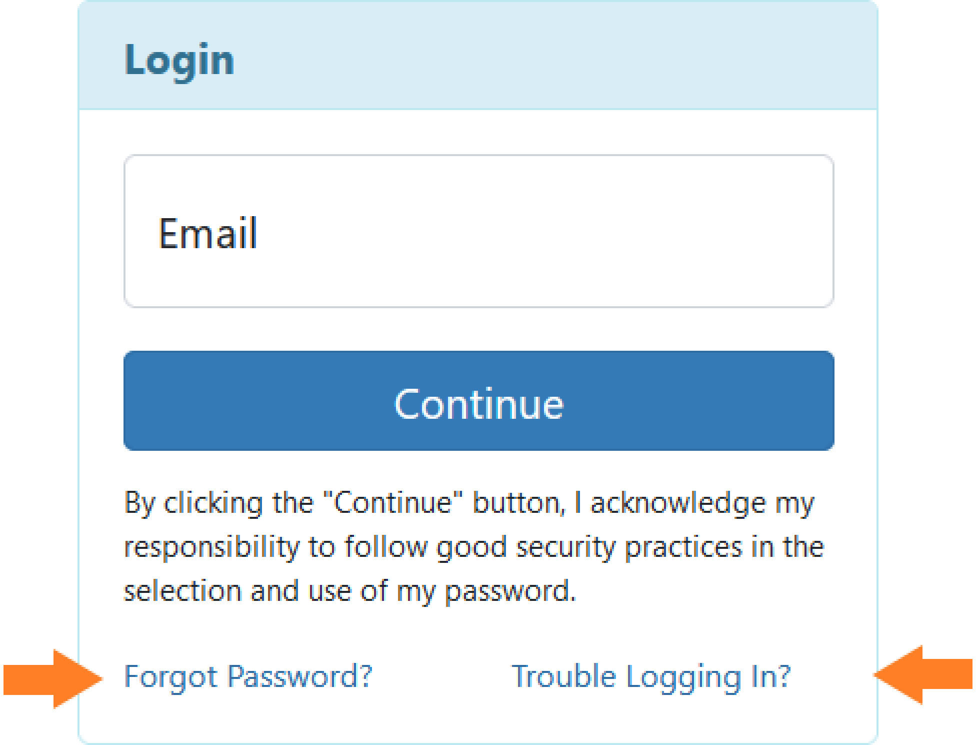
Providing the correct verification code will successfully verify the Email address and users will see this confirmation as a green check mark. Users should click “Update,” and this setup is complete.



Self Password Reset Configuration

Email	ada@domain.com	
Phone/Text Message Email	ada@domain.com	✓ Verified

Users can reset their password by themselves should they forget their current password. For that, Users need to Go to Forgot Password? Link or Trouble Logging In? from the Login page.

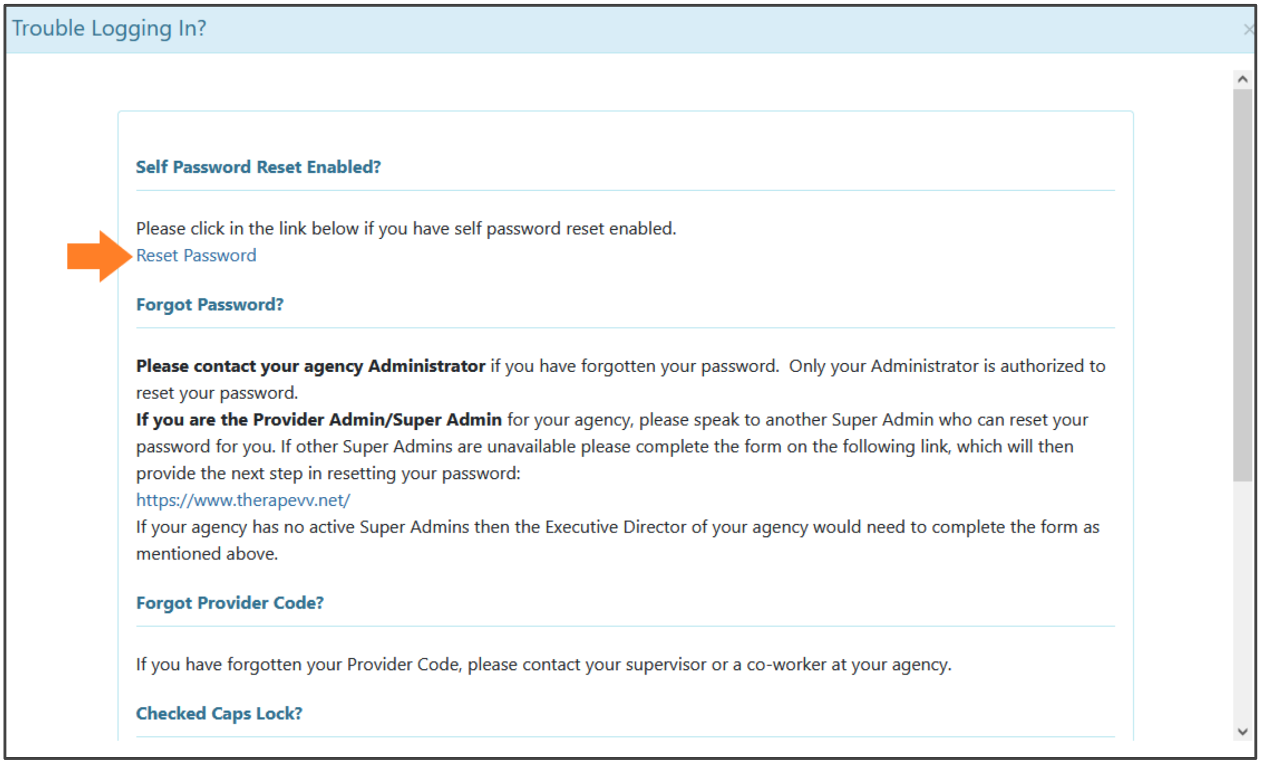


Login

Email

By clicking the "Continue" button, I acknowledge my responsibility to follow good security practices in the selection and use of my password.

Clicking the Trouble Logging In? link will take Users to the screen below.



Trouble Logging In?

Self Password Reset Enabled?

Please click in the link below if you have self password reset enabled.
Reset Password

Forgot Password?

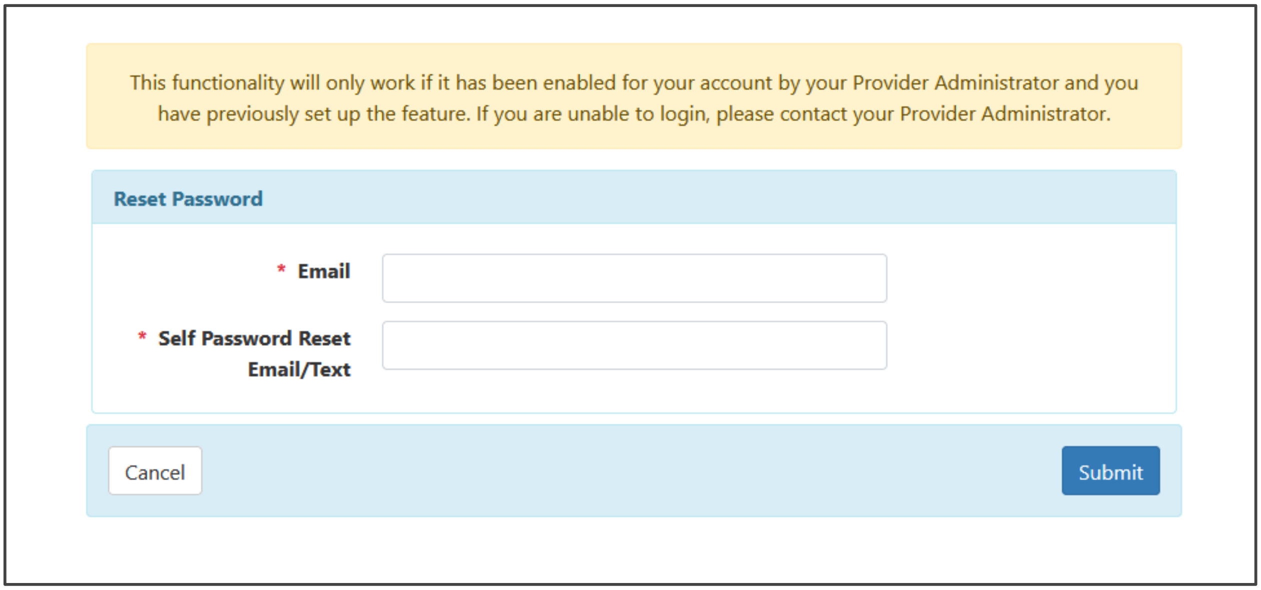
Please contact your agency Administrator if you have forgotten your password. Only your Administrator is authorized to reset your password.
If you are the Provider Admin/Super Admin for your agency, please speak to another Super Admin who can reset your password for you. If other Super Admins are unavailable please complete the form on the following link, which will then provide the next step in resetting your password:
https://www.therapevv.net/
If your agency has no active Super Admins then the Executive Director of your agency would need to complete the form as mentioned above.

Forgot Provider Code?

If you have forgotten your Provider Code, please contact your supervisor or a co-worker at your agency.

Checked Caps Lock?

Users can go to the Reset Password page by clicking on either Forgot Password? directly from the Login Page or the Reset Password link from Trouble Logging In? link. Users will have to submit their login Email and Self Password Reset Email/Text to obtain a Password Token.

