CVS Health®

Return Ready™ by CVS Health® Reporting Tool
Quick Start Guide

This guide is designed to help you navigate the CVS Health® Return Ready™ reporting tool and access the Return Ready dashboards.
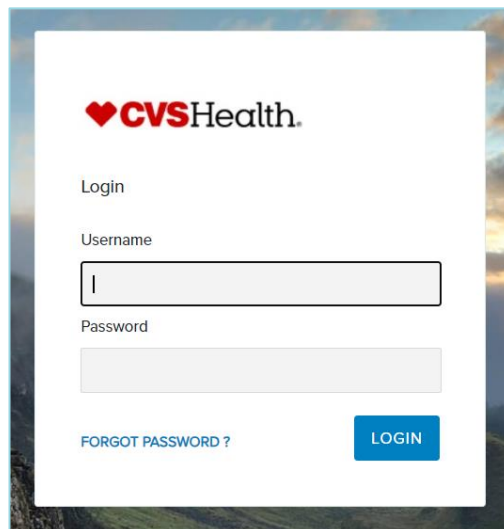
Part 1: Navigating the CVS Health® Return Ready™ reporting tool

CVS Health®

## Navigating the CVS Health® Return Ready™ reporting tool

Signing in

1. Access the Return Ready product using the following URL:
    https://reports.cvshealth.com.
2. Type your Username and Password provided by your CVS Health point of contact.
3. Click Sign In.

Note: The first time you sign in, you will be asked to reset your password. Please follow the password requirements provided on the screen.
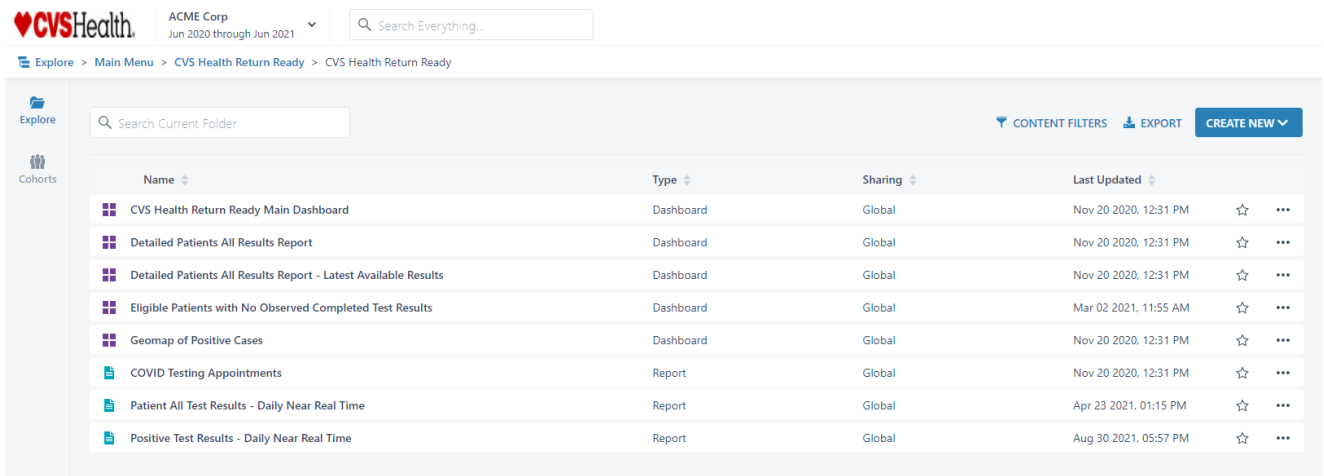
Accessing your COVID-19 Dashboards

