

COVID-19 Data Clearinghouse

Jurisdiction Portal User Guide



F49516-02
April 2022



COVID-19 Data Clearinghouse Jurisdiction Portal User Guide,

F49516-02

Copyright © 2021, 2022, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Documentation accessibility	iv
Diversity and Inclusion	iv

1 Get started

Introduction	1-2
Vaccination record processing	1-2
Two-factor authentication	1-3
Activate your account with a QR code	1-3
Activate your account without a QR code	1-5
Sign in to Jurisdiction Portal	1-8
Manage multiple jurisdictions	1-9
Sign out of Jurisdiction Portal	1-10
Jurisdiction Portal	1-10
Provide feedback	1-11
Contact support	1-11

2 Manage vaccination records

Review the Dashboard	2-2
Report display options	2-3
Create private File Load Transactions reports	2-4
Manage vaccination file uploads	2-4
Requirements to upload files	2-4
Upload vaccination records	2-5
File upload status information	2-6
Manage vaccination file downloads	2-6
Requirements to download files	2-7
Download vaccination records	2-7
Search for vaccination records	2-8
Download CVRS vaccination records	2-8

Preface

This preface contains the following sections:

- [Documentation accessibility](#)
- [Diversity and Inclusion](#)

Documentation accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

Get started

The United States Centers for Disease Control (CDC) COVID-19 Data Clearinghouse application manages the collection and processing of COVID-19 vaccination records. Data Clearinghouse provides Jurisdiction Portal for organizations that collect COVID-19 vaccination records to upload and download vaccination records to the CDC.

- [Introduction](#)
COVID-19 Data Clearinghouse provides Jurisdiction Portal as a tool for authorized users to upload COVID-19 vaccination records to Data Clearinghouse databases. You can also download your records from Data Clearinghouse databases if authorized.
- [Vaccination record processing](#)
Jurisdictions upload COVID-19 vaccination records with Jurisdiction Portal to the COVID-19 Data Clearinghouse. The non-redacted database stores complete vaccination records, while the redacted database stores records with personal identifiable information (PII) redacted.
- [Two-factor authentication](#)
To ensure security, Jurisdiction Portal uses two-factor authentication (TFA) codes when you sign in. TFA ensures the security of Jurisdiction Portal by requiring all users to enter something they know (their passwords) and something they have (TFA codes) before they can access the system.
- [Activate your account with a QR code](#)
Once you receive your Jurisdiction Portal Welcome email, you can activate your account by setting a password and scanning a QR code with a mobile app during the account activation process.
- [Activate your account without a QR code](#)
Once you receive your Jurisdiction Portal Welcome email, you can activate your account by setting a password and requesting your two-factor authentication (TFA) code in an email instead of scanning a QR code with a mobile device.
- [Sign in to Jurisdiction Portal](#)
Jurisdiction Portal uses two-factor authentication (TFA) to ensure secure access when uploading COVID-19 vaccination records. Once you activate your account, use your mobile device or email to access your TFA code.
- [Manage multiple jurisdictions](#)
If you work at multiple jurisdictions, you can switch views to work with vaccination records at other jurisdictions.
- [Sign out of Jurisdiction Portal](#)
Jurisdiction Portal automatically signs you out of the system after a set amount of time (for example, 1-8 hours). Once that time expires, you need to sign in again using two-factor authentication. But, you can sign out at any time.
- [Jurisdiction Portal](#)
Jurisdiction Portal includes a Home page with links to portal pages where you can monitor your activity, upload files, download files, and display records successfully uploaded to the CDC.

- [Provide feedback](#)
Jurisdiction Portal includes a way to provide feedback directly to your organization's headquarters at any time.
- [Contact support](#)
The CDC provides all user support for Jurisdiction Portal.

Introduction

COVID-19 Data Clearinghouse provides Jurisdiction Portal as a tool for authorized users to upload COVID-19 vaccination records to Data Clearinghouse databases. You can also download your records from Data Clearinghouse databases if authorized.

Authorized users work for jurisdictions. A jurisdiction is a CDC-recognized organization that collects COVID-19 vaccination records including:

- Agencies of states and other geographical entities
- Federal agencies
- Healthcare organizations
- Pharmacy networks

To protect personal identifiable information (PII), Jurisdiction Portal displays only show redacted data, even if you are authorized to work with non-redacted data.

Vaccination record processing

Jurisdictions upload COVID-19 vaccination records with Jurisdiction Portal to the COVID-19 Data Clearinghouse. The non-redacted database stores complete vaccination records, while the redacted database stores records with personal identifiable information (PII) redacted.

