

## Account Authentication is mandatory for staff for all databases.

You have the option to use our already available (default), standard 2-factor authentication. You will either be emailed or receive a text with your authentication code. Or you can use a widely available Authentication App.

- We have tested , Google Authenticator, Microsoft Authenticator and Duo Mobile.

To continue using our default, standard 2-factor authentication you will only need to verify that email addresses are valid/correct for your user list. Alternatively, your users have the option to utilize a text message to receive their code. If users would like to receive their code vis SMS, they will need to complete the full text message address in their user profiles.

To ensure accounts are set up for authentication jump to [ATS 2-Factor](#).

Please also speak with your IT Staff to ensure the address, noreply@athletictrainersystem.com is on their allowed list.

If you would like to switch to Authentication Apps this will affect all of your users. Make sure to have them install and set up a Authentication of their choosing.

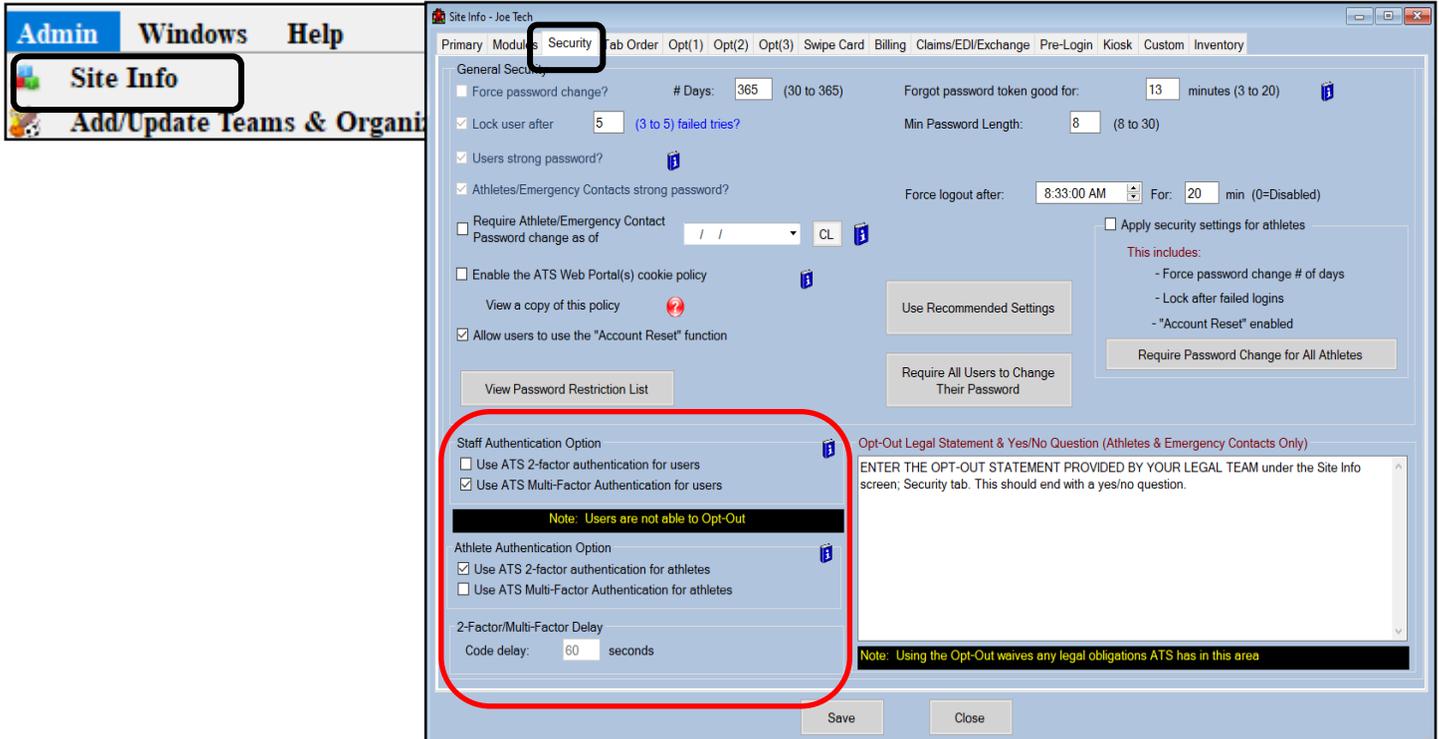
To set up your ATS database to use the authentication app, jump to [ATS and Authentication Apps](#).