After logging in, you will be directed to the explorer view with a folder titled "CVS Health Return Ready." To access your reports, double-click on this folder twice.
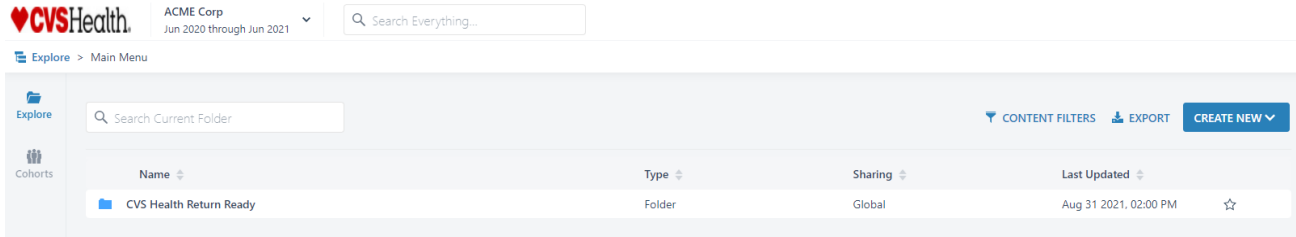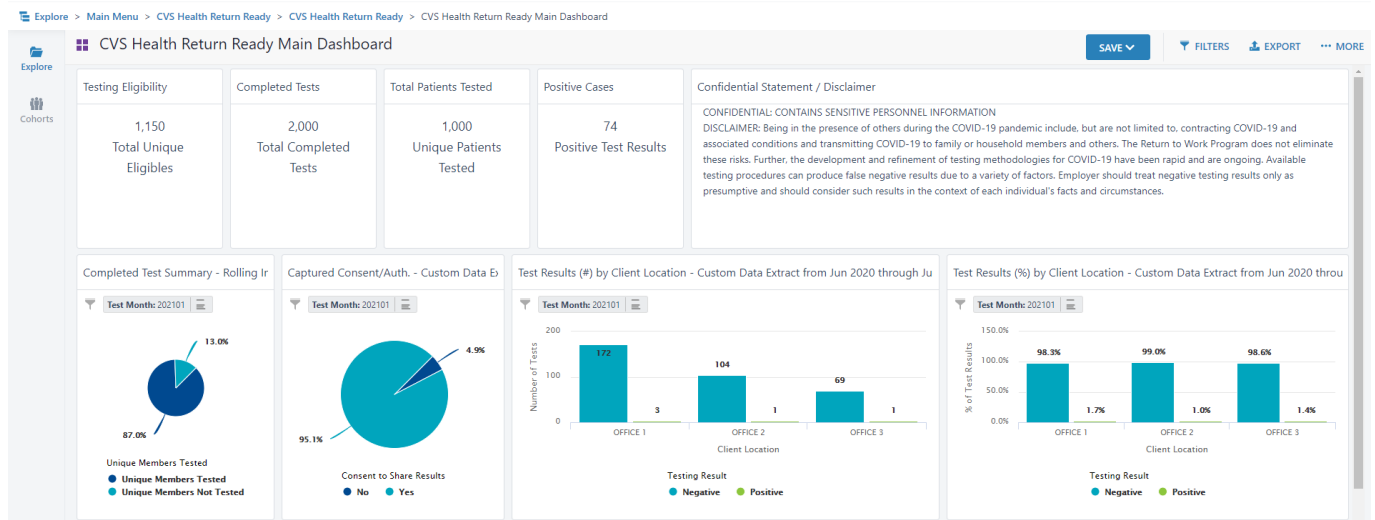

Once you open the folder, you will see the following eight standard reports and dashboards, plus any additional personal/group share reports:
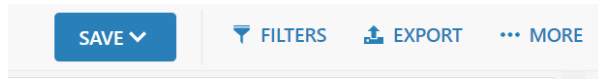
Running your COVID-19 Dashboards

To run a report, simply double-click on the title of the report. This will open the report in your current browser tab.
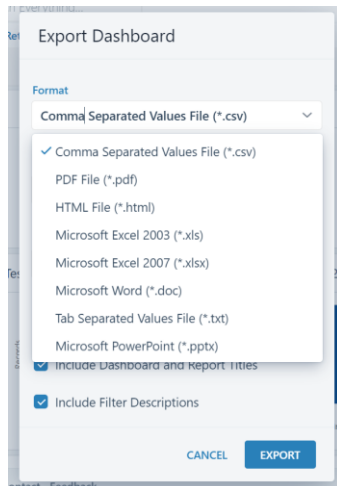

Exporting your COVID-19 Dashboards

To export a report, click on the "EXPORT" button in the top right corner of the screen.

