Secure Inbox
Quick Guide

2022-2023

Updated April 20, 2023

Prepared by Cambium Assessment, Inc.

Secure Inbox

The Cambium Assessment, Inc. (CAI) suite of online systems includes the Secure Inbox feature that is integrated with the following assessment systems: Test Information Distribution Engine (TIDE), Authoring, and Reporting System (CRS). The Secure Inbox serves as a central repository for protected documents uploaded by administrators (such as state personnel) or shared between users, data files exported by users from within a CAI online assessment system, and hotline alerts that can be accessed by users from the Idaho Portal page or from most CAI online assessment systems. When you export a file from a CAI system, you will receive an email notification when the file is available in the Secure Inbox, allowing you to continue working while the file exports. This message is sent to the email address associated with your TIDE account, not to the Secure Inbox. The file is only available in the Secure Inbox.

Each user's Secure Inbox is personal to them and not shared among other users. Users can easily manage the files in their Secure Inbox. The files are categorized into different tabs to allow users to view non-archived and archived files. Users can also search for files by keyword. Files are listed in the order in which they were created. The file creation and file expiration dates appear, if applicable. The number of days remaining until a file expires is also displayed next to a file. Users can also choose to download, archive, or delete files.

Student Alert Responses will be sent directly from the CAI testing systems to the School Coordinators (SCs) of the student. These responses are flagged as containing text in which schools may want to discuss with the student. Topics that may be flagged by the CAI test systems may include, but are not limited to, student references to:

- Suicide

- Criminal activity

- Alcohol or drug use

- Extreme depression

- Extreme violence

- Sexual assault or physical abuse

- Self-harm or intent to harm others

- Neglect

- Bullying

Alert Responses for students that have dual enrollment will be sent to the Secure Inbox of the School Coordinators where they are enrolled, regardless of which school the student was testing when they provided the response that was flagged.

Access the Secure Inbox

You can access the Secure Inbox directly through a link in your Portal or through TIDE, Authoring, and CRS.

Access from the Idaho Portal

Users can access their Secure Inboxes directly from their Idaho Portal.

1. Navigate to the Idaho Portal, and select either ELA/Literacy and Math Assessments, Science Assessments, or Idaho Alternate Assessments.

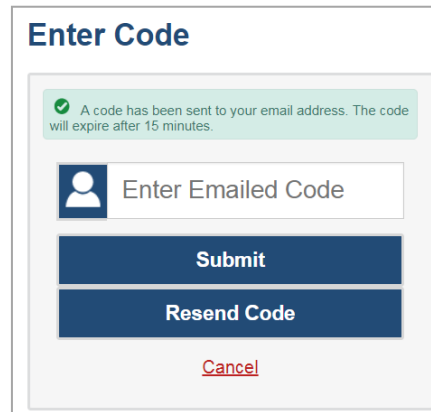2. Select the **Secure Inbox** card (Figure 1).

Figure 1. Secure Inbox Card
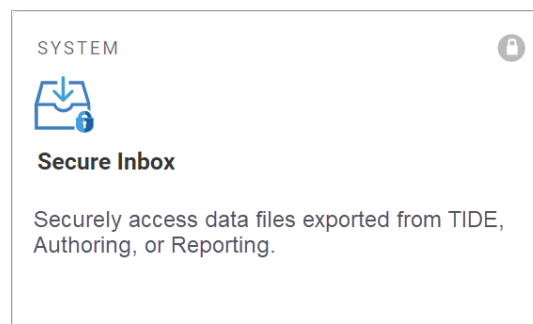
3. The *Login* page appears (Figure 2). Enter your email address and password.

Figure 2. Login Page

4. Click **Secure Login**.

   a. If you have not logged in using this browser before, or if you have cleared your browser cache, the ***Enter Code*** page appears (Figure 3) and an email containing an authentication code is sent to your address.

      i. In the *Enter Emailed Code* field, enter the emailed code.

      ii. Click **Submit** to view the ***Secure Inbox*** page.

      You must use the authentication code within fifteen minutes of the email being sent. If the code has expired, click **Resend Code** to request a new code.
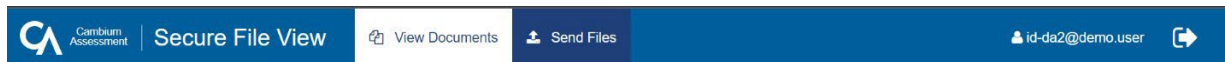
Figure 3. Enter Code Page

1. If the **Terms and Conditions** page appears, you should review the terms on this page and click **Accept** to proceed.

