Cognivue® Portal

User Manual

© 2023 COGNIVUE, INC. 7911 Rae Blvd | Victor, NY 14564 | 585.203.1969

Cognivue® Portal User Manual

Contents

About This Guide

This User Manual contains information that describes the access and operation of the Cognivue Portal. Additional information can be found at www.cognivue.com. Cognivue Support personnel can be reached from 9-5pm EST at 1-585-433-2992 or support@cognivue.com.

UM-450-G Cognivue Portal User Manual, 2/14/2023

cognivue®

7911 Rae Blvd | Victor, NY 14564 | 585.203.1969

1.0 About the Cognivue Portal

Cognivue Clarity® Device is a computerized cognitive assessment aid that objectively, quantitatively and reliably evaluate cognitive function. Cognivue Thrive® Device is a computerized cognitive assessment aid that objectively, quantitatively and reliably screens out cognitive impairment. After a user completes a series of subtests, both devices produce easy-to-interpret reports with scores of various cognitive domains. The test results and associated reports are stored on the Cognivue device used to take the test.

The Cognivue Portal enables you to access your Cognivue Clarity Device or Cognivue Thrive Device data from anywhere you have access to the internet. In addition, the Portal makes it easier for you to search for and find reports. Specifically the Portal allows authorized users in your organization to:

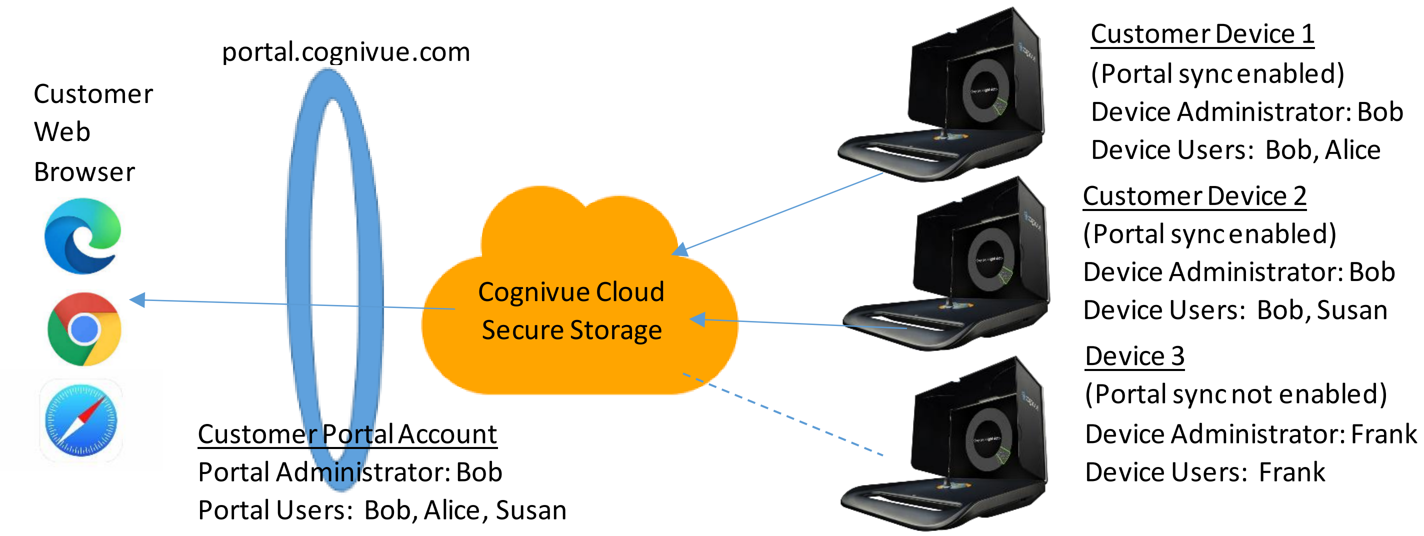
- Search for patients who have taken a Cognivue test on your devices
- View a summary of the test results available for that patient
- View reports for that patient
- View a trend of the scores for that patient
- List and view all reports across all your patients and devices
- Download and share reports

The Portal is to be used by subscribed Cognivue Customers only and is not intended to provide direct patient access to Cognivue Test Reports. Its purpose is solely to transfer, store and display results. It is the responsibility of the Customer to provide patient access to Patient Data in accordance with their data privacy and security procedures and guidelines. This may include procedures such as giving a printed copy to a patient or sending secure email (outside of the Cognivue product).

For information about the Cognivue Clarity Device and Thrive Device, including a description of the intended use of the devices and their test results, please refer to their respective User Manual.

2.0 Portal Description

The Cognivue Portal uses secure cloud-based storage to enable access across all your devices (see the figure below).



As shown, you can use any modern web browser to access the portal. Access to the portal is controlled separately from access on the device. In order to access data via the portal the following must occur:

1) The device must be configured to sync with the portal. Each device needs to be configured separately.
2) Cognivue Device users must separately be given access to the portal.
3) Portal users need to be assigned to devices that they have access to.

Cognivue implements a management approved and funded Information Security and Privacy Program that is HIPAA Compliant and ISO 27001 aligned. This program has been implemented to help ensure the confidentiality, integrity, availability, and privacy of its clients and partners. The program includes administrative, physical and technical controls that include, but are not limited to, the following:

1. Risk Management and Assessments
2. Data Management and Classification
3. Asset and Vendor Management, including BAAs in place for all critical vendors
4. Physical Security Controls
5. Workforce Security Controls
6. Identity and access Management Controls
7. Software Development Lifecycle and Change Management
8. Infrastructure Security Controls
9. Contingency Planning, Disaster Recovery and Business Continuity
10. Privacy and Data Use Controls

3.0 Recommendations for Use

To provide an efficient, secure use of the portal, Cognivue recommends the following practices.

1) Follow your organizational procedures for protecting patient security, privacy, and access to reports.
2) The Portal is developed for customer staff only. Patients should not have direct access or a login to the portal.
3) Implement Minimum Necessary access to accounts. Device Administrators do not need to be Portal Administrators. It is not recommended to give Portal Administrator access to a user unless they are intended to manage your portal accounts and settings.
4) Cognivue reports should be shared with patients using HIPAA compliant and secure procedures maintained by the customer organization. This may include secure email, paper printout or EMR integrations.
5) Passwords for the portal should be long and complex and be developed according to the customer organization's security policies. Where possible they should be random and stored in a password manager.

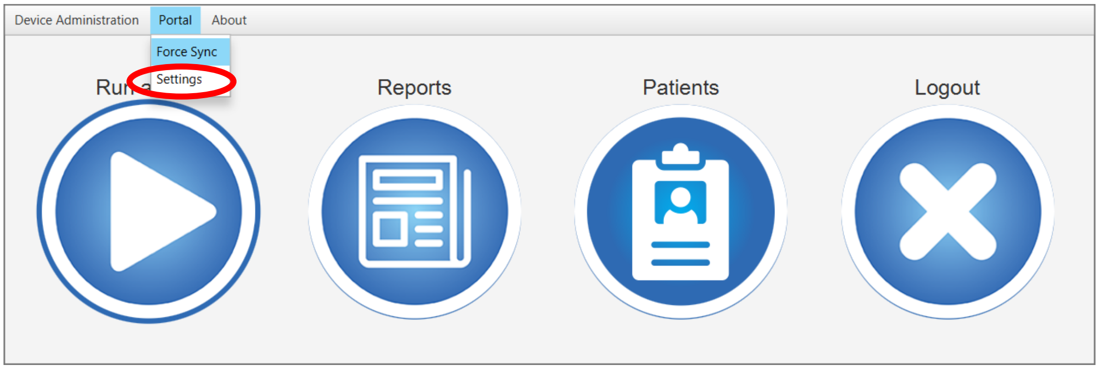
4.0 Getting Started & User Management

4.1 Configuring a Cognivue Device to Sync to the Portal

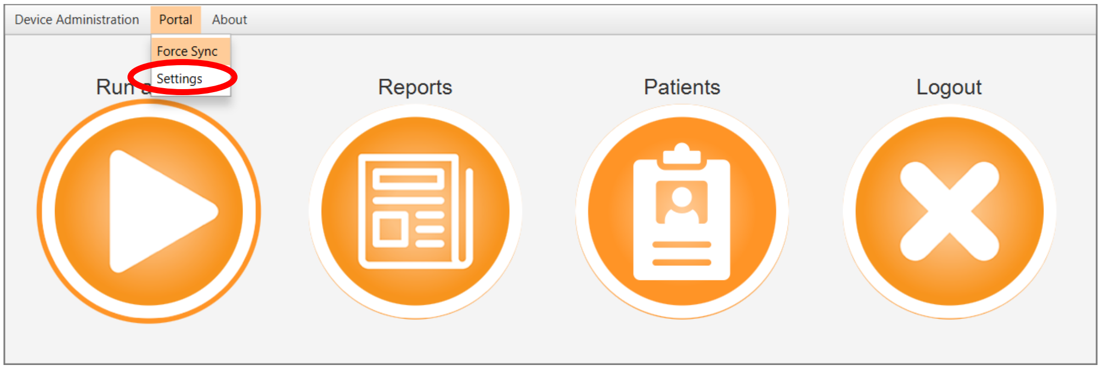
An Administrator can enable this functionality by going to the Portal menu in the main window and clicking on settings.

To enable the device to sync to the portal, the Device Administrator first selects "*Portal*" and "*Settings*" from the main window.

Main Device Window – Device Administration Menu – Clarity

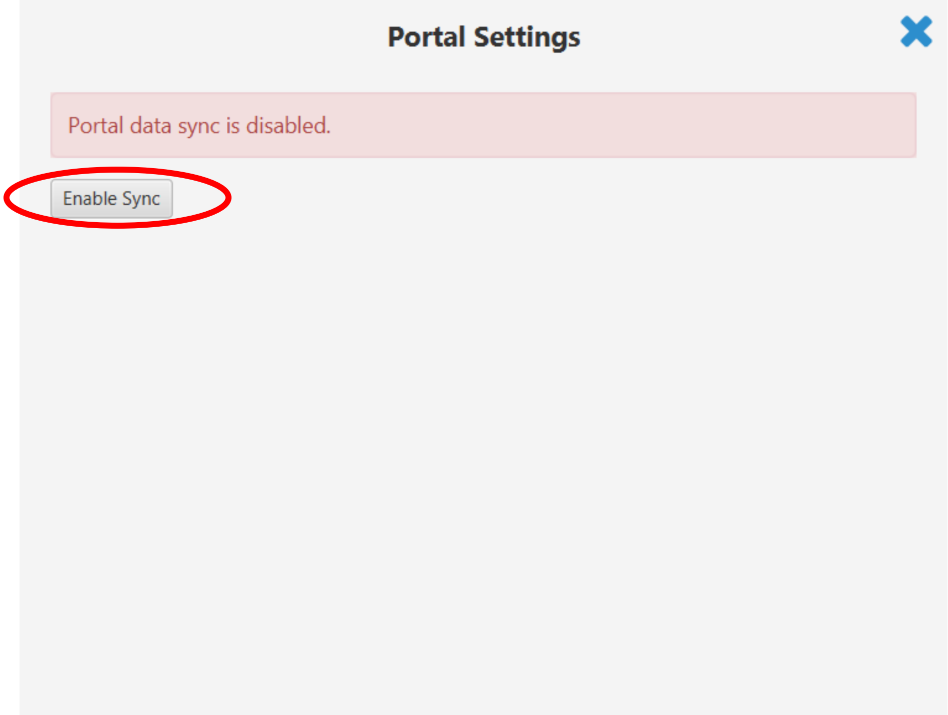


Main Device Window – Device Administration Menu - Thrive



In the portal settings window, click on the "Enable Sync" button(circled below).

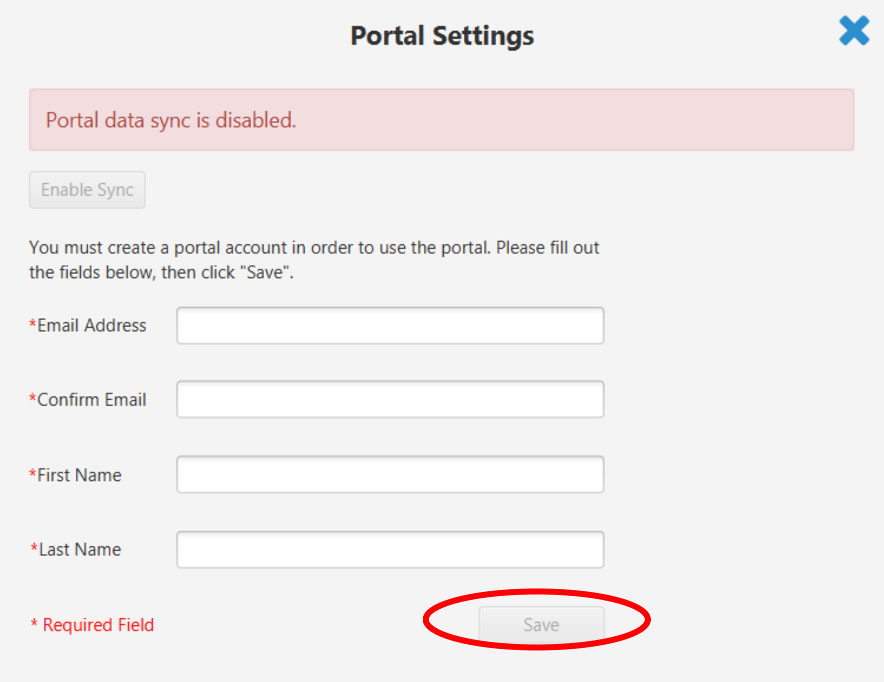
Portal Settings Window



Portal Settings

Portal data sync is disabled.

Fill in the information and click the save button. This will create the initial administrator account in the portal.



Portal Settings

Portal data sync is disabled.

You must create a portal account in order to use the portal. Please fill out the fields below, then click "Save".