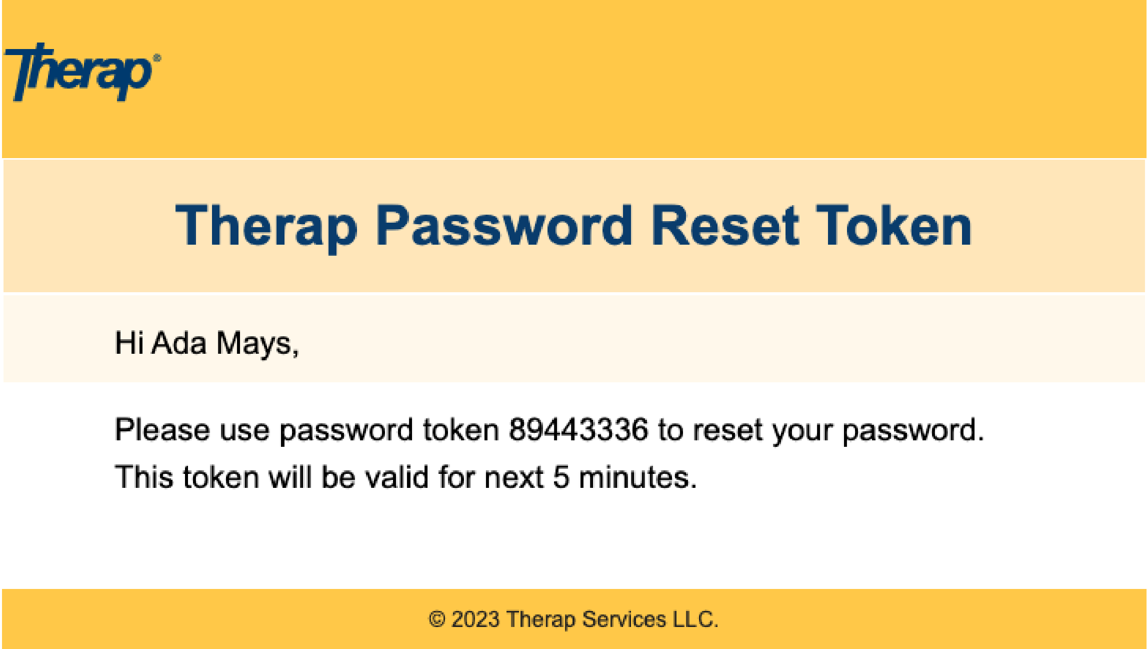


This functionality will only work if it has been enabled for your account by your Provider Administrator and you have previously set up the feature. If you are unable to login, please contact your Provider Administrator.

Reset Password

* **Email**	
* **Self Password Reset Email/Text**	

This token will be sent to their configured Email address.



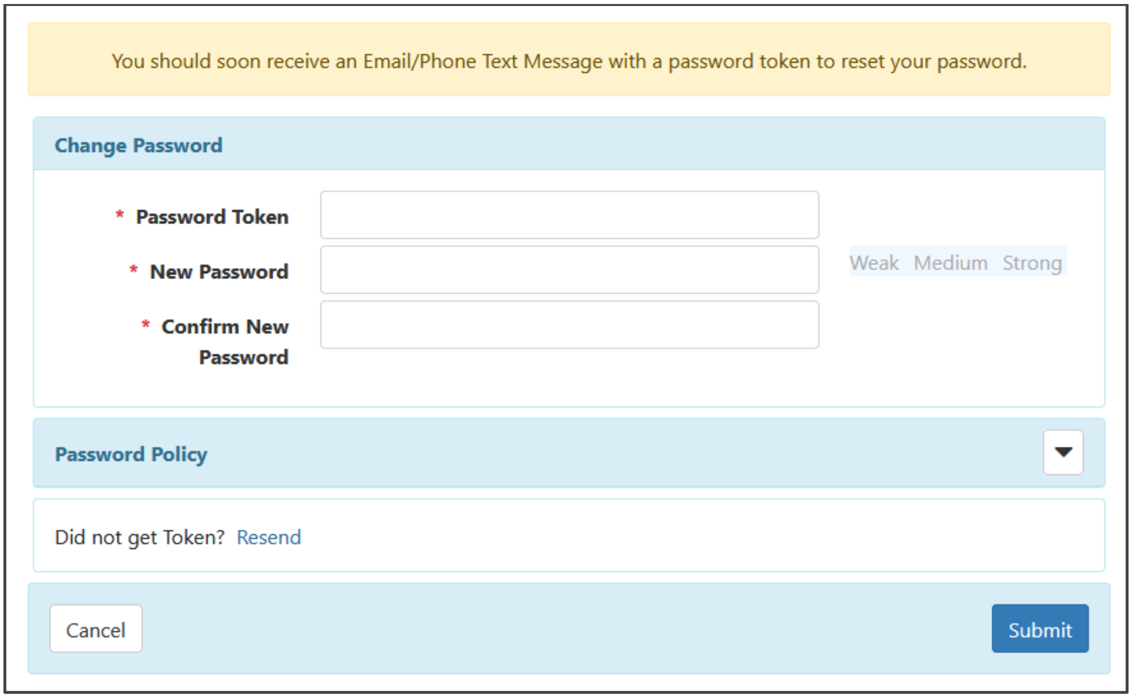
Therap Password Reset Token

Hi Ada Mays,

Please use password token 89443336 to reset your password.
This token will be valid for next 5 minutes.

© 2023 Therap Services LLC.

This Token will be valid for 5 minutes and will enable the verified user to create a new password.



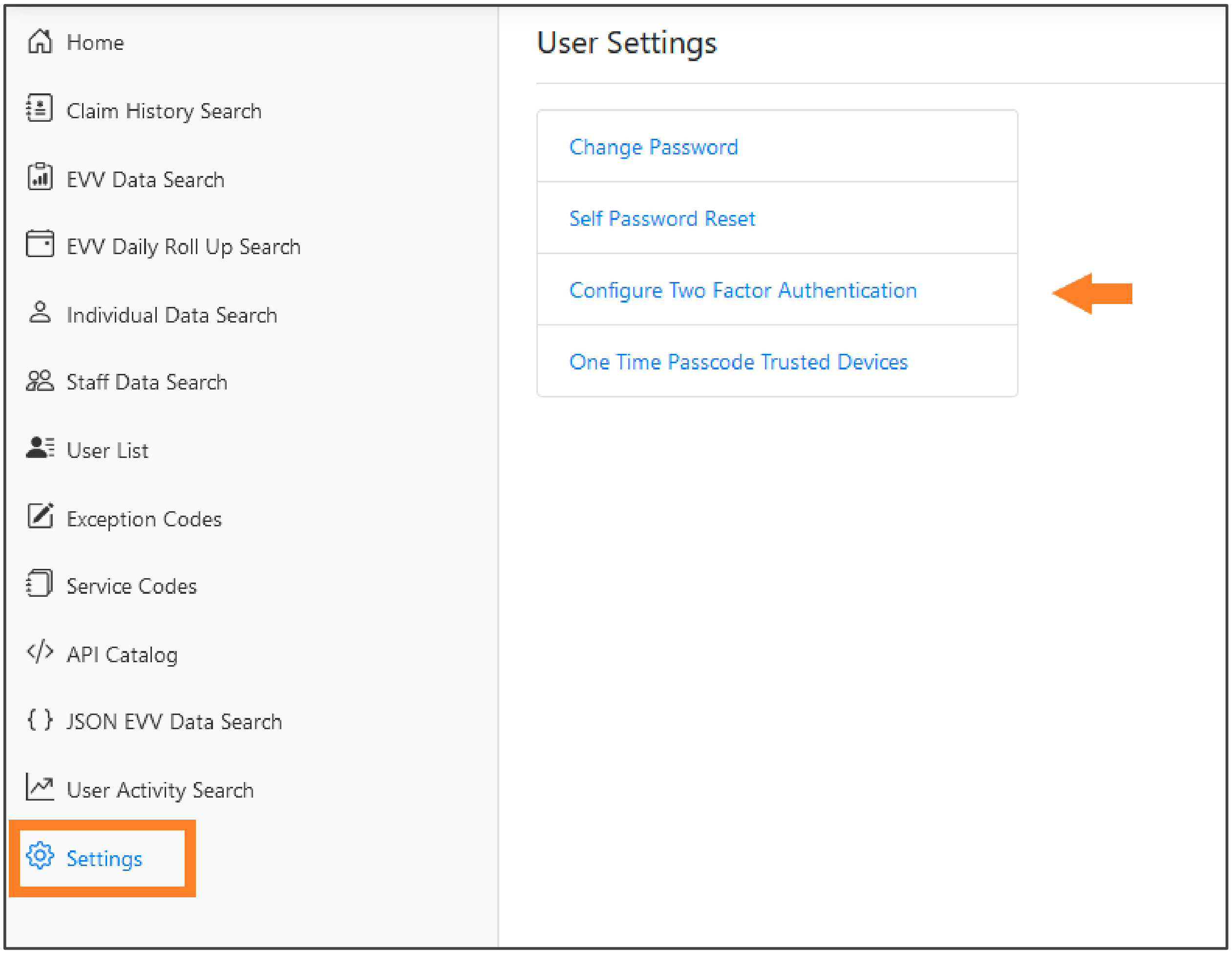
You should soon receive an Email/Phone Text Message with a password token to reset your password.