Task:	Page:
Site Info Options	<a href="#">2</a>
Account set up for 2-factor	<a href="#">3</a>
Desktop 2-factor use	<a href="#">4</a>
Staff Portal/Phone 2-factor use	<a href="#">5</a>
Intro to MFA in ATS	<a href="#">6</a>
Desktop- Generating your User Secret code	<a href="#">7</a>
Linking Secret Code to Auth App	<a href="#">8-9</a>
Logging in with the MFA Code	<a href="#">10</a>
Staff Portal– Generating your User Secret Code	<a href="#">11</a>
Logging in on the Staff Portal or Phone with MFA	<a href="#">12</a>

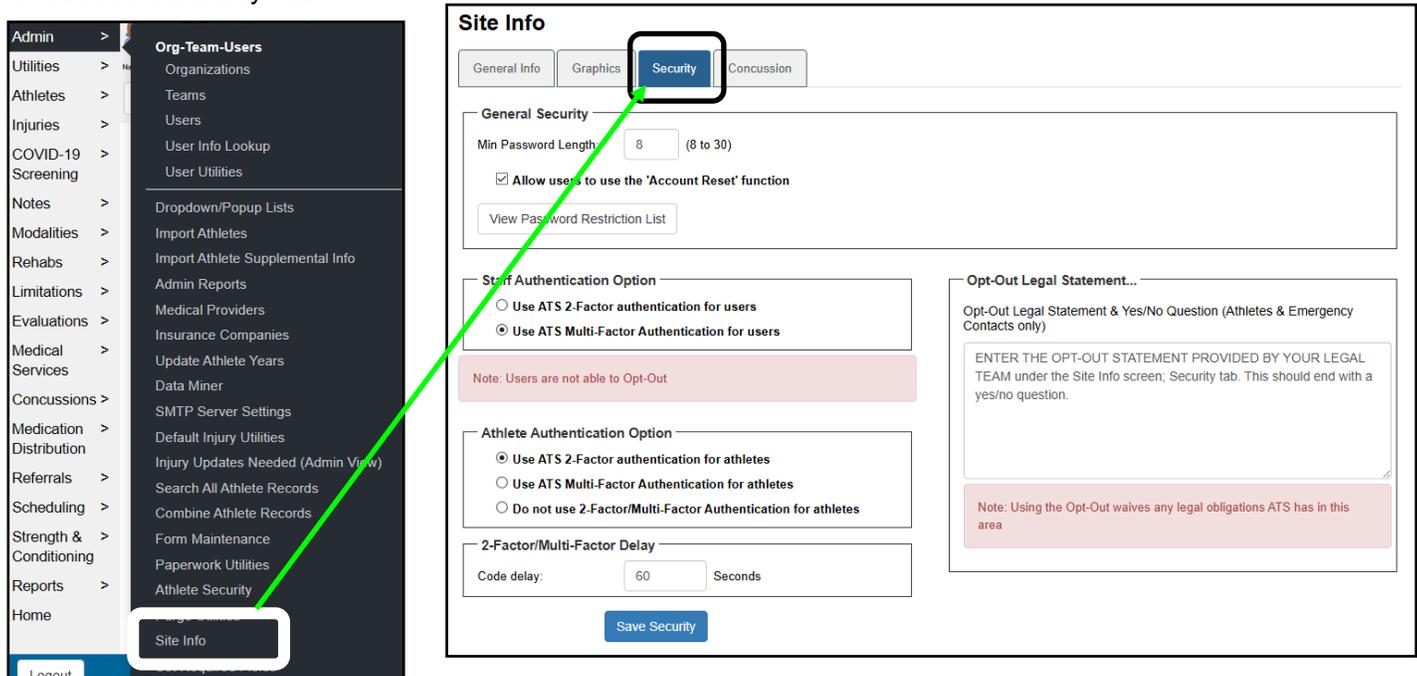
## ATS 2-Factor Authentication:

On Desktop go to Admin—> Site Info—> Security Tab, you will see the Staff Authentication, and Athlete Authentication. These options are an “either” selection, either you will use the 2-factor or you will select the authentication app.

**Delay Settings:** This is the amount of time you will have to enter your code to verify/authenticate your account. The Auth Code Delay is for both receiving an email/text or accessing your auth app. Depending on email servers, it can take 1-3 minutes to obtain your verification code.