*Email Address

*Confirm Email

*First Name

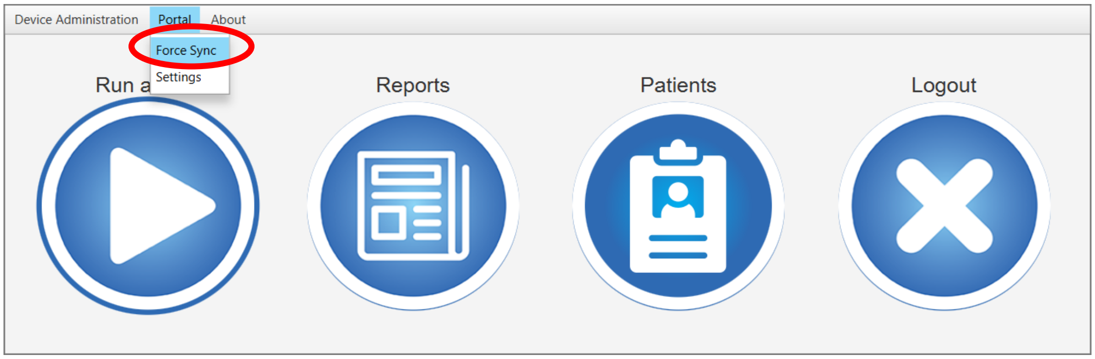
*Last Name

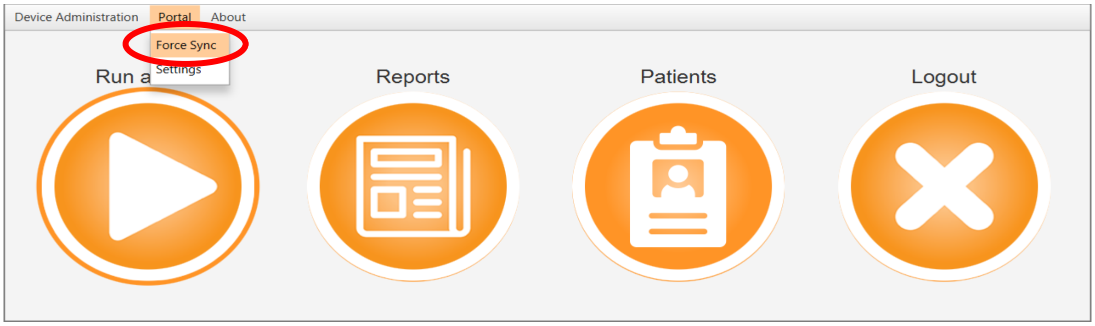
* Required Field

By default, the data sync will begin upon completion of the next patient test. If an administrator wants to force the sync to occur immediately, they can select the "Force Sync" option from the

Portal menu to send data from the device to the Portal system. At the main window, click the "*Portal*" menu and select "*Force Sync*".

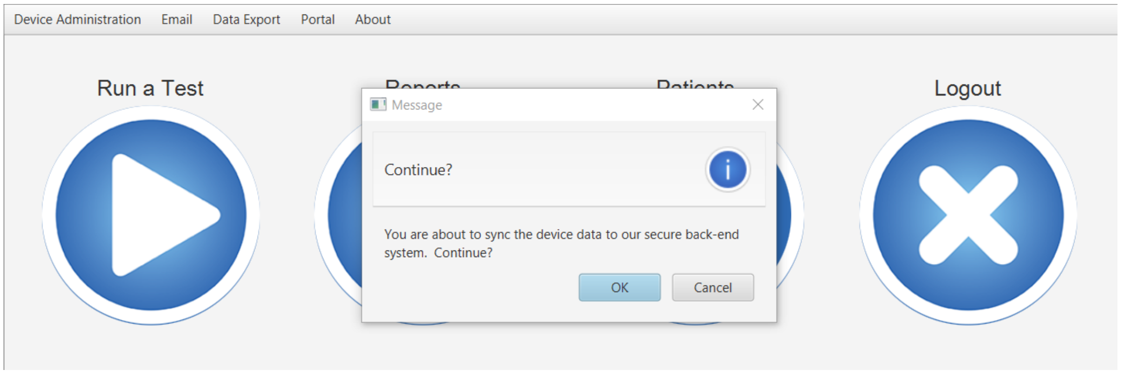
Force Sync – Clarity





Force Sync - Thrive

A pop-up window will allow you to confirm or cancel the start of the data sync.



Continue?

You are about to sync the device data to our secure back-end system. Continue?

The next step is to setup the Portal Accounts.

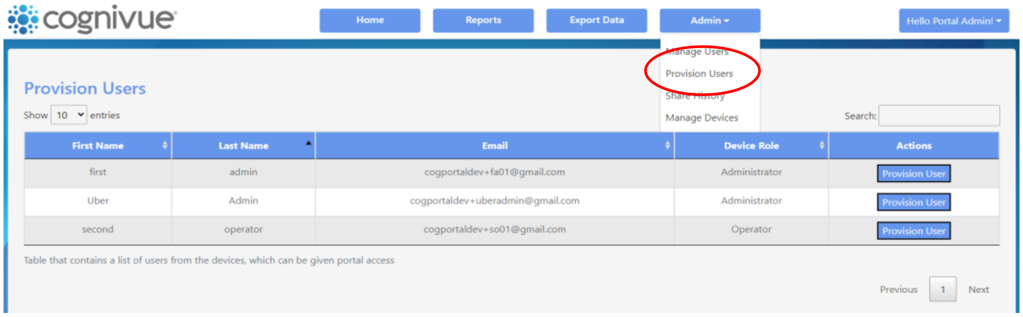
4.2 Setting up the First Portal Account

The initial portal administrator account is created with the information provided by the device administrator, when enabling the sync in the portal settings window.

4.3 Granting Device Users to Access the Portal (Provisioning Users)

Device Users don't automatically have access to the Portal - instead, they must be granted access to the Portal by a process called "provisioning". To do this, a Portal Administrator uses the ***Provision Users*** menu on the Portal to grant device users access to the portal. The process for provisioning users is provided below.

1. Log into the Portal as an administrator.
2. Navigate to the Admin drop-down button, then select Provision Users:



Provision Users

Show 10 entries Search:

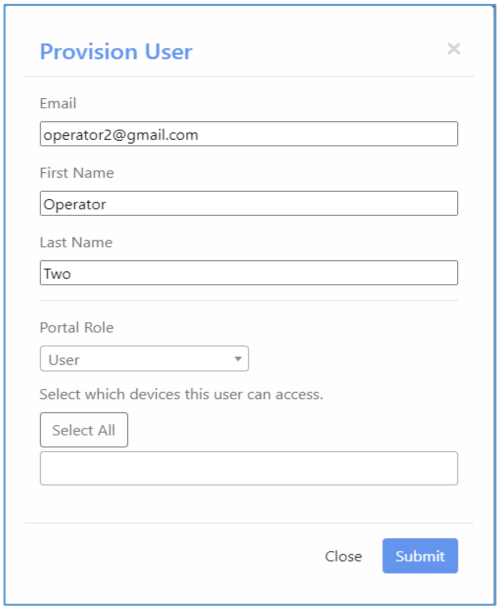
First Name	Last Name	Email	Device Role	Actions
first	admin	cogportaldev+fa01@gmail.com	Administrator	Provision User
Uber	Admin	cogportaldev+uberadmin@gmail.com	Administrator	Provision User
second	operator	cogportaldev+so01@gmail.com	Operator	Provision User

Table that contains a list of users from the devices, which can be given portal access

Previous 1 Next

Portal Provision Users Window

3. Find the user you would like to give access to, then click Provision User:



Provision User ×

Email
operator2@gmail.com

First Name
Operator

Last Name
Two

Portal Role
User ▾

Select which devices this user can access.

Select All

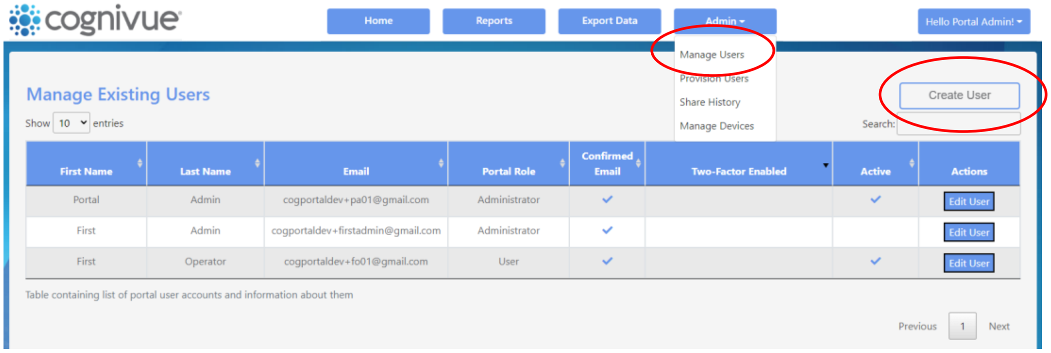
Close Submit

4. Ensure the user's information is correct
5. Assign the correct user role
6. The user will have access to information from the devices selected from their account. Users with the Administrator role will have access to information from all testing devices for their account. Administrators also have the ability to manage and provision Users.
7. When finished, click the Submit button
8. The user will receive an email asking them to finish setting up their Portal account. The email will contain a link to the Portal and a temporary password.

4.4 Adding a New User that is not a Device User to the Portal

A user can be created directly in the Portal, rather than provisioned from a user on the device. This user will be associated with the same account as the admin who created it.

1. From the Portal Admin Page – Manage Users click the Create User button.



Manage Existing Users

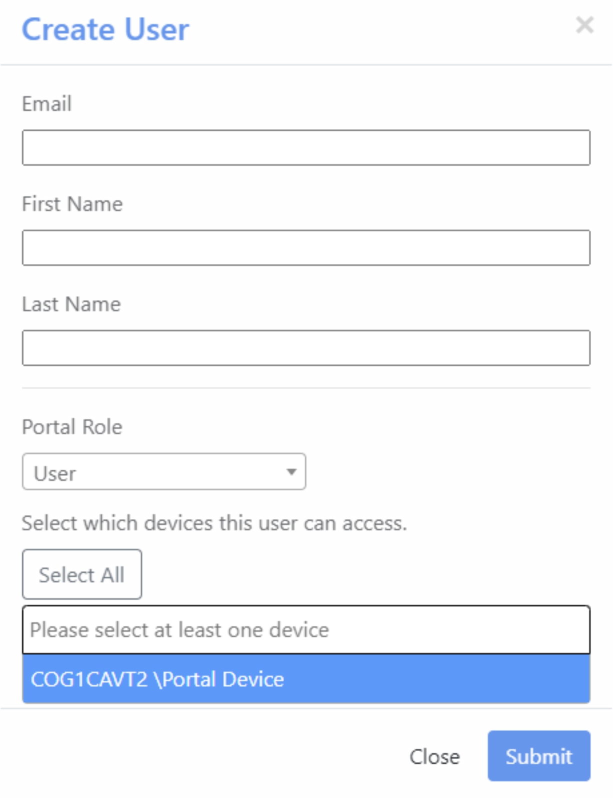
Show 10 entries

First Name	Last Name	Email	Portal Role	Confirmed Email	Two-Factor Enabled	Active	Actions
Portal	Admin	cogportaldev+pa01@gmail.com	Administrator	✓		✓	Edit User
First	Admin	cogportaldev+firstadmin@gmail.com	Administrator	✓			Edit User
First	Operator	cogportaldev+fo01@gmail.com	User	✓		✓	Edit User

Table containing list of portal user accounts and information about them

Previous 1 Next

2. Fill in the information for the User:



Create User

Email

First Name

Last Name

Portal Role

User

Select which devices this user can access.

Select All

Please select at least one device

COG1CAVT2 \Portal Device

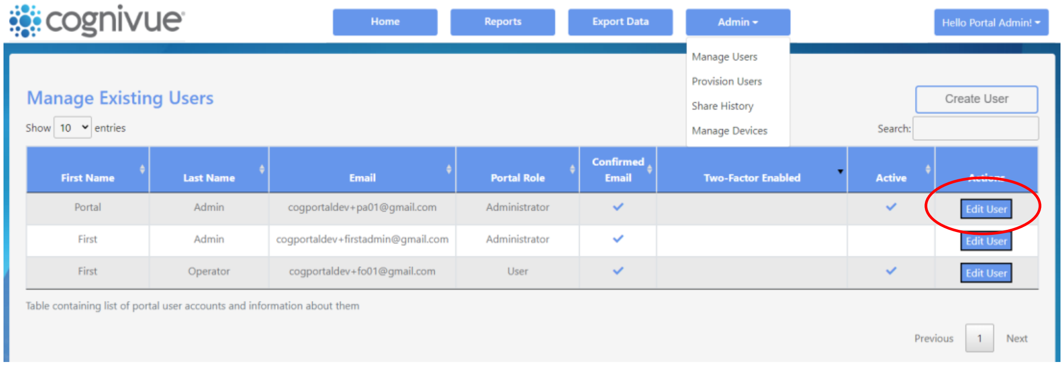
Create User Window

3. Assign the desired user role for the user. It is not recommended to give Administrator access to a user unless they are intended to manage your portal accounts and settings.

4. The user will have access to information from the devices selected from their account. Users with the Administrator role will have access to information from all testing devices for the account. Devices deactivated and then reactivated, will be selectable if the device has been used to run tests for your Account, previously.
5. When finished, click the Submit button.
6. The user will receive an email asking them to finish setting up their account.

4.5 Editing a user

The characteristics of existing users can be modified if the 'Edit User' button is selected on the Portal Admin page.



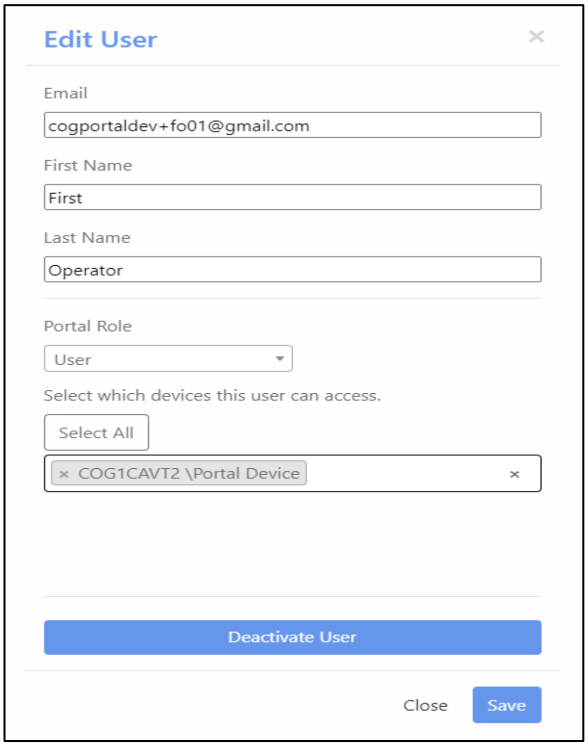
Manage Existing Users

Show 10 entries

First Name	Last Name	Email	Portal Role	Confirmed Email	Two-Factor Enabled	Active	Actions
Portal	Admin	cogportaldev+pa01@gmail.com	Administrator	✓		✓	Edit User
First	Admin	cogportaldev+firstadmin@gmail.com	Administrator	✓			Edit User
First	Operator	cogportaldev+fo01@gmail.com	User	✓		✓	Edit User

Table containing list of portal user accounts and information about them

The window shown below can then be used to modify the appropriate user data. The button on the bottom of the window can be used to either deactivate or activate users.



Email: cogportaldev+fo01@gmail.com

First Name: First

Last Name: Operator

Portal Role: User

Select which devices this user can access.