Change Password

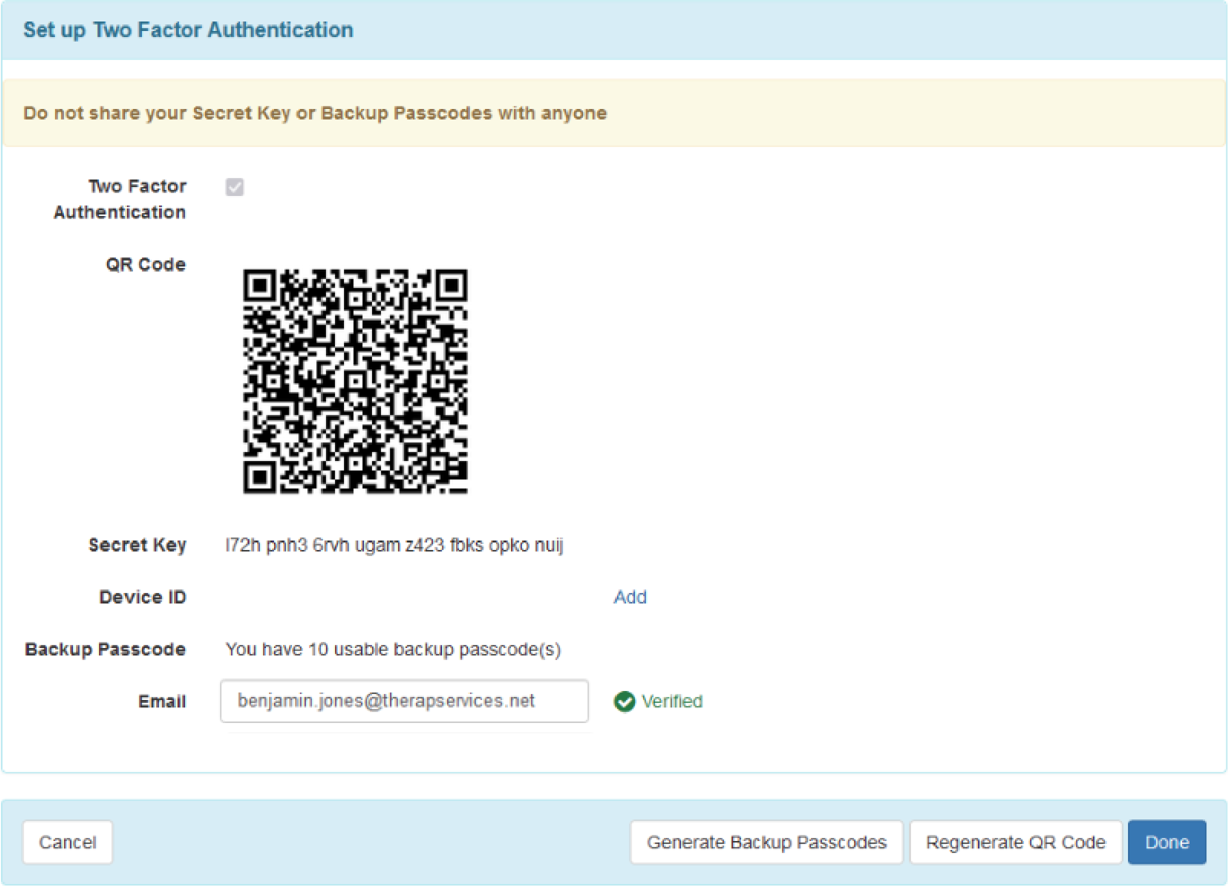
Did not get Token? Resend

Two Factor Authentication

Users will be able to configure their Two Factor Authentication from the following link.



While setting up their Two Factor Authentication, they will have the option to Regenerate QR Code, Generate Backup Passcodes, Add Hardware Token Device, and Setup Passcode Email.



Set up Two Factor Authentication

Do not share your Secret Key or Backup Passcodes with anyone

Two Factor Authentication ☑

QR Code

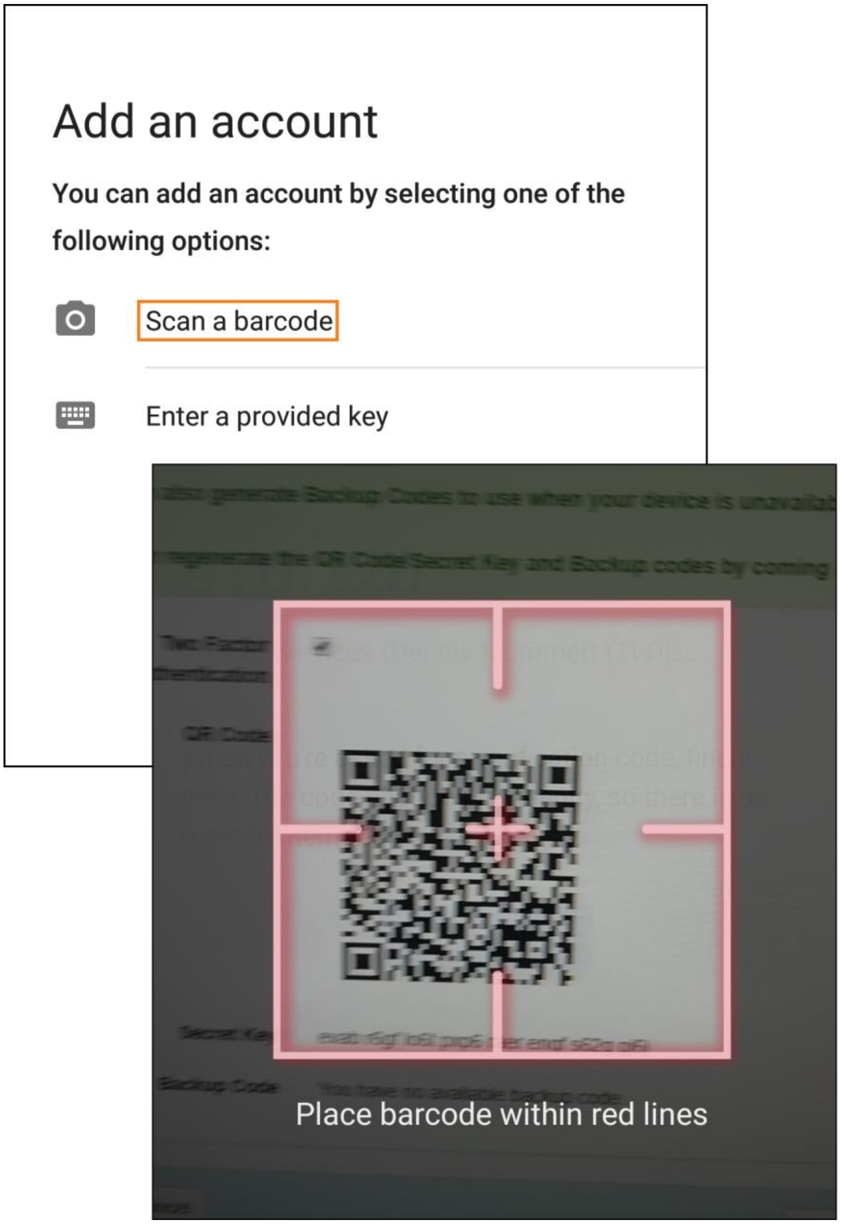
Secret Key l72h pnh3 6rvh ugam z423 fbks opko nuij

Device ID Add

Backup Passcode You have 10 usable backup passcode(s)

Email benjamin.jones@therapservices.net ✓ Verified

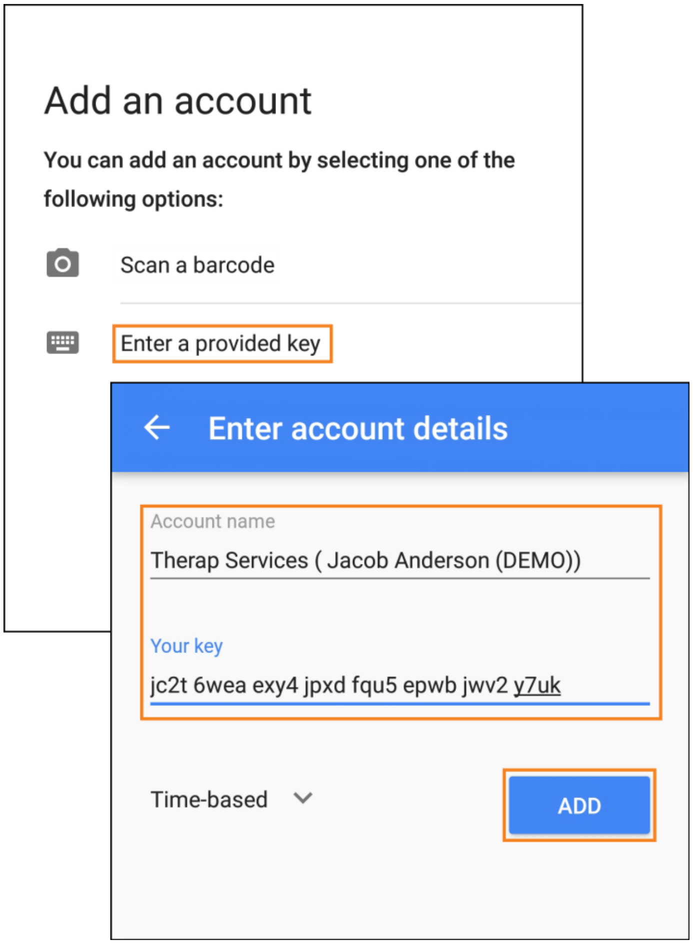
QR Code: This image can be scanned by a 2-step verification software that uses a time-based One Time Password algorithm to gain a one-time password every 30 seconds. The One Time Password can then be entered into the Authenticator App when logging into Therap.



Add an account

You can add an account by selecting one of the following options:

Secret Key: If you are unable to scan the QR Code, this key can be entered into a 2-step verification software that uses Time-based One-time Password algorithm to receive a one-time password every 30 seconds and enter it into the Authenticator App.



