

## App-Specific Passwords

Starting on May 30<sup>th</sup>, 2022, Google will no longer allow clients to turn on the “Less Secure App Access” setting within their Google accounts. The setting will be removed entirely from the security screen and, presumably, many of our clients using the free texting feature will all end up getting BAD CREDENTIAL errors. While this is not 100% confirmed, it’s better to be safe than sorry. The steps listed below will explain how to setup “App-Specific Passwords” for Gmail users (so far this has been tested and works).

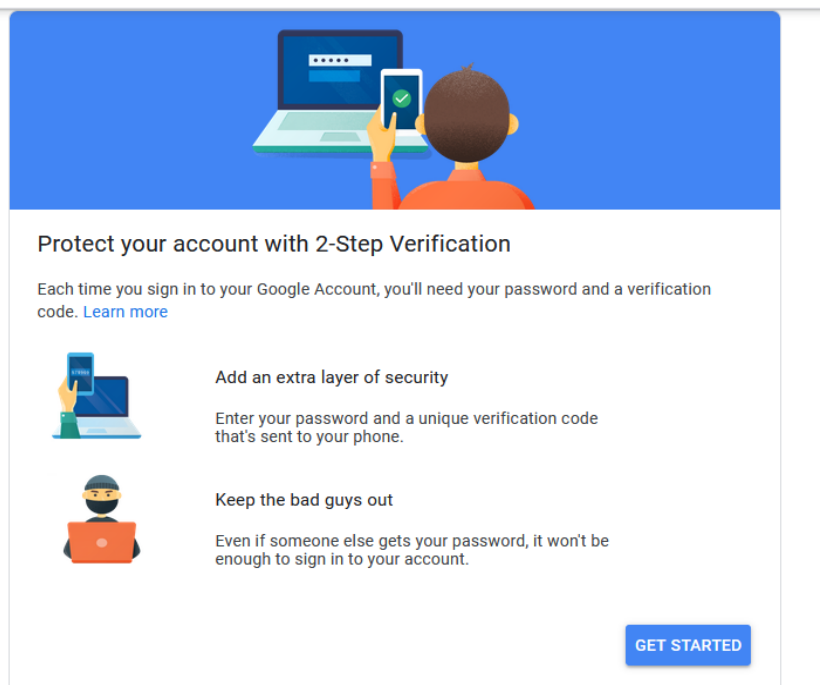
1. To begin, we will be doing the same steps as we would to get to “Less Secure App Access”. Simply open Gmail, and select the Profile icon in the top right of the screen. In the pop-out menu, select “Manage Your Google Account”.

2. In the past, we’ve always told everyone to turn off “Two-Step Authentication” for the “Less Secure App Access” setting to appear. Now, we will be turning **ON** “Two-Step Authentication”.

**NOTE: Please keep in mind, the Client will NEED a working Cell Phone for this to work. Make SURE the phone number being used is ALWAYS accessible. If we turn this setting on they will need their password and a code from their phone to sign in. My suggestion would be to use the Provider/Owner’s Cell Phone # for this, however, defer to the Office for what they would prefer.**


3. Click on Security from the left menu. In the middle of the screen in the Signing in to Google section you will see 2-Step Verification. Click on the Off icon to enable it. Once you elect to turn on Two-Step Authentication, you will be brought to this screen. Click “Get Started”.

← 2-Step Verification




Protect your account with 2-Step Verification

Each time you sign in to your Google Account, you'll need your password and a verification code. [Learn more](#)

 Add an extra layer of security

Enter your password and a unique verification code that's sent to your phone.


 Keep the bad guys out

Even if someone else gets your password, it won't be enough to sign in to your account.

[GET STARTED](#)


4. Enter in the Gmail Account's password, and on the next screen confirm the Phone Number for the account. At this point, the Client can change the phone number to whatever they prefer. At the bottom, they can select how they would like to receive their codes. They can choose either Text Message or Phone Call. Again, for simplicity sake, I'd select Text Message. After making your selection, click Next.