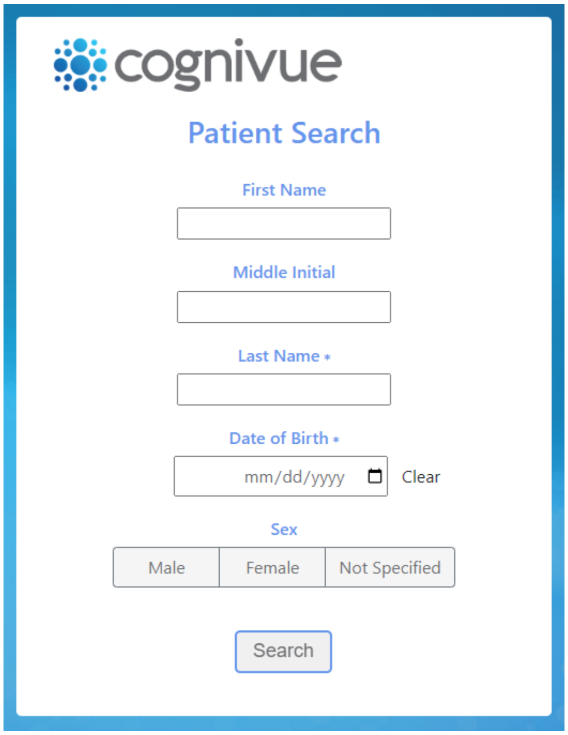
× COG1CAVT2 \Portal Device

Edit User Window

5.0 Portal Functionality

5.1 Searching for Patients & The Patient Dashboard

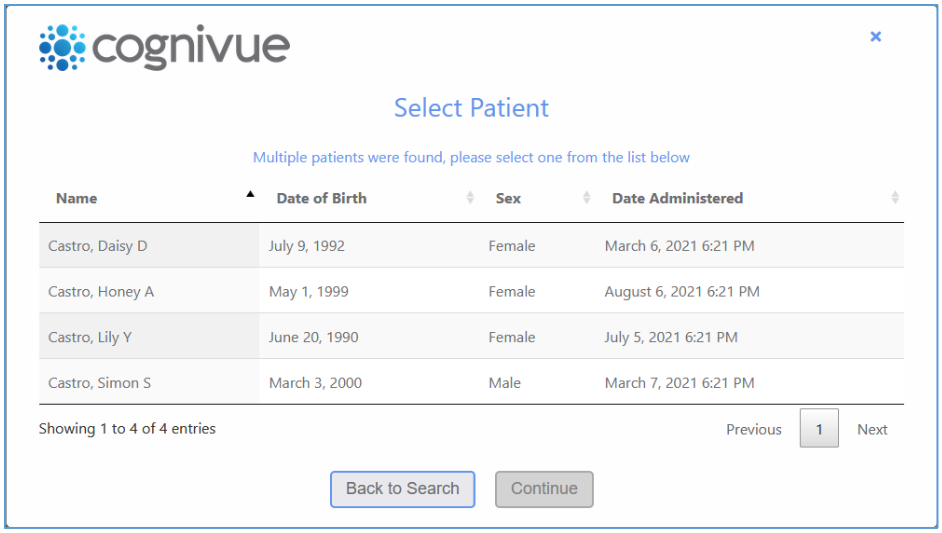
When first logging into the site, or after clicking the New Search button from the Patient Information Dashboard, the patient search box will be available:



Patient Search Window

1. The minimum information required to search is either Date of Birth or Last Name , though providing more information will help make finding the right person easier.

2. If your search produces multiple results, you will be asked to select a single person from a list:



Select Patient

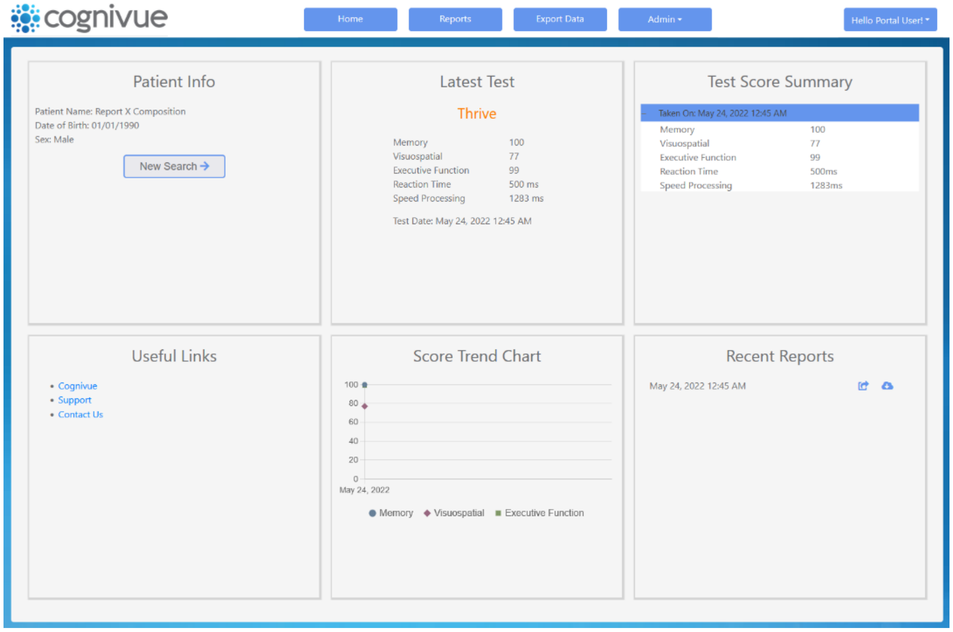
Multiple patients were found, please select one from the list below

Name	Date of Birth	Sex	Date Administered
Castro, Daisy D	July 9, 1992	Female	March 6, 2021 6:21 PM
Castro, Honey A	May 1, 1999	Female	August 6, 2021 6:21 PM
Castro, Lily Y	June 20, 1990	Female	July 5, 2021 6:21 PM
Castro, Simon S	March 3, 2000	Male	March 7, 2021 6:21 PM

Showing 1 to 4 of 4 entries

Select Patient Window

3. Once you've selected a patient, you will be taken to the patient dashboard that contains an overview of that patient's most recent test results.



Patient Info

Patient Name: Report X Composition
Date of Birth: 01/01/1990
Sex: Male

Latest Test

Thrive

Memory	100
Visuospatial	77
Executive Function	99
Reaction Time	500 ms
Speed Processing	1283 ms

Test Date: May 24, 2022 12:45 AM

Test Score Summary

Taken On: May 24, 2022 12:45 AM

Memory	100
Visuospatial	77
Executive Function	99
Reaction Time	500ms
Speed Processing	1283ms

Useful Links

- Cognivue
- Support
- Contact Us

Score Trend Chart

Recent Reports

May 24, 2022 12:45 AM

Example Patient Dashboard

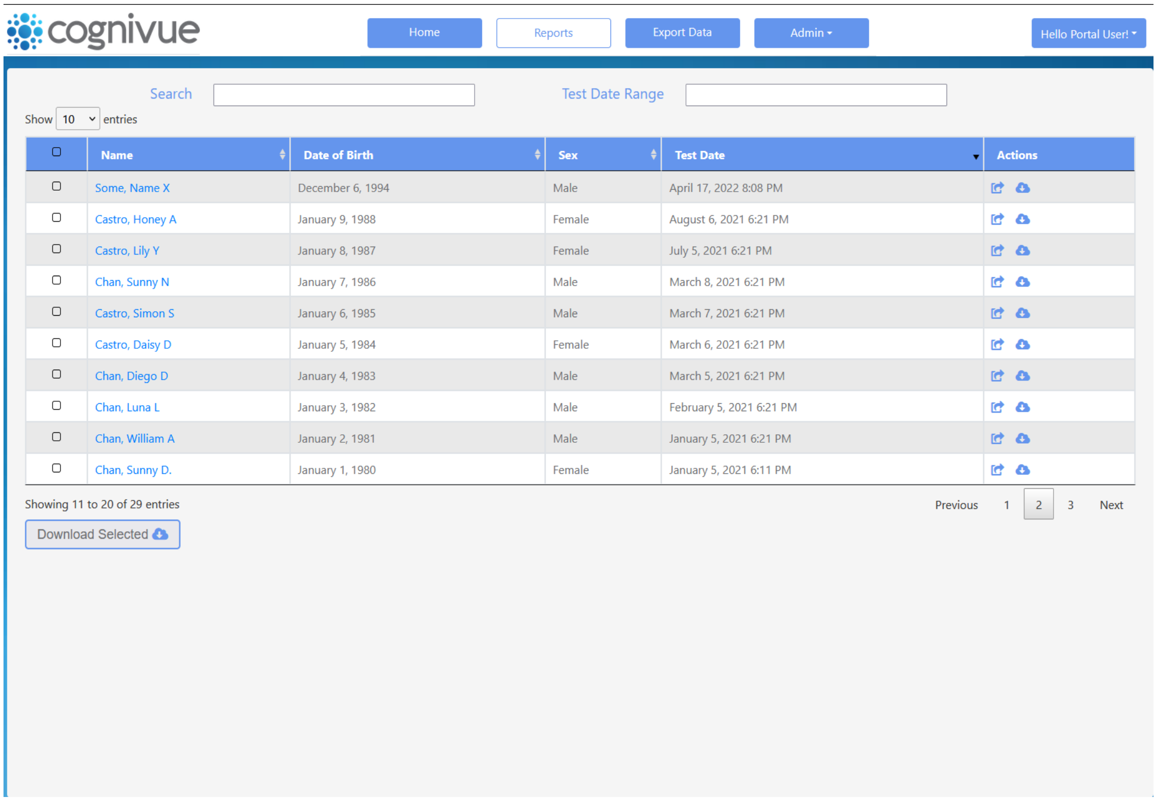
The left panels of the dashboard provides patient information, the ability to start a new search, and some useful links for contacting Cognivue.

In the center panel, the latest test score and test score trend are displayed.

In the right panel, a listing of test scores and recent reports are provided. If you select the links on this panel, you will be able to share or download the selected report.

5.2 The Reports Page

When the Reports Button at the top of the window is selected, a listing of all reports on all the devices that you have access to will be provided. This listing can be sorted by any of the columns as well as searched by patient name or test report range.



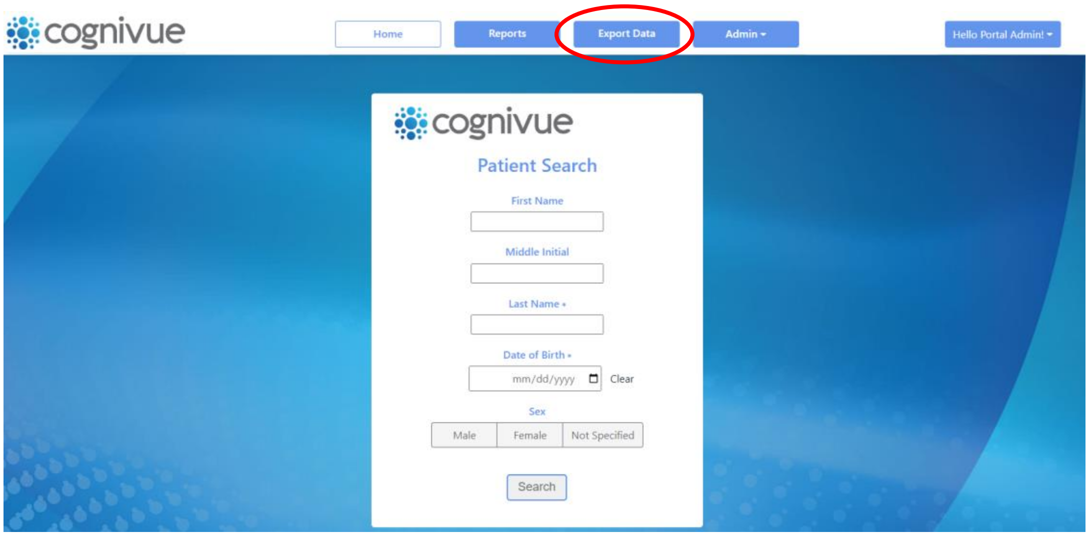
□	Name	Date of Birth	Sex	Test Date	Actions
□	Some, Name X	December 6, 1994	Male	April 17, 2022 8:08 PM	↗ ☁
□	Castro, Honey A	January 9, 1988	Female	August 6, 2021 6:21 PM	↗ ☁
□	Castro, Lily Y	January 8, 1987	Female	July 5, 2021 6:21 PM	↗ ☁
□	Chan, Sunny N	January 7, 1986	Male	March 8, 2021 6:21 PM	↗ ☁
□	Castro, Simon S	January 6, 1985	Male	March 7, 2021 6:21 PM	↗ ☁
□	Castro, Daisy D	January 5, 1984	Female	March 6, 2021 6:21 PM	↗ ☁
□	Chan, Diego D	January 4, 1983	Male	March 5, 2021 6:21 PM	↗ ☁
□	Chan, Luna L	January 3, 1982	Male	February 5, 2021 6:21 PM	↗ ☁
□	Chan, William A	January 2, 1981	Male	January 5, 2021 6:21 PM	↗ ☁
□	Chan, Sunny D.	January 1, 1980	Female	January 5, 2021 6:11 PM	↗ ☁

Showing 11 to 20 of 29 entries

Individual reports can be downloaded by clicking on the cloud icon in the right-most column. Reports may also be emailed to recipients with the page-with-arrow icon in the right-most column. You can also select multiple reports in the first column and download them at the same time using the "Download Selected" button at the bottom of the screen.

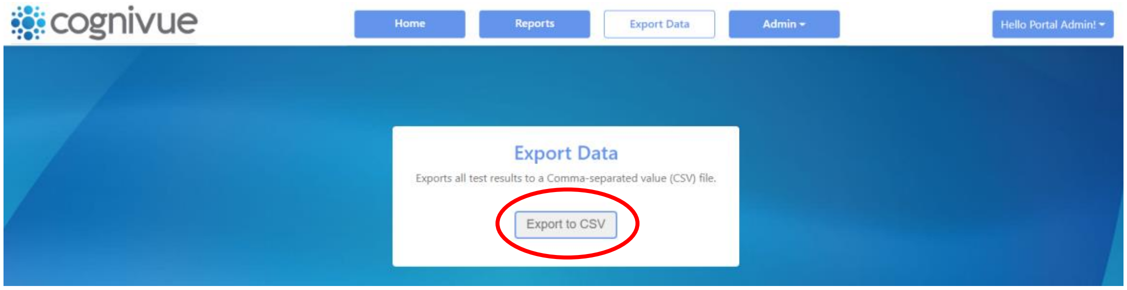
5.3 Downloading Test Data

An Administrator Account can export all of their patient test data. Click on the Export Data option on the navigation bar, to go to the Export Data page.



Home Page

On the Export Data page, click on the 'Export to CSV' button. This will download all patient test results for the administrator's account, into a .zip file containing the patient test results in a .csv file. If there are test results for both Clarity and Thrive devices on the Administrator's account, then there will be one .csv file for any Clarity test results, and one .csv file for any Thrive test results.

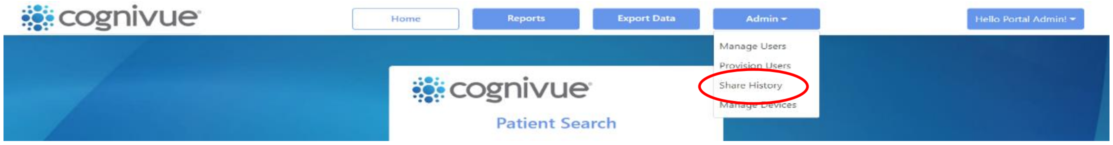


Exports all test results to a Comma-separated value (CSV) file.