Add an account

You can add an account by selecting one of the following options:

Scan a barcode

Enter a provided key

Enter account details

Account name

Therap Services (Jacob Anderson (DEMO))

Your key

jc2t 6wea exy4 jpxd fqu5 epwb jwv2 y7uk

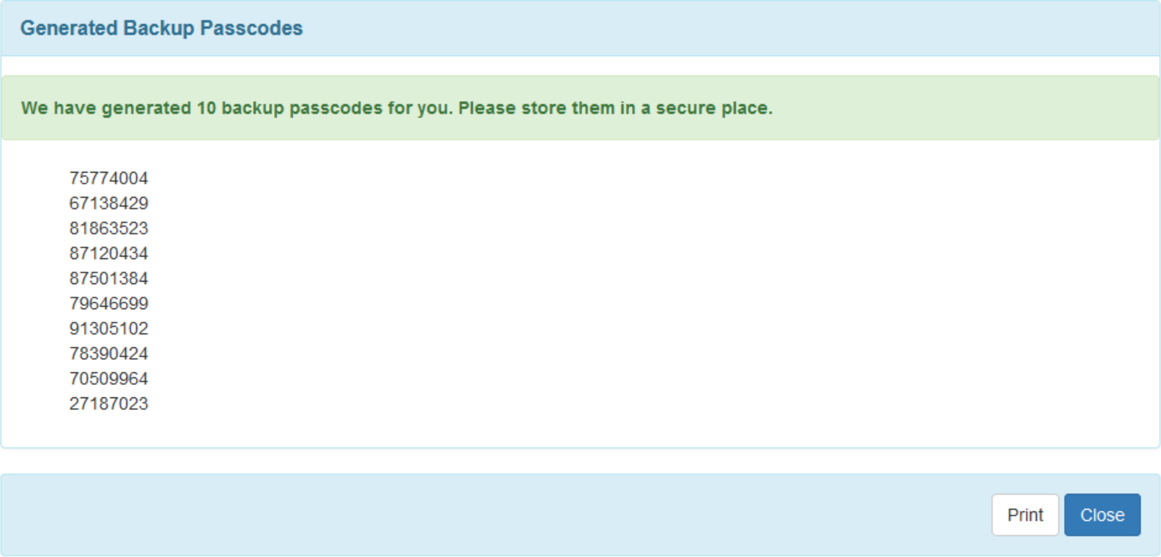
Time-based

ADD

To generate passwords from the QR Code or Secret Key, several two-step verification software that uses Time-based One-time Passcode algorithm can be used on mobile devices. Some Software that can be used are:

- Google Authenticator
- Authy
- Microsoft Authenticator

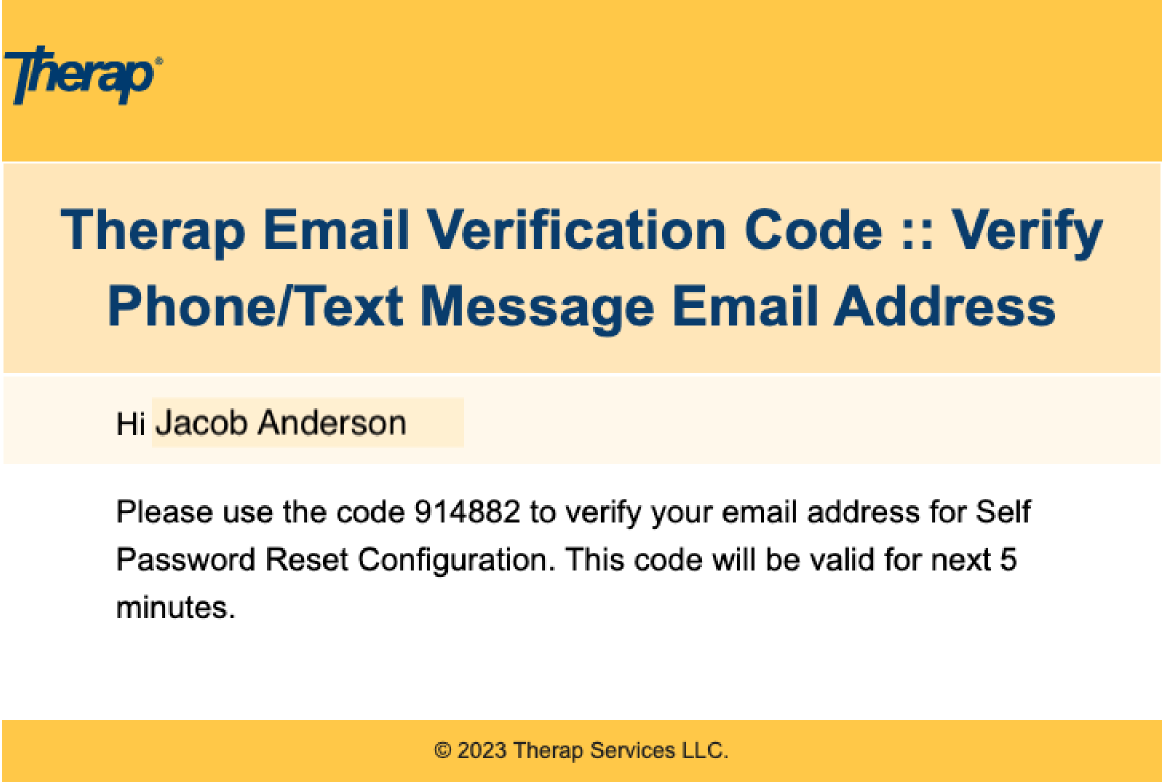
While generating Backup Passcodes, 10 usable Backup Passcodes will be generated. Generated Backup code can be stored or printed in a secure place for future one-time uses.



Generated Backup Passcodes

We have generated 10 backup passcodes for you. Please store them in a secure place.

75774004
67138429
81863523
87120434
87501384
79646699
91305102
78390424
70509964
27187023



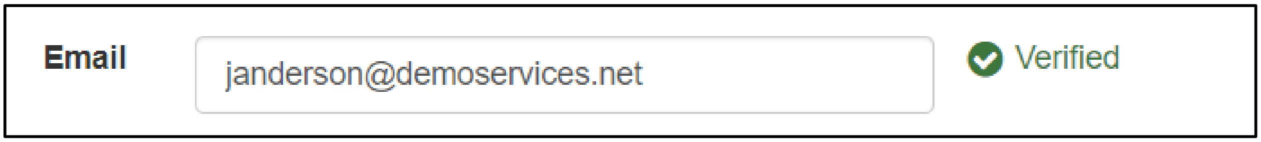
Therap Email Verification Code :: Verify Phone/Text Message Email Address

Hi Jacob Anderson

Please use the code 914882 to verify your email address for Self Password Reset Configuration. This code will be valid for next 5 minutes.

© 2023 Therap Services LLC.

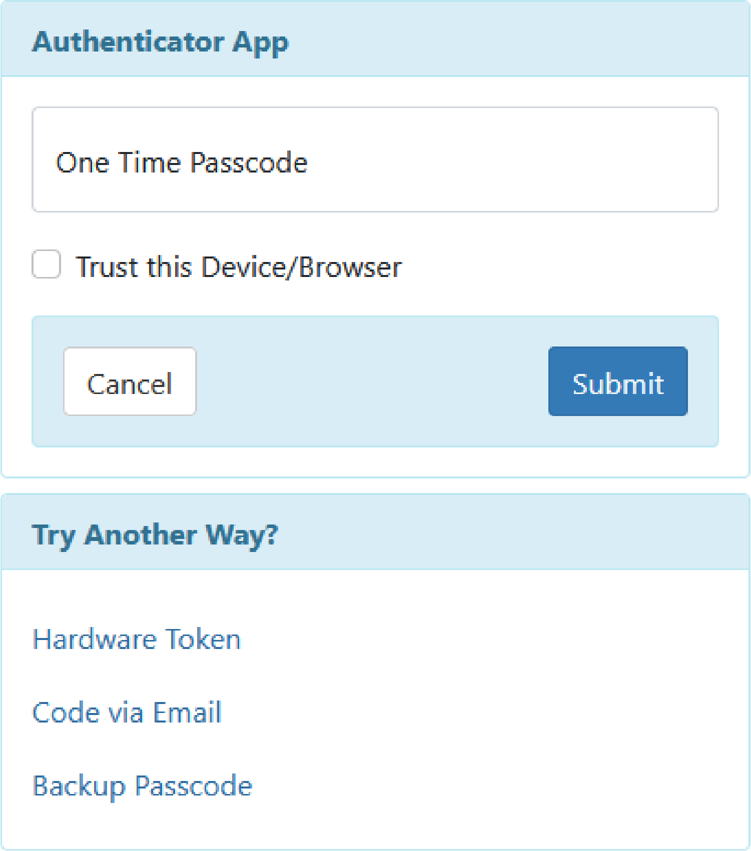
Providing the correct verification code will successfully verify the Email address, and users will see this confirmation as a green check mark.



Email janderson@demoservices.net ✓ Verified

After successfully configuring the Two-factor authentication, users can log in using two-factor authentication. A list of options in Try Another Way? will be available by the two-factor authentication configuration done by the users. If the user wants to use another method than the current method they simply need to choose from the list mentioned in Try Another Way? Only a valid submission of OTP will result in a successful Login.

Authenticator App: This interface is for entering the one-time passcode provided by a 2-step verification software.