Data Clearinghouse processes records in different ways depending on the jurisdiction settings. For example, your jurisdiction settings may process the records in one of the following ways after you upload them to Data Clearinghouse:

- Validates and processes records to store complete (full) vaccination records in the non-redacted database.
- Validates and processes records to store redacted (PII removed) vaccination records in the redacted database.
- Validates and processes records to store complete vaccination records in the non-redacted database and redacted versions of the records in the redacted database.
- Stores files of vaccination records in object storage only without validation or processing.
- Validates vaccination records and sends details on any errors (if found) only.

Upload file and vaccination record processing follows this workflow:

1. You upload a file through Jurisdiction Portal containing requests to do one of the following: add records, change records, or delete records. Your jurisdiction administrator sets the permissions on the options you can use in Jurisdiction Portal.
2. Data Clearinghouse validates that it can read each record in the upload file and logs a *validation error* for each failed read.

3. Data Clearinghouse processes the valid records. If it finds an error while processing a record, it logs a *processing error*.
4. For each error-free record, Data Clearinghouse stores it in the specified database or databases or simply returns error information for validation only users.
5. Jurisdiction Portal collects data in reports to help you track successful and failed uploads, validation and processing errors, and other information.

When ready, the CDC automatically exports records to the CDC IZ Data Lake (IZDL), if authorized by the jurisdiction. Authorized users can access the IZDL COVID-19 vaccination records. The IZDL export is a separate process from the Data Clearinghouse workflow.

**Note:**

Only records from the redacted database can be exported to IZDL.

Two-factor authentication

To ensure security, Jurisdiction Portal uses two-factor authentication (TFA) codes when you sign in. TFA ensures the security of Jurisdiction Portal by requiring all users to enter something they know (their passwords) and something they have (TFA codes) before they can access the system.

A TFA code is also known as a one-time code because it changes or expires within a set amount of time to ensure no one can guess it.

You can access your TFA code for Jurisdiction Portal by scanning a QR code with Google Authenticator or Microsoft Authenticator on your mobile device. From then on, you only open the mobile app to access your TFA code when you sign in. If you do not want to use your mobile device, you can choose to receive your TFA code in an email during the sign in process. For example, if your location does not permit cell phones, you can use the email method. But, you must use a TFA code to sign in to Jurisdiction Portal.

For details on activating your account with a TFA code, see one of the following topics:

Activate your account with a QR code

Once you receive your Jurisdiction Portal Welcome email, you can activate your account by setting a password and scanning a QR code with a mobile app during the account activation process.

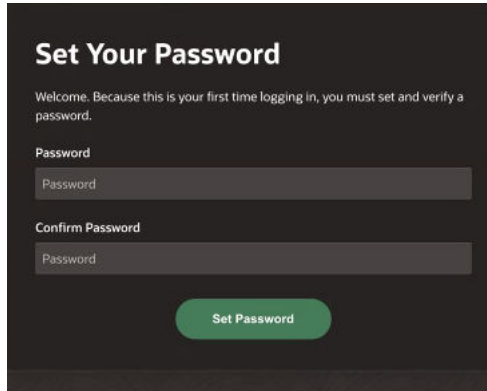
To scan the QR code, you must download the Google Authenticator or Microsoft Authenticator app to your phone or tablet. You only need to scan the QR code once. From then on, Google Authenticator or Microsoft Authenticator generate a new TFA code for your account each time you need it. You must leave the app on your phone to open it and access a new TFA code each time you sign in to Jurisdiction Portal.

 **Note:**

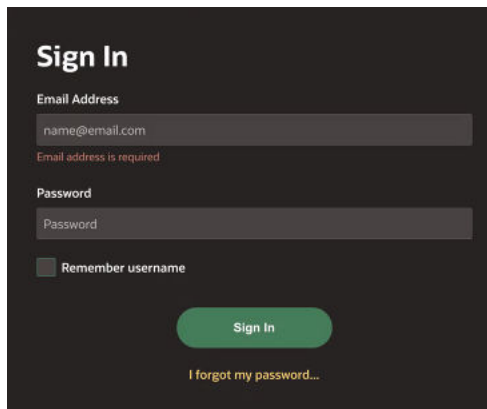
If you cannot or do not want to use your mobile device to scan the QR code, you can skip the scanning step and receive your TFA code through an email message. For details on activating your account with a TFA code in an email, see [Activate your account without a QR code](#).