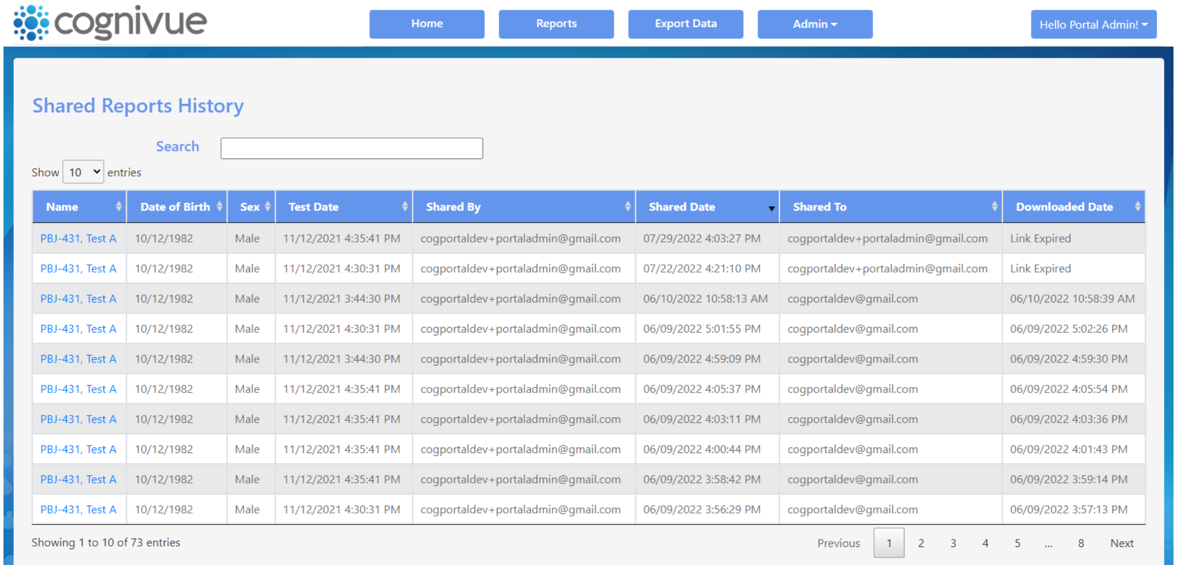
Export Data Page

5.4 History of Shared Reports

An Administrator Account is able to view the history of shared reports for their patients and devices. To navigate there, click on the Admin drop-down menu and select the Share History option.



Admin Menu – Share History



Shared Reports History

Search

Show 10 entries

Name	Date of Birth	Sex	Test Date	Shared By	Shared Date	Shared To	Downloaded Date
PBJ-431, Test A	10/12/1982	Male	11/12/2021 4:35:41 PM	cogportaldev+portaladmin@gmail.com	07/29/2022 4:03:27 PM	cogportaldev+portaladmin@gmail.com	Link Expired
PBJ-431, Test A	10/12/1982	Male	11/12/2021 4:30:31 PM	cogportaldev+portaladmin@gmail.com	07/22/2022 4:21:10 PM	cogportaldev+portaladmin@gmail.com	Link Expired
PBJ-431, Test A	10/12/1982	Male	11/12/2021 3:44:30 PM	cogportaldev+portaladmin@gmail.com	06/10/2022 10:58:13 AM	cogportaldev@gmail.com	06/10/2022 10:58:39 AM
PBJ-431, Test A	10/12/1982	Male	11/12/2021 4:30:31 PM	cogportaldev+portaladmin@gmail.com	06/09/2022 5:01:55 PM	cogportaldev@gmail.com	06/09/2022 5:02:26 PM
PBJ-431, Test A	10/12/1982	Male	11/12/2021 3:44:30 PM	cogportaldev+portaladmin@gmail.com	06/09/2022 4:59:09 PM	cogportaldev@gmail.com	06/09/2022 4:59:30 PM
PBJ-431, Test A	10/12/1982	Male	11/12/2021 4:35:41 PM	cogportaldev+portaladmin@gmail.com	06/09/2022 4:05:37 PM	cogportaldev@gmail.com	06/09/2022 4:05:54 PM
PBJ-431, Test A	10/12/1982	Male	11/12/2021 4:35:41 PM	cogportaldev+portaladmin@gmail.com	06/09/2022 4:03:11 PM	cogportaldev@gmail.com	06/09/2022 4:03:36 PM
PBJ-431, Test A	10/12/1982	Male	11/12/2021 4:35:41 PM	cogportaldev+portaladmin@gmail.com	06/09/2022 4:00:44 PM	cogportaldev@gmail.com	06/09/2022 4:01:43 PM
PBJ-431, Test A	10/12/1982	Male	11/12/2021 4:35:41 PM	cogportaldev+portaladmin@gmail.com	06/09/2022 3:58:42 PM	cogportaldev@gmail.com	06/09/2022 3:59:14 PM
PBJ-431, Test A	10/12/1982	Male	11/12/2021 4:30:31 PM	cogportaldev+portaladmin@gmail.com	06/09/2022 3:56:29 PM	cogportaldev@gmail.com	06/09/2022 3:57:13 PM

Showing 1 to 10 of 73 entries

Previous 1 2 3 4 5 ... 8 Next

Share History Page

The Administrator Account is able to navigate to the patient dashboard by clicking on the patient's name.

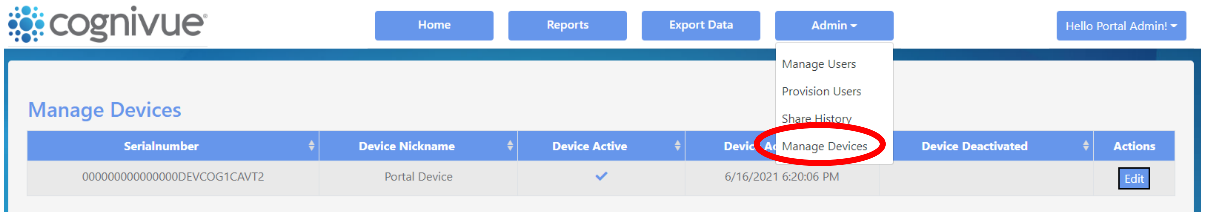
As with the report page, the Account may select to show 10, 25, 50, or 100 records per page, and may navigate between the pages of the table by using the buttons below the table.

The 'Downloaded Date' column reflects the state of the shared report link. If a Portal Account has shared a report multiple times, there will be one entry on this table for each time that report has been shared. If the Downloaded Date is empty, then the shared report has not been downloaded and the link is still valid for use. If 'Link Expired' appears, then the shared report was not downloaded and the link has expired. When the shared report is downloaded a timestamp will appear in this field.

6.0 Devices Page

6.1 Accessing the Devices Page

The User is able to review their devices by accessing the devices page. The User may access the Page by clicking on the Admin button and selecting 'Manage Devices' from the list. This will bring the User to the Devices Page.

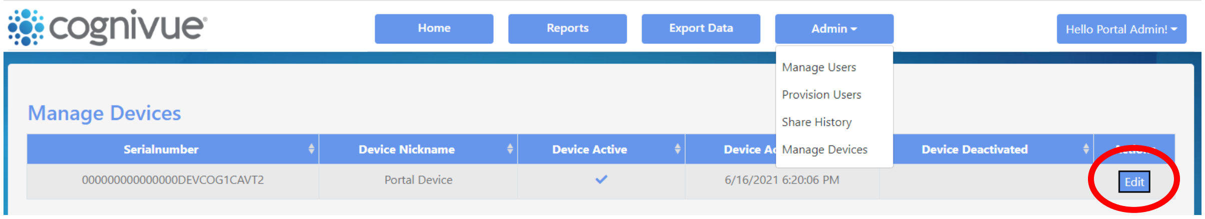


Serialnumber	Device Nickname	Device Active	Devic Ac	Device Deactivated	Actions
000000000000000DEVCOG1CAVT2	Portal Device	✓	6/16/2021 6:20:06 PM		Edit

Manage Devices Button

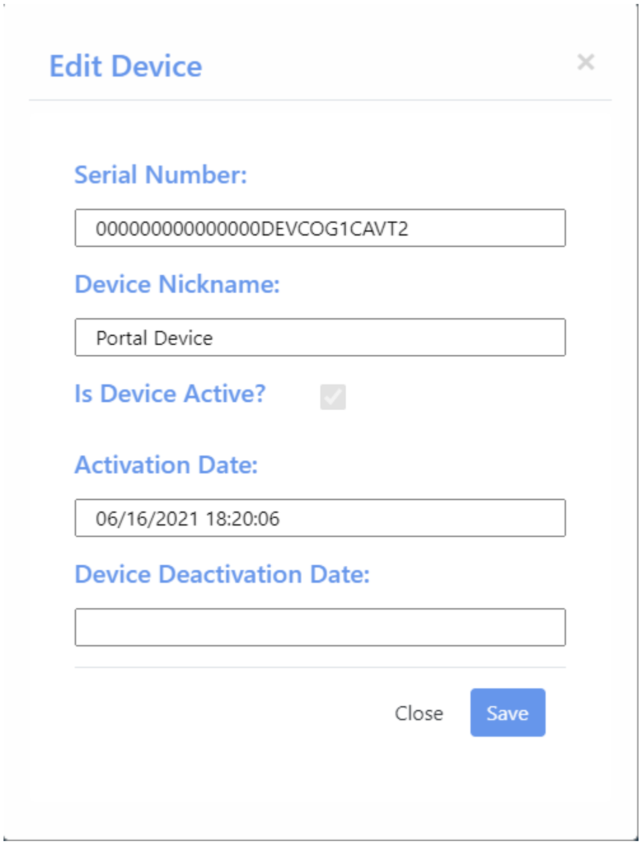
6.1.1 Adding a Nickname to a Device

The User can add or change the portal nickname for a device by selecting the Edit button in the Actions column, for the device. This will open a window with the device information and a field to add or change the nickname.



Serialnumber	Device Nickname	Device Active	Device Ac	Device Deactivated	
000000000000000DEVCOG1CAVT2	Portal Device	✓	6/16/2021 6:20:06 PM		Edit

Edit Button



Edit Device

Serial Number:

000000000000000DEVCOG1CAVT2

Device Nickname:

Portal Device

Is Device Active? ☑

Activation Date:

06/16/2021 18:20:06

Device Deactivation Date:

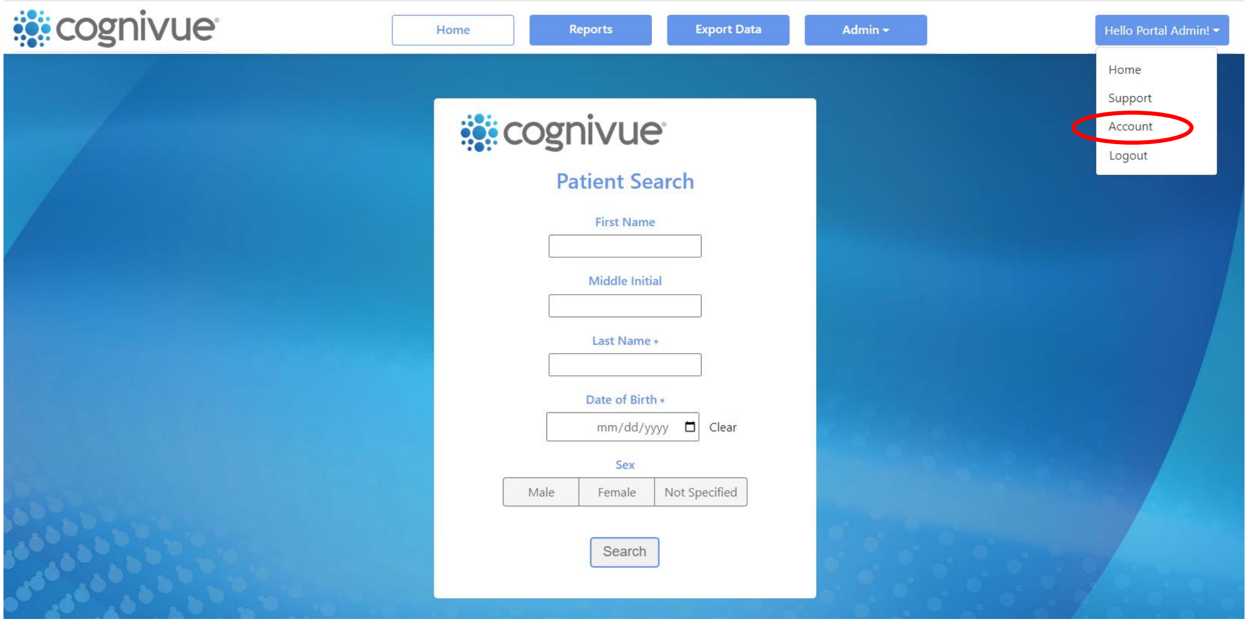
Edit Device Modal

Fill in the Device Nickname field and click the Save button, to add or change the portal nickname assigned to the device.

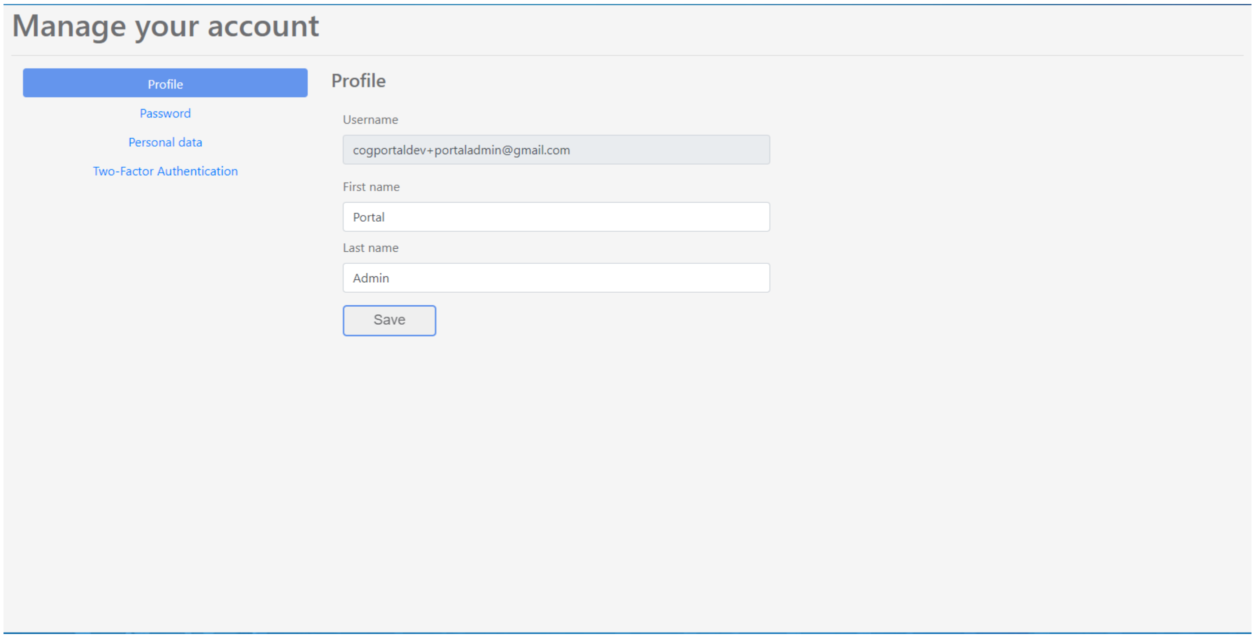
7.0 Account Management

7.1 Accessing the Account Management Page

The User is able to manage various aspects of their account by accessing the account management page. The User may access the page by clicking on the button in the top right of any page, which says ‘Hello’ followed by their username, and select ‘Account. This will bring the User to the Account Management page.