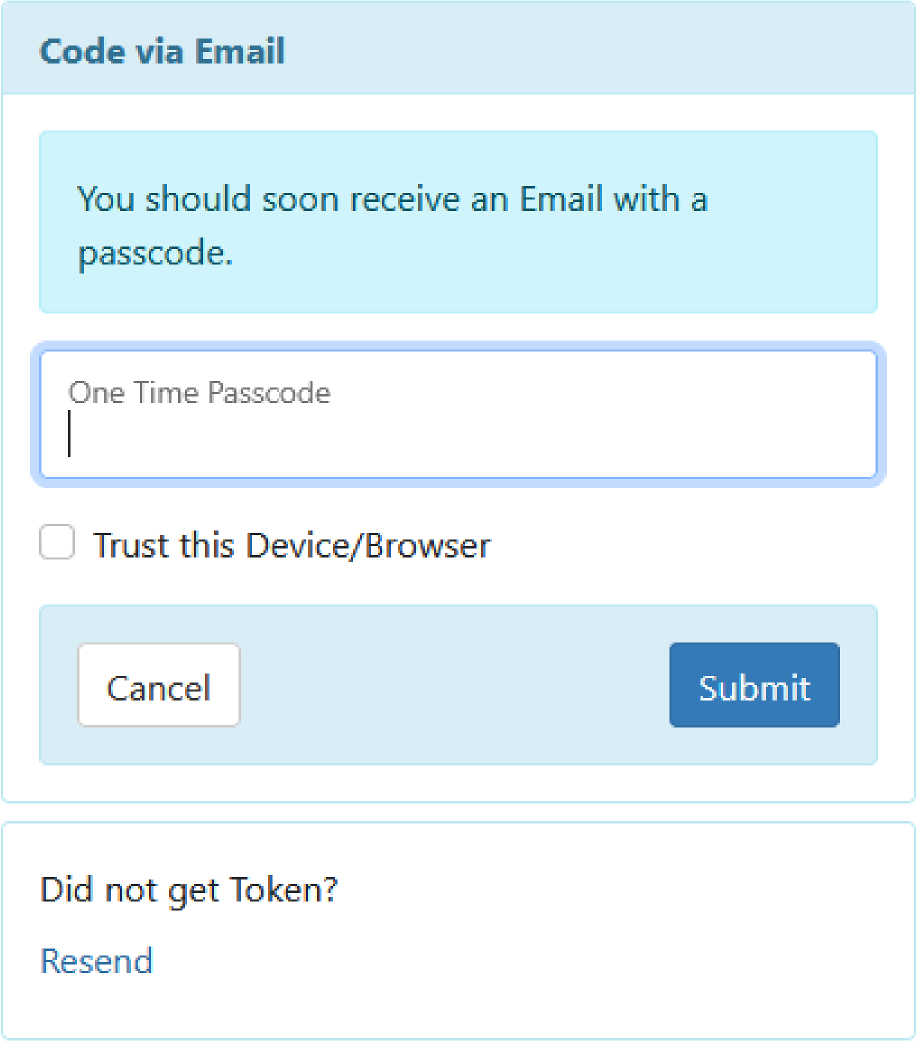


Authenticator App

One Time Passcode

□ Trust this Device/Browser

The one-time passcode must be based on the QR Code or Secret Key generated during 2FA configuration. The passcode is updated every 30 seconds in the 2-step verification software.



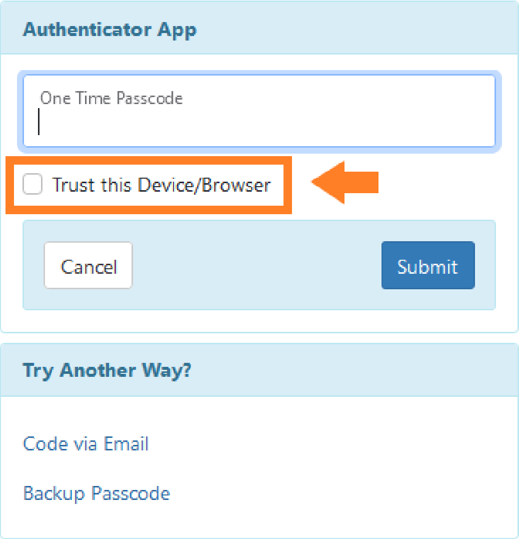
Code via Email

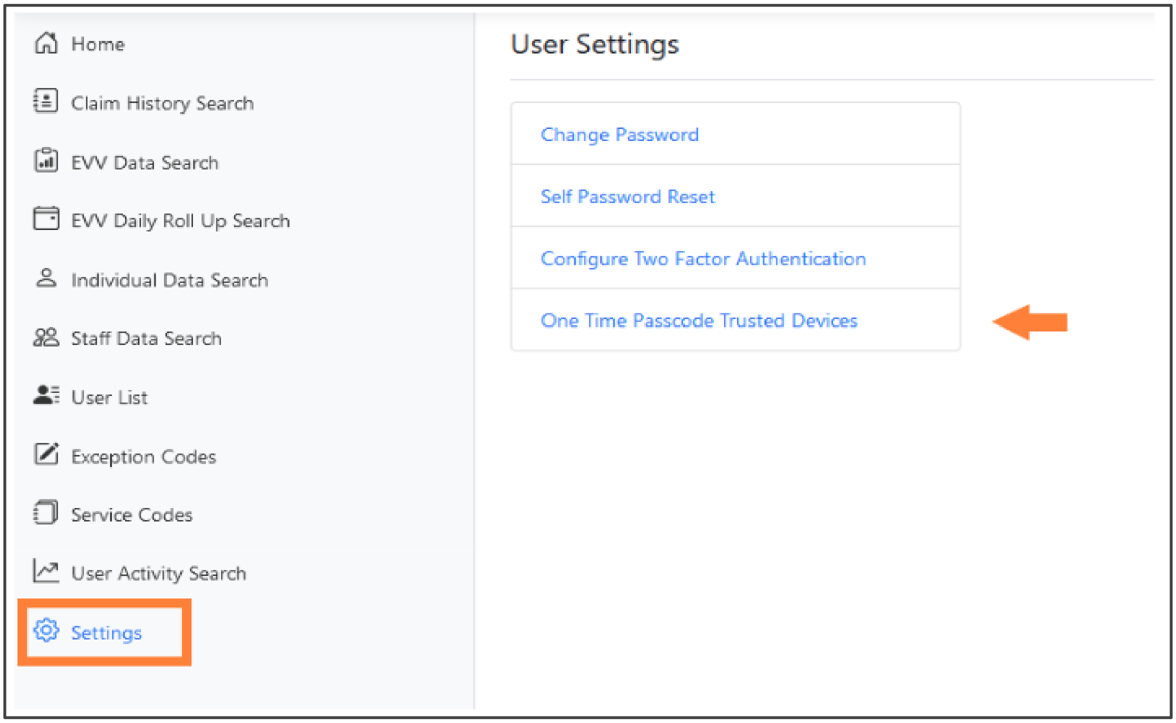
You should soon receive an Email with a passcode.

Did not get Token?

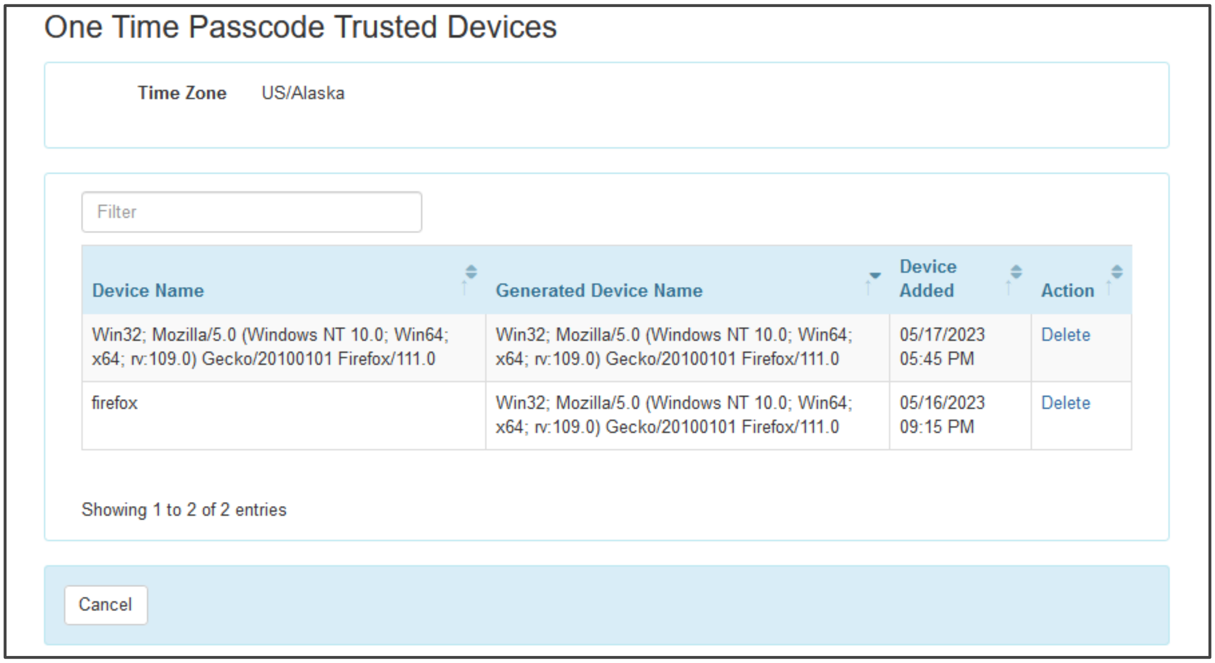
One-Time Passcode Trusted Devices

Users will have the ability to save their Device/Browser when they log in. This will enable the user to log in without any second factor for up to 15 days.