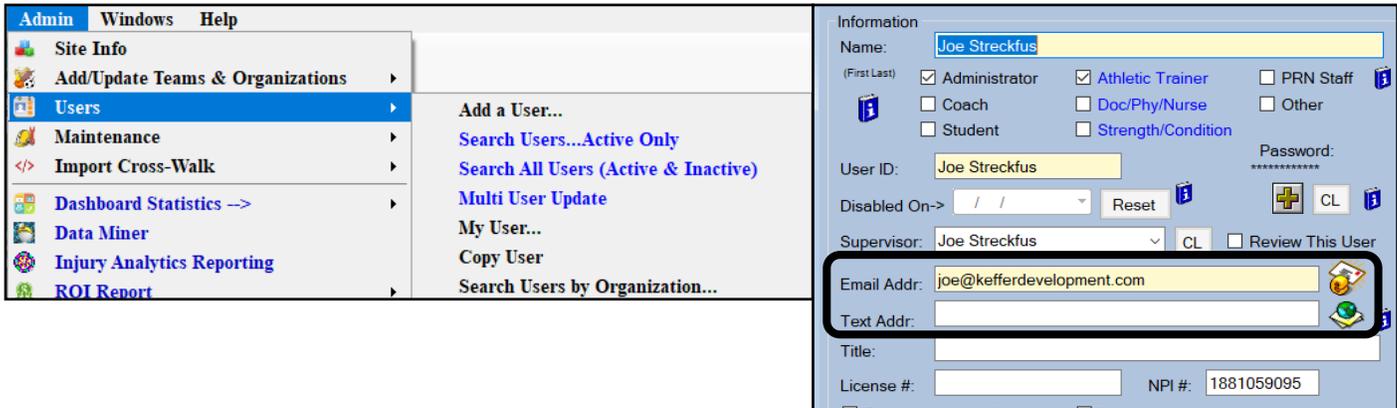
To access Site Info on the portal go to your Admin tab, and Select Site Info. Then select the Security Tab.



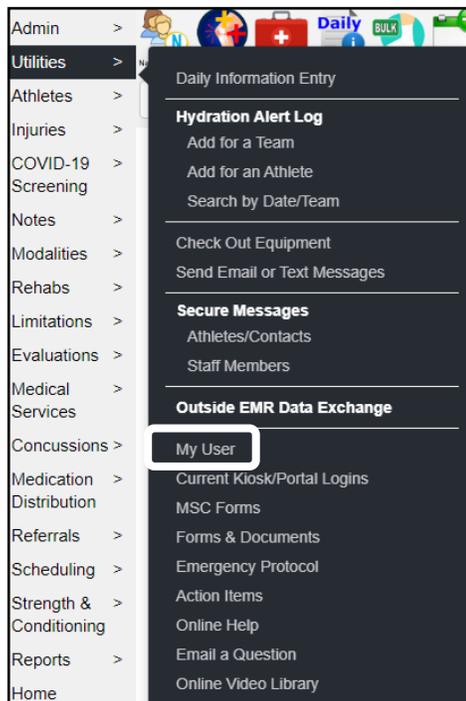
## User Profiles for 2-factor:

Please have your users verify the email address that is in their user account, is valid. This is the address that the 2-factor code will be emailed. Admin—> Users—> MY user, or on the portal Utilities—> My user.

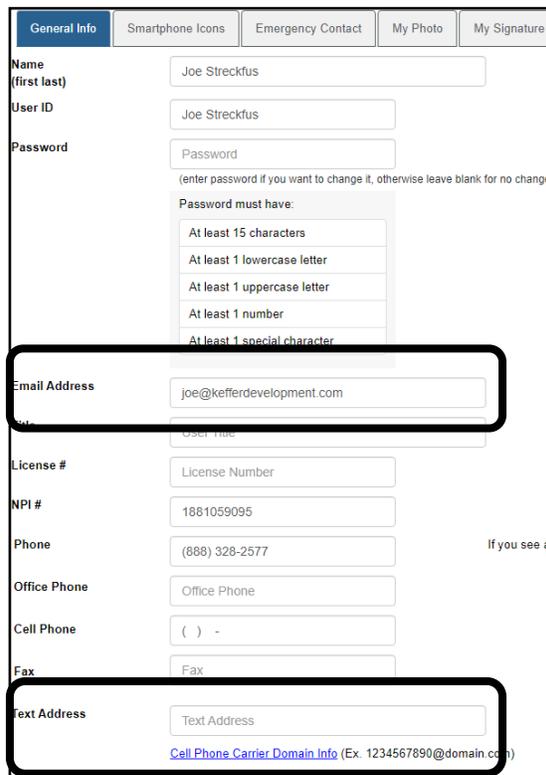
- If they would like to utilize the Text Message option, they will need to complete add their 10 digit cell number in the Text Addr: line complete with the extension that goes with their company.
  - Example:1234567890@vtext.com. Please use the  icon for a common list of carriers



The screenshot shows the 'Admin' menu with 'Users' selected, displaying options like 'Add a User...', 'Search All Users (Active & Inactive)', and 'Multi User Update'. To the right is the 'Information' form for user 'Joe Streckfus'. The 'Email Addr:' field is highlighted with a red box and contains 'joe@kefferdevelopment.com'. The 'Text Addr:' field is also highlighted with a red box and is empty. Other fields include Name, User ID, Password, Supervisor, License #, and NPI #.