Account Management Button



Profile

Username: cogportaldev+portaladmin@gmail.com

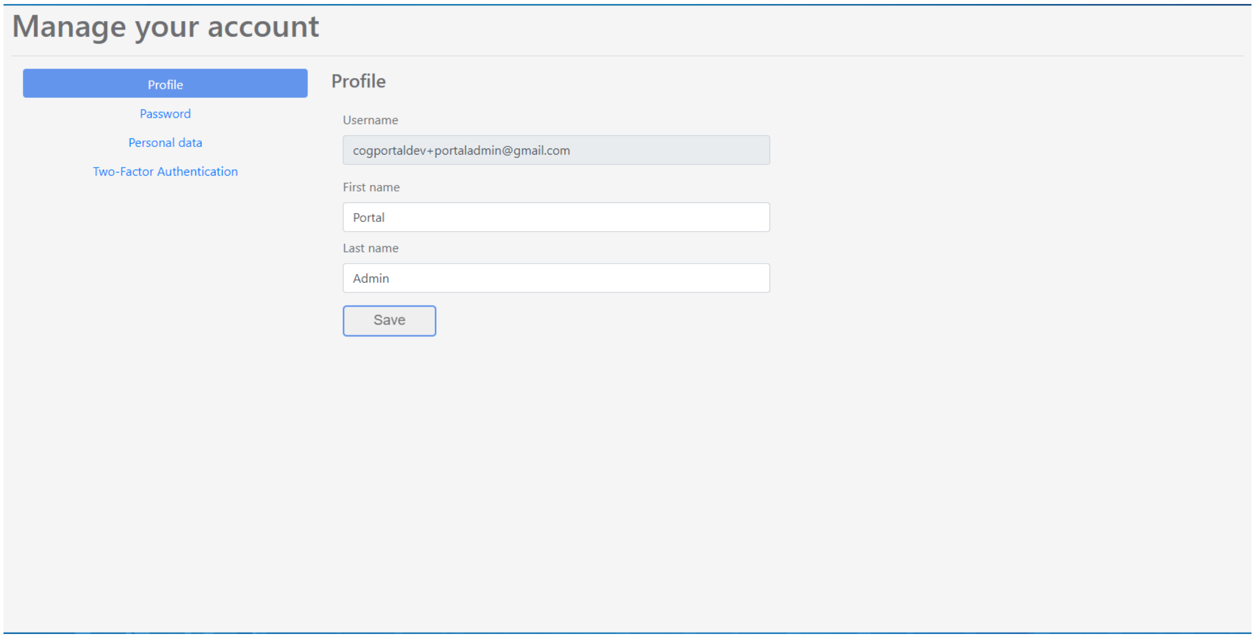
First name: Portal

Last name: Admin

Account Management Page

7.2 Profile Page

On this page the User is able to change their first name and/or last name. To do so, edit the contents of either field and click the Save button.



Manage your account

Profile

Username: cogportaldev+portaladmin@gmail.com

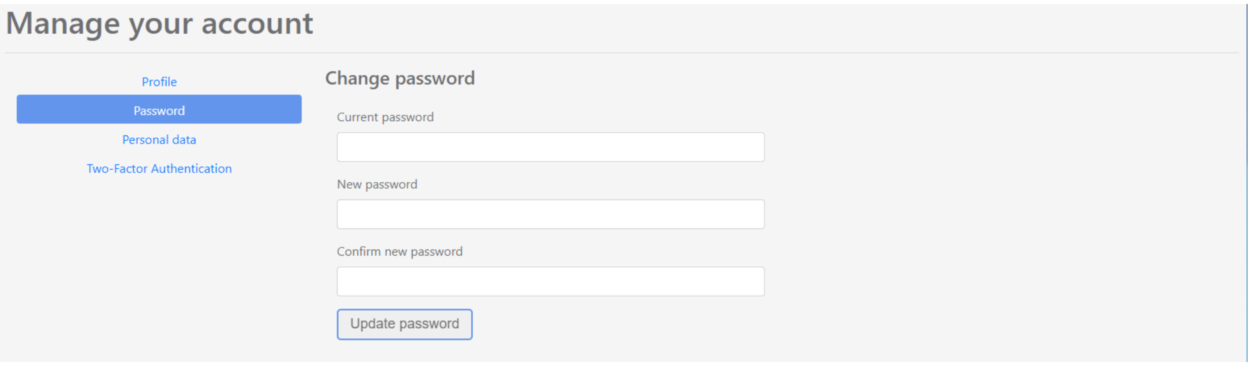
First name: Portal

Last name: Admin

Profile Page

7.3 Password Page

On this page the User is able to change their password for logging into the portal. To do so, enter the current password in the first field, and the new password in the second and third fields. Passwords must contain at least 1 uppercase letter, 1 lowercase letter, 1 number, and 1 special character, and must be a minimum of 8 characters.



Manage your account

Change password

Current password

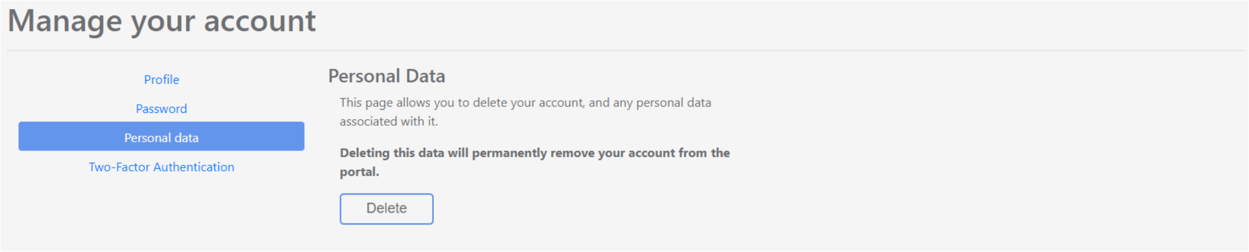
New password

Confirm new password

Password Page

7.4 Personal Data Page

On this page the User is able to delete their portal user account and associated data. The deleted data includes the phone number and email associated with the User account.



Manage your account

Personal Data

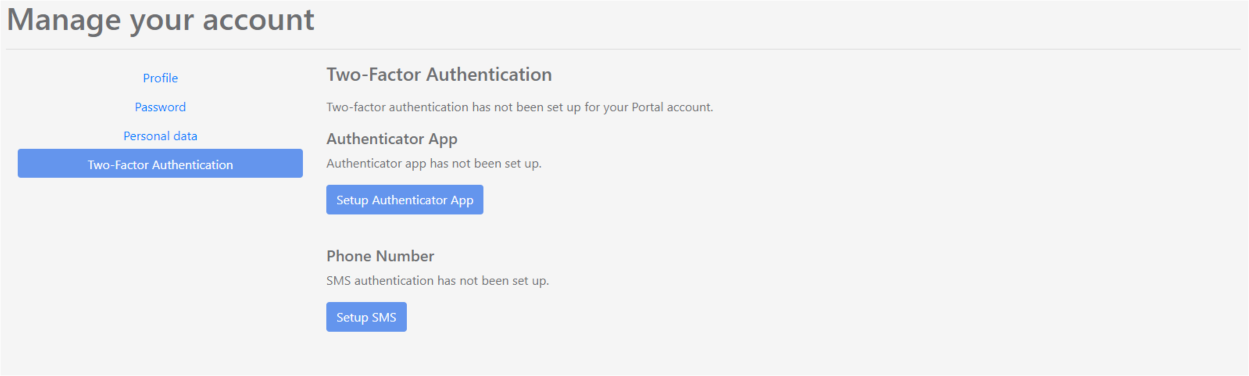
This page allows you to delete your account, and any personal data associated with it.

Deleting this data will permanently remove your account from the portal.

Personal Data Page

7.5 Two-Factor Authentication

In order to provide better security for Users, a User is able to set up two-factor authentication with an authenticator app and/or a phone number where they can receive verification codes through texts.



Manage your account

Two-Factor Authentication

Two-factor authentication has not been set up for your Portal account.

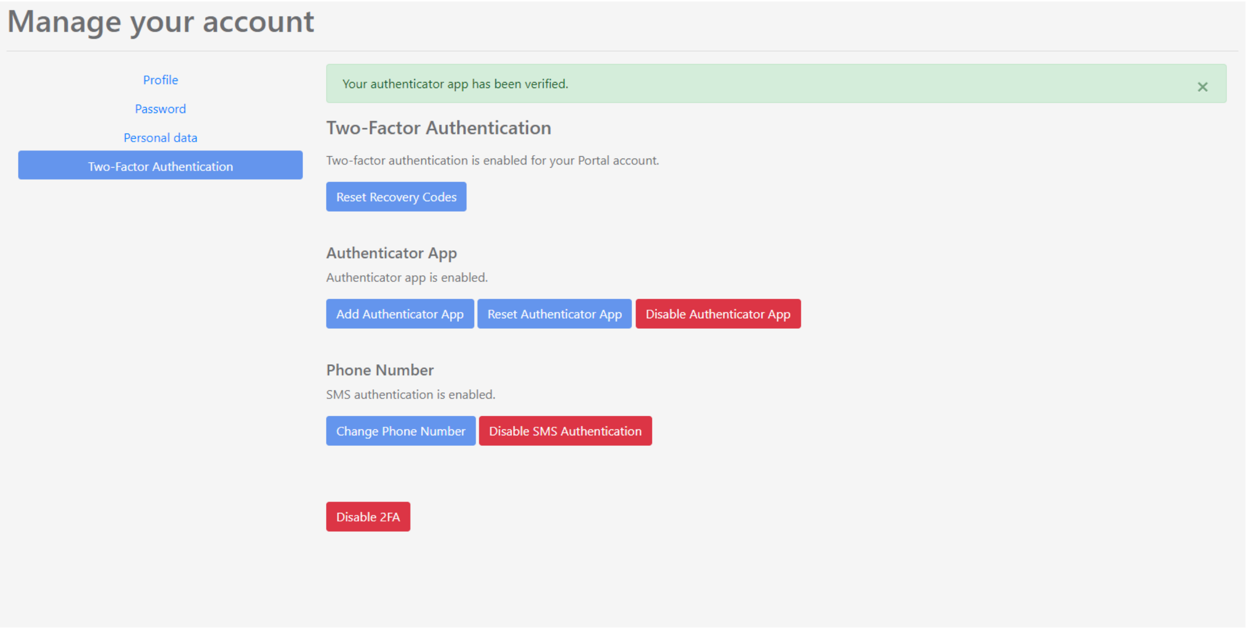
Authenticator App

Authenticator app has not been set up.

Phone Number

SMS authentication has not been set up.

Two-Factor Authentication Page with no 2FA set up



Your authenticator app has been verified.

Two-Factor Authentication

Two-factor authentication is enabled for your Portal account.

Authenticator App

Authenticator app is enabled.

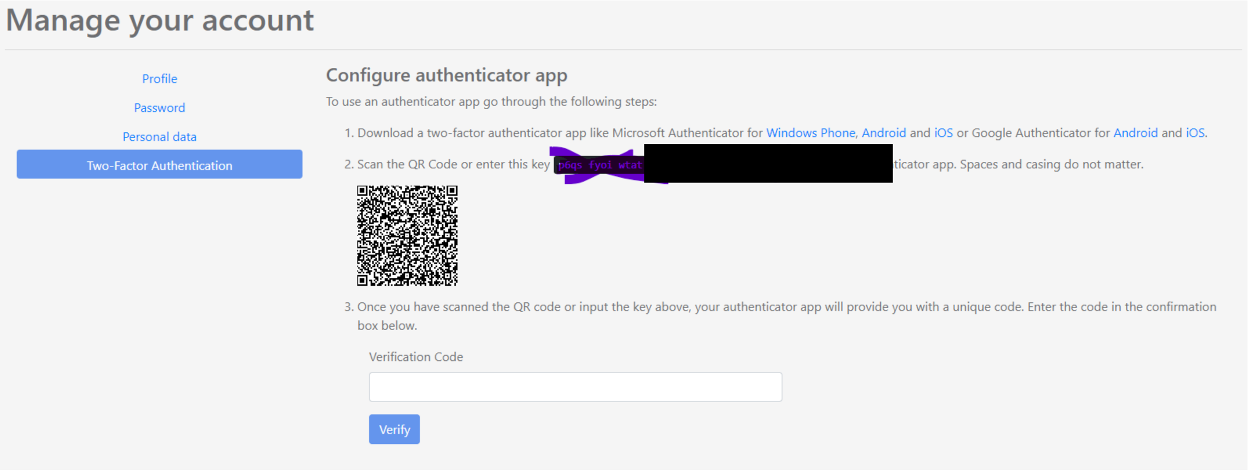
Phone Number

SMS authentication is enabled.

Two-Factor Authentication with multiple methods configured

7.5.1 Setup Authenticator App

If you select the Setup Authenticator App button, you can connect an authenticator app that you have, to your user account. Follow the instructions of the authenticator app that you have installed, and the on-screen instructions on this page, to connect your authenticator app with your user account.



Configure authenticator app

To use an authenticator app go through the following steps:

1. Download a two-factor authenticator app like Microsoft Authenticator for Windows Phone, Android and iOS or Google Authenticator for Android and iOS.
2. Scan the QR Code or enter this key [redacted]ticator app. Spaces and casing do not matter.
3. Once you have scanned the QR code or input the key above, your authenticator app will provide you with a unique code. Enter the code in the confirmation box below.

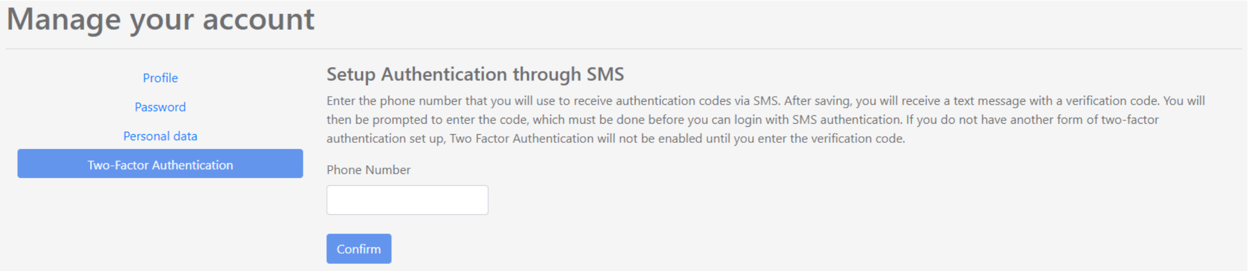
Verification Code

Setup Authenticator App

After connecting to your authenticator app, enter the verification code into the field and click the 'Verify' button, to complete the setup for the User account.