After trusting a device/ Browser users will be able to view the saved device/browser list.



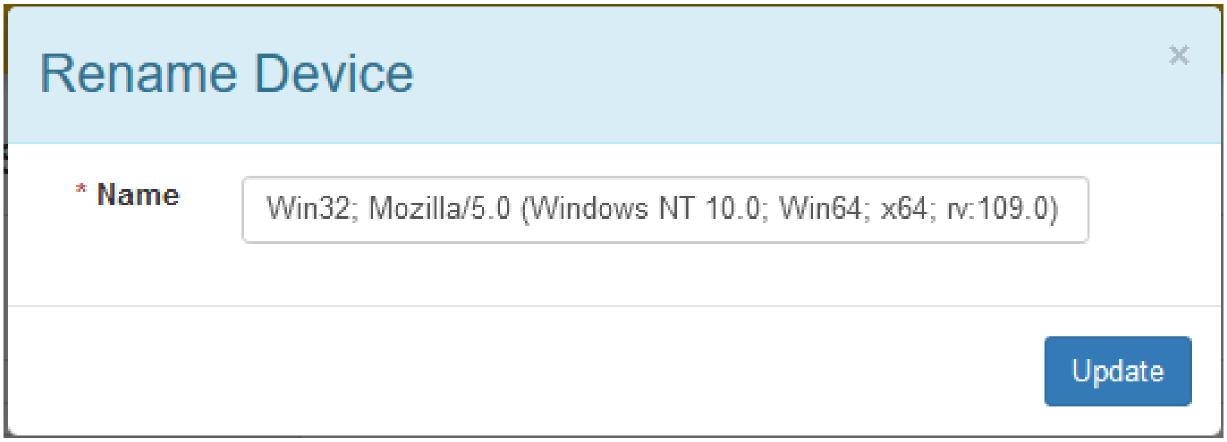
One Time Passcode Trusted Devices

Time Zone US/Alaska

Device Name	Generated Device Name	Device Added	Action
Win32; Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0	Win32; Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0	05/17/2023 05:45 PM	Delete
firefox	Win32; Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0	05/16/2023 09:15 PM	Delete

Showing 1 to 2 of 2 entries

They will also have the ability to remove the device or rename it.

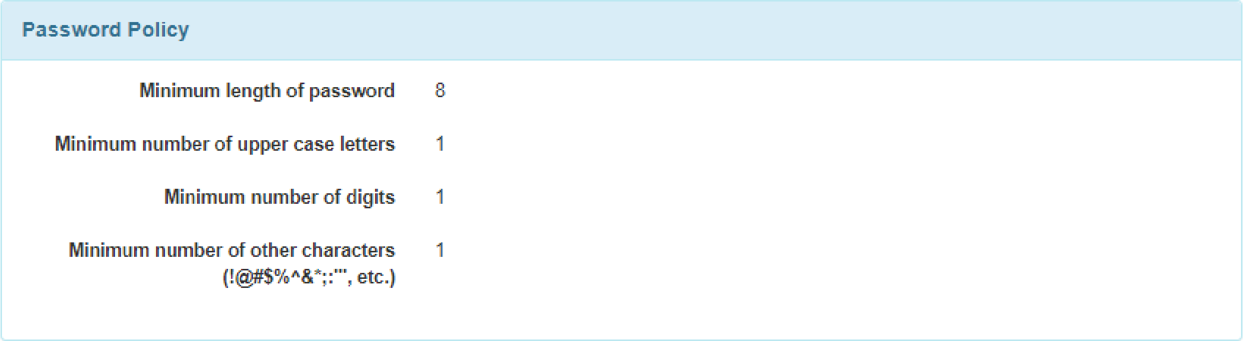


Rename Device

* Name: Win32; Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)

Password Policy

Provider Super Admins MUST follow the minimum password requirements established by the State of Alaska. They can view the Aggregator password requirements here.



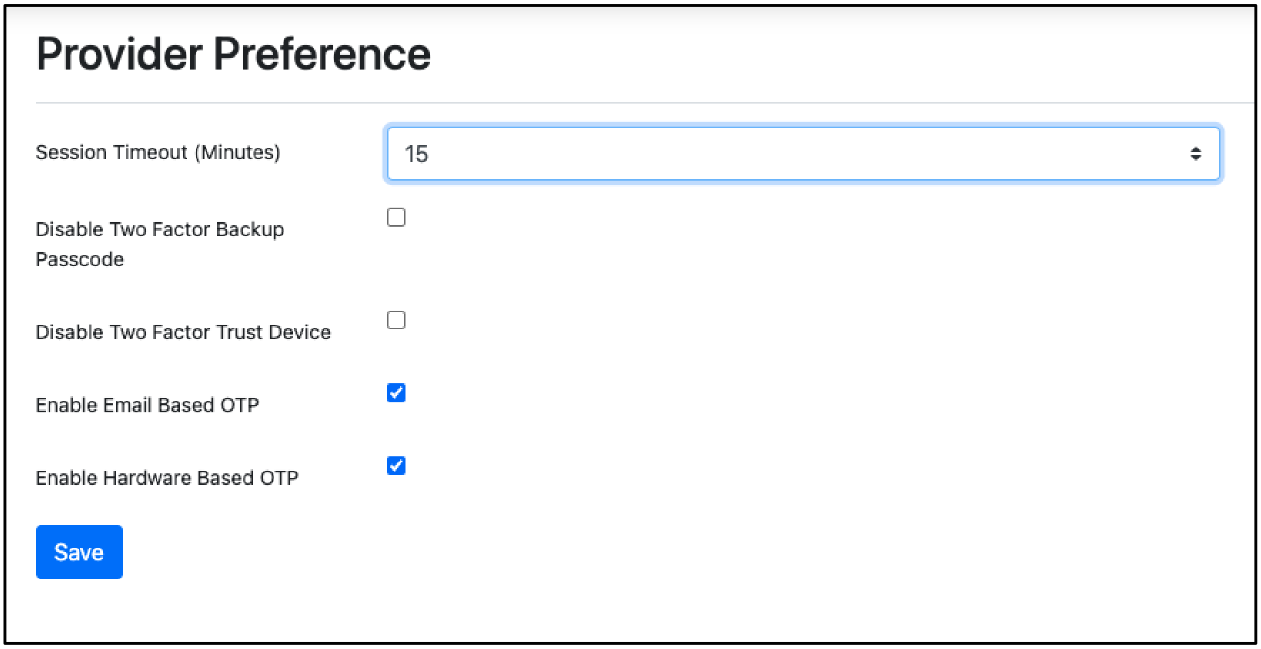
Password Policy

Minimum length of password	8
Minimum number of upper case letters	1
Minimum number of digits	1
Minimum number of other characters (!@#$%^&*;:'", etc.)	1

State of Alaska Password Policy:
Password policies are established by Alaska within the parameters of the Therap system, including multi-factor options. Current password policy requires:
Minimum length of password: 8
Minimum number of uppercase letters: 1
Minimum number of digits: 1
Minimum number of other characters (!@#$%^&;:'", etc.): 1
Maximum number of incorrect passwords tolerated: 5
Number of days before password expires for Admin & Regular users: 90
Number of the most recently used passwords that can not be reused (enter 5 to prevent reuse of last 5 passwords): 5

Provider Preference

Provider Super Admins will have the option to set several parameters for their Provider. For example, Session Timeout, Disable Two Factor Backup Passcode, Disable Two Factor Trust Device, Enable Email Based OTP.



Provider Preference

Session Timeout (Minutes)	15
Disable Two Factor Backup Passcode	☐
Disable Two Factor Trust Device	☐
Enable Email Based OTP	☑
Enable Hardware Based OTP	☑

Session Timeout (Minutes): Provider Super Admins will be able to select the minutes from the Session Timeout (Minutes) drop-down field under the 'Session Timeout (Minutes)' section. This session timeout value can be as low as 15 minutes to as high as 60 minutes and will be applied to users across the agency.

Disable Two Factor Backup Passcode: When the Disable Two Factor Backup Passcode option is enabled on the Provider Preference page, users will no longer find the Generated Backup code option when configuring their 2FA Setup. This will ensure that users who have Two Factor Backup Passcode disabled will not be able to generate and use their Backup Passcode.

Disable Two Factor Trust Device: When the Disable Two Factor Trust Device option is enabled on the Provider Preference page, users will no longer find the Remember this Device/Browser checkbox when entering their 2FA One Time Passcode (OTP) during login. This will ensure that users who have 2FA enabled will always have to enter their 2FA OTP during login and will not be able to save new devices to their 'One Time Passcode Trusted Devices' list.