An overlay window will pop up asking what format you would like. Select your desired format and click "EXPORT." Your file will pop up in the lower left-hand corner of the screen.

Note: If your file does not pop up, make sure that your "pop ups" are not blocked.

Optional Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA), sometimes called Two-Factor Authentication (2FA), is an extra layer of security designed to prevent someone from accessing your account even if they have your password. This functionality will provide an extra layer of protection for your sensitive healthcare data. Your organization may require MFA to be active for you to access the reporting portal.

This extra security measure requires identity verification using a randomized 6-digit code provided via Google Authenticator on your mobile device. To Set-up, please follow the instruction below.

Download Google Authenticator

1. On your mobile device, open Google Play or the Apple App Store.

2. Download Google Authenticator. resembles the multi-gray circle prior to downloading.
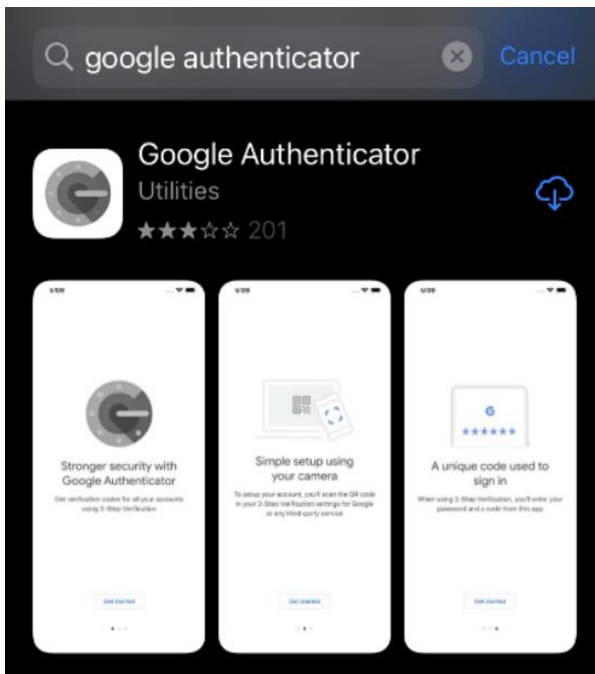
Initial Setup

1. Open Google Authenticator on your mobile device.

2. Next, go to the reporting tool login screen and enter your Username and Password and click Login.

3. Open Google Authenticator and scan the QR image. Alternatively, if you cannot scan, enter the provided code.

4. A validation code will display in the application under the appropriate login.

5. In the reporting tool, enter your unique validation code into the field.

Note: When the validation code is about to expire, it will flash red and blink. You may want to wait for a new code to be generated.

6. Enter your password that you use to login to the reporting tool.

7. Click Enable2FA.

8. If successful, a confirmation message will display. At this point, you can continue your session or logout and setup MFA/2FA for any additional logins.

9. To add additional logins in Google Authenticator, click on the plus sign in the

lower right corner of the utility.

10. For future login sessions, you will be prompted to enter a validation code provided on

your mobile device via Google Authenticator.

Using MFA/2FA

1. After initially enabling the security measure, your login will utilize this additional security

measure for future logins.

2. Go to your login page and enter your Username and Password and click Login.

3. Open Google Authenticator to access the 6-digit validation code for the appropriate

login and enter it into the field for the reporting too