The screenshot shows the 'Utilities' menu with 'My User' highlighted. Other options include 'Daily Information Entry', 'Hydration Alert Log', 'Secure Messages', and 'Outside EMR Data Exchange'.



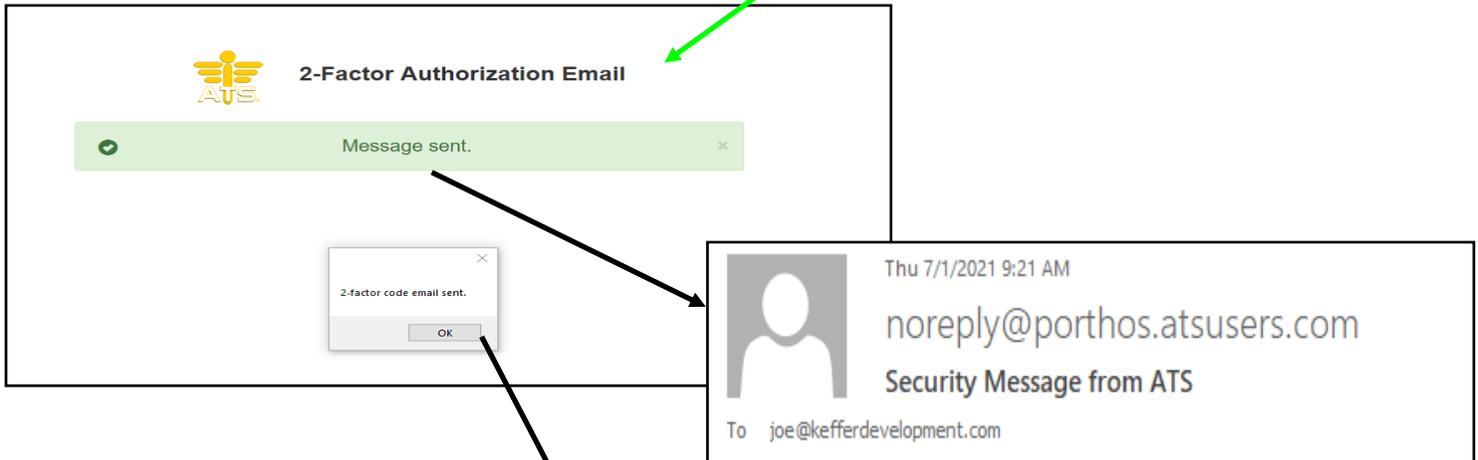
The screenshot shows the 'General Info' tab of the user profile form for 'Joe Streckfus'. The 'Email Address' field is highlighted with a red box and contains 'joe@kefferdevelopment.com'. The 'Text Address' field is also highlighted with a red box and is empty. Other fields include Name, User ID, Password, License #, NPI #, Phone, Office Phone, Cell Phone, and Fax.

## 2-Factor Process ATS Desktop:

After providing their login credentials, users will see this prompt. If they have both email and a text address filled out, they will have both options. Otherwise email will be the only choice. Choose the method of delivery.

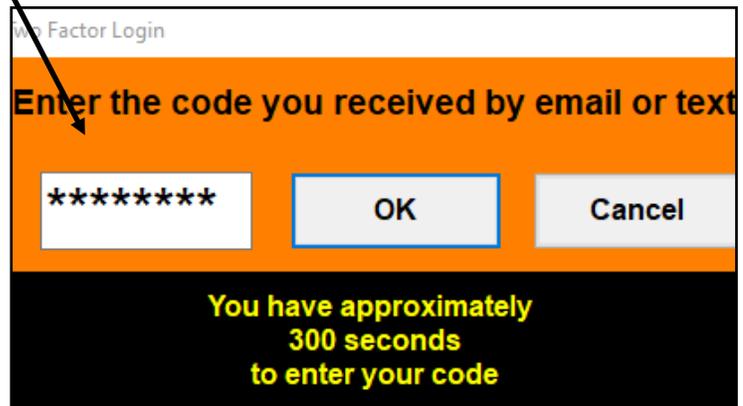


A new window opens notifying you a code was sent.



Clicking OK on the message above will then open the authorization box. Here you will enter the code you were sent into the box.

If you successfully enter the code that was delivered to you, you will continue to ATS.