To activate your account and scan a QR code to see your TFA code:

1. Locate the Welcome email message sent to you from Jurisdiction Portal.
2. Select **Activate Account** from the email to open the Set Your Password page in Jurisdiction Portal:



3. Enter the password you want to use for your account and confirm it. Use a password with eight characters that includes one uppercase letter, one special character, and one number (for example, aBcd_ef1).
4. Select **Set Password** to open the Sign In page:



5. Enter your email address (same as the address used for the Welcome email) and the password you created. Select **Sign In** to open the Two-Factor Authentication (TFA) page.
6. On your mobile device, open Google Authenticator or Microsoft Authenticator.

 **Note:**

If you need to download the app, open the store used to download applications on your phone or tablet. Search for the Google Authenticator or Microsoft Authenticator app and download it. For example, open the App Store for an iPhone or Google Play Store for an Android phone. Once you download Google Authenticator or Microsoft Authenticator, keep it on your phone to access a TFA code each time you log in. (If you use Google Authenticator, you can click the link at the bottom of the page to watch the video.)

7. In Google Authenticator or Microsoft Authenticator, tap **Scan a QR Code**. When prompted, allow access to your camera.
8. Hold your phone up to the QR code on your screen so the camera can focus and automatically scan the code. (You do not take a picture.) You should see the QR code come up on your camera screen as it focuses.
9. Once scanned, you see a six-digit code appear in Google Authenticator or Microsoft Authenticator. You also see the name of the Jurisdiction Portal application and your user name.

For security, this code changes approximately every 30 seconds.
10. Enter the six-digit code shown in your mobile app into the Two-Factor Authentication (TFA) field in Jurisdiction Portal.
11. Select **Continue** to authenticate and open Jurisdiction Portal.

The next time you sign in, you just enter your email address, password, and the TFA code shown in Google Authenticator or Microsoft Authenticator.

Activate your account without a QR code

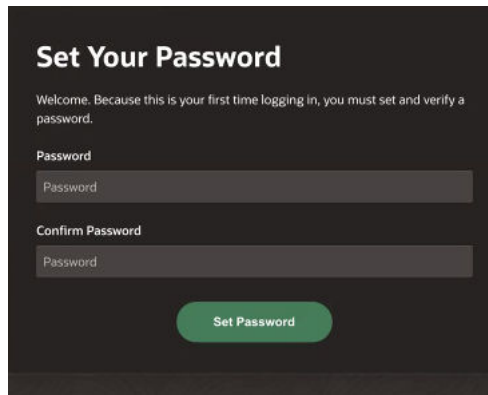
Once you receive your Jurisdiction Portal Welcome email, you can activate your account by setting a password and requesting your two-factor authentication (TFA) code in an email instead of scanning a QR code with a mobile device.

 **Note:**

If you want to scan a QR code to receive a TFA code when you activate your account, see [Activate your account with a QR code](#).

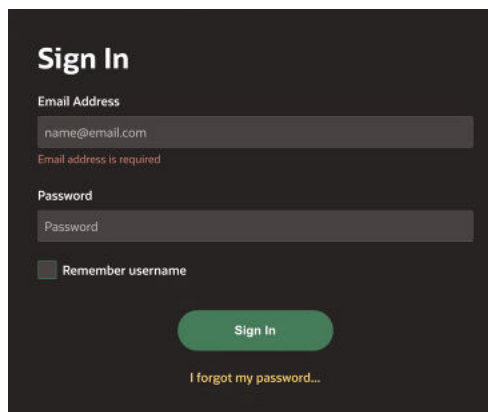
To activate your account without scanning a QR code:

1. Locate the Welcome email message sent to you from Jurisdiction Portal.
2. Select **Activate Account** from the email to open the Set Your Password page:



The screenshot shows a dark-themed form titled "Set Your Password". Below the title is a welcome message: "Welcome. Because this is your first time logging in, you must set and verify a password." There are two input fields: "Password" and "Confirm Password", both containing the placeholder text "Password". At the bottom of the form is a green button labeled "Set Password".

3. Enter the password you want to use for your account and confirm it. Use a password with eight characters that includes one uppercase letter, one special character, and one number (for example, aBcd_ef1).
4. Select **Set Password** to open the Sign In page:



The screenshot shows a dark-themed form titled "Sign In". It has two input fields: "Email Address" with the placeholder "name@email.com" and a red error message "Email address is required" below it; and "Password" with the placeholder "Password". There is a checkbox labeled "Remember username" which is currently unchecked. At the bottom is a green button labeled "Sign In" and a link "I forgot my password..." below it.