2. The **Secure Inbox** pop-up window appears ([Figure 6](#)).

3. When finished working with secure files, select ⬛ to log out of the Secure Inbox ([Figure 4](#)).

Figure 4. Secure Inbox Header

Access from a CAI Online Assessment System

Since the Secure Inbox is integrated with the CAI online assessment systems that allow users to export files, it can be easily accessed from the banner within these systems.

1. Log in to TIDE, Authoring, or the Reporting System.

2. From the banner, select **Secure Inbox** ([Figure 5](#)).
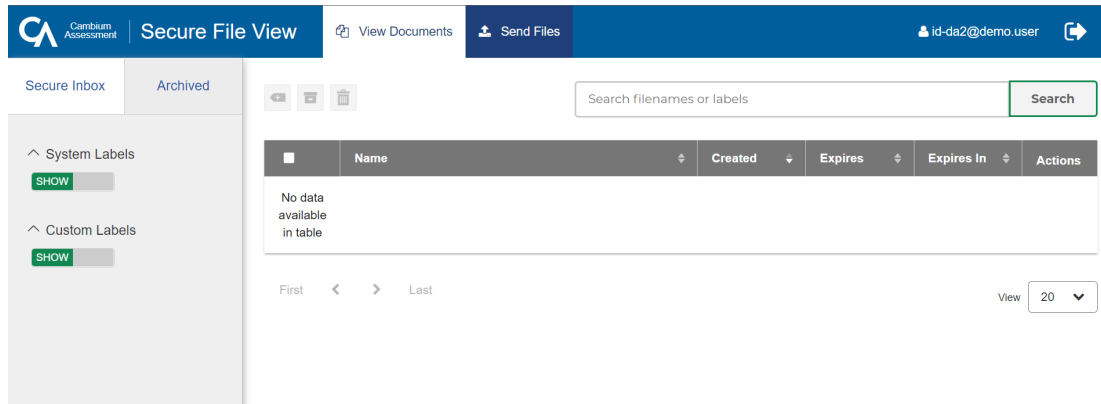
Figure 5. Banner from TIDE
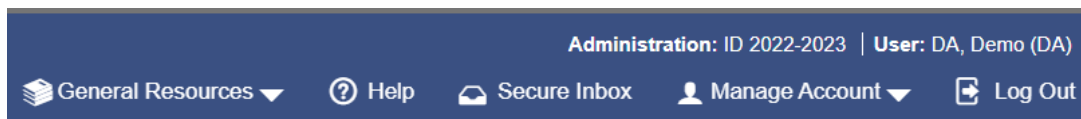
3. The **Secure Inbox** pop-up window appears ([Figure 6](#)).

4. When finished working with secure files, close the **Secure Inbox** pop-up window by selecting ❌.

View Documents

1. The *Secure Inbox* page displays the *View Documents* tab by default (Figure 6).

Figure 6. Secure Inbox – View Documents

2. *Optional*: On the **View Documents** page, select a file view from the available tabs:

    - **Secure Inbox**: This is the default view and displays all the files except for the ones that you have archived.

    - **Archived**: Displays the files that you have archived.

3. *Optional*: To filter the files by keyword, enter a search term in the text box above the list of files. The Secure Inbox displays only those files containing the entered file name.

4. *Optional*: To hide or display system labels, toggle HIDE / SHOW .

    - **System Labels:** Labels that appear next to messages in the Secure Inbox corresponding to which system the message came from. Example: 2022121_6452_ValidationLog.log TIDE

5. *Optional*: To hide files with a particular system label, unmark the checkbox for that system label.

6. *Optional*: To hide files with a particular custom label, unmark the checkbox for that custom label.

7. Do one of the following:

    - To download a file, select the file name.

    - To add a new custom label or apply an existing custom label to a file, select ⬅ after marking the checkbox for a file.

        - To apply a new custom label, mark the checkbox for the textbox, enter a new custom label in the text box, and select **Save New Label**.

        - To apply an existing custom label, mark the checkbox, enter an existing custom label in the text box, and select **Apply Label**.

    - To archive a file, select 🗄. To return a file to the Secure Inbox from the Archived tab, select 📥.

▪ To delete a file, select 🗑. Files exported to the Secure Inbox or archived can be deleted. Secure documents uploaded to the Secure Inbox by admin users cannot be deleted.