## 2-Factor Process ATS Staff Portal:

Portal:

### Login



User ID:

Password:

[Forgot your Password?](#)

[Reset your Login](#)

Database:

Number of active users: 2

497 days remaining until your activation expires

Version 1.0.0.0  
Copyright © 2021, Keffer Development Services, LLC

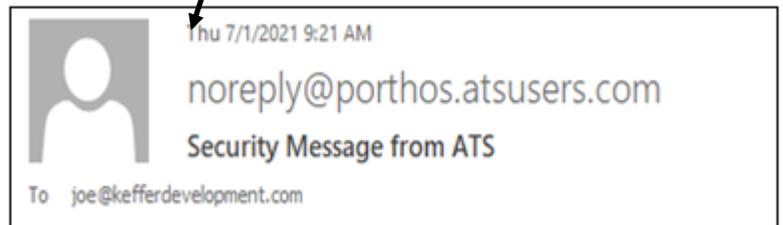
On the Staff Portal, the user will provide their login in credentials. Since they are on the portal, they will see a different delivery method screen. Again, if a text account is entered, both options will be available. They will select how they want the code delivered.

Which method do you want to use to complete the validation process?

Email

Email:

Enter your authorization code.



Enter the verification code you received in the box and you will continue into the site.

## **MFA using an Authentication App:**

*ATS is not recommending one Authenticator app over the other. The process was implemented so that it should work with any available app. We do not have in-depth knowledge of the processes of these and will do our best to help if/as needed.*

During the testing and implementation of the MFA using an authentication app, we utilized Google Authenticator, Microsoft Authentication apps, both have 100+ million downloads as well as Duo Mobile 10+ million, and know they all work. The process should work with any others out there, since there is a variety of apps, we tested these three, on Android and Apple devices. We are not endorsing those, they are what we as staff had downloaded for personal use.

To start using MFA with an Authenticator App, be sure to enable it in Site Info. Please refer to [page 2](#).

ATS does not support Single Sign On (SSO) or other similar features.

## Linking your account to your Authenticator App:

To link your account, go to Admin—> Users—> My User—> Account Security. On the bottom left, along with your Reset Account Questions, you will be able to generate your User Secret Code.

Your User **Secret Code**, is a code unique to you that ties your account in the database to your Authenticator App. Only the user/staff member will be able to see their Secret and/or QR Code.

The screenshot shows the 'User' profile page for 'Joe Streckfus'. The 'Account Security' tab is selected. Under the 'Secret Code' section, there are three buttons: 'Generate', 'View', and 'QR Code'. Below these buttons are two checkboxes: 'MFA Complete' (checked) and 'MFA by Email/Text' (unchecked). The 'Reset Account Questions' section is also visible, with three questions and their answers: 'In what city or town was your first job?' (another city), 'What is the color of your eyes?' (purple), and 'What was the name of your first pet?' (doggo).

Secret Code: **Generate**

**Generate:** will generate your account a string of random characters that will be your secret code. This links your account to the authenticator.

**View**

**View:** Will show your generated code, if you cannot scan the QR code with your Auth app or are having difficulties, this allows for manual entry to tie accounts together. There will be 20 characters

**QR Code**

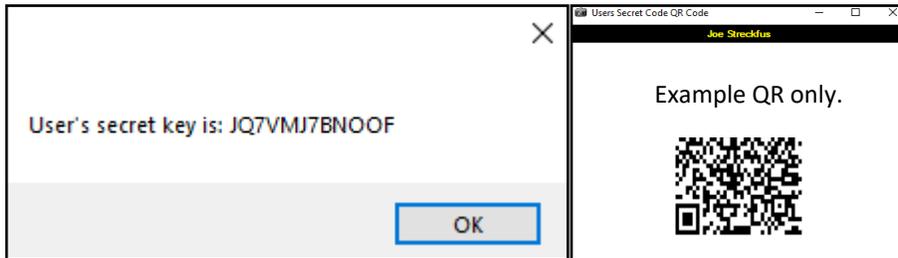
**QR Code:** This will display your account information in a QR code, so you can scan it with your authentication app to tie your accounts together.

MFA Complete  MFA by Email/Text

**MFA Complete or MFA by Email/Text:** If you set up your secret code and QR, this will automatically check off indicating you have completed the setup. If you choose not to use an Auth App, you can check MFA by email/text to satisfy your requirements and not be asked to set it up.

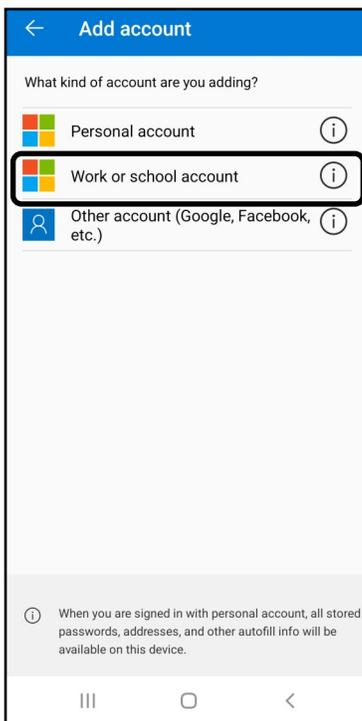
## Linking your account to your Authenticator App Ctd.:

Choose how you want to link your account either with the Code itself, or the QR code. Enter the 20 digit secret key or scan the QR code with your authenticator app. It will register and display an ATS entry.