5. Enter your email address (same as the address used for the Welcome email) and the password you created. Select **Sign In** to open the Two-Factor Authentication (TFA) page.
6. Ignore the QR code shown and select **Click Here** in the message box under the **Continue** button to send the email to your account. This opens the Two-Factor Authentication (TFA) page for email users:

Two-Factor Authentication (TFA)

Welcome back to the CDC Jurisdiction Portal. Open **Google Authenticator** or **Microsoft Authenticator** on your cell phone. Next, enter the 6 digit code you see in **Google Authenticator** or **Microsoft Authenticator** into the field below and click **Continue**.

Enter your TFA Code

Continue

Prefer to have a code sent to your email instead? [Click Here](#)

7. Locate the message from `noreply@covid19.oracle.com` in your email and open it. It contains your six-digit TFA code. This code expires in approximately 30 minutes.

Two-Factor Authentication (TFA)

An message with a code has been sent to your email address. Once you receive it, enter the 6 digit code into the field below and click **Continue**.

Enter your TFA Code

[Back](#) **Continue**

8. Enter the six-digit code you see in your email into the Two-Factor Authentication (TFA) field in Jurisdiction Portal.
9. Select **Continue** to authenticate and open Jurisdiction Portal.

The next time you sign in with your account, just enter your email address, password, select the option to get a new TFA code in an email, and enter the code.

Sign in to Jurisdiction Portal

Jurisdiction Portal uses two-factor authentication (TFA) to ensure secure access when uploading COVID-19 vaccination records. Once you activate your account, use your mobile device or email to access your TFA code.

If you did not activate your account yet, see [Activate your account with a QR code](#) or [Activate your account without a QR code](#).

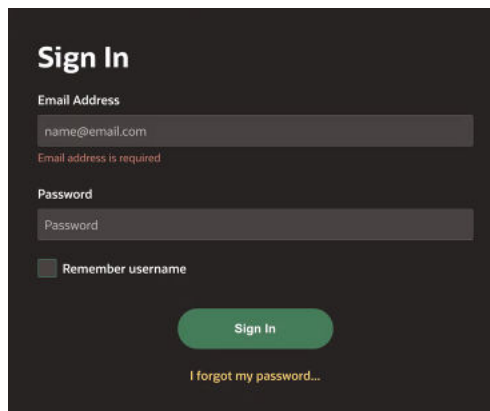
⚠ Caution:

Jurisdiction Portal administrators set the permissions for Jurisdiction Portal users. If you cannot sign in, you do not have permission to perform the task.

To sign in (after activating your account):

1. Open Jurisdiction Portal by navigating to the URL provided to you by your administrator in your browser to access the Sign In page.

The Sign In page appears.



✎ Note:

Select **I forgot my password** if you need to reset your password. You see a prompt to enter your email address. Check your mailbox for the message from Jurisdiction Portal and follow the prompts to reset your password.

2. Enter your email address and password. Then select **Sign In** to open the Two-Factor Authentication (TFA) page:

Two-Factor Authentication (TFA)

Welcome back to the CDC Jurisdiction Portal. Open **Google Authenticator** or **Microsoft Authenticator** on your cell phone. Next, enter the 6 digit code you see in **Google Authenticator** or **Microsoft Authenticator** into the field below and click **Continue**.

Enter your TFA Code

Continue

Prefer to have a code sent to your email instead? [Click Here](#)

3. Do one of the following:
 - If you use Google Authenticator or Microsoft Authenticator on your mobile device to obtain a TFA code, open the app to see the six-digit code for Jurisdiction Portal.
 - If you use email to get your TFA code, select **Click Here** at the bottom of the dialog box. Check your inbox for the message. It contains your TFA code. The code expires within 30 minutes.
4. Enter the six-digit code in the Two-Factor Authentication (TFA) field in Jurisdiction Portal. Then select **Continue** to open Jurisdiction Portal.

 **Note:**

If you can access more than one location, the Select a Jurisdiction page opens for you to select the location where you want to work. See [Manage multiple jurisdictions](#).

Manage multiple jurisdictions

If you work at multiple jurisdictions, you can switch views to work with vaccination records at other jurisdictions.

If you can access multiple jurisdictions, you see a prompt to choose a jurisdiction after signing in. You can choose to work with data from all your clients, or just one jurisdiction. You can switch jurisdictions at any time while signed in by selecting the name of the jurisdiction you want to view from the top of the page (next to Feedback).



Note:

If you do not see the jurisdiction that you need to view, send a message to your CDC Data Clearinghouse administrator.

To manage multiple locations:

1. To the right of the banner, locate the name of the jurisdiction you want to work in and select it. (Your current location appears with a building icon.) For example:



2. On the Change Jurisdiction to page, select the jurisdiction where you want to work or choose **All Clients** to see data from all your authorized jurisdictions.