← 2-Step Verification



**Let's set up your phone**

What phone number do you want to use?

 ▼ +1 352-346-3513

Google will only use this number for account security.  
Don't use a Google Voice number.  
Message and data rates may apply.

How do you want to get codes?

Text message     Phone call

[Show more options](#)

5. Within a few minutes of clicking Next, they will receive a code to the device. Simply enter the Code and Click next.

6. On the next screen, select "TURN ON" and it will bring you to your Two-Step Authentication page. On this screen, click on the backwards facing arrow to return to the security page.



## ← 2-Step Verification

2-Step Verification is ON since Apr 1, 2022

**TURN OFF**

### Available second steps

A second step after entering your password verifies it's you signing in. [Learn more](#)

**Note:** If you sign in to your Google Account on any eligible phone, Google prompts will be added as another method for 2-Step Verification.



#### Voice or text message (Default) ⓘ

(352) 346-3513 **Verified**

Verification codes are sent by text message.



### Add more second steps to verify it's you

Set up additional backup steps so you can sign in even if your other options aren't available.



#### Backup codes

These printable one-time passcodes allow you to sign in when away from your phone, like when you're traveling.



7. Click the back arrow to go back to the Security Page and scroll down to the box labeled “Signing in to Google” you’ll notice a new option has been added labeled “App-Specific Passwords”. Click this. It will ask for your password, enter it and proceed.

## Signing in to Google



Password

Last changed Mar 2, 2021



2-Step Verification

On



App passwords

None



8. You will be prompted for your password. Once entered, click OK and on this Page, titled “App Passwords” you will have two boxes. One says “Select App” the other says “Select Device”. Under the Box that says “Select App” choose “Other”, the box will then change to a text field, allowing you to name the App using this password. Simply type “ECLIPSE” and click “Generate”. Your screen should look like this:

## ← App passwords

---

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)

You don't have any app passwords.

Select the app and device you want to generate the app password for.

Select app ▼ Select device ▼

[GENERATE](#)

After you choose “Other” and fill in the name, it will look like this:

## ← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)

You don't have any app passwords.

Select the app and device you want to generate the app password for.

ECLIPSE ×

GENERATE

Click Generate and you will then be given this screen:

## Generated app password

Your app password for your device

eakq oliq itjs noug

How to use it

Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above.

Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

DONE

10. Copy the password from the box (highlight it, copy it (ctrl + c)). In ECLIPSE, click on File | Database Tables | Users. Enter your System Administrator Password and click OK.

Open each user that will be using this email and replace the current password with the app password from Google. Once you've done this, click "DONE".

**IMPORTANT: DO NOT CLOSE THIS SCREEN UNTIL YOU ARE 100% DONE WITH CHANGING THE PASSWORD IN EVERY ECLIPSE USER THAT WILL BE EMAILING. FAILURE TO DO SO WILL REQUIRE YOU TO DELETE THE PASSWORD AND GENERATE A NEW ONE. YOU CAN NOT RETRIEVE THIS PASSWORD AFTER CLOSING THIS SCREEN.**

# Using App Passwords

## For Emailing and Texting:

1. To correct issues related to sending Emails and Text Messages using Gmail, first copy the password on the screen. You can do this by left clicking and dragging from the left to the right. Right click when all the letters are highlighted and choose “Copy”.
2. Go into the ECLIPSE program and open up File > Database Tables > Users. Enter in your Admin password and open up any of the users that send emails/text messages. On the right side of this screen, you will see a section headed “Email”.

**Edit User Information**

**Personal** **Permits**

First: default Middle:

Last: administrator

Dept. / ID#:  0

Logon ID: ADMIN

User type:

Password:  Enter up to 20 characters

This user is currently active & will appear in the user name index (all users appear in the ID index).