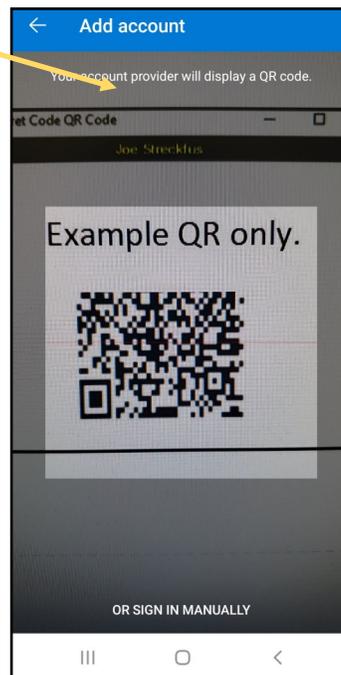


### **Example Setup:**

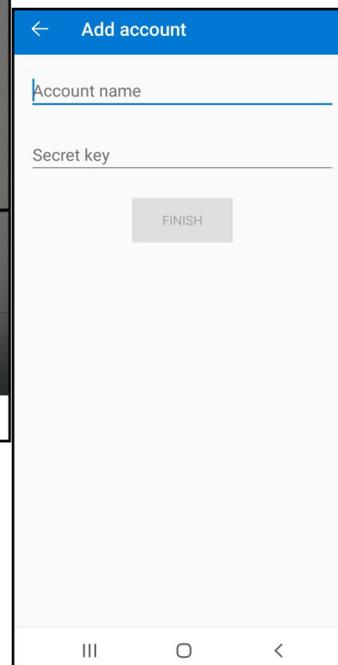
Before continuing on with the authentication app, make sure you do allow your app permission to access the camera on your device. If you do not, you will need to type in the Secret Code.

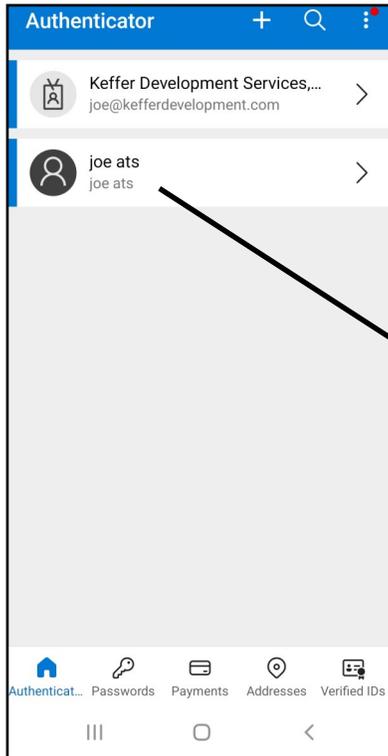


Select the account type you want to add. This example is from Microsoft Authenticator, other apps may have different options or none at all. Google Authenticator just adds on to one list.

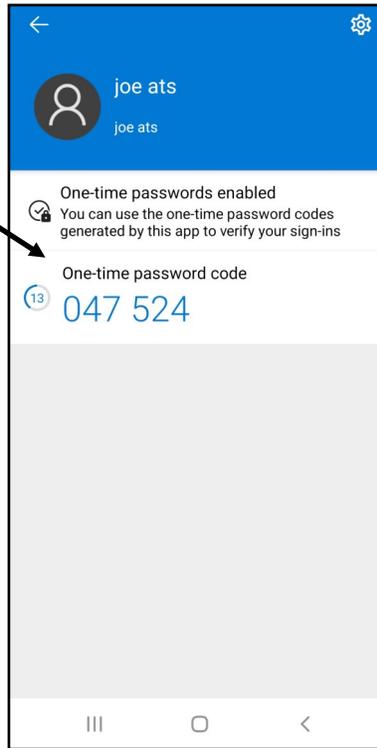


Scan the QR Code with your camera, if you're having trouble, you can input manually. It will ask for an account name and the "key"