The Home page opens with details for the jurisdiction you chose.

Sign out of Jurisdiction Portal

Jurisdiction Portal automatically signs you out of the system after a set amount of time (for example, 1-8 hours). Once that time expires, you need to sign in again using two-factor authentication. But, you can sign out at any time.

To sign out of Jurisdiction Portal:

- Locate your user name (email address) on the right side of the banner and select **Sign Out** from the menu.

Jurisdiction Portal

Jurisdiction Portal includes a Home page with links to portal pages where you can monitor your activity, upload files, download files, and display records successfully uploaded to the CDC.

Jurisdiction Portal pages:

- **Dashboard:** Displays interactive graphs showing weekly summaries of file load status and CVRS records added to Data Clearinghouse databases. The interactive File Load Transactions report displays detailed information on the record transactions for each file upload attempt. See [Review the Dashboard](#).
- **Upload Files:** Links to the Upload Action page where you upload your files. The page also contains the Upload Files report that displays information about uploaded files. See [Manage vaccination file uploads](#)
- **Download History:** Links to the Download Files page where you can download previously uploaded files or Data Clearinghouse database records. The page also contains the Download History report that provides details of file downloads. See [Manage vaccination file uploads](#).
- **Vaccination Report:** Displays a report of successfully uploaded vaccination records in Data Clearinghouse databases. See [Search for vaccination records](#).

Provide feedback

Jurisdiction Portal includes a way to provide feedback directly to your organization's headquarters at any time.

If you encounter an error in Jurisdiction Portal, please send feedback so that we can correct the issue. Your feedback is associated with your name and location.

1. Make sure that you are on the page or pop-up that is most closely related to your feedback.

The feedback mechanism records the page that you are on, and your support team can better help you if they know the product area that you are providing feedback for.

2. From the top of the page, click **Feedback**.
3. In the **Experience** section of the **Feedback** dialog box, select a facial expression that captures your experience (smile = Good, Neutral = Okay, Sad = Bad).
4. In the **Feedback Type** section, select one of the following options:
 - **Comment:** You need help or want to provide a suggestion or opinion.
 - **Bug:** An error occurred or the application did not function in the way you expected.
5. In the **Feedback** section, enter information about your suggestion, issue, or opinion.

 **Note:**

Do not include any personally identifiable information (PII) in your feedback.

6. Do one of the following: Select **Submit**.
 - If you do not need to include a screen shot, select **Submit**.
 - If you want to include a screen shot to provide more details, select **Submit and Add Screenshot**. Drag and drop your saved screen shot (without PII) to the drop area or click the area to browse and upload it. Select **OK**. You see a green check mark to indicate that you successfully added your screen shot and submitted your feedback.

Your organization headquarters receives the feedback.

Contact support

The CDC provides all user support for Jurisdiction Portal.

To obtain technical support, contact your CDC Data Clearinghouse administrator.

2

Manage vaccination records

Use Jurisdiction Portal to add vaccination records, update records, delete records, and download your records from Data Clearinghouse.

- [Review the Dashboard](#)
Use the Dashboard to see graphs and data that track uploaded files and the vaccination record transactions contained in those files. For example, you can see data on successful and failed vaccination record transactions.
- [Report display options](#)
You can change the display of Jurisdiction Portal reports using options found on the Actions menu. Available report display options vary for each report.
- [Create private File Load Transactions reports](#)
You can modify the default Upload File report and save it as a private report for your use.
- [Manage vaccination file uploads](#)
Use the Upload Files page to upload files of vaccination records and track your upload files with the report.
- [Requirements to upload files](#)
The files you upload to Jurisdiction Portal need to conform to content, file format, and record format rules.
- [Upload vaccination records](#)
You can upload a file of new record requests, change record requests, or delete record requests.
- [File upload status information](#)
The portal reports contains status information for files uploaded through the portal, the synchronous APIs, and the asynchronous APIs.
- [Manage vaccination file downloads](#)
You use the Download History page to download records from raw files your jurisdiction uploaded or your processed records from Data Clearinghouse databases. The Download History report provides details of all downloaded files.
- [Requirements to download files](#)
You can download unprocessed or processed records after you obtain an additional permission from your administrator.
- [Download vaccination records](#)
From the Download History page, you can download vaccination records from jurisdictions you are authorized to work for.
- [Search for vaccination records](#)
You use the Vaccination Report page to select a date range and download matching CVRS records from Data Clearinghouse databases that originated in your jurisdiction. The page displays the redacted version of the CVRS records.
- [Download CVRS vaccination records](#)
You use the Vaccination Report page to download CVRS vaccination records that originated in your jurisdiction and match the specified date range.