7.5.2 Setup SMS (texting)

If the User selects the Setup SMS button, they can configure a phone number to receive codes via SMS (Texting.) Follow the on-screen instructions to complete the configuration. Only one phone number may be configured for SMS for the User account.



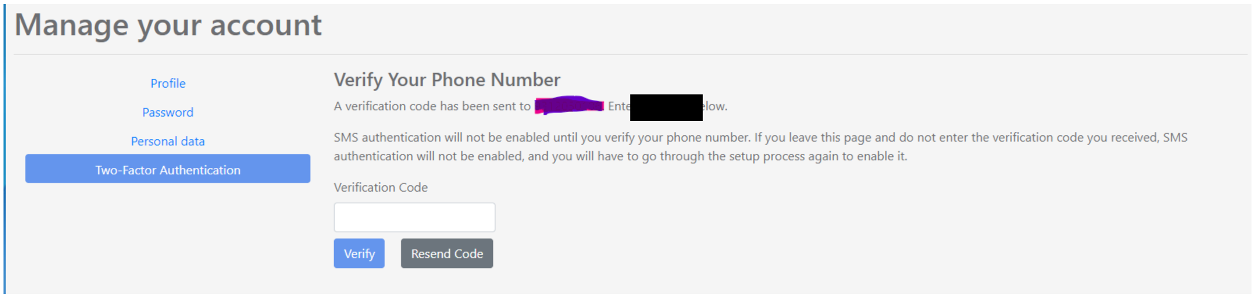
Manage your account

Setup Authentication through SMS

Enter the phone number that you will use to receive authentication codes via SMS. After saving, you will receive a text message with a verification code. You will then be prompted to enter the code, which must be done before you can login with SMS authentication. If you do not have another form of two-factor authentication set up, Two Factor Authentication will not be enabled until you enter the verification code.

Phone Number

Setup SMS Page



Manage your account

Verify Your Phone Number

A verification code has been sent to [redacted] Ente[redacted]low.

SMS authentication will not be enabled until you verify your phone number. If you leave this page and do not enter the verification code you received, SMS authentication will not be enabled, and you will have to go through the setup process again to enable it.

Verification Code

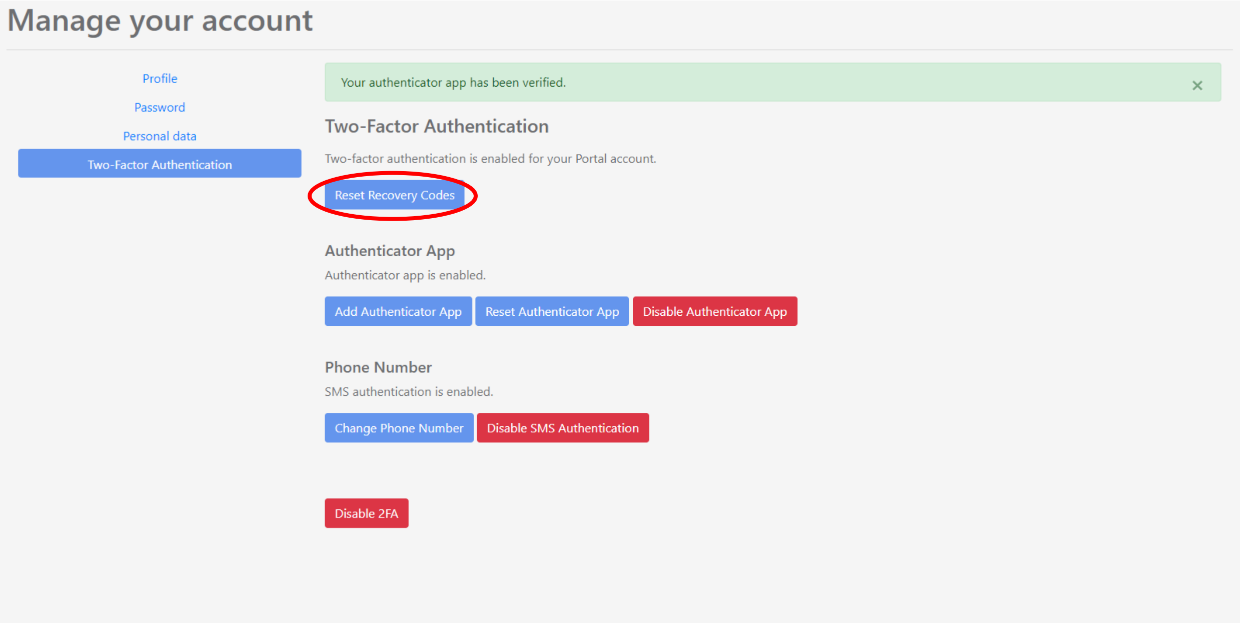
Verify Phone Number Page

7.5.3 Recovery Codes

Recovery codes are single-use codes that can be used to verify the User account. These are intended to be used in the event that the User does not have access to the authentication method(s) that have been configured for their User account. For example, the User does not have their mobile device with the authenticator app, available.

When the User initially configures either the authenticator app or SMS, for two-factor authentication, 10 recovery codes will be automatically generated and displayed to the screen. The User will be unable to retrieve these codes once they leave that page.

The User can manually generate recovery codes by clicking on the Reset Recovery Codes button. This will take the User to the Generate Recovery Codes page. Follow the on-screen instructions to generate 10 recovery codes and display them to the screen. The User will be unable to retrieve them once they leave the page.



Your authenticator app has been verified.

Two-Factor Authentication

Two-factor authentication is enabled for your Portal account.

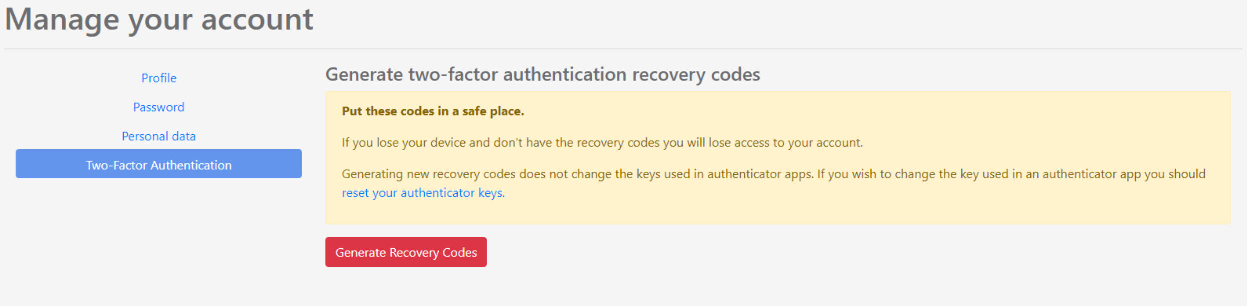
Authenticator App

Authenticator app is enabled.

Phone Number

SMS authentication is enabled.

Two-factor Authentication Page; Reset Recovery Codes button



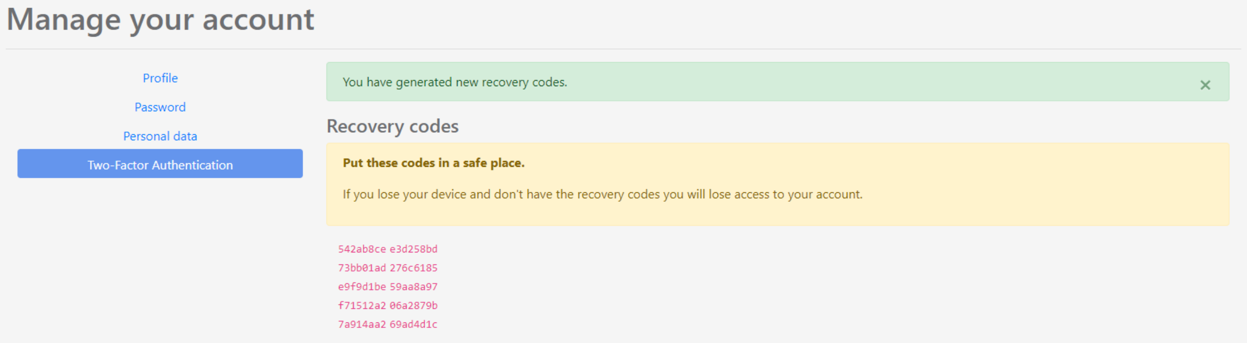
Generate two-factor authentication recovery codes

Put these codes in a safe place.

If you lose your device and don't have the recovery codes you will lose access to your account.

Generating new recovery codes does not change the keys used in authenticator apps. If you wish to change the key used in an authenticator app you should reset your authenticator keys.

Generate Recovery Codes Page



You have generated new recovery codes.

Recovery codes

Put these codes in a safe place.

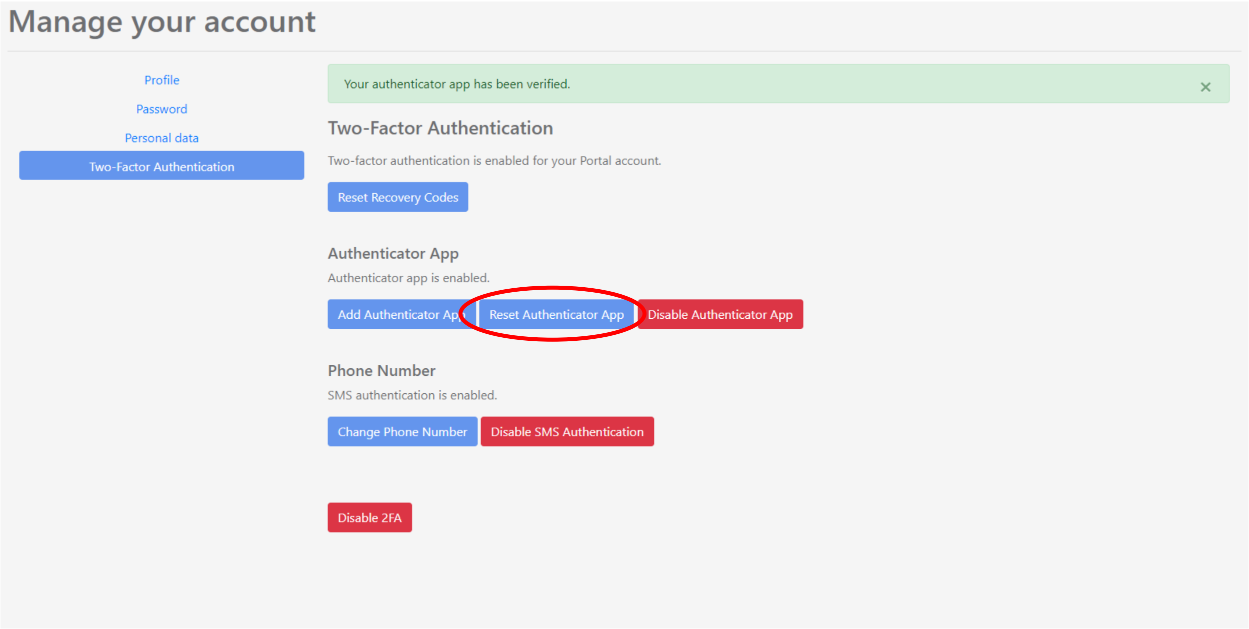
If you lose your device and don't have the recovery codes you will lose access to your account.

```
542ab8ce e3d258bd
73bb01ad 276c6185
e9f9d1be 59aa8a97
f71512a2 06a2879b
7a914aa2 69ad4d1c
```

Recovery Codes Page

7.5.4 Resetting Authenticator App

The User can reset the authenticator app to disconnect it and allow them to connect to a different authenticator app. To reset the authenticator app security on their User account, the User must click on the Reset Authenticator App button.



Manage your account

Your authenticator app has been verified. ×

Two-Factor Authentication

Two-factor authentication is enabled for your Portal account.

Authenticator App

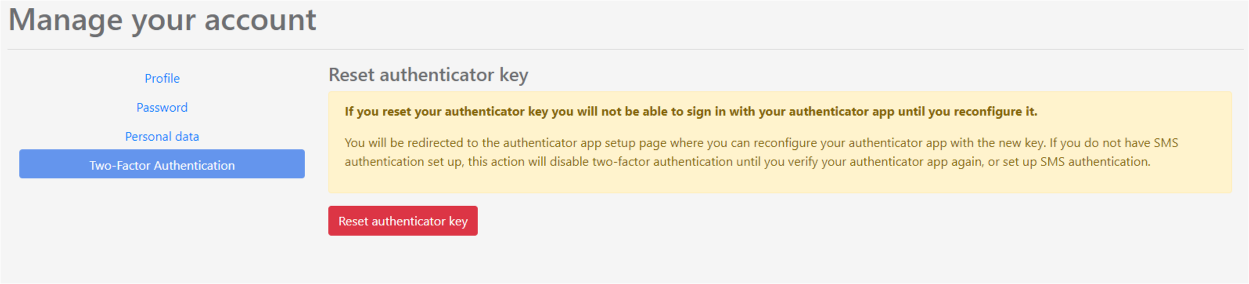
Authenticator app is enabled.

Phone Number

SMS authentication is enabled.

Two-Factor Authentication Page; Reset Authenticator App button

Follow the instructions on the Reset Authenticator App page, in order to reset the authenticator app for the User account.



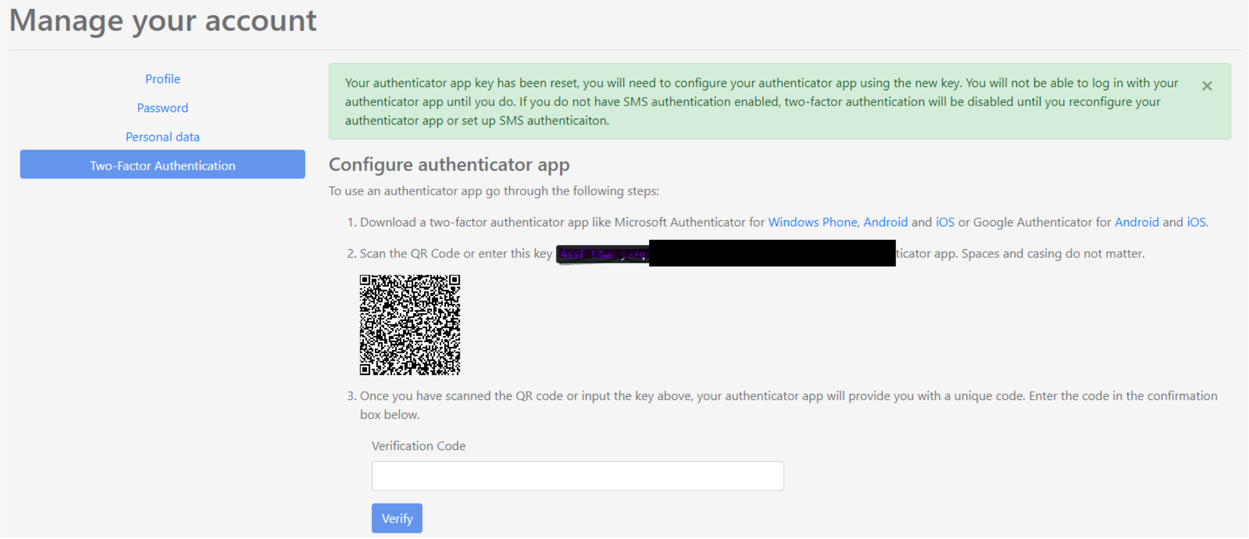
Manage your account

Reset authenticator key

If you reset your authenticator key you will not be able to sign in with your authenticator app until you reconfigure it.