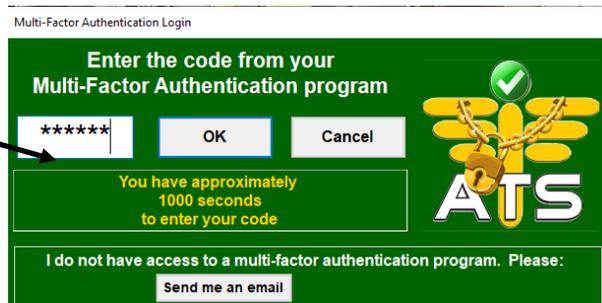
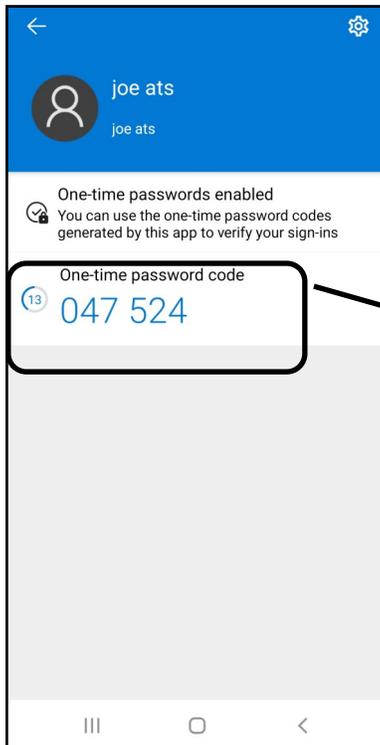
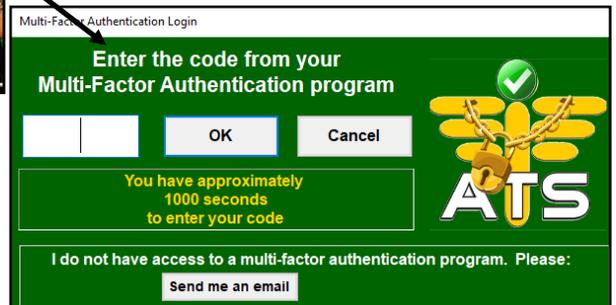
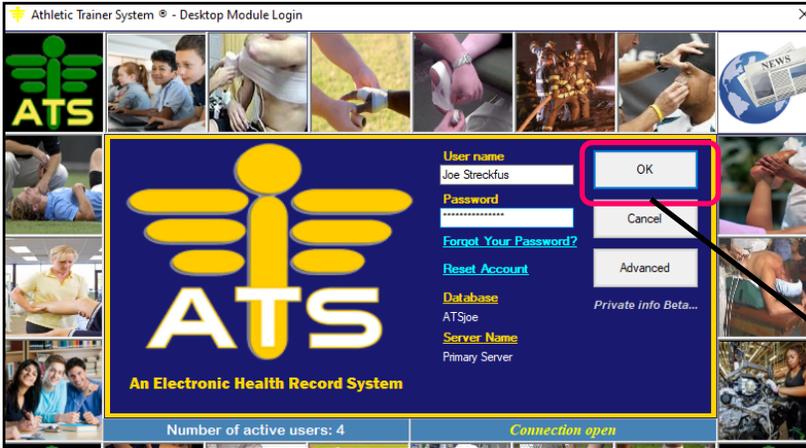
After you successfully scan or enter your Key, you will then have the account show up on the home screen of your authenticator. Select the account for ATS, after logging into ATS, you will be prompted for a code. Enter the code you see on the screen in the box.



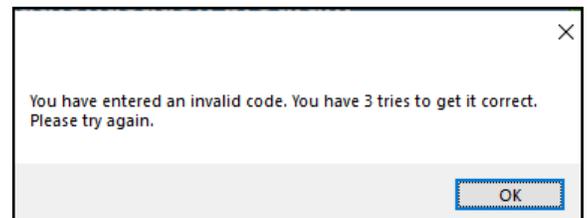
## Using the Authenticator to login:

After you have provided the correct user name, and the correct password, which is Step 1 of the multi-Factor Authentication. You will be prompted for an authentication code from your Authentication app.

- The initial login before you can set it up, you will need to use the send me an email to get into ATS to link your account to your Auth app.



If you enter incorrectly, you will see this message.  
Enter your code again.



## Authenticator App Setup— Staff Portal:

To link your accounts on the staff portal, you will need to navigate to the Utilities Menu. Then to the My User menu.

Only you will be able to see your Secret and/or the QR code. Your admin will not be able to see it or give it to you.

Your first/initial login after this is enabled. If you have not set up an authenticator app, you will be able to select send me an email. That will provide you a code to access the system to set this up.

To access your user screen go to Utilities—> My User—> Account Security.

The screenshot shows the Staff Portal interface. On the left is a navigation menu with categories: Admin, Utilities, Athletes, Injuries, COVID-19 Screening, Notes, Modalities, Rehabs, Limitations, Evaluations, Medical Services, Concussions, Medication, and Distribution. The 'Utilities' menu is expanded, showing sub-items: Daily Information Entry, Hydration Alert Log (Add for a Team, Add for an Athlete, Search by Date/Team), Check Out Equipment, Send Email or Text Messages, Secure Messages (Athletes/Contacts, Staff Members), and Outside EMR Data Exchange. The 'My User' option is highlighted in the Utilities menu. A yellow arrow points from 'My User' to the 'Account Security' tab in the 'My User Maintenance' section. The 'My User Maintenance' section has tabs for General Info, Smartphone Icons, Emergency Contact, My Photo, My Signature, Email Signature, Home Address, and Account Security. The 'Account Security' tab is active, showing a form with three questions and answers: Question #1 (In what city or town was your first job? - another city), Question #2 (What is the color of your eyes? - purple), and Question #3 (What was the name of your first pet? - doggo). Below the form is a 'Save Account Security' button and a 'Secret Code' section with 'Generate', 'View', and 'QR Code' buttons. A black arrow points from the 'Account Security' tab to the 'Secret Code' section.



**Generate:** will generate your account a string of random characters that will be your secret code. This links your account to the authenticator.



**View:** Will show your generated code, if you cannot scan the QR code with your Auth app or are having difficulties, this allows for manual entry to tie accounts together. There will be 20 characters



**QR Code:** This will display your account information in a QR code, so you can scan it with your authentication app to tie your accounts together.

## Logging in on the Staff Portal or Staff Phone with the Auth code:

ATS Staff Portal: Login

User ID: Joe strecktus

Password: .....

Forgot your Password?

Reset your Login

Database: atsjoe

Number of active users: 3

2485 days remaining until your activation expires

Version 1.0.0.0

Copyright © 2024, Keffer Development Services, LLC | Privacy Policy

Log in with your credentials, when you hit log in you will see the screen show to enter your MFA code.

Multi-Factor Authentication Login

Enter the code from your Multi-Factor Authentication program

You have approximately 1 minute to enter your code

OK Cancel

I do not have access to a multi-factor authentication program. Please:

Send me an Email Send me a Text

Enter your MFA code from your authenticator app here.

If you do not have an auth app set up, or wish to not use one, you will be able to utilize a send me an email option or text option.

## MFA for Athletes and Emergency contacts:

In line with the user/staff side, you will also not be able to see the athlete's secret codes.

Athletes and emergency contacts will also need to establish a second factor, either the MFA or using the standard 2-factor.

In their accounts, athletes will need to go to Account Security. And repeat the same process the staff did:

- ⇒ Generate a Secret Key
- ⇒ Either manually View and enter the key, or scan the QR code in their authenticator app.

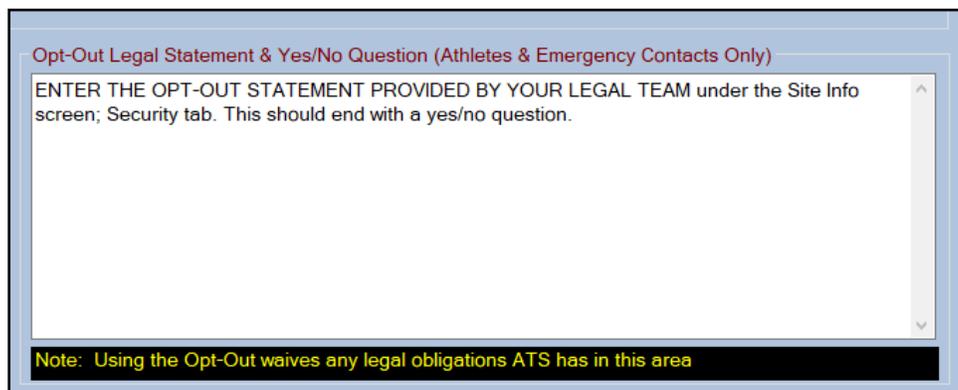


The screenshot shows a web interface with a top navigation bar containing tabs for: General, Medical History, Sickle Cell, Screen/Test/Vacc, Immunizations/Paperwork, Insurance, Contacts, Forms, eFiles, and Account Security (which is highlighted in blue). Below the tabs, there is a section labeled "Secret Code" with three buttons: "Generate", "View", and "QR Code". At the bottom of this section is a "Save Account Security" button.

## Athletes and emergency contacts opting out of MFA:

If you wish to allow athletes/emergency contacts to opt out of using MFA, they will have to do that through their accounts. For security reasons and because it is their account information, there is not a way to opt them out administratively.

To allow them the option of opting out, you will need to enter a statement in Admin—> Site Info—> Security.



The screenshot shows a form titled "Opt-Out Legal Statement & Yes/No Question (Athletes & Emergency Contacts Only)". The form contains a text area with the instruction: "ENTER THE OPT-OUT STATEMENT PROVIDED BY YOUR LEGAL TEAM under the Site Info screen; Security tab. This should end with a yes/no question." Below the text area is a "Note: Using the Opt-Out waives any legal obligations ATS has in this area".