Send Files

You can send a file or files from the Secure Inbox to individual recipients by email address or to groups of recipients by user role. Sent files will appear in each recipient's Secure Inbox. You can send files from any system that allows you to access the Secure Inbox.
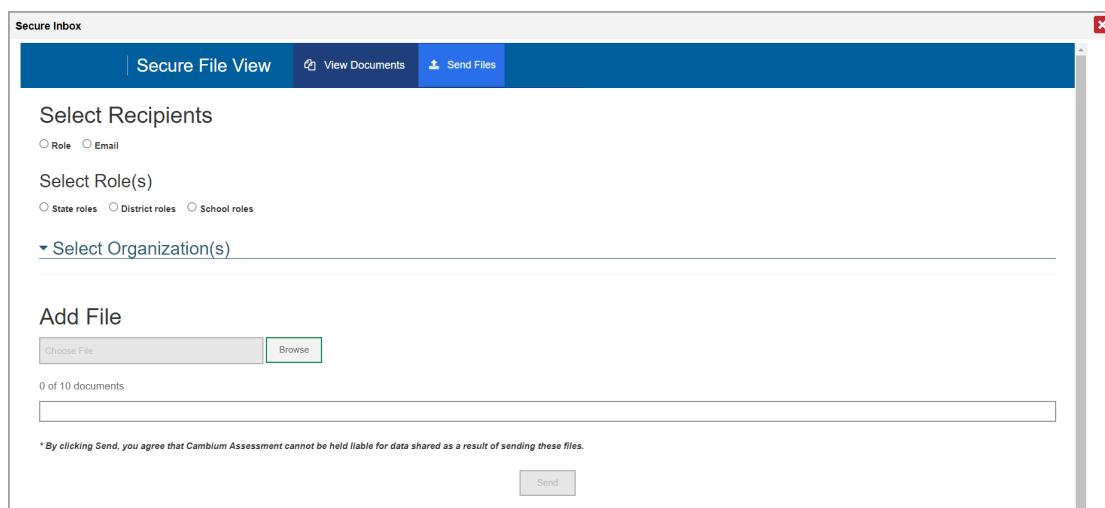
Only users who can access tasks under the Users menu in TIDE can send files.

Figure 7. TIDE User Tasks
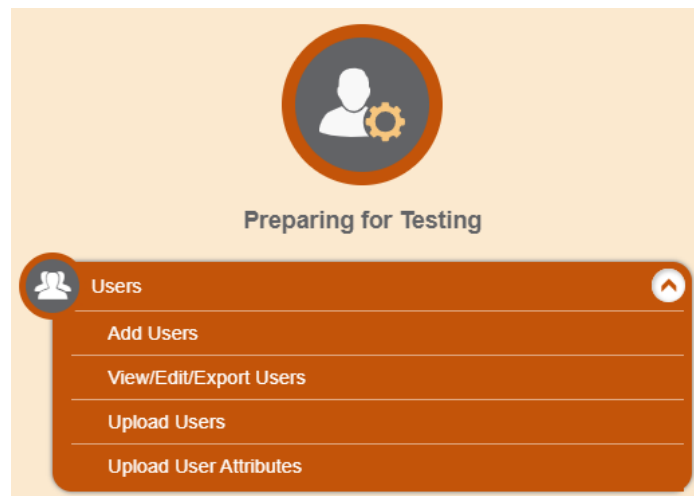
1. From the *Secure Inbox* window, select the **Send Files** tab. The ***Send Files*** page appears (Figure 8).

Figure 8. Secure Inbox – Send Files

2. Under *Select Recipients*, do one of the following:

   ▪ Select **Role** to send a file or files to a group of users by user role.

   ▪ Select **Email** to send a file or files to a single recipient by email address.

- If you select **Email**, skip to step 7.

3. Under *Select Role(s)*, select the role group to which you want to send a file or files. A drop-down list appears.

4. From the drop-down list, select the role(s) to which you want to send a file or files. You can choose **Select all** to send a file or files to all roles in the selected role group.

5. From the *Select Organization(s)* drop-down lists, select organizations that will receive the file(s) you send.

    These drop-down lists adhere to TIDE's user role hierarchy. For example, district-level users will be able to filter at their role level and below.

6. If you selected **Role** in step 2, skip this step. If you selected **Email** in step 2 enter the email address of the recipient to whom you wish to send a file or files.

    You can only enter one valid email address at a time.

7. To select a file or files to send, in the *Add File* field, select **Browse**. A file browser appears.

8. Select the file(s) you wish to send.

9. Select **Send**.

Files display in the Secure Inbox after you send them.