You will be redirected to the authenticator app setup page where you can reconfigure your authenticator app with the new key. If you do not have SMS authentication set up, this action will disable two-factor authentication until you verify your authenticator app again, or set up SMS authentication.

Reset Authenticator App Page



Manage your account

Your authenticator app key has been reset, you will need to configure your authenticator app using the new key. You will not be able to log in with your authenticator app until you do. If you do not have SMS authentication enabled, two-factor authentication will be disabled until you reconfigure your authenticator app or set up SMS authenticaiton. ×

Configure authenticator app

To use an authenticator app go through the following steps:

1. Download a two-factor authenticator app like Microsoft Authenticator for Windows Phone, Android and iOS or Google Authenticator for Android and iOS.
2. Scan the QR Code or enter this key [redacted]ticator app. Spaces and casing do not matter.
3. Once you have scanned the QR code or input the key above, your authenticator app will provide you with a unique code. Enter the code in the confirmation box below.

Verification Code

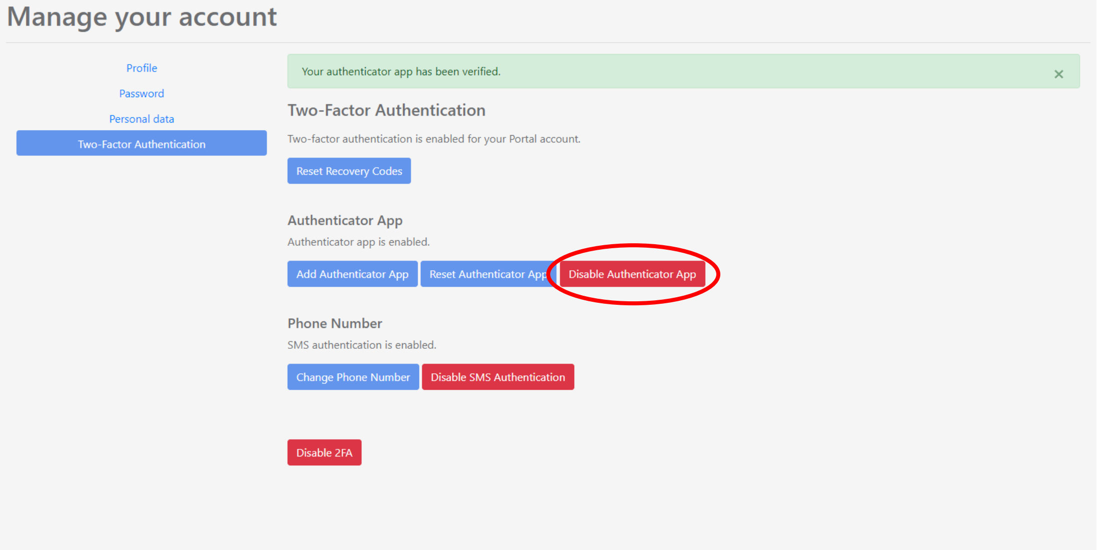
Setup Authenticator App Page after resetting the authenticator app

7.5.5 Disabling Two-Factor Authentication

The User may disable two-factor authentication on their account, either for a specific method, or completely. It is recommended that the User maintain at least one configured method for two-factor authentication.

7.5.5.1 Disabling Authenticator App 2FA

To disable two-factor authentication for the authenticator app only, click on the Disable Authenticator App Authentication button.



Your authenticator app has been verified.

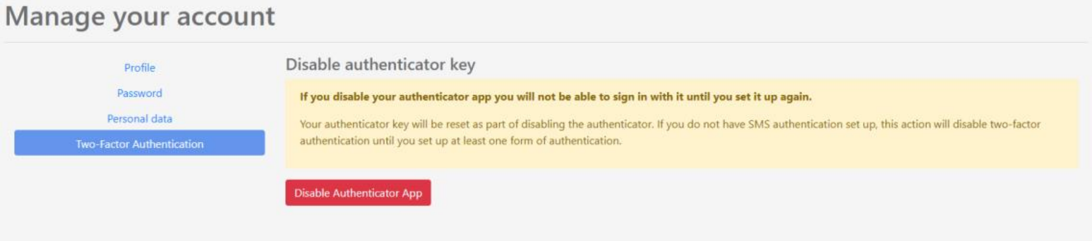
Two-factor authentication is enabled for your Portal account.

Authenticator app is enabled.

SMS authentication is enabled.

Two-Factor Authentication Page; Disable Authenticator App button

Follow the on-screen instructions to disable the authenticator app for the User.


Manage your account
Profile
Password
Personal data
Two-Factor Authentication
Disable authenticator key
Disable Authenticator App

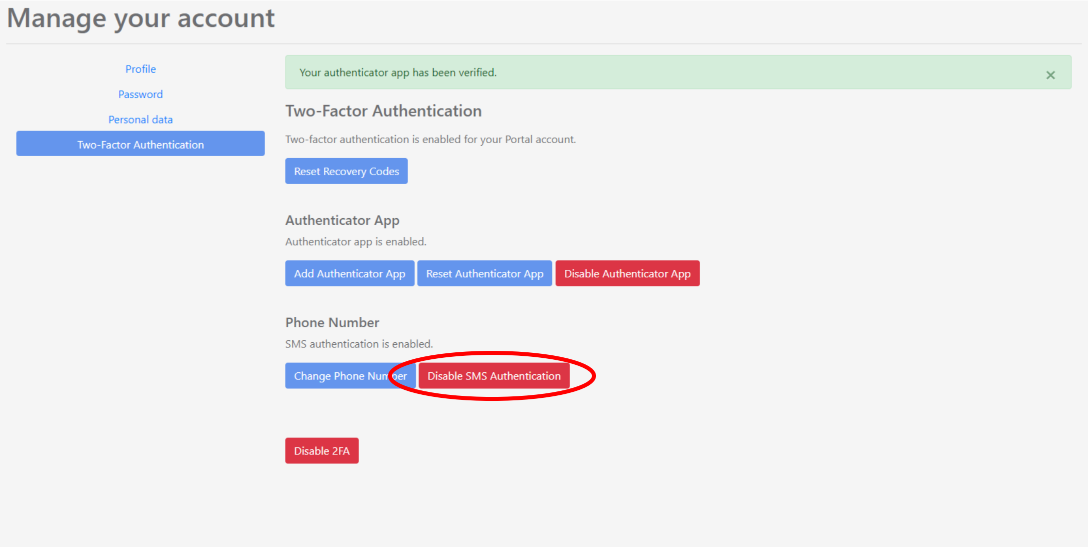
If you disable your authenticator app you will not be able to sign in with it until you set it up again.

Your authenticator key will be reset as part of disabling the authenticator. If you do not have SMS authentication set up, this action will disable two-factor authentication until you set up at least one form of authentication.

Disable Authenticator App Page

7.5.5.2 Disable SMS 2FA

To disable two-factor authentication for SMS only, click on the Disable SMS Authentication button.


Manage your account

Your authenticator app has been verified.

Two-Factor Authentication

Two-factor authentication is enabled for your Portal account.

Authenticator App

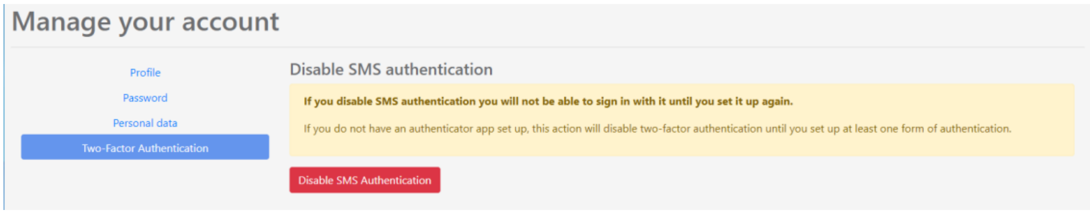
Authenticator app is enabled.

Phone Number

SMS authentication is enabled.

Two-Factor Authentication Page; Disable SMS Authentication button

Follow the on-screen instructions to disable SMS authentication for the User.


Manage your account

Disable SMS authentication

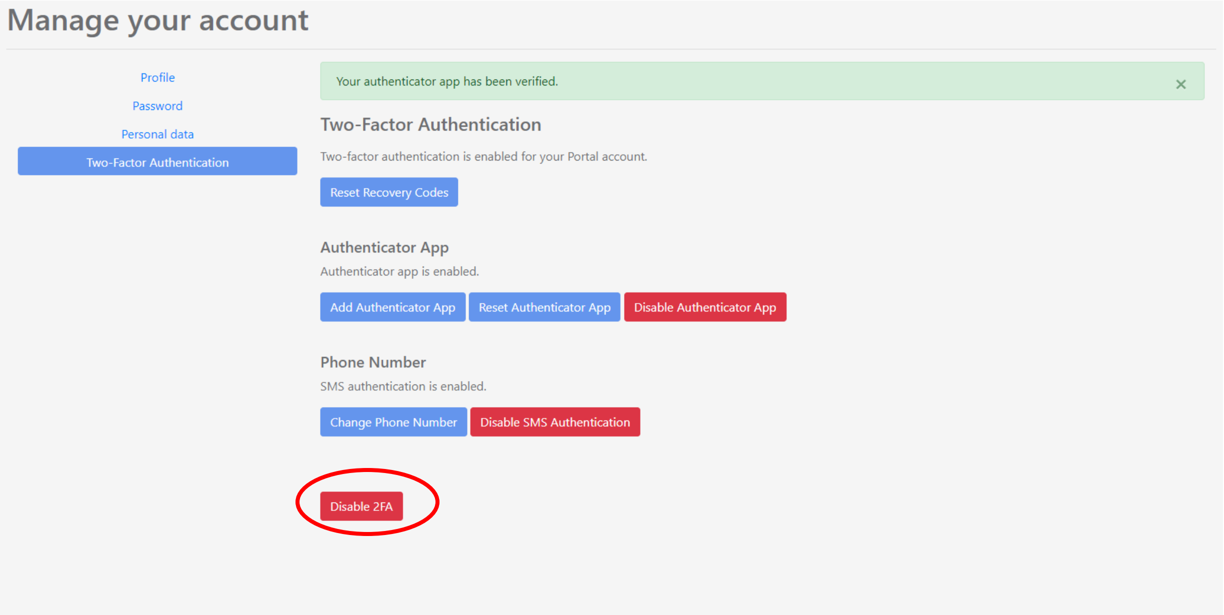
If you disable SMS authentication you will not be able to sign in with it until you set it up again.

If you do not have an authenticator app set up, this action will disable two-factor authentication until you set up at least one form of authentication.

Disable SMS Authentication Page

7.5.5.3 Disable Two-Factor Authentication

To disable all two-factor authentication for their user account, click the Disable 2FA Button. **It is recommended that a User have at least one method of authentication configured for their account.**



Manage your account

Your authenticator app has been verified. ×

Two-Factor Authentication

Two-factor authentication is enabled for your Portal account.

Authenticator App

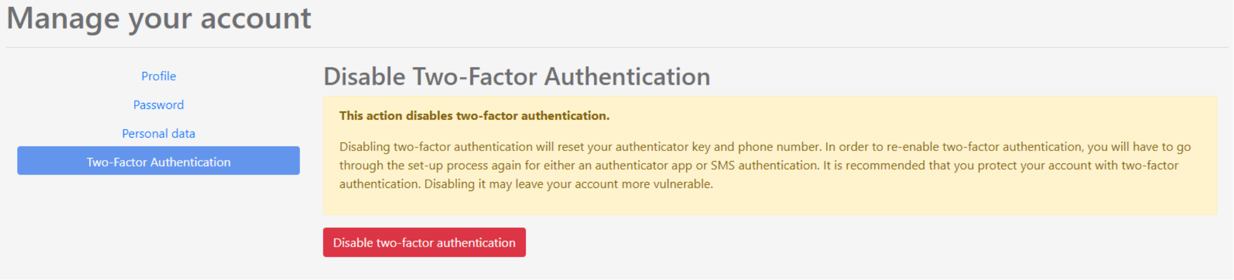
Authenticator app is enabled.

Phone Number

SMS authentication is enabled.

Two-Factor Authentication Page; Disable 2FA button

Follow the on-screen instructions to disable two-factor authentication for all methods, on the User account.



Manage your account

Disable Two-Factor Authentication

This action disables two-factor authentication.

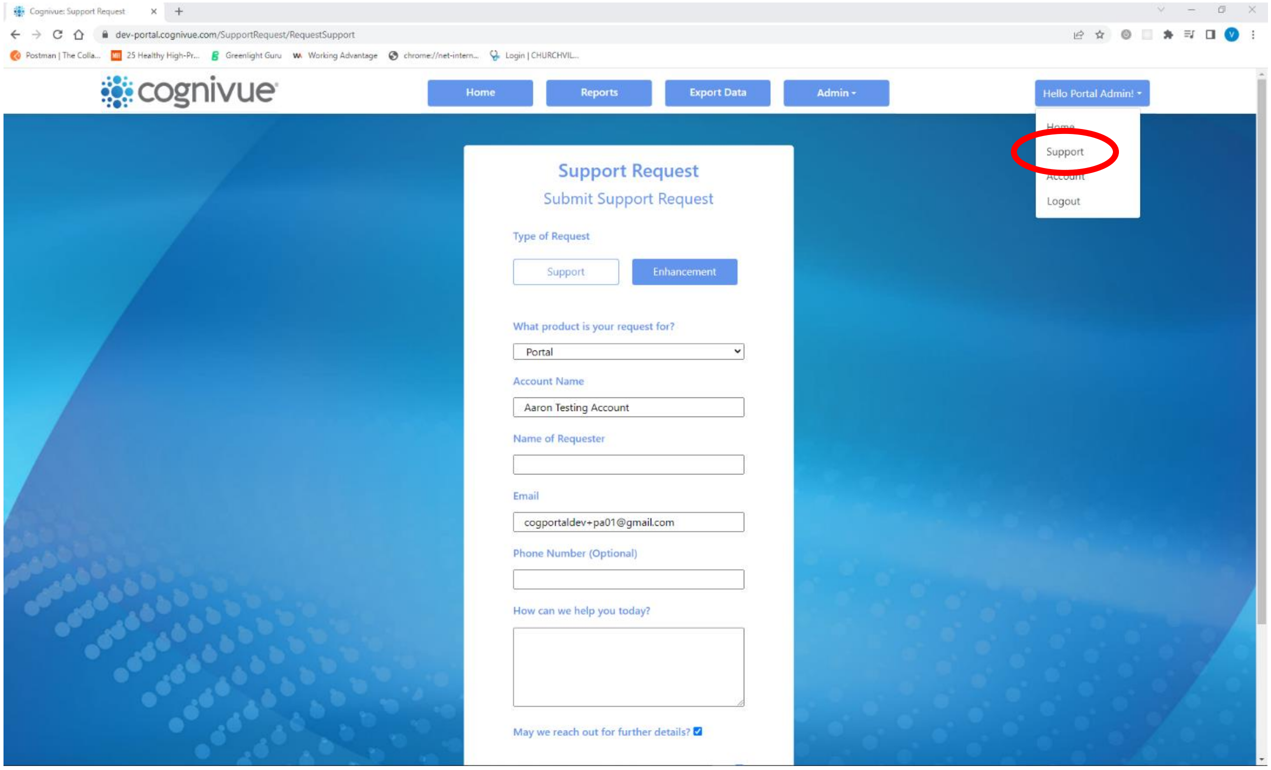
Disabling two-factor authentication will reset your authenticator key and phone number. In order to re-enable two-factor authentication, you will have to go through the set-up process again for either an authenticator app or SMS authentication. It is recommended that you protect your account with two-factor authentication. Disabling it may leave your account more vulnerable.