Review the Dashboard

Use the Dashboard to see graphs and data that track uploaded files and the vaccination record transactions contained in those files. For example, you can see data on successful and failed vaccination record transactions.

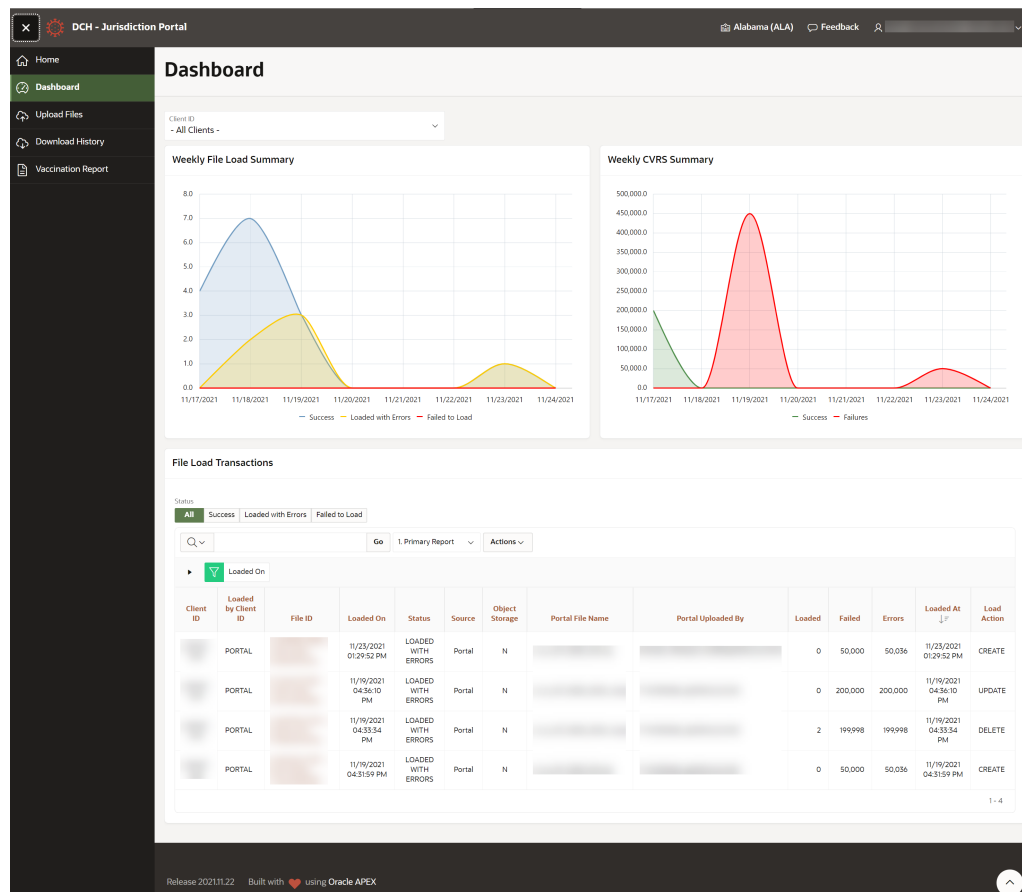


Table 2-1 Dashboard elements

Element	Description
Client ID	When set to All Clients, the Dashboard displays the combined activity from all your authorized jurisdictions. When set to a specific jurisdiction, the Dashboard displays only the activity from that jurisdiction.

Table 2-1 (Cont.) Dashboard elements

Element	Description
Weekly File Load Summary	<p>This interactive graph tracks the status of files uploaded during the past week. Each point on the graph indicates the number of files uploaded on that date. The three graph lines separate the files by result:</p> <ul style="list-style-type: none">• Successful uploads• Uploads with record errors• Failed uploads <p>Hover over a label at the bottom of the graph to bring one of the graph lines into focus. Select a label to toggle that graph line on or off.</p>
Weekly CVRS Summary	<p>The interactive Weekly CRVS Summary graph tracks the number of CVRS record transactions that succeeded or failed to upload to Data Clearinghouse in the past week. Each point on the graph indicates the number of record transactions routed to Data Clearinghouse on that date. The two graph lines segregate the files into successful transactions and failed transactions. Hover over a label at the bottom of the graph to bring one of the graph lines into focus. Select a label to toggle that graph line on or off.</p>
File Load Transactions	<p>Use the File Load Transactions report to see information about file uploads and information about the vaccination records in those files. For information on status codes from this report see File upload status information.</p>

Report display options

You can change the display of Jurisdiction Portal reports using options found on the Actions menu. Available report display options vary for each report.