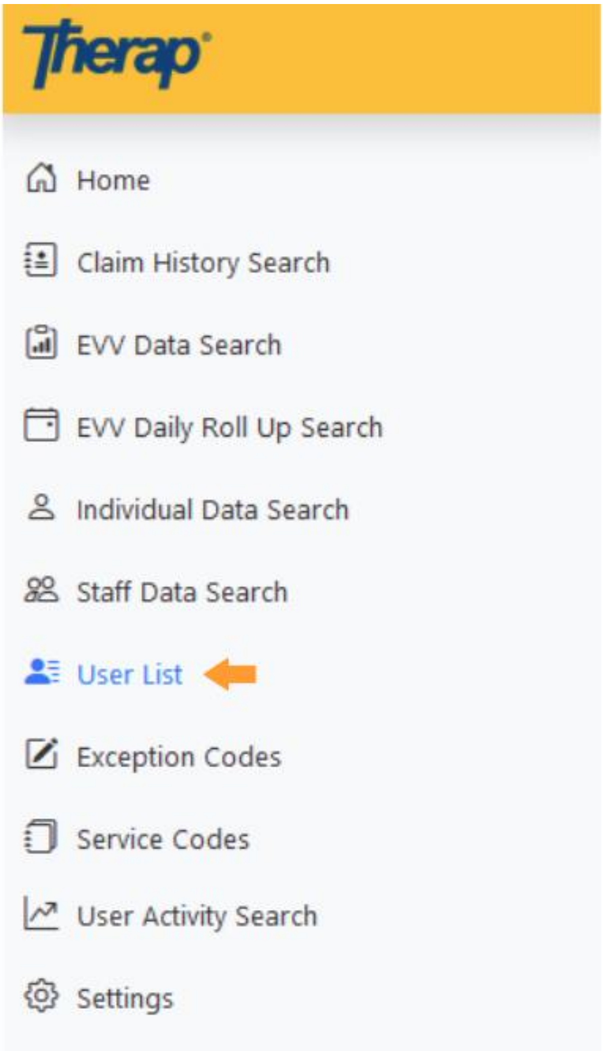
Enable Email Based OTP: Enabling the Email Based OTP option on the Provider Preference page will make a new Email field be available to users who are configuring their 2FA on the 'Set up Two Factor Authentication' page.
Entering an email address in the 'Set up Two Factor Authentication' page will allow users to receive a code via email when performing a 2FA login.

Enable Hardware Based OTP: Enabling the Hardware Based OTP option on the Provider Preference page will make a new Device ID field be available to users who are configuring their 2FA on the 'Set up Two Factor Authentication' page.

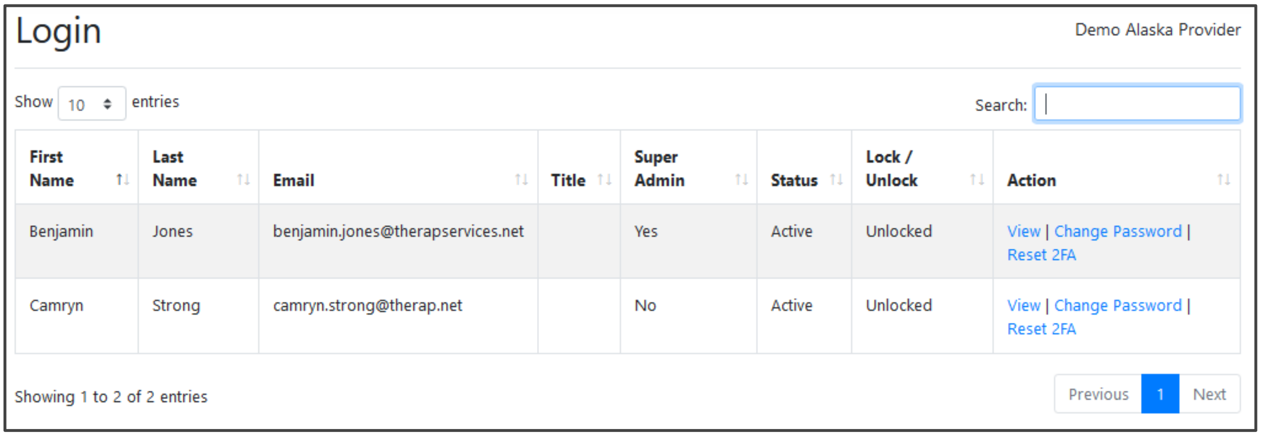
Entering an Device ID in the 'Set up Two Factor Authentication' page will allow users to receive a Passcode via hardware device when performing a 2FA login.

NOTE: This is not available in the current release.

User List (Admin User Control Features)



Clicking on the User List will allow Users to see other users in their account, their titles, whether they are Super Admins or not, their current Status, and whether or not their Account is Locked or Unlocked.



Login

Demo Alaska Provider

Show 10 entries

Search:

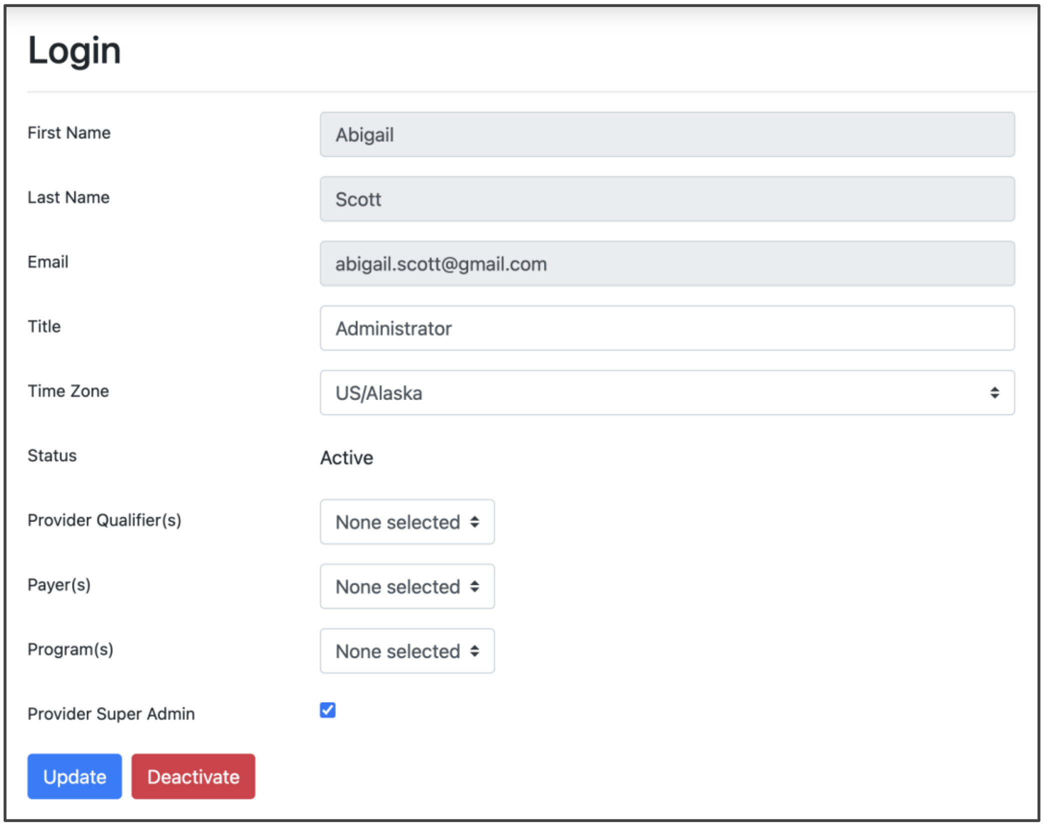
First Name	Last Name	Email	Title	Super Admin	Status	Lock / Unlock	Action
Benjamin	Jones	benjamin.jones@therapservices.net		Yes	Active	Unlocked	View | Change Password | Reset 2FA
Camryn	Strong	camryn.strong@therap.net		No	Active	Unlocked	View | Change Password | Reset 2FA

Showing 1 to 2 of 2 entries

Admin Users will see options to View and Update User Privileges, Reset or Change User Passwords when they are locked out, or reset a User's 2FA when they need to start over and re-configure this by clicking on the Action links on the User directly.

User View

Clicking on View will open up the User Screen. Administrative Users will be able to update users' access. If None Selected is set for Provider Qualifier(s), Payer(s), or Program(s) it will default to having access to all the information in that section.

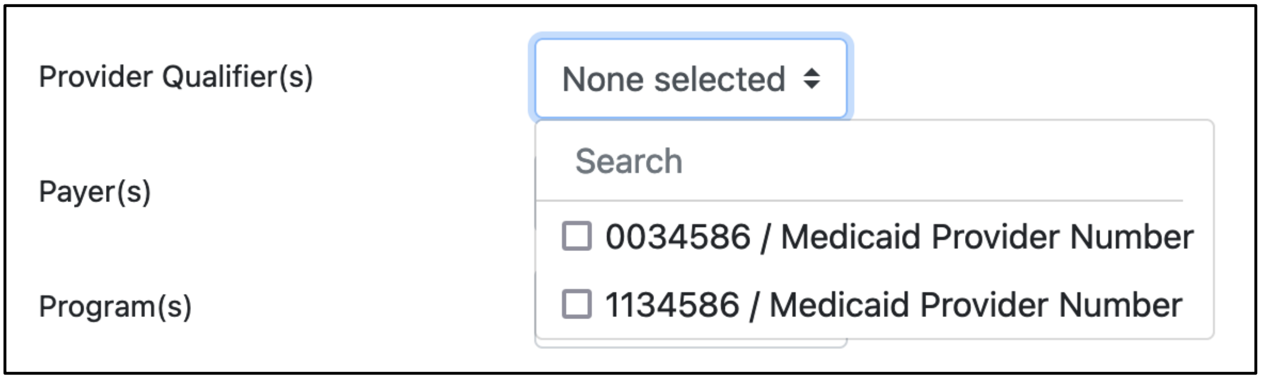


Login

First Name	Abigail
Last Name	Scott
Email	abigail.scott@gmail.com
Title	Administrator
Time Zone	US/Alaska
Status	Active
Provider Qualifier(s)	None selected
Payer(s)	None selected
Program(s)	None selected
Provider Super Admin	☑

Provider Qualifier(s)

Agencies with multiple Medicaid Provider IDs will have a list of options here and will be able to allow Users to see all data related to a single Medicaid Provider ID or multiple Medicaid Provider IDs based on the User's specific agency requirements.