Disable 2FA Page

8.0 Portal Support

8.1 Accessing the Portal Support Page

The User is able to submit requests related to the Portal to Cognivue. The User can submit requests for portal support, and submit requests for enhancements to the portal. The User may access the page by clicking on the button in the top right of any page, which says 'Hello' followed by their username, and select 'Support'. This will bring the User to the Portal Support page.



Support Request

Submit Support Request

Type of Request

What product is your request for?

Portal

Account Name

Aaron Testing Account

Name of Requester

Email

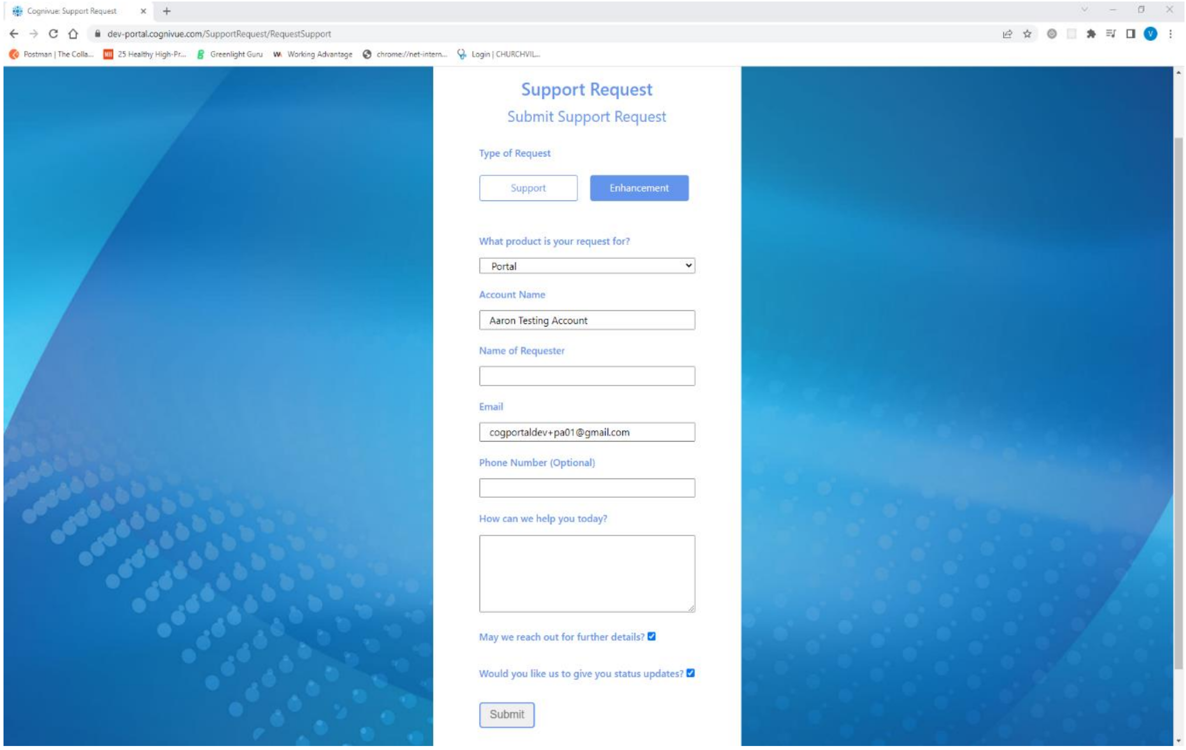
cogportaldev+pa01@gmail.com

Phone Number (Optional)

How can we help you today?

May we reach out for further details? ☑

Support Button



Support Request

Submit Support Request

Type of Request

Support | Enhancement

What product is your request for?

Portal

Account Name

Aaron Testing Account

Name of Requester

Email

cogportaldev+pa01@gmail.com

Phone Number (Optional)

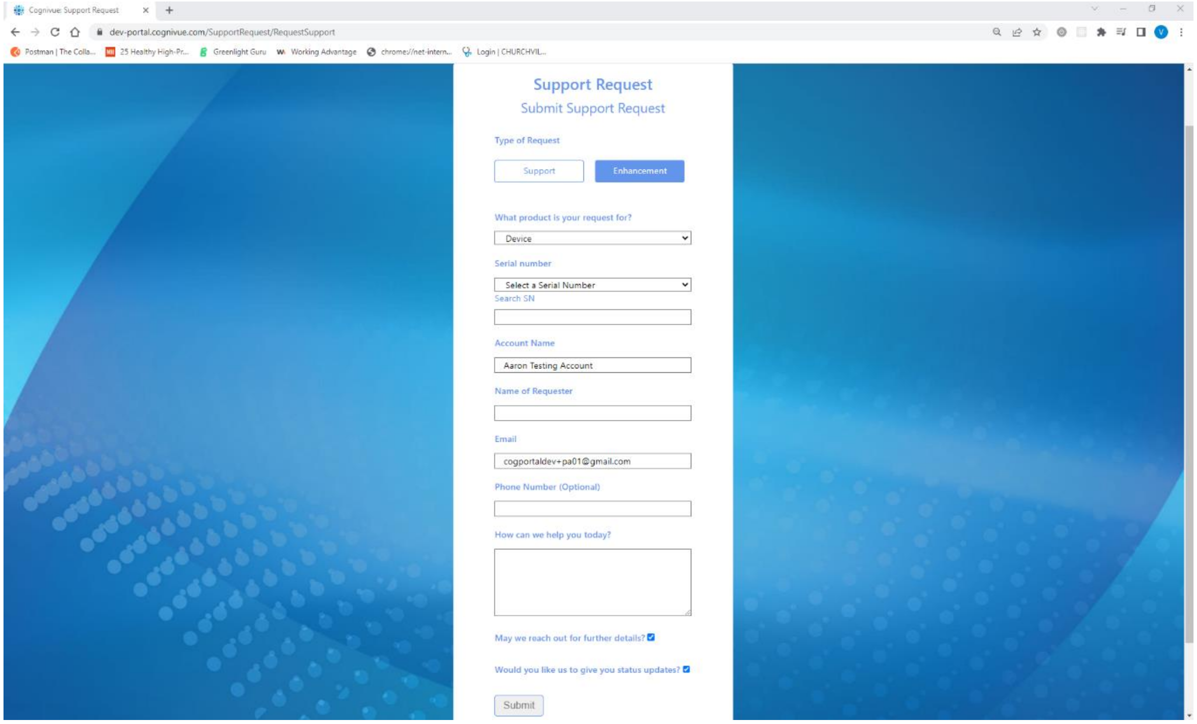
How can we help you today?

May we reach out for further details? ☑

Would you like us to give you status updates? ☑

Submit

Support Request Form



Support Request

Submit Support Request

Type of Request

Support | Enhancement

What product is your request for?

Device

Serial number

Select a Serial Number

Search SN

Account Name

Aaron Testing Account

Name of Requester

Email

cogportaldev+pa01@gmail.com

Phone Number (Optional)

How can we help you today?

May we reach out for further details? ☑

Would you like us to give you status updates? ☑

Submit

Support Request Form – Device Requests

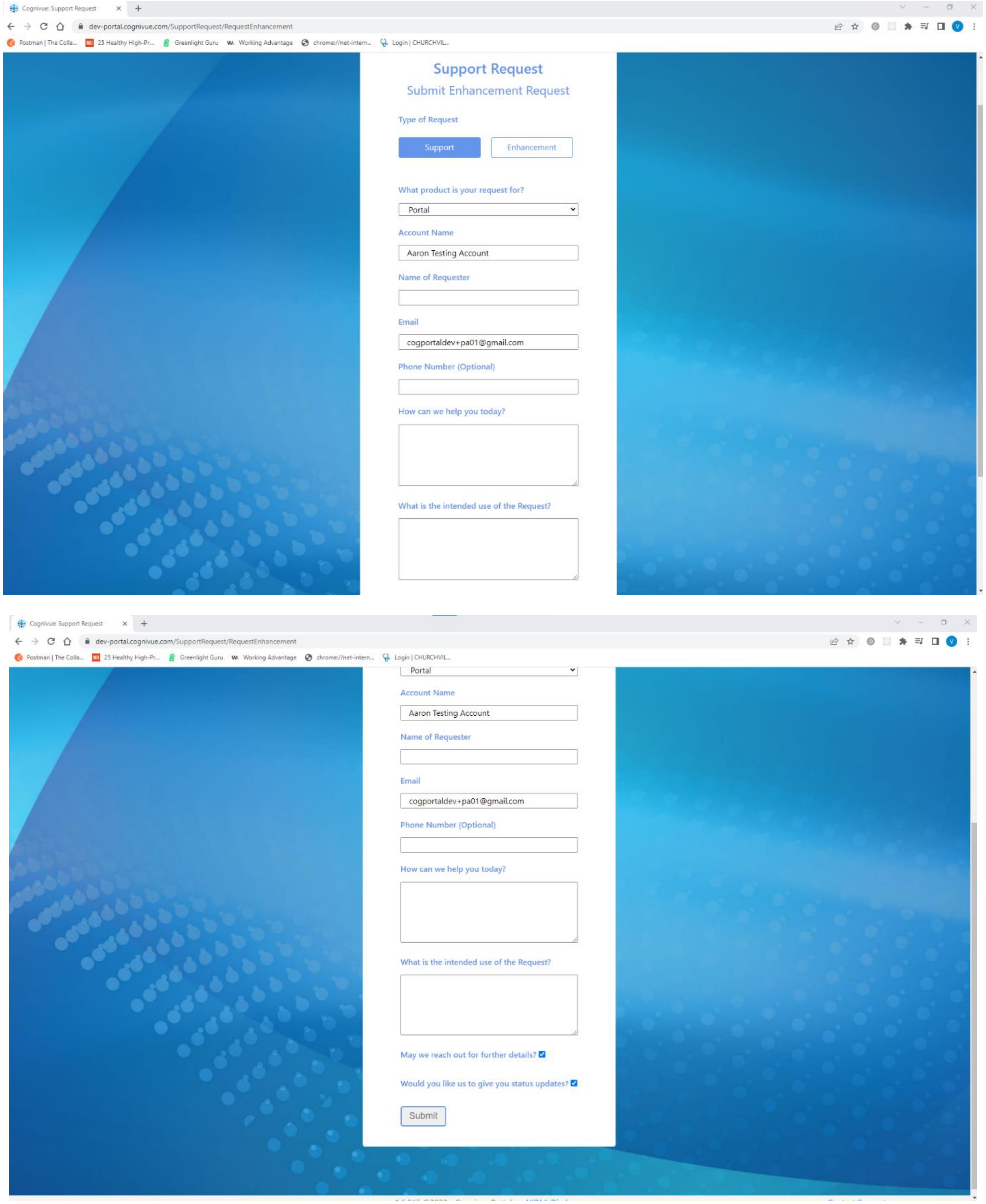
8.2 Submit a Request

The User can toggle between Support and Enhancement requests by clicking on the buttons labeled 'Support' and 'Enhancement' on the Support page.

8.2.1 Support Request

The User can submit requests for portal support on the Submit Support Request page.

- *What product is your request for?* The User making the request should select from the dropdown menu whether their request is for the portal, a device, or some other unclassified Cognivue service or product.
- *Serial Number (for Device Support Requests Only):* The User selects the serial number of the device that they are submitting the request for. This field only appears when the User selects the Device option on the Support Page.
- *Search SN:* The User may type into this field to search for a specific device serialnumber. The serial number dropdown menu will try and select the serialnumber that best matches the current value of the field, as the User types.
- *Account Name:* The name of the User's account that their devices are classified under.
- *Name of Requester*: The User making the request should enter their name here
- *Email*: The User making the request should enter the email address where they would like any correspondence sent to; a copy of the support request will be sent to this email address. This field will be initially populated with the email of the Portal User that is logged in.
- *Phone Number*: The User may optionally include a phone numbrer that they may be contacted at.
- *How can we help you today*?: This is where the User should enter what portal issue they are experiencing including details on what happened, what was going on at the time, and any actions performed.
- *May we reach out for further details*?: The User should check this box if they would like Cognivue Support to reach out to them for further information and clarification.
- *Would you like us to give you status updates*?: The User should check this box if they would like Cognivue Support to provide them with updates on the status of their Support Request.



dev-portal.cognivue.com/SupportRequest/RequestEnhancement

Support Request

Submit Enhancement Request

Type of Request

What product is your request for?

Portal

Account Name

Aaron Testing Account

Name of Requester

Email

cogportaldev+pa01@gmail.com

Phone Number (Optional)

How can we help you today?

What is the intended use of the Request?

May we reach out for further details? ☑

Would you like us to give you status updates? ☑

Enhancement Request Form

8.2.2 Enhancement Request

The User can submit requests for portal enhancements on the Submit Enhancement Request page.

- *What product is your request for?* The User making the request should select from the dropdown menu whether their request is for the portal, a device, or some other unclassified Cognivue service or product.
- *Account Name:* The name of the User's account that their devices are classified under.
- *Name of Requester*: The User making the request should enter their name here
- *Email*: The User making the request should enter the email address where they would like any correspondence sent to; a copy of the support request will be sent to this email address. This field will be initially populated with the email of the Portal User that is logged in.
- *Phone Number*: The User may optionally include a phone numbrer that they may be contacted at.
- *How can we help you today*?: This is where the User should enter what they would like to see changed or added in the portal.
- *What is the intended use of the Request*?: This is where the User should describe what the request is intended for. The User should provide examples and scenarios for application.
- *May we reach out for further details*?: The User should check this box if they would like Cognivue Support to reach out to them for further information and clarification.
- *Would you like us to give you status updates*?: The User should check this box if they would like Cognivue Support to provide them with updates on the status of their Support Request.