The Oracle Application Express (Apex) platform provides the report display options in the Actions menu. See the [Oracle Application Express End User's Guide: Using the Column Heading Menu](#) for more information on all report options.

Options include:

- **Columns:** add or delete columns and change their order.
- **Filter:** drill down into the data. For example, you can specify a date range on a date column.
- **Data:** change the sort order.
- **Format:** change the number of rows per page.
- **Chart, Group By, and Pivot:** view the data in a different way.

The next time you sign in to the portal, you see the standard report layout. You may have permission to create private reports for the Dashboard report (File Load Transactions). See [File upload status information](#).

Create private File Load Transactions reports

You can modify the default Upload File report and save it as a private report for your use.

The portal has a default Upload File report called Primary Report. You can modify this report with the Actions menu during your portal session. If you want to save this modified report for later use, you can save it as a private report.

To create a private report:

1. If you currently have no private reports, use the **Actions** menu options to create the report you want to save.

Alternatively, if you currently have private reports, you can select either the Primary Report or one of your private reports from the **Report** menu next to the **Actions** menu as a starting point. The portal adds the **Report** menu to your view only after you create your first report.

2. When you complete your new report, select **Actions > Report > Save Report**.
3. From the dialog box, enter the report name in the **Name** field, and a short **Description**.
4. Select **Apply**.

You see the new report in the Report menu next to the **Actions** menu. The last report you view in a session becomes the report you see when you start your next portal session.

Manage vaccination file uploads

Use the Upload Files page to upload files of vaccination records and track your upload files with the report.

The **Upload Files** page contains:

- Access to the Upload Action page where you upload files.
- The Upload Files report on the file upload and the complete Data Clearinghouse Web Service Response. The Upload Status column includes notification of the current in-process phase for asynchronous uploads.

Acceptable vaccination records must use valid file formats, data formats, and be uploaded in files containing only a single record type: new, change, or delete requests.

Requirements to upload files

The files you upload to Jurisdiction Portal need to conform to content, file format, and record format rules.

Jurisdiction Portal requires that each upload file include only one type of record. Upload file content types include:

- **New records:** The file contains vaccination records that do not currently exist in Data Clearinghouse databases. If the file contains existing records, Data Clearinghouse logs a processing error for each one.
- **Changed records:** Contains existing vaccination records with updated data. If the file contains records that do not match an existing record, Data Clearinghouse logs a processing error for each one.
- **Delete record requests:** Contains records that uniquely identify existing vaccination records to delete. If the file contains requests that do not match an existing record, the system logs a processing error for each one.

 **Note:**

Records deleted in error can be restored by re-uploading the file that created the records.

Jurisdiction Portal accepts batch (text) files.

Jurisdiction Portal accepts vaccination records in the upload file with the following payloads (data format):

- **CVRS:** The CDC COVID-19 Vaccine Reporting Specifications is the native format of Data Clearinghouse databases.
- **HL7:** The Health Level Seven (HL7) format is an industry standard for sharing information between medical applications. Data Clearinghouse processes the HL7 data to create CVRS records.

In Jurisdiction Portal, you can choose to upload CVRS records synchronously or asynchronously.

Synchronous uploads use a persistent connection between your computer and Data Clearinghouse that ends only when the upload completes. Both CVRS and HL7 records can only be uploaded synchronously.

Asynchronous uploads for CVRS records communicate without the need for a persistent connection. Thus a failure during the upload process need not be a fatal flaw. Asynchronous uploads are useful for large file uploads. This upload type provides more status information than synchronous uploads. The status information indicates the processing stage of asynchronous uploads. You can view this information in the Upload Status column of the Upload File report while Data Clearinghouse processes the asynchronous upload. See [File upload status information](#).

Upload vaccination records

You can upload a file of new record requests, change record requests, or delete record requests.

To upload a file of vaccination record requests:

1. Navigate to the **Upload Files** page.
2. Select **Upload** in the upper-right corner. The Upload Action page opens.
3. Select the record type contained in the upload: **Add New**, **Update**, or **Delete**.
4. In the dialog box, select the **Client ID** for the upload file.

5. For **Payload Type**, select either **CVRS**, **CVRS Async**, or **HL7**.
For information on payload types, see [Requirements to upload files](#).
6. Select the **File** field to open the standard **File Open** window. Locate and select your upload file.
7. Select **Upload**.
See [File upload status information](#) for a description of the status values in the Upload Files report.

When the file completes processing, Jurisdiction Portal adds the upload information to the Upload File Transactions and File Upload reports.