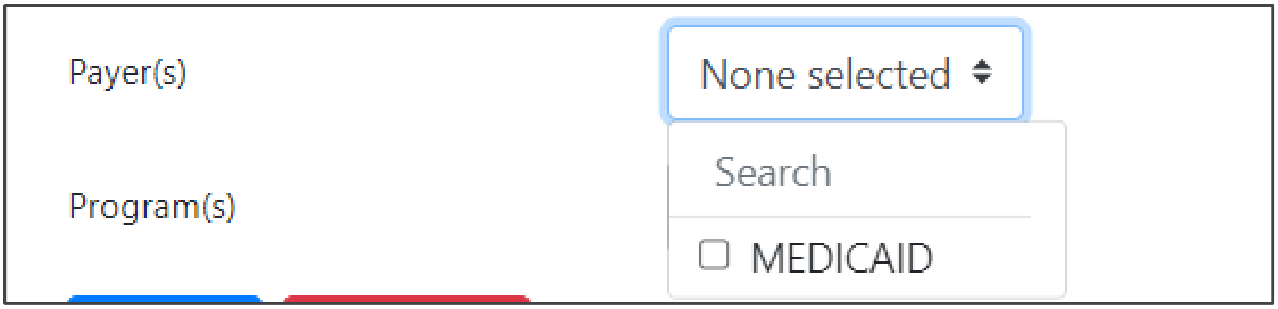


□ 0034586 / Medicaid Provider Number

□ 1134586 / Medicaid Provider Number

Payer(s)

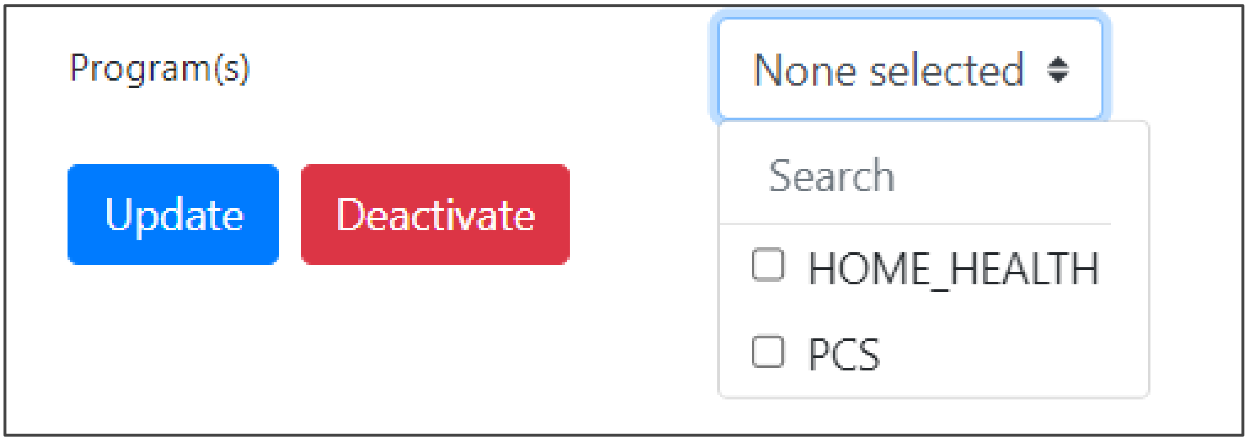
Agencies with multiple Payers will see choices here and will be able to allow Users to see all data related to a single Payer or multiple Payers based on the User’s specific agency requirements.



□ MEDICAID

Program(s)

Agencies with multiple Programs will see a list of options here and will be able to allow Users to see all data related to a single Program or multiple Programs based on the Users specific agency requirements.



Update/ Deactivate

In order to save changes made on this screen Admin Users must click Update.

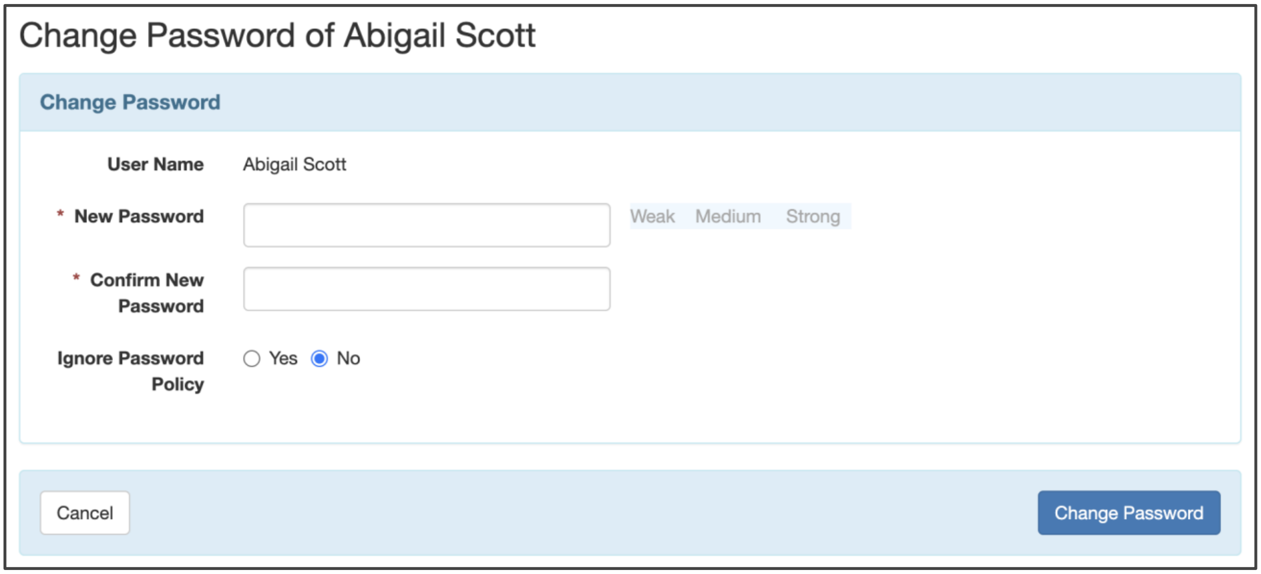
To Deactivate a User that is permanently or temporary not logging into the Aggregator click Deactivate.

Activate

Users that have been Deactivated can be re- Activated by clicking Activate.

Change Password

Users that are locked or have forgotten their password and can not log in using one of the other methods can have their password reset by an Admin user. Once the password is reset, the Admin User should share this securely with the User, and this User will be able to log in and be forced to change their password immediately to complete login.



Change Password of Abigail Scott

Change Password

User Name: Abigail Scott

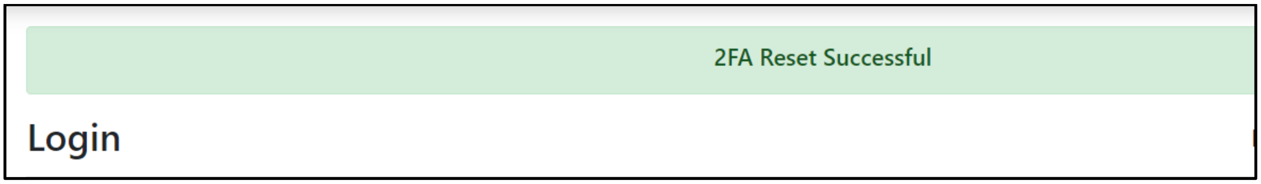
* New Password:

* Confirm New Password:

Ignore Password Policy: ○ Yes ● No

Reset 2FA

Admin Users can click Reset 2FA to enable/ force the User to reconfigure their 2FA method(s).

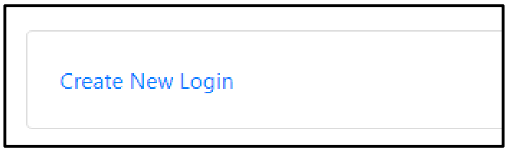


2FA Reset Successful

Login

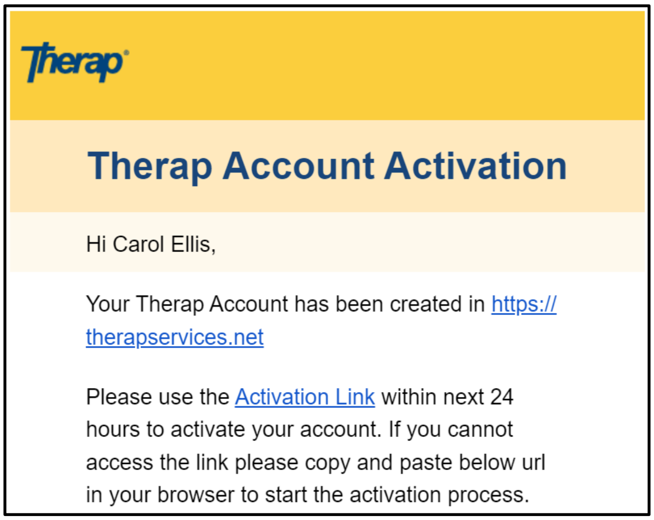
Create New Login

Admin Users can now add Users to their organization and control their access to their agency's data in the Aggregator.



Create New Login

Newly created Users Logins will have to activate their account at the initial login. To do this, an activation email will be sent to their provided corresponding Email address with an activation link. After clicking on the activation link they received, users will need to complete their account setup by creating their password. This activation link will be valid for 24 hours.



Therap Account Activation

Hi Carol Ellis,

Your Therap Account has been created in https://therapservices.net

Please use the Activation Link within next 24 hours to activate your account. If you cannot access the link please copy and paste below url in your browser to start the activation process.

New Users will be prompted to create their password and will also be required to set up their Two Factor Authentication as described above. Only after this setup users will be able to successfully log in.

Please contact AKsupport@therapservices.net if there are any problems with your first-time login.

Reference Materials

File Source	File Type	File Name