Encounters: Limit locks to provider below (0-0 = all) & assign as default provider for new Encounters. Office Stats, (0-0)

Email: User name: testemail@gmail.com Password:  Return address: testemail@gmail.com  User name & password required for authentication

DrFirst Prescription Module: User name:  Password:  Log off this user after idle for: Not used  Don't log off: terminate the program

3. Right click in the password box and, in the pop-out menu, click “Paste”. This will paste your new, 16-character password in the box, it will not have the spaces that seem to be present on the App Password section, however, that is intended. Your screen should now look like this:

Personal Permits

First default Middle

Last administrator

Dept. / ID# 0

Logon ID ADMIN

User type

Password •••••  
Enter up to 20 characters

This user is currently active & will appear in the user name index (all users appear in the ID index).

Encounters  
Limit locks to provider below (0-0 = all) & assign as default provider for new Encounters.

Office Stats, (0-0)

Email

User name testemail@gmail.com

Password drrtyuuopiolkjyu

Return address testemail@gmail.com

User name & password required for authentication

Test Email Settings

DrFirst Prescription Module

User name

Password

Log off this user after idle for  
Not used

Don't log off: terminate the program

OK Cancel Help

4. Simply follow these instructions for all users who send emails/text messages and you should be able to resume sending as normal. You must log off of ECLIPSE and log back in for the changes to take affect.




## For Google Calendar:

1. To correct issues related to using the Google Calendar, first copy the password on the screen. You can do this by left clicking and dragging from the left to the right. Right click when all the letters are highlighted and choose "Copy".
2. Go into the ECLIPSE program and open up File > Database Tables > Providers. On the right side of this screen, you will see a line titled "Email" and one below that titled "Password".

Edit Provider Information ×

General PIN's Appointments

Office ID	<input type="text" value="0"/>	Phone / Ext	<input type="text" value="575-353-2312"/>
Provider ID	<input type="text" value="1"/>	Fax	<input type="text"/>
Office name	<input type="text" value="Florida Doctors"/>	E-mail	<input type="text" value="stemail@gmail.com"/>
Provider first	<input type="text" value="John"/>	Password	<input type="password"/> 
Provider last	<input type="text" value="Florida"/>	Direct	<input checked="" type="checkbox"/>
Suffix	<input type="text" value="Sr"/>	Degree	<input type="text" value="D.C."/> ▾
Address	<input type="text" value="123 Anywhere Blvd"/>	Entity type	<input type="text" value="Person"/> ▾
City	<input type="text" value="Tampa"/>	Provider Code	<input type="text" value="Billing"/> ▾
State / Zip	<input type="text" value="FL"/> <input type="text" value="33605-145"/>	CC Merchant ID Override	<input type="text"/>
Comments	<input type="text"/>	Retail (swipe)	<input type="text"/>
		Stored CC	<input type="text"/>

This provider is not currently active & will not appear in the active provider name index (all providers appear in the other indexes).

Enable Google calendar updates

Hold (do not create) new bills. NOTE: This disallows all new bills for current patient case once a service is added for this provider.

3. Right click in the password box and, in the pop-out menu, click “Paste”. This will paste your new, 16-character password in the box, it will not have the spaces that seem to be present on the App Password section, however, that is intended. Your screen should now look like this:

Office ID: 0

Provider ID: 1

Office name: Florida Doctors

Provider first: John

Provider last: Florida

Suffix: Sr

Address: 123 Anywhere Blvd

City: Tampa

State / Zip: FL 33605-145

Comments:

Phone / Ext: 575-353-2312

Fax:

E-mail: testemail@gmail.com

Password: drtyuuopiolkjyu

Direct:

Degree: D.C.

Entity type: Person

Provider Code: Billing

CC Merchant ID Override

Retail (swipe):

Stored CC:

This provider is not currently active & will not appear in the active provider name index (all providers appear in the other indexes).

Enable Google calendar updates

Hold (do not create) new bills. NOTE:  This disallows all new bills for current patient case once a service is added for this provider.

Copy existing database entry

OK Cancel Help

4. Simply follow these instructions for all providers who utilize the Google Calendar. This concludes the portion of the setup related to Google Calendar Updates.