File upload status information

The portal reports contains status information for files uploaded through the portal, the synchronous APIs, and the asynchronous APIs.

The File Uploads report Upload Status column uses the following status values for all upload types:

Table 2-2 File Uploads report Upload Status values

Upload type	Status	Description
All	COMPLETED	The upload job is done.
All	MAX ROWS	The file exceeded the row limit per file upload. The upload was not processed.
All	FAILED TO LOAD	The file could not be uploaded.
All	ERROR	See the Web Services Response Message column in the File Uploads report for more detail.
Asynchronous	QUEUED	The job is in the Async request job queue but not yet processed.
Asynchronous	DE-QUEUED	The job has moved to processing.
Asynchronous	VALIDATING	The job is currently in the validation processing phase.
Asynchronous	PROCESSING	The job is in the data processing phase, which takes the most time.

Manage vaccination file downloads

You use the Download History page to download records from raw files your jurisdiction uploaded or your processed records from Data Clearinghouse databases. The Download History report provides details of all downloaded files.

The Download History page contains:

- Access to the **Download Files** dialog box where you can select the records you want to download.
- The Download History report that contains details about all vaccination record downloads.

Requirements to download files

You can download unprocessed or processed records after you obtain an additional permission from your administrator.

Jurisdiction Portal can download the following types of files from Data Clearinghouse:

- **Processed, non-redacted CVRS:** This file format contains records from the non-redacted Data Clearinghouse database that originated from a single jurisdiction.
- **Processed, redacted CVRS:** This file format contains records from the redacted Data Clearinghouse database that originated from a single jurisdiction.
- **Raw CVRS:** This file format contains non-redacted, unprocessed CVRS records from files uploaded by a single jurisdiction. In other words, you download the records uploaded to Data Clearinghouse in their unprocessed state.
- **Raw HL7:** This file format contains non-redacted, unprocessed HL7 records from files uploaded by a single jurisdiction. In other words, you download the records uploaded to Data Clearinghouse in their unprocessed state.

Jurisdiction Portal users who need to download vaccination records request an additional permission from their CDC Data Clearinghouse administrator. Jurisdiction Portal permissions are called *scopes*. Two scopes determine the kinds of records you can download:

- **EXPORT_NON_REDACTED scope:** You require this scope to download all format types.
- **EXPORT_REDACTED scope:** You require this scope to download only the **Processed, Redacted CVRS** format type.

Download vaccination records

From the Download History page, you can download vaccination records from jurisdictions you are authorized to work for.

To select records for download:

1. Navigate to the **Download History** page.
2. Select the **Download** button in the top-right corner.

The **Download Files** dialog box appears.

3. From the Download Files dialog box, in the **Date Type** section, specify the target date or date range.

The portal uses dates based on the UTC time zone. You can download records uploaded on the current day after a one day delay for processing.

4. Select the download type **Format**. If you have the EXPORT_REDACTED scope, you can only select the **Processed, Redacted CVRS** format. If you have the EXPORT_NON_REDACTED scope, you can select any format.
5. Select the **Client ID** of the jurisdiction that uploaded the records you want to download.
6. Select the **Download** button.

The Download dialog box provides status messages or requests for you to alter your query if the record count is zero or too large. Select the **Back** button to alter your query.

7. Select the **Close** button to return to the Download History page.

The portal saves your report to your Downloads folder on your computer.

 **Note:**

The Download History report uses the same status codes as the File Uploads report. See [File upload status information](#). The report also has an optional column named **Message** that you can add to the report using the **Actions > Columns** dialog.

Search for vaccination records

You use the Vaccination Report page to select a date range and download matching CVRS records from Data Clearinghouse databases that originated in your jurisdiction. The page displays the redacted version of the CVRS records.

You can do the following from the Vaccination Report page:

- Select records from a specific date range and download matching records from Data Clearinghouse.
- Review the downloaded, redacted CVRS records matching the specified date range.

Download CVRS vaccination records

You use the Vaccination Report page to download CVRS vaccination records that originated in your jurisdiction and match the specified date range.

To select records for download:

1. Navigate to the **Vaccinate Report** page.
2. Enter the **From Date** and the **To Date** or use the pop-up calendars to select the dates.
3. Select the **Apply** button.

Jurisdiction Portal requests matching records that originated in your jurisdiction from the Data Clearinghouse databases.

If no records or too many records (more than 100,000) match your date range, change your date range or apply filters to reduce the number of records. To apply filters, select the **Actions** menu, and then select **Filters**.

 **Note:**

Dates are based on the UTC time zone and there is a one day delay before you can download today's